RSA NETWITNESS® PLATFORM

NetWitness Investigate – Benutzerhandbuch

für Version 11.2

Kontaktinformationen

RSA Link unter https://community.rsa.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme sowie Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Marken

Eine Liste der RSA-Marken finden Sie unter germany.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Lizenzvereinbarung

Drittanbieterlizenzen

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

Dell ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

Februar 2019

Inhalt

Wie funktioniert NetWitness Investigate?

NetWitness Investigate bietet die Datenanalysefunktionen, die in RSA NetWitness® Platform verfügbar sind, mit denen Analysten Paket-, Protokoll- und Endpunktdaten analysieren und mögliche interne oder externe Bedrohungen für die Sicherheit und die IP-Infrastruktur erkennen können.

Hinweis: In Version 11.1 und höher geben die Ansichten „Hosts“ und „Dateien“ einen Einblick in Endpunktdaten. Frühere Versionen bieten über einen eigenständigen NetWitness Endpoint-Server Zugriff auf Endpunktdaten.

Metadaten, Metaschlüssel, Metawerte und Metaentitäten

RSA NetWitness Platform prüft und überwacht den gesamten Datenverkehr in einem Netzwerk. Ein Servicetyp, ein Decoder, kümmert sich um die Aufnahme, Analyse und Speicherung der Pakete, Protokolle und Endpunktdaten, die über das Netzwerk übertragen werden.

Mit den konfigurierten Parsern und Feeds auf dem Decoder werden *Metadaten* erstellt, die Analysten zum Untersuchen der aufgenommenen Protokolle und Pakete verwenden können. Ein anderer Servicetyp, der als Concentrator bezeichnet wird, indiziert und speichert die Metadaten.

Die Metadaten liegen als *Metaschlüssel* und *Metawerte* für den Schlüssel vor. Beispielsweise ist `ip.src` ein Metaschlüssel, und eine IP-Adresse, die die Quelle des Datenverkehrs ist, ist als `ip.src` markiert. Wenn Sie Daten in Investigate anzeigen, sehen Sie den Metaschlüssel `ip.src` und alle IP-Adressen (Werte), die mit diesem Schlüssel markiert sind. Einige Metaschlüssel sind integriert, andere sind möglicherweise benutzerdefinierte Schlüssel, die vom Administrator definiert werden.

Metaentitäten sind ab Version 11.1 verfügbar. Eine *Metaentität* ist ein Alias, der die Ergebnisse aus anderen Metaschlüsseln zusammenfasst. Metaentitäten organisieren ähnliche Metaschlüssel in einem einzigen, einfacher zu verwendenden Metatyp. Einige Metaentitäten sind bereits standardmäßig enthalten und der Administrator kann benutzerdefinierte Metaentitäten erstellen. Analysten können eine Metaentität in einer Abfrage, einer Metagruppe, einer Spaltengruppe und einem Profil verwenden. Visualisierungen zu Parallelkoordinaten bieten keine Unterstützung für Metaentitäten. Administratoren können Metaentitäten verwenden, um ein Abfragepräfix zu definieren, das auf eine Benutzerrolle und einen Benutzer angewendet werden soll. Der *Konfigurationsleitfaden für Decoder* enthält zusätzliche Informationen zum Erstellen von Metaentitäten und zu ihrer Verwendung in Regeln.

Die Standardsprache der Core-Datenbank enthält beispielsweise eindeutige Metaschlüssel für IP-Quelle und IP-Ziel. Eine der integrierten Metaentitäten mit dem Namen `ip.all` stellt den kombinierten Satz aller IP-Quellen und IP-Ziele dar.

Analysten fragen in der Regel den Concentrator ab, um Bedrohungen zu erkennen. Der Concentrator verarbeitet Abfragen und wechselt erst dann zum Decoder, wenn eine vollständige Rekonstruktion von Sitzungen oder unverarbeiteten Protokollen erforderlich ist. ESA, Malware Analysis und Reporting Engine fragen auch den Concentrator ab, wo sie schnell alle relevanten Metadaten erhalten, die mit einem Ereignis verknüpft sind, und Informationen über das Ereignis erzeugen können, ohne zu jedem Decoder gehen zu müssen. In einigen besonderen Fällen können Analysten einen Decoder abfragen.

Hinweis: Während eine hybride Appliance die Concentrator-Funktion ausführen kann, benötigt eine einzelne Concentrator-Appliance eine größere Umgebung, für die wiederum mehr Bandbreite oder Ereignisse pro Sekunde (EPS) erforderlich sind. Die Concentrator-Appliance hat ein Speicherlayout mit Solid State Drives für den Index, das die Leseperformance steigert.

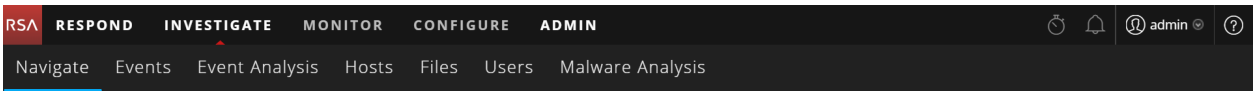
Auslöser für eine Ermittlung

Es folgen einige Beispiele für Auslöser einer Ermittlung:

- Sie erhalten Informationen von einem Drittanbieter zu einem neuen Active Directory-Hack. Öffnen Sie die Ansicht „Ereignisse“ und verwenden Sie dort diese Informationen, um eine Suche in all Ihren unverarbeiteten Active Directory-Protokolldaten der letzten 24 Stunden durchzuführen.
- Sie werden vom SOC-Manager gebeten, aufgrund der derzeitigen Beliebtheit von Pokemon Go diesbezügliche Malware zu finden. Öffnen Sie die Ansicht „Navigation“ und erstellen Sie dort eine Abfrage zur Suche einer HTTP-Sitzung unter Verwendung eines bestimmten Benutzer-Agent, der in Bezug zu der Schadsoftware steht, die er in einem Sicherheitsblog gefunden hat.
- Ein Incident-Experte eskaliert ein Ticket, das einige seltsame Indikatoren in Bezug auf einen Host zeigt. Öffnen Sie die Ansicht „Hosts“ und überprüfen Sie dort diesen Host, um spezifische Details zu finden.
- Sie suchen den nächsten Zero-Day-Angriff und navigieren in der Ansicht „Navigation“ durch Netzwerkmetadaten, um ungewöhnliche automatisierte Sitzungen zu finden, die aus dem Unternehmen heraus gelangen.
- Sie werden von Ihrem SOC-Manager gebeten, Informationen im Zusammenhang mit Benutzer `jarvis` zu finden, einem Mitarbeiter, der gerade entlassen wurde. Öffnen Sie die Ansicht „Hosts“ und führen Sie dort eine Abfrage für die letzte Woche nach diesem Benutzernamen durch.

Workflow einer Ermittlung

Analysten können von NetWitness Platform erfasste Daten untersuchen und umfassende Einblicke anhand von Informationen zu einem NetWitness Platform-Dashboard, einem NetWitness Respond-Incident bzw. einer Warnmeldung, einem von der NetWitness Platform Reporting Engine erstellten Bericht oder zu einer Drittanbieteranwendung gewinnen. Während einer Ermittlung können Analysten nahtlos zwischen den Ansichten im Modul „Ermittlungen“ navigieren: Ansicht „Navigation“, Ansicht „Ereignisse“, Ansicht „Ereignisanalyse“, Ansicht „Hosts“, Ansicht „Dateien“ und Ansicht „Malware Analysis“. Diese Abbildung zeigt die Untermenüs in NetWitness Investigate.



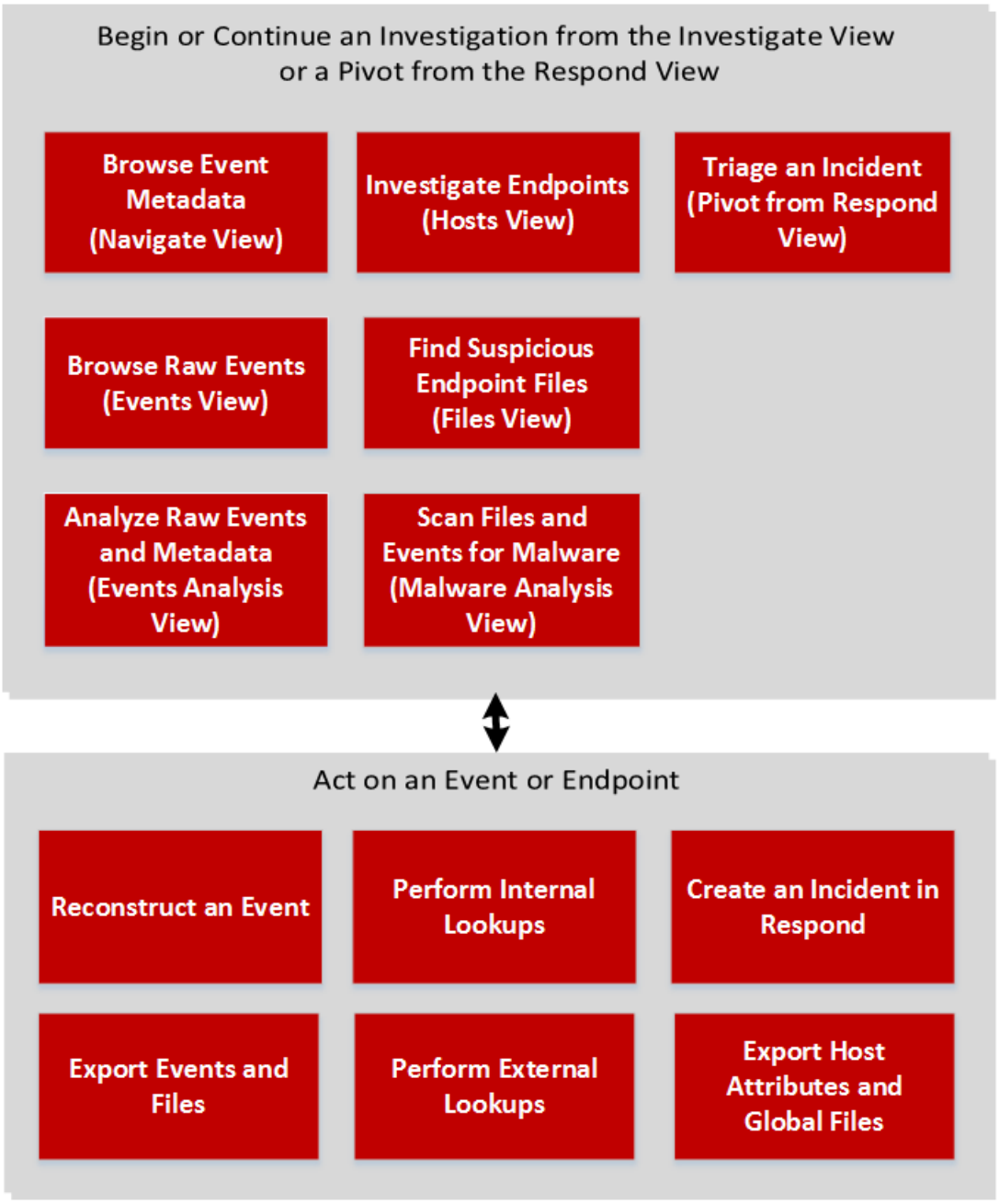
Hinweis: Die Ansichten „Dateien“ und „Hosts“ sind in Version 11.1 und höher verfügbar. Die Ansicht „Benutzer“ ist in Version 11.2 und höher verfügbar. Ein Benutzer benötigt spezifische Benutzerrollen und -berechtigungen, damit er Ermittlungen und Schadsoftwareanalysen in NetWitness Platform durchführen kann. Wenn Sie eine Analyseaufgabe nicht durchführen oder eine Ansicht nicht sehen können, muss der Administrator unter Umständen die für Sie konfigurierten Rollen und Berechtigungen anpassen.

Sie können aus dem Untermenü im Modul „Investigate“ und aus anderen Ansichten von „Investigate“ auf jede Ansicht zugreifen. Sie können auch direkt von NetWitness Respond aus in eine Investigate-Ansicht navigieren sowie direkt von NetWitness Investigate zu NetWitness Respond und in die eigenständige NetWitness Endpoint-Anwendung wechseln. Ihr Anwendungsbeispiel bestimmt den Ausgangspunkt für Ihre Ermittlung. Diese Tabelle enthält allgemeine Richtlinien zur Startansicht für verschiedene Anwendungsbeispiele.

Navigieren Sie zu ...	Schwerpunkt
Ansicht „Navigation“	Alle Metaschlüssel und Metawerte für Protokolle, Endpunkte und Pakete, die nach Metaschlüsseln gruppiert werden. Sie können durch die Daten navigieren, um Ergebnisse zu verfeinern, und dann zur Ansicht „Ereignisse“ oder zur Ansicht „Ereignisanalyse“ wechseln. Sie können auch Malware Analysis oder Live durchsuchen. Dies ist die Standardansicht in NetWitness Investigate. (Siehe Untersuchen von Metadaten in der Ansicht „Navigation“.)
Ansicht „Ereignisse“	Ereignisse werden geordnet nach Uhrzeit aufgelistet. Sie können das unverarbeitete Ereignis und die zugehörigen Metadaten sowie eine Rekonstruktion anzeigen und Ereignisse und Dateien herunterladen. Sie können zur Ansicht „Ereignisanalyse“ wechseln. (Siehe Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse“).
Ansicht „Ereignisanalyse“	Ereignisse werden geordnet nach Uhrzeit aufgelistet. Sie können alle Metaschlüssel und Metawerte für Protokolle, Endpunkte und Pakete anzeigen. Sie können das unverarbeitete Ereignis und die zugehörigen Metadaten sowie eine Rekonstruktion anzeigen, die nützliche Hinweise zur Identifizierung interessanter Punkte in einer Rekonstruktion bietet. Sie können zur Ansicht „Hosts“ navigieren, zur eigenständigen Endpoint-Anwendung wechseln, in Live nachschlagen und externe Suchen durchführen. Mit externen Suchen können Sie das Internet nach Metawerten durchsuchen, mit denen Sie interagiert haben, passive DNS-Informationen im Zusammenhang mit einer IP-Adresse bestimmen, feststellen, ob eine URL auf die schwarze Liste gesetzt wurde, sowie nach anderen Drittanbieter-Kontextintegrationen suchen. (Siehe Analysieren von Raw-Ereignissen und Metadaten in der Ansicht „Ereignisanalyse“).Analysieren von Raw-Ereignissen und Metadaten in der Ansicht „Ereignisanalyse“
(Version 11.1 und höher) Ansicht „Hosts“	Hosts, auf denen die NetWitness Endpoint Insights-Agents ausgeführt werden, werden aufgelistet. Für jeden Host können Sie Prozesse, Treiber, DLLs, (ausführbare) Dateien, Services und automatische Ausführungen sehen, die gerade aktiv sind, sowie Informationen in Bezug auf angemeldete Benutzer. Von der Ansicht „Hosts“ können Sie zu den Ansichten „Navigation“ und „Ereignisanalyse“ wechseln. (Siehe Untersuchen von Hosts.)
(Version 11.1 und höher) Ansicht „Dateien“	Eindeutige Dateien wie PE, Macho und ELF in Ihrer Bereitstellung werden aufgeführt. Für jede Datei können Sie Details wie Dateigröße, Entropie, Format, Firmenname, Signatur und Prüfsumme anzeigen. Von der Ansicht **Dateien** können Sie zu den Ansichten „Navigation“ und „Ereignisanalyse“ wechseln. (Siehe Untersuchen von Dateien.)

Navigieren Sie zu ...	Schwerpunkt
Ansicht „Malware Analysis“	Wenn Sie eine Malware Analysis-Appliance ausführen, können Sie Dateien automatisch oder manuell scannen und die Ergebnisse der vier Analysetypen anzeigen: Netzwerk, statisch, Community und Sandbox. Wenn eine Datei Schadsoftware ist, können Sie die Ansicht „Hosts“ öffnen und dort feststellen, welche Hosts die Datei heruntergeladen haben. (Siehe Durchführen von Schadsoftwareanalysen.)
(Version 11.2 und höher) Ansicht „Benutzer“	Mit NetWitness UEBA wird die Transparenz von riskantem Benutzerverhalten in Ihrem Unternehmen gewährleistet. Sie können eine Liste der Benutzer mit hohem Risiko und eine Zusammenfassung der wichtigsten Warnmeldungen für riskantes Verhalten für Ihre Umgebung anzeigen. Dann können Sie einen Benutzer oder eine Benachrichtigung auswählen und Details über das riskante Verhalten und eine Zeitleiste anzeigen, in der die Verhaltensweisen aufgetreten sind. Die Benutzer von NetWitness Platform, denen die Rollen „Administrator“ oder „UEBA-Analyst“ zugewiesen sind, haben Zugriff auf diese Ansicht. Weitere Informationen zu dieser Funktion finden Sie im *NetWitness UEBA – Benutzerhandbuch*.Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Jede Situation ist einzigartig in Bezug auf die Art der Informationen, die der Analyst sucht. Viele Untersuchungen beginnen in einer Ansicht und enden in einer anderen Ansicht, weil der Analyst etwas lernt und dann dieses Ergebnis mit einer anderen Fragestellung nachverfolgen muss. Diese Abbildung zeigt den allgemeinen Workflow einer Ermittlung.



Legen des Schwerpunkts auf Metadaten, Abfrage und Uhrzeit

Analysten verwenden NetWitness Investigate, um Ereignisse zu suchen, die den Workflow für die Reaktion auf Incidents voranbringen, und um strategische Analysen durchzuführen, nachdem ein anderes Tool ein Ereignis erzeugt hat. Beginnend in der Ansicht „Navigation“, „Ereignisse“ oder „Ereignisanalyse“:

- Sie beginnen mit der Ausführung einer Abfrage an einem Service für einen bestimmten Zeitbereich, filtern dann mithilfe von Metadaten eine Teilmenge der Ereignisse heraus, rekonstruieren oder analysieren ein Ereignis und wiederholen anschließend das Verfahren zum Rekonstruieren oder Analysieren eines anderes Ereignisses.
- Wenn Sie ein Ereignis finden, das eines genaueren Blicks bedarf, zeigen Sie den Kontext des Ereignisses an und entscheiden, ob Sie einen Incident erstellen oder das Ereignis zu einem Incident hinzufügen. Wenn Sie sich entscheiden, das Ereignis nicht zu einem Incident hinzuzufügen, führen Sie eine weitere Abfrage aus, um weitere Einblicke zu erhalten, womit Sie erneut am Anfang des Workflows beginnen.
- Wenn Sie verdächtige Aktivitäten oder Dateien auf einem bestimmten Host im Netzwerk erkennen, können Sie zusätzliche Informationen über den Host und den auf dem Host gefundenen Dateien in der Ansicht „Hosts“ und „Dateien“ oder auf einem eigenständigen NetWitness Endpoint-Server erfassen.
- Wenn Sie eine Datei oder ein Ereignis finden, das potenziell Malware enthält, können Sie einen Malware Analysis-Scan der Datei durchführen oder Malware Analysis öffnen und einen Scan des Service starten, in dem das Ereignis erkannt wurde.

Wenn zum Beispiel Befürchtungen in Bezug auf verdächtigen Datenverkehr mit dem Ausland bestehen, gibt der Metaschlüssel „Zielland“ Aufschluss über alle Ziele und Häufigkeit des Kontakts. Ein Drill-down in diese Werte ergibt die Einzelheiten des Datenverkehrs, wie etwa die IP-Adresse des Absenders und des Empfängers. Eine Überprüfung weiterer Metadaten kann Informationen über die Natur von zwischen den beiden IP-Adressen ausgetauschten Anhängen aufdecken.

Legen des Schwerpunkts auf die Endpunktanalyse

Analysten verwenden die Ansichten „Hosts“ und „Dateien“ zum Untersuchen oder Durchführen einer Analyse auf Hosts oder in Dateien mithilfe von Attributen wie IP-Adresse, Hostname, MAC-Adresse usw.

- Während einer Incident-Sichtung in der Ansicht „Reagieren“ überprüfen Sie die Schlüsselinformationen (z. B. Hostname, Dateiname) und zeigen Sie die Kontextmarkierungen an.
- Wechseln Sie zu „Ermittlungen“, um die Ansicht „Navigation“ zu öffnen. Wählen Sie die Metagruppe „Endpunktanalyse“ und überprüfen Sie die erstellten Metadaten.
- Zeigen Sie die Metadaten in der Ansicht „Ereignisanalyse“ an, um die Ereignisse zu analysieren. Wählen Sie die Option „Host ermitteln“ über den Bereich „Ereignis-Metadaten“ aus.
- Klicken Sie in der Ansicht „Hosts“ auf den Hostnamen, um die Übersicht der Endpunktdaten, Snapshots, Sicherheitskonfigurationen usw. anzuzeigen.
- Führen Sie einen Scan nach Bedarf aus, um die neuesten Informationen zu erhalten (sofern erforderlich).

- Suchen Sie in allen Snapshots nach einem bestimmtem Dateinamen, Pfad oder Hash, um die Suche einzuschränken.
- Überprüfen Sie die Prozesse, automatischen Ausführungen, Dateien, Bibliotheken, Treiber und Systeminformationen für eine weitergehende Untersuchung.
- Filtern Sie in der Ansicht „Dateien“ mithilfe einiger Indikatoren (z. B. Dateiname, Dateigröße, Entropie, Format, Firmenname, Signatur, Prüfsumme) nach Dateien und navigieren Sie zur Ansicht „Navigation“, um festzustellen, ob diese auf anderen Hosts im Netzwerk vorhanden sind.

Legen des Schwerpunkts auf Incidents und Warnmeldungen in NetWitness Respond

Ein Analyst, der in NetWitness Respond an einem Incident oder einer Warnmeldung arbeitet, kann diesen bzw. diese in NetWitness Investigate öffnen (Ansicht „Navigation“), um eine tiefergehende Analyse des Ereignisses oder der Warnmeldung durchzuführen.

- Der Workflow für die Reaktion auf einen Incident beginnt normalerweise in der Ansicht „Reagieren“, in der der Analyst, der einen Incident untersucht, Informationen zum Incident in NetWitness Investigate erfassen muss. Sie können den Mauszeiger über eine unterstrichene Entität in einem Incident oder einer Warnmeldung bewegen, z. B. über eine IP-Adresse, und dann die Aktion „Zu „Ermittlungen“ > „Navigation“ wechseln“ auswählen. Die Ansicht „Navigation“ öffnet sich und wird für die ausgewählte Entität gefiltert. Nachdem Sie in NetWitness Respond eine Ermittlung gestartet haben, werden definierte Metaschlüssel abgefragt und der Inhalt der erfassten Pakete, Protokolle und Endpunktereignisse in der Ansicht „Navigation“ angezeigt.
- Wenn Sie Ereignisse finden, die für den Incident relevant sind, können Sie diese zum Incident in Respond hinzufügen. Sie können auch einen neuen Incident in Respond basierend auf ein oder mehrere in Investigate gefundene Ereignisse erstellen.
- (Version 11.2 und höher) Aus der Ansicht „Incident-Details“ in Respond können Sie die Ansicht „Ereignisanalyse“ öffnen, um mehr Informationen zu einem Indikatorereignis anzuzeigen.

Ansichten in NetWitness Investigate

Dieser Abschnitt enthält eine kurze Beschreibung und ein Beispiel für jede Hauptansicht („Navigation“, „Ereignisse“, „Ereignisanalyse“, „Hosts“, „Dateien“ und „Malware Analysis“). Hier werden auch Ansichten erläutert, die zusätzlichen Kontext für gefundene Daten bieten: der Bereich „Kontextabfrage“ und die Ereignisrekonstruktion.

Ansicht „Navigation“

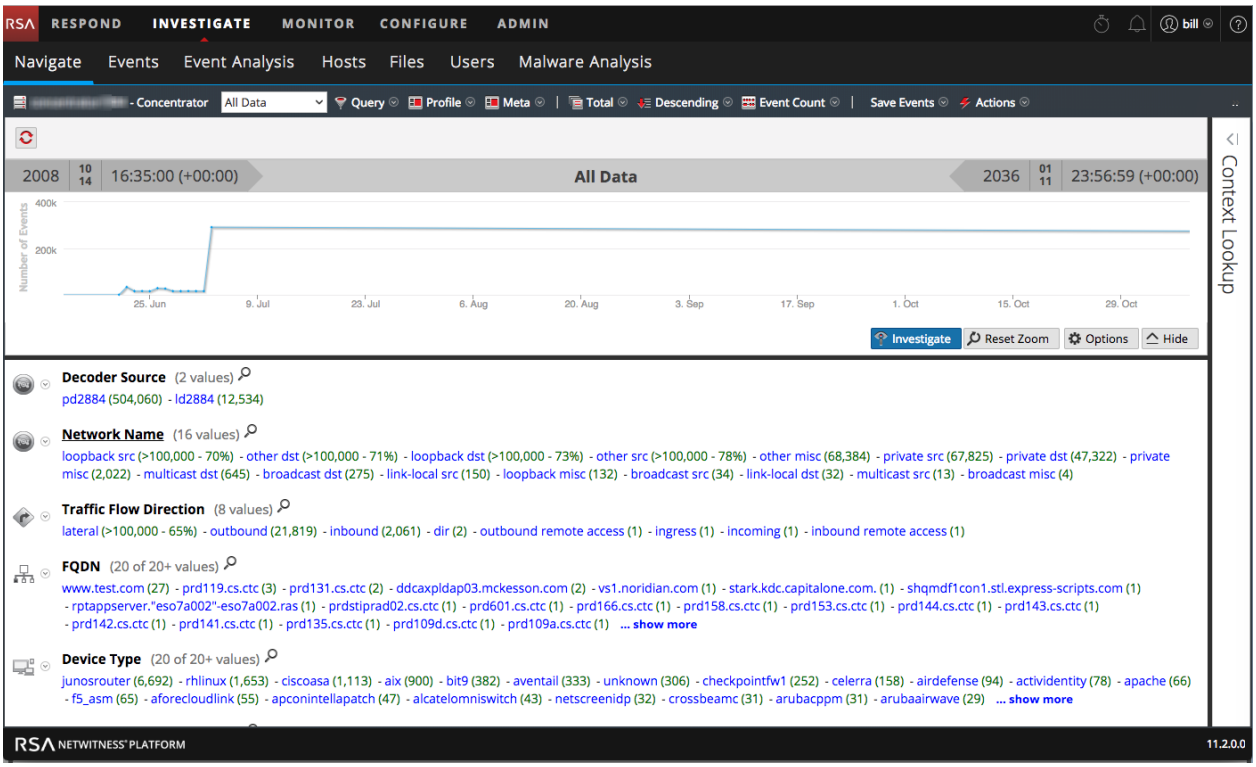
Die Ansicht „Navigation“ bietet die Möglichkeit, einen Drill-down vorzunehmen und die Inhalte von erfassten Paketen, Protokollen und Endpunktereignissen auf einem Broker, Concentrator oder Decoder abzufragen (obwohl die Untersuchung eines Decoder nicht üblich ist).

- Bei Auswahl eines Services werden die definierten Metaschlüssel für diesen Service abgefragt und die Werte werden zusammen mit der Anzahl der Ereignisse zurückgegeben. Wenn Sie auf einem

beliebigen Level auf einen Wert klicken, werden die Ergebnisse detailliert angezeigt.

- Sie können mit dem Context Hub für bestimmte konfigurierte Metaschlüssel wie IP-Adresse oder Hostname nach zusätzlichen Kontextinformationen rund um einen Wert suchen. Der zusätzliche Kontext kann Incidents, Warnmeldungen und andere Quellen umfassen, in denen der Wert erwähnt wurde.
- Die Ansicht „Navigation“ bietet auch eine sequenzielle Visualisierung der Daten auf einer Zeitachse. Hier können Sie einen ausgewählten Zeitraum vergrößern.

Diese Abbildung zeigt die Ansicht „Navigieren“.



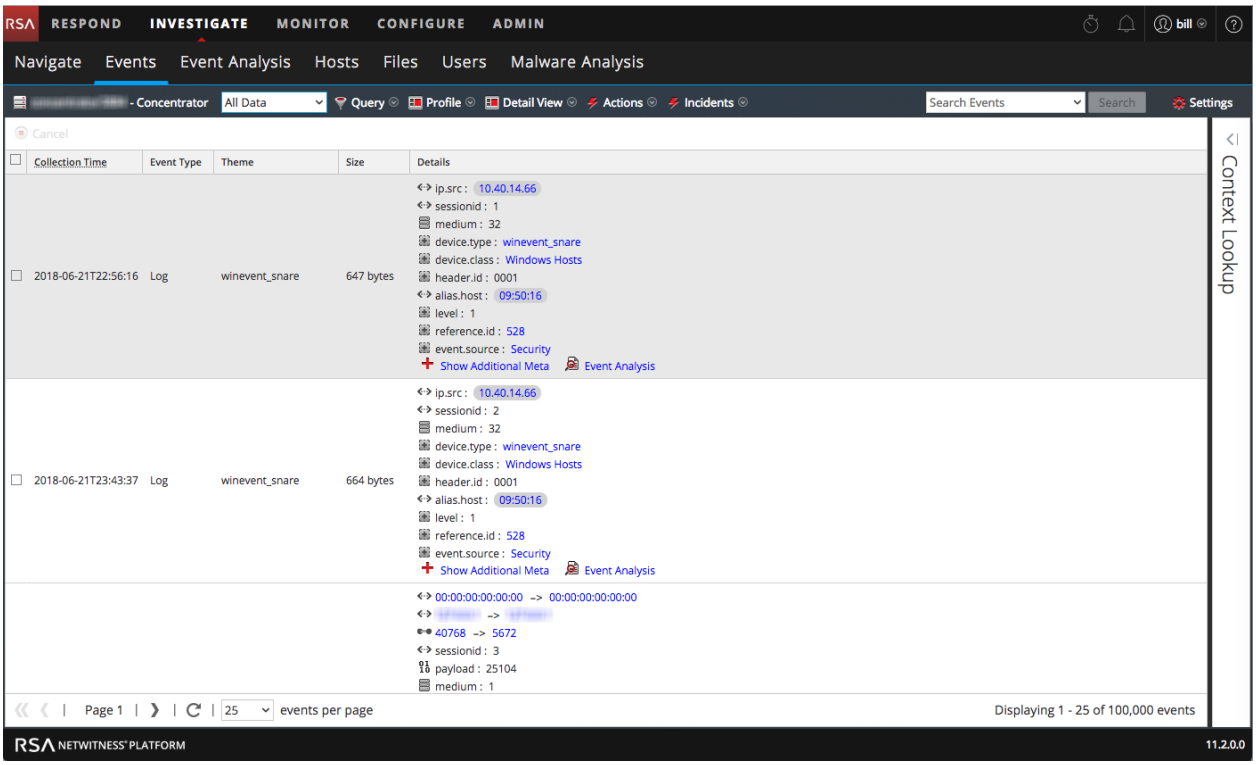
Ansicht „Ereignisse“

Die Ansicht „Ereignisse“ bietet eine Ansicht der Paket-, Protokoll- und Endpunktereignisse in Listenform, sodass Sie Ereignisse sequenziell anzeigen und sicher rekonstruieren können.

- Sie können die Ansicht „Ereignisse“ für einen Metawert öffnen, der in der Ansicht „Navigation“ angezeigt wird.
- Für Analysten ohne ausreichende Berechtigungen für die Navigation in einem Service ist die Ansicht „Ereignisse“ eine eigenständige Ermittlungsansicht, in der Analysten auf eine Liste von Netzwerk-, Protokoll- und Endpunktereignissen von einem NetWitness Platform Core-Service zugreifen können, ohne zuerst ein Drill-down durch Metadaten durchführen zu müssen.

- Die Ansicht „Ereignisse“ präsentiert Ereignisinformationen in drei Standardformaten: eine einfache Liste von Ereignissen, eine detaillierte Auflistung von Ereignissen und eine Protokollansicht.
- Sie können mit dem Context Hub für bestimmte konfigurierte Metaschlüssel wie IP-Adresse oder Hostname nach zusätzlichen Kontextinformationen rund um einen Wert suchen. Der zusätzliche Kontext kann Incidents, Warnmeldungen und andere Quellen umfassen, in denen der Wert erwähnt wurde.
- Sie können Ereignisse und zugehörige Dateien exportieren sowie einen Incident aus einem Ereignis erstellen.

Diese Abbildung zeigt die Ansicht „Ereignisse“.



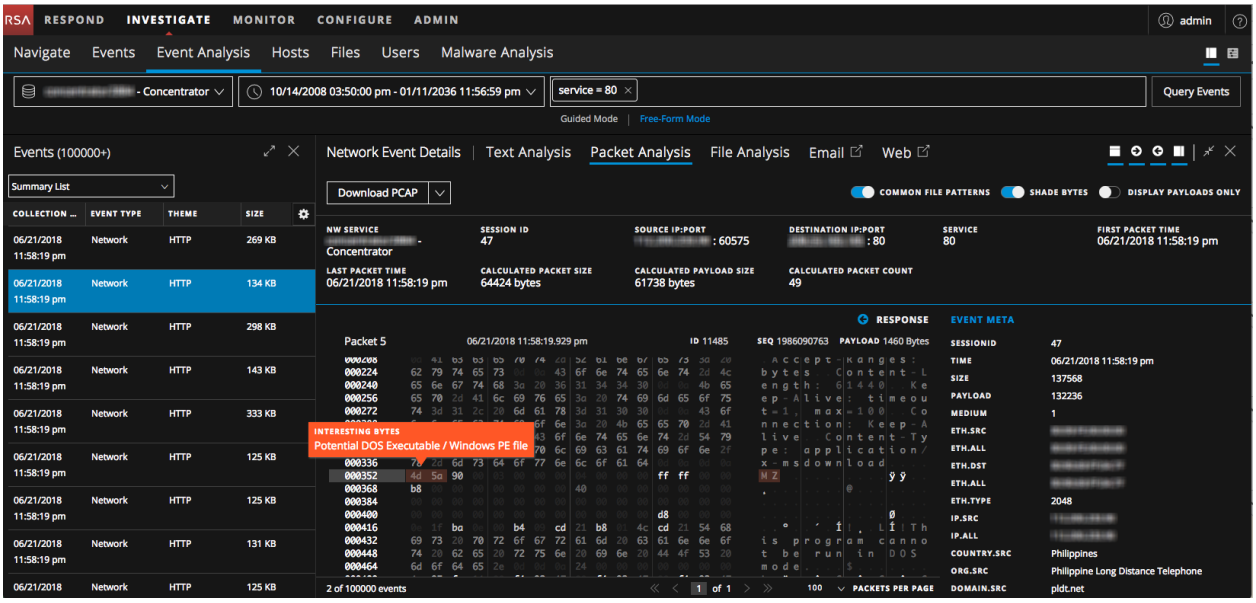
Ansicht „Ereignisanalyse“

Die Ansicht „Ereignisanalyse“ ist ein interaktives Tool, mit dem Analysten Pakete, Text, oder Dateien in einem Ereignis mit visuellen Hervorhebungen bestimmter Arten von Informationen anzeigen können. Je nach Typ der Rekonstruktion, z. B. Pakete, Text oder Dateien, sind unterschiedliche Informationen relevant.

- Sie können mit dem Context Hub für bestimmte konfigurierte Metaschlüssel wie IP-Adresse oder Hostname nach zusätzlichen Kontextinformationen rund um einen Wert suchen. Der zusätzliche Kontext kann Incidents, Warnmeldungen und andere Quellen umfassen, in denen der Wert erwähnt wurde.

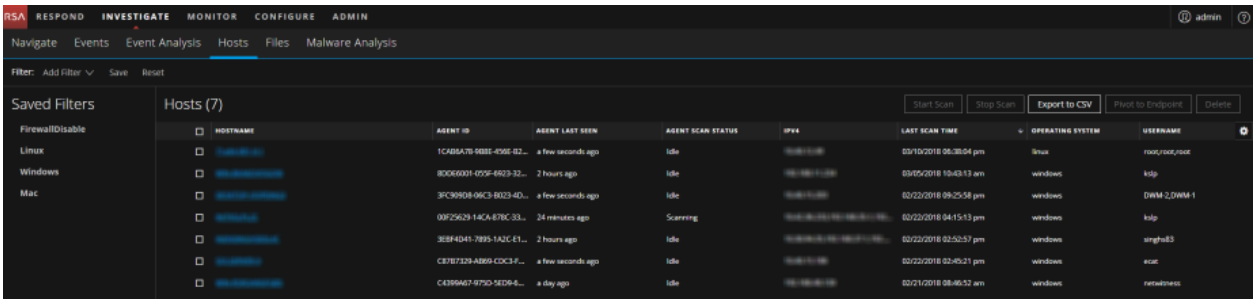
- Beim Anzeigen von Dateien können Sie diese in einem Zip-Archiv in Ihr lokales Dateisystem exportieren.
- Sie können Protokolle aus der Ansicht „Text“ herunterladen und Pakete aus der Ansicht „Paket“ exportieren.

Diese Abbildung zeigt ein Beispiel der Ansicht „Ereignisanalyse“.



Ansicht „Hosts“

In der Ansicht „Untersuchen > Hosts“ werden alle Hosts mit einem Agent aufgelistet. Standardmäßig werden die Hosts basierend auf der Zeit des letzten Scans aufgelistet, wobei die zuletzt gescannten Hosts in der Liste an oberster Position aufgeführt werden. In dieser Ansicht kann auch ein Drill-down in die Hostdetails durchgeführt werden. Dies ist ein Beispiel für die Ansicht „Hosts“.



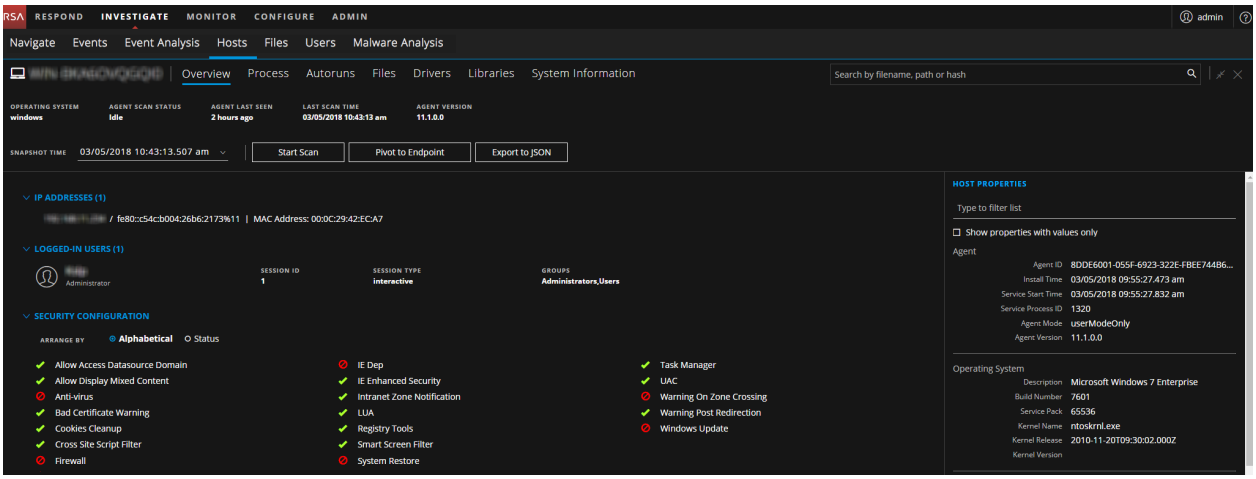
In dieser Ansicht können Sie:

- Hosts filtern und sortieren, um eine Host-Ermittlung zu erzielen, die Details des Hosts anzuzeigen und Hosts zu löschen.
- Die Hostattribute in eine CSV-Datei exportieren.
- Einen Scan für die ausgewählten Hosts starten oder stoppen.

- Zur Ansicht „Navigation“ oder „Ereignisanalyse“ wechseln, um den Host zu untersuchen.

Hinweis: Wenn in Ihrer Bereitstellung NetWitness Endpoint 4.4.0.2 oder höher installiert ist, werden die Hosts aufgeführt, auf denen der 4.4.0.2-Agent installiert ist. Sie können anhand der Agent-Version identifiziert werden. Weitere Informationen zum Untersuchen dieser Hosts finden Sie unter Untersuchen von NetWitness Endpoint 4.4.0.2 oder später Hosts.

Detaillierte Scanergebnisse für einen Host können Sie durch Anklicken des Hostnamens anzeigen. In dieser Abbildung ist ein Beispiel für die detaillierten Scanergebnisse auf der Registerkarte „Übersicht“ dargestellt.



Sie können Folgendes tun:

- In allen Snapshots suchen (die unterstützten Suchfelder sind „Dateiname“, „Dateipfad“ und „SHA-256-Prüfsumme“).
- Mehrere Snapshots anzeigen. Standardmäßig werden die Daten für den neuesten Snapshot angezeigt.
- Zusätzliche Hostinformationen auf den folgenden Registerkarten anzeigen: Übersicht, Prozesse, Automatische Ausführungen, Dateien, Treiber, Bibliotheken und Systeminformationen.
- Alle Kategorien von Endpunktdaten für den ausgewählten Host für einen bestimmten Snapshot im JSON-Format exportieren.

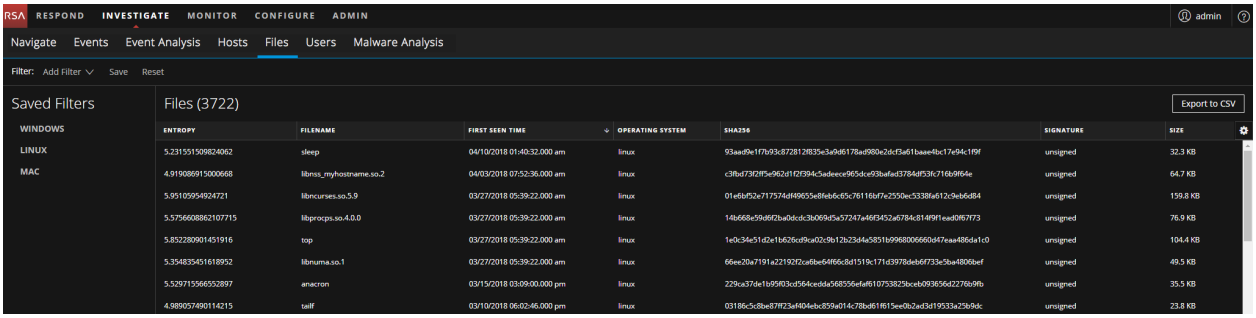
Ansicht „Dateien“

Die Ansicht „Dateien“ enthält eine Liste eindeutiger Dateien, die in Ihrer Bereitstellung gefunden wurden, sowie die zugehörigen Eigenschaften. Standardmäßig werden die Dateien basierend auf der Zeit des ersten Auftretens aufgelistet. Die folgenden Dateitypen, die in den Arbeitsspeicher geladen wurden, werden während des Scanvorgangs erfasst.

- Portable Executable (PE) (Windows): Hierbei handelt es sich um `exe`-, `dll`- und `sys`-Dateien. Sie können die folgenden Eigenschaften für jede Datei anzeigen: Prüfsumme, kompilierte Details, verschiedene Abschnitte in der Datei, importierte Bibliotheken und Details des Zertifikats (Signaturgeber, Fingerabdruck und Name des Unternehmens).

- Macho (Mac): Hierbei handelt es sich um App-Bundles, Dylibs und Kernel-Erweiterungen. Sie können die folgenden Eigenschaften für jede Datei anzeigen: Prüfsumme, verschiedene Abschnitte in der Datei, importierte Bibliotheken und Details des Zertifikats (Signaturgeber, Fingerabdruck und Name des Unternehmens).
- Executable and Linking Format (ELF) (Linux): Jede Datei enthält Informationen über die Prüfsumme, verschiedene Abschnitte in der Datei und importierte Bibliotheken.

Diese Abbildung zeigt ein Beispiel für die Ansicht „Dateien“.

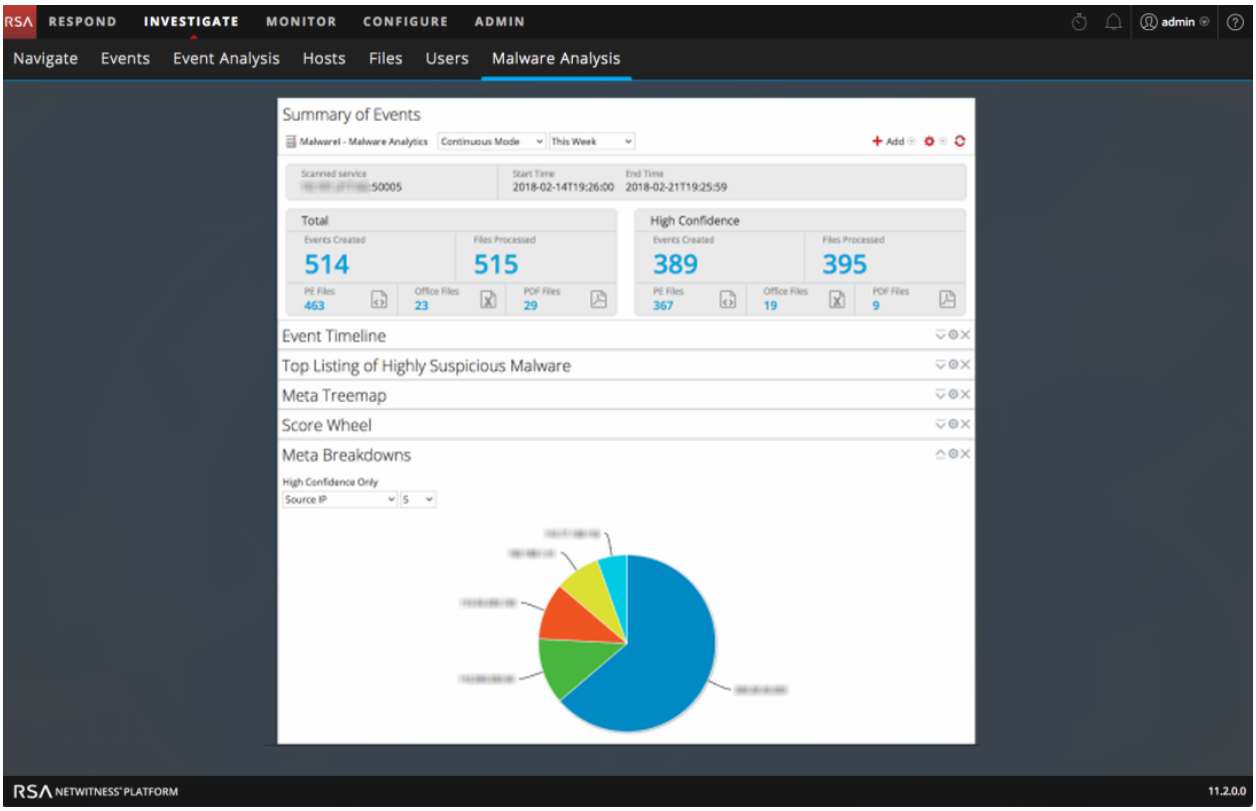


In der Ansicht „Dateien“ können Sie folgende Aufgaben ausführen:

- Dateien filtern und sortieren, um die Ermittlung einzugrenzen.
- Zur Ansicht „Navigation“ oder „Ereignisanalyse“ wechseln, um die Datei zu untersuchen.
- Die Dateien in eine CSV-Datei exportieren.

Ansicht „Malware Analysis“

Die Malware Analysis-Ansicht bietet ein Mittel, bestimmte Typen von Dateiobjekten (zum Beispiel Windows PE, PDF und MS Office) zu analysieren, um die potenzielle Schädlichkeit einer Datei zu bewerten. Diese Abbildung zeigt die Ansicht „Malware Analysis“.



Sie können die Ansicht „Malware Analysis“ direkt öffnen oder mit der rechten Maustaste klicken, um von einem Metawert in einem aktuellen Drill-down-Punkt in der Ansicht „Navigation“ aus auf Schadsoftware zu scannen. Sie können die Multi-Level-Auswertungsmodule nutzen, um die enorme Anzahl an erfassten Dateien zu priorisieren, von denen potenziell die größte Gefahr ausgeht.

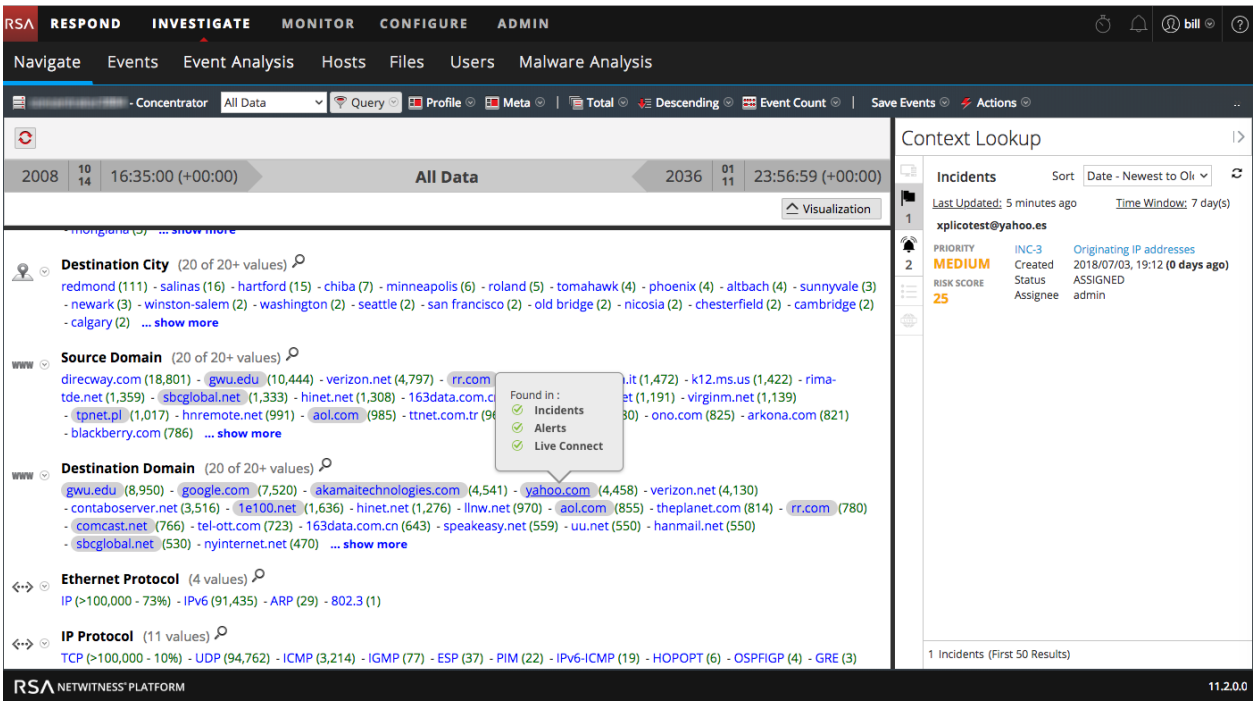
Kontextbezogene Informationen für ein Ereignis

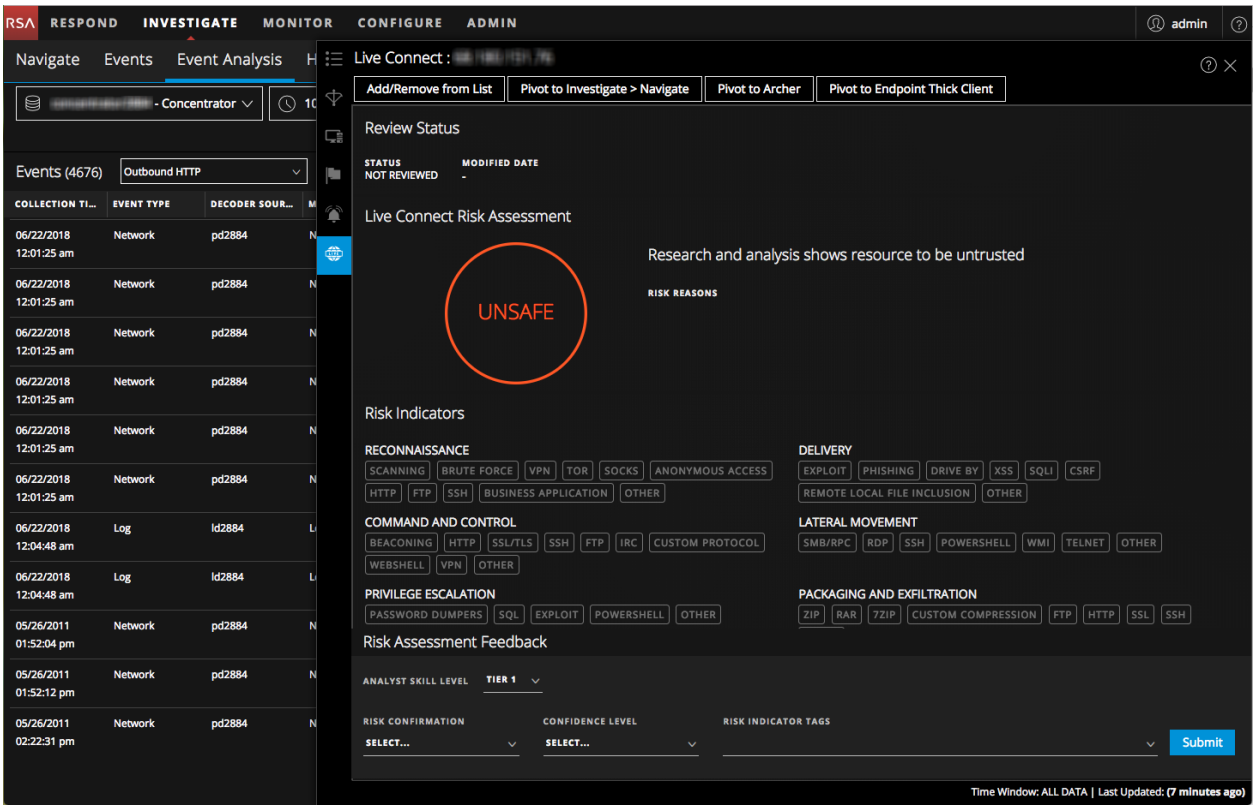
In den Ansichten „Navigation“ und „Ereignisse“ und „Ereignisanalyse“ (Version 11.2 und höher) werden im Bereich „Kontextabfrage“ Details zu Elementen angezeigt, die mit einem Ereignis (IP-Adresse, Benutzer, Host, Domain, MAC-Adresse, Dateiname und Datei-Hash) im Context Hub zusammenhängen.

- Sie können mit den Elementen eines Ereignisses interagieren, um weitere Einblicke zu erhalten, einschließlich verwandter Incidents, Warnmeldungen, benutzerdefinierter Listen, Archer-Ressourcen, Active Directory-Details und NetWitness Endpoint-IIOCs.
- Sie können auf einen Datenpunkt klicken, um die Ansicht „Navigation“ zu öffnen.

Hinweis: Archer-Assets und Active Directory-Details sind in der Kontextabfrage der Ereignisanalyse verfügbar. Für NetWitness Endpoint 4.4.0.2-Hosts oder höher ist eine Endpunkt-Kontextabfrage verfügbar, jedoch nicht für NetWitness Endpoint 11.1-Hosts.

In den folgenden Abbildungen ist der Bereich „Kontextabfrage“ in Ansicht „Navigation“ und der Ansicht „Ereignisanalyse“ dargestellt.

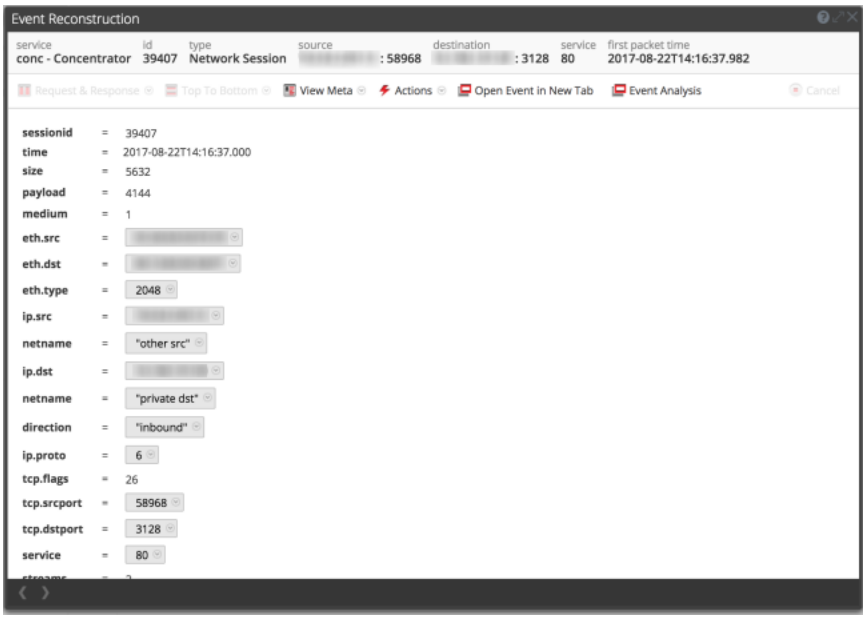

RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
bill
Navigate
Events
Event Analysis
Hosts
Files
Users
Malware Analysis
Concentrator
All Data
Query
Profile
Meta
Total
Descending
Event Count
Save Events
Actions
2008
16:35:00 (+00:00)
All Data
2036
23:56:59 (+00:00)
Visualization
Destination City (20 of 20+ values)
redmond (111) - salinas (16) - hartford (15) - chiba (7) - minneapolis (6) - roland (5) - tomahawk (4) - phoenix (4) - altbach (4) - sunnyvale (3) - newark (3) - winston-salem (2) - washington (2) - seattle (2) - san francisco (2) - old bridge (2) - nicosia (2) - chesterfield (2) - cambridge (2) - calgary (2) ... show more
Source Domain (20 of 20+ values)
direcway.com (18,801) - gwu.edu (10,444) - verizon.net (4,797) - rr.com
Found in :
Incidents
Alerts
Live Connect
k12.ms.us (1,422) - rima-tde.net (1,359) - sbcglobal.net (1,333) - hinet.net (1,308) - 163data.com.c
virginm.net (1,139) - tpnet.pl (1,017) - hnremote.net (991) - aol.com (985) - ttnet.com.tr
ono.com (825) - arkona.com (821) - blackberry.com (786) ... show more
Destination Domain (20 of 20+ values)
gwu.edu (8,950) - google.com (7,520) - akamaitechnologies.com (4,541) - yahoo.com (4,458) - verizon.net (4,130) - contaboserver.net (3,516) - 1e100.net (1,636) - hinet.net (1,276) - llnw.net (970) - aol.com (855) - theplanet.com (814) - rr.com (780) - comcast.net (766) - tel-ott.com (723) - 163data.com.cn (643) - speakeasy.net (559) - uu.net (550) - hanmail.net (550) - sbcglobal.net (530) - nyinternet.net (470) ... show more
Ethernet Protocol (4 values)
IP (>100,000 - 73%) - IPv6 (91,435) - ARP (29) - 802.3 (1)
IP Protocol (11 values)
TCP (>100,000 - 10%) - UDP (94,762) - ICMP (3,214) - IGMP (77) - ESP (37) - PIM (22) - IPv6-ICMP (19) - HOPOPT (6) - OSPFIGP (4) - GRE (3)
Context Lookup
Incidents
Sort
Date - Newest to Ol
Last Updated: 5 minutes ago
Time Window: 7 day(s)
xplicotest@yahoo.es
PRIORITY
MEDIUM
RISK SCORE
25
INC-3
Created
Status
Assignee
Originating IP addresses
2018/07/03, 19:12 (0 days ago)
ASSIGNED
admin
1 Incidents (First 50 Results)
RSA NETWITNESS PLATFORM
11.2.0.0


RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Navigate
Events
Event Analysis
Concentrator
Events (4676)
Outbound HTTP
COLLECTION TI...
EVENT TYPE
DECODER SOUR...
06/22/2018 12:01:25 am Network pd2884
06/22/2018 12:04:48 am Log ld2884
05/26/2011 01:52:04 pm Network pd2884
05/26/2011 01:52:12 pm Network pd2884
05/26/2011 02:22:31 pm Network pd2884
Live Connect :
Add/Remove from List
Pivot to Investigate > Navigate
Pivot to Archer
Pivot to Endpoint Thick Client
Review Status
STATUS
NOT REVIEWED
MODIFIED DATE
Live Connect Risk Assessment
UNSAFE
Research and analysis shows resource to be untrusted
RISK REASONS
Risk Indicators
RECONNAISSANCE
SCANNING
BRUTE FORCE
VPN
TOR
SOCKS
ANONYMOUS ACCESS
HTTP
FTP
SSH
BUSINESS APPLICATION
OTHER
DELIVERY
EXPLOIT
PHISHING
DRIVE BY
XSS
SQLI
CSRF
REMOTE LOCAL FILE INCLUSION
OTHER
COMMAND AND CONTROL
BEACONING
HTTP
SSL/TLS
SSH
FTP
IRC
CUSTOM PROTOCOL
WEBSHELL
VPN
OTHER
LATERAL MOVEMENT
SMB/RPC
RDP
SSH
POWERSHELL
WMI
TELNET
OTHER
PRIVILEGE ESCALATION
PASSWORD DUMPERS
SQL
EXPLOIT
POWERSHELL
OTHER
PACKAGING AND EXFILTRATION
ZIP
RAR
7ZIP
CUSTOM COMPRESSION
FTP
HTTP
SSL
SSH
Risk Assessment Feedback
ANALYST SKILL LEVEL
TIER 1
RISK CONFIRMATION
SELECT...
CONFIDENCE LEVEL
SELECT...
RISK INDICATOR TAGS
Submit
Time Window: ALL DATA | Last Updated: (7 minutes ago)

Ereignisrekonstruktion

Drei Ansichten in NetWitness Investigate bieten die Möglichkeit, ein Ereignis zu rekonstruieren: Ansicht „Navigation“, Ansicht „Ereignisse“ und Ansicht „Ereignisanalyse“. Wenn Sie ein Ereignis ermitteln, das zusätzliche Untersuchungen erfordert, können Sie dieses sicher in einer Form ähnlich seiner nativen Form rekonstruieren. Die Wiedergabe von Ereignissen schränkt die Verwendung von dynamischem oder aktivem Code ein, der in dem Ereignis enthalten sein könnte, um negative Auswirkungen auf das System oder den Browser zu begrenzen. Ein Cache wird verwendet, um die Performance zu verbessern, wenn Sie zuvor angezeigte Ereignisse anzeigen. Jeder Analyst hat einen separaten Cache von Rekonstruktionsdaten und Sie können nur auf rekonstruierte Ereignisse in Ihrem eigenen Cache zugreifen.

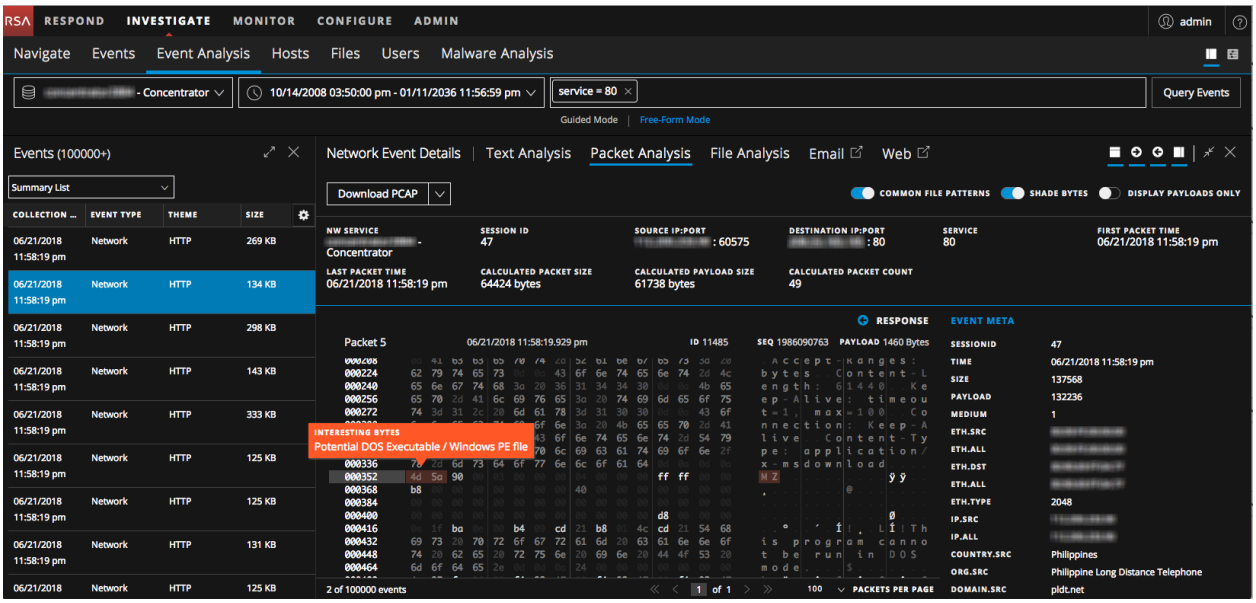
Das Dialogfeld „Ereignisrekonstruktion“ in der Ansicht „Ereignisse“ oder „Navigation“ enthält die Rohdaten, die Metaschlüssel und die Metawerte für ein Ereignis in Listenform. Diese Abbildung ist ein Beispiel für die Ereignisrekonstruktion.



In der Ereignisrekonstruktion haben Sie in der Ansicht „Navigation“ oder „Ereignisse“ folgende Möglichkeiten:

- Sie können durch die Rekonstruktion blättern, um das nächste Ereignis in dieser Liste anzuzeigen.
- Ereignisse können je nach der Art der Daten (Metadaten, Text, hexadezimal, Pakete, Web, E-Mail, Dateien oder automatische Auswahl der besten Rekonstruktion) anhand von verschiedenen Methoden wiederhergestellt werden.
- Sie können Paketerfassungsdateien exportieren, Dateien extrahieren und die Metawerte für das Ereignis exportieren.

Die Ansicht „Ereignisanalyse“ stellt eine interaktive Ereignisrekonstruktion dar, die Rohdaten, Metaschlüssel und Metawerte enthält. Diese Abbildung zeigt ein Beispiel für eine Rekonstruktion in der Ansicht „Ereignisanalyse“.



In der Rekonstruktion in der Ansicht „Ereignisanalyse“ haben Sie folgende Möglichkeiten:

- Ereignisse können je nach der Art der Daten (Metadaten, Text, Hexadezimalwerte, Pakete und Dateien) anhand von verschiedenen Methoden wiederhergestellt werden.
- Informationen in Headern und Nutzdaten werden hervorgehoben.
- Sie können dekodierte und verschlüsselte Nutzdaten anzeigen und gängige Dateisignaturen sehen.
- Sie können nach Speicherorten von Metaschlüsseln oder Metawerten in der Rekonstruktion suchen.
- Exportieren von Ereignissen und Dateien

Konfigurieren von Ansichten und Voreinstellungen von NetWitness Investigate

Analysten können einige Merkmale der Ansichten und des Verhaltens von NetWitness Investigate konfigurieren. Sie können die Art anpassen, in der die Investigate-Ansichten angezeigt werden, die Typen der dargestellten Informationen sowie Faktoren, die die Performance beim Zurückgeben von Ergebnissen und Rekonstruieren von Ereignissen beeinflussen. Alle konfigurierbaren Einstellungen haben Standardwerte, die in den meisten Bereitstellungen wirksam sind, Analysten haben jedoch die Möglichkeit, die Option gegebenenfalls anzupassen.

Für Analysten, die Analysen mithilfe von Investigate durchführen, müssen die entsprechenden Systemrollen und Berechtigungssätze in den Benutzerkonten eingerichtet werden. Ein Administrator muss Rollen und Berechtigungen konfigurieren, wie unter *Handbuch Systemsicherheit und Benutzerverwaltung* beschrieben. (Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.)

Diese Themen enthalten weitere Informationen:

- Konfigurieren der Ansichten „Navigation“ und „Ereignisse“
- Konfigurieren der Ansicht „Ereignisanalyse“
- Konfigurieren der Ansicht „Malware Analysis-Ereigniszusammenfassung“

Konfigurieren der Ansichten „Navigation“ und „Ereignisse“

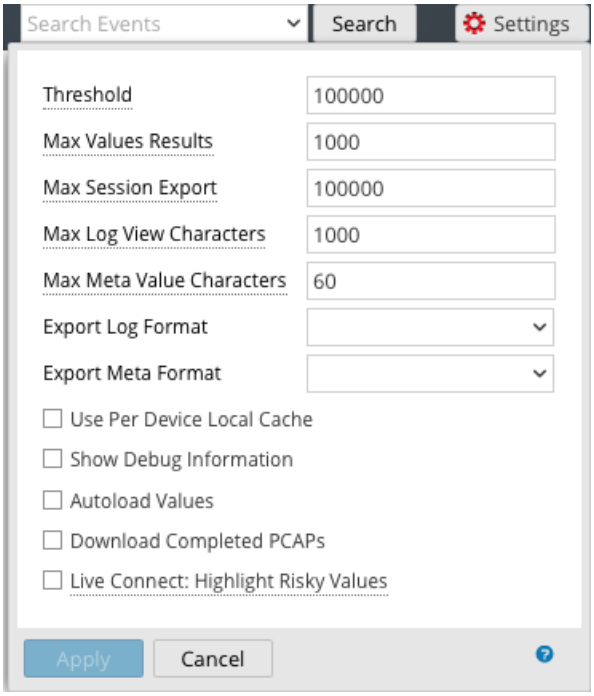
Analysten können Einstellungen festlegen, die die Performance und das Verhalten von NetWitness Platform beim Analysieren von Daten in den Ansichten „Navigation“ und „Ereignisse“ beeinflussen. Einige dieser Einstellungen sind an zwei Stellen in NetWitness Platform verfügbar. Änderungen, die an der einen Stelle vorgenommen werden, werden auch in der anderen Ansicht angewendet:

- Ansicht „Untersuchen“ > Dialogfeld „Einstellungen“ für die Ansichten „Navigation“ und „Ereignisse“.
- „Profile“ > Bereich „Einstellungen“ > Registerkarte „Untersuchen“
- Ansichten „Navigation“ „Ereignisse“, Drop-down-Liste „Suchoptionen“.

Zugreifen auf die Einstellungen der Ansichten „Navigation“ und „Ereignisse“

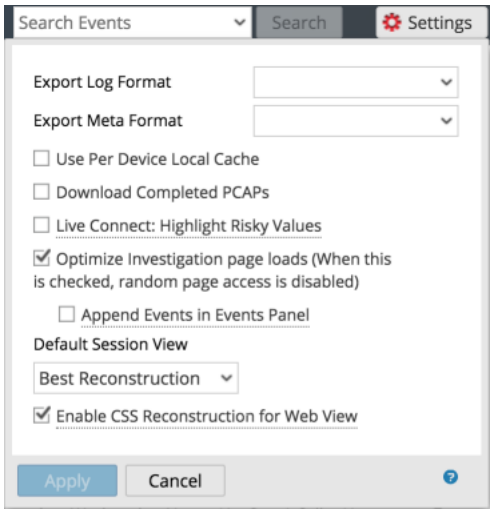
Wählen Sie eine der folgenden Möglichkeiten, um die auf die Einstellungen zuzugreifen:

- Klicken Sie in der Symbolleiste der Ansicht **Navigation** auf die Option **Einstellungen**.
  Das Dialogfeld „Einstellungen“ der Ansicht „Navigation“ wird angezeigt.



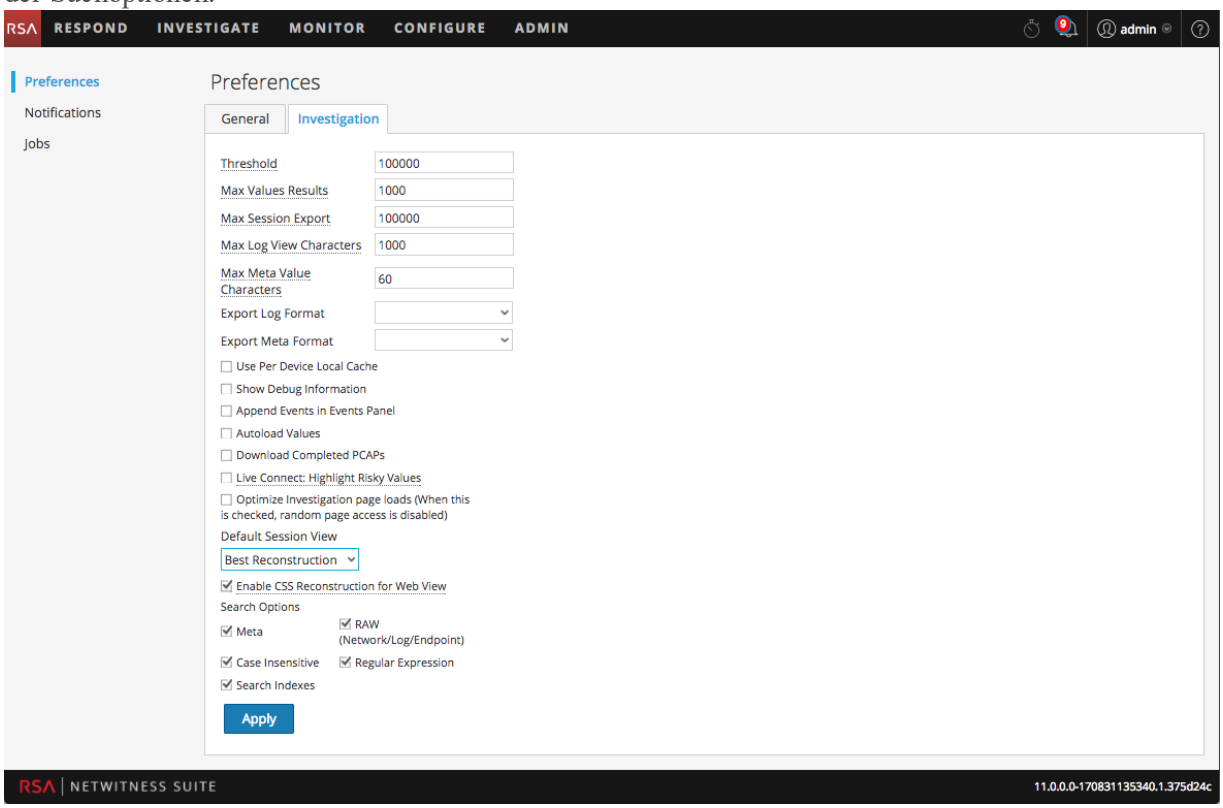
Hinweis: Version 11.0 enthielt eine Einstellung für das Anhängen von Ereignissen im Bereich „Ereignisse“. Diese Funktion wurde in der Version 11.1 in den Bereich „Einstellungen“ der Ansicht „Ereignisse“ verschoben.

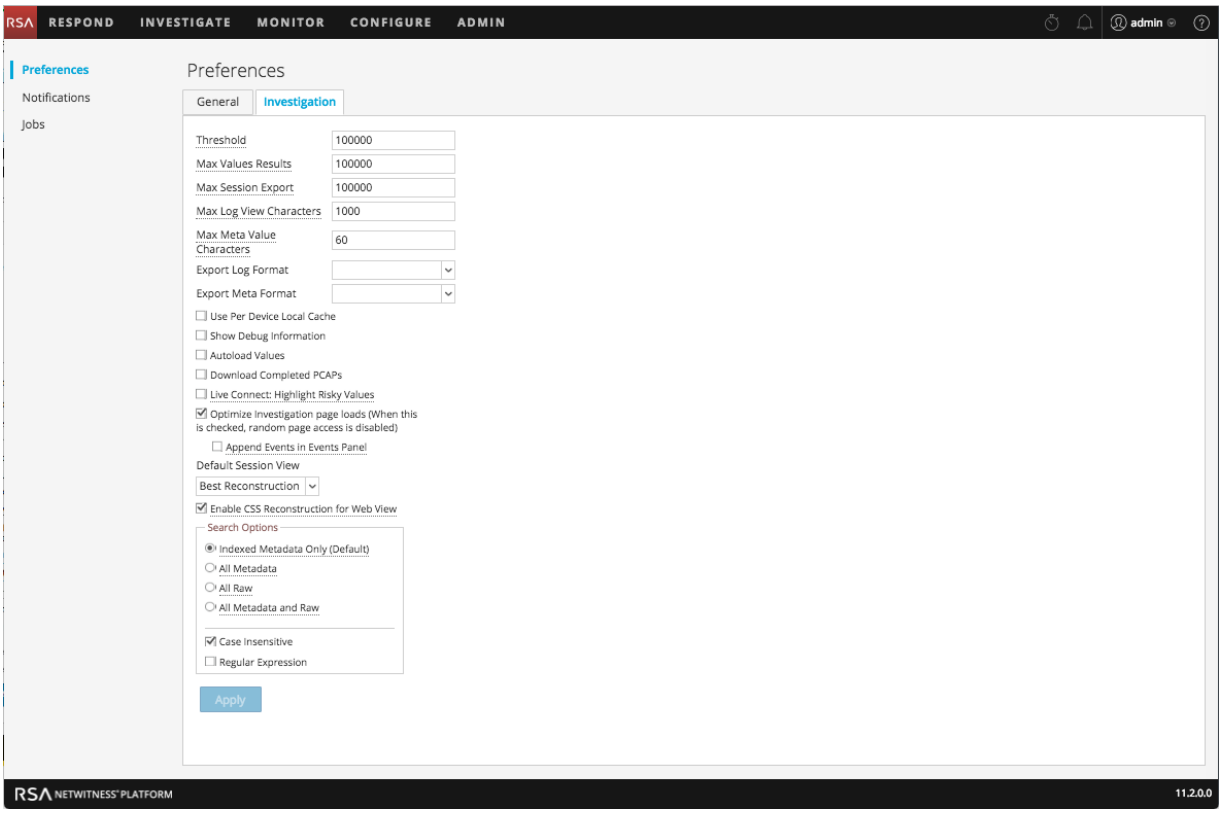
- Wählen Sie in der Symbolleiste der Ansicht **Ereignisse** die Option **Einstellungen** aus.
  Das Dialogfeld „Einstellungen“ der Ansicht „Ereignisse“ wird angezeigt.



Hinweis: Version 11.1 und höher enthalten die Einstellung „Ereignisse in Ereignisbereich anhängen“.

- Navigieren Sie oben rechts in NetWitness Platform zu > Profile und klicken Sie im Bereich **Einstellungen** auf die Registerkarte **Ermittlungen**.
  Der Bereich „Untersuchen“ wird angezeigt. Die erste Abbildung unten veranschaulicht den Bereich „Ermittlungen“ in Version 11.1, die zweite Abbildung den Bereich in 11.2 mit verbessertem Layout der Suchoptionen.





Kalibrieren der Werte der Ladeparameter in der Ansicht „Navigation“

Verschiedene Einstellungen beeinflussen die Performance von NetWitness Platform beim Laden von Werten im Bereich „Werte“. Die Standardwerte basieren auf der gängigen Verwendung und einzelne Analysten können diese Einstellungen für ihre eigenen Ermittlungen anpassen. So passen Sie diese Einstellungen an:

1. Navigieren Sie zur Registerkarte **Untersuchen** oder zum Dialogfeld **Einstellungen** der Ansicht „Navigation“.
2. Passen Sie die folgenden Parameter an:
   - **Schwellenwert:** Legen Sie den Schwellenwert für die maximale Anzahl der für einen Metaschlüsselwert geladenen Sitzungen im Bereich Werte fest. Ein höherer Schwellenwert ermöglicht genauere Zählerangaben für einen Wert, verursacht aber auch längere Ladezeiten. Der Standardwert ist **100.000**.
   - **Max. Wertergebnisse:** Legen Sie die maximale Anzahl von Werten fest, die in der Navigationsansicht geladen werden, wenn die Option Max. Ergebnisse im Metaschlüsselmenü für einen offenen Metaschlüssel ausgewählt ist. Der Standardwert ist **1.000**.
   - **Max. Sitzungsexport:** Geben Sie die Anzahl der Ereignisse an, die in eine einzelne PCAP- oder Protokolldatei exportiert werden können.
   - **Max. Zeichenzahl für Protokollansicht:** Legen Sie die Anzahl der Zeichen fest, die maximal in **Untersuchen > Ereignisse > Protokolltext** angezeigt werden sollen. Der Standardwert ist **1000**.

- **Max. Zeichenzahl für Metawert:** Legen Sie die maximale Anzahl der Zeichen in einem Metawertenamen fest, der im Bereich „Werte“ der Ansicht „Navigation“ angezeigt wird. Der Standardwert ist **60**.
- **Debuginformationen anzeigen:** Wenn Sie möchten, dass NetWitness Platform die `where`-Klausel unterhalb der Brotkrümelnavigation in der Ansicht „Navigation“ sowie die verstrichene Ladezeit für jeden aggregierten Service für einen Broker anzeigt, aktivieren Sie diese Option. Der Standardwert ist **Aus**.
- **Ereignisse in Ereignisbereich anhängen:** Diese Option wirkt sich auf die Paginierung in der Ansicht „Ereignisse“ aus und wird nachfolgend unter „Kalibrieren des Abrufs und der Standardrekonstruktion in der Ansicht „Ereignisse““ beschrieben.
- **Werte automatisch laden:** Wenn Sie möchten, dass NetWitness Platform automatisch Werte für den ausgewählten Service in der Navigationsansicht lädt, aktivieren Sie diese Option. Wurde diese Option nicht ausgewählt, zeigt NetWitness Platform die Schaltfläche **Werte laden** an, über die Sie die Optionen ändern können. Der Standardwert ist **Aus**.

3. Klicken Sie auf **Anwenden**.

Die Einstellungen werden sofort wirksam und sind sichtbar, wenn Sie das nächste Mal Werte laden.

Konfigurieren der Parameter der Ansichten „Navigation“ und „Ereignisse“

Verschiedene Einstellungen beeinflussen die Performance von NetWitness Platform beim Laden von Werten in den Ansichten „Navigation“ und „Ereignisse“. Die Standardwerte basieren auf der gängigen Verwendung und einzelne Analysten können diese Einstellungen für ihre eigenen Ermittlungen anpassen. Sie können diese Parameter in den Ansichten „Navigation“ und „Ereignisse“ jeweils separat festlegen. Bei der Konfiguration in einer Ansicht wird die Einstellung nicht automatisch auf die andere Ansicht angewendet. So passen Sie diese Einstellungen an:

1. Navigieren Sie zur Registerkarte **Untersuchen** oder zum Dialogfeld **Einstellungen** der Ansicht „Navigation“ oder der Ansicht „Ereignisse“.
2. Passen Sie die folgenden Parameter an:
   - **Live Connect: Riskante Werte markieren**: Wenn Sie möchten, dass NetWitness Platform nur IP-Adressen hervorhebt und anzeigt, die von der RSA-Community als riskant betrachtet werden, aktivieren Sie diese Option. Wenn diese Option nicht aktiviert ist, zeigt NetWitness Platform alle IP-Adressen an. Diese Option ist standardmäßig deaktiviert (**Aus**).
   - **- Lokaler Cache pro Gerät:** Sie können festlegen, wie im lokalen Cache gespeicherte Daten vom ausgewählten Service verwendet werden. Diese Option ist standardmäßig deaktiviert (**Aus**). Wenn diese Option deaktiviert ist, sendet Investigate eine neue Abfrage an die Datenbank anstatt im Cache gespeicherten Daten in den Investigation-Ansichten nach dem Laden anzuzeigen. Wenn diese Option aktiviert ist, verwendet Investigate die Daten aus dem lokalen Cache.
   - **- Abgeschlossene PCAPs herunterladen:** Sie können den Download extrahierter PCAPs in den Ansichten „Navigation“ und „Ereignisse“ automatisieren, damit der Browser die extrahierten PCAPs herunterlädt und in der Standardanwendung zum Öffnen von PCAP-Dateien öffnet (z. B. Wireshark). Diese Option ist standardmäßig deaktiviert (**Aus**). Wenn Sie diese Option aktivieren

möchten, muss eine Anwendung zum Öffnen von PCAP-Dateien auf Ihrem lokalen Dateisystem installiert und als Standardanwendung für PCAP-Dateiformate konfiguriert sein.

- **Live Connect: Riskante Werte markieren:** Wenn diese Option deaktiviert ist, werden alle Metawerte, die in Live Connect verfügbaren Kontext haben, im Bereich „Werte“ der Ansicht „Navigation“ hervorgehobenen. Wenn die Option aktiviert ist, werden unter allen Werten, die in Live Connect Kontext haben, nur die Werte, die von der Community als „Riskant/Verdächtig/Unsicher“ erachtet werden, hervorgehoben. Diese Option ist standardmäßig deaktiviert (**Aus**).

3. Klicken Sie auf **Anwenden**.
   Die Einstellungen werden sofort wirksam.

Konfigurieren des Standard-Exportprotokollformats

Sie können Protokolle aus den Ansichten „Navigation“ und „Ereignisse“ in unterschiedlichen Formaten exportieren. Verfügbare Optionen sind Text, XML, CSV (Comma-Separated Values) und JSON. Es gibt keinen integrierten Standardwert für das Protokollexportformat. Wenn Sie hier kein Format auswählen, zeigt NetWitness Platform ein Auswahldialogfenster an, wenn Sie einen Protokollexport aufrufen. So wählen Sie das Format der exportierten Protokolle aus:

1. Navigieren Sie zur Registerkarte **Untersuchen** oder zum Dialogfeld **Einstellungen** der Ansicht „Navigation“ oder der Ansicht „Ereignisse“.
2. Wählen Sie im Drop-down-Menü **Exportprotokollformat** eine der Optionen aus.
3. Klicken Sie auf **Anwenden**.
   Die Einstellung wird sofort wirksam.

Konfigurieren des Standard-Metaexportformats

Sie können Metawerte aus den Ansichten „Navigation“ und „Ereignisanalyse“ in unterschiedlichen Formaten exportieren. Verfügbare Optionen sind Text, CSV, TSV (Tab-Separated Values) und JSON. Es gibt keinen integrierten Standardwert für das Metaexportformat. Wenn Sie hier kein Format auswählen, zeigt NetWitness Platform ein Auswahldialogfeld an, wenn Sie einen Export von Metawerten aufrufen. So wählen Sie das Format der exportierten Metawerte aus:

1. Navigieren Sie zur Registerkarte **Untersuchen** oder zum Dialogfeld **Einstellungen** der Ansicht „Navigation“ oder der Ansicht „Ereignisse“.
2. Wählen Sie im Drop-down-Menü **Format exportierte Metadaten** eine der Optionen aus.
3. Klicken Sie auf **Anwenden.**
   Die Einstellung wird sofort wirksam.

Kalibrieren des Abrufs und der Standardrekonstruktion in der Ansicht „Ereignisse“

Sie können mehrere Parameter konfigurieren, mit denen Sie steuern, wie NetWitness Platform Ereignisse abruft und in der Ansicht „Ereignisse“ rekonstruiert. So passen Sie diese Parameter an:

1. Navigieren Sie zur Registerkarte **Untersuchen** oder zum Dialogfeld **Einstellungen** der Ansicht „Ereignisse“.
2. Konfigurieren Sie die folgenden Parameter.
   - **Optimieren des Ladens der Seite „Investigation“**: Legen Sie eine Auslagerungsoption fest. Wenn optimiert, werden die Ergebnisse so schnell wie möglich zurückgegeben. Dabei geht die ursprüngliche Möglichkeit verloren, zu einer bestimmten Seite der Ereignisliste zu wechseln. Durch die Deaktivierung dieses Kontrollkästchens wird die Paginierung der Ereignislisten geändert, damit Sie auf eine bestimmte Seite in der Liste (oder auf die letzte Seite) springen können. Der Standardwert ist **aktiviert**.
   - **Standardsitzungsansicht:** Wählt den Standardrekonstruktionstyp für die anfängliche Rekonstruktion in der Ansicht „Ereignisse“ aus. Der Standardwert ist **Beste Rekonstruktion**, bei dem die Ereignisse mithilfe der am besten für das Ereignis geeigneten Rekonstruktionsmethode wiederhergestellt werden.
3. Navigieren Sie zur Registerkarte **Ermittlungen** oder zum Dialogfeld **Einstellungen** der Ansicht „Navigation“ (11.1) oder in der Ansicht „Ereignisse“ (11.2) und legen Sie die Option **Ereignisse in Ereignisbereich anhängen** fest. Wenn diese Option ausgewählt ist, werden die im Bereich **Ereignisse** angezeigten Ereignisse inkrementell hinzugefügt. Zum Beispiel wird jedes Mal, wenn Sie auf das Nächste-Seite-Symbol klicken, das nächste Inkrement der Ereignisse hinzugefügt. Zuerst sehen Sie 1 bis 25, dann 1 bis 50, dann 1 bis 75 usw. Diese Option ist nur verfügbar, wenn die Option **Optimieren des Ladens der Seite „Untersuchen“** aktiviert ist.
4. Klicken Sie auf **Anwenden**, um die Änderungen sofort zu übernehmen.

Aktivieren oder Deaktivieren der Cascading Style Sheet-Darstellung in Rekonstruktionen von Webinhalt

Analysten können CSS (Cascading Style Sheets) für die Rekonstruktion von Webinhalt aktivieren. Wenn die Einstellung aktiviert ist, werden bei der Webrekonstruktion auch CSS-Stilvorlagen und Bilder mit einbezogen, sodass die Darstellung der Originalansicht in einem Webbrowser entspricht. Dies schließt das Scannen und Rekonstruieren von verbundenen Ereignissen sowie das Suchen nach Stylesheets und Bildern ein, die im Zielereignis verwendet werden. Diese Option ist standardmäßig aktiviert. Deaktivieren Sie diese Option, wenn Probleme bei der Anzeige bestimmter Websites auftreten.

Hinweis: Die Darstellung des rekonstruierten Inhalts stimmt eventuell nicht genau mit der ursprünglichen Webseite überein, wenn die entsprechenden Bilder und Formatvorlagen nicht gefunden werden oder aus dem Cache des Webbrowsers geladen wurden. Zudem werden Layouts oder Formate, die dynamisch über das clientseitige JavaScript erstellt werden, in der Rekonstruktion nicht dargestellt, weil alle clientseitigen JavaScripts aus Sicherheitsgründen entfernt werden.

So aktivieren oder deaktivieren Sie diese Option:

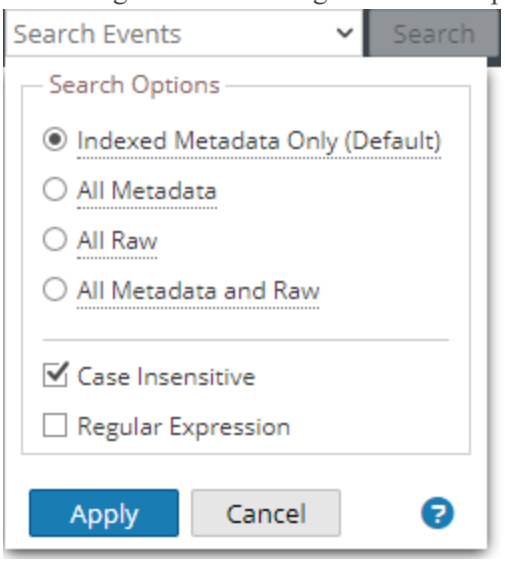
1. Klicken Sie auf die Registerkarte **Untersuchen**.
2. Aktivieren Sie das Kontrollkästchen **CSS-Rekonstruktion für Webansicht ermöglichen**.

3. Klicken Sie auf **Anwenden**.
   Die Einstellung wird sofort wirksam und wird bei der nächsten Rekonstruktion von Webinhalt angezeigt.

Konfigurieren von Suchoptionen

Sie können Suchoptionen konfigurieren, die bei der Eingabe einer Suchzeichenfolge in das Feld „Suche“ angewendet werden. Bearbeiten Sie die Suchoptionen auf der Registerkarte „Profil“ > Bereich „Einstellungen“ > Registerkarte „Ermittlungen“ oder im Drop-down-Menü „Suchoptionen“ in den Ansichten „Navigation und „Ereignisse“. So konfigurieren Sie Suchoptionen:

1. Navigieren Sie zu den Suchoptionen.
   In der folgenden Abbildung wird das Drop-Down-Menü „Suchoptionen“ für Version 11.2 dargestellt.



2. Wählen Sie eine oder mehrere Suchoptionen aus, die auf die Suche angewendet werden sollen. Suchen nach Textmustern bietet detaillierte Informationen zu jeder Option.
3. Zum Speichern der Sucheinstellungen klicken Sie auf **Anwenden**.
   Die Einstellungen werden gespeichert und sind sofort wirksam.

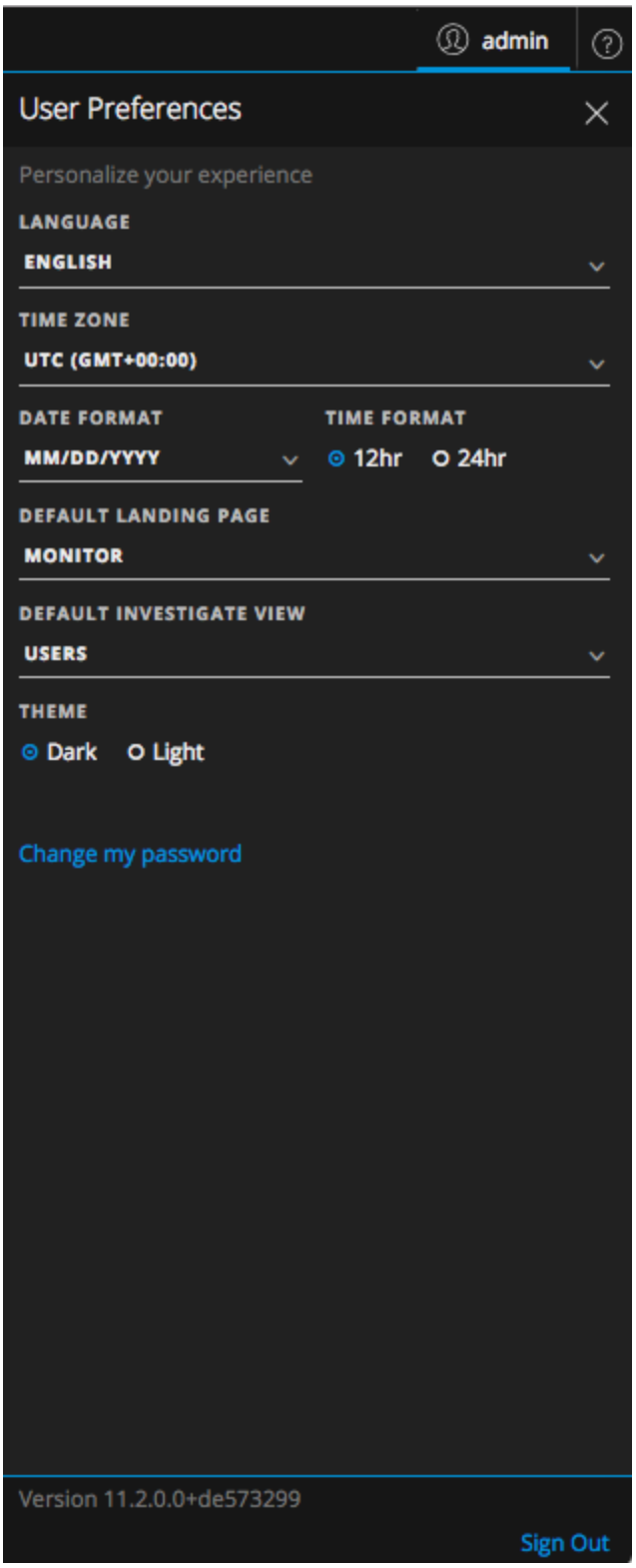
Konfigurieren der Ansicht „Ereignisanalyse“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Ab Version 11.1 können Analysten Einstellungen festlegen, die das Verhalten von NetWitness Platform beeinflussen, wenn Daten mit der Ansicht „Untersuchen > Ereignisanalyse“ analysiert werden. Die Hauptsymbolleiste in „Untersuchen“ wird anders dargestellt, wenn die Ansicht „Ereignisanalyse“ geöffnet ist. Diese zwei Schaltflächen ermöglichen den Zugriff auf die folgenden Einstellungsdialogfelder: und . Im Menü „Benutzer“ ( ) können hauptsächlich globale Einstellungen wie etwa die Einstellung der Zeitzone vorgenommen werden. Im Menü mit den Einstellungen für die Ereignisanalyse ( ) hingegen finden sich überwiegend Einstellungen für das Verhalten in der Ansicht „Ereignisanalyse“. Im weiteren Verlauf dieses Abschnitts werden die Einstellungen beider Menüs beschrieben.

Festlegen der Standardansicht von „Untersuchen“

Die Standardansicht von „Untersuchen“ wird im Dialogfeld „Benutzereinstellungen“ (oben rechts im NetWitness Platform-Browserfenster auswählen) festgelegt.
Im Dialogfeld „Benutzereinstellungen“ werden die aktuellen Einstellungen für die Ansicht Investigate angezeigt. Sie können die Standardansicht auswählen, wenn Sie „Untersuchen“ in einer der folgenden Ansichten öffnen: Ansicht „Ereignisanalyse“, Ansicht „Hosts“ oder Ansicht „Dateien“.



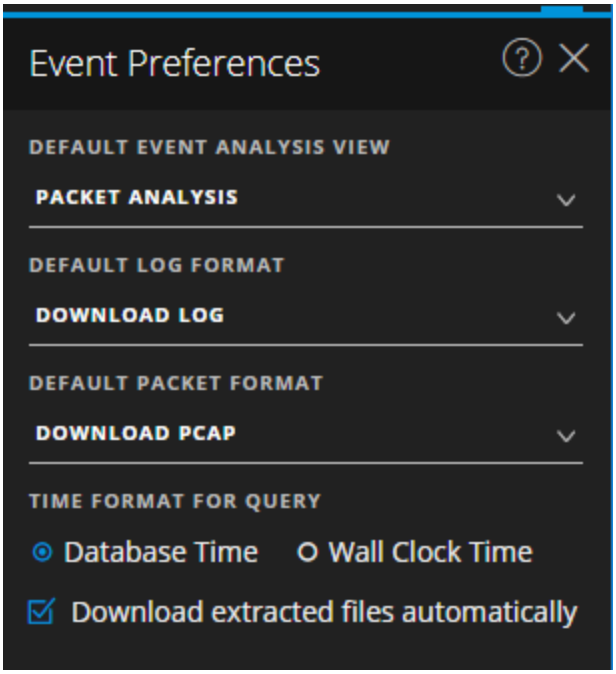
Die globalen Nutzereinstellungen werden im *Leitfaden für die ersten Schritte mit RSA NetWitness Platform* ausführlich beschrieben.Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Festlegen von Nutzereinstellungen für die Ansicht „Ereignisanalyse“

In Version 11.1 und höher können Sie Einstellungen für die Ansicht „Ereignisanalyse“ festlegen. Die hier ausgewählten Einstellungen gelten für einzelne Benutzer und sind verfügbar, wann immer sich der jeweilige Benutzer bei der Anwendung anmeldet.

So legen Sie Standardwerte für das Arbeiten in der Ansicht „Ereignisanalyse“ fest:

1. Klicken Sie bei geöffneter Ansicht „Ereignisanalyse“ auf .



2. Wählen Sie im Drop-down-Menü **Standardmäßige Ansicht „Ereignisanalyse“** den standardmäßigen Rekonstruktionstyp aus, wenn Sie ein Ereignis im Bereich „Ereignisanalyse“ öffnen: **Textanalyse**, **Paketanalyse** und **Dateianalyse**.
   Wenn Sie für die Analyse keinen Standardtyp ausgewählt haben, wird als standardmäßiger Rekonstruktionstyp „Paketanalyse“ verwendet, wenn Sie ein Ereignis öffnen. Nur für Protokoll- und Endpunktereignisse wird der Rekonstruktionstyp „Textanalyse“ verwendet. Wenn Sie einen standardmäßigen Rekonstruktionstyp auswählen, wird automatisch dieser Rekonstruktionstyp verwendet. In beiden Fällen ist der ausgewählte Standardtyp der Ausgangspunkt. Wenn Sie den Typ während dem Arbeiten ändern, wird für die nächste Rekonstruktion der neu ausgewählte Typ verwendet.
3. Wählen Sie im Drop-down-Menü **Standardmäßiges Protokollformat** das Download-Format für den Protokollexport aus: **Protokoll herunterladen**, **XML-Datei herunterladen**, **CSV herunterladen** oder **JSON-Datei herunterladen**. Wenn Sie hier kein Format auswählen, wird **Download-Protokoll** als Standardformat verwendet. Diese Optionen stehen auch beim Download in einem Drop-down-Menü zur Verfügung.
4. Wählen Sie im Drop-down-Menü **PCAP herunterladen** das Standardformat für das Herunterladen von Paketen aus. Diese Optionen stehen auch beim Download in einem Drop-down-Menü zur

Verfügung:

- **PCAP herunterladen** zum Herunterladen des gesamten Ereignisses als eine Paketerfassungsdatei (*.pcap).
- **Alle Nutzdaten herunterladen** zum Herunterladen der Nutzdaten als *.payload-Datei
- **Anforderungsnutzdaten herunterladen** zum Herunterladen der Anforderungsnutzdaten als *.payload1-Datei.
- **Antwortnutzdaten herunterladen** zum Herunterladen der Antwortnutzdaten als *.payload2-Datei

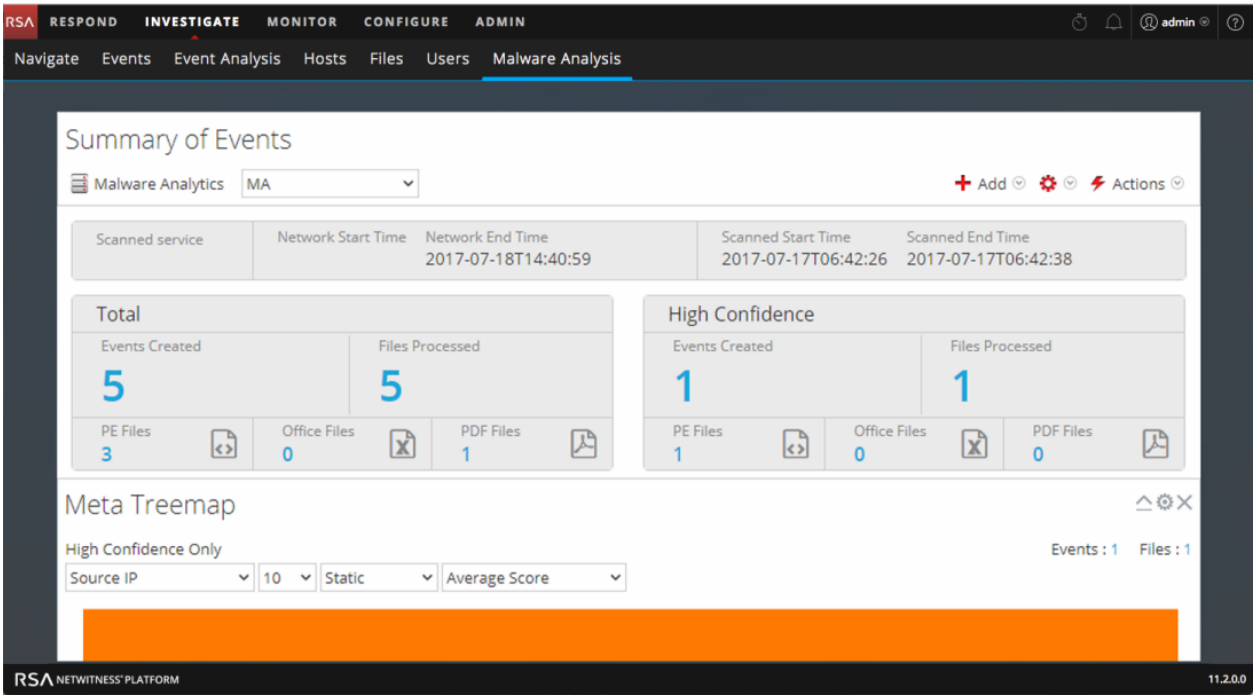
5. Klicken Sie unter **Zeitformat für Abfragen** entweder auf **Datenbankzeit** oder **Uhrzeit**. Die Ansicht „Ereignisanalyse“ kann Ergebnisse basierend auf der Datenbankzeit oder der aktuellen Uhrzeit anzeigen. Wenn Sie das Zeitformat hier festlegen, wird Ihre individuelle Benutzereinstellung gespeichert, bis sie erneut geändert wird. Die Standardeinstellung für diese Einstellung ist **Datenbankzeit**. Dieses Zeitformat wird auch zur Anzeige von Abfrageergebnissen in den Ansichten „Navigation“ und „Ereignisse“ verwendet.
   - Wenn **Datenbankzeit** ausgewählt ist, basieren Start- und Endzeit für eine Abfrage auf der Zeit, zu der das Ereignis gespeichert wurde.
   - Wenn **Uhrzeit** ausgewählt ist, wird die Abfrage mit der aktuellen Zeit gemäß der in den Nutzereinstellungen festgelegten Zeitzone ausgeführt.

Konfigurieren der Ansicht „Malware Analysis-Ereigniszusammenfassung“

Die Ereigniszusammenfassung bietet eine Zusammenfassung des untersuchten Scans und unter der Zusammenfassung befinden sich konfigurierbare Dashlets, z. B. Visualisierungsdiagramme und Listen. Standardmäßig öffnet sich die Ereigniszusammenfassung für einen Scan mit der Anzeige der Standard-Dashlets. Sie können die Ansicht durch das Hinzufügen, Ändern und Löschen von Standard-Dashlets anpassen. Die konfigurierte Anpassung der Dashlets bleibt für verschiedene Scanuntersuchungen erhalten und Sie können die Standard-Dashlets jederzeit wiederherstellen. Die Standard-Dashlets sind:

- Ereigniszusammenfassung (korrigiert)
- Ereigniszeitachse
- Top-Liste höchst verdächtiger Schadsoftware
- Meta-Treemap
- Ergebnisrad
- Meta-Strukturen

Die folgende Abbildung ist ein Beispiel für eine standardmäßige Ereigniszusammenfassung.



Der Rest dieses Themas enthält Anweisungen für Management und Konfiguration von Dashlets.

Dashlet hinzufügen

Sie können mehrere Kopien von Dashlets in der Schadsoftwareanalyse-Ereigniszusammenfassung hinzufügen. So fügen Sie ein Dashlet hinzu:

1. Wählen Sie in der Symbolleiste **Hinzufügen** aus.
   Die Drop-down-Liste der Dashlets wird angezeigt. Es gibt vier Visualisierungsoptionen: Egebnisrad, Meta-Treemap, Meta-Strukturen und Ereigniszeitachse. Die anderen drei Dashlets sind die gleichen Dashlets, die im Dashboard „NetWitness Platform“ verfügbar sind: Schadsoftware mit IOCs mit hoher Wahrscheinlichkeit und hohen Werten, Top-Liste höchst verdächtiger Schadsoftware, Top-Liste möglicher Zero-Day-Schadsoftware. Details zu diesen gemeinsamen Dashlets finden Sie unter „Dashlets“ in der RSA Content für die RSA NetWitness Platform.
2. Wählen Sie ein Dashlet aus.
   Das neue Dashlet wird als letztes Dashlet unter den bestehenden Dashlets hinzugefügt.
3. Wenn das Dashlet ein Duplikat eines bestehenden Dashlet ist, ändern Sie den Namen des neuen Dashlet, damit es eindeutig ist.

Ändern oder Löschen eines Dashlet mithilfe von Symbolleistenoptionen

Jedes Dashlet hat eine Symbolleiste, die Optionen zur Änderung des Dashlet bieten. Die Visualisierungsdiagramme verfügen über dieselben Konfigurationseinstellungen, während einige andere Dashlets zusätzliche Einstellungen bieten.

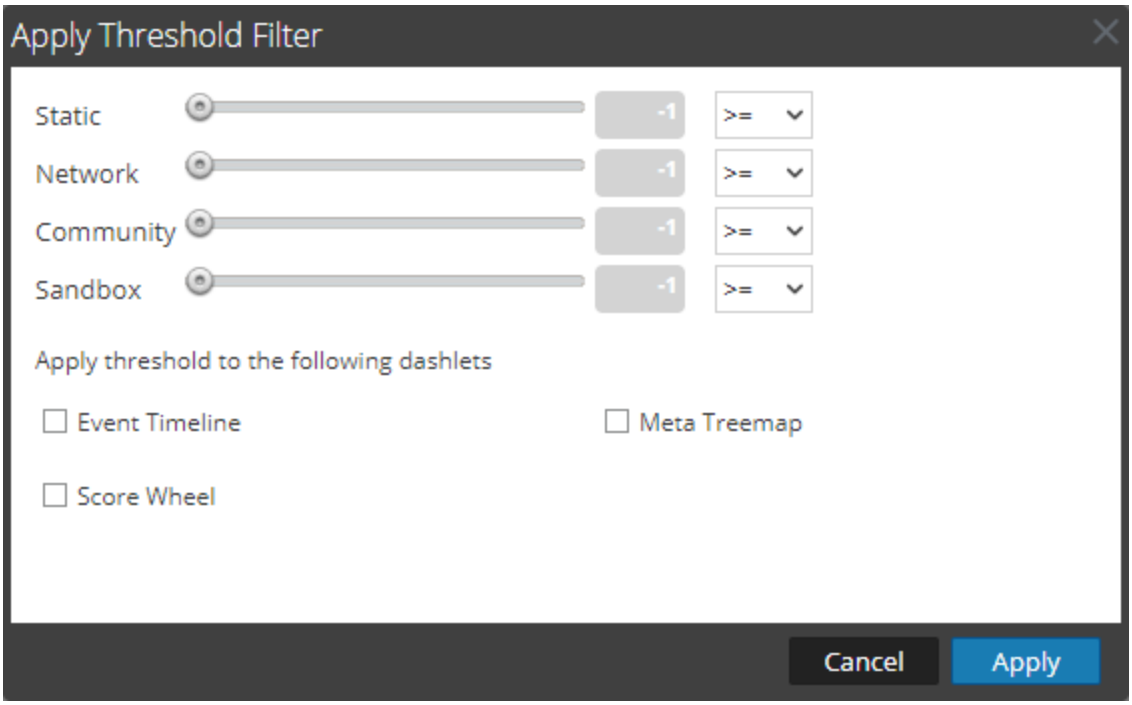
So verwenden Sie die Symbolleistenoptionen:

- Klicken Sie zum Schließen eines Dashlet, so dass nur die Titelleiste angezeigt wird, auf .
- Klicken Sie zum Öffnen eines Dashlet, das geschlossen ist, auf .
- Klicken Sie zum Anzeigen der konfigurierbaren Einstellungen für ein Dashlet auf .
  Das Dialogfeld „Einstellungen“ für das Dashlet wird angezeigt.
- Klicken Sie zum Löschen eines Dashlet auf .

Anwenden des Schwellenwertfilters auf mehrere Dashlets

Sie können innerhalb von Dashlets einen Schwellenwert festlegen, damit nur Ereignisse mit oder unter einem bestimmten Ergebnis in den vier Kategorien (Statisch, Netzwerk, Community und Sandbox) angezeigt werden. Dieses Verfahren legt die Schwellenwerte für diese Dashlets nach Dashlet-Typ fest: Ereigniszeitachse, Ergebnisrad und Meta-Treemap. Außerdem können Sie den Schwellenwert für einzelne Dashlets festlegen.

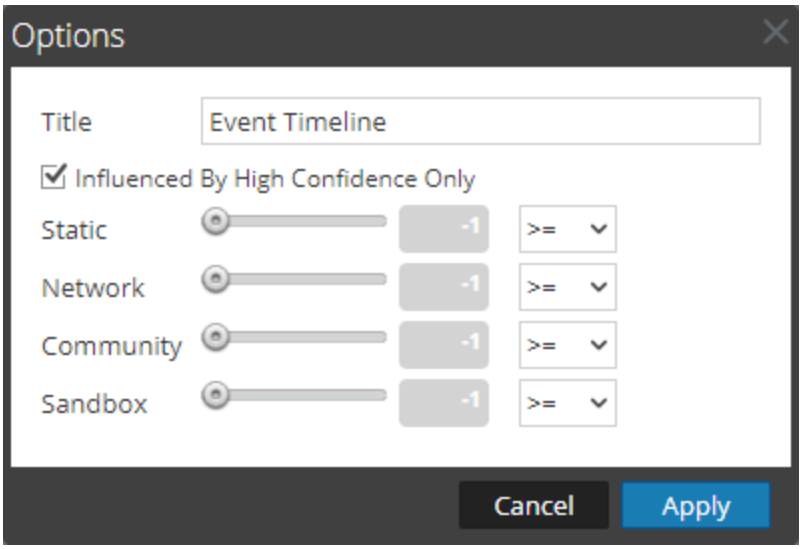
1. Wählen Sie in der Symbolleiste > **Schwellenwertfilter anwenden** aus.
   Das Dialogfeld „Schwellenwertfilter anwenden“ wird angezeigt.



2. Wählen Sie einen oder mehrere Dashlet-Typen aus: Ereigniszeitachse, Ergebnisrad und Meta-Treemap.
3. Ziehen Sie den entsprechenden Schieberegler oder geben Sie einen numerischen Wert ein und wählen Sie dann in der Drop-down-Liste einen Operator aus: =, >= oder <=.
4. Klicken Sie auf **Anwenden**.
   Die Schwellenwertfilter werden auf die ausgewählten Dashlet-Typen in der Ereigniszusammenfassung angewendet.

Einstellen des Titels und der Kategorieoptionen für ein Dashlet

1. Klicken Sie zum Anzeigen der konfigurierbaren Einstellungen für ein Dashlet auf ⚙.
   Das Dialogfeld „Optionen“ für das Dashlet wird angezeigt.

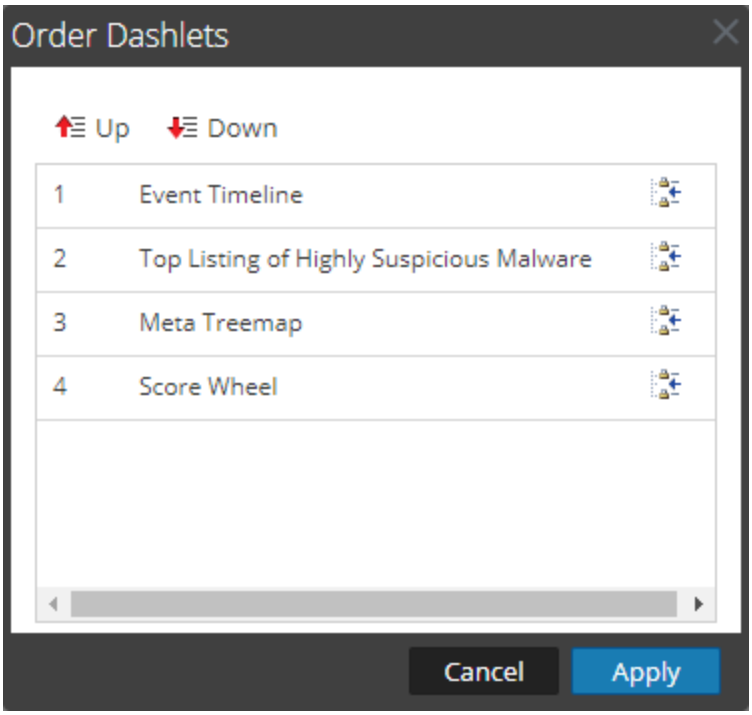


2. Geben Sie einen neuen Titel für das Dashlet in das Feld **Titel** ein.
3. Wenn Sie nur Ereignisse sehen möchten, die von dem Tag Hohe Wahrscheinlichkeit beeinflusst sind, was bedeutet, dass eine hohe Wahrscheinlichkeit besteht, dass das Ereignis gefährlichen Code enthält, aktivieren Sie die Optionen **Nur durch hohe Wahrscheinlichkeit beeinflusst**.
4. Wenn Sie nur Ereignisse sehen möchten, die ein Ergebnis über einem bestimmten Wert in den vier Kategorien (Statisch, Netzwerk, Community und Sandbox) erhalten haben, ziehen Sie den entsprechenden Schieberegler oder geben Sie einen numerischen Wert ein und wählen Sie dann einen Operator in der Drop-down-Liste aus: =, >= oder <=.
5. Klicken Sie auf **Anwenden**.
   Der Titel und der Filter werden auf das Dashlet angewendet.

Dashlets anordnen

So ändern Sie die Reihenfolge der Dashlets, wie sie unter der Ereigniszusammenfassung angezeigt werden:

1. Wählen Sie in der Symbolleiste > **Dashlets anordnen** aus.
   Das Dialogfeld „Dashlets anordnen“ wird angezeigt.



2. Wählen Sie ein Dashlet aus, das Sie nach oben oder unten bewegen möchten, und klicken Sie auf Up oder Down.
3. Wenn Sie mit der Reihenfolge zufrieden sind, klicken Sie auf **Anwenden**.
   Das Dialogfeld wird geschlossen und die Reihenfolge der Dashlets unter der Ereigniszusammenfassung wird entsprechend Ihren Wünschen geändert.

Wiederherstellen von Standard-Dashlets

Nachdem Sie Dashlets hinzugefügt, geändert und angeordnet haben, können Sie zu den Standardeinstellungen für die Anzeige der Dashlets zurückkehren. So stellen Sie die Standard-Dashlets wieder her:

1. Wählen Sie in der Symbolleiste > **Standardkonfiguration wiederherstellen** aus.
   Ein Dialogfeld fordert Sie auf, zu bestätigen, dass Sie die Konfiguration wiederherstellen möchten.
2. Führen Sie einen der folgenden Schritte aus:
   a. Wenn Sie sich entscheiden, die Anordnung der Dashlets so zu lassen, wie Sie sie konfiguriert haben, klicken Sie auf **Nein**.
   b. Wenn Sie sicher sind, dass Sie die Standardkonfiguration wiederherstellen möchten, klicken Sie auf **Ja**.
      Die Anzeige der Dashlets wird auf die Standardanzeige zurückgesetzt.

Starten einer Ermittlung

NetWitness Platform bietet verschiedene Ausgangspunkte, basierend auf der Frage, die Sie beantworten möchten: „Navigation“, „Ereignisse“, „Ereignisanalyse“, „Hosts“, „Dateien“ oder „Malware Analysis“.

Hinweis: Spezifische Benutzerrollen und -berechtigungen werden von einem Benutzer benötigt, damit dieser Ermittlungen in NetWitness Platform durchführen kann. Wenn Sie eine Analyseaufgabe nicht durchführen oder eine Ansicht nicht sehen können, muss der Administrator unter Umständen die für Sie konfigurierten Rollen und Berechtigungen anpassen. Die Ansichten „Hosts“ und „Dateien“ sind in Version 11.1 und höher verfügbar. Die Ansicht „Ereignisanalyse“ war in Version 11.0 verfügbar, aber die Zugriffsmethode erfolgte über die Ansicht „Ereignisse“. In Version 11.1 und höher können Sie direkt auf die Ansicht „Ereignisanalyse“ zugreifen.

Fokus auf Metadaten, Raw-Ereignisse und Ereignisanalyse

Um nach Ereignissen zu suchen, die den Workflow für die Reaktion auf Incidents voranbringen, oder um strategische Analysen durchzuführen, nachdem ein anderes Tool ein Ereignis erzeugt hat, sollten Sie in der Ansicht „Navigation“, „Ereignisse“ oder „Ereignisanalyse“ beginnen. Untersuchen Sie die Metadaten auf einen einzelnen Broker oder Concentrator. In jeder dieser Ansichten starten Sie die Ermittlung, indem Sie die Ansicht öffnen, in dem Sie eine Abfrage ausführen und die Ergebnisse filtern können, indem Sie den Zeitbereich eingrenzen und Metadaten abfragen. Diese Themen bieten Details zum Starten einer Ermittlung in jeder Ansicht:

- Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
- Starten einer Ermittlung in der Ansicht „Ereignisanalyse“

Fokus auf Hosts und Dateien

Um Informationen auf Hosts zu suchen, auf denen der Agent ausgeführt wird, starten Sie die Ermittlung in der Ansicht „Hosts“ (**Untersuchen > Hosts**). Für jeden Host können Sie Prozesse, Treiber, DLLs, (ausführbare) Dateien, Services und automatische Ausführungen sehen, die ausgeführt werden, sowie Informationen in Bezug auf angemeldete Benutzer. (Siehe Untersuchen von Hosts.)

Sie können die Ermittlung auf Dateien in Ihrer Bereitstellung in der Ansicht „Dateien“ starten (**Untersuchen > Dateien**). (Siehe Untersuchen von Dateien.)

Hinweis: Zum Laden der Ansicht „Hosts und Dateien“ müssen Sie die Berechtigung `endpoint-server.filter.manage` haben.

Fokus auf Scannen von Dateien auf Malware

Um Dateien auf potenzielle Schadsoftware zu scannen oder um den kontinuierlichen Scan eines Service einzurichten, können Sie in der Ansicht „Malware Analysis“ beginnen. Ergebnisse werden mithilfe von vier Arten von Analysen ausgedrückt: Netzwerk, statisch, Community und Sandbox, mit einem IOC-Rating (Indicator of Compromise, Indikator für eine Infizierung). Es gibt mehrere Möglichkeiten, mit Malware Analysis zu beginnen:

- Sie können Malware Analysis von den Malware Analysis-Dashlets in der Überwachungsansicht aus starten, um schnell die risikoreichsten potenziellen Bedrohungen zu sehen.
- Gehen Sie zu **Untersuchen > Malware Analysis**, um die Ereigniszusammenfassung in Malware Analysis zu öffnen.
- Sie können mit der rechten Maustaste auf einen Metaschlüssel in der Ansicht „Navigation“ klicken und **Auf Schadsoftware scannen** auswählen.

Weitere Informationen zum Arbeiten in der Ansicht „Malware Analysis“ finden Sie unter Durchführen von Schadsoftwareanalysen.

Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Die Ansicht Navigieren ist die Standardansicht für Untersuchen, es sei denn, Sie haben eine andere Ansicht als Ihre Startansicht ausgewählt. Diese Benutzereinstellung wird auf Anwendungsebene festgelegt, wie beschrieben unter Konfigurieren von Ansichten und Voreinstellungen von NetWitness Investigate. In den Ansichten „Navigation“ und „Ereignisse“ suchen Sie basierend auf einer Abfrage nach Ereignissen von Interesse. In der Navigationsansicht können Sie auch Ergebnisse optimieren, indem Sie auf Metaschlüssel und Metawerte klicken. Wenn Sie interessante Ereignisse finden, können Sie sich das Ereignis in den anderen Untersuchen-Ansichten genauer ansehen.

Um eine Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“ zu starten, muss ein Service angegeben werden.

- NetWitness Platform öffnet die Ansicht „Navigation“ oder „Ereignisse“ mit dem ausgewählten benutzerdefinierten Standardservice.
- Wenn derzeit kein Standardservice festgelegt ist und die Service-ID sich nicht in der URL befindet, öffnet NetWitness Platform ein Dialogfeld zur Auswahl des zu untersuchenden Services oder der Sammlung.
- Wenn ein Service manuell oder standardmäßig in der Ansicht „Navigation“ oder „Ereignisse“ ausgewählt wurde, können Sie den zu untersuchenden Service ändern, indem Sie in der Symbolleiste den Servicenamen auswählen. NetWitness Platform öffnet das Dialogfeld zur Auswahl des zu untersuchenden Services.

Hinweis: Der Archiver-Service wird nicht in der Ansicht „Navigation“ angezeigt, damit Benutzer während einer Ermittlung keine Verlangsamung der Performance erfahren. Der Archiver ist in der Ansicht „Ereignisse“ zum Exportieren von Protokollen und erweiterten Suchfunktionen verfügbar.

Sobald ein Service oder eine Sammlung ausgewählt wurde, ist NetWitness Platform bereit, Daten für den Service oder die Sammlung zu laden. Es wird empfohlen, auch einen Zeitbereich auszuwählen, damit Ergebnisse schneller geladen werden. Mehrere Einstellungen im Einstellungsdialog der Ansichten „Navigation“ und „Ereignisse“ oder auf der Registerkarte „Profile“ > Bereich „Einstellungen“ > „Ermittlungen“ wirken sich auf den Ladevorgang aus: „Schwellenwert“, „Max. Wertergebnisse“, „Debuginformationen anzeigen“, „Werte automatisch laden“ und „Optimieren des Ladens der Seite Investigation“ (siehe Konfigurieren von Ansichten und Voreinstellungen von NetWitness Investigate).

Hinweis: In der Ansicht „Ereignisse“ werden Daten automatisch geladen. Wenn Sie „Werte automatisch laden“ in den Einstellungen der Ansicht „Navigation“ angegeben haben, aktualisiert NetWitness Platform die Daten automatisch. Andernfalls müssen Sie auf die Schaltfläche „Werte laden“ klicken. NetWitness Platform aktualisiert die Metadaten im Bereich „Werte“ in der Ansicht „Navigation“ und die Ergebnisse werden sofort angezeigt.

Der restliche Teil dieses Themas bietet Anleitungen zum Starten einer Ermittlung von Daten für einen Service.

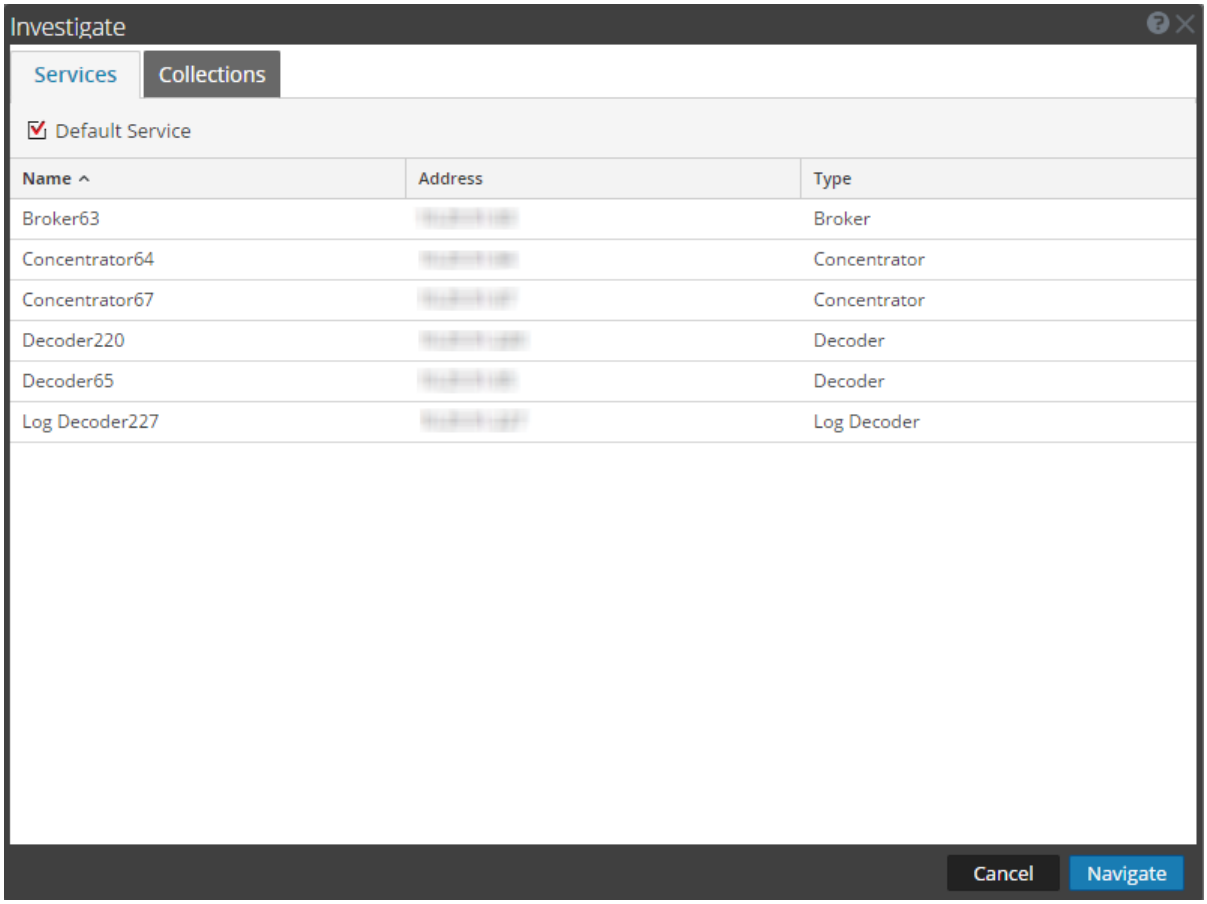
Hinweis: Nur Benutzer mit Administratorrolle können eine Sammlung erstellen und nur der Ersteller der Sammlung kann eine Ermittlung zu einer Sammlung durchführen.

Nach dem Laden von Daten in der Ansicht „Navigation“ oder „Ereignisse“:

1. Optimieren Sie Ergebnisse, visualisieren Sie Daten und führen Sie Aktionen an einem Drill-down-Punkt durch (siehe Untersuchen von Metadaten in der Ansicht „Navigation“ und Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse“. Möglich ist beispielsweise das Suchen von weiteren Kontexten in den Ansichten „Navigation“ und „Ereignisse“, das Starten eines Malware Analysis-Scans in der Ansicht „Navigation“ oder das Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion.
2. Rekonstruieren Sie ein Ereignis (siehe Rekonstruieren eines Ereignisses) oder zeigen Sie die interaktive Ereignisanalyse eines Ereignisses an (siehe Starten einer Ermittlung in der Ansicht „Ereignisanalyse“).

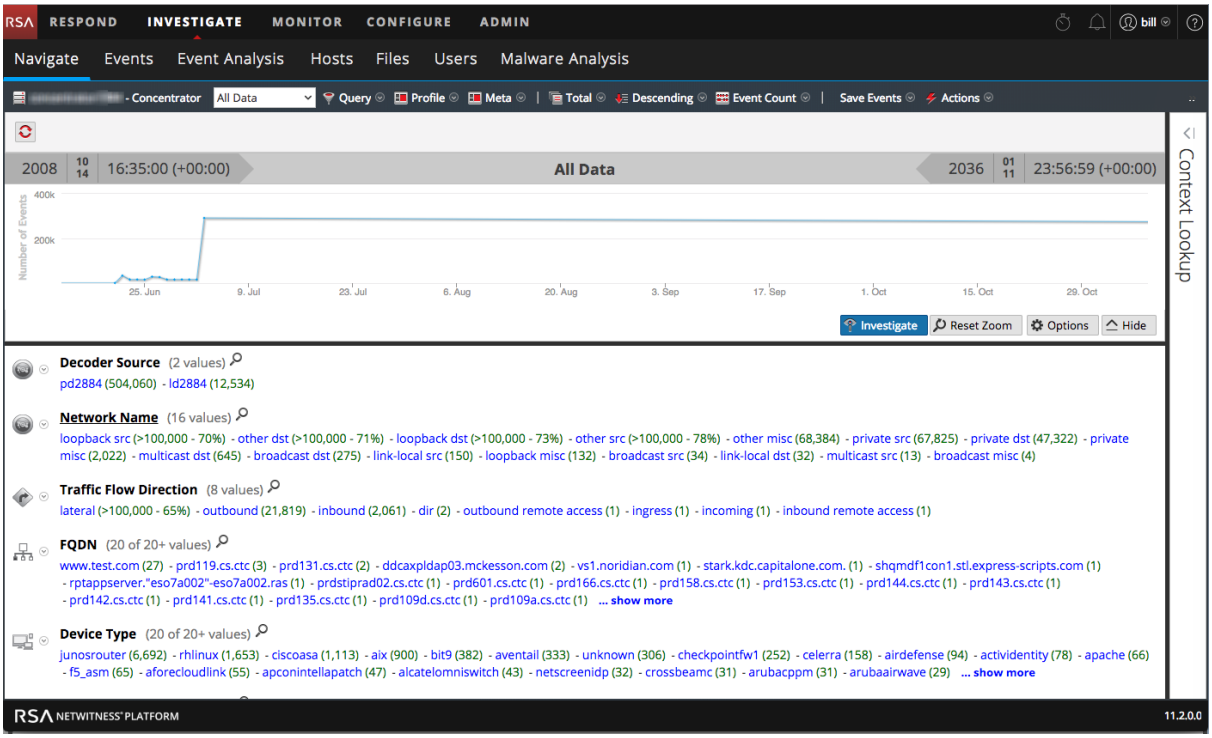
Starten einer Ermittlung (ohne Standardservice)

1. Navigieren Sie zu **UNTERSUCHEN > Navigation** oder **Ereignisse**.
   Das Dialogfeld „Untersuchen“ wird angezeigt.



2. Doppelklicken Sie auf einen Service oder wählen Sie einen Service, in der Regel einen Concentrator, aus und klicken Sie auf **Navigieren**.
   In der Ansicht „Ereignisse“ werden Daten automatisch geladen. Wenn Sie in der Ansicht „Navigation“ arbeiten, zeigt der daraufhin angezeigte Bereich die Aktivität für den ausgewählten Service an, aber die Daten werden nicht automatisch geladen.

3. (Empfohlen) Wählen Sie einen bestimmten Zeitbereich aus, damit Ergebnisse schneller laden.
4. Wenn Sie die Ermittlungsoptionen vor dem Laden ändern möchten, können Sie z. B. ein benutzerdefiniertes Profil erstellen oder ändern, einen anderen Zeitraum anwenden, eine Metagruppe erstellen oder anwenden und eine benutzerdefinierte Abfrage ausführen, wie in Abfragen von und Reagieren auf Daten in den Ansichten „Navigation“ und „Ereignisse“ beschrieben. Sie können auch jederzeit während der Untersuchung Optionen ändern.
5. Klicken Sie zum Laden von Daten in der Ansicht „Navigation“ auf Load Values.
   Der Vorgang des Ladens der Daten des ausgewählten Services beginnt.

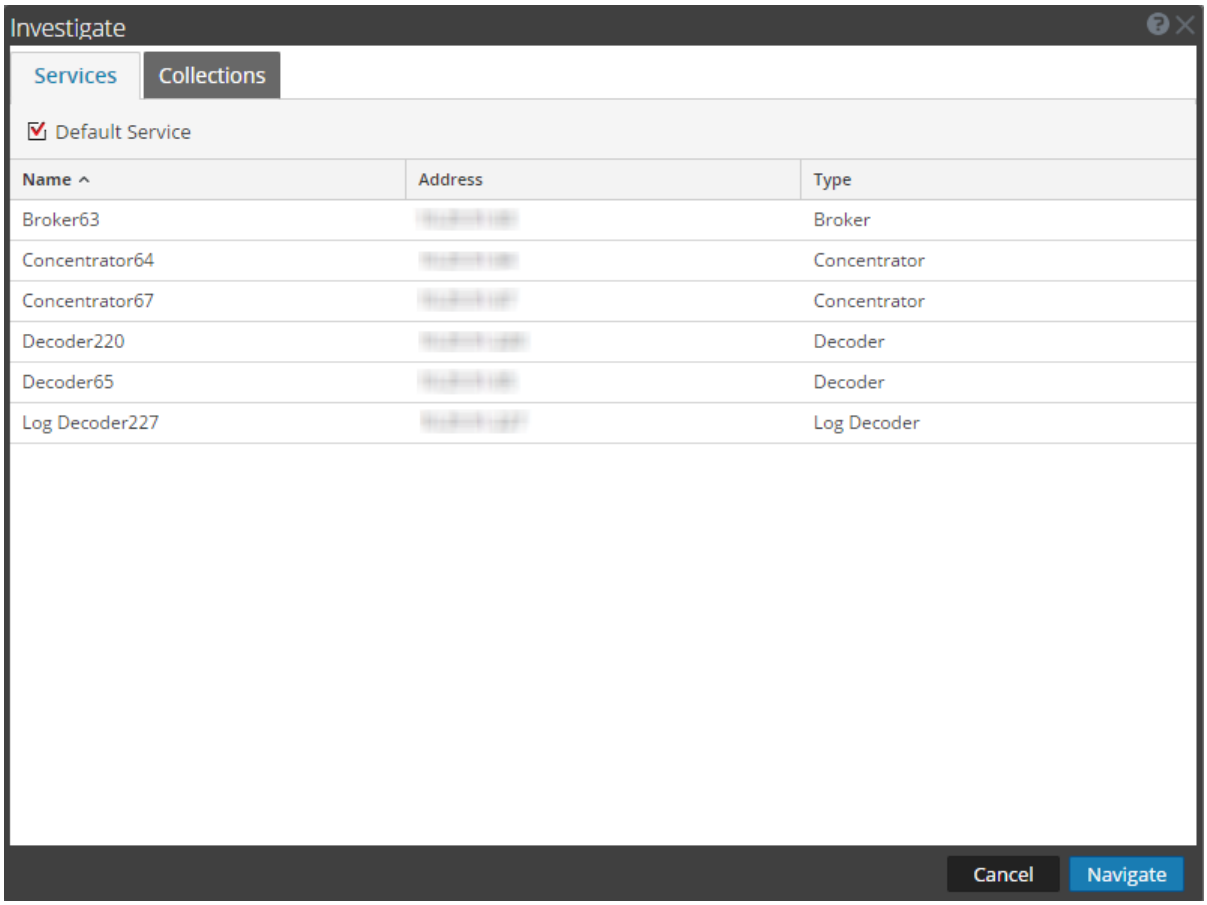


   Wenn der Service ausgewählt ist und die Daten geladen sind, können Sie mit dem Analysieren der Daten beginnen.

Einrichten oder Löschen des Standardservices

Sie können den Standardservice im Dialogfeld „Service ermitteln“ festlegen oder löschen.

1. Klicken Sie auf der Symbolleiste auf den Servicenamen.
   Das Dialogfeld „Untersuchen“ wird angezeigt.



2. Wählen Sie im Raster **Services** einen Service aus und klicken Sie auf Default Service.
   Der Service wird als Standard eingestellt (angezeigt durch **Standard** in Klammern hinter dem Servicenamen).

3. Löschen Sie den Standardservice, indem Sie ihn im Raster auswählen, auf Default Service und anschließend auf **Abbrechen** klicken, um das Dialogfeld zu schließen.
   Es wurde kein Standardservice eingerichtet.

   Hinweis: Durch die Schaltfläche Abbrechen wird der von Ihnen ausgewählte Standardservice nicht abgebrochen. Es wird lediglich das Dialogfeld geschlossen, ohne im Raster zum aktuell ausgewählten Service zu navigieren. Durch das Einrichten eines Standardservices, der sich vom aktuell einer Ermittlung unterzogenen Service unterscheidet, wird die Ansicht Navigation nicht automatisch aktualisiert. Sie müssen explizit einen anderen Service auswählen und zu diesem navigieren.

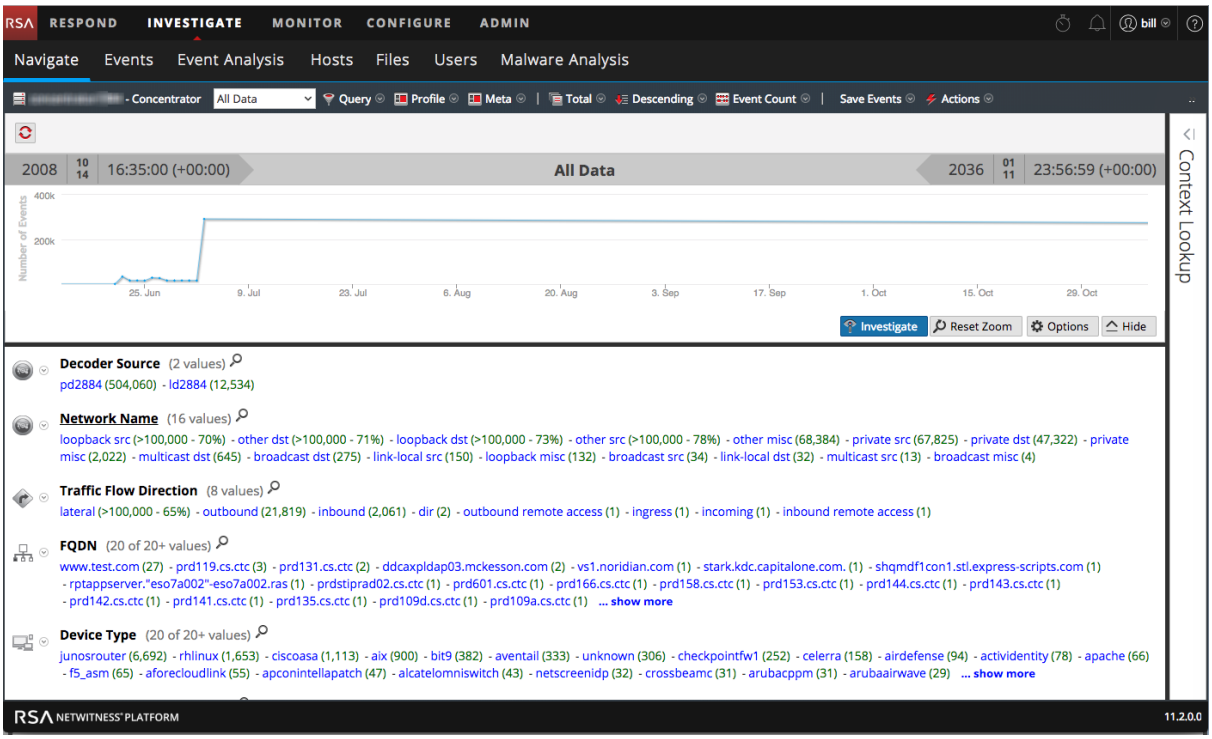
Starten einer Ermittlung (Standardservice angegeben)

1. Navigieren Sie zu **Ermittlung > Navigieren** oder **Ereignisse**.
   Wenn „Werte automatisch laden“ deaktiviert ist, wird die Ansicht „Navigation“ mit dem ausgewählten Standardservice angezeigt und ist bereit zum Laden von Daten. Wenn Werte

automatisch laden aktiviert ist, werden die Werte wie in Schritt 3 dargestellt geladen. In der Ansicht „Ereignisse“ werden Daten automatisch geladen.

2. Wenn Sie die Ermittlungsoptionen in der Ansicht „Navigation“ vor dem Laden ändern möchten, können Sie z. B. ein benutzerdefiniertes Profil erstellen oder ändern, einen anderen Zeitraum anwenden, eine Metagruppe erstellen oder anwenden und eine benutzerdefinierte Abfrage ausführen.

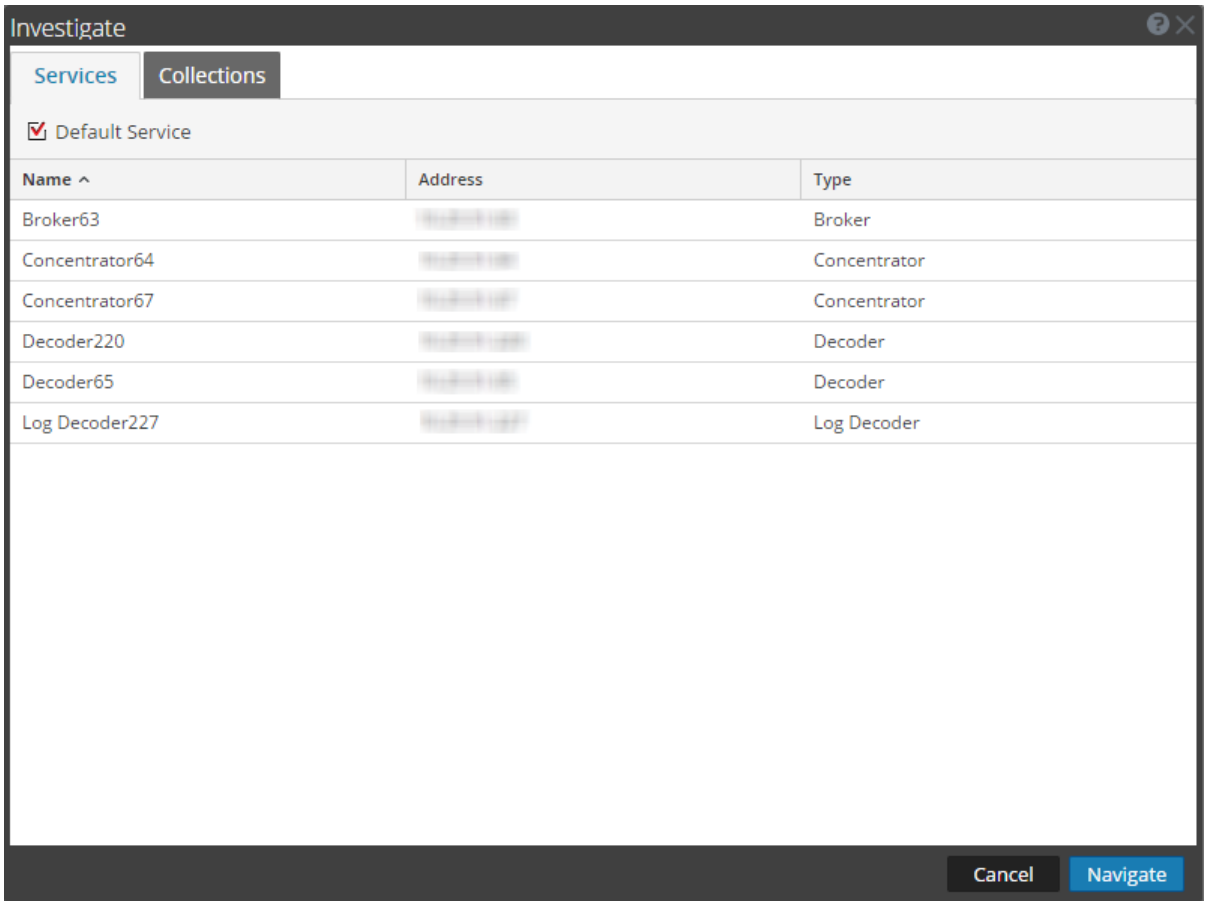
3. Wenn Sie dies abgeschlossen haben, klicken Sie auf Load Values.
   Die Werte für den Service werden entsprechend der ausgewählten Optionen geladen.



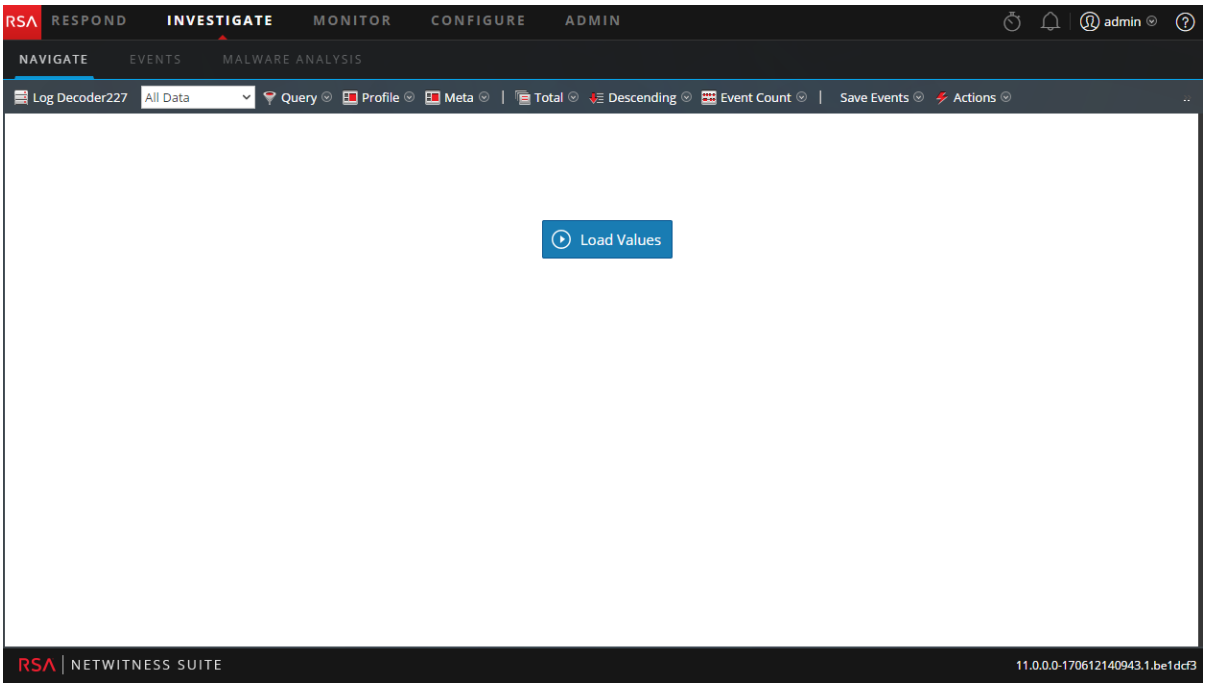
Wenn der Service ausgewählt ist und die Daten geladen sind, können Sie mit dem Analysieren der Daten beginnen.

Ändern des zu untersuchenden Services oder der Sammlung

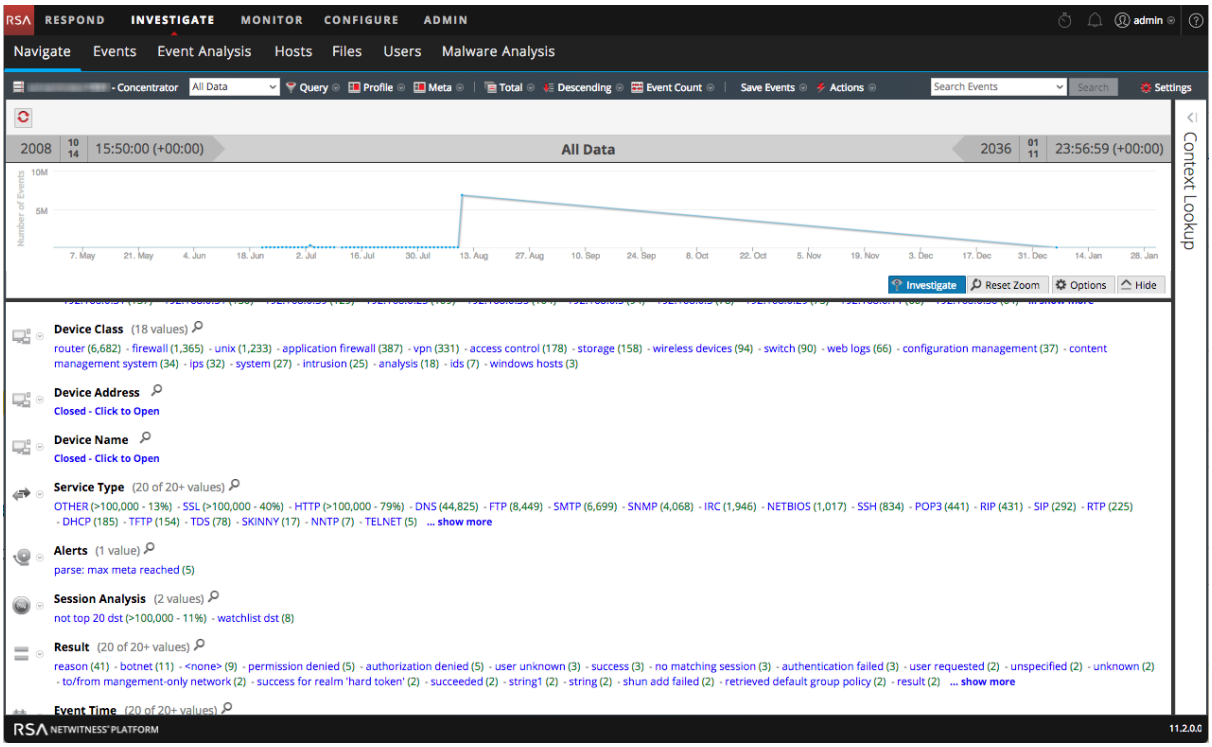
1. Klicken Sie in der Ansicht „Navigation“ oder „Ereignisse“ auf den Servicenamen ganz oben im Bereich „Optionen“.
   Das Dialogfeld „Untersuchen“ wird angezeigt.



2. Doppelklicken Sie auf einen Service oder wählen Sie einen Service aus und klicken Sie auf **Navigation**. Der daraufhin angezeigte Bereich enthält die Aktivität für den ausgewählten Service. Wenn Werte automatisch laden aktiviert ist, werden die Werte wie in Schritt 3 dargestellt geladen. Andernfalls wird die Ansicht „Navigation“ mit dem ausgewählten Standardservice angezeigt und die Daten können geladen werden. In der Ansicht „Ereignisse“ werden Daten automatisch geladen.



3. Wenn Sie fertig sind, klicken Sie auf Load Values.
   Die Werte für den Service werden entsprechend den ausgewählten Optionen geladen.



Wenn der Service ausgewählt ist und die Daten geladen sind, können Sie mit dem Analysieren der Daten beginnen.

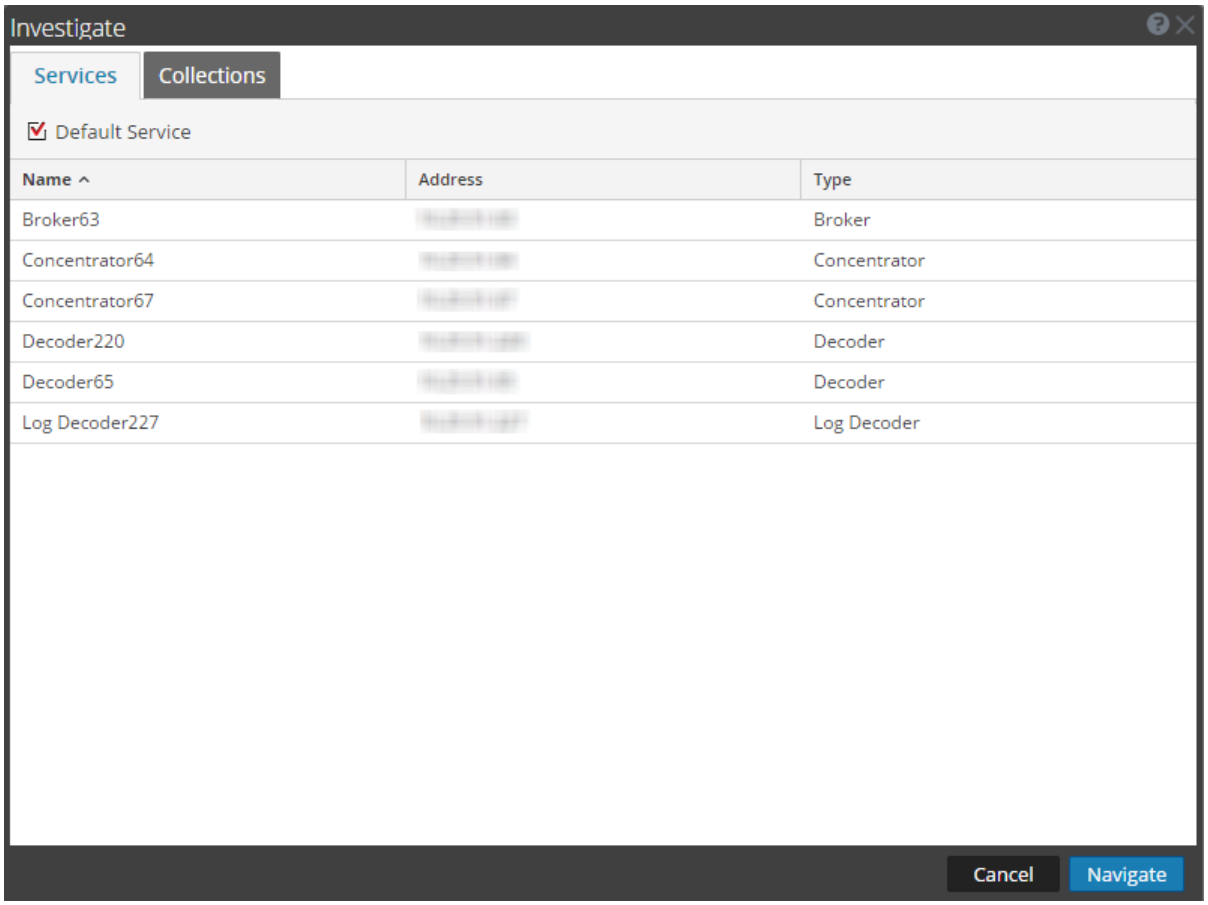
Untersuchen von Workbench-Wiederherstellungssammlungen

Mithilfe dieses Verfahrens können Administratoren Inhalte aus einer bestehenden Sammlung zur erneuten Verarbeitung für eine tiefergehende Ermittlung auswählen. Dies gilt für Decoder, die Workbench-Services nutzen.

Hinweis: Nur Benutzer mit Administratorrechten können eine Sammlung erstellen und Sie können nur die Sammlungen anzeigen, die Sie erstellt haben.

So verarbeiten Sie Daten für eine tiefergehende Untersuchung erneut:

1. Navigieren Sie zu **Ermittlung > Navigieren** oder **Ereignisse**.
   Das Dialogfeld „Untersuchen“ wird angezeigt.



2. Wählen Sie einen zu untersuchenden Workbench-Service und Workbench-Namen aus.
3. Klicken Sie auf **Navigation**, um eine Ermittlung zu dem von Ihnen ausgewählten Workbench-Service durchzuführen.
   Klicken Sie auf **Abbrechen**, um einen anderen Workbench-Service für die Ermittlung auszuwählen.
   Die Ansicht „Ermittlungen“ wird angezeigt.

Wenn die Sammlung ausgewählt ist und die Daten geladen sind, können Sie mit dem Analysieren der Daten beginnen.

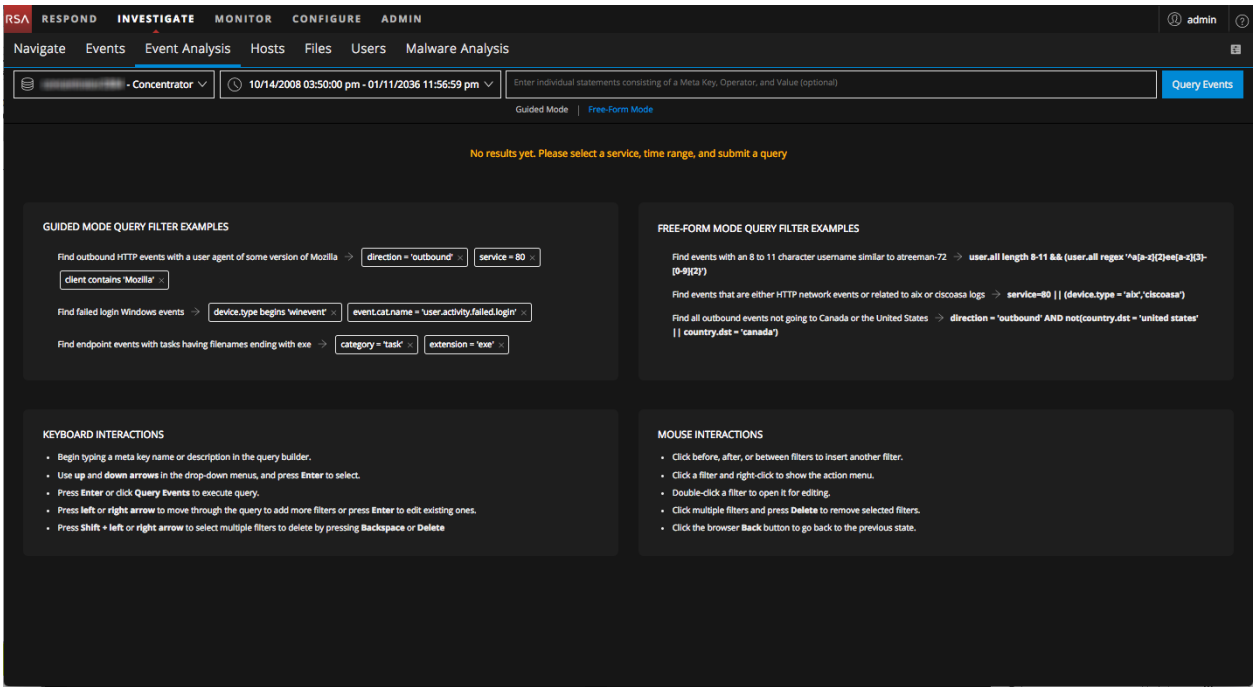
Starten einer Ermittlung in der Ansicht „Ereignisanalyse“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Die Ansicht „Ereignisanalyse“ bietet die meisten Funktionen, die in den Ansichten „Navigation“ und „Ereignisse“ verfügbar sind. Ähnlich wie in der Ansicht „Navigation“ gibt es eine Ansicht von Metaschlüsseln und Metawerten für Protokolle, Endpunkte und Pakete. Wie in der Ansicht „Ereignisse“ zeigt eine Ereignisliste Ereignisse nach Uhrzeit geordnet an und Sie können das Raw-Ereignis, zugehörige Metadaten und eine Rekonstruktion eines Ereignisses anzeigen. Die Rekonstruktion der Ereignisanalyse gibt einige nützliche Hinweise zur Identifizierung interessanter Punkte in einer Rekonstruktion. Siehe Analysieren von Raw-Ereignissen und Metadaten in der Ansicht „Ereignisanalyse“

Hinweis: In Version 11.0 können Sie in der Ansicht „Ereignisanalyse“ keine Ermittlung beginnen. Stattdessen beginnen Sie die Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“ und öffnen ein Ereignis in der Ansicht „Ereignisanalyse“. In Version 11.1 erhalten Sie über ein Untermenü „UNTERSUCHEN“ direkten Zugriff auf die Ansicht „Ereignisanalyse“ sowie die Möglichkeit, einen anderen Service und Zeitraum auszuwählen und eine Abfrage zu erstellen.

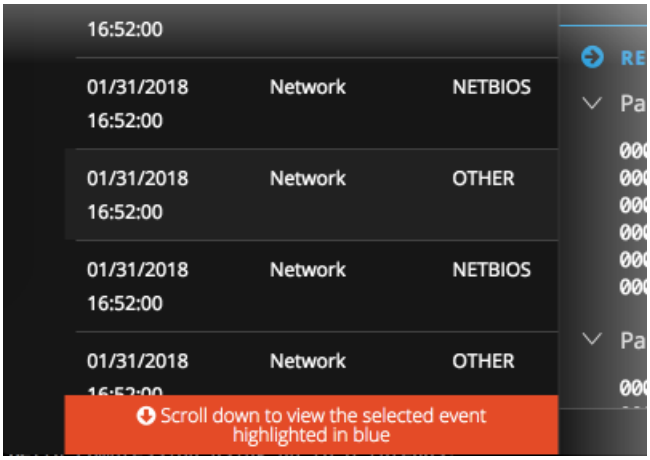
In der folgenden Abbildung ist die ursprüngliche Ansicht „Ereignisanalyse“ mit Kurzinformationen zu Abfragebeispielen dargestellt.



Öffnen Sie die Ansicht „Ereignisanalyse“ (ab Version 11.1)

Sie können die Ansicht „Ereignisanalyse“ in Version 11.1 auf verschiedene Weisen öffnen.

- Wenn Sie die Option **Aktionen > In Ereignisanalyse zu Ereignis wechseln** in der Ansicht „Navigation“ verwenden und eine Ereignis-ID eingeben, öffnet die Ansicht „Ereignisanalyse“ das Einzelereignis als eine Rekonstruktion. Zur Vereinfachung der Ansicht enthält die Symbolleiste nicht die unnötigen Optionen zum Erweitern, Verkleinern und Schließen von Fenstern. Sie können mit der Arbeit beginnen, wie unter Analysieren von Raw-Ereignissen und Metadaten in der Ansicht „Ereignisanalyse“ beschrieben.
- Wenn Sie den Mauszeiger über einen Zähler (grüne Zahl nach einem Metawert steht) in der Navigationsansicht bewegen und auf **Ereignisanalyse in neuer Registerkarte öffnen** klicken, öffnet sich die Ansicht „Ereignisanalyse“ mit der Liste der Ereignisse für den ausgewählten Drill-down-Punkt und Sie können mit der Arbeit beginnen, wie unter Analysieren von Raw-Ereignissen und Metadaten in der Ansicht „Ereignisanalyse“ beschrieben. Die Liste der Ereignisse kann sehr lang sein und es besteht die Möglichkeit, dass das Ereignis, das Sie ausgewählt haben, auf der aktuellen Seite der Ereignisse nicht angezeigt wird. In diesem Fall empfiehlt eine Meldung, dass Sie nach unten blättern, um das Ereignis anzuzeigen.



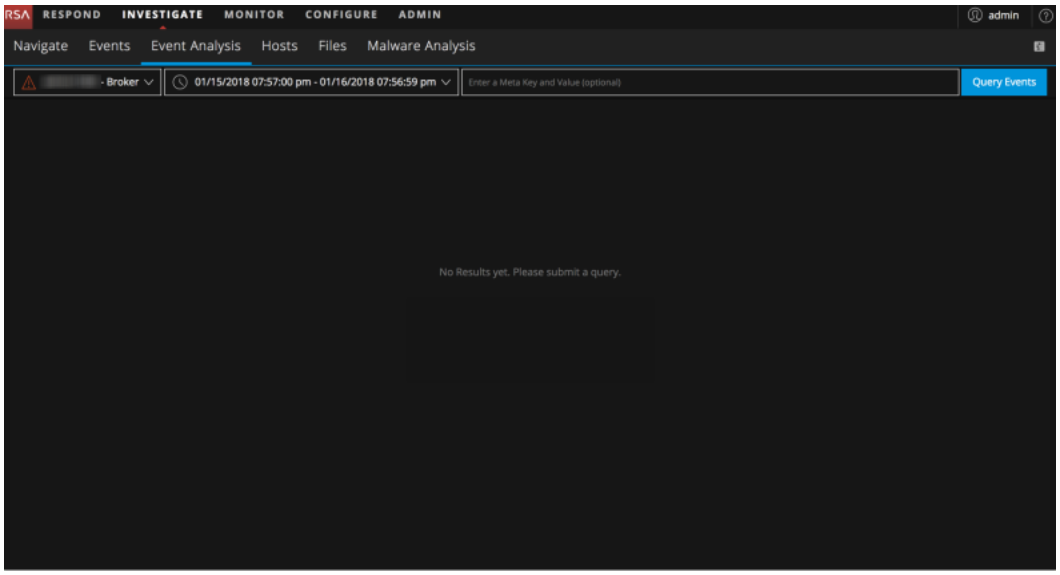
- Sie können auf die Ansicht „Ereignisanalyse“ auch direkt zugreifen, indem Sie zu **UNTERSUCHEN > Ereignisanalyse** oder zu **UNTERSUCHEN** wechseln, wenn Sie festgelegt haben, dass sich die Ansicht „Ereignisanalyse“ als erste Ermittlungsansicht öffnet. Wenn Sie sich erstmals auf der Ansicht „Ereignisanalyse“ befinden, müssen Sie einen Service auswählen, um die Analyse zu beginnen. Wenn Sie die Ansicht „Ereignisanalyse“ nicht zum ersten Mal öffnen, wird der zuletzt verwendete Service solange gespeichert, bis der lokale Browserspeicher gelöscht wird. Wenn Sie die Ansicht „Ereignisanalyse“ von einem der anderen Ermittlungsansichten aus öffnen, werden Service und Abfrage aus dieser Ansicht übernommen. Sie können den Service ändern, einen Zeitraum wählen und eine Abfrage eingeben, wenn Sie die Ergebnisse verfeinern möchten, bevor Sie die Ansicht „Ereignisanalyse“ öffnen, wie unter Filtern von Ergebnissen in der Ansicht „Ereignisanalyse“ beschrieben.

So greifen Sie direkt auf die Ansicht „Ereignisanalyse“ zu:

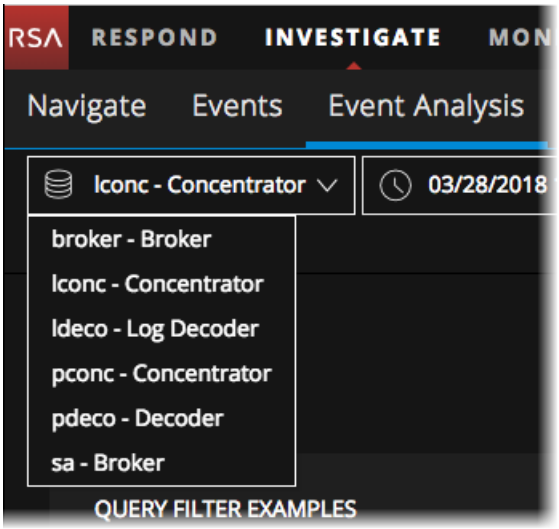
1. Navigieren Sie zu **UNTERSUCHEN** > **Ereignisanalyse**.
   Die Ansicht „Ereignisanalyse“ öffnet sich, wobei der erste Service in der Liste der Services ausgewählt ist und keine Daten angezeigt werden. Das Feld **Service auswählen** wird zunächst mit dem ersten Service in der Liste oder mit dem letzten ausgewählten Service ausgefüllt. Ein Drop-

down-Menü bietet eine Liste der verfügbaren Services in alphabetischer Reihenfolge zur Auswahl. Standardmäßig wird die Liste der verfügbaren Services alle zwölf Stunden aktualisiert und auf dem NetWitness-Server zwischengespeichert. Wenn ein Service vom NetWitness-Server entfernt oder diesem hinzugefügt wird, wird der Cache mit der aktuellen Liste der Services aktualisiert. Am Anfang des Felds zeigt ein Symbol den Status der Abfrage an.

- und kein Servicename = kein Service ist ausgewählt.
- und Name des ausgewählten Services = der Service ist ausgewählt.
- = Investigate versucht, eine Verbindung zu dem ausgewählten Service herzustellen.
- = Investigate kann keine Verbindung zu dem ausgewählten Service herstellen oder es sind keine Daten vorhanden. In diesem Zustand wird das Steuerelement zur Auswahl von Services rot und eine Kurzinformation erklärt, warum der Verbindungsversuch fehlgeschlagen ist, und rät Ihnen, einen anderen Service auszuwählen.



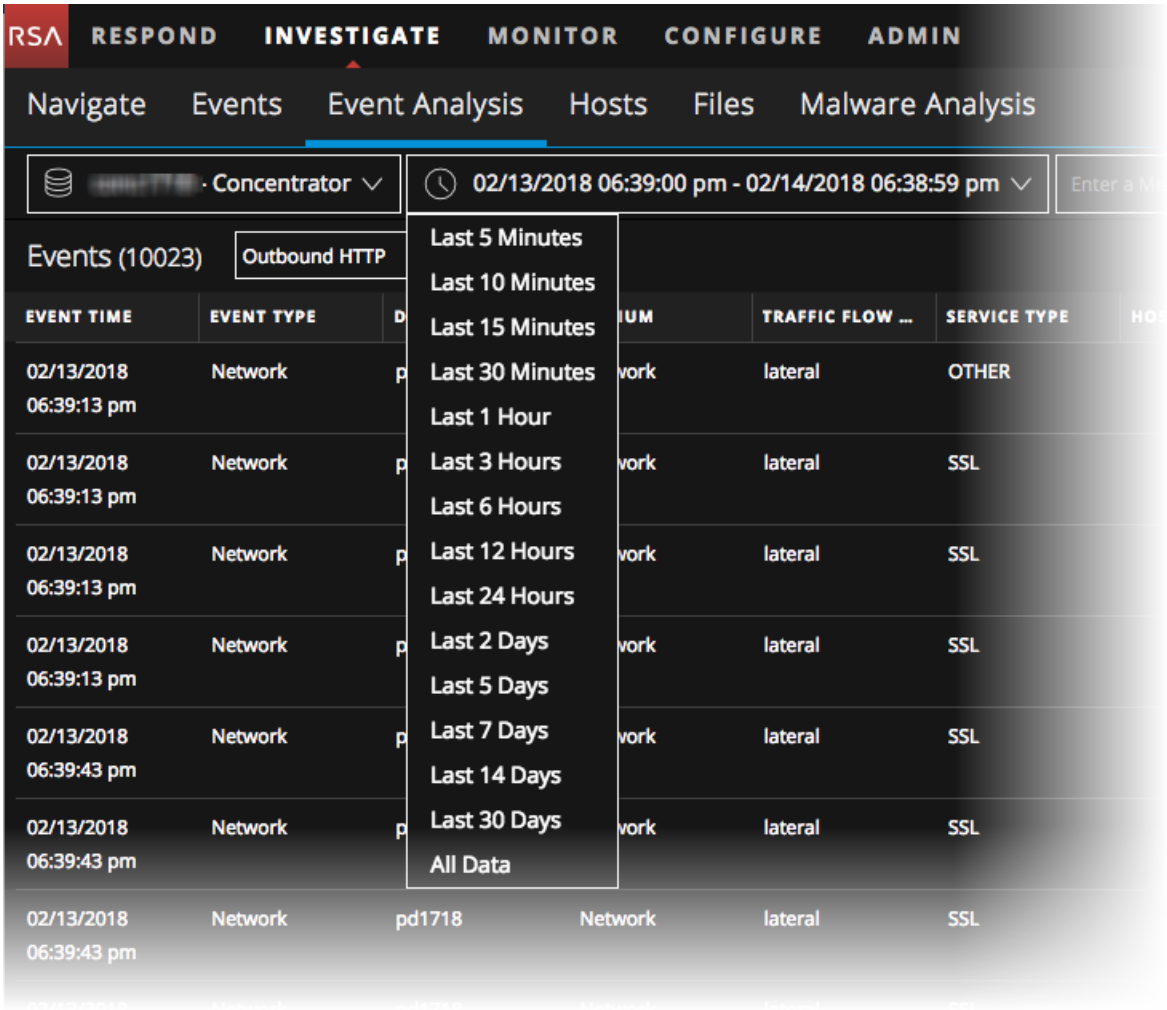
2. (Optional) Wählen Sie einen Service, in der Regel einen Concentrator, aus der Drop-down-Liste aus.



Die Zeitbereichsauswahl zeigt entweder den Standardzeitbereich von 24 Stunden oder den

Zeitbereich an, den Sie für diesen Service zuletzt ausgewählt haben. Die Schaltfläche „Ereignisse abfragen“ wird aktiviert und Sie können Filter eingeben. Wenn Sie jetzt eine Abfrage starten, wird die ausgewählte Zeit verwendet.

3. (Optional) Klicken Sie, um einen Zeitbereich in der Zeitbereichsauswahl auszuwählen, in die Auswahl **Zeitbereich** und wählen Sie einen Zeitbereich aus der Drop-down-Liste aus. Sie können aus den letzten 5, 10, 15 oder 30 Minuten, den letzten 1, 3, 6, 12 oder 24 Stunden oder den letzten 2, 5, 7, 14 oder 30 Tagen oder alle Daten wählen. (Der Zeitbereich basiert auf Einstellungen, die für die Ansicht „Ereignisanalyse“ vorgenommen wurden. Die Standardbasis für den Zeitbereich ist die Datenbankzeit; Sie können stattdessen die Uhrzeit auswählen.)
Der ausgewählte Zeitbereich wird in Ihrem Browser für diesen Service; gespeichert. Sie können verschiedene Zeitbereiche für verschiedene Services festlegen.



4. Geben Sie eine Abfrage ein, indem Sie einen oder mehrere Filter erstellen, die mindestens einen Metaschlüssel oder eine Metaentität, einen Operator und einen optionalen Wert enthalten. Details zur Eingabe von Abfragen finden Sie unter Filtern von Ergebnissen in der Ansicht „Ereignisanalyse“.

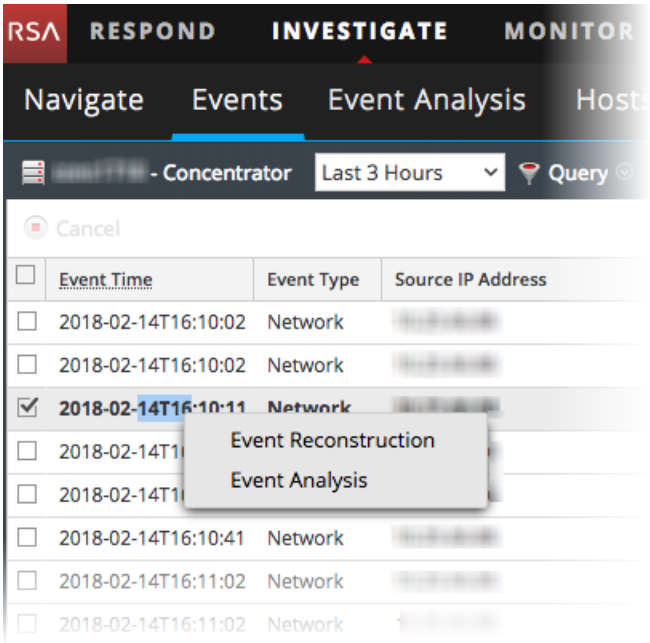
5. Klicken Sie auf **Ereignisse abfragen**.
Die Ansicht „Ereignisanalyse“ zeigt die Aktivität für den ausgewählten Service und Zeitbereich an, in Übereinstimmung mit den Berechtigungen, die Ihrer Rolle vom Administrator zugewiesen wurden.

Wenn der Service ausgewählt ist und die Daten geladen sind, können Sie mit dem Analysieren der Daten beginnen. Informationen dazu, wie Sie in der Ansicht „Ereignisanalyse“ arbeiten können, finden Sie unter Analysieren von Raw-Ereignissen und Metadaten in der Ansicht „Ereignisanalyse“.

Öffnen Sie die Ansicht „Ereignisanalyse“ (Version 11.0)

So öffnen Sie ein Ereignis in der Ansicht „Ereignisanalyse“:

1. Navigieren Sie zu **UNTERSUCHEN** > **Ereignisse**.
2. Klicken Sie mit der rechten Maustaste auf die aufgelisteten Ereignisse und wählen Sie **Ereignisanalyse**.



Informationen dazu, wie Sie in der Ansicht „Ereignisanalyse“ arbeiten können, finden Sie unter Analysieren von Raw-Ereignissen und Metadaten in der Ansicht „Ereignisanalyse“.

Untersuchen von Metadaten in der Ansicht „Navigation“

Bei der Durchführung einer Ermittlung in der Navigationsansicht stehen Analysten mehrere für die Navigationsansicht spezifische Methoden zur Verfügung, um die Ergebnisse zu verfeinern, Daten zu visualisieren und auf Daten zu reagieren.

- Filtern von Ergebnissen in der Ansicht „Navigation“
- Metagruppen managen
- Visualisieren von Metadaten als Parallelkoordinaten
- Öffnen eines Ereignisses in der Ereignisliste
- Exportieren oder Drucken eines Drill-down-Punkts
- Starten einer externen Suche eines Metaschlüssels
- Starten eines Malware Analysis-Scans in der Ansicht „Navigation“
- Visualisieren des aktuellen Drill-Punkts in Informer

Darüber hinaus können Sie diese Methoden der Abfrage von Daten und Reagieren auf Ergebnisse verwenden, die die Ansichten „Navigation“ und „Ereignisse“ gemeinsam haben.

- Suchen nach Textmustern
- Erstellen einer angepassten Abfrage
- Anzeigen und Ändern von Abfragen mithilfe von URL-Integration
- Einkapseln von benutzerdefinierten Ansichten mithilfe von Profilen
- Verwalten von Context-Hub-Listen und Listenwerten in den Ansichten „Navigation“ und „Ereignisse“
- Suchen von weiteren Kontexten in den Ansichten „Navigation“ und „Ereignisse“
- Rekonstruieren eines Ereignisses

Filtern von Ergebnissen in der Ansicht „Navigation“

Im Zuge von Untersuchungen in der Ansicht „Navigation“ können die angezeigten Ergebnisse beim Laden von Metaschlüsselwerten in der Ansicht „Navigation“ mithilfe von mehreren Methoden verfeinert werden. Analysten stehen folgende grundlegende Filtermethoden zur Verfügung:

- Einstellen des Zeitbereichs
- Einstellen der Quantifizierungsmethode und Sortierreihenfolge von Metaschlüsselergebnissen
- Verwalten und Anwenden von Standardmetaschlüsseln in einer Untersuchung
- Drill-down in die Daten im Zeitdiagramm der Ansicht „Navigation“
- Drill-down zu Daten im Bereich „Werte“

Der Rest dieses Themas konzentriert sich auf die grundlegenden Methoden der Datenfilterung. Darüber hinaus ermöglichen erweiterte Methoden die Konfiguration von Metagruppen, Profilen und Parallelkoordinatenvisualisierungen.

- Visualisieren von Metadaten als Parallelkoordinaten
- Metagruppen managen
- Einkapseln von benutzerdefinierten Ansichten mithilfe von Profilen

Jeder der erweiterten Methoden ist ein separates Thema gewidmet.

Einstellen des Zeitbereichs

Bei der Durchführung einer Untersuchung in der Ansicht „Navigation“ werden die zurückgegebenen Ergebnisse durch die Optionen für den Zeitbereich eingeschränkt. Zur Auswahl stehen:

- Ein Zeitbereich relativ zur Sammlung. Zeitbereiche relativ zur Sammlung basieren auf dem letzten Datenerfassungszeitbereich.
- Ein Zeitbereich relativ zum Kalender.
- Ein angepasster Datumsbereich.
- Alle Daten.

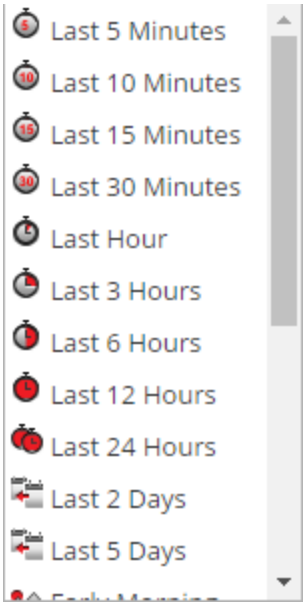
Der ausgewählte Zeitbereich wird in der Symbolleiste der Ansicht „Navigation“ angezeigt. Standardmäßig lautet die Bezeichnung **Letzte 3 Stunden**. In der Ansicht „Zeitbereich“ wird der erste und letzte Zeitstempel für den Datumsbereich angezeigt, der für die Metadaten verwendet wird.

Hinweis: Ein Zeitbereich basiert auf der Zeitzone, die unter „Profileinstellungen“ konfiguriert wurde, wie in „Festlegen von Nutzereinstellungen“ im *Leitfaden für die ersten Schritte mit RSA NetWitness Platform* beschrieben.

So wählen Sie einen vordefinierten Zeitbereich aus:

1. Klicken Sie auf der Symbolleiste der Ansicht „Navigation“ auf die Option **Zeitbereich**.Der standardmäßige Zeitraum lautet **Letzte 3 Stunden, jedoch kann ein anderer Wert, z. B. Alle**

Daten oder **Letzte Stunde**, bereits aus der Auswahlliste ausgewählt worden sein und als Bezeichnung im Bereich „Optionen“ angezeigt werden.
Die Auswahlliste „Zeitbereich“ wird angezeigt.



2. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie alle Daten anzeigen möchten, wählen Sie **Alle Daten** aus.
   - Wenn Sie einen Zeitraum in Minuten, Stunden oder Tagen relativ zur Sammlung festlegen möchten, wählen Sie einen Wert wie z. B. **Letzte 10 Minuten**, **Letzte 3 Stunden** oder **Letzte 5 Tage** aus.
   - Wenn Sie einen Zeitraum relativ zum aktuellen Datum festlegen möchten, wählen Sie **Gestern**, **Diese Woche** (Version 11.1), **Letzte Woche** (Version 11.1), **Den ganzen Tag** oder einen Tagesabschnitt wie **Morgen**, **Vormittag**, **Nachmittag** oder **Abend** aus.
   - Wenn Sie einen eindeutigen Datumsbereich festlegen möchten, wählen Sie im Menü **Zeitbereich** die Option **Angepasst** und befolgen Sie das unten beschriebene Verfahren.
     Der ausgewählte Zeitbereich wird auf die aktuellen Ergebnisse im Bereich Werte angewendet.

So geben Sie einen benutzerdefinierten Zeitbereich an:

1. Wählen Sie im Menü **Zeitbereich** die Option **Benutzerdefiniert** aus.
   In der Symbolleiste werden Optionen zur Auswahl des Datums eingeblendet.

2. Führen Sie die folgenden Schritte aus, um das Datum und die Uhrzeit anhand der in den Feldern **Startdatum** und **Enddatum** angegebenen Werte festzulegen:
   a. Klicken Sie im Kalender auf ein Datum.
   b. (Optional) Wählen Sie die Uhrzeit in den Feldern „Stunde“ und „Minute“ aus oder klicken Sie auf **Jetzt**. Die Uhrzeitauswahl wird standardmäßig auf die aktuelle Uhrzeit eingestellt.

Hinweis: Der Wert für die Startzeit in Sekunden wird standardmäßig immer auf „:00“ und der Wert für die Endzeit in Sekunden standardmäßig immer auf „:59“ festgelegt. Wenn Sie zum Beispiel ein Drill-down in ein Problem durchführen, wird die Zeit für diesen Drill-down als „HH:MM:00 - HH:MM:59“ interpretiert.

3. Zum Anwenden des Zeitraums klicken Sie auf **Start**.
   Der ausgewählte Zeitbereich wird auf die aktuellen Ergebnisse im Bereich Werte angewendet.

Einstellen der Quantifizierungsmethode und Sortierreihenfolge von Metaschlüsselergebnissen

Sie können die Methode auswählen, mit der die Ergebnisse für den jeweiligen Metaschlüssel quantifiziert und in der Ansicht „Navigation“ in einer Reihenfolge sortiert werden.

Hinweis: Wenn Metaeinheiten (Version 11.1 oder höher) in Metagruppen verwendet werden, zeigen die Ergebnisse die 20 Top-Werte an, die mit einem beliebigen Metaschlüssel in der Metaeinheit übereinstimmten.

Jeder Metaschlüsselabschnitt in der Ansicht „Navigation“ enthält eine sortierte Liste von Werten, in der jeder Metaschlüsselwert (Wert) und dessen Anzahl (Gesamt) angezeigt werden. Sie können folgende Einstellungen festlegen:

- Sortierung der Ergebnisse in jedem Metaschlüsselabschnitt anhand von „Wert“ oder „Gesamt“.
- Sortierung der Ergebnisse in aufsteigender oder absteigender Reihenfolge.
- Quantifizierung der Werte für jeden Metaschlüssel anhand der Anzahl von Paketen (Paketanzahl), der Anzahl von Sitzungen oder Protokollen (Nach Ereignisanzahl quantifizieren) oder nach der Größe von Ereignissen (Nach Ereignisgröße quantifizieren).

Hinweis: Wenn Sie die Metaschlüssel sowohl für einen vorhandenen Log Decoder als auch für einen Packet Decoder anzeigen, hängt die Berechnung dessen, was tatsächlich gezählt wird, vom Schlüsseltyp ab. Wenn Sie die Option „Nach Paketanzahl quantifizieren“ auswählen, sehen Sie in den Protokollen, dass diese Ausgabe der Ansicht „Navigation“ mit der Ausgabe übereinstimmt, die Sie bei einer Auswahl der Option „Nach Ereignisanzahl quantifizieren“ erhalten würden. (Weitere Informationen hierzu erhalten Sie unter Ansicht „Navigation“.)

In diesem Bild wird der Metaschlüssel `Event Type` gezeigt, der nach **Gesamt** in der Reihenfolge **Absteigend** sortiert ist. Der Wert mit der höchsten Anzahl von Übereinstimmungen wird zuerst aufgeführt. Der Wert `failure audit` hat 71 Übereinstimmungen und wird zuerst aufgelistet. Der Wert `logon` hat nur eine Übereinstimmungen und wird an letzter Stelle aufgeführt. Die Quantifizierungsmethode ist **Ereignisanzahl**.

In diesem Bild werden die Metaschlüssel `Event Type` gezeigt, die nach **Wert** in der Reihenfolge **Absteigend** sortiert sind. Die Namen der Werte werden in alphabetischer Reihenfolge aufgeführt, beginnend mit dem Ende des Alphabets. Der Wert `success audit` wird zuerst aufgeführt. Der Wert `connect` wird an letzter Stelle aufgeführt. Die Quantifizierungsmethode ist **Ereignisanzahl**.

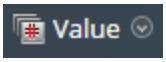
So wählen Sie die Quantifizierungsmethode für die Metaschlüsselanzahl und die Sortierung der Metaschlüsselergebnisse aus, die in der Ansicht „Navigation“ angezeigt werden:

1. Wählen Sie in der Symbolleiste **Ereignisanzahl**, **Ereignisgröße** oder **Paketanzahl** und im Drop-down-Menü eine der Quantifizierungsoptionen aus. Die Bezeichnung für das Menü zeigt die ausgewählte Option an.

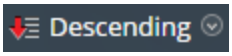
   Die aktuelle Ansicht wird gemäß Ihrer Auswahl erneut geladen.

2. Wählen Sie in der Symbolleiste **Gesamt** oder **Wert** und im Drop-down-Menü eine Sortierreihenfolge aus. Die Bezeichnung für das Menü zeigt die ausgewählte Option an.

   Die aktuelle Ansicht wird gemäß Ihrer Auswahl erneut geladen.

3. Wählen Sie in der Symbolleiste **Aufsteigend** oder **Absteigend** und im Drop-down-Menü eine Sortierreihenfolge aus. Die Bezeichnung für das Menü zeigt die ausgewählte Option an.
   Die aktuelle Ansicht wird gemäß Ihrer Auswahl erneut geladen.

Verwalten und Anwenden von Standardmetaschlüsseln in einer Untersuchung

Wenn Analysten eine Ermittlung erfasster Daten in Investigation durchführen, wird eine Standardanzahl von Metaschlüsseln geladen und in einer Standardsequenz in der Ansicht „Navigation“ > Bereich „Werte“ angezeigt. Der Standardcontent und die Standardsequenz basieren auf den Metaschlüsseln für den Service, der ermittelt wird. Analysten können die Metaschlüssel, die während der Navigation angezeigt werden, spezifizieren, indem sie die Standardmetaschlüssel oder eine benutzerdefinierte Gruppe von Metaschlüsseln auswählen. Dies bietet große Flexibilität bei der Definition von Metaschlüsseln. Dies kann ein direktes Drill-down in die gewünschten Daten erleichtern und die Ladezeit verringern, indem Metadaten, die für diese Ermittlung nicht relevant sind, nicht geladen werden.

Hinweis: In Version 11.1 und höher können Sie bei Verwendung von Metaschlüsseln auch konfigurierte Metaeinheiten verwenden.

Wenn keine benutzerdefinierten Metagruppen aktiv sind, wird die Ansicht „Navigation“ mit der Metaschlüsselsichtbarkeit angezeigt, die im Dialogfeld „Standardmetaschlüssel“ angegeben ist. Um das Laden von Metaschlüsseln in der Ansicht „Navigation“ > Bereich „Werte“ zu optimieren, werden von NetWitness Platform nicht indizierte Metaschlüssel nicht standardmäßig geöffnet. Wenn Sie einen nicht indizierten Metaschlüssel in der Ansicht „Werte“ öffnen, beginnt NetWitness Platform, die Werte dieses Metaschlüssels zu laden. Handelt es sich um eine übermäßige Ladezeit, wird das Laden des Metaschlüssels angehalten und Sie erhalten eine Meldung. Für Titel, Werte und Zähler von nicht indizierten Metaschlüsseln kann kein Drill-down im Bereich Werte angewendet werden. Zusätzliches Bezeichnen bei der Ermittlung identifiziert die nicht indizierten Metaschlüssel.

Zur Auswahl des anzuwendenden Metaschlüssels für Ihre Ermittlung können Sie:

- Die Standardmetaschlüssel auswählen.
- Einen Metaschlüsselsatz – Metagruppe genannt – auswählen.

Hinweis: Investigate stellt vordefinierte Metagruppen und benutzerdefinierte Metagruppen zur Verfügung. Sobald benutzerdefinierte Metagruppen erstellt wurden, können diese bearbeitet, gelöscht, zur Verwendung in anderen Services exportiert und in den gerade ermittelten Service importiert werden. Diese Verfahren werden in einem separaten Thema behandelt: Metagruppen managen

Das Dialogfeld „Standardmetaschlüssel“ ermöglicht es Ihnen, die Standardansicht zu spezifizieren und die Sequenz für Metaschlüssel während der Navigation in der Ansicht „Untersuchen > Navigation“ für einen spezifischen Service anzuzeigen. Sie können die Standardansicht für jeden einzelnen Schlüssel oder für alle Schlüssel folgendermaßen einstellen:

- Ausgeblendet: Die Ergebnisse für Standardmetaschlüssel sind ausgeblendet und können nicht geladen werden.
- Offen: Die Ergebnisse für Standardmetaschlüssel sind offen und alle Werte und Zähler werden angezeigt.
- Geschlossen: Die Ergebnisse für Standardmetaschlüssel sind geschlossen und nur der Metaname ist sichtbar.
- Auto: Der Ladevorgang von Standardmetaschlüsseln wird vom Index-Level kontrolliert, das nach Werten indiziert sein muss.

Achten Sie bei der Verwendung von Standardmetaschlüsseln darauf, dass diese für verschiedene Services verändert werden können, und Sie möglicherweise bei der Navigation zu einem Drill-down-Punkt auf verschiedenen Services verschiedene Standardmetaschlüssel-Sets sehen. Wenn Sie nicht die erwarteten Daten sehen, müssen Sie möglicherweise die anfängliche Ansicht der Standardmetaschlüssel ändern.

Wenn Sie den anfänglichen Status der Standardmetaschlüssel in der Ansicht „Navigation“ ändern, bleiben die Änderungen für diesen Service erhalten. Wenn neue Schlüssel zu der angepassten Indexdatei für einen Core-Service hinzugefügt werden (zum Beispiel `concentrator-custom-index.xml` oder `decoder-custom-index.xml`), werden die neuen Schlüssel zur Liste der Standardmetaschlüssel hinzugefügt. Die in der Ansicht Navigieren durchgeführten Änderungen werden nur für den aktuellen Service angewendet.

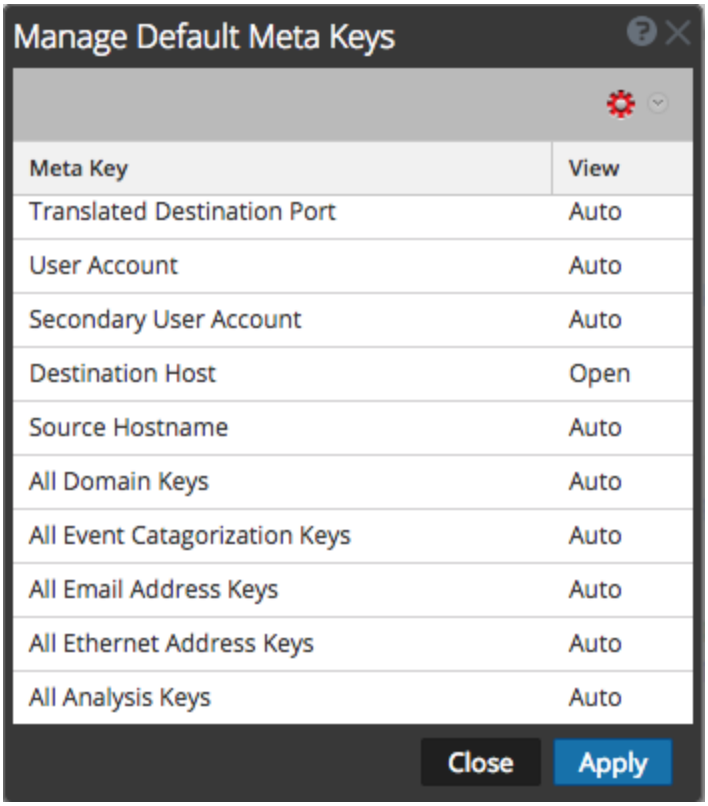
So spezifizieren Sie, dass die anfängliche Ansicht „Navigation“ geöffnet wird, indem Standardmetaschlüssel verwendet werden:

1. Navigieren Sie zu **Ermittlung** > Navigation**.**
2. Wählen Sie einen Service und anschließend **Navigation** aus.
3. Wählen Sie im Menü **Meta** die Option **Standardmetaschlüssel verwenden** aus.
   Wenn Ermittlungen bereits im Gange sind, werden die Daten in der aktuellen Ansicht neu geladen und ein Symbol hebt die gewählte Option hervor. Wenn noch keine Daten geladen sind, werden die Standardmetaschlüssel für das nächste Laden verwendet.

So konfigurieren Sie die Standardansicht der Standardmetaschlüssel in der Ansicht „Navigation“:

1. Wählen Sie in der Symbolleiste der Ansicht **Navigation** die Optionen **Meta** > **Standardmetaschlüssel managen** aus.

Das Dialogfeld „Standardmetaschlüssel managen“ wird mit der Liste der für den Service verfügbaren Metaschlüssel angezeigt.



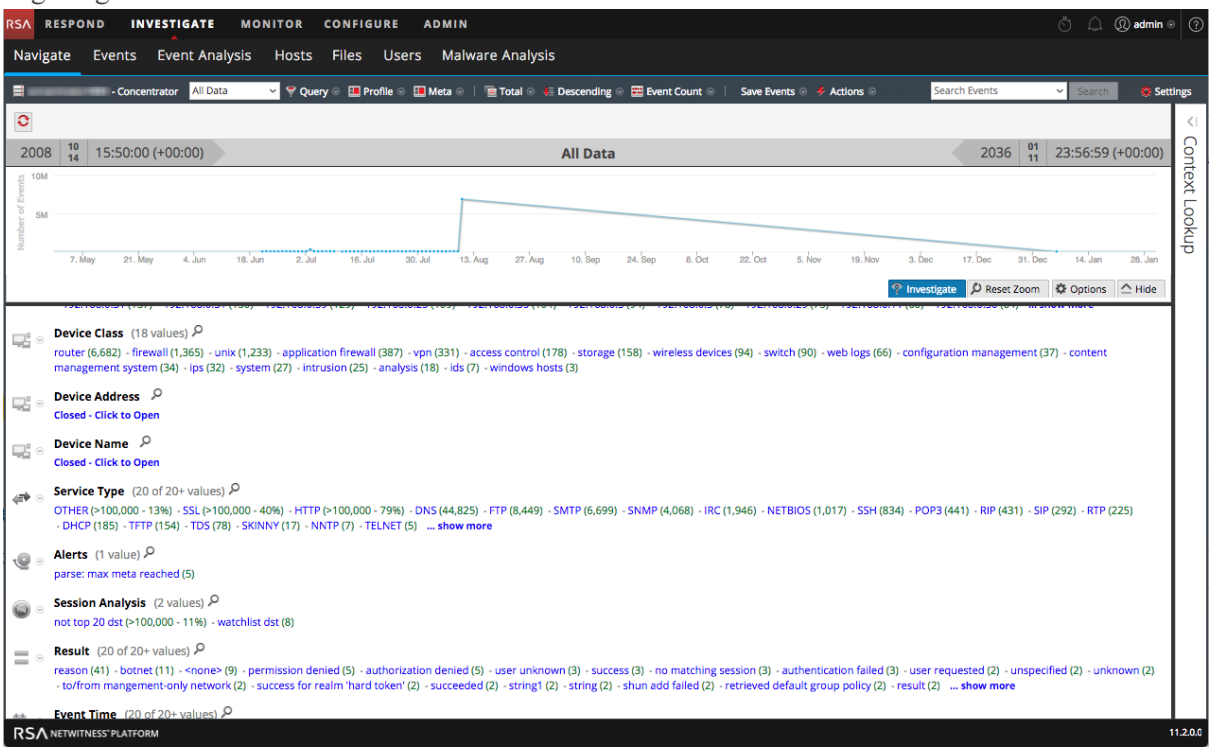
2. (Optional) Um die Reihenfolge der Schlüssel zu ändern, wählen Sie einen oder mehrere Schlüssel aus und verschieben Sie die Werte in der Liste der Schlüssel nach oben oder nach unten.
3. Führen Sie einen der folgenden Schritte aus:
   - (Optional) Um die Standardansicht für alle Metaschlüssel zu ändern, stellen Sie sicher, dass keine Metaschlüssel ausgewählt sind und wählen Sie in der Symbolleiste aus.
   - (Optional) Um die Standardansicht für einen oder mehrere Schlüssel zu ändern, wählen Sie die Schlüssel aus und wählen Sie in der Symbolleiste .
     Ein Drop-down-Menü der möglichen Anfangsansichten für alle Standardmetaschlüssel wird angezeigt.
   - (Optional) Um die Standardansicht für Metaschlüssel wie in der Serviceindexdatei angegeben wiederherzustellen, stellen Sie sicher, dass keine Schlüssel ausgewählt sind und wählen Sie in der Symbolleiste > **Auto** aus.
     Wenn Sie die Standardansicht für einen nicht indizierten Metaschlüssel ändern, können Sie den Schlüssel nicht auf OPEN einstellen. Wenn Sie die Standardansicht für eine Gruppe von Metaschlüsseln in OPEN ändern und einige der Metaschlüssel nicht indiziert sind, werden die nicht indizierten Metaschlüssel auf AUTO zurückgesetzt. Daher wird der Metaschlüssel nur automatisch geladen, wenn er indiziert ist, und nicht indizierte Metaschlüssel haben den Status CLOSED, bis sie manuell geöffnet werden.
4. Wählen Sie eine der Ansichten aus.

5. Klicken Sie zum Speichern der Änderungen auf **Anwenden**.
   Die in der Ansicht „Navigation“ angezeigten Metaschlüssel werden auf Ihre Spezifikationen eingestellt. Wenn die Standardmetaschlüssel ausgeblendet sind, werden die Werte der Metaschlüssel in der Ermittlung nicht angezeigt. Wenn die Standardmetaschlüssel geschlossen sind, werden die Werte der Metaschlüssel nicht standardmäßig geladen. Sie können aber einzelne Metaschlüssel in der Ansicht „Navigation“ manuell laden.

Drill-down in die Daten im Zeitdiagramm der Ansicht „Navigation“

Das Zeitdiagramm bietet Analysten eine visuelle Darstellung der Aktivität im Zeitverlauf. Sie können die Daten mit Zoom vergrößern, indem Sie ein Zeitfenster und dann die Option Untersuchen auswählen. Sie können die Navigation auf den Zeitbereich zurücksetzen, der vor Anwendung des Zooms aktiv war.

1. Navigieren Sie zu **Ermittlung > Navigation**.
   Das Zeitdiagramm für den aktuellen Drill-down-Punkt und den ausgewählten Zeitbereich wird angezeigt.



2. Zur Markierung eines Zeitbereichs im Zeitdiagramm klicken Sie auf den gewünschten Zeitbereich und ziehen Sie die Maus.
   Das Zeitdiagramm wird für den ausgewählten Zeitbereich neu gezeichnet, die Metawerte bleiben jedoch unverändert.
3. Zum Drill-down in die Daten für den ausgewählten Zeitbereich klicken Sie auf **Untersuchen**.
   Die URL und der Bereich mit den Ermittlungsoptionen werden aktualisiert, um den neuen Zeitbereich widerzuspiegeln. Das Zeitdiagramm wird neu gezeichnet und die Metawerte für den ausgewählten Zeitbereich werden geladen.

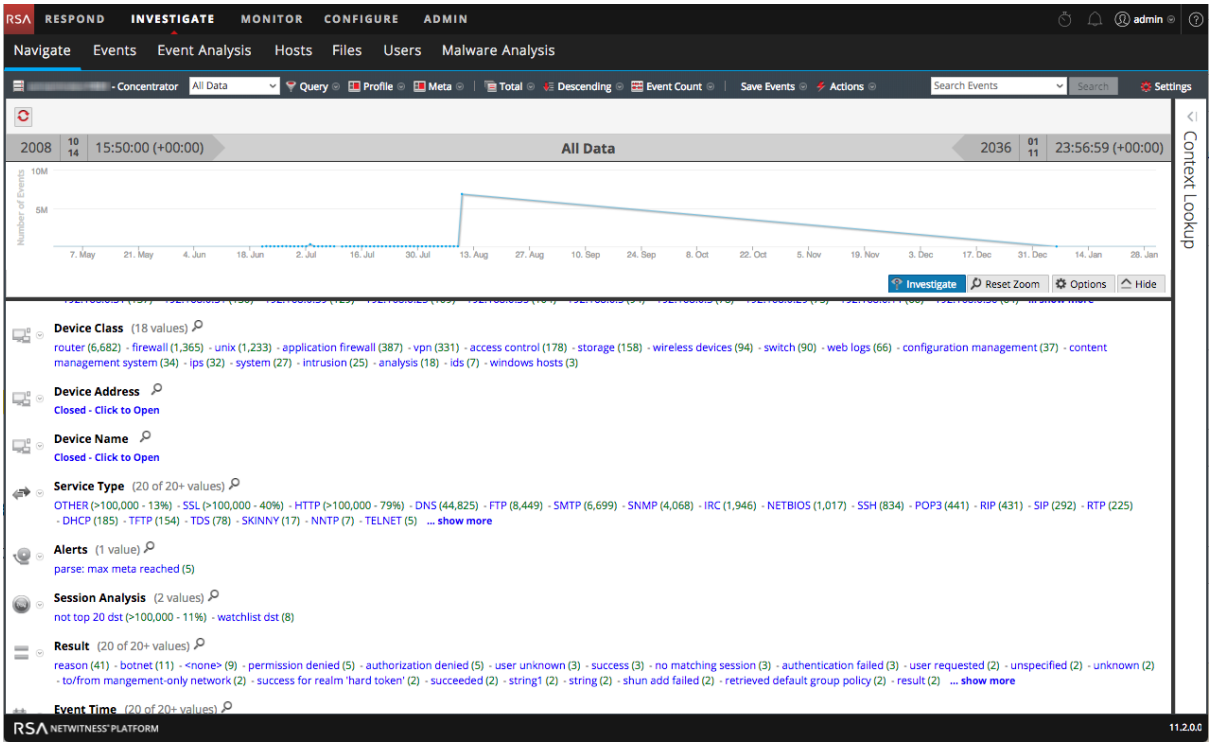
4. Zum Zurücksetzen des Zeitdiagramms auf den ursprünglichen Zeitbereich klicken Sie auf **Zoom zurücksetzen**.
   Die URL und der Bereich mit den Ermittlungsoptionen werden aktualisiert und zeigen wieder den Zustand vor der Zoomanwendung an. Das Zeitdiagramm wird für den ausgewählten Zeitbereich neu gezeichnet und die Metawerte für diesen Zeitbereich werden geladen.

Drill-down zu Daten im Bereich „Werte“

NetWitness Platform zeigt die Aktivität und Werte des ausgewählten Services in der Ansicht „Investigation > Navigation“ an. Analysten führen zur Ermittlung von Daten einen Drill-down in Daten durch, indem sie auf einen Metaschlüssel oder einen Metawert klicken, der als Abfrage behandelt wird. Jede Abfrage wird im Bereich „Werte“ den Brotkrümelnavigationsdaten hinzugefügt. Dies führt zu einer Brotkrümelnavigation oben mit einem Brotkrümel-Element für jede Abfrage. Sie können die Brotkrümelnavigation bearbeiten, um eine Abfrage einzufügen oder zu entfernen.

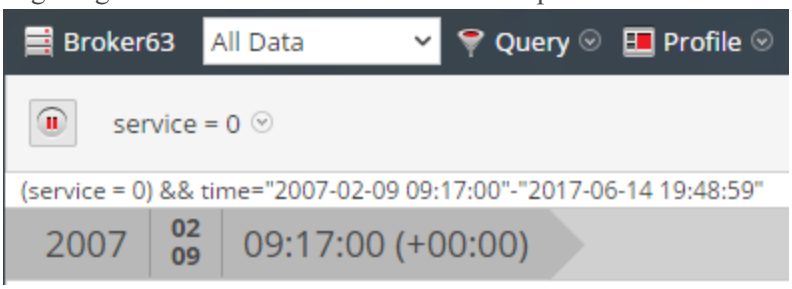
So führen Sie einen Drill-down in einer Untermenge der Metadaten durch:

1. Starten Sie eine Untersuchung, sodass Metadaten in der Ansicht „Navigation“ angezeigt werden.

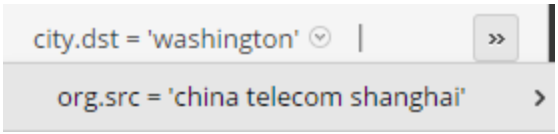


2. Um einen Drill-down in den Metadaten durchzuführen, führen Sie eine der folgenden Aktionen aus:
   a. Klicken Sie auf einen **Metaschlüssel**, z. B. **Servicetyp**.
   b. Klicken Sie auf einen **Metawert**. Dies ist der blaue Text in den Ergebnissen. Beispielsweise **SONSTIGE**.
      Jedes Mal, wenn Sie auf einen Metaschlüssel oder Metawert klicken, konzentriert sich die Ermittlungsabfrage auf einen Fokus- bzw. Drill-down-Punkt in den Daten. An jedem Drill-down-Punkt wird der Bereich Werte aktualisiert und der neue Drill-down-Punkt wird im Breadcrumb

angezeigt. Unten stehend finden Sie ein Beispiel für das erste Breadcrumb.



Dies ist ein Beispiel eines langen Breadcrumbs, das zu lang für die Symbolleiste ist. Der letzten Abfrage, die in der Symbolleiste aufgelistet ist, folgt ein Drop-down-Menü, das die zusätzlichen Abfragen auflistet. Um einen Drill-down-Punkt innerhalb des Überlaufs auszuwählen, klicken Sie auf das Überlaufsymbol und auf eine Abfrage in der Drop-down-Liste.

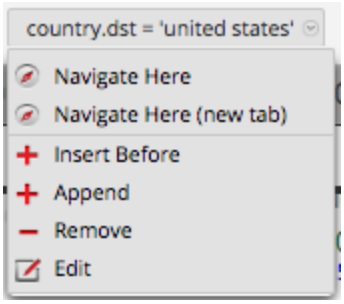


So fügen Sie dem Breadcrumb eine Abfrage hinzu:

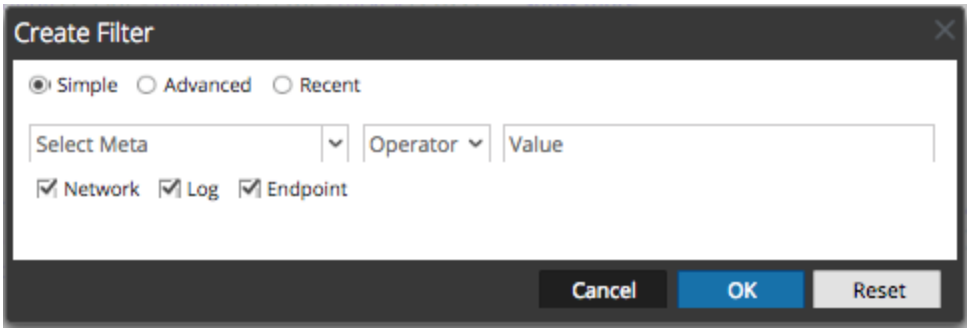
Sie können auf eines der Elemente der Brotkrümelnavigation klicken, um das Menü „Abfrage“ anzuzeigen. Sie können vor einem Breadcrumb-Element eine neue Abfrage einfügen und am Ende des Breadcrumbs eine neue Abfrage anfügen. Nach jeder Bearbeitung im Breadcrumb aktualisiert NetWitness Platform die Ergebnisse.

So fügen Sie dem Breadcrumb eine Abfrage hinzu:

1. Klicken Sie auf ein Breadcrumb-Element.
   Das Breadcrumb-Menü wird angezeigt.



2. Um dem Breadcrumb eine Abfrage hinzuzufügen, klicken Sie auf **Anfügen** oder **Einfügen vor**.
   Das Dialogfeld „Filter erstellen“ wird angezeigt.



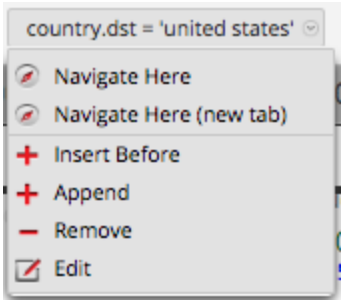
3. Erstellen Sie die Abfrage wie unter Erstellen einer angepassten Abfrage beschrieben.

So bearbeiten Sie eine Abfrage in der Brotkrümelnavigation:

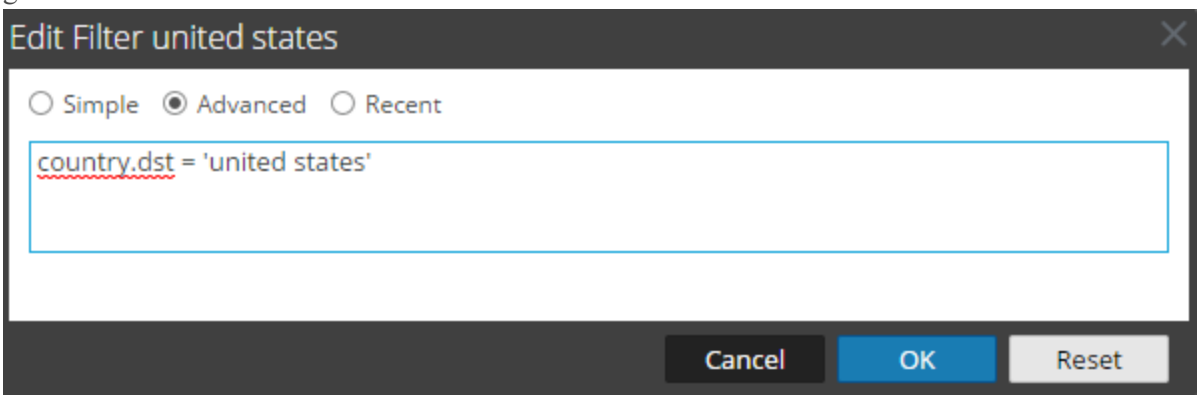
Sie können auf eines der Elemente der Brotkrümelnavigation klicken, um das Menü „Abfrage“ anzuzeigen. Sie können ein Breadcrumb-Element löschen und eine Abfrage in einem Breadcrumb-Element bearbeiten. Nach jeder Bearbeitung im Breadcrumb aktualisiert NetWitness Platform die Ergebnisse.

So arbeiten Sie mit Abfragen in einem Breadcrumb:

1. Klicken Sie auf ein Breadcrumb-Element.
   Das Breadcrumb-Menü wird angezeigt.



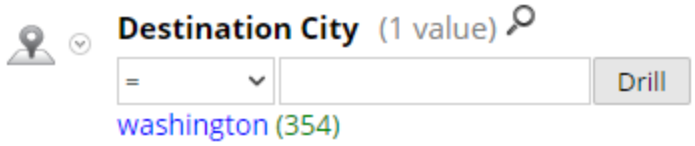
2. Um eine Abfrage im Breadcrumb zu bearbeiten, klicken Sie auf **Bearbeiten**.
   Das Dialogfeld „Erstellen“ wird angezeigt und die ausgewählte Abfrage wird zur Bearbeitung geöffnet.



3. Bearbeiten Sie die Felder wie unter Erstellen einer angepassten Abfrage beschrieben.

So führen Sie eine Schnellsuche innerhalb eines Metaschlüssels durch:

1. Bewegen Sie die Maus über den Abschnitt „Metaschlüssel“ und klicken Sie auf die Lupe.
   Das Formular „Schnellsuche“ mit einem Vergleichsoperator und einem optionalen Operanden für die Suche wird angezeigt.

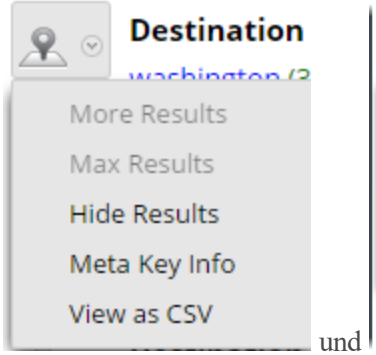


2. (Optional) Zum Schließen des Suchformulars klicken Sie nochmals auf die Lupe.
3. Wählen Sie den Vorgang aus der Drop-down-Liste auf der linken Seite aus und geben Sie den zu suchenden Textwert ein. Klicken Sie anschließend auf **Drill**, um die Ausführung zu starten.
   Die Metadaten für diesen Metaschlüssel werden für den Drill-down in den aktuellen Metadaten verwendet.

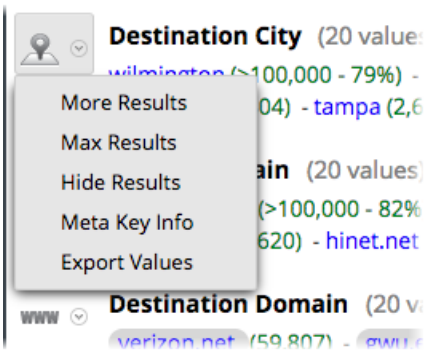
So zeigen Sie die Metaschlüsselinformationen an:

So können Sie Details eines Metaschlüssels, im Besonderen den Schlüsselnamen, das festgelegte Indexlevel für die Anzeige des Metaschlüssels und die Standardansicht des Metaschlüssels anzeigen lassen.

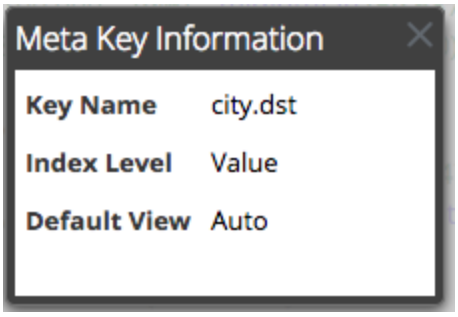
1. Klicken Sie auf das Drop-down-Menü neben dem Metaschlüssel. Diese zwei Abbildungen zeigen das Drop-down-Menü für die Versionen 11.0.0.x, 11.1 und höher.



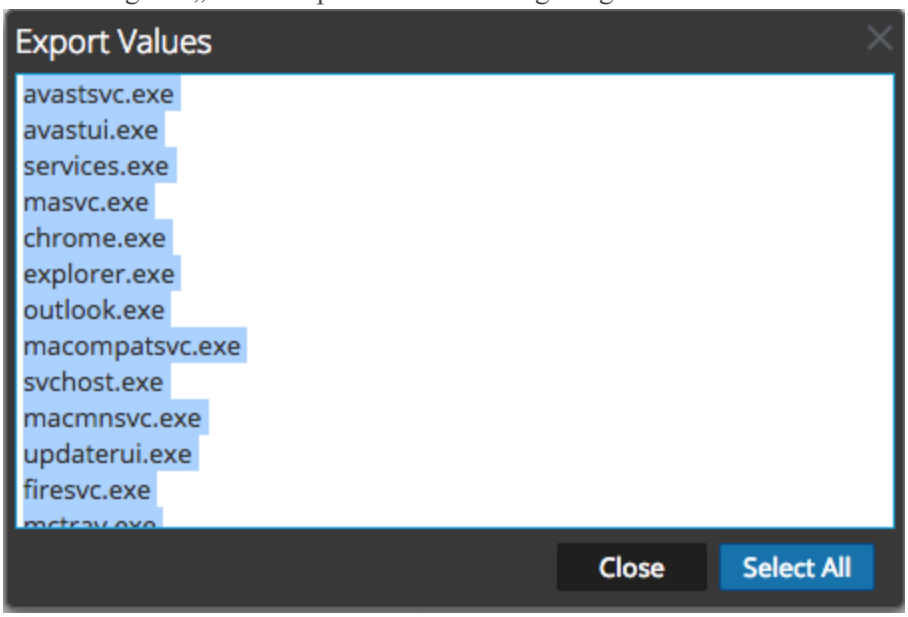
und



2. Klicken Sie auf **Metaschlüsselinformationen**.
   Das Dialogfeld „Metaschlüsselinformationen“ wird angezeigt.



3. Klicken Sie nach dem Betrachten auf ■.
4. (Optional für Version 11.0) Um die gefundenen Metanamen des Metaschlüssels als eine durch Kommas getrennte Werteliste anzeigen zu lassen, klicken Sie auf das Drop-down-Menü neben dem Metaschlüssel und wählen Sie **Als CSV anzeigen** aus.
   Das Dialogfeld „Werte werden im CSV-Format angezeigt“ wird angezeigt. Klicken Sie nach dem Betrachten auf **Schließen**.
5. (Optional für Version 11.1) Um die gefundenen Metanamen des Metaschlüssels in einer Liste anzeigen zu lassen, klicken Sie auf das Drop-down-Menü neben dem Metaschlüssel und wählen Sie **Werte exportieren** aus.
   Das Dialogfeld „Werte exportieren“ wird angezeigt.



6. (Optional) Wenn Sie die Ergebnisse für den Metaschlüssel im aktuellen Drill-down-PunktF ausblenden möchten, klicken Sie auf das Drop-down-Menü neben dem Metaschlüssel und klicken Sie auf **Ergebnisse ausblenden**.

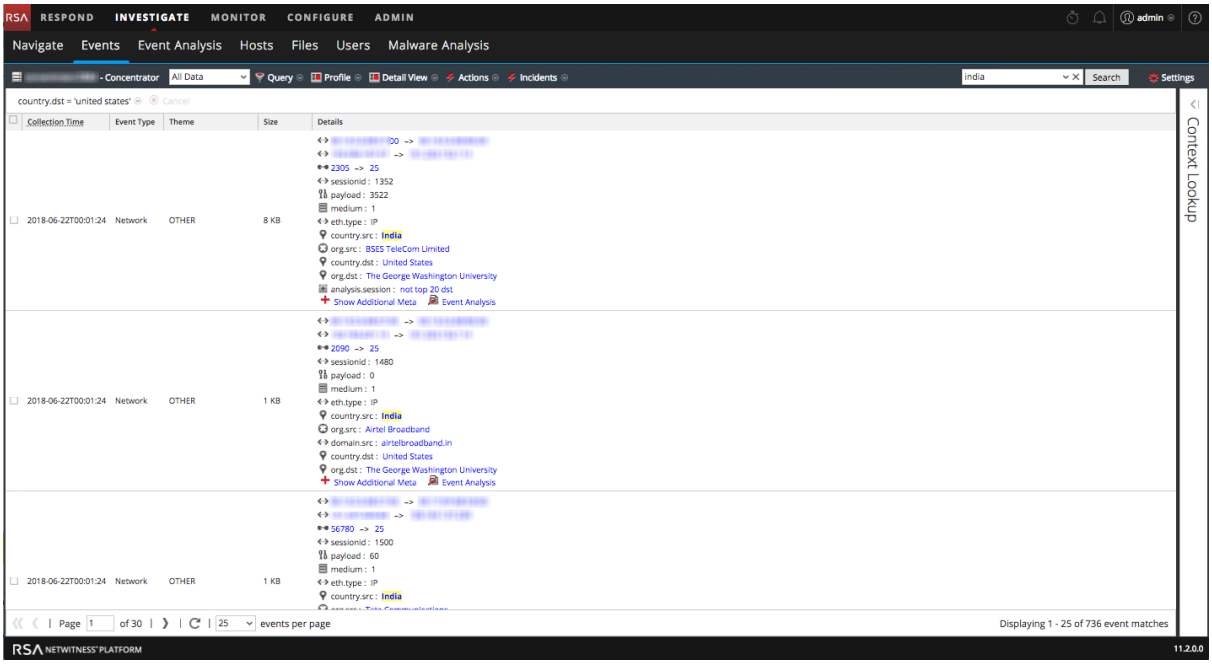
So zeigen Sie Ereignisse an, die einem Metawert zugeordnet sind:

Die Ansicht „Ereignisse“ bietet zwei unterschiedliche Ansichten für zusätzliche Ereignisinformationen: Die Ereignisliste und die Detailansicht.

1. Führen Sie in der Ansicht Navigieren einen Drill-down zu den Metadaten durch, die den Schwerpunkt Ihrer Ermittlungen bilden sollen.
2. Klicken Sie auf den Zähler (grüne Nummer) neben dem blauen Metawert.
   Die Ansicht „Ereignisse“ des entsprechenden aktuellen Drill-down-Punkts wird geöffnet.
   Die verschiedenen Vorgänge, die Sie in der Ansicht „Ereignisse“ ausführen können, werden unter Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse“ beschrieben.

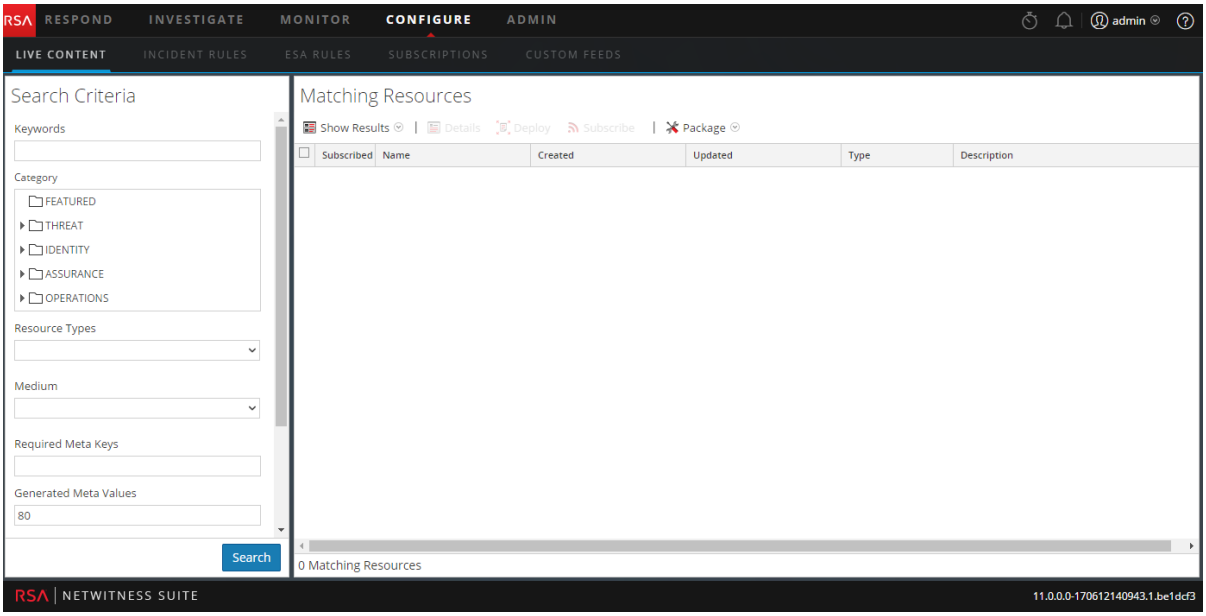
So suchen Sie nach bestimmten Ereignissen im Zusammenhang mit einem Metawert:

1. Führen Sie in der Ansicht „Navigation“ einen Drill-down zu den Metadaten durch, die den Schwerpunkt Ihrer Ermittlungen bilden sollen (klicken Sie auf einen Metawert oder fügen Sie eine Abfrage hinzu).
2. Geben Sie eine Suchzeichenfolge in das Suchfeld ein und drücken Sie die **Eingabetaste** oder klicken Sie auf **Suche**.
   Sie können Ihre Suchmoduseinstellungen auch auswählen und festlegen. Detaillierte Suchinformationen finden Sie unter Suchen nach Textmustern.
   Die Ansicht „Ereignisse“ wird in einer neuen Registerkarte geöffnet und zeigt die Suchergebnisse an. Wenn der Suchbegriff nicht markiert angezeigt wird, klicken Sie auf **Zusätzliche Metadaten anzeigen**. Ihre Zeitbereichsauswahl und Drill-Downs (Abfragen) werden in die Ansicht „Ereignisse“ übertragen.



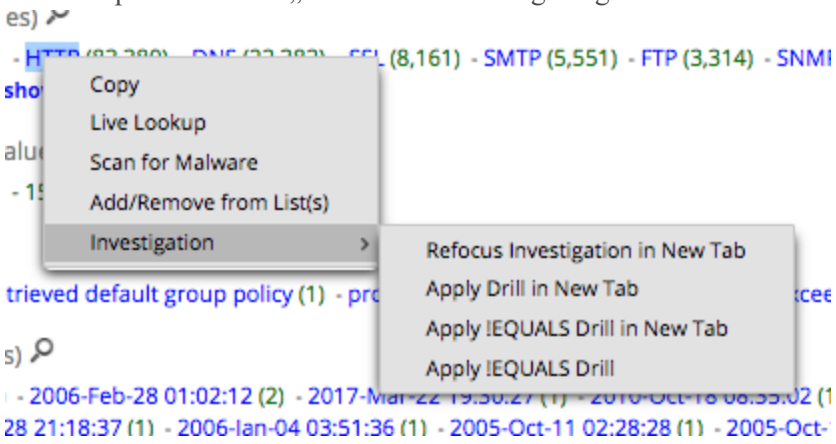
So zeigen Sie einen ausgewählten Metawert in RSA Live an:

1. Führen Sie in der Ansicht Navigieren einen Drill-down zu den Metadaten durch, die den Schwerpunkt Ihrer Ermittlungen bilden sollen.
2. Klicken Sie mit der rechten Maustaste auf einen Metawert (den Text in Blau).
   Das Drop-down-Menü Metawert wird angezeigt.
3. Um den Metawert in RSA Live zu suchen, klicken Sie auf **Live-Suche**.
   Die Ansicht „Live-Suche“ mit dem eingegebenen Metawert im Feld „Erzeugte(r) Metawert(e)“ wird angezeigt und Sie können die Suche starten.



So fokussieren Sie die Untersuchungin einem Drill-down-Punkt neu:

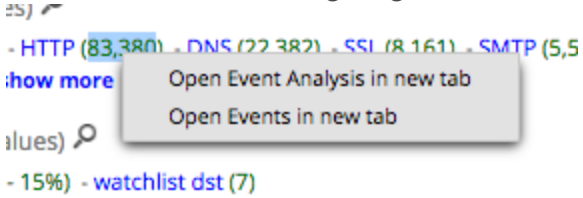
1. Klicken Sie mit der rechten Maustaste auf einen Metawert (den Text in Blau).
   Das Drop-down-Menü „Metawert“ wird angezeigt.



2. Wählen Sie eine der folgenden Neufokussierungs-Optionen aus.
   Der Drill-down wurde gemäß Ihrer Auswahl neu fokussiert.

So betrachten Sie einen spezifischen Zähler in einer neuen Registerkarte:

Wenn Sie eine Zählung für einen Metawert in der Ansicht „Ereignisse“ oder „Ereignisanalyse“ anzeigen möchten, klicken Sie mit der rechten Maustaste auf eine Zählung für einen Metawert (die grüne Zahl nach dem blauen Metawert).
Das Kontextmenü wird angezeigt.



Metagruppen managen

Eine Metagruppe kombiniert ausgewählte Metaschlüssel in einer Gruppe, um nur Daten anzuzeigen, in denen die Metaschlüssel und -einheiten gefunden wurden.

Hinweis: In Version 11.1 und höher können Sie auch konfigurierte Metaeinheiten in Metagruppen verwenden.

In der Ansicht „Untersuchen > Navigation“ können Metagruppen zum Filtern der in einer Ermittlung angezeigten Daten verwendet werden. Eine Neuinstallation von NetWitness Platform umfasst vordefinierte Metagruppen, damit Sie interessante Datasets in Investigate finden können. Zur Identifizierung wird den OOTB-Metagruppen, die dupliziert, aber nicht gelöscht werden können, das Präfix RSA vorangestellt. Sie können Ihre eigenen Gruppen erstellen und eine OOTB-Gruppe zum Erstellen einer benutzerdefinierten Gruppe duplizieren und bearbeiten.

Mit einer während einer Untersuchung wirksamen Metagruppe zeigen die Informationen im Bereich „Werte“ nur die Metaschlüssel in der ausgewählten Gruppe an. Wenn Sie eine Parallelkoordinatenvisualisierung öffnen, werden die Metaschlüssel und -einheiten in einer Gruppe als Achsen von links nach rechts angezeigt. Es kann hilfreich sein, zwei Versionen jeder benutzerdefinierten Metagruppe zu erstellen: eine für die Analyse von Metawerten und eine für das Erstellen eines Parallelkoordinatendiagramms, das auf eine kleinere Untergruppe des gleichen Anwendungsfalls fokussiert ist.

Benutzerdefinierte Metagruppen werden allen Benutzern eines Service angezeigt und können für den Import in einen beliebigen Service exportiert werden, sind jedoch durch die verfügbaren Metaschlüssel für diesen Service begrenzt.

Hinweis: Wenn Administratoren benutzerdefinierte Metagruppen manuell durch Bearbeiten der benutzerdefinierten Indexdatei für einen Service hinzufügen, sind die neuen Gruppen in Investigate verfügbar, nachdem der Service erneut gestartet wurde.

In diesem Abschnitt wird erläutert, wie Sie die während der Navigation in einem bestimmten Service zu verwendenden benutzerdefinierten Metagruppen hinzufügen, bearbeiten, importieren, exportieren und löschen.

Out-of-the-Box-Metagruppen

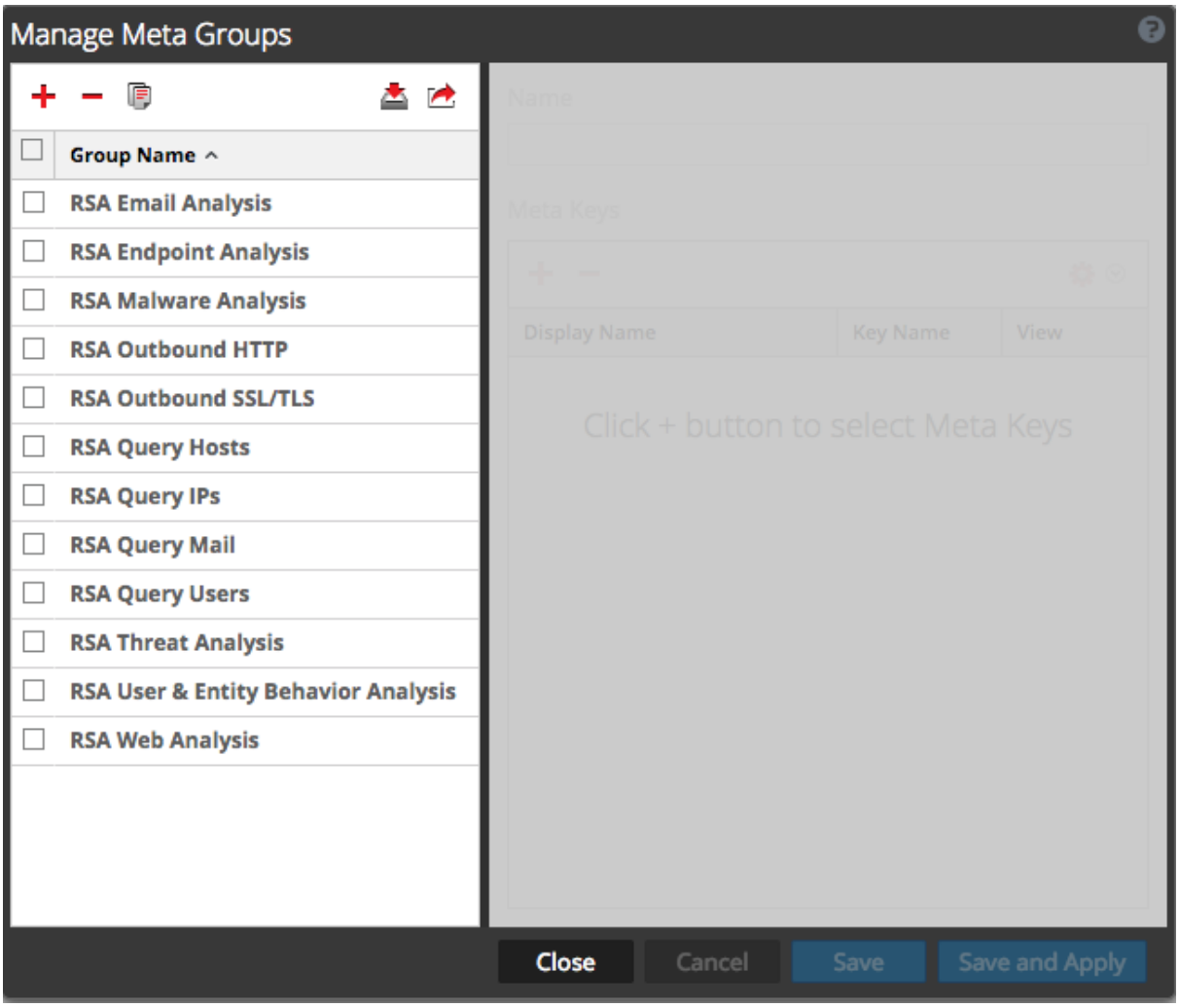
In RSA NetWitness Platform sind Standardmetagruppen vordefiniert. Die Standardmetagruppen sind nützlich, um den Fokus einer Ermittlung auf typische Anwendungsbeispiele zu setzen und die Bedrohungserkennung anhand des RSA Hunting Pack zu unterstützen. Dies sind die OOTB-Metagruppen:

- RSA-E-Mail-Analyse umfasst Metaschlüssel, die E-Mail-Aktivitäten beschreiben.
- RSA-Endpunktanalyse enthält Metaschlüssel, die einen Einblick in die Prozesse, die Dateien, die Benutzer und die Verbindungen von NetWitness Endpoint-Hosts (NWE) bieten.
- RSA Malware Analysis umfasst Metaschlüssel, die Indikatoren für eine Infizierung in den Dateien in den Ereignissen markieren.
- Ausgehender HTTP-Datenverkehr von RSA umfasst Metaschlüssel, die einen Einblick in ausgehenden Webdatenverkehr bieten.

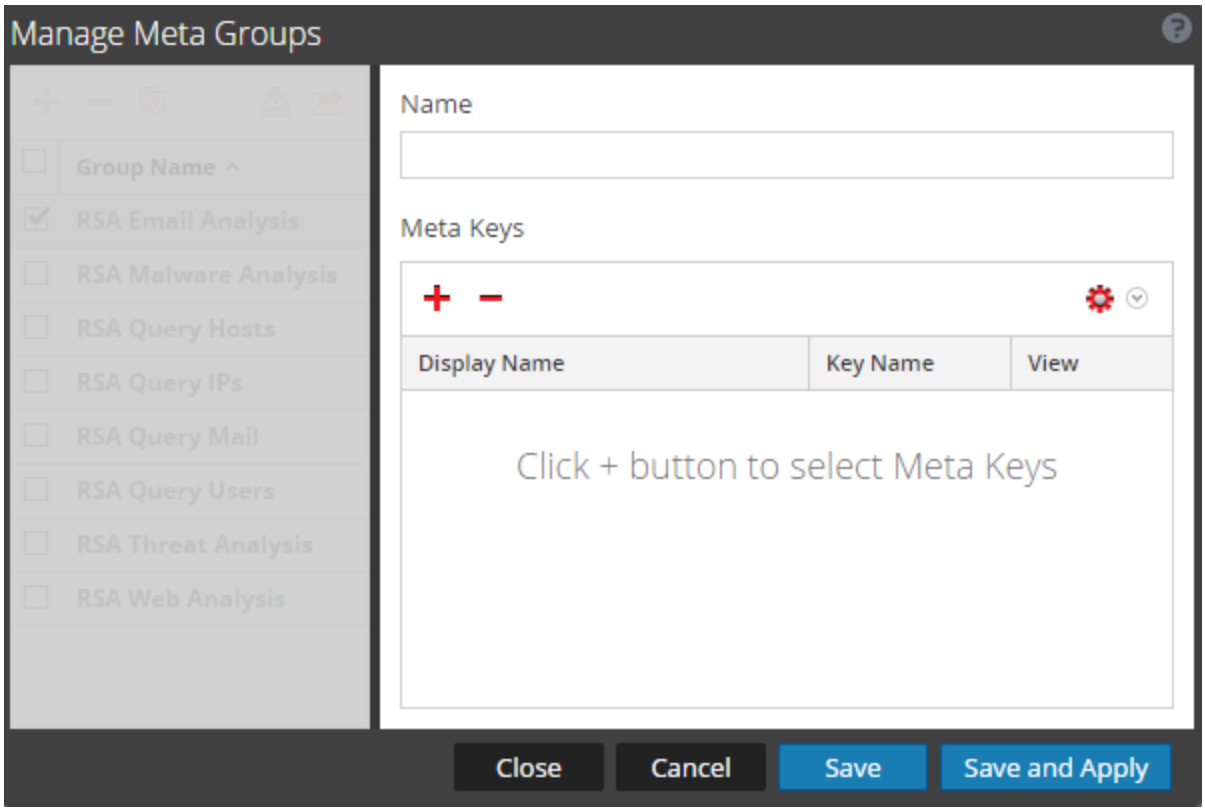
- Ausgehendes SSL/TLS von RSA umfasst Metaschlüssel, die sich auf verschlüsselten Webdatenverkehr konzentrieren.
- Die RSA-Hostabfrage umfasst Metaschlüssel, die alle Metaschlüssel zum Finden von Hosts umfassen.
- Die RSA-IP-Abfrage umfasst Metaschlüssel, die alle Metaschlüssel zum Finden von IP-Adressen umfassen.
- Die RSA-E-Mail-Abfrage umfasst Metaschlüssel, die alle Metaschlüssel zum Finden von E-Mails umfassen.
- Die RSA-Benutzerabfrage umfasst Metaschlüssel, die alle Metaschlüssel zum Finden von Benutzern umfassen.
- Die RSA-Bedrohungsanalyse umfasst Metaschlüssel, die potenzielle Bedrohungen im Dataset markieren.
- Die RSA-Nutzer- und Entitätsverhaltensanalyse enthält Metaschlüssel, die alle Metaschlüssel umfassen, mit denen das Verhalten von Nutzern und Entitäten analysiert wird.
- Die RSA-Webanalyse umfasst Metaschlüssel, die Anomalien im Webdatenverkehr markieren.

Erstellen von Metagruppen und Hinzufügen von Metaschlüsseln

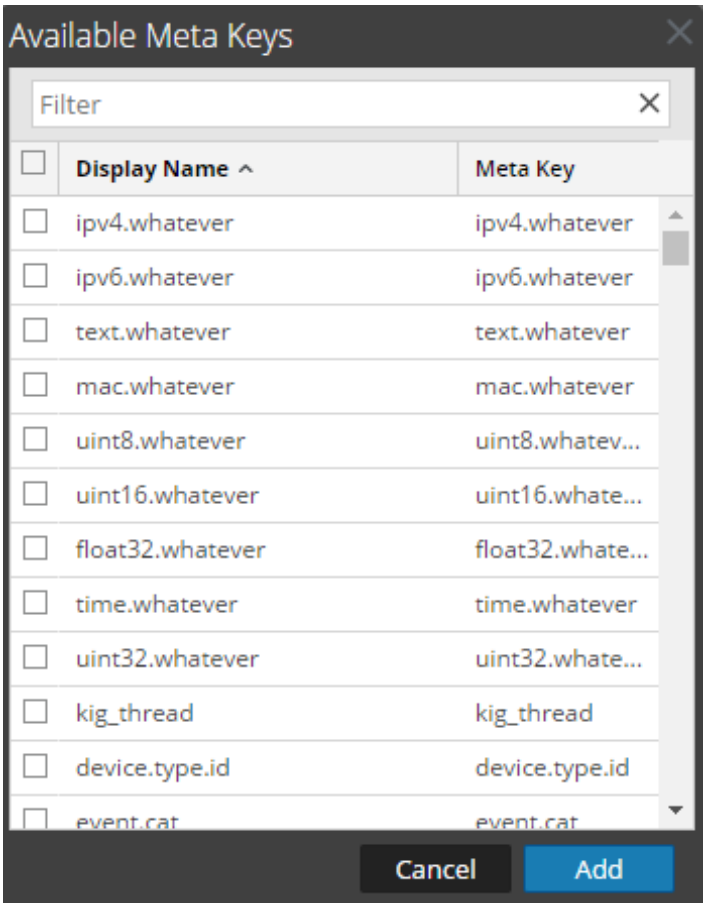
1. Wenn Sie einen Service in der Ansicht **Untersuchen > Navigation** untersuchen möchten, wählen Sie in der Symbolleiste **Metadaten > Metagruppen managen** aus.
   Das Dialogfeld „Metagruppen managen“ wird angezeigt. Zu Beginn sind nur OOTB-Gruppen für einen Service konfiguriert und unter „Gruppenname“ aufgeführt. Wenn andere benutzerdefinierte Gruppen konfiguriert wurden, werden sie ebenfalls unter „Gruppenname“ aufgelistet.



2. Klicken Sie in der Symbolleiste über den Metagruppen auf +.
   Über der Liste „Metagruppen“ wird eine neue Zeile eingefügt.
3. Geben Sie einen Namen für die neue Metagruppe ein und drücken Sie die **Eingabetaste**.
   Das Formular rechts wird zur Bearbeitung geöffnet.



4. (Optional) Wenn Sie den Namen der Metagruppe ändern möchten, geben Sie einen neuen Wert im Feld **Name** ein.
5. Klicken Sie in der Symbolleiste **Metaschlüssel** auf +.
   Das Dialogfeld „Verfügbare Metaschlüssel“ wird mit den Schlüsseln in alphabetischer Reihenfolge geöffnet.

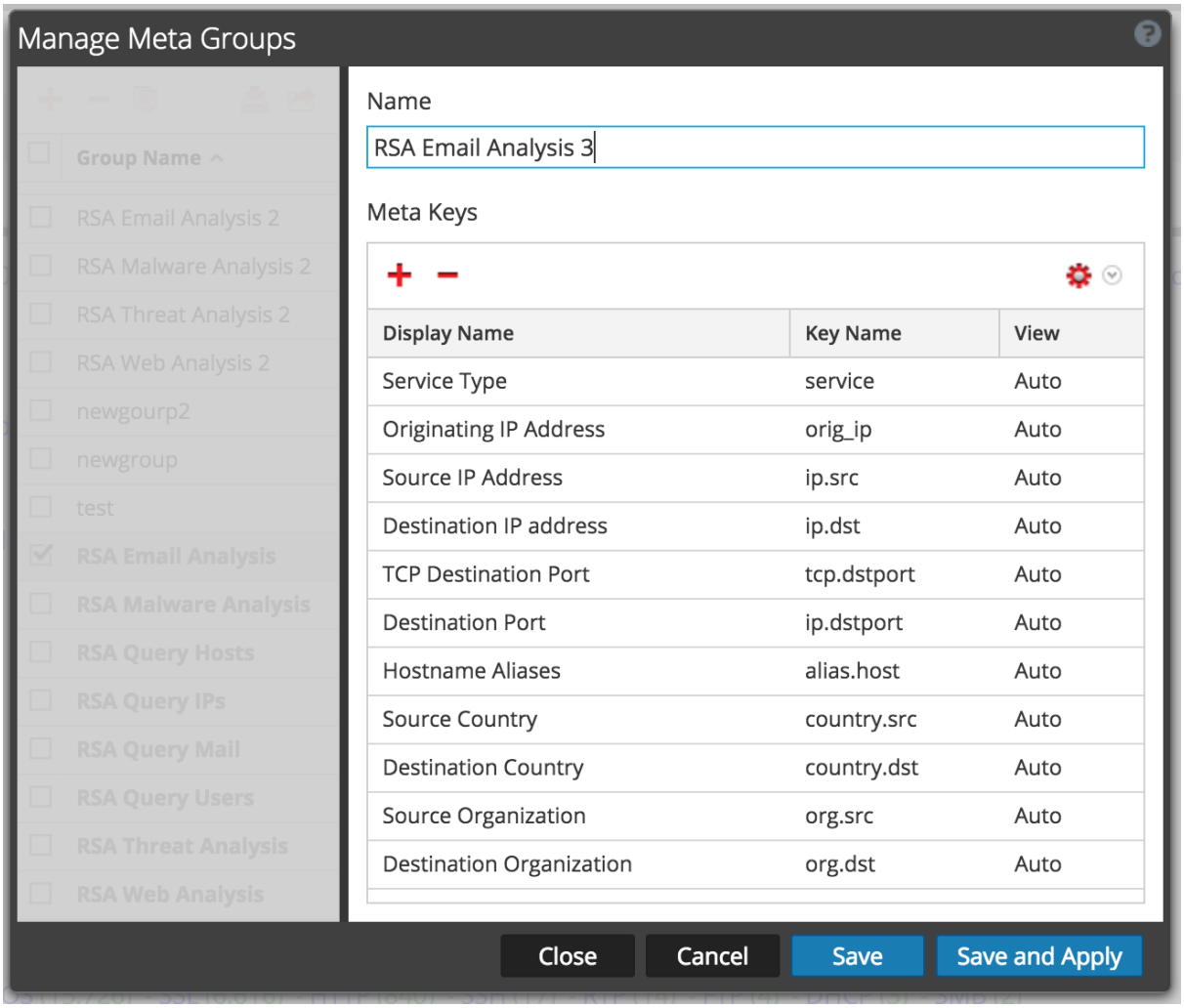


6. Um die Liste der Metaschlüssel zu filtern, geben Sie ein Wort oder einen Begriff im Feld **Filtern** ein und drücken Sie die **Eingabetaste**.
   In der Liste werden Metaschlüssel basierend auf einer Suche ohne Berücksichtigung der Groß- und Kleinschreibung angezeigt. Löschen Sie den Filtertext und drücken Sie die **Eingabetaste**, um den Filter zu entfernen.
7. Zum Auswählen der in der Metagruppe zu berücksichtigenden Metaschlüssel aktivieren Sie die Kontrollkästchen. Zum Auswählen aller Metaschlüssel aktivieren Sie das Kontrollkästchen in der Titelleiste und klicken Sie auf **Hinzufügen**.
   Die ausgewählten Metaschlüssel werden zur Liste „Metaschlüssel“ hinzugefügt.
8. (Optional) Wenn Sie die Reihenfolge ändern möchten, in der die Metaschlüssel geladen und in einer Ermittlung aufgelistet werden, klicken Sie auf einen oder mehrere Metaschlüssel und ziehen Sie ihn bzw. sie an eine neue Position.
9. Führen Sie einen der folgenden Schritte aus, um die Erstellung der Metagruppe abzuschließen:
   a. Klicken Sie zum Speichern der Metagruppe auf **Speichern**.
      Die Gruppe wird erstellt und kann nun verwendet werden.
   b. Um die Metagruppe zu speichern und in die aktuelle Investigation-Ansicht zu übernehmen, klicken Sie auf **Speichern und übernehmen**.
      Die Gruppe wird gespeichert und sofort in die aktuelle Investigation-Ansicht übernommen.
10. Klicken Sie auf **Schließen**.

Duplizieren und Bearbeiten einer Standardmetagruppe

Wenn Sie eine OOTB-Metagruppe anpassen möchten, müssen Sie die Gruppe duplizieren und anschließend das Duplikat bearbeiten.

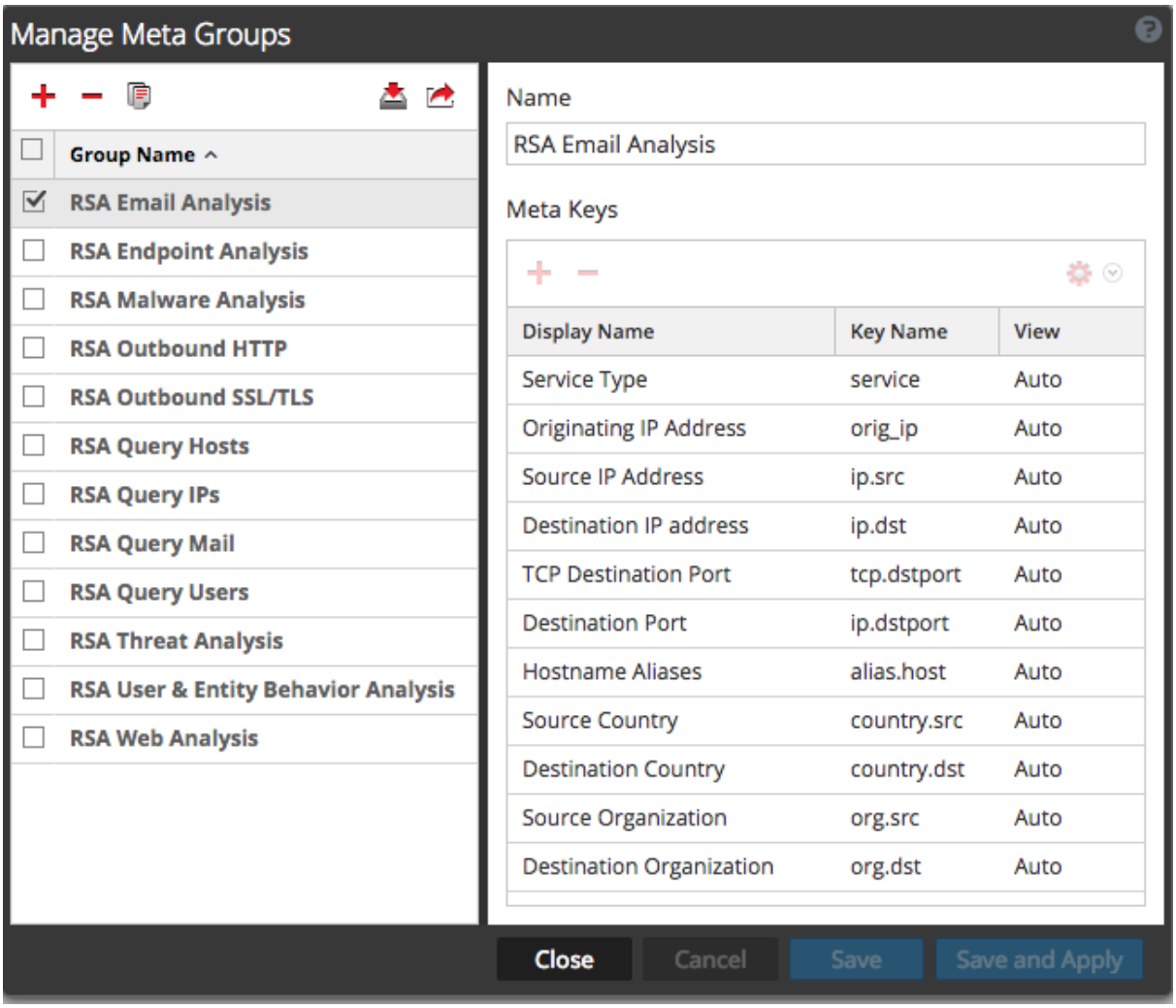
1. Wählen Sie in der Liste „Metagruppen managen“ eine Standardmetagruppe und klicken Sie auf . Das Formular rechts wird zur Bearbeitung geöffnet und enthält alle Metaschlüssel, die in der Standardgruppe enthalten sind.



2. Geben Sie einen Namen für die neue Gruppe ein und setzen Sie die Bearbeitung wie unter „Bearbeiten von Metagruppen“ unten beschrieben fort.

Bearbeiten von Metagruppen

1. Wählen Sie eine Gruppe in der Liste **Metagruppen** aus.
   Das Formular rechts wird zur Bearbeitung geöffnet.



2. (Optional) Bearbeiten Sie den Namen der Gruppe.
3. (Optional) Fügen Sie neue Metaschlüssel hinzu, wie im obigen Abschnitt „Erstellen von Metagruppen und Hinzufügen von Metaschlüsseln“ beschrieben.
4. (Optional) Um die Reihenfolge für die Schlüssel festzulegen, ziehen Sie einen oder mehrere Schlüssel per Drag-and-drop.
5. (Optional) Zum Ändern der ursprünglichen Ansicht eines Metaschlüssels klicken Sie auf und wählen Sie eine der möglichen Ansichten aus.
   Wenn Sie die Metagruppe ändern, kann der Schlüssel nicht auf OPEN eingestellt werden. Wenn Sie die Standardansicht für eine Gruppe von Metaschlüsseln in OPEN ändern und einige der Metaschlüssel nicht indiziert sind, werden die nicht indizierten Metaschlüssel auf AUTO zurückgesetzt. Daher wird der Metaschlüssel nur automatisch geladen, wenn er indiziert ist, und nicht indizierte Metaschlüssel haben den Status „CLOSED“, bis sie manuell geöffnet werden.
   Der Wert für die ursprüngliche Ansicht wird in der Spalte „Ansicht“ angezeigt.
6. Klicken Sie zum Speichern der Änderungen auf **Speichern**.

7. Zum Anwenden der Änderungen auf die aktuelle Ansicht „Navigation“ klicken Sie auf **Speichern und übernehmen**.

Löschen von Metagruppen

1. Wählen Sie die zu entfernende Gruppe in der Liste **Metagruppen** aus.
2. Klicken Sie auf .
   Ein Bestätigungsdialogfeld wird angezeigt, in dem Sie die Anforderung abbrechen oder abschließen können.
3. Klicken Sie auf **OK**.
   Die Metagruppe wird gelöscht. Wenn Sie das Fenster schließen und es sich bei der gelöschten Gruppe um die derzeit angewendete Metagruppe handelte, wird sie entfernt und die Standardmetaschlüssel werden zum Erstellen der Ansicht verwendet.

Exportieren von Metagruppen

Benutzerdefinierte Metagruppen werden für einzelne Services erstellt. Um die Metagruppen für einen anderen Service zur Verfügung zu stellen, müssen Sie sie in Ihr lokales Dateisystem exportieren. So exportieren Sie eine oder mehrere Metagruppen:

1. Wählen Sie eine oder mehrere zu exportierende Gruppen in der Liste **Metagruppen** aus.
2. Klicken Sie auf .
   Die ausgewählten Gruppen werden auf Ihr lokales Dateisystem als **MetaGroups.jsn** heruntergeladen. Alle heruntergeladenen Metagruppen haben denselben Namen mit einer angefügten Zahl, um das Überschreiben vorheriger Downloads zu vermeiden.

Importieren von Metagruppen

Um benutzerdefinierte Metagruppen eines anderen Service dem derzeit untersuchten Service zur Verfügung zu stellen, müssen Sie die Datei `MetaGroups.jsn` aus dem lokalen Dateisystem importieren. Beim Importieren von Metagruppen zeigt eine Fehlermeldung an, ob eine der Gruppen bereits vorhanden ist. Zum Importieren einer Gruppe, die ein Duplikat darstellt, müssen Sie zuerst die vorhandene Gruppe löschen. Wenn Sie eine Metagruppe löschen möchten, darf diese nicht von einem Profil verwendet werden.

So importieren Sie Metagruppen:

1. Wählen Sie in der Liste **Metagruppen** eine Datei für den Import aus und klicken Sie auf .
   Das Auswahldialogfeld wird angezeigt.

2. Klicken Sie auf **Durchsuchen** und navigieren Sie zu dem Verzeichnis in Ihrem lokalen Dateisystem, in dem die heruntergeladenen `MetaGroups.jsn`-Dateien gespeichert sind. Wählen Sie eine Datei aus und klicken Sie auf **Öffnen**.
   Der Dateiname wird im Feld Datei hochladen angezeigt.
3. Klicken Sie auf **Hochladen**.
   Der Hochladevorgang wird gestartet und in einer Meldung wird angezeigt, ob der Upload erfolgreich war. Die Metagruppen werden zur Liste „Metagruppen“ hinzugefügt. Wenn es sich bei der Datei um ein Duplikat einer vorhandenen Metagruppe handelt, werden Sie in einem Dialogfeld darüber informiert, dass die Metagruppe bereits vorhanden ist.

Visualisieren von Metadaten als Parallelkoordinaten

Analysten können mithilfe der Parallelkoordinatenvisualisierung in der Ansicht „Navigation“ die Ermittlung auf Kombinationen aus Metaschlüsseln und -werten fokussieren, die eventuell auf abnormale Ereignisse hindeuten und eine Ermittlung wert sind.

Hinweis: In Version 11.1 und höher können Sie bei Verwendung von Metaschlüsseln auch konfigurierte Metaeinheiten verwenden.

Im Parallelkoordinatendiagramm können Sie den aktuellen Drill-down-Punkt in Investigate visualisieren und so mehr als zwei Metaschlüssel gleichzeitig betrachten. Die gleichzeitige Visualisierung mehrerer Metaschlüssel kann helfen, Sicherheitsprobleme im Zusammenhang mit multivarianten Mustern und Vergleichen zu identifizieren. So zum Beispiel, wenn einzelne Metaschlüssel und -werte nicht wichtig sind, ihre Kombination jedoch abnormale Muster oder Beziehungen zutage fördert. Metagruppen (siehe Metagruppen managen) können effektiv verwendet werden, um eine Sammlung von Metaschlüsseln zu definieren, die Sie als Parallelkoordinaten visualisieren möchten.

Best Practices für effektive Parallelkoordinatendiagramme

Befolgen Sie diese Empfehlungen, um effektive Parallelkoordinatendiagramme zu erstellen:

- Starten Sie von einem Drill-down-Punkt in der Ansicht „Navigation“, statt zu versuchen, alle Daten zu visualisieren.
- Begrenzen Sie den Zeitbereich, falls erforderlich.
- Wählen Sie den kleinsten nützlichen Satz Metaschlüssel als Achsen.
- Legen Sie die Reihenfolge der Achsen fest, um Anomalien zwischen Metawerten hervorzuheben, wenn Sie einer Linie über das Diagramm folgen.
- Wenn Sie einen nützlichen Satz Metaschlüssel und eine Reihenfolge identifizieren können, erstellen Sie eine benutzerdefinierte Metagruppe für zukünftige Ermittlungen. Beispiel: Sie können eine benutzerdefinierte Metagruppe für ausführbare Windows-Dateitypen erstellen.
- Verwenden Sie die RSA Out-of-the-Box(OOTB)-Metagruppen, die in einer neuen Installation enthalten sind.
- Nutzen Sie benutzerdefinierte Metagruppen erneut und teilen Sie sie durch Importieren und Exportieren der Gruppen als `.jsn`-Dateien.
- Es kann hilfreich sein, zwei Versionen jeder benutzerdefinierten Metagruppe zu erstellen: eine für die Analyse von Metawerten und eine für das Erstellen eines Parallelkoordinatendiagramms, das auf eine kleinere Untergruppe des gesamten Anwendungsfalls fokussiert ist.

Hinweis: Beim Importieren von Metagruppen zeigt eine Fehlermeldung an, ob eine der Gruppen bereits vorhanden ist. Zum Importieren einer Gruppe, die ein Duplikat darstellt, müssen Sie zuerst die vorhandene Gruppe löschen. Wenn Sie eine Metagruppe löschen möchten, darf diese nicht von einem Profil verwendet werden.

Um Sie bei der Erstellung besserer Parallelkoordinatendiagramme zu unterstützen, enthält NetWitness Platform mehrere Optimierungen.

- Analysten können angeben, dass nur Sitzungen in dem Diagramm dargestellt werden, in denen alle Metaschlüssel vorkommen.
- Der Administrator kann die Anzahl der dargestellten Metawerte in den „Einstellungen zu Parallelkoordinaten“ in der Ansicht „Administration, System“ > Bereich „Ermittlungen“ > Registerkarte „Navigation“ festlegen.

RSA-Metagruppen für Parallelkoordinaten – Anwendungsbeispiele

Eine Reihe von vordefinierten Metagruppen ist im Lieferumfang von NetWitness Platform enthalten. Wenn Sie die neueste Version erhalten möchten, können Sie die Metagruppen-Datei `MetaGroups_ootb_w_query.jsn` im Dialogfeld „Metagruppen managen“ importieren. Einige gut für die Parallelkoordinatenvisualisierung geeignete Aktivitäten sind:

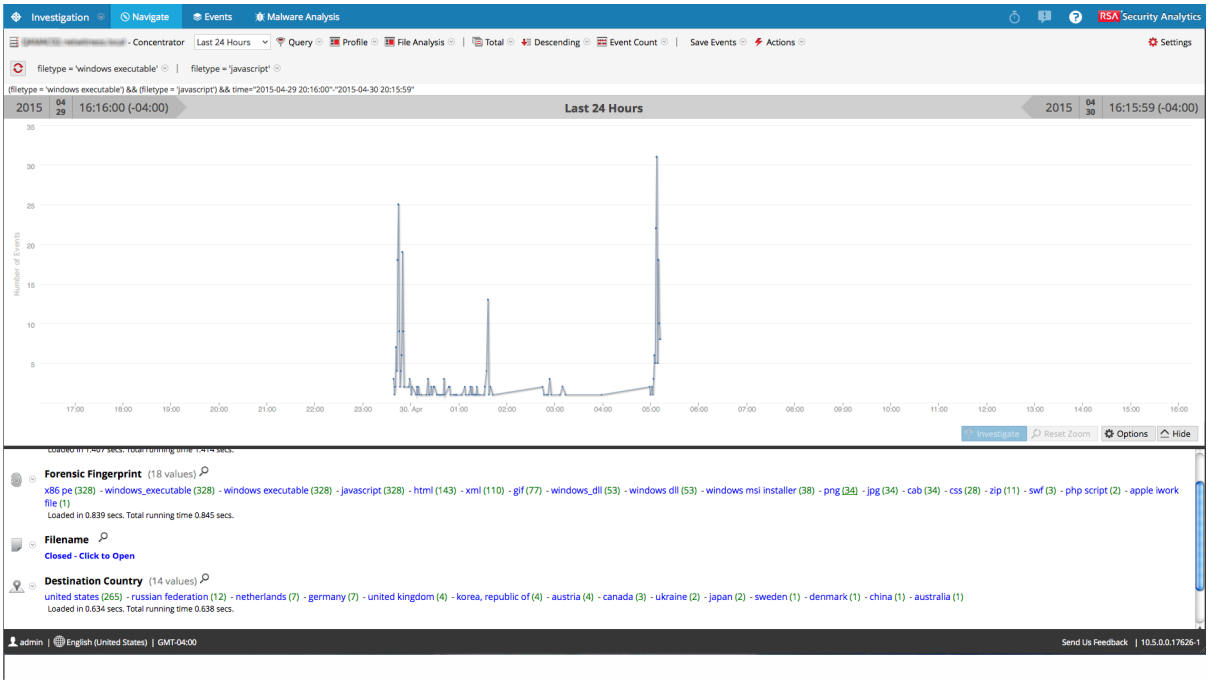
- Botnet Beaconing
- Verdeckte Kanäle
- E-Mail
- Verschlüsselte Sitzungen
- Endpunktanalyse
- Dateianalyse
- Malware Analysis
- Ausgehender HTTP
- Ausgehendes SSL/TLS
- SQL-Injektionsangriffe
- Bedrohungsanalyse
- Webanalyse

Anzeigen einer Parallelkoordinatenvisualisierung

Führen Sie in einer Ermittlung in der Ansicht „Investigate > Navigation“ folgende Schritte aus:

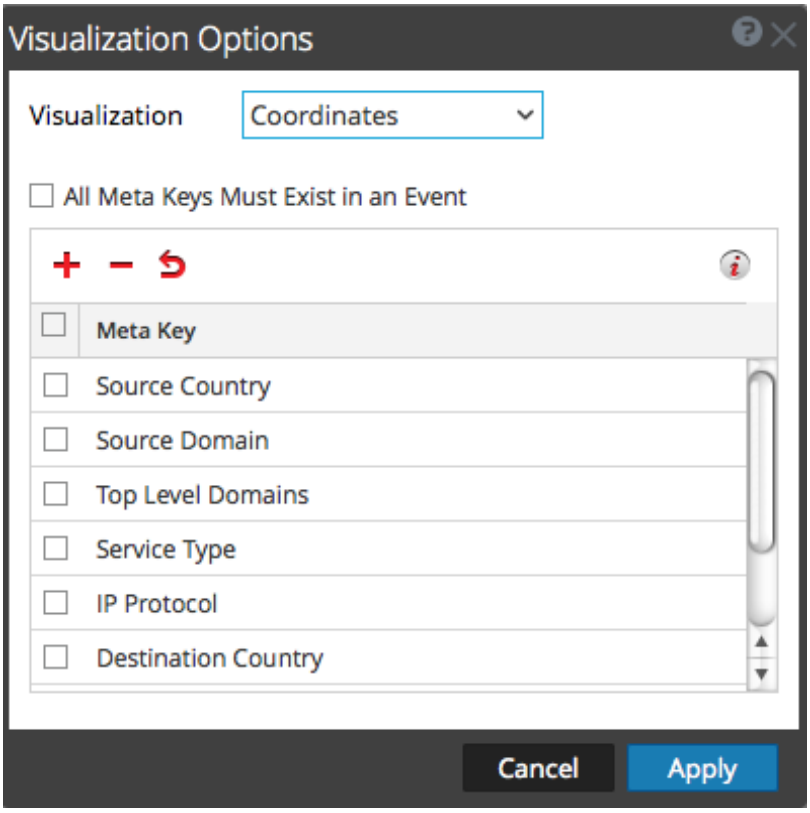
1. Wenn der Bereich „Visualisierung“ über dem Bereich „Werte“ geschlossen ist, wählen Sie **Visualisierung** aus.
2. Wählen Sie in der Symbolleiste **Meta** > **Metagruppe verwenden > Dateianalyse (Malware Analysis)** aus.
3. Klicken Sie im Bereich **Werte** im Metaschlüssel **Forensischer Fingerabdruck** auf `windows_executable` und dann auf `x86 pe`, sodass die Brotkrümelnavigation `filetype = 'windows_executable' | filetype = 'x86 pe'` lautet.

4. Als Zeitachse wird eine Standardvisualisierung für den aktuellen Drill-down-Punkt angezeigt.

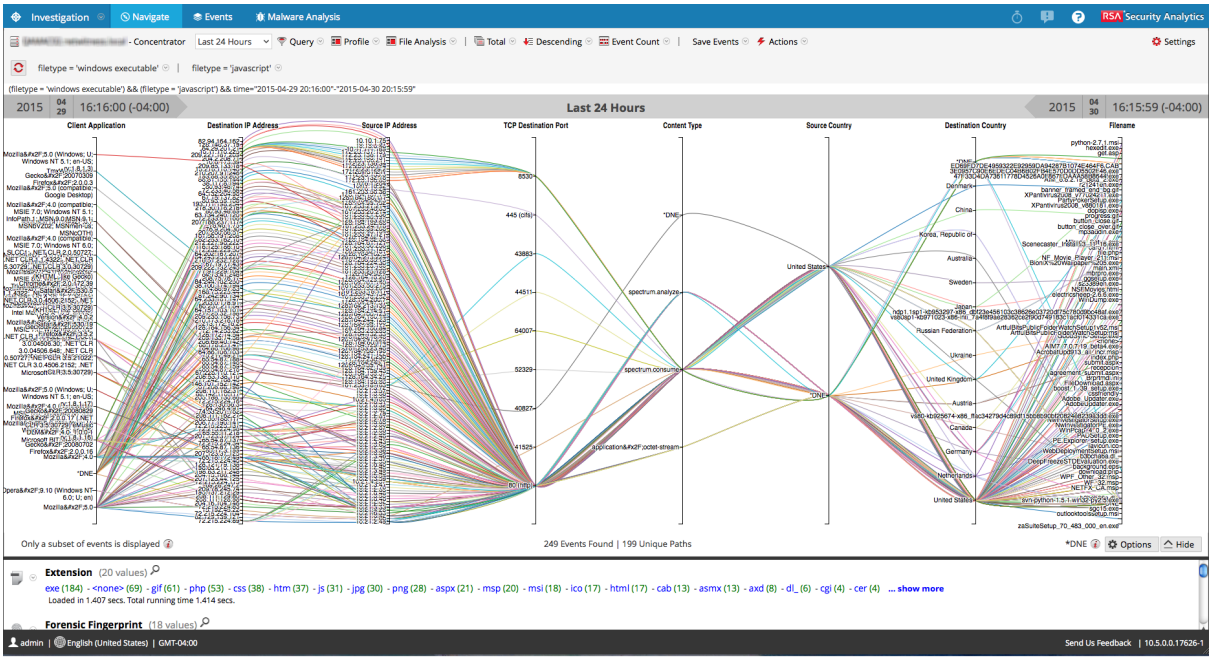


5. Wählen Sie im Bereich **Visualisierung** den Punkt **Optionen** aus.
   Das Dialogfeld „Visualisierungsoptionen“ wird angezeigt.

6. Wählen Sie in der Drop-down-Liste **Visualisierung** die Option **Koordinaten** aus und klicken Sie auf **Anwenden**.



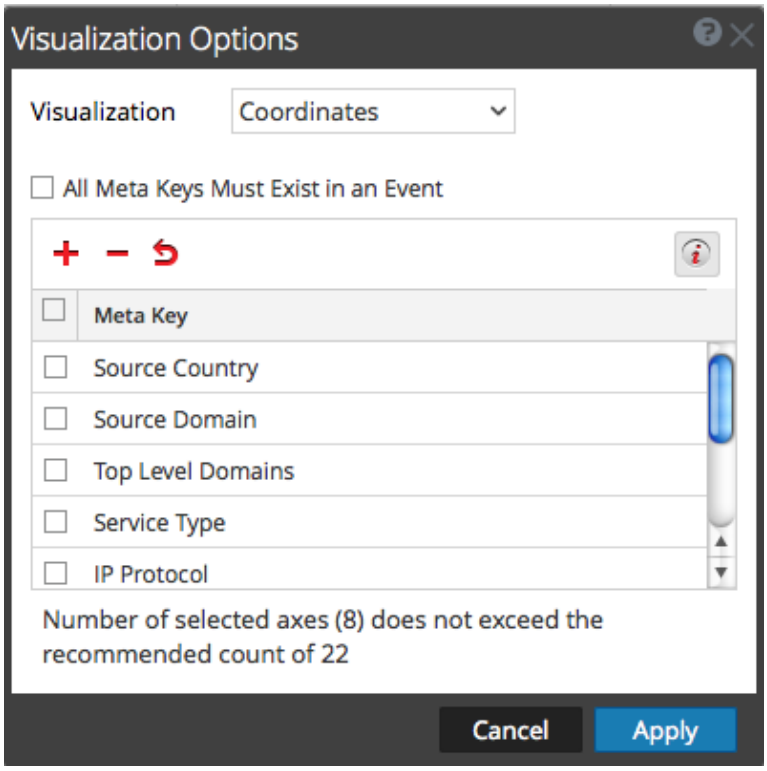
Die Visualisierung wird geladen. In diesem Beispiel wurden 249 Ereignisse gefunden und es werden 199 eindeutige Pfade visualisiert.



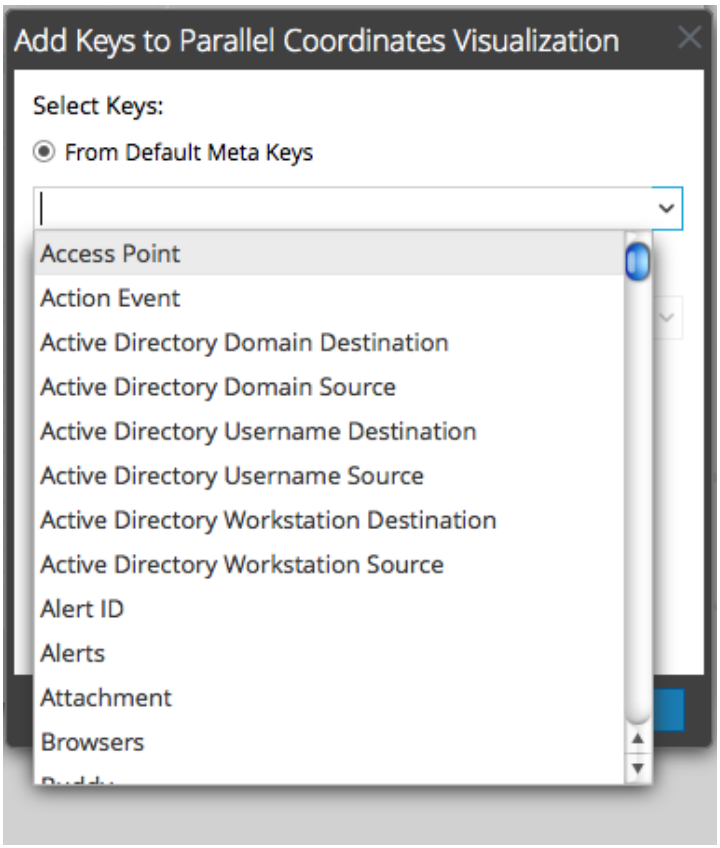
Auswählen der Metaschlüssel für eine Parallelkoordinatenvisualisierung

Gehen Sie bei geöffneter Parallelkoordinatenvisualisierung wie folgt vor:

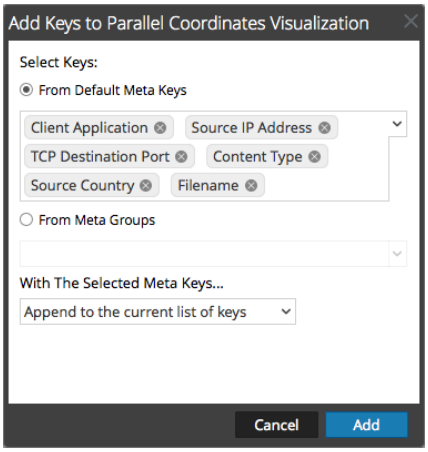
1. Wählen Sie im Bereich „Visualisierung“ den Punkt **Optionen** aus.
   Das Dialogfeld „Visualisierungsoptionen“ wird angezeigt. Klicken Sie in der Symbolleiste auf , um die empfohlene Anzahl an Achsen für eine lesbare Visualisierung anzuzeigen. Wenn eine empfohlene Anzahl an Schlüsseln angezeigt wird, ändert sich diese basierend auf der Browsergröße. Wenn Sie das Browserfenster vergrößern, steigt die empfohlene Anzahl.



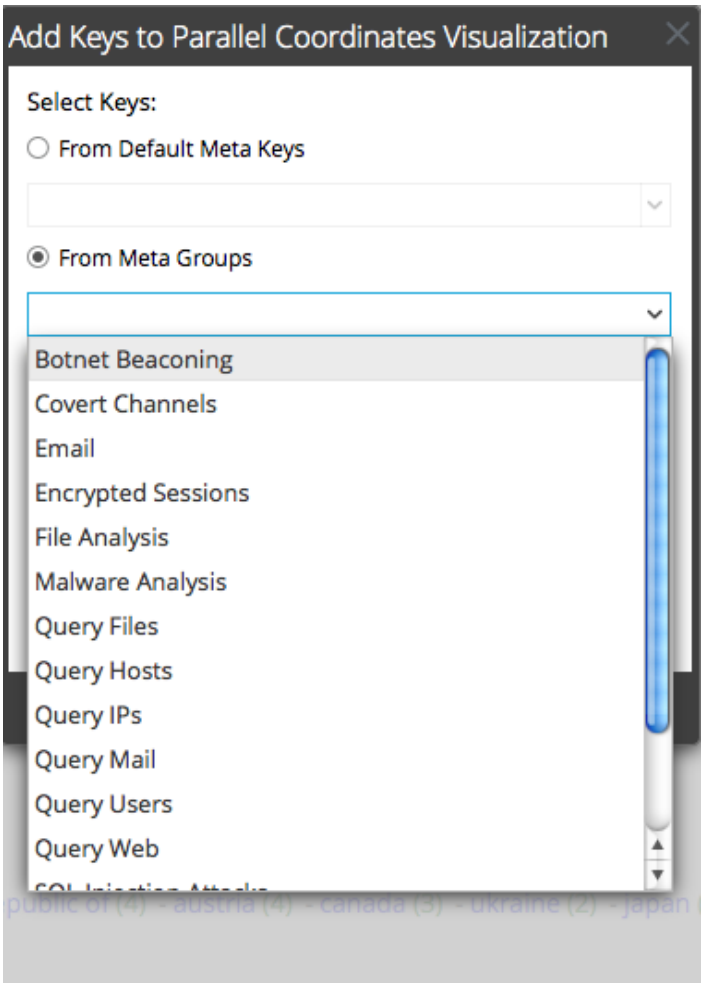
2. Wenn Sie die Reihenfolge der Metaschlüssel ändern möchten, ziehen Sie die Metaschlüssel in die gewünschte Reihenfolge nach oben oder unten.
3. Wenn Sie Metaschlüssel löschen möchten, klicken Sie in das Auswahlfeld und klicken Sie auf .
   Die Metaschlüssel werden entfernt, aber die Änderung wurde nicht angewendet.
4. Wenn Sie den vorherigen Zustand wiederherstellen möchten, klicken Sie auf .
   Die von Ihnen gelöschten Metaschlüssel werden wiederhergestellt und alle vorgenommenen Änderungen werden entfernt.
5. Wenn Sie einzelne Metaschlüssel auswählen möchten, klicken Sie auf , wählen Sie **Aus Standardschlüsseln** aus und wählen Sie in der Drop-down-Liste die Metaschlüssel aus.



Die ausgewählten Schlüssel werden aufgeführt.

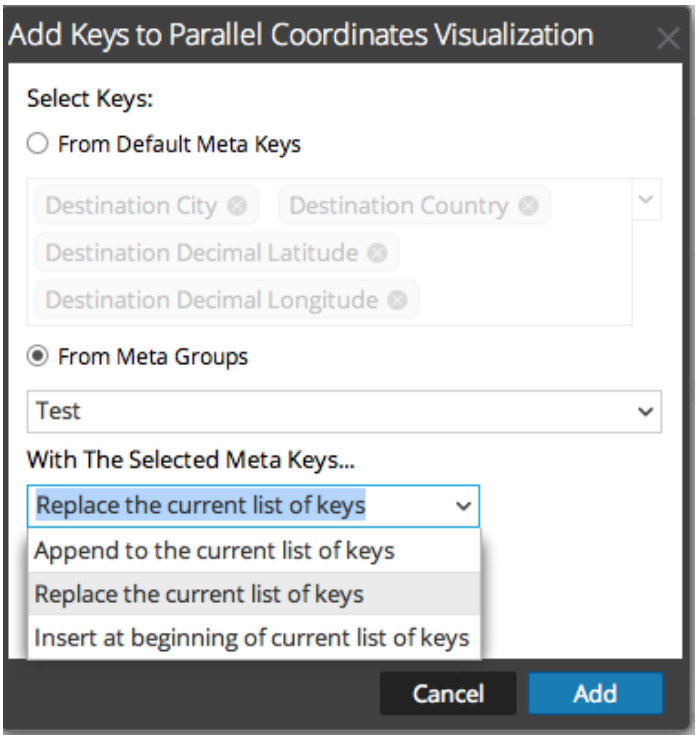


6. Wenn Sie alle Schlüssel einer Metagruppe hinzufügen möchten, können Sie keine einzelnen Schlüssel hinzufügen. Wählen Sie **Aus Metagruppen** aus und wählen Sie in der Drop-down-Liste eine Gruppe aus.

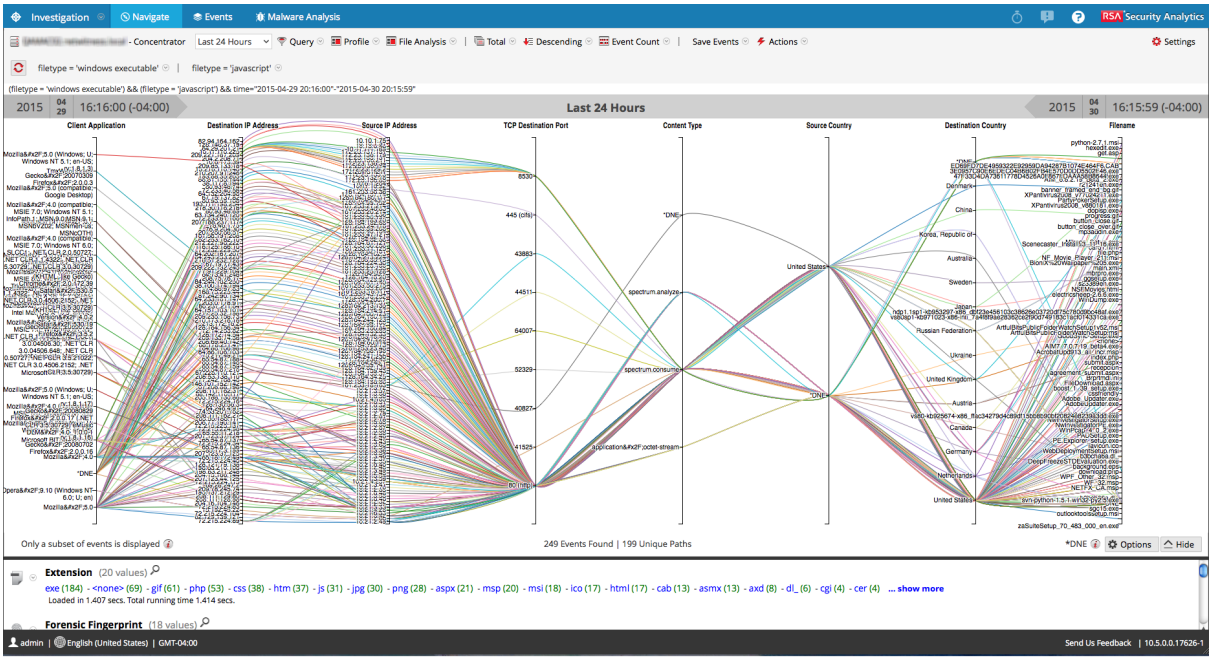


Die ausgewählten Metagruppen werden in dem Feld aufgelistet.

7. Wählen Sie die Methode für das Hinzufügen von Schlüsseln oder Gruppen aus: **Aktuelle Schlüsselliste ersetzen**, **An aktuelle Schlüsselliste anhängen** (am Ende) oder **Am Anfang der aktuellen Schlüsselliste einfügen.**

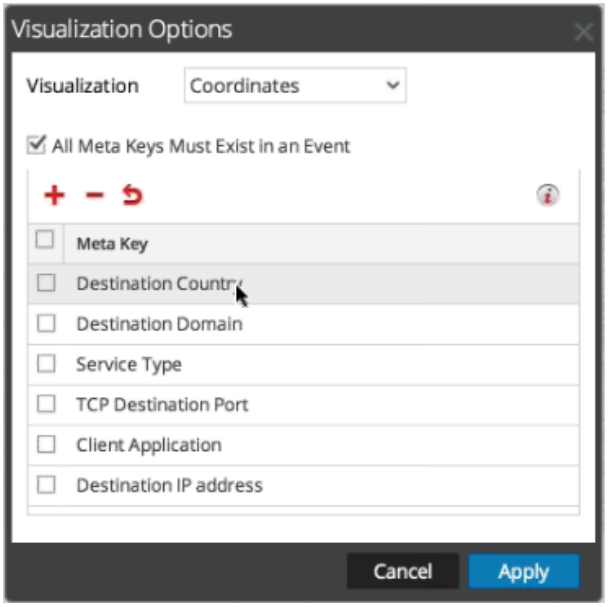


8. Klicken Sie auf **Hinzufügen**, um das Verfahren abzuschließen.
   Das Dialogfeld „Visualisierungsoptionen“ wird mit den ausgewählten Metaschlüsseln oder -gruppen angezeigt.
9. Klicken Sie zum Anzeigen des neuen Visualisierungsdiagramms auf **Anwenden**.

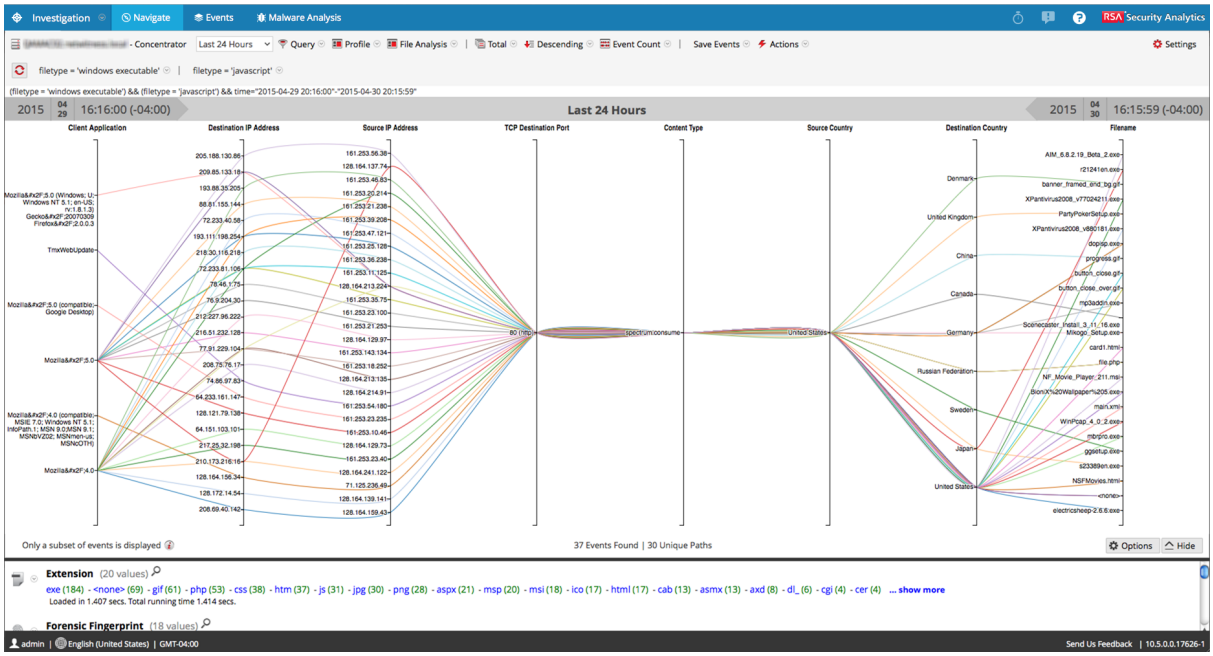


Optimieren einer Parallelkoordinatenvisualisierung

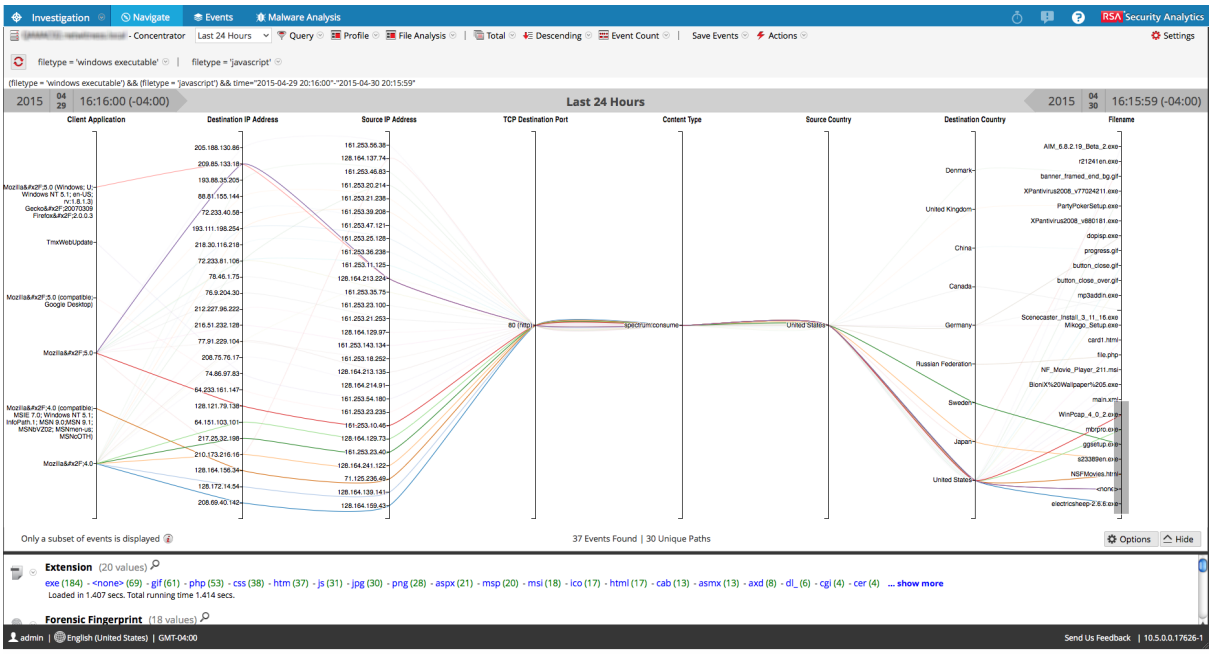
1. Wählen Sie zum Optimieren der Visualisierung durch Entfernen der Ereignisse, in denen nicht alle Metaschlüssel enthalten sind, **Optionen** aus.



2. Wählen Sie im Dialogfeld „Visualisierungsoptionen“ die Option **Alle Metaschlüssel müssen in einem Ereignis vorhanden sein** aus. Klicken Sie auf **Anwenden**.
   Das resultierende Diagramm ist besser lesbar und nützlicher und enthält eine geringere Anzahl eindeutiger Pfade.



3. Wenn Sie einen kleinen Satz Punkte hervorheben möchten, um den Pfad der Linie von links nach rechts zu verfolgen, klicken Sie auf eine Achse. Der Cursor ändert sich zu einem Fadenkreuz, das Sie ziehen können, um einen oder mehrere Werte auszuwählen. Wenn Sie die Maus loslassen, werden die Linien hervorgehoben. Im Beispiel unten ist der SSL-Servicetyp durch ein graues Feld hervorgehoben.



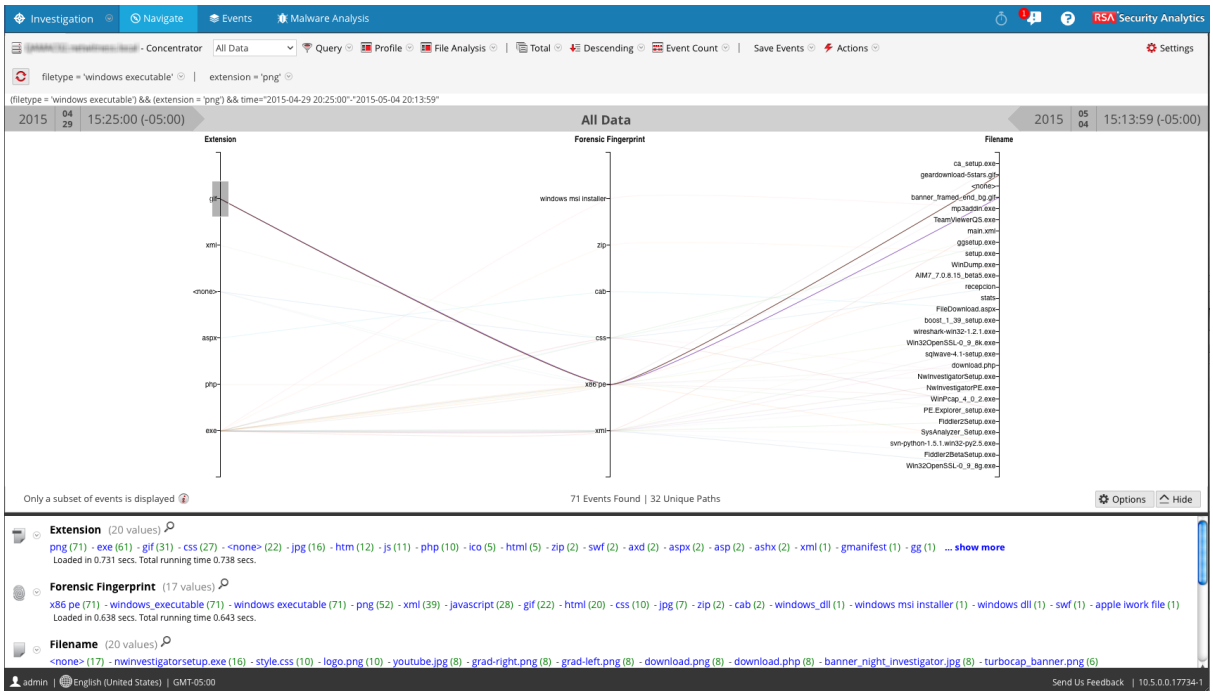
4. Wenn Sie die Visualisierung vergrößern möchten, ziehen Sie die untere Ecke des Bereichs nach unten und ziehen Sie die rechte Ecke des Browserfensters breiter.

Anwendungsbeispiel

Unten sehen Sie ein Beispiel für eine Parallelkoordinatenvisualisierung von Metaschlüsseln, die Dateimetadaten in einer Sitzung repräsentieren. Von links nach rechts gibt es drei Metaschlüssel oder Achsen: „Erweiterungen“, „Forensischer Fingerabdruck“ und „Dateiname“ mit Werten für jede Achse. Die Werte auf der Achse „Erweiterungen“ zeigen die Dateierweiterungen an und die Werte auf der Achse „Forensischer Fingerabdruck“ sind ausführbare Windows-Dateien. Normalerweise passt der Dateityp zum erwarteten forensischen Fingerabdruck. Es ist jedoch abnormal, dass ein `gif`-Dateityp mit dem Fingerabdruck einer ausführbaren Windows-Datei kombiniert ist. Der `gif`-Dateityp ist ausgewählt, um die Korrelationen dieses Dateityps, `x86pe` und zwei Dateinamen in der dritten Achse hervorzuheben, sodass ein Analyst Dateien, die eine Ermittlung erfordern, schnell erkennen kann.

So gelangen Sie zu dieser Ansicht:

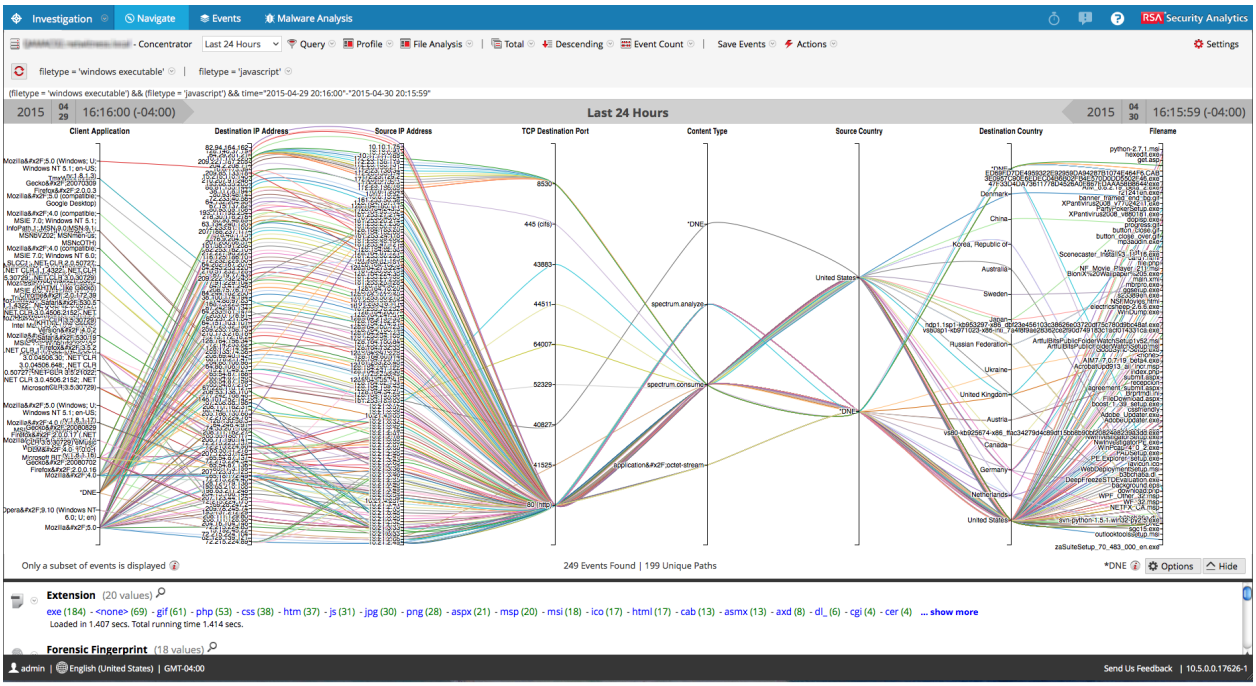
1. Nach Wert ordnen und In aufsteigender Reihenfolge sortieren.
2. Wenden Sie in der Ansicht „Navigation“ zwei Filter an (Dateityp = „ausführbare Windows-Datei“ und Erweiterung = „gif“), um die Datenmenge zu begrenzen.
3. Konfigurieren Sie ein Parallelkoordinatendiagramm durch Auswählen von drei Achsen: `file extension`, `forensic fingerprint` und `filename`.



Beispielvisualisierung eines großen Datensatzes

Dieses Beispiel für eine Parallelkoordinatenvisualisierung, die auf einen größeren Datensatz angewendet wurde, veranschaulicht mehrere Meldungen, anhand derer Analysten verstehen können, was visualisiert wurde.

- Zum Erstellen des Diagramms beginnt NetWitness Platform mit dem Scannen von Metawerten und der Ausgabe von Ergebnissen. Ein typischer Zeitbereich könnte bis zu 10.000.000 Metawerte enthalten. Wenn die Anzahl der zurückgegebenen Metawerte den Ergebnisgrenzwert für Metawerte erreicht, wird das Diagramm dargestellt, auch wenn die von NetWitness Platform gescannte Anzahl an Metawerten nicht dem Scangrenzwert für Metawerte entspricht.
- Es gibt eine feste Höchstgrenze für die Datenmenge, die als Parallelkoordinatendiagramm gerendert werden kann. In NetWitness Platform 10.4 und früher basiert diese Grenze auf der Anzahl von Achsen multipliziert mit den Datenwerten: 1000 x die Anzahl der Achsen zum Schutz der Performance. In NetWitness Platform 10.5 konfiguriert der Administrator die Grenzen für Parallelkoordinatenvisualisierungen in den Investigation-Einstellungen in der Ansicht „Administration System“.



Bei einem größeren Datensatz dauert die Verarbeitung des Parallelkoordinatendiagramms länger als bei einem kleinen Satz Daten und Metaschlüssel. Zur Wahrung der Performance stellt NetWitness Platform die Metawerte aus dem Bereich „Werte“ unten so lange dar, bis die vom Administrator festgelegten Grenzen erreicht sind. Es wird folgende Informationsmeldung angezeigt: **Nur eine Teilmenge der Ereignisse wird angezeigt.**

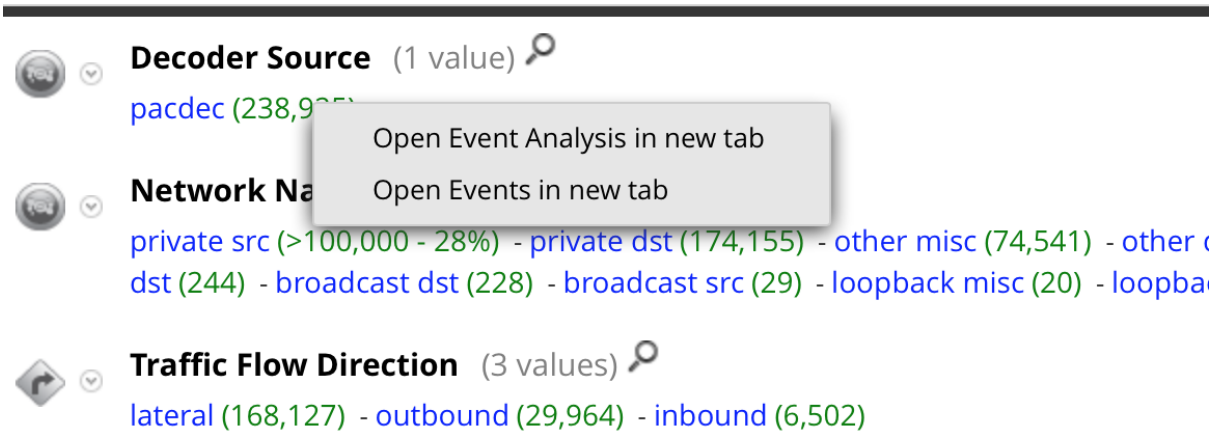
Unter allen für 249 Ereignisse visualisierten Daten gab es nur 199 eindeutige Parallelkoordinatenpfade. Einige Ereignisse sind enthalten, obwohl darin einige Metaschlüssel fehlen. Sie sind mit **DNE** gekennzeichnet, da die Metadaten in dem Ereignis nicht vorhanden sind.

Öffnen eines Ereignisses in der Ereignisliste

Analysten können in den Ansichten „Untersuchen > Ereignisse“ oder „Ereignisanalyse“ eine Liste von Ereignissen anzeigen, die einer Sitzung zugeordnet sind.

Führen Sie einen der folgenden Schritte durch, um Ereignisse in der Ansicht „Ereignisse“ anzuzeigen:

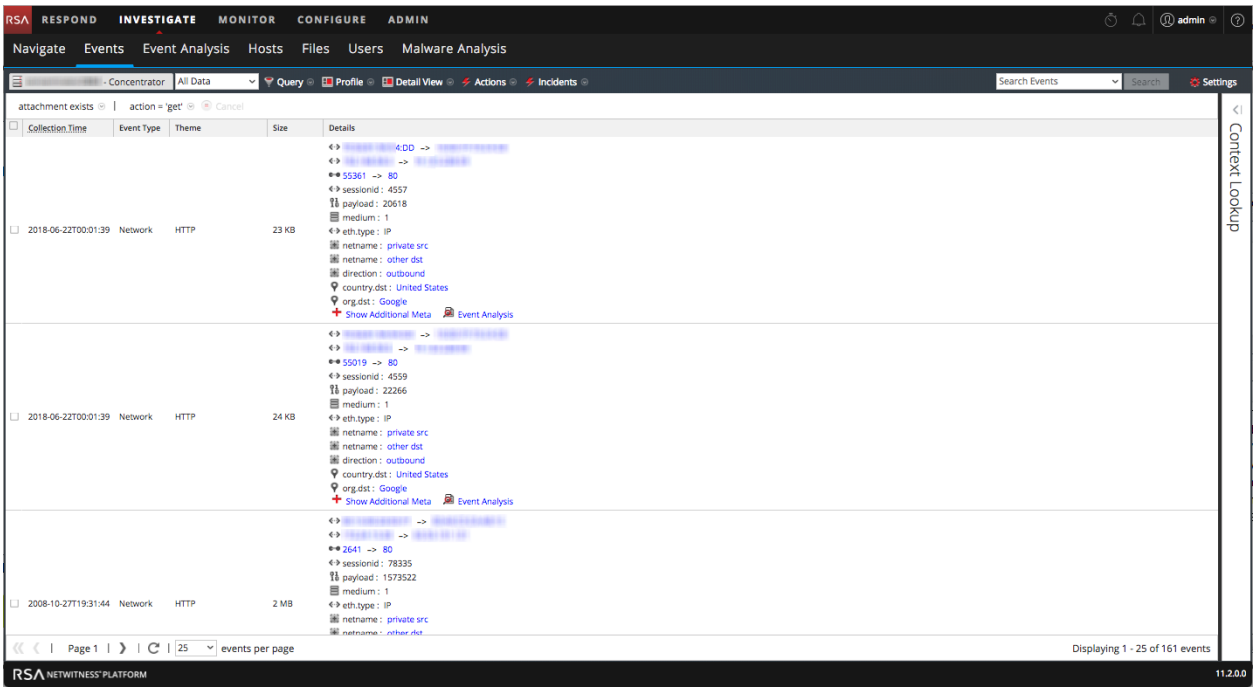
1. Navigieren Sie zu **INVESTIGATE** > **Ereignisse**, um die Standardabfrage für den Standardservice zu verwenden.
   NetWitness Platform führt eine Standardabfrage über die letzten drei Stunden für den Standardservice (sofern festgelegt) aus oder zeigt ein Dialogfeld an, in dem Sie einen Service auswählen können, und führt dann die Standardabfrage aus. Die Standardabfrage wählt alle Ereignisse aus und die Ansicht „Ereignisse“ zeigt Ereignisse des ausgewählten Services an, mit den ältesten Ereignissen zuerst.
2. Zeigen Sie die Ereignisse für einen bestimmten Metawert an, indem Sie zu **INVESTIGATE** > **Navigation** wechseln und auf eine Metaanzahl (die Metaanzahl erscheint als grüner Text) klicken, nachdem Ereignisse im Bereich „Werte“ geladen wurden. Sie können auch mit der rechten Maustaste auf die Metaanzahl für einen Metawert klicken. Wenn das Kontextmenü angezeigt wird, klicken Sie auf **Ereignisse auf neuer Registerkarte öffnen**. (Die Option „Ereignisanalyse in neuer Registerkarte öffnen“ ist in Version 11.1 oder höher verfügbar.)



   In der Ansicht „Ereignisse“ werden die Ereignisse für den ausgewählten Metawert angezeigt.

Die Ansicht „Ereignisse“ bietet drei integrierte Darstellungsarten für Ereignisdaten: die Detailansicht, die Listenansicht und die Protokollansicht.

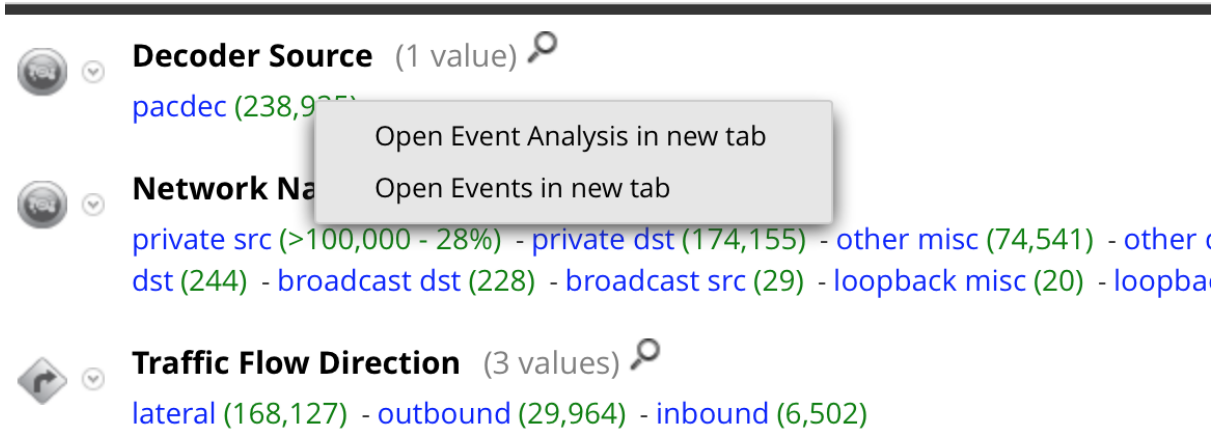
Diese Abbildung zeigt ein Beispiel für die Detailansicht.



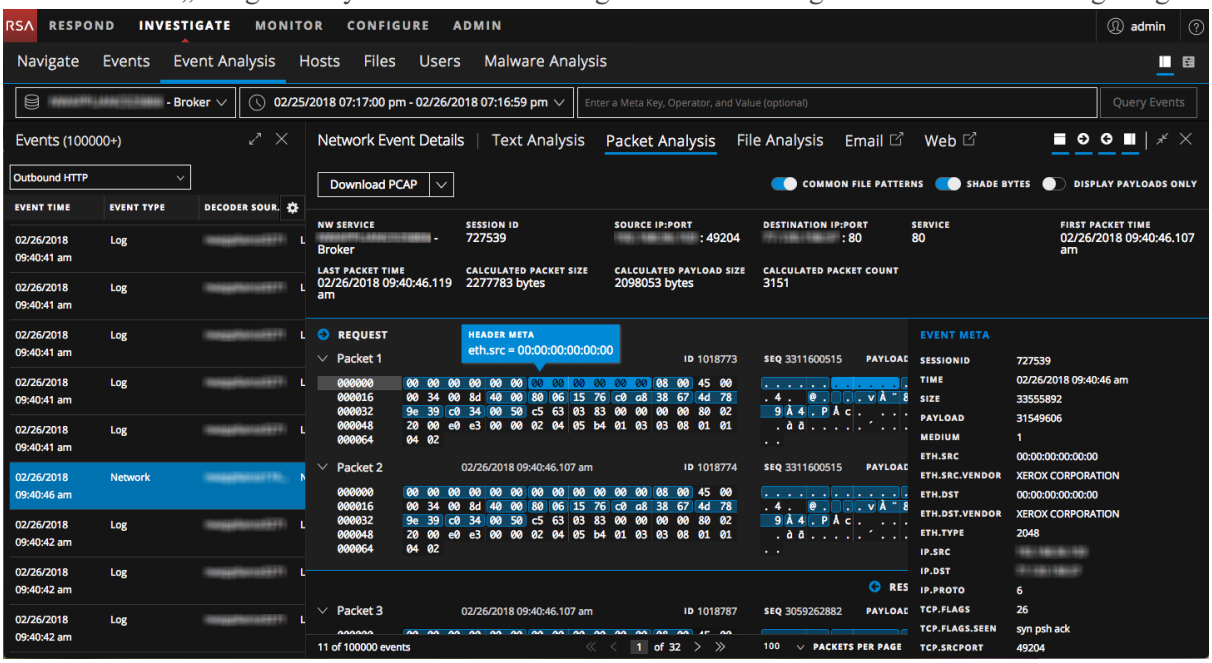
Sie können Abfragen, die Zeitbereichseinstellung und Profile verwenden, um die in der Ansicht „Ereignisse“ aufgeführten Ereignisse zu filtern. Von jedem der Ereignistypen in der Ereignisansicht aus können Sie Dateien extrahieren, Ereignisse exportieren, Protokolle exportieren und den Bereich Ereignisrekonstruktion öffnen, indem Sie auf ein Ereignis doppelklicken. Weitere Informationen über diese Funktionen finden Sie unter Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse“.

Führen Sie einen der folgenden Schritte durch, um Ereignisse in der Ansicht „Ereignisanalyse“ anzuzeigen:

1. Wechseln Sie in Version 11.0 und höher zu **UNTERSUCHEN > Navigation** und klicken Sie auf die Anzahl für einen Metawert (die Anzahl der Metawerte erscheint als grüner Text). Wenn das Kontextmenü angezeigt wird, wählen Sie **Ereignisanalyse in neuer Registerkarte öffnen** aus.



In der Ansicht „Ereignisanalyse“ werden die Ereignisse für den ausgewählten Metawert angezeigt.



Detaillierte Informationen über die Arten der Analyse, die Sie in dieser Ansicht verwenden können, finden Sie unter Analysieren von Raw-Ereignissen und Metadaten in der Ansicht „Ereignisanalyse“.

Exportieren oder Drucken eines Drill-down-Punkts

Wenn in NetWitness Investigate die Daten für einen Drill-down-Punkt in der Ansicht „Navigation“ angezeigt werden, können Sie:

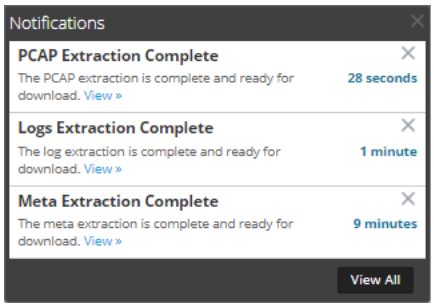
- Dateien aus einer Sitzung extrahieren und den Typ der zu extrahierenden Dateien wählen: Archive, Audio-BitTorrent, Dokumente, ausführbare Dateien, Bilder, andere, Video und Web.
- Den Drill-down-Punkt als Paketerfassungsdatei (PCAP), Protokolldatei oder Metadatendatei exportieren.
- Den Drill-down-Punkt drucken.

Die zu exportierenden Detailinformationen werden sowohl durch den Zeitbereich als auch durch den Drill-down-Punkt zum Zeitpunkt des Exports beeinflusst.

Hinweis: Wenn Sie den Drill-down-Punkt als Protokolldatei exportieren, werden nur die Protokollsitzungen exportiert. Die Jobwarteschlangenmeldung bezieht sich auf die Gesamtanzahl an Sitzungen in dem Drill-down-Punkt statt auf die Anzahl der Protokolle. Beispiel: Wenn der Drill-down-Punkt 505 Sitzungen und nur fünf Protokollsitzungen umfasst, wird in der Jobwarteschlangenmeldung angegeben, dass NetWitness Platform Protokolle für 505 Sitzungen exportiert.

So exportieren Sie einen Drill-down-Punkt aus der Ansicht „Navigation“:

1. Führen Sie Ermittlungen durch, bis Sie den gewünschten Drill-down-Punkt erreichen.
2. Wählen Sie bei Version 11.0 in der Symbolleiste **Aktionen > Exportieren** und dann eine der folgenden Exportoptionen aus: **PCAP**, **Protokolle** oder **Meta**.
   Der Drill-down-Punkt wird extrahiert und eine Meldung angezeigt, dass der Job geplant ist. Den Status können Sie auf der Jobseite prüfen.
3. Wählen Sie in Version 11.1 in der Symbolleiste **Ereignisse speichern** und eine der Exportoptionen aus: **PCAP**, **Protokolle**, **Dateien** oder **Metawerte**.
   Ein Dialogfeld gibt Ihnen die Möglichkeit, den Standarddateinamen für die Datei zu bearbeiten. Der Standardwert hat das Format `investigation-Feb-21-15-44-33`. Wenn Sie ein PCAP exportieren, wird die Datei ohne Formatauswahl exportiert. Wenn Sie eine der anderen Exportoptionen nutzen, wird ein Dialog angezeigt.
4. Im Dialog wählen Sie Folgendes aus:
   - Das Exportprotokollformat: **Text**, **XML**, **CSV** oder **JSON**.
   - Den zu exportierenden Inhaltstyp: Archive, BitTorrent, Dokumente, ausführbare Dateien, Bilder, Video, Web und andere
   - Das Meta-Format: **Text**, **CSV**, **TSV**, **JSON**.
5. Wenn die geplante Datei-Extrahierung abgeschlossen ist, wird sie im Jobbenachrichtigungsbereich angezeigt.



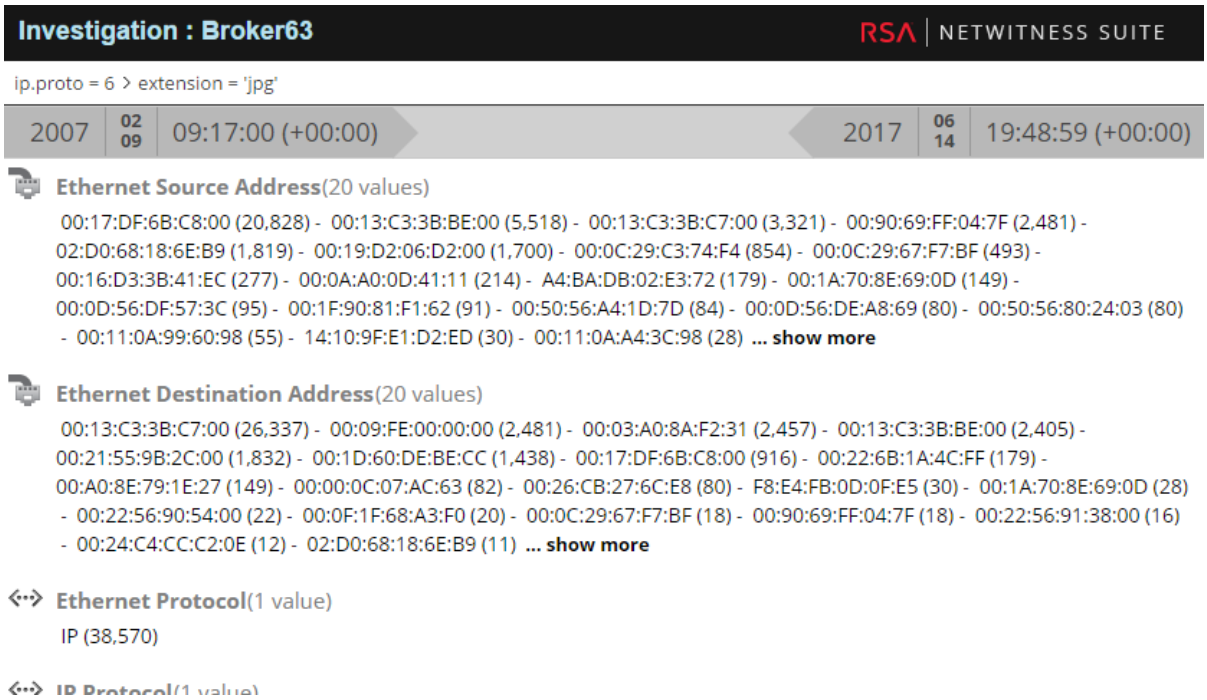
6. Klicken Sie auf den Link **Ansicht** zur Jobkurzübersicht und laden Sie die angeforderte Extraktionsdatei herunter.

So drucken Sie den aktuellen Drill-down-Punkt:

In der Ansicht „Navigation“ können Sie den Inhalt des aktuellen Drill-down-Punkts in einem druckerfreundlichen Format im Browserfenster anzeigen.

So zeigen Sie den aktuellen Drill-down-Punkt in einer Druckansicht an:

1. Wählen Sie, während ein Drill-down-Punkt in der Ansicht **Navigation** geöffnet ist, in der Symbolleiste **Aktionen** > **Drucken** aus.
   Es wird eine neue Registerkarte mit der Druckansicht des aktuellen Drill-down-Punkts erstellt.



2. Wählen Sie die Option Drucken in Ihrem Browser, um die druckbare Ansicht an den Drucker zu senden.

Starten einer externen Suche eines Metaschlüssels

Dieses Thema enthält Anweisungen für die Verwendung sofort einsatzfähiger Investigate-Plug-ins, um mithilfe von NetWitness Platform-externen Tools eine externe Suche bestimmter Metaschlüssel zu starten, während Daten in der Ansicht „Navigation“ oder „Ereignisse“ ermittelt werden.

Analysten können sofort einsatzfähige externe Suchen mit NetWitness Platform Investigate verwenden, um bei den Ermittlungen Zeit zu sparen. Die sofort einsatzfähigen Lookups sind verfügbar durch Klicken mit der rechten Maustaste auf einen dieser Metaschlüssel: IP-Adresse (`ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip`), `host (alias-host, domain.dst)`, `client`, und `file-hash`.

Für alle `IP`- und `host`-Metaschlüssel sind die folgenden Suchen in NetWitness Platform integriert:

- Google Malware: Öffnet eine Google Malware-Suche in einer neuen Registerkarte.
- SANS-IP-Verlauf: Öffnet eine SANS IP-Verlaufssuche in einer neuen Registerkarte.
- McAfee SiteAdvisor: Öffnet eine McAfee SiteAdvisor-Suche in einer neuen Registerkarte.
- Endpunkt Thick-Clientsuche: Öffnet eine Suche im NetWitness Endpoint-Thick-Client in einer neuen Registerkarte.
- BFK-passive DNS-Erfassung: Öffnet eine BFK-passive DNS-Erfassungsuche in einer neuen Registerkarte.
- CentralOps WHOIS für IP-Adressen und Hostnamen: Öffnet eine CentralOps Whois-Suche nach IP-Adressen und Hostnamen in einer neuen Registerkarte.
- Suche auf Malwaredomainlist.com: Öffnet eine Suche auf Malwaredomainlist.com in einer neuen Registerkarte.
- Robtex IP-Suche: Öffnet eine Robtex IP-Suche in einer neuen Registerkarte.
- ThreatExpert-Suche: Öffnet eine ThreatExpert-Suche in einer neuen Registerkarte.
- IPVoid-Suche: Öffnet eine UrlVoid-Suche in einer neuen Registerkarte.

Für die Metaschlüssel `file-hash` und `alias-host` öffnet Google-Lookup eine Google-Suche in einer neuen Registerkarte.

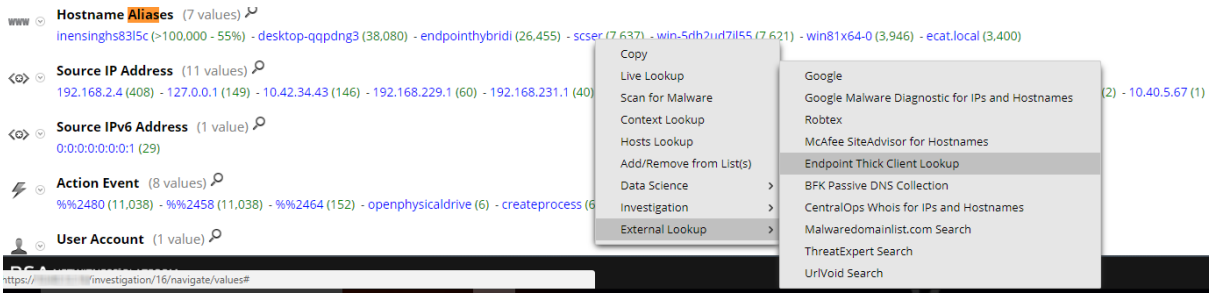
Für den Metaschlüssel `client` öffnet die Suchoption von NetWitness Endpoint einen Endpoint-Thick-Client in einer neuen Registerkarte, sofern der Client auf dem gleichen System installiert ist, auf dem der Browser verwendet wird.

Administratoren können zusätzliche externe Lookups hinzufügen und andere angepasste Aktionen durchführen, wie unter „Hinzufügen benutzerdefinierter Kontextmenüaktionen“ im *Systemkonfigurationsleitfaden* beschrieben.

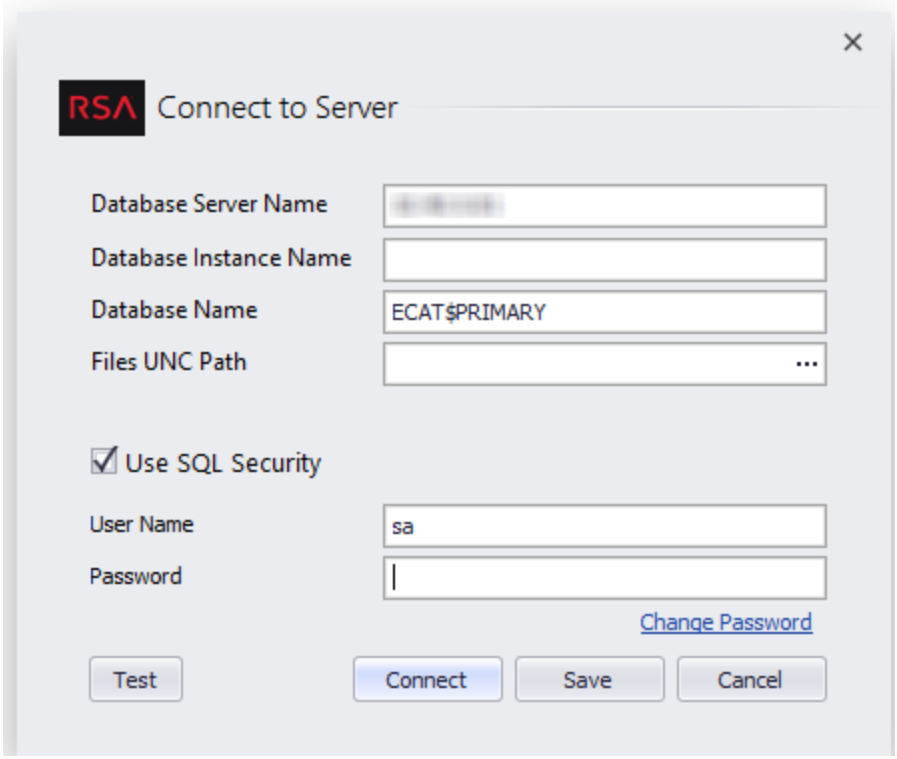
Starten einer Endpunkt Thick-Clientsuche:

So starten Sie eine Endpunkt Thick-Clientsuche von Daten in der Ansicht „Navigation“:

1. Klicken Sie mit der rechten Maustaste auf einen Metawert für einen der folgenden Metaschlüssel: `ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip, alias-host, domain.dst, client.`
2. Wählen Sie **Externe Suche** im Kontextmenü.
   Ein Untermenü mit externen Suchoptionen wird angezeigt.

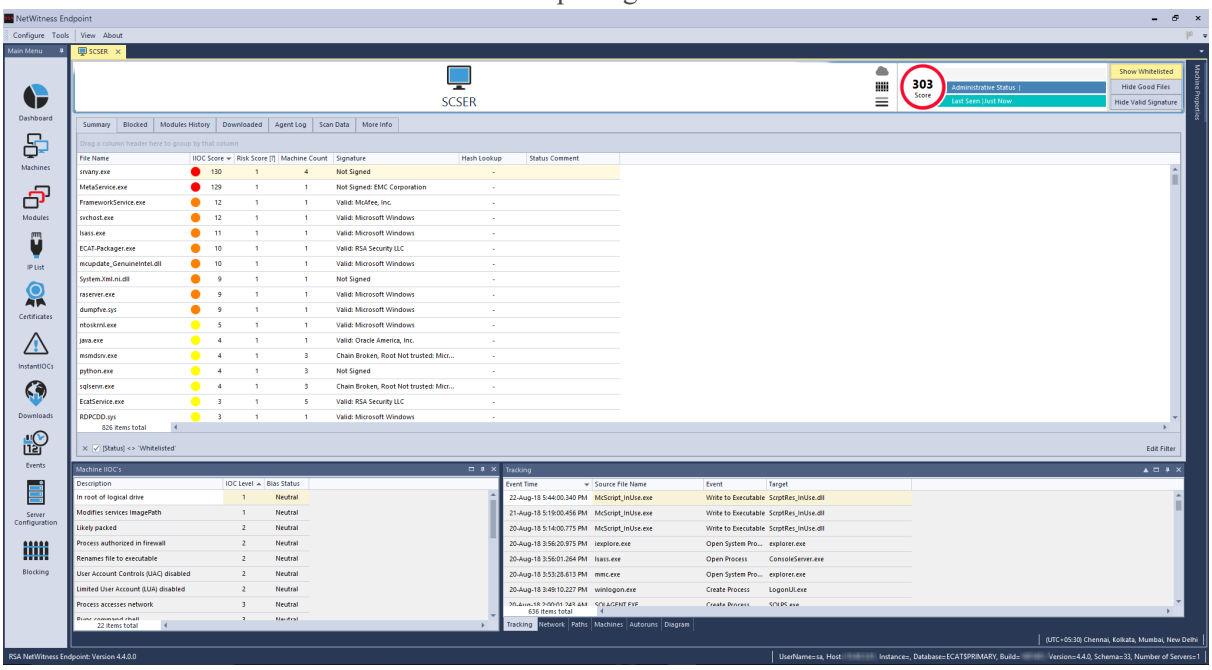


3. Wählen Sie **Endpunkt Thick-Clientsuche** aus.
   Das Dialogfeld „Verbindung mit Server“ wird angezeigt.



4. Geben Sie den Benutzernamen und das Passwort ein, die für die Anmeldung am Endpoint-Thick-Client erforderlich sind, und klicken Sie auf **Verbinden.**

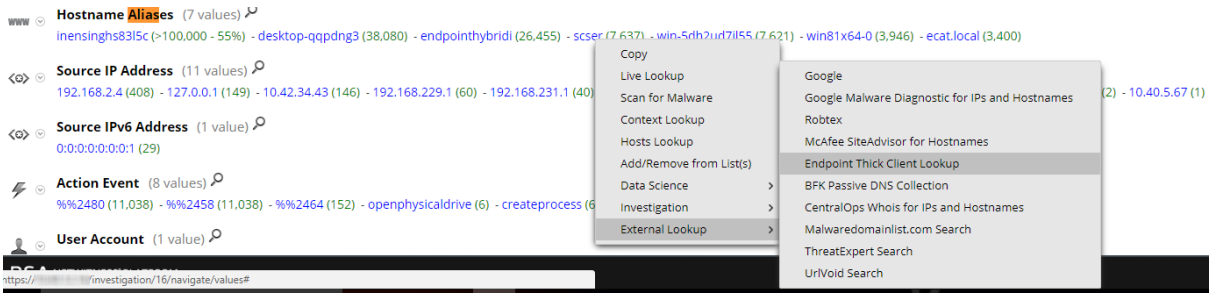
Der Drill-down-Punkt wird in NetWitness Endpoint geöffnet.



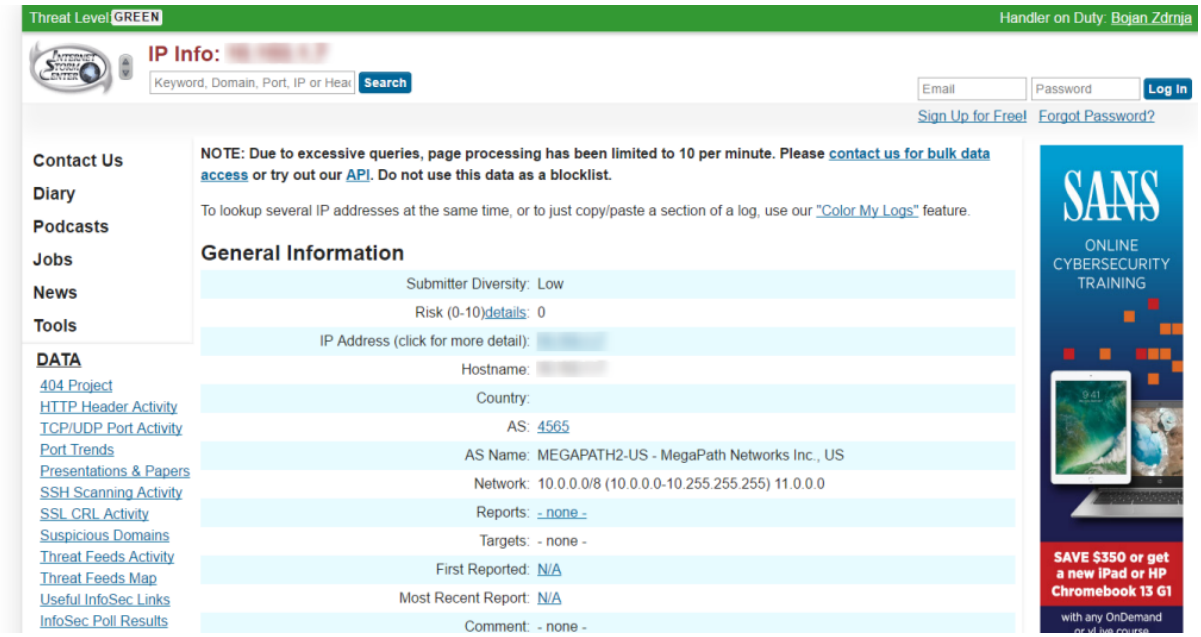
Starten weiterer externer Suchen

So starten Sie eine externe Suche (außer NetWitness Endpoint-Thick-Client-Suche) nach Daten aus der Ansicht „Navigation“:

1. Klicken Sie mit der rechten Maustaste auf einen Metawert für einen der folgenden Metaschlüssel:
   `ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip, alias-host, domain.dst, client.`
2. Wählen Sie **Externe Suche** im Kontextmenü.
   Ein Untermenü mit externen Suchoptionen wird angezeigt.



3. Wählen Sie eine der Suchoptionen aus.
   Der ausgewählte Metawert öffnet sich in der ausgewählten Suche. Wenn Sie zum Beispiel SANS-IP-Verlauf ausgewählt haben, wird die Information über den Drill-down-Punkt im SANS Internet Storm Center angezeigt.

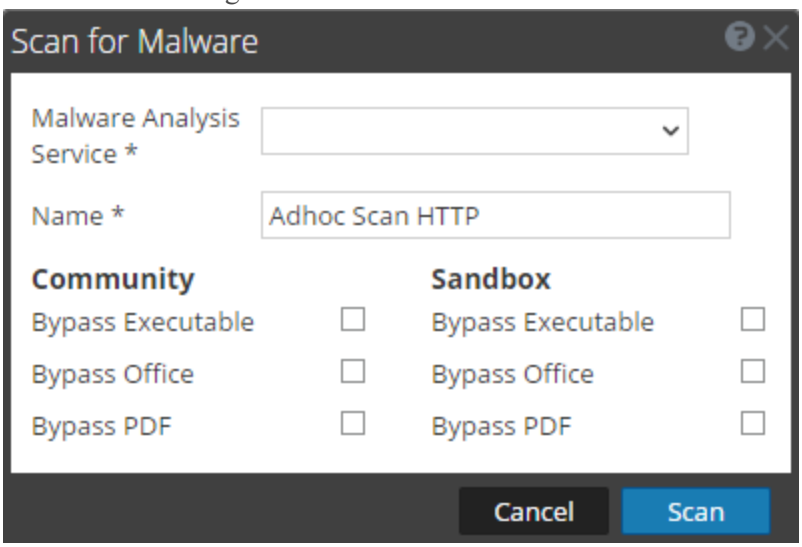

Threat Level GREEN
Handler on Duty: Bojan Zdrnja
IP Info:
Keyword, Domain, Port, IP or Hea
Search
Email
Password
Log In
Sign Up for Free!
Forgot Password?
Contact Us
Diary
Podcasts
Jobs
News
Tools
DATA
404 Project
HTTP Header Activity
TCP/UDP Port Activity
Port Trends
Presentations & Papers
SSH Scanning Activity
SSL CRL Activity
Suspicious Domains
Threat Feeds Activity
Threat Feeds Map
Useful InfoSec Links
InfoSec Poll Results
NOTE: Due to excessive queries, page processing has been limited to 10 per minute. Please contact us for bulk data access or try out our API. Do not use this data as a blocklist.
To lookup several IP addresses at the same time, or to just copy/paste a section of a log, use our "Color My Logs" feature.
General Information
Submitter Diversity: Low
Risk (0-10)details: 0
IP Address (click for more detail):
Hostname:
Country:
AS: 4565
AS Name: MEGAPATH2-US - MegaPath Networks Inc., US
Network: 10.0.0.0/8 (10.0.0.0-10.255.255.255) 11.0.0.0
Reports: - none -
Targets: - none -
First Reported: N/A
Most Recent Report: N/A
Comment: - none -
SANS
ONLINE CYBERSECURITY TRAINING
SAVE $350 or get a new iPad or HP Chromebook 13 G1
with any OnDemand

Starten eines Malware Analysis-Scans in der Ansicht „Navigation“

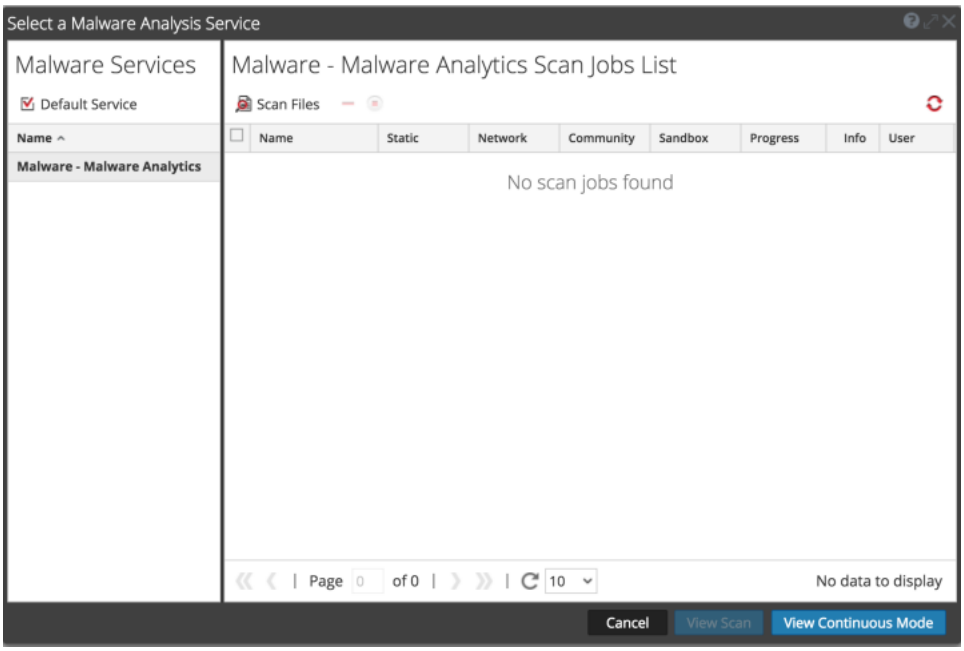
Analysten können aus Investigate heraus einen Malware Analysis-Scan nach Bedarf starten, indem sie einen Service und einen Metawert und dann eine Option aus dem Kontextmenü auswählen. Wenn die Abfrage abgeschlossen ist, stehen die gescannten Daten für die Schadsoftwareanalyse zur Verfügung.

So starten Sie einen Malware Analysis-Scan von Daten aus der Ansicht „UNTERSUCHEN“ > „Navigation“:

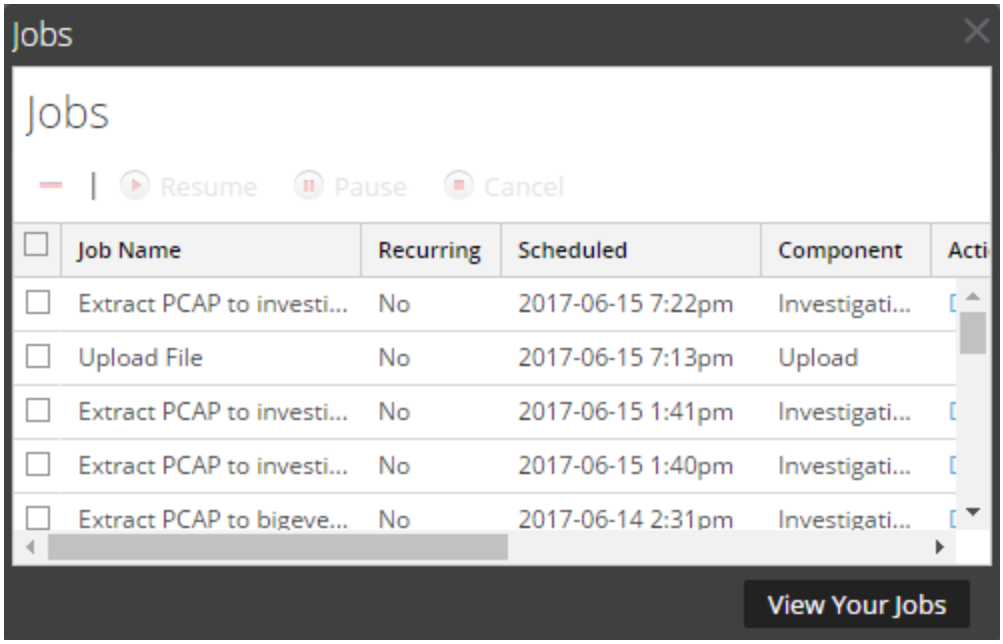
1. Klicken Sie mit der rechten Maustaste auf einen Metawert (zum Beispiel OTHER, DNS oder FTP) und wählen Sie im Kontextmenü **Auf Schadsoftware scannen** aus.
   Das Dialogfeld „Auf Schadsoftware scannen“ wird mit einem vorgeschlagenen Namen für den Scan nach Bedarf und ohne ausgewählten Service angezeigt.
2. Wählen Sie im Dialogfeld „Auf Schadsoftware scannen“ einen Service aus, um den Scan auszuführen, bearbeiten Sie den Namen und wählen Sie die Dateitypen aus, die unter Community und Sandbox zu umgehen sind.



3. Klicken Sie auf **Scannen**.
   Die Scananforderung wird dem Dashlet „Liste der Scanjobs“ und der Jobkurzübersicht hinzugefügt. Die Überbrückungseinstellungen in diesem Dialogfeld überschreiben die Standardeinstellungen in den Malware Analysis-Basiskonfigurationseinstellungen.
4. Führen Sie für den Zugriff auf diese Ansicht einen der folgenden Schritte aus:
   a. Navigieren Sie zu der Liste der Scanjobs in der Ansicht „Malware Analysis“ oder im Dashboard „Unified“. Doppelklicken Sie auf einen Scan, um ihn anzuzeigen.



b. Klicken Sie zur Ansicht des Jobs in der Jobkurzübersicht auf in der NetWitness Platform-Symbolleiste. Blättern Sie nach Abschluss des Jobs nach links und klicken Sie auf **Anzeigen**.



Die Schadsoftware-Ereigniszusammenfassung für den ausgewählten Scan wird angezeigt. Der Scan wird auch zu der Liste verfügbarer Scans im Dialogfeld zur Auswahl von Scans in der Registerkarte „Investigation > Schadsoftware“ hinzugefügt.

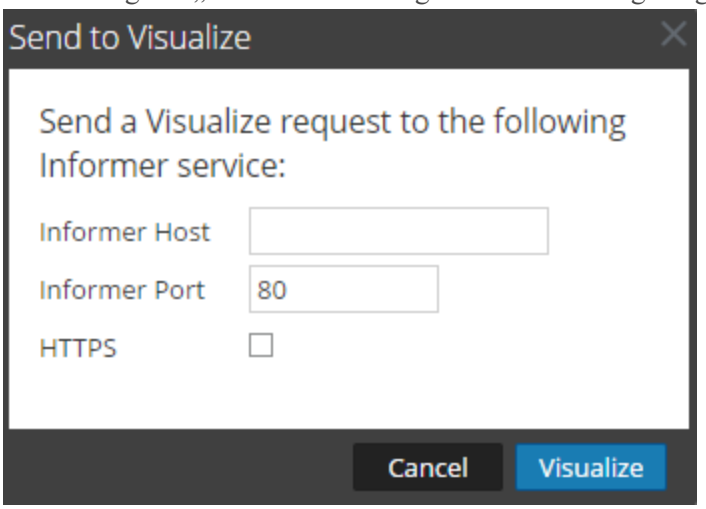
Visualisieren des aktuellen Drill-Punkts in Informer

Dieses Thema bietet Anweisungen zum Senden eines Drill-down-Punkts in der Ansicht „Navigation“ an eine Informer-Visualisierung.

Informer muss in Ihrem Netzwerk installiert und vom zu untersuchenden Service aus zugänglich sein. Sie müssen den Hostnamen und den auf dem Informantenhost verwendeten Port angeben, um mit NetWitness Platform zu kommunizieren.

So zeigen Sie eine Visualisierung des aktuellen Drill-down-Punkts in Informer an:

1. Klicken Sie mit geöffnetem Drill-down-Punkt in der Ansicht „Navigation“ auf **Aktionen** > **Visualisieren**.
   Das Dialogfeld „Zur Visualisierung senden“ wird angezeigt.



2. Geben Sie den Informer-Hostnamen oder die Informer-IP-Adresse ein und überprüfen Sie den NetWitness Platform-Serverport, der zum Kommunizieren mit dem Informer-Host verwendet wird.
3. (Optional) Wählen Sie die Option „HTTPS“, wenn der Informantenhost sichere Kommunikation verwendet.
4. Klicken Sie auf **Visualisieren**.
   Die Visualisierung wird auf einer neuen Registerkarte angezeigt.

Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse“

Analysten, die mit Investigate Daten ermitteln, können die mit einer Sitzung verknüpften Ereignisse anzeigen und rekonstruieren.

- Analysten, die Analysen mit NetWitness Platform Investigate durchführen und die entsprechenden Systemrollen und Berechtigungen für ihre Benutzerkonten eingerichtet haben, können von einem Navigations-Drill-down-Punkt zur Ansicht „Ereignisse“ wechseln.
- Analysten, die keinen Zugriff auf die Ansicht „Navigation“ haben oder die direkt zur Ansicht „Ereignisse“ wechseln möchten, können Sitzungen in der Ansicht „Ereignisse“ öffnen und die Ereignisse untersuchen, aus denen die Sitzung besteht.
- Analysten können im Fenster „Abfrageverlauf“ Abfragen auswählen.

Arbeitsmethoden in der Ansicht „Ereignisse“ werden in gesonderten Themen beschrieben:

- Filtern und Durchsuchen von Ergebnissen in der Ansicht „Ereignisse“
- Managen von Spaltengruppen in der Ansicht „Ereignisse“
- Exportieren von Ereignissen in der Ansicht „Ereignisse“
- Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion
- Kombinieren von Ereignissen aus geteilten Sitzungen

Darüber hinaus können Sie diese Methoden der Abfrage von Daten und Reagieren auf Ergebnisse verwenden, die die Ansichten „Navigation“ und „Ereignisse“ gemeinsam haben.

- Suchen nach Textmustern
- Erstellen einer angepassten Abfrage
- Anzeigen und Ändern von Abfragen mithilfe von URL-Integration
- Einkapseln von benutzerdefinierten Ansichten mithilfe von Profilen
- Verwalten von Context-Hub-Listen und Listenwerten in den Ansichten „Navigation“ und „Ereignisse“
- Suchen von weiteren Kontexten in den Ansichten „Navigation“ und „Ereignisse“
- Rekonstruieren eines Ereignisses

Filtern und Durchsuchen von Ergebnissen in der Ansicht „Ereignisse“

Analysten können die Ergebnisse in der Ansicht „Ereignisse“ filtern und durch Suchen nach Ereignissen oder Auswahl des Service, zu dem Ereignisse angezeigt werden sollen, den Zeitbereich festlegen und Metadaten abfragen.

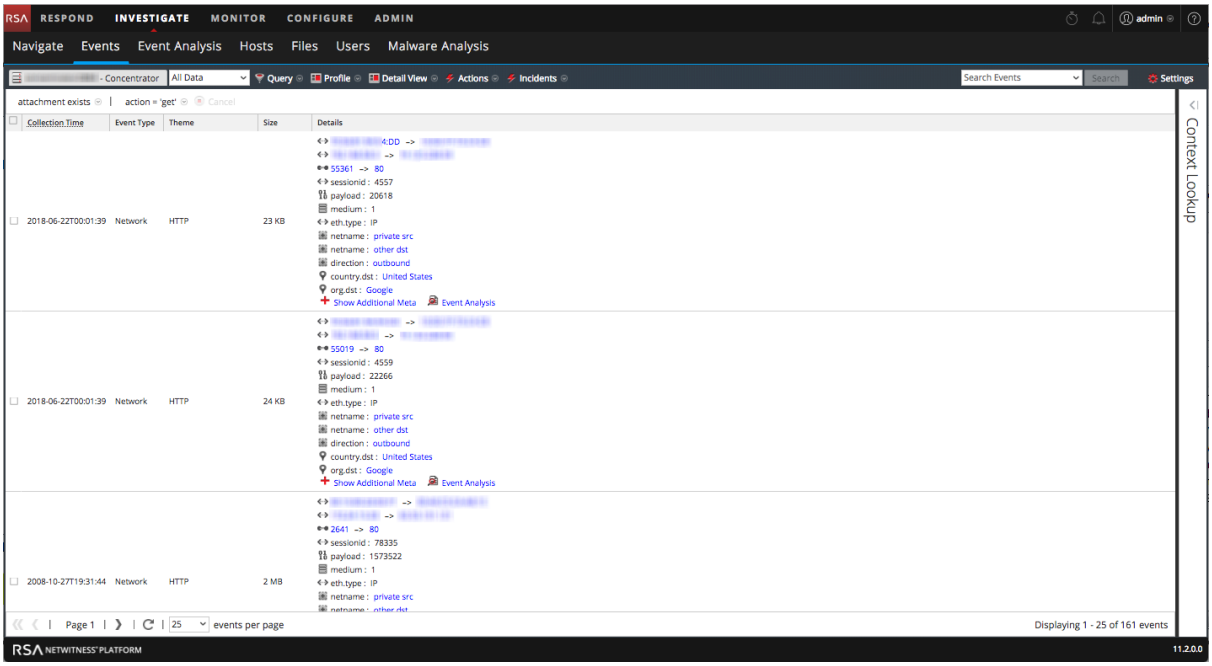
Wenn Sie die Ansicht „Ereignisse“ von einem Drill-down-Punkt der Ansicht „Navigation“ aus geöffnet haben, wird sie standardmäßig in der Ansicht „Ereignisdetails“ geöffnet. Analysten, die nicht über die Berechtigungen zum Verwenden der Ansicht Navigieren verfügen, können die Services direkt in der Ansicht Ereignisse abfragen. Es gibt mehrere Konfigurationsoptionen, um die in der Ansicht „Ereignisse“ angezeigten Informationen zu filtern.

Hinweis: Wenn in der Ansicht „Ereignisse“ als Service zurzeit ein Archiver ausgewählt ist und Sie einen Broker oder Concentrator durchsuchen, erfolgt der Suchvorgang langsamer als beim Durchführen einer Suche für einen Broker oder Concentrator, da die Daten auf dem Archiver komprimiert wurden und normalerweise mehr Daten vorhanden sind.

Filtern von Ereignissen in der Ansicht Ereignisse

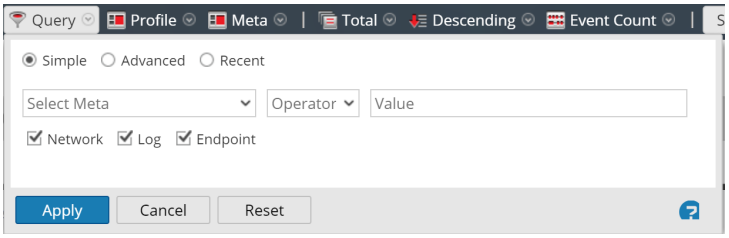
So filtern Sie die in der Ansicht „Ereignisse“ angezeigten Daten:

1. Navigieren Sie zu **UNTERSUCHEN** > **Ereignisse**.
   In der Ansicht „Ereignisse“ wird standardmäßig die Ansicht „Details“ anzeigt.

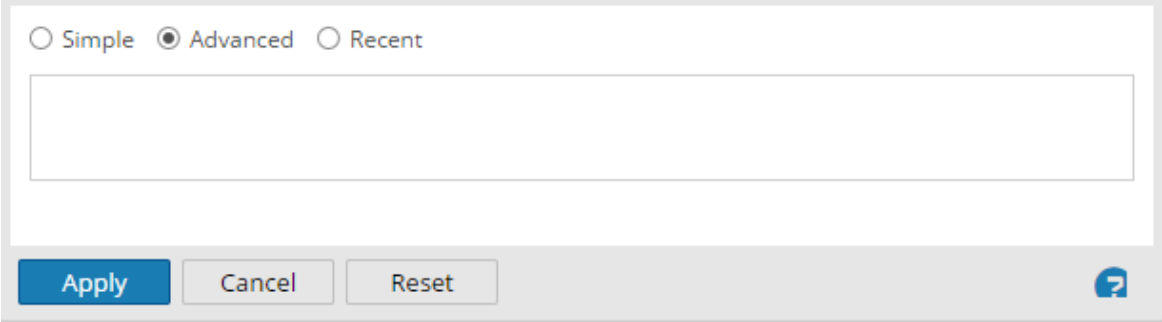


2. Wählen Sie einen anderen Zeitraum als den Standardzeitraum (**Letzte 3 Stunden**) aus, indem Sie auf der Symbolleiste in das Feld „Zeitraum“ klicken und einen Wert auswählen. Zum Beispiel **Letzte Stunde**.
   Die Ansicht „Ereignisse“ wird mit dem ausgewählten Zeitraum aktualisiert.

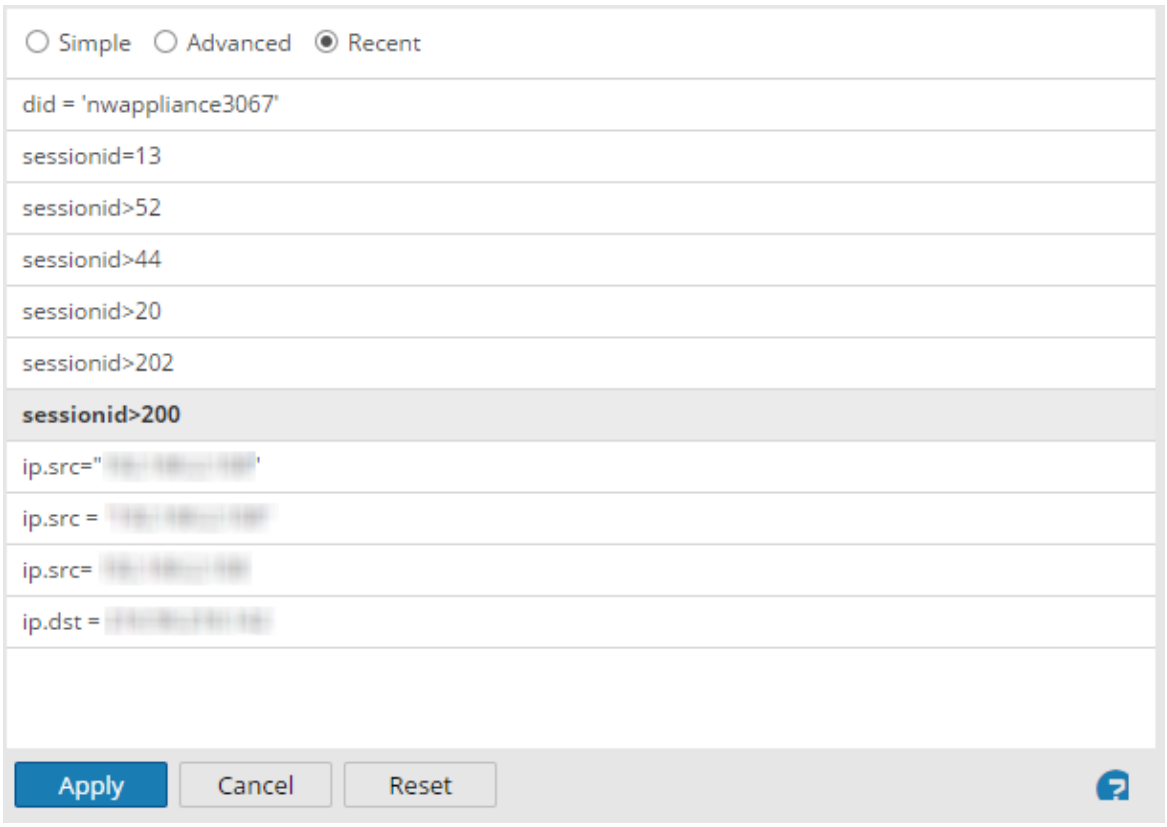
3. Klicken Sie zum Eingeben einer Abfrage für den ausgewählten Service und Zeitraum auf der Symbolleiste auf **Abfrage**.
   Das Dialogfeld „Abfrage“ wird mit ausgewählter Option „Einfach“ angezeigt.



4. Wenn Sie eine einfache Abfrage mit der AutoVervollständigen-Funktion eingeben möchten, um Metadaten und Operatoren auszuwählen, führen Sie einen der folgenden Schritte aus:
   a. Klicken Sie in das Feld **Metadaten auswählen** und wählen Sie in der Drop-down-Liste einen Metaschlüssel aus.
   b. Wählen Sie im Feld **Operator** in der Drop-down-Liste einen Operator aus.
   c. Geben Sie im Feld **Wert** einen entsprechenden Wert ein.
   d. Aktivieren Sie das Kontrollkästchen **Netzwerk**, **Protokoll** oder **Endpunkt** als zu verwendende Daten und klicken Sie auf **Anwenden**.
      Die entsprechenden Daten werden in der Ansicht „Ereignisse“ angezeigt.
5. Wenn Sie eine komplexere Abfrage basierend auf Ihren Kenntnissen über Metadaten und Operatoren eingeben möchten:
   a. Klicken Sie auf **Erweitert**.
      Das Dialogfeld „Abfrage“ wird mit ausgewählter Option „Erweitert“ angezeigt.



   b. Geben Sie eine Abfrage ein. Während der Eingabe, beginnend mit dem Metaschlüssel, werden Drop-down-Listen der verfügbaren Metaschlüssel und Operatoren eingeblendet. Klicken Sie abschließend auf **Anwenden**.
6. Wenn Sie eine Abfrage aus einer Liste aktueller Abfragen auswählen möchten:
   a. Wählen Sie **Aktuell** aus.
      Das Dialogfeld „Abfrage“ wird mit ausgewählter Option „Aktuell“ angezeigt.



b. Wählen Sie eine Abfrage aus und klicken Sie auf **Anwenden**.
Die übereinstimmenden Ergebnisse für die Abfrage werden in der Detailansicht der Ansicht „Ereignisse“ angezeigt. Die Brotkrümelnavigation spiegelt die Abfrage wider.

c. Sie können auf eines der Elemente der Brotkrümelnavigation klicken, um das Menü „Abfrage“ anzuzeigen. Sie können vor einem Breadcrumb-Element eine neue Abfrage einfügen und am Ende des Breadcrumbs eine neue Abfrage anfügen. Nach jeder Bearbeitung im Breadcrumb aktualisiert NetWitness Platform die Ergebnisse.

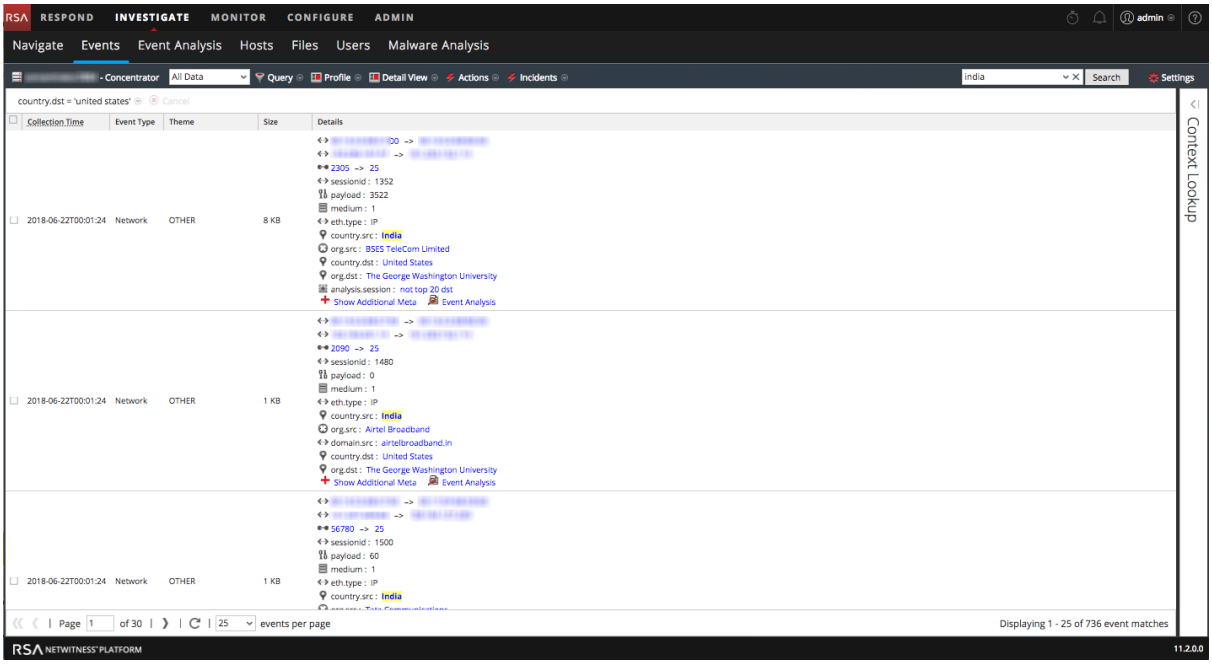
Suchen nach Ereignissen in der Ansicht „Ereignisse“

Sie können die aktuell in der Ansicht „Ereignisse“ angezeigten Daten durchsuchen, indem Sie im Feld „Suche“ eine Zeichenfolge zum Suchen eingeben. Bei der Zeichenfolge zum Suchen kann es sich um einen RegEx (regulären Ausdruck) oder eine einfache Textsuche handeln. Zu diesen Suchtypen sind detaillierte Informationen verfügbar.

So führen Sie eine Suche in den aktuell angezeigten Daten in der Ansicht „Ereignisse“ durch:

1. Führen Sie die Suche durch, indem Sie den Cursor im Feld „Suche“ platzieren, eine Zeichenfolge zum Suchen eingeben und die **Eingabetaste** drücken oder auf **Suche** klicken.
Die Suchergebnisse werden in der Ansicht „Ereignisse“ angezeigt. Ereignisse, die den Suchkriterien entsprechen, werden im Raster der Ansicht „Ereignisse“ angezeigt. In den Ansichten „Details“und „Liste“ sind die Übereinstimmungen in der Spalte „Details“ markiert. Beim Durchsuchen von RAW sind Übereinstimmungen darüber hinaus in der Protokollansicht in der Spalte „Protokolle“ markiert.

Im Folgenden ist ein Beispiel für die Suchergebnisse des Suchbegriffs **India** in der Ereignisdetailansicht angegeben. Bei Ereignisrekonstruktionen sind die Treffer der Suche nicht markiert.



2. Wenn Sie die Suche eingrenzen möchten, ändern Sie die Abfrage und die Uhrzeit, wie oben unter »Filtern von angezeigten Ereignissen in der Ansicht „Ereignisse“« beschrieben.
3. Wenn Sie die Suche beenden und zur Ansicht „Ereignisse“ zurückkehren möchten, klicken Sie auf **Abbrechen**.
   Alle angezeigten Ergebnisse bleiben erhalten.
4. Um den Eintrag im Suchfeld zu löschen und zur normalen Ansicht „Ereignisse“ zurückzukehren, klicken Sie im Suchfeld auf **X**.

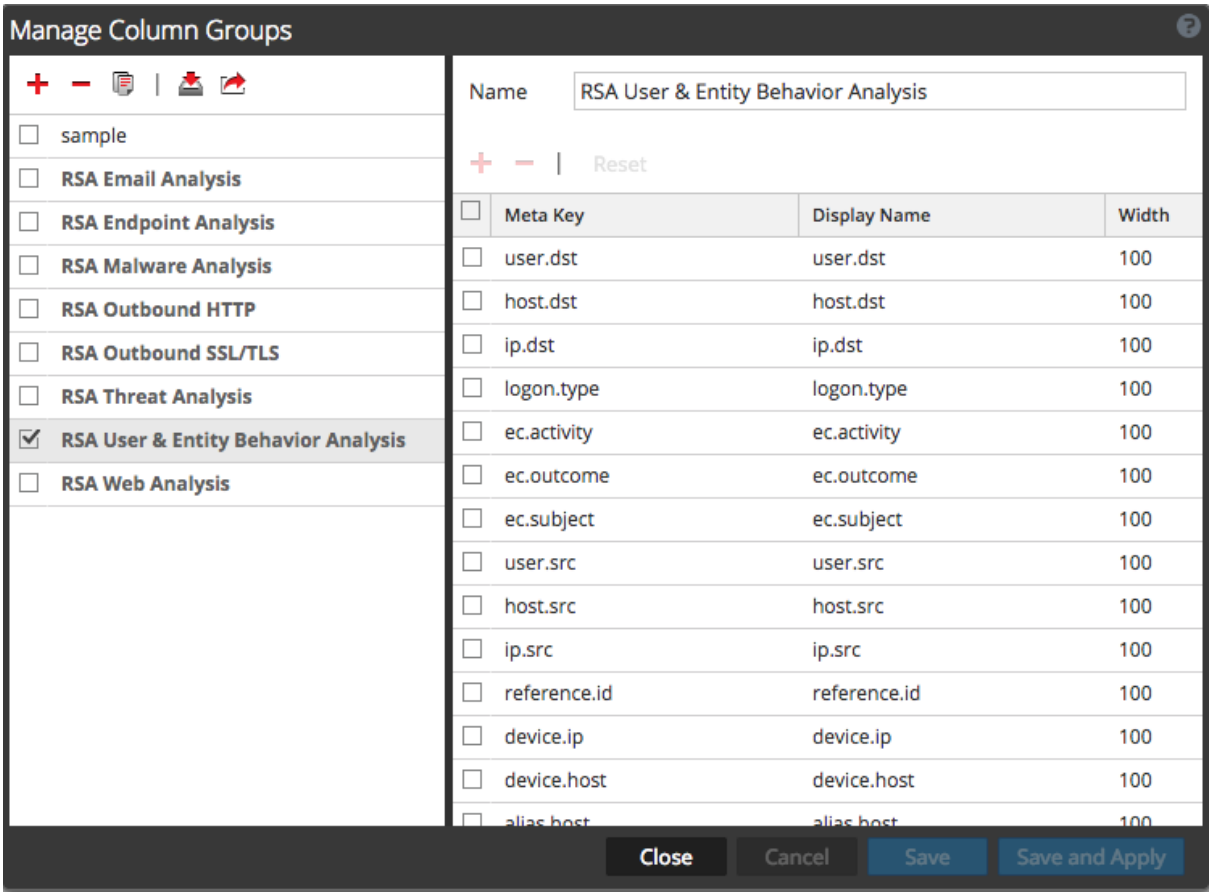
Managen von Spaltengruppen in der Ansicht „Ereignisse“

Wenn Sie eine Liste der Ereignisse in der Ansicht „Ereignisse“ anzeigen, können Sie die Art der Anzeige von Daten anpassen, indem Sie die in einer Spalte anzuzeigenden Metadaten, die Spaltenposition im Raster und die Standardspaltenbreite definieren.

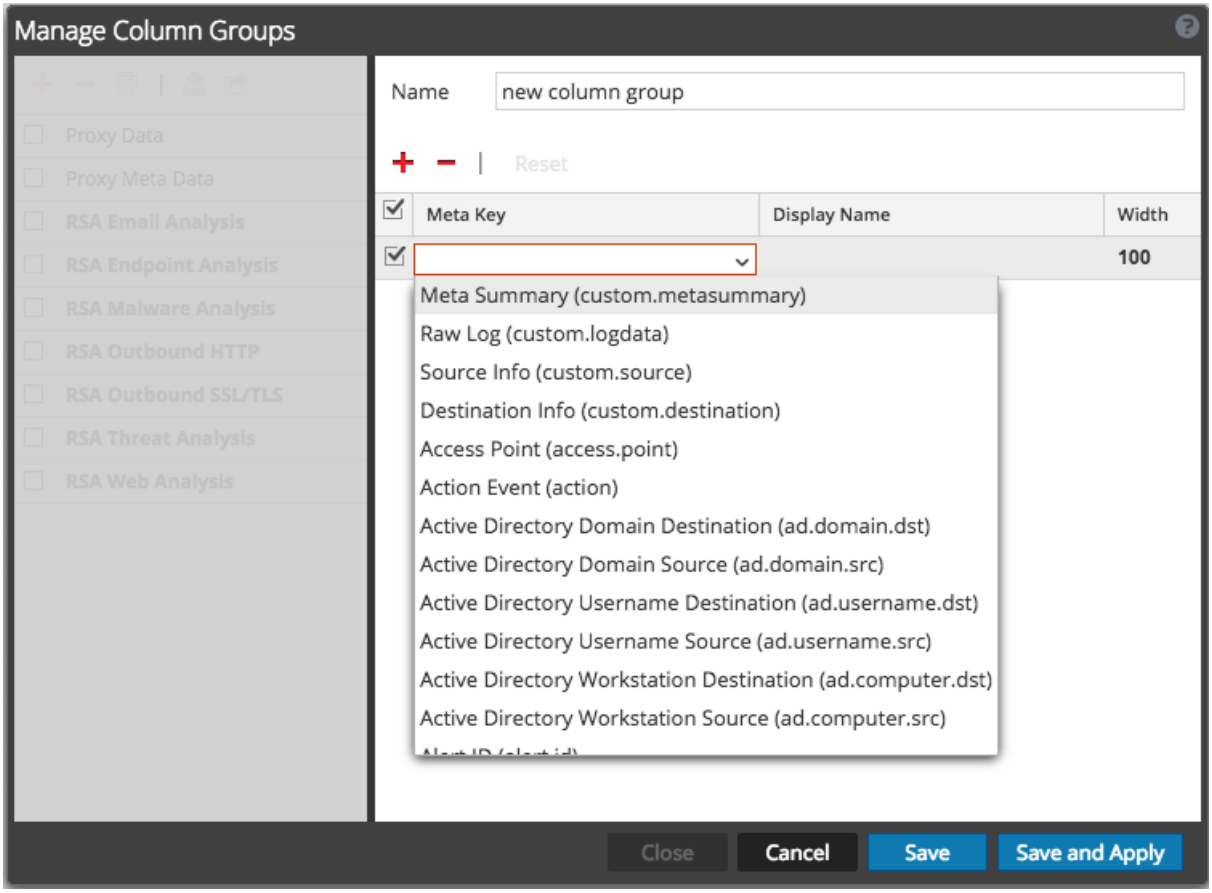
Hinweis: In Version 11.1 und höher können Sie bei Verwendung von Metaschlüsseln auch konfigurierte Metaeinheiten verwenden.
Ermittlungsprofile können auch benutzerdefinierte Spaltengruppen enthalten. Wenn eine benutzerdefinierte Spaltengruppe in einem Profil verwendet wird und Sie die Ereignisse in der Ereignisansicht mit einer benutzerdefinierten Spaltengruppe anzeigen, können Sie den Ansichtstyp (Details, Liste oder Protokoll) nicht ändern.

Erstellen von benutzerdefinierten Spaltengruppen

1. Navigieren Sie zu **NAVIGATION** > **Ereignisse**.
2. Wählen Sie **Spaltengruppen managen** im Drop-down-Menü **Ansicht**. Die Option „Anzeigen“ wird nach dem aktuellen Wert benannt, z. B. Detailansicht, Listenansicht, Protokollansicht, oder nach der aktuell ausgewählten Spaltengruppe.
   Das Dialogfeld „Spaltengruppen managen“ wird angezeigt.

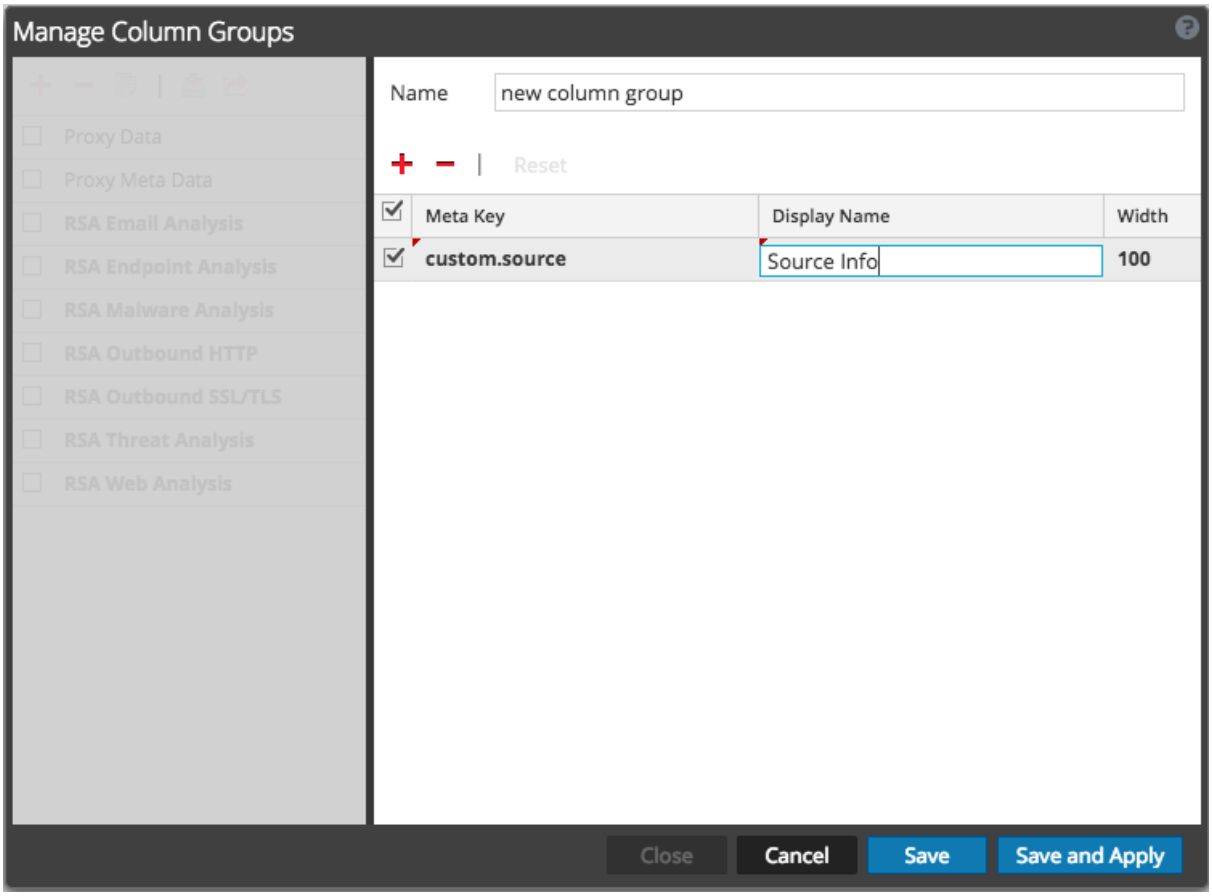


3. Klicken Sie zum Hinzufügen einer neuen Spaltengruppe im Bereich „Spaltengruppe“ auf + und geben Sie den Namen der Spaltengruppe im angezeigten Feld ein.
   Auf der rechten Seite wird der Bereich für die Spaltendefinition geöffnet, in dem der Gruppenname bereits ausgefüllt ist. Sie können den Gruppennamen bearbeiten.
4. Klicken Sie zum Hinzufügen einer Spalte zur Gruppe auf +. Klicken Sie dann im leeren Feld **Metaschlüssel**, um die Drop-down-Liste **Metaschlüssel** anzuzeigen. Wählen Sie ein Metadatenschlüsselfeld aus der Liste aus und wiederholen Sie diesen Schritt so lange, bis die Spalte vollständig ist.



5. (Optional) Klicken Sie zum Löschen eines Metadatenschlüssels aus der Spaltengruppe auf −.
6. (Optional) Wenn Sie die Reihenfolge ändern möchten, in der die Spalten in der Ereignisliste angezeigt werden, ziehen Sie die Metadatenschlüssel an die gewünschte Position.

7. (Optional) Klicken Sie zum Einrichten der Standardbreite für eine Spalte auf den entsprechenden Wert in der Spalte **Breite** und geben Sie eine neue Spaltenbreite ein.

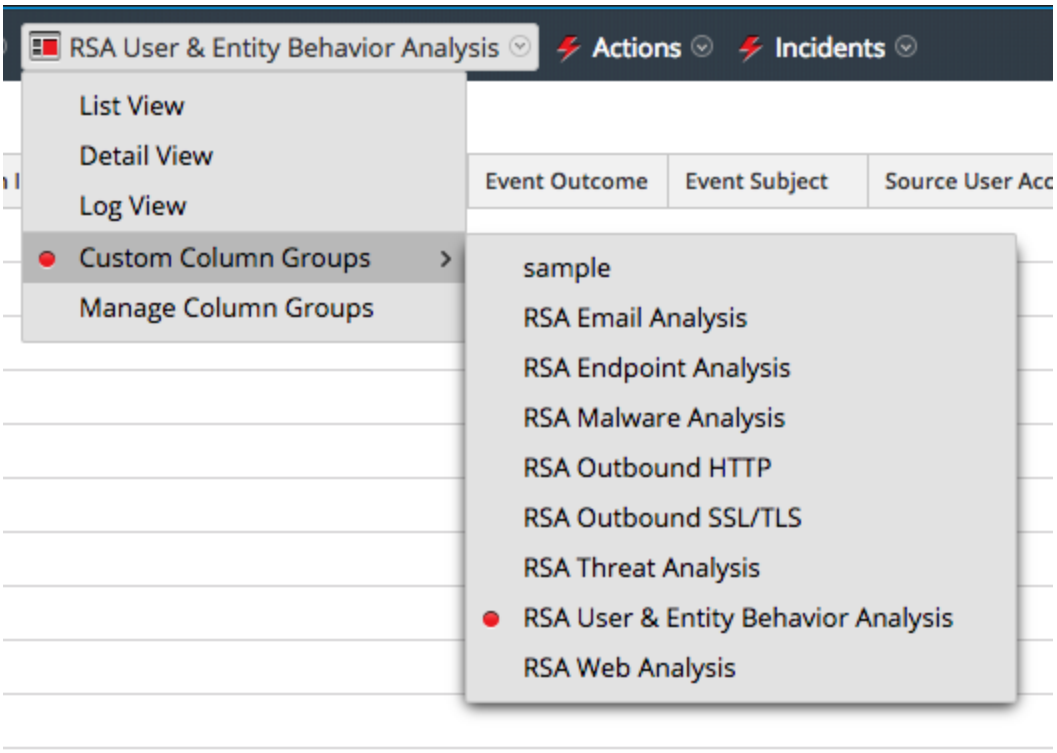


8. (Optional) Klicken Sie auf **Zurücksetzen**, um die vorherigen Spalteneinstellungen wiederherzustellen und alle Änderungen rückgängig zu machen.
9. Führen Sie zum Speichern einen der folgenden Schritte durch:
   a. Klicken Sie zum Speichern der bearbeiteten Spaltengruppe und zum Aktualisieren der Ereignisansicht in den Spaltengruppeneinstellungen auf **Speichern und übernehmen**.
   b. Klicken Sie zum Speichern der bearbeiteten Spaltengruppe ohne Aktualisierung der Ereignisansicht auf **Speichern**.

Auswählen einer Spaltengruppe

So wählen Sie eine Spaltengruppe aus:

1. Wählen Sie bei geöffneter Ereignisansicht **Benutzerdefinierte Spaltengruppen** im Drop-down-Menü **Ansicht**. Der Optionsname ist der Standardwert (Detailansicht oder der aktuelle Wert).



2. Wählen Sie eine der Spaltengruppen aus dem Untermenü aus.
   Die Ereignisansicht wird aktualisiert und zeigt die benutzerdefinierte Spaltengruppe an.

Exportieren von Ereignissen in der Ansicht „Ereignisse“

In der Ansicht „Ereignisse“ umfasst das Menü „Aktionen“ eine Option, um Ereignisse aus dem aktuell angezeigten Ereignis in ein Archiv zu exportieren.

Hinweis: Sie können nur Dateien exportieren, für die Sie über Lese- oder Zugriffsberechtigung verfügen.

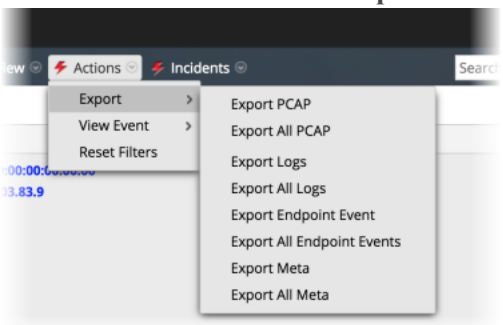
Bei der Exportfunktion wird der Service auf alle Sitzungen für den ausgewählten Zeitbereich und Drill-down-Punkt abgefragt, um die Inhalte jeder Sitzung zu extrahieren. Die zu exportierenden Detailinformationen werden sowohl durch den Zeitbereich als auch durch den Drill-down-Punkt zum Zeitpunkt des Exports beeinflusst. Im Dialogfeld „Dateiextraktion“ können Sie Folgendes für den Export auswählen:

- PCAPs
- Protokolle
- NetWitness Endpoint-Ereignis
- Metawerte

das Format des exportierten Archivs: ZIP- oder GZIP-Datei Wenn Sie eine Anforderung gesendet haben, wird ein Job geplant und Sie können den Job in der Jobkurzübersicht nachverfolgen Wenn beim Abrufen des Protokolls oder PCAP auf dem Service ein Fehler auftritt, zeigt NetWitness Platform eine Fehlerbenachrichtigung an.

So extrahieren Sie Dateien aus einem Ereignis:

1. Klicken Sie in der**Ereignisansicht** auf ein Ereignis.
2. Klicken Sie auf **Aktionen** > **Exportieren**.



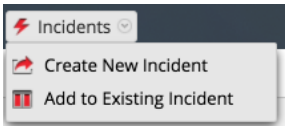
3. Wählen Sie die Exportoption und das Dateiformat aus.
   In einer Meldung werden Sie informiert, dass ausgewählte Daten heruntergeladen werden.

Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion

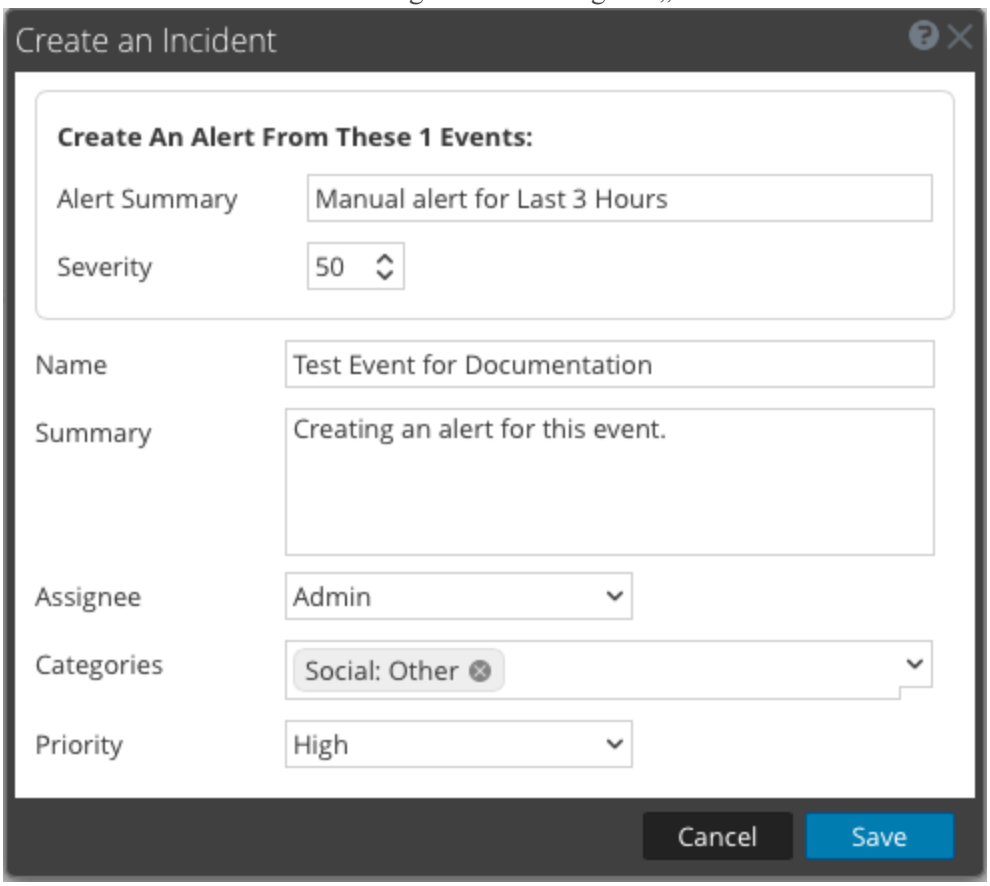
Bei der Durchführung von Ermittlungen in der Ansicht „Ereignisse“ können Sie ein oder mehrere Ereignisse auswählen und einen Incident erstellen, der für Incident Responders in Respond verfügbar ist. Sie können Ereignisse auch zu einem vorhandenen Incident in Respond hinzufügen, auf den Sie Zugriff haben.

Hinweis: Ein Administrator muss die erforderlichen Rollen und Berechtigungen konfigurieren, wie in „Rollenberechtigungen“ und „Managen von Benutzern mit Rollen und Berechtigungen“ im *Handbuch Systemsicherheit und Benutzerverwaltung* beschrieben ist.

1. Navigieren Sie zu **UNTERSUCHEN** > **Ereignisse**.
2. Wählen Sie in der Ansicht „Ereignisse“ ein oder mehrere Ereignisse aus und wählen Sie dann **Incidents** > **Neuen Incident erstellen**.



3. Machen Sie die erforderlichen Angaben im Dialogfeld „Incident erstellen“.



a. Wählen Sie den Schweregrad, eine Ganzzahl zwischen 1 und 100, wobei 100 der höchste Schweregrad ist.

b. Geben Sie einen Namen für den Incident ein und beschreiben Sie den Incident im Feld **Übersicht**.

c. Wählen Sie einen Zuweisungsempfänger für den Incident aus der Drop-down-Liste aus. Diese Liste enthält die integrierten Rollen, die Zugriff auf Respond haben, sowie die benutzerdefinierten Rollen, die dem System hinzugefügt wurden. Diese Liste kann z. B. Rollen für Administrator, Analyst, DPO, Anwender und Rollen für Incident Responders enthalten.

d. Wählen Sie in der Drop-down-Liste **Kategorien** eine oder mehrere Kategorien von Warnmeldungen, die für diesen Incident gelten.

e. Wählen Sie in der Drop-down-Liste **Prioritäten** eine Kategorie für den Incident aus. Ein Incident kann beispielsweise kritische, hohe, mittlere oder niedrige Priorität haben.

f. Klicken Sie auf **Speichern**.
Der neue Incident wird erstellt und steht sofort in der Incident-Warteschlange für die ausgewählte Rolle in Respond zur Verfügung.

4. Um ein oder mehrere Ereignisse zu einem Incident hinzuzufügen, wählen Sie ein oder mehrere Ereignisse und dann **Incidents > Zu vorhandenem Incident hinzufügen** aus.

5. Wählen Sie im Dialogfeld „Ereignisse zu einem Incident hinzufügen“ den Schweregrad und wählen Sie einen oder mehrere Incidents, zu denen die Ereignisse hinzugefügt werden. Sie können über die Incident-ID oder den Incident-Namen nach einem vorhandenen Incident suchen. Wenn Sie fertig sind, klicken Sie auf **Einem Incident hinzufügen**.
Die Ereignisse werden den ausgewählten Incidents hinzugefügt und in Respond aktualisiert.

Kombinieren von Ereignissen aus geteilten Sitzungen

Analysten können Sitzungen identifizieren, die aufgrund der Sitzungsgröße in der Ansicht „Ereignisse“ geteilt wurden, und sie können die fragmentierten Sitzungen so kombinieren, dass die gesamte Sitzung als ein einziges Abfrageergebnis in der Ansicht „Ereignisse“ dargestellt werden kann. Wenn geteilte Sitzungen wieder zusammengefügt werden, enthält ein einziger Paketexport der Sitzung in der Ansicht Ereignisse alle Fragmente der Sitzung.

Version 10.4 und frühere Decoders werden mit einer Standardsitzungsgröße von 32 MB konfiguriert. Wenn eine Sitzung die 32-MB-Grenze überschreitet, teilt der Decoder die Sitzung und alle folgenden Pakete werden Teil einer neuen Sitzung, wodurch die tatsächliche Netzwerksitzung in mehrere Decoder-Sitzungen fragmentiert wird. Geteilte Sitzungen werden ohne den Kontext analysiert, dass es sich um ein Fragment einer größeren Netzwerksitzung handelt. Dies führt manchmal zu Sitzungsfragmenten mit vertauschten Quell- und Zieladressen und -ports und nicht identifizierten Anwendungsprotokollen. Ein weiteres Ergebnis geteilter Sitzungen können Probleme beim Anzeigen aller Sitzungsfragmente als ein einziges Abfrageergebnis oder beim Erstellen eines einzigen Paketexports aller Sitzungsfragmente sein.

Durch Decoder-Verbesserungen in NetWitness Platform 10.5 wurde die Verarbeitung fragmentierter Sitzungen optimiert:

- Kontextuelle Fragmentanalyse
- Hervorhebung von Sitzungsfragmenten
- Suchen von Sitzungsfragmenten
- Exportieren aller Pakete in eine einzige PCAP-Datei

Kontextuelle Fragmentanalyse

Der Decoder beendet die Sitzungsanalyse vor dem Teilen der Sitzung basierend auf der konfigurierten maximalen Sitzungsgröße (32 MB) oder dem konfigurierten Timeout (60 Sekunden). Nach Abschluss der Analyse enthalten die Analyseergebnisse die korrekte Adressrichtung und das korrekte Anwendungsprotokoll, die für jedes folgende Sitzungsfragment übernommen werden, um die Konsistenz mit der logischen Netzwerksitzung, die sie repräsentieren, zu wahren.

Hinweis: Alle erforderlichen Decoder-Konfigurationsänderungen werden beim Upgrade auf 10.5 vorgenommen. Für die Funktion „Sitzungsfragmente finden“ ist es jedoch erforderlich, dass die TCP- und die UDP-Quellport-Metadaten (tcp.srcport und udp.srcport) vollständig indexiert sind. Dies entspricht nicht der Standardkonfiguration vor Version 10.5. Dies limitiert die Möglichkeit zur Suche nach Fragmenten funktional auf Sitzungen, die nach dem Upgrade des Decoder auf die Version 10.5 erfasst wurden.

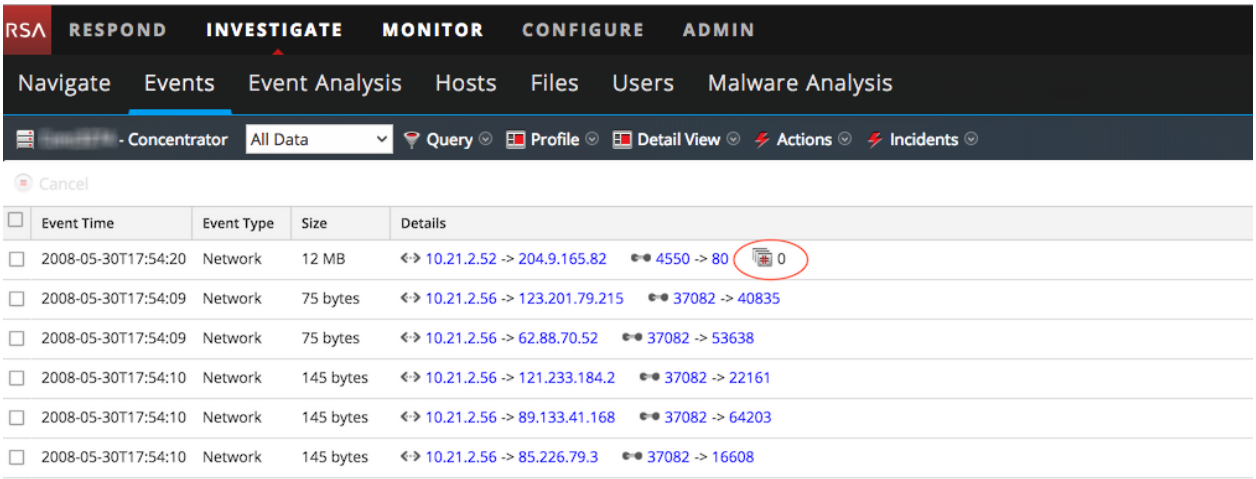
Hervorhebung von Sitzungsfragmenten

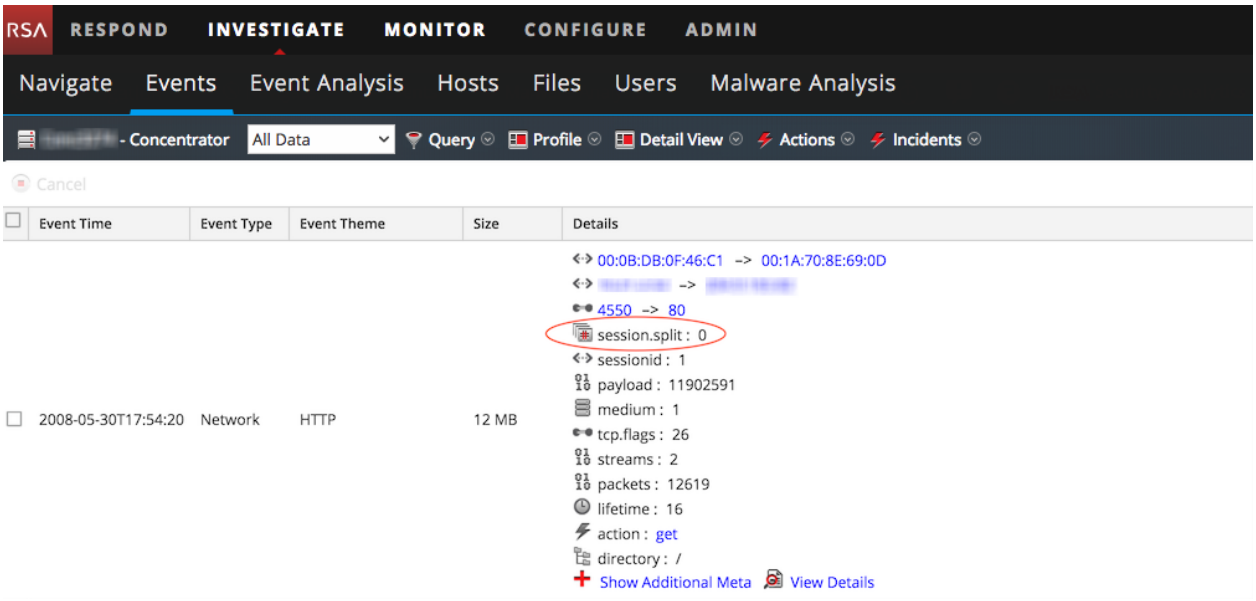
Jedes Sitzungsfragment verfügt über zusätzliche Metadatenelemente: `session.split`. Der Wert des `session.split`-Metadatenelements eines bestimmten Sitzungsfragments gibt an, wie viele Fragmente vor diesem Fragment existieren. Beim Anzeigen einer Sitzung in der Ansicht „Ereignisse“ identifizieren die `session.split`-Metadatenelemente Sitzungen, bei denen es sich um Fragmente in den Ansichten „Ereignisliste“ und „Ereignisdetails“ handelt.

Die Teilung der Sitzung erfolgt, wenn der konfigurierte Decoder `assembler.size.max` oder `assembler.timeout.session` (Latenz zwischen Sitzungen) erreicht ist. Das erste Fragment ist Sitzung 0 und Sitzungen mit einem späteren Zeitstempel werden schrittweise mit 1, 2, 3 usw. nummeriert. Die `session.split`-Metadaten zeigen die Anzahl der vorhergehenden Sitzungsfragmente an. Dennoch ist dies nicht immer ein Hinweis darauf, dass auch folgende Fragmente vorhanden sind, auch bei einem Wert von 0. Es ist auch möglich, dass für das erste Fragment einer Sitzung keine `session.split`-Metadatenelemente existieren, wenn die Sitzung analysiert wurde, bevor die maximale Sitzungsgröße überschritten wurde.

Wenn Sie die Sitzungsfragmente anzeigen, können Sie die erforderliche maximale Sitzungsgröße und den erforderlichen Sitzungs-Timeout bestimmen, die für die Analyse für das Zusammensetzen der Sitzungen erforderlich sind. Beispiel: Wenn vier Fragmente mit 32 MB vorliegen, müssen Sie den Test-Decoder (normalerweise eine virtuelle Maschine, die getrennt vom Hauptproduktionsservice erstellt wurde) mit einer maximalen Sitzungsgröße von mehr als 128 MB konfigurieren. Die Schritte zur Suche nach allen Fragmenten basierend auf dem Sitzungs-Timeout sind identisch. Die Abbildungen unten zeigen die Ansichten „Ereignisliste“ und „Ereignisdetails“ an, bei denen die fragmentierten Sitzungsinformationen hervorgehoben sind.

Hinweis: Bei der Erstellung der Screenshots unten war eine maximale Sitzungsgröße von 12 MB konfiguriert.





Die `session.split`-Metadaten werden in der Detailansicht immer direkt hinter den Adress- und Portmetadaten angezeigt. Sie sind nie als zusätzliche Metadaten ausgeblendet. Diese Verbesserungen ermöglichen ein schnelles:

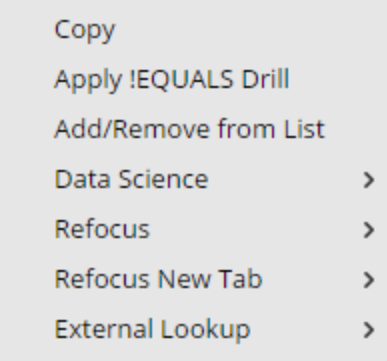
- Identifizieren von Sitzungen, die Fragmente einer Netzwerksitzung sind.
- Anzeigen aller Sitzungsfragmente einer bestimmten Netzwerksitzung oder eines einzigen Sitzungsfragments.
- Exportieren der Pakete für die gesamte Netzwerksitzung als eine einzige PCAP-Datei.

Suchen und Kombinieren von Fragmenten

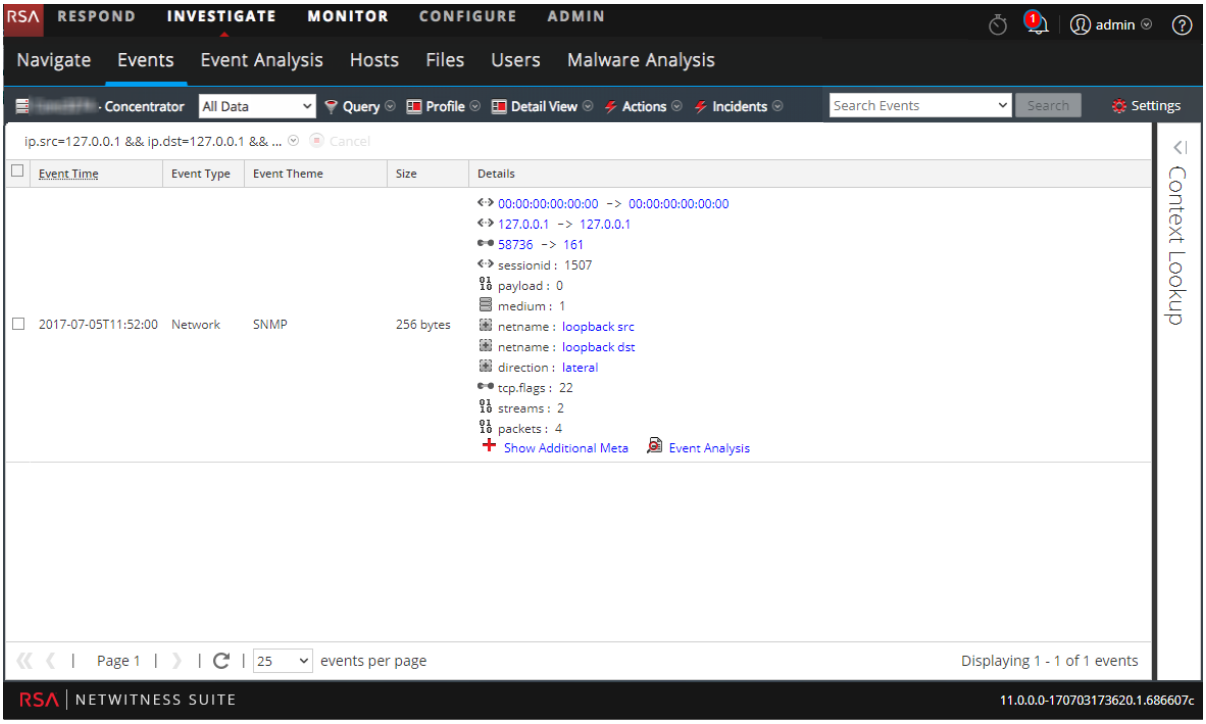
Innerhalb der Ansicht „Ereignisse“ können Sie nach Sitzungsfragmenten suchen, indem Sie die Kontextmenüoptionen „Neu fokussieren > Sitzungsfragmente finden“ verwenden. NetWitness Platform erstellt mithilfe der Quell- und Zieladressen und -ports der ausgewählten Sitzung eine Abfrage und zeigt alle Sitzungen im aktuellen Zeitfenster an, die der Abfrage entsprechen.

So suchen Sie Sitzungsfragmente:

1. Klicken Sie in der Ansicht **Ereignisse** mit der rechten Maustaste auf einen der Werte für Quell- und Zieladressen und -ports: `ip.src`, `ip.dst`, `ipv6.src`, `ipv6.dst`, `tcp.srcport`, `tcp.dstport`, `udp.srcport` und `udp.dstport`) sowie `session.split`-Werte.
   Das Kontextmenü wird angezeigt.



2. Wählen Sie **Neu fokussieren > Sitzungsfragmente finden** oder **Neue Registerkarte neu fokussieren > Sitzungsfragmente suchen** aus.
   NetWitness Platform füllt die Ereignisliste neu mit Sitzungsfragmenten für eine einzige Sitzung innerhalb des aktuellen Zeitraums aus. Je nach ausgewählter Option ersetzt die Neufokussierung die aktuelle Ansicht oder es wird eine neue Registerkarte geöffnet. (In diesen Beispielen werden alle Daten verwendet, aber auf Produktionssystemen wird dies nicht empfohlen).



3. Passen Sie, sofern erforderlich, den Zeitraum an, um alle Sitzungsfragmente einzuschließen, die vor oder hinter dem aktuellen Zeitfenster liegen. Dass der Zeitraum erweitert werden muss, erkennen Sie daran, dass Fragmente an den Grenzen des Zeitraums vorhanden sind, besonders dann, wenn das erste sichtbare Fragment nicht den Teilungswert 0 (oder keinen) hat. Alternativ können Sie durch Betrachten der Pakete der letzten sichtbaren Sitzung feststellen, dass die Sitzung vermutlich weiter geht. Hier ein Beispiel:

a. Wenn Sie Fragmente betrachten, die offensichtlich nicht das erste Fragment sind, z. B. 1, 2, 3 und 4 im Zeitraum 10:30 bis 10:35, dann muss ein Fragment 0 vorhanden sein. Sie können den Zeitraum erweitern, sodass er früher beginnt (hier 10:25), um das zusätzliche Fragment zu finden.

b. Wenn die Sitzungsgröße des letzten Fragments nahe der maximalen Sitzungsgröße ist (hier 12 MB), suchen Sie nach weiteren Fragmenten, indem Sie das Zeitfenster auf einen späteren Zeitpunkt erweitern (hier 10:40).
Wenn alle Sitzungsfragmente einer Netzwerksitzung in einer einzigen Ereignisliste enthalten sind, kann die Liste mehrere Seiten lang sein.

4. (Optional) Wählen Sie zum Exportieren der Pakete jedes Sitzungsfragments in eine einzige PCAP-Datei **Aktionen > Alle PCAP exportieren** aus.
In einer Meldung werden Sie informiert, dass PCAP heruntergeladen wird. Wenn der Download abgeschlossen ist, enthält die PCAP-Datei die gesamte Netzwerksitzung, die fragmentiert wurde.

Abfragen von und Reagieren auf Daten in den Ansichten „Navigation“ und „Ereignisse“

In diesem Thema werden Methoden der Abfrage von Daten und der Reaktion auf Ergebnisse beschrieben, die die Ansichten „Navigation“ und „Ereignisse“ gemeinsam haben. Analysten können:

- Suchen nach Textmustern
- Erstellen einer angepassten Abfrage
- Anzeigen und Ändern von Abfragen mithilfe von URL-Integration
- Einkapseln von benutzerdefinierten Ansichten mithilfe von Profilen
- Verwalten von Context-Hub-Listen und Listenwerten in den Ansichten „Navigation“ und „Ereignisse“
- Suchen von weiteren Kontexten in den Ansichten „Navigation“ und „Ereignisse“
- Rekonstruieren eines Ereignisses

Erstellen einer angepassten Abfrage

Sie können in der Ansicht „Untersuchen > Navigation“ oder „Ereignisse“ eine Abfrage erstellen, anstatt sich durch die Metaschlüssel und Werte zu klicken, um einen Drill-down in die Metadaten auszuführen. Die Dialogfelder zum Erstellen einer Abfrage bieten Syntaxhilfe mit Drop-down-Listen der anwendbaren Metaschlüssel und Operanden. Wenn Sie die Drop-down-Liste anzeigen, können Sie alle Metagruppen erweitern und reduzieren, um die einzelnen Metaschlüssel in der Gruppe anzuzeigen oder diese auszublenden.

Hinweis: In Version 11.1 und höher können Sie Metaentitäten sowie Metaschlüssel abfragen.

Wenn Sie eine Metagruppe ausgewählt haben, erzeugt NetWitness Platform eine komplexe Abfrage, die einer Abfrage entspricht, bei der alle Metaschlüssel in dieser Gruppe mit „OR“ verknüpft werden. Wenn eine Metagruppe also `ip.src` und `ip.dst` enthält, wäre die generierte Abfrage `ip.src = <value> OR ip.dst = <value>`. Wenn eine Metagruppe Metaschlüssel mit unterschiedlichen Typen von Metawerten enthält, wird die Werteingabe deaktiviert und die Abfrage verwendet `exists`-Anweisungen. Eine Metagruppe, die zum Beispiel `ip.src`, `ip.dst` und `alias.host` enthält, umfasst Metaschlüssel, die unterschiedliche Typen von Werten haben; `ip.src` und `ip.dst` sind IP-Adressen und `alias.host` ist Text. Die generierte Abfrage lautet `ip.src exists OR ip.dst exists OR alias.host exists`.

Eine Basisabfrage hat folgende Form:

```
<metakey> <operator> [<metavalue>]
```

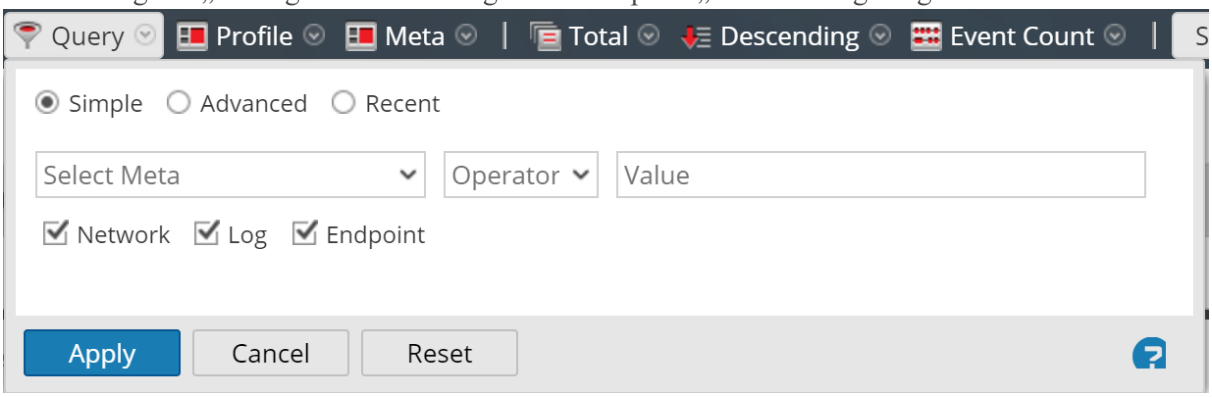
Es folgen einige Beispiele:

```
action exists
action = 'get'
alias.host = '10.25.55.115'
extension = 'exe'
orig_ip != "10.0.0.0" - "10.255.255.255"
```

Erstellen einer Abfrage mithilfe der Basismethode

Wenn Sie mithilfe der Basismethode eine Abfrage erstellen, liefert NetWitness Platform Drop-down-Listen von Metadaten und Operatoren.

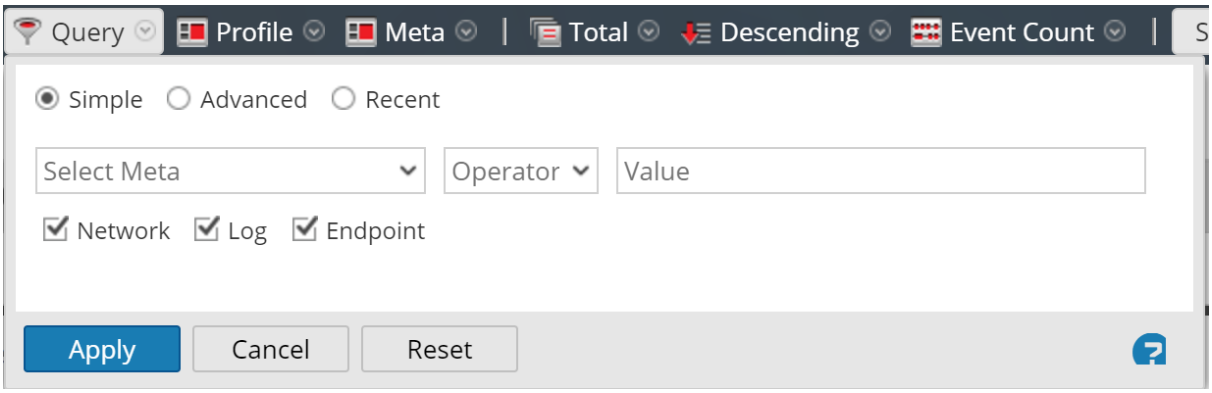
1. Wählen Sie in der Symbolleiste der Ansicht **Navigation** oder der Ansicht **Ereignisse** die Option **Abfrage** aus.
   Das Dialogfeld „Abfrage“ wird mit ausgewählter Option „Einfach“ angezeigt.



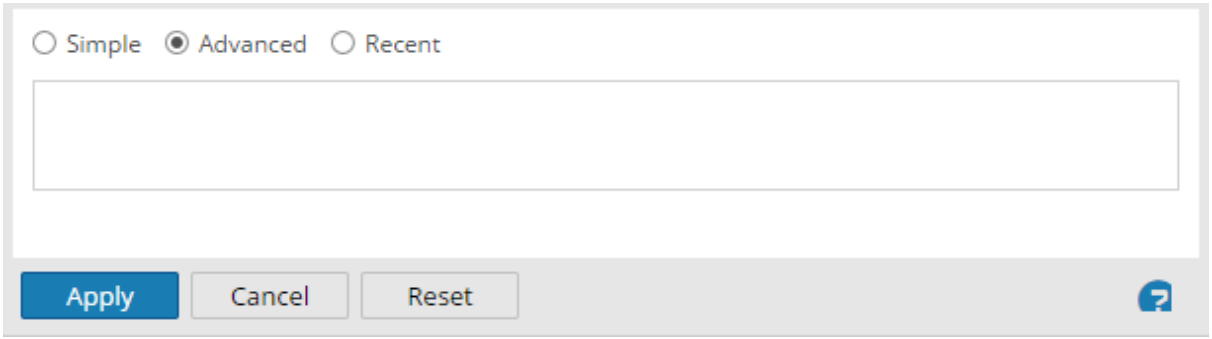
2. Klicken Sie in das Feld **Metadaten auswählen**, um die Drop-down-Liste anzuzeigen. Die Drop-down-Liste besteht aus zwei Abschnitten: Metagruppen und Alle Metadaten.
3. Wählen Sie einen einzigen Metaschlüssel unter **Alle Metadaten** aus oder wählen Sie eine Metagruppe unter **Metagruppen** aus. Sie können auch einen Metaschlüssel oder eine Metagruppe in das Feld eingeben.
4. Geben Sie in das Feld **Operand** einen Operanden ein oder klicken Sie auf die Drop-down-Liste, um einen gültigen Operanden auszuwählen.
5. (Optional) Wenn Sie einen Operator auswählen, der einen Wert erfordert, zum Beispiel „BEGIN“, geben Sie im dritten Feld den Wert für den Metaschlüssel ein.
6. Wählen Sie in den Kontrollkästchen „Netzwerk“, „Protokoll“ und „Endpunkt“ den Datentyp zur Abfrage aus. Führen Sie einen der folgenden Schritte aus:
   a. Begrenzen Sie die Abfrage auf Pakete, indem Sie **Netzwerk** auswählen und **Protokoll** und **Endpunkt** deaktivieren.
   b. Begrenzen Sie die Abfrage auf Protokolle, indem Sie **Protokoll** auswählen und **Netzwerk** und **Endpunkt** deaktivieren.
   c. Begrenzen Sie die Abfrage auf Endpunktereignisse, indem Sie **Endpunkt** auswählen und **Netzwerk** und **Protokoll** deaktivieren.
   d. Wenden Sie die Abfrage auf Pakete, Protokolle und Endpunkte an, indem Sie **Netzwerk**, **Protokoll** und **Endpunkt** auswählen.
7. Führen Sie einen der folgenden Schritte aus:
   a. Klicken Sie auf **Anwenden**.
      Das Fenster wird geschlossen und die Ansicht wird mit den Ergebnissen der neuen Abfrage aktualisiert. Die Abfrage wird im Breadcrumb angezeigt.
   b. Klicken Sie auf **Abbrechen**.
      Das Fenster wird geschlossen und es werden keine Änderungen an der Ansicht oder aktuellen Abfrage vorgenommen.

Erstellen einer Abfrage mithilfe der erweiterten Methode

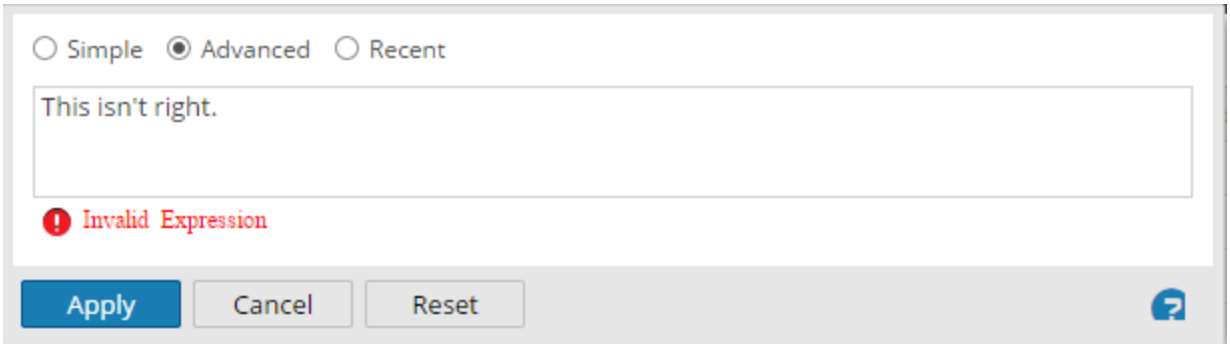
1. Wählen Sie in der Symbolleiste der **Ansicht „Navigation“** oder der Ansicht „Ereignisse“ die Option **Abfrage** aus.
   Das Dialogfeld „Abfrage“ wird angezeigt.



2. Wählen Sie die Option **Erweitert** aus.
   Das Feld „Erweiterte Abfrage“ wird angezeigt.



3. Erstellen Sie in dem Feld eine Abfrage, welche den Metaschlüssel, den Operator und den Wert enthalten kann. Wenn Sie mit dem Eingeben eines Metaschlüssels in das Feld beginnen, wird eine Drop-down-Liste mit den verfügbaren Metaschlüsseln für den ausgewählten Service angezeigt.
4. Wählen Sie den Metaschlüssel für Ihre Abfrage aus.
   Die Anzeige wird aktualisiert. Wenn der Ausdruck noch nicht abgeschlossen ist, gibt der Status an, dass die Abfrage ungültig ist.
5. Fahren Sie mit einem Operanden aus der Drop-down-Liste fort und dann, falls erforderlich, mit einem Wert. Die Anzeige wird aktualisiert, wenn Sie mit der Eingabe der Abfrage fortfahren. Wenn Sie einen Operator wie **exists** oder **!exists** eingeben, der das Feld „Werte“ nicht verwendet, wird das Feld „Werte“ deaktiviert und der Status „ungültig“ aufgehoben. Wenn Sie einen Operanden wie = eingeben, bei dem das Feld Werte erforderlich ist, bleibt der Status „ungültig“ so lange erhalten, bis Sie einen Wert eingeben. Wenn die Abfrage gültig ist, wird der Status „ungültig“ nicht länger angezeigt.

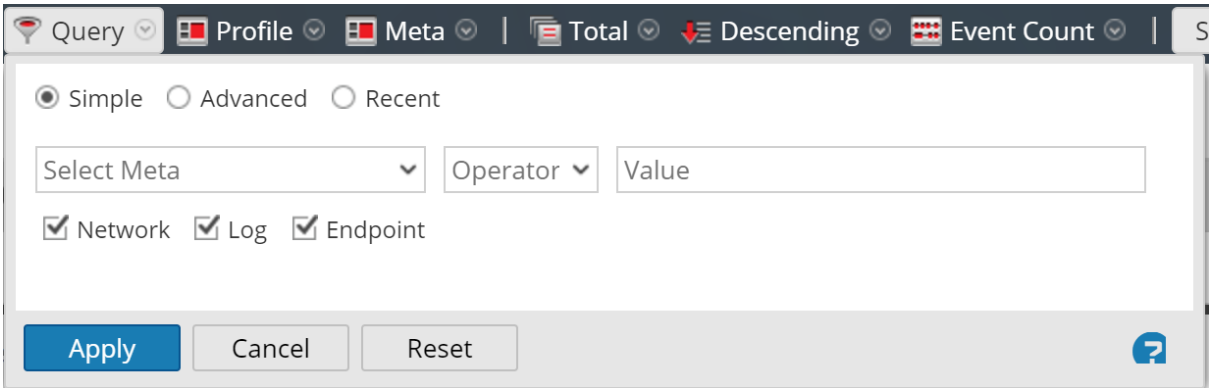


6. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Anwenden**.
     Das Fenster wird geschlossen und die Ansicht wird mit den Ergebnissen der neuen Abfrage aktualisiert. Die Abfrage wird im Breadcrumb angezeigt.
   - Klicken Sie auf **Abbrechen**.
     Das Fenster wird geschlossen und es werden keine Änderungen an der Ansicht oder aktuellen Abfrage vorgenommen.

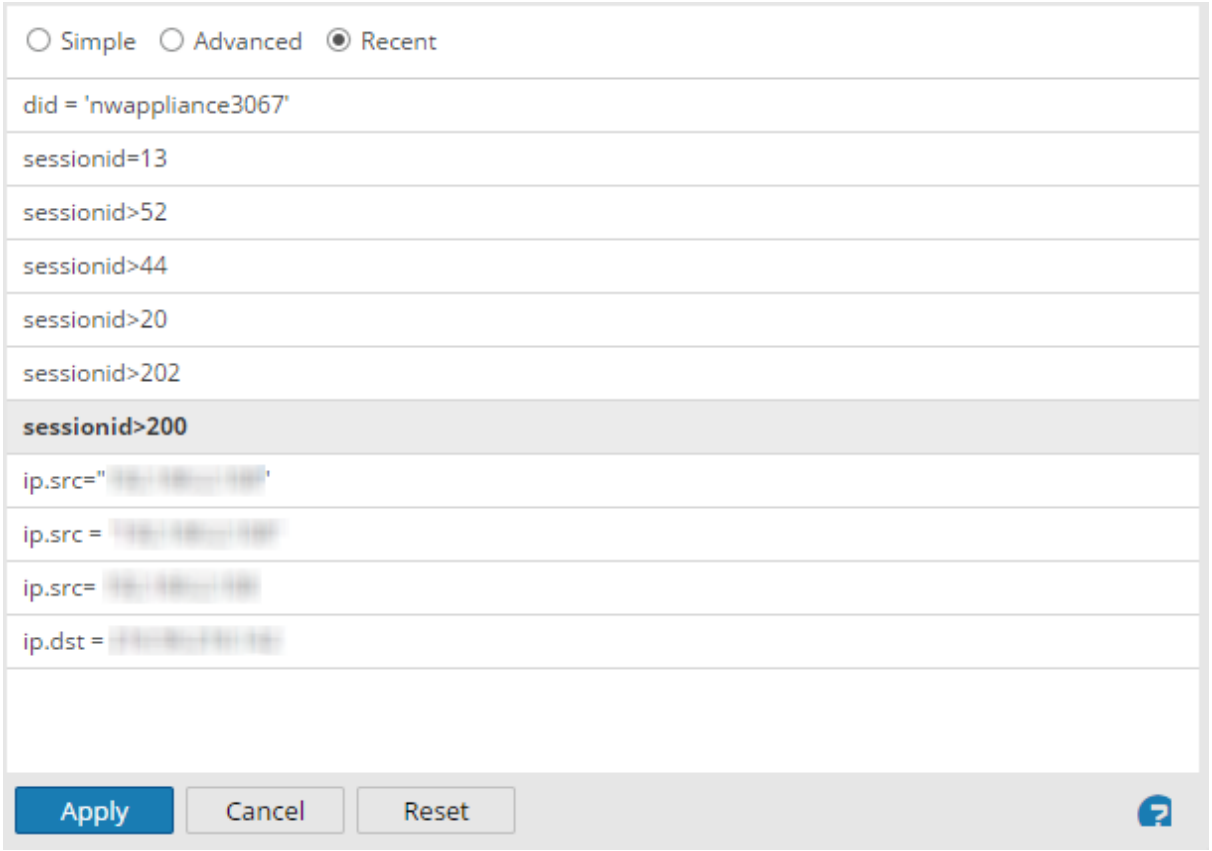
Anwenden einer zuletzt verwendeten Abfrage

Sie können zuletzt verwendete Abfragen anzeigen und eine auswählen, um sie auf den aktuell untersuchten Service anzuwenden. So wählen Sie eine zuletzt verwendete Abfrage aus:

1. Wählen Sie in der Symbolleiste der **Ansicht „Navigation“** oder der Ansicht „Ereignisse“ die Option **Abfrage** aus.
   Das Dialogfeld „Abfrage“ wird mit ausgewählter Option „Einfach“ angezeigt.



2. Wählen Sie die Option **Zuletzt verwendet** aus.
   Die Liste der zuletzt verwendeten Abfragen wird im unteren Teil des Dialogfelds angezeigt.



3. Klicken Sie in die Liste der zuletzt verwendeten Abfragen, um eine Abfrage auszuwählen.
4. Führen Sie einen der folgenden Schritte aus:
   - Doppelklicken Sie auf eine Abfrage.
   - Wählen Sie eine Abfrage aus und klicken Sie auf **Anwenden**.
     Das Fenster wird geschlossen und die Ansicht wird mit den Ergebnissen der neuen Abfrage aktualisiert. Die Abfrage wird im Breadcrumb angezeigt.
   - Klicken Sie auf **Abbrechen**.
     Das Fenster wird geschlossen und es werden keine Änderungen an der Ansicht oder aktuellen Abfrage vorgenommen.

Verwalten von Context-Hub-Listen und Listenwerten in den Ansichten „Navigation“ und „Ereignisse“

Analysten können Listen und Listenwerte für die Context Hub-Erweiterung in den Ansichten „Navigation“ und „Ereignisse“ hinzufügen. (In Version 11.2 und höhen können Analysten in der Ansicht „Ereignisanalyse“ Listen und Listenwerte hinzufügen, wie unter Suchen von zusätzlichem Kontext in der Ansicht „Ereignisanalyse“ beschrieben.)

Wenn der Context-Hub-Service aktiviert und konfiguriert ist, stellt NetWitness Platform Erweiterungsdaten von Incident-Management, benutzerdefinierte Listen und NetWitness Endpoint direkt in den Ansichten „Navigation“ und „Ereignisse“ bereit. Eine visuelle Orientierungshilfe hebt Metawerte hervor, für die Erweiterungsdaten in den Investigate-Ansichten verfügbar sind, und Sie können auf den hervorgehobenen Wert klicken, um die Kontextinformationen und -daten anzuzeigen.

Darüber hinaus können Sie im Bereich „Werte“ in der Ansicht „Navigation“ und der Ansicht „Ereignisse“ Listen anzeigen, Metawerte in einer vorhandenen Liste bearbeiten oder eine neue Liste erstellen. Wenn Sie einer Liste Metawerte hinzufügen, können Sie mithilfe der Kontextabfrageoption Metawerte untersuchen.

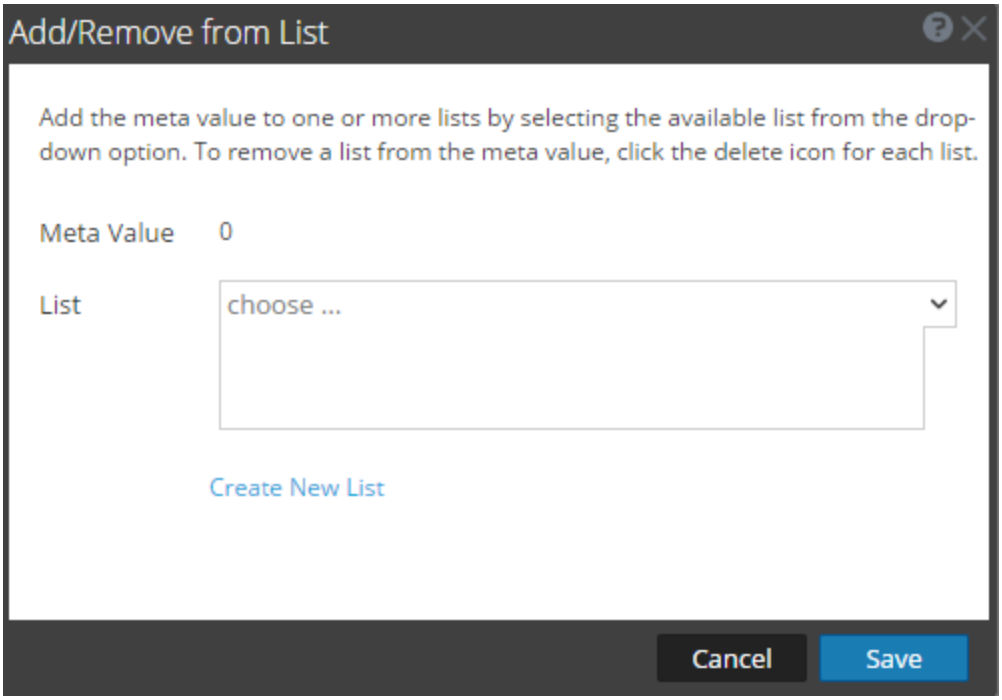
Damit ein Analyst Listen in Investigate managen kann, muss der Administrator Folgendes tun:

- Den Context-Hub-Service aktivieren.
- Dem Benutzer, der die Kontextabfrage aus „Investigation“-Ansichten durchführen wird, eine Analystenrolle mit der Berechtigung `Manage List from Investigation` zuweisen.
- Geeignete Rollen und Berechtigungen konfigurieren, wie in „Rollenberechtigungen“ und „Managen von Benutzern mit Rollen und Berechtigungen“ im *Handbuch Systemsicherheit und Benutzerverwaltung* beschrieben.

Hinzufügen von Metawerten zu einer vorhandenen Liste

So fügen Sie Metawerte zu einer vorhandenen Liste in Context Hub hinzu:

1. Klicken Sie beim Untersuchen eines Services in der Ansicht **Navigation** oder der Ansicht **Ereignisse** mit der rechten Maustaste auf einen Metawert (zum Beispiel auf Werte unter „Quell-IP“, „Ziel-IP“ oder „Benutzername“) und wählen Sie **Zu Liste hinzufügen/Aus Liste entfernen** im Kontextmenü aus.
   Das Dialogfeld Zu Liste hinzufügen/Aus Liste entfernen wird angezeigt.



2. Wählen Sie im Feld **Liste** eine oder mehrere Listen aus der Drop-down-Option aus, der der Metawert hinzugefügt werden muss.
3. Klicken Sie auf **Speichern**.
   Der Metawert wird den ausgewählten Listen hinzugefügt.

Entfernen eines Metawerts aus einer Context Hub-Liste

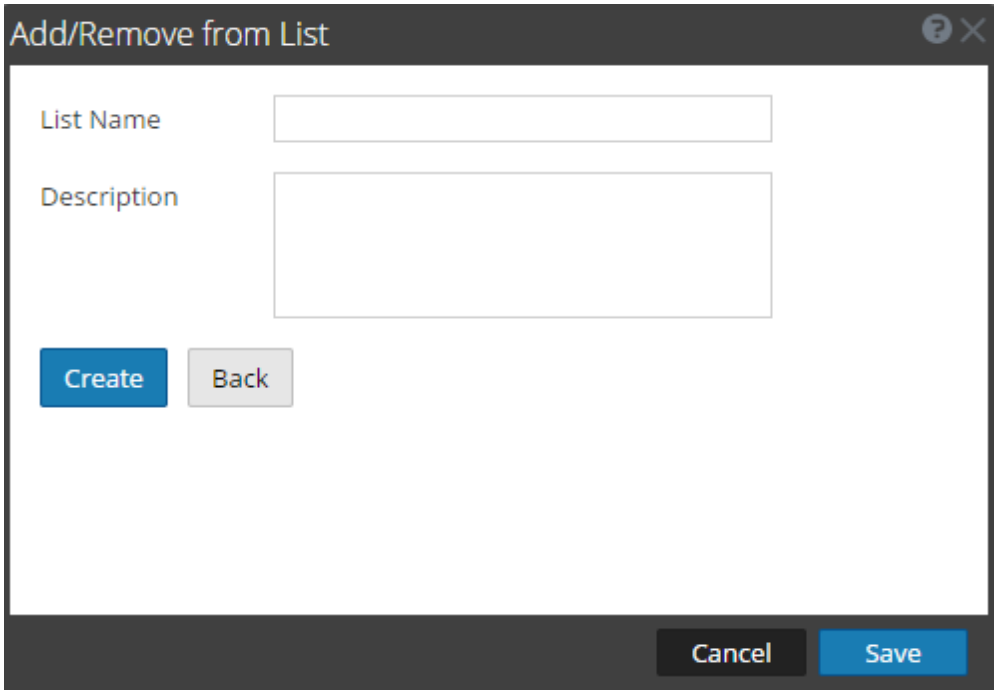
So entfernen Sie einen Metawert aus einer Liste:

1. Zeigen Sie im Dialogfeld **Zu Liste hinzufügen/Aus Liste entfernen** im Feld **Liste** die Listen an, die den Metawert enthalten.
2. Klicken Sie auf das Löschsymbol (x) für jede Liste, die den Metawert nicht enthalten soll.
3. Klicken Sie auf **Speichern**.
   Der Metawert wird aus der gelöschten Liste entfernt.

Erstellen einer neuen Liste

So erstellen Sie eine Context Hub-Liste in Investigate:

1. Klicken Sie im Dialogfeld **Zu Liste hinzufügen/Aus Liste entfernen** auf **Neue Liste erstellen**.



2. Geben Sie im Feld **Listenname** einen eindeutigen Namen für die Liste ein.
3. Geben Sie im Feld **Beschreibung** die Beschreibung für die Liste ein.
4. Klicken Sie auf **Erstellen**, um die Liste zu erstellen.
5. Klicken Sie auf **Speichern**, um den Metawert der erstellten Liste hinzuzufügen.
   Diese Listen werden als Datenquellen für das Abrufen von Kontextinformationen betrachtet.

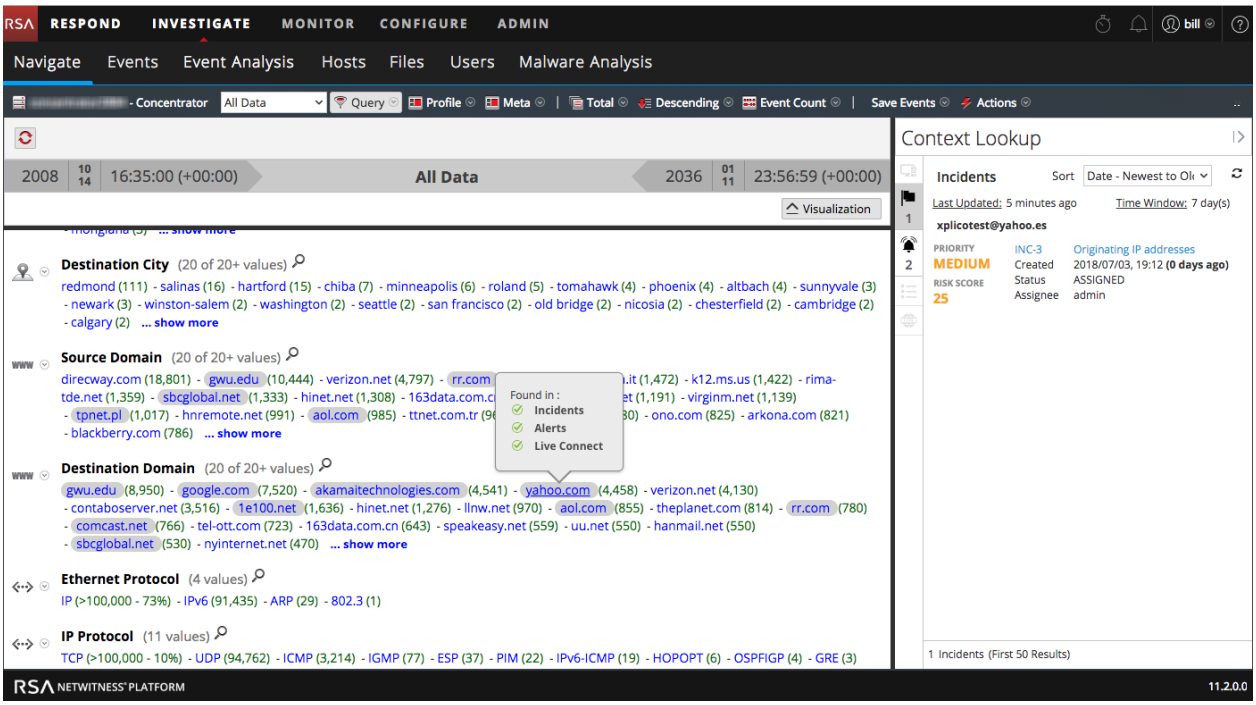
Suchen von weiteren Kontexten in den Ansichten „Navigation“ und „Ereignisse“

In der Ansicht „Ereignisse“ und der Ansicht „Navigation“ können Sie Details und Informationen zu Elementen nachschlagen, die mit einem Ereignis im Context Hub verknüpft sind. (In der Version 11.2 und höher können Sie auch in der Ansicht „Ereignisanalyse“ nach weiteren Kontexten suchen (siehe Beschreibung unter Suchen von zusätzlichem Kontext in der Ansicht „Ereignisanalyse“). Bei diesen Elementen oder Entitäten handelt es sich um Identifikatoren, wie z. B. eine IP-Adresse, ein Benutzername, ein Hostname, ein Domain-Name, ein Dateiname oder ein Dateihash. Die Daten aus konfigurierten Quellen wie RSA NetWitness Endpoint können Ihnen helfen, die Vorfälle zu verstehen.

Hinweis: Damit Sie kontextbezogene Informationen anzeigen können, muss Ihr Administrator den Context-Hub-Service in RSA NetWitness Platform hinzufügen und Datenquellen für den Context-Hub-Service konfigurieren wie im *Context-Hub-Konfigurationsleitfaden* beschrieben. Analysten müssen eine Rolle mit der Berechtigung `Context Lookup` haben, wie unter „Rollenberechtigungen“ und „Managen von Nutzern mit Rollen und Berechtigungen“ im Handbuch *Systemsicherheit und Benutzerverwaltung* beschrieben wird. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Der Context Hub ist ein zentralisierter Service, der Daten zu Entitäten aus mehreren konfigurierbaren Datenquellen aggregiert. Diese Daten können Ihre Untersuchung durch zusätzlichen Kontext über die sofortigen Ergebnisse einer bestimmten Abfrage hinaus erweitern. Zum Beispiel kann Ihnen der Context Hub sagen, ob eine bestimmte Entität in Incidents, Warnmeldungen, Feeds oder Veröffentlichungen von Communityinformationen erwähnt wurde.

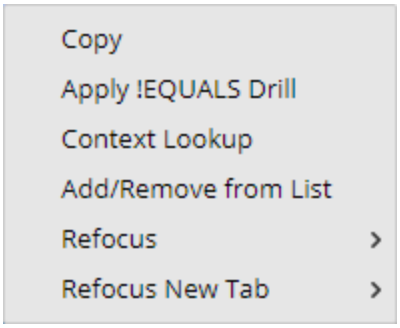
In der Ansicht „Navigation“ und der Ansicht „Ereignisse“ werden Entitäten, die zugehörige Kontextdaten haben, mit grauem Hintergrund hervorgehoben. Wenn Sie den Mauszeiger über eine Entität bewegen, wird ein Popup-Feld mit einer Zusammenfassung der verfügbaren Daten angezeigt. Wenn Sie mit der rechten Maustaste auf die Entität klicken, fragt der Context Hub die konfigurierten Datenquellen nach relevanten Informationen ab und auf der rechten Seite des Browserfensters wird der Bereich „Kontextabfrage“ geöffnet. Der Bereich „Kontextabfrage“ wird mit den Informationen aus dem Context Hub gefüllt, sobald diese verfügbar sind. Zum Ausführen weiterer Suchen klicken Sie mit der rechten Maustaste auf eine andere Entität und der Bereich „Kontextabfrage“ wird mit den Informationen zu dieser Entität aktualisiert.



Im Bereich „Kontextabfrage“ können Sie einzelne Datenquellen anzeigen und weiter durchsuchen. Eine detaillierte Beschreibung der Informationen, die für jede Datenquelle angezeigt werden, finden Sie unter Bereich „Kontextabfrage“.

So zeigen Sie Informationen im Bereich „Kontextabfrage“ in der Ansicht „Navigation“ oder der Ansicht „Ereignisse“ an:

1. Bewegen Sie den Mauszeiger über verschiedene Metawerte, um die für die Daten verfügbaren Datenquellen anzuzeigen.
   Ein Popup-Fenster zeigt eine Liste der Datenquellen an, für die Kontextdaten für den Metawert zur Verfügung stehen. Mögliche Datenquellen sind: NetWitness Endpoint, Incidents, Warnmeldungen, Hosts, Dateien, Feeds und Live Connect.
2. Klicken Sie mit der rechten Maustaste auf einen Metawert und klicken Sie im Drop-down-Menü auf **Kontextabfrage**, um den Bereich „Kontextabfrage“ zu öffnen.



   Der Bereich „Kontextabfrage“ wird auf der rechten Seite des Browserfensters geöffnet. Der Bereich „Kontextabfrage“ wird mit den Informationen aus dem Context Hub gefüllt, sobald diese

verfügbar sind.

3. Zum Ausführen von Aktionen aus dem Bereich „Kontextabfrage“ klicken Sie mit der rechten Maustaste auf eine Entität, z. B. IP-Adresse.
   Folgende Optionen sind verfügbar: „Link in neuer Registerkarte öffnen“, „In Investigate abfragen“, „Link kopieren“, „Einfügen“, „Google-Abfrage“, VirusTotal-Abfrage“ und „In Endpoint abfragen“.
4. Um den Bereich „Kontextabfrage“ zu schließen, klicken Sie im Bereich auf ■.

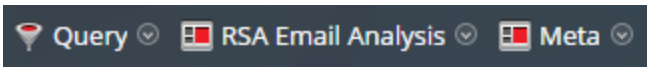
Einkapseln von benutzerdefinierten Ansichten mithilfe von Profilen

Die Verwendung von Profilen ist eine schnelle und einfache Methode, um anzupassen, welche Daten in der Ansicht „Navigation“ und der Ansicht „Ereignisse“ angezeigt werden. Im Dialogfeld „Profile managen“ können Sie mithilfe eines Profils bestimmen, welche Metagruppen und Spaltengruppen standardmäßig angezeigt werden, um Abfragen an eine Ermittlung anzuhängen und um Profile zu importieren oder zu exportieren.

Hinweis: Profile werden für Benutzer in demselben NetWitness Platform-Netzwerk freigegeben. Wenn ein Benutzer ein Profil ändert oder löscht, hat das Auswirkungen darauf, was für die anderen Benutzer verfügbar ist.

Wenn Sie mehrere Profile haben, können Sie zwischen ihnen wechseln, um schnell zu den Einstellungen des ausgewählten Profils zu gelangen. Wenn ein Profil aktuell aktiv ist, wird der Titel des Profilmenüs durch den Namen des Profils ersetzt.

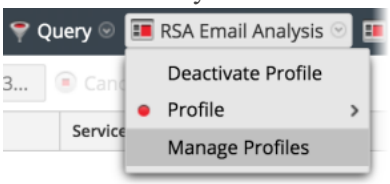
Die folgende Abbildung illustriert dies in der Navigationsansicht. Der Profilname wird rechts von der Option „Abfrage“ angezeigt. Das gilt auch für die Ansicht „Ereignisse“.



Ab Version 11.2 sind die Profile in Profilgruppen organisiert. Die vordefinierten Profile befinden sich in der nicht bearbeitbaren Standardprofilgruppe. Analysten können neue Profilgruppen für alle Nutzer erstellen. Sie können eine erstellte Profilgruppe bearbeiten und Profile hinzufügen, entfernen oder von einer Gruppe in eine andere verschieben. Ein erstelltes Profil wird standardmäßig nicht zu einer Profilgruppe hinzugefügt. Beim Export von Profilen werden Informationen über die Profilgruppe gespeichert und Profile in dieselbe Gruppe importiert, aus der sie exportiert wurden.

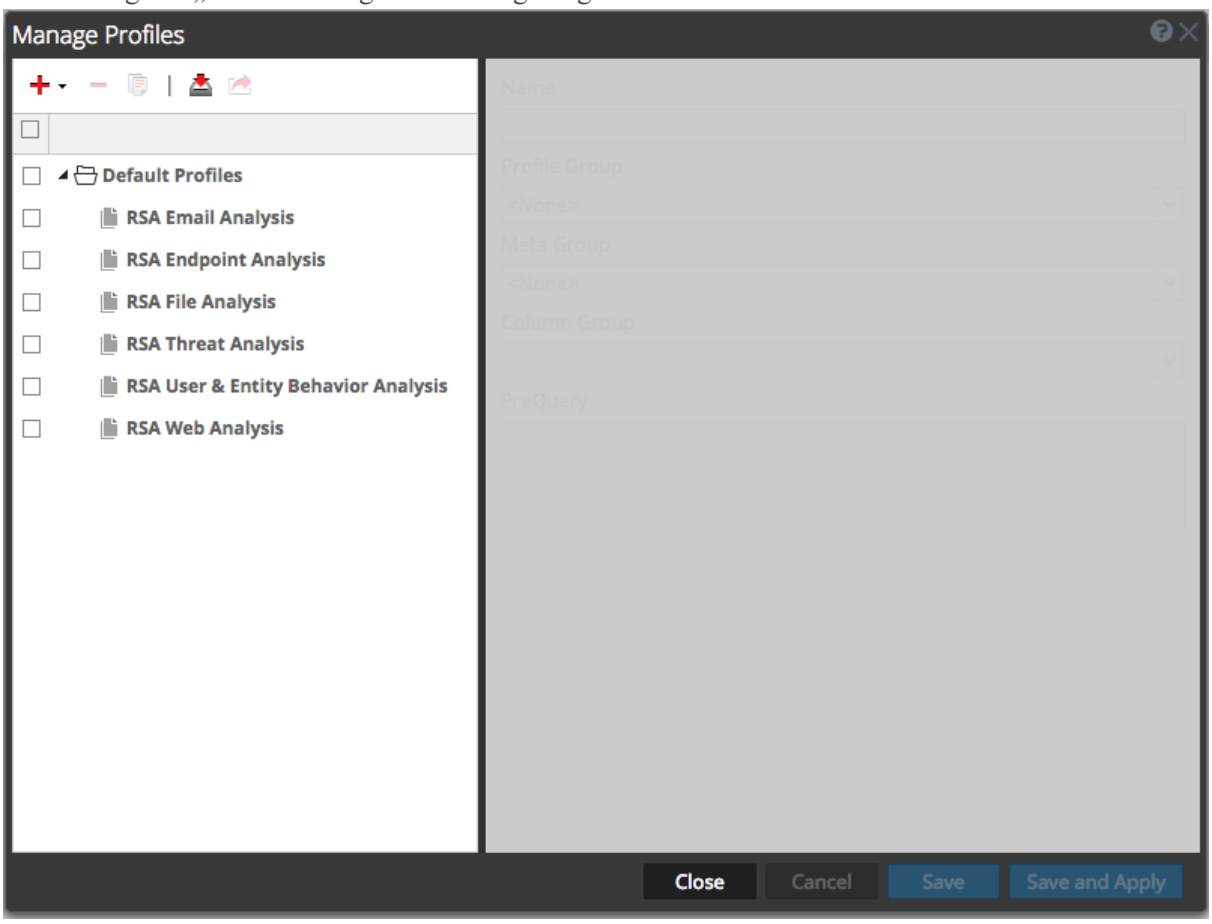
Navigieren Sie zum Dialogfeld „Profile managen“.

1. Navigieren Sie zu Ermittlung > **Ereignisse** oder **Ermittlung** > **Navigation**. Wenn das Dialogfeld **Untersuchen** angezeigt wird, wählen Sie einen Service aus und klicken Sie auf **Navigation**.
2. Wählen Sie in der Symbolleiste **Profile > Profile managen**.



aus.

Das Dialogfeld „Profile managen“ wird angezeigt.



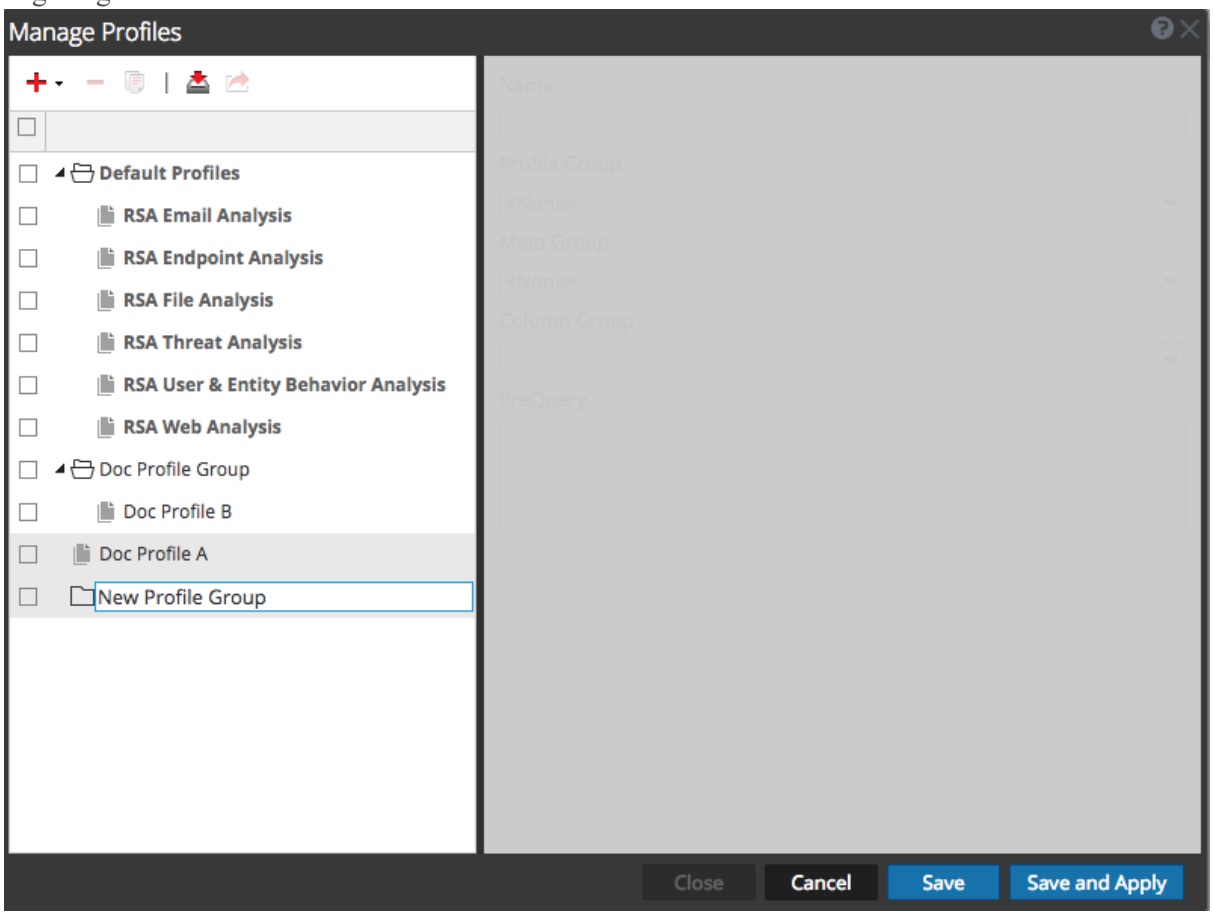
Erstellen, Bearbeiten oder Löschen einer Profilgruppe (Version 11.2 und höher)

Sie können eine eigene Profilgruppe erstellen, in der Sie verschiedene Profile organisieren können. In einer erstellten Profilgruppe können Sie lediglich den Namen der Profilgruppe direkt bearbeiten. Zum Hinzufügen oder Entfernen eines Profils einer Gruppe müssen Sie das Profil bearbeiten und es einer anderen Profilgruppe zuweisen wie unter Erstellen und Bearbeiten von Profilen beschrieben.

1. Führen Sie auf der Registerkarte **Profile managen** einen der folgenden Schritte aus:
   - Zum Auswählen einer zu bearbeitenden Profilgruppe doppelklicken Sie auf die Profilgruppe.
   - Zum Hinzufügen einer neuen Profilgruppe klicken Sie auf + und wählen Sie **Neue Profilgruppe hinzufügen** aus.

Hinweis: Zum Bearbeiten einer vordefinierten Profilgruppe klicken Sie auf , um eine bearbeitbare Kopie zu erstellen.

Am unteren Ende der Profilliste in der linken Spalte wird ein Ordner mit einem leeren Feld angezeigt.



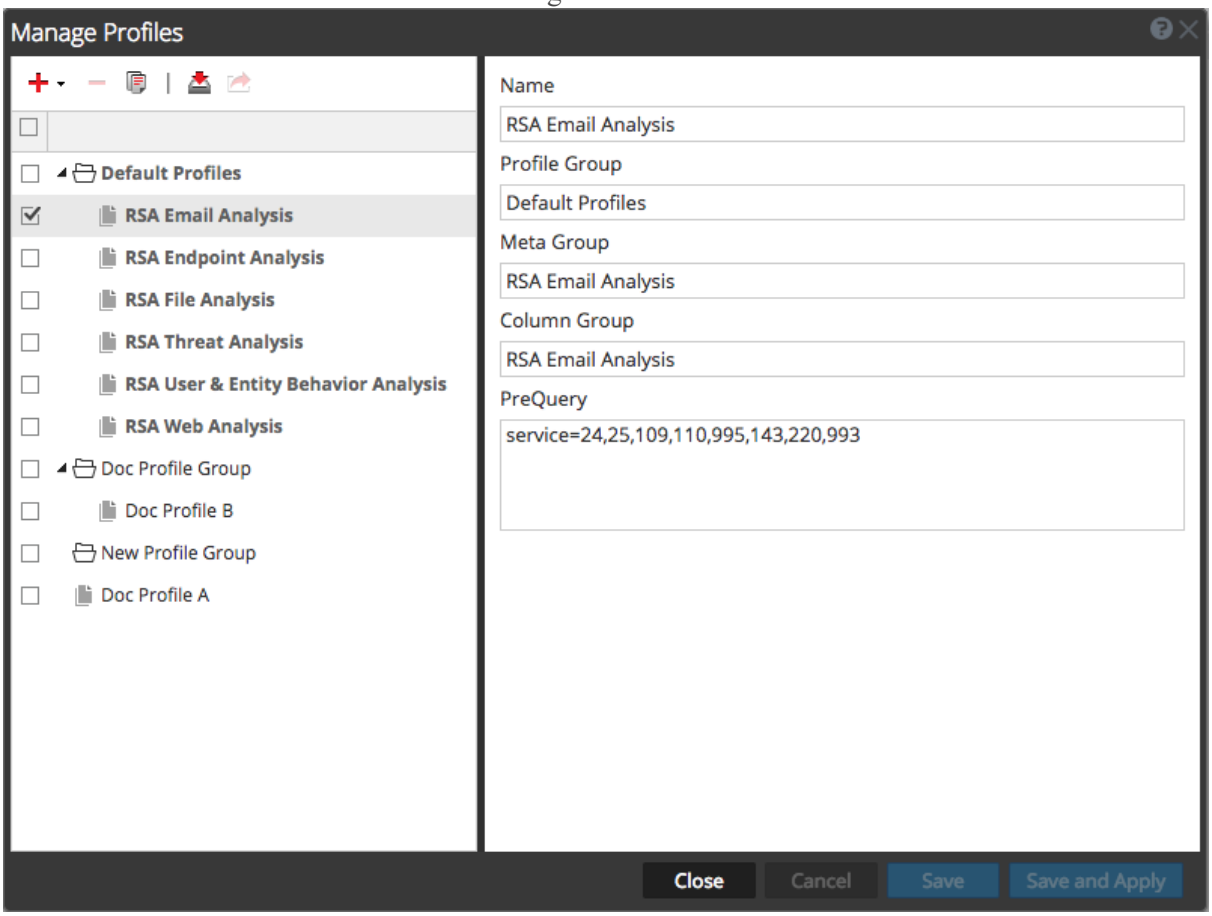
2. Zum Bearbeiten oder Eingeben des Namens der Profilgruppe doppelklicken Sie auf die Profilgruppe und geben Sie den Namen in das Eingabefeld ein. Der Name muss zwischen 2 und 80 Zeichen lang sein.
   Der Name der Profilgruppe wird auf eine neue Profilgruppe oder auf die von Ihnen bearbeitete Profilgruppe angewendet. Die Profilgruppe ist nun bei der Konfiguration eines Profils verfügbar.
3. Um eine Profilgruppe zu löschen, führen Sie einen der folgenden Schritte aus:
   - Wenn Sie eine Profilgruppe löschen wollen, aber die Profile behalten möchten, wählen Sie die Gruppe durch Aktivieren des Kontrollkästchens aus. Deaktivieren Sie die Kontrollkästchen für die Profile in der Gruppe und klicken Sie auf „Löschen“.
   - Wenn Sie eine Profilgruppe und die Profile in der Gruppe löschen möchten, wählen Sie die Gruppe durch Aktivieren des Kontrollkästchens aus und deaktivieren Sie die Kontrollkästchen für die zu löschenden Profile nicht.
     Sie müssen in einem Dialogfeld bestätigen, dass Sie die ausgewählte Gruppe löschen möchten. Wenn Sie das Kontrollkästchen neben den Profilen nicht deaktiviert haben, werden die Gruppe und die Profile in der Gruppe gelöscht. Wenn Sie die Kontrollkästchen für die Profile deaktiviert haben, wird nur die Profilgruppe gelöscht. Die Profile werden aus der Gruppe verschoben und können in einer anderen Profilgruppe hinzugefügt werden.

Erstellen und Bearbeiten von Profilen

1. Führen Sie auf der Registerkarte **Profile managen** einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben dem Namen eines vorhandenen Profils, um es zur Bearbeitung auszuwählen.
   - Zum Hinzufügen eines neuen Profils in Version 11.2 und höher klicken Sie auf + oder auf den Pfeil unten neben + und wählen Sie **Neues Profil hinzufügen** aus.
   - Zum Erstellen eines neuen Profils in Versionen vor 11.2 klicken Sie auf +.

   Hinweis: Zum Bearbeiten von vordefinierten Profilen klicken Sie auf , damit eine Kopie erstellt wird, die Sie bearbeiten können.

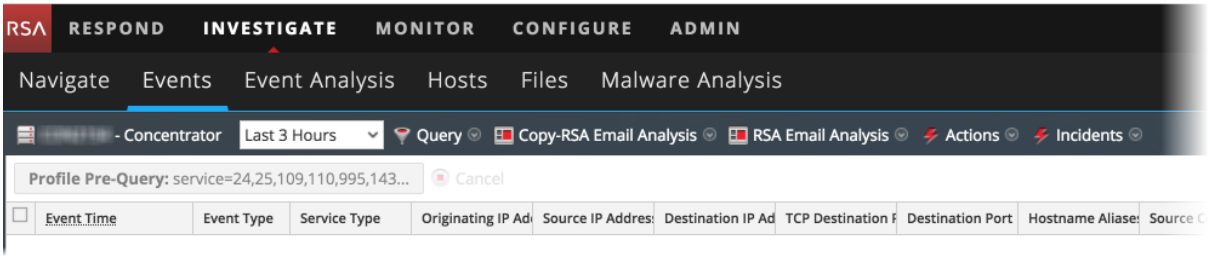
   Die Definition des Profils kann im rechten Bereich bearbeitet werden. In dieser Abbildung ist die Definition eines der vordefinierten Profile dargestellt.



2. Bearbeiten Sie den Profilnamen oder geben Sie ihn ein, indem Sie in das Feld **Name** schreiben. Der Name muss zwischen 2 und 80 Zeichen lang sein.
3. (Optional für Version 11.2 und höher) Wenn Sie das Profil zu einer Profilgruppe hinzufügen möchten, wählen Sie eine Profilgruppe aus der Drop-down-Liste **Profilgruppe** aus.

Wenn Sie eine Profilgruppe auswählen, wird das Profil der Gruppe beim Speichern der Änderungen hinzugefügt. Wenn Sie keine Profilgruppe auswählen, ist das Profil nicht Teil einer Gruppe.

4. Wählen Sie eine Metagruppe aus der Drop-down-Liste **Metagruppe** aus. Sie können benutzerdefinierte Metagruppen hinzufügen, wie unter Metagruppen managen beschrieben ist.
5. Wählen Sie eine Spaltengruppe für die Drop-down-Liste **Spaltengruppe** aus. Sie können benutzerdefinierte Spaltengruppen hinzufügen, wie beschrieben in Managen von Spaltengruppen in der Ansicht „Ereignisse“.
6. Geben Sie Abfragen zum Filtern von Ergebnissen in das Feld **Vorabfrage** ein. PreQuery folgt der gleichen Syntax wie die Abfrageerstellung. Für die PreQuery in der Abbildung wird eine Metagruppe namens **service = 24,25,109,110,995,143,220,993** verwendet.
7. Klicken Sie auf **Speichern**, um das Profil zu speichern, ohne es zu übernehmen, oder klicken Sie auf **Speichern und übernehmen**, um das Profil zu speichern und es sofort zu übernehmen.
   Wenn Sie auf **Speichern und übernehmen** klicken, wird ein Bestätigungsdialogfeld angezeigt, bevor das ausgewählte Profil angewendet wird. Für Version 11.2 und höher wird die von Ihnen im Dialogfeld „Profile managen“ eingegebene PreQuery in der Brotkrümelnavigation angezeigt.



Löschen eines Profils

1. Wählen Sie im Dialogfeld **Profile managen** ein Profil aus. Aktivieren Sie dazu das Kontrollkästchen neben dem entsprechenden Namen.

   Hinweis: Sie können keines der vordefinierten Profile löschen.

2. Klicken Sie auf .
   In einer Eingabeaufforderung müssen Sie bestätigen, dass Sie das Profil löschen wollen, und das Profil wird gelöscht. Der Optionsname in der Symbolleiste ändert sich in **Profil**. Damit wird angezeigt, dass kein Profil aktiv ist.

Wechseln des aktiven Profils

Wenn Sie in der Ansicht „Navigation“ oder „Ereignisse“ nicht genügend Ergebnisse oder nicht die richtigen Ergebnisse sehen, haben Sie eventuell ein aktives Profil, auf das eine PreQuery angewendet wird. Wenn Sie keine Profile verwenden möchten, können Sie auf **Profile deaktivieren** im Drop-down-Menü **Profile** klicken.

So verwenden Sie ein anderes Profil:

1. Öffnen Sie in der Symbolleiste der Ansicht **Navigieren** oder **Ereignisse** das Drop-down-Menü **Profile**.
2. Bewegen Sie den Mauszeiger über die Option **Profil**, um eine Drop-down-Liste verfügbarer Profile anzuzeigen.
3. Wählen Sie das Profil aus, das Sie verwenden möchten.
   Die Profileinstellungen werden sofort übernommen.

Wenn Sie das aktive Profil im Dialogfeld „Profil managen“ ändern möchten:

1. Wählen Sie in der Symbolleiste der Ansicht **Navigation** oder **Ereignisse** die Optionen **Profile > Profile managen** aus.
   Das Dialogfeld „Profile managen“ wird angezeigt.
2. Wählen Sie ein Profil aus dem linken Bereich aus und klicken Sie auf **Speichern und übernehmen**.
   Ein Bestätigungsdialogfeld wird angezeigt.
3. Klicken Sie auf **Yes**.
   Die Profileinstellungen werden sofort übernommen.

Importieren von Profilen

Sie können `.jsn`-Dateien hochladen oder importieren, die von einem anderen Service heruntergeladen wurden. Wenn Profilgruppen exportiert und dann importiert werden, wird die Gruppierung der Profile beibehalten.

1. Klicken Sie im Dialogfeld **Profile managen** auf  in der Symbolleiste im linken Bereich.
   Das Dialogfeld „Profilimport“ wird angezeigt.
2. Klicken Sie auf **Durchsuchen** oder auf das Feld **Datei hochladen**, um eine Datei von Ihrem Rechner auszuwählen.
3. Wenn die Datei ausgewählt ist, klicken Sie auf **Hochladen**.
   Das Profil wird im linken Bereich angezeigt.

Herunterladen von Profilen

Profile werden als .jsn-Dateien heruntergeladen.

1. Wählen Sie im Dialogfeld **Profile managen** eines oder mehrere Profile aus dem linken Bereich aus.
2. Klicken Sie in der Symbolleiste auf der linken Seite auf  .
   Der Download startet sofort.

Suchen nach Textmustern

Sie können in den Ansichten „Navigation“ und „Ereignisse“ im aktuellen Satz von Ereignissen nach Textmustern suchen. Sie können eine Textsuche nach Schlüsselworten oder einen Musterabgleich nach regulären Ausdrücken (regex) durchführen. In der Navigationsansicht können Sie auf einen Metawert klicken, wie etwa HTTP, um einen Drill-down in die Daten durchzuführen und dann eine Suchzeichenfolge in das Suchfeld einzugeben, um nach Ereignissen innerhalb dieser Untermenge von Daten zu suchen. Die Suche öffnet eine Registerkarte in der Ereignisansicht, bringt Ihren Drill-down-Punkt und Zeitbereich nach vorn und zeigt die Suchergebnisse an. Sie können auch mithilfe von Abfragen einen Drill-down in die Daten durchführen, bevor Sie eine Suche starten. Geben Sie zur Durchführung der Suche eine Suchzeichenfolge im Suchfeld ein und drücken Sie die **Eingabetaste** oder klicken Sie auf **Suche**.

Schlüsselworttextsuche

Die Textsuche bietet folgende Möglichkeiten:

- Die durch Leerzeichen begrenzten Wörter werden mit dem Operator UND versehen, sodass jedes Wort gefunden werden muss, jedoch spielt die Reihenfolge oder die Position in Bezug auf die anderen Wörter keine Rolle. Wenn Sie zum Beispiel nach `Mark Albert` suchen, muss sowohl „Mark“ als auch „Albert“ in der Sitzung gefunden werden, diese Wörter müssen jedoch nicht zusammen stehen oder sich in einer bestimmten Reihenfolge befinden.
- Für den Operator ODER gelten Besonderheiten. Wenn Sie nach `Mark OR Albert` suchen, muss entweder „Mark“ oder „Albert“ in der entsprechenden Sitzung gefunden werden, sie sind jedoch nicht beide erforderlich.
- Sie können implizite UND- und ODER-Operatoren in der Suchzeichenfolge beliebig zusammenstellen und verwenden. Der explizite ODER-Operator hat eine höhere Priorität als der implizite UND-Operator (mit Leerzeichen). Im folgenden Beispiel wird dieselbe logische Anweisung verwendet, die erfordert, dass eine Übereinstimmung die beiden Wörter „cheese“ und „dumplings“ sowie entweder „toast“ oder „bread“ enthalten muss:
  ```
  cheese toast OR bread dumplings
  cheese AND (toast OR bread) AND dumplings
  ```
- Sie können Wörter mithilfe des Operators – aus den Suchergebnissen ausschließen. Die Suche nach `cheese -toast` würde beispielsweise alle Ergebnisse zurückgeben, die das Wort „cheese“ enthalten, es sei denn, das Wort „toast“ ist auch vorhanden.
- Die Schlüsselwortsuche kann Metadaten finden, die den folgenden Mustern entsprechen:
  - **IPv4- und IPv6-Adressen**. Jeder Ausdruck, der als eine IP-Adresse erkannt werden kann, wird in das native Metadatenformat konvertiert, sodass er in indizierten Metadaten gefunden werden kann.
  - **IPv4-CIDR-Adressbereich**. Sie können mithilfe der CIDR-Notation IPv4-Adressen innerhalb eines Bereichs finden.
  - **Zeitstempel**. Zeitstempel werden mit den nativen Zeitmetadaten und allen zusätzlichen Zeitmetafeldern, die mit dem Typ „Zeit“ gespeichert sind, verglichen.

- **Nummern**. Die Suchfunktion versucht, automatisch dezimale Suchbegriffe zu identifizieren und sie gegen numerische Metadatenfelder abzugleichen.

Optionen zum Steuern des Suchverhaltens

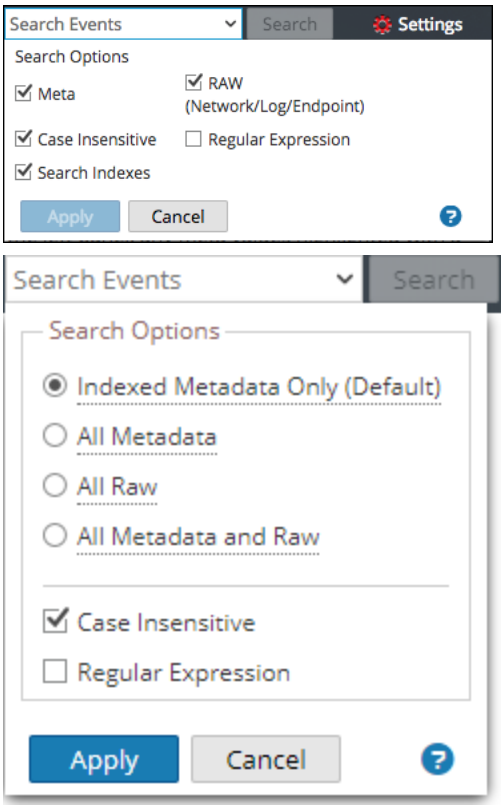
So greifen Sie auf das Suchfeld und die Suchoptionen in den Ansichten „Navigation“ oder „Ereignisse“ zu.

1. In der Symbolleiste wird das Feld „Ereignisse suchen“ angezeigt.

   Fehlerbehebung: Wenn das Feld „Ereignisse suchen“ nicht in der Symbolleiste angezeigt wird, klicken Sie auf der rechten Seite der Symbolleiste auf ..

2. Klicken Sie auf das Suchfeld, um das Drop-down-Menü „Suchoptionen“ anzuzeigen. In der Version 11.2 und höher sind die Menüoptionen etwas anders. In der ersten Abbildung ist das Menü für 11.1 und früher dargestellt. In der zweiten Abbildung ist das Menü für Version 11.2 und höher veranschaulicht.

Die in diesem Feld ausgewählten Optionen ändern die Ausführung der Suche. Im Standardsuchmodus werden Indizes nur für indizierte Metadaten und Rohdaten gesucht.

Hinweis: Da die Kontrollkästchen „Index“ oder „Nur indizierte Metadaten (Standard)“ aktiviert sind, gibt die Suche Ergebnisse basierend auf indizierten Daten zurück. Wenn Sie nach einem vollständigen Satz Metadaten oder Rohdaten suchen möchten, aktivieren Sie diese Kontrollkästchen und deaktivieren Sie das Kontrollkästchen „Index“ oder „Nur indizierte Metadaten (Standard)“. Diese Art der Suche dauert länger, gibt jedoch einen umfassenderen Satz von Daten zurück.

In der folgenden Tabelle werden die Investigation-Suchoptionen beschrieben.

Funktion	Beschreibung
Kontrollkästchen **Nur indexierte Metadaten (Standard)** (Version 11.2) Optionsfeld **Index** (Version 11.1)	Die Suche gibt nur Ergebnisse aus indizierten Daten zurück. Das Durchsuchen des Index ist der schnellste Weg, innerhalb einer großen Datenmenge Schlüsselwörter zu finden. Die Indexsuche verwendet alle relevanten Indizes innerhalb Ihrer Datensammlung. **Achtung:** Übereinstimmungen von Teilzeichenfolgen werden durch eine Indexsuche nicht gefunden. Wenn Sie Übereinstimmungen von Teilzeichenfolgen benötigen, deaktivieren Sie dieses Kontrollkästchen und verwenden Sie einen Nicht-Index-Suchmodus.
Optionsfeld **Alle Metadaten** (Version 11.2) Kontrollkästchen **Metadaten** (Version 11.1)	Durchsucht die Metadaten. Ihr Schlüsselwort oder Regex-Muster wird mit allen geparsten Metadaten verglichen.
Optionsfeld **Alle Rohdaten** (Version 11.2) Kontrollkästchen **RAW** (Netzwerk/Protokoll/Endpunkt) (Version 11.1)	Sucht den Text für Netzwerk-, Protokoll- und Endpunktereignisse. Jedes Ereignis wird entschlüsselt und sein Inhalt wird nach Übereinstimmungen für das Schlüsselwort oder ein Regex-Muster durchsucht. Wenn Sie alle Daten ohne Filter auf dem Archiver auswählen, kann die Ausführungszeit sehr lange dauern, sodass eine Warnmeldung angezeigt wird. **Achtung:** Das Durchsuchen von Raw-Netzwerksitzungen führt dazu, dass Sitzungen dekodiert werden, was äußerst zeitaufwendig ist. Sie können Raw-Suchen auch deaktivieren, wenn Sie Nur-Netzwerksammlungen betrachten.
Optionsfeld **Alle Metadaten und Rohdaten** (Version 11.2)	Sucht die Metadaten und den Protokoll- oder Ereignistext. Diese Option ist eine Kombination aus zwei Optionen in Version 11.1: Metadaten und RAW (Netzwerk/Protokoll/Endpunkt), die Sie gemeinsam auswählen können. In Version 11.2 können Sie nur ein Optionsfeld auswählen.
Groß- und Kleinschreibung nicht beachten	Bei der Suche wird die Groß- und Kleinschreibung nicht beachtet.

Funktion	Beschreibung
Regulärer Ausdruck	Sucht unter Verwendung eines regulären Perl-Ausdrucks und nicht einer Textzeichenfolge. Führt standardmäßig eine Textsuche aus. Um eine Suche nach einem regulären Ausdruck auszuführen, aktivieren Sie das Kontrollkästchen „Regulärer Ausdruck“. **Achtung:** – Suchen nach regulären Ausdrücken können sehr langsam sein. – Bei der Kombination von regulären Ausdrücken mit Indexsuchoptionen wird das Muster für den regulären Ausdruck mit eindeutigen Indexwerten anstelle von Metawerten verglichen. Dies führt schneller zu Ergebnissen, aber es ist keine vollständige Suche über alle Metadaten oder Rohdaten.
Anwenden	Legt die Standardsuchoptionen fest, die auf eine Suche in der Navigations- und Ereignisansicht angewendet werden sollen. Dadurch werden auch die Einstellungen zu Investigation in Ihrem Profil aktualisiert („Profil“ > „Einstellungen“ > Registerkarte „Investigation“). Die Einstellungen werden gespeichert und sind sofort wirksam. Sie können Suchoptionen auswählen, die für eine bestimmte Suche gelten sollen, ohne Ihre Standardsucheinstellungen zu ändern.

Syntax für die Suche nach regulären Ausdrücken

Eine Suche nach regulären Ausdrücken verwendet die Perl-Syntax für reguläre Ausdrücke, die auf der Website http://perldoc.perl.org/perlre.html ausführlicher erläutert wird.

Rohtext-Schlüsselwortsuche

Mit dem Log Decoder kann ein Rohtextindex für nicht geparste Protokollereignisse erstellt werden. Diese Funktion erstellt Metadatenelemente, die einen Volltextindex auf Downstream-Services wie Concentrators und Archivers bilden. Wenn Sie die Option „Suchindizes“ in ihren Sucheinstellungen aktivieren, verwendet Ihre Suche automatisch den Textindex. Beachten Sie, dass der Textindex Metaelemente erzeugt, die eine grobe Granularität haben. Z. B. kürzt die Standardkonfiguration für Text-Indexer Textausdrücke. Durch den Vergleich der Index-Übereinstimmung mit Rohdaten findet die Suchmaschine genauere Ergebnisse für Ihre Suche. Sie können aber die Suchzeiten verbessern, indem Sie das Kontrollkästchen „Suche in Rohdaten“ deaktivieren. Wenn Sie dies tun, werden Ergebnisse schneller zurückgegeben, aber es werden möglicherweise falsch positive Treffer in Ihren Suchergebnissen angezeigt.

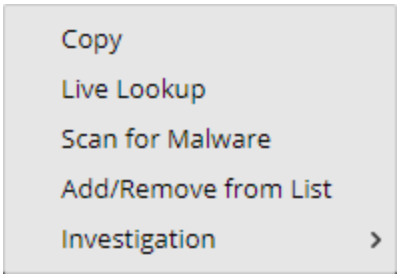
Suchbeispiele

Die folgenden Beispiele zeigen Suchvorgänge ausgehend von der Navigations- und der Ereignisansicht an.

Suchen in der Ansicht „Navigation“

So führen Sie eine Suche in den zurzeit angezeigten Daten in der Ansicht „Navigation“ durch:

1. Zum Durchführen eines Drill-down in die Daten klicken Sie auf einen Metawert, z. B. HTTP, im Bereich „Werte“.



2. Geben Sie eine Suchzeichenfolge in das Suchfeld ein und drücken Sie die **Eingabetaste** oder klicken Sie auf **Suche**.
3. Um den Eintrag im Suchfeld zu löschen und zur normalen Ereignisansicht zurückzukehren, klicken Sie im Suchfeld auf das **X**.

Suchen in der Ansicht „Ereignisse“

So führen Sie eine Suche in den zurzeit angezeigten Daten in der Ansicht „Ereignisse“ durch:

1. Geben Sie eine Suchzeichenfolge in das Suchfeld ein und drücken Sie die **Eingabetaste** oder klicken Sie auf **Suche**.
   Die Suchergebnisse werden in der Ansicht „Ereignisse“ angezeigt. Ereignisse, die den Suchkriterien entsprechen, werden in den Ereignissen angezeigt. In den Ansichten „Details“ und „Liste“ sind die Übereinstimmungen in der Spalte „Details“ markiert. Beim Durchsuchen von RAW sind Übereinstimmungen darüber hinaus in der Protokollansicht in der Spalte „Protokolle“ markiert.
2. Wenn Sie die Suche eingrenzen möchten, ändern Sie die Abfrage und die Uhrzeit.
3. Wenn Sie die Suche beenden und zur Ansicht „Ereignisse“ zurückkehren möchten, klicken Sie auf **Abbrechen**.
   Alle angezeigten Ergebnisse bleiben erhalten.
4. Um den Eintrag im Suchfeld zu löschen und zur normalen Ansicht „Ereignisse“ zurückzukehren, klicken Sie im Suchfeld auf **X**.

Anzeigen und Ändern von Abfragen mithilfe von URL-Integration

NetWitness Investigate umfasst eine externe URL-Integration, die über die Suche in der NetWitness Platform-Architektur die Integration von Drittanbieterprodukten ermöglicht. Indem Sie eine Abfrage in einer URI verwenden, können Sie ausgehend von jedem Produkt, das benutzerdefinierte Links erlaubt, zu einem bestimmten Drill-down-Punkt in der Ansicht „Ermittlung“ wechseln. Diese Integration ermöglicht eine interne Präsentation der Benutzerabfrage.

Mithilfe der URL-Integration kann der Benutzer den Service entweder über die Host-ID oder über den Service und den Port identifizieren. Dies wird in NetWitness Platform definiert. Kann NetWitness Platform den Service nicht auflösen, wird der Analyst zur Ansicht „Navigation“ umgeleitet. Dort wird das Dialogfeld zur Serviceauswahl angezeigt. Nach Auswahl des Services wird die Ansicht „Navigation“ mit dem in der Abfrage definierten Drill-down-Punkt geladen.

Bekannte Service-ID

Ist die ID des zur Ermittlung genutzten Services bekannt, erfolgt die Eingabe einer URI mithilfe einer URL-kodierten Abfrage in folgendem Format:

```
http://<sa host:port>/investigation/<deviceId>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

Hierbei gilt:

- `<sa host: port>` ist die IP-Adresse oder DNS, mit oder ohne einen Port, soweit anwendbar (SSL oder nicht). Diese Bezeichnung ist nur erforderlich, wenn der Zugriff über einen nicht standardmäßigen Port über einen Proxy konfiguriert ist.
- `<deviceId>` ist die interne Service-ID in der NetWitness Platform-Instanz für den abzufragenden Service. Die Service-ID kann nur als ganze Zahl repräsentiert werden. Sie können die relevante Service-ID in der URL einsehen, wenn Sie in NetWitness Platform auf die Ansicht „Investigation“ zugreifen. Dieser Wert ändert sich basierend auf dem für die Analyse verbundenen Service.
- `<encoded query>` steht dabei für die URL-kodierte NetWitness Platform-Abfrage. Die Länge der Abfrage ist durch die HTML-URL-Begrenzungen begrenzt.
- `<start date>` und `<end date>` definieren den Datumsbereich für die Abfrage. Das Format lautet: `<yyyy-mm-dd>T<hh:mm:ss>Z`. Start- und Enddatum sind erforderlich. Falls kein Datum angegeben wird, werden die Benutzerstandards für diesen Service verwendet. Relative Bereiche (zum Beispiel „Letzte Stunde“) werden nicht unterstützt. Alle Zeiten werden als UTC ausgeführt.
  Beispiel:
  `http://localhost:9191/investigation/12/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

Host und Port bekannt

Sind Host und Port des zur Ermittlung genutzten Services bekannt, erfolgt die Eingabe einer URI mithilfe einer URL-kodierten Abfrage in folgendem Format:

```
http://<sa host:port>/investigation/<device host:port>/navigate/query/<encoded query>/date/<start date>/<enddate>
```

wobei

- `<sa host: port>` ist die IP-Adresse oder DNS, mit oder ohne einen Port, soweit anwendbar (SSL oder nicht). Diese Bezeichnung ist nur erforderlich, wenn der Zugriff über einen nicht standardmäßigen Port über einen Proxy konfiguriert ist.
- `<device host:port>` sind dabei Host und Port eines definierten Services in der NetWitness Platform-Instanz für den abzufragenden Service. NetWitness Platform versucht, Host und Port als eine in NetWitness Platform definierte Service-ID aufzulösen.
- `<encoded query>` steht dabei für die URL-kodierte NetWitness Platform-Abfrage. Die Länge der Abfrage ist durch die HTML-URL-Begrenzungen begrenzt.
- `<start date> and <end date>` definieren den Datumsbereich für die Abfrage. Das Format lautet: `<yyyy-mm-dd>T<hh:mm:ss>Z`. Start- und Enddatum sind erforderlich. Falls kein Datum angegeben wird, werden die Benutzerstandards für diesen Service verwendet. Relative Bereiche (zum Beispiel Letzte Stunde) werden in dieser Version nicht unterstützt. Alle Zeiten werden als UTC ausgeführt.
  Beispiel:
  `http://localhost:9191/investigation/concentrator:50105/navigate/query/alias%20exists/date/2012-09-01T00:00:00Z/2012-10-31T00:00:00Z`

Beispiele

Dies sind Abfragebeispiele, in denen der NetWitness-Server 192.168.1.10 ist und die deviceID als 2 erkannt wurde.

Alle Aktivitäten am 03/12/2013 zwischen 5:00 und 6:00 Uhr mit einem registrierten Hostnamen

- Angepasster Pivot: `alias.host exists`
- `https://192.168.1.10/investigation/2/navigate/query/alias%2Ehost%20exists/date/2013-03-12T05:00:00Z/2013-03-12T06:00:00Z`

Alle Aktivitäten am 03/12/2013 zwischen 17:00 und 17:10 Uhr mit Http-Datenverkehr zu und von der IP-Adresse 10.10.10.3

- Angepasster Pivot: `service=80 && (ip.src=10.10.10.3 || ip.dst=10.0.3.3)`
- Kodierter Pivot analysiert:
  - `service=80 => service&3D80`
  - `ip.src=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `ip.dst=10.10.10.3 => ip%2Esrc%3D10%2E10%2E10%2E3`
  - `https://192.168.1.10/investigation/2/navigate/query/service%3D80%20%26%26%20%28ip%2Esrc%3D10%2E10%2E10%`

```
 2E3%20%7C%7C%20ip%2Edst%3D10%2E10%2E10%2E3%29/date/2013-03-
12T17:00:00Z/2013-03-12T17:10:00Z
```

Weitere Hinweise

Einige Werte müssen eventuell nicht als Teil der Abfrage kodiert werden. Zum Beispiel werden normalerweise die IP src und dst für diesen Integrationspunkt verwendet. Wenn zur Integration dieser Funktion eine Drittanbieter-Anwendung genutzt wird, ist es möglich, diese Werte ohne angewandte Codierung zu referenzieren.

Rekonstruieren eines Ereignisses

Beim Anzeigen einer Ereignisliste in der Ansicht „Ereignisse“ können Sie eine Rekonstruktion des Ereignisses in einem lesbaren Format sicher erstellen, das dem Original entspricht. Standardmäßig ist die ursprüngliche Ansicht eines rekonstruierten Ereignisses das geeignetste Format (beste Rekonstruktion). Zum Beispiel wird der Webinhalt als Webseite rekonstruiert und eine Chatunterhaltung wird mit beiden Teilen der Unterhaltung angezeigt. Jeder Benutzer kann in der Ansicht „Profil“ > „Einstellungen“ eine andere Standardrekonstruktion auswählen.

Sie können eine Rekonstruktion auch über die Ansicht „Navigation“ öffnen, wenn Sie die Ereignis-ID des Ereignisses kennen.

In der Rekonstruktion können Sie:

- die anzuzeigenden Ereignisinformationen auswählen Mögliche Werte: Anforderungsdaten, Antwortdaten sowie Anforderungs-und Antwortdaten
- den Rekonstruktionstyp auswählen: Details, Text, Hexadezimalwert, Pakete, Web, E-Mail oder Chat
- Rohdatenprotokolle exportieren
- das Ereignis als PCAP-Datei exportieren
- alle im Ereignis verfügbaren Dateien extrahieren
- Extrahieren Sie alle Metadaten, die dem Ereignis zugeordnet sind.

  Achtung: Lassen Sie Vorsicht walten, wenn Sie in der Rekonstruktion auf einen Link zu einer Datei klicken möchten. Falls in Ihrem System eine Anwendung mit der Datei verknüpft ist oder der Browser die Datei öffnen kann, kann dies negative Auswirkungen auf Ihr System haben, wenn der Anhang schädlichen Code enthält.

- das Ereignis in einem separaten Fenster oder auf einer separaten Registerkarte anzeigen (je nach Browserkonfiguration)
- Wenn Sie die Rekonstruktion als Vorschau in der aktuellen Ansicht anzeigen, können Sie mithilfe der Navigationsschaltflächen unten links zum nächsten Ereignis vor- bzw. zum vorherigen Ereignis zurücknavigieren.

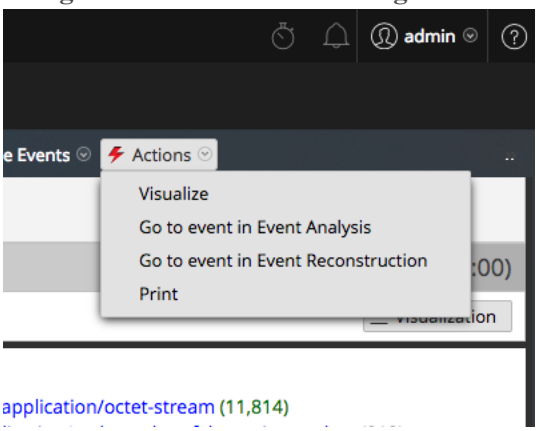
Hinweis: Die Rekonstruktionseinstellungen und die Rekonstruktionscacheeinstellungen ermöglichen es einem Administrator, die Anwendungsperformance für das Modul „Investigation“ zu managen. Da Analysten Sitzungen, über die sie ermitteln, rekonstruieren, können sich zwei Situationen auf Performance und Ergebnisse auswirken.
- Einige Ereignisse können sehr groß sein und Tausende von Quellenpaketen enthalten. Die Rekonstruktion dieser Typen von Sitzungen kann die Anwendungsperformance beeinträchtigen.
-In einigen Fällen kann der Rekonstruktionscache falsche Inhalte darstellen. Aus diesem Grund leert NetWitness Platform alle 24 Stunden den Cache, dessen Daten älter als einen Tag sind. Zwischen den täglichen Cache-Bereinigungen können gewisse Aktionen dazu führen, dass ein nicht mehr gültiger Cache für die Rekonstruktion verwendet wird, und wenn es erforderlich wird, können Administratoren den Cache für einen oder mehrere Services, die mit dem aktuellen NetWitness Server verbunden sind, manuell löschen.

Rekonstruieren eines Ereignisses über die Ansicht „Navigation“

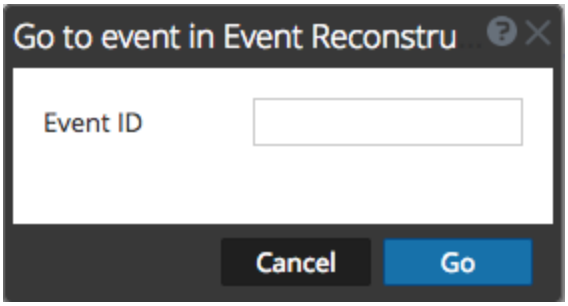
Sie können ein Ereignis direkt über die Ansicht „Navigation“ rekonstruieren, wenn Sie die Ereignis-ID kennen. Sie können diese Option verwenden, ohne eine Abfrage auszuführen, wie Sie das in der Regel bei Beginn einer Ermittlung tun. Sie müssen einen Service und einen Zeitbereich auswählen, um mithilfe der entsprechenden `eventid` direkt zu einem Ereignis zu springen.

So zeigen Sie eine Rekonstruktion oder Ereignisanalyse direkt über die Ansicht „Navigation“ an:

1. Navigieren Sie zu **Ermittlung** > **Navigieren** und wählen Sie **Aktionen** > **In Ereignisanalyse zu Ereignis wechseln** oder **In Ereignisrekonstruktion zu Ereignis wechseln** aus.



   Das Dialogfeld „Zu Ereignis wechseln“ wird angezeigt. Es gibt zwei Dialogfelder: eines für die Ereignisanalyse und eines für die Ereignisrekonstruktion. In beiden werden Sie nach der Ereignis-ID gefragt.

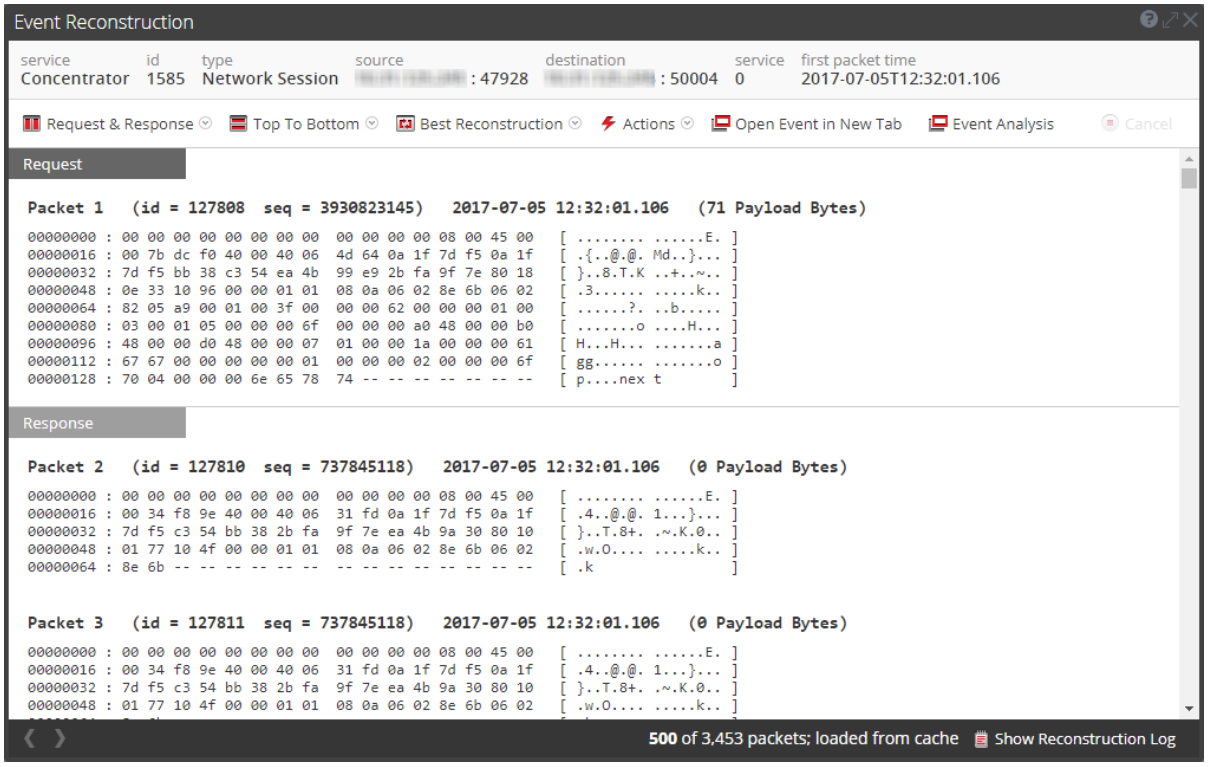


2. Geben Sie im Feld **Ereignis-ID** die ID ein und klicken Sie auf **Los**.
   Das angegebene Ereignis wird in der Ansicht „Ereignisrekonstruktion“ oder in der Ansicht „Ereignisanalyse“ rekonstruiert.

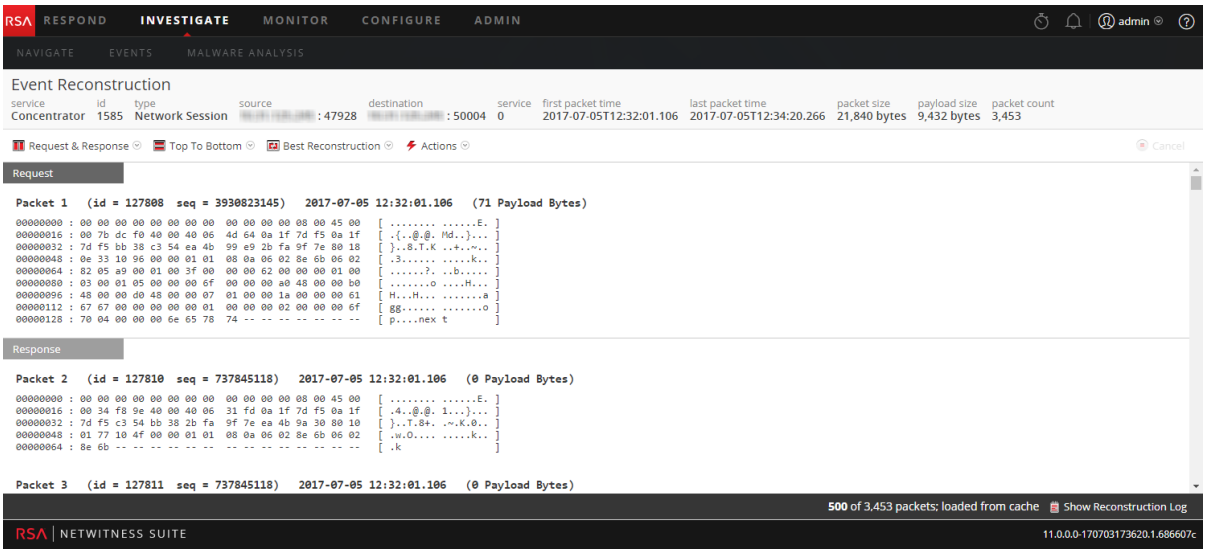
Ein Ereignis von der Ereignisliste wiederherstellen

1. Öffnen Sie einen Drill-down-Punkt in der Ansicht **Ereignisse**.
2. Klicken Sie auf + Show Additional Meta , um alle Metadaten anzuzeigen.
3. Öffnen Sie eine Ereignisrekonstruktion in der aktuellen Ansicht. Wählen Sie dazu ein zu rekonstruierendes Ereignis und dann **Aktionen** > **Ereignis anzeigen** > **Inline-Vorschau** aus.
   Das Dialogfeld „Ereignisrekonstruktion“ wird in der gleichen Ansicht in einem Pop-up-Fenster geöffnet. Standardmäßig wird in NetWitness Platformentweder die beste Rekonstruktion für das

Ereignis in Bezug auf den Ereignisinhalt angezeigt oder die Rekonstruktion, die Sie in der Einstellung „Standardsitzungsansicht“ für das Modul „Investigation“ ausgewählt haben. Über die Optionen in der Symbolleiste „Ereignisrekonstruktion“ können Sie die Rekonstruktionsmethode ändern, Ergebnisse nebeneinander anzeigen, ein Ereignis exportieren, einen E-Mail-Anhang öffnen, Dateien extrahieren und das Ereignis in einer neuen Registerkarte öffnen. Die Optionen der Symbolleiste variieren je nach Typ des zu rekonstruierenden Ereignisses (Netzwerkereignis, Protokollereignis oder Endpunktereignis). Dies ist ein Beispiel für die Rekonstruktion eines Netzwerkereignisses.



4. Um eine Rekonstruktion des nächsten Ereignisses in einer Vorschau anzuzeigen, klicken Sie auf .
   Um eine Rekonstruktion des vorherigen Ereignisses anzuzeigen, klicken Sie auf .
5. Führen Sie einen der folgenden Schritte aus, um eine Ereignisrekonstruktion in einer neuen Registerkarte zu öffnen:
   a. Wählen Sie in der Ansicht **Ereignisse** ein zu rekonstruierendes Ereignis und dann **Aktionen** Ereignis anzeigen **In neuer Registerkarte öffnen** aus.
   b. Klicken Sie auf der Symbolleiste **Ereignisrekonstruktion** der in einer Vorschau angezeigten Rekonstruktion auf **Ereignis in neuer Registerkarte öffnen**.
      Das Dialogfeld „Ereignisrekonstruktion“ wird in einer neuen Registerkarte geöffnet.



Anzeige nebeneinander oder von oben nach unten

So wählen Sie die Methode aus, wie Anforderungen und Antworten für ein Ereignis angezeigt werden:

1. Klicken Sie in der Symbolleiste **Ereignisrekonstruktion** auf **Von oben nach unten** oder **Nebeneinander**.
2. Wählen Sie im Drop-down-Menü die Informationen aus, die Sie im Ereignis sehen möchten: **Nebeneinander** oder **Von oben nach unten.**
   Die Rekonstruktion wird anhand der ausgewählten Informationen aktualisiert.

Auswählen der anzuzeigenden Ereignisinformationen

So wählen Sie aus, welche Ereignisinformationen angezeigt werden sollen:

1. Klicken Sie in der Symbolleiste **Ereignisrekonstruktion** auf **Anforderung und Antwort**.
2. Wählen Sie im Drop-down-Menü die Informationen aus, die Sie im Ereignis sehen möchten: **Anforderung und Antwort**, **Anforderung** oder **Antwort**.
   Die Rekonstruktion wird anhand der ausgewählten Informationen aktualisiert.

Auswählen des Ereignisrekonstruktionstyps

So wählen Sie den Rekonstruktionstyp für ein Ereignis aus:

1. Klicken Sie in der Symbolleiste **Ereignisrekonstruktion** auf **Beste Rekonstruktion**.
2. Wählen Sie in dem Drop-down-Menü den anzuzeigenden Rekonstruktionstyp aus: **Meta**, **Text**, **Hex**, **Pakete**, **Web**, **E-Mail** oder **Dateien**.
   Die Rekonstruktion wird anhand des ausgewählten Rekonstruktionstyps aktualisiert.

Öffnen oder Herunterladen eines E-Mail-Anhangs

Wenn Sie eine Rekonstruktion einer E-Mail mit Anhängen anzeigen, können Sie unterstützte Dateitypen öffnen oder die Dateien in das lokale System herunterladen.

Achtung: Lassen Sie beim Auswählen von Dateianhängen Vorsicht walten. Falls in Ihrem System eine Anwendung mit dem Dateianhang verknüpft ist oder der Browser die Datei öffnen kann, kann dies negative Auswirkungen auf Ihr System haben, wenn der Anhang schädlichen Code enthält.

So öffnen oder downloaden Sie E-Mail-Anhänge:

1. Klicken Sie auf der Symbolleiste **Ereignisrekonstruktion** auf das Drop-down-Menü **Ansicht** und wählen Sie **E-Mail anzeigen** aus.
   Die Ereignisrekonstruktion wird angezeigt.
2. Klicken Sie im Bereich **Ereignisrekonstruktion** der E-Mail auf den Anhang.
   Sofern der Browser den Dateityp unterstützt, wird der Anhang in einer neuen Registerkarte geöffnet.
   Falls der Dateityp nicht unterstützt wird, öffnet sich das Downloaddialogfenster, über das Sie den Anhang herunterladen können.

Exportieren eines Ereignisses als PCAP-Datei

Mit der PCAP-Exportoption werden die Sitzungen für den aktuellen Zeitraum und Drill-down-Punkt in eine PCAP-Datei heruntergeladen. So exportieren Sie ein Ereignis als PCAP-Datei:

1. Klicken Sie in der Symbolleiste **Ereignisrekonstruktion** auf **Aktionen**.
2. Klicken Sie auf **PCAP exportieren**.
3. Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **OK**.
   Der Job wird geplant und nach Abschluss wird die PCAP-Datei in das lokale Dateisystem heruntergeladen. Die PCAP-Datei können auf der Registerkarte „Profil > Jobs“ heruntergeladen werden.

Extrahieren von Dateien aus einem rekonstruierten Ereignis

Mit der Option „Dateien extrahieren“ werden die mit dem Ereignis verknüpften Dateien extrahiert und heruntergeladen. So extrahieren Sie Dateien:

1. Klicken Sie in der Symbolleiste **Ereignisrekonstruktion** auf **Aktionen**.
2. Klicken Sie auf **Dateien extrahieren**.
   Das Dialogfeld „Dateiextraktion“ wird geöffnet.
3. Wählen Sie die Typen der zu extrahierenden Dateien aus und klicken Sie auf **OK**.
4. Der Job wird geplant und nach Abschluss werden die ausgewählten Dateitypen in das lokale Dateisystem heruntergeladen. Die Dateien können auf der Registerkarte „Profil > Jobs“ heruntergeladen werden.

Analysieren von Raw-Ereignissen und Metadaten in der Ansicht „Ereignisanalyse“

Raw-Ereignisse und Daten in der gleichen Ansicht zu analysieren ist möglich, wenn Sie in der Ansicht „Ereignisanalyse“ arbeiten. Nachdem Sie Rekonstruktionstypen in der Ansicht „Ereignisanalyse“ verstanden haben, können Sie Folgendes tun:

- Filtern von Ergebnissen in der Ansicht „Ereignisanalyse“
- Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“
- Suchen von zusätzlichem Kontext in der Ansicht „Ereignisanalyse“
- Herunterladen von Daten in der Ansicht „Ereignisanalyse“
- Reagieren auf Daten in der Ansicht „Ereignisanalyse“

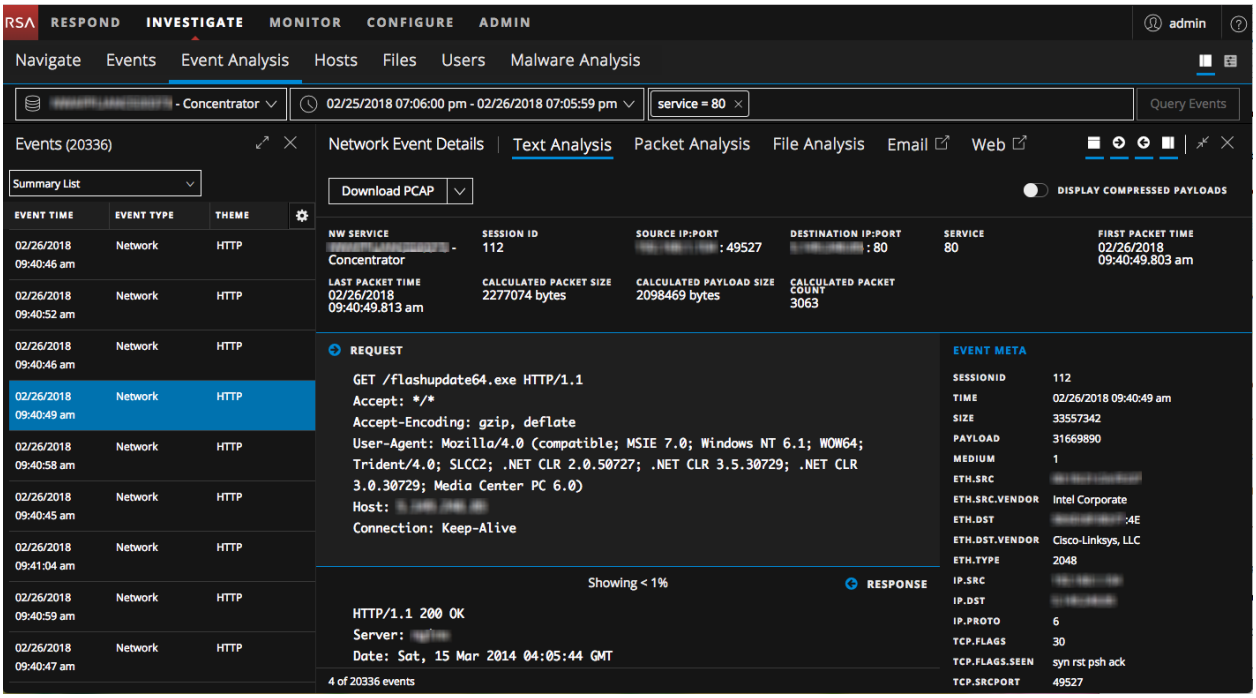
Rekonstruktionstypen in der Ansicht „Ereignisanalyse“

Bei der Suche nach möglichen Bedrohungen in erfassten Netzwerkdaten können Sie Drill-downs an verschiedenen interessanten Punkten in den Daten durchführen. Wenn eine Sitzung verdächtige Ereignisse enthält, können Sie die Liste der Ereignisse für die Sitzung untersuchen und auch eine Rekonstruktion des Ereignisses mit Funktionen zur Mustererkennung sicher anzeigen. (Unter Starten einer Ermittlung finden Sie die verschiedenen Methoden zum Aufrufen der Ansicht „Ereignisanalyse“.)

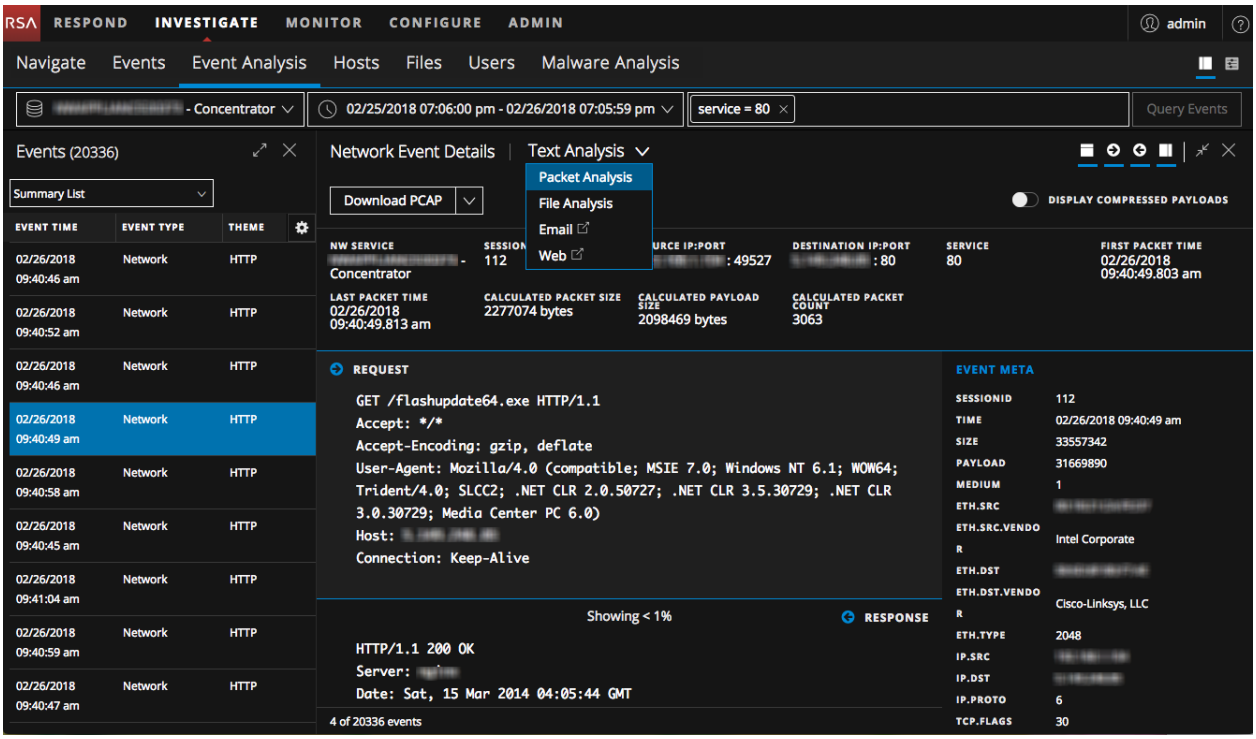
Hinweis: Wenn Sie Ereignisse in einem Service der Version 10.6.x oder 11.0.0.x von einem NetWitness-Server der Version 11.1 oder 11.2 aus untersuchen, variiert das Downloadverhalten in der Ansicht „Ereignisanalyse“ für Dateien, PCAP-Dateien, Protokolle, Nutzdaten und Metawerte. Möglicherweise wird eine Ereignisnutzlast in einem 10.6.x- oder 11.0.0.x-Service angezeigt, für den Sie keine Berechtigung haben, aber Sie werden nicht in der Lage sein, Dateien oder Nutzlasten herunterzuladen.

In der Ansicht „Ereignisanalyse“ können Sie das Format für die Rekonstruktion auswählen: Paketanalyse, Dateianalyse oder Textanalyse, **E-Mail** (Version 11.1 oder höher) und **Web** (Version 11.1 oder höher). Wenn der Metaschlüssel `medium` ein Ereignis als Protokollereignis oder Endpunktereignis markiert, ist nur die Textanalyse verfügbar. Die Standardrekonstruktion für Netzwerkereignisse ist Textanalyse. Jedoch überschreibt bei einem Netzwerkereignis das zuletzt geöffnete Rekonstruktionsformat die Standardeinstellung. Mithilfe der E-Mail-und Webrekonstruktion wird das Ereignis in der Ansicht „Ereignisanalyse“ geöffnet und in „Auswählen des Typs der Ereignisanalyse“ in Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“ beschrieben.

Diese Abbildung ist ein Beispiel für den Bereich „Netzwerkereignisdetails: Textanalyse“ in einem Webbrowserfenster, das so breit ist, dass die Optionen für das Rekonstruktionsformat in einer Zeile angezeigt werden können.



Wenn das Browserfenster zu schmal ist, um alle Ansichtsoptionen horizontal anzuzeigen, werden die Optionen in einer Drop-down-Liste aufgeführt.



Innerhalb jeder Analyseart sind Einstellungen für die Optimierung Ihrer Analyse verfügbar. Wenn Sie eine Einstellung ändern, wird die Einstellung zwischen Browseraktualisierungen und Anmeldungen im selben Browser beibehalten. Dies sind die beibehaltenen Einstellungen:

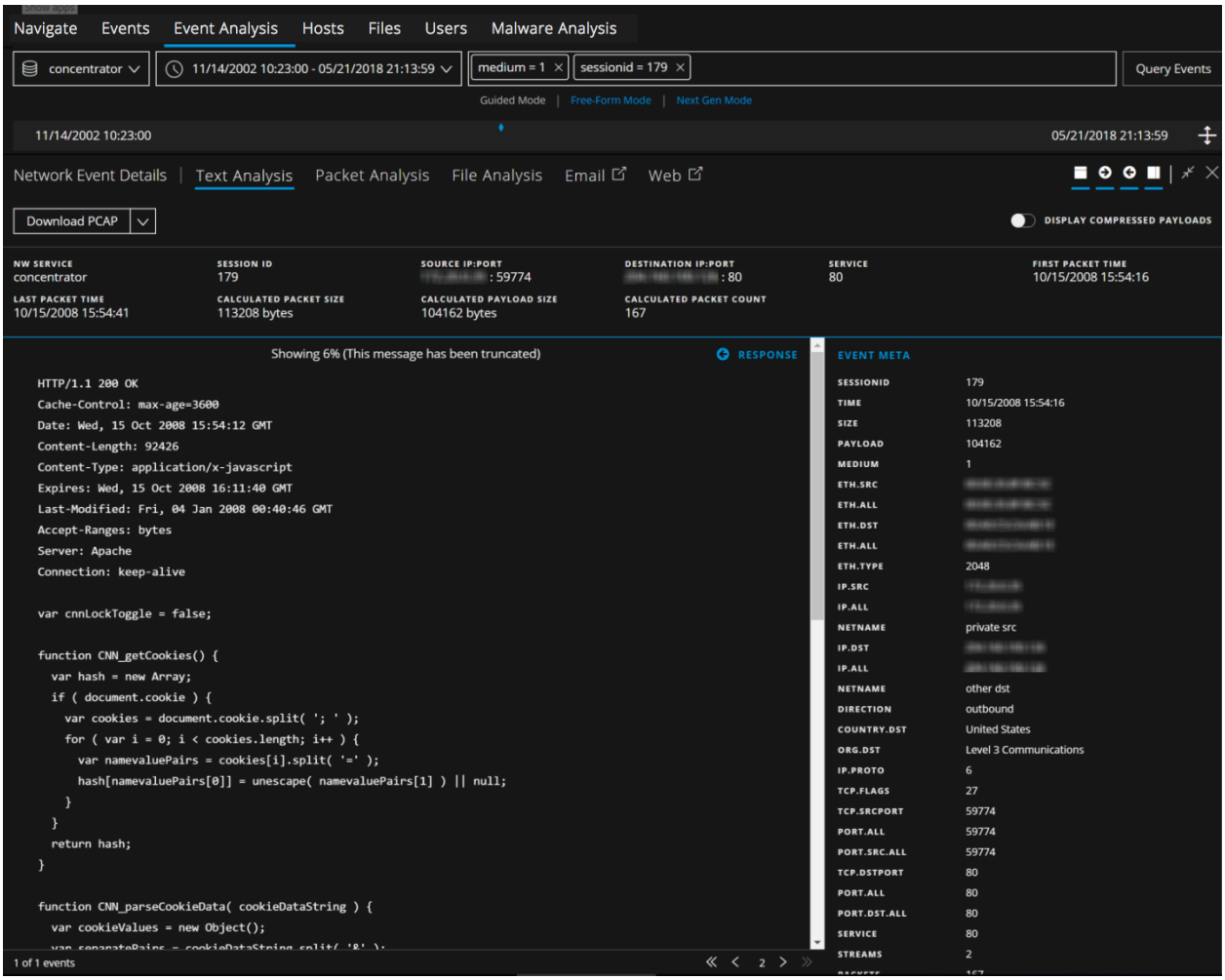
- Die aktuell ausgewählte Rekonstruktion: Textanalyse, Paketanalyse oder Dateianalyse.
- Ob der Bereich „Ereignis-Metadaten“ offen oder geschlossen ist.
- Ob der Ereignis-Header offen oder geschlossen ist.
- Ob die Anforderung oder die Antwort oder beide angezeigt werden.
- Ob Paketnutzlasten im Bereich Paketanalyse angezeigt werden.
- Ob schattierte Byte im Bereich Paketanalyse angezeigt werden.
- Ob andere gängige Dateitypen im Bereich Paketanalyse hervorgehoben sind.
- Die Anzahl der Pakete pro Seite im Paketanalyse-Bereich.
- Ob komprimierter oder unkomprimierter Text im Bereich „Textanalyse“ angezeigt wird.
- Die Textdekodierungseinstellung im Bereich „Textanalyse“ eines Netzwerkereignisses.

Der Bereich „Textanalyse“

Sie können alle Arten von Ereignissen (Netzwerkereignisse, Protokollereignisse und Endpunktereignisse) in ihrem ursprünglichen Textformat im Bereich Textanalyse anzeigen. Seitenumbruchhilfen erhöhen die Flexibilität bei der Paginierung des rekonstruierten Textes eines Ereignisses.

Hinweis: Endpunktereignisse sind für Ermittlungen in Version 11.1 und höher verfügbar. Die Seitenumbruchhilfen sind in der Version 11.2 und höher verfügbar.

Der Bereich Textanalyse für einige Netzwerkereignisse kann sehr groß sein. Zur optimalen Darstellung und bessern Passfähigkeit werden große Nutzdaten abgeschnitten. Wenn eine einzelne rekonstruierte Anfrage oder Antwort im rekonstruierten Ereignis die maximale Anzahl von Bytes überschreitet, zeigt der Header an, dass die Nachricht abgeschnitten wurde. In dieser Abbildung ist eine einzige gekürzte Antwort dargestellt, weil sie die maximale Anzahl von Bytes überschreitet (Version 11.2).



In Version 11.1 werden große Nutzdaten anders behandelt. Die Nutzdaten für ein einzelnes Ereignis sind auf 2500 Pakete begrenzt. Wenn das Paketlimit erreicht ist, weist eine Warnung in der Fußzeile darauf hin, dass das Limit erreicht ist, und zeigt die Gesamtzahl der Pakete im Ereignis an. In dieser Abbildung werden Kurzinformationen dargestellt, die angezeigt werden, wenn Sie den Mauszeiger über die Warnung bewegen.

Hinweis: Die Option „Mehr anzeigen“ ist weiterhin für gekürzte Nachrichten verfügbar. Allerdings ist der gesamte Text der Nachricht ohne Herunterladen der Nutzdaten nicht sichtbar.

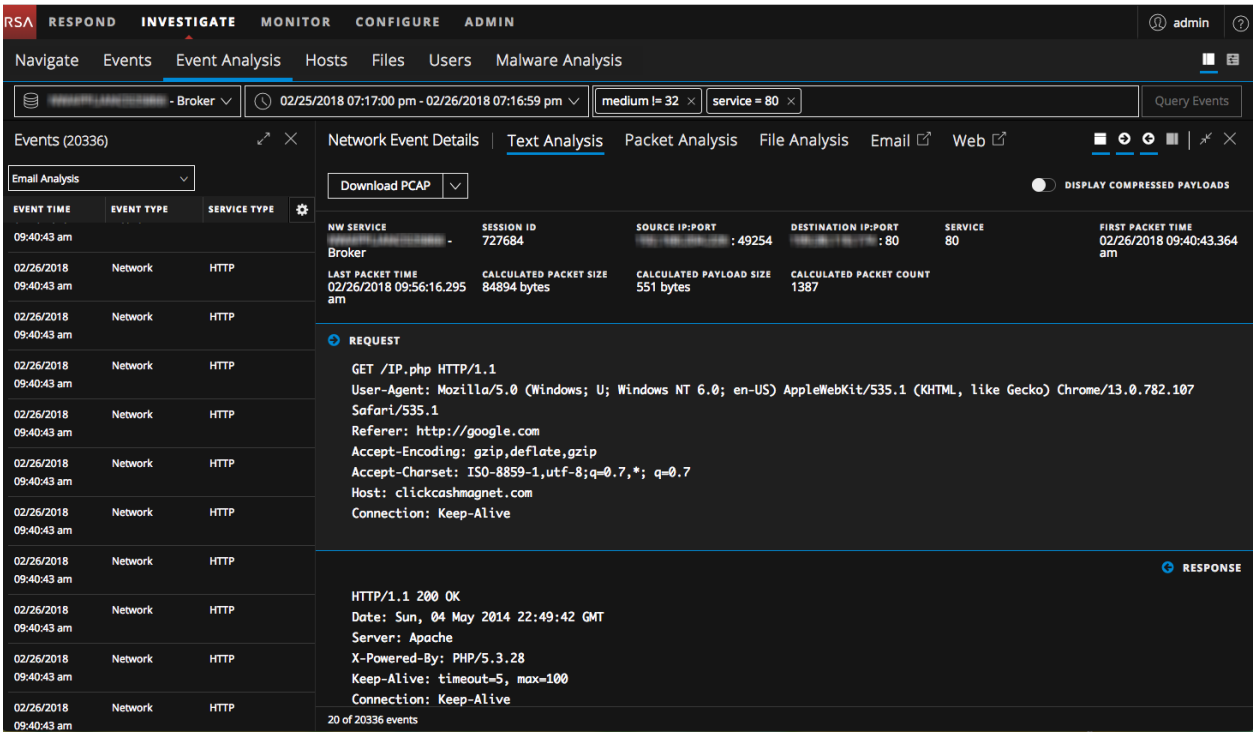
Im Bereich Textanalyse werden Netzwerkereignisse, Protokollereignisse und Endpunktereignisse unterschiedlich angezeigt.

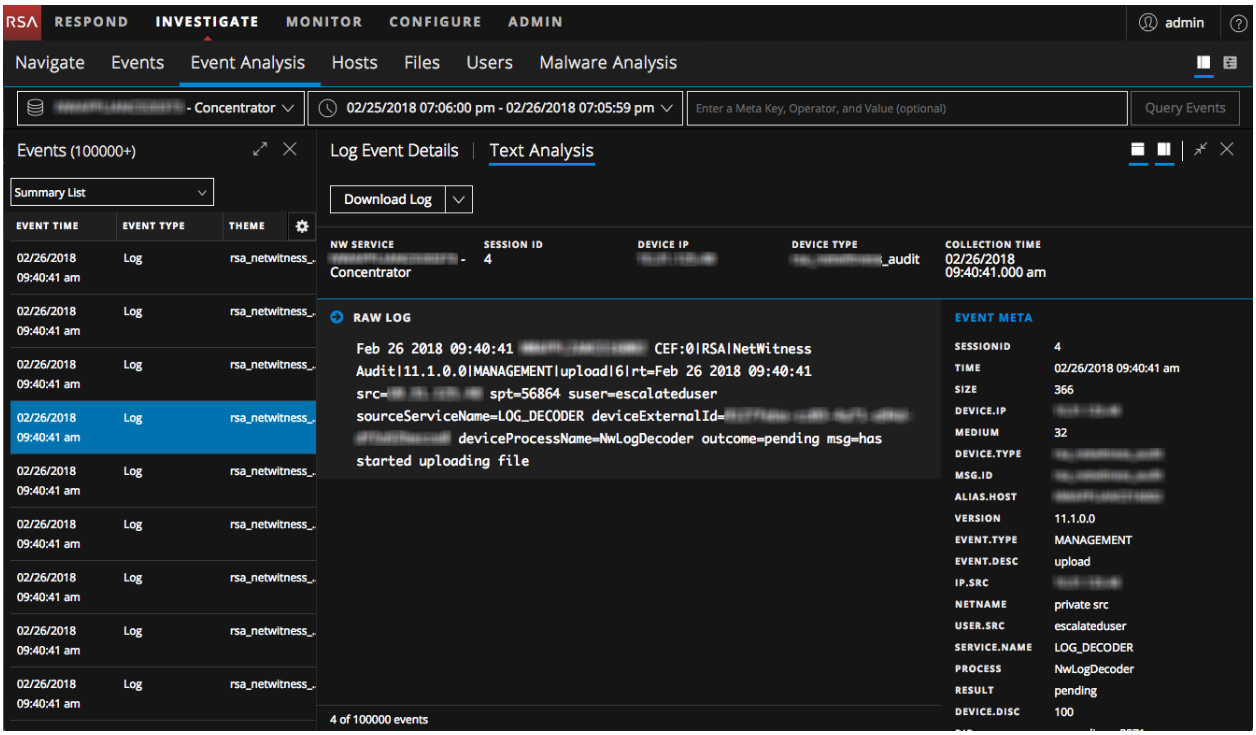
- Für Netzwerkereignisse stellt Investigate die Richtung des Pakets (Anforderung oder Antwort) und die Inhalte jedes Pakets im Textformat bereit. Wenn Sie ein Netzwerkereignis rekonstruieren, ist der BereichTextanalyse scrollbar. Wenn Sie einen Bildlauf durchführen, bleiben die Informationen zur Identifizierung des Texts sowie die Anforderungs- und Antwortbezeichnungen sichtbar, anstatt dass aus der Ansicht herausgescrollt wird.
- Protokollereignisse und Endpunktereignisse haben keine Anforderung oder Antwort. Nur das Rohereignis wird im Bereich Textanalyse angezeigt.

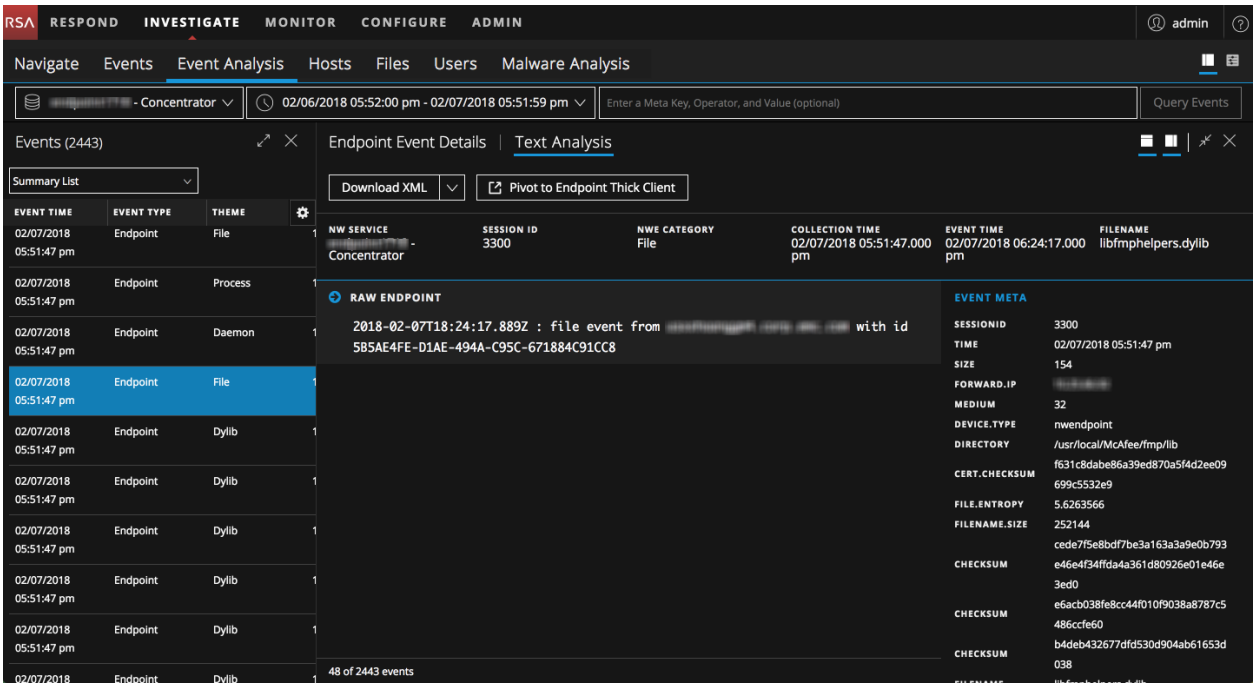
Für jeden Ereignistyp (Netzwerk, Protokoll oder Endpunkt) gibt es einige Unterschiede:

- Der Ereignis-Header enthält Informationen, die für jede Art von Ereignis relevant sind.
- Es gibt verschiedene Optionen für den Export.

Unten finden Sie ein Beispiel für den Bereich „Textanalyse“ für jede Art von Ereignis, ein Netzwerkereignis, ein Protokollereignis und ein Endpunktereignis.



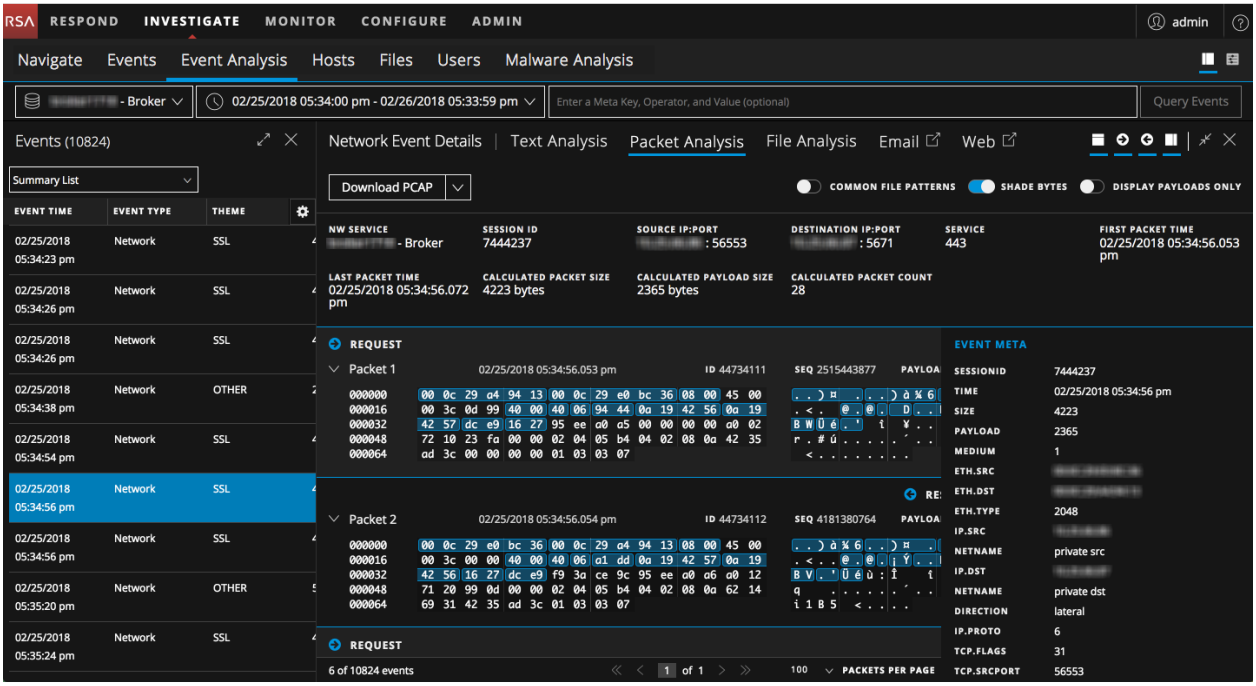




Hinweis: Die berechnete Paketanzahl, berechnete Paketgröße und berechnete Nutzdatengröße im Ereignis-Header kann sich von derselben Statistik im Bereich „Ereignis-Metadaten“ unterscheiden, da die Metadaten gelegentlich bereits vor Abschluss der Ereignisanalyse geschrieben werden und daher duplizierte Pakete enthalten können.

Der Bereich „Paketanalyse“

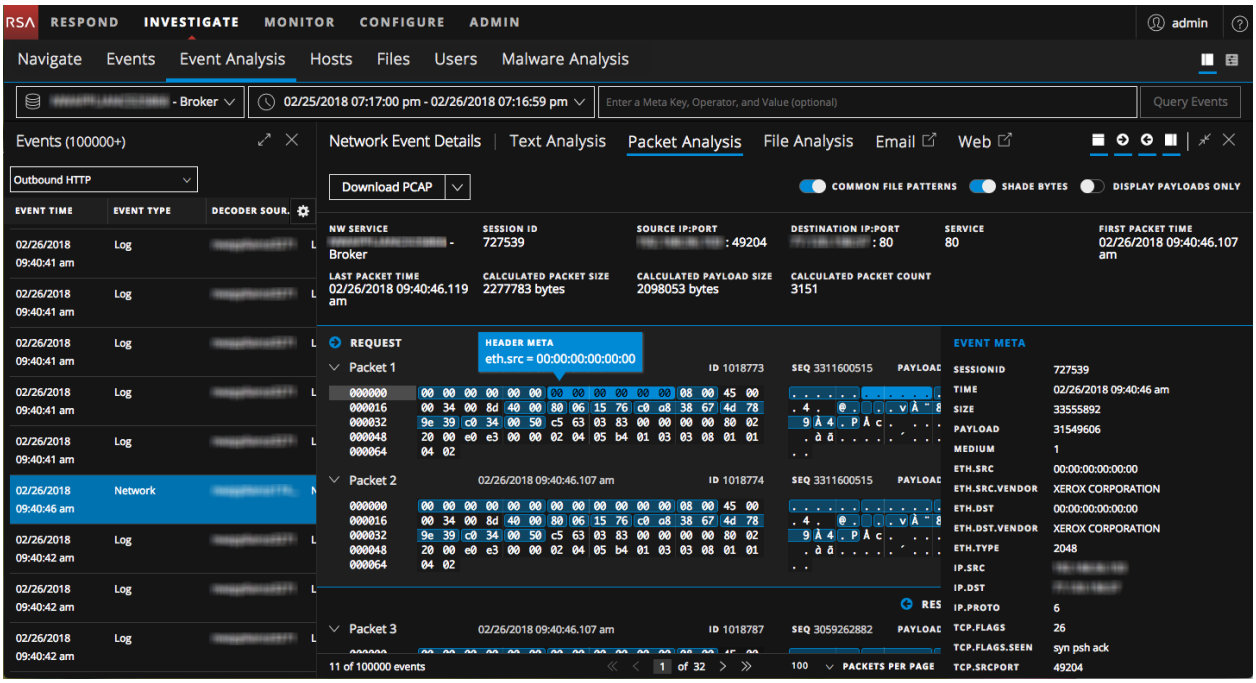
Der Bereich Paketanalyse ist nur für Netzwerkereignisse bestimmt. Der Bereich Paketanalyse ist scrollbar und die Informationen zur Identifizierung des Pakets sowie die Anforderungs- und Antwortbezeichnungen bleiben sichtbar, anstatt dass aus der Ansicht herausgescrollt wird.



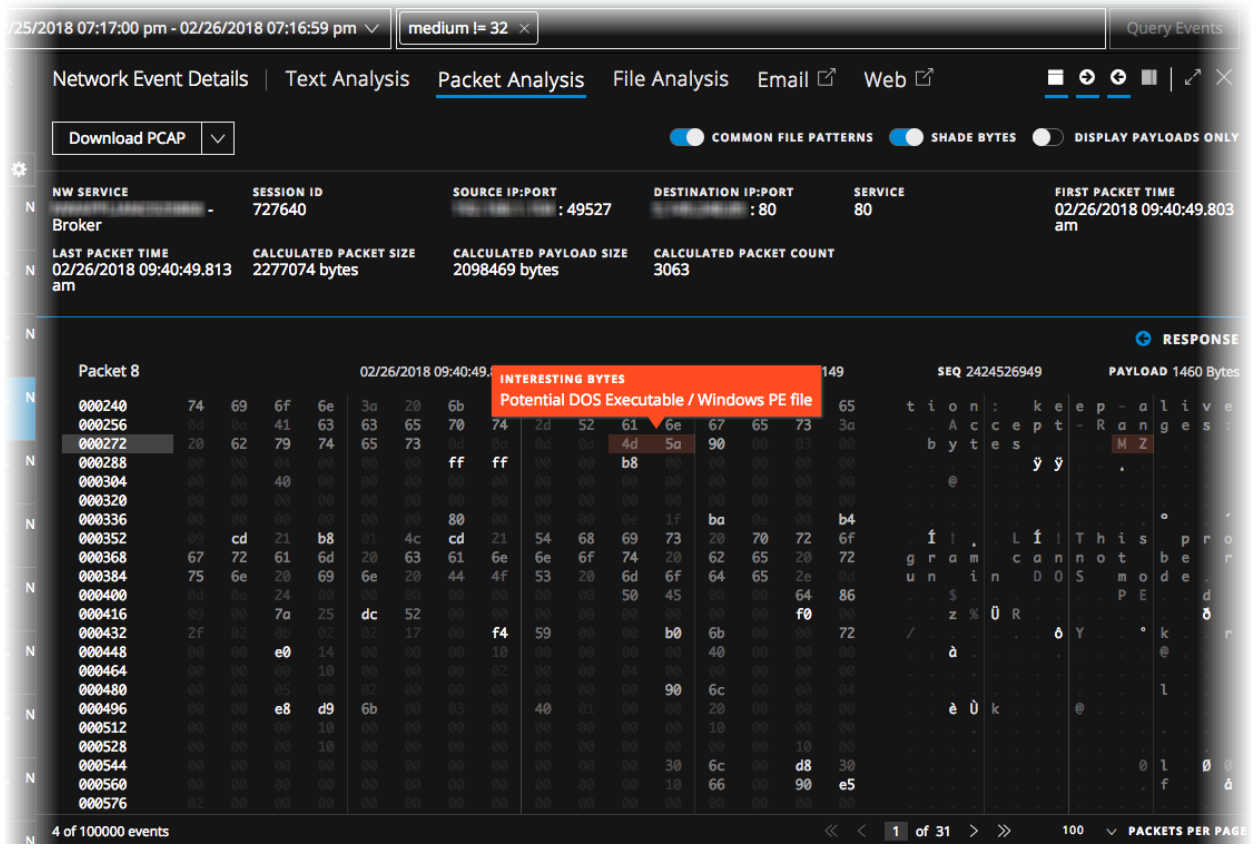
Im Bereich Paketanalyse geben die Überschriften die Richtung des Pakets (Anforderung oder Antwort), die Anzahl der Pakete, die Startzeit des Pakets, die Paket-ID und die Reihenfolge sowie die Nutzlastgröße an. Alle Pakete beginnen mit einer Kopfzeile und einige Pakete haben eine Fußzeile. Einige Pakete haben eine Nutzlast.

In Version 11.1 bieten Seitenumbruchshilfen zusätzliche Flexibilität beim Blättern durch Pakete.

Die Metadaten in den Hexadezimal- und ASCII-Daten sind blau hervorgehoben. Wenn Sie den Cursor über den hervorgehobenen Metadaten platzieren, werden die Metaschlüssel-/Metawertinformationen in einem Kasten mit Hover-Effekt angezeigt.

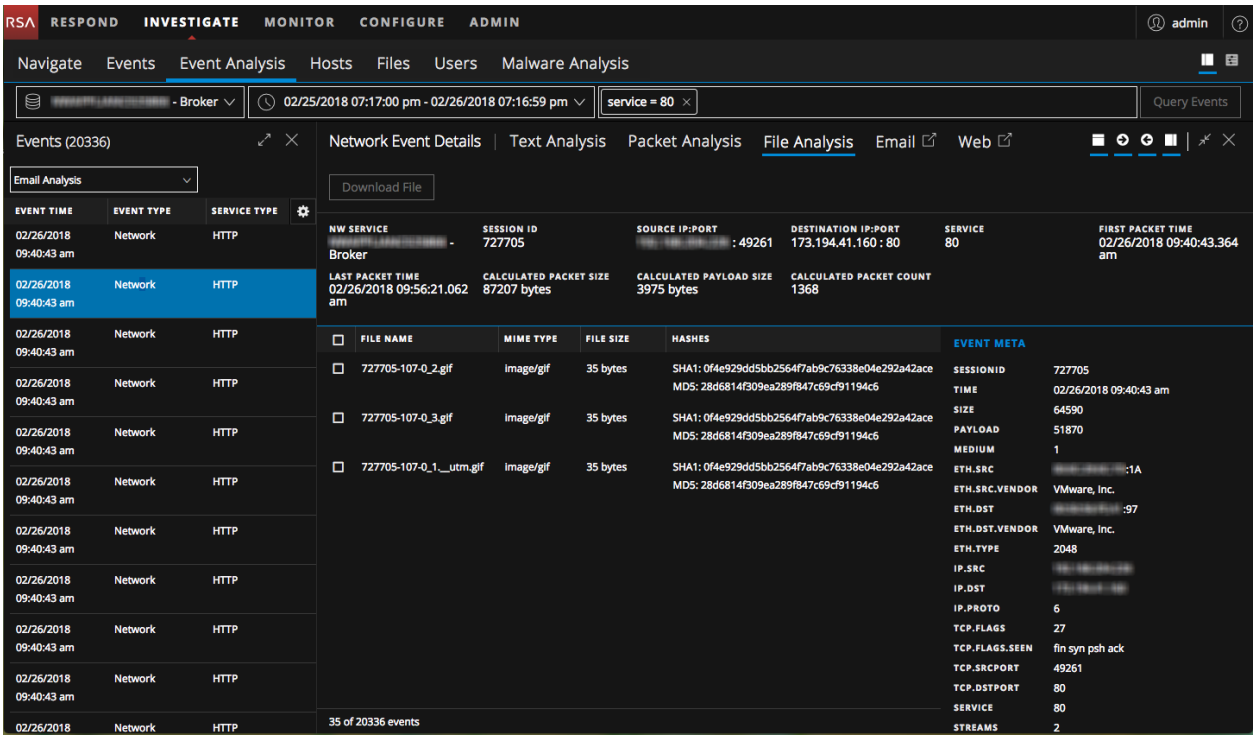


Gebräuchliche Dateisignaturen sind mit einem orangefarbenen Hintergrund hervorgehoben. Wenn Sie den Cursor über den hervorgehobenen Text bewegen, wird die Beschreibung des Dateityps in einem Kasten mit Hover-Effekt angezeigt.

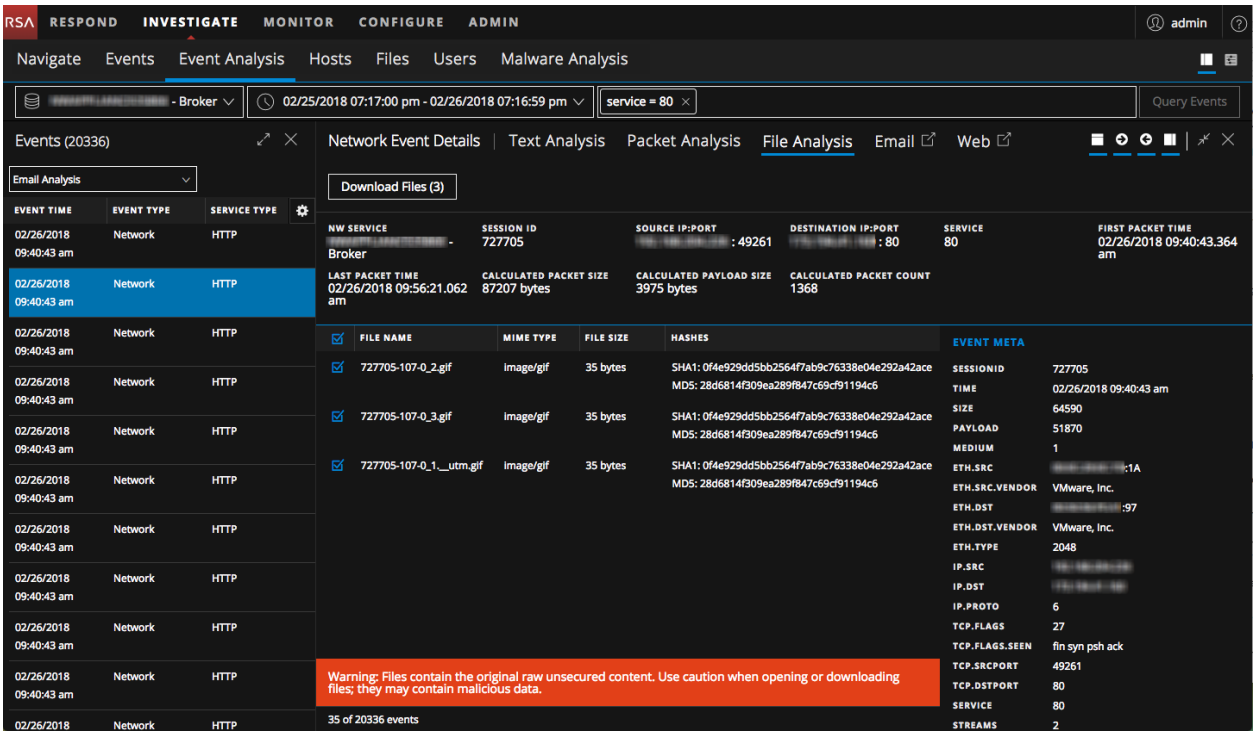


Der Bereich „Dateianalyse“

Der Bereich Dateianalyse zeigt eine Liste der Dateien, die mit dem ausgewählten Netzwerkereignis verknüpft sind. Dies ist ein Beispiel für den Bereich Dateianalyse.



Sie können eine Datei, mehrere Dateien oder alle Dateien für den Export in Ihr lokales Dateisystem auswählen. Wenn Dateien ausgewählt sind, wird die Schaltfläche „Dateien exportieren“ aktiviert, auf der die Anzahl der ausgewählten Dateien angezeigt wird.



Achtung: Beim Entpacken und Öffnen von Dateien, die mit einer Standardanwendung verknüpft sind, ist Vorsicht geboten; beispielsweise könnte eine Excel-Tabelle automatisch in Excel geöffnet werden, bevor Sie überprüfen konnten, ob sie sicher ist.

Analysetools für jede Art von Ereignisanalyse

Die Analysetools in der Ansicht „Ereignisanalyse“ sollen Analysten dabei unterstützen, die relevanten Informationen für verschiedene Arten von Ereignissen (Netzwerkereignis, Protokollereignis und Endpunktereignis) zu finden. In dieser Tabelle werden die Aktionen aufgeführt, die Sie nach Ereignistyp ergreifen können. Der Rest dieses Abschnitts enthält Verfahren zur Durchführung der Aktionen.

Aktion	Netzwerkereignis	Ereignis protokollieren	Endpunktereignis
Anzeigen des Bereichs „Textanalyse“	✓	✓	✓
Anzeigen des Bereichs „Dateianalyse“	✓		
Anzeigen des Bereichs „Paketanalyse“	✓		
Öffnen, Schließen und Anpassen der Größe der Bereiche	✓	✓	✓
Anpassen der Anzeige von Anforderungen und Antworten	✓		

Aktion	Netzwerkereignis	Ereignis protokollieren	Endpunktereignis
Anzeigen oder Ausblenden des Ereignis-Headers im Bereich „Textanalyse“	✓	✓	✓
Erweitern abgeschnittener Texteinträge im Bereich „Textanalyse“	✓		
Wechseln zwischen einer komprimierten und dekomprimierten Ansicht der Nutzlasten im Bereich „Textanalyse“	✓		
Anzeigen hervorgehobener Bytes im Bereich „Paketanalyse“	✓		
Hervorheben gängiger Dateitypen im Bereich „Paketanalyse“	✓		
Anzeigen nur der Nutzlast im Bereich „Paketanalyse“	✓		
Schattieren von Bytes im Bereich „Paketanalyse“ beim Anzeigen nur der Nutzlast	✓		
Durchführen von URL- und Base64-Codierung und -Decodierung im Bereich „Textanalyse“	✓		
Anzeigen von dekomprimiertem Text für eine HTTP-Netzwerksitzung im Bereich „Textanalyse“	✓		
Anzeigen von Ereignismetadaten für ein Ereignis im Bereich „Textanalyse“	✓	✓	✓
Herunterladen eines Netzwerkereignisses (als PCAP-Datei, nur Nutzlast, nur Anforderung oder nur Antwort) im Bereich „Paketanalyse“ oder im Bereich „Textanalyse“	✓		
Exportieren von Dateien aus einem Netzwerkereignis im Bereich „Dateianalyse“	✓		

Aktion	Netzwerkereignis	Ereignis protokollieren	Endpunktereignis
Herunterladen der Datei für ein Protokollereignis im Bereich „Textanalyse“		✓	
Herunterladen der Datei für ein Endpunktereignis im Bereich „Textanalyse“			✓
Öffnen des aktuellen Endpunktereignisses im Bereich „Textanalyse“			✓

Filtern von Ergebnissen in der Ansicht „Ereignisanalyse“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

In NetWitness PlatformVersion 11.0 senden Sie eine Abfrage in der Ansicht „Navigation“ oder der Ansicht „Ereignisse“ und wenn Sie zur Ansicht „Ereignisanalyse“ wechseln, zeigt eine schreibgeschützte Brotkrümelnavigation die eingereichte Abfrage an. Sie müssen zur Ansicht „Ereignisse“ oder zur Ansicht „Navigation“ zurückkehren, wenn Sie eine andere Abfrage eingeben möchten.

In Version 11.1 oder höher füllt eine Abfrageerstellung die interaktive Brotkrümelnavigation in der Ansicht „Ereignisanalyse“ auf, sodass Sie jeden `<meta key> <operator> <meta value>`-Filter in der Brotkrümelnavigation erstellen und bearbeiten können. Darüber hinaus können Sie einen anderen Service und Zeitbereich auswählen, ohne zur Ansicht „Navigation“ oder „Ereignisse“ zurückzukehren. Der Rest dieses Abschnitts enthält Informationen zur Verwendung der Funktionen der Abfrageerstellung.

Funktionsweise der Brotkrümelnavigation

Wenn Sie in Investigate auf die Option „Ereignisanalyse“ klicken, um die Ansicht zu öffnen, wird die Service- und Zeitbereichsauswahl angezeigt. Standardmäßig ist der erste Service automatisch ausgewählt (es sei denn, Sie haben zuvor einen Service ausgewählt und der ausgewählte Service befindet sich im Browser). Wenn Sie keinen Zeitbereich auswählen, wird der Standardzeitbereich (3 Stunden) verwendet. Das Abfrageerstellungsfeld ist ein leeres Feld rechts neben dem Zeitbereich.

Wenn Sie die Ansicht „Ereignisanalyse“ über die Ansicht „Ereignisse“ oder die Ansicht „Navigation“ öffnen, werden der Service, der Zeitbereich und alle Filter, die in der Ansicht „Ereignisse“ oder der Ansicht „Navigation“ ausgewählt wurden, in der Brotkrümelnavigation angezeigt. Der Service, der Zeitbereich und die einzelnen Filter können geändert werden.

Ab Version 11.2 können fortgeschrittene Analysten zusätzlich zum Erstellen einer Frage im geleiteten Modus eine Abfrage im Freitextmodus eingeben. Der Standardmodus ist der geleitete Modus. Er enthält Optionen für automatische Vorschläge und Validierung. Im Freitextmodus können Sie eine komplexe Frage eingeben. Die Validierung erfolgt, wenn Sie die Abfrage ausführen.

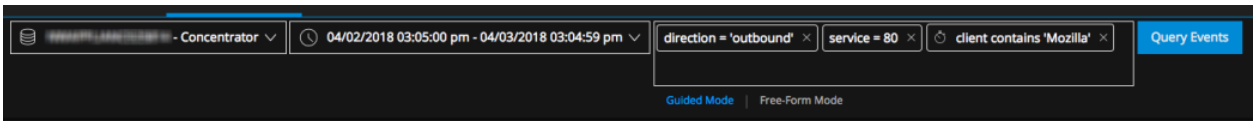
Hinweis: Eine komplexe Abfrage ist jede andere Abfrage als ein grundlegender Filter aus <Metaschlüssel> <Operator> <Wert>, der die Operatoren `()`, `||`, `&&`, `length` oder `regex` enthält.

Mithilfe von zwei Schaltflächen wechseln Sie zwischen den Modi und platzieren einen Cursor in der Abfrageleiste, sodass Sie direkt mit der Erstellung der Abfrage beginnen können. Wenn Sie bei der letzten Verwendung den Freitextmodus ausgewählt haben, ist diese Auswahl bei der nächsten Anmeldung noch aktiv.

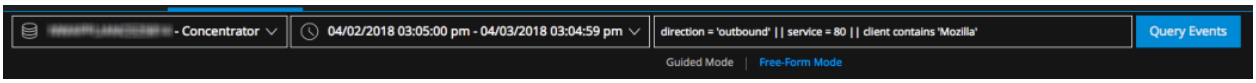
- Wenn Sie vom geleiteten Modus in den Freitextmodus wechseln, werden die im geleiteten Modus erstellten Filter auf eine Textabfrage im Feld „Freitext“ übertragen.
- Wenn Sie vom Freitextmodus in den geleiteten Modus wechseln, wird die von Ihnen eingegebene Abfrage der Abfrageerstellung als einzelner, nicht bearbeitbarer Filter hinzugefügt.

- Wenn Sie mit dem Erstellen einer Abfrage mit mehreren Filtern im geleiteten Mode beginnen, dann in den Freitextmodus und ohne Änderungen wieder zurück zum geleiteten Modus wechseln, behalten die Mehrfachfilter den gleichen Status.

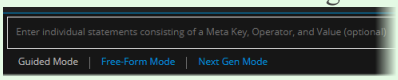
In der folgenden Abbildung ist ein Beispiel für die Ansicht „Ereignisanalyse“ mit aktiver Abfrageerstellung im geleiteten Modus dargestellt.



In der folgenden Abbildung ist ein Beispiel für die Abfrageerstellung im Freitextmodus dargestellt.

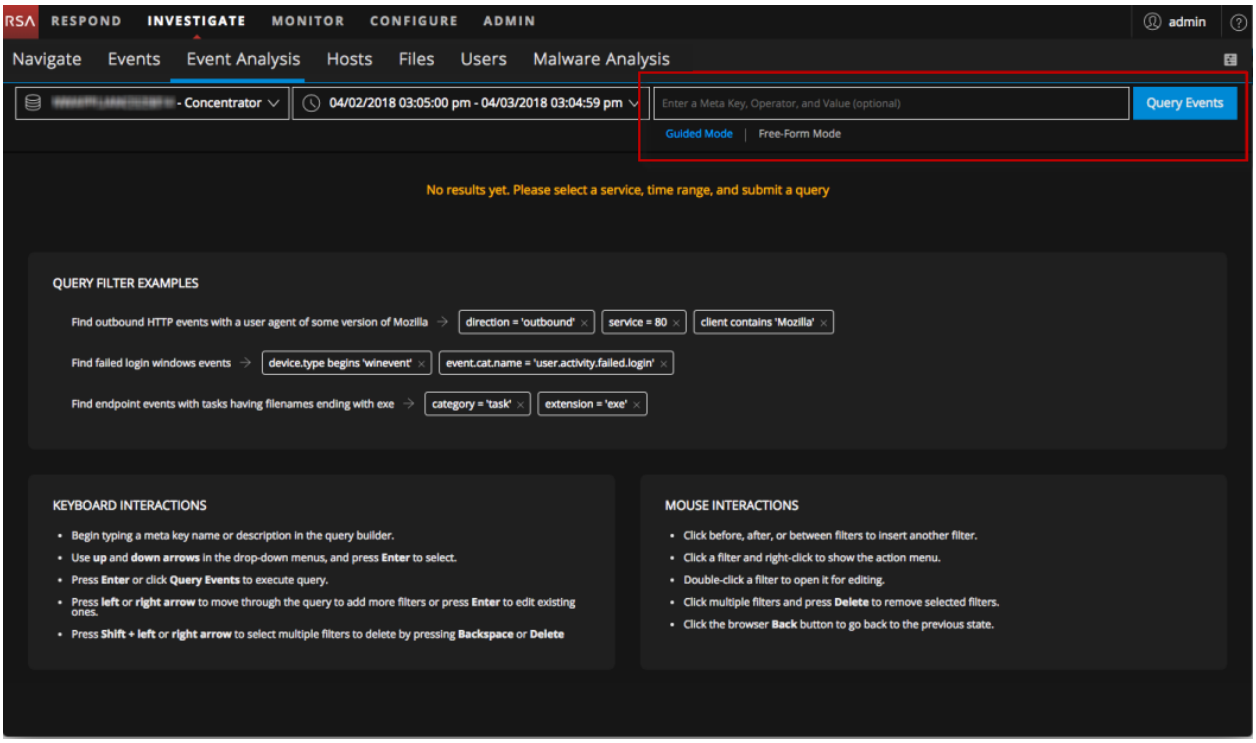


Hinweis: Version 11.2 enthielt eine undokumentierte Beta-Funktion, den sogenannten NextGen-Modus, in der Abfrageerstellung der Ansicht „Ereignisanalyse“, der noch entwickelt und getestet wurde. Der NextGen-Modus wurde im Patch 11.2.0.1 deaktiviert. Wenn der NextGen-Modus angezeigt wird, sollten Sie ihn nicht verwenden. Verwenden Sie nur den geleiteten oder den Freitextmodus in der Abfrageerstellung, um konsistente und vorhersagbare Ergebnisse zu erzielen.



Abfrageerstellung im geleiteten Modus

Der geleitete Modus ist der einfachste Weg, mit dem Analysten gültige Abfragen mit Funktionen für die Eingabe erstellen können. In der folgenden Abbildung ist die ursprüngliche Ansicht „Ereignisanalyse“ mit aktiver Abfrageerstellung im geleiteten Modus dargestellt.



Hinweis: Der geleitete Modus für die Abfrageerstellung unterstützt nur einfache Filter im Format `<meta key><operator><meta value>`. Wenn die Ansicht „Ereignisse“ oder die Ansicht „Navigation“ über einen Filter mit mehr als einem Operator, `not`, `>`, `<`, `<=`, `>=`, `||`, `&&`, `()`, `REGEX` oder `LENGTH` verfügt, wird der Filter hinzugefügt. Eine Bearbeitung wird in der Ansicht „Ereignisanalyse“ allerdings nicht unterstützt. Gleiches gilt für einen Filter aus der Abfrageerstellung im Freitextmodus.

Wenn Sie Filter in der Abfrageerstellung im geleiteten Modus erstellen, wird die Brotkrümelnavigation mit jedem Filter in einem bearbeitbaren Feld aktualisiert. Wenn Sie die Abfrage übermitteln, werden alle Filter mit UND verknüpft, um Ergebnisse zu erzeugen. Die Abfrage wird erst übermittelt, wenn Sie auf „Ereignisse abfragen“ klicken. Filter werden von links nach rechts in der Reihenfolge aufgelistet, in der sie erstellt wurden. Jeder Filter ist ein einfacher Ausdruck des Formats `<meta key> <operator> <optional value>`. Wenn weitere Filter hinzugefügt werden und sie nicht in einer einzelnen Zeile angezeigt werden können, werden sie in eine andere Zeile umgebrochen und der Eingabebereich wird vertikal erweitert, sodass alle Filter ohne Bildlauf nach rechts sichtbar sind.

Beim Erstellen und Bearbeiten von Filtern werden Sie mit Vorschlägen für Autovervollständigung unterstützt, die nur gültige Metaschlüssel und Operatoren in der Drop-down-Liste anzeigen. Sie können Daten eingeben oder aus der Drop-down-Liste auswählen. In der Drop-down-Liste sind Vorgänge, deren Ausführung länger dauert, mit einem Stoppuhrsymbol markiert. Ungültige Filter sind durch einen roten Rahmen gekennzeichnet und wenn Sie den Mauszeiger über den Filter bewegen, wird eine Kurzinformation mit einer Erläuterung des Fehlers angezeigt.

Die Schaltfläche „Ereignisse abfragen“ befindet sich rechts neben der Brotkrümelnavigation und wird aktiv, wenn dies zum Senden einer Abfrage erforderlich ist. Wenn Sie auf „Ereignisse abfragen“ klicken oder nach der Filtererstellung die Eingabetaste drücken, wird eine Abfrage durchgeführt. Wenn Sie über eine Reihe von geladenen Ergebnissen verfügen und Sie den Service, den Zeitraum oder einen Filter ändern, wird die Schaltfläche „Ereignisse abfragen“ blau dargestellt, was darauf hinweist, dass die Daten in der Ansicht nun veraltet sind. In Version 11.2 und höher wird die Schaltfläche „Ereignisse abfragen“ auch nach Ablauf von mehr als einer Minute blau dargestellt, weil der Zeitbereich der ursprünglichen Abfrage nicht mehr die gleiche Ergebnismenge erzeugt.

Hinweis: Wenn Sie den Service ändern, verwendet ein Netzwerkaufruf von Daten für Rekonstruktionen oder von Daten im Bereich „Ereignisse“ (z. B. „Weitere laden“) die vorherigen Service-/Zeitbereichs-/Metadatenfilter. Der Netzwerkaufruf verwendet so lange diese vorherigen Abfrageparameter, bis Sie die neue Abfrage übermitteln.

Tastaturaktionen im geleiteten Modus

Im geleiteten Modus können Sie in der Abfrageerstellung Filter über die Tastatur eingeben, bearbeiten und löschen, ohne einen Zeiger verwenden zu müssen. Sie können den Zeiger zwar verwenden, doch Sie haben die Möglichkeit, die Finger auf der Tastatur zu lassen. In dieser Tabelle sind die verfügbaren Tastaturaktionen angegeben, wenn sich der Cursor im Bereich der Abfrageerstellung im geleiteten Modus der Brotkrümelnavigation befindet. Diese gelten nicht für die Serviceauswahl und den Zeitbereich.

Aktion	Tastatureingabe
Senden Sie eine Abfrage.	Drücken Sie die **Eingabetaste**, während die Abfrageerstellung markiert ist und keine Filter anstehen.
Wählen Sie den Filter, der sich unmittelbar links befindet, falls vorhanden.	Drücken Sie die **linke Pfeiltaste**, ohne eine Auswahl in der Abfrageerstellung vorgenommen zu haben.
Wählen Sie den Filter, der sich unmittelbar rechts befindet, falls vorhanden.	Drücken Sie die **rechte Pfeiltaste**, ohne eine Auswahl in der Abfrageerstellung vorgenommen zu haben.
Fügen Sie direkt links neben dem ausgewählten Filter einen neuen Filter ein.	Drücken Sie die linke Pfeiltaste, wobei ein Filter ausgewählt ist.
Fügen Sie direkt rechts neben dem ausgewählten Filter einen neuen Filter ein.	Drücken Sie die rechte Pfeiltaste, wobei ein Filter ausgewählt ist.
Fügen Sie direkt links neben dem ausgewählten Filter einen neuen Filter ein und öffnen Sie ihn zur Bearbeitung.	Drücken Sie gleichzeitig die Umschalttaste und die linke Pfeiltaste, wobei ein Filter ausgewählt ist.
Fügen Sie direkt links neben dem ausgewählten Filter einen neuen Filter ein und öffnen Sie ihn zur Bearbeitung.	Drücken Sie gleichzeitig die Umschalttaste und die rechte Pfeiltaste, wobei ein Filter ausgewählt ist.
Wählen Sie alle Filter rechts neben dem aktuellen Filter aus.	Drücken Sie gleichzeitig die Umschalttaste und Nach-unten-Taste, wobei ein Filter ausgewählt ist.

Aktion	Tastatureingabe
Wählen Sie alle Filter links neben dem aktuellen Filter aus.	Drücken Sie gleichzeitig die Umschalttaste und Nach-oben-Taste, wobei ein Filter ausgewählt ist.
Bearbeiten eines ausgewählten Filters	Drücken Sie die **ESC-Taste**, wobei ein Filter ausgewählt ist.
Heben Sie die Auswahl aller Filter auf.	Drücken Sie die **ESC-Taste**, wobei ein einzelner Filter ausgewählt ist.
Löschen Sie alle ausgewählten Filter.	Wählen Sie, wobei Filter ausgewählt sind, die Option **Rechtsklick > Ausgewählte Filter löschen** aus, drücken Sie **Löschen**, oder drücken Sie die Rücktaste.
Aktualisieren Sie die Abfrage nur mit den ausgewählten Filtern.	Wählen Sie, wobei Filter ausgewählt sind, die Option **Rechtsklick > Abfrage mit ausgewählten Filtern durchführen** aus.
Öffnen Sie eine neue Registerkarte mit den ausgewählten Filtern.	Wählen Sie, wobei Filter ausgewählt sind, die Option **Rechtsklick > Abfrage mit ausgewählten Filtern auf neuer Registerkarte durchführen** aus.

Feedback im geleiteten Modus

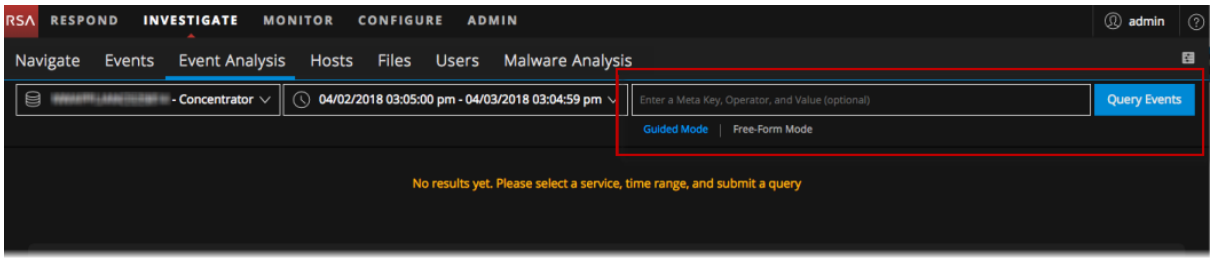
Der geleitete Modus sorgt für visuelles Feedback während der Abfragekonstruktion. In dieser Tabelle wird das mögliche Feedback aufgeführt und beschrieben.

Feedback	Symbol	Beschreibung
Grüner Kreis		Der Cursor wurde zwischen zwei vorhandenen Filtern platziert. Durch Klicken wird an dieser Stelle ein neuer Filter eingefügt.
Rote Umrisslinie eines Filters		Der Werttyp ist für den ausgewählten Metaschlüssel nicht gültig, z. B. ein Zeichenfolgewert für einen Metaschlüssel, für den eine Ganzzahl erwartet wird Eine Kurzinformation mit einer Erklärung zum Fehler.
Stoppuhr		Für die ausgewählte Metaschlüssel/Bediener-Kombination ist zusätzliche Zeit für die Bearbeitung erforderlich. Die Abfrage ist zwar noch ausführbar, es sollte aber ein effizienterer Metaschlüssel oder Operator verwendet werden.

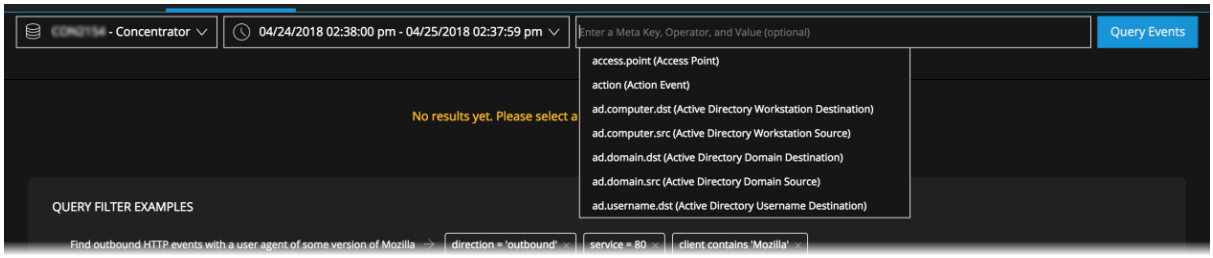
Hinzufügen eines Filters im geleiteten Modus

So filtern Sie die Daten, die in der Ansicht „Ereignisanalyse“ im geleiteten Modus angezeigt werden:

1. Gehen Sie zur **Ereignisanalyse** und wählen Sie unter der Abfrageerstellung **Geleiteter Modus** aus. Dies ist ein Beispiel für eine leere Abfrageerstellung im geleiteten Modus vor der Eingabe eines Filters.

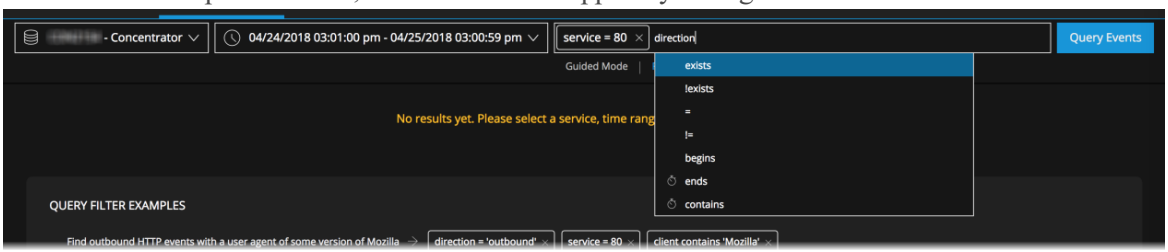


2. Wenn Sie einen Filter einfügen möchten, klicken Sie in das leere Feld für die Abfrageerstellung oder vor oder nach einem vorhandenen Filter.
   Wenn sich die Einfügemarke zwischen zwei Filtern befindet, ist der Einfügepunkt durch einen grünen Punkt gekennzeichnet. Wenn sich die Einfügemarke am Ende der vorhandenen Brotkrümelnavigation befindet, wird das Filtereingabefeld geöffnet und der Cursor blinkt am Eingabepunkt. In einem Drop-down-Menü sind die verfügbaren Metaschlüssel für den ausgewählten Service in alphabetischer Reihenfolge aufgeführt. Die verfügbaren Metaschlüssel werden von dem untersuchten Service übergeben und Metaschlüssel, deren Verarbeitung mehr Zeit in Anspruch nimmt, sind durch ein Stoppuhrsymbol gekennzeichnet.

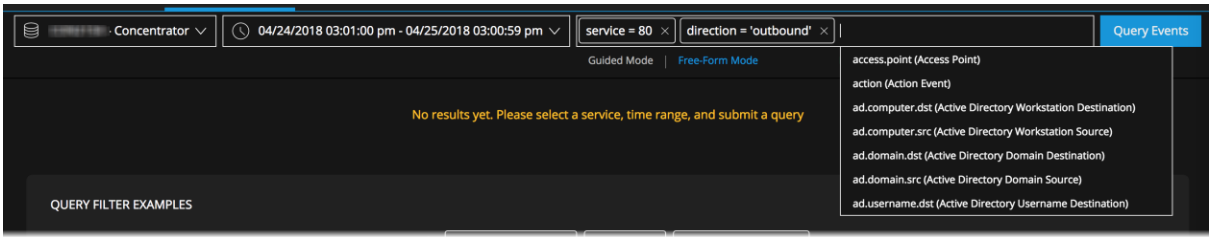


3. Führen Sie zum Auswählen eines Metaschlüssels einen der folgenden Schritte aus:
   a. Wenn das Drop-down-Menü nur eine Option enthält, drücken Sie die **Eingabetaste**.
   b. Wenn das Drop-down-Menü zwei oder mehr Optionen enthält, klicken Sie auf den Metaschlüssel oder verwenden Sie den Pfeil nach oben/nach unten und drücken Sie die **Eingabetaste**.
   c. Geben Sie den Metaschlüssel ein. Während Sie den Metaschlüssel eingeben, wird die Liste weiter aktualisiert. Zur Auswahl des Metaschlüssels drücken Sie die **Eingabetaste**.
   d. Wenn Sie den Metaschlüssel bearbeiten oder löschen wollen, drücken Sie die **Rückschritttaste** oder **Löschen**.
      Während Sie ein Zeichen löschen, wird die Drop-down-Liste mit den Metaschlüsseln so gefiltert, dass Metaschlüssel enthalten sind, die mit diesem Zeichen beginnen. Zur Auswahl eines Metaschlüssels drücken Sie die **Eingabetaste**.
      Der Metaschlüssel wird der Abfrageerstellung hinzugefügt und eine Liste der gültigen Operatoren für den ausgewählten Metaschlüssel wird angezeigt. Vorgänge, deren Verarbeitung

mehr Zeit in Anspruch nimmt, sind durch ein Stoppuhrsymbol gekennzeichnet.



4. Führen Sie zum Auswählen eines Operators einen der folgenden Schritte aus:
   a. Wenn das Drop-down-Menü nur eine Option enthält, drücken Sie die **Eingabetaste**.
   b. Wenn das Drop-down-Menü zwei oder mehr Optionen enthält, klicken Sie auf den Operator oder verwenden Sie den Pfeil nach oben/nach unten und drücken Sie**Eingabetaste**.
   c. Geben Sie den Operator ein und drücken Sie die Eingabetaste.
   Die Drop-Down-Liste wird geschlossen und Sie können einen Wert hinzufügen, wenn der Operator einen Wert akzeptiert.
5. (Optional) Geben Sie einen Wert ein und drücken die **Eingabetaste**.
6. Um den Filter zu erstellen, drücken Sie die Eingabetaste. Wenn Sie auf eine beliebige Stelle außerhalb des Felds klicken, bevor Sie die Eingabetaste drücken, wird der Filter nicht erstellt.
   Der neue Filter wird eingefügt und der Cursor wird nach dem letzten Filter neu fokussiert. Die Drop-down-Liste mit den Metaschlüsseln wird angezeigt. Wenn der Filter einen Fehler enthält, wird er rot umrandet. Sie können den Mauszeiger über den Filter bewegen, um eine Kurzinformation zum Fehler anzuzeigen. In dieser Abbildung ist eine Abfrage dargestellt, die ohne Fehler erstellt wird.



7. Korrigieren Sie alle Filter, die Fehler aufweisen.
8. Wenn Sie bereit sind, die Abfrage in der Brotkrümelnavigation auszuführen, klicken Sie auf **Ereignisse abfragen**.
9. Die Ereignisliste wird aktualisiert und zeigt die Abfrage an.

Bearbeiten eines Filters im geleiteten Modus

Mit einer Abfrage in der Abfrageerstellung im geleiteten Modus können Sie einen Filter bearbeiten. So bearbeiten Sie einen Filter:

1. Zum Bearbeiten eines Filters doppelklicken Sie darauf oder klicken Sie auf den Filter und drücken Sie die **Eingabetaste**.
2. Bearbeiten Sie den Filter. Drücken Sie nach dem Bearbeiten die Eingabetaste, um den Filter zu aktualisieren.

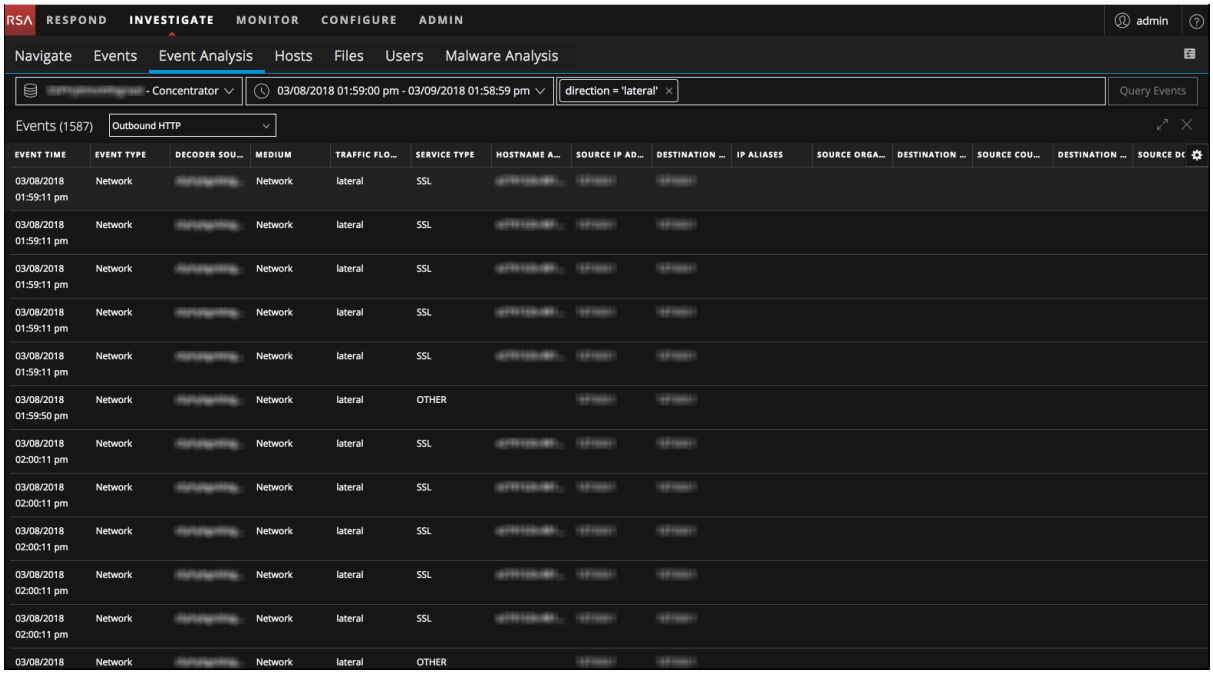
3. Wenn Sie die Abfrage erneut ausführen möchten, klicken Sie auf die Schaltfläche **Abfrage**. Die Ereignisliste wird aktualisiert und zeigt den aktualisierten Filter an.

Abfrage mit ausgewählten Filtern im geleiteten Modus

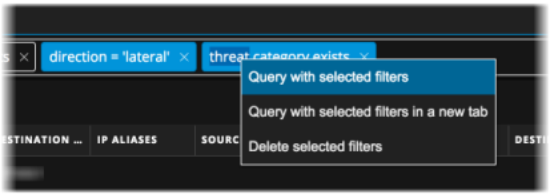
Mit einem oder mehreren Filtern in der Abfrageerstellung im geleiteten Modus können Sie dieselbe Abfrage neu fokussieren, sodass nur ausgewählte Filter eingeschlossen werden. Die Ergebnisse werden in der aktuellen Browser-Registerkarte oder einer neuen Browser-Registerkarte angezeigt. So aktualisieren Sie die Abfrage nur mit ausgewählten Filtern:

1. Beginnen Sie mit einer Abfrage im geleiteten Modus mit einem oder mehreren Filtern, z. B. einer Abfrage mit drei Filtern: `risk.info = exists`, `direction ="lateral"` und `threat.category exists`.
2. Zum Öffnen einer neuen Registerkarte mit den ausgewählten Filtern wählen Sie `direction = "lateral"` aus, klicken mit der rechten Maustaste auf den Filter und wählen im Drop-down-Menü die Option **Abfrage mit ausgewählten Filtern auf neuer Registerkarte durchführen** aus.

Eine neue Registerkarte mit den Ergebnissen für den ausgewählten Filter wird geöffnet und die ursprüngliche Abfrage bleibt unverändert auf der vorherigen Registerkarte.



3. Zum Abfragen der ausgewählten Filter auf der gleichen Registerkarte klicken Sie auf `direction = "lateral"` und `threat.category exists`. Klicken Sie dann mit der rechten Maustaste und wählen Sie im Drop-down-Menü die Option **Abfrage mit ausgewählten Filtern durchführen** aus.



Eine Abfrage nur mit den ausgewählten Filtern wird eingereicht und alle verbleibenden Filter werden entfernt.

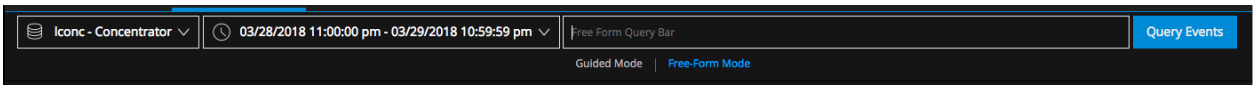
Löschen eines Filters im geleiteten Modus

So löschen Sie einen Filter:

1. Klicken Sie in einem Filter auf **X**, klicken Sie auf den Filter, um ihn auszuwählen, und drücken Sie **Löschen**, oder klicken Sie mit der rechten Maustaste auf einen oder mehrere Filter und wählen Sie im Drop-down-Menü **Ausgewählte Filter löschen** aus.
2. Wenn Sie die Abfrage erneut ausführen möchten, klicken Sie auf die Schaltfläche **Abfrage**.
   Der ausgewählte Filter wird gelöscht und die Ereignisliste wird aktualisiert.

Freitextabfrageerstellung

Freitextabfragen sind am sinnvollsten, wenn Sie eine komplexe Abfrage schnell eingeben möchten und die Metaschlüssel, gültigen Operatoren und gültige Syntax für die Eingabe von Werten kennen. In der folgenden Abbildung ist die ursprüngliche Ansicht „Ereignisanalyse“ mit dem leeren Feld für die Freitextabfrageerstellung dargestellt.



Der blinkende Cursor zeigt an, dass sie eine Abfrage eingeben können. Hier können Sie freien Text eingeben. Wenn weitere Ausdrücke hinzugefügt, aber nicht in einer einzigen Zeile angezeigt werden können, werden sie in eine andere Zeile umgebrochen und der Eingabebereich wird vertikal erweitert, sodass alle Filter ohne Bildlauf nach rechts sichtbar sind.

Dies sind einige Beispiele für Abfragen, die Sie im Freitextmodus eingeben können:

Zum Finden von Ereignissen mit einem 8- bis 11-stelligen Namen, wie z. B. atreeman-72:
```
user.all length 8-11 && (user.all regex '^a[a-z]{2}ee[a-z]{3}-[0-9]{2}')
```

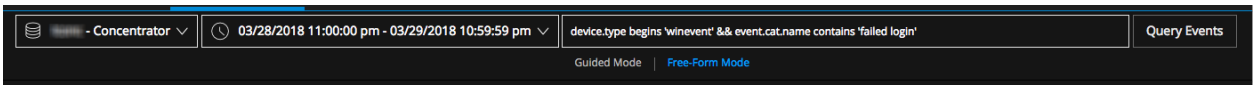
Zum Finden von Ereignissen, die entweder HTTP-Netzwerkereignisse sind oder denen die aix- oder ciscoasa-Protokolle zugewiesen sind:
```
service=80 || (device.type = 'aix','ciscoasa')
```

Zum Finden aller ausgehenden Ereignisse, die nicht nach Kanada oder in die Vereinigten Staaten gehen:
```
direction = 'outbound' AND not(country.dst = 'united states' || country.dst =
'canada')
```

Wenn Sie eine Abfrage im geleiteten Modus eingereicht haben, wird diese in Text umgewandelt, sobald Sie auf den Freitextmodus klicken. Dies ist ein Beispiel für eine Abfrage, die im geleiteten Mode eingereicht wurde.

Hier können Sie freien Text eingeben. Wenn weitere Ausdrücke hinzugefügt, aber nicht in einer einzigen Zeile angezeigt werden können, werden sie in eine andere Zeile umgebrochen und der Eingabebereich wird vertikal erweitert, sodass alle Filter ohne Bildlauf nach rechts sichtbar sind.

Die Schaltfläche „Ereignisse abfragen“ befindet sich rechts neben der Brotkrümelnavigation und wird in Blau hervorgehoben, wenn dies zur Eingabe einer Abfrage erforderlich ist. Die Abfrage wird angewendet, wenn Sie auf „Ereignisse abfragen“ klicken. Zu diesem Zeitpunkt wird die Abfrage validiert, sodass Syntax- und Logikfehler angezeigt werden.



Vorgänge, die mehr Bearbeitungszeit erfordern, werden nicht hervorgehoben, da sie sich im geleiteten Mode befinden. Aber in dieser Tabelle ist eine Zusammenfassung der leistungsaufwändigen Vorgänge aufgeführt.

Indexmethode	Nichttextwert	Textwert	Regelmäßige Vorgänge	Leistungsaufwändige Vorgänge
Nach Schlüssel	✓		`exists`, `!exists`	`eq`, `!eq`
Nach Schlüssel		✓	`exists`, `!exists`	`eq`, `!eq`, `begins`, `ends`, `contains`
Nach Wert	✓		`exists`, `!exists`, `eq`, `!eq`	Keine aufwändigen Operatoren
Nach Wert		✓	`exists`, `!exists`, `eq`, `!eq`, `begins`	`ends`, `contains`
Keine Angabe	Sonderfall für `sessionid`		`exist`, `!exits`, `eq`, `!eq`	Keine aufwändigen Operatoren

Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“

Bei der Untersuchung von Raw-Ereignissen und Metadaten in der Ansicht „Ereignisanalyse“ können Sie bei der Transparenz und der Größe der Bereiche einfache Anpassungen vornehmen. Im Bereich „Paketanalyse“ und im Bereich „Textanalyse“ verwenden Sie zusätzliche Funktionen, um die Art und Weise anzupassen, wie die Rekonstruktion angezeigt wird, und interessante Daten in den Fokus zu rücken.

Auswählen des Typs der Ereignisanalyse

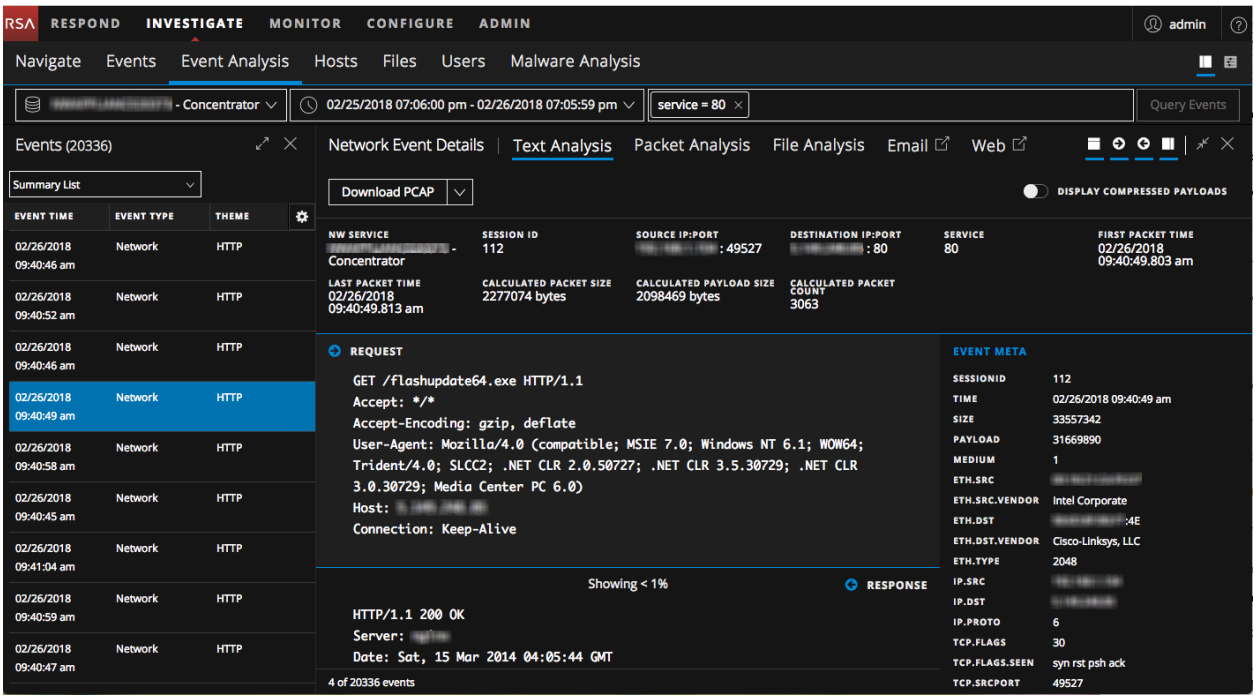
Um den Typ der Ereignisanalyse für ein Ereignis auszuwählen, führen Sie einen der folgenden Schritte aus:

1. Klicken Sie in der Symbolleiste der **Ansicht „Ereignisanalyse“** auf den Analysetyp in der Symbolleiste.
2. Wählen Sie im Drop-down-Menü den Typ der Analyse aus: **Dateianalyse**, **Textanalyse**, **Paketanalyse**, **E-Mail** (Version 11.1 und höher) oder **Web** (Version 11.1 und höher).
   Wenn Sie **Dateianalyse**, **Textanalyse** oder **Paketanalyse** auswählen, wird die Ansicht mit geöffnetem Bereich „Paketanalyse“, „Dateianalyse“ oder „Textanalyse“ aktualisiert.
   Wenn Sie **E-Mail** oder **Web** ausgewählt haben, wird die E-Mail- oder Web-Rekonstruktion der Ansicht „Ereignisse“ des einzelnen Ereignisses in einer neuen Registerkarte geöffnet. Dies ist die gleiche Rekonstruktion einer E-Mail- oder Web-Sitzung, die in der Ansicht „Ereignisse“ verwendet wird. Die Ansicht „Ereignisse“ bietet mehr Funktionen, wenn Sie eine E-Mail- oder Webrekonstruktion anzeigen: Sie können die Ereignisse dann in dieser Ansicht durchblättern, anstatt nur ein Ereignis anzuzeigen (siehe Rekonstruieren eines Ereignisses).

Hinweis: Der Bereich „Paketanalyse“ ist nur für Netzwerkereignisse verfügbar.

Öffnen, Schließen und Anpassen der Größe der Bereiche in der Ansicht „Ereignisanalyse“

Die Ansicht „Ereignisanalyse“ wird mit der Ereignisliste geöffnet und ohne dass ein Ereignis ausgewählt oder rekonstruiert wird. Wenn Sie ein Ereignis auswählen, wird auf der rechten Seite der Bereich „Netzwerkereignisdetails“, „Protokollereignisdetails“ oder „Endpunktereignisdetails“ geöffnet. Zunächst belegt der Bereich „Netzwerkereignisdetails“, „Protokollereignisdetails“ oder „Endpunktereignisdetails“ standardmäßig 75 % der Fensterbreite.



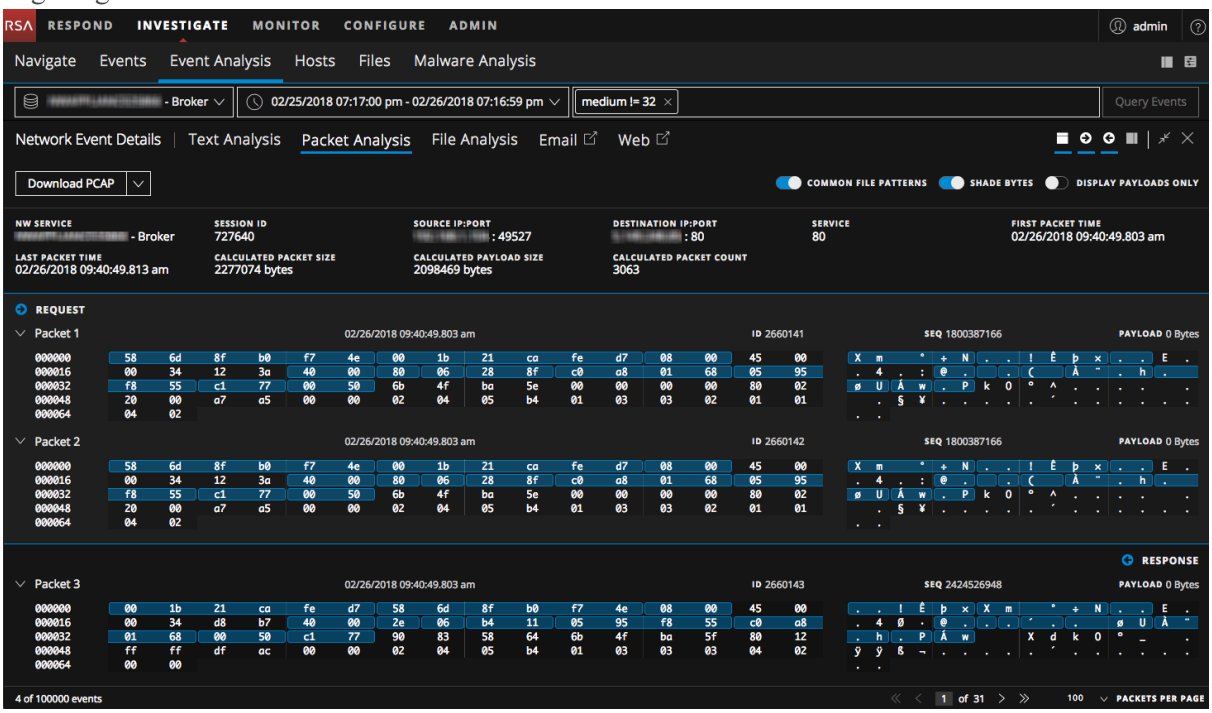
Sie können das Größenverhältnis der beiden Bereiche anpassen, um die Lesbarkeit zu verbessern, indem Sie einen der Bereiche erweitern, einen der Bereiche verkleinern und einen der Bereiche schließen. Nach dem Schließen eines Bereichs können Sie diesen erneut öffnen. Das Verhältnis, das Sie auswählen, bleibt bestehen, bis Sie es ändern oder den Browser aktualisieren.

- Um den Bereich „Ereignisse“ erneut zu öffnen, klicken Sie oben rechts auf ☐.

Um die Ansicht zu optimieren:

1. Um das Größenverhältnis der beiden Bereiche anzupassen, führen Sie einen der folgenden Schritte aus:
   a. Klicken Sie in der Symbolleiste des Bereichs, den Sie erweitern möchten, auf ◪.
   b. Klicken Sie in der Symbolleiste des Bereichs, den Sie verkleinern möchten, auf ◪.
2. Um einen der Bereiche zu schließen und die volle Breite des offenen Bereichs wiederherzustellen, klicken Sie auf ◪.
   Dies ist ein Beispiel für die Rekonstruktion, die über die gesamte Breite des Browserfensters

angezeigt wird.



3. Um den Bereich „Ereignisse“ nach dem Schließen erneut zu öffnen, klicken Sie in der oberen rechten Ecke der Ansicht „Navigation“ auf □.
   Der Bereich „Ereignisse“ wird mit dem letzten Zustand geöffnet (25 %:75 % bzw. 50 %:50 %).
4. Um den Bereich „Ereignisdetails“ erneut zu öffnen, klicken Sie auf ein Ereignis im Bereich „Ereignisse“.

Auswählen einer Spaltengruppe und von Spalten in der Ereignisanalyse

In Version 11.1 oder höher können Sie im Bereich „Ereignisse“ integrierte oder benutzerdefinierte Spaltengruppen verwenden. Die Spaltengruppen werden in der Ansicht „Ereignisse“ erstellt und verwaltet (siehe Managen von Spaltengruppen in der Ansicht „Ereignisse“); diese Gruppen werden in der Ansicht „Ereignisanalyse“ angezeigt. Wenn Sie die Spaltengruppe ändern, beziehen sich die Änderungen, die Sie an einer Spaltengruppe vornehmen, nur auf die aktuelle Ansicht. Wenn Sie die Seite verlassen und zur Ansicht „Ereignisanalyse“ zurückkehren, werden die Spaltenänderungen nicht im Bereich „Ereignisse“ beibehalten.

Hierbei handelt es sich um die integrierten Spaltengruppen.

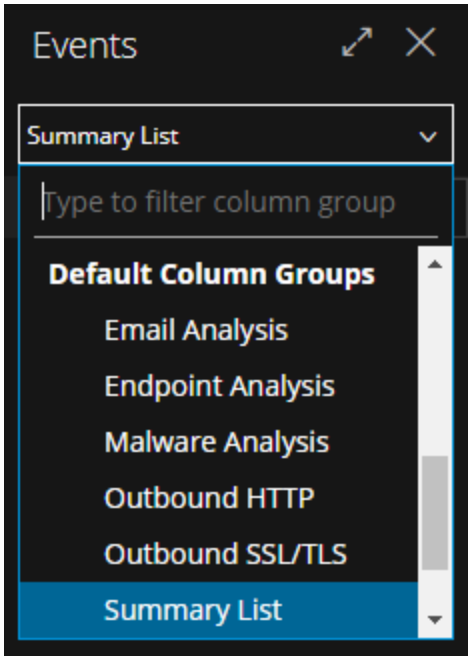
- **E-Mail-Analyse**: umfasst Metaschlüssel, die nützlich sind, wenn Sie E-Mail-bezogene Metadaten untersuchen.
- **Endpunktanalyse**: umfasst Metaschlüssel, die nützlich sind, wenn Sie endpunktbezogene Metadaten untersuchen.
- **Malware Analysis**: umfasst Metaschlüssel, die nützlich sind, wenn Sie Malware-bezogene Metadaten untersuchen.

- **Ausgehender HTTP**: umfasst Metaschlüssel, die nützlich sind, wenn Sie Metadaten im Zusammenhang mit ausgehendem HTTP untersuchen.
- **Ausgehendes SSL/TLS**: umfasst Metaschlüssel, die nützlich sind, wenn Sie Metadaten im Zusammenhang mit ausgehender SSL-/TTS-Analyse untersuchen.
- **Listenübersicht**: umfasst Metaschlüssel, die in einer allgemeinen Ermittlung hilfreich sind. **Dies ist die Standardspaltengruppe.**
- **Bedrohungsanalyse**: umfasst Metaschlüssel, die potenzielle Bedrohungen im Dataset markieren.
- **Webanalyse**: umfasst Metaschlüssel, die Anomalien im Webdatenverkehr markieren.

Eine Spaltengruppe enthält möglicherweise mehr Spalten, als ohne Bildlauf nach rechts sichtbar sind. In Version 11.1 können Sie die Spalten auswählen, die in der Ansicht „Ereignisanalyse“ angezeigt werden. Die Reihenfolge der Spalten entspricht der Reihenfolge in der Ansicht „Ereignisse“ der Standardspaltengruppe. Standardmäßig werden die ersten 15 Spalten angezeigt, wenn Sie eine Spaltengruppe auswählen. Für eine optimale Anzeige wird empfohlen, nur 15 Spalten gleichzeitig anzuzeigen; Sie können allerdings zusätzliche Spalten auswählen, die angezeigt werden sollen, und angezeigte Spalten entfernen.

So wählen Sie eine Spaltengruppe aus:

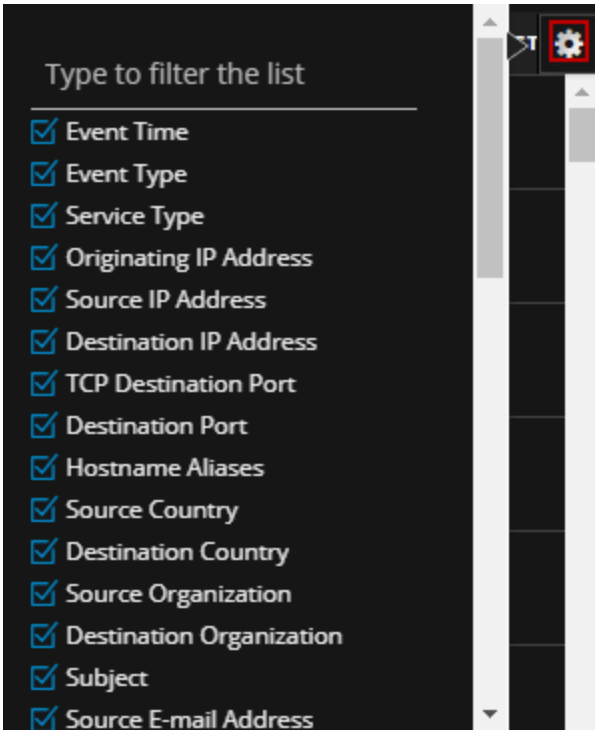
1. Wählen Sie im Drop-down-Menü neben „Ereignisse“ eine Spaltengruppe aus (z. B. **Übersichtsliste**). Außerdem können Sie den Anfang des Namens der Spaltengruppe eingeben und eine Gruppe auswählen, wenn die Gruppen im Drop-down-Menü angezeigt werden.



   Der Bereich „Ereignisse“ zeigt Daten in den Spalten an, die der ausgewählten Spaltengruppe angehören.

So wählen Sie Spalten zur Anzeige aus:

1. Klicken Sie bei der Arbeit in der Ansicht „Ereignisanalyse“ mit einer ausgewählten Spaltengruppe auf , um die Spaltenauswahl anzuzeigen.



2. Wählen Sie die Metaschlüssel aus oder geben Sie den Namen eines Metaschlüssels ein, der in zusätzlichen Spalten angezeigt werden soll.
3. Wenn in einer Spalte kein Metaschlüssel angezeigt werden soll, heben Sie die Auswahl des Metaschlüssels auf.
   Die Daten werden unter Verwendung der ausgewählten Spalten erneut angezeigt.

Anpassen der Anzeige von Anforderungen und Antworten

Für Ereignistypen, die Anforderungen und Antworten enthalten, können Sie mehrere Anpassungen vornehmen.

Hinweis: Wenn der Analysetyp keine Anforderungen und Antworten enthält, kann die Option nicht ausgewählt werden. Der Bereich Dateianalyse ist ein Beispiel für einen Rekonstruktionstyp ohne Anforderungen und Antworten. Ein rekonstruiertes Protokollereignis in der Ansicht „Text“ ist ein weiteres Beispiel.

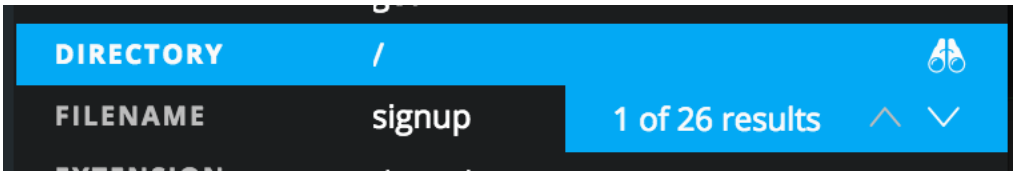
Um auszuwählen, welche Seite des Gesprächs angezeigt werden soll – Anforderung, Antwort oder beide –, klicken Sie auf eines der Richtungssymbole oder auf beide ( ). Die Rekonstruktion wird anhand der ausgewählten Informationen aktualisiert.

Hinweis: Wenn keine Daten angezeigt werden, haben Sie möglicherweise Anforderung und Antwort deaktiviert. Sie müssen eine der beiden Optionen auswählen, damit Daten angezeigt werden.

Anzeigen von Ereignismetadaten für ein Ereignis

Bei der Untersuchung von Ereignissen im Bereich Textanalyse, Paketanalyse oder Dateianalyse können Sie auf klicken, um die zugehörigen Metadaten in einem benachbarten Bereich, dem Bereich „Ereignis-Metadaten“, anzuzeigen.

Wenn Sie bei der Anzeige der Bereiche „Textanalyse“ und „Ereignis-Metadaten“ den Mauszeiger über die Metaschlüssel-/Metwawert-Paare bewegen, wird ein Fernglas angezeigt, wenn der Metawert im unformatierten Text durchsucht werden kann. Dies ist ein Beispiel für das Fernglas-Symbol, wenn der Mauszeiger über das **Verzeichnis** und das / Metaschlüssel-/Metawert-Paar bewegt wird.



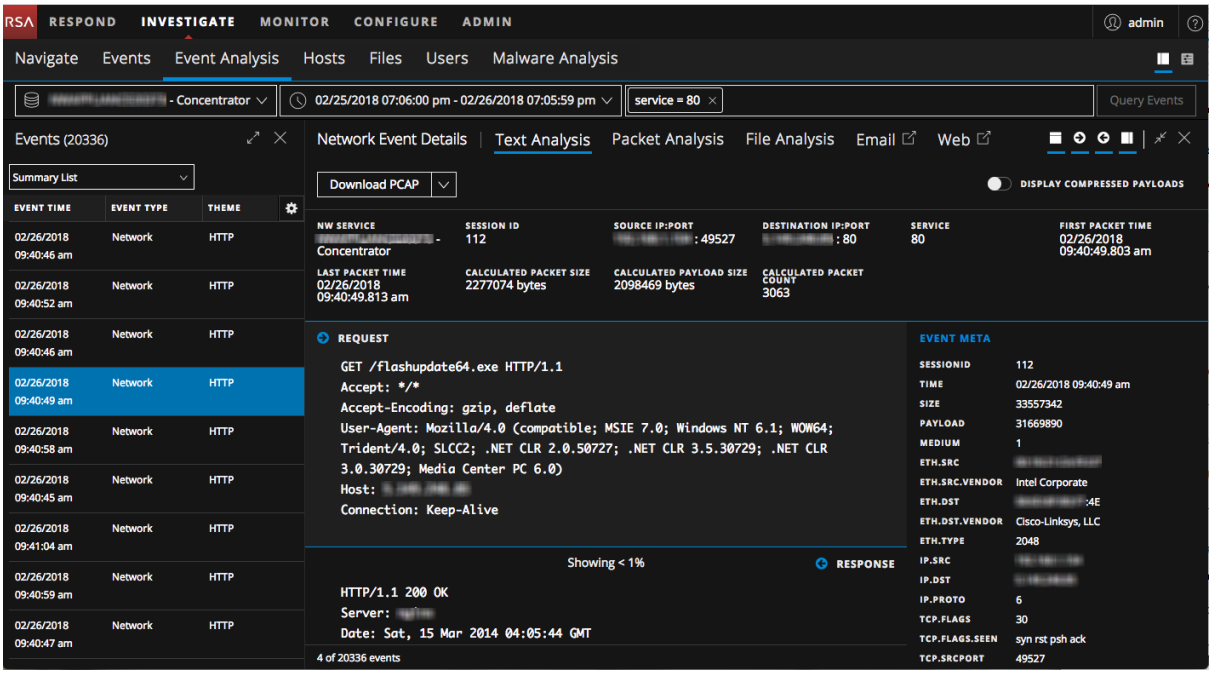
Durch Klicken auf das Symbol wird eine Suche nach dem Metaschlüssel-/Metawert-Paar (ohne Beachtung der Groß- und Kleinschreibung) im Bereich Textanalyse ausgelöst und jede Instanz wird hervorgehoben. Im Bereich „Ereignis-Metadaten“ werden in der hervorgehobenen Zeile die Anzahl der Ergebnisse und ein Scroller angezeigt, den Sie verwenden können, um die einzelnen Ergebnisse schnell im Bereich Textanalyse zu finden. Sie können jeden hervorgehobenen Speicherort der Daten anzeigen, die die Erzeugung des Metaschlüssels ausgelöst haben, und die nächsten und vorherigen anzeigen.

Nur Metaschlüssel mit relevanten Werten im Rohtext können durchsucht werden. Sie können jeweils nur einen Metaschlüssel durchsuchen. Wenn der Wert aktuell aufgrund der Kürzungen eines Texteintrags mit mehr als 3.000 Zeichen ausgeblendet ist, wird der Texteintrag vollständig eingeblendet, um den gefundenen Metawert anzuzeigen.

Wenn Sie auf das gleiche Metaschlüssel-/Metawert-Paar oder ein anderes Metaschlüssel-/Metawert-Paar im Bereich „Ereignis-Metadaten“ klicken, wird die Hervorhebung des unformatierten Texts entfernt. Die Hervorhebung wird ebenfalls entfernt, wenn Sie den Bereich „Ereignis-Metadaten“ schließen.

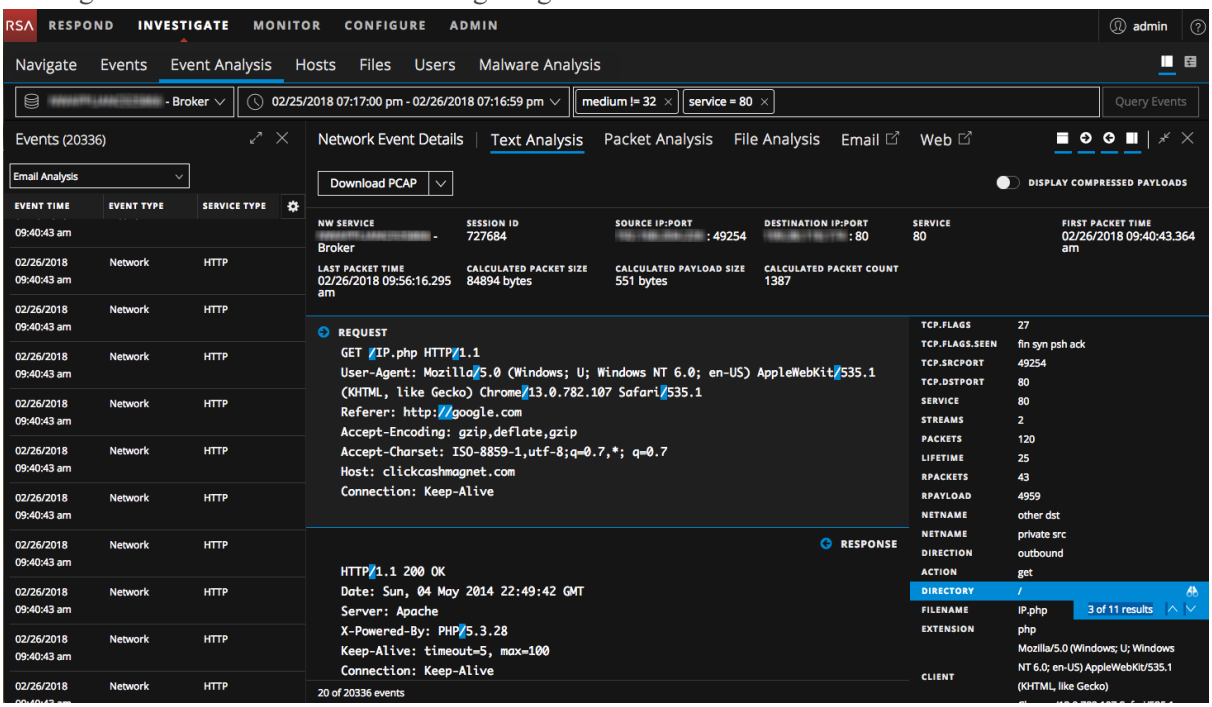
So durchsuchen Sie den unformatierten Text nach Metawerten, die einen Metaschlüssel ausgelöst haben:

1. Öffnen Sie ein Netzwerkereignis im Bereich Textanalyse.



2. Klicken Sie in der Symbolleiste auf  , um das den Bereich „Ereignis-Metadaten“ zu öffnen. Wenn Sie den Mauszeiger über die Metawertpaare key:meta in der Liste bewegen, identifiziert ein Fernglas-Symbol Werte, die im Bereich Textanalyse durchsucht werden können.
3. Um den Wert im unformatierten Text zu suchen, klicken Sie auf eine Zeile mit dem Fernglas-Symbol, welches angibt, dass sie durchsucht werden kann.
   Wenn es kein relevantes Vorkommen des Werts im Text gibt, wird der gesuchte Wert im Bereich „Ereignis-Metadaten“ hervorgehoben und im Bereich Textanalyse wird nichts hervorgehoben.
   Wenn eine oder mehrere relevante Instanzen des Werts im Bereich Textanalyse gefunden werden, wird jedes Vorkommen hervorgehoben. Der gesuchte Wert wird im Bereich „Ereignis-Metadaten“

hervorgehoben und der Scroller wird angezeigt.



4. Um die Hervorhebung zu entfernen, schließen Sie den Bereich „Ereignis-Metadaten“, klicken Sie auf das gleiche Metaschlüssel-/Metawert-Paar im Bereich „Ereignis-Metadaten“ oder klicken Sie auf ein anderes Metaschlüssel-/Metawert-Paar im Bereich „Ereignis-Metadaten“.
   Die Hervorhebung wird aus dem unformatierten Text entfernt.

Anzeigen oder Ausblenden des Ereignis-Headers

Zum Verbergen des Ereignis-Headers im Bereich Paketanalyse, Textanalyse oder Dateianalyse und Schaffen von mehr vertikalem Platz für die Daten klicken Sie auf .

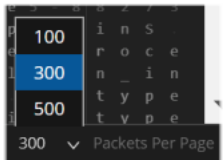
Blättern durch Ereignisse in den Bereichen „Paketanalyse“ und „Textanalyse“

Seitenumbruchshilfen ermöglichen mehr Flexibilität beim Blättern durch eine Liste von Paketen oder Text. Im Bereich „Paketanalyse“ können Sie die Anzahl der Pakete auswählen, die pro Seite angezeigt werden, und Ihre Auswahl wird über Anmeldungen hinweg in der NetWitness-Anwendung gespeichert. Wenn ein Steuerelement nicht verfügbar ist, ist es abgeblendet; wenn Sie z. B. die Seite 1 anzeigen, sind die Steuerelemente und abgeblendet.

Hinweis: Für die Paketanalyse sind Seitenumbruchshilfen in der Version 11.1 und höher verfügbar. Für die Textanalyse sind Seitenumbruchshilfen in der Version 11.2 und höher verfügbar.

So verwenden Sie Seitenumbruchshilfen:

1. (Nur für die Paketanalyse) Öffnen Sie ein Ereignis in der Ansicht „Ereignisanalyse“, klicken Sie auf die aktuelle Anzahl der Pakete pro Seite (**100**, **300** oder **500**) und wählen Sie im Drop-down-Menü die neue Anzahl an Paketen pro Seite aus.



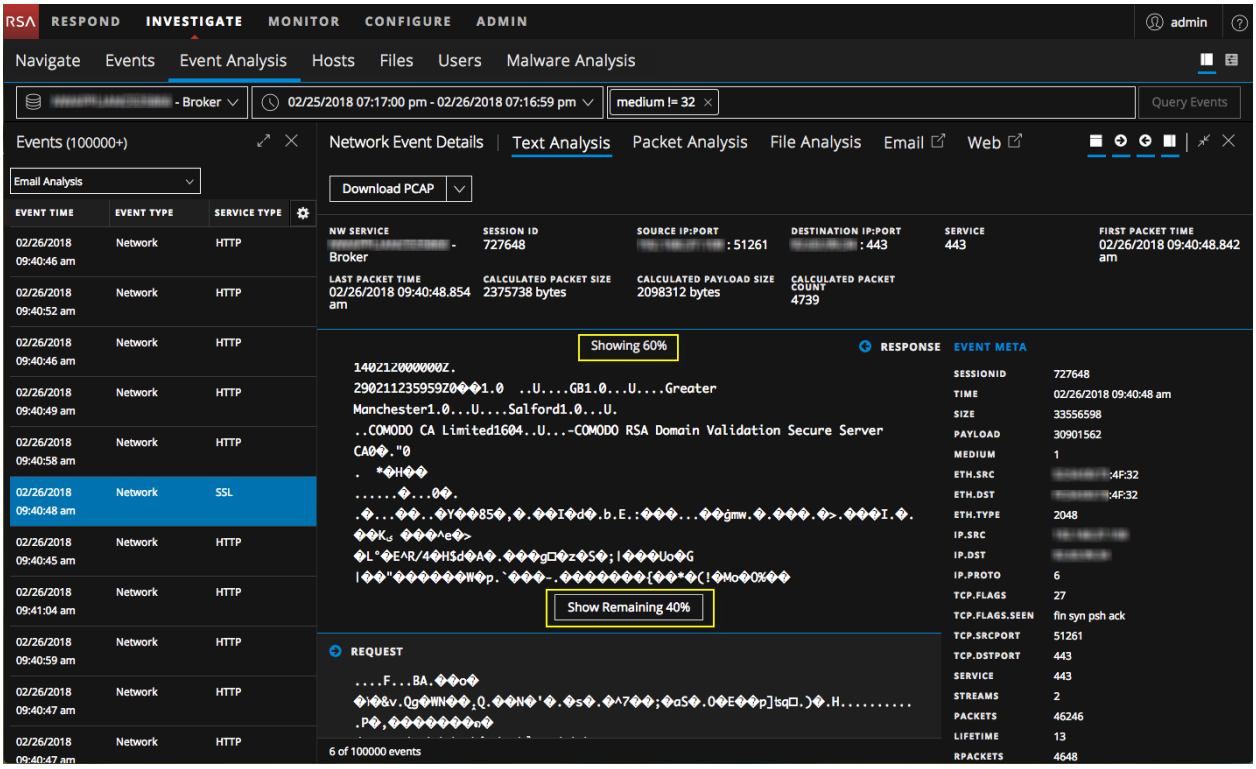
2. Verwenden Sie zum Vor- oder Zurückblättern die Seitensteuerelemente:
   Klicken Sie auf ▶, um die nächste Seite anzuzeigen.
   Klicken Sie auf ⏭, um die letzte Seite anzuzeigen.
   Klicken Sie auf ◀, um die vorherige Seite anzuzeigen.
   Klicken Sie auf ⏮, um die erste Seite anzuzeigen.
3. (Nur für die Paketanalyse) Geben Sie zum Aufrufen einer bestimmten Seite in das Seitenzahlfeld 

eine Seitenzahl ein.

Hinweis: Im Bereich „Textanalyse“ müssen Sie manuell zur letzten Seite navigieren, bevor das letzte Seitenkontrollsymbol verfügbar ist.

Erweitern abgeschnittener Texteinträge im Bereich „Textanalyse“

Eine Rekonstruktion eines Netzwerkereignisses im Bereich Textanalyse kann Anforderungen und Antworten mit vielen Hunderttausenden von Zeichen enthalten und das Blättern durch einen langen Eintrag von mehr als 6000 Zeichen, die nicht von Interesse sind, kann Zeit verschwenden. Um die Erfahrung für Analysten zu verbessern, werden alle Texteinträge mit mehr als 6000 Zeichen gekürzt, sodass nur die ersten 2.000 Zeichen angezeigt werden. Dieses Beispiel zeigt einen Eintrag mit mehr als 2000 Zeichen. Eine Meldung in der Kopfzeile gibt den Prozentsatz der insgesamt angezeigten Zeichen an.



Sie können sehen, dass 60 % der Zeichen (die ersten 2000) angezeigt werden. Klicken Sie auf **Verbleibende 40 % anzeigen**, um den Rest des Eintrags anzuzeigen.

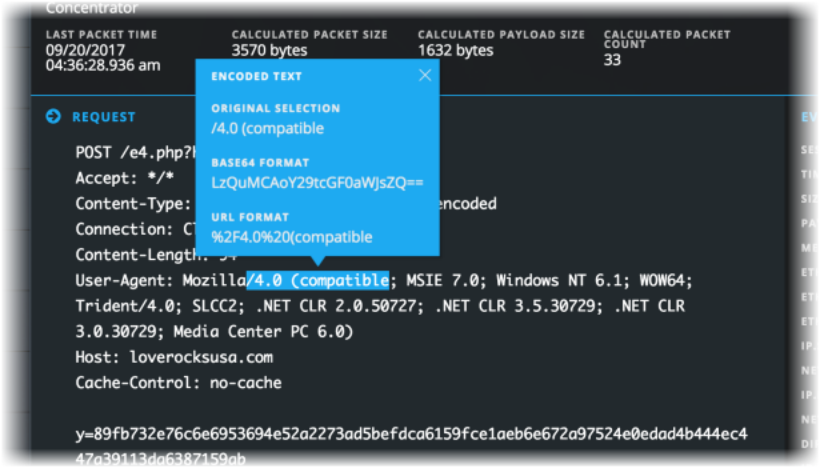
Wenn Sie im Bereich „Ereignis-Metadaten“ nach Metadaten suchen, während Text im Bereich Textanalyse gekürzt wird, wird der abgeschnittene Text durchsucht. Wenn die Metadaten in ausgeblendetem Text vorhanden sind, wird der Texteintrag erweitert, um den Text mit den gefundenen Metadaten anzuzeigen.

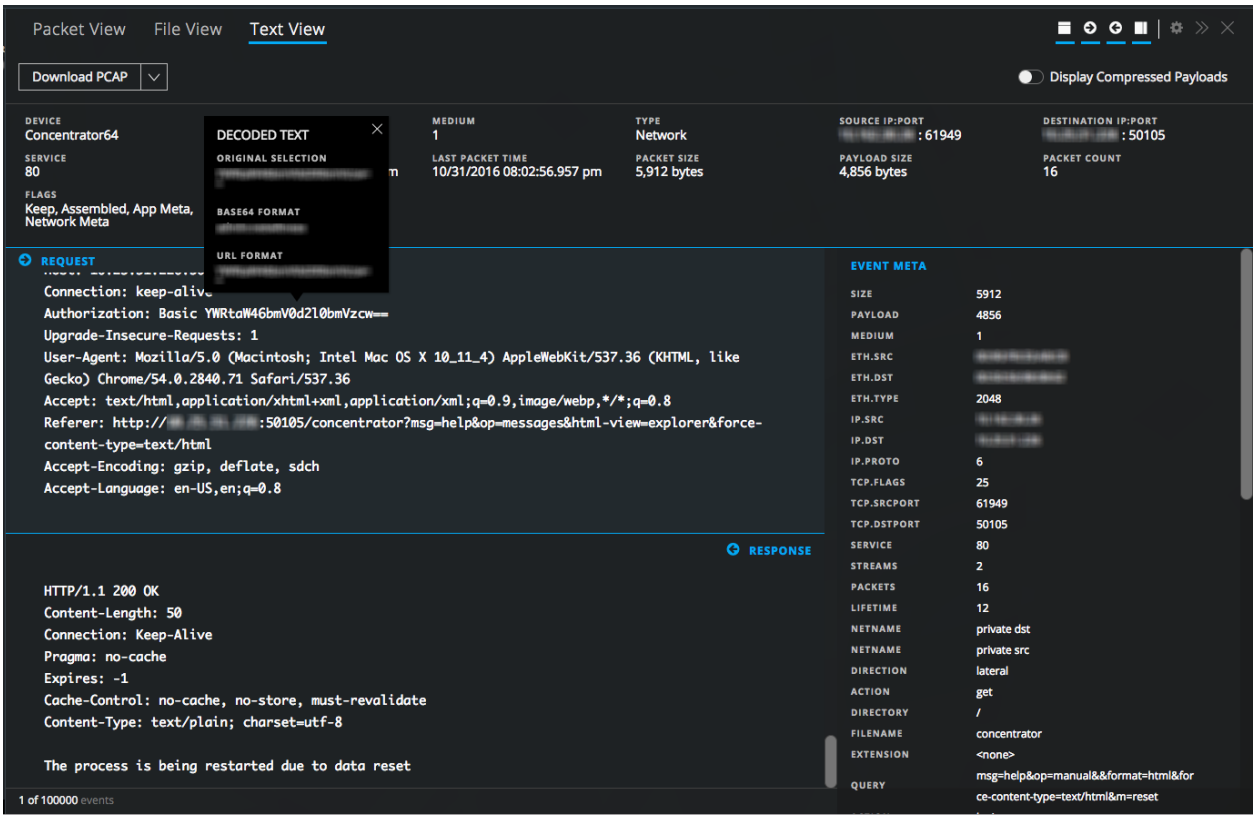
Durchführen von URL- und Base64-Codierung und -Decodierung im Bereich „Textanalyse“

Wenn eine Netzwerksitzung, die im Bereich Textanalyse rekonstruiert wird, Base64- oder URL-kodierte Zeichenfolgen enthält, können Sie eine Zeichenfolge zum besseren Verständnis der Sitzung dekodieren. Wenn die Sitzung dekodierte Zeichenfolgen für Base64 oder URL enthält, können Sie eine Zeichenfolge in der verschlüsselten Form anzeigen, um zusätzliche Instanzen des codierten Texts in anderen Sitzungen zu suchen.

Wenn Sie eine Netzwerksitzung anzeigen, die codierten Text im Bereich Textanalyse enthält, können Sie einen Teil des Texts in einer einzigen Anforderung oder Antwort zur Anzeige in codierter oder decodierter Form auswählen. Je nach dem auf dem Decoder geladenen Inhalt gibt es möglicherweise zusätzliche Metadaten, die angeben, dass Base64- oder URL-codierte Daten in der Sitzung enthalten sind.

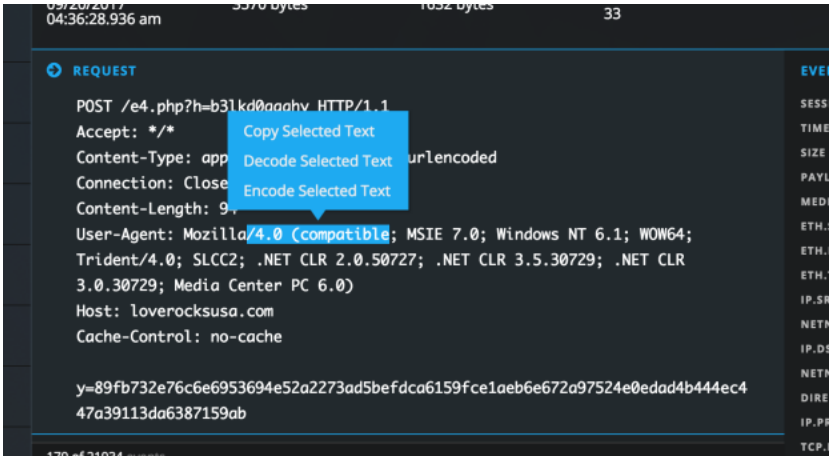
Im Folgenden finden Sie Beispiele für ein Feld mit Hover-Effekt, in dem URL-Codierung und codierter Base-64-Text angezeigt wird.





Durchführen von Codierung bzw. Decodierung im Bereich Textanalyse:

1. Navigieren Sie in der **Ansicht „Ereignisanalyse“** in den Bereich Textanalyse einer Sitzung, der codierten oder decodierten Content enthält.
2. Um decodierten Text in codierter Form anzuzeigen, ziehen Sie den Mauszeiger, um den Text innerhalb einer einzigen Anforderung oder Antwort auszuwählen.
   Ein Menü bietet Optionen zur Codierung und Decodierung.

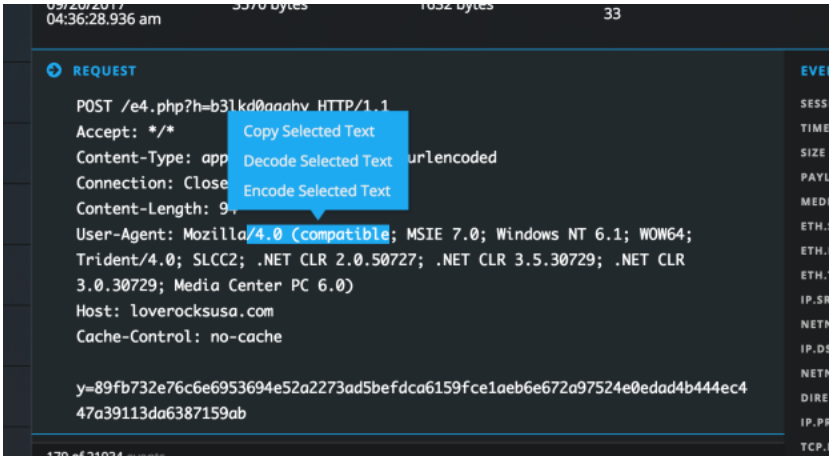


3. Klicken Sie auf **Ausgewählten Text codieren.**
   Der codierte Text wird in einem Feld mit Hover-Effekt angezeigt, das beibehalten wird, bis Sie auf das ■ klicken, anderen Text im Bereich Textanalyse wählen, den Bereich Bereich „Ereignisse“

schließen, ein anderes Ereignis für die Rekonstruktion auswählen oder zu einer anderen Rekonstruktionsansicht wechseln.

Bei Auswahl eines längeren Textes ist das Feld mit Hover-Effekt scrollbar und so groß, dass der gesamte ausgewählte Text und der dekodierte Text hinein passen.

4. Wenn die Sitzung codierten Text enthält, den Sie in decodierter Form anzeigen möchten, ziehen Sie den Mauszeiger, um den Text innerhalb einer einzigen Anforderung oder Antwort auszuwählen. Ein Menü bietet Optionen zur Codierung und Decodierung.
5. Klicken Sie auf **Ausgewählten Text codieren.**
   Der decodierte Text wird in einem Feld mit Hover-Effekt angezeigt, das beibehalten wird, bis Sie auf ✉ klicken, anderen Text im Bereich Textanalyse wählen, den Bereich Bereich „Ereignisse“ schließen, ein anderes Ereignis für die Rekonstruktion auswählen oder zu einer anderen Rekonstruktionsansicht wechseln.
6. Wenn Sie Text aus der Textrekonstruktion kopieren möchten, führen Sie einen der folgenden Schritte aus:
   a. Wählen Sie Text durch Ziehen der Maustaste aus, klicken Sie mit der rechten Maustaste und wählen Sie **Ausgewählten Text kopieren** im Menü.



   b. Ziehen Sie die Maustaste, um Text auswählen, und wählen Sie dann entweder **Ausgewählten Text decodieren** oder **Ausgewählten Text codieren**. Wählen Sie im Pop-up-Feld den

gewünschten Text und geben Sie **Steuerung-C** ein.
Der ausgewählte Text wird in die Zwischenablage kopiert und kann in eine Abfrage eingefügt werden.

7. Klicken Sie abschließend auf ■, um das Feld mit Hover-Effekt zu schließen.

Anzeigen von dekomprimiertem Text in einer HTTP-Netzwerksitzung im Bereich „Textanalyse“

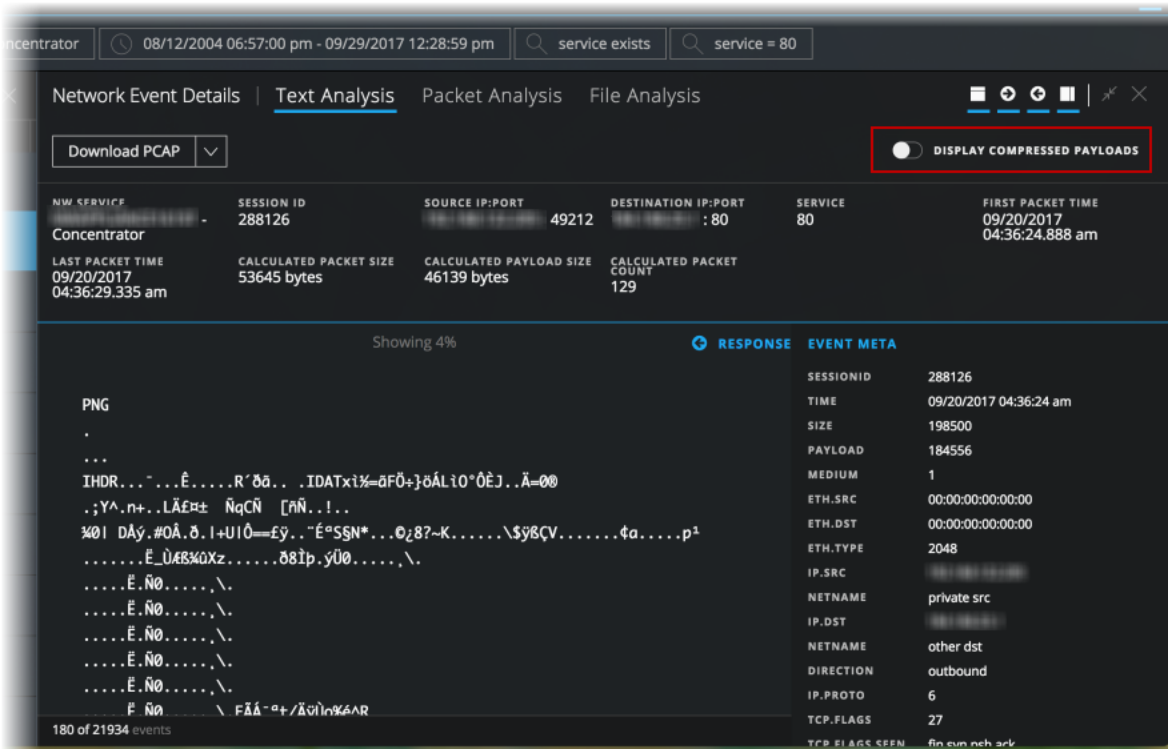
Wenn der Inhalt einer HTTP-Netzwerksitzung komprimiert wird und Sie den Bereich Textanalyse anzeigen, zeigt NetWitness Platform standardmäßig dekomprimierten Inhalt. Dies hilft Ihnen, zu bestimmen, ob Muster vorhanden sind, und Sie können die besten lesbaren Zeichen anzeigen. Sie können zwischen einer komprimierten und einer dekomprimierten Ansicht des komprimierten Texts wechseln.

Hinweis: Dekomprimierter Text ist nicht für den Bereich Paketanalyse, Dateianalyse, nicht-HTTP-Netzwerksitzungen und Protokolldaten verfügbar.

Das Umschalten zwischen komprimiertem und dekomprimiertem Text wird nur im Bereich Textanalyse angezeigt und ist nur verfügbar, wenn es komprimierten Textinhalt gibt.

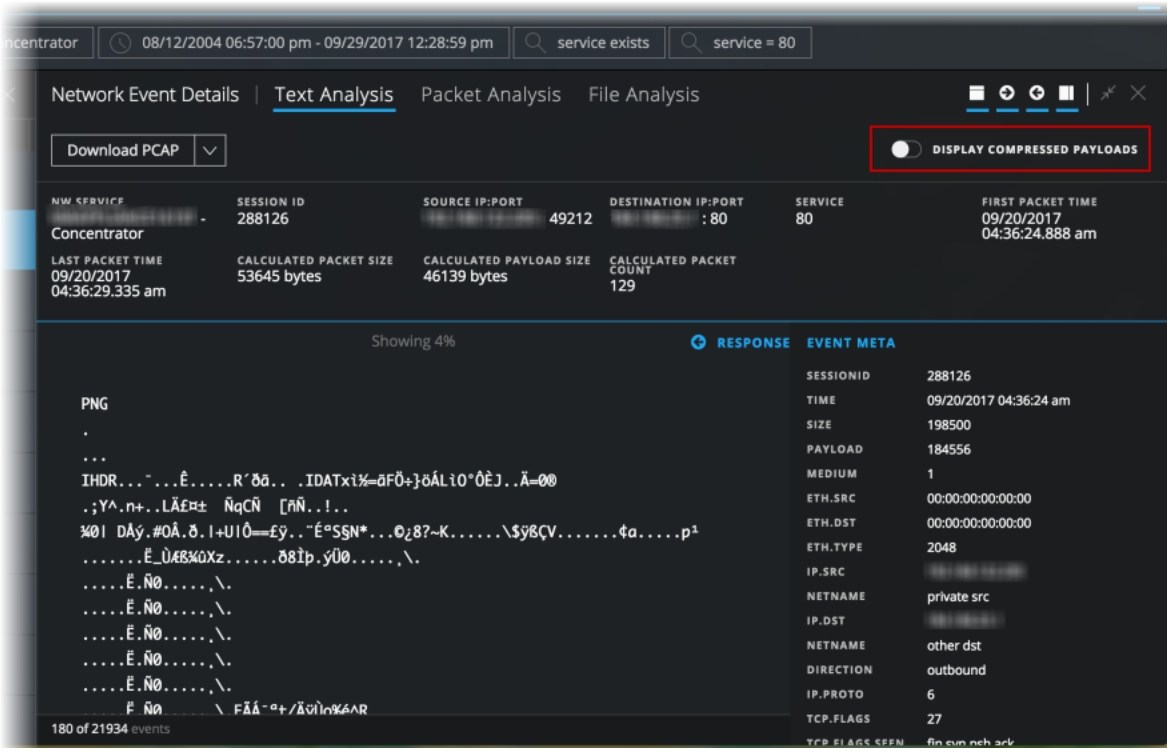
So zeigen Sie dekomprimierten Text an:

1. Öffnen Sie den Bereich Textanalyse einer HTTP-Sitzung, der komprimierten Content enthält. Standardmäßig wird die Sitzung mit dem dekomprimierten Text rekonstruiert und über der Rekonstruktion befindet sich der Umschalter **Komprimierte Nutzdaten anzeigen**.



2. Um den gleichen Text in komprimierter Form anzuzeigen, klicken Sie auf den Umschalter.
Die Ansicht ändert sich, sodass der komprimierte Text nicht mehr lesbar ist, und der Umschalter gibt

an, dass „Komprimierte Pakete anzeigen“ aktiviert ist.



3. Um zur Ansicht mit dekomprimiertem Text zurückzukehren, klicken Sie erneut auf den Umschalter.

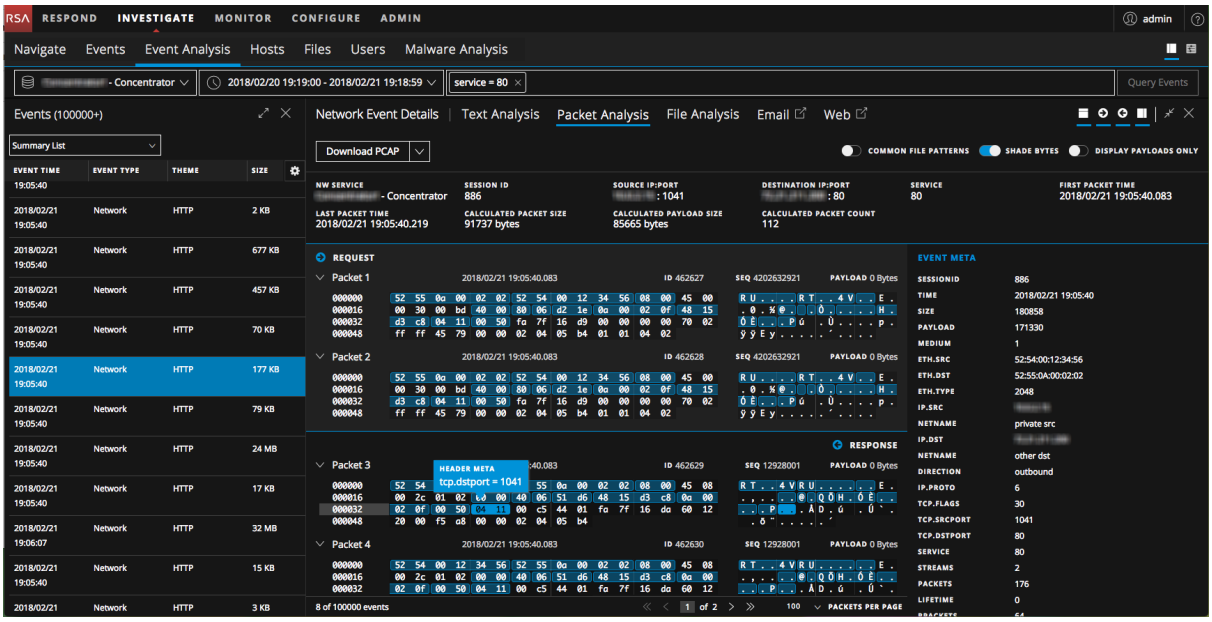
Verwenden der Option „Nur Nutzlast“ im Bereich „Paketanalyse“ einer Netzwerksitzung

Bei der Anzeige der Rekonstruktion einer Netzwerksitzung im Bereich „Paketanalyse“ können Sie auswählen, nur die Hauptnutzlast für jedes Paket anzuzeigen. Standardmäßig werden Kopf- und Fußzeilen-Bytes für jedes Paket angezeigt. Sie können diese durch Klicken auf den Umschalter „Nur Nutzdaten anzeigen“ ausblenden. Wenn Sie nur die Nutzlast-Bytes anzeigen, können Sie die Standardeinstellung wiederherstellen, indem Sie den Umschalter „Nur Nutzdaten anzeigen“ auf „Ein“ stellen. Diese Einstellung wird beibehalten, bis Sie sie ändern oder den Browser aktualisieren.

- Bei deaktivierter Option „Nur Nutzdaten anzeigen“ werden die Anzahl der Pakete, Paket-Kopfzeile, Packet-Fußzeile und Nutzdaten angezeigt.
- Bei aktivierter Option „Nur Nutzdaten anzeigen“ werden keine Kopf- und Fußzeilen-Bytes angezeigt. Nur die Paketinhalte von 16 hexadezimalen Bytes pro Zeile und das entsprechende ASCII pro Zeile werden angezeigt.

So zeigen Sie nur Nutzdaten an:

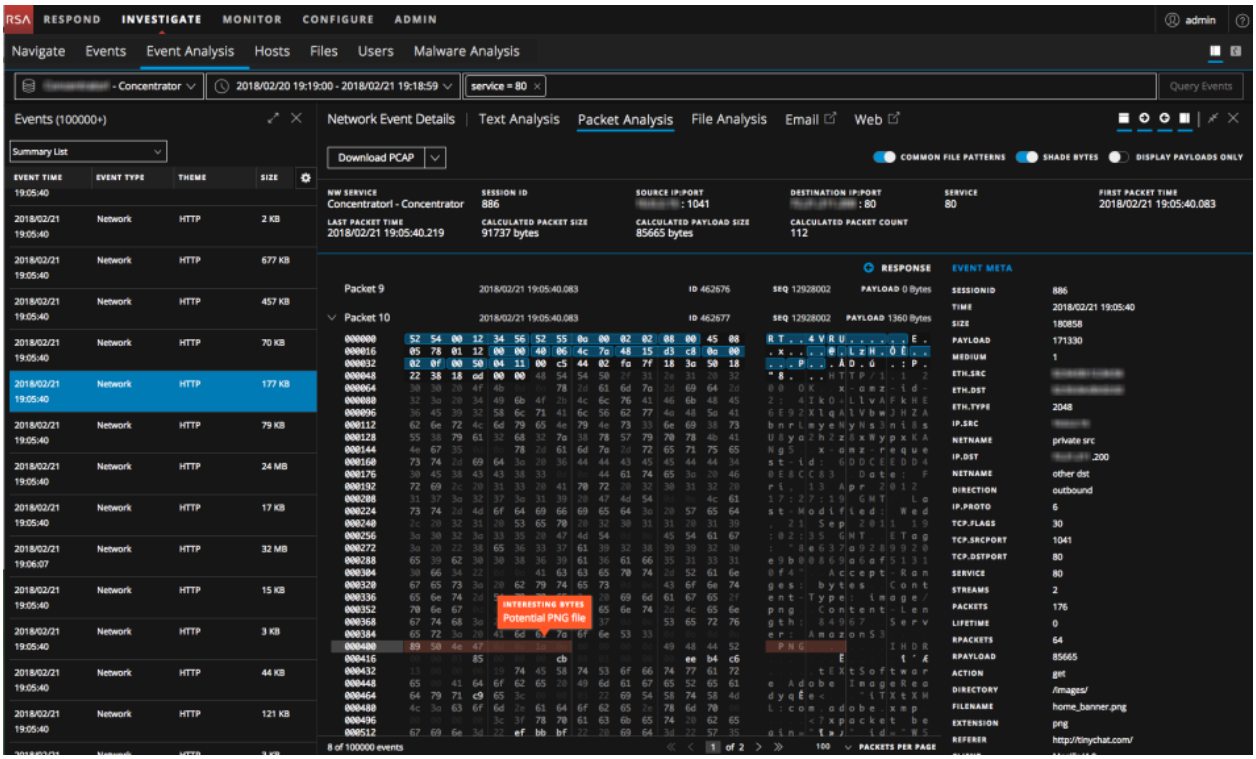
1. Navigieren Sie in der Ansicht **Ereignisanalyse** zum Bereich Paketanalyse einer Netzwerksitzung. Standardmäßig wird die Sitzung mit Anzeige von Kopfzeile, Fußzeile und Nutzlast des Pakets rekonstruiert.



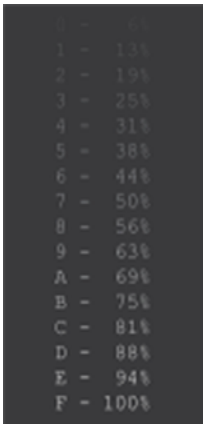
2. Um die Ansicht zu ändern und nur die Nutzlast für jedes Paket anzuzeigen, klicken Sie auf den Umschalter **Nur Nutzdaten anzeigen**.
   Die Ansicht ändert sich, sodass nur die Nutzdaten sichtbar sind und zusammenhängende Pakete auf der gleichen Seite verkettet werden, um die Nutzdaten besser lesbar und verständlich zu machen.

Anzeigen hervorgehobener Bytes im Bereich „Paketanalyse“

Beim ersten Öffnen einer Rekonstruktion im Bereich Paketanalyse werden die wichtigen Kopfzeilen-Bytes in den einzelnen Paketen blau hervorgehoben und die Nutzlast-Bytes werden anhand von Schattierung unterschieden, um Ihnen die Inhalte des Pakets verständlich zu machen. Diese Abbildung zeigt die standardmäßige Paketanalyse mit Hervorhebung und Byte-Schattierung.



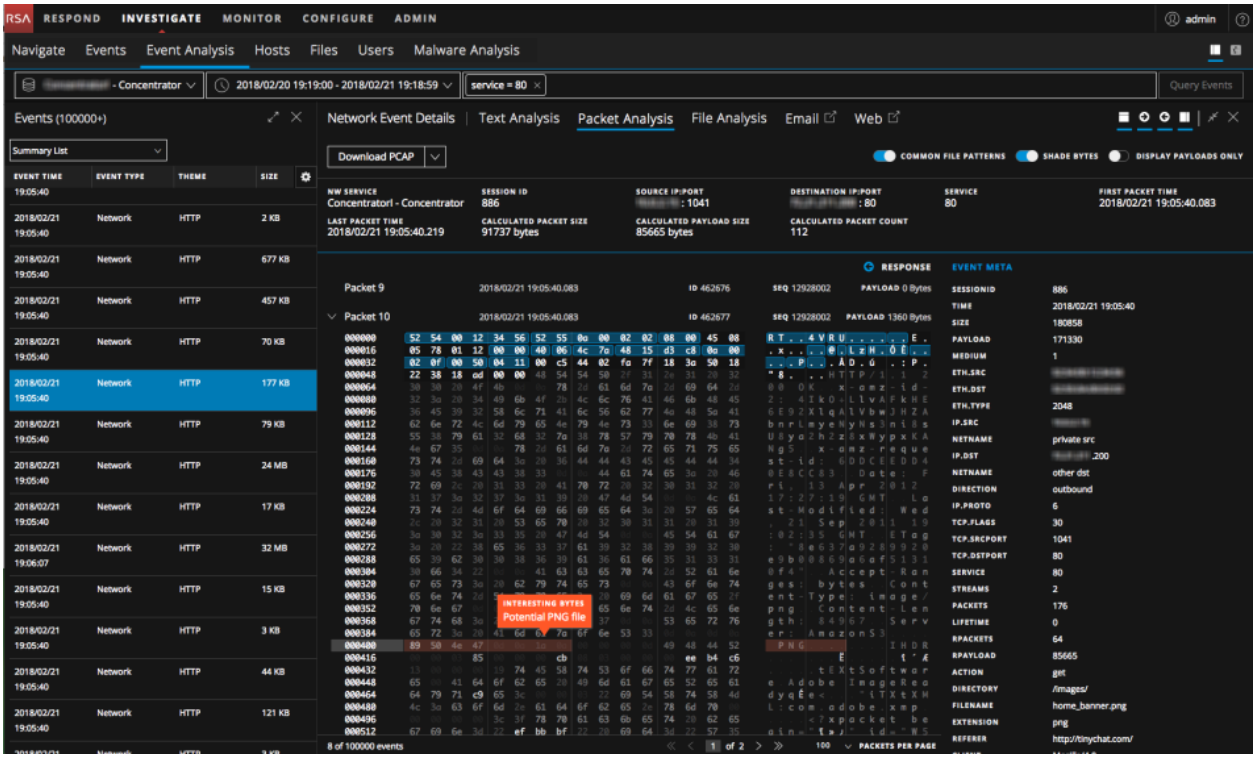
Über die Option „Byte schattieren“ wird eine Schattierung hinzugefügt. Die unterschiedlichen Hexadezimalbytes (00 bis FF) werden dann verschieden stark hervorgehoben. Bytes nahe dem unteren Bereich sind transparenter und Bytes, die sich 255 annähern, sind undurchsichtiger. Hexadezimal- und ASCII-Bytes werden schattiert. Dies ist ein Beispiel für die Schattierung jedes hexadezimalen Byte.



Der Umschalter „Byte schattieren“ steuert die Schattierung der Bytes. Wenn Sie „Byte schattieren“ ein- oder ausschalten, wird die Einstellung beibehalten, bis Sie sie ändern oder den Browser aktualisieren.

Hervorheben gängiger Dateitypen im Bereich „Paketanalyse“

Im Bereich „Paketanalyse“ können Analysten die Hervorhebung bestimmter gängiger Dateitypen basierend auf der Signatur der Datei anzeigen oder ausblenden. Bei Aktivierung der Funktion „Gebräuchliche Dateimuster“ werden die Bytes der magischen Zahl in der Dateisignatur in der Nutzlast hervorgehoben und Sie können den Mauszeiger über die Hervorhebung bewegen, um den potenzielle Dateityp anzuzeigen. In diesem Beispiel ist `89 50 4e 47` in der hexadezimalen Nutzlast hervorgehoben und `PNG` ist in der ASCII-Nutzlast hervorgehoben. Wenn Sie den Mauszeiger über die hervorgehobenen Bytes bewegen, wird der potenzielle Dateityp für die magische Zahl in einem Kasten mit Hover-Effekt angezeigt.



Dies sind die Dateitypen und die entsprechenden magischen Zahlen, die ggf. in der Nutzlast hervorgehoben werden:

Dateityp	Hexadezimale Signatur	ASCII-Codierung
Ausführbare DOS-Datei/Windows PE	4D 5A	MZ
Portable Network Graphics (PNG)	89 50 4E 47 0D 0A 1A 0A	PNG
JPEG	FF D8 FF	JPEG
JPEG/JFIF	4A 46 49 46	JFIF
JPEG/EXIF	45 78 69 66	EXIF

Dateityp	Hexadezimale Signatur	ASCII-Codierung
GIF	47 49 46 38 37 61	GIF87a
GIF	47 49 46 38 39 61	GIF89a
Nicht portable ausführbare Datei	5A 4D	ZM
BMP	42 4D	BM
PDF	25 50 44 46	%PDF
Altes Office-Dokument (DOC, XLS, PPT, MSG und andere)	D0 CF 11 E0 A1 B1 1A E1	ÐÏ.à¡±.á
ZIP-Dateiformate und darauf basierende Formate, z. B. JAR, ODF, OOXML	50 4B	PK..
7-Zip-Dateiformat (7z)	37 7A BC AF 27 1C	7z¼¯'
Java-Klassendatei, Mach-O Fat-Binärdatei	CA FE BA BE	Êþº¾
PostScript	25 21 50 53	%!PS
UNIX/Linux-Shell-Skript	23 21	#!
Ausführbare Dateien und ausführbare Dateien im Executable and Linking Format (ELF)	7F 45 4C 46	.ELF

So zeigen Sie gängige Dateisignaturen im Bereich „Paketanalyse“ an:

1. Navigieren Sie zum Bereich „Paketanalyse“ und aktivieren Sie die Option **Gebräuchliche Dateimuster**.
   Wenn es mehr als eine Hervorhebung in der Ansicht gibt, werden alle angezeigt.
2. Um das Feld mit Hover-Effekt anzuzeigen, platzieren Sie den Mauszeiger über der Hervorhebung.

Suchen von zusätzlichem Kontext in der Ansicht „Ereignisanalyse“

Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.2 und höher.In früheren Versionen können Sie auch zusätzlichen Kontext in der Ansicht „Navigation“ oder „Ereignisse“ suchen, wie unter Suchen von weiteren Kontexten in den Ansichten „Navigation“ und „Ereignisse“ beschrieben.

In der Ansicht „Ereignisanalyse“ oder der Ansicht „Navigation“ können Sie Details und Informationen zu Elementen nachschlagen, die mit einem Ereignis im Context Hub verknüpft sind. Diese Elemente oder Entitäten sind Kennungen, z. B. eine IP-Adresse, ein Benutzername, ein Hostname, ein Domain-Name, ein Dateiname oder ein Datei-Hash. Die Daten aus konfigurierten Quellen wie RSA NetWitness Endpoint können Ihnen helfen, die Vorfälle zu verstehen.

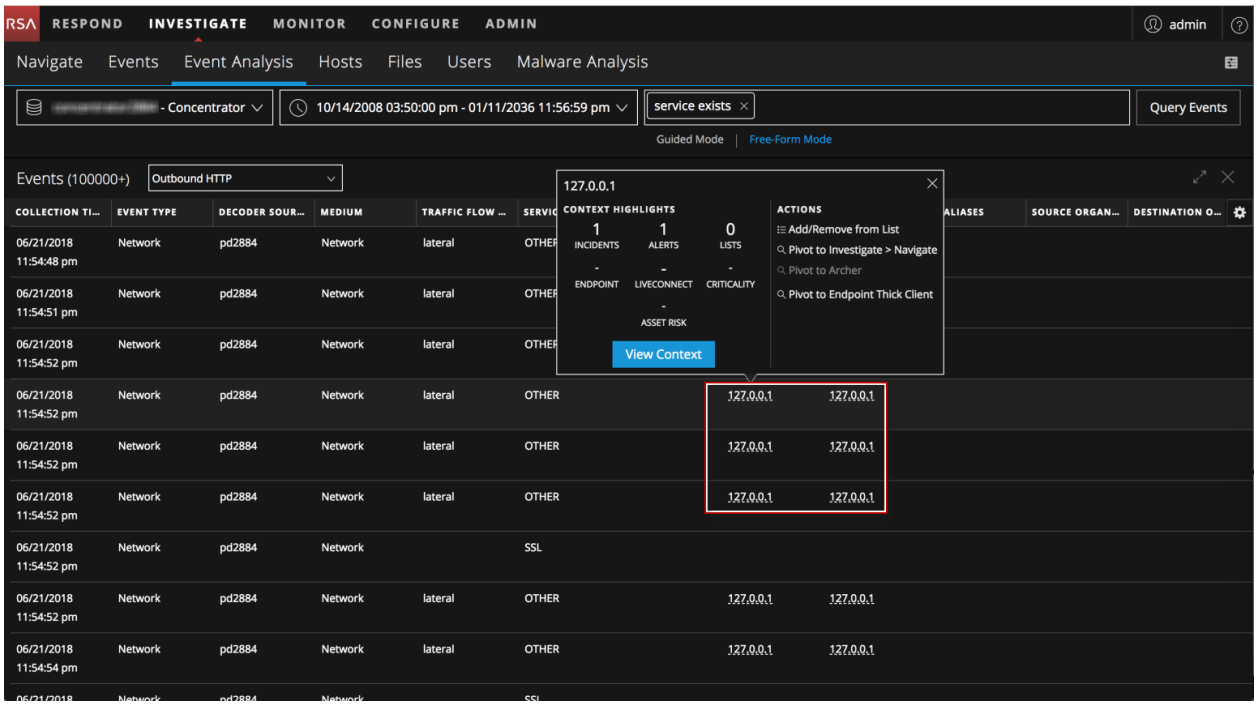
Hinweis: Damit Sie kontextbezogene Informationen anzeigen können, muss Ihr Administrator den Context-Hub-Service in RSA NetWitness Platform hinzufügen und Datenquellen für den Context-Hub-Service konfigurieren wie im *Context-Hub-Konfigurationsleitfaden* beschrieben. Analysten müssen eine Rolle mit der Berechtigung `Context Lookup` haben, wie unter „Rollenberechtigungen“ und „Managen von Nutzern mit Rollen und Berechtigungen“ im Handbuch *Systemsicherheit und Benutzerverwaltung* beschrieben wird. Navigieren Sie zu Masterinhaltsverzeichnis, worüber alle Dokumente für NetWitness Platform Logs & Network 11.x aufgerufen werden können.

Der Context Hub ist ein zentralisierter Service, der Daten zu Entitäten aus mehreren konfigurierbaren Datenquellen aggregiert. Diese Daten können Ihre Untersuchung durch zusätzlichen Kontext über die sofortigen Ergebnisse einer bestimmten Abfrage hinaus erweitern. Zum Beispiel kann Ihnen der Context Hub sagen, ob eine bestimmte Entität in Incidents, Warnmeldungen, Feeds oder Veröffentlichungen von Communityinformationen erwähnt wurde.

Im Bereich „Ereignisse“, der Kopfzeile des Ereignisses oder dem Bereich „Ereignis-Metadaten“ werden unterstrichene Entitäten angezeigt. Wenn eine Entität unterstrichen ist, werden Informationen zu diesem Entitätentyp in Context Hub von NetWitness Platform aufgefüllt. Möglicherweise sind zusätzliche Informationen zu dieser Entität im Context Hub verfügbar.

Hinweis: Active Directory-Entitäten mit verfügbaren Kontextinformationen sind nicht unterstrichen, aber Sie können den Mauszeiger über diese Entitäten bewegen, um zu sehen, ob Kontextinformationen verfügbar sind.

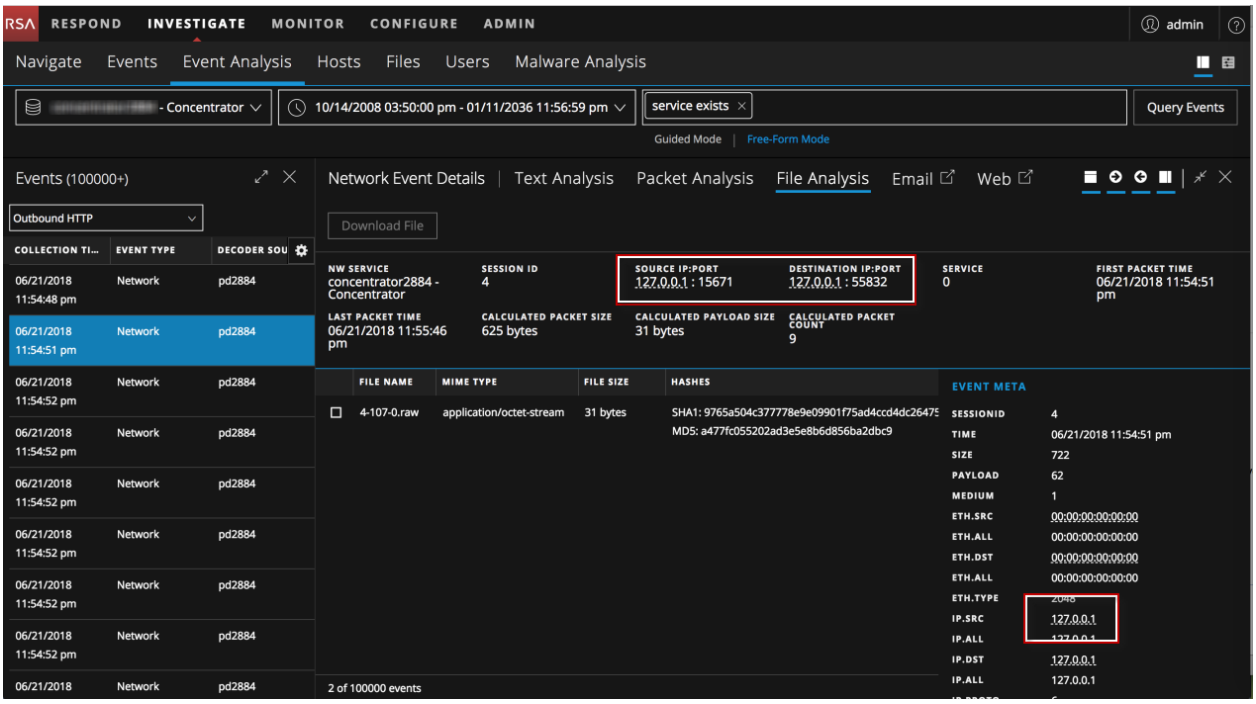
In der folgenden Abbildung werden unterstrichene Entitäten im Bereiche „Ereignisse“ mit dem geöffneten Kontextwerkzeug dargestellt.



Die Kontext-Kurzinformation besteht aus zwei Abschnitten: Kontexthighlights und -aktionen.

- Die Informationen im Abschnitt Kontexthighlights helfen Ihnen, die Aktionen zu bestimmen, die Sie durchführen möchten. Es können verwandte Daten für Incidents, Warnmeldungen, Listen, Endpunkt, Live Connect, Bedeutung und Risiko für Bestände angezeigt werden. Abhängig von Ihren Daten können Sie möglicherweise auf diese Elemente klicken, um weitere Informationen anzuzeigen.
- Im Abschnitt Aktionen werden die verfügbaren Aktionen aufgeführt. Im obigen Beispiel sind die Optionen „Zu Liste hinzufügen/Aus Liste entfernen“, „Zu „Ermittlungen“ > Navigation“ wechseln“, „Zu Archer wechseln“ und „Zu Endpunkt-Thick-Client wechseln“ verfügbar.

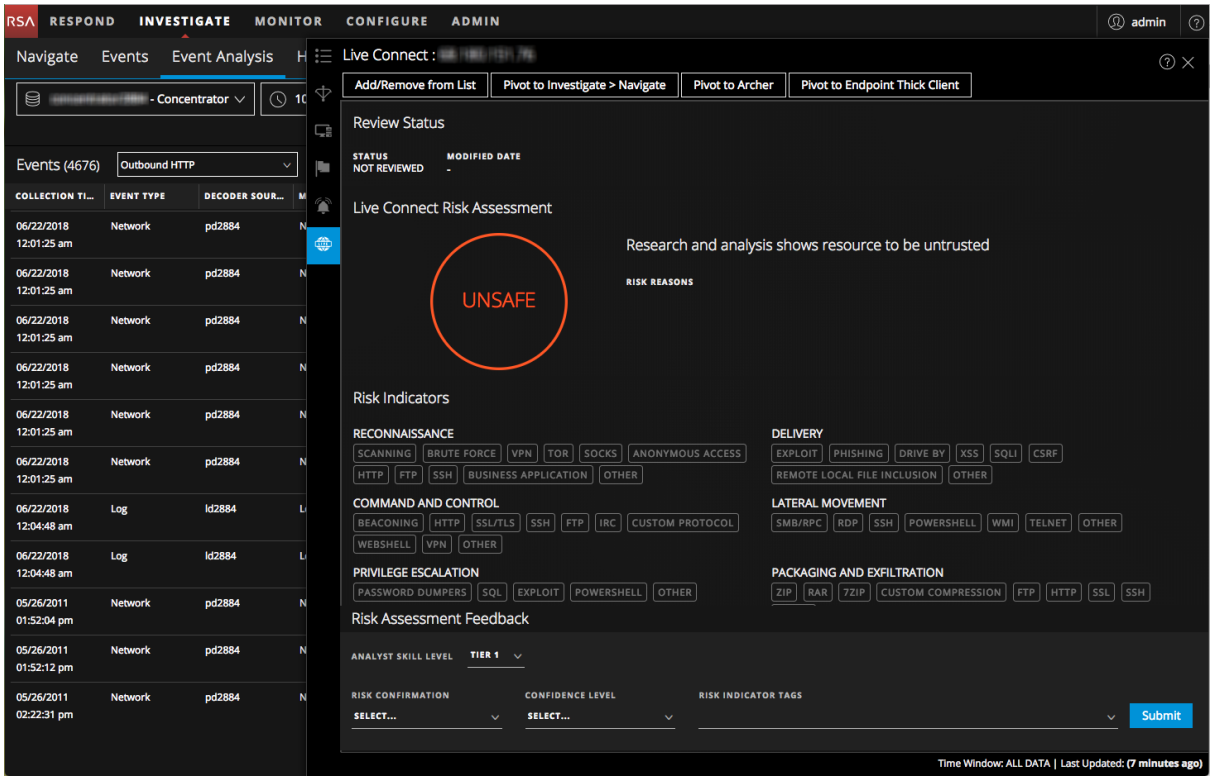
In der folgenden Abbildung sind unterstrichene Entitäten in den Bereichen „Ereignis-Kopfzeile“ und „Ereignis-Metadaten“ dargestellt.



Wenn Sie in den Kontext-Kurzinformationen auf „Kontext anzeigen“ klicken, fragt der Context Hub die konfigurierten Datenquellen nach relevanten Informationen ab und auf der rechten Seite des Browserfensters wird der Bereich für die Kontextabfrage geöffnet. Der Bereich „Kontextabfrage“ wird mit den Informationen aus dem Context Hub gefüllt, sobald diese verfügbar sind. Im Bereich „Kontextabfrage“ können Sie einzelne Datenquellen anzeigen und weiter durchsuchen. Eine detaillierte Beschreibung der Informationen, die für jede Datenquelle im Bereich „Kontextabfrage“ angezeigt werden, finden Sie unter Bereich „Kontextabfrage“. Sie können auch alle verfügbaren Aktionen im Abschnitt „Aktionen“ durchführen.

So zeigen Sie Informationen im Bereich „Kontextabfrage“ in der Ansicht „Ereignisanalyse“ an:

1. Bewegen Sie den Mauszeiger über verschiedene Metawerte, um die für die Daten verfügbaren Datenquellen anzuzeigen.
   In einer Kontext-Kurzinformation wird eine Liste der für die ausgewählten Metawerte verfügbaren Kontextdaten angezeigt.
2. Klicken Sie in den Kontext-Kurzinformationen auf **Kontext anzeigen**, um den Bereich „Kontextabfrage“ zu öffnen.
   Der Bereich „Kontextabfrage“ wird auf der rechten Seite des Browserfensters geöffnet. Der Bereich „Kontextabfrage“ wird mit den Informationen aus dem Context Hub gefüllt, sobald diese verfügbar sind.



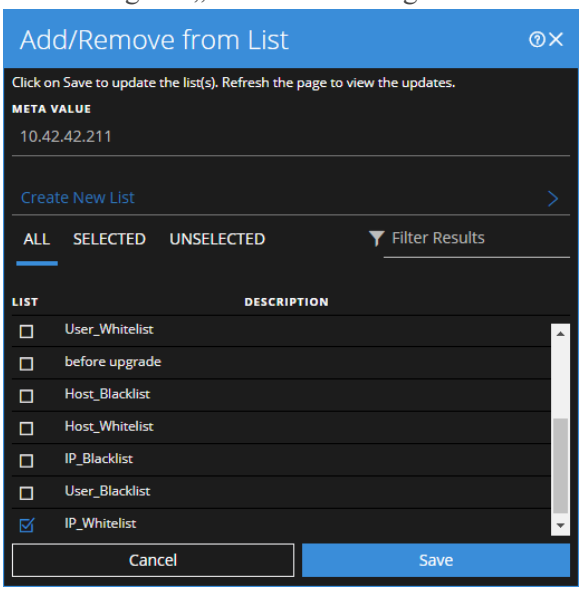
3. Zum Durchführen von Aktionen für eine Entität wählen Sie eine der verfügbaren Aktionen in den Kontext-Kurzinformationen aus: Zu Liste hinzufügen/Aus Liste entfernen, Zu „Ermittlungen“ > „Navigation“ wechseln, Zu Archer wechseln, Zu Endpunkt-Thick-Client wechseln. Weitere Informationen finden Sie unter Wechseln zu „Ermittlungen“ > „Navigation“, Wechseln zu Archer, Wechseln zu NetWitness Endpoint-Thick-Client und Hinzufügen einer Entität zu einer Whitelist.

Hinweis: Die Aktion „Zu Archer wechseln“ ist deaktiviert, wenn die Archer-Daten nicht verfügbar sind oder wenn die Archer-Datenquelle nicht reagiert. Überprüfen Sie, ob die RSA Archer-Konfiguration aktiviert und richtig konfiguriert ist. Das Gleiche gilt für „Zu NetWitness Endpoint-Thick-Client wechseln“. Wenn diese Option deaktiviert ist, überprüfen Sie, ob der NetWitness Endpoint-Thick-Client korrekt installiert und konfiguriert ist.

Hinzufügen einer Entität zu einer Whitelist

Sie können eine beliebige unterstrichene Entität aus einer Kontext-Kurzinformation zu einer Liste, etwa einer Whitelist oder Blacklist, hinzufügen. Zum Beispiel können Sie zur Reduzierung falsch positiver Ergebnisse eine unterstrichene Domain zur eine Whitelist hinzufügen, um sie aus den verwandten Entitäten auszuschließen.

1. Bewegen Sie den Mauszeiger in den Bereichen „Ereignisse“, „Ereignis-Kopfzeile“ oder „Ereignis-Metadaten“ über die unterstrichene Entität, die Sie einer Context-Hub-Liste hinzufügen möchten. (Active Directory-Entitäten mit Kontextdaten können ebenfalls hinzugefügt werden, werden aber nicht unterstrichen.)
   Ein Kontextwerkzeug mit den verfügbaren Aktionen wird angezeigt.
2. Klicken Sie im Abschnitt **AKTIONEN** der Kurzinformation auf **Zu Liste hinzufügen/Aus Liste entfernen**.
   Das Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ zeigt die verfügbaren Listen.



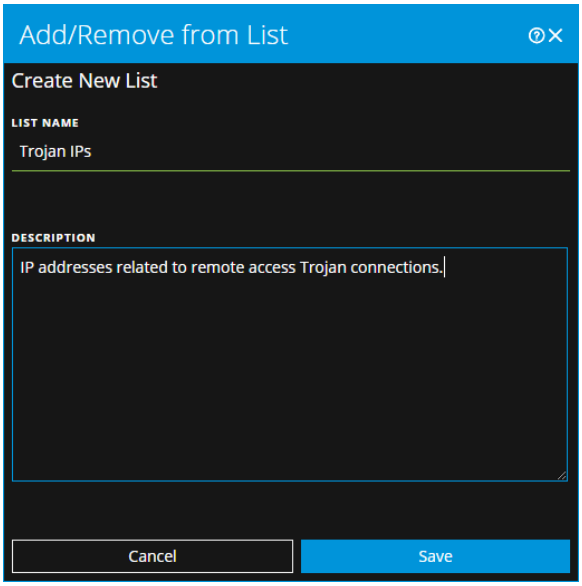
3. Wählen Sie eine oder mehrere Listen aus und klicken Sie auf **Speichern**.
   Die Entität wird den ausgewählten Listen hinzugefügt. Das Dialogfeld Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“bietet zusätzliche Informationen.

Eine Liste erstellen

Sie können Listen im Context Hub aus der Ansicht „Ereignisanalyse“ erstellen. Abgesehen von der Verwendung von Listen für Whitelist- und Blacklist-Entitäten können Sie Listen verwenden, um Entitäten auf abnormales Verhalten zu überwachen. Beispielsweise können Sie zur Verbesserung der Sichtbarkeit einer verdächtigen IP-Adresse und Domain unter Investigation diese in zwei separate Listen übernehmen. Eine Liste könnte für Domains sein, die verdächtigt werden, mit Befehls- und Kontrollverbindungen in Zusammenhang zu stehen, und eine andere Liste könnte für IP-Adressen sein, die mit Remotezugriffen über Trojaner-Verbindungen in Zusammenhang stehen. Sie können dann Indikatoren für Infizierungen anhand dieser Listen identifizieren.

So erstellen Sie eine Liste in Context Hub:

1. Bewegen Sie den Mauszeiger in den Bereichen „Ereignisse“, „Ereignis-Kopfzeile“ oder „Ereignis-Metadaten“ über die unterstrichene Entität, die Sie einer Context-Hub-Liste hinzufügen möchten. (Active Directory-Entitäten mit Kontextdaten können ebenfalls zu einer neuen Liste hinzugefügt werden, werden aber nicht unterstrichen.)
   Ein Kontextwerkzeug mit den verfügbaren Aktionen wird angezeigt.
2. Klicken Sie im Abschnitt **AKTIONEN** der Kurzinformation auf **Zu Liste hinzufügen/Aus Liste entfernen**.
3. Klicken Sie im Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ auf **Neue Liste erstellen**.



4. Geben Sie einen eindeutigen **LISTENNAMEN** für die Liste ein. Bei dem Listennamen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
5. (Optional) Geben Sie eine **BESCHREIBUNG** für die Liste ein.
   Analysten mit den entsprechenden Berechtigungen können Listen auch im CSV-Format exportieren, um sie für die weitere Nachverfolgung und Analyse an andere Analysten zu senden. Im *Context Hub-Konfigurationsleitfaden* finden Sie zusätzliche Informationen.

Wechseln zu „Ermittlungen“ > „Navigation“

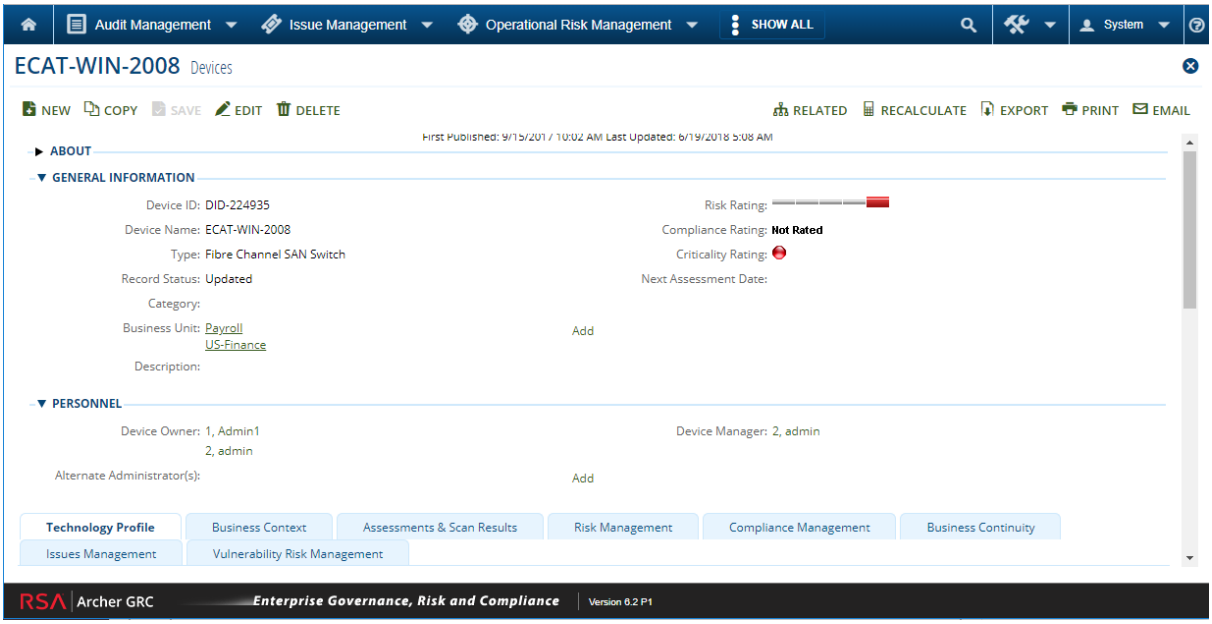
Für eine gründlichere Ermittlung einer Entität können Sie die Ansicht „Navigation“ öffnen.

1. Bewegen Sie den Mauszeiger in den Bereichen „Ereignisse“, „Ereignis-Kopfzeile“ oder „Ereignis-Metadaten“ über eine beliebige unterstrichene Entität. (Active Directory-Entitäten mit Kontextdaten können ebenfalls untersucht werden, werden aber nicht unterstrichen.)
2. Wählen Sie im Abschnitt **AKTIONEN** der Kurzinformation **Zu „Ermittlungen“ > „Navigation“ wechseln** aus.
   Die Ansicht „Navigation“ wird geöffnet, sodass Sie eine umfassendere Ermittlung durchführen können. Weitere Informationen finden Sie unter Untersuchen von Metadaten in der Ansicht „Navigation“.

Wechseln zu Archer

Wenn Sie mehr Details zum Gerät in RSA Archer® Cyber Incident & Breach Response anzeigen möchten, können Sie auf die Seite mit den Gerätedetails wechseln. Diese Informationen werden nur für IP-Adresse, Host und Mac-Adresse angezeigt.

1. Bewegen Sie den Mauszeiger in den Bereichen „Ereignisse“, „Ereignis-Kopfzeile“ oder „Ereignis-Metadaten“ über eine unterstrichene Entität (IP-Adresse, Host und Mac-Adresse).
2. Wählen Sie im Abschnitt **AKTIONEN** der Kurzinformation **Zu Archer wechseln** aus.
3. Wenn Sie in der Anwendung angemeldet sind, wird die Seite mit den Gerätedetails in **Reaktion auf Cyber-Incidents und Sicherheitsverletzungen von RSA Archer** geöffnet. Anderenfalls wird der Anmeldebildschirm angezeigt.



Hinweis: Der Link „Zu Archer wechseln“ ist deaktiviert, wenn die Archer-Daten nicht verfügbar sind oder wenn die Archer-Datenquelle nicht reagiert. Überprüfen Sie, ob die RSA Archer-Konfiguration aktiviert und richtig konfiguriert ist.

Weitere Informationen finden Sie im *Archer-Integrationsleitfaden*.

Wechseln zu NetWitness Endpoint-Thick-Client

Wenn bei Ihnen die NetWitness Endpoint-Thick-Clientanwendung installiert ist, können Sie sie über die Kontext-Kurzinformation starten. Von dort können Sie verdächtige IP-Adressen, Hosts oder MAC-Adressen weiter untersuchen.

1. Bewegen Sie den Mauszeiger in den Bereichen „Ereignisse“, „Ereignis-Kopfzeile“ oder „Ereignis-Metadaten“ über eine beliebige unterstrichene Entität.
2. Wählen Sie im Abschnitt **AKTIONEN** der Kurzinformation **Zu Endpunkt-Thick-Client wechseln** aus.
   Die NetWitness Endpoint-Thick-Clientanwendung wird außerhalb des Webbrowsers geöffnet.

Hinweis: Version 4.4 des NetWitness Endpoint (NWE)-Thick-Client muss auf demselben Server installiert sein, die NWE-Metaschlüssel müssen in der `table-map.xml`-Datei auf dem Log Decoder und die NWE-Metaschlüssel müssen in der `index-concentrator-custom.xml`-Datei vorhanden sein. Der NWE-Thick-Client ist eine reine Windows-Anwendung. Umfassende Anweisungen zur Installation finden Sie im *NetWitness Endpoint-Benutzerhandbuch* für Version 4.4.

Herunterladen von Daten in der Ansicht „Ereignisanalyse“

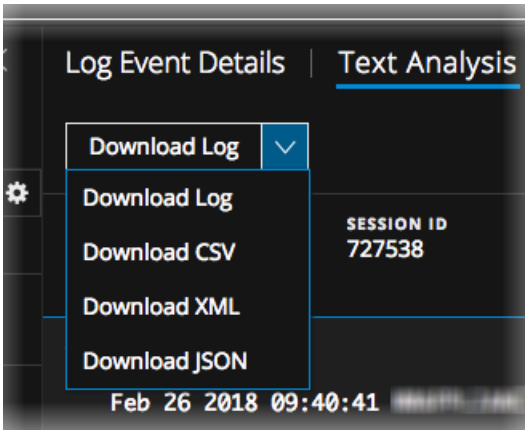
In der Ansicht „Ereignisanalyse“ können Sie Ereignisse, Protokolle und Dateien herunterladen.

Herunterladen eines Protokolls im Bereich „Textanalyse“

Beim Anzeigen einer Protokollrekonstruktion in Bereich Textanalyse können Sie eine Protokolldatei mithilfe der Optionen im Drop-down-Menü „Download-Protokoll“ in den folgenden Formaten herunterladen:

- Rohdatenprotokoll (Protokoll) mithilfe der Option **Download-Protokoll**
- Durch Kommas getrennte Werte (CSV) mithilfe der Option **CSV herunterladen**
- Extensible Markup Language (XML) mithilfe der Option **XML herunterladen**
- JavaScript Object Notation (JSON) mithilfe der Option **JSON herunterladen**

Dies ist ein Beispiel für eine Protokollrekonstruktion, wobei die Menüoptionen für „Download-Protokoll“ angezeigt werden.



Hinweis: Die Option „Download-Protokoll“ ist nur für Endpoint-Ereignisse mit mindestens einem Metawert von mehr als 256 Zeichen anwendbar. Für ein Endpoint-Ereignis wird das Raw-Protokoll nur dann ausgefüllt, wenn der Metawert 256 Zeichen überschreitet. Dateien, die über längere Zeiträume ausgeführt oder in der Vergangenheit heruntergeladen wurden, können nicht heruntergeladen werden. Zum Beispiel können Metawerte wie Startargumente 256 Zeichen überschreiten. In diesem Fall stehen 256 Zeichen als Metawert zur Verfügung, während der vollständige Wert im Raw-Protokoll verfügbar ist.

Die heruntergeladene Protokolldatei enthält das Protokoll und wird mit dem Namen des Services, auf dem das Protokoll erfasst wurde, der Sitzungs-ID und dem Dateityp benannt. Dies ist ein Beispiel des Dateinamens für ein Rohdatenprotokoll: **Concentrator_SID2.log**. Die exportierte Protokolldatei wird nach der folgenden Konvention benannt:

```
<service-ID or host name>_SID<n>.<filetype>
```

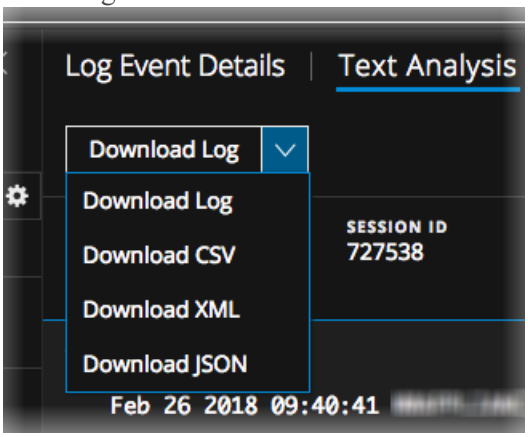
Hierbei gilt:

- `<service-ID or host name>` ist der Name des Services (z. B. ein Concentrator oder Broker), in dem die Sitzung gespeichert wurde.
- `SID<n>` ist die Sitzungs-ID-Nummer.
- `<filetype>` gibt das Format des heruntergeladenen Protokolls an. Dies sind die möglichen Protokolltypen: Rohdatenprotokoll, CSV, XML und JSON. Standardmäßig ist das Format ein Rohdatenprotokoll.

Hinweis: Einige Formate besitzen keine Zeitstempel oder Geräte-IP, an der das Ereignis erzeugt wurde, weshalb ein in CSV, XML oder JSON heruntergeladenes Protokoll zusätzlich zum Inhalt des Rohdatenprotokolls einen Wert namens `timestamp` hat. Die zusätzlichen Informationen im Protokoll weisen das folgende Format auf: `Log timestamp="1490824512" source="10.12.35.65"`.

So laden Sie das Protokoll für eine Sitzung herunter:

Wählen Sie im Bereich Textanalyse eines Protokollereignisses eines der Dateiformate für das heruntergeladene Protokoll.
- Um das Protokoll als ein Rohdatenprotokoll (das Standardformat) herunterzuladen, klicken Sie auf **Download-Protokoll**.
- Um das Protokoll in einem der anderen Formate herunterzuladen, klicken Sie auf den Pfeil nach unten auf der Schaltfläche **Download-Protokoll** und wählen Sie eines der Dateiformate für das heruntergeladenen Protokoll.



Die Protokolldatei wird im angegebenen Format auf Ihr lokales Dateisystem heruntergeladen. Wenn Sie einen Download starten und die Ansicht verlassen, während das Protokoll extrahiert wird und bevor der Download des Protokolls gestartet wird, wird das Protokoll nicht in Ihren Browser heruntergeladen. Eine Meldung benachrichtigt Sie, dass Sie das heruntergeladene Protokoll in der Jobwarteschlange finden.

Herunterladen von Netzwerkereignisdaten im Bereich „Textanalyse“ oder „Paketanalyse“

Beim Anzeigen eines rekonstruierten Netzwerkereignisses im Bereich Paketanalyse oder Textanalyse Bereich können Sie Netzwerk-Datendateien zur weiteren Analyse exportieren. Der Download enthält Ereignisse für den aktuellen Zeitbereich und Drill-down-Punkt. Sie können die Daten in den folgenden Formaten herunterladen:

- Das gesamte Ereignis als eine Paketerfassung (`*.pcap`) mithilfe der Option **PCAP herunterladen**.
- Die Nutzlast als eine `*.payload`-Datei mithilfe der Option **Alle Nutzdaten herunterladen**.
- Die Anforderungsnutzlast als eine `*.payload1`-Datei mithilfe der Option **Anforderungsnutzdaten herunterladen**.
- Die Antwortnutzlast als eine `*.payload2`-Datei mithilfe der Option **Antwortnutzdaten herunterladen**.

Dies ist ein Beispiel des Dateinamens für eine PCAP-Datei: `C01 - Concentrator_SID1697309.pcap`. Die exportierte Netzwerkdatendatei wird nach der folgenden Konvention benannt:

`<service-ID or host name>_SID<n>.<filetype>`

Hierbei gilt:

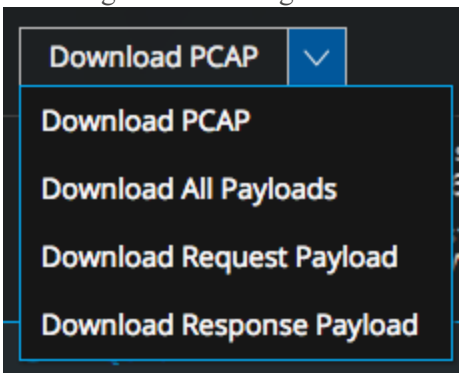
- `<service-ID or host name>` ist der Name des Services (z. B. ein Concentrator oder Broker), in dem die Sitzung gespeichert wurde.
- `SID<n>` ist die Sitzungs-ID-Nummer.
- `<filetype>` ist pcap, payload, payload1 oder payload2.

Die Netzwerkdaten werden direkt in Ihren Browser heruntergeladen, wenn der Download schnell ist. Wenn der Download aufgrund von Netzwerkfaktoren oder Dateigröße länger dauert, wird die Datei wird im Hintergrund heruntergeladen und die Aufgabe wird in der Jobs-Warteschlange nachverfolgt. In diesem Fall können Sie Ihre Jobs in der Warteschlange prüfen und die Datei abrufen, wenn der Download abgeschlossen ist.

Hinweis: Wenn Sie einen Download starten und die Ansicht verlassen, während die Datei extrahiert wird und bevor der Download der Datei gestartet wird, wird die Datei nicht in Ihren Browser heruntergeladen. Eine Meldung benachrichtigt Sie, dass Sie das heruntergeladene Dokument in der Jobwarteschlange finden.

So exportieren ein Ereignis als eine Netzwerk-Datendatei:

Navigieren Sie zum Bereich Paketanalyse eines Netzwerkereignisses und wählen Sie eines der Dateiformate für die heruntergeladene Datei.
- Um das Ereignis als PCAP-Datei (das Standardformat) herunterzuladen, klicken Sie auf **PCAP herunterladen**.
- Um das Ereignis in einem der anderen Formate herunterzuladen, klicken Sie auf den Pfeil nach unten auf der Schaltfläche **PCAP herunterladen** und wählen Sie eines der Dateiformate für die heruntergeladenen Ereignisdaten.



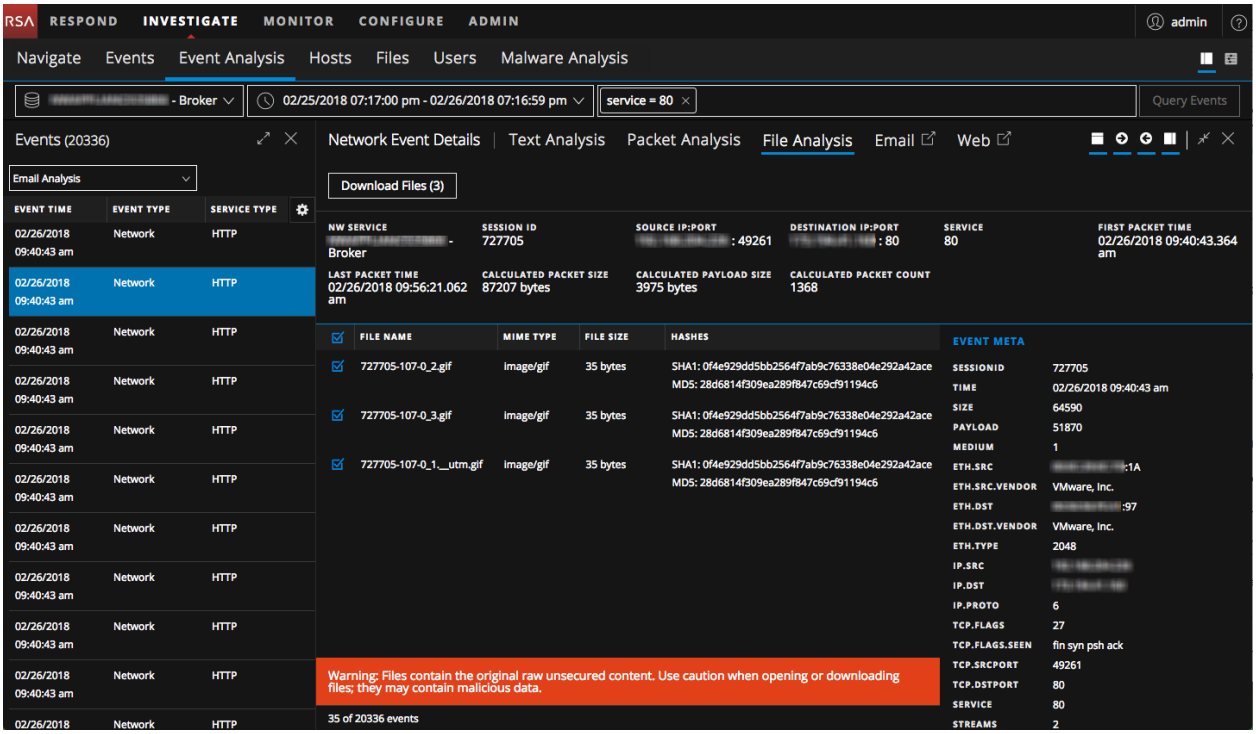
Die Netzwerkdatendatei wird im angegebenen Format auf Ihr lokales Dateisystem heruntergeladen.

Herunterladen von Dateien aus einem Netzwerkereignis im Bereich „Dateianalyse“

Bei der Anzeige von rekonstruierten Netzwerkereignissen, die Dateien im Bereich Dateianalyse enthalten, können Sie eine Datei, eine oder mehrere Dateien oder alle Dateien für den Download in Ihr lokales Dateisystem auswählen.

Hinweis: Wenn Sie einen Download starten und die Ansicht verlassen, während die Datei extrahiert wird und bevor der Download der Datei gestartet wird, wird die Datei nicht in Ihren Browser heruntergeladen. Eine Meldung benachrichtigt Sie, dass Sie die heruntergeladene Datei in der Jobwarteschlange finden.

Wenn Dateien ausgewählt sind, wird die Schaltfläche „Dateien herunterladen“ aktiv und gibt die Anzahl der ausgewählten Dateien. an.



Durch Klicken auf die Schaltfläche werden die ausgewählten Dateien als passwortgeschütztes Zip-Archiv exportiert. Das Passwort zum Öffnen des exportierten Archivs lautet `netwitness`. Durch das Exportieren der Dateien in dieser Form wird sichergestellt, dass:

- Das Archiv wird nicht durch eine Virenschutzsoftware isoliert.
- Potenziell schädliche Dateien werden nicht automatisch von der Standardanwendung geöffnet und ausgeführt.

Dies ist ein Beispiel des Dateinamens für ein Archiv: `C01 - Concentrator_SID1697309_FC1.zip`. Das exportierte Archiv wird nach der folgenden Konvention benannt:

`<service-ID or host name>_SID<n>_FC<n>.zip`

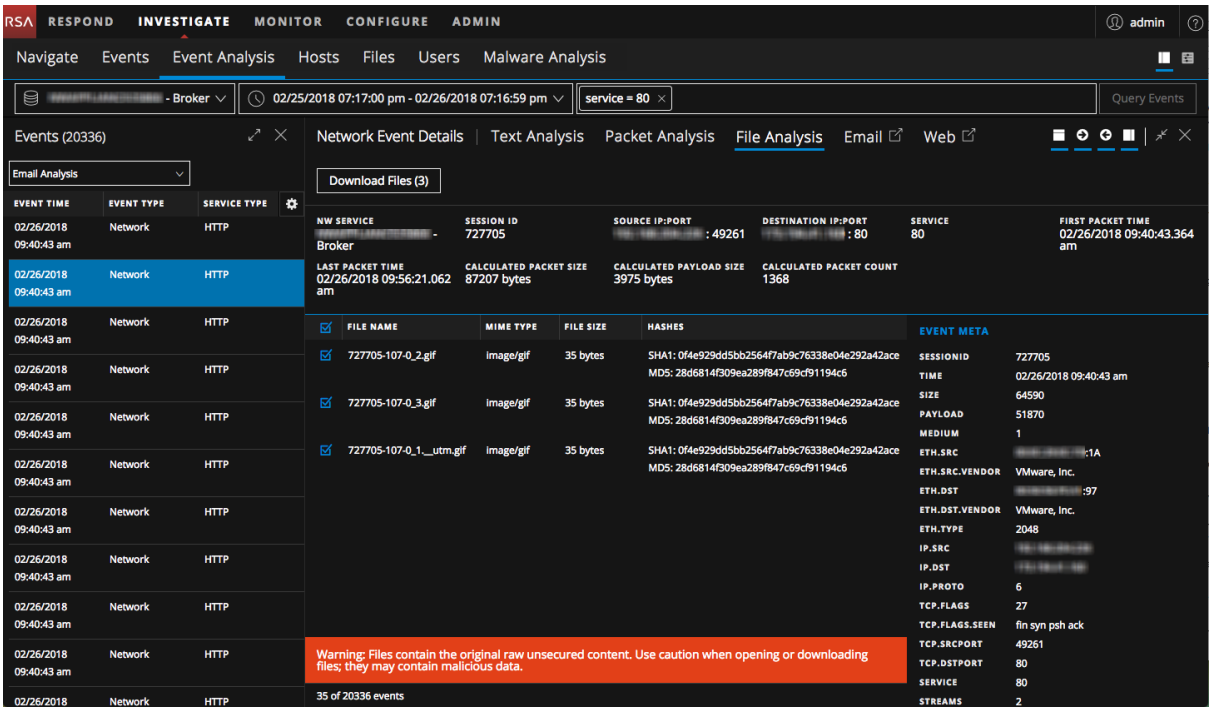
Hierbei gilt:

- `<service-ID or host name>` ist der Name des Services (z. B. ein Concentrator oder Broker), in dem die Sitzung gespeichert wurde.
- `SID<n>` ist die Sitzungs-ID-Nummer.
- `FC<n>` ist die Dateianzahl oder die Anzahl der Dateien im Archiv.

Achtung: Beim Entpacken und Öffnen von Dateien, die mit einer Standardanwendung verknüpft sind, ist Vorsicht geboten; beispielsweise könnte eine Excel-Tabelle automatisch in Excel geöffnet werden, bevor Sie überprüfen konnten, ob sie sicher ist.

So exportieren Sie Dateien in einem rekonstruierten Ereignis:

1. Navigieren Sie in der Ansicht **Ereignisanalyse** zum Bereich Dateianalyse eines Ereignisses, das Dateien enthält.



2. Klicken Sie auf eine oder mehrere Dateien, die Sie extrahieren möchten, und klicken Sie auf **Dateien herunterladen**.
   Der Job wird geplant und nach Abschluss werden die ausgewählten Dateien als passwortgeschütztes ZIP-Archiv in das lokale Dateisystem heruntergeladen.
3. Um das Archiv im lokalen Dateisystem zu öffnen, geben Sie bei Aufforderung das folgende Passwort ein: `netwitness`.

Reagieren auf Daten in der Ansicht „Ereignisanalyse“

Wenn Sie in der Ansicht „Ereignisanalyse“ für Sie interessante Daten gefunden haben, können Sie in NetWitness Endpoint oder RSA Live interne Suchen ausführen sowie in Communityressourcen wie SANS-IP-Verlauf und ThreatExpert-Suche externe Suchen von Metawerten ausführen.

Öffnen eines Endpoint-Ereignisses im Thick-Client von NetWitness Endpoint

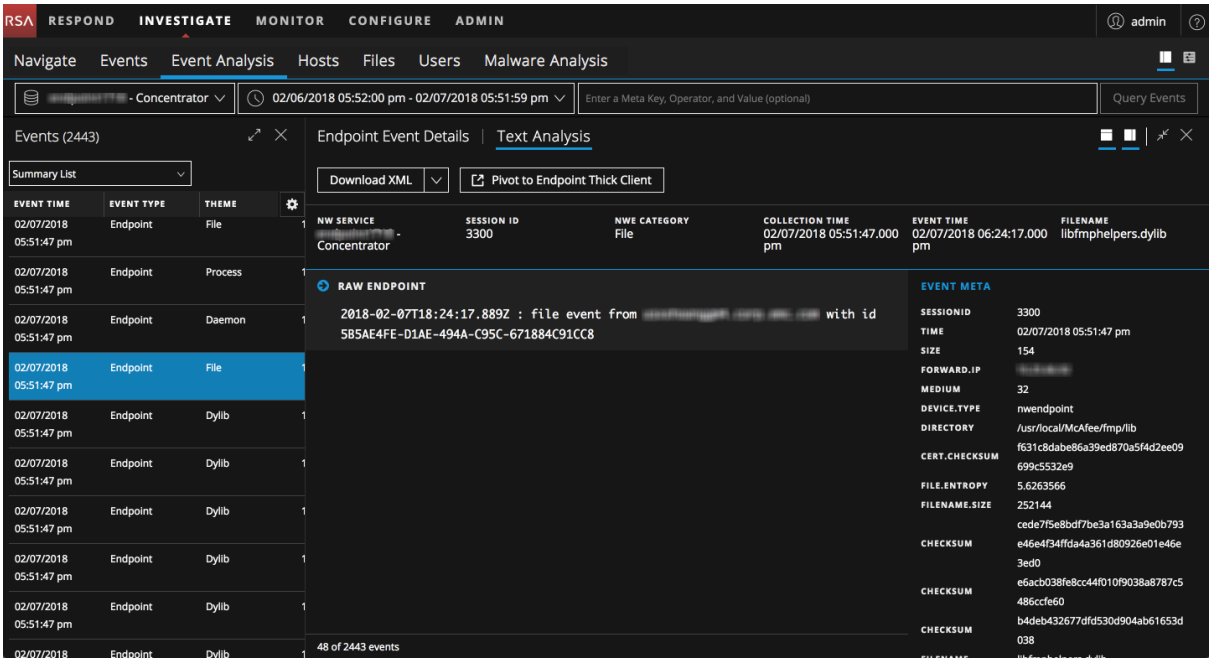
Beim Anzeigen eines Endpunktereignisses im Bereich „Textanalyse“ können Sie zur Analyse des gleichen Ereignisses in NetWitness Endpoint wechseln. Der Thick-Client von NWE bietet zusätzliche Funktionen, die über die in NetWitness Endpoint Insights integrierten Funktionen hinausgehen.

Hinweis: Version 4.4 des NetWitness Endpoint (NWE)-Thick-Client muss auf demselben Server installiert sein, die NWE-Metaschlüssel müssen in der `table-map.xml`-Datei auf dem Log Decoder und die NWE-Metaschlüssel müssen in der `index-concentrator-custom.xml`-Datei vorhanden sein. Der NWE-Thick-Client ist eine reine Windows-Anwendung. Umfassende Anweisungen zur Installation finden Sie im *NetWitness Endpoint-Benutzerhandbuch* für Version 4.4.

So öffnen Sie ein Ereignis in NetWitness Endpoint:

1. (Version 11.0 und höher) Gehen Sie zu **UNTERSUCHEN > Navigation** und führen Sie diese Schritte aus:
   a. Wählen Sie in der Drop-down-Liste **Abfrage Erweitert** aus und geben Sie eine der folgenden Abfragen ein: `nwe.callback_id exists` oder `device.type='nwendpoint'` Endpunktdaten werden im Bereich „Werte“ angezeigt.
   b. Klicken Sie mit der rechten Maustaste auf ein Ereignis und wählen Sie im Menü **Ereignisanalyse** aus.
2. (Version 11.1 und höher) Navigieren Sie zu **UNTERSUCHEN** > **Ereignisanalyse**. Wählen Sie in der Drop-down-Liste **Abfrage Erweitert** aus und geben Sie eine der folgenden Abfragen ein: `nwe.callback_id exists` oder `device.type='nwendpoint'` Endpunktdaten werden im Bereich „Ereignisse“ angezeigt.

3. Wählen Sie ein Ereignis aus.
   Die Ereignisanalyse wird unter Anzeige des ausgewählten Ereignis in der Textanalyse geöffnet.

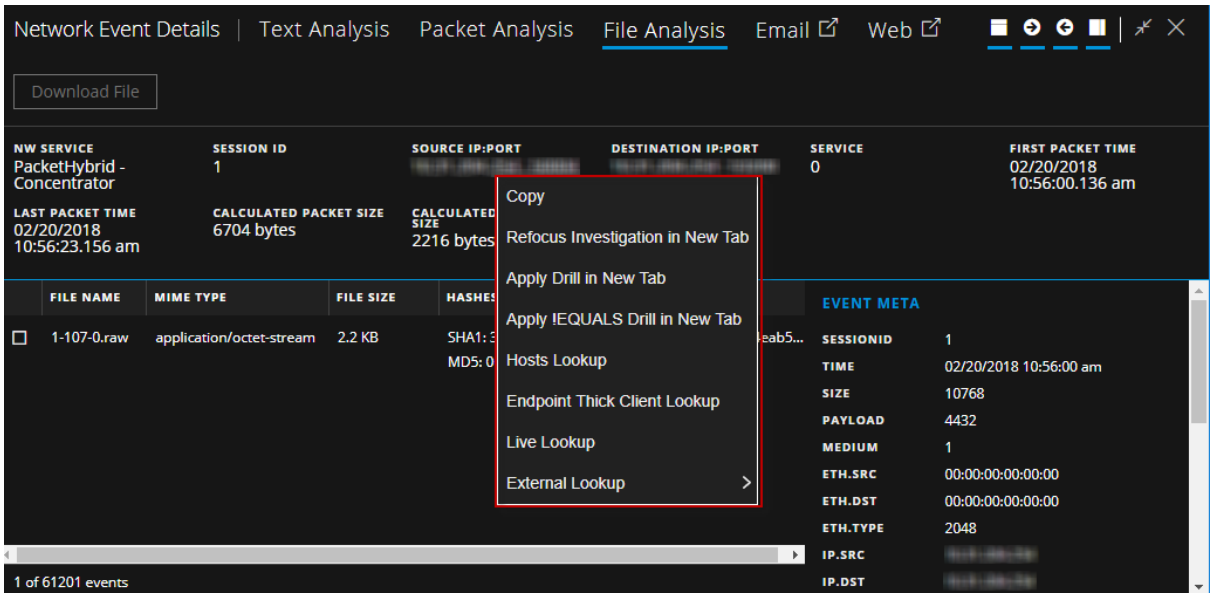


4. Klicken Sie im Ereignis-Header auf **Zu Endpoint wechseln.** Eine neue Registerkarte mit der URL `ecatui://<id>` wird im Browser geöffnet und der NWE-Thick-Client wird gestartet. Wenn der NetWitness Endpoint-Thick-Client nicht installiert ist, werden keine Daten angezeigt und die folgende Meldung wird angezeigt: `Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`

Durchführen von Suchen von Metawerten in der Ereignisanalyse

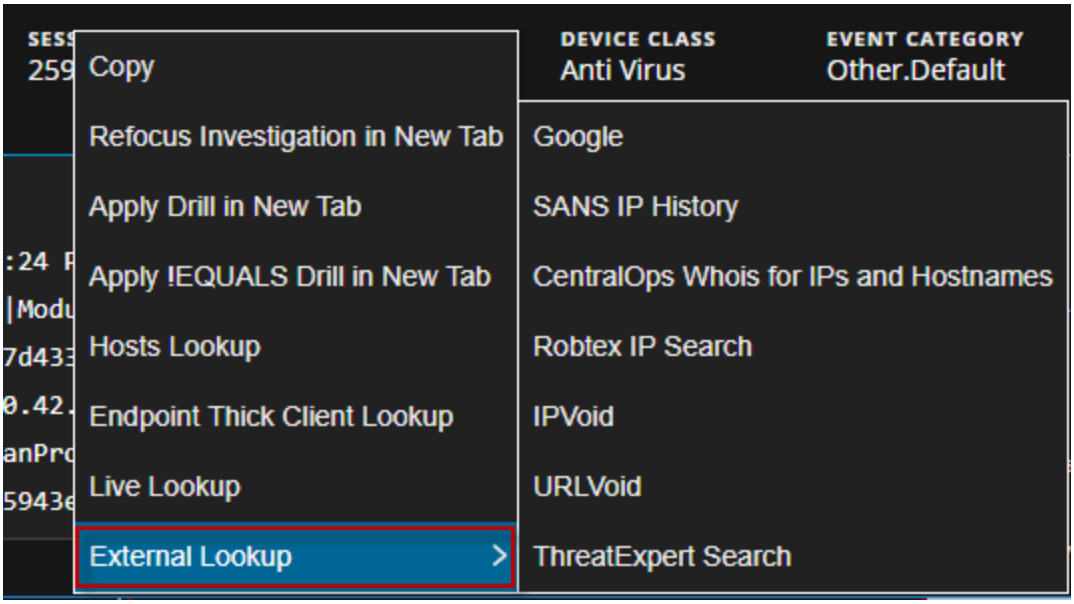
In der Ansicht „Ereignisanalyse“ können Sie Metawerte in einem Ereignis weiter untersuchen. Klicken Sie dazu mit der rechten Maustaste auf bestimmte Metawerte und verwenden Sie die Optionen in einem Drop-down-Menü. Nicht alle Felder weisen Aktionen auf, die über die rechte Maustaste ausgeführt werden. So führen Sie interne und externe Suchen durch:

1. Klicken Sie in der Ansicht „Ereignisanalyse“ mit der rechten Maustaste auf einen Metawert in der Ereignisliste, im Bereich „Ereignis-Metadaten“ oder im Ereignis-Header. Einige Metawerte weisen ein Drop-down-Menü auf.



2. Wählen Sie eine der folgenden internen Aktionen aus:
   - **Kopieren**: Kopiert den Metawert in die Zwischenablage.
   - **Ermittlungen in neuer Registerkarte neu fokussieren**: Startet eine andere Untersuchung in einer neuen Registerkarte mit Fokus auf dem ausgewählten Metawert.
   - **Drill-down in neuer Registerkarte anwenden**: Wendet den Drill-down in einer neuen Registerkarte an und öffnet ihn hier, um einen Drill-down auf die Daten in der Ansicht „Navigation“ auszuführen.
   - **!=Drill-down in neuer Registerkarte anwenden**: Wendet (!EQUALS) auf den Metawert an und öffnet eine neue Registerkarte, wobei der Metawert effektiv aus den Ergebnissen ausgeschlossen wird.
   - **Hosts ermitteln**: Sucht den Wert in der Ansicht „Untersuchen > Hosts“.
   - **Endpunkt Thick-Clientsuche**: Analysiert den Metawert im Endpoint-Thick-Client (für Clients mit Endpunkt-Agent).
   - **Live-Suche**: Sucht einen Metawert auf RSA Live zur weiteren Analyse.

3. Bewegen Sie den Mauszeiger für eine externe Suche über einen Metawert, klicken Sie mit der rechten Maustaste und wählen Sie **Externe Suche** aus.



4. Wählen Sie im Untermenü eine der verfügbaren externen Suchen aus:
   - **Google**: Sucht nach einem Metawert auf Google.com.
   - **SANS-IP-Verlauf**: Sucht nach einem Metawert auf SANS-IP-Verlauf, Domain = `http://isc.sans.org/ipinfo.html?ip=ipaddress`
   - **CentralOps WHOIS für IP-Adressen und Hostnamen**: Sucht nach einem Metawert auf CentralOps WHOIS für IP-Adressen und Hostnamen, Domain = `http://centralops.net/co/DomainDossier.aspx?addr=domain&dom_whois=true&dom_dns=true&net_whois=true`
   - **Robtex IP-Suche**: Sucht nach einem Metawert auf Robtext IP Search, Domain = `https://www.robtex.com/cidr/domain.ipaddress`
   - **IPVoid**: Sucht nach einem Metawert auf IPVoid, Domain = `http://www.ipvoid.com/scan/domain/`
   - **URLVoid**: Sucht nach einem Metawert auf URLVoid, Domain = `http://www.urlvoid.com/scan/ipaddress/`
   - **ThreatExpert-Suche**: Sucht nach einem IP-Metawert auf ThreatExpert Search, Domain = `http://www.threatexpert.com/reports.aspx?find=IP address`

Untersuchen von Hosts und Dateien

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Analysten können die Ansichten „Hosts“ und „Dateien“ von RSA NetWitness Platform verwenden, um Hosts oder Dateien zu untersuchen.

Für Analysten, die Analysen mithilfe von Investigate durchführen, müssen die entsprechenden Systemrollen und Berechtigungssätze in den Benutzerkonten eingerichtet werden. Ein Administrator muss Rollen und Berechtigungen konfigurieren, wie unter Rollen und Berechtigungen für Endpunkt-Analysten beschrieben. Weitere Informationen über Rollen und Berechtigungen finden Sie im *Handbuch Systemsicherheit und Benutzerverwaltung*.

Analysten können:

- Untersuchen von Hosts
- Untersuchen von NetWitness Endpoint 4.4.0.2 oder später Hosts
- Untersuchen von Dateien

Untersuchen von Hosts

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

So führen Sie eine Untersuchung von Hosts durch:

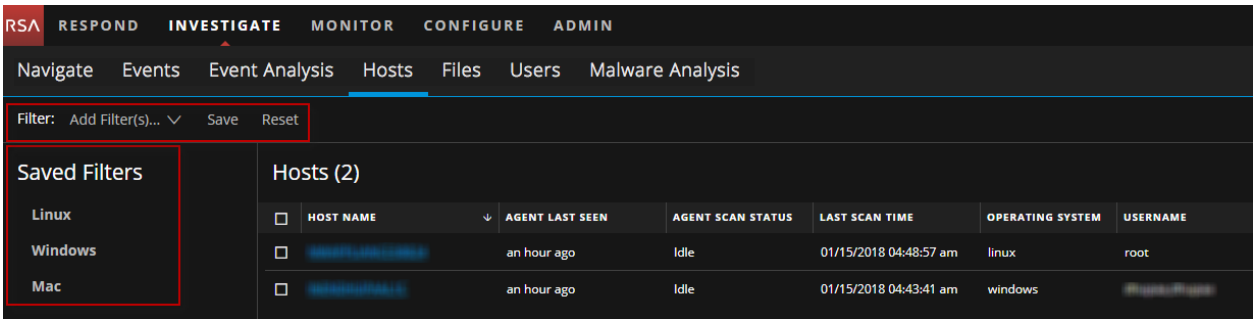
1. Navigieren Sie zu **UNTERSUCHEN** > **Hosts**.
   Eine Liste der Hosts mit einem installierten Endpoint-Agenten wird angezeigt.
2. Wählen Sie die Hosts, die Sie scannen möchten, und klicken Sie auf **Scan starten**. Weitere Informationen finden Sie unter Scannen von Hosts.
3. Klicken Sie nach Abschluss des Scannens der Hosts auf den Hostnamen, um die Ergebnisse des Scans zu untersuchen. Weitere Informationen finden Sie unter Untersuchen von Details zum Host.

Hinweis: Informationen zum Untersuchen von NetWitness Endpoint 4.4-Hosts finden Sie unter Untersuchen von NetWitness Endpoint 4.4.0.2 oder später Hosts.

Hosts filtern

Sie können Hosts im Betriebssystem filtern oder die Felder im Drop-down-Menü „Filter hinzufügen“ auswählen.

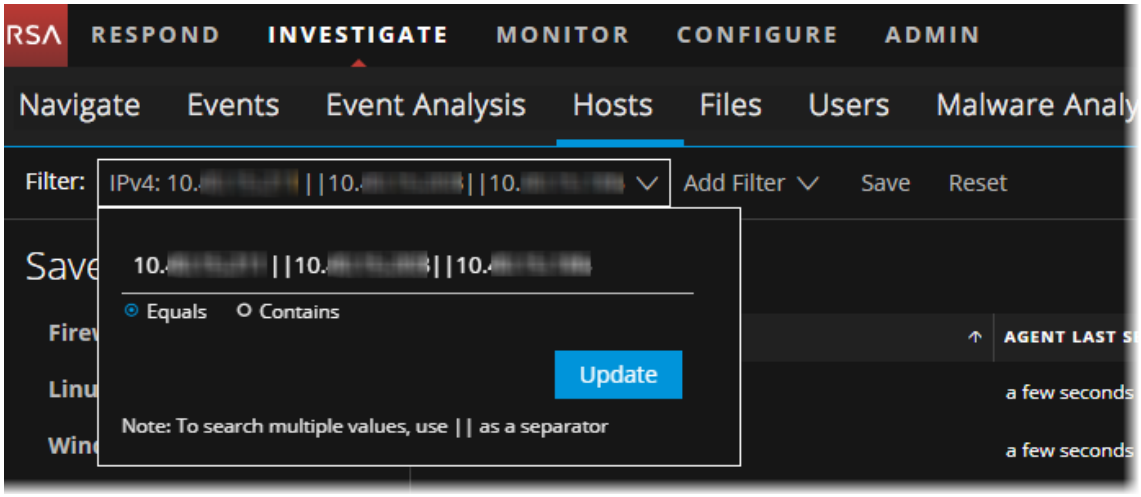
Hinweis: Verwenden Sie beim Filtern einer großen Datenmenge mindestens ein indiziertes Feld mit dem Operator `Equals` für eine bessere Performance. Die folgenden Felder werden in der Datenbank indexiert `Hostname`, `IPV4`, `Operating System` und `Last Scan Time`.



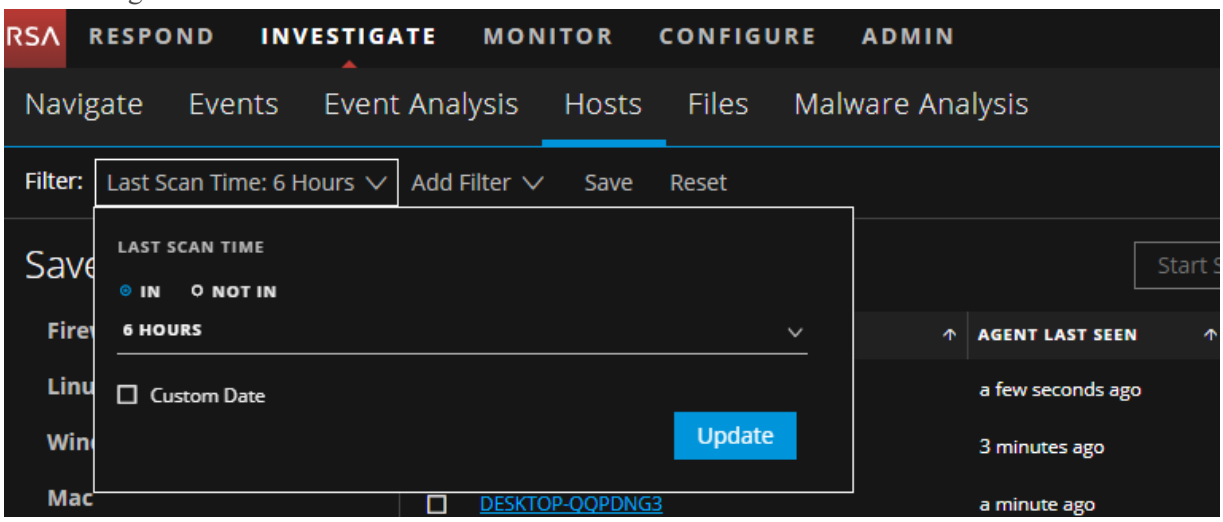
Um mehrere Werte in einem Feld zu suchen, legen Sie die Filteroption auf `Equals` fest und verwenden Sie `||` als Trennzeichen.

Es folgen einige Beispiele:

- Verwenden des Operators `Equals` für mehrere IPV4-Werte mit einem Trennzeichen `||`.



- Verwenden des Operators `IN` für „Zeit des letzten Scans“, um Agents zu filtern, die in den letzten 6 Stunden gescannt wurden.



Klicken Sie auf **Speichern**, um die Suche zu speichern, und geben Sie einen Namen an (bis zu 250 alphanumerische Zeichen). Der Filter wird dem Bereich „Gespeicherte Filter“ auf der linken Seite hinzugefügt. Bewegen Sie zum Löschen eines Filters den Mauszeiger über den Namen und klicken Sie auf  .

Hinweis: Sonderzeichen außer Unterstrich (_) und Bindestrich (-) sind beim Speichern des Filters nicht erlaubt.

Scannen von Hosts

Sie können entweder einen Scan nach Bedarf durchführen oder einen Scan täglich oder wöchentlich planen. Informationen zur Planung eines Scans finden Sie unter *Endpoint Insights – Konfigurationsleitfaden*.

Hinweis: Sie können von der Benutzeroberfläche von NetWitness Platform aus keinen Scan für die NetWitness Endpoint 4.4-Agenten durchführen.

Scan nach Bedarf

Einen Scan nach Bedarf durchzuführen, kann sinnvoll sein, wenn:

- Eine Datei im Bereich „Globale Dateien“ sich als schädlich herausstellt.
- Eine schädliche Datei auf verschiedenen Hosts im Netzwerk vorhanden ist.
- Sie einen Host untersuchen möchten, der infiziert ist.
- Sie den aktuellen Snapshot des Hosts abrufen möchten.

Wenn die Hosts gescannt werden, ruft der Endpoint-Agent die folgenden Daten ab, die zur Untersuchung verwendet werden können:

- Treiber, Prozesse, DLLs, (ausführbare) Dateien, Services und automatische Ausführungen, die auf dem Host ausgeführt werden.
- Hostdateieinträge und geplante Aufgaben.
- Systeminformationen wie Netzwerk-Share, installierte Windows-Patches, Windows-Aufgaben, angemeldete Benutzer, Bash-Verlauf und installierte Sicherheitsprodukte.

So starten Sie einen Scan:

1. Navigieren Sie zu **UNTERSUCHEN** > **Hosts**.
2. Wählen Sie jeweils einen oder mehrere Hosts (bis zu 100) für Scans nach Bedarf aus und klicken Sie auf **Scan starten**.
3. Klicken Sie auf **Scan starten** im Dialogfeld.
   Dies führt einen schnellen Scan aller ausführbaren Module durch, die im Speicher geladen sind. Dieser Scan dauert etwa 10 Minuten.

Im Folgenden sind die Scanstatus aufgeführt.

Status	Beschreibung
Leerlauf	Kein Scan wird gerade ausgeführt.
Wird gescannt	Scan wird gerade ausgeführt.
Scan wird gestartet	Scananforderung wird an den Server gesendet, aber der Agent erhält die Anforderung erst, wenn er das nächste Mal mit dem Server kommuniziert.
Scan wird beendet	Anforderung zum Beenden wird an den Server gesendet, aber der Agent erhält die Anforderung erst, wenn er das nächste Mal mit dem Server kommuniziert.

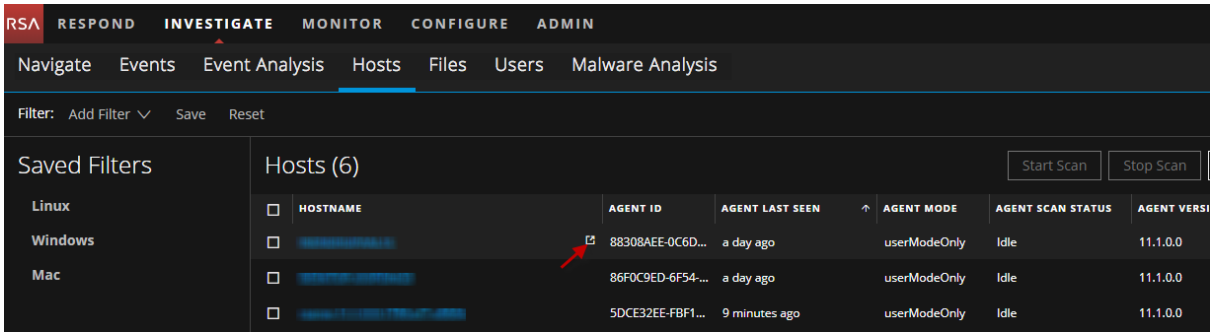
Wechseln zu den Ansichten „Navigation“ und „Ereignisanalyse“

Wenn Sie einen bestimmten Host, eine IP-Adresse (IPV4) oder einen Benutzernamen untersuchen müssen, um nach zugehörigen Aktivitäten über einen Zeitraum hinweg zu suchen, können Sie in die Ansicht „Navigation“ oder „Ereignisanalyse“ wechseln, um den gesamten Kontext der Aktivität zu erhalten. Standardmäßig ist der Zeitbereich auf einen Tag festgelegt. Sie können den Zeitbereich ändern.

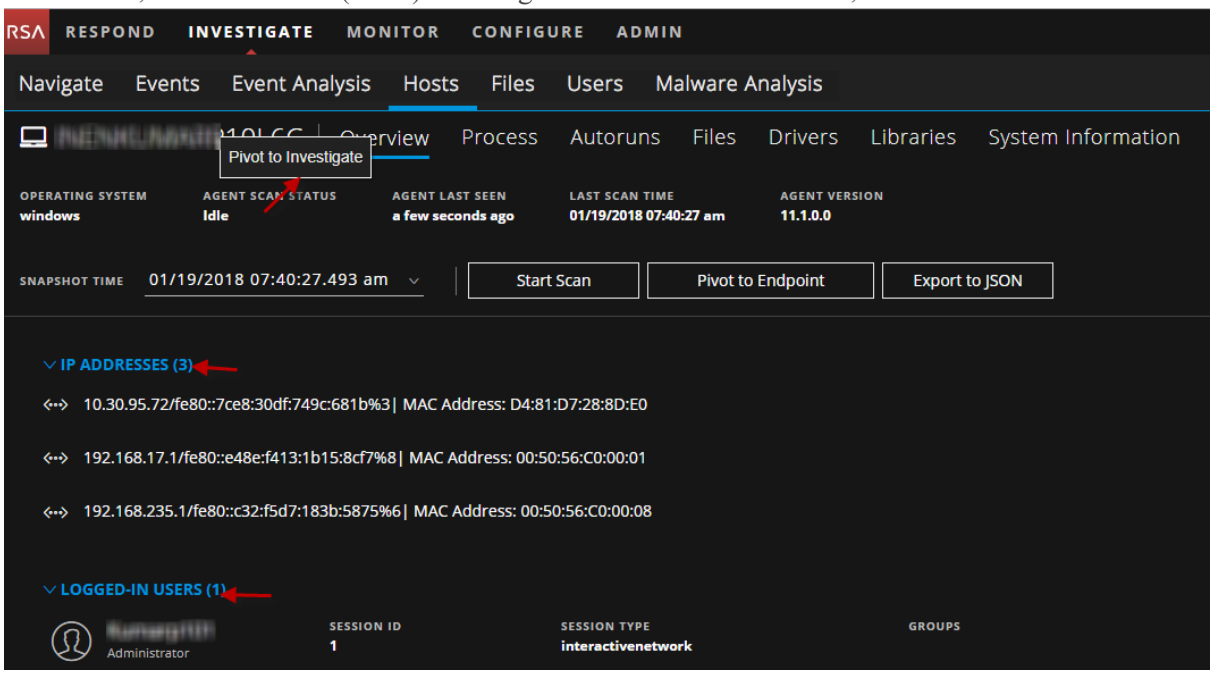
Hinweis: Das Wechseln zu den Ansichten „Navigation“ und „Ereignisanalyse“ wird für IPV6 nicht unterstützt.

So wechseln Sie zu der Ansicht „Navigation“ oder „Ereignisanalyse“:

1. Navigieren Sie zu **UNTERSUCHEN** > **Hosts** oder **UNTERSUCHEN** > **Dateien**.
2. Klicken Sie auf  neben dem Hostnamen.



Alternativ können Sie auf der Registerkarte „Übersicht“ mit der rechten Maustaste auf den Hostnamen, die IP-Adresse (IPV4) oder angemeldete Benutzer klicken, um zu wechseln.

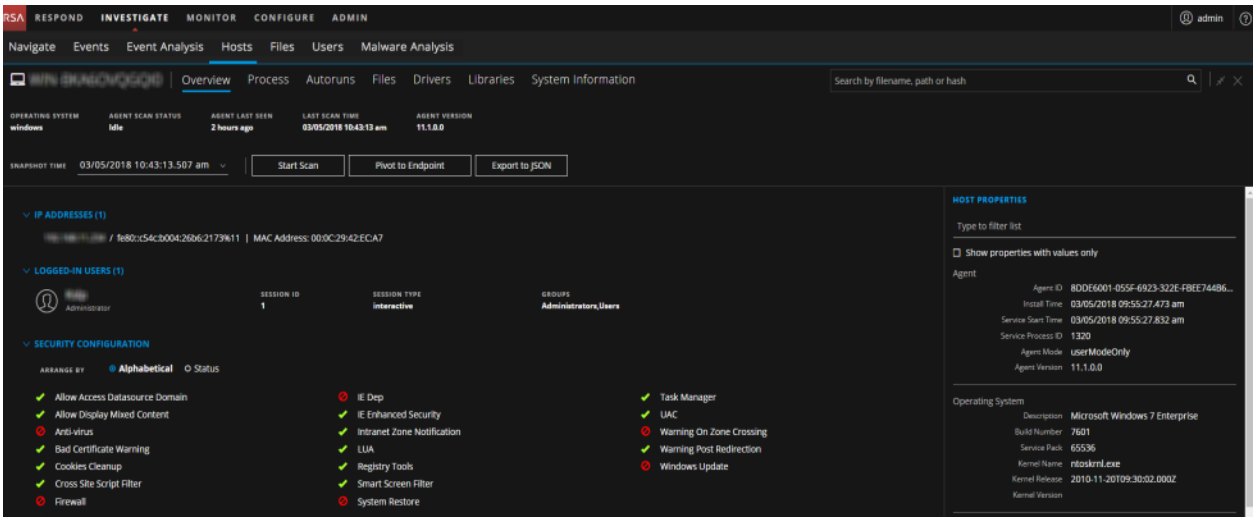


3. Wählen Sie im Dialogfeld „Service auswählen“ einen der für die Ermittlung erforderlichen Services aus.

4. Klicken Sie auf **Navigieren** oder **Ereignisanalyse**, um die Daten zu analysieren.

Untersuchen von Details zum Host

Um nach verdächtigen Dateien auf einem Host zu suchen, klicken Sie auf den Hostnamen und zeigen Sie die Details des Hosts an oder starten Sie einen Scan nach Bedarf, um aktuelle Informationen zu erhalten.



Suchen in Snapshots

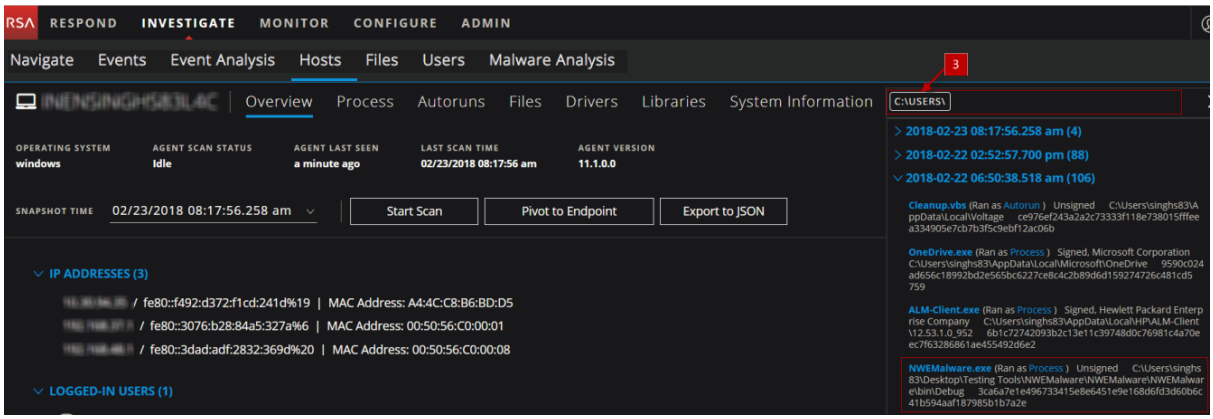
Um einen Host zu untersuchen oder um zu prüfen, ob er mit einer bekannten Schadsoftware infiziert ist, können Sie nach Vorkommen des Dateinamens, des Dateipfads oder der SHA-256-Prüfsumme suchen.

Hinweis: Um nach einer SHA-256-Prüfsumme zu suchen, geben Sie die ganze Hash-Zeichenfolge in das Suchfeld ein.

Als Ergebnis werden Details angezeigt, z. B. Dateiname, Informationen zur Signatur und zur Interaktion mit dem System (ob sie als Prozess, Bibliothek, automatische Ausführung, Service, Aufgabe oder Treiber ausgeführt wurde). Um weitere Details für diese Ergebnisse anzuzeigen, klicken Sie auf die Kategorie.

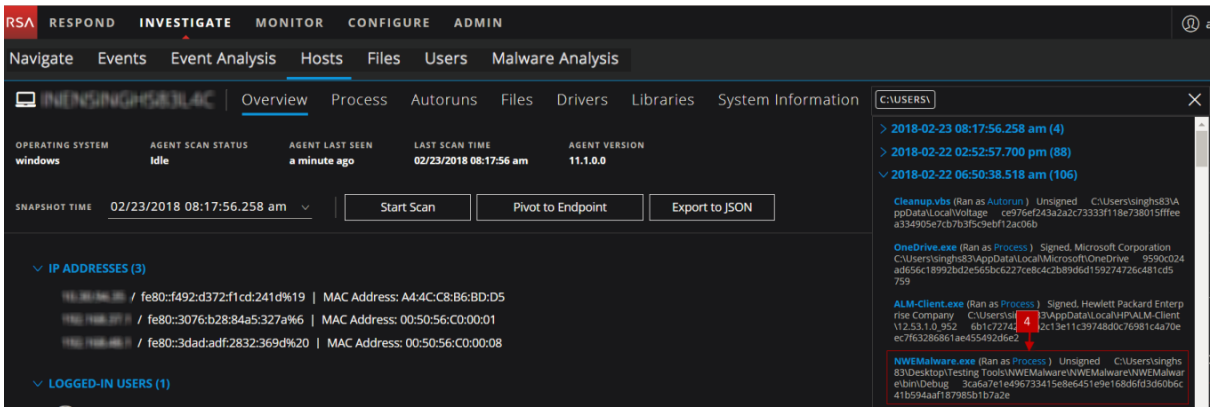
Beispielsweise hat ein Benutzer auf einen schädlichen Anhang in einer Phishing-E-Mail geklickt und ihn ausgeführt und nach `C:\Users` heruntergeladen. So untersuchen Sie diese Datei:

1. Navigieren Sie zu **UNTERSUCHEN** > **Hosts**.
2. Wählen Sie den Host aus, den Sie untersuchen möchten.
3. Geben Sie auf der Registerkarte **Übersicht** den Dateipfad `C:\Users` in das Suchfeld ein.
   Die Suche zeigt alle ausführbaren Dateien in diesem Ordner an. In diesem Beispiel ist die Datei `NWEMalware.exe` eine nicht signierte-Datei, die möglicherweise schädlich ist.



Diese Datei wurde als Prozess ausgeführt.

4. Zum Anzeigen von Details zu dieser Datei klicken Sie im Ergebnis auf **Prozess**.
   Daraufhin wird die Registerkarte „Prozess“ geöffnet, auf der Sie die Prozessdetails anzeigen können.



Analyse der Prozesse

Wählen Sie in der Ansicht „Hosts“ die Registerkarte **Prozess** aus. Sie können die Prozesse anzeigen, die zum Zeitpunkt des Scans für den ausgewählten Host ausgeführt wurden. Die Spalten „Prozessname“ und „Prozess-ID (PID)“ werden auf eine der beiden Weisen angezeigt:

- Strukturansicht: Sie können ein Drill-down für jeden Prozess durchführen und die mit ihm verknüpften unter- und übergeordneten Prozesse anzeigen.
- Listenansicht: Sie können die Spalten „Prozessname“ und „PID“ sortieren.

Klicken Sie auf , um die Ansichten zu wechseln.

Nachfolgend finden Sie ein Beispiel für die Strukturansicht:

Bei der Prüfung von Prozessen ist es wichtig, die Startargumente zu sehen. Auch legitime Dateien können für schädliche Zwecke missbraucht werden, daher ist es wichtig, alle von ihnen zu sehen, um herauszufinden, ob eine schädliche Aktivität vorliegt.

Beispiel:

- `rundll32.exe` ist eine legitime ausführbare Windows-Datei, die als saubere Datei kategorisiert wird. Aber ein Angreifer kann diese ausführbare Datei verwenden, um eine schädliche DLL zu laden. Aus diesem Grund müssen Sie, wenn Sie Prozesse überprüfen, die Argumente der `rundll32.exe`-Datei anzeigen.
- `LSASS.EXE` ist ein untergeordnetes Element von `WININIT.EXE`. Es darf keine untergeordneten Prozesse haben. Oft nutzt Malware diese ausführbare Datei für Passwort-Dumps oder um sich auf einem System zu verstecken (`lass.exe`, `lssass.exe`, `lsasss.exe` usw.).
- Die meisten seriösen Benutzeranwendungen wie Adobe, Webbrowser etc. erzeugen keine untergeordneten Prozesse wie `cmd.exe`. Wenn Sie darauf stoßen, untersuchen Sie die Prozesse.

Automatische Ausführungen analysieren

Wählen Sie in der Ansicht „Hosts“ die Registerkarte **Automatische Ausführungen** aus. Sie können die automatischen Ausführungen, Services, Aufgaben und Cronjobs anzeigen, die für den ausgewählten Host ausgeführt werden.

Auf der Registerkarte „Services“ können Sie z. B. nach dem Erstellungszeitpunkt der Datei suchen. Die Kompilierzeit finden Sie in jeder portablen ausführbaren (PE) Datei in der PE-Kopfzeile. Der Zeitstempel wird nur selten manipuliert, obwohl ein Angreifer ihn einfach vor der Bereitstellung am Endpunkt eines Opfers ändern kann. Dieser Zeitstempel kann anzeigen, ob eine neue Datei eingeführt wurde. Sie können den Zeitstempel der Datei mit dem Erstellungszeitpunkt des Systems vergleichen, um den Unterschied zu finden. Wenn eine Datei vor ein paar Tagen kompiliert wurde, aber der Zeitstempel dieser Datei auf dem System zeigt an, dass sie vor einigen Jahren erstellt wurde, so deutet dies darauf hin, dass die Datei manipuliert wurde.

Analysieren von Dateien

Wählen Sie in der Ansicht „Hosts“ die Registerkarte **Dateien** aus. Sie können die Liste der auf dem Host gescannten Dateien zum Zeitpunkt des Scans anzeigen. Standardmäßig werden in der Tabelle 100 Dateien angezeigt. Um weitere Dateien anzuzeigen, klicken Sie auf **Weitere laden** am unteren Rand der Seite.

Beispielsweise schreiben viele Trojaner zufällige Dateinamen, wenn sie ihre Nutzlasten ablegen, um eine einfache Suche über die Endpunkte im Netzwerk anhand des Dateinamens zu vermeiden. Wenn eine Datei `svch0st.exe`, `scvhost.exe` oder `svchosts.exe` heißt, bedeutet dies, dass die legitime Windows-Datei namens `svchost.exe` imitiert wird.

Analyse von Bibliotheken

Wählen Sie in der Ansicht „Hosts“ die Registerkarte **Bibliotheken** aus. Sie können die Liste der Bibliotheken anzeigen, die zum Zeitpunkt des Scans geladen sind.

Beispielsweise wird eine Datei mit hoher Entropie als gepackt markiert. Eine gepackte Datei bedeutet, dass sie komprimiert ist, um ihre Größe zu reduzieren (oder schädliche Zeichenfolgen und Konfigurationsinformationen zu verschleiern).

Analysieren von Treibern

Wählen Sie in der Ansicht „Hosts“ die Registerkarte **Treiber** aus. Sie können die Liste der auf dem Host ausgeführten Treiber zum Zeitpunkt des Scans anzeigen.

So können Sie mit diesem Bereich z. B. prüfen ob die Datei signiert oder unsigniert ist. Wenn eine Datei von einem vertrauenswürdigen Anbieter wie Microsoft und Apple mit dem Ausdruck `valid` signiert ist, bedeutet dies, dass es eine saubere Datei ist.

Analysieren der Systeminformationen

Wählen Sie in der Ansicht „Hosts“ die Registerkarte **Systeminformationen** aus. Dieser Bereich listet die Systeminformationen zum Agent auf. Für das Windows-Betriebssystem zeigt der Bereich die Einträge der Hostdatei und Netzwerkfreigaben dieses Hosts an.

Beispielsweise verwendet Malware möglicherweise Einträge der Hostdatei, um Virenschutzaktualisierungen zu blockieren.

Löschen eines Hosts

So löschen Sie Hosts manuell aus der Benutzeroberfläche:

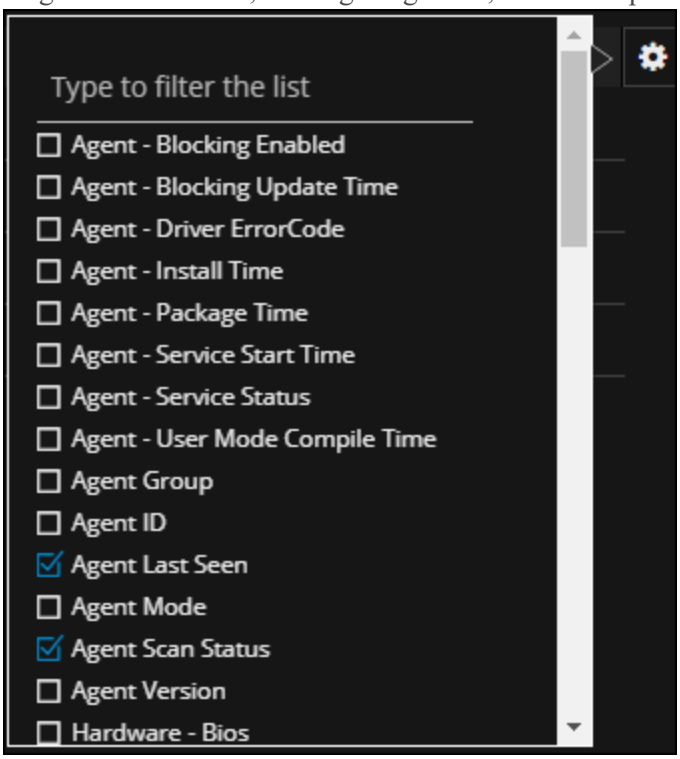
1. Navigieren Sie zu **UNTERSUCHEN > Hosts**.
2. Wählen Sie die Hosts aus, die aus der Ansicht „Hosts“ gelöscht werden sollen und klicken Sie **Löschen**.
   Hierdurch werden alle gesammelten Endpunktdaten für die ausgewählten Hosts gelöscht.

Hinweis: Wenn Sie versehentlich einen Host aus der Ansicht „Hosts“ löschen, verbietet der Endpunktserver alle Anforderungen von diesem Agent. Der Agent muss manuell vom Host deinstalliert und neu installiert werden, damit er in der Ansicht „Hosts“ angezeigt wird.

Festlegen von Hosteinstellungen

Standardmäßig zeigt die Ansicht „Hosts“ einige Spalten an und die Hosts werden nach „Zeit des letzten Scans“ sortiert. Wenn Sie bestimmte Spalten anzeigen und Daten nach einem bestimmten Feld sortieren möchten:

1. Navigieren Sie zur Ansicht **UNTERSUCHEN > Hosts**.
2. Wählen Sie die Spalten aus, indem sie auf in der rechten Ecke klicken. Das folgende Beispiel zeigt den Bildschirm, der angezeigt wird, während Spalten hinzugefügt werden:



3. Sortieren Sie die Daten in der erforderlichen Spalte.

Hinweis: Dies wird als Standardansicht festgelegt, die jedes Mal angezeigt wird, wenn Sie sich in der Ansicht „Hosts“ anmelden.

Exportieren von Hostattributen

Sie können jeweils bis zu 100.000 Hostattribute exportieren. So extrahieren Sie die Hostattribute in eine kommagetrennte Datei (CSV-Datei).

1. Navigieren Sie zu **UNTERSUCHEN > Hosts**.
2. Filtern Sie die Hosts, indem Sie die erforderlichen Filteroptionen auswählen.

3. Fügen Sie Spalten hinzu, indem sie auf  in der rechten Ecke klicken.
4. Klicken Sie auf **In CSV-Datei exportieren**.

Sie können die CSV-Datei entweder speichern oder öffnen.

Untersuchen von NetWitness Endpoint 4.4.0.2 oder später Hosts

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Wenn Sie NetWitness Endpoint 4.4.0.2 oder später in Ihrer Bereitstellung haben, können Sie die Endpunktdaten dieser Hosts in den Ansichten **UNTERSUCHEN > Hosts** und **UNTERSUCHEN > Dateien** anzeigen.

Wenn die hier aufgeführten Hosts in NetWitness Endpoint 4.4.0.2 nicht angezeigt werden, finden Sie weitere Informationen unter „Integrieren von NetWitness Endpoint 4.4.0.2 oder höher in NetWitness Endpoint 11.1“ im *RSA NetWitness Endpoint Insights – Konfigurationsleitfaden*.

Die NetWitness Endpoint 4.4.0.2 Hosts können in der Ansicht „Hosts“ mithilfe der Agent-Version identifiziert werden. Sie können auf diesen Hosts keinen Scan nach Bedarf durchführen. Um diese Hosts zu untersuchen, müssen Sie die Benutzeroberfläche ab NetWitness Endpoint 4.4.0.2 verwenden.

Hinweis: Um zum Thick Client vom der Benutzeroberfläche der NetWitness Suite zu wechseln, muss NetWitness Endpoint 4.4.0.2 oder höher installiert sein.

So untersuchen Sie einen Host in der NetWitness Endpoint-Benutzeroberfläche:

1. Navigieren Sie zu **UNTERSUCHEN** > **Hosts**.
2. Wählen Sie den 4.4-Host aus der Tabelle aus.
3. Klicken Sie auf **Zu Endpoint wechseln**.

Hinweis: Die Option **Zu Endpoint wechseln** gilt nicht für die NetWitness Endpoint Insights 11.1-Hosts.

Untersuchen von Dateien

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Analysten können in der Ansicht „Dateien“ (**UNTERSUCHEN > Dateien**) verdächtige Dateien identifizieren. Dazu müssen sie Dateinamen, Dateigröße, Entropie, Format, Firmennamen, Signatur und Prüfsumme untersuchen.

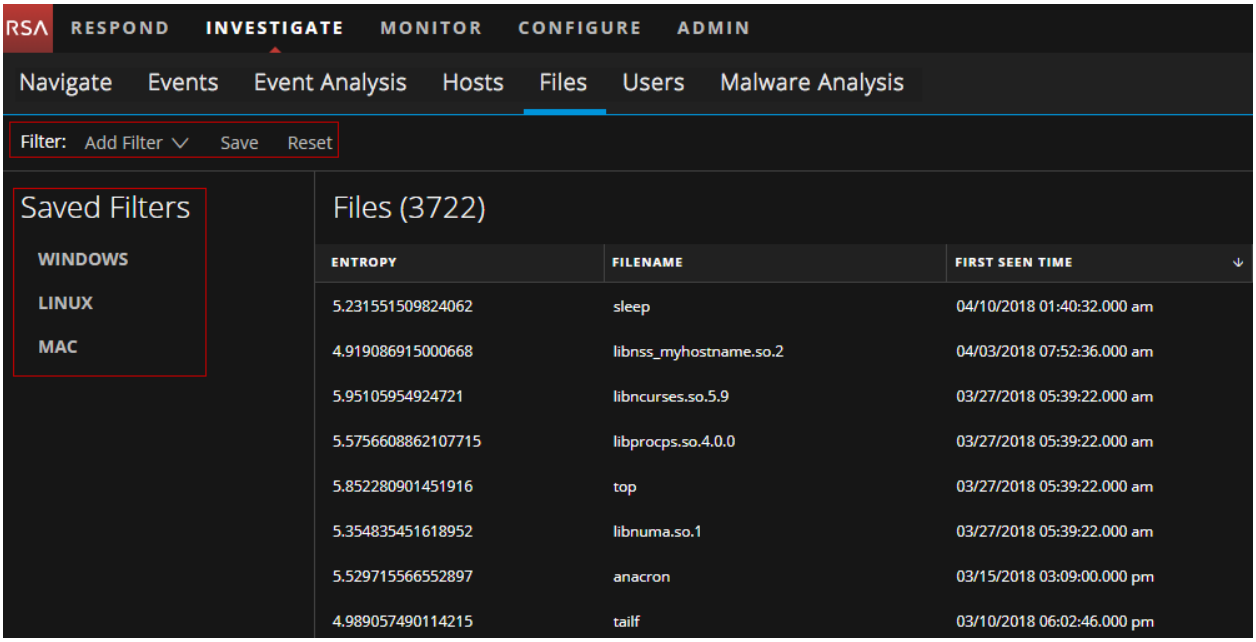
Beispielsweise kann im Falle einer Infektion einer Umgebung durch die Ransomware WannaCry ein Analyst anhand des Dateinamens die Liste filtern. Sie können nach dieser Ransomware auch mithilfe der Prüfsumme suchen.

Die Dateigröße kann ein Indikator bei der Bewertung einer Datei sein. Trojaner sind in der Regel kleiner als 1 MB und die meisten sind kleiner als 500 KB.

Filtern von Dateien

Sie können entweder die Dateien im Betriebssystem filtern oder die Felder im Drop-down-Menü „Filter hinzufügen“ auswählen.

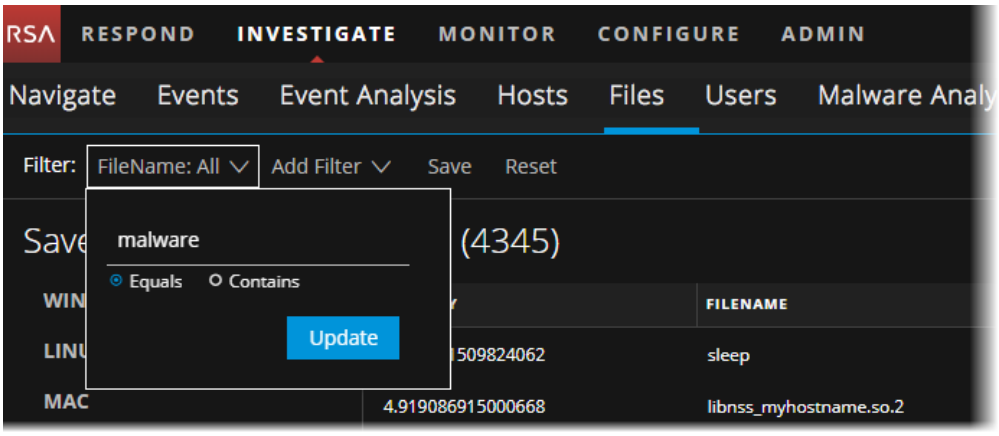
Hinweis: Verwenden Sie beim Filtern einer großen Datenmenge mindestens ein indiziertes Feld mit dem Operator `Equals` für eine bessere Performance. Die folgenden Felder sind in der Datenbank indexiert: Dateiname, MD5, Betriebssystem, Zeit des ersten Auftretens und Format.



Klicken Sie auf **Speichern**, um die Suche zu speichern, und geben Sie einen Namen an (bis zu 250 alphanumerische Zeichen). Der Filter wird dem Bereich „Gespeicherte Filter“ auf der linken Seite hinzugefügt. Bewegen Sie zum Löschen eines Filters den Mauszeiger über den Namen und klicken Sie auf  .

Hinweis: Sonderzeichen außer Unterstrich (_) und Bindestrich (-) sind beim Speichern des Filters nicht erlaubt.

Beispielsweise Filtern von Dateien mit dem Dateinamen `malware` mithilfe des Operators `Equals`.



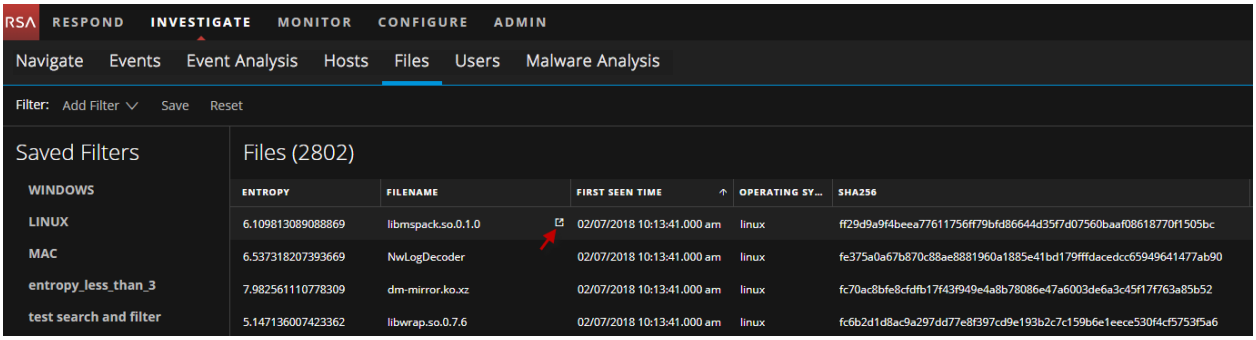
Hinweis: Für die Dateigröße wird 1 KB als 1024 Byte berechnet. Wenn also die tatsächliche Größe der Datei 8.421 Byte ist, wird sie in der Benutzeroberfläche als 8,2 KB statt 8,22 KB angezeigt. Es wird empfohlen, im Byte-Format zu suchen, wenn der Operator `Equals` verwendet wird.

Wechseln zu den Ansichten „Navigation“ und „Ereignisanalyse“

Wenn Sie einen bestimmten Dateinamen oder Hash (SHA256 und MD5) in den globalen Dateien untersuchen müssen, um nach zugehörigen Aktivitäten über einen Zeitraum hinweg zu suchen, können Sie in die Ansicht „Navigation“ oder „Ereignisanalyse“ wechseln, um den gesamten Kontext der Datei zu erhalten. Standardmäßig ist der Zeitbereich auf einen Tag festgelegt. Sie können den Zeitbereich entsprechend ändern.

So wechseln Sie zu den Ansichten „Navigation“ oder „Ereignisanalyse“:

1. Navigieren Sie zu **UNTERSUCHEN > Dateien**.
2. Klicken Sie auf  neben dem Dateinamen oder Hash.



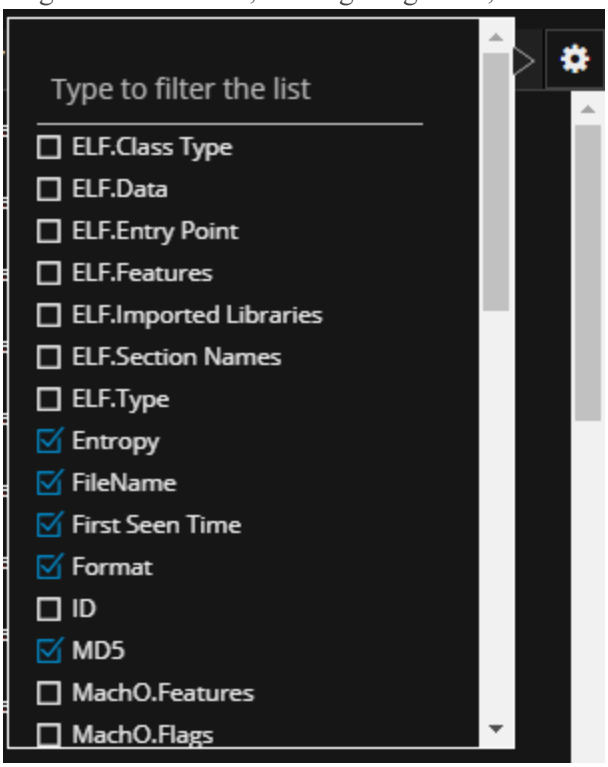
3. Wählen Sie im Dialogfeld „Service auswählen“ einen der für die Ermittlung erforderlichen Services aus.
4. Klicken Sie auf **Navigieren** oder **Ereignisanalyse**, um die Daten zu analysieren.

Hinweis: Wenn beim Wechsel zu der Ansicht „Navigation“ oder „Ereignisanalyse“ die Werte nicht indexiert sind, dauert das Laden der Ergebnisse länger. Weitere Informationen finden Sie unter Troubleshooting von NetWitness Investigate.

Festlegen von Dateieinstellungen

Standardmäßig zeigt die Ansicht „Dateien“ einige Spalten an und die Dateien werden nach „Zeit des ersten Auftretens“ sortiert. Wenn Sie bestimmte Spalten anzeigen und Daten nach einem bestimmten Feld sortieren möchten:

1. Navigieren Sie zu **UNTERSUCHEN > Dateien**.
2. Wählen Sie die Spalten aus, indem sie auf  in der rechten Ecke klicken. Das folgende Beispiel zeigt den Bildschirm, der angezeigt wird, während Spalten hinzugefügt werden:



3. Sortieren Sie die Daten in der erforderlichen Spalte.

Hinweis: Dies wird als Standardansicht festgelegt, die jedes Mal angezeigt wird, wenn Sie sich in der Ansicht „Dateien“ anmelden.

Exportieren globaler Dateien

So extrahieren Sie die Liste der globalen Dateien in eine CSV-Datei.

Hinweis: Verwenden Sie beim Filtern einer großen Datenmenge mindestens ein indiziertes Feld mit dem Operator `Equals` für eine bessere Performance. Sie können jeweils bis zu 100.000 Dateien exportieren.

1. Navigieren Sie zu **UNTERSUCHEN > Dateien**.
2. Filtern Sie die Dateien, indem Sie die erforderliche Filteroption auswählen.
3. Fügen Sie Spalten hinzu, indem sie auf  in der rechten Ecke klicken.
4. Klicken Sie auf **In CSV-Datei exportieren**.

Sie können die CSV-Datei entweder speichern oder öffnen.

Durchführen von Schadsoftwareanalysen

Analysten können den RSA NetWitness Platform Malware Analysis-Service zur Erkennung von Schadsoftware in ausgewählten Daten und Dateien nutzen.

Für Analysten, die Analysen mithilfe von NetWitness Platform Malware Analysis durchführen, müssen die entsprechenden Systemrollen und Berechtigungen in den Benutzerkonten eingerichtet werden.

Die folgenden Verfahren bieten Anweisungen für die Verwendung von Malware Analysis:

- Beginnen einer Schadsoftwareanalyse-Ermittlung
- Hochladen von Dateien für Malware Analysis-Scans
- Implementieren von angepassten YARA-Inhalten
- Filtern der Dashlet-Daten in der Ansicht Ereigniszusammenfassung
- Überprüfen von Scandateien und Ereignissen in Listenform
- Anzeigen der detaillierten Schadsoftwareanalyse eines Ereignisses

Malware Analysis-Funktionen

NetWitness Platform Malware Analysis ist eine automatisierte Verarbeitungssoftware zur Analyse von Schadsoftware, die bestimmte Typen von Dateiobjekten analysiert (z. B. Windows PE, PDF und MS Office), um die potenzielle Schädlichkeit einer Datei zu bewerten.

Malware Analysis erkennt Indikatoren für infizierte Dateien mit vier verschiedenen Analysemethoden:

- Netzwerksitzungsanalyse (Netzwerk)
- Statische Dateianalyse (Statisch)
- Dynamische Dateianalyse (Sandbox)
- Sicherheitscommunityanalyse (Community)

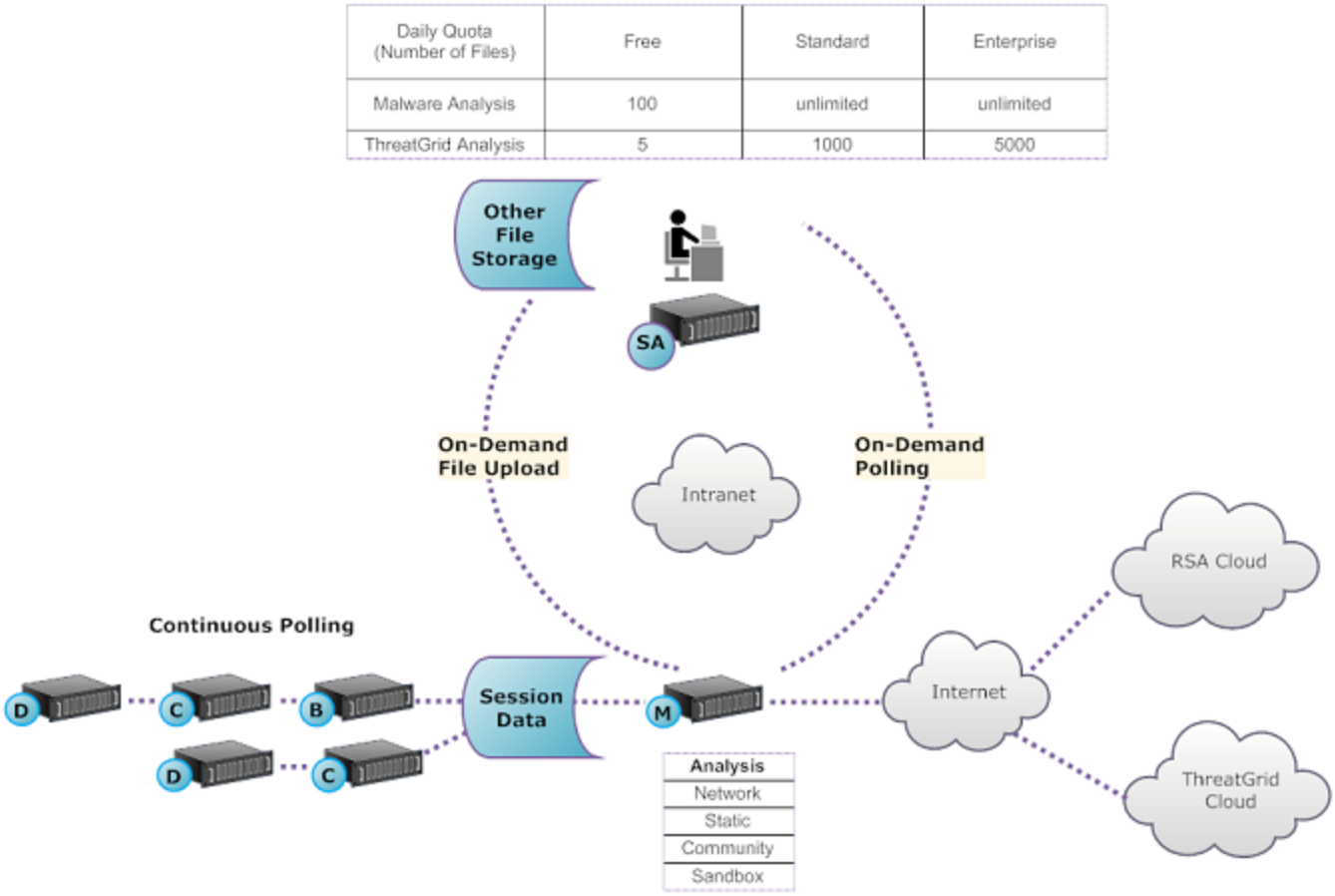
Jede dieser vier Analysemethoden ist so konzipiert, dass sie inhärente Schwachstellen der jeweils anderen ausgleicht. Die dynamische Dateianalyse erkennt zum Beispiel Zero-Day-Angriffe, die in der Phase der Sicherheitscommunityanalyse nicht erkannt werden. Indem bei der Schadsoftwareanalyse mehrere Methoden eingesetzt werden, werden nicht so viele falsche negative Ergebnisse erzeugt.

Zusätzlich zu den integrierten Indikatoren für eine Infizierung unterstützt Malware Analysis auch in YARA geschriebene Indikatoren für eine Infizierung. YARA ist eine Regelsprache, die es Schadsoftwareforschern ermöglicht, Schadsoftwaremuster zu identifizieren und zu klassifizieren. Dies ermöglicht es IOC-Autoren, Erkennungsfunktionen zu RSA Malware Analysis hinzuzufügen, indem sie YARA-Regeln erstellen und in RSA Live veröffentlichen. Diese YARA-basierten IOCs in RSA Live werden automatisch heruntergeladen und in dem abonnierten Host aktiviert, um die bestehenden Analysen, die in jeder Datei durchgeführt werden, zu ergänzen.

Malware Analysis bietet auch Funktionen, die Warnmeldungen für das Incident-Management unterstützen.

Funktionsübersicht

In dieser Abbildung ist die funktionelle Beziehung zwischen den Core-Services (Decoder, Concentrator und Broker), dem Malware Analysis-Service und dem NetWitness Server dargestellt.



Der Malware Analysis-Service analysiert Dateiobjekte mit einer beliebigen Kombination der folgenden Methoden:

- **Kontinuierliche automatische Abfrage eines Concentrator oder Broker**, um Sitzungen zu extrahieren, die von einem Parser als potenziell mit Schadsoftware infiziert eingestuft werden
- **Abfrage eines Concentrator oder Broker nach Bedarf**, um Sitzungen zu extrahieren, die von einem Schadsoftwareanalysten als potenziell mit Schadsoftware infiziert eingestuft werden
- **Hochladen von Dateien nach Bedarf** aus einem vom Benutzer definierten Ordner

Wenn der automatische Abruf eines Concentrator oder Broker aktiviert ist, extrahiert und priorisiert der Malware Analysis-Service fortlaufend ausführbaren Inhalt, PDF-Dokumente und Microsoft Office-Dokumente in Ihrem Netzwerk, die direkt von den erfassten Daten stammen und vom Core-Service analysiert werden. Da der Malware Analysis-Service eine Verbindung mit einem Concentrator oder Broker herstellt, um nur solche ausführbaren Dateien zu extrahieren, die als mögliche Schadsoftware markiert sind, ist der Prozess schnell und effizient. Dieser Prozess ist kontinuierlich und erfordert keine Überwachung.

Bei der bedarfsweisen Abfrage eines Concentrator oder Broker verwendet der Schadsoftwareanalyst Security Analytics Investigation, um sich die erfassten Daten genauer anzusehen und die zu analysierenden Sitzungen auszuwählen. Der Malware Analysis-Service nutzt diese Informationen, um den Concentrator oder Broker automatisch abzufragen und die angegebenen Sitzungen zur Analyse herunterzuladen.

Beim Hochladen von Dateien bei Bedarf kann der Analyst Dateien prüfen, die außerhalb der Core-Infrastruktur erfasst wurden. Die Schadsoftware wählt einen Ordnerspeicherort aus und identifiziert eine oder mehrere Dateien, die hochgeladen und von Malware Analysis analysiert werden sollen. Diese Dateien werden mithilfe derselben Methodik analysiert wie Dateien, die automatisch aus Netzwerksitzungen extrahiert werden.

Analysemethode

Für die Netzwerkanalyse sucht der Malware Analysis-Service ähnlich einem Analysten nach Merkmalen, die dem Anschein nach von der Norm abweichen. Durch die Untersuchung von Hunderten bis Tausenden von Merkmalen und eine Kombination der Ergebnisse in einem Bewertungssystem mit entsprechenden Gewichtungen werden harmlose Sitzungen, die zufälligerweise einige anormale Merkmale aufweisen, ignoriert, während die potenziell bedrohlichen Sitzungen hervorgehoben werden. Ein Benutzer kann die Muster erlernen, die auf eine anormale Aktivität in den Sitzungen hinweisen und einer weiteren Untersuchung bedürfen; diese Muster werden auch als Indikatoren für eine Infizierung bezeichnet.

Der Malware Analysis-Service kann statische Analysen von verdächtigen Objekten durchführen, die er im Netzwerk findet, und ermitteln, ob diese Objekte schädlichen Code enthalten. Bei der Communityanalyse wird neue im Netzwerk entdeckte Schadsoftware in die RSA-Cloud übertragen, um sie anhand der RSA-Daten zur Schadsoftwareanalyse und der Feeds vom SANS Internet Storm Center, von SRI International, vom US-Finanzministerium und von VeriSign zu prüfen. Für Sandbox-Analysen können die Services auch Daten mittels Push an die wichtigen SIEM-Hosts (Security, Information and Event Management) übertragen (die ThreatGrid-Cloud).

Malware Analysis verfügt über eine einzigartige Methode für die Analyse, bei der mit führenden Unternehmen und Experten der Branche zusammengearbeitet wird, die mit ihren Technologien das Bewertungssystem von Malware Analysis ideal ergänzen.

NetWitness Server Zugreifen auf den Malware Analysis-Service

Der NetWitness Server wird so konfiguriert, dass er eine Verbindung mit dem Malware Analysis-Service herstellen und markierte Daten für eine tiefer gehende Analyse in Investigation importieren kann. Der Zugriff erfolgt auf Basis auf drei Abonnementebenen.

- Kostenloses Abonnement: Alle NetWitness Platform-Kunden verfügen über ein kostenloses Abonnement, das sie über einen Schlüssel für eine kostenlose Testversion der ThreatGrid-Analyse nutzen können. Die Rate des Malware Analysis-Services ist auf 100 Dateistichproben pro Tag begrenzt. Die Anzahl der Stichproben (aus den oben beschriebenen Dateigruppen), die für die Sandbox-Analyse an die ThreatGrid-Cloud übertragen werden kann, ist hierbei auf 5 pro Tag begrenzt. Wenn eine Netzwerksitzung 100 Dateien aufweist, würde das Limit nach Verarbeitung dieser einen Netzwerksitzung bereits erreicht sein. Wenn 100 Dateien manuell hochgeladen werden, würde das Limit ebenfalls erreicht sein.
- Standardabonnement: Die Anzahl der Übertragungen an den Malware Analysis-Service ist unbegrenzt. Die Anzahl an Stichproben, die zur Sandbox-Analyse an die ThreatGrid Cloud übermittelt werden, beläuft sich auf 1.000 pro Tag.
- Enterprise-Abonnement: Die Anzahl der Übertragungen an den Malware Analysis-Service ist unbegrenzt. Die Anzahl an Stichproben, die an die ThreatGrid Cloud zur Sandbox-Analyse übermittelt wurden, beläuft sich auf 5.000 pro Tag.

Bewertungsmethode:

Standardmäßig werden die Indikatoren für eine Infizierung (Indicators of Compromise, IOC) anhand von Branchen-Best-Practices gewichtet. Während der Analyse führen die ausgelösten IOCs dazu, dass die Bewertung ansteigt oder reduziert wird. Dies gibt die Wahrscheinlichkeit an, ob die Stichprobe schädlich ist. Die Gewichtung der IOCs ist in NetWitness Platform einsehbar, sodass der Schadsoftwareanalyst selbst entscheiden kann, ob die zugeordnete Bewertung ignoriert werden soll oder ob ein IOC komplett aus der Bewertung herausgenommen werden soll. Der Analyst hat die Flexibilität, entweder die standardmäßige Gewichtung zu verwenden oder die Gewichtung vollständig an bestimmte Anforderungen anzupassen.

YARA-basierte IOCs werden mit den integrierten IOCs in jeder integrierten Kategorie verschachtelt und lassen sich nicht von den systemeigenen IOCs unterscheiden. Bei der Anzeige von IOCs in der Servicekonfigurationsansicht können Administratoren YARA in der Auswahlliste „Modul“ auswählen, um eine Liste der YARA-Regeln einzusehen.

Nachdem eine Sitzung in NetWitness Platform importiert wurde, stehen alle Anzeige- und Analysefunktionen in Investigation zur Verfügung, um die Indikatoren für eine Infizierung genauer zu analysieren. Bei der Anzeige in Investigation werden YARA-IOCs von den integrierten IOCs durch das Tag `Yara rule.` unterschieden.

Bereitstellung

Der Malware Analysis-Service wird als separater RSA Malware Analysis-Host bereitgestellt. Der dedizierte Malware Analysis-Host verfügt über einen integrierten Broker, der eine Verbindung mit der Core-Infrastruktur herstellt (entweder ein anderer Broker oder ein Concentrator). Vor dieser Verbindung müssen den Decoders, die mit den Concentrators und Brokers verbunden sind, von denen der Malware Analysis-Service Daten abruft, eine Reihe von Parsern und Feeds hinzugefügt werden. Auf diese Weise können verdächtige Datendateien zur Extraktion markiert werden. Der Inhalt dieser Dateien ist mit dem Tag `malware analysis` gekennzeichnet und steht über das RSA Live-Contentmanagementsystem zur Verfügung.

Schadsoftware-Auswertungsmodule

RSA NetWitness Platform Malware Analysis analysiert und wertet Sitzungen und die integrierten Dateien in diesen Sitzungen anhand von vier Kategorien aus: Netzwerk, Statische Analyse, Community und Sandbox. Jede Kategorie umfasst viele einzelne Regeln und Prüfungen, die verwendet werden, um eine Punktzahl zwischen 1 und 100 zu berechnen. Je höher die Punktzahl, desto wahrscheinlicher enthält die Sitzung Schadsoftware und desto eher wird sich eine detaillierte Folgeermittlung lohnen.

Malware Analysis kann Untersuchungen des Verlaufs von Ereignissen vereinfachen, die zu einem Netzwerkalarm oder Incident führen. Wenn Sie wissen, dass eine bestimmte Art von Aktivität in Ihrem Netzwerk stattfindet, können Sie nur die in Frage kommenden Berichte auswählen, um den Content von Datensammlungen zu überprüfen. Sie können auch das Verhalten für jede Auswertungskategorie basierend auf der Auswertungskategorie oder dem Dateityp (Windows PE, PDF und Microsoft Office) ändern.

Sobald Sie sich mit Datennavigationsmethoden vertraut gemacht haben, können Sie die Daten vollständiger untersuchen, indem Sie Folgendes tun:

- Suchen nach bestimmten Arten von Informationen
- Überprüfen bestimmten Contents im Detail.

Kategorieauswertungen für Netzwerk, Statische Analyse, Community und Sandbox werden unabhängig voneinander verwaltet und berichtet. Wenn Ereignisse basierend auf den unabhängigen Auswertungen angezeigt werden, geht aus dem Analyseabschnitt hervor, sobald eine Kategorie Schadsoftware entdeckt.

Netzwerk

Die erste Kategorie überprüft jede Core-Netzwerksitzung, um zu ermitteln, ob die Bereitstellung der Schadsoftwarekandidaten verdächtig war. Beispielsweise gilt eine gutartige Software, die von einer bekannten sicheren Website mithilfe geeigneter Ports und Protokolle heruntergeladen wird, als weniger verdächtig als eine als gefährlich bekannte Software von einer als zweifelhaft bekannten Downloadsite. Die Beispielfaktoren, die bei der Auswertung dieses Kriterienkatalogs verwendet werden, können Sitzungen enthalten, die:

- Bedrohungsfeedinformationen enthalten
- Sich mit wohlbekannten gefährlichen Websites verbinden
- Sich mit Domains/Ländern mit hohem Risiko verbinden (z. B. einer .cc-Domain)
- Wohlbekannte Protokolle auf nicht standardmäßigen Ports verwenden
- Getarntes JavaScript verwenden

Statische Analyse

Die zweite Kategorie analysiert jede Datei in der Sitzung auf Anzeichen einer Tarnung, um die Wahrscheinlichkeit vorherzusagen, dass sich die Datei schädlich verhalten wird, sobald sie ausgeführt wird. Beispielsweise wird eine Software, die sich mit Netzwerkbibliotheken verbindet, wahrscheinlicher verdächtige Netzwerkaktivitäten durchführen. Zu den Beispielfaktoren, die bei der Auswertung dieses Kriterienkatalogs verwendet werden, können die Folgenden gehören:

- Dateien, die als XOR-kodiert erkannt wurden
- Dateien, die als eingebettet innerhalb nicht ausführbarer Formate erkannt wurden (z. B. eine PE-Datei, die in einem GIF-Format eingebettet ist)
- Dateien, die sich mit riskanteren Importbibliotheken verbinden
- Dateien, die in hohem Maße vom PE-Format abweichen

Community

Die dritte Kategorie wertet die Sitzung und die Dateien basierend auf dem kollektives Wissen der Sicherheits-Community aus. So werden z. B. Dateien, deren Fingerabdruck/Hash angesehenen Virenschutzanbietern (AV) bereits als positiv oder negativ bekannt ist, entsprechend klassifiziert. Eine Datei wird auch aufgrund des Wissens, dass sie von einer Website stammt, die von der Sicherheits-Community als positiv oder negativ bekannt ist, klassifiziert.

Die Auswertung durch die Community zeigt auch an, ob der AV in Ihrem Netzwerk die Dateien als schädlich markiert hat. Es zeigt nicht an, ob das vorhandene AV-Produkt Maßnahmen ergriffen hat, um Ihr System zu schützen.

Sandbox

Die vierte Kategorie untersucht das Verhalten der Software, indem sie in einer Sandbox-Umgebung tatsächlich ausgeführt wird. Durch Ausführung der Software, um ihr Verhalten zu beobachten, kann durch die Erkennung wohlbekannter schädlicher Aktivitäten eine Punktzahl berechnet werden. Beispielsweise erhielte eine Software, die sich bei jedem Neustart automatisch startet und IRC-Verbindungen herstellt, eine höhere Punktzahl als eine Datei, die kein als schädlich bekanntes Verhalten zeigt.

Beginnen einer Schadsoftwareanalyse-Ermittlung

Sie können Daten untersuchen, die von Malware Analysis gescannt, markiert und klassifiziert wurden als Indikatoren für eine Infizierung aufweisend. Dazu gehören alle Typen von Malware Analysis-Scans: Abfrage im kontinuierlichen Modus, Abfrage nach Bedarf und nach Bedarf hochgeladene Dateien. Abfrage im kontinuierlichen Modus muss aktiviert werden, wenn der Administrator grundlegende Einstellungen für den Malware Analysis-Service konfiguriert.

NetWitness Platform bietet mehrere Methoden zum Starten einer Malware Analysis-Ermittlung.

Am schnellsten: Sofortiges Starten von Malware Analysis-Dashlets

Die schnellste Art, eine Malware Analysis-Ermittlung zu beginnen, ist ein Sofortstart im NetWitness Platform-Dashboard über eines der Malware Analysis-Dashlets, die Ereignisse oder Dateien auflisten, die wahrscheinlich Schadsoftware enthalten. Die Dashlets werden als Teil des RSA NetWitness-Inhalts unter Dashlets beschrieben. Von einem dieser Dashlets können Sie direkt zu den Analyseergebnissen für ein bestimmtes Ereignis gehen, das als ermittelnswert aufgelistet wurde:

- Top-Liste höchst verdächtiger Schadsoftware
- Top-Liste möglicher Zero-Day-Schadsoftware
- Dashlet Schadsoftware mit IOCs mit hoher Wahrscheinlichkeit und hohen Werten

Abfrage nach Bedarf von einem Metawert in der Navigationsansicht

Sie können die Abfrage nach Bedarf von innerhalb einer Ermittlung starten, indem Sie mit der rechten Maustaste auf einen Metawert in der Navigationsansicht klicken und eine Option aus dem Kontextmenü auswählen. Wenn die Abfrage abgeschlossen ist, stehen die gescannten Daten für die Schadsoftwareanalyse zur Verfügung (siehe Starten eines Malware Analysis-Scans in der Ansicht „Navigation“.

Untersuchen eines bestimmten RSA-Services

Sie können eine Malware Analysis-Ermittlung eines Services auch in der Ansicht „Untersuchen > Malware Analysis“ beginnen. Für Schadsoftwareanalyse-Ermittlungen auf Servicebasis muss ein Service in der Ansicht „Untersuchen > Malware Analysis:Inve“ angegeben werden.

1. Investigate öffnet die Ansicht „Malware Analysis“, wobei der benutzerdefinierte Standardservice ausgewählt ist.
2. Wenn gegenwärtig kein Standardservice angegeben ist, kann in einem Dialogfeld der zu untersuchende Malware Analysis-Service ausgewählt werden kann.
3. Wenn ein Service in der Ansicht „Malware Analysis“ ausgewählt wurde, werden die Ereigniszusammenfassung für den ausgewählten Service und kontinuierliche Scandaten für den Service angezeigt.

Dieses Thema enthält Anweisungen für alle Methoden, eine Malware Analysis-Ermittlung zu starten.

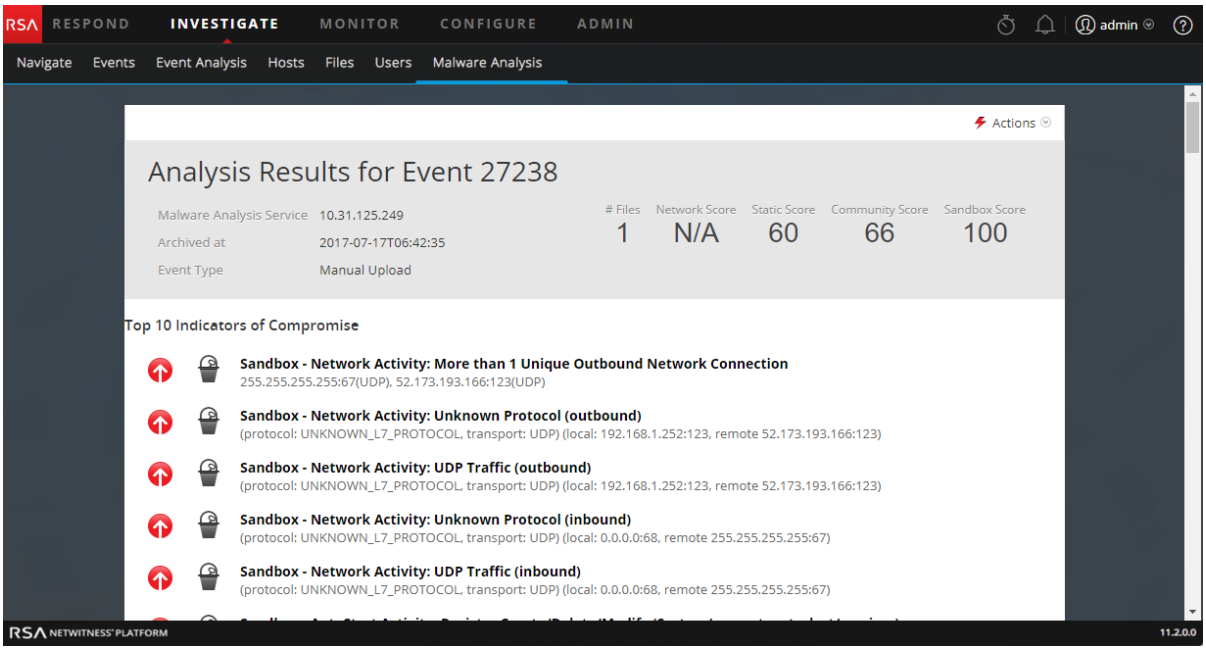
Starten einer Schadsoftwareermittlung von einem Malware Analysis-Dashlet aus

Eine Vorbedingung für dieses Verfahren ist, dass eines der folgenden Dashlets im NetWitness Platform-Dashboard oder in der Malware Analysis-Ansicht sichtbar sein und aufgelistete Ereignisse oder Dateien enthalten muss. Wenn Sie die Dashlets nicht sehen, fügen Sie sie hinzu und konfigurieren Sie sie.

- Top-Liste höchst verdächtiger Schadsoftware
- Top-Liste möglicher Zero-Day-Schadsoftware
- Dashlet Schadsoftware mit IOCs mit hoher Wahrscheinlichkeit und hohen Werten

So starten Sie eine Malware Analysis-Ermittlung von einem Dashlet aus:

1. Melden Sie sich bei NetWitness Platform an und suchen Sie nach einem der oben genannten Dashlets in der Ansicht „Überwachung“ oder in der Ansicht „Malware Analysis“.
2. Doppelklicken Sie im Dashlet auf ein Ereignis oder eine Datei für eine genauere Analyse. In der Malware Analysis-Ansicht wird eine detaillierte Analyse des Ereignisses in der Ereignisliste oder des Ereignisses, mit dem die Datei in der Dateiliste verbunden ist, geöffnet.



Weitere Informationen über die Konfiguration von Malware Analysis-Dashlets im Dashboard „Überwachung“ finden Sie unter „Dashlets“ im *Leitfaden für die ersten Schritte mit NetWitness Platform*.

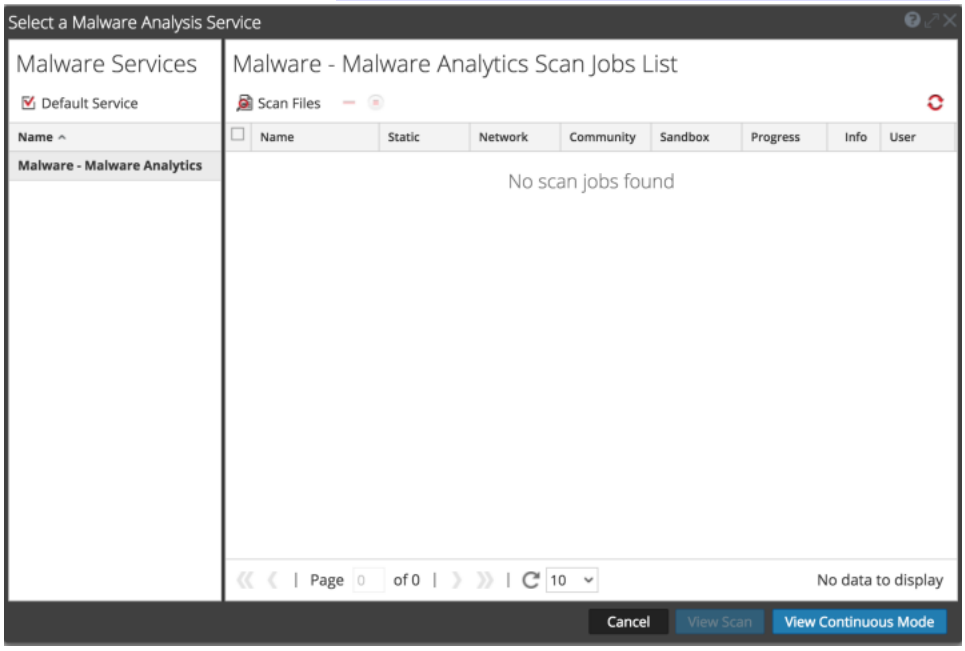
Weitere Informationen über Methoden, Informationen in Dashlets in der Malware Analysis-Ansicht zu konfigurieren und zu filtern, finden Sie unter Filtern der Dashlet-Daten in der Ansicht Ereigniszusammenfassung.

Weitere Informationen über die Aktionen, die Sie in den Analyseergebnissen durchführen können, finden Sie unter Anzeigen der detaillierten Schadsoftwareanalyse eines Ereignisses.

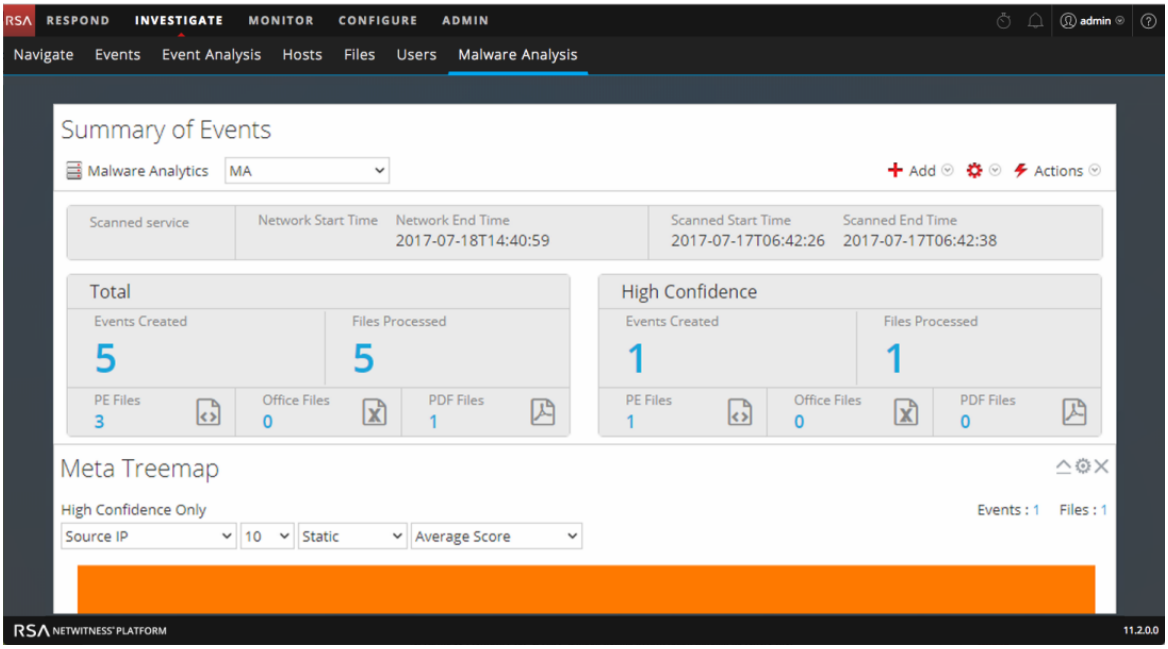
Beginnen einer Malware Analysis Investigation (ohne Standardservice)

So starten Sie eine Ermittlung ohne angegebenen Standardservice:

1. Gehen Sie zu **UNTERSUCHEN** > **Malware Analysis**.
   Das Dialogfeld „Malware Analysis Service auswählen“ wird mit verfügbaren Malware Analysis-Hosts und -Services für den aktuellen Nutzer im linken Bereich und verfügbaren Scanjobs im rechten Bereich angezeigt. Dieser Scanjob-Bereich enthält dieselben Spalten wie das Dashlet „Schadsoftwarescanjobs“ im Dashboard „Unified“. Darüber hinaus hat es eine Symbolleiste und Ansichtsoptionen, die unter Dialogfeld „Malware Analysis Service auswählen“ beschrieben sind.



2. Wählen Sie aus der Liste von Malware Analysis-Hosts einen Host aus. Anschließend wird eine Liste von Scanjobs im rechten Bereich angezeigt. Diese Jobs werden erstellt, wenn Sie ein Ereignis oder eine Datei scannen (siehe Hochladen von Dateien für Malware Analysis-Scans und Starten eines Malware Analysis-Scans in der Ansicht „Navigation“).
3. Führen Sie einen der folgenden Schritte aus, um mit der Analyse eines Scans zu beginnen:
   a. Wählen Sie einen Scan aus und klicken Sie auf **Scan anzeigen**.
   b. Klicken Sie auf **Fortlaufenden Modus anzeigen**.
   Die Ereigniszusammenfassung für den ausgewählten Scan wird mit geöffneten Standard-Dashlets angezeigt. Jeder Benutzer kann Standard-Dashlets hinzufügen, ändern und löschen, die für verschiedene Scanermittlungen persistent sind. Benutzer können außerdem Standard-Dashlets wiederherstellen, wie in Filtern der Dashlet-Daten in der Ansicht Ereigniszusammenfassung beschrieben.

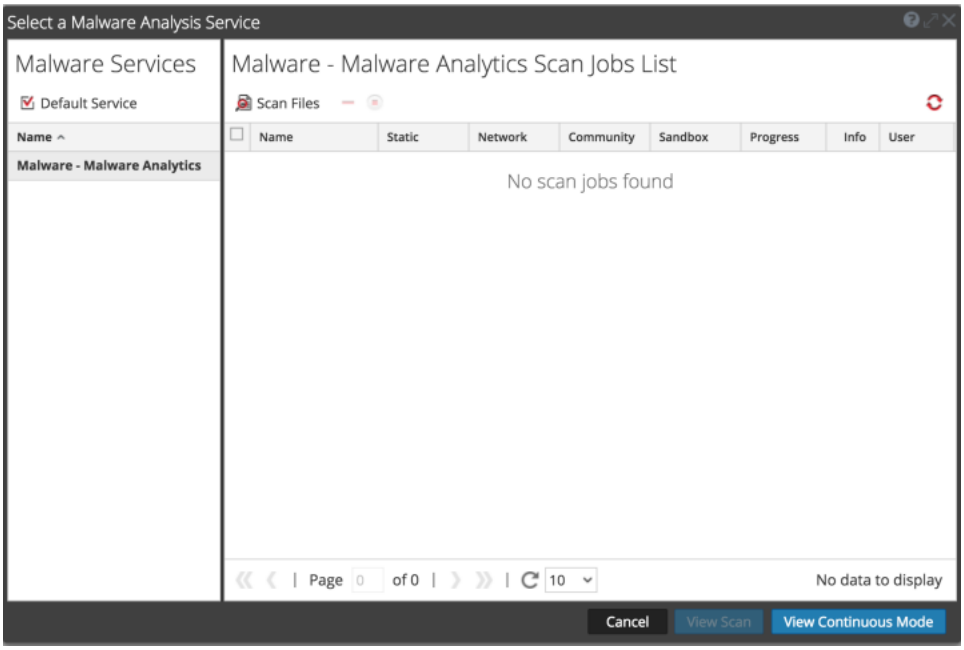


Einrichten oder Löschen des Standardservices

Im Dialogfeld Malware Analysis Service auswählen können Sie den Standardservice festlegen und löschen.

So richten Sie einen Standardservice ein:

1. Klicken Sie in der Symbolleiste „Ereigniszusammenfassung“ auf den Servicenamen.
   Das Dialogfeld Malware Analysis Service auswählen wird angezeigt.



2. Wählen Sie einen Service aus der Liste verfügbarer Schadsoftwareservices aus und klicken Sie auf Default Service.

   Der Service wird zum Standardservice (angezeigt durch ☑ vor dem Hostnamen).

3. Wählen Sie zum Löschen des Standardservices den Service aus dem Raster aus und klicken Sie auf Default Service.

   Es wurde kein Standardservice eingerichtet.

Hochladen und Scannen von Dateien

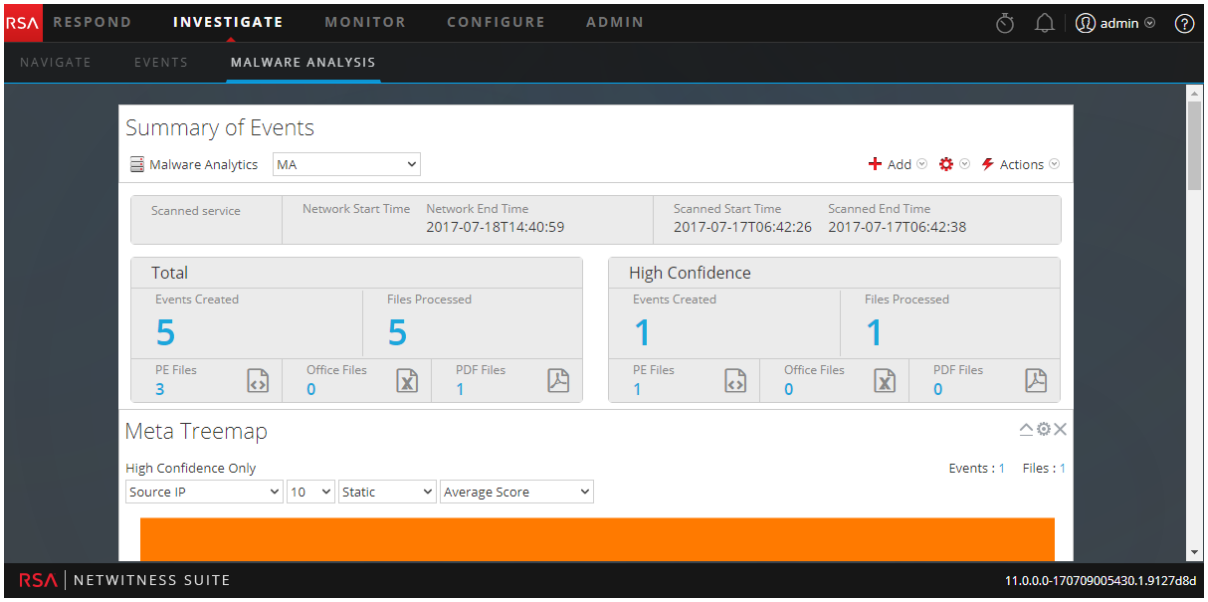
Ein Schadsoftwareanalyst mit der Berechtigung für `Initiate Malware Analysis Scan` kann zu scannende Dateien mithilfe der Option „Dateien scannen“ des Dialogfelds „Malware Analysis Service auswählen“ hochladen (siehe Hochladen von Dateien für Malware Analysis-Scans). Ein Administrator kann Paketerfassungsdateien zu einem Decoder für Malware Analysis in der Ansicht „Services-System“ hochladen, wie in „Hochladen einer Paketerfassungsdatei“ im *Konfigurationsleitfaden für Decoder und Log Decoder* beschrieben.

Starten einer Ermittlung (Standardservice angegeben)

So starten Sie eine Ermittlung mit angegebenem Standardservice:

1. Gehen Sie zu **UNTERSUCHEN** > **Malware Analysis**.

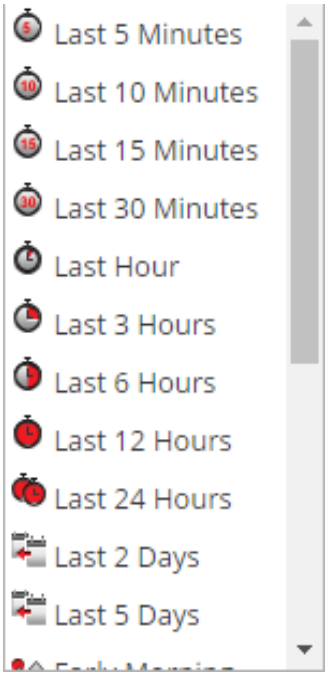
   Die Ereigniszusammenfassung für den kontinuierlichen Scan des ausgewählten Services wird mit den geöffneten Standard-Dashlets angezeigt. Jeder Benutzer kann Standard-Dashlets hinzufügen, ändern und löschen, die für verschiedene Scanermittlungen persistent sind. Benutzer können außerdem Standard-Dashlets wiederherstellen, wie in Filtern der Dashlet-Daten in der Ansicht Ereigniszusammenfassung beschrieben.



Anwenden von Zeitparameterfilter auf Ergebnisse

Sie können einen Schwellenwertfilter anwenden, um die Ergebnisse der ausgewählten Dashlets zu aktualisieren.

1. Wählen Sie zur Auswahl eines anderen Zeitraums entweder **Kontinuierlicher Modus** oder einen anderen Scan aus der Symbolleiste aus.
   Die Schadsoftware-Ereigniszusammenfassung für den ausgewählten Scan wird angezeigt.
2. Klicken Sie zur Auswahl eines neuen Zeitraums für den Scan auf die Bereichsauswahlliste in der Symbolleiste. Folgende Bereiche sind verfügbar: Letzte 5 Minuten, letzte 10 Minuten, letzte 15 Minuten, letzte 30 Minuten, letzte Stunde, letzte 3 Stunden, letzte 6 Stunden, letzte 12 Stunden, letzte 24 Stunden, letzte 2 Tage, letzte 5 Tage, Morgen, Vormittag, Nachmittag, Abend, den ganzen Tag, gestern, diese Woche, letzte Woche oder benutzerdefiniert.



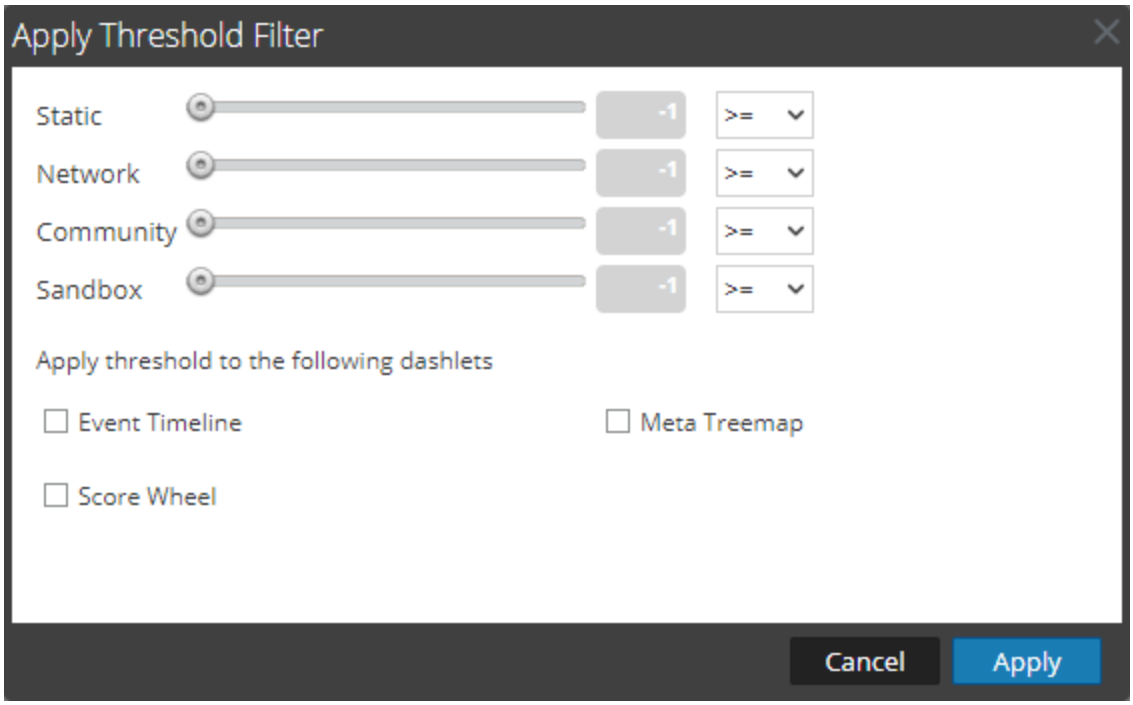
   Die Ergebnisse werden sofort aktualisiert.
3. Klicken Sie zur Aktualisierung eines Scans im kontinuierlichen Modus mit neuen Daten auf .

Anwenden eines Schwellenwertfilters auf Ergebnisse von Scans im kontinuierlichen Modus

Sie können einen neuen Schwellenwertfilter auf eine Instanz des Dashlet „Schadsoftware mit IOCs mit hoher Wahrscheinlichkeit und hohen Werten“, des Dashlet „Meta-Treemap“, des Dashlet „Ergebnisrad“ und des Dashlet „Ereigniszeitachsen“ anwenden.

Gehen Sie zur Anpassung der auf den Scan angewendeten Auswertung in der Symbolleiste wie folgt vor:

1. Wählen Sie > **Schwellenwertfilter anwenden.**
   Das Dialogfeld „Schwellenwertfilter anwenden“ wird angezeigt.



2. Wenn Sie die Anzahl der angezeigten Ereignisse auf Ereignisse beschränken möchten, die einen Wert über einem bestimmten Schwellenwert erhalten haben, gehen Sie wie folgt vor:
   a. Ziehen Sie die Schieberegler für Statisch, Netzwerk, Community und Sandbox.
   b. Aktivieren Sie zur Auswahl der Dashlets, auf die die Schwellenwerte zutreffen, die entsprechenden Kontrollkästchen.
   c. Klicken Sie auf **Anwenden**.

Löschen oder erneutes Übermitteln eines Scans nach Bedarf mit neuen Umgehungseinstellungen

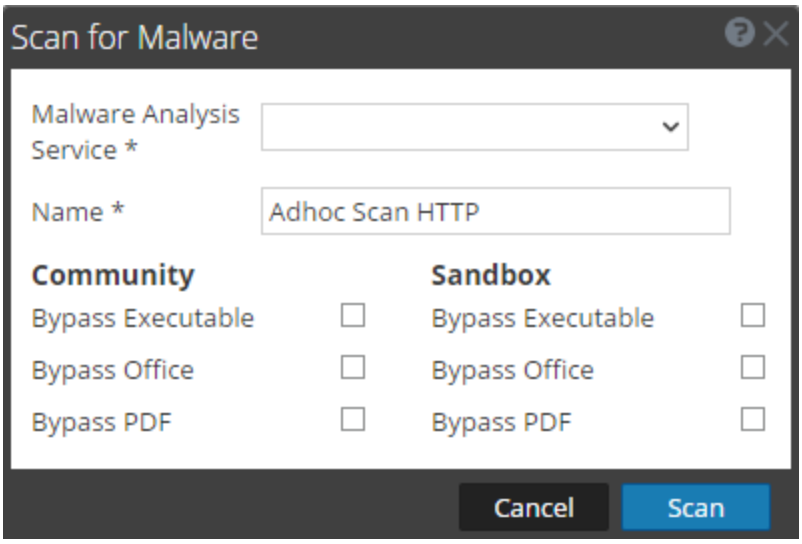
Sie können einen Scan nach Bedarf löschen oder ihn mit anderen Umgehungseinstellungen als denjenigen, die in der Servicekonfigurationsansicht für einen Malware Analysis-Service angegeben sind, erneut übermitteln.

Gehen Sie zum Löschen eines Scans während der Anzeige eines Scans nach Bedarf wie folgt vor:

1. Wählen Sie **Aktionen** > **Scan löschen** aus.
   Ein Dialogfeld fordert Sie auf, zu bestätigen, dass Sie den Scan löschen möchten.
2. Klicken Sie auf **Yes**.
   Der ausgewählte Scan wird gelöscht.

So wenden Sie andere Umgehungseinstellungen auf den aktuellen Scan an:

1. Wählen Sie **Aktionen > Scan erneut übermitteln** aus.
   Das Dialogfeld „Auf Schadsoftware scannen“ wird angezeigt.



2. Wählen Sie die Umgehungseinstellungen aus, die Sie auf den neuen Scan anwenden möchten, und klicken Sie auf **Scannen**.
   Malware Analysis setzt den Cache zurück und übermittelt die Datei für einen neuen Scan erneut und die Scanjobs werden der Jobwarteschlange hinzugefügt.
3. Blättern Sie nach Abschluss des Jobs nach links und wählen Sie **Anzeigen** aus.
   Die Schadsoftware-Ereigniszusammenfassung für den ausgewählten Scan wird angezeigt.

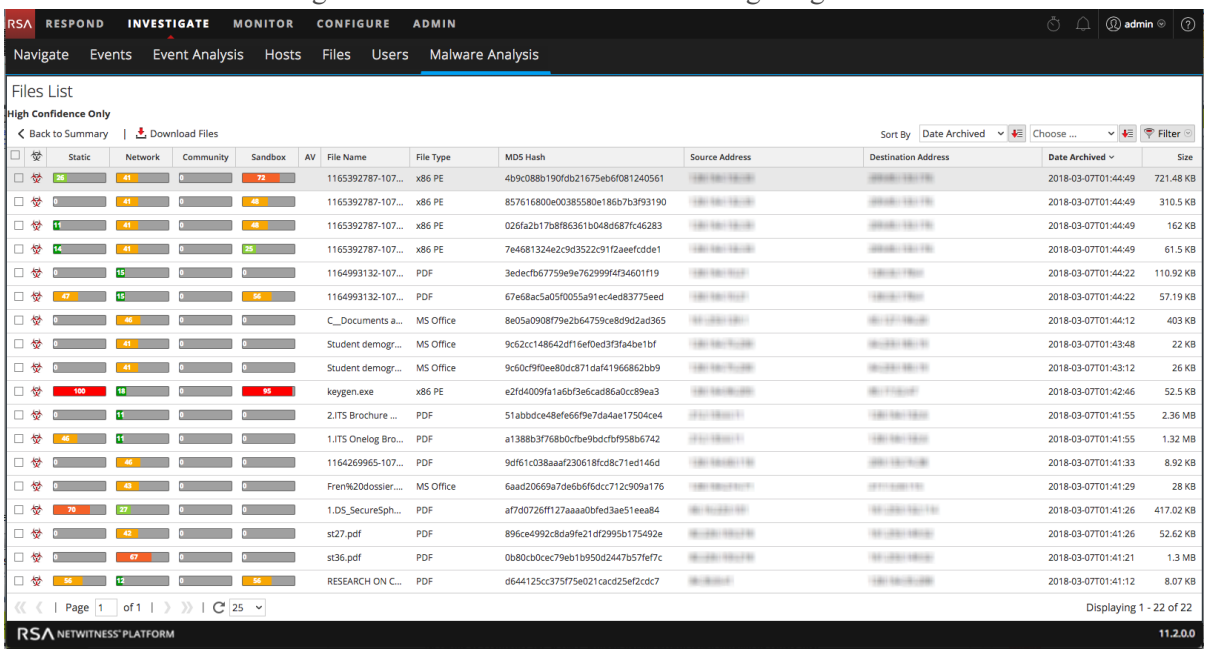
Anzeigen der Dateiliste

Sie können eine Liste von Dateien für ein Ereignis von der Malware Analysis-Ereigniszusammenfassung und von jedem der Visualisierungsdiagramme anzeigen: Ereigniszeitachse, Meta-Strukturen, Meta-Treemap und Ergebnisrad.

Führen Sie für den Zugriff auf die Dateiliste einen der folgenden Schritte aus:

- Klicken Sie in der Ereigniszusammenfassung auf die Anzahl der Dateien in der Zeile **Gesamt** oder in der Zeile **Hohe Wahrscheinlichkeit** unter **Verarbeitete Dateien**, **PE-Dateien**, **Office-Dateien** oder **PDF-Dateien**. Die Dateiliste wird angezeigt.
- Klicken Sie in einem Visualisierungs-Dashlet auf die Zahl neben dem Feld **Dateien** oben rechts im Dashlet.

Die Dateiliste für den ausgewählten Drill-down-Punkt wird angezeigt.



In der Dateiliste können Sie nach einer Datei nach Dateiname oder MD5-Datei-Hash suchen, die Liste nach zwei Kriterien und in aufsteigender oder absteigender Reihenfolge sortieren und Dateien herunterladen wie in Überprüfen von Scandateien und Ereignissen in Listenform beschrieben.

Um zur Ereigniszusammenfassung zurückzukehren, klicken Sie auf **Zurück zur Zusammenfassung**.

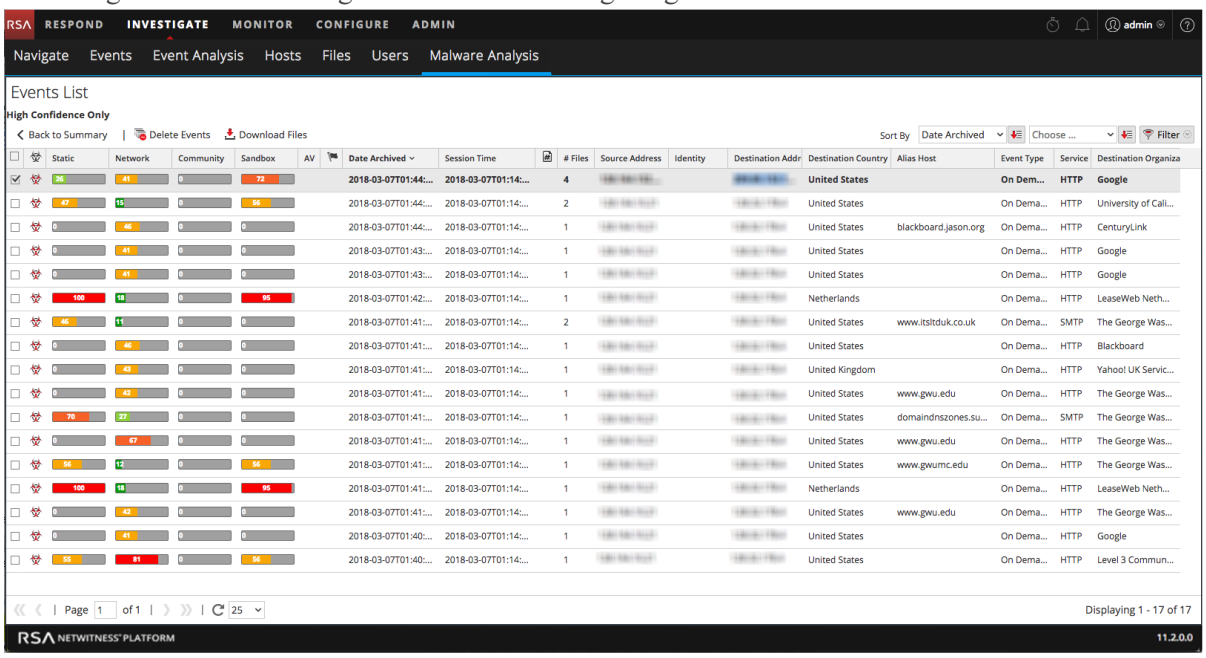
Anzeigen der Ereignisliste

Von der Malware Analysis-Ereigniszusammenfassung und von jedem der Visualisierungsdiagramme aus (Ereigniszeitachse, Meta-Strukturen, Meta-Treemap und Ergebnisrad) können Sie Ereignisse zur Ansicht im Raster „Ereignisse“ auswählen.

Führen Sie für den Zugriff auf die Ereignisliste einen der folgenden Schritte aus:

- Klicken Sie in der Ereigniszusammenfassung auf die Anzahl der erstellten Ereignisse in der Zeile **Gesamt** oder in der Zeile **Hohe Wahrscheinlichkeit**. Die Ereignisliste wird angezeigt.
- Klicken Sie in einem Visualisierungs-Dashlet auf die Zahl neben dem Feld „Ereignisse“ oben rechts im Dashlet.

Die Ereignisliste für die ausgewählte Zeit wird angezeigt.



Implementieren von angepassten YARA-Inhalten

Zusätzlich zu den integrierten Indikatoren für eine Infizierung unterstützt Malware Analysis auch in YARA geschriebene Indikatoren für eine Infizierung. YARA ist eine Regelsprache, die es Schadsoftware-Forschern erlaubt, Muster von Schadsoftware zu identifizieren und zu klassifizieren. RSA stellt integrierte YARA-basierte IOCs (Indicators of Compromise, Indikatoren für eine Infizierung) in RSA Live zur Verfügung. Diese werden automatisch auf abonnierte Hosts heruntergeladen und dort aktiviert.

Kunden mit fortgeschrittenen Fähigkeiten und Kenntnissen können die Erkennungsfunktionen von RSA Malware Analysis erweitern, indem sie YARA-Regeln erstellen und in RSA Live veröffentlichen oder diese zur Verarbeitung durch den Host in einen beobachteten Ordner platzieren.

Da Schadsoftwares und Bedrohungen immer häufiger vorkommen, ist es wichtig, die bestehenden benutzerdefinierten Regeln zu überprüfen und zu überwachen. Oft sind Updates notwendig, um neue Erkennungsmethoden zu übernehmen. Zudem aktualisiert RSA gelegentlich YARA-Regeln in Live. Wenn Sie Updates erhalten möchten, können Sie den RSA-Blog oder RSA Live unter http://blogs.rsa.com/feed abonnieren.

Dieses Dokument stellt Kunden Informationen bereit, die bei der Implementierung von benutzerdefinierten YARA-Regeln in Malware Analysis helfen sollen.

Voraussetzungen

Der Host, dem Sie benutzerdefinierte Regeln hinzufügen, muss so konfiguriert werden, dass die Erstellung von YARA-Regeln unterstützt wird, wie unter „Aktivieren von benutzerdefinierten YARA-Inhalten“ im *Malware Analysis-Konfigurationsleitfaden* beschrieben.

YARA-Version und -Ressourcen

RSA Malware Analysis verfügt über die YARA-Version 3.7 (rev:167). Um die genaue Version zu ermitteln, können Sie `yara -v` auf dem Malware Analysis-Host ausführen, wie in diesem Beispiel gezeigt wird:

```
[root@TESTHOST yara] # yara -v
 yara 3.7 (rev:167)
```

Metaschlüssel in YARA-Regeln

Malware Analysis ist mit anderen Quellen von YARA-Regeln konform und ruft zusätzliche Metaschlüssel ab, die für Malware Analysis spezifisch sind. Jede YARA-Regel entspricht einem Indikator für eine Infizierung (Indicator of Compromise, IOC) innerhalb von Malware Analysis. Das unten stehende Beispiel zeigt die Metadefinitionen in einer Regel:

```
meta:
 iocName = "FW.ecodedGenericCLSID"
        fileType = "WINDOWS_PE"
        score = 25
        ceiling = 100
        highConfidence = false
```

Metaschlüssel	Beschreibung
IOC-Name	(Erforderlich) Dies ist der Name, den MA als Name der Regel verwendet. Er ist ein für Malware Analysis spezifischer Name, der erforderlich ist, um die Regel der IOC-Liste hinzuzufügen.
fileType	Gibt den Dateityp an. Die möglichen Werte sind: WINDOWS_PE, MS_OFFICE, und PDF. Wenn keine Angabe gemacht wird, ist der Standardwert WINDOWS_PE.
score	Dieser Wert wird zum statischen Wert addiert, wenn die YARA-Regel ausgelöst wird. Wenn kein Wert angegeben wird, ist der Standardwert 10.
ceiling	Dies ist der maximale Wert, der zum statischen Wert hinzuaddiert wird, wenn eine Regel mehrere Male während einer Sitzung ausgelöst wird. Beispiel: Jedes Mal, wenn eine Regel ausgelöst wird, werden 20 Punkte zum statischen Wert addiert. Möchten Sie, dass nicht mehr als 40 Punkte hinzuaddiert werden, wenn die Regel mehr als zweimal ausgelöst wird, können Sie eine Grenze (Ceiling) von 40 Punkten setzen. Wenn kein Wert angegeben wird, ist der Standardwert 100.
highConfidence	Dies markiert die hohe Wahrscheinlichkeit, die für IOCs bestimmt wurden. Anzeichen weisen so darauf hin, dass mit hoher Wahrscheinlichkeit eine Schadsoftware vorliegt. Wenn kein Wert angegeben wird, lautet der Standarddateiwert „False“.

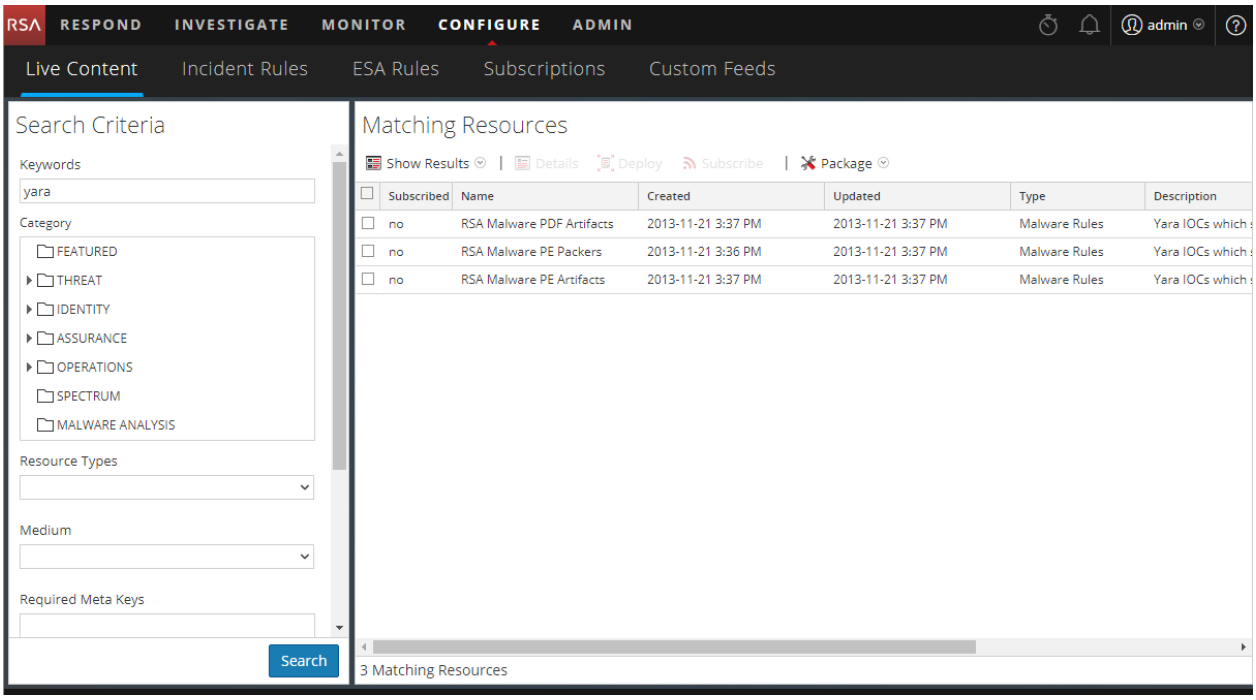
Hinweis: Weitere Informationen zu YARA-Ressourcen erhalten Sie unter der folgenden URL: https://code.google.com/p/yara-project/downloads/list. NetWitness Platform nutzt YARA 3.7, nicht YARA 2.0.

YARA-Inhalte

RSA Live beinhaltet drei Arten von YARA-Regeln:

- PE Packers
- PDF Artifacts
- PE Artifacts

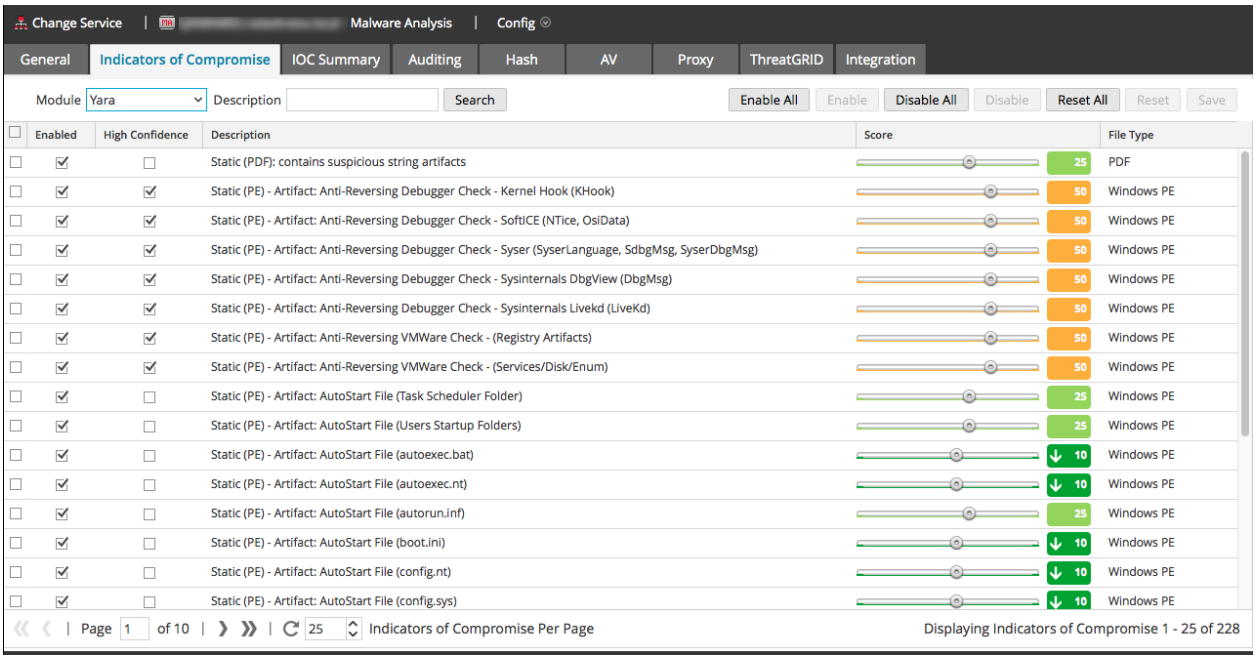
Die folgende Abbildung zeigt YARA-Inhalte verfügbar als YARA-Regeln in NetWitness Platform Live.



Auf dem Malware Analysis-Host befinden sich die YARA-Regeln in `/var/lib/netwitness/malware-analytics-server/spectrum/yara`, wie im folgenden Beispiel gezeigt.

```
[root@TESTHOST yara]# pwd
 /var/lib/netwitness/malware-analytics-server/spectrum/yara
 [root@TESTHOST yara]# ls *.yara
 rsa_mw_pdf_artifacts.yara rsa_mw_pe_artifacts.yara rsa_mw_pe_packers.yara
```

Die einzelnen Regeln sind als IOCs in der Malware Analysis-Ansicht „Service-Konfiguration“ > Registerkarte „Indikatoren für eine Infizierung“ aufgeführt. Verwenden Sie das YARA-Modul als Filter, um diese Regeln anzuzeigen. Sie können die Konfiguration einer einzelnen Regel auf die gleiche Weise anpassen, wie Sie andere IOCs konfigurieren.



Hinzufügen von benutzerdefinierten YARA-Regeln

So integrieren Sie YARA-Regeln aus anderen Quellen:

1. Um sicherzugehen, dass YARA-Regeln dem richtigen Format und der richtigen Syntax folgen, verwenden Sie den YARA-Befehl, um die YARA-Regel wie im folgenden Beispiel zu kompilieren. Wenn die Regel ohne Fehlermeldung kompiliert wird, folgt die YARA-Regel der richtigen Syntax.
   ```
   [root@TESTHOST yara]# yara rsa_mw_pe_packers.yara dummy.txt
    [root@TESTHOST yara]#
   ```
2. Stellen Sie sicher, dass benutzerdefinierte Regeln keine bestehenden YARA-Regeln aus RSA oder anderen Quellen duplizieren. Alle YARA-Regeln befinden sich in `/var/lib/netwitness/malware-analytics-server/spectrum/yara`
3. Stellen Sie sicher, dass die von RSA unterstützten Metaschlüssel enthalten sind, sodass die YARA-Regeln als Teil der konfigurierbaren IOCs organisiert werden können und fügen Sie am Ende des Dateinamens die yara-Erweiterung (<filename>.yara).an. Sie können eine bessere Organisation gewährleisten, indem Sie sicher stellen, dass der Metawert `iocName` wie im folgenden Beispiel in der Metadefinition enthalten ist.

   Beispiel:
   ```
   rule HEX_EXAMPLE
    {
        meta:
            author = "RSA"
            info = "HEX Detection"
           iocName = "Hex Example"
         strings:
            $hex1 = { E2 34 A1 C8 23 FB }
   ```

```
        $wide_string = "Ausov" wide ascii
    condition:
        $hex1 or $wide_string
}
```

4. Wenn Sie fertig sind, platzieren Sie die benutzerdefinierten YARA-Dateien in den Ordner, der vom Malware Analysis-Service beobachtet wird:
   `/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`
   Die Datei wird innerhalb einer Minute verarbeitet.
   Sobald die Datei verarbeitet wurde, wird sie von NetWitness Platform in den Ordner `processed` verschoben und die neue Regel wird in der Malware Analysis-Ansicht „Service-Konfiguration“ > auf der Registerkarte „Indikatoren für eine Infizierung“ hinzugefügt.

Überprüfen von Scandateien und Ereignissen in Listenform

Wenn Sie die Ereigniszusammenfassung eines Scans in Malware Analysis anzeigen, können Sie auf die Anzahl der Dateien oder Ereignisse klicken, um die Datei- bzw. Ereignisliste für den Scan anzuzeigen (siehe Beginnen einer Schadsoftwareanalyse-Ermittlung). In der Datei- bzw. Ereignisliste können Sie über den Dateinamen oder MD5-Datei-Hash nach einer Datei suchen, die Liste anhand von zwei Kriterien auf- oder absteigend sortieren und Dateien herunterladen. Wenn Sie in der Ereignis- oder Dateiliste auf Ereignisse oder Dateien stoßen, über die Sie mehr erfahren möchten, können Sie zahlreiche Details zu diesem Ereignis in der Ansicht „Ereignisdetails“ anzeigen.

Die folgenden Informationen werden von NetWitness Platform für jedes Ereignis in der Ereignisliste angegeben:

- Markiert als ein Ereignis mit hoher Wahrscheinlichkeit, das wahrscheinlich Indikatoren für eine Infizierung enthält.
- Die numerische Punktzahl für jedes Bewertungsmodul: Statisch, Netzwerk, Community und Sandbox.
- Auswertungen der Virenschutzanbieter.
- Das Flag Von benutzerdefinierter Regel beeinflusst.
- Das Datum, an dem das Ereignis archiviert wurde.
- Die Sitzungszeit.
- Der MD5-Hash-Filter.
- Die Anzahl der Dateien im Ereignis.
- Die Quell-IP-Adresse des Ereignisses.
- Die Identität.
- Die Ziel-IP-Adresse.
- Das Zielland.
- Der Name des Aliashosts.
- Der Ereignistyp, zum Beispiel Netzwerk.
- Der vom Ereignis verwendete Service.
- Die Zielorganisation

Die folgenden Informationen werden von NetWitness Platform für jede Datei in der Dateiliste angegeben:

- Markiert als ein Ereignis mit hoher Wahrscheinlichkeit, das wahrscheinlich Indikatoren für eine Infizierung enthält.
- Die numerische Punktzahl für jedes Bewertungsmodul: Statisch, Netzwerk, Community und Sandbox.
- Auswertungen der Virenschutzanbieter.
- Der Dateiname.

- Der Dateityp.
- Der MD5-Hash-Filter.
- Die Quell-IP-Adresse des Ereignisses, in dem die Datei enthalten war.
- Die Ziel-IP-Adresse.
- Das Datum, an dem das Ereignis, in dem die Datei enthalten war, archiviert wurde.
- Die Dateigröße.

Sortieren der Datei- bzw. Ereignisliste

Sie können die Datei- bzw. Ereignisliste nach Spaltenname in auf- oder absteigender Reihenfolge sortieren. Sie können eine oder zwei Spalten auswählen.

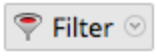
So sortieren Sie die Liste:

1. Wählen Sie in der ersten Drop-down-Liste **Sortieren nach** einen Spaltennamen und die Sortierreihenfolge aus:  für die absteigende oder  für die aufsteigende Reihenfolge.
2. (Optional) Wählen Sie in der zweiten Drop-down-Liste **Sortieren nach** einen Spaltennamen und die Sortierreihenfolge aus:  für die absteigende oder  für die aufsteigende Reihenfolge.
   Im Spaltentitel wird die ausgewählte Sortierreihenfolge angezeigt.

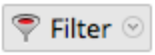
Filtern der Liste nach Dateinamen oder MD5-Datei-Hash

Sie können die Datei- bzw. Ereignisliste nach Dateinamen oder Datei-Hash filtern. Mit dieser Funktion können Sie eine begrenzte Teilmenge der ursprünglichen Daten anhand der Suchkriterien festlegen.

Hinweis: Wenn Sie eine Suche durchführen, wird der aktuell angezeigte Scan durchsucht (nicht alle Scans).

1. Klicken Sie auf 

   .
   Das Dialogfeld „Filter“ wird angezeigt.
2. Geben Sie unter **Dateiname** oder **MD5-Hash** einen Wert ein und klicken Sie auf **Filter**. Bei den Feldern Dateiname und Hash wird nicht zwischen Groß- und Kleinschreibung unterschieden. Platzhalter und reguläre Ausdrücke werden nicht unterstützt. Der Filter basiert auf genauen Übereinstimmungen. Sie können den Cursor über einen Dateinamen oder Hash ziehen, um das Element in der Datei- bzw. Ereignisliste auszuwählen. Dann können Sie den Namen kopieren und in das Dialogfeld einfügen.
3. Klicken Sie auf **Filter**.
   Malware Analysis filtert die Liste, sodass nur Dateien oder Ereignisse mit dem ausgewählten Hash angezeigt werden.

4. Um zur nicht gefilterten Liste zurückzukehren, klicken Sie auf 

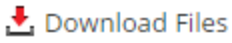
. Wenn das Dialogfeld „Filter“ angezeigt wird, klicken Sie auf **Zurücksetzen**.

Herunterladen von Dateien aus der Dateiliste

In NetWitness Platform können Sie Dateien in der Datei- bzw. Ereignisliste auswählen und herunterladen.

Achtung: Seien Sie vorsichtig, wenn Sie Dateien aus Malware Analysis herunterladen. Manche Dateien können schädlichen Code enthalten. Der Dateidownload ist eine konkrete konfigurierbare Berechtigung. Ausführlichere Informationen erhalten Sie unter „Definieren von Rollen und Berechtigungen für Benutzer der Schadsoftwareanalyse“ im *Konfigurationsleitfaden Malware Analysis*.

So laden Sie Dateien aus der Datei- bzw. Ereignisliste herunter:

1. Aktivieren Sie in der Datei- bzw. Ereignisliste das Kontrollkästchen neben einer oder mehreren Zeilen.
2. Wählen Sie in der Symbolleiste die Option 

aus.
   Das Dialogfeld „Schadsoftware-Dateidownload“ wird angezeigt.
3. Führen Sie einen der folgenden Schritte aus:
   a. Wenn Sie die Datei doch nicht herunterladen möchten, klicken Sie auf **Abbrechen**.
   b. Wenn Sie die Datei herunterladen möchten, klicken Sie auf die Schaltfläche **Herunterladen**.
      Die ausgewählten Dateien werden in einem ZIP-Archiv mit dem Namen `Malware_Files.zip` heruntergeladen.

Löschen von Ereignissen aus dem Scan

Wählen Sie in der Ereignisliste ein oder mehrere Ereignisse aus und löschen Sie diese aus dem Scan. Auf diese Weise können Sie Ereignisse entfernen, die nicht von Interesse sind.

So entfernen Sie ein Ereignis aus dem angezeigten Scan:

1. Wählen Sie in der **Ereignisliste** mindestens ein Ereignis aus.
2. Klicken Sie in der Symbolleiste auf die Option 

.
   NetWitness Platform fordert eine Bestätigung an, dass Sie die Ereignisse löschen möchten.
3. Klicken Sie im Bestätigungsdialogfeld auf **Ja**.
   Die ausgewählten Ereignisse werden gelöscht.

Rückkehr zur Ereigniszusammenfassung

Um die Datei- oder Ereignisliste zu verlassen und zur Ereigniszusammenfassung zurückzukehren, klicken Sie auf **Zurück zur Zusammenfassung**.

Öffnen der detaillierten Analyse für ein Ereignis

Während Sie Ereignisse oder Dateien in der Datei- bzw. Ereignisliste untersuchen, können Sie auf ein Ereignis bzw. eine Datei doppelklicken, um eine detaillierte Analyse des Ereignisses in der Ereignisliste bzw. des Ereignisses aufzurufen, dem die Datei in der Dateiliste zugeordnet ist (siehe Anzeigen der detaillierten Schadsoftwareanalyse eines Ereignisses).

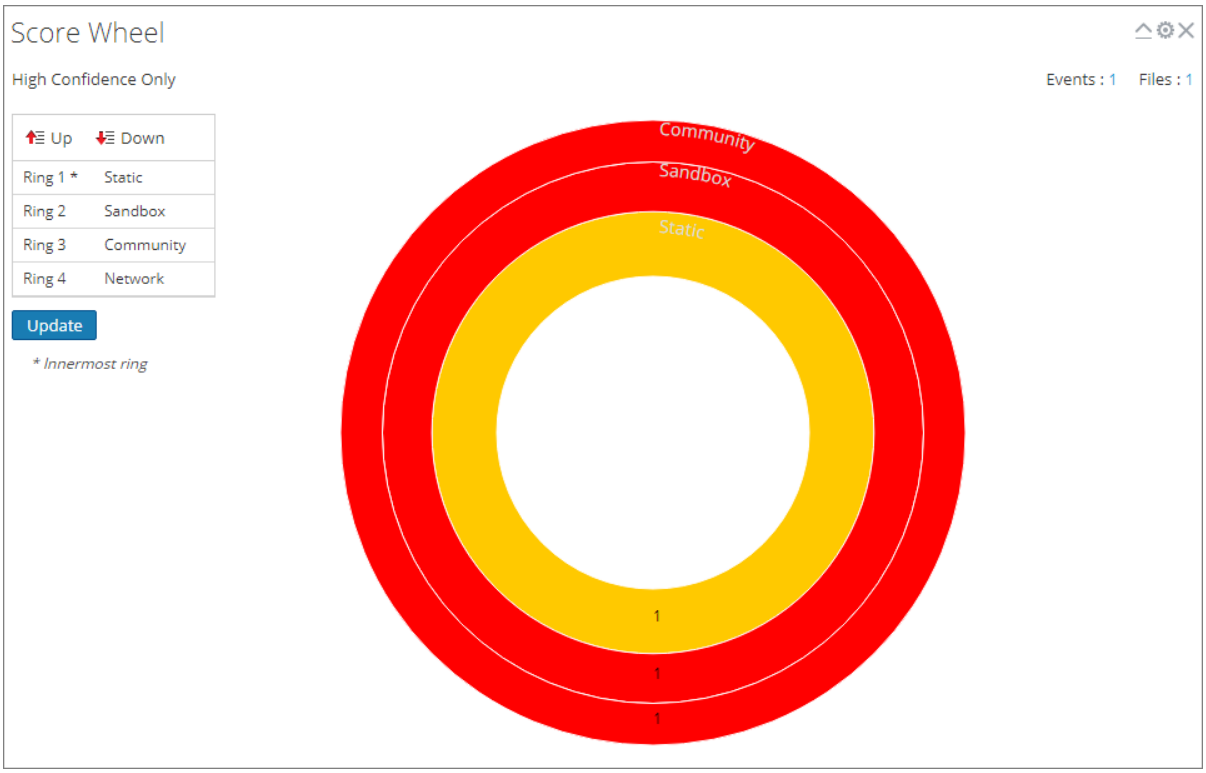
Filtern der Dashlet-Daten in der Ansicht Ereigniszusammenfassung

Ereigniszusammenfassung enthält eine Zusammenfassung des untersuchten Scans mit auswählbaren Dashlets. Die Ereigniszusammenfassung ist fest definiert, jedoch können Analysten jedes Dashlet so konfigurieren, dass Informationen gefiltert werden und ein Drill-down in die Daten erfolgen kann.

Der Rest dieses Themas enthält Anweisungen für Management und Konfiguration von Dashlets.

Konfiguration des Dashlet „Ergebnisrad“

Das Ergebnisrad ist eine allgemeine Visualisierung von analysierten Sitzungen, die eine hohe, mittlere oder niedrige Punktezahl in den jeweiligen Bewertungskategorien erzielt haben: Statisch, Netzwerk, Community und Sandbox. Das Ergebnisrad bietet eine schnelle Möglichkeit, einen Drill-down zur Überprüfung von Sitzungen auszuführen. Jeder Ring steht für eine andere Bewertungskategorie, sodass Sie die Ergebnisse nach Kategorien visuell vergleichen können.

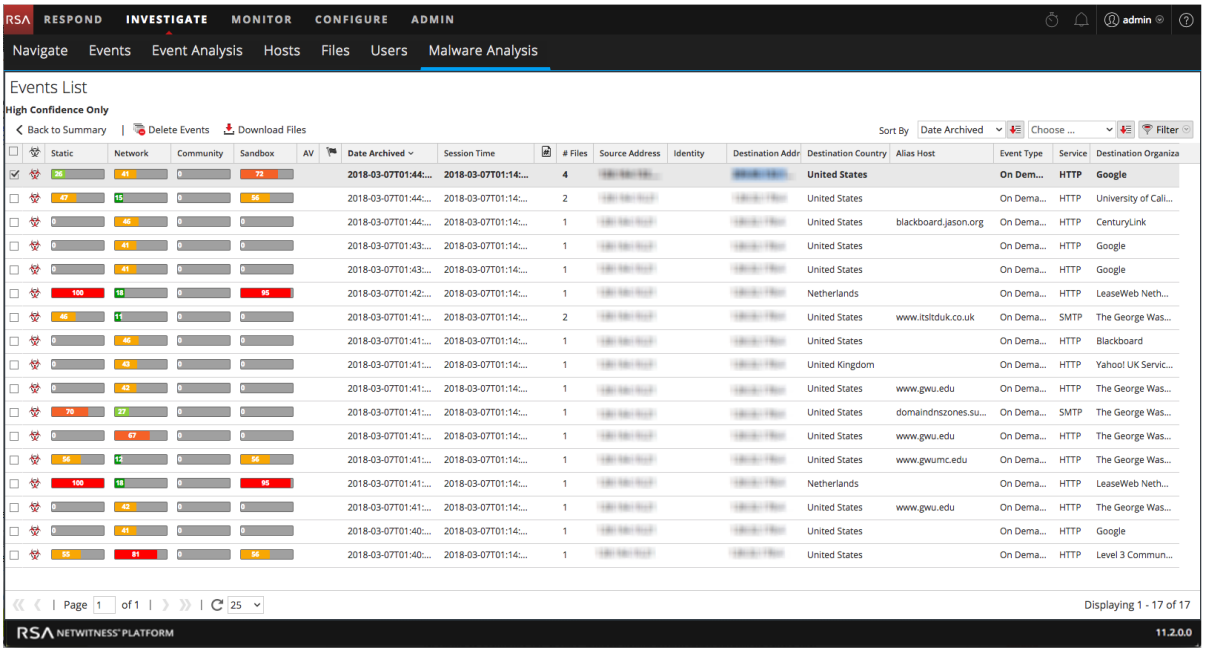


Sie können die Reihenfolge der Ringe ändern, um Indikatoren für eine Infizierung hervorzuheben, die nur in einer der Kategorien gekennzeichnet wurden. Das Vergleichen derselben Ergebnisse in unterschiedlichen Reihenfolgen der Ringe liefert Einblicke in zusätzliche Anfälligkeiten während einer Sitzung und Sie können bei der entsprechenden Sitzung einen Drill-down durchführen. Es folgen zwei Anwendungsbeispiele.

Beispiel: Zero-Day-Kandidaten

Dieses Beispiel zeigt, wie man einen Drill-down bei einer Sitzung durchführt, die von der Kategorie Community zwar nicht als schädlich gekennzeichnet wurde, dafür aber von allen anderen Bewertungskategorien. Die daraus resultierende Liste der Sitzungen hebt Zero-Day-Kandidaten hervor.

1. Konfigurieren Sie die Bereiche des Ergebnisrads in der folgenden Reihenfolge: **Community** (ganz innen) > **Statisch** > **Netzwerk** > **Sandbox** (ganz außen)
2. Klicken Sie auf das rote Segment im äußersten Ring (Sandbox), das auf ein grünes Segment im innersten Ring (Community) ausgerichtet ist: grün (innerster) -> **Statisch**: rot -> **Netzwerk**: rot -> **Sandbox**: rot (äußerster).



Beispiel: Schädliche Sitzungen

In diesem Beispiel wird gezeigt, wie man einen Drill-down bei Sitzungen durchführt, bei denen alle Bewertungskategorien die resultierende Sitzungsliste als schädlich identifizieren, indem angegeben wird, dass Malware Analysis dafür die höchste Wahrscheinlichkeit aufweist.

1. Konfigurieren Sie die Bereiche des Ergebnisrads in der folgenden Reihenfolge: **Community** (ganz innen) > **Statisch** > **Netzwerk** > **Sandbox** (ganz außen)
2. Klicken Sie auf das rote Segment des äußersten Bereichs (Sandbox), der auf ein rotes Segment im innersten Bereich (Community) ausgerichtet ist: rot (innerster) -> Statisch: rot -> Netzwerk: rot -> Sandbox: rot (äußerster).

Ordnen der Reihenfolge der Bereiche nach dem Bewertungsmodul

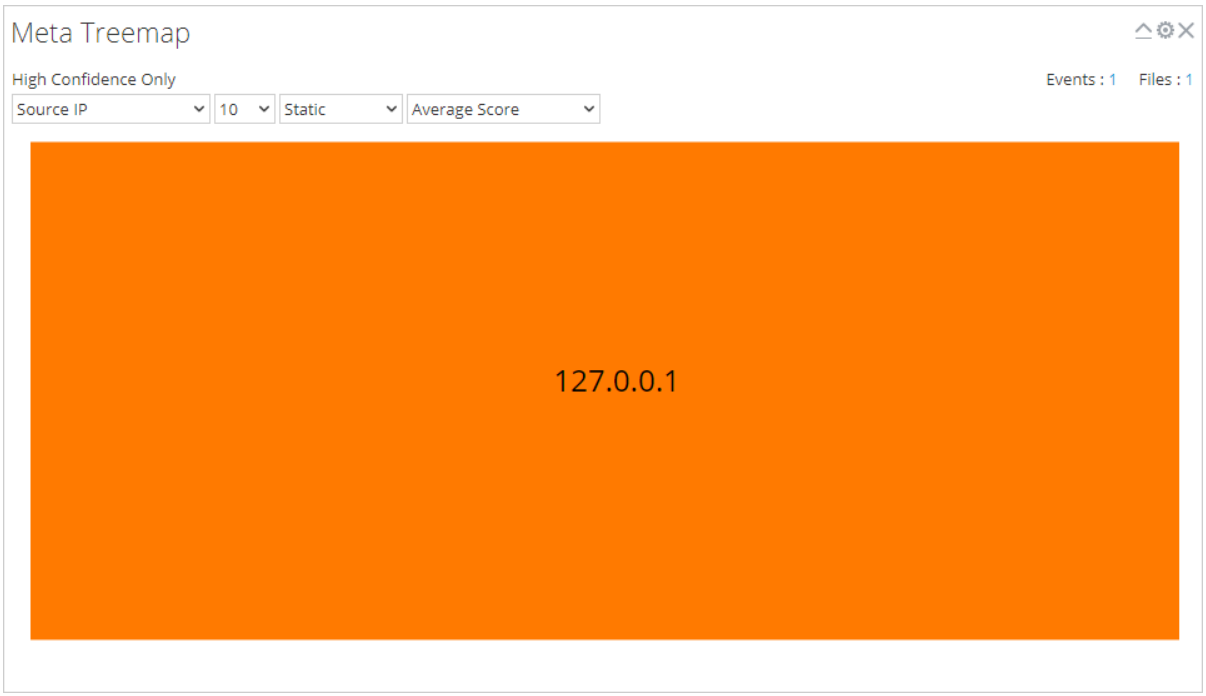
Im Ergebnisrad können Sie die Reihenfolge der Bereiche nach dem Bewertungsmodul ordnen. Zunächst ist die Reihenfolge der Bereiche von innen nach außen wie folgt: Statisch, Netzwerk, Community, und Sandbox.

So verändern Sie die Reihenfolge der Bereiche:

1. Führen Sie einen der folgenden Schritte aus:
   a. Klicken Sie die einzelnen Bewertungsmodule an und verschieben Sie diese nach oben oder unten.
   b. Wählen Sie die einzelnen Bewertungsmodule aus und verwenden Sie die Schaltflächen „Nach oben“ und „Nach unten“, um sie zu verschieben.
2. Wenn die Bereiche die gewünschte Reihenfolge haben, klicken Sie auf die Schaltfläche **Aktualisieren**.
   Das Ergebnisrad wird mit der neuen Reihenfolge aktualisiert.

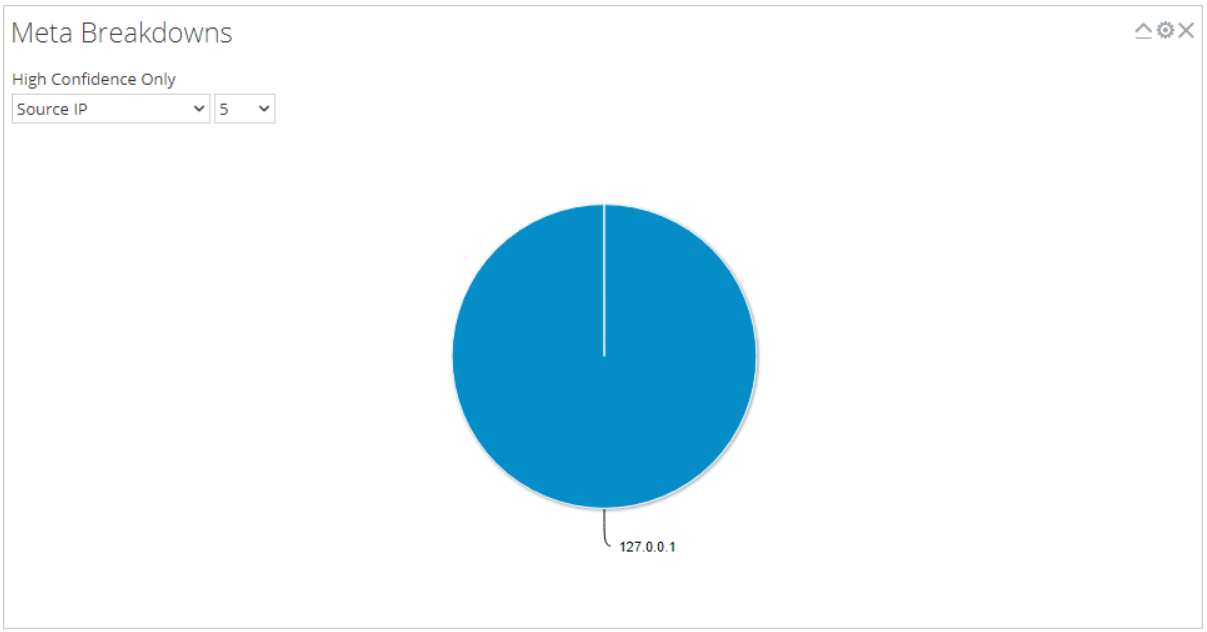
Konfiguration des Dashlet „Meta-Treemap“

Im Diagramm Meta-Treemap können Sie Meta-Strukturen nach Metadatentyp, Zähler und Analysetyp filtern und anzeigen. Verwenden Sie die drei Auswahllisten, um den Filter einzustellen. Das Diagramm „Meta-Treemap“ wird sofort aktualisiert.



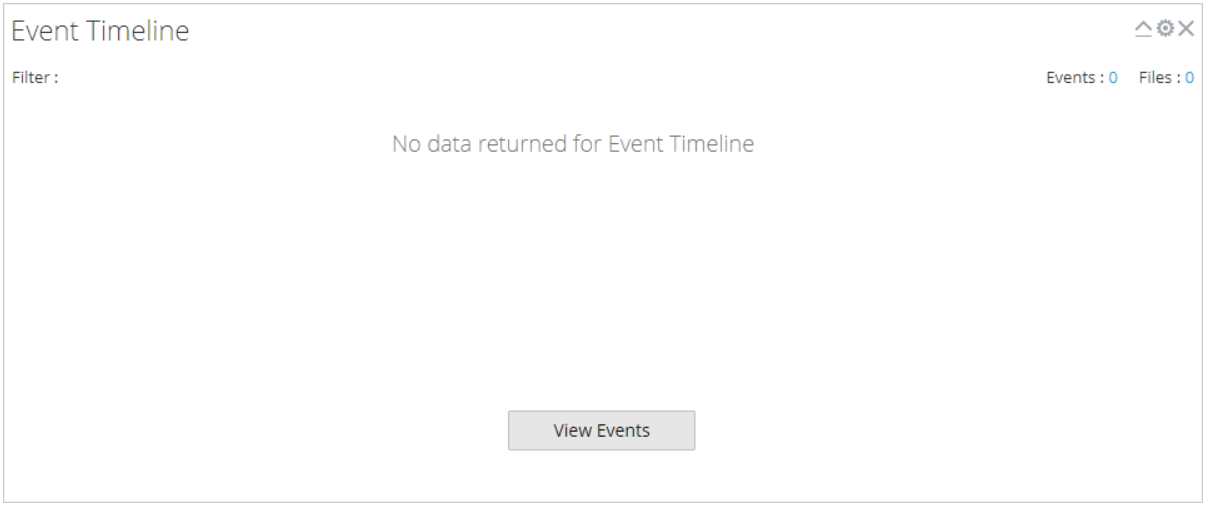
Konfiguration des Dashlet „Meta-Strukturen“

Das Dashlet Meta-Strukturen ist eine Darstellung der Werte für einen bestimmten Metaschlüssel in Form eines Kreisdiagramms. Im Diagramm „Meta-Strukturen“ können Sie Meta-Strukturen nach Metadatentyp und Zähler filtern. Verwenden Sie die zwei Auswahllisten, um den Filter einzustellen. Das Diagramm „Meta-Strukturen“ wird sofort aktualisiert.



Konfiguration des Dashlet „Ereigniszeitachse“

Das Dashlet Ereigniszeitachse ist eine Darstellung von Ereignissen innerhalb eines bestimmten Zeitraums. Für die Ereigniszeitachse sind keine zusätzlichen Filter verfügbar.

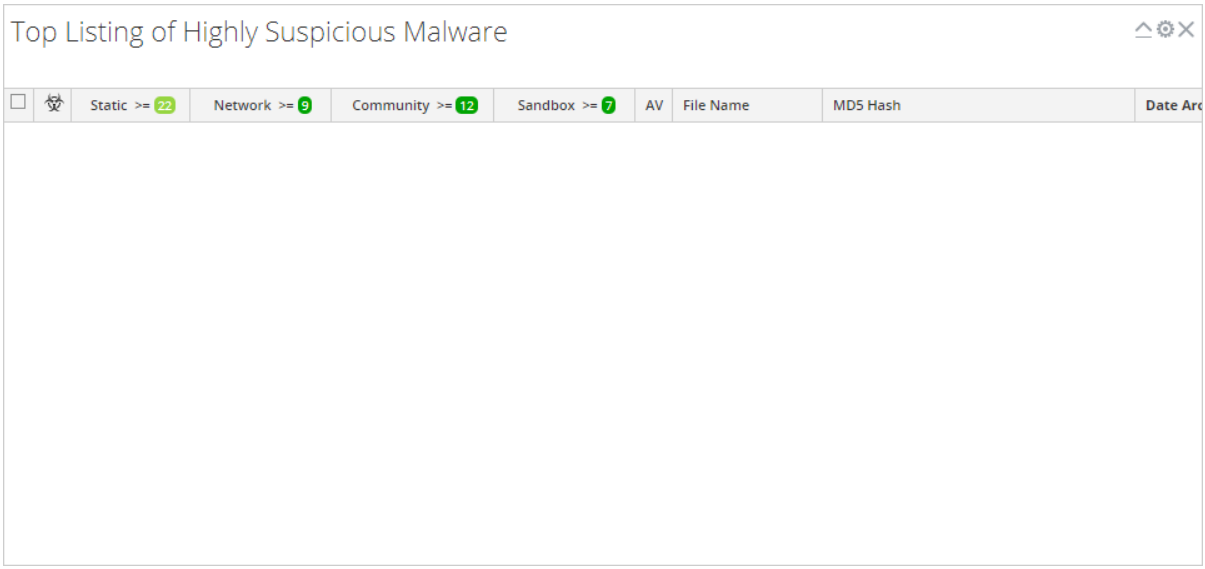


Öffnen aller Ereignisse in der Ereignisliste

Von der Ereigniszeitachse aus können Sie in der Ereignisliste die gesamte Liste der Ereignisse öffnen. Klicken Sie dazu auf **Ereignisse anzeigen**. Bei dieser Option handelt es sich nicht um dieselbe wie beim Anklicken des Zählers neben den Ereignissen, welcher für alle Visualisierungsdiagramme derselbe ist und den aktuellen Drill-down-Punkt in der Ereignisliste öffnet.

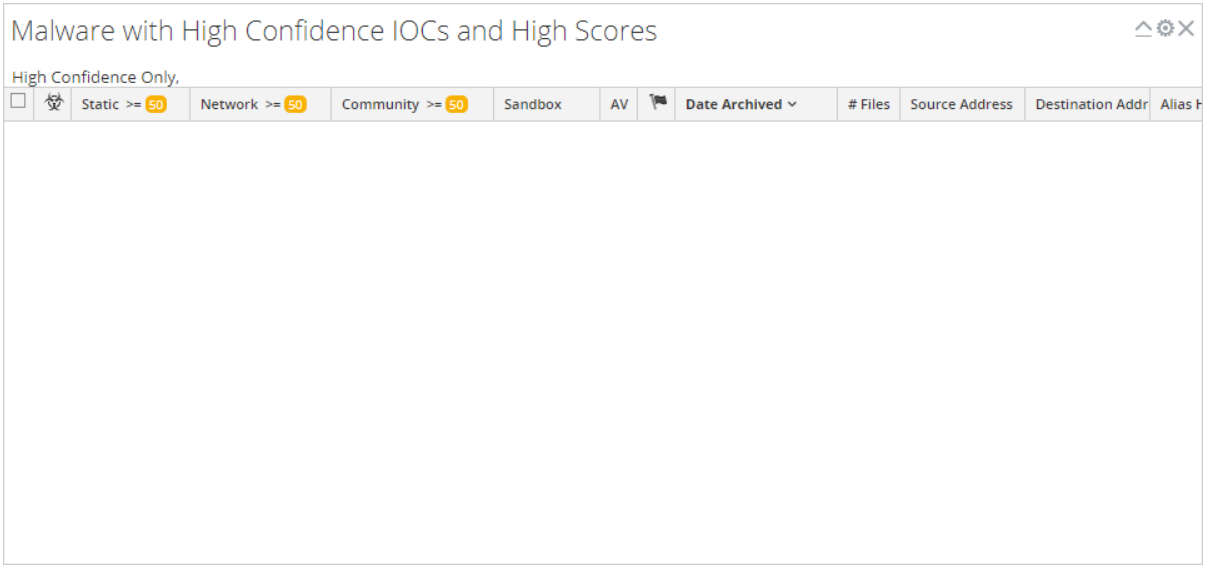
Konfiguration des Dashlet „Top-Liste höchst verdächtiger Schadsoftware“

Das Dashlet „Top-Liste höchst verdächtiger Schadsoftware“ zeigt die Top 10 der höchst verdächtigen Ereignisse aus der Ereignisliste oder der Dateiliste an. Dieses Dashlet ist auch im Dashboard „Überwachung“ verfügbar und die Konfigurationsoptionen werden als Teil des RSA NetWitness-Inhalts unter Dashlets beschrieben.



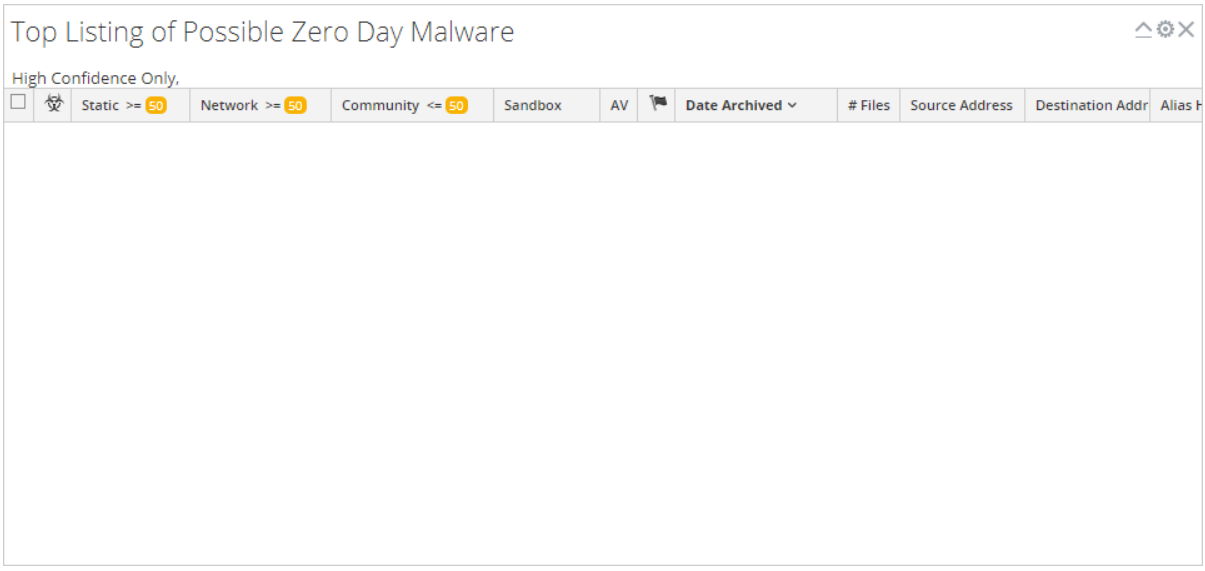
Konfiguration des Dashlet „Schadsoftware mit IOCs mit hoher Wahrscheinlichkeit und hohen Werten“

Das Dashlet „Schadsoftware mit IOCs mit hoher Wahrscheinlichkeit und hohen Werten“ stellt Indikatoren für eine Infizierung (IOCs) dar, die sowohl eine hohe Bewertung als auch eine hohe Wahrscheinlichkeit aufweisen, dass die Ereignisse wahrscheinlich Schadsoftware enthalten. Dieses Dashlet ist auch im Dashboard „Unified“ verfügbar und die Konfigurationsoptionen werden als Teil des RSA NetWitness-Inhalts unter Dashlets beschrieben.



Konfiguration des Dashlet „Top-Liste möglicher Zero-Day-Schadsoftware“

Das Dashlet „Top-Liste möglicher Zero-Day-Schadsoftware“ stellt potenzielle Zero-Day-Ereignisse in der Ereignisliste oder Dateiliste dar. Dieses Dashlet ist auch im Dashboard „Unified“ verfügbar und die Konfigurationsoptionen werden als Teil des RSA NetWitness-Inhalts unter Dashlets beschrieben.



Hochladen von Dateien für Malware Analysis-Scans

Es gibt zwei Methoden, mit denen Analysten Dateien für Malware Analysis-Scans hochladen können.

Ein Schadsoftwareanalyst mit der Berechtigung Malware Analysis-Scan initiieren kann zu scannende Dateien mithilfe der Option „Dateien scannen“ des Dialogfelds „Malware Analysis Service auswählen“ hochladen.

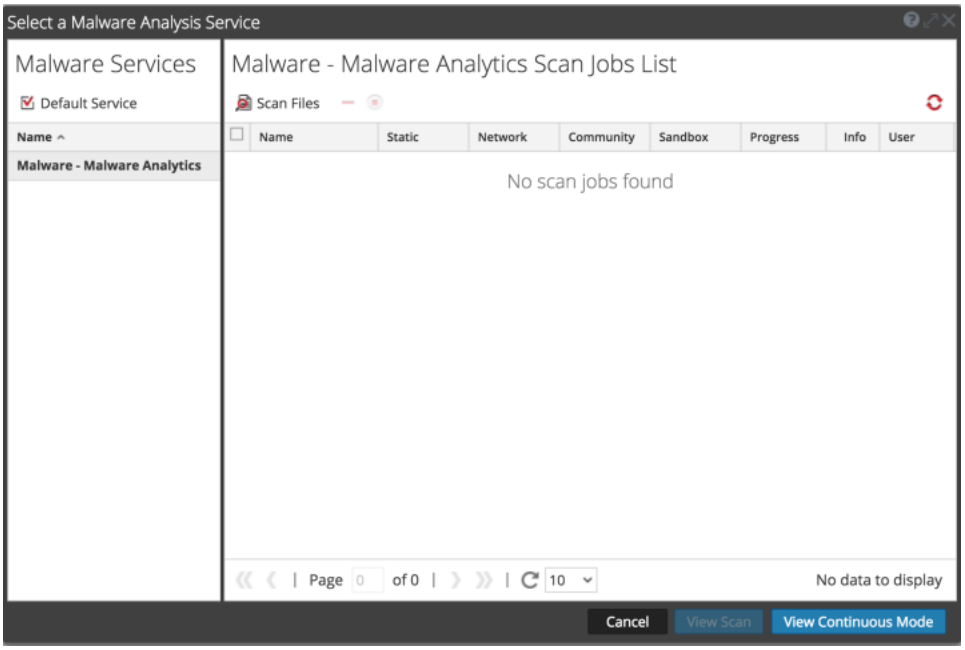
Es ist außerdem möglich, eine Datei zum Scannen mithilfe einer beobachteten Dateifreigabe hochzuladen.

Manuelles Hochladen von Dateien

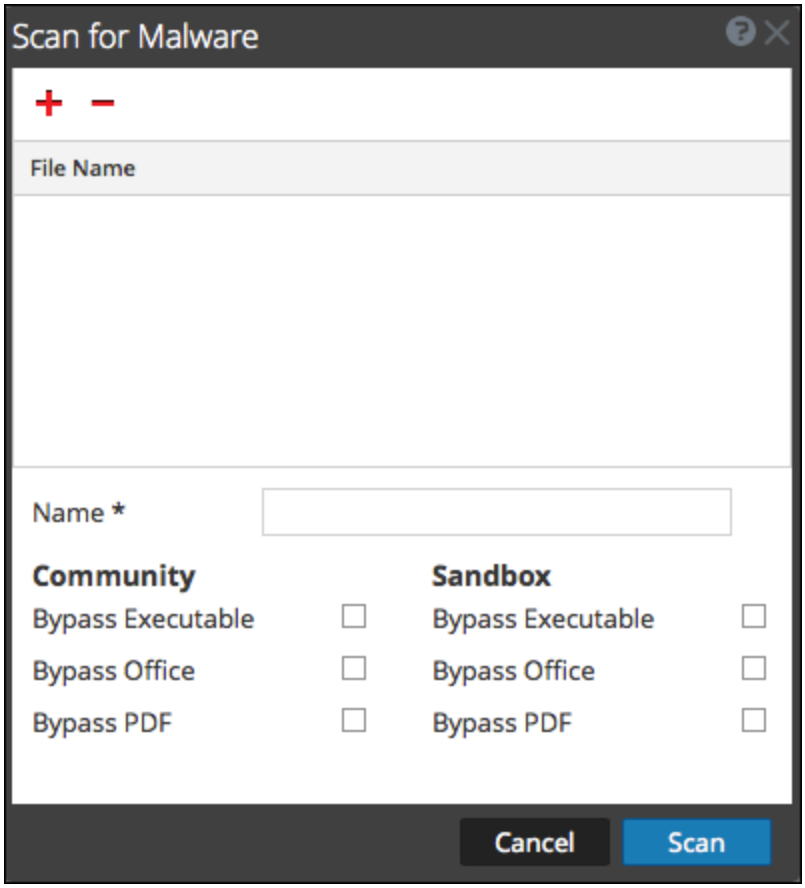
Dieses Thema beinhaltet Anweisungen zum Einleiten eines Scans von einer hochgeladenen Datei nach Bedarf. Wenn Sie eine Datei zum Scannen hochladen, startet NetWitness Platform den Uploadjob und fügt diesen der Jobwarteschlange hinzu. Wenn der Job beendet wurde, können Sie den Scan in Malware Analysis aufrufen.

So laden Sie eine Datei zum Scannen hoch:

1. Navigieren Sie zu **Ermittlung > Malware Analysis**.
   Das Dialogfeld „Malware Analysis Service auswählen“ wird zusammen mit den verfügbaren Malware Analysis-Hosts und -Services für den aktuellen Benutzer im linken Bereich angezeigt.



2. Klicken Sie auf **Scan anzeigen**.
   Das Dialogfeld „Auf Schadsoftware scannen“ wird angezeigt.



3. Klicken Sie auf + .
   Eine Ansicht des Dateisystems wird angezeigt, sodass Sie die Dateien zum Hochladen auswählen können.
4. Wählen Sie eine oder mehrere Dateien in der Liste aus und klicken Sie auf **Öffnen**.
   Die Dateinamen werden hinzugefügt. Malware Analysis versieht die Zeichen des Dateinamens vor der Verarbeitung einer Datei mit Escape-Zeichen. Die maximale Anzahl der Zeichen im Dateinamen nach dem Einfügen von Escape-Zeichen ist 200. Wenn der Dateiname mehr als 200 Zeichen hat, kürzt Malware Analysis den Dateinamen ab und zeigt den verkürzten Dateinamen auf der NetWitness Platform-Benutzeroberfläche an.
5. Fahren Sie mit dem Hinzufügen und Löschen von Dateien solange fort, bis Sie eine Liste der Dateien haben, die Sie hochladen möchten.
6. Benennen Sie den Scan und wählen Sie die zu überbrückenden Dateitypen aus. Dies ist für ein Zip-Archiv nützlich, welches verschiedene Dateitypen enthält, und überschreibt die standardmäßigen Umgehungseinstellungen.
7. Klicken Sie auf **Scannen**.
   Der Scanjob wird übermittelt und NetWitness Platform zeigt eine Bestätigungsmeldung über die erfolgreiche Übermittlung an. Die Scananforderung wird zum Dashlet mit der Liste der Scanjobs

hinzugefügt. Die Überbrückungseinstellungen in diesem Dialogfeld überschreiben die Standardeinstellungen in den Malware Analysis-Basiskonfigurationseinstellungen.

8. Der Job wird der Liste „Scanjobs“ im Dialogfeld „Malware Analysis Service auswählen“ und im Dashlet „Liste der Scanjobs“ des „Unified“-Dashboards hinzugefügt.
9. Zeigen Sie den Scan nach Abschluss an, indem Sie darauf doppelklicken.
   Die Schadsoftware-Ereigniszusammenfassung für den ausgewählten Scan wird angezeigt.

Hochladen von Dateien aus einem beobachteten Ordner

Um Dateien aus einem beobachteten Ordner hochzuladen, können Sie Dateien in einer beobachteten Dateifreigabe für Malware Analysis ablegen. Mit Malware Analysis können Analysten YARA-Regeln, Hash-Dateien und infizierte ZIP-Archive freigeben.

Malware Analysis überwacht eine Dateifreigabe und verarbeitet automatisch Dateien, die in bestimmten Ordnern in der Dateifreigabe gespeichert sind. Diese Funktion ist für folgende Aktionen hilfreich:

- Massenimport von Hash-Dateien aus `/var/lib/rsamalware/spectrum/hashWatch`
- Hinzufügen von benutzerdefinierten YARA-Regeln zur Liste mit den Indikatoren für eine Infizierung auf dem Host aus `/var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`
- Erstellen von bedarfsorientierten Scanjobs von einem Zip-Archiv infizierter Zip-Dateien aus `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`

Analysten müssen die Dateien gemäß den Anforderungen für die Nutzung vorbereiten. Die Dateierweiterung muss richtig sein und die Datei muss in den richtigen beobachteten Ordner in der Dateifreigabe kopiert werden.

Importieren von Hash-Listen

Um eine Hash-Liste aus dem beobachteten Verzeichnis zu importieren, muss die Hash-Liste in dem angegebenen Format sein und auf md5 sortiert werden. Sie können eine formatierte Datei in einen Ordner (`/var/lib/rsamalware/spectrum/hashWatch`) auf dem Malware Analysis-Host einfügen. Sie wird dann automatisch in die lokale Hash-Datenbank importiert. Dies wird in „Konfigurieren eines Hash-Filters“ im *Malware Analysis-Konfigurationsleitfaden* genauer beschrieben.

So importieren Sie mithilfe der Methode des beobachteten Ordners eine Hash-Liste:

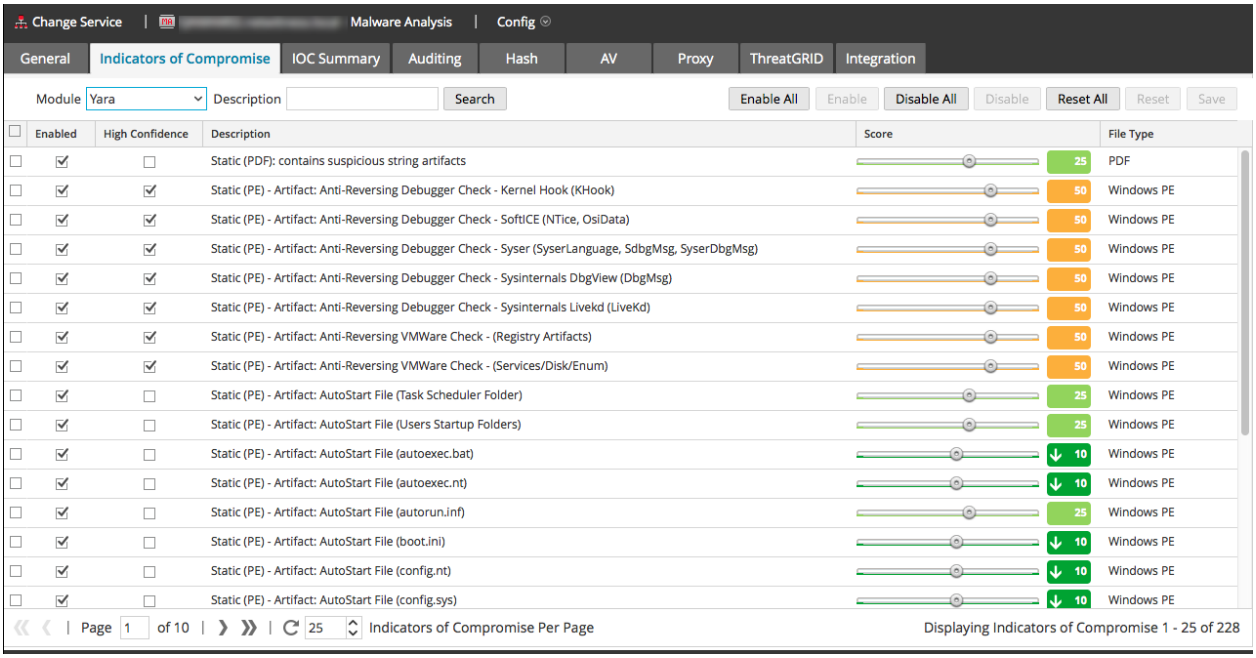
1. Kopieren Sie die Hash-Listen, die Sie importieren möchten, in das **`/var/lib/rsamalware/spectrum/hashWatch`**-Verzeichnis.
   NetWitness Platform Malware Analysis beobachtet diesen Ordner automatisch und verarbeitet die hier gespeicherten Dateien.
   a. Malware Analysis fügt diesem Hash-Filter jeden in der Hash-Liste gefundenen Hash hinzu.
   b. Falls Verarbeitungsfehler auftreten, werden die Hashes im folgenden Ordner protokolliert: `/var/lib/rsamalware/spectrum/hashWatch/error`.
   c. Verarbeitete Dateien werden in diesem Ordner katalogisiert: `/var/lib/rsamalware/spectrum/hashWatch/processed`.
   d. Verarbeitete Dateien werden aus dem Verzeichnis hashWatch nicht entfernt.

2. Nachdem die Masse der Hashes importiert wurde, kann der Systemadministrator mithilfe eines Cron-Jobs alte verarbeitete Dateien bereinigen.

Importieren von YARA-Regeln in die Liste mit den Indikatoren für eine Infizierung

Kunden mit fortgeschrittenen Fähigkeiten und Kenntnissen können die Erkennungsfunktionen von RSA Malware Analysis erweitern, indem sie YARA-Regeln erstellen und in RSA Live veröffentlichen oder diese zur Verarbeitung durch den Host in einen beobachteten Ordner platzieren. Unter Implementieren von angepassten YARA-Inhalten finden Sie umfassende Informationen zu den Voraussetzungen für die Verwendung von benutzerdefiniertem YARA-Inhalt und den Erstellungsregeln.

Wenn die Regeln fertiggestellt sind, platzieren Sie die benutzerdefinierten YARA-Dateien in den Ordner, der vom Malware Analysis-Service beobachtet wird:
`./var/lib/netwitness/malware-analytics-server/spectrum/yara/watch`
Die Datei wird innerhalb einer Minute verarbeitet.
Sobald die Datei verarbeitet wurde, wird sie von NetWitness Platform in den Ordner `processed` verschoben und die neue Regel wird in der Malware Analysis-Ansicht „Service-Konfiguration“ > auf der Registerkarte „Indikatoren für eine Infizierung“ hinzugefügt.



Importieren von Dateien in die Liste der Scanjobs

Wenn Sie Beispiele aus anderen Sicherheitslösungen erhalten und die Dateien weiter analysieren möchten, können Sie die Dateien komprimieren, das Archiv mit dem Passwort `infected` schützen und das Archiv dann zur Verarbeitung durch Malware Analysis zum beobachteten Ordner hinzufügen. Das komprimierte Archiv kann dann in den beobachteten Ordner verschoben werden:
`/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.

Hinweis: Die maximale Größe des Archivs beträgt 100 MB.

Für die Analyse infizierter, passwortgeschützter ZIP-Dateien verarbeitet Malware Analysis die Archive im beobachteten Ordner und erstellt einen Job nach Bedarf, der der Liste der Scanjobs hinzugefügt wird.

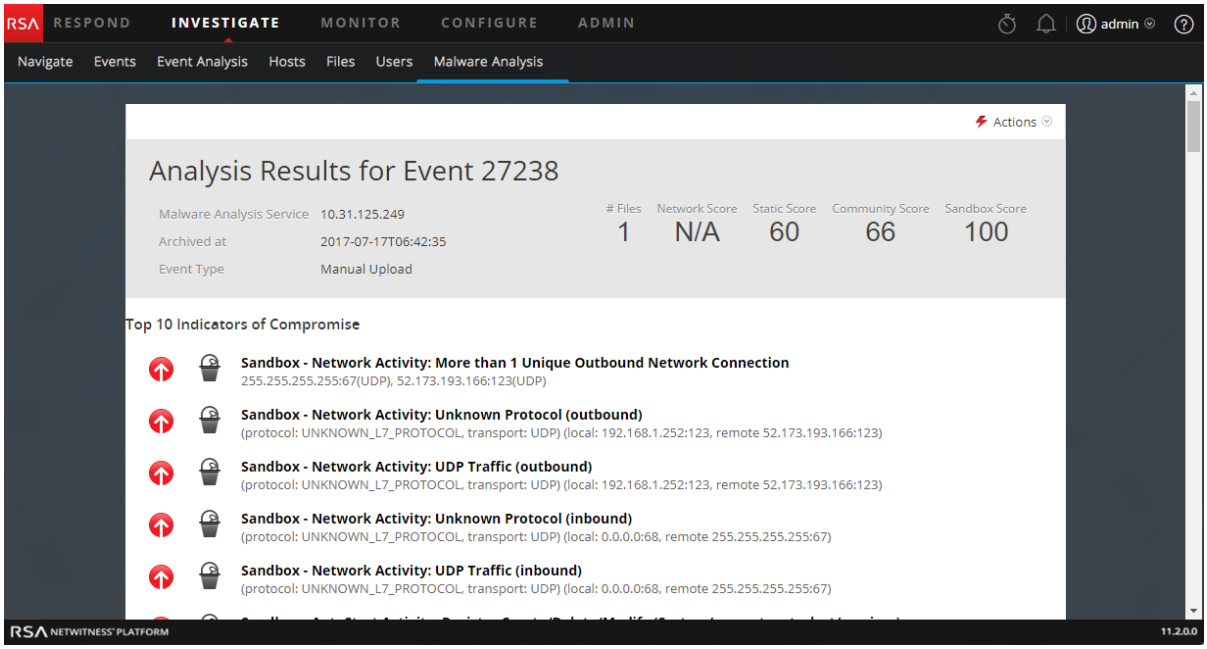
1. Komprimieren Sie, wenn Sie als Administrator angemeldet sind, die zu verarbeitenden Dateien in einer ZIP-Datei mit dem Passwort `infected` und speichern Sie sie unter `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`.
   Innerhalb von ein oder zwei Minuten verarbeitet Malware Analysis das Archiv und erstellt bedarfsgesteuert einen Job in der Liste der Scanjobs. Der Name des Scanjobs entspricht dem Namen der Datei, der Benutzer ist **Dateifreigabe** und der Ereignistyp lautet 1. Das Archiv wird in `/var/lib/rsamalware/spectrum/infectedZipWatch/processed` verschoben.
2. Sobald der Job der Scanjobliste hinzugefügt wurde, führen Sie ein Skript oder einen Cron-Job aus, um die ZIP-Datei im Verzeichnis `/var/lib/rsamalware/spectrum/infectedZipWatch/processed` zu bereinigen.

Anzeigen der detaillierten Schadsoftwareanalyse eines Ereignisses

Wenn Sie die Liste individueller Ereignisse in einem Malware Analysis-Scan im Malware Analysis-Ereignisraster anzeigen, können Sie durch einen Doppelklick auf ein Ereignis die detaillierten Analyseergebnisse für dieses Ereignis anzeigen.

Anzeigen der Malware Analysis-Details für ein Ereignis

1. Starten Sie eine Ermittlung in der Registerkarte **Malware Analysis**.
   Die Schadsoftware-Ereigniszusammenfassung wird angezeigt und weist vier Diagramme einschließlich der Ereigniszeitachse auf.
2. Führen Sie einen der folgenden Schritte aus:
   a. Klicken Sie zum Anzeigen aller Ereignisse in der Ereigniszeitachse auf die Schaltfläche **Ereignisse anzeigen**.
   b. Doppelklicken Sie auf Daten in der **Metaaufschlüsselung**, im **Meta-Treemap-Diagramm** oder im **Ergebnisrad.**.
   Die Ereignisliste wird angezeigt.
3. Doppelklicken Sie auf ein Ereignis.
   Die Analyseergebnisse für das Ereignis werden angezeigt.

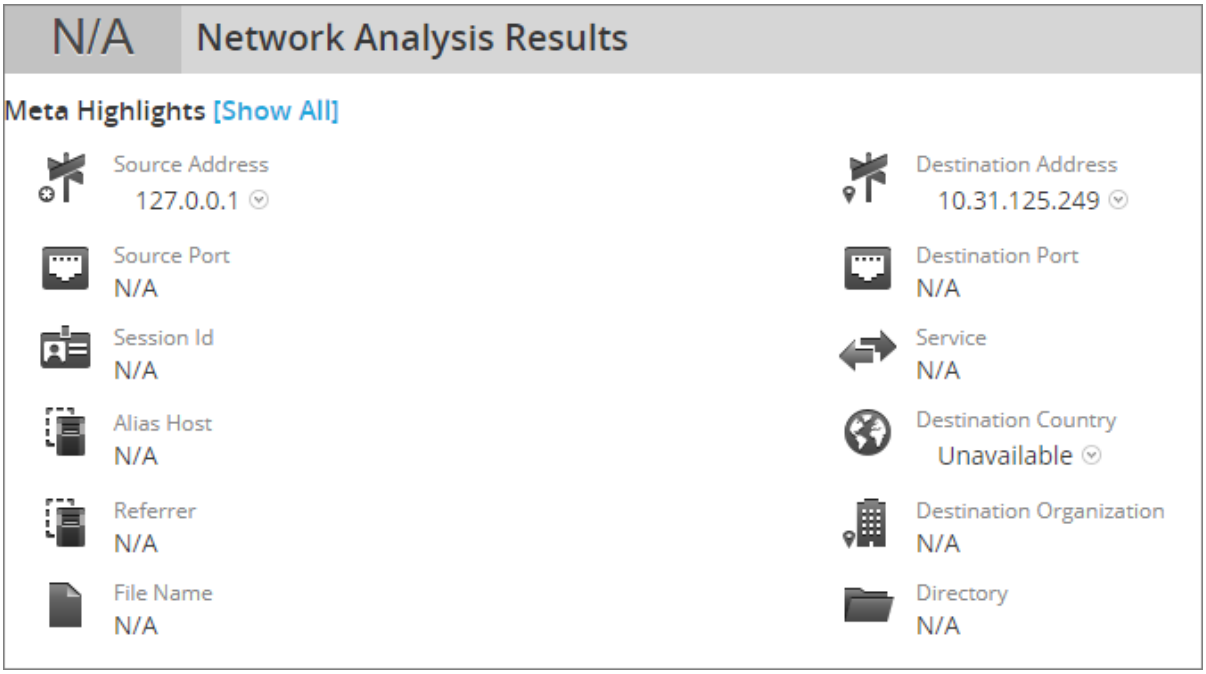


4. (Optional) Wenn Sie ein Ereignis löschen möchten, wählen Sie **Aktionen > Ereignis löschen**.
5. Wenn Sie eine Rekonstruktion der Netzwerksitzung anzeigen möchten, wählen Sie **Aktionen > Netzwerksitzung anzeigen**.
   Die Sitzung wird in der Ansicht „Navigation“ > „Ereignisrekonstruktion“ angezeigt.

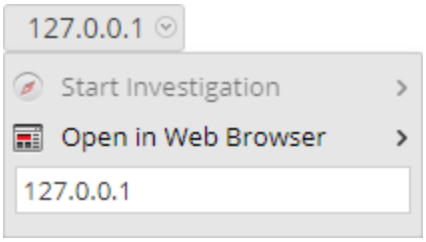
Pivotieren der Netzwerkanalyse-Ergebnisse

Sie können die Netzwerkanalyse-Ergebnisse auf mehreren Wegen pivotieren.

1. Blättern Sie nach unten zu den Netzwerkanalyse-Ergebnissen.



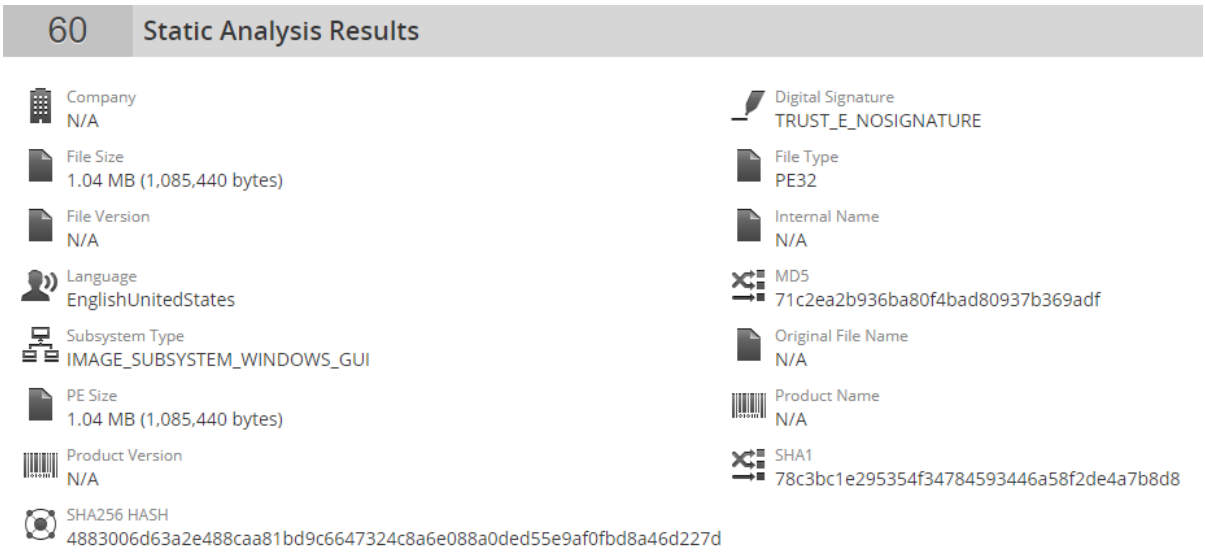
2. Bewegen Sie den Mauszeiger über einen Metawert und klicken Sie mit der linken Maustaste. Das Kontextmenü wird angezeigt.



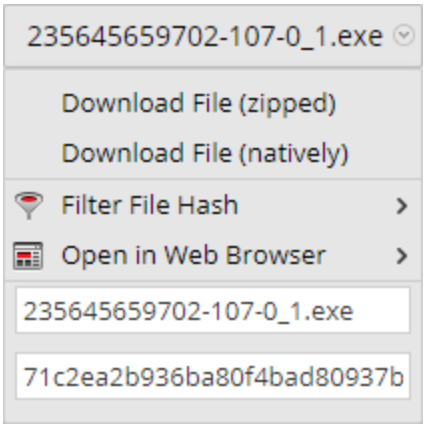
3. Um den ausgewählten Metawert in der Ansicht **Navigieren** anzuzeigen, wählen Sie **Ermittlungen starten** und eine Zeitoption aus.
4. Um den ausgewählten Metawert in einem Browser anzuzeigen, wählen Sie **In Webbrowser öffnen > In Google öffnen**.

Verwenden der Option „Dateiaktionen“ in der Ansicht „Statische Analyseergebnisse“

1. Blättern Sie nach unten zu den statischen Analyseergebnissen.



2. Wenn Sie eine Datei herunterladen möchten, wählen Sie den Dateinamen und die Option **Datei herunterladen (gezippt)** oder **Datei herunterladen (systemintern)** aus. Es ist sicherer, eine Datei im zip-Format herunterzuladen.



3. Wenn Sie die Datei in der Hash-Liste als sicher oder unsicher markieren möchten, wählen Sie **Datei-Hash filtern** und die Option **Hash als gut markieren oder Hash als schlecht markieren**.

Anzeigen der Details der Communityanalyseergebnisse

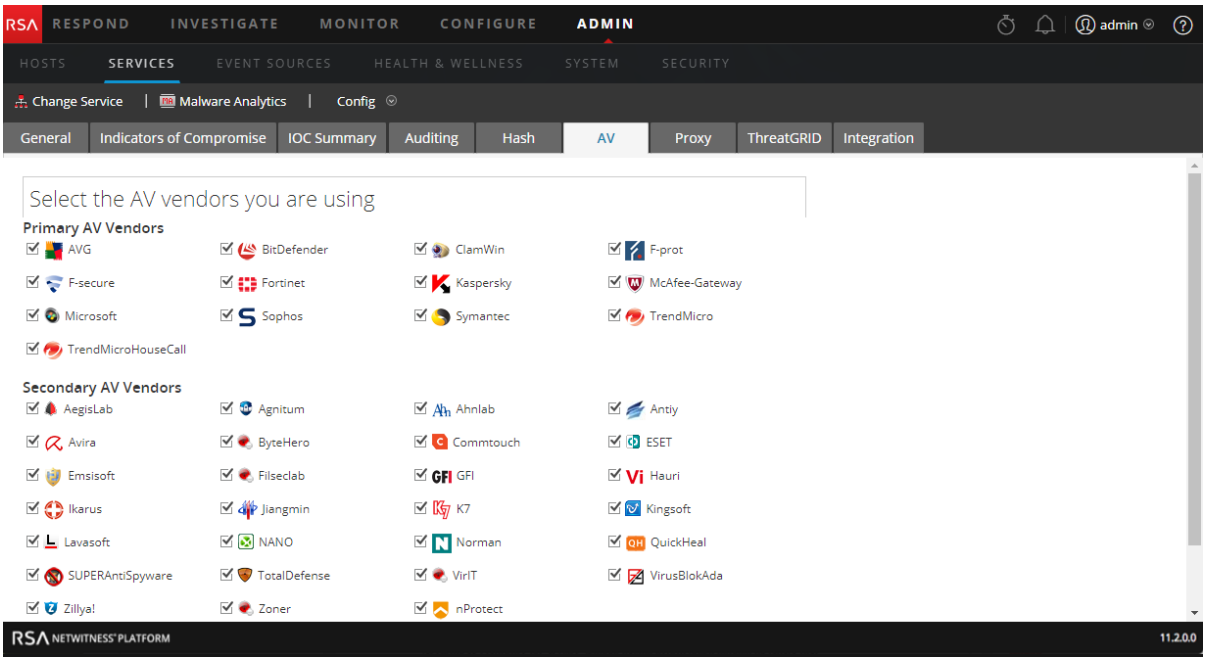
Die Communityanalyseergebnisse fassen Ergebnisse zusammen, die Indikatoren für eine Infizierung identifizieren, die als Risiko oder als harmlos markiert wurden.

Zudem listet die Ansicht die Ergebnisse von eingesetzten AV-Anbietern und nicht eingesetzten AV-Anbietern auf. Sie können die Ergebnisse der eingesetzten AV-Anbieter, die für den aktuellen Malware Analysis-Service konfiguriert sind, mit den Communityergebnissen vergleichen. Sie können zudem Ergebnisse einer Liste von AV-Anbietern anzeigen, die nicht für den aktuellen Malware Analysis-Service eingesetzt und konfiguriert sind.

Jede Zeile AV-Anbieterergebnisse beinhaltet das Schildsymbol, das anzeigt, ob der IOC von einem primären ( ) oder sekundären ( ) AV-Anbieter in der Community entdeckt wurde, den Namen des eingesetzten oder nicht eingesetzten Anbieters und den Namen der Schadsoftware oder des Risikos, die von der Community und dem AV-Anbieter identifiziert wurden. Hat der AV-Anbieter kein Risiko entdeckt, wird die Meldung **-- Nicht entdeckt --** anstelle des Namens des Risikos angezeigt.

Der Abschnitt „Nicht eingesetzte AV-Anbieter“ kann so vergrößert werden, dass alle Einträge angezeigt werden können, ist jedoch standardmäßig auf eine Größe begrenzt, die das Scrollen minimiert. Wenn Sie auf + klicken, wird die Liste vergrößert.

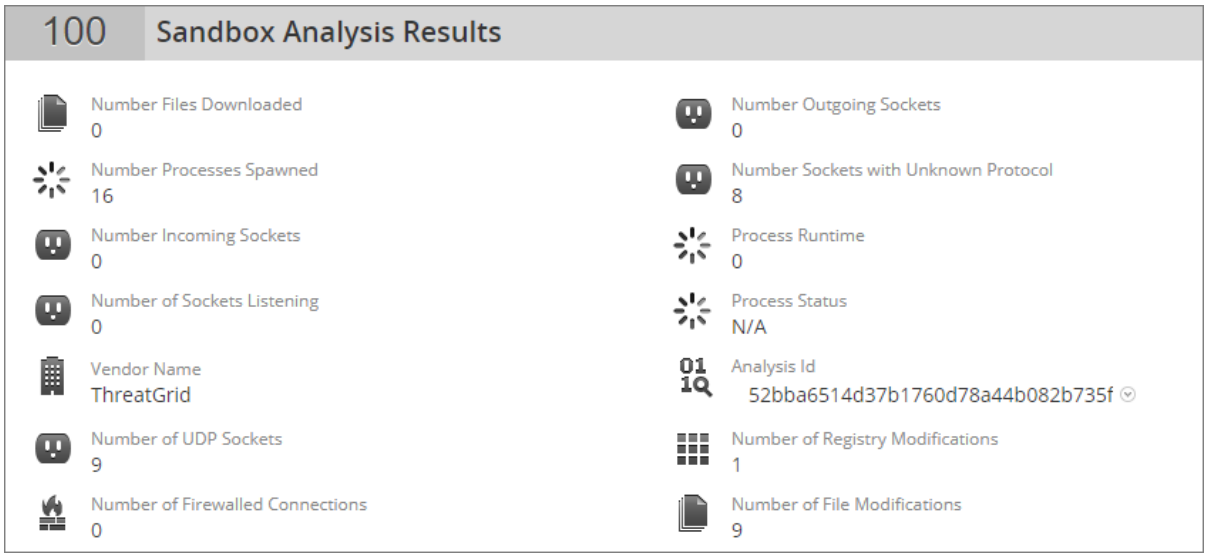
Wenn keine eingesetzten AV-Anbieter für den aktuellen Malware Analysis-Service konfiguriert wurden, wird folgende Meldung angezeigt: Es wurden keine AV-Anbieter als „Eingesetzt“ markiert. Rufen Sie die Seite „Malware Analysis-Servicekonfiguration“ auf, um die eingesetzten AV-Anbieter zu identifizieren.



Anzeige der Sandbox-Analyseergebnisse in der ThreatGrid-Benutzeroberfläche

Wenn Sie sich bei ThreatGrid registriert haben, können Sie die Sandbox-Ergebnisse direkt in ThreatGrid anzeigen.

1. Blättern Sie nach unten zu den Sandbox-Analyseergebnissen.



2. Klicken Sie auf die **Analyse-ID** und wählen Sie **In ThreatGrid öffnen**.
   Der Analysereport wird in ThreatGrid angezeigt.

Troubleshooting von NetWitness Investigate

Dieser Abschnitt enthält Informationen zu möglichen Problemen bei der Verwendung von NetWitness Investigate.

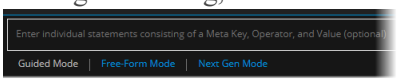
Probleme in den Ansichten „Navigation“ und „Ereignisse“

Message	`Not indexed; will experience longer than usual load times.` im Dialogfeld „Metagruppen managen“.
Problem	Die Metaschlüssel im Dialogfeld „Metagruppen managen“ werden durch ein rotes Ausrufezeichen markiert und die Fehlermeldung wird angezeigt. Dies kann bei der Untersuchung eines Brokers oder Decoders und beim Hinzufügen einer Metagruppe mit Metaschlüsseln geschehen, die nicht in der Indexdatei oder der benutzerdefinierten Indexdatei für den Service indiziert sind. Für einen Broker könnte dies bedeuten, dass er nicht damit begonnen hat, Daten von einem Concentrator zu aggregieren. In diesem Fall verfügt der Broker nicht über den Inhalt der benutzerdefinierten Indexdatei aus den Aggregatservices und die Schlüssel werden nicht indiziert. Für einen Decoder bedeutet dies, dass die Metaschlüssel nicht im Decoder-Index oder in der benutzerdefinierten Indexdatei indiziert sind.
Erläuterung	Zur Behebung des Problems auf einem Broker melden Sie sich an und starten Sie den Broker-Service neu, sodass er die Metaschlüsselinformationen von angeschlossenen Concentrators zusammenfassen kann. Zur Behebung des Problems auf einem Decoder bearbeiten Sie die angepasste Indexdatei, damit die Metaschlüssel indiziert werden. Melden Sie sich ab und wieder an und starten Sie den Decoder-Service erneut.

Verhalten	Wenn Protokolle und Metadaten über die Ansicht „Ereignisrekonstruktion“ heruntergeladen werden, weisen sie immer das Textformat auf, unabhängig von dem in der Ansicht „Ereignisse“ ausgewählten Format.
Problem	Wenn Sie Metadaten oder ein Protokoll in der Ansicht „Ereignisrekonstruktion“ herunterladen, wird das Format, die Sie in der Ansicht „Ereignisse“ ausgewählt haben, nicht verwendet. Die exportierten Daten weisen immer das Textformat auf.
Erläuterung	Laden Sie Metadaten und Protokolle über die Ansicht „Ereignisse“ herunter, wenn Sie ein anderes Format als das Textformat verwenden möchten.

Probleme bei der Ereignisanalyse

Verhalten	Die Abfrageerstellung in Version 11.2 enthält den NextGen-Modus, eine undokumentierte Beta-Funktion.

Problem	Die Version 11.2 enthielt eine undokumentierte Beta-Funktion, den sogenannten NextGen-Modus, in der Abfrageerstellung der Ansicht „Ereignisanalyse“, der noch entwickelt und getestet wurde. Der NextGen-Modus wurde im Patch 11.2.0.1 deaktiviert.
Erläuterung	Wenn der NextGen-Modus angezeigt wird, sollten Sie ihn nicht verwenden. Verwenden Sie stattdessen nur den geleiteten Modus und den Freitextmodus in der Abfrageerstellung, damit Sie konsistente und vorhersehbare Ergebnisse erzielen. 

Meldung	`Investigation Profiles/OOTB column groups are not present in Event Analysis`
Problem	Nach dem Upgrade auf RSA NetWitness v11.1 werden die Standardspaltengruppen „Endpunktanalyse“, „Ausgehende SSL“ und „Ausgehende Http“ unter Spaltengruppen nicht hinzugefügt. Darüber hinaus fehlen nach dem Upgrade einige der Ermittlungsprofile.
Erläuterung	Es wurde beobachtet, dass dieses Problem nur dann auftritt, wenn Sie eine benutzerdefinierte Spaltengruppe mit einem Namen erstellt haben, der mit einem der neuen 11.1 OOTB-benutzerdefinierten Spaltengruppennamen identisch ist. So sollten z. B. in 11.0 eine benutzerdefinierte Spaltengruppe mit dem Namen **RSA Endpoint-Analyse** nur nach dem Upgrade auf 11.1 erstellen. Aufgrund des gleichen Namens wie in 11.1 sind Standard-Spaltengruppen und Standardprofile in der UI nicht verfügbar. Zur Fehlerbehebung ändern Sie den Namen der benutzerdefinierten Spaltengruppe und starten Sie den jetty-Server mithilfe des folgenden Befehls auf dem NetWitness-Server neu: `systemctl restart jetty`

Meldung	`Applicable for hosts with 4.x Endpoint agents installed, please install the NetWitness Endpoint Thick Client.`
Problem	Wenn Sie auf **Zu Endpoint wechseln** in der Ansicht „Ereignisanalyse“ klicken, werden keine Daten angezeigt und die Meldung wird angezeigt.
Erläuterung	Version 4.4 des NetWitness Endpoint-Thick-Client muss auf demselben Server installiert sein, die NWE-Metaschlüssel müssen in der `table-map.xml`-Datei auf dem Log Decoder vorhanden sein und die NWE-Metaschlüssel müssen in der `index-concentrator-custom.xml`-Datei vorhanden sein. Der NWE-Thick-Client ist eine reine Windows-Anwendung. Umfassende Anweisungen zur Installation finden Sie im *NetWitness Endpoint-Benutzerhandbuch* für Version 4.4.

Meldung	`Event Analysis requires all core services to be NetWitness 11.1. Connecting prior versions of services to the 11.1 NetWitness Server results in limited functionality (see "Investigate in Mixed Mode" in the *Physical Host Upgrade Guide*).`

Problem	Beim Versuch, einen Service in der Ansicht „Ereignisanalyse“ zu untersuchen, der nicht auf Version 11.1 aktualisiert wurde, wird die Meldung zur Information angezeigt.
Erläuterung	Wenn ein Analyst die Ansicht „Ereignisanalyse“ im gemischten Modus öffnet (d. h. einige Services wurden auf 11.1 aktualisiert und einige sind immer noch auf 11.0.0.x oder 10.6.x), wird rollenbasierter Zugriff (Role-Based Access, RBAC) nicht einheitlich angewendet. Dies wirkt sich auf das Anzeigen und Herunterladen von Inhalten sowie die Validierung von Filtern in der interaktiven Brotkrümelnavigation aus. Sie sehen diese Meldung zur Information, wenn Sie Ereignisanalyse öffnen. Wenn Sie einen Service auswählen, werden Services, die nicht auf dem aktuellen Stand sind, in einem roten Feld mit der Meldung angezeigt, dass der Service nicht auf dem aktuellen Stand ist. Wenn Ihr Administrator alle verbundenen Services auf 11.1 aktualisiert hat, arbeiten diese Funktionen wie erwartet.

Meldung	`Forbidden. You cannot access the requested page.`
Problem	Beim Versuch, auf die Ansicht „Ereignisanalyse“ zuzugreifen, wird die Ansicht mit der Meldung geöffnet.
Erläuterung	Ihr Administrator hat den Zugriff auf die Ansicht „Ereignisanalyse“ mithilfe von Rolle und Berechtigungen verhindert.

Meldung	`Insufficient permissions for the requested data.`
Problem	Beim Versuch, auf ein Ereignis in der Ereignisanalyse zuzugreifen, wird die Rekonstruktion nicht angezeigt und die Meldung wird angezeigt.
Erläuterung	Sie haben eine Ereignis-ID für ein Ereignis eingegeben, für das Sie über keine Berechtigung zur Anzeige verfügen. Der Administrator hat möglicherweise Einschränkungen vorgenommen, um den Zugriff nach Rolle und Berechtigungen zu beschränken.

Meldung	`Invalid session ID: <<eventId>>`
Problem	Keine `sessionId` entspricht der `sessionId`, die Sie abgefragt haben.
Erläuterung	Es kann verschiedene Gründe für eine ungültige Sitzungs-ID geben. Vielleicht haben Sie die Sitzungs-ID manuell bearbeitet und es ist keine derartige Sitzung vorhanden. Ein anderer Fall kann vorliegen, wenn Sie einen Broker abfragen und die zusammengefassten Daten nicht aktualisiert wurden. Dann kann dieser Fehler für eine Sitzung angezeigt werden, die nicht länger vorhanden ist.

Meldung	`No text data was generated during content reconstruction. This could mean that the event data was corrupt/invalid, or that an administrator has disabled the transmission of raw endpoint events in the Endpoint server configuration. Check the other reconstruction views.`

Problem	Wenn Sie ein Ereignis als Text in der Ansicht „Ereignisanalyse“ rekonstruieren, werden keine Daten angezeigt und die Meldung wird angezeigt.
Erläuterung	Wenn Sie den Rohtext in anderen Ansichten der Ereignisanalyse oder in Rekonstruktionen der Ereignisansicht nicht sehen und glauben, dass die Daten nicht beschädigt oder ungültig sind, hat Ihr Administrator wahrscheinlich die Übertragung von rohen Endpunktereignissen auf dem NetWitness Endpoint Server deaktiviert. Wenden Sie sich für weitere Informationen an den Administrator.

Meldung	`Session is unavailable for viewing.`
Problem	Bei der Abfrage einer Ereignis-ID wird die Rekonstruktion nicht angezeigt und die Meldung wird angezeigt.
Erläuterung	Die von Ihnen eingegebene Abfrage versucht, eingeschränkte Daten zu betrachten. Wenn Sie z. B. nur Protokolldaten sehen dürfen, aber einen Link zu Netzwerkdaten verwenden, die Sie gestern sehen durften.

Meldung	`The session id is too large to be handled:<<eventId>`
Problem	Die SessionId-Ganzzahl, die Sie eingegeben, bearbeitet oder aus der Ansicht „Ereignisse“ oder „Navigation“ erhalten haben, ist zu groß.
Erläuterung	Wenn Sie manuell die SessionId eingegeben oder eine SessionId in der Ansicht „Ereignisanalyse“ bearbeitet haben, haben Sie möglicherweise eine Ganzzahl erstellt, die für eine Verarbeitung der Ereignisanalyse zu groß ist.

Verhalten	Beim Erstellen eines Filters in der Ansicht „Ereignisanalyse“ können Sie keinen komplexen Ausdruck mit den Operatoren `AND` oder `OR` in einer Abfrageerstellung eingeben.
Problem	Die Abfrageerstellung in der Ansicht „Ereignisanalyse“ unterstützt nur einfache Ausdrücke der Form `<meta key><operator><meta value>`.
Erläuterung	Wenn Sie einen Filter eingeben möchten, der den Operator `AND` oder `OR` verwendet, müssen Sie die Abfrage von der Ansicht „Navigation“ oder „Ereignisse“ aus eingeben und sie dann in der Ansicht „Ereignisanalyse“ öffnen. Sie können komplexe Ausdrücke als zwei separate Filter in der Ansicht „Ereignisanalyse“ eingeben. Die Filter werden mit AND verbunden, wenn Sie die Abfrage ausführen.

Probleme mit der Hostansicht

Meldung	`An error has occurred. The Endpoint Server may be offline or inaccessible.`
Problem	Beim Versuch, auf die Ansicht „Hosts“ oder „Dateien“ zuzugreifen, wird die Ansicht mit der Meldung geöffnet.

Erläuterung	Endpunktserver oder Nginx-Server wird nicht ausgeführt. Prüfen Sie den Status des Endpunktservers unter **Admin** > **Service** oder prüfen Sie, ob die Host-IP-Adresse des Endpunktservers mit dem Admin-Server registriert ist. Weitere Informationen finden Sie im *Handbuch zur Installation physischer Hosts* oder im *Handbuch zur Installation virtueller Hosts*. Wenn der Service nicht ausgeführt wird, starten Sie den Endpunktserver.

Problem	Die Ansichten „Hosts“ und „Dateien“ werden im Safari-Browser nicht geladen.
Erläuterung	Wenn Sie die Ember-Seiten im Safari-Browser mit einem nicht vertrauenswürdigen SSL-Zertifikat öffnen, werden die Ansichten „Hosts“ und „Dateien“ nicht geladen. So laden Sie die Ansichten: 1. Klicken Sie auf das Pop-up-Menü **Zertifikat anzeigen**. 2. Aktivieren Sie das Kontrollkästchen **NetWitness beim Verbinden mit <IP-Adresse> immer vertrauen**. 3. Klicken Sie auf **Weiter**. 4. Geben Sie Ihren Benutzernamen und das Passwort ein. 5. Klicken Sie auf **Einstellungen aktualisieren**.

Meldung	`No process information was found.`
Problem	Beim Versuch, auf die Registerkarte „Prozess“ oder „Bibliotheken“ in der Ansicht „Details zum Host“ zuzugreifen, sind die detaillierten Hostinformationen nicht verfügbar und die Ansicht wird mit der Meldung angezeigt.
Erläuterung	Scandaten sind aus einem der folgenden Gründe nicht verfügbar: • Der erstmalige Scan wurde nicht abgeschlossen. • Datenaufbewahrungs-Policy hat alle Scan-Snapshots gelöscht.

Probleme mit der Ansicht „Dateien“

Verhalten	Das Laden von Metawerten dauert lang.
Problem	Metawerte werden nicht nach Werten indiziert festgelegt.
Erläuterung	Während der Ermittlung beim Wechseln zur Ansicht „Navigation“ oder „Ereignisanalyse“ von der Ansicht „Dateien“ aus, wenn der Dateiname oder Hash (SHA256 und MD5) nicht nach Werten indiziert festgelegt ist, dauert es lange, die übereinstimmenden Ergebnisse zu laden, da der Concentrator den Index erzeugen muss, indem er auf die Metadatenbank zugreift und den Wert der Metadaten für jedes Ereignis abruft. Sie müssen die Werte vor dem Wechsel manuell indexieren.

Problem	Beim Filtern von Dateien dauert es länger, Ergebnisse auf die Benutzeroberfläche zu

Erläuterung	laden.
	In der Ansicht „Dateien“ dauert es beim Filtern von Dateien mit dem Operator `Contains` einige Sekunden, bis die Ergebnisse auf die Benutzeroberfläche geladen werden. Sie müssen mindestens ein indiziertes Feld mit dem Operator `Equals` verwenden, während die Dateien gefiltert werden.

Investigate-Referenzmaterialien

In diesem Abschnitt finden Sie Informationen zu Zweck und Anwendung der Ansichten von NetWitness Investigate. Für jede Ansicht gibt es eine kurze Einführung und eine Tabelle zu „Was möchten Sie tun?“ mit Links zu verwandten Verfahren. Außerdem enthalten einige der Referenzmaterialien Workflows und Übersichten zur Hervorhebung wichtiger Funktionen in der Benutzeroberfläche.

Dies sind die wichtigsten Ansichten:

- Ansicht „Untersuchen“
- Ansicht „Navigation“
- Ansicht „Ereignisse“
- Ansicht „Ereignisanalyse“
- Ansicht „Dateien“
- Ansicht „Hosts“
- Ansicht „Malware Analysis“

Dies ist eine alphabetische Liste der anderen Ansichten, Bereiche und Dialogfelder.

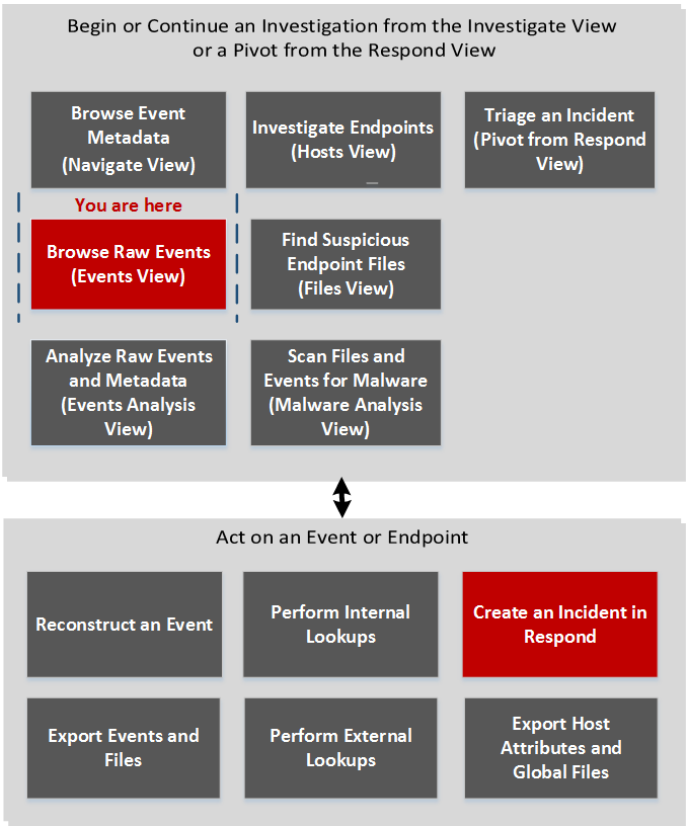
- Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“
- Bereich „Kontextabfrage“
- Dialogfeld „Incident erstellen“
- Ansicht „Ereignisanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Textanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Paketanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Dateianalyse“
- Ansicht „Ereignisrekonstruktion“
- Ansicht „Hosts“ – Registerkarte „Automatische Ausführungen“
- Ansicht „Hosts“ – Registerkarte „Treiber“
- Ansicht „Hosts“ – Registerkarte „Dateien“
- Ansicht „Hosts“ – Registerkarte „Bibliotheken“
- Ansicht „Hosts“ – Registerkarte „Übersicht“
- Ansicht „Hosts“ – Registerkarte „Prozess“
- Ansicht „Hosts“ – Registerkarte „Systeminformationen“
- Dialogfeld „Untersuchen“
- Registerkarte „Investigation“ – Bereich „Nutzereinstellungen“

- Malware Analysis-Ereignisliste und -Dateiliste
- Dialogfeld „Spaltengruppen managen“
- Dialogfeld „Standardmetaschlüssel managen“
- Dialogfeld „Metagruppen managen“
- Dialogfeld „Profile managen“
- Ansicht „Navigation“
- Dialogfeld „Abfrage“
- Dialogfeld „Auf Schadsoftware scannen“
- Dialogfeld „Malware Analysis Service auswählen“
- Dialogfelder „Einstellungen“ für Investigate-Ansichten

Dialogfeld „Ereignisse zu einem Incident hinzufügen“

Im Dialogfeld „Ereignisse zu einem Incident hinzufügen“ können Analysten Warnmeldungen zu einem vorhandenen Incident hinzufügen, damit Incident-Experten bei der Bearbeitung des Incident alle zugehörigen Ereignisse sehen können. Öffnen können Sie dieses Dialogfeld wie folgt: Klicken Sie bei der Untersuchung eines Service in der Ansicht „Ereignisse“ auf der Symbolleiste auf **Incidents > Zu vorhandenem Incident hinzufügen**.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter oder Incident Responder	Ein oder mehrere Ereignisse zu einem vorhandenen Incident oder einem neuen Incident hinzufügen*	Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion

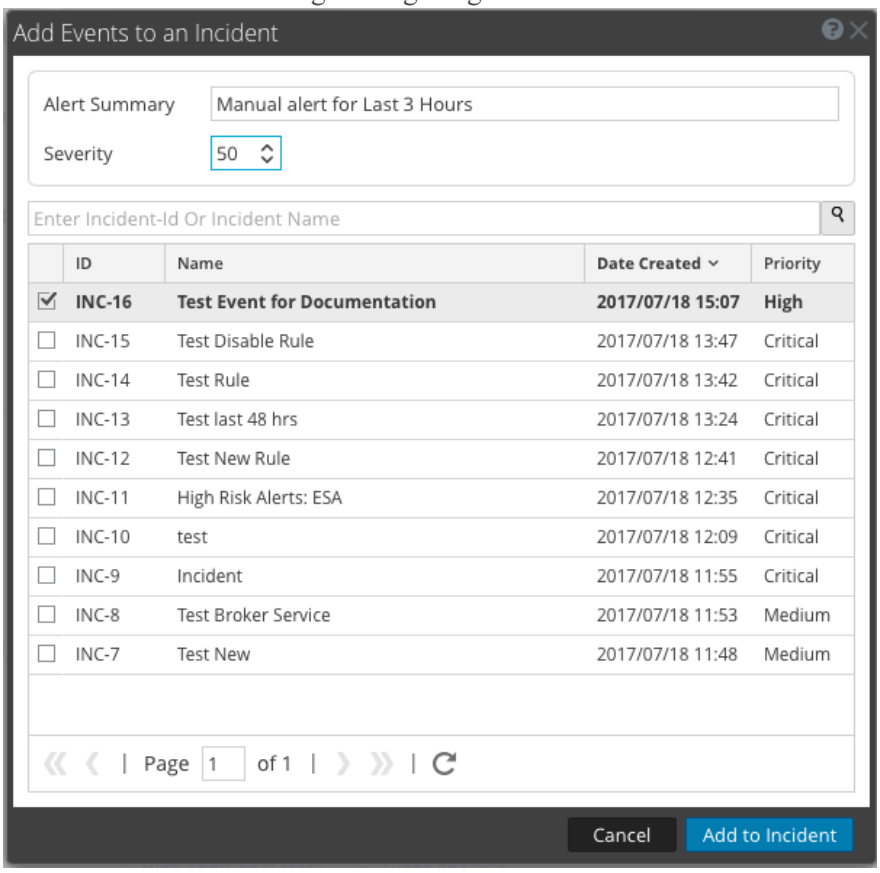
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Ereignisse“

Überblick

Die folgende Abbildung zeigt ein Beispiel für das Dialogfeld „Ereignisse zu einem Incident hinzufügen“. In der Tabelle werden die Informationen und Optionen beschrieben, die im Dialogfeld „Warnmeldungen zu einem Incident hinzufügen“ angezeigt werden.



Funktion	Beschreibung
Warnmeldungszusammenfassung	Das Feld „Warnmeldungszusammenfassung“ wird von der Abfrage ausgefüllt, die die ausgewählten Warnmeldungen produziert hat, die Sie ausgewählt haben, um diesen Incident zu erstellen. Das Feld „Schweregrad“ zeigt den Schweregrad der ausgewählten Warnmeldung an, eine Ganzzahl zwischen 1 und 100.
Suchen	Erlaubt die Suche nach einem vorhandenen Ereignis.
ID	Die ID des Incident. Sie können IDs in auf- oder absteigender Reihenfolge sortieren.
Name	Der Name des Incident. Sie können Namen in auf- oder absteigender Reihenfolge sortieren.
Erstellungsdatum	Zeigt das Datum und die Uhrzeit der Erstellung des Incident an. Sie können die Datumsangaben in aufsteigender oder absteigender Reihenfolge sortieren.

Funktion	Beschreibung
Priorität	Zeigt die Priorität des Incident an: entweder niedrig oder kritisch.
Abbrechen	Schließt das Dialogfeld, ohne die Änderungen zu speichern.
Einem Incident hinzufügen	Fügt die Warnmeldungen zu dem Incident hinzu. Ein Dialogfeld bestätigt, dass Warnmeldungen erfolgreich hinzugefügt wurden.

Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“

Im Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ können Sie eine Entität oder einen Metawert zu einer vorhandenen Context-Hub-Liste hinzufügen, eine Entität oder einen Metawert aus einer vorhandenen Context-Hub-Liste entfernen oder eine neue Context-Hub-Liste mit der Entität oder dem Metawert erstellen. Wenn Sie eine IP-Adresse oder eine andere Entität abfragen und sie als verdächtig oder interessant bewerten, können Sie sie zu einer Liste hinzufügen, die als Datenquelle hinzugefügt wurde. Beispiele für häufig verwendete Listen sind Whitelists oder Blacklists. Das verbessert die Sichtbarkeit verdächtiger IP-Adressen und verringert falsch positive Ergebnisse, die keiner weiteren Untersuchung bedürfen.

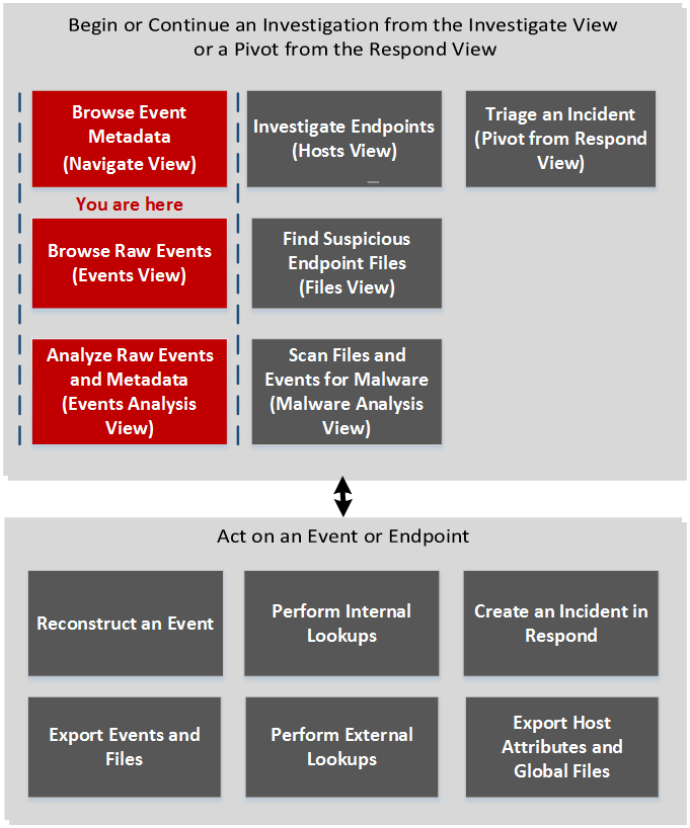
Sie können Entitäten oder Metawerte zu mehr als einer Liste hinzufügen. Beispielsweise können Sie sie einerseits zu einer Liste mit verdächtigen Domains im Zusammenhang mit Command-and-Control-Verbindungen hinzufügen und andererseits zu einer weiteren Liste mit für Remotezugriff verwendeten IP-Adressen mit Trojanerverbindung. Ist keine Liste verfügbar, können Sie eine erstellen.

Das Dialogfeld ist in NetWitness Investigate und in NetWitness Respond verfügbar. Beim Arbeiten in Investigate können Sie in den Ansichten „Navigation“, „Ereignisse“ oder „Ereignisanalyse“ (Version 11.2) Metawerte für die Metaschlüssel `Source IP`, `Destination IP` oder `Username` zu einer vorhandenen Context-Hub-Liste hinzufügen oder Sie können eine neue Liste mit diesen Metawerten erstellen. Wenn Sie einer Liste Metawerte hinzufügen, können Sie nach zusätzlichem Kontext für diese Metawerte suchen.

- Rufen Sie das Dialogfeld in der Ansicht „Navigieren“ oder der Ansicht „Ereignisse“ auf, indem Sie unter `Source IP`, `Destination IP` oder `Username` mit der rechten Maustaste auf einen Metawert klicken und im Kontextmenü **Zu Liste hinzufügen/Aus Liste entfernen** auswählen.
- Um das Dialogfeld in der Ansicht „Ereignisanalyse“ anzuzeigen, bewegen Sie den Mauszeiger über einen Wert und wählen Sie im Bereich „Aktionen“ der Kontext-Kurzinformation **Zu Liste hinzufügen/Aus Liste entfernen** aus.

Workflow

Das folgende Workflowdiagramm zeigt den allgemeinen Workflow für „Untersuchen“. Die Position der Aufgabe „Zur Liste hinzufügen“ ist hervorgehoben.



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*

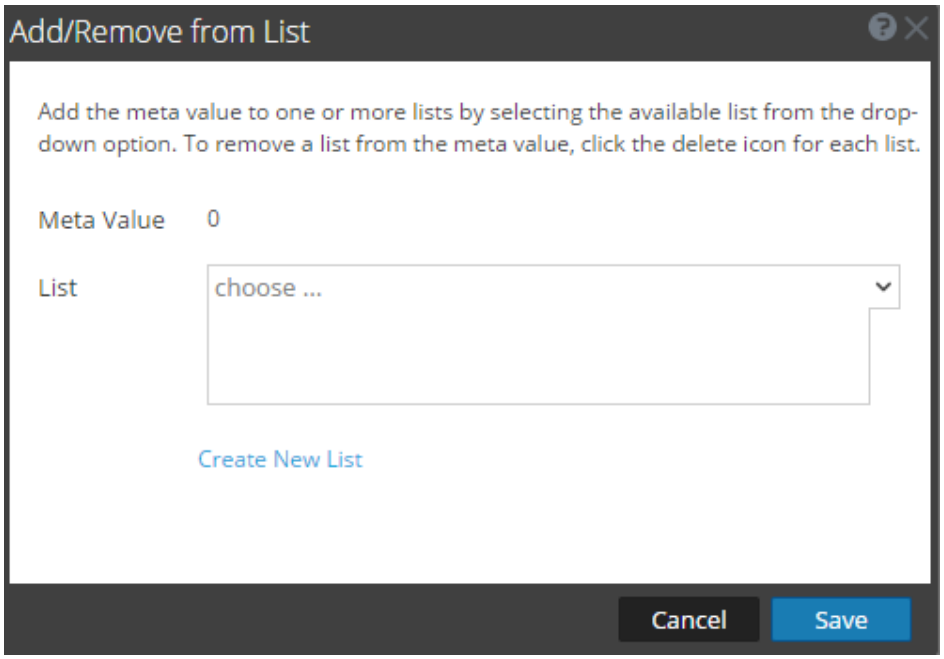
Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Erstellen oder Hinzufügen von Metawerten zu einer Context-Hub-Liste*	Verwalten von Context-Hub-Listen und Listenwerten in den Ansichten „Navigation“ und „Ereignisse“ oder Suchen von zusätzlichem Kontext in der Ansicht „Ereignisanalyse“

Verwandte Themen

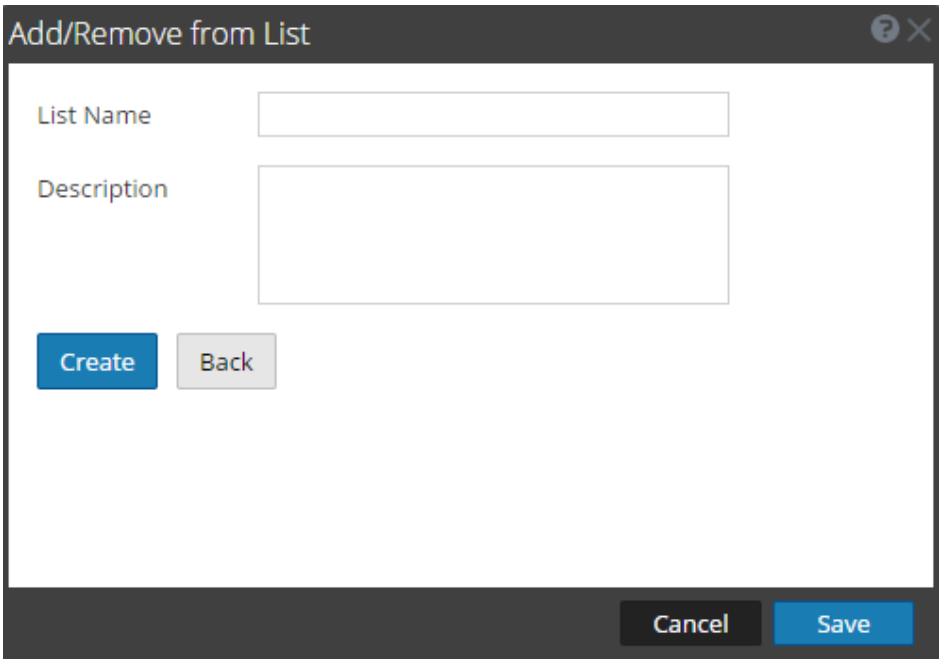
- Suchen von weiteren Kontexten in den Ansichten „Navigation“ und „Ereignisse“
- Ansicht „Navigation“
- Ansicht „Ereignisse“
- Ansicht „Ereignisanalyse“

Überblick über die Ansichten „Navigation“ und „Ereignisse“

Die folgende Abbildung zeigt ein Beispiel des Dialogfelds „Zu Liste hinzufügen/Aus Liste entfernen“ beim ersten Öffnen.



Die folgende Abbildung zeigt das Dialogfeld, wenn Sie „Neue Liste erstellen“ auswählen.

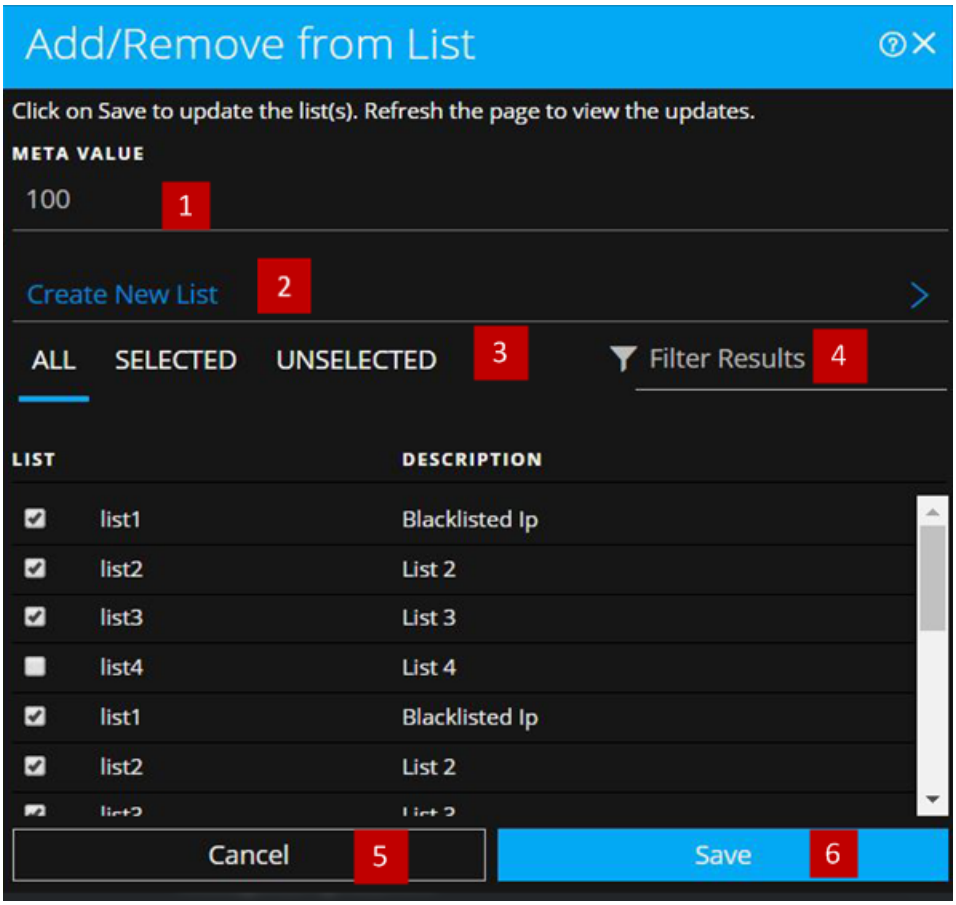


Die folgende Tabelle beschreibt die Funktionen der Dialogfelder „Zu Liste hinzufügen/Aus Liste entfernen“ und „Neue Liste erstellen“.

Funktion	Beschreibung
Metawert	Der ausgewählte Metawert, der zu der vorhandenen oder neuen Liste hinzugefügt werden soll.
Liste	Die Liste, zu der der ausgewählte Metawert hinzugefügt werden muss. Ein Drop-down-Menü bietet eine Liste der verfügbaren Listen an, denen Sie den Metawert hinzufügen können.
Neue Liste erstellen	Öffnet ein neues Dialogfeld, in dem Sie eine neue Liste für den ausgewählten Metawert erstellen können.
Listenname	Der Name der neuen Liste
Beschreibung	Die Beschreibung der neuen Liste
Erstellen	Erstellt eine neue Liste, nachdem Sie die erforderlichen Felder eingegeben haben.
Zurück	Bricht im Neue-Listen-Modus die Erstellung einer neuen Liste ab und kehrt wieder zum ursprünglichen Dialogfeld zurück.
Abbrechen	Bricht das Hinzufügen des Metawerts zu einer Liste ab und schließt das Dialogfeld.
Speichern	Speichert die Änderungen an den Listen und schließt das Dialogfeld.

Überblick über die Ansicht „Ereignisanalyse“ (ab Version 11.2)

Unten sehen Sie ein Beispiel für das Dialogfeld **Zu Liste hinzufügen/Aus Liste entfernen** in der Ansicht „Ereignisanalyse“.



1 Hinzuzufügende oder zu entfernende Entities oder Metawerte
2 Erstellen einer neuen Liste mit den ausgewählten Metawerten
3 Auswählbare Registerkarten: „Alle“, „Ausgewählt“ und „Nicht ausgewählt“
4 Suche nach Listenname oder Listenbeschreibung
5 Abbrechen der Aktion
6 Speichern zur Aktualisierung einer Liste oder zur Erstellung einer neuen Liste

In der folgenden Tabelle sind die Optionen im Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ aufgeführt.

Option	Beschreibung
METAWERT	Zeigt die Entity oder den Metawert an, die/der zum Hinzufügen zu oder Entfernen aus einer oder mehreren Listen ausgewählte wurde. Sie können auch eine neue Liste mit dem ausgewählten Wert erstellen.
Neue Liste erstellen	Zeigt ein Dialogfeld zur Erstellung einer neuen Liste mit dem ausgewählten Metawert an.

Option	Beschreibung
ALLE	Zeigt alle verfügbaren Context-Hub-Listen an. Listen, die die ausgewählte Entity bzw. den ausgewählten Wert enthalten, sind bereits ausgewählt. Aktivieren Sie das entsprechende Kontrollkästchen, um eine Entity oder einen Metawert zu einer Liste hinzuzufügen. Deaktivieren Sie das entsprechende Kontrollkästchen, um einen Wert oder eine Entity aus der Liste zu entfernen.
AUSGEWÄHLT	Zeigt nur die Listen an, in denen die ausgewählte Entity oder der ausgewählte Metawert enthalten ist. (Alle Listen sind ausgewählt.)
NICHT AUSGEWÄHLT	Zeigt nur die Listen an, in denen die ausgewählte Entity oder der ausgewählte Metawert nicht enthalten ist. (Keine Liste ist ausgewählt.)
Filtern von Ergebnissen	Geben Sie hier den Namen oder die Beschreibung einer bestimmten Liste ein, um sie unter mehreren Listen zu finden.
LISTE	Zeigt den Namen aller Listen an.
DESCRIPTION	Zeigt Informationen zur ausgewählten Liste an. In diesem Dialogfeld wird die Beschreibung angezeigt, die Sie bei der Erstellung einer Liste angeben. Beispiel: Diese Liste enthält alle IP-Adressen in der Blacklist.
Abbrechen	Bricht den Vorgang ab.
Speichern	Speichert die Änderungen.

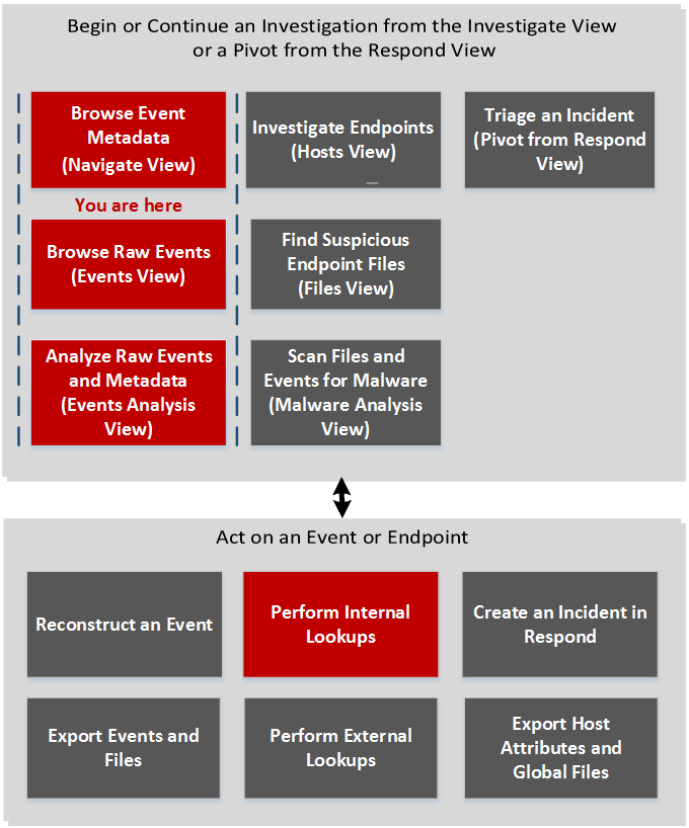
Bereich „Kontextabfrage“

Nachdem ein Administrator den Context-Hub-Service konfiguriert hat, können Sie die Kontextinformationen für die Metawerte in den Ansichten „Navigation“, „Ereignisse“ und „Ereignisanalyse“ (Version 11.2) anzeigen. Der Context-Hub-Service ist mit einer Standardzuordnung von Metadatentypen und Metaschlüsseln vorkonfiguriert. Informationen über die Zuordnung von Context Hub-Metawerten zu Investigation-Metaschlüsseln finden Sie unter „Managen der Metadatentyp- und Metaschlüsselzuordnung“ im *Context Hub-Konfigurationsleitfaden*.

Der Bereich „Kontextabfrage“ wird rechts neben der Ansicht „Navigation“ und der Ansicht „Ereignisse“ angezeigt. Metawerte, die einer Context Hub-Liste hinzugefügt wurden, sind in den Ergebnissen der Ansichten „Navigation“ oder „Ereignisse“ grau hervorgehoben. In der Ansicht „Ereignisanalyse“ sind sie mit einem Unterstrich gekennzeichnet. Sobald Sie mit der rechten Maustaste auf einen hervorgehobenen Wert klicken und im Kontextmenü **Kontextabfrage** auswählen, werden im Bereich „Kontextabfrage“ die zu dem ausgewählten Metawert gehörenden Abfrageerbenisse aus den konfigurierten Quellen angezeigt. In der Symbolleiste des Bereichs „Kontextabfrage“ können Sie die jeweils gewünschte Quelle auswählen, um die entsprechenden Kontextinformationen abzurufen.

Bei Darstellung und Inhalt des Bereichs „Kontextabfrage“ gibt es einige Unterschiede, wenn er in der Ansicht „Navigation“ oder „Ereignisse“ und in der Ansicht „Ereignisanalyse“ geöffnet wird.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Zusätzlichen Kontext zu einem Metawert abrufen*	Suchen von weiteren Kontexten in den Ansichten „Navigation“ und „Ereignisse“ und Suchen von zusätzlichem Kontext in der Ansicht „Ereignisanalyse“

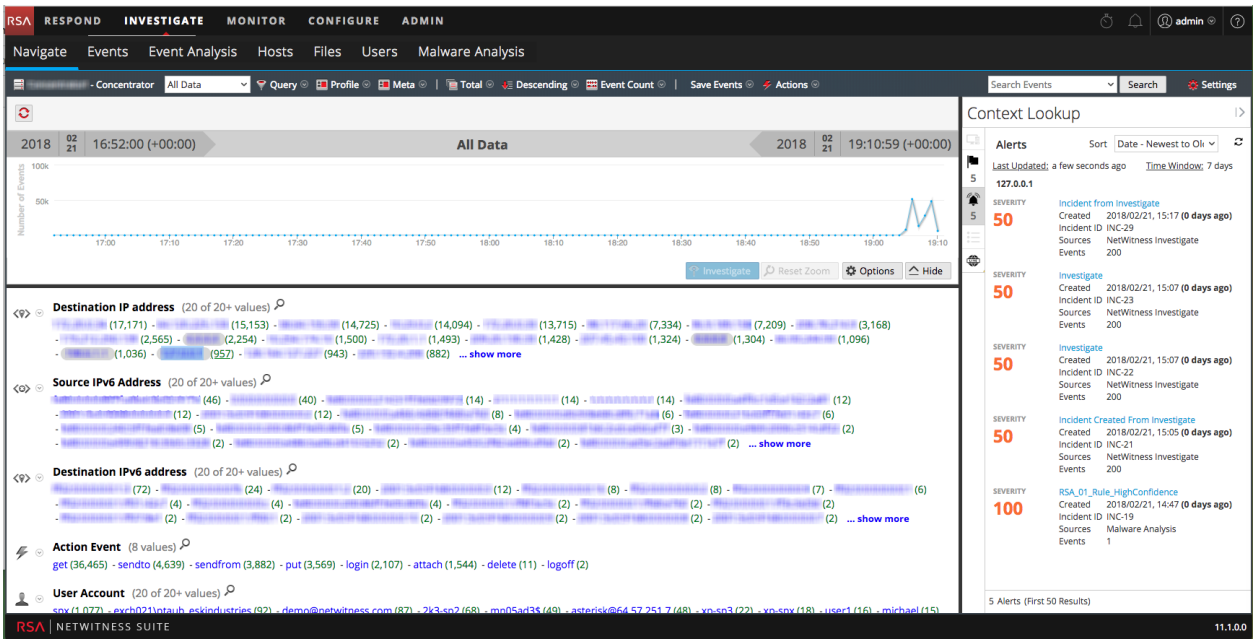
* Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Ereignisse“
- Ansicht „Navigation“
- Ansicht „Ereignisanalyse“
- „NetWitness-Feedback und Datenfreigabe“ im *Handbuch Live-Services-Management*

Überblick (über die Ansichten „Navigation“ und „Ereignisse“)

Die folgende Abbildung ist ein Beispiel für die Anzeige des Bereichs „Kontextabfrage“ in den Ansichten „Navigation“ und „Ereignisse“. Bedienelemente und Funktionen sind in der Tabelle beschrieben.



Funktion	Beschreibung
Leiste mit Quellenoptionen	Zeigt die Symbole für die verfügbaren Quellen an: Endpoint, Incidents, Warnmeldungen und Listen.
Quellenname	Zeigt den Quellennamen basierend auf dem ausgewählten Symbol an: • Endpoint • Incidents • Warnmeldungen • Listen • Live Connect
Sortieren	Bietet eine Drop-down-Liste der Sortieroptionen für die aufgelisteten Kontextinformationen. Mögliche Sortieroptionen sind: „Schweregrad: Hoch bis Niedrig“, „Schweregrad: Niedrig bis Hoch“, „Datum (ältestes bis neuestes)“ und „Datum (neuestes bis ältestes)“. Die Sortieroptionen variieren je nach Typ der Datenquelle.
	Aktualisiert die Abfrageergebnisse.
<n Elemente> (erste <n> Ergebnisse)	Die Fußzeile zeigt die Anzahl der derzeit angezeigten Ergebnisse sowie die Gesamtzahl von Ergebnissen an. Beispiel: 5 Warnmeldungen (erste 50 Warnmeldungen)

Incidents

Incidents werden zunächst basierend auf Zeit (Neuestes bis Ältestes) und dann auf Prioritätsstatus angezeigt. Die folgenden Informationen werden für Incident-Abfragen angezeigt:

- Name und ID des Incident
- Prioritätsstatus der Incidents
- Risikowert der Incidents
- Datum der Erstellung des Incident
- Status des Incident
- Zuweisungsempfänger für Incident
- Letzte Aktualisierung: Gibt an, wann zuletzt kontextbezogene Daten aus der Datenquelle abgerufen und im Cache aktualisiert wurden.
- Zeitfenster: Diese Angabe basiert auf dem Wert, den Sie im Feld „Letzte Abfrage (Tage)“ im Fenster zum Konfigurieren von „Respond“ festgelegt haben. Weitere Informationen finden Sie im Thema „Konfigurieren von Respond als Datenquelle“ im *Context Hub-Konfigurationsleitfaden*.
- Sortieren: Dieses Drop-down-Feld bietet Optionen zum Sortieren der Ergebnisse auf Basis von Zeitpunkt oder Priorität.

Warnmeldungen

Warnmeldungen werden basierend auf dem Schweregrad angezeigt. Die folgenden Informationen für ECAT-Abfragen werden angezeigt:

- Name der Warnmeldung
- Schweregradwert der Warnmeldungen
- Datum der Erstellung der Warnmeldung
- Incident-ID: die ID des Incident, dem die Warnmeldung zugeordnet ist (falls zutreffend)
- Quellen: Name der Ereignisquelle
- Anzahl der Ereignisse, die der Warnmeldung zugeordnet sind
- Letzte Aktualisierung: Gibt an, wann zuletzt kontextbezogene Daten aus der Datenquelle abgerufen und im Cache aktualisiert wurden.
- Zeitfenster: Diese Angabe basiert auf dem Wert, den Sie im Feld „Letzte Abfrage (Tage)“ im Fenster zum Konfigurieren von „Respond“ festgelegt haben. Weitere Informationen finden Sie im Thema „Konfigurieren von Respond als Datenquelle“ im *Context Hub-Konfigurationsleitfaden*.
- Sortieren: Dieses Drop-down-Feld bietet die Option, die Sortierung des Ergebnisses basierend auf Zeit oder Priorität zu ändern.

Listen

Die folgenden Informationen werden für Listenabfragen angezeigt:

- Listenname
- Eigentümer, der die Liste erstellt hat
- Erstellungsdatum

- Datum der letzten Aktualisierung
- Beschreibung der Liste

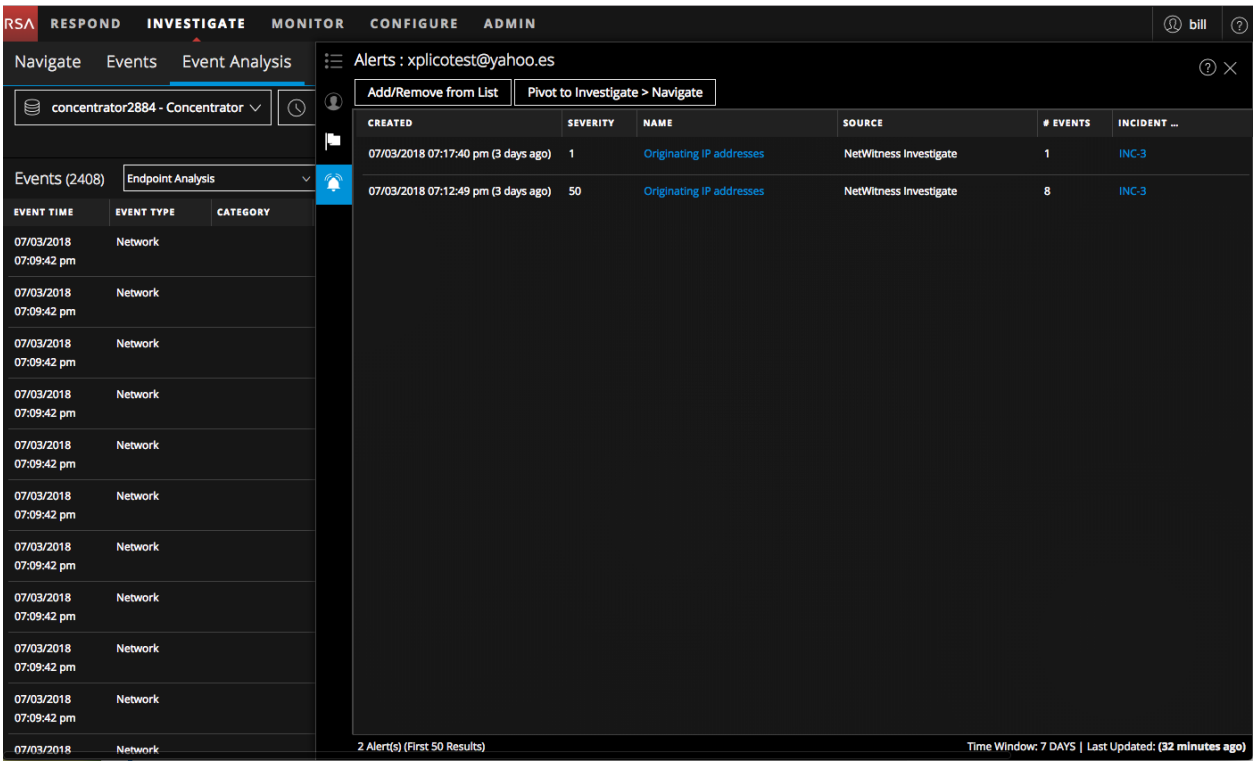
Endpoint

Bei Endpoint-Abfragen werden die folgenden Informationen angezeigt:

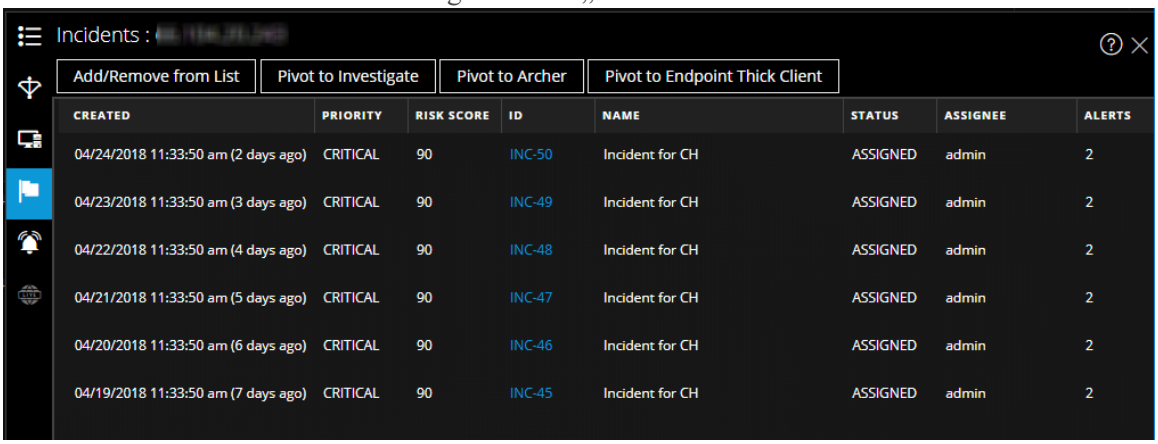
- Computername und IP-Adresse des Computers.
  Durch Klicken auf die IP-Adresse oder den Endpoint-Rechernamen werden Sie zur Endpoint-Benutzeroberfläche weitergeleitet, wo Sie weitere Untersuchungen vornehmen können.
- Letzte Aktualisierung: Gibt an, wann zuletzt kontextbezogene Daten aus der Datenquelle abgerufen und im Cache aktualisiert wurden.
- Rechnerwert Hier wird ein Rechner-IIOC-Wert aggregiert, basierend auf den Modulwerten.
- Anzahl der Module: Anzahl der aktiven Dateien für den ausgewählten Computer.
- Letzte Aktualisierung: Gibt an, wann die Scanergebnisse zuletzt in der Endpoint-Datenbank aktualisiert wurden.
- Zuletzt angemeldeter Nutzer
- MAC-Adresse des Computers
- Betriebssystemversion
- Administratorhinweise (falls vorhanden)
- Administratorstatus (falls vorhanden)
- Verdächtigste Module (Module mit einem IIOC-Wert > 500): Diese Angabe basiert auf dem Wert im Feld „IIOC-Mindestwert“, den Sie im Fenster „Endpoint konfigurieren“ festgelegt haben. Der Standardwert für „IIOC-Mindestwert“ beträgt 500.
- Rechner-IIOC-Ebenen

Überblick über die Ansicht „Ereignisanalyse“ (ab Version 11.2)

Die folgende Abbildung ist ein Beispiel für die Anzeige des Bereichs „Kontextabfrage“ in der Ansichte „Ereignisanalyse“.



Welche kontextbezogenen Informationen oder Abfrageergebnisse im Bereich „Kontextabfrage“ angezeigt werden, hängt von der ausgewählten Einheit und den ihr zugeordneten Datenquellen ab. Für jede Datenquelle wird im Bereich „Kontextabfrage“ eine separate Registerkarte angezeigt. Die Registerkarten sind: Listen, Archer, Active Directory, Endpoint, Incidents, Warnmeldungen und Live Connect. Die folgende Abbildung zeigt den Bereich „Kontextabfrage“ für eine ausgewählte Entität in der Incident-Detailansicht mit der Registerkarte „Incidents“.

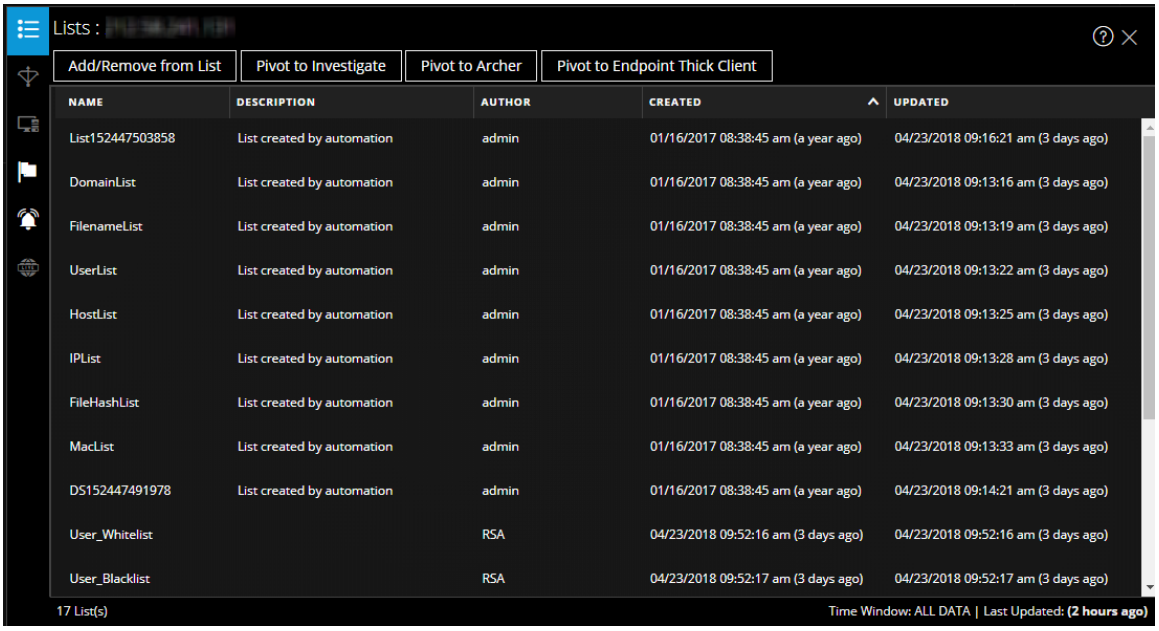


In der folgenden Tabelle sind die auf den verschiedenen Registerkarten verfügbaren Daten und die unterstützten Entitäten beschrieben.

Registerkarte	Beschreibung	Unterstützte Entitäten
 (Listen)	Zeigt alle Listendaten an, die der ausgewählten Entität bzw. dem ausgewählten Metawert zugeordnet sind. Die Ergebnisse werden beginnend ab der zuletzt aktualisierten Liste angezeigt.	Alle Entitäten
 (Archer)	Zeigt Informationen zu Ressourcen sowie Wichtigkeitsratings an, basierend auf der Archer-Datenquelle.	IP, Host und Mac
 (Active Directory)	Zeigt alle Benutzerinformationen für den ausgewählten Benutzer an.	Benutzer
 (NetWitness Endpoint)	Zeigt die aus der NetWitness Endpoint-Datenquelle abgerufenen Informationen zu der ausgewählten Entität bzw. zu dem ausgewählten Metawert an, inklusive der Angaben „Rechner“, „Module“ und „IIOC-Stufen“. Module werden auf Basis des IOC-Werts sortiert (vom höchsten Wert zum niedrigsten Wert), IIOC-Stufen von der höchsten Stufe zur niedrigsten Stufe.	IP, MAC-Adresse und Host
 (Incidents)	Zeigt eine Liste aller Incidents an, die der ausgewählten Entität bzw. dem ausgewählten Metawert zugeordnet sind. Die Ergebnisse werden beginnend ab dem neuesten Incident sortiert.	Alle Entitäten
 (Warnmeldungen)	Zeigt eine Liste aller Warnmeldungen an, die der ausgewählten Entität bzw. dem ausgewählten Metawert zugeordnet sind. Die Ergebnisse werden beginnend ab der neuesten Warnmeldung sortiert.	Alle Entitäten
 (Live Connect)	Zeigt Live Connect-Informationen an.	IP, Domain und Datei-Hash

Registerkarte „Listen“

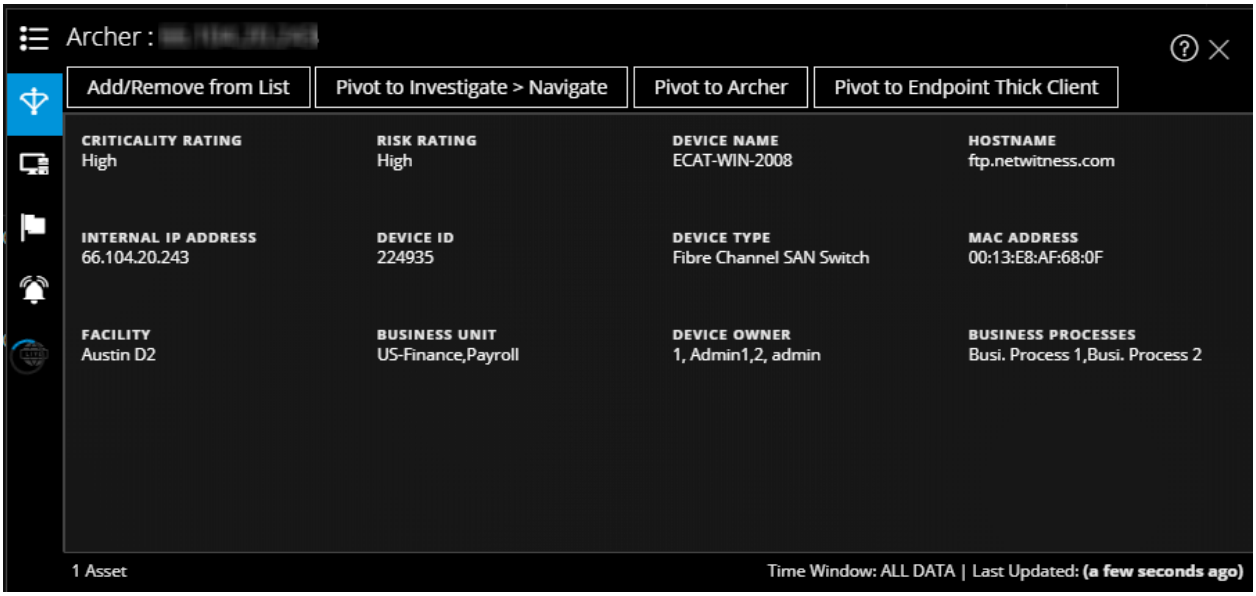
Auf der Registerkarte „Listen“ im Bereich „Kontextabfrage“ werden alle Listen angezeigt, die der ausgewählten Entität bzw. dem ausgewählten Metawert zugeordnet sind. Die folgende Abbildung zeigt ein Beispiel eines Kontextbereichs für Listen und in der Tabelle werden die Felder beschrieben.



Feld	Beschreibung
Name	Name der Liste (definiert bei der Erstellung der Liste)
Beschreibung	Beschreibung der Liste (definiert bei der Erstellung der Liste)
Verfasser	Eigentümer, der die Liste erstellt hat
Erstellt	Datum der Listenerstellung
Updated	Datum, an dem die Liste zuletzt aktualisiert oder geändert wurde
Anzahl	Anzahl der Listen, in denen die ausgewählte Entität bzw. der ausgewählte Metawert aufgeführt werden
Zeitfenster	Das Zeitfenster basierend auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfeld „Antworten konfigurieren“ festgelegt wurde. Standardmäßig werden alle Listendaten abgerufen.
Letzte Aktualisierung	Zeitpunkt, zu dem Context Hub die Abfragedaten abgerufen und im Cache gespeichert hat

Registerkarte „Archer“

Auf der Registerkarte „Archer“ im Bereich „Kontextabfrage“ werden Informationen zu Ressourcen zusammen mit Wichtigkeitsratings angezeigt. Hierfür wird auf die Archer-Datenquellen für IP-, Host- und Mac-Entitäten zugegriffen. Die folgende Abbildung zeigt ein Beispiel des Bereichs „Kontextabfrage“ für Archer und in der Tabelle werden die Felder beschrieben.



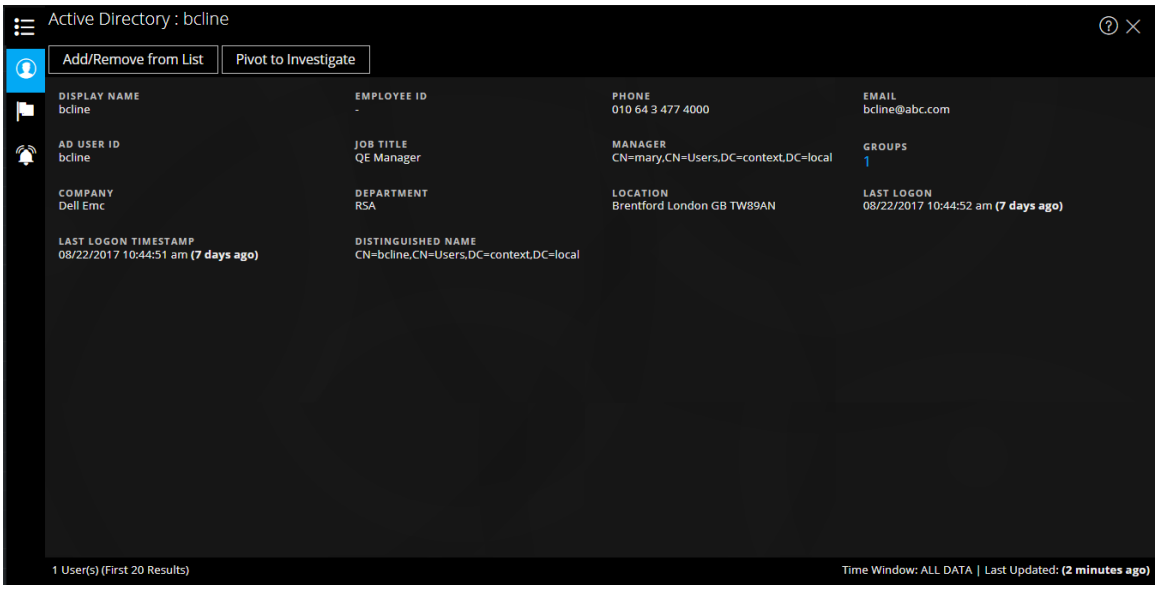
Feld	Beschreibung
Wichtigkeitsrating	Die operative Wichtigkeit des Geräts anhand der von ihm unterstützten Anwendungen. Mögliche Wichtigkeitsratings sind „Ohne Rating“, „Niedrig“, „Mittelniedrig“, „Mittel“, „Mittelhoch“ oder Hoch.
Risikorating	Das berechnete Risikorating des Geräts auf Basis der letzten Bewertung und des durchschnittlichen Risikoratings aller Anlagen, in denen das Gerät eingesetzt wird. Mögliche Risikoratings sind „Schwerwiegend“, „Hoch“, „Mittel“, „Niedrig“ oder „Minimal“.
Gerätename	Der eindeutige Name des Geräts.
Hostname	Der Hostname des Geräts.
IP-Adresse	Geben Sie die primäre, interne IP-Adresse des Geräts ein.
Geräte-ID	Der automatisch ausgefüllte Wert, der den Datensatz in allen Anwendungen innerhalb des Systems eindeutig identifiziert.
Typ	Der Gerätetyp, zum Beispiel Server, Laptop, Desktop und andere.
Anlagen	Links zu Datensätzen der Anwendung „Anlagen“, die mit dem Gerät in Verbindung stehen.
Geschäftsbereich	Links zu Datensätzen der Anwendung „Geschäftsbereich“, die mit dem Gerät in Verbindung stehen. Bei mehr als drei Geschäftsbereichswerten können Sie mit der Maus auf das Feld zeigen, um alle Werte zu sehen.

Feld	Beschreibung
Device-Eigentümer	Die Person, die für das Gerät verantwortlich ist und über Berechtigungen zum Lesen und Aktualisieren für den Datensatz verfügt.
Anzahl	Die Anzahl der verfügbaren Ressourcen.
Zeitfenster	Das Zeitfenster basierend auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfeld „Antworten konfigurieren“ festgelegt wurde. Standardmäßig werden alle Archer-Daten abgerufen.
Letzte Aktualisierung	Zeitpunkt, zu dem Context Hub die Abfragedaten abgerufen und im Cache gespeichert hat

Hinweis: In den lokalisierten Versionen werden nur diese zwölf Felder angezeigt: Wichtigkeitsrating, Risikorating, Device-Eigentümer, Geschäftsbereich, Hostname, MAC-Adresse, Anlagen, IP-Adresse, Typ, Geräte-ID, Gerätename und Geschäftsprozesse.

Registerkarte „Active Directory“

Die folgende Abbildung zeigt ein Beispiel für den Bereich „Kontextabfrage“ für Active Directory.



Auf der Registerkarte „Active Directory“ im Bereich „Kontextabfrage“ werden sämtliche Informationen zu einem Benutzer sowie alle ihm zugeordneten Incidents und Warnmeldungen aufgeführt. Abfragen können die folgenden Formate haben:

- Benutzerprinzipalname
- Domain/Benutzername
- SAM-Konto-Name

Existiert ein Benutzer in mehreren Domains oder Gesamtstrukturen, werden alle verfügbaren Kontextinformationen zu dem Benutzer angezeigt.

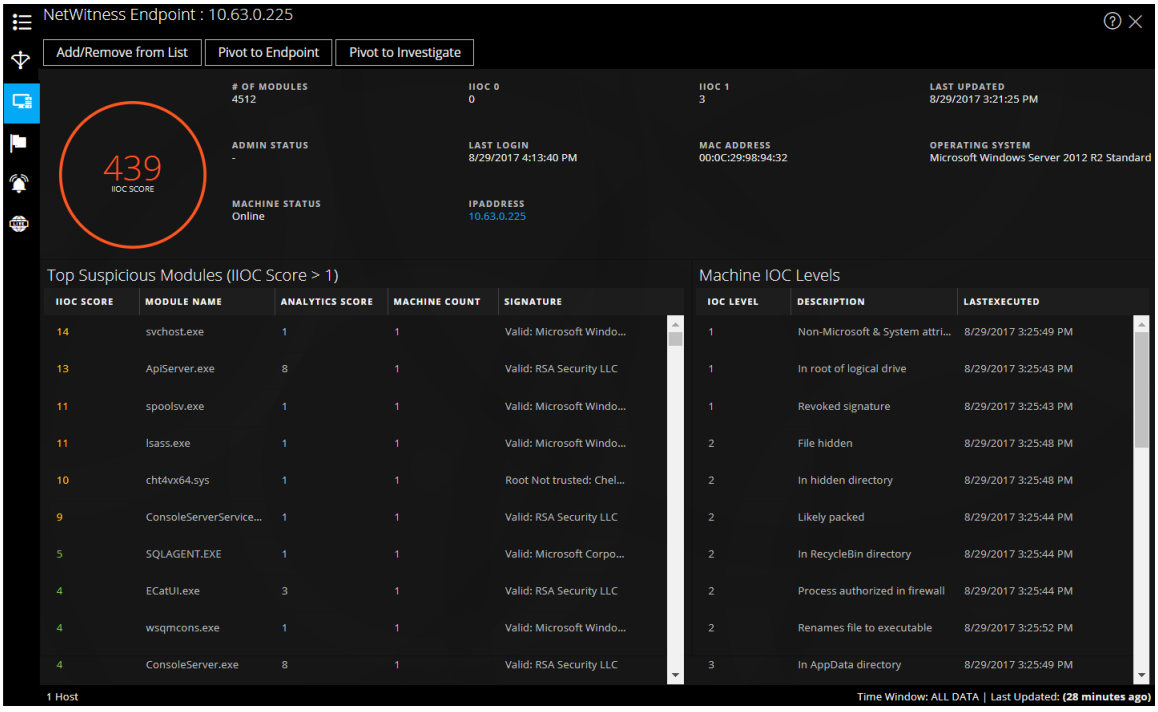
Auf der Registerkarte „Active Directory“ werden die nachfolgend aufgeführten Informationen angezeigt.

Feld	Beschreibung
Anzeigename	Der Name des Nutzers.
Mitarbeiterkennung	Die Mitarbeiter-ID des Nutzers.
Telefon	Die Telefonnummer des Nutzers
E-Mail	Die E-Mail-ID des Nutzers.
AD-Nutzer-ID	Zeigt die eindeutige Kennung des Nutzers innerhalb einer Organisation an.
Position	Die Bezeichnung des Nutzers.
Manager	Der Name des Managers des Nutzers.
Gruppen	Die Liste der Gruppen, bei denen der Nutzer Mitglied ist.

Feld	Beschreibung
Unternehmen	Der Name des Unternehmens des Nutzers.
Abteilung	Zeigt den Namen der Abteilung an, zu der der Nutzer innerhalb der Organisation gehört.
Standort	Der geografische Standort des Nutzers.
Letzte Anmeldung	Zeitpunkt, zu dem sich der Nutzer zuletzt beim System angemeldet hat (nur wenn der globale Katalog definiert ist).
Zeitstempel letzte Anmeldung	Zeitpunkt, zu dem sich der Nutzer zuletzt beim System angemeldet hat.
Distinguished Name	Eindeutiger Name, der dem Nutzer zugewiesen wurde.
Anzahl	Die Anzahl der Benutzer.
Zeitfenster	Das Zeitfenster basierend auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfeld zum Konfigurieren der Datenquelleneinstellungen festgelegt wurde. Standardmäßig werden alle Active Directory-Daten abgerufen.
Letzte Aktualisierung	Zeitpunkt, zu dem Context Hub die Abfragedaten abgerufen und im Cache gespeichert hat

Registerkarte „NetWitness Endpoint“

Die folgende Abbildung zeigt ein Beispiel für den Bereich „Kontextabfrage“ für NetWitness Endpoint.



Es werden die nachfolgend aufgeführten IIOC-Informationen angezeigt.

Feld	Beschreibung
Modulanzahl	Die Anzahl der Module, die abgefragt werden.
Administratorstatus	Administratorstatus (falls vorhanden).
Letzte Aktualisierung	Zeitpunkt der letzten Datenaktualisierung.
Letzte Anmeldung	Der Zeitpunkt, zu dem der Nutzer sich das letzte Mal angemeldet hat.
MAC-Adresse	MAC-Adresse des Computers.
Betriebssystem	Die Version des vom NetWitness Endpoint-Computer verwendeten Betriebssystems.
Computerstatus	Der Status des angezeigten Moduls: Online, Offline, Aktiv oder Inaktiv.
IP-Adresse	Die IP-Adresse des betreffenden Moduls.

Es werden die nachfolgend aufgeführten Modulinformationen angezeigt.

Feld	Beschreibung
IIOC-Wert	Der IIOC-Wert eines Computers ist der aus den Modulwerten aggregierte Wert. Dies ist abhängig von dem im Feld „IIOC-Mindestwert“ im Dialogfeld für die Datenquelleneinstellungen von Context Hub festgelegten Wert. Der Standardwert für „IIOC-Mindestwert“ beträgt 500. Siehe „Konfigurieren der Einstellungen von Datenquellen für den Context Hub“ im *Context Hub-Konfigurationsleitfaden*.
Modulname	Der Name des abgefragten Moduls.
Analysewert	Die Anzahl der aktiven Dateien für den ausgewählten Computer.
Rechneranzahl	Die Anzahl der Computern, auf denen dieser spezielle IOC ausgelöst wurde.
Signatur	Gibt an, ob die Datei signiert oder unsigniert bzw. gültig oder ungültig ist. Ebenfalls angegeben sind Informationen zum Unterzeichner (z. B. Google oder Apple).

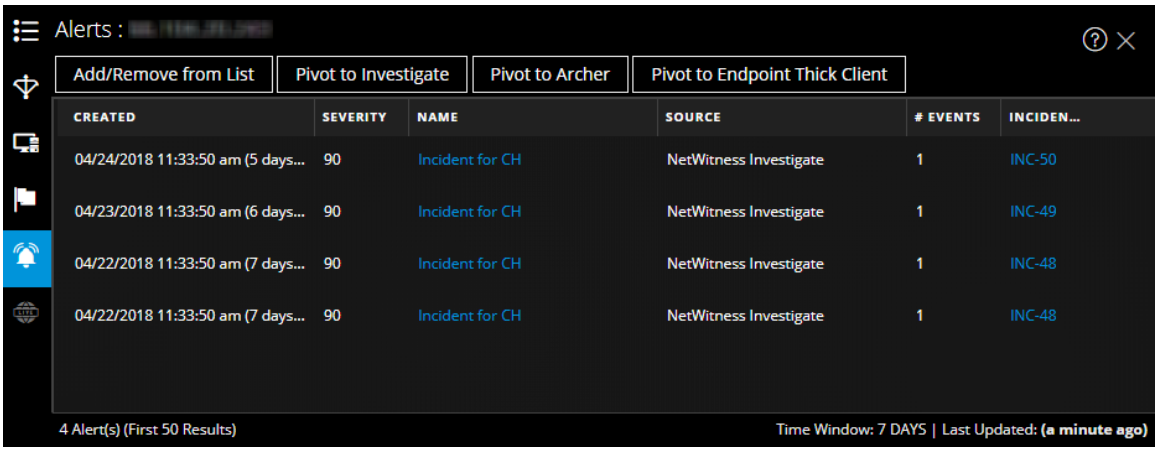
Für Computer werden die nachfolgend aufgeführten Informationen angezeigt.

Feld	Beschreibung
IOC-Ebene	Die IOC-Ebenen.
Beschreibung	Die Beschreibung der IOC-Ebene (falls verfügbar).
Letzte Ausführung	Zeitpunkt der letzten Ausführung der Aktion.
Anzahl	Die Anzahl der abgefragten Hosts.
Zeitfenster	Das Zeitfenster basierend auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfeld zum Konfigurieren von Datenquelleneinstellungen festgelegt wurde. Standardmäßig werden alle NetWitness Endpoint-Daten abgerufen.

Feld	Beschreibung
Letzte Aktualisierung	Zeitpunkt der letzten Aktualisierung der Scanergebnisse in der NetWitness Endpoint-Datenbank.

Registerkarte „Warnmeldungen“

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Alerts“ im Kontextbereich. Die Ergebnisse werden zuerst nach Eingang der Warnmeldung (neu nach alt) und dann nach Schweregrad sortiert.



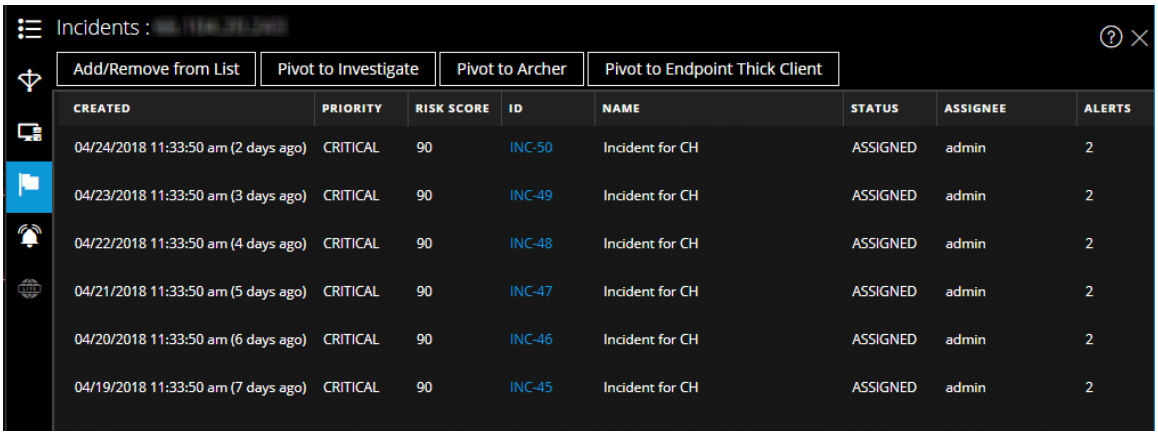
Auf der Registerkarte „Warnmeldungen“ im Bereich „Kontextabfrage“ werden die nachfolgend aufgeführten Informationen angezeigt.

Feld	Beschreibung
Erstellt	Datum und Uhrzeit der Erstellung der Warnmeldung.
Schweregrad	Schweregradwert der Warnmeldungen.
Name	Der Name der Warnmeldung. Klicken Sie auf den Namen, um die Details einer Warnmeldung einzusehen.
Quelle	Name der Warnmeldungsquelle, die die Warnmeldung ausgelöst hat.
Ereignisanzahl	Anzahl der Ereignisse, die der Warnmeldung zugeordnet sind.
Incident-ID	Die ID des Incident, dem die Warnmeldung zugeordnet ist (falls zutreffend). Klicken Sie auf die ID, um die Details einer Warnmeldung einzusehen.
Anzahl	Anzahl der Warnmeldungen. Standardmäßig werden nur die ersten 100 Warnmeldungen angezeigt. Weitere Informationen zur Konfiguration der Einstellungen finden Sie im Thema „Konfigurieren der Einstellungen von Datenquellen für den Context Hub“ im *Context Hub-Konfigurationsleitfaden*.
Zeitfenster	Das Zeitfenster basierend auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfeld zum Konfigurieren von Datenquelleneinstellungen festgelegt wurde. Standardmäßig werden die Warnmeldungsdaten der letzten 7 Tage abgerufen.

Feld	Beschreibung
Letzte Aktualisierung	Zeitpunkt, zu dem zuletzt kontextbezogene Daten aus der Datenquelle abgerufen wurden.

Registerkarte „Incidents“

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Incidents“ im Kontextbereich. Die Ergebnisse werden zuerst nach Eingang des Incidents (neu nach alt) und dann nach Prioritätsstatus sortiert.



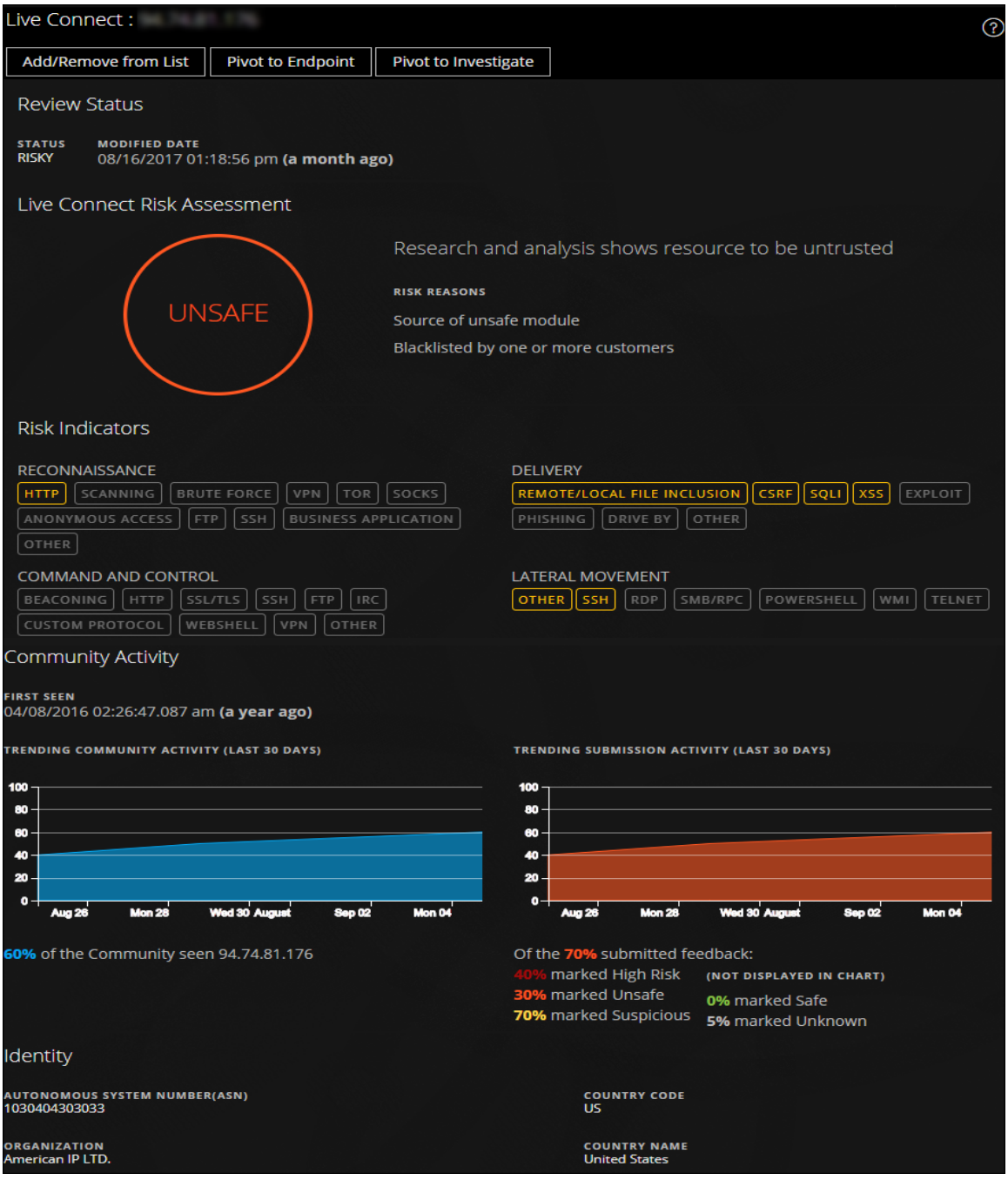
Auf der Registerkarte „Incidents“ im Bereich „Kontextabfrage“ werden die nachfolgend aufgeführten Informationen angezeigt.

Feld	Beschreibung
Erstellt	Datum der Erstellung des Incident.
Priorität	Der Prioritätsstatus der Incidents.
Risikowert	Risikowert der Incidents.
ID	Die ID des Incident. Klicken Sie auf die ID, um die Details des Incident anzuzeigen.
Name	Der Name des Incident.
Status	Der Status des Incident.
Zuweisungsempfänger	Der aktuelle Eigentümer des Incident.
Warnmeldungen	Die Anzahl der Warnmeldungen, die dem Incident zugeordnet sind.
Anzahl	Die Anzahl der Incidents. Standardmäßig werden nur die ersten 100 Incidents angezeigt. Weitere Informationen zur Konfiguration der Einstellungen finden Sie im Thema „Konfigurieren der Einstellungen von Datenquellen für den Context Hub“ im *Context Hub-Konfigurationsleitfaden*.

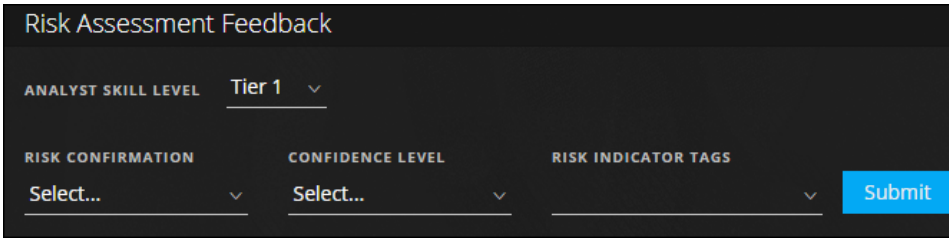
Feld	Beschreibung
Zeitfenster	Das Zeitfenster basierend auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfeld zum Konfigurieren von Datenquelleneinstellungen festgelegt wurde. Standardmäßig werden die Warnmeldungsdaten der letzten 7 Tage abgerufen.
Letzte Aktualisierung	Zeitpunkt, zu dem zuletzt kontextbezogene Daten aus der Datenquelle abgerufen wurden.

Registerkarte „Live Connect“

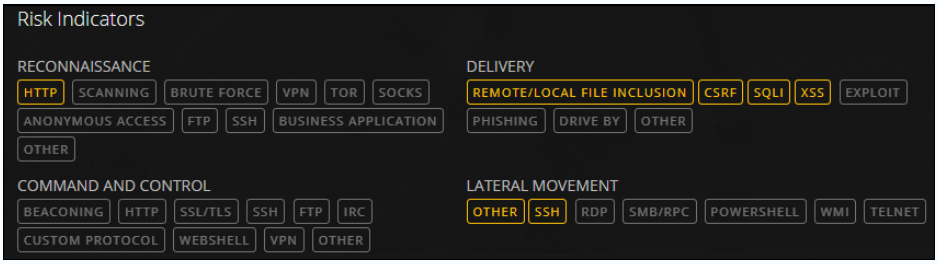
Die folgende Abbildung zeigt das Beispiel eines Kontextbereichs für „Live Connect“ und in der Tabelle werden die angezeigten Informationen beschrieben.

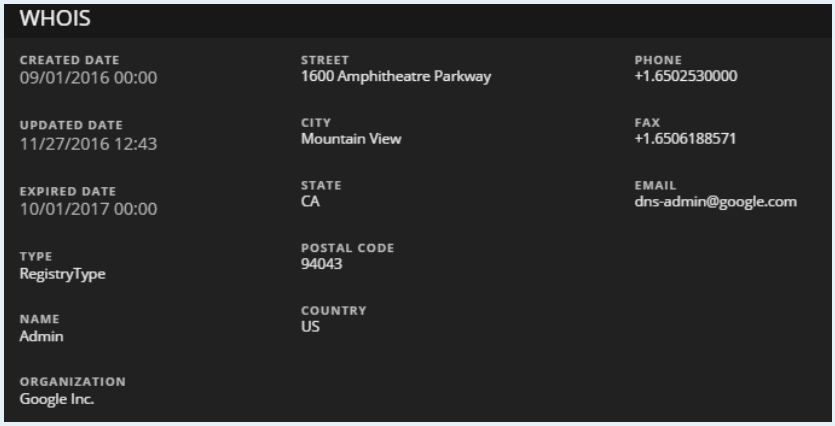


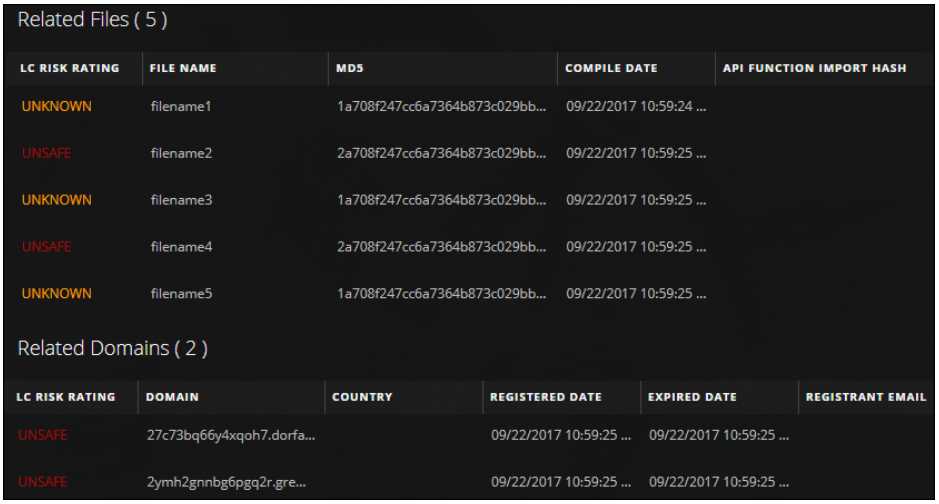
Feld	Beschreibung
Prüfstatus	Der Überprüfungsstatus der ausgewählten Live Connect-Entität (IP, Datei oder Domain), basierend auf der Analystenaktivität. Das ermöglicht Transparenz hinsichtlich der Analystenaktivität innerhalb eines Unternehmens. **Status** Nachfolgenden finden Sie die Statustypen: • **Neu:** Abfrageergebnisse für eine IP-Adresse werden zum ersten Mal innerhalb des Unternehmens angezeigt. • **Angezeigt:** Die Abfrageergebnisse für eine IP-Adresse wurden bereits von Analysten innerhalb des Unternehmens abgerufen. • **Als sicher markiert:** Ein Analyst innerhalb des Unternehmens hat die Abfrageergebnisse für die IP-Adresse bereits gesichtet und als sicher markiert. • **Als riskant markiert:** Ein Analyst innerhalb des Unternehmens hat die Abfrageergebnisse bereits gesichtet die IP-Adresse als riskant markiert.
Risikobewertung	Die Risikobewertung für die ausgewählte Live Connect-Entität (IP, Datei oder Domain), basierend auf der Live Connect-Analyse und Feedback von Analysten. Die Kategorien der Risikobewertung lauten: • **Sicher:** Die Live Connect-Entität gilt als sicher. • **Unbekannt:** In Live Connect liegen nicht genügend Informationen zu der Entität vor, um das Risiko berechnen zu können. • **Hohes Risiko**: Basierend auf der Analyse und den Risikogründen der Community mit „Hohes Risiko“ gekennzeichnet. Die mit „Hohes Risiko“ gekennzeichneten Entitäten erfordern sofortige Maßnahmen. • **Verdächtig**: Basierend auf der Analyse und den Risikogründen der Community als „Verdächtig“ gekennzeichnet. Die Analyse deutet auf eine potenziell bedrohliche Aktivität hin, die Maßnahmen erfordert. • **Unsicher:** Basierend auf der Analyse und den Risikogründen der Community als „Unsicher“ gekennzeichnet. Die Entität wurde als „Hohes Risiko“, „Verdächtig“ oder „Unsicher“ eingestuft. Die entsprechenden Risikogründe werden angezeigt.

Feld	Beschreibung
Feedback zur Risikobewertung	 Über das Feedback zur Risikobewertung können Analysten Threat Intelligence-Feedback zu einer Entität an den Live Connect-Server übermitteln. • **Kompetenzebene des Analysten** Nachfolgend sind die möglichen Kompetenzebenen eines Analysten aufgeführt: ◦ **Tier 1:** Analysten dieser Kompetenzebene definieren Korrekturverfahren und entscheiden, ob ein Incident an andere Stellen innerhalb des SOC (Security Operations Center) eskaliert werden soll. Dies ist der Standardwert. ◦ **Tier 2:** Analysten dieser Kompetenzebene untersuchen Incidents, dokumentieren die Untersuchung und leiten ihr Feedback an die anderen SOC-Workflows weiter. ◦ **Tier 3:** Analysten dieser Kompetenzebene leiten die Untersuchungsergebnisse an die SOC-Teams weiter. Sie sind im Allgemeinen für das Incident-Management verantwortlich und verfügen über umfassende, fundierte Fähigkeiten in Bezug auf die Incident-Reaktion und den Umgang mit den zugehörigen Tools. **Hinweis:** Bei der Erstellung eines neuen NetWitness Platform-Benutzers (Analysten) sollten Administratoren angeben, ob es sich um einen Tier-1-, Tier-2- oder Tier-3-Analysten handelt. • **Risikobestätigung:** die Risikobestätigung für die ausgewählte Live Connect-Entität (IP, Datei oder Domain). Es existieren folgende Kategorien für die Risikobestätigung: ◦ **Sicher**: Die Live Connect-Entität gilt als sicher. ◦ **Unbekannt**: Dem Analysten liegen nicht genügend Informationen für eine Risikobestätigung vor. ◦ **Hohes Risiko**: Basierend auf der Analyse und den Risikogründen der Community mit „Hohes Risiko“ gekennzeichnet. Die mit „Hohes Risiko“ gekennzeichneten Entitäten erfordern sofortige Maßnahmen. ◦ **Verdächtig**: Basierend auf der Analyse und den Risikogründen der Community als „Verdächtig“ gekennzeichnet. Die Analyse deutet auf

Feld	Beschreibung
	eine potenziell bedrohliche Aktivität hin, die Maßnahmen erfordert. ◦ **Unsicher**: Basierend auf der Analyse und den Risikogründen der Community als „Unsicher“ gekennzeichnet. • **Konfidenzniveau:** das Konfidenzniveau, das ein Analyst seinem Feedback zur Live Connect-Entität beimisst. Es existieren folgende Kategorien für das Konfidenzniveau: Hoch, Mittel und Niedrig. • **Risikoindikatortags:** Hier können Sie eine Tagkategorie auswählen, basierend auf der Analyse.
Community-Aktivität	Community-Aktivitäten wie: • Datum, an dem die Community das Problem erstmals bemerkt hat. • Verstrichene Zeit, seitdem die Community die IP/Datei/Domain erstmals bemerkt hat (aktueller Zeitpunkt - Zeitpunkt des ersten Bemerkens) **Trending-Community-Aktivität:** Wenn die IP-Adresse innerhalb der RSA-Community bekannt ist, wird eine grafische Darstellung des Community-Aktivitätstrends für folgende Parameter angezeigt: • Benutzer (in %), von denen die IP-Adresse in der Live Connect-Community im Lauf der Zeit angezeigt wurde • Nutzer (in %), die Feedback für die IP-Adresse übermittelt haben. • Nutzer (in %), von denen die IP-Adresse im Lauf der Zeit als „Unsicher“ markiert wurde

Feld	Beschreibung
Risikoindikatoren	 Risikoindikatoren werden basierend auf den Tags hervorgehoben, die den Entitäten (IPs, Dateien oder Domains) von der Community zugewiesen werden. Die Tags sind wie folgt kategorisiert: Aufklärung, Lieferung, Befehl und Kontrolle, Laterale Bewegung, Rechteerweiterung, Verpackung und Exfiltration. Diese Tags sind Muster und variieren je nach den Eingaben aus der Community, die auf dem Live Connect-Server eingehen. Der Analyst kann die entsprechenden Risikoindikatortags auswählen, während er Prüfungsfeedback verfasst. Hervorgehobene Tags bedeuten, dass die ausgewählte Entität der betreffenden Kategorie und dem betreffenden Tag zugeordnet ist. Durch Klicken auf ein hervorgehobenes Tag können Sie die Beschreibung des Tags einsehen.
Identität	Zeigt die folgenden Identitätsinformationen für die ausgewählte Entität bzw. den ausgewählten Metawert an: Für IP-Adressen: Autonomous System Nummer (ASN), Präfix, Ländercode und Name des Landes, Registrierter Nutzer (Organisation) und Datum. Für Datei-Hashes: Dateiname, Dateigröße, MD5, SH1, SH256, Kompilierzeit und MIME-Typ. Für Domains: Domainname und Zugeordnete IP-Adresse.
Zertifikatinformationen	Zeigt die folgenden Zertifikatinformationen für den ausgewählten Datei-Hash an Aussteller des Zertifikats, Gültigkeit des Zertifikats, Signaturalgorithmus und Seriennummer des Zertifikats.

Feld	Beschreibung
WHOIS-Informationen	 Die **WHO IS**-Informationen geben Details bezüglich des Eigentümers einer bestimmten Domain an. Die folgenden Informationen zum Domaineigentümer werden angezeigt: Erstellungsdatum, Aktualisierungsdatum, Ablaufdatum, Typ (Registrierungstyp), Name, Organisation, Adresse mit Postleitzahl, Land, Telefon, Fax und E-Mail.
Verwandte Dateien	Verwandte Dateien werden für Entitäten der Typen „IP“ und „Domain“ angezeigt. Eine Liste der bekannten zugehörigen Dateien wird zusammen mit den folgenden Informationen angezeigt: Live Connect-Risikorating (Sicher, Riskant und Unbekannt), Dateiname, MD5, Kompilierzeit und Kompilierdatum, Import-Hash der API-Funktion und MIME-Typ.
Verwandte Domains	Verwandte Domains werden für Entitäten der Typen „IP“ und „Dateien“ angezeigt. Eine Liste der bekannten zugehörigen Domains wird zusammen mit den folgenden Informationen angezeigt: Live Connect-Risikorating (Sicher, Riskant und Unbekannt), Domainname, Name des Landes, Registrierungsdatum, Ablaufdatum und E-Mail-Adresse des Registranten.

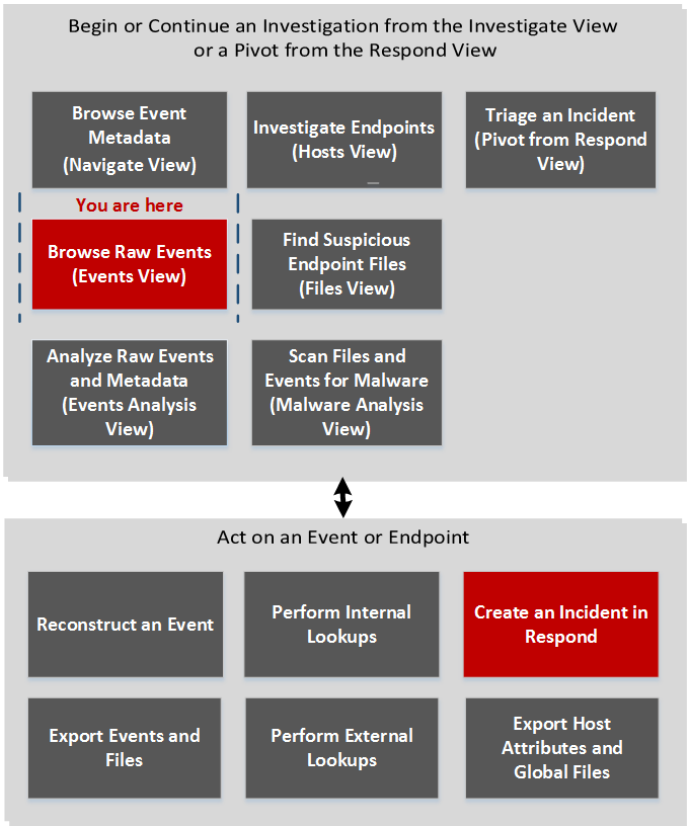
Feld	Beschreibung
Verwandte IPs	 Zugehörige IPs werden für Einheitentypen-Domain und -Dateien angezeigt. Eine Liste der bekannten zugehörigen IPs wird zusammen mit den folgenden Informationen angezeigt: Live Connect-Risikorating (Sicher, Riskant und Unbekannt), IP-Adresse, Domainname, Ländercode und Name des Landes, Registrierungsdatum, Ablaufdatum und E-Mail-Adresse des Registranten.

Dialogfeld „Incident erstellen“

In dem Dialogfeld „Incident erstellen“ können Analysten einen Incident aus ausgewählten Ereignissen in der Ansicht „Ereignisse“ erstellen. Der Incident ist dann für Incident-Experten verfügbar, die in Respond arbeiten.

Zugreifen können Sie auf dieses Dialogfeld wie folgt: Klicken Sie während der Untersuchung eines Service in der Investigation-Ansicht „Ereignisse“ auf der Symbolleiste auf **Incidents > Neuen Incident erstellen**.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“

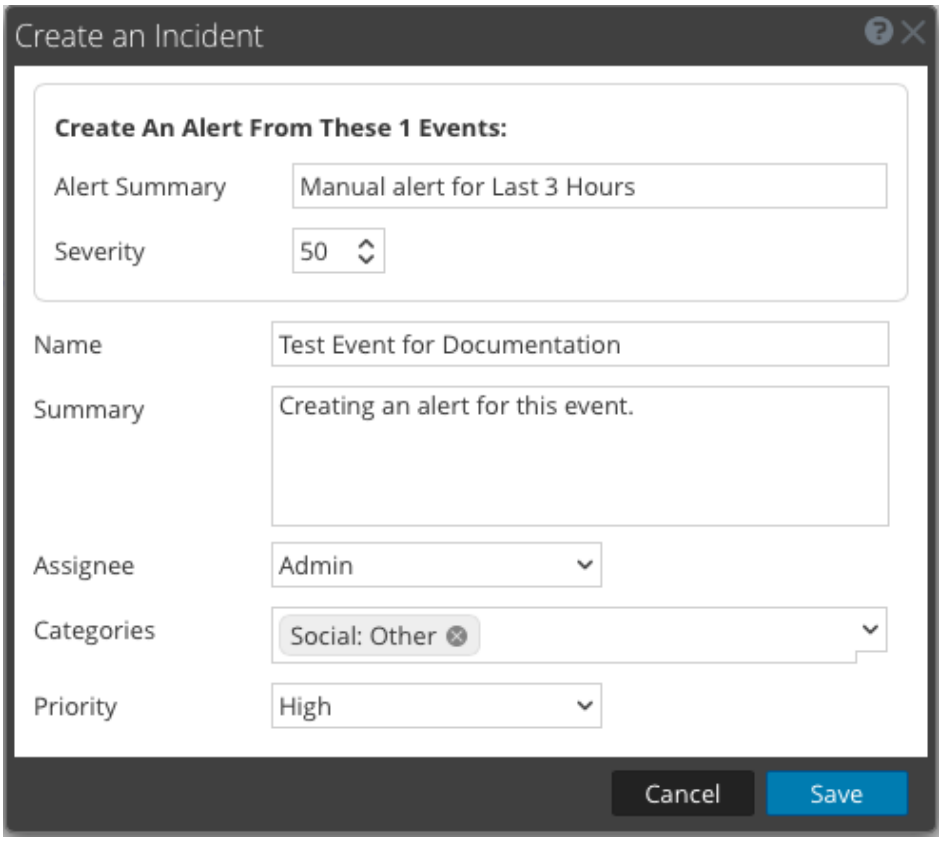
Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter oder Incident Responder	Ein oder mehrere Ereignisse zu einem vorhandenen Incident oder einem neuen Incident hinzufügen*	Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Navigation“
- Ansicht „Ereignisse“

Überblick

Die folgende Abbildung zeigt ein Beispiel für das Dialogfeld „Incident erstellen“. Die entsprechenden Funktionen werden in der Tabelle beschrieben.



Funktion	Beschreibung
Erstellen einer Zusammenfassung aus diesen Ereignissen	Das Feld „Warnmeldungszusammenfassung“ wird von der Abfrage ausgefüllt, die die ausgewählten Warnmeldungen produziert hat, die Sie ausgewählt haben, um diesen Incident zu erstellen. Das Feld „Schweregrad“ zeigt den Schweregrad der ausgewählten Warnmeldung an, eine Ganzzahl zwischen 1 und 100.
Name	(Erforderlich) Gibt einen Namen an, um den Incident zu identifizieren. In diesem Beispiel lautet der Name „Sample Incident“. Sie können einen Namen angeben, der deutlich die Art der Ereignisse identifiziert, die diesem Incident hinzugefügt werden.
Zusammenfassung	(Optional) Gibt eine Beschreibung für den Incident an. Eine gute Zusammenfassung identifiziert den Incident deutlich für andere Analysten und Experten.
Zuweisungsempfänger	(Optional) Weist den Incident einem Nutzer im SOC zu. Durch Klicken auf „Zuweisungsempfänger“ wird eine Drop-down-Liste mit den Namen von SOC-Mitarbeitern geöffnet, die auf Incidents reagieren.
Kategorien	(Optional) Identifiziert Kategorien von Incidents. Durch Klicken auf „Kategorien“ wird eine Drop-down-Liste von Incident-Kategorien und -Unterkategorien geöffnet. Sie können mindestens eine Kategorie auswählen, mit der der Incident verknüpft ist. Kategorien fallen in diese Hauptgruppen: Umgebung, Fehler, Hacking, Malware, Missbrauch und Social Media.

Funktion	Beschreibung
Priorität	Identifiziert die Priorität des Incident. Durch Klicken auf „Priorität“ öffnet sich eine Drop-down-Liste der Prioritäten: „Kritisch“, „Hoch“, „Mittel“ oder „Niedrig“ werden in der Drop-down-Liste angezeigt.
Abbrechen	Schließt das Dialogfeld, ohne die Änderungen zu speichern.
Speichern	Der Incident wird gespeichert und das Dialogfeld wird geschlossen. Eine Meldung bestätigt, dass der Incident erfolgreich erstellt wurde.

Ansicht „Ereignisanalyse“

In der Ansicht „Ereignisanalyse“ können Analysten Raw-Ereignisse und Metadaten mit interaktiven Funktionen anzeigen, die ihnen helfen, bedeutsame Datenmuster zu identifizieren. Diese Ansicht ist eine Alternative zur statischen Ansicht „Ereignisrekonstruktion“. Sie können Netzwerk-, Protokoll- und Endpunktereignisse in der Ansicht „Ereignisanalyse“ untersuchen. Die Ansicht „Ereignisanalyse“ bietet Paket-, Text und Protokollrekonstruktion und unterstützt keine direkte E-Mail- und Webrekonstruktion. In Version 11.1 und später können Sie jedoch eine E-Mail- oder Webrekonstruktion der aktuellen Ergebnisse in der e-Mail- oder Web Rekonstruktion der Ansicht „Ereignisse“ öffnen.

Hinweis: Der Administrator legt Berechtigungen für Analysten fest, um auf diese Ansicht zuzugreifen. Wenn Ihr Administrator Ihnen keinen Zugriff gewährt hat und Sie zur Ansicht „Ereignisanalyse“ navigieren, wird die folgende Meldung angezeigt: `Forbidden. You cannot access the requested page.` Wenn Sie z. B. eine Rekonstruktion der Ansicht „Ereignisse“ anzeigen und versuchen, dieselbe Rekonstruktion in der Ansicht „Ereignisanalyse“ anzuzeigen, sehen Sie die Meldung `Forbidden`.

Die in der Ansicht „Ereignisanalyse“ angezeigten Ereignisse sind für den aktuellen Drill-down-Punkt in der Ansicht „Navigation“ oder der Ansicht „Ereignisse“. Ab Version 11.1 können die Ereignisse die Ergebnisse einer Abfrage sein, die in der Brotkrümelnavigation der Ansicht „Ereignisanalyse“ eingegeben wurden. Woher die Abfrage auch immer stammt, in der Ansicht „Ereignisanalyse“ werden Ereignisse nach Zeit sortiert. Sie können die Spalten neu anordnen und ihre Größe ändern. Ab Version 11.1 können Sie auch die Spalten, die Sie sehen möchten, auswählen und eine der integrierten Spaltengruppen oder eine angepasste Spaltengruppe auswählen.

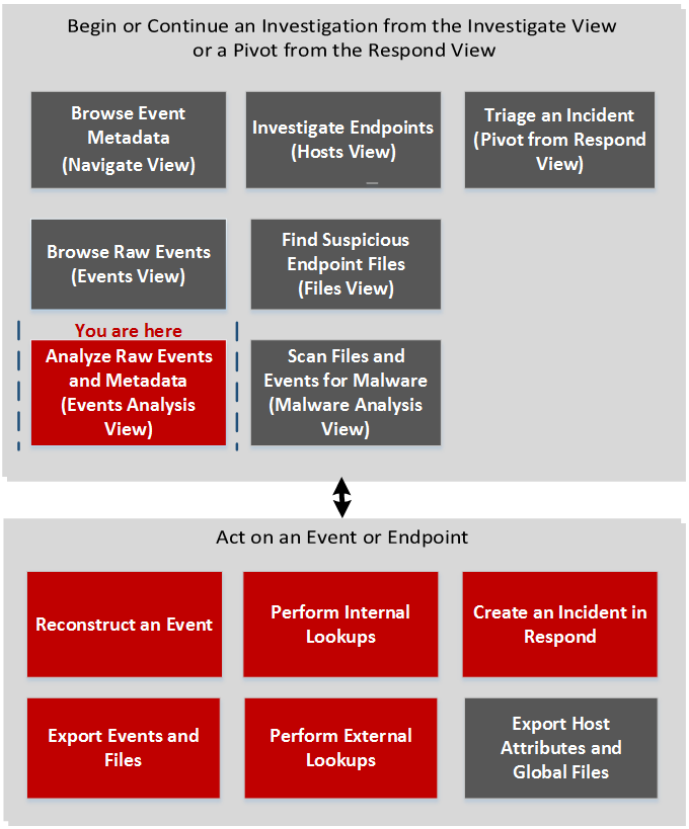
Wenn Sie auf ein Ereignis klicken, wird im selben Browserfenster entweder der Bereich „Netzwerkereignisdetails“, der Bereich „Protokollereignisdetails“ oder der Bereich „Endpunktereignisdetails“ geöffnet. Für jeden Ereignistyp stehen ein oder mehrere Analysetypen zur Verfügung: Textanalyse, Paketanalyse und Dateianalyse.

Es gibt mehrere Zugriffspunkte auf diese Ansicht, die unter Starten einer Ermittlung in der Ansicht „Ereignisanalyse“ beschrieben werden.

Hinweis: Wenn Sie über die Ansicht „Reagieren“ auf die Ereignisanalyse zugreifen, wird die Ereignisanalyse für ein ausgewähltes Ereignis in einem Incident angezeigt. Bei den verfügbaren Optionen handelt es sich um eine Auswahl der Optionen, die Ihnen zur Verfügung stehen, wenn Sie ein Ereignis aus der Ansicht „Untersuchen“ heraus öffnen. Um Zugriff auf den vollen Funktionsumfang zu erhalten und andere Ereignisse untersuchen zu können, rufen Sie die Ansicht „Ereignisanalyse“ direkt auf (Untersuchen > Ereignisanalyse).

Workflow

Die folgende Abbildung zeigt einen allgemeinen Workflow, der die Aufgaben veranschaulicht, die Sie in NetWitness Investigate durchführen können, wobei die Aufgaben der Ansicht „Ereignisanalyse“ rot hervorgehoben sind.



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten*	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Ereignisanalyse“ (Version 11.1)*	Filtern von Ergebnissen in der Ansicht „Ereignisanalyse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“*	Herunterladen von Daten in der Ansicht „Ereignisanalyse“
Threat Hunter	Rekonstruktion von Ereignissen in der Ansicht „Ereignisanalyse“*	Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Durchführen externer Suchen von der Ansicht „Ereignisanalyse“ aus (Version 11.1)*	Reagieren auf Daten in der Ansicht „Ereignisanalyse“
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Navigation“	Untersuchen von Metadaten in der Ansicht „Navigation“
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Ereignisse“	Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Ereignisanalyse“ – Bereich „Paketanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Textanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Dateianalyse“

Überblick

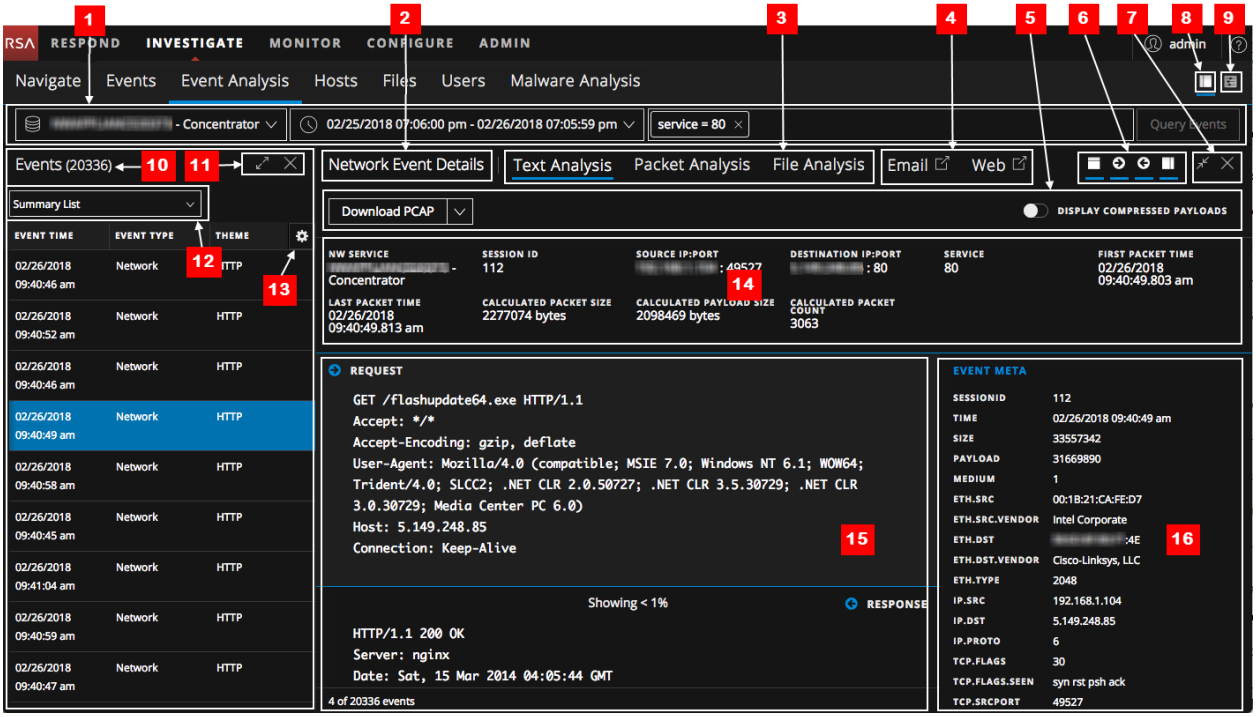
Wenn Sie „Untersuchen“ zum ersten Mal öffnen, werden die Eingabefelder für eine Abfrage angezeigt, damit Sie einen Service und Zeitbereich auswählen und eine optionale Abfrage eingeben können.

- Version 11.0 hat die Eingabefelder in den Ansichten „Navigation“ und „Ereignisse“.
- Version 11.1 hat die Eingabefelder in den Ansichten „Navigation“, „Ereignisse“ und „Ereignisanalyse“.

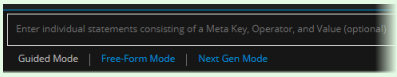
Sobald Sie einen Drill-down-Punkt in der Ansicht „Ereignisanalyse“ öffnen, zählt der untersuchte Service die Ergebnisse der ersten Abfrage bis zu einem Limit von 100.000 Ereignissen. Die ersten 100 Ereignisse (Pakete, Protokolle und Endpunkte) werden in den Bereich „Ereignisse“ geladen. Die Spalten im Bereich „Ereignisse“ sind Ereigniszeit, Ereignistyp (Netzwerk, Protokoll oder Endpunkt), Ereignisgröße und Übersicht. Sie können Folgendes tun:

- Blättern Sie durch die Liste und klicken Sie auf **Weitere laden**, um die nächsten 100 Ereignisse anzuzeigen.
- Wählen Sie eine Spaltengruppe aus (Version 11.1 und später).
- Wählen Sie die Spalten aus, die enthalten sein sollen (Version 11.1 und später).
- Ziehen Sie die Spalten, um die Reihenfolge zu ändern.
- die Spaltenbreite anpassen.
- die Ereignisanalyse eines Ereignisses anzeigen.

In der folgenden Abbildung sind die wichtigsten Funktionen der Ansicht „Ereignisanalyse“ für Version 11.1 und später hervorgehoben.

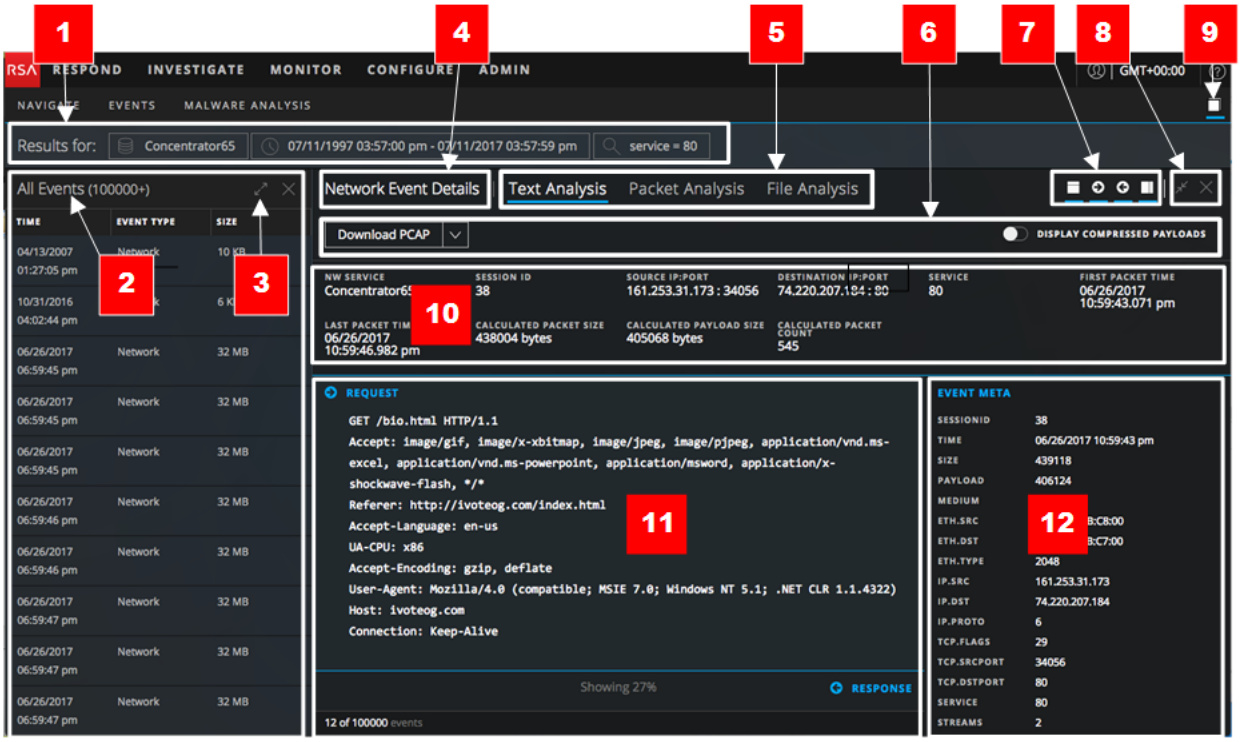


Hinweis: Die Version 11.2 enthielt eine undokumentierte Beta-Funktion, den sogenannten NextGen-Modus, in der Abfrageerstellung der Ansicht „Ereignisanalyse“, der noch entwickelt und getestet wurde. Der NextGen-Modus wurde mit dem Patch 11.2.0.1 deaktiviert. Wenn der NextGen-Modus angezeigt wird, sollten Sie ihn nicht verwenden. Verwenden Sie stattdessen nur den geleiteten Modus und den Freitextmodus in der Abfrageerstellung, damit Sie konsistente und vorhersehbare Ergebnisse erzielen.



1	**Interaktive Brotkrümelnavigation**: Wenn ein Service ausgewählt wird, werden die Serviceauswahl, Zeitbereichsauswahl und die eingegebenen Abfragen angezeigt. In Version 11.1 und später können Sie einen Service auswählen, wie in Starten einer Ermittlung in der Ansicht „Ereignisanalyse“ beschrieben, und die Abfrage verfeinern, wie in Filtern von Ergebnissen in der Ansicht „Ereignisanalyse“ beschrieben. Durch Klicken auf die Schaltfläche **Abfrage senden** wird die Abfrage gesendet und es wird eine Anforderung an den ausgewählten Service gesendet, die Daten zu laden.
2	An der Überschrift können Sie erkennen, welcher Typ Ereignis analysiert wird: **Netzwerkereignisdetails**, **Protokollereignisdetails** oder **Endpunktereignisdetails**. Jede Ansicht wird unter Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“ ausführlich erläutert.
3	Verfügbare Analysetypen für den betreffenden Ereignistyp. Für Netzwerkereignisse können alle Analysetypen durchgeführt werden: „Textanalyse“, „Paketanalyse“ und „Dateianalyse“. Für Protokoll- und Endpunktereignisse wird nur der Typ „Textanalyse“ unterstützt.
4	Die Typen E-Mail- und Webanalyse öffnen das aktuelle Ereignis als eine E-Mail- oder Webrekonstruktion in der Ansicht „Ereignisse“.
5	Diese Optionen variieren je nach Analysetyp. Sie werden unter Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“ ausführlich erläutert.
6	Steuerelemente zum Ein- und Ausblenden des Ereignis-Headers, zum Ein- und Ausblenden von Anforderungen und Antworten sowie zum Öffnen des Bereichs „Ereignis-Metadaten“ (16). Die Steuerelemente werden in Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“ beschrieben.
7, 11	Steuerelemente zum Anpassen der Bereichsgröße sowie zum Schließen des Bereichs
8	Öffnet den Bereich „Ereignisse“ oder den Bereich „Ereignis-Metadaten“ erneut, falls sie geschlossen wurden.
9	Legt Einstellungen für die Ansicht „Ereignisanalyse“ fest (siehe Konfigurieren der Ansicht „Ereignisanalyse“).
10	Der Bereich „Ereignisse“ für Version 11.1 ist interaktiv und zeigt Abfrageergebnisse an, während Sie aktualisierte Abfragen senden. Der Bereich „Ereignisse“ enthält die Gesamtanzahl der Ereignisse. Reihenfolge und Breite der Spalten lassen sich anpassen. Sie können bis zum Ende der Liste scrollen und dort weitere Ereignisse laden (siehe Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“).
12	Die Drop-down-Liste „Spaltengruppe“ listet integrierte und benutzerdefinierte Spaltengruppen auf, die Sie auf den Bereich „Ereignisse“ anwenden können. Die integrierten Spaltengruppen sind E-Mail-Analyse, Endpunktanalyse, Malware Analysis, Ausgehendes HTTP, Ausgehendes SSL/TLS und Übersichtsliste. Übersichtsliste ist die Standardspaltengruppe.
13	Einstellungen zur Auswahl der Spalten, die im Bereich „Ereignisse“ enthalten sind.
14	Der Ereignis-Header bietet Übersichtsinformationen zu dem Ereignis. Welche Informationen angezeigt werden, variiert je nach Ereignistyp (Paket, Protokoll oder Endpunkt).
15	Die Ereignisdaten (bei Paketen gelegentlich als Paylod/Nutzlast bezeichnet). Bei den Ereignisdaten eines Protokollereignisses oder eines Endpunktereignisses handelt es sich in der Regel um eine Textzeile aus dem Rohprotokoll. Für Paketereignissen werden die Anforderung und die zugehörige Antwort angezeigt.
16	Im Bereich Bereich „Ereignis-Metadaten“ werden die Metaschlüssel und Metawerte aufgelistet, die in den Daten gefunden wurden. Einige Metadaten können durchsucht werden; sie sind mit einem Fernglas-Symbol gekennzeichnet. Wenn Sie auf dieses Symbol klicken, werden die zugehörigen Daten in den Ereignisdaten hervorgehoben (siehe Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“).

In der folgenden Abbildung sind die wichtigsten Funktionen der Ansicht „Ereignisanalyse“ für Version 11.0.0.x hervorgehoben.



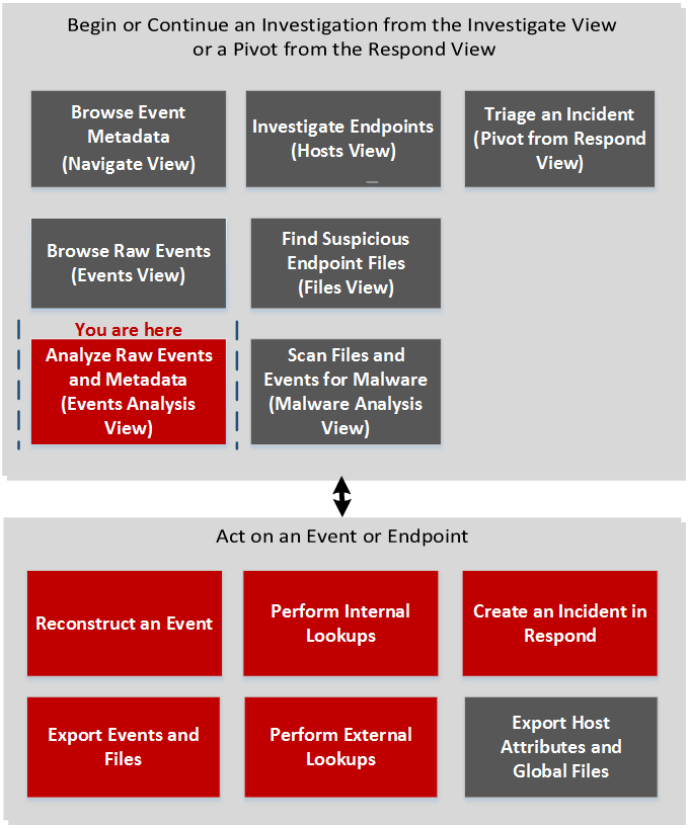
1	Die schreibgeschützte Brotkrümelnavigation zeigt den ausgewählten Service, den Zeitbereich und die Abfrage an, die in den Ansichten „Navigation“ und „Ereignisse“ eingegeben wurden.
2	Eine schreibgeschützte Liste aller Ereignisse, zusammengestellt auf Basis der Abfrage aus der Ansicht „Navigation“ oder der Ansicht „Ereignisse“. Der Bereich „Ereignisse“ enthält die Gesamtanzahl der Ereignisse. Reihenfolge und Breite der Spalten lassen sich anpassen. Sie können bis zum Ende der Liste scrollen und dort weitere Ereignisse laden (siehe Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“).
3, 8	Steuerelemente zum Anpassen der Bereichsgröße sowie zum Schließen des Bereichs
4	An der Überschrift können Sie erkennen, welcher Typ Ereignis analysiert wird: Netzwerkereignisdetails, Protokollereignisdetails oder Endpunktereignisdetails. Jede Ansicht wird unter Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“ ausführlich erläutert.
5	Verfügbare Analysetypen für den betreffenden Ereignistyp. Für Netzwerkereignisse können alle drei Analysetypen durchgeführt werden: „Textanalyse“, „Paketanalyse“ und „Dateianalyse“. Für Protokoll- und Endpunktereignisse wird nur der Typ „Textanalyse“ unterstützt.
6	Diese Optionen variieren je nach Analysetyp. Sie werden unter Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“ ausführlich erläutert.
7	Steuerelemente zum Ein- und Ausblenden des Ereignis-Headers, zum Ein- und Ausblenden von Anforderungen und Antworten sowie zum Öffnen des Bereichs „Ereignis-Metadaten“ (12). Die Steuerelemente werden in Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“ beschrieben.
9	Öffnet den Bereich „Ereignisse“ oder den Bereich „Ereignis-Metadaten“ erneut, falls sie geschlossen wurden.
10	Der Ereignis-Header bietet Übersichtsinformationen zu dem Ereignis. Welche Informationen angezeigt werden, variiert je nach Ereignistyp (Paket, Protokoll oder Endpunkt).

11	Die Ereignisdaten (bei Paketen gelegentlich als Paylod/Nutzlast bezeichnet). Bei den Ereignisdaten eines Protokollereignisses oder eines Endpunktereignisses handelt es sich in der Regel um eine Textzeile aus dem Rohprotokoll. Für Paketereignissen werden die Anforderung und die zugehörige Antwort angezeigt.
12	Im Bereich Bereich „Ereignis-Metadaten“ werden die Metaschlüssel und Metawerte aufgelistet, die in den Daten gefunden wurden. Einige Metadaten können durchsucht werden; sie sind mit einem Fernglas-Symbol gekennzeichnet. Wenn Sie auf dieses Symbol klicken, werden die zugehörigen Daten in den Ereignisdaten hervorgehoben (siehe Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“).

Ansicht „Ereignisanalyse“ – Bereich „Dateianalyse“

Im Bereich Dateianalyse (**Ereignisanalyse** > **Dateianalyse)** können Sie ohne Sicherheitsrisiko eine Liste aller Dateien einsehen und eine oder mehrere Dateien aus einem Ereignis herunterladen.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Ereignisanalyse“ (Version 11.1)	Filtern von Ergebnissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“*	Herunterladen von Daten in der Ansicht „Ereignisanalyse“
Threat Hunter	Rekonstruktion von Ereignissen in der Ansicht „Ereignisanalyse“	Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Durchführen externer Suchen von der Ansicht „Ereignisanalyse“ aus (Version 11.1)	Reagieren auf Daten in der Ansicht „Ereignisanalyse“
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Navigation“	Untersuchen von Metadaten in der Ansicht „Navigation“
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Ereignisse“	Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

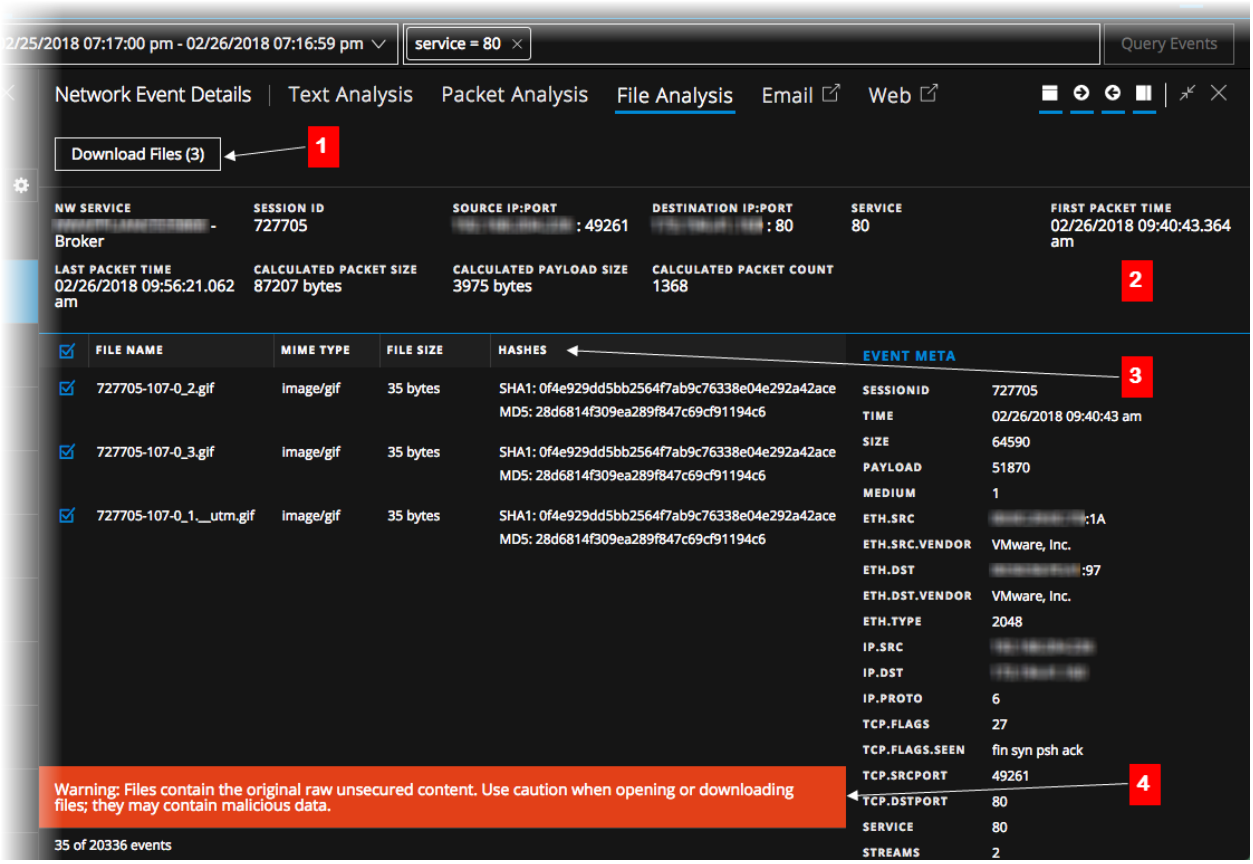
- Wie funktioniert NetWitness Investigate?
- Ansicht „Ereignisanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Textanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Paketanalyse“

Überblick

Im Bereich „Dateianalyse“ finden Sie eine Liste aller Dateien, die einem Netzwerkereignis zugeordnet sind. Sie können die Dateien in dieser Ansicht herunterladen.

Es folgt ein Beispiel des Bereichs „Dateianalyse“ mit beschrifteten Funktionen.

Hinweis: Die E-Mail- und Webrekonstruktionstypen am oberen Rand der Abbildung sind in Version 11.1 und später verfügbar.

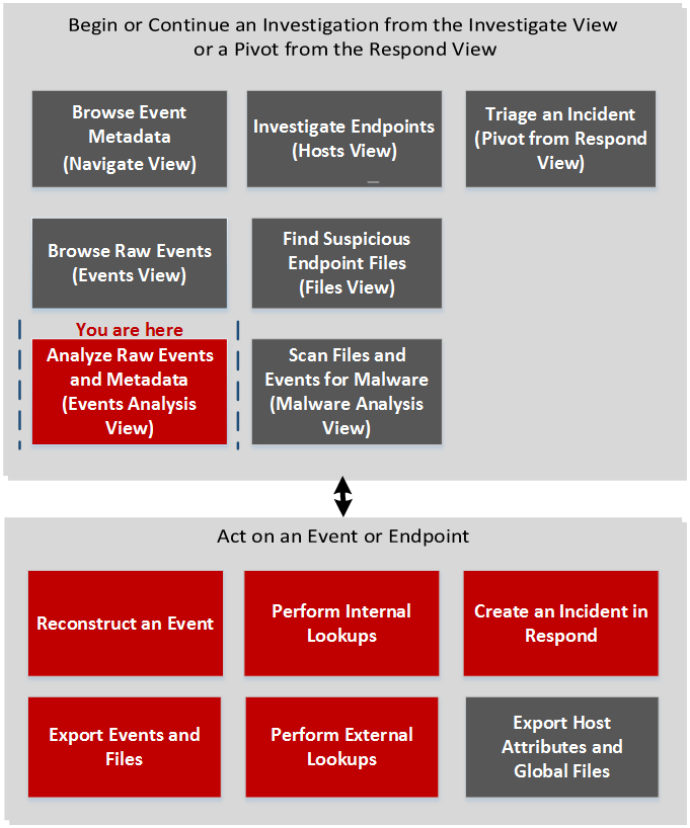


1	Klicken Sie auf diese Schaltfläche, um eine oder mehrere ausgewählte Dateien herunterzuladen.
2	Im Ereignis-Header sind Übersichtsinformationen zu dem Netzwerkereignis aufgeführt, das die Dateien enthält.
3	Scrollbare Liste mit allen dem Ereignis zugeordneten Dateien, die sich jeweils auswählen und herunterladen lassen
4	Erinnerung, beim Herunterladen potenziell schädlicher Dateien Vorsicht walten zu lassen

Ansicht „Ereignisanalyse“ – Bereich „Paketanalyse“

Im Bereich Paketanalyse (**Ereignisanalyse > Paketanalyse**) können Sie ohne Sicherheitsrisiko die Pakete und die Nutzlast eines Ereignisses anzeigen und interaktiv analysieren.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Ereignisanalyse“ (Version 11.1)	Filtern von Ergebnissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“*	Herunterladen von Daten in der Ansicht „Ereignisanalyse“
Threat Hunter	Rekonstruktion von Ereignissen in der Ansicht „Ereignisanalyse“*	Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Durchführen externer Suchen über die Ansicht „Ereignisanalyse“ (Version 11.1)*	Reagieren auf Daten in der Ansicht „Ereignisanalyse“
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Navigation“	Untersuchen von Metadaten in der Ansicht „Navigation“
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Ereignisse“	Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*

* Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Ereignisanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Textanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Dateianalyse“

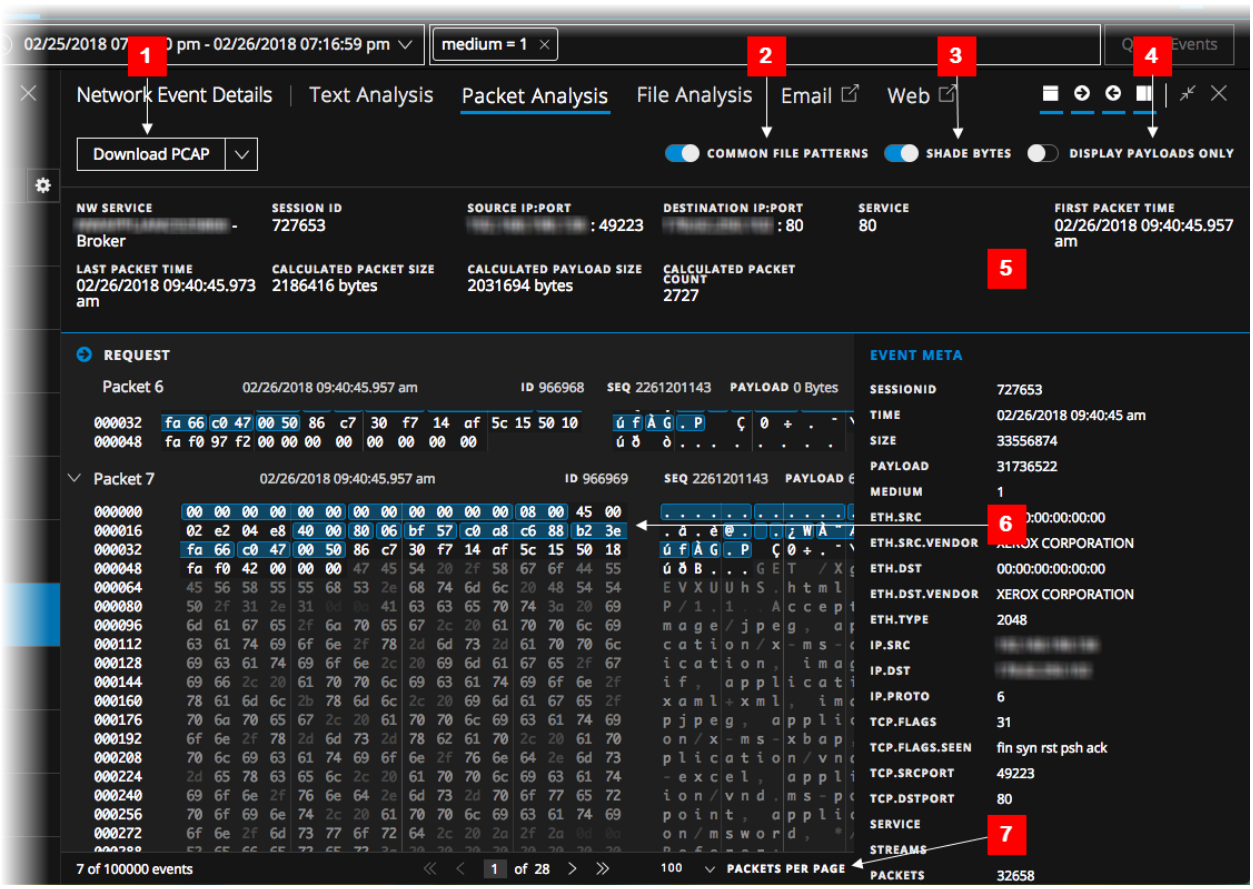
Überblick

Im Bereich Paketanalyse können ausschließlich Netzwerkereignisse analysiert werden. Im Bereich Paketanalyse werden alle Pakete in einem Ereignis aufgeführt. Die Paketliste ist scrollbar. Wenn Sie scrollen, bleiben die Informationen zur Identifizierung des Pakets oder des Texts ebenso sichtbar wie die Anforderungs- und Antwortbezeichnungen. Sie verschwinden beim Scrollen also nicht aus dem sichtbaren Bereich.

Ab Version 11.1 können Sie mithilfe von Seitenumbruchshilfen vor und zurück durch die Seiten wechseln, zu einer bestimmten Seite navigieren und die Anzahl der Pakete auswählen, die pro Seite angezeigt werden (100, 300 oder 500).

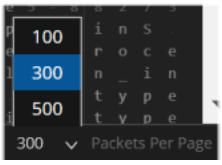
Jedes Paket wird mit Schattierungen und Hervorhebungen angezeigt, anhand derer Sie häufige Dateimuster erkennen können: wichtige Header- und Nutzlastbytes, hexadezimale Bytes und ASCII-Bytes sowie häufig vorkommende Dateisignaturen. Darüber hinaus können Sie anpassen, wie Anforderungen und Antworten angezeigt werden sollen, und die Paketzusammenfassung ein- oder ausblenden.

Es folgt ein Beispiel des Bereichs „Paketanalyse“ mit Bezeichnungen zur Erkennung von Funktionen. Weitere Informationen und Beispiele für jede Funktion finden Sie unter Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“.



1 Optionen zum Exportieren eines Netzwerkereignisses. Sie können zwecks eingehenderer Analyse oder Weiterleitung an Dritte wahlweise eine PCAP-Datei, alle Nutzlasten, Anforderungsnutzlasten oder Antwortnutzlasten exportieren.

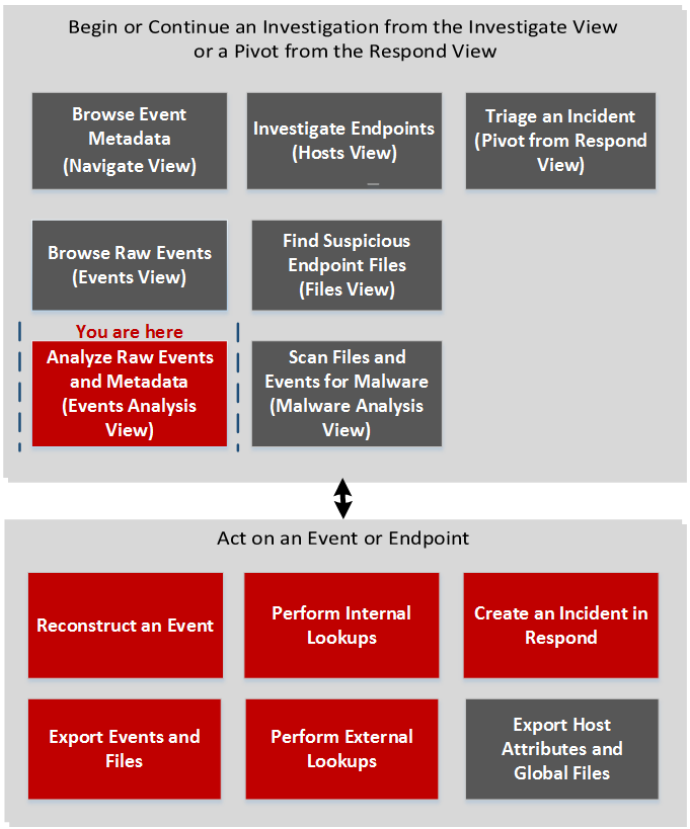
2 Die Option zur Identifizierung häufig vorkommender Dateisignaturen ist standardmäßig aktiviert.

	Häufig vorkommende Dateisignaturen sind orangefarben hervorgehoben. Wenn Sie den Mauszeiger auf einer Hervorhebung platzieren, wird der Dateityp angezeigt.
3	Über die Option „Byte schattieren“ wird eine Schattierung hinzugefügt. Die unterschiedlichen Hexadezimalbytes (00 bis FF) werden dann verschieden stark hervorgehoben.
4	Mit der Option „Nur Nutzdaten anzeigen“ können Sie die Paket-Header ausblenden. So ist auf dem Bildschirm mehr Platz für die Nutzlast.
5	Ereignis-Header
6	Wichtige Bytes werden blau hinterlegt. Wenn Sie den Mauszeiger auf einer Hervorhebung platzieren, werden die Metadaten in einem Pop-up-Feld angezeigt.
7	(Ab Version 11.1) Paket-Seitenumbruchshilfen ermöglichen mehr Flexibilität beim Blättern durch eine Liste von Paketen. Wenn ein Steuerelement nicht verfügbar ist, wird das Bild abgeblendet; wenn Sie z. B. die Seite 1 anzeigen, sind die Steuerelemente ⟪ und ⟨ abgeblendet. ⟪: Gehe zur ersten Seite ⟨: Gehe zur vorherigen Seite 1 of 206: Gehe zu spezifischer Seite ⟩: Gehe zur nächsten Seite ⟫: Gehe zur letzten Seite  : Wählen Sie die Anzahl der Pakete pro Seite aus

Ansicht „Ereignisanalyse“ – Bereich „Textanalyse“

Im Bereich Textanalyse (**Ereignisanalyse > Textanalyse)** können Sie die Rohtextnutzdaten eines Ereignisses sicher anzeigen und analysieren. Der Bereich Textanalyse umfasst Funktionen, die dekomprimierten oder komprimierten Text anzeigen, abgeschnittene Einträge erweitern, URL- und Base64-Codierung und -Decodierung durchführen sowie Netzwerkereignisprotokolle und Endpunktereignisse herunterladen können. Der Bereich „Textanalyse“ ist für alle Arten von Ereignissen verfügbar: Netzwerk, Protokoll und Endpunkt.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Ereignisanalyse“ (Version 11.1)	Filtern von Ergebnissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“*	Herunterladen von Daten in der Ansicht „Ereignisanalyse“
Threat Hunter	Rekonstruktion von Ereignissen in der Ansicht „Ereignisanalyse“*	Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Durchführen externer Suchen von der Ansicht „Ereignisanalyse“ aus (Version 11.1)*	Reagieren auf Daten in der Ansicht „Ereignisanalyse“
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Navigation“	Untersuchen von Metadaten in der Ansicht „Navigation“
Threat Hunter	Abfragen von Ereignissen in der Ansicht „Ereignisse“	Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*

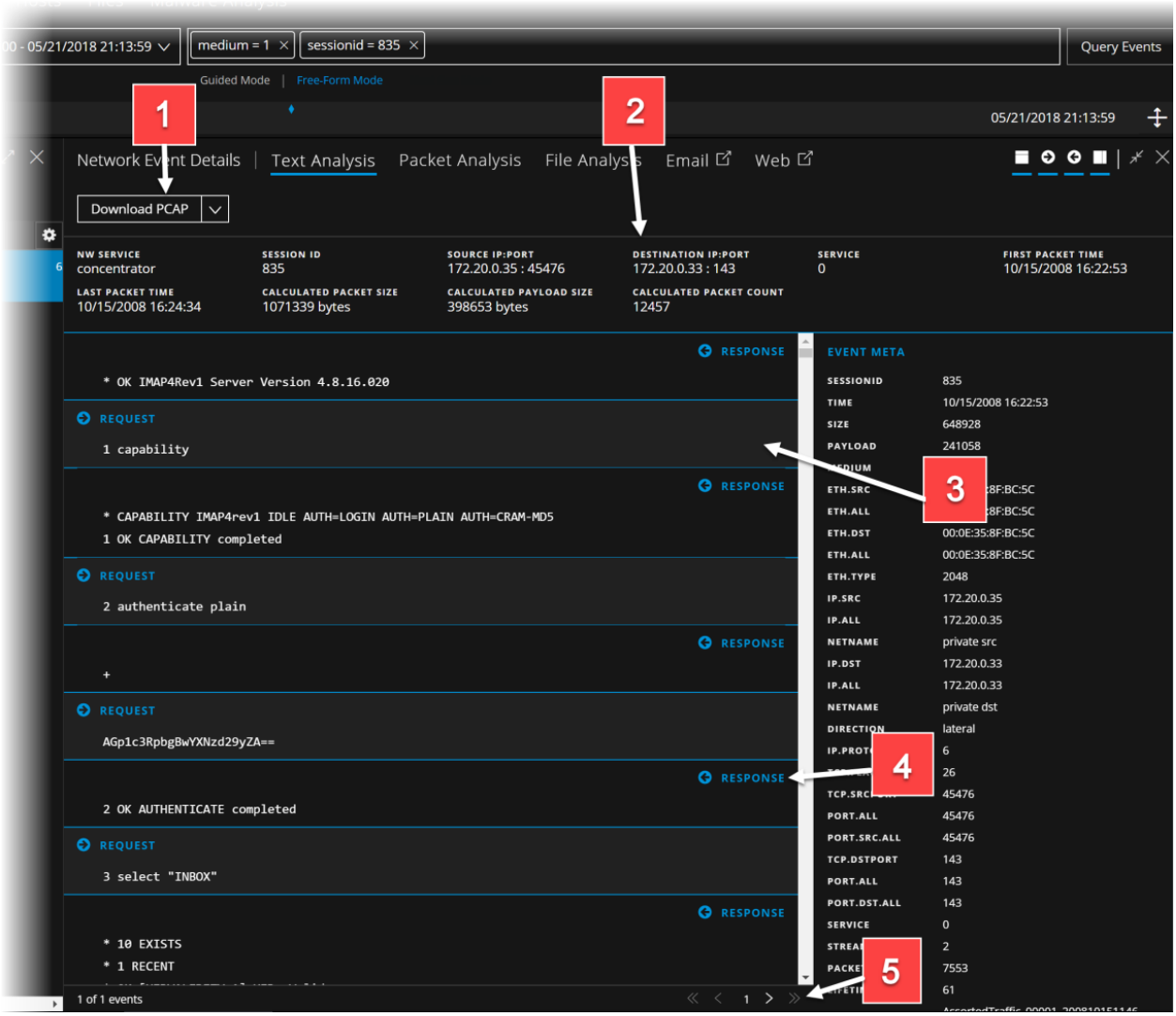
* Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Ereignisanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Paketanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Dateianalyse“

Überblick

Die Ansicht „Ereignisanalyse“ zeigt den Text eines einzelnen Ereignisses im Bereich Textanalyse an. Wenn Sie auf ein Ereignis im Bereich „Ereignisliste“ klicken, wird im angrenzenden Bereich die Textanalyse anzeigt. Nur das Rohdatenprotokoll für Protokollereignisse und Endpunktereignisse wird im Bereich Textanalyse angezeigt. Für Netzwerkereignisse werden die Richtung des Pakets (Anforderung oder Antwort) und die Inhalte jedes Pakets im Textformat bereitgestellt. Weitere Beispiele für Textanalyse finden Sie unter Analysieren von Raw-Ereignissen und Metadaten in der Ansicht „Ereignisanalyse“. Detaillierte Verfahren finden Sie unter Untersuchen von Ereignissen in der Ansicht „Ereignisanalyse“.



1	Optionen zum Exportieren eines Protokolls, einer PCAP-Datei oder von Dateien zur genaueren Analyse und zum Teilen mit anderen Dieses Download-Menü ist für Netzwerkdaten vorgesehen.
2	Die Ereignis-Header-Informationen.
3	Die Nutzdaten für ein Netzwerkereignis umfassen Anforderungen und Antworten. Dies ist der Anforderungsseite des Pakets.
4	Dies ist der Antwortseite des Pakets.

5 (ab Version 11.2) Ereignis-Seitenumbruchshilfen ermöglichen mehr Flexibilität beim Blättern durch eine Liste von Ereignissen. Wenn ein Steuerelement nicht verfügbar ist, wird das Bild abgeblendet; wenn Sie z. B. die Seite 1 anzeigen, sind die Steuerelemente und abgeblendet.

: Gehe zur ersten Seite

: Gehe zur vorherigen Seite

: Gehe zur nächsten Seite

: Gehe zur letzten Seite (Nur verfügbar, nachdem die letzte Seite bereits aufgerufen wurde.)

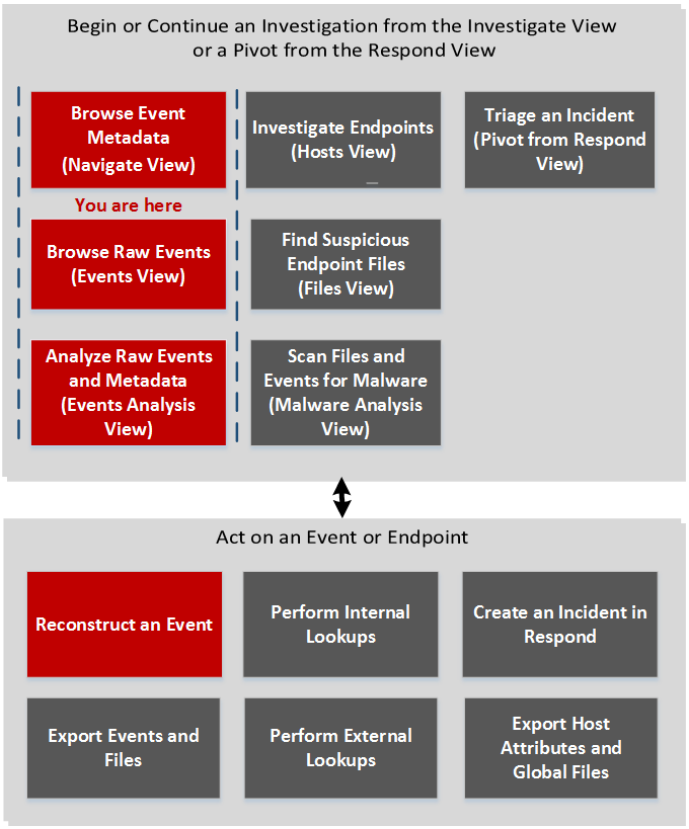
Ansicht „Ereignisrekonstruktion“

In der Ansicht „Ereignisrekonstruktion“ finden Sie eine Rekonstruktion eines ausgewählten Ereignisses aus der Ansicht „Ereignisse“. Standardmäßig wird inNetWitness Platform entweder die beste Rekonstruktion des Ereignisses auf Basis des Ereignisinhalts angezeigt oder die Standardrekonstruktion, die Sie in der Einstellung „Standardsitzungsansicht“ für das Modul „Investigation“ ausgewählt haben. Über die Optionen in der Symbolleiste der Ansicht „Ereignisrekonstruktion“ können Sie die Rekonstruktionsmethode ändern, Ergebnisse von oben nach unten oder nebeneinander anzeigen, die Anzeigeoptionen für Anforderungen und Antworten festlegen, Ereignisse exportieren, Metawerte exportieren, Dateien extrahieren, E-Mail-Anhänge öffnen und Ereignisse auf einer neuen Registerkarte öffnen.

Um auf diese Ansicht zuzugreifen, führen Sie einen der folgenden Schritte aus:

- Doppelklicken Sie in einer beliebigen Ereignisansicht auf ein Ereignis.
- Klicken Sie in der Ansicht „Ereignisse“ bei geöffneter Detailansicht mit der rechten Maustaste auf **Ereignisanalyse** am Ende des Ereignisses und wählen Sie **Ereignisrekonstruktion** aus.
- Klicken Sie in der Vorschau einer Rekonstruktion auf der „Ereignisrekonstruktion“-Symbolleiste auf **Ereignis in neuer Registerkarte öffnen**.
- Wählen Sie in der Ansicht „Navigation“ **Aktionen > In Ereignisrekonstruktion zu Ereignis wechseln** aus und geben Sie eine Ereignis-ID ein.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen

Nutzerrolle	Ziel	Details anzeigen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Rekonstruieren eines Ereignisses*	Rekonstruieren eines Ereignisses
Threat Hunter	Extrahieren von Dateien aus einem rekonstruierten Ereignis	Rekonstruieren eines Ereignisses

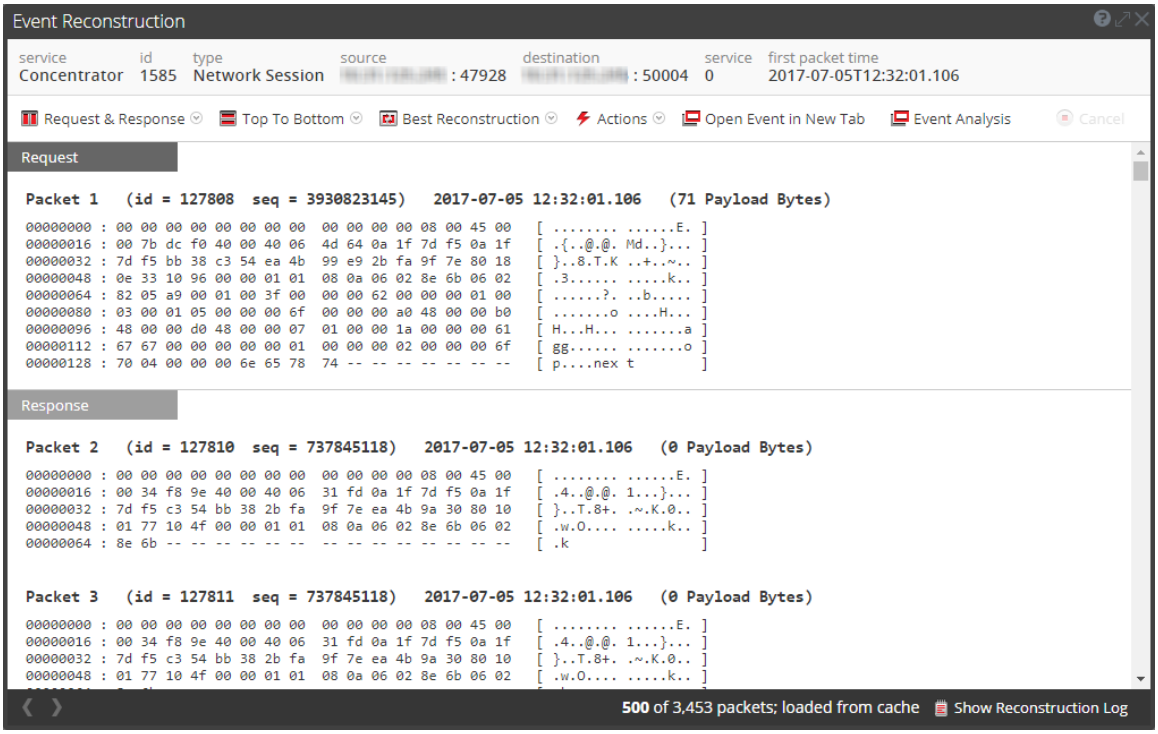
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Ereignisanalyse“

Überblick

Diese Abbildung zeigt ein Beispiel für die Ansicht „Ereignisrekonstruktion“. In der nachfolgenden Tabelle sind die Optionen auf der Symbolleiste beschrieben.



Funktion	Beschreibung
Anforderung und Antwort	Zeigt ein Drop-down-Menü an, in dem Sie auswählen können, was in der Ansicht angezeigt werden soll: • Anforderung und Antwort • Anforderung • Antwort
Organisation	Zeigt ein Drop-down-Menü an, um auszuwählen, ob die Informationen von oben nach unten oder nebeneinander angezeigt werden.
View	Zeigt ein Drop-down-Menü an, um auszuwählen, welche Informationen angezeigt werden. Standardmäßig ist Beste Rekonstruktion ausgewählt. Andere Optionen sind: • Metadaten anzeigen • Text anzeigen • Hex anzeigen • Pakete anzeigen • Web anzeigen • E-Mail anzeigen • Dateien anzeigen
Aktionen	Zeigt ein Drop-down-Menü mit den in der Ansicht „Ereignisrekonstruktion“ verfügbaren Aktionen an.
Ereignis in neuer Registerkarte öffnen	Öffnet das Ereignis in einer neuen Browserregisterkarte.

Unterhalb der Symbolleiste befindet sich eine Liste mit Metaschlüsseln und Werten. Einige Schlüssel stellen ein Drop-down-Menü mit verfügbaren Aktionen bereit.

Die Leiste unten in der Ansicht bietet mehrere Optionen.

Funktion	Beschreibung
	Zeigt das vorherige Ereignis an.
	Zeigt das nächste Ereignis an.
Rekonstruktionsprotokoll anzeigen	Zeigt das Rekonstruktionsprotokoll unten in der Ansicht an. Sobald Sie auf diese Schaltfläche klicken, wird sie in „Rekonstruktionsprotokoll ausblenden“ geändert.

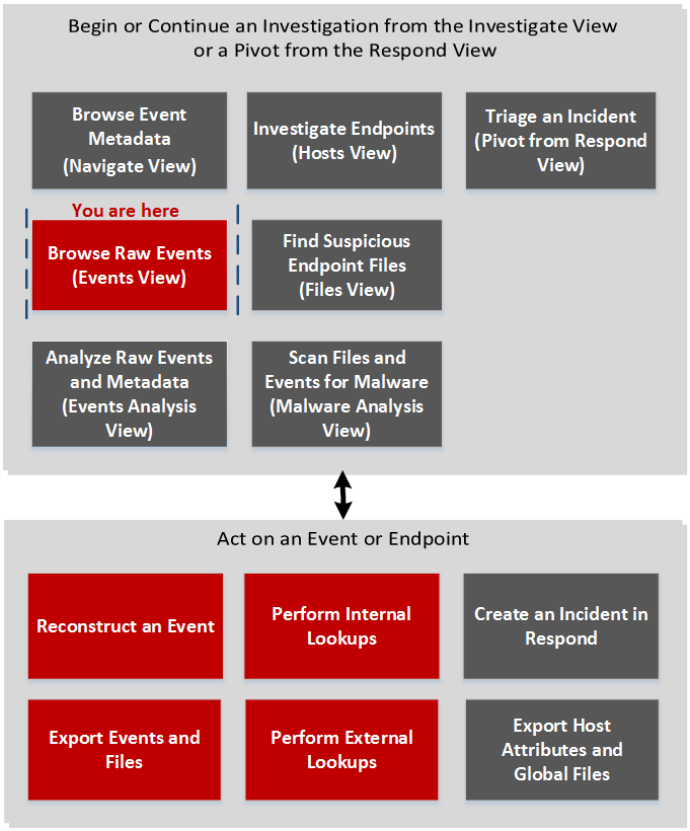
Ansicht „Ereignisse“

Im Ansicht „Ereignisse“ ist eine Liste der Ereignisse, die einer Sitzung zugeordnet ist verfügbar. Diese Ansicht ist optimiert, um Raw-Ereignisse zeitlich geordnet anzuzeigen. Sie können die Ereignisliste in verschiedenen Formen anzeigen, Ereignisse filtern, Ereignisse suchen und eine Rekonstruktion eines Ereignisses öffnen.

Es gibt zwei Möglichkeiten, die Ansicht Ereignisse anzuzeigen:

- Klicken Sie auf **UNTERSUCHEN > Ereignisse**. NetWitness Platform führt dann für den Standardservice (sofern festgelegt) eine Standardabfrage über die letzten drei Stunden aus oder öffnet ein Dialogfeld, in dem Sie einen Service auswählen können. Anschließend wird für diesen Service die Standardabfrage ausgeführt. Die Standardabfrage wählt alle Ereignisse aus und in der Ansicht „Ereignisse“ werden alle Ereignisse für den ausgewählten Service aufgeführt, beginnend mit den ältesten Ereignissen.
- Doppelklicken Sie in der Ansicht **Navigieren** auf ein Ereignis. In der Ansicht „Ereignisse“ werden nun die Ereignisse für den ausgewählten Service angezeigt, basierend auf dem Drill-down-Punkt in der Ansicht „Navigation“.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen*	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Nutzereinstellungen für die Ansicht „Ereignisse“ festlegen*	Konfigurieren der Ansichten „Navigation“ und „Ereignisse“
Threat Hunter	ein Ereignis rekonstruieren*	Rekonstruieren eines Ereignisses
Threat Hunter	Exportieren von Ereignissen und Dateien*	Exportieren von Ereignissen in der Ansicht „Ereignisse“
Threat Hunter	Durchführen interner Suchen	Suchen von weiteren Kontexten in den Ansichten „Navigation“ und „Ereignisse“
Threat Hunter	Durchführen externer Suchen	Starten einer externen Suche eines Metaschlüssels
Threat Hunter oder Incident Responder	Ein oder mehrere Ereignisse zu einem vorhandenen Incident oder einem neuen Incident hinzufügen*	Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Untersuchen von Raw-Ereignissen in der Ansicht „Ereignisse“

- Abfragen von und Reagieren auf Daten in den Ansichten „Navigation“ und „Ereignisse“

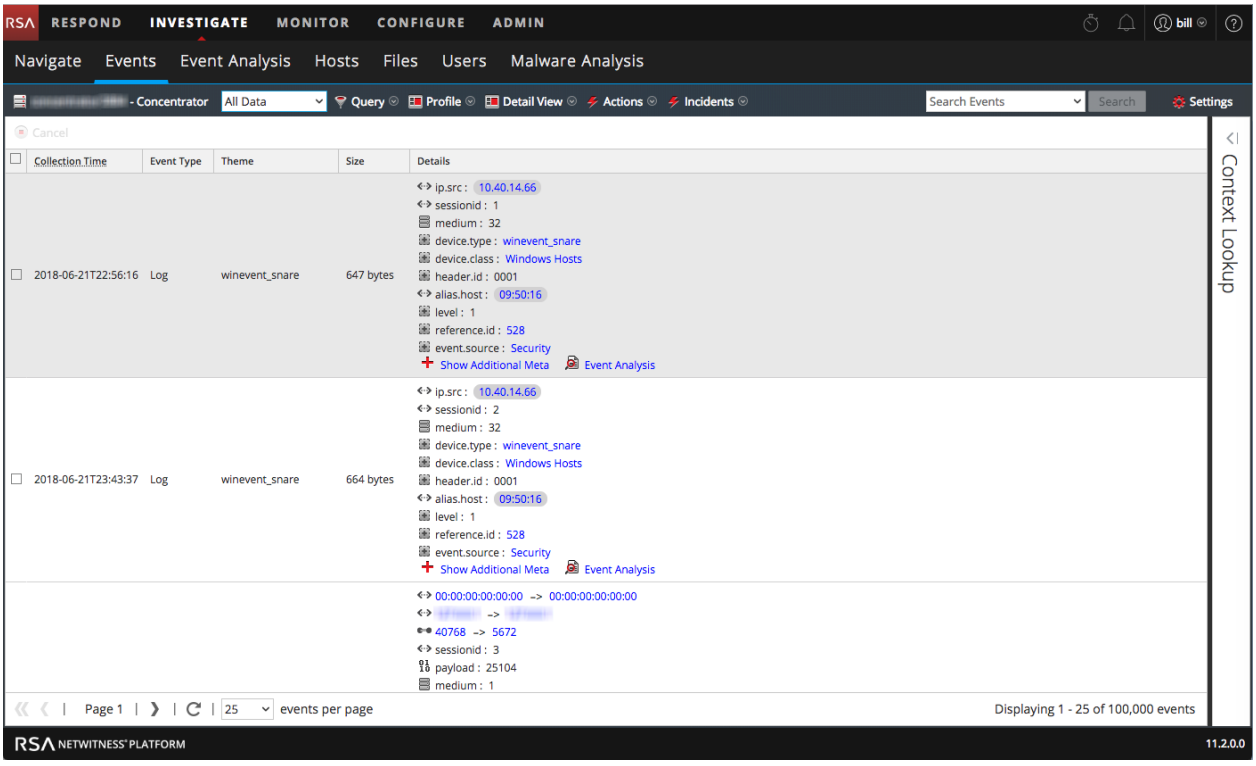
Überblick

Die Ansicht „Ereignisse“ bietet drei integrierte Darstellungsarten für Ereignisdaten: die Detailansicht, die Listenansicht und die Protokollansicht. Die Listenansicht und die Detailansicht dienen zur Anzeige von Ereignissen in Paketdaten und enthalten weitere Informationen für jedes Ereignis, darunter Zeitstempel, Ereignistyp, Ereignisthema und Größe.

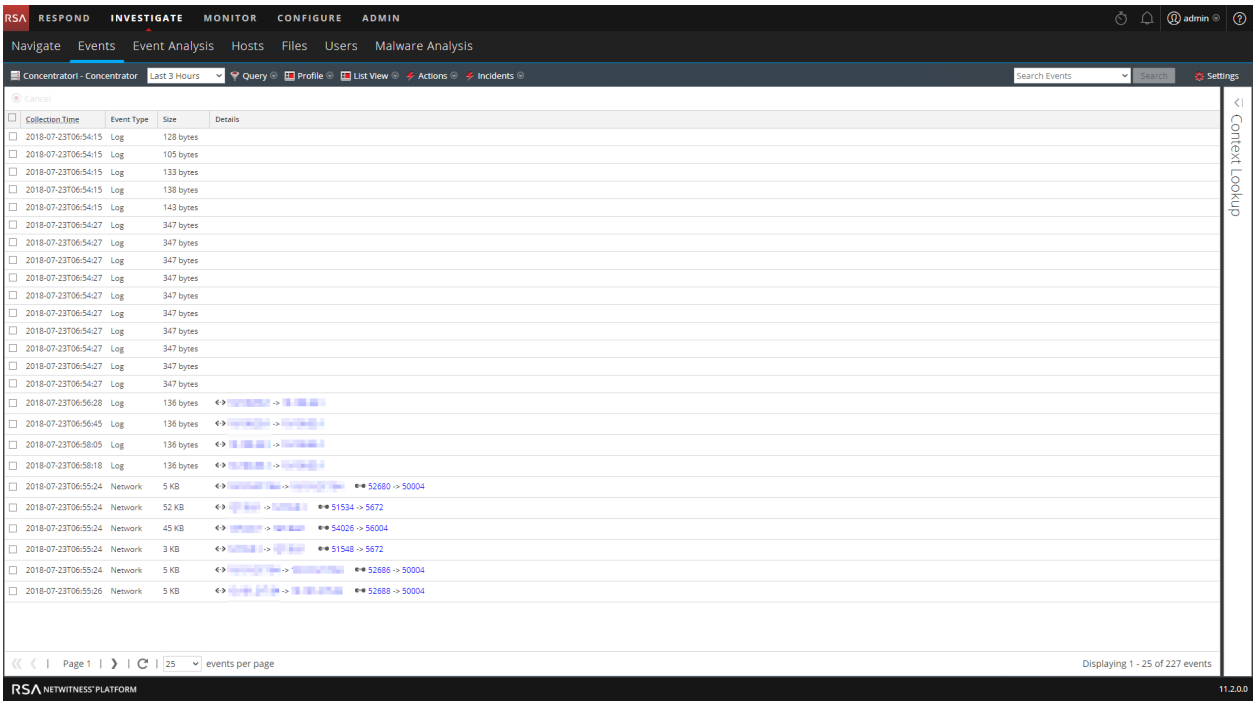
- In der Listenansicht werden die einander entsprechenden Quellen- und Zieladressen sowie Portinformationen zu Ereignissen in zusammengefasster Form in einem Raster dargestellt.
- Die Detailansicht enthält alle zum Ereignis gesammelten Metadaten in Seitenform.
- Die Protokollansicht ist für die Anzeige von Protokollinformationen optimiert und enthält weitere Informationen zu jedem Protokoll, darunter Zeitstempel, Ereignistyp, Servicetyp, Serviceklasse und die Protokolle.

Sie können Abfragen, die Zeitbereicheinstellung und Profile verwenden, um die Ereignisse zu filtern, die in der Ereignisansicht aufgeführt sind. In jeder der in der Ansicht „Ereignisse“ verfügbaren Ansichtsvarianten können Sie Dateien extrahieren, Ereignisse, Protokolle sowie Metawerte exportieren und den Bereich „Ereignisrekonstruktion“ sowie den Bereich „Ereignisanalyse“ öffnen.

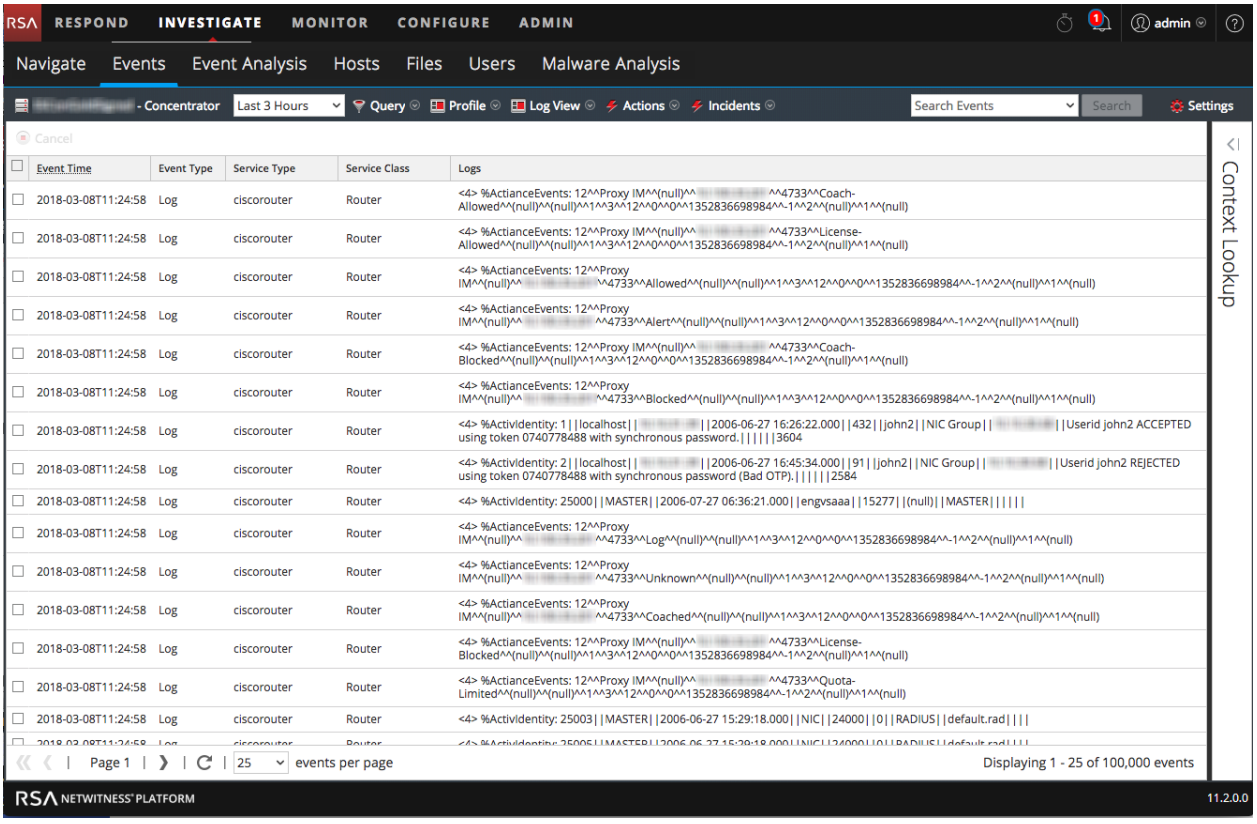
Die folgende Abbildung ist ein Beispiel für Ereignisse in der Detailansicht. Der Bereich „Kontextabfrage“ ist nur sichtbar, wenn der Context-Hub-Service konfiguriert ist.



Die folgende Abbildung zeigt ein Beispiel für Ereignisse in der Listenansicht.



Die folgende Abbildung ist ein Beispiel für die Protokollansicht:



Detaillierte Beschreibung

Die Ereignisansicht verfügt im oberen Bereich über eine Symbolleiste mit den folgenden Optionen:

Funktion	Beschreibung
Service auswählen	Zeigt neben dem Symbol den Namen des ausgewählten Services an. Öffnet das Dialogfeld Service auswählen, in dem Sie einen Service auswählen können, für den die Ereignisliste angezeigt wird.
Zeitbereich	Zeigt ein Drop-down-Menü zur Auswahl des Zeitbereichs an, der für die Ereignisliste gelten soll. Sie können eine der Standardoptionen auswählen oder einen eigenen Zeitbereich angeben.
Abfrage	Zeigt das Dialogfeld „Filter erstellen“ an, in das Sie eine benutzerdefinierte Abfrage direkt eingeben können, anstatt ein Drill-down in die Daten durchzuführen (siehe Erstellen einer angepassten Abfrage).
Profil	Zeigt das Menü Profil verwenden an; das aktuell ausgewählte Profil wird in der Symbolleiste angezeigt. Ein Profil erlaubt Ihnen, Profile zu verwalten und zu verwenden, die angepasste Metagruppen, eine Standard-Spaltengruppe und eine beginnende Abfrage enthalten können. Die Profile gelten für die Ansicht Navigieren (Metagruppen und Abfragen) und die Ansicht Ereignisse (Spaltengruppen und Abfragen).
Drop-down Ansichtstyp	Zeigt ein Drop-down-Menü für die Auswahl des Typs der Ereignisansicht an. • Die Detailansicht zeigt Ereignisse im Seitenformat an, der sich detaillierte Informationen zu jedem Ereignis entnehmen lassen. • In der Listenansicht erfolgt die Darstellung von Ereignissen im Rasterformat, in dem jedes Ereignis in einer einzelnen Zeile aufgeführt wird. • In der Protokollansicht wird ein protokollbezogenes Ereignisraster angezeigt, das die Zusammenfassung des jeweiligen Protokolls in einer einzelnen Zeile enthält. • Im Ansichtstyp Nutzerdefinierte Spaltengruppen wird die Ereignisliste unter Verwendung einer Spaltengruppe angezeigt, die in einer Drop-down-Liste mit benutzerdefinierten Spaltengruppen ausgewählt wird. • In der Ansicht Spaltengruppen managen erscheint ein Dialogfeld zur Erstellung und Bearbeitung benutzerdefinierter Spaltengruppen.

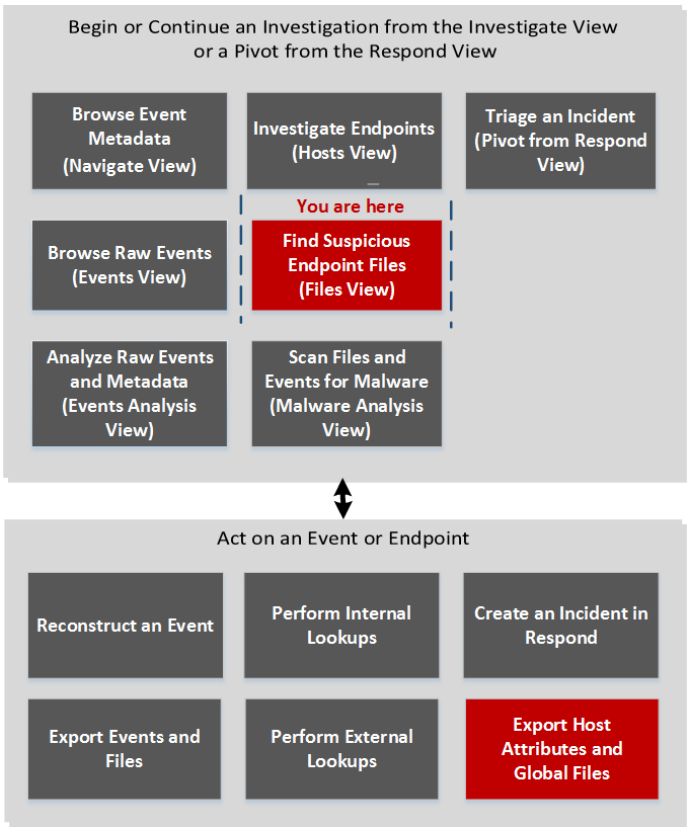
Funktion	Beschreibung
Aktionen	Zeigt ein Drop-down-Menü mit Aktionen in der Ereignisansicht an: • Extrahieren von Dateien, Exportieren von Ereignissen als PCAP-Datei, Exportieren von Protokollen oder Exportieren von Metawerten • Anzeigen von wiederhergestellten Ereignissen in einem Pop-up-Fenster oder in einer neuen Registerkarte • Anzeigen der Ansicht „Ereignisanalyse“ • Zurücksetzen aller Filter in der Ereignisansicht
Incidents	Hier können Sie einen neuen Incident in Respond erstellen und ihm die jeweils ausgewählten Ereignisse hinzufügen. Alternativ können Sie die ausgewählten Ereignisse auch einem bereits in „Reagieren“ vorhandenen Incident hinzufügen.
Suchen	Zeigt die Optionen unter „Ereignisse suchen“ an. Mit ihrer Hilfe können Sie das Format für den Protokollexport und den Export von Metawerten festlegen. Weitere Optionen sind unter Suchen nach Textmustern erläutert.
Einstellungen	Zeigt die Investigation-Einstellungen für die Ereignisansicht an (die auch in der Profilansicht verfügbar sind), sodass Sie die Investigation-Einstellungen ändern können, ohne die Ereignisansicht verlassen zu müssen. Wenn Sie eine Einstellung in der Ereignisansicht ändern, wird diese auch in der Profilansicht geändert (siehe Konfigurieren der Ansichten „Navigation“ und „Ereignisse“).

Ansicht „Dateien“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

In der Ansicht **Dateien** ist eine Liste von eindeutigen ausführbaren Dateien verfügbar, die sich in der Bereitstellung befinden. Um auf diese Ansicht zuzugreifen, navigieren Sie zu **UNTERSUCHEN > Dateien**. Standardmäßig zeigt die Ansicht „Dateien“ 100 Dateien. Um weitere Dateien anzuzeigen, klicken Sie auf **Weitere laden** am unteren Rand der Seite.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	finden von verdächtigen Endpunktdateien (Version 11.1)*	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Exportieren von Hostattributen und globalen Dateien*	Untersuchen von Dateien

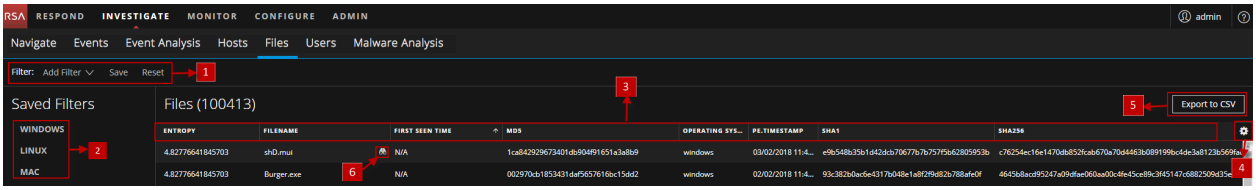
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Untersuchen von Hosts und Dateien

Überblick

Es folgt ein Beispiel für die Ansicht „Dateien“:



1	**Drop-down-Menü „Filter“ hinzufügen**. Sie können die Dateien filtern, indem Sie ein Betriebssystem (Windows, Linux oder Mac), gespeicherte Filter oder Optionen im Drop-Down-Menü „Filter hinzufügen“ auswählen. Weitere Informationen finden Sie unter Filtern von Dateien.
2	**Gespeicherte Filter.** Der Bereich „Gespeicherte Filter“ enthält eine Liste der gespeicherten Filter. Weitere Informationen finden Sie unter Filtern von Dateien.

3 **Spalten sortieren.** Sie können die Liste sortieren nach:

Dateiname: Name der Datei.

Zeit des ersten Auftretens: Erstmaliges Auftreten des Hash im Host.

Signatur: Gibt an, ob die Datei signiert oder unsigniert bzw. gültig oder ungültig ist. Ebenfalls angegeben sind Informationen zum Unterzeichner.

Größe: Größe der Datei.

Entropie: Bestimmt, ob die Inhalte komprimiert oder verschlüsselt werden.

Format: Format der Datei; Windows (PE), Linux (ELF und Skripte) und Mac (Macho).

PE.Resources.Company: Name des Unternehmens.

Hinweis: Beim Sortieren nach Spalten wird die Groß-/Kleinschreibung beachtet. Die Sortierung erfolgt zuerst nach Zahl, gefolgt von Großbuchstaben und dann Kleinbuchstaben.

4 **Menü „Einstellungen“.** Sie können die Einstellungen der Ansicht „Dateien“ festlegen, indem Sie Spalten aus dem Menü „Einstellungen“ auswählen. Weitere Informationen finden Sie unter Festlegen von Dateieinstellungen.

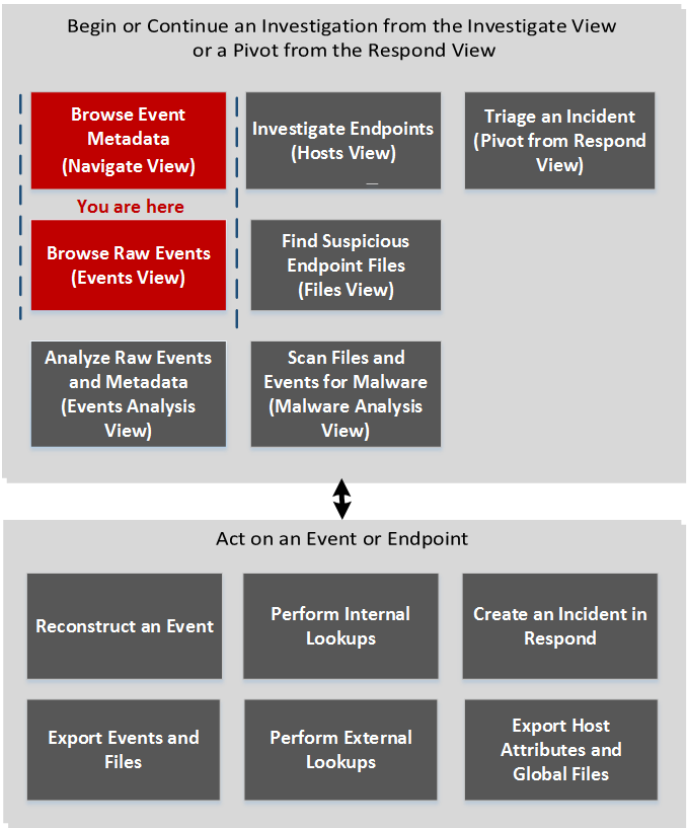
5 **In CSV-Datei exportieren**: Extrahiert globale Dateien in eine CSV-Datei. Weitere Informationen finden Sie unter Untersuchen von Dateien.

6 **Zu den Ansichten „Navigation“ und „Ereignisanalyse“ wechseln.** Um einen bestimmten Dateinamen oder Hash (SHA256 und MD5) zu untersuchen, können Sie zu den Ansichten „Navigation“ und „Ereignisanalyse“ wechseln. Weitere Informationen finden Sie unter Wechseln zu den Ansichten „Navigation“ und „Ereignisanalyse“.

Dialogfeld „Untersuchen“

Im Dialogfeld „Untersuchen“ können Analysten einen Service oder eine Sammlung für eine Ermittlung auswählen. Das Dialogfeld wird automatisch angezeigt, wenn Sie zuerst die Ansicht „Navigation“ oder „Ereignisse“ aufrufen und kein Standardservice für die Ermittlung ausgewählt ist. Wählen Sie zum Aufrufen des Dialogfelds aus einer aktuellen Ermittlung heraus den aktuellen Servicenamen in der Symbolleiste aus.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“

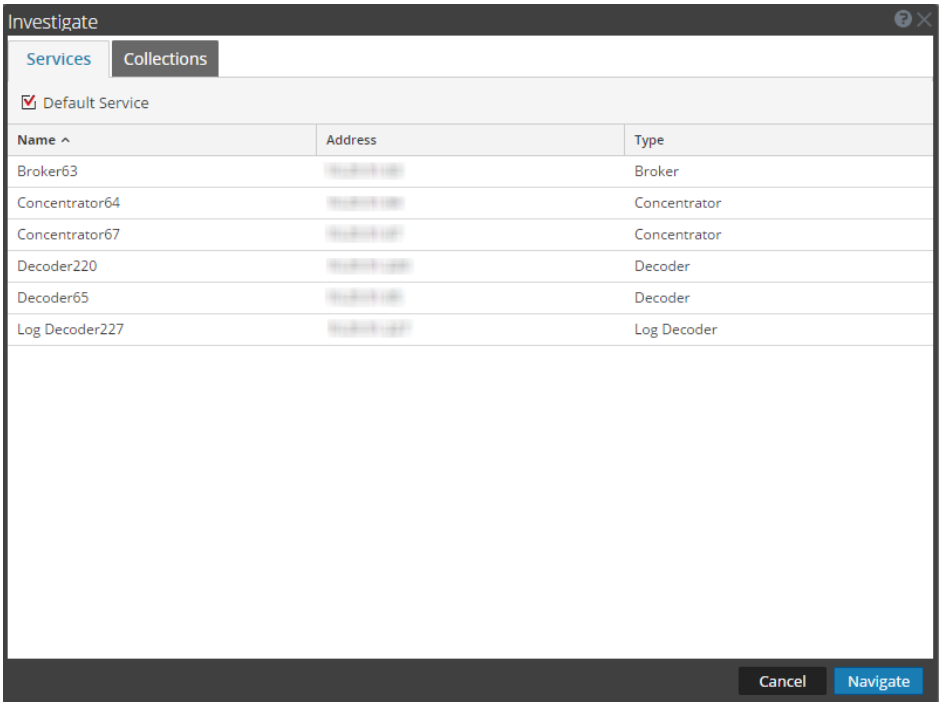
Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Auswählen eines Service zur Ermittlung*	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Navigation“
- Ansicht „Ereignisse“

Überblick



Das Dialogfeld „Untersuchen“ verfügt über zwei Registerkarten: „Services“ und „Sammlungen“.

Hinweis: Sammlungen werden auch als Workbench-Sammlungen bezeichnet. Sie können nur Workbench-Sammlungen anzeigen, die Sie erstellt haben, und nur Administratoren können eine Workbench-Sammlung erstellen.

Die Registerkarte „Services“ enthält eine Liste der für eine Ermittlung verfügbaren Services sowie drei Schaltflächen. Alle Funktionen sind in der folgenden Tabelle beschrieben.

Funktion	Beschreibung
Standardservice	Durch Klicken auf diese Schaltfläche wird der Service, der standardmäßig untersucht wird, ausgewählt oder gelöscht. Wenn ein Service als Standardservice festgelegt wurde, wird hinter dem Namen des Services das Wort (Standard) angezeigt.
Name	Der Name des Services.
Adresse	Die IP-Adresse des Services
Typ	Der Servicetyp
Abbrechen	Schließt das Dialogfeld.
Navigieren	Öffnet den ausgewählten Service in der Ansicht „Navigation“ oder „Ereignisse“.

Die Registerkarte „Sammlungen“ enthält zwei Schaltflächen und zwei Bereiche: „Workbench“ und „Sammlungen“.

Im Bereich „Workbench“ sind die verfügbaren Workbench-Services nach Name aufgeführt. Sobald ein Workbench-Service ausgewählt wurde, können Sie im Bereich „Sammlungen“ eine Sammlung auswählen.

Im Bereich „Sammlungen“ sind die für eine Ermittlung verfügbaren Sammlungen aufgeführt. Sobald eine Sammlung ausgewählt wurde, können Sie auf „Navigation“ klicken, um die Sammlung anzuzeigen.

In der folgenden Tabelle sind die Funktionen im Dialogfeld „Sammlungen“ beschrieben.

Funktion	Beschreibung
Name	Der Name der Sammlung
Typ	Der Sammlungstyp.
Größe	Die Größe der Sammlung
Datentyp	Der Typ der Daten in der Sammlung
Erstellungsdatum	Das Datum, an dem die Sammlung erstellt wurde

Registerkarte „Investigation“ – Bereich „Nutzereinstellungen“

In der Ansicht „Profil“ > Bereich „Einstellungen“ > Registerkarte „Investigation“ können Nutzer verschiedene Einstellungen festlegen, die die Performance und das Verhalten von NetWitness Platform bei der Datenanalyse sowie bei der Anzeige und Rekonstruktion von Ereignissen in NetWitness Investigation beeinflussen. Um auf diese Registerkarte zuzugreifen, wählen Sie > Profile aus. Wenn die Ansicht „Profil“ angezeigt wird, wählen Sie die Registerkarte **Einstellungen > Investigation** aus. Sie können Nutzereinstellungen in NetWitness Platform zu jedem beliebigen Zeitpunkt ändern.

Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Nutzereinstellungen für Investigate anzeigen und ändern*	Konfigurieren der Ansichten „Navigation“ und „Ereignisse“

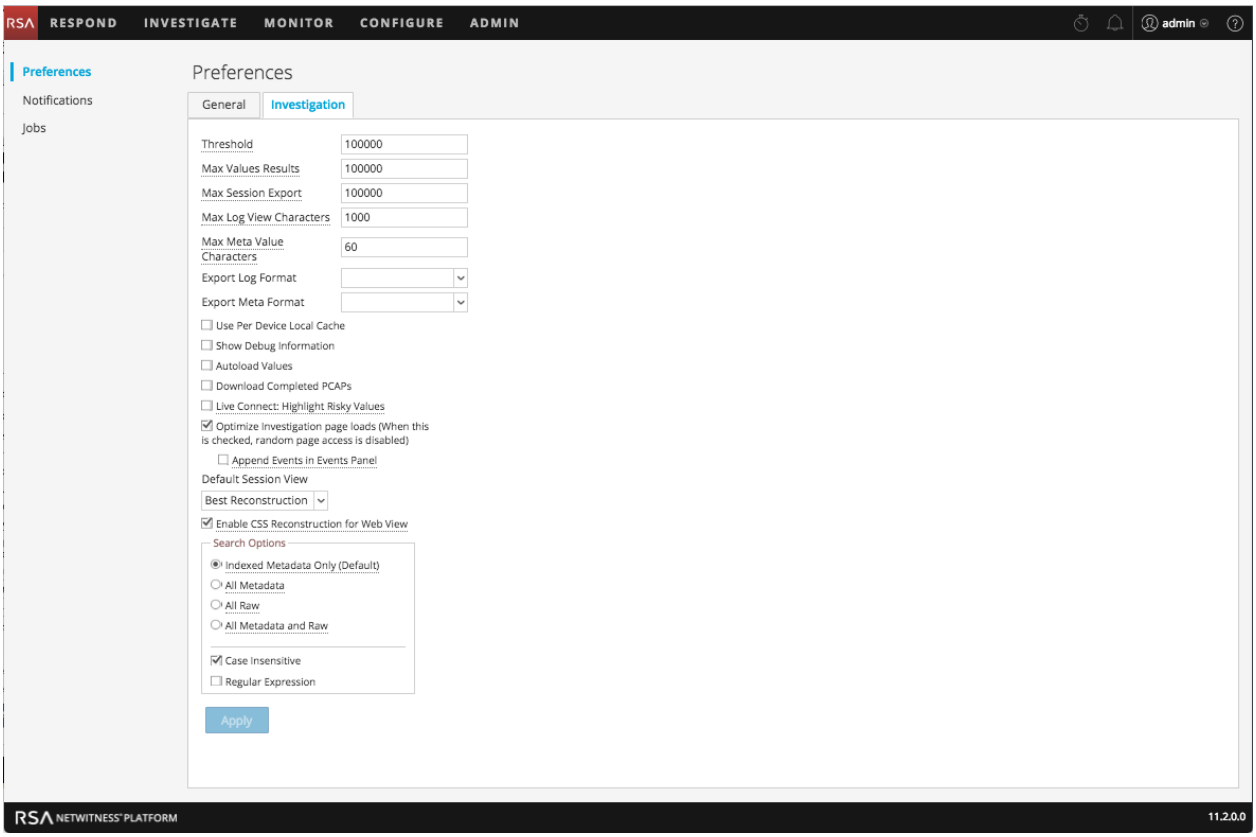
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Navigation“
- Ansicht „Ereignisse“

Überblick

Diese Abbildung ist ein Beispiel der Registerkarte „Investigation“ und in der folgenden Tabelle sind die Einstellungen beschrieben, die sich auf die Untersuchung auswirken. Es gibt leichte Unterschiede bei den Sucheinstellungen zwischen den Versionen 11.1 und 11.2, die unter Suchen nach Textmustern erläutert werden.



Funktion	Beschreibung
Schwellenwert	Diese Einstellung steuert den Zähler, der während des Ladens für den Wert Metaschlüssel in der Ansicht „Navigation“ angezeigt wird. Ein höherer Schwellenwert ermöglicht genauere Zählerangaben für einen Wert. Allerdings verursacht ein höherer Schwellenwert längere Ladezeiten. Wenn der Schwellenwert erreicht ist, wird in NetWitness Platform die Summe und der Prozentsatz der Zeit angezeigt, die zum Erreichen des Zählerstandes im Vergleich zu der für das Laden aller Sitzungen mit diesem Wert erforderlichen Zeit verwendet wurde. Beispiel: **(>100.000 – 18 %)** zeigt an, dass der Schwellenwert auf 100.000 festgelegt wurde und dass für diese Last nur 18 % der Zeit aufgewandt wurde, die es ohne festgelegten Schwellenwert gedauert hätte. Der Standardwert ist **100.000**.
Max. Wertergebnisse	Diese Einstellung steuert die maximale Anzahl an Werten, die in der Ansicht „Navigation“ geladen werden, wenn die Option „Max. Ergebnisse“ im Menü „Metaschlüssel“ für einen offenen Metaschlüssel ausgewählt ist. Der Standardwert ist **1000**.
Max. Sitzungsexport	Mit dieser Einstellung wird die maximale Anzahl von exportierbaren Sitzungen festgelegt. Der Standardwert ist **100.000**.

Funktion	Beschreibung
Max. Zeichenzahl für Protokollansicht	Diese Einstellung legt die Anzahl der Zeichen fest, die maximal in **Investigation > Ereignisse > Protokolltext** angezeigt werden sollen. Der Standardwert ist **1.000**.
Exportprotokollformat	Mit dieser Einstellung wird das Standardformat für das Exportieren von Protokollen aus Investigation festgelegt. Die verfügbaren Optionen sind **Text**, **XML**, **CSV** und **JSON**. Es gibt keinen integrierten Standardwert für das Protokollexportformat. Wenn Sie hier kein Format auswählen, zeigt NetWitness Platform ein Auswahldialogfenster an, wenn Sie einen Protokollexport aufrufen. Wenn Sie eine der Optionen im Drop-down-Menü „Exportprotokollformat“ auswählen und auf „Anwenden“ klicken, werden die Einstellungen sofort wirksam.
Format exportierte Metadaten	Mit dieser Einstellung wird das Standardformat für das Exportieren von Protokollen aus „Investigation“ festgelegt. Die verfügbaren Optionen sind Text, XML, CSV und JSON. Es gibt keinen integrierten Standardwert für das Metaexportformat. Wenn Sie hier kein Format auswählen, zeigt NetWitness Platform ein Auswahldialogfeld an, wenn Sie einen Export von Metadaten aufrufen. Wenn Sie eine der Optionen im Drop-down-Menü „Format exportierte Metadaten“ auswählen und auf „Anwenden“ klicken, werden die Einstellungen sofort wirksam.
Lokaler Cache pro Gerät	
Debuginformationen anzeigen	Wenn diese Option aktiviert ist, zeigt NetWitness Platform die `where`-Klausel unter der Brotkrümelnavigation in der Ansicht „Navigation“ an. Für jeden Ladevorgang von Metawerten wird die Ladezeit angezeigt. Wenn der Service ein Broker ist, wird die verstrichene Zeit für jeden aggregierten Service gemeldet. Der Standardwert ist **Aus**.
Ereignisse in Ereignisbereich anhängen	Wenn diese Option ausgewählt ist, werden die im **Bereich „Ereignisse“** angezeigten Ereignisse inkrementell hinzugefügt und die aktuell angezeigten Ereignisse werden nicht überschrieben. Bei jedem Klicken auf das Symbol „Nächste Seite“ werden die weiteren Ereignisse an die vorherigen Ereignisse angehängt; 1 – 25, dann 1 – 50 und dann 1 – 75 usw. **Hinweis:** Diese Option ist nur verfügbar, wenn die Option „Optimieren des Ladens der Seite ‚Investigation‘“ aktiviert ist.
Werte automatisch laden	Wenn diese Option aktiviert ist, werden die Servicewerte automatisch in der Navigationsansicht geladen. Wenn sie nicht aktiviert ist, zeigt NetWitness Platform eine Schaltfläche **Werte laden** an, über die der Nutzer die Optionen ändern kann. Der Standardwert ist **Aus**.
Abgeschlossene PCAPs herunterladen	Diese Einstellung automatisiert den Download von extrahierten PCAPs in Investigation, damit Sie extrahierte PCAP-Dateien nicht manuell in einer Anwendung wie Wireshark, mit der Daten im PCAP-Format angezeigt werden können, herunterladen und öffnen müssen.

Funktion	Beschreibung
Live Connect: Riskante Werte markieren	
Optimieren des Ladens der Seite „Investigation“	Diese Option ist standardmäßig aktiviert und legt fest, wie in der Ereignisansicht Ereignisse abgerufen werden. Im Optimalfall werden Ergebnisse so schnell wie möglich zurückgegeben. Dadurch entfällt die ursprüngliche Möglichkeit, auf einer spezifischen Seite in der Ereignisliste zu springen. Durch die Deaktivierung dieses Kontrollkästchens wird die Paginierung der Ereignislisten geändert, damit Sie auf eine bestimmte Seite in der Liste (oder auf die letzte Seite) springen können. Die Möglichkeit, auf alle Seiten in der Liste springen zu können, hat negative Folgen auf die Geschwindigkeit beim Zurückgeben der Ergebnisse aufgrund von zusätzlichem Overhead beim Festlegen der Ereignisse im Voraus.
Standardsitzungsansicht	Diese Einstellung wählt den Typ Standardrekonstruktion für die erstmalige Rekonstruktionsansicht aus. Ereignisse werden standardmäßig mithilfe der Rekonstruktionsmethode, die sich für das Ereignis am besten eignet, neu erstellt.
CSS-Rekonstruktion für Webansicht ermöglichen	Diese Einstellung steuert, wie die Rekonstruktion von Webinhalten durchgeführt wird. Wenn die Einstellung aktiviert ist, werden bei der Webrekonstruktion auch Cascaded Style-Sheet-Stilvorlagen (CSS) und Bilder mit einbezogen, sodass die Darstellung der Originalansicht in einem Webbrowser entspricht. Dies umfasst das Scannen und Rekonstruieren von verwandten Ereignissen sowie die Suche nach den im Zielereignis verwendeten Formatvorlagenund Bildern. Diese Option ist standardmäßig aktiviert. Deaktivieren Sie die Option, wenn Probleme beim Anzeigen bestimmter Websites auftreten. **Hinweis:** Die Darstellung der rekonstruierten Inhalte entspricht möglicherweise nicht einwandfrei der ursprünglichen Webseite, wenn verwandte Bilder und Formatvorlagen nicht gefunden oder aus dem Cache des Webbrowsers geladen wurden. Zudem werden Layouts oder Formate, die dynamisch über das clientseitige JavaScript erstellt werden, in der Rekonstruktion nicht dargestellt, weil alle clientseitigen JavaScripts aus Sicherheitsgründen entfernt werden.
Suchoptionen	Mit dieser Einstellung werden die Standardsuchoptionen, die auf eine Suche angewendet werden sollen, in den Ansichten „Navigation“ und „Ereignisse“ festgelegt. Unter Suchen nach Textmustern finden Sie detaillierte Informationen.
Anwenden	Speichert Ihre Einstellungen und macht sie sofort wirksam.

Ansicht „Untersuchen“

Die Ansicht Investigate (Ermittlung) ist der primäre Einstiegspunkt in NetWitness Investigate. Die Ansicht „Untersuchen“ hat sechs Untermenüs, die unterschiedliche Ansichten öffnen, mit denen Sie Ereignisse aus verschiedenen Perspektiven analysieren können. Der Untermenüs sind: „Navigation“, „Ereignisse“, „Ereignisanalyse“, „Hosts“, „Dateien“, „Nutzer“ und „Malware Analysis“.

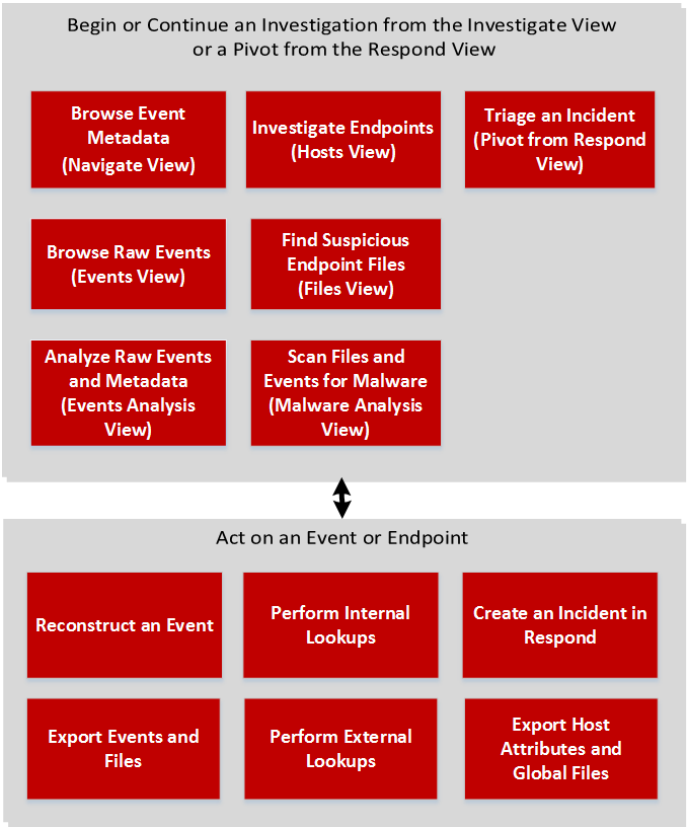
Hinweis: Der Untermenüs „Ereignisanalyse“, „Hosts“ und „Dateien“ sind ab Version 11.1 verfügbar. Das Menü „Nutzer“ ist in Version 11.2 und höher verfügbar. Konfigurierte Berechtigungen pro Nutzerrolle und Nutzer bestimmen, welche Untermenüs angezeigt werden.

Mithilfe der Untermenüoptionen können Sie zwischen den verschiedenen Ansichten wechseln.

- Die Ansichten „Navigation“, „Ereignisse“ und „Ereignisanalyse“ bieten Verknüpfungen zueinander, um die aktuellen Ergebnisse aus einer anderen Perspektive betrachten zu können, was eine gewisse Kontinuität für die Untersuchung bietet, wenn Sie zwischen den Ansichten wechseln.
- Die Ansichten „Hosts“ und „Dateien“ integrieren NetWitness Endpoint in Investigate und bieten eine Ansicht aller Hosts, bei denen ein NetWitness Endpoint-Agent installiert ist und eine Ansicht der spezifischen ausführbaren Dateien in der bereitgestellten Umgebung.
- Mit der Ansicht „Nutzer“ von NetWitness UEBA wird die Transparenz von riskantem Nutzerverhalten in Ihrem Unternehmen gewährleistet. Sie können eine Liste der Nutzer mit hohem Risiko und eine Zusammenfassung der wichtigsten Warnmeldungen für riskantes Verhalten für Ihre Umgebung anzeigen. Dann können Sie einen Nutzer oder eine Benachrichtigung auswählen und Details über das riskante Verhalten und eine Zeitleiste anzeigen, in der die Verhaltensweisen aufgetreten sind.
- Die Ansicht „Malware Analysis“ bietet die Möglichkeit, Dateien zu scannen, die in einem der anderen Ansichten gefunden oder durch kontinuierliches Durchsuchen des Netzwerkverkehrs erfasst wurden.

Workflow

Der Workflow unten zeigt die allgemeinen Aufgaben zur Untersuchung von Ereignissen.



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen*	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten*	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)*	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)*	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen*	Durchführen von Schadsoftwareanalysen

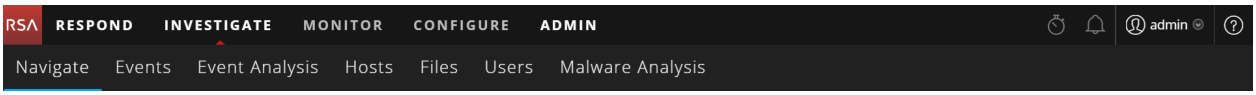
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Starten einer Ermittlung
- Konfigurieren von Ansichten und Voreinstellungen von NetWitness Investigate
- Ansicht „Navigation“
- Ansicht „Ereignisse“
- Ansicht „Ereignisanalyse“
- Ansicht „Hosts“
- Ansicht „Dateien“
- Ansicht „Malware Analysis“
- *NetWitness UEBA – Benutzerhandbuch*

Überblick

Die Ansicht „Untersuchen“ besteht aus sechs Ansichten, die jeweils einen anderen Ansatz zur Analyse von Daten darstellen. Standardmäßig öffnet sich „Untersuchen“ auf die Ansicht „Navigation“. Sie können die Standardansicht auf eine der anderen Ansichten ändern. Eine Einführung in die Verwendungsmöglichkeiten jeder Ansicht finden Sie unter Wie funktioniert NetWitness Investigate? Die folgende Abbildung zeigt die Untermenüs unter „UNTERSUCHEN“.



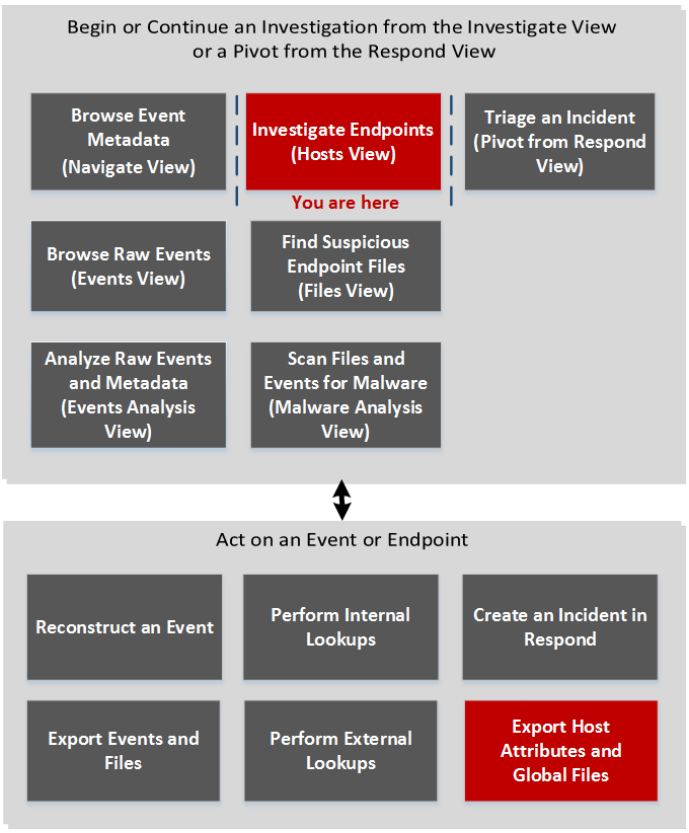
Ansicht „Hosts“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

In NetWitness Investigate zeigt die Ansicht „Hosts“ eine Liste aller Hosts, auf denen ein Endpunkt-Agent installiert ist. Die Tabelle zeigt eine Reihe von Standardspalten für den Host an. Sie können diese Ansicht anpassen, indem Sie die Hosteinstellungen festlegen. Um auf diese Ansicht zuzugreifen, navigieren Sie zu **UNTERSUCHEN > Hosts**.

Workflow

Die folgende Abbildung zeigt den anspruchsvollen Untersuchungsworkflow mit hervorgehobenen Endpunkten der Untersuchung.



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)*	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Exportieren von Hostattributen und globalen Dateien*	Untersuchen von Hosts

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

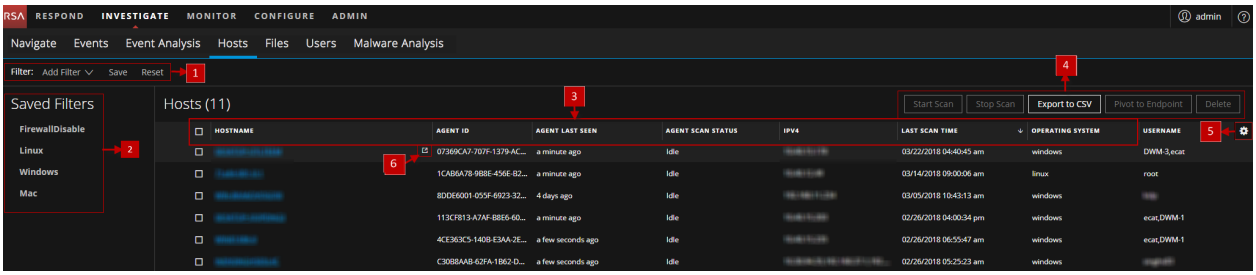
Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Untersuchen von Hosts und Dateien
- Ansicht „Hosts“ – Registerkarte „Übersicht“
- Ansicht „Hosts“ – Registerkarte „Prozess“
- Ansicht „Hosts“ – Registerkarte „Automatische Ausführungen“
- Ansicht „Hosts“ – Registerkarte „Dateien“
- Ansicht „Hosts“ – Registerkarte „Treiber“
- Ansicht „Hosts“ – Registerkarte „Bibliotheken“
- Ansicht „Hosts“ – Registerkarte „Systeminformationen“

Überblick

In der Ansicht „Hosts“ können Sie Hostattribute und globale Dateien exportieren, einen Scan nach Bedarf durchführen, Hosteinstellungen festlegen, eine Liste von Hosts anzeigen und in der Ansicht „Navigation“ oder „Ereignisse“ untersuchen.

Es folgt ein Beispiel für die Ansicht „Hosts“.



1 **Drop-down-Menü „Filter“ hinzufügen**. Sie können die Hosts filtern, indem Sie ein Betriebssystem (Windows, Linux oder Mac), gespeicherte Filter oder Optionen im Drop-down-Menü „Filter hinzufügen“ auswählen. Weitere Informationen finden Sie unter Hosts filtern.

2 **Gespeicherte Filter.** Der Bereich „Gespeicherte Filter“ enthält eine Liste der gespeicherten Filter. Weitere Informationen finden Sie unter Hosts filtern.

3 **Spalten sortieren**. Ermöglicht das Sortieren von Spalten.

> **Hinweis:** Beim Sortieren nach Spalten wird die Groß-/Kleinschreibung beachtet. Die Sortierung erfolgt zuerst nach Zahl, gefolgt von Großbuchstaben und dann Kleinbuchstaben. Die Sortierung nach den Feldern „Agent-Scanstatus“ und „Agent zuletzt gesehen“ wird nicht in der richtigen Reihenfolge angezeigt.

4 **Aktionen in der Symbolleiste:**
Scan starten: Startet den Scan für die ausgewählten Hosts.
Scan stoppen: Beendet den Scan für die ausgewählten Hosts.
In CSV-Datei exportieren: Extrahiert Hostattribute in eine CSV-Datei. Weitere Informationen finden Sie unter Exportieren von Hostattributen.
Zu Endpoint wechseln: Erlaubt das Untersuchen des NetWitness Endpoint-Hosts (Version 4.4.0.2 oder später). Weitere Informationen finden Sie unter Untersuchen von NetWitness Endpoint 4.4.0.2 oder später Hosts.
Löschen: Hiermit können Sie Hosts über die Benutzeroberfläche manuell löschen. Nach dem Löschen verarbeitet der Endpunktserver keine Anforderung von diesem Host.

> **Hinweis:** Stellen Sie sicher, dass der Agent vom Host deinstalliert wurde, bevor Sie ihn von der Benutzeroberfläche löschen. Weitere Informationen finden Sie unter Löschen eines Hosts.

5 **Menü „Einstellungen“.** Sie können die Einstellungen der Ansicht „Hosts“ festlegen, indem Sie Spalten aus dem Menü „Einstellungen“ auswählen. Weitere Informationen finden Sie unter Festlegen von Hosteinstellungen.

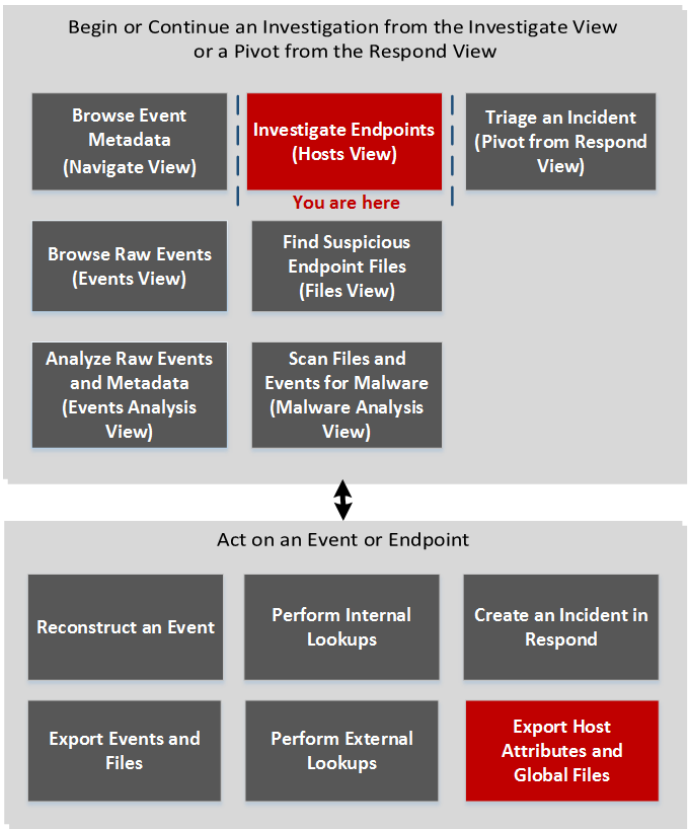
6 **Zu den Ansichten „Navigation“ und „Ereignisanalyse“ wechseln**. Um einen bestimmten Host, eine IP-Adresse oder einen Nutzernamen zu untersuchen, können Sie zu den Ansichten „Navigation“ und „Ereignisanalyse“ wechseln. Weitere Informationen finden Sie unter Wechseln zu den Ansichten „Navigation“ und „Ereignisanalyse“.

Ansicht „Hosts“ – Registerkarte „Automatische Ausführungen“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Der Bereich „Automatische Ausführungen“ enthält eine Liste der automatischen Ausführungen, Services, Aufgaben und Cronjobs, die auf dem Host ausgeführt werden. Um auf diese Registerkarte zuzugreifen, wählen Sie einen Host aus der Ansicht **Hosts** aus und klicken Sie auf die Registerkarte **Automatische Ausführungen**.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)*	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Anzeigen der automatischen Ausführungen, Services, Aufgaben und Cronjobs, die auf dem Host ausgeführt werden*	Automatische Ausführungen analysieren

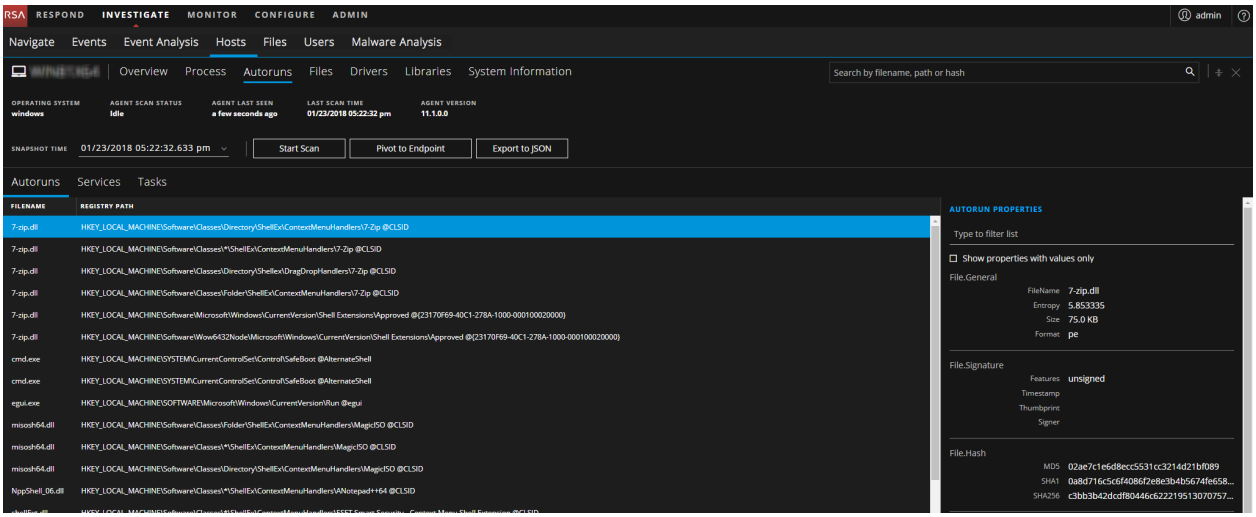
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Untersuchen von Hosts und Dateien
- Ansicht „Hosts“

Überblick

Es folgt ein Beispiel für die Registerkarte „Automatische Ausführungen“:



Kategorie	Beschreibung
Automatische Ausführungen	Dateien, die beim Start ausgeführt werden. Zeigt die folgenden Spalten an: • Dateiname: `cmd.exe` • Registrierungspfad: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot @AlternateShell`
Services	Dateien, die als Service für den ausgewählten Host ausgeführt werden. Zeigt die folgenden Spalten an: • Servicename: `acsock` • Betriebsstatus: `stopped` • Zeitpunkt der Dateierstellung: `07/11/2017 11:47:00 am` • Signatur: `Microsoft, signed, valid` • Dateipfad: `C:\Windows\System32\drivers`
Aufgaben/Cronjobs	Dateien, die zur Ausführung als geplante Aufgaben zusammen mit dem Auslöser konfiguriert sind. Zeigt die folgenden Spalten an: • Name: `shell32.dll` • Hash: `cafa6e7b6a9220e7c805ea476a89a78800f48bb48c66fe5f935057940df3909c` • Letzte Ausführungszeit: `01/19/2018 05:34:50 pm` • Nächste Ausführungszeit: `12/30/1899 05:30:00 am` • Auslöser: `No Trigger`

Bereich „Eigenschaften von automatischen Ausführungen“

In diesem Bereich werden alle Eigenschaften der ausgewählten Datei angezeigt. Er ist wie folgt gruppiert:

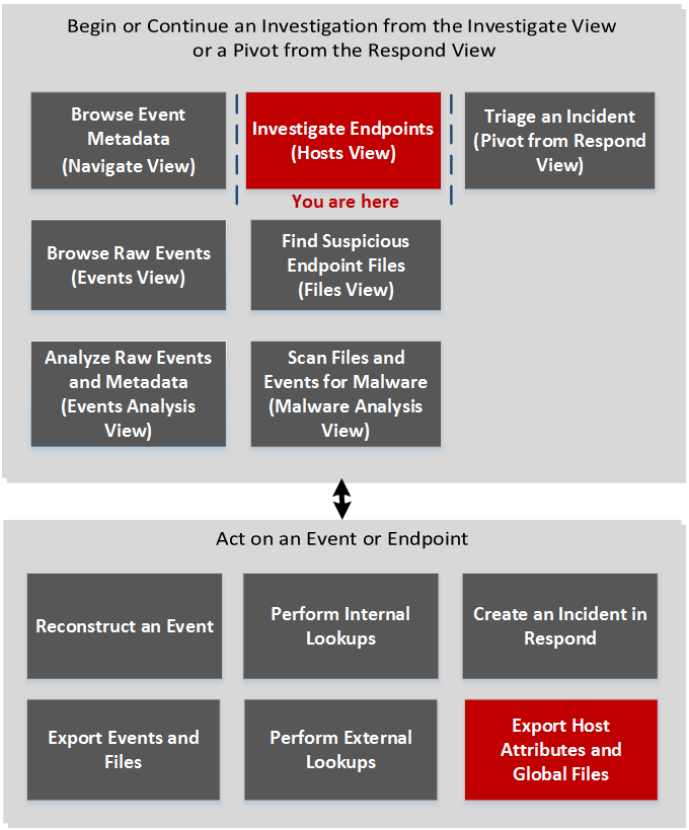
Kategorie	Beschreibung
Signatur	Gibt Informationen zum Unterzeichner an.
Hash	Hash-Typ der Datei (MD5, SHA256 und SHA1).
Zeit	Zeitpunkt, zum dem die Datei erstellt, geändert oder auf sie zugegriffen wurde.
Speicherort	Speicherort der Datei.
Bild	Lädt das Bild.

Ansicht „Hosts“ – Registerkarte „Treiber“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Die Registerkarte „Treiber“ listet die Treiber auf, die auf den Hosts zum Scanzeitpunkt ausgeführt werden. Um auf diese Registerkarte zuzugreifen, wählen Sie einen Host aus der Ansicht **Hosts** aus und klicken Sie auf die Registerkarte **Treiber**.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)*	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Anzeigen der auf dem Host ausgeführten Treiber*	Untersuchen von Hosts

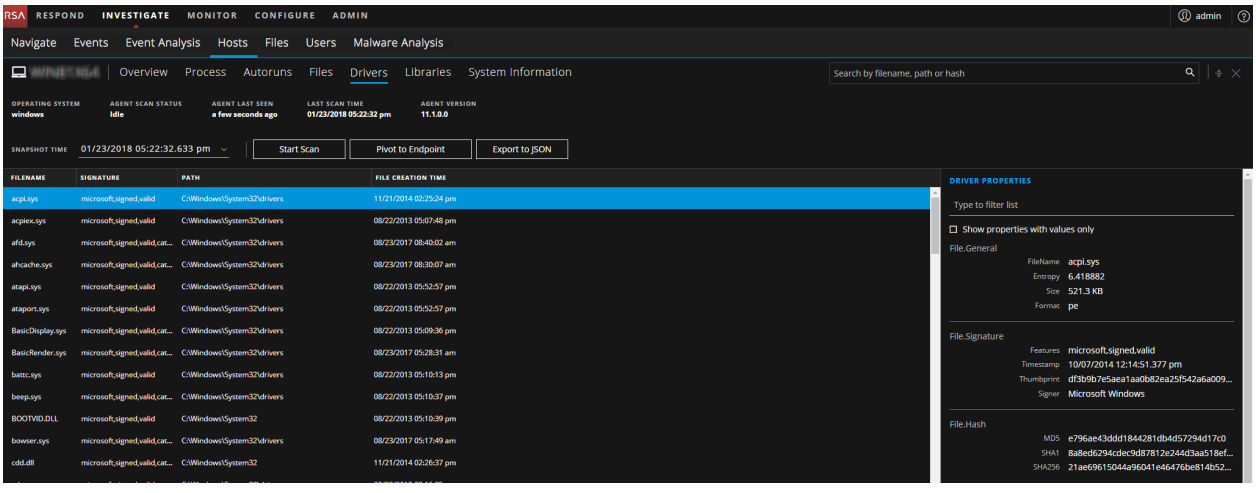
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Untersuchen von Hosts und Dateien
- Ansicht „Hosts“

Überblick

Es folgt ein Beispiel der Registerkarte „Treiber“:



Feld	Beschreibung
Dateiname	Name der Datei. Beispiel: `acpi.sys`.

Feld	Beschreibung
Signatur	Gibt an, ob die Datei signiert oder unsigniert bzw. gültig oder ungültig ist. Ebenfalls angegeben sind Informationen zum Unterzeichner.
Pfad	Pfad der Datei. Beispiel: `C:\Windows\System32\drivers`.
Zeitpunkt der Dateierstellung	Zeitpunkt der Erstellung der Datei.

Bereich „Treibereigenschaften“

In diesem Bereich werden alle Eigenschaften der ausgewählten Datei angezeigt. Er ist wie folgt gruppiert:

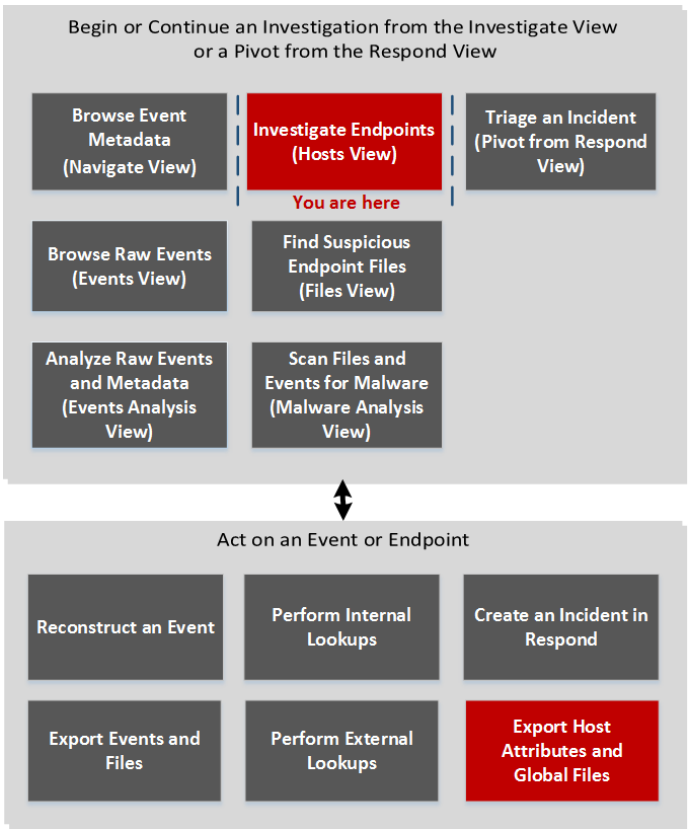
Kategorie	Beschreibung
Allgemein	Allgemeine Informationen über die Datei, z. B. Dateiname, Entropie, Größe und Format.
Signatur	Gibt Informationen zum Unterzeichner an.
Hash	Hash-Typ der Datei (MD5, SHA256 und SHA1).
Zeit	Zeitpunkt, zum dem die Datei erstellt, geändert oder auf sie zugegriffen wurde.
Speicherort	Speicherort der Datei.
Image	Geladenes Image.

Ansicht „Hosts“ – Registerkarte „Dateien“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Die Registerkarte „Dateien“ zeigt alle auf dem Host gescannten Dateien an. Um auf diese Registerkarte zuzugreifen, wählen Sie einen Host aus der Ansicht **Hosts** aus und klicken Sie auf die Registerkarte **Dateien**. Standardmäßig werden 100 Dateien angezeigt. Um weitere Dateien anzuzeigen, klicken Sie auf **Weitere laden** am unteren Rand der Seite.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)*	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Anzeigen der auf dem Host gescannten Dateien*	Analysieren von Dateien

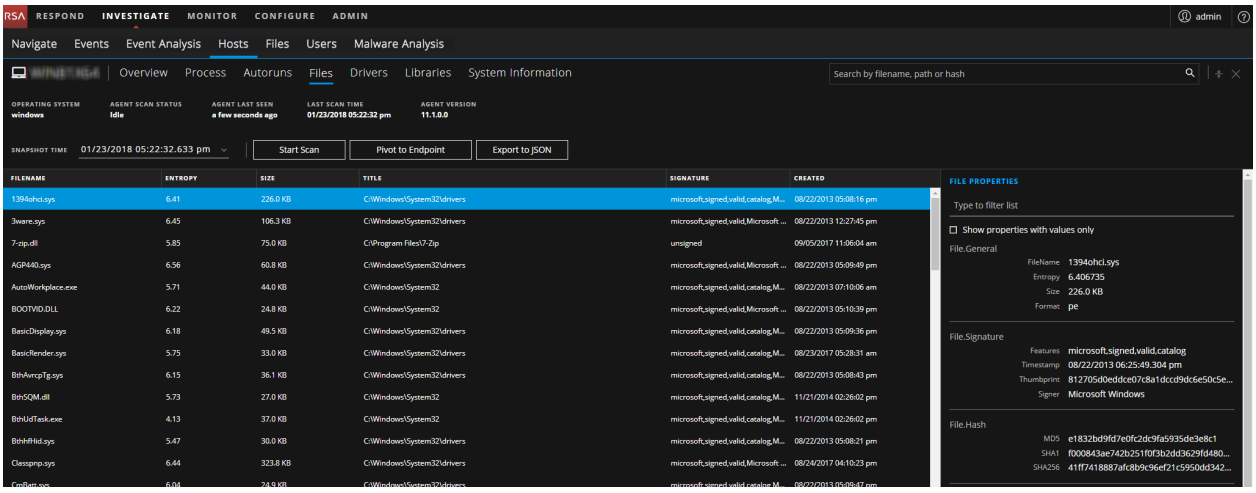
* Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Untersuchen von Hosts und Dateien
- Ansicht „Hosts“

Überblick

Es folgt ein Beispiel für die Registerkarte „Dateien“.



Feld	Beschreibung
Dateiname	Name der Datei. Beispiel: `7-zip.dll`.
Entropie	Entropie der Imagedaten, mit Ausnahme der PE-Kopfzeilen. Sie bestimmt, ob die Inhalte gepackt werden (komprimiert oder verschlüsselt).
Größe	Größe der Datei. Das kann ein Indikator bei der Bewertung einer Datei sein.
Pfad	Pfad der Datei. Manchmal platzieren Malware-Autoren die Datei in Verzeichnisse, in denen in der Regel keine solche Dateien vorhanden sind. Schädliche Dateien sind in der Regel eigenständige Dateien (z. B. eine Datei im Stammverzeichnis `C:\ProgramData`) im Gegensatz zu einer Gruppe von Dateien in einem legitimen Ordner (z. B. Dateien in `C:\Program Files\<folder name>\`).
Signatur	Gibt an, ob die Datei signiert oder unsigniert bzw. gültig oder ungültig ist. Ebenfalls angegeben sind Informationen zum Unterzeichner.
Erstellt	Zeitstempel der Datei.
Nutzername	Nutzer der Datei (für Linux). Beispiel: `root`.
Gruppenname	Die Gruppe, zu der der Nutzer gehört (für Linux). Beispiel: `root (0)`.

Bereich „Dateieigenschaften“

In diesem Bereich werden alle Eigenschaften der ausgewählten Datei angezeigt. Er ist wie folgt gruppiert:

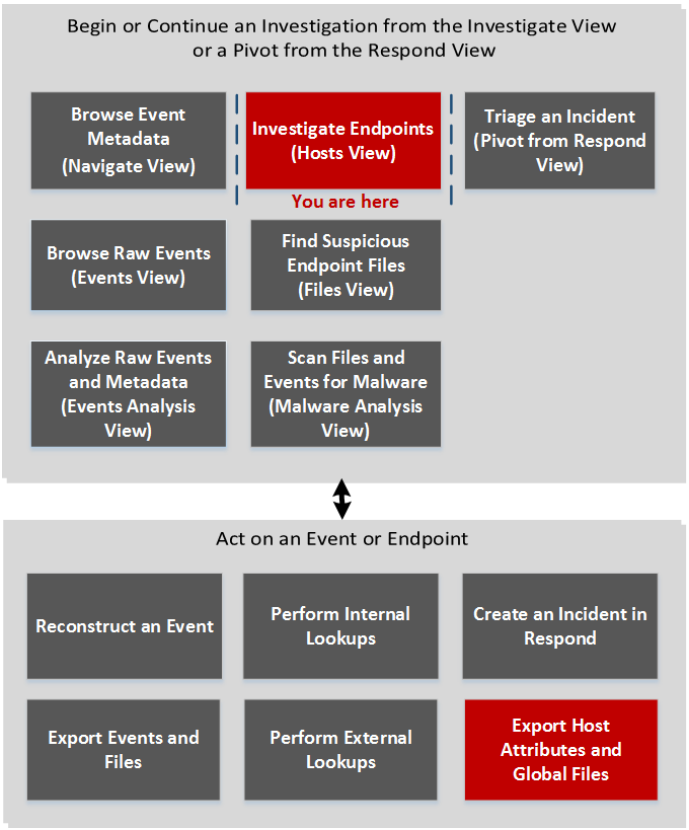
Kategorie	Beschreibung
Allgemein	Allgemeine Informationen über die Datei, z. B. Dateiname, Entropie, Größe und Format.
Signatur	Gibt Informationen zum Unterzeichner an.
Hash	Hash-Typ der Datei (MD5, SHA256 und SHA1).
Zeit	Zeitpunkt, zum dem die Datei erstellt, geändert oder auf sie zugegriffen wurde.
Speicherort	Speicherort der Datei.

Ansicht „Hosts“ – Registerkarte „Bibliotheken“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Die Registerkarte „Bibliotheken“ listet die zum Zeitpunkt des Scans geladenen Bibliotheken auf. Um auf diese Registerkarte zuzugreifen, wählen Sie einen Host aus der Ansicht **Hosts** aus und klicken Sie auf die Registerkarte **Bibliotheken**.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)*	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Anzeigen der geladenen Bibliotheken*	Analyse von Bibliotheken

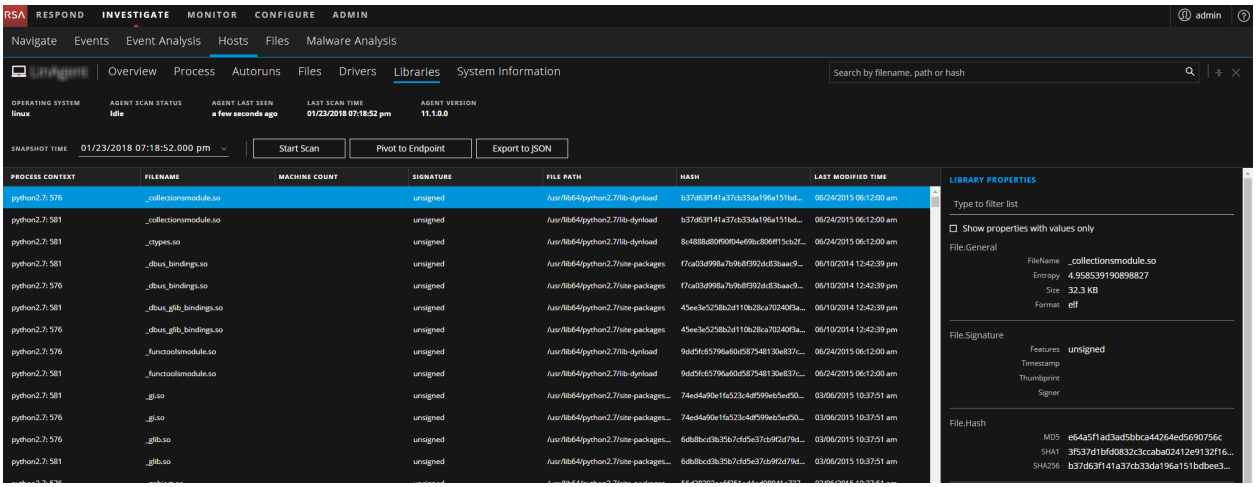
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Untersuchen von Hosts und Dateien
- Ansicht „Hosts“

Überblick

Es folgt ein Beispiel für die Registerkarte „Bibliotheken“:



Feld	Beschreibung
Kontext verarbeiten	Name und PID des Prozesses, der die Bibliothek in den Arbeitsspeicher geladen hat. Beispiel: `explorer.exe: 1916`.
Dateiname	Name der Datei. Beispiel: `7-zip.dll`.
Signatur	Gibt an, ob die Datei signiert oder unsigniert bzw. gültig oder ungültig ist. Ebenfalls angegeben sind Informationen zum Unterzeichner. Beispiel: `signed, valid`.
Dateipfad	Pfad der Datei. Beispiel: `C:\Program Files\7-Zip`.
Hash	SHA256 der Datei. Beispiel: `c3bb3b42dcdf80446c622219513070757e618c06afd9ee0ac37cbce5befcb897`.
Zeitpunkt der Dateierstellung	Zeitpunkt der Erstellung der Datei.
Zeitpunkt der letzten Änderung	Zeitpunkt der Änderung der Datei.

Bereich „Bibliothekseigenschaften“

In diesem Bereich werden alle Eigenschaften der ausgewählten Datei angezeigt. Er ist wie folgt gruppiert:

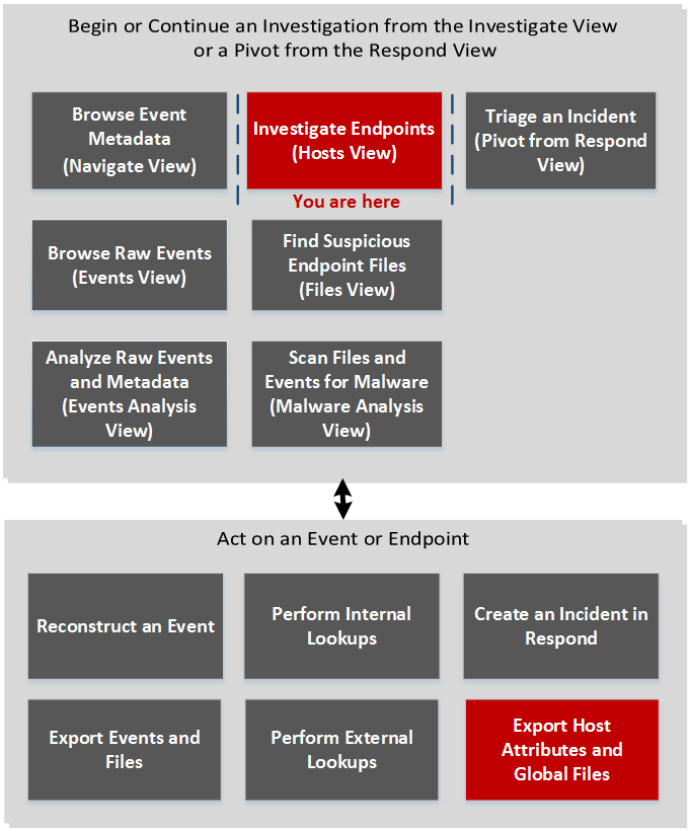
Kategorie	Beschreibung
Allgemein	Allgemeine Informationen über die Datei, z. B. Dateiname, Entropie, Größe und Format.
Signatur	Gibt Informationen zum Unterzeichner an.
Hash	Hash-Typ der Datei (MD5, SHA256 und SHA1).
Zeit	Zeitpunkt, zum dem die Datei erstellt, geändert oder auf sie zugegriffen wurde.
Speicherort	Speicherort der Datei.
Prozess	Details des Prozesses, z. B. Imagegröße und PID.

Ansicht „Hosts“ – Registerkarte „Übersicht“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Die Registerkarte „Übersicht“ bietet detaillierte Scanergebnisse des ausgewählten Hosts. Standardmäßig wird das neueste Scanergebnis angezeigt. Um auf diese Ansicht zuzugreifen, navigieren Sie zu **UNTERSUCHEN > Hosts** und wählen Sie einen Host aus der Ansicht **Hosts** aus.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)*	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Anzeigen der Zusammenfassung des Hosts*	Untersuchen von Hosts

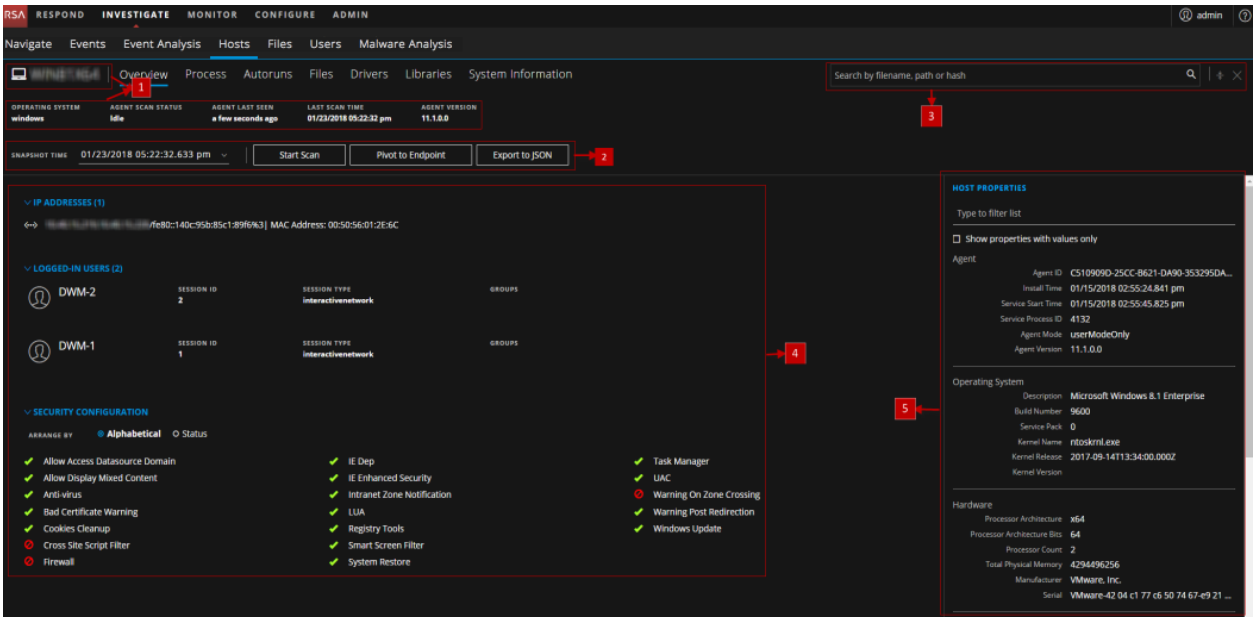
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Untersuchen von Hosts und Dateien
- Ansicht „Hosts“

Überblick

Es folgt ein Beispiel für die Registerkarte „Übersicht“:



1 **Agent- und Scandetails**. Sie können die folgenden Agent- und Scandetails des ausgewählten Hosts anzeigen:

Hostname: Name des Hosts. Beispielsweise `WIN-ABC`.
Betriebssystem: Betriebssystem, auf dem der Agent ausgeführt wird (Linux, Windows oder Mac).

Agent-Scanstatus: Aktueller Status des Scanvorgangs – Leerlauf, Wird gescannt, Scan wird gestartet oder Scan wird gestoppt. Weitere Informationen finden Sie unter Untersuchen von Hosts.

Agent zuletzt gesehen: Zeitpunkt, zu dem der Agent zuletzt mit dem Server kommuniziert hat.

Zeit des letzten Scans: Zeitpunkt, zu dem der Agent zuletzt gescannt wurde. Das Datum und die Uhrzeit entspricht der Zeitzone, die in den Nutzereinstellungen festgelegt und lokal für den Server ist.

Agent-Version: Version des Agent Beispiel: `11.1.0.0`.

2 **Aktionen in der Symbolleiste:**
Snapshot-Zeit: Listet gescannte Zeitstempel auf. Um den Scanverlauf anzuzeigen, wählen Sie die Snapshot-Zeit aus dem Drop-down-Menü aus.
Scan starten: Startet den Scan für die ausgewählten Hosts. Weitere Informationen finden Sie unter Untersuchen von Hosts.
In CSV-Datei exportieren: Extrahiert Hostattribute in eine CSV-Datei. Weitere Informationen finden Sie unter Exportieren von Hostattributen.
Zu Endpoint wechseln: Erlaubt das Untersuchen des NetWitness Endpoint-Hosts (Version 4.4.0.2 oder später). Weitere Informationen finden Sie unter Untersuchen von NetWitness Endpoint 4.4.0.2 oder später Hosts.
In JSON-Datei exportieren: Extrahiert Hostattribute und Endpunktdaten in eine JSON-Datei des ausgewählten Snapshot.

3 **Suche in Snapshots**. Erlaubt die Suche auf allen Snapshots (Dateiname, Dateipfad und SHA-256-Prüfsumme). Weitere Informationen finden Sie unter Suchen in Snapshots.

4 **Übersicht über den ausgewählten Host**. Zeigt die folgenden Felder an:

IP-Adressen: Mit dem Host verknüpfte IP-Adressen Beispiel: `10.10.10.3`.

Angemeldete Nutzer: Auf dem Host angemeldete Nutzer. Beispiel: `abc`.

Sicherheitskonfiguration: Details zur Sicherheitskonfiguration auf dem Host. Beispielsweise Firewall deaktiviert oder aktiviert, intelligenter Bildschirmfilter deaktiviert oder aktiviert. Dieses Feld gilt nur für Windows und Mac.

> **Hinweis:** Agent-Version, IP-Adressen, Angemeldete Nutzer und Sicherheitskonfiguration können sich bei jedem Scan ändern.

5 **Bereich „Hosteigenschaften“**. Zeigt alle Eigenschaften des ausgewählten Hosts an. Er ist wie folgt gruppiert:

Agent: Informationen im Zusammenhang mit dem Agent, z. B. Agent-ID, Fehlercode Installationszeit und Agent-Modus.

Betriebssystem: Betriebssystemversion und Informationen zum Build.

Hardware: Informationen im Zusammenhang mit der Architektur.

Netzwerkschnittstellen: Netzwerkadapterinformationen, z. B. Mac-Adresse, Gateway.

Nutzer: Informationen im Zusammenhang mit dem Nutzer.

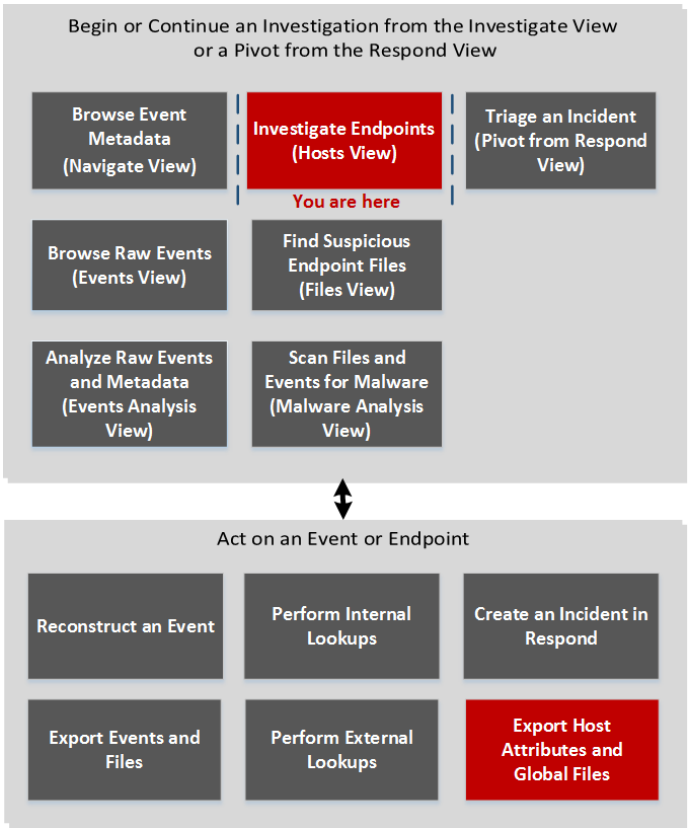
Gebietsschema: Zeitzone und Sprache, die lokal für den Host gelten.

Ansicht „Hosts“ – Registerkarte „Prozess“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Der Bereich „Prozess“ enthält eine Liste der auf dem Host ausgeführten Prozesse. Um auf diese Registerkarte zuzugreifen, wählen Sie einen Host aus der Ansicht **Hosts** aus und klicken Sie auf die Registerkarte **Prozesse**.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)*	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Anzeigen der Prozesse, die auf dem Host ausgeführt werden*	Untersuchen von Hosts

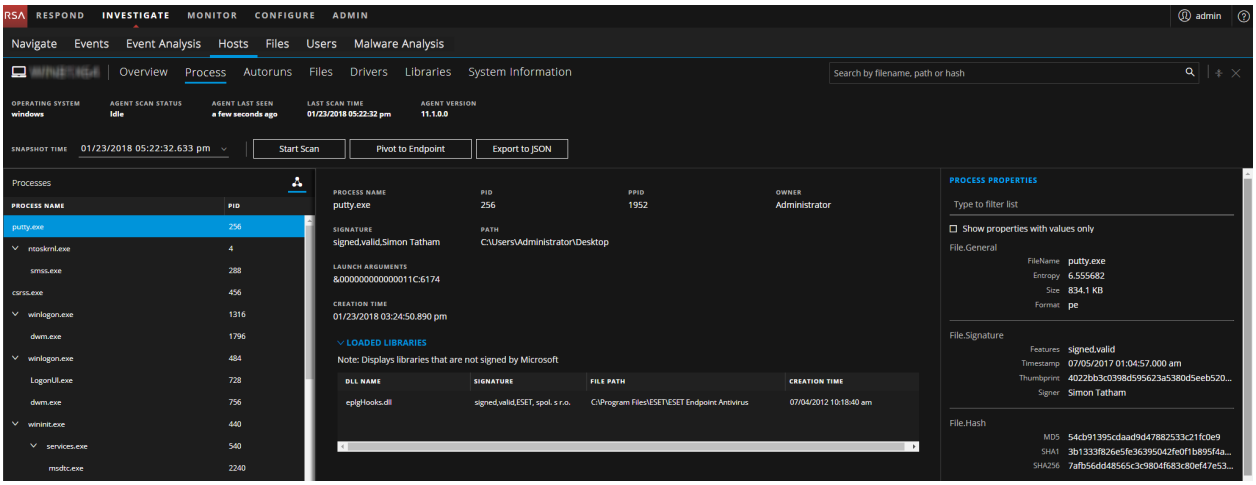
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Untersuchen von Hosts und Dateien
- Ansicht „Hosts“

Überblick

Es folgt ein Beispiel der Registerkarte „Prozess“:



Im Bereich „Prozess“ werden unter „Prozessdetails“ die folgenden Informationen angezeigt:

Feld	Beschreibung
Prozessname	Name des Prozesses. Beispiel: `server.exe`.
PID	ID des Prozesses. Beispiel: `492`.
Übergeordneter Prozess (PPID)	Name und Prozess-ID des übergeordneten Prozesses. Beispiel: `4`.
Eigentümer	Eigentümer des Prozesses. Beispiel: `SYSTEM`.
Signatur	Gibt an, ob die Datei signiert oder unsigniert bzw. gültig oder ungültig ist. Ebenfalls angegeben sind Informationen zum Unterzeichner.
Pfad	Pfad der Datei, die dem Prozess auf der Festplatte zugeordnet ist. Beispiel: `C:\Windows\System32`.
Startargumente	Befehlszeilenargumente, die dem Prozess beim Start übergeben werden. Beispiel: `-k LocalServiceNoNetwork`.
Erstellungszeit	Zeitpunkt der Erstellung des Prozesses. Beispiel: `01/19/2018 11:32:29.908 am`.

- Liste der geladenen Bibliotheken für den ausgewählten Prozess wie etwa DLLs (für Windows), Dylibs (für Mac) oder .SO (für Linux).
- Liste der automatischen Ausführungen (sofern konfiguriert).

Bereich „Prozesseigenschaften“

In diesem Bereich werden alle Eigenschaften des ausgewählten Prozesses angezeigt. Er ist wie folgt gruppiert:

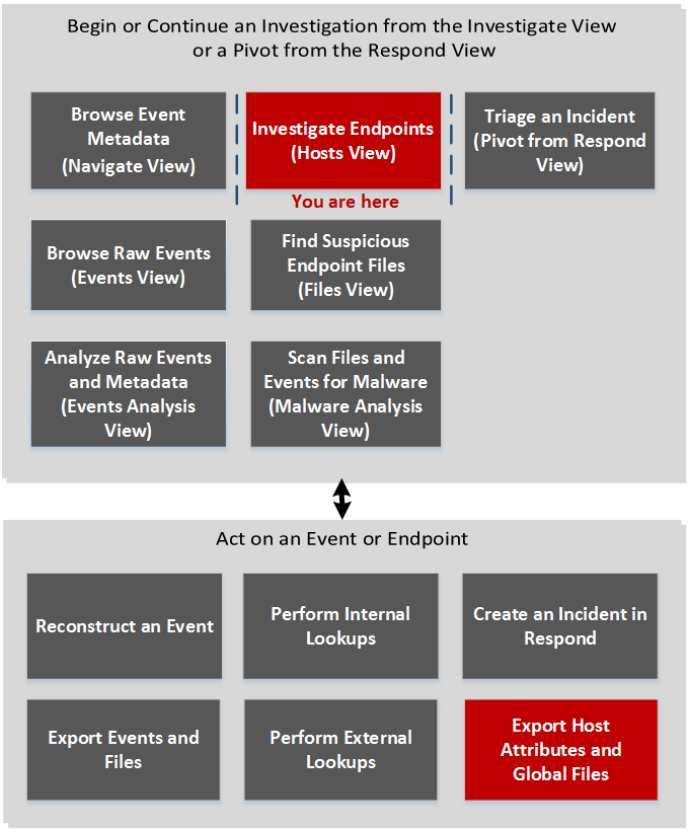
Kategorie	Beschreibung
Allgemein	Allgemeine Informationen über die Datei, z. B. Dateiname, Entropie, Größe und Format.
Signatur	Gibt Informationen zum Unterzeichner an.
Hash	Hash-Typ der Datei (MD5, SHA1 und SHA256).
Zeit	Zeitpunkt, zum dem die Datei erstellt, geändert oder auf sie zugegriffen wurde.
Speicherort	Speicherort der Datei.
Prozess	Details des Prozesses, z. B. Imagegröße und PID.
Image	Vom Prozess geladene Details des Image.

Ansicht „Hosts“ – Registerkarte „Systeminformationen“

Hinweis: Die Informationen in diesem Thema gelten für RSA NetWitness® Platform Version 11.1 und höher.

Die Registerkarte „Systeminformationen“ listet die Systeminformationen zum Agent auf. Um auf diese Registerkarte zuzugreifen, wählen Sie einen Host aus der Ansicht **Hosts** aus und klicken Sie auf die Registerkarte **Systeminformationen**.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)*	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Anzeigen der Systeminformationen zum Agent*	Analysieren der Systeminformationen

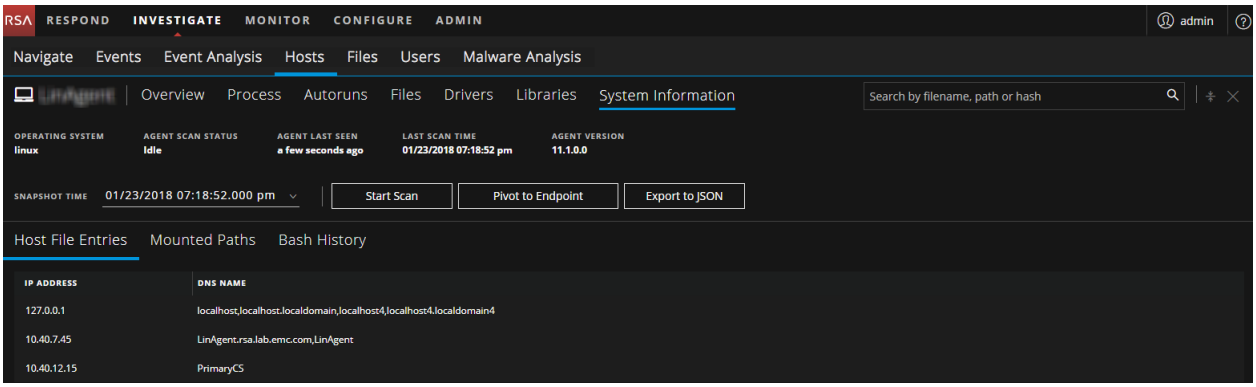
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Untersuchen von Hosts und Dateien
- Ansicht „Hosts“

Überblick

Im folgenden ist ein Beispiel der Registerkarte „Systeminformationen“:



Feld	Beschreibung
Hostdateieinträge	Alle in die Hostdatei geschriebenen Netzwerkumleitungen. Beispielsweise IP-Adresse: `10.10.10.3` und DNS-Name: `localhost,localhost.localdomain,localhost4,localhost4.localdomain4`

Feld	Beschreibung
Netzwerkfreigaben	Netzwerkname des gemeinsam genutzten Ressource (nur für Windows). Beispielsweise Name: `Admin$`, Beschreibung: `Remote Admin`, Pfad: `C:\`, Berechtigungen: `None`, Typ: `disk, special`, Maximale Nutzer: `4294967295`, Aktuelle Nutzer: `0`.
Sicherheitsprodukte	Installierte Sicherheitsprodukte (nur für Windows). Beispielsweise Anzeigename: `Windows Defender`, Instanz: `D68DDC3A-831F-4FAE-9E44-DA132C1ACF46`, Funktionen: `Enabled`, Typ: `antiVirus`.
Patches für Windows	Liste der durch Windows-Aktualisierungen angewendeten Patches (nur für Windows). Beispiel: `KB2959936`.
Gemountete Pfade	Pfad, auf dem gemountet wird. Beispielsweise Pfad: `/`, Dateisystem: `rootfs`, Remotepfad: `rootfs`, Optionen: `rw`.
Bash-Verlauf	Nutzername und ausgeführter Befehl. Beispielsweise Nutzername: `root` und Befehl: `ls`.

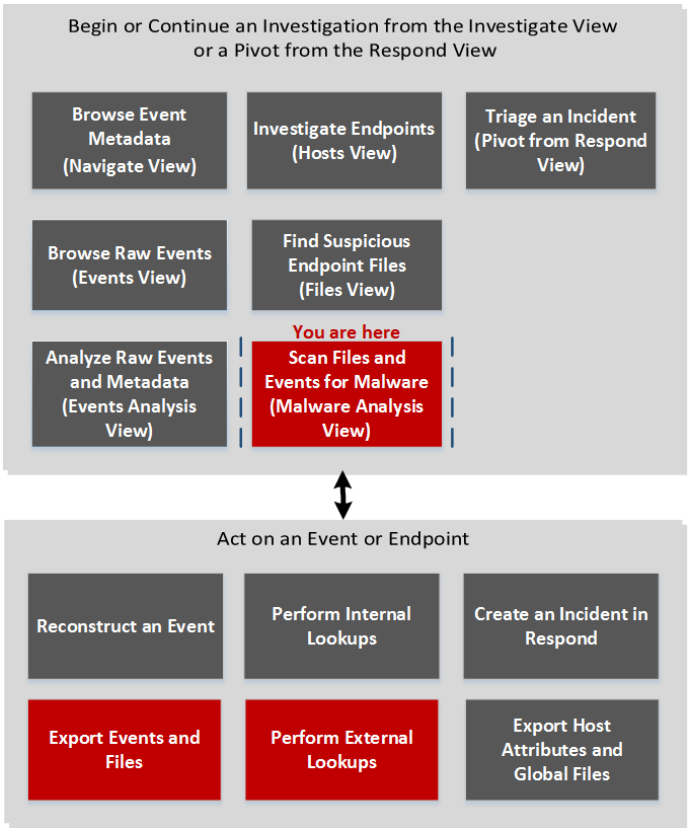
Hinweis: Für Mac-Hosts sind die Felder „Gemountete Pfade“ und „Bash-Verlauf“ leer.

Ansicht „Malware Analysis“

In NetWitness Investigation stellt die Ansicht „Malware Analysis“ die Benutzeroberfläche zur Durchführung einer Schadsoftwareanalyse bereit. Die Ansicht „Malware Analysis“ hat die Form eines anpassbaren Dashboards, in dem Standard-Dashlets in der anfänglichen Ansicht auf der Nutzerrolle (Administration oder Analyst) und Nutzeranpassungen basieren. Anfänglich wird das Dashlet Ereigniszusammenfassung in der Ansicht Malware Analysis angezeigt. Zusätzliche Dashlets präsentieren verschiedene Visualisierungen der angezeigten Ereignisse und jede Darstellung ist konfigurierbar, um Ihre Ansicht weiter zu verbessern, während Sie nach Indikatoren für eine Infizierung suchen. Die Malware-Analysis-Dashlets, die auf dem -Dashboard verfügbar sind, sind auch in der Ansicht „Malware Analysis“ verfügbar.

Um auf diese Ansicht zuzugreifen, wählen Sie **Ermittlung > Malware Analysis** aus. Wenn kein Standardservice ausgewählt wurde, wird das Dialogfeld „Malware Analysis Service auswählen“ angezeigt. Wählen Sie einen Service aus und klicken Sie anschließend auf **Fortlaufenden Modus anzeigen**.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen*	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Exportieren von Ereignissen und Dateien*	Überprüfen von Scandateien und Ereignissen in Listenform
Threat Hunter	Durchführen externer Suchen*	Anzeigen der detaillierten Schadsoftwareanalyse eines Ereignisses

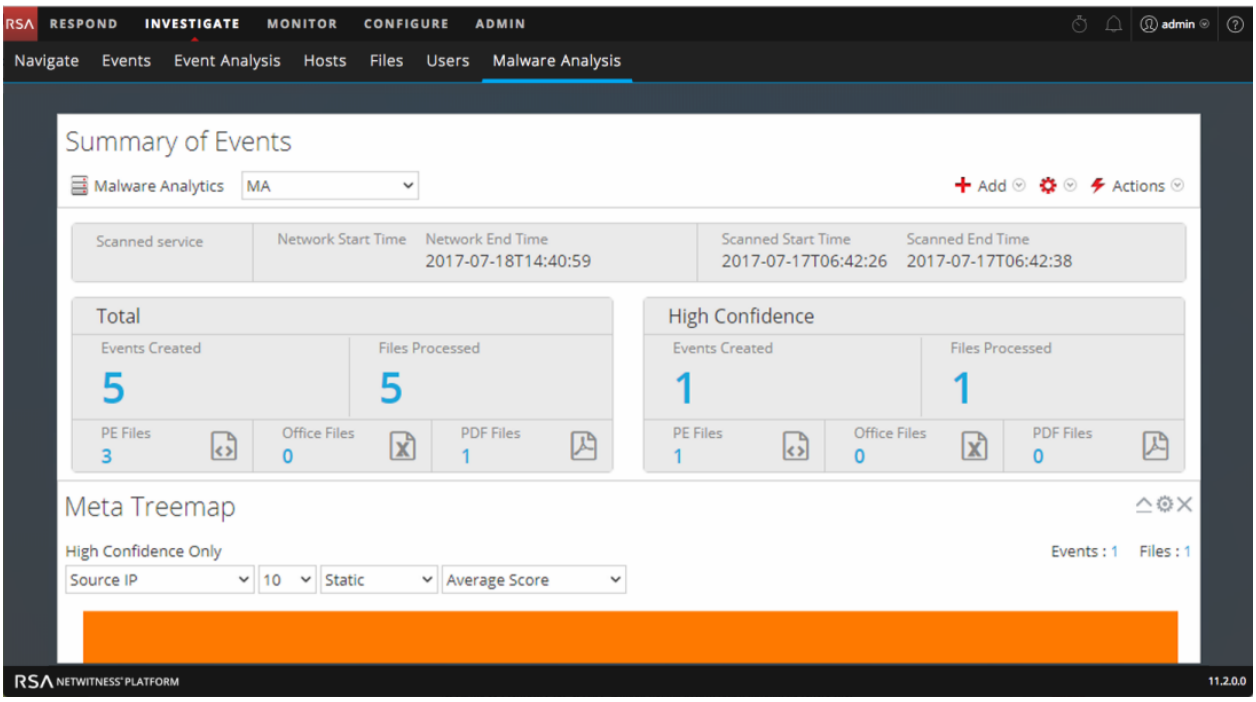
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Starten eines Malware Analysis-Scans in der Ansicht „Navigation“

Überblick

Es folgt ein Beispiel für die Ansicht Malware Analysis.



Die Ansicht „Malware Analysis“ enthält den Bereich „Ereigniszusammenfassung“ und vier für diese Ansicht spezifische Dashlets. Jedes dieser spezifischen Dashlets hat identische Dialogfelder „Optionen“. Die Malware Analysis-Dashlets in der Ansicht „ÜBERWACHEN“ sind ebenfalls verfügbar und werden im Thema „Dashlets“ unter RSA Content für die RSA NetWitness Platform beschrieben.

Bereich „Ereigniszusammenfassung“

Im Bereich Ereigniszusammenfassung können Sie den Service, den Scanmodus und den Zeitbereich auswählen. Zudem können Sie einen Datenpunkt auswählen und die dem Ereignis zugeordneten Ereignisse anzeigen.

In der folgenden Tabelle werden alle Funktionen im Bereich „Ereigniszusammenfassung“ beschrieben.

Funktion	Beschreibung
	Wählt einen Service für die Anzeige aus.
Scanmodus	Zeigt eine Drop-down-Liste der verfügbaren Scanmodi an.
Zeitbereich	Zeigt eine Drop-down-Liste der Zeitbereiche für die Anzeige von Ereignissen an.
Startdatum	Wenn der Zeitbereich auf „benutzerdefiniert“ eingestellt ist, wird ein Kalender angeboten, in dem Sie das Startdatum des Zeitbereichs auswählen können.
Enddatum	Wenn der Zeitbereich auf „benutzerdefiniert“ eingestellt ist, wird ein Kalender angeboten, in dem Sie das Enddatum des Zeitbereichs auswählen können.
	Zeigt eine Drop-down-Liste der Dashlets an, die Sie der Ansicht hinzufügen können.

Funktion	Beschreibung
	Zeigt eine Drop-down-Liste der Aktionen an, die Sie in dieser Ansicht ausführen können: • Standardkonfiguration wiederherstellen • Dashlets anordnen • Schwellenwertfilter anwenden
	Aktualisiert die Ansicht „Malware Analysis“.

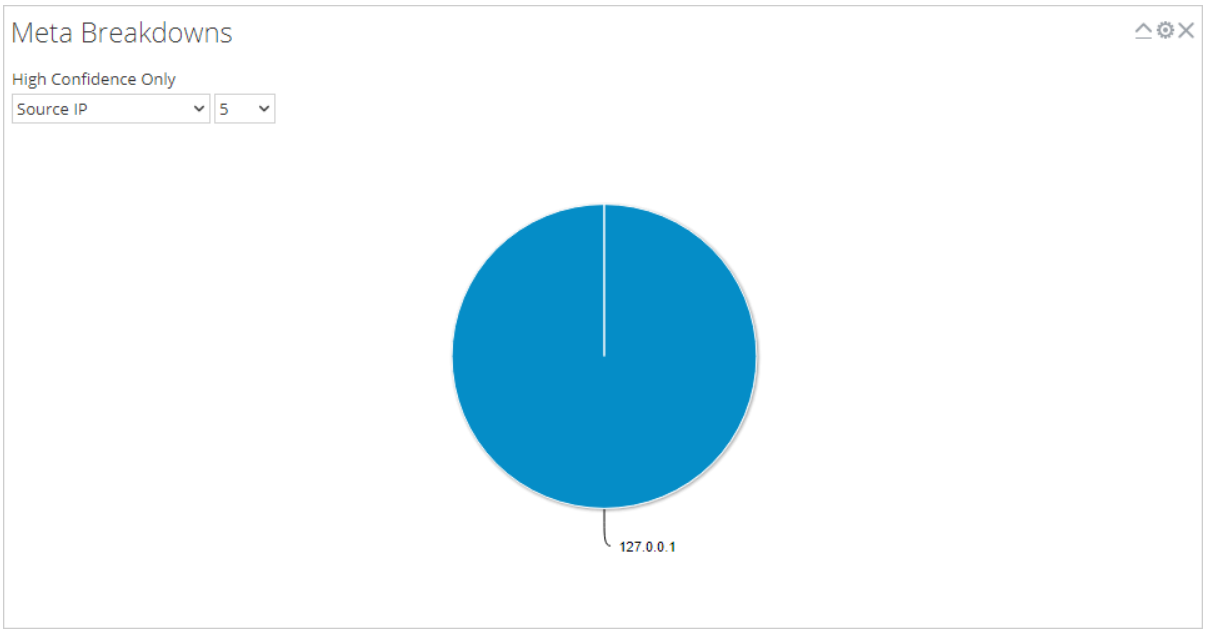
Dialogfeld „Optionen“

Im Dialogfeld „Optionen“ können Sie die Ergebnisse anpassen, die im Dashlet angezeigt werden. Sie öffnen dieses Dialogfeld, indem Sie oben rechts in den einzelnen Dashlets auf das Symbol klicken. In der folgenden Tabelle werden die Funktionen im Dialogfeld „Optionen“ beschrieben.

Funktion	Beschreibung
Titel	Gibt an, ob die angezeigten Daten auf Ereignisse beschränkt sind, die als hoch vertraulich markiert sind. Wenn die Daten nicht eingeschränkt sind, wird diese Zeile nicht angezeigt.
Nur durch hohe Wahrscheinlichkeit beeinflusst	Gibt an, ob die angezeigten Daten auf Ereignisse beschränkt sind, die als hoch vertraulich markiert sind.
Statisch, Netzwerk, Community, Sandbox	Hier können Sie die Ergebnisse basierend auf den Bewertungen in den Bewertungsmodulen filtern.
Abbrechen	Schließt das Dialogfeld, ohne die Änderungen zu speichern.
Anwenden	Wendet die Änderungen sofort auf das Dashlet an und schließt das Dialogfeld.

Meta-Strukturen

Meta-Strukturen präsentieren Ereignisse in der Form eines Tortendiagramms, in dem jedes Tortenstück einen Metawert für den angegebenen Metaschlüssel darstellt. Sie können den Metaschlüssel und die Anzahl der im Diagramm darzustellenden Metawerte für diesen Schlüssel auswählen, beginnend mit dem Metawert, der die meisten Ereignisse hat. Wenn Sie den Mauszeiger über das Ereignis bewegen, wird die Anzahl angezeigt.

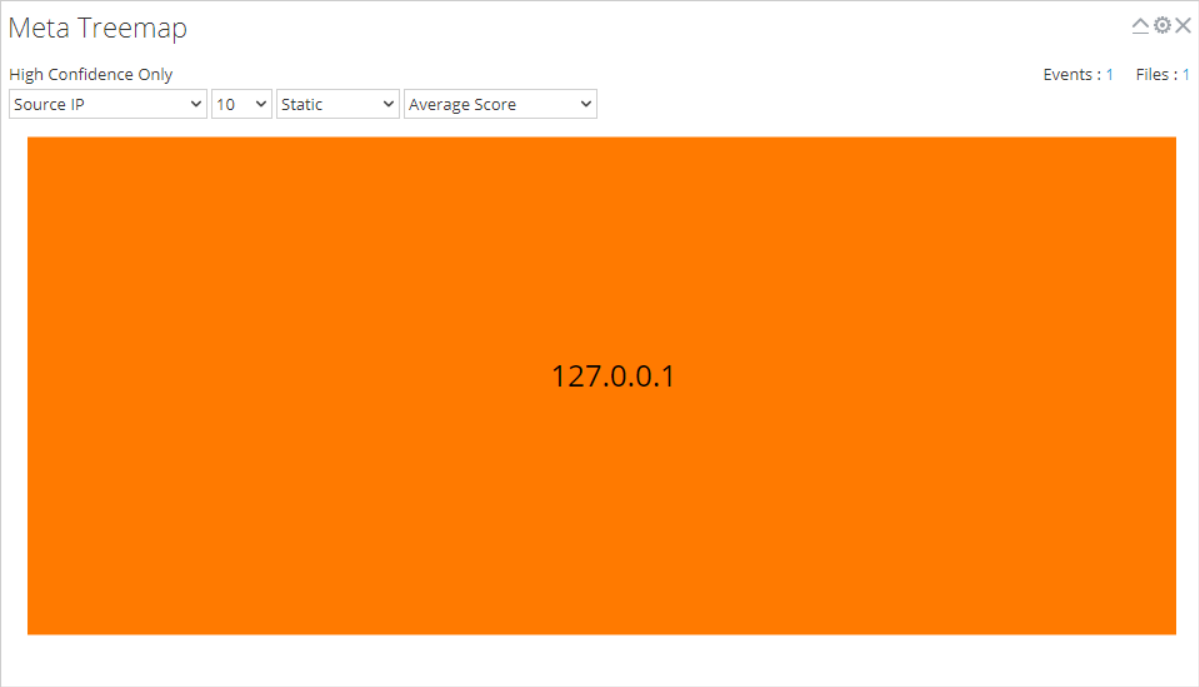


In der folgenden Tabelle sind die Optionen im Dashlet „Meta-Strukturen“ beschrieben.

Funktion	Beschreibung
Nur hohe Wahrscheinlichkeit	Gibt an, ob die angezeigten Daten auf Ereignisse beschränkt sind, die als hoch vertraulich markiert sind. Wenn die Daten nicht eingeschränkt sind, wird diese Zeile nicht angezeigt.
Metaschlüssel	Drop-down-Liste der verfügbaren Metaschlüssel
Count	Drop-down-Liste mit der Anzahl der besten Ergebnisse, die angezeigt werden

Meta-Treemap

Eine Meta-Treemap stellt Ereignisse in Form einer Heatmap dar. Sie können den Metaschlüssel und die Anzahl der im Diagramm darzustellenden Metawerte für diesen Schlüssel auswählen, beginnend mit den Metawerten, die die meisten Ereignisse haben. Darüber hinaus können Sie das Modul auswählen, das den Metawert in den Ereignissen erkannt hat: Static, Netzwerk, Community oder Sandbox.

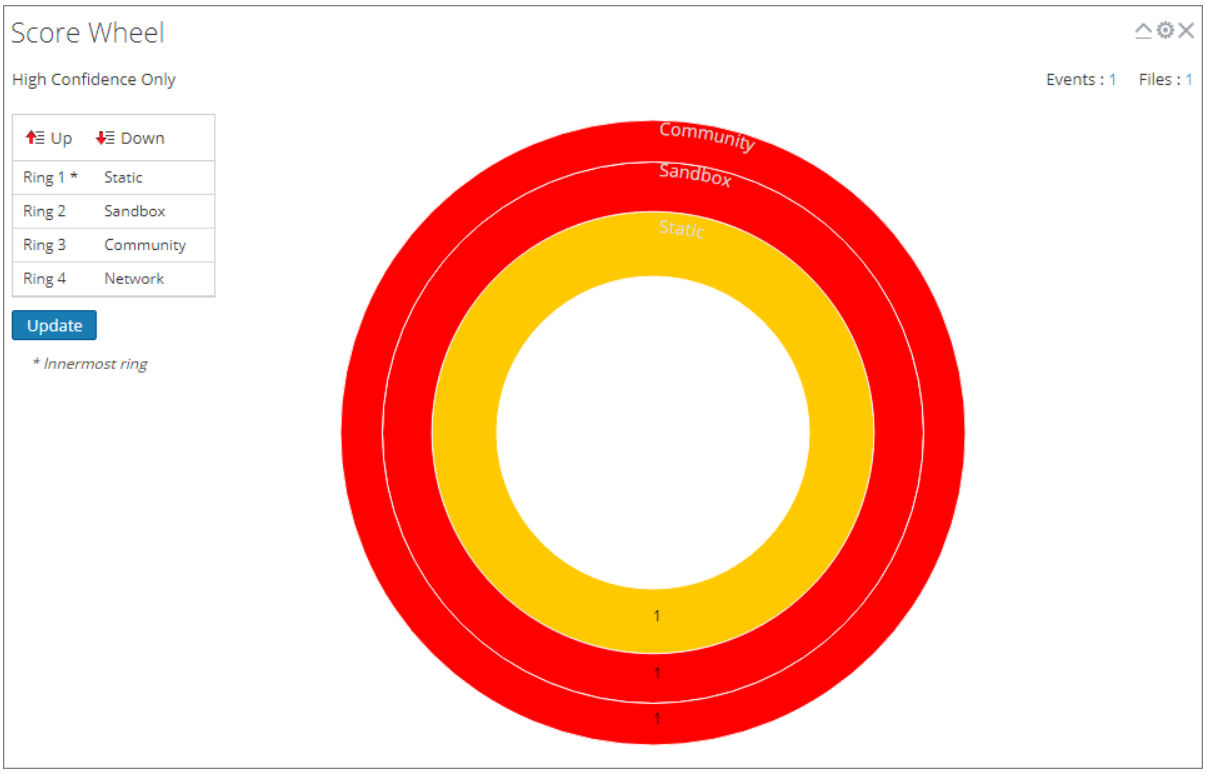


In der folgenden Tabelle sind die Optionen im Dashlet „Meta-Treemap“ beschrieben.

Funktion	Beschreibung
Nur hohe Wahrscheinlichkeit	Gibt an, ob die Ergebnisse auf Ereignisse beschränkt sind, die als hoch vertraulich markiert sind. Wenn die Ergebnisse nicht eingeschränkt sind, wird diese Zeile nicht angezeigt.
Metaschlüssel	Drop-down-Liste der verfügbaren Metaschlüssel, die als Filter ausgewählt werden können
Count	Drop-down-Liste mit der Anzahl der besten Ergebnisse, die angezeigt werden
Modul	Drop-down-Liste, in der angegeben wird, aus welchem Modul die Ergebnisse abgerufen werden
Wert	Drop-down-Liste mit den Informationen, die angezeigt werden, wenn die Maus über ein Ergebnis (z. B. Durchschnittliche Bewertung) bewegt wird

Ergebnisrad

Das Ergebnisrad bietet eine Ansicht der Ereignisse als konzentrische Ringe mit Farben, die Punktzahlen für Ereignisse darstellen, die auf Indikatoren für eine Infizierung und dem Bewertungsmodul basieren. Sie können die Position der Ringe mithilfe der Pfeile nach oben und nach unten anpassen, um eine Ansicht zu erhalten, die Ereignisse hervorhebt, die von einem Bewertungsmodul (rot) und nicht von anderen Bewertungsmodulen erkannt wurden.

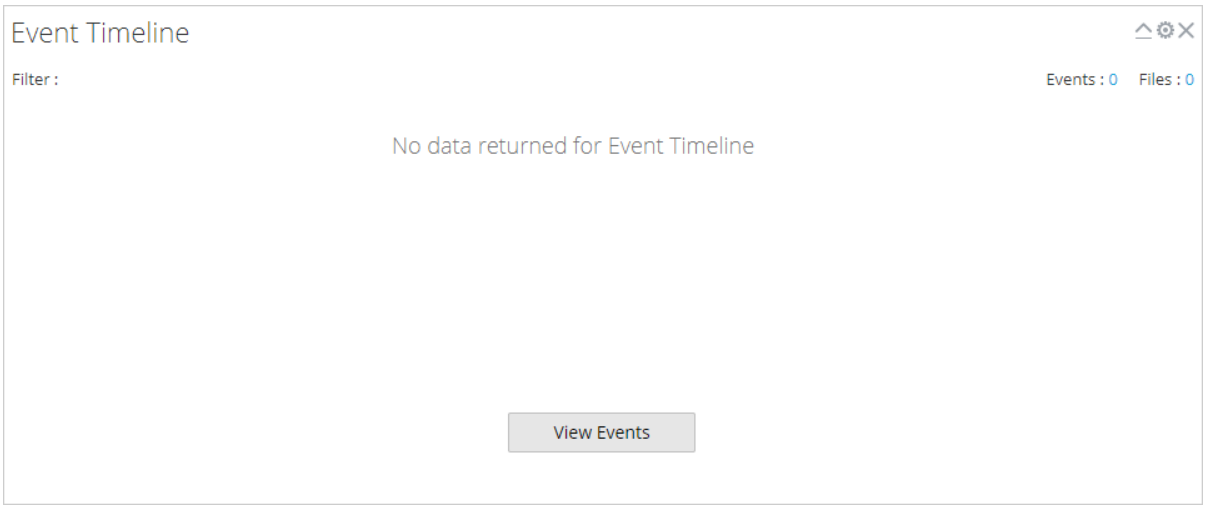


In der folgenden Tabelle werden die Funktionen im Dashlet „Ergebnisrad“ beschrieben.

Funktion	Beschreibung
Nur hohe Wahrscheinlichkeit	Gibt an, ob die Ergebnisse auf Ereignisse beschränkt sind, die als hoch vertraulich markiert sind. Wenn die Ergebnisse nicht eingeschränkt sind, wird diese Zeile nicht angezeigt.
Raster Modulreihenfolge	Zeigt die Reihenfolge der Ringe im Ergebnisrad an. Dabei ist Ring 1 der innerste Ring und Ring 4 der äußerste Ring. Sie können auf die Schaltflächen **Nach oben** und **Nach unten** klicken, um die Reihenfolge der Module zu ändern. Anschließend klicken Sie auf **Aktualisieren**, damit die Änderungen wirksam werden.

Ereigniszeitachse

In der Ereigniszeitachse wird eine Ansicht der Ereignisse angeboten, die nach dem Zeitpunkt ihres Auftretens in einem Balkendiagramm dargestellt sind. Wenn Sie klicken und ziehen, um einen Zeitbereich im Diagramm auszuwählen, wird die ausgewählte Zeit eingestellt.



In der folgenden Tabelle sind die Funktionen im Dashlet „Ereigniszeitachse“ beschrieben.

Funktion	Beschreibung
Nur hohe Wahrscheinlichkeit	Gibt an, ob die Ergebnisse auf Ereignisse beschränkt sind, die als hoch vertraulich markiert sind. Wenn die Ergebnisse nicht eingeschränkt sind, wird diese Zeile nicht angezeigt.
Ereignisse anzeigen	Zeigt die Ansicht „Investigation > Ereignisse“ an.

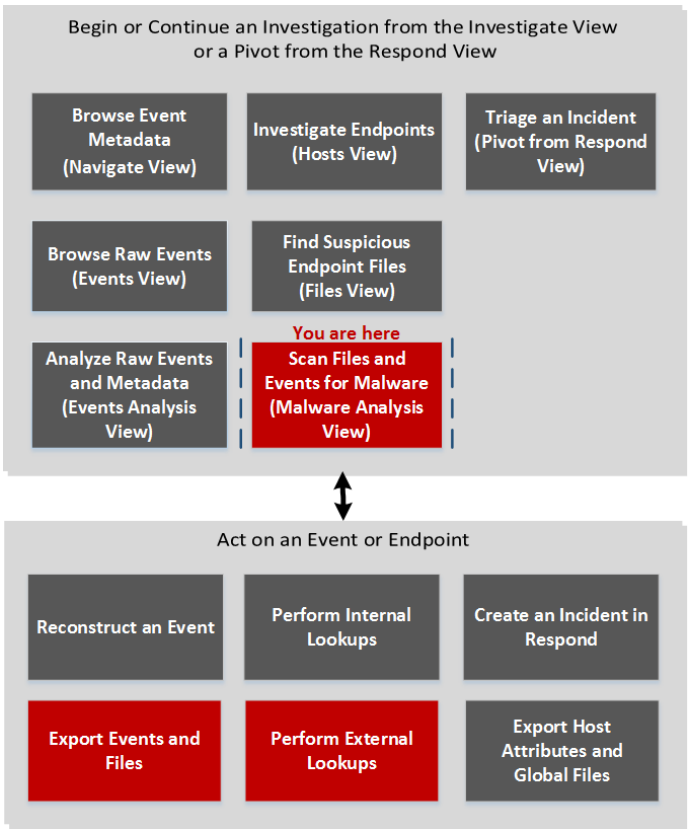
Malware Analysis-Ereignisliste und -Dateiliste

Die Malware Analysis-Ereignisliste und -Dateiliste bietet eine detaillierte Ansicht von Ereignissen oder Dateien. Sie können auf ein Ereignis oder eine Datei in jeder der Listen doppelklicken, um die Ansicht „Analyseergebnisse“ in einer neuen Registerkarte im Browser anzuzeigen.

Um auf diese Ansicht zuzugreifen, navigieren Sie zu **Ermittlung > Malware Analysis** > **Dialogfeld „Malware Analysis Service auswählen“**. Wählen Sie aus dem linken Bereich einen Service aus, wählen Sie dann im rechten Bereich einen Job aus und klicken Sie auf **Scan anzeigen**. Führen Sie in der Ansicht „Ereigniszusammenfassung“ einen der folgenden Schritte aus:

- Klicken Sie entweder im Bereich **Gesamt** oder im Bereich **Hohe Wahrscheinlichkeit** auf die Anzahl im Abschnitt **Erstellte Ereignisse**.
- Wenn Sie die Dateiliste anzeigen möchten, klicken Sie auf die Anzahl im Abschnitt **Verarbeitete Dateien**.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen*	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Exportieren von Ereignissen und Dateien*	Überprüfen von Scandateien und Ereignissen in Listenform
Threat Hunter	Durchführen externer Suchen*	Anzeigen der detaillierten Schadsoftwareanalyse eines Ereignisses

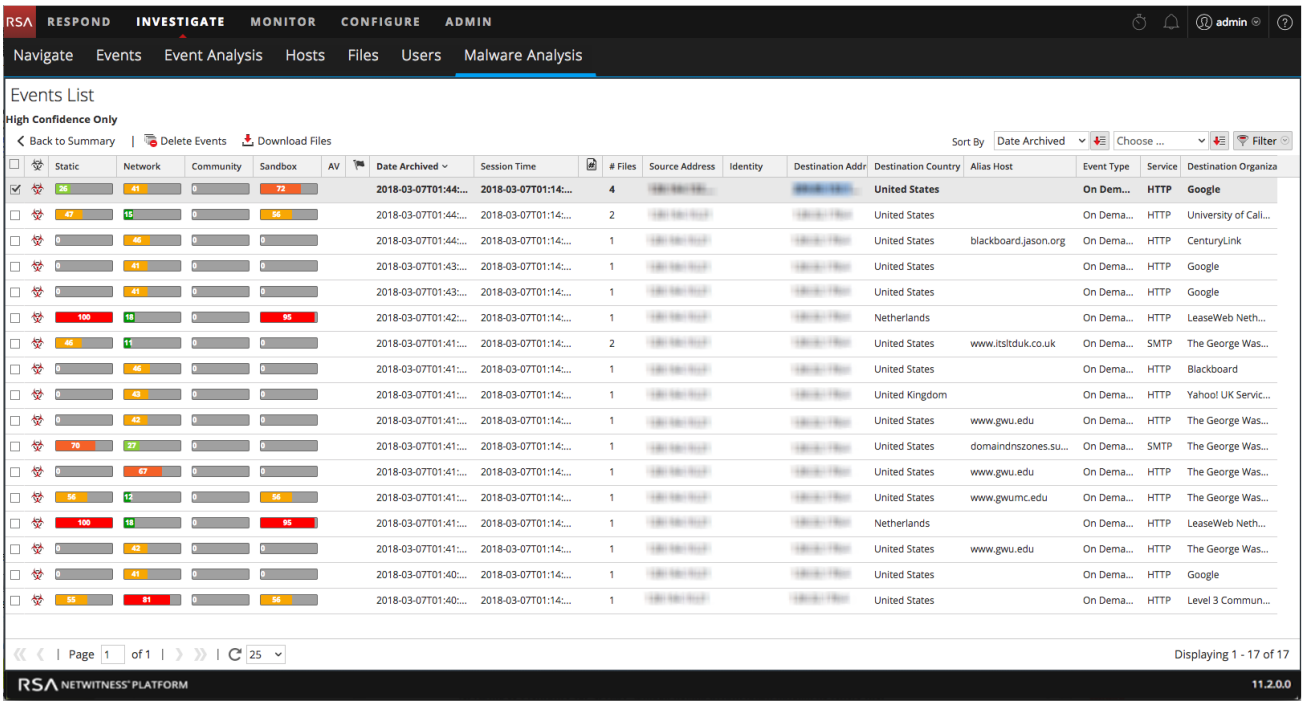
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

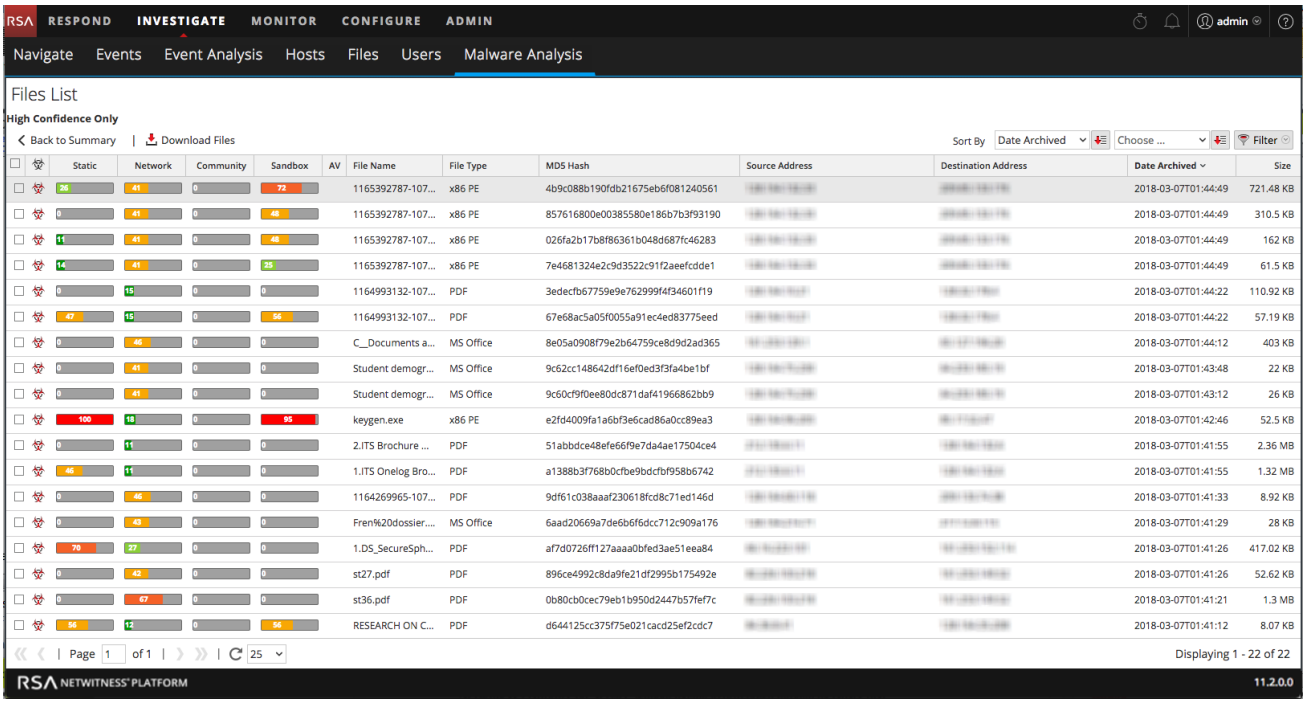
- Wie funktioniert NetWitness Investigate?

Überblick

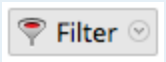
Dies ist ein Beispiel für die Ereignislistenansicht.



Dies ist ein Beispiel für die Ansicht „Dateiliste“.



Dies sind die Funktionen in der Symbolleiste „Ereignisliste“. Die Symbolleiste „Dateiliste“ ist mit dieser Symbolleiste identisch, außer dass sie keine Option zum Löschen von Ereignissen enthält.

Funktion	Beschreibung
Zurück zur Zusammenfassung	Kehrt zur Ansicht Ereigniszusammenfassung zurück.
Ereignisse löschen	Entfernt die ausgewählten Ereignisse aus der aktuellen Ereignisliste.
Dateien herunterladen	Zeigt das Dialogfeld „Schadsoftware-Dateidownload“ an, mit dem Sie verfügbare Dateien herunterladen können.
	Zeigt ein Drop-down-Menü an, aus dem Sie die Sortierreihenfolge der Liste auswählen können. Dies sind die Optionen für die Sortierung: • Hohe Wahrscheinlichkeit • Static • Netzwerk • Community • Sandbox • AV • Dateiname • Dateityp • Hash • Archivierungsdatum • Größe Die Schaltfläche direkt rechts neben dieser Drop-down-Liste zeigt an, ob die Liste aufsteigend oder absteigend sortiert wird.
	Zeigt ein Drop-down-Menü an, aus dem Sie eine zweite Sortierreihenfolge auswählen können. Dieses Menü enthält auch die OptionNetWitness Platform**Keine**, sodass die Auswahl einer zweiten Sortierreihenfolge nicht notwendig ist.
	Zeigt ein Drop-down-Fenster an, in dem Sie die Liste nach Dateinamen oder MD5-Hash filtern können.

Die Ereignisliste verfügt über folgende Funktionen.

Funktion	Beschreibung
	Zeigt an, ob das Ereignis durch die Kennzeichnung „Hohe Wahrscheinlichkeit“ beeinflusst ist.
Statisch, Netzwerk, Community, Sandbox	Zeigt die Bewertungen für jedes Bewertungsmodul an.

Funktion	Beschreibung
AV	Zeigt an, ob das Virenschutzprogramm dieses Ereignis als verdächtig gekennzeichnet hat.
	Zeigt an, ob das Ereignis durch eine angepasste Regel beeinflusst ist.
Archivierungsdatum	Zeigt Datum und Uhrzeit der Archivierung des Ereignisses an.
Sitzungszeit	Zeigt die Uhrzeit der Sitzung des Ereignisses an.
	Zeigt an, ob der Hash-Wert als vertrauenswürdig gekennzeichnet ist.
Anzahl Dateien	Zeigt die Anzahl der im Ereignis enthaltenen Dateien an.
Quelladresse	Zeigt die Adresse der Ereignisquelle an.
Identität	Zeigt die Identität der Ereignisquelle an.
Zieladresse	Zeigt die Adresse des Ereignisziels an.
Zielland	Zeigt das Land des Ereignisziels an.
Aliashost	Zeigt den Hostnamen des Alias an.
Ereignistyp	Gibt den Ereignistyp an. Zum Beispiel Manuell hochladen.
Service	Zeigt den Service an, auf dem das Ereignis geschah.
Zielorganisation	Zeigt die Organisation des Ziels an.

Das Dateilistenraster verfügt über folgende Funktionen.

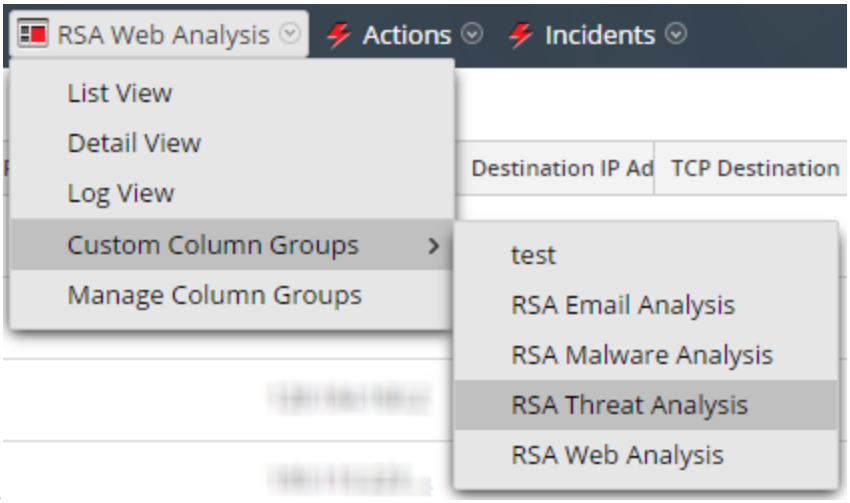
Funktion	Beschreibung
	Zeigt an, ob das Ereignis durch die Kennzeichnung „Hohe Wahrscheinlichkeit“ beeinflusst ist.
Statisch, Netzwerk, Community, Sandbox	Zeigt die Bewertungen für jedes Bewertungsmodul an.
AV	Zeigt an, ob das Virenschutzprogramm dieses Ereignis als verdächtig gekennzeichnet hat.
Dateiname	Zeigt den Namen der Datei an.
Dateityp	Zeigt den Typ der Datei an (z. B., PDF oder x86 PE)
MD5-Hash	Zeigt den MD5-Hash an.
Quelladresse	Zeigt die Adresse der Dateiquelle an.
Zieladresse	Zeigt die Adresse des Dateiziels an.

Funktion	Beschreibung
Archivierungsdatum	Zeigt Datum und Uhrzeit der Archivierung der Datei an.
Größe	Zeigt die Größe der Datei an.

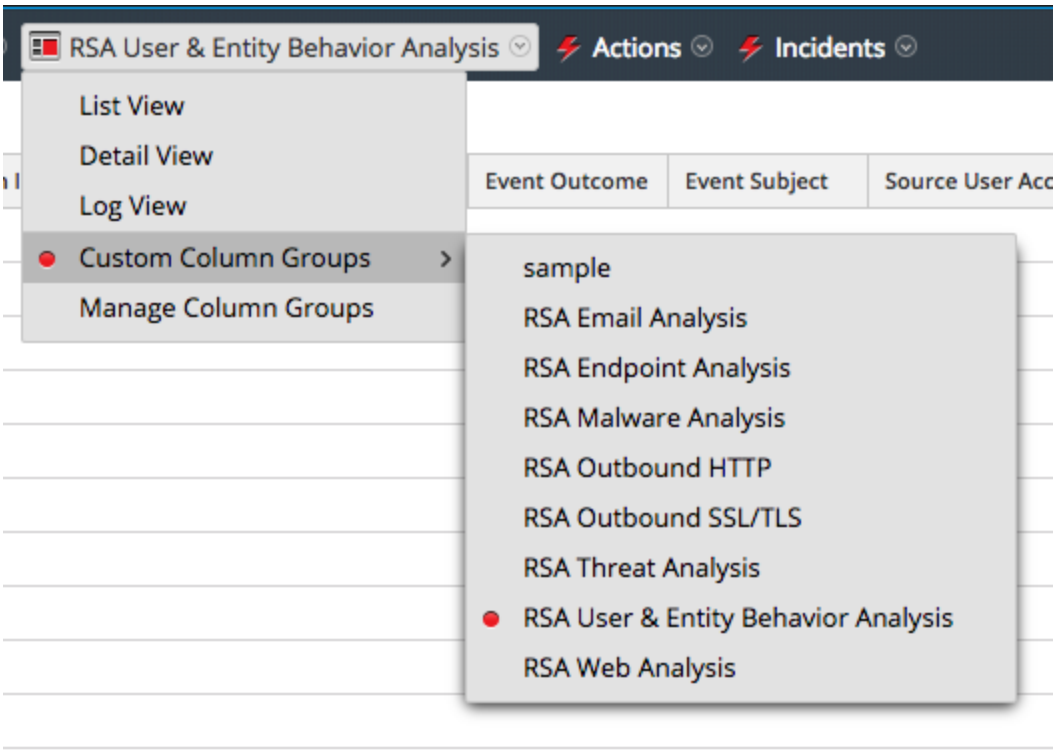
Dialogfeld „Spaltengruppen managen“

Sie können die Art der Anzeige von Daten anpassen, indem Sie die in einer Spalte anzuzeigenden Metadaten, die Spaltenposition im Raster und die Standardspaltenbreite festlegen. Im Dialogfeld „Spaltengruppen managen“ können Sie zum Anzeigen bestimmter Metaschlüssel Spaltengruppen hinzufügen, löschen, importieren, exportieren und bearbeiten. Nach der Neuinstallation sind OOTB-Spaltengruppen (Out-of-the-Box) für die Verwendung im Dialogfeld „Spaltengruppen managen“ verfügbar. Zur Identifizierung wird den OOTB-Spaltengruppen, die dupliziert, aber nicht gelöscht werden können, das Präfix RSA vorangestellt. Sie können auch benutzerdefinierte Spaltengruppen erstellen.

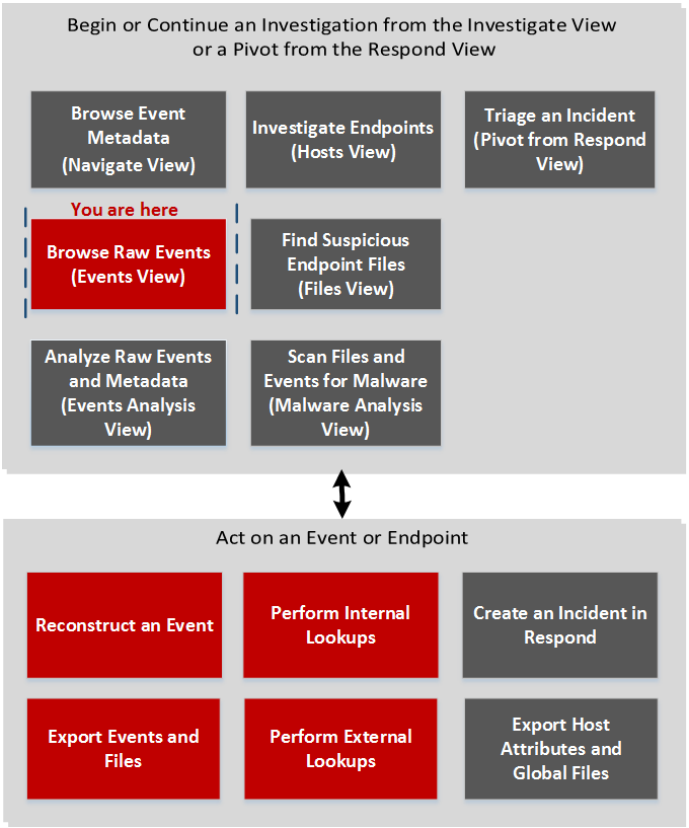
Um auf dieses Dialogfeld zuzugreifen, navigieren Sie zu **Ermittlung > Ereignisse** und wählen in der Drop-Down-Liste **Ansicht** die Option **Spaltengruppen managen** aus. Die Option **Ansicht** wird nach dem aktuellen Wert benannt, z. B. Detailansicht, Listenansicht, Protokollansicht, oder nach der aktuell



ausgewählten Spaltengruppe.


RSA User & Entity Behavior Analysis
Actions
Incidents
List View
Detail View
Log View
Custom Column Groups
Manage Column Groups
Event Outcome
Event Subject
Source User Acc
sample
RSA Email Analysis
RSA Endpoint Analysis
RSA Malware Analysis
RSA Outbound HTTP
RSA Outbound SSL/TLS
RSA Threat Analysis
RSA User & Entity Behavior Analysis
RSA Web Analysis

Workflow


Begin or Continue an Investigation from the Investigate View or a Pivot from the Respond View
Browse Event Metadata (Navigate View)
Investigate Endpoints (Hosts View)
Triage an Incident (Pivot from Respond View)
You are here
Browse Raw Events (Events View)
Find Suspicious Endpoint Files (Files View)
Analyze Raw Events and Metadata (Events Analysis View)
Scan Files and Events for Malware (Malware Analysis View)
Act on an Event or Endpoint
Reconstruct an Event
Perform Internal Lookups
Create an Incident in Respond
Export Events and Files
Perform External Lookups
Export Host Attributes and Global Files

Was möchten Sie tun?

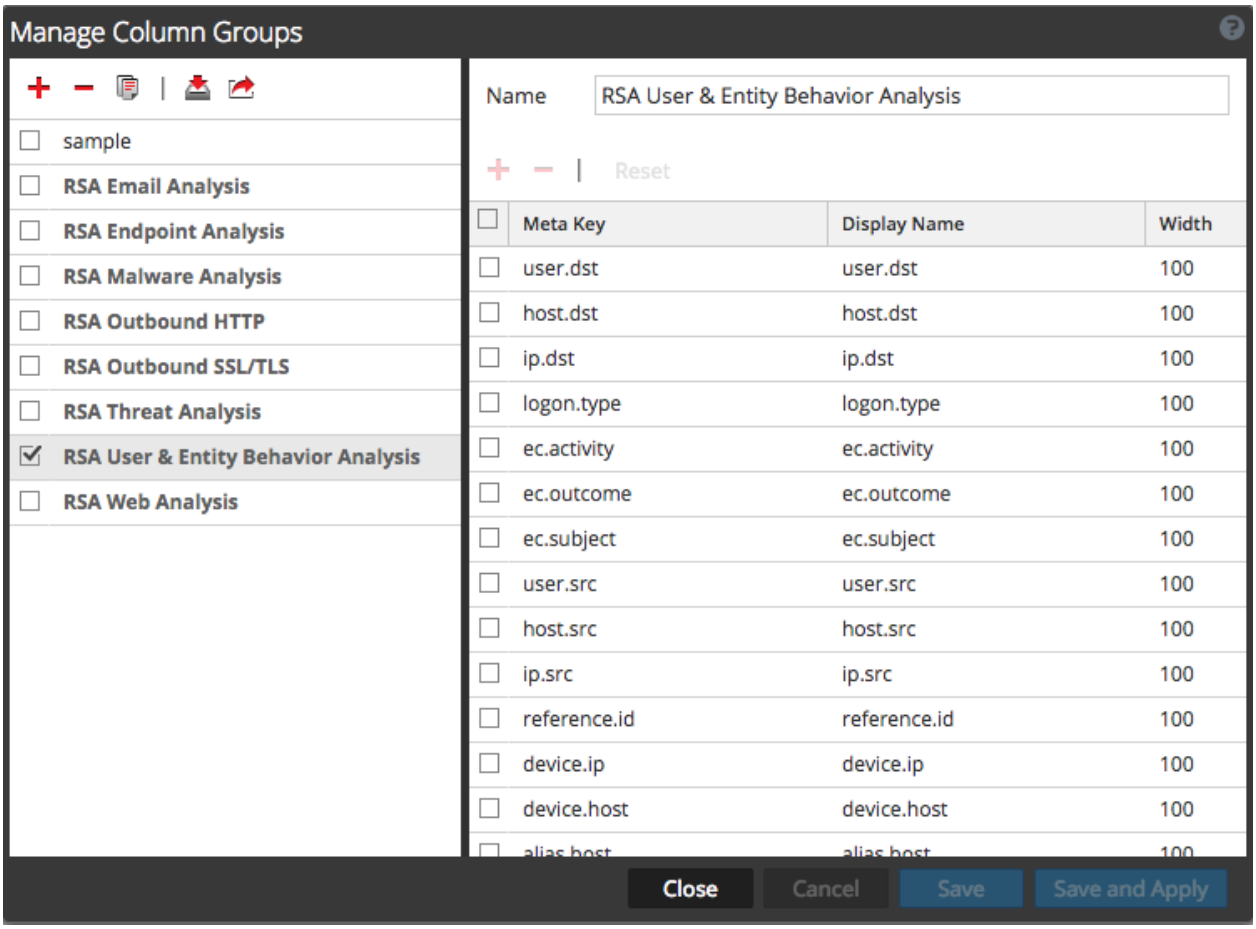
Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Konfigurieren von Spaltengruppen	Managen von Spaltengruppen in der Ansicht „Ereignisse“

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Ereignisse“

Überblick



Das Dialogfeld „Spaltengruppen managen“ umfasst zwei Bereiche: Gruppen und Einstellungen.

Unten in diesem Dialogfeld befinden sich vier Schaltflächen: Schließen, Abbrechen, Speichern und Speichern und übernehmen. In der folgenden Tabelle werden diese Schaltflächen beschrieben.

Funktion	Beschreibung
Schließen	Schließt das Dialogfeld, ohne zu speichern
Abbrechen	Verwirft alle ungespeicherten Änderungen
Speichern	Speichert alle Änderungen, ohne das Dialogfeld zu schließen
Speichern und übernehmen	Speichert und wendet alle Änderungen sofort an und schließt das Dialogfeld

Bereich „Gruppen“

Der linke Bereich ist der Bereich „Gruppen“. Hier können Sie Spaltengruppen hinzufügen, löschen, importieren oder exportieren. Oben in dem Bereich finden Sie eine Symbolleiste mit Aktionen. Unter der Symbolleiste wird eine Liste hinzugefügter Spaltengruppen angezeigt, in der Sie eine oder mehrere Gruppen auswählen können.

In der folgenden Tabelle sind die Aktionen in der Symbolleiste aufgeführt.

Aktion	Beschreibung
	Fügt eine Spaltengruppe hinzu. Durch Klicken auf diese Schaltfläche wird der Bereich Einstellungen auf der rechten Seite hervorgehoben, in dem Sie die Spaltengruppe benennen und Metaschlüssel hinzufügen oder löschen können. Es ist mindestens ein Metaschlüssel erforderlich, um eine Gruppe hinzuzufügen.
	Löscht eine Spaltengruppe. Es wird ein Bestätigungsdialogfeld angezeigt, bevor die ausgewählte Gruppe gelöscht wird.
	Zeigt das Dialogfeld „Spaltengruppen importieren“ an, in dem Sie eine hochzuladende Datei auswählen können.
	Exportiert eine oder mehrere ausgewählte Gruppen auf Ihren Computer.

Bereich Einstellungen

Der rechte Bereich ist der Bereich Einstellungen. Hier können Sie Spaltengruppen erstellen und bearbeiten. Dieser Bereich enthält das Feld Name, eine Symbolleiste und ein Raster.

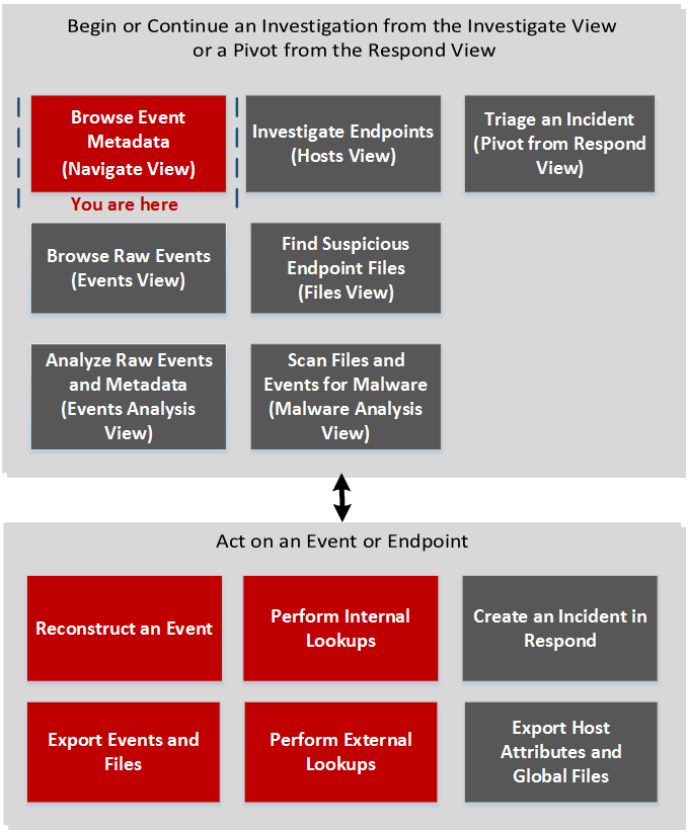
In der folgenden Tabelle sind die Funktionen des Bereichs „Einstellungen“ beschrieben.

Funktion	Beschreibung
Name	Der Name der ausgewählten Spaltengruppe.
	Fügt der Liste der Metaschlüssel eine neue Zeile hinzu, in der Sie zum Auswählen eines neuen Metaschlüssels ein Drop-down-Menü öffnen können.
	Löscht einen oder mehrere ausgewählte Metaschlüssel. Vor dem Löschen wird ein Bestätigungsdialogfeld angezeigt.
Zurücksetzen	Setzt die Spaltengruppe auf die zuletzt gespeicherten Einstellungen zurück.
Metaschlüssel	Listet alle der ausgewählten Spaltengruppe hinzugefügten Metaschlüssel auf.
Angezeigter Name	Listet die Namen der Metaschlüssel so auf, wie sie in der Ansicht Ereignisse angezeigt werden.
Breite	Legt die Breite der Spalte jedes Metaschlüssels fest. Als Grenze können Sie einen Wert zwischen **10** und **1.000** verwenden. Die Standardbreite ist **100**.

Dialogfeld „Standardmetaschlüssel managen“

Im Dialogfeld „Standardmetaschlüssel managen“ können Analysten die Metaschlüssel angeben, die bei der Navigation in einem bestimmten Service angezeigt werden sollen. Dies ist hilfreich, um die gewünschten Daten schneller zu finden und das Laden von Metadaten, die nicht von Interesse sind, zu vermeiden. Wählen Sie in der Symbolleiste der Ansicht **Navigieren** die Option **Meta > Standardmetaschlüssel managen** aus, um dieses Dialogfeld zu öffnen.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Standardmetaschlüssel für einen Service konfigurieren*	Filtern von Ergebnissen in der Ansicht „Navigation“

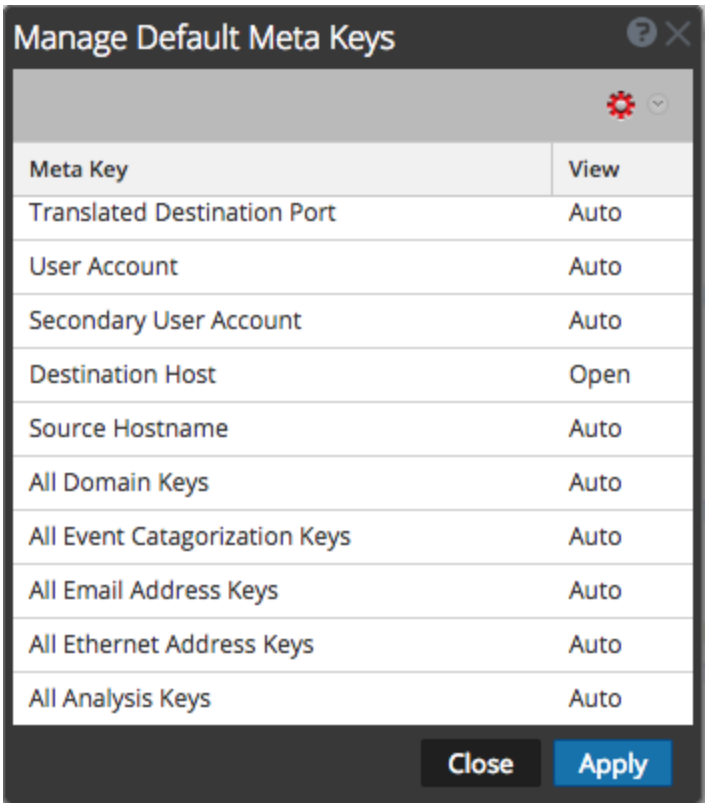
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Metagruppen managen
- Metagruppen managen

Überblick

Die folgende Abbildung zeigt das Dialogfeld „Standardmetaschlüssel managen“, das eine Liste der Metaschlüssel, eine Symbolleiste sowie die Schaltflächen „Schließen“ und „Anwenden“ enthält. In der Liste können Sie Standardmetaschlüssel anzeigen, sortieren und managen. Durch Klicken und Ziehen können Sie die Reihenfolge der Metaschlüssel ändern. In der folgenden Tabelle sind die Spalten der Liste beschrieben.



Spalte	Beschreibung
Metaschlüssel	In dieser Spalte werden die Metaschlüssel aufgeführt, die für den Service verfügbar sind. Ab Version 11.1 sind auch Standardmetaentitäten enthalten, z. B. „Alle Domainschlüssel“ und „Alle E-Mail-Adressschlüssel“.

Spalte	Beschreibung
Ansicht	In dieser Spalte wird der Ansichtstyp angegeben, der den einzelnen Metaschlüsseln zugeordnet ist. Durch Klicken auf die Ansicht in jeder Zeile können Sie dem Metaschlüssel eine andere Standardansicht zuordnen. Es gibt vier verschiedene Ansichten: • Auto: Setzt die Metaschlüssel auf die in der Serviceindexdatei angegebene Standardansicht zurück. • Geschlossen: Die Werte dieses Metaschlüssels sind standardmäßig geschlossen und können manuell geöffnet werden. • Ausgeblendet: Diese Metaschlüssel sind standardmäßig ausgeblendet und werden in Investigation gar nicht angezeigt. • Offen: Die Werte dieses Metaschlüssels werden standardmäßig angezeigt. Wenn Sie die Standardmetaschlüssel für einen nicht indizierten Metaschlüssel ändern, können Sie den Schlüssel nicht auf **Offen** einstellen. Wenn Sie die Standardansicht für eine Gruppe von Metaschlüsseln in **Offen** ändern und einige der Metaschlüssel nicht indiziert sind, werden die nicht indizierten Metaschlüssel auf **Auto** zurückgesetzt. Daher wird der Metaschlüssel nur automatisch geladen, wenn er indiziert ist, und nicht indizierte Metaschlüssel haben den Status **Geschlossen**, bis sie manuell geöffnet werden.

In der folgenden Tabelle sind die Optionen und Schaltflächen der Symbolleiste beschrieben.

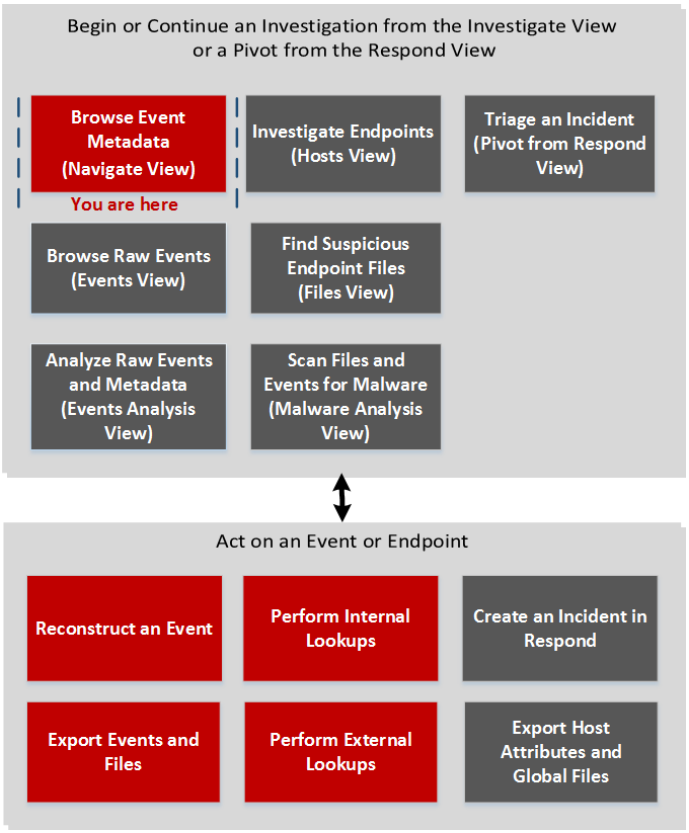
Funktion	Beschreibung
	Durch Klicken auf das Menü „Aktionen“ können Sie die Standardansicht für alle Metaschlüssel ändern. Es gibt vier verschiedene Ansichten: • Auto: Setzt die Metaschlüssel auf die in der Serviceindexdatei angegebene Standardansicht zurück. • Geschlossen: Die Werte dieses Metaschlüssels sind standardmäßig geschlossen. • Ausgeblendet: Die Werte dieses Metaschlüssels sind standardmäßig ausgeblendet. • Offen: Die Werte dieses Metaschlüssels werden standardmäßig angezeigt.
Schließen	Schließt das Dialogfeld. Alle nicht gespeicherten Änderungen gehen verloren.
Anwenden	Wendet alle Änderungen an. Diese werden sofort wirksam.

Dialogfeld „Metagruppen managen“

Nach der Neuinstallation sind im Dialogfeld „Metagruppen managen“ OOTB-Metagruppen verfügbar. Zur Identifizierung wird den OOTB-Metagruppen, die dupliziert, aber nicht gelöscht werden können, das Präfix RSA vorangestellt. Im Dialogfeld „Metagruppen managen“ können Sie Metagruppen hinzufügen, löschen, importieren und exportieren.

Wählen Sie in der Symbolleiste der Ansicht **Investigation > Navigieren** die Option **Meta > Metagruppen managen** aus, um dieses Dialogfeld zu öffnen.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Metagruppen hinzufügen, bearbeiten und löschen*	Metagruppen managen

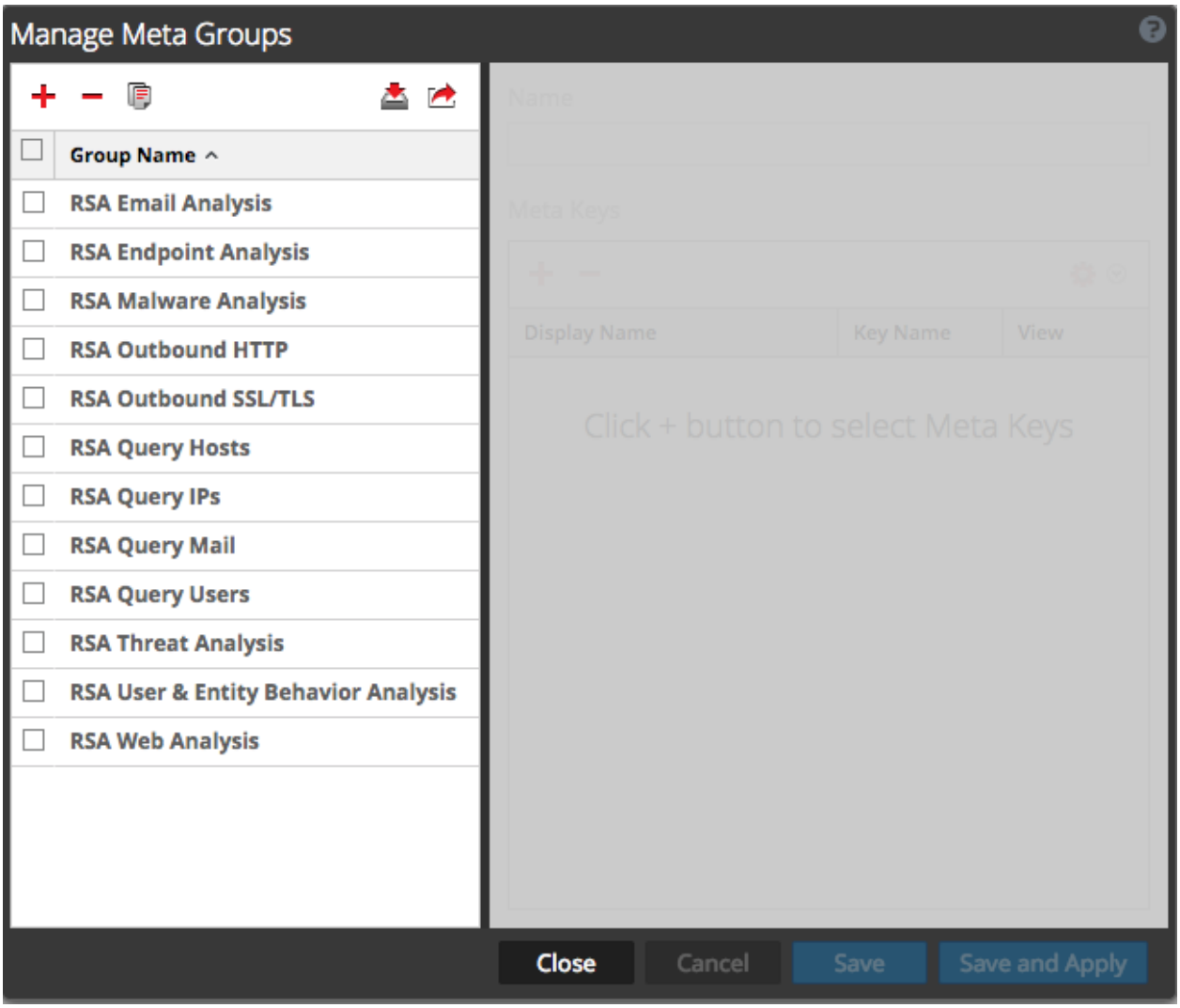
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Filtern von Ergebnissen in der Ansicht „Navigation“
- Wie funktioniert NetWitness Investigate?

Überblick

Es folgt ein Beispiel des Dialogfelds für Version 11.1, in dem zusätzliche OOTB-Metagruppen verfügbar sind: RSA Endpoint Analysis, RSA Outbound HTTP und RSA Outbound SSL/TLS. Das Dialogfeld „Metagruppen managen“ hat zwei Bereiche. In der folgenden Tabelle werden die Schaltflächen unten im Dialogfeld beschrieben.



Funktion	Beschreibung
Schließen	Schließt das Dialogfeld.
Abbrechen	Bricht alle Änderungen ab.
Speichern	Speichert alle Änderungen.
Speichern und übernehmen	Speichert alle Änderungen und wendet sie unmittelbar an.

Der Bereich „Metagruppen“ befindet sich auf der linken Seite des Dialogfelds „Metagruppen managen“. Dies ist der Bereich, in dem Sie Metagruppen hinzufügen, löschen, importieren und exportieren können.

In der folgenden Tabelle werden die Funktionen im Bereich „Metagruppen“ beschrieben.

Funktion	Beschreibung
	Fügt über den Bereich „Einstellungen“ auf der rechten Seite des Dialogfelds „Metagruppen managen“ eine Metagruppe hinzu.
	Löscht die ausgewählte Metagruppe. Es wird ein Bestätigungsdialogfeld angezeigt, bevor die Metagruppe gelöscht wird.
	Zeigt das Dialogfeld „Metagruppenimport“ an, mit dem Sie eine Datei hochladen können.
	Exportiert die ausgewählte Metagruppe auf Ihren Computer.
Gruppenname	Listet alle Metagruppennamen auf.

Der Bereich „Einstellungen“ befindet sich auf der rechten Seite des Dialogfelds „Metagruppen managen“. Dies ist der Bereich, in dem Sie Metagruppen erstellen und bearbeiten können. Unter dem Feld Name ist das Raster Metaschlüssel.

In der folgenden Tabelle sind die Funktionen des Bereichs „Einstellungen“ beschrieben.

Funktion	Beschreibung
Name	Zeigt den Namen der ausgewählten Metagruppe an.
	Zeigt das Dialogfeld „Verfügbare Metaschlüssel“ an, in dem Sie Metaschlüssel auswählen können, die der Gruppe hinzugefügt werden.
	Löscht die ausgewählten Metaschlüssel.
	Zeigt ein Drop-down-Menü an, in dem Sie die Ansicht für alle Metaschlüssel auswählen können. Es gibt vier Optionen, denen die möglichen Werte der Eigenschaft `defaultAction` zugrunde liegen, die zur Definition eines Schlüssels in der benutzerdefinierten Indexdatei für den Service dienen: • Ausgeblendet: Diese Metaschlüssel sind standardmäßig ausgeblendet und werden in Investigation gar nicht angezeigt. • Offen: Die Werte dieses Metaschlüssels werden standardmäßig angezeigt. • Geschlossen: Die Werte dieses Metaschlüssels sind standardmäßig geschlossen und können manuell geöffnet werden. • Auto: Setzt die Metaschlüssel auf die in der Serviceindexdatei angegebene Standardansicht zurück.
Angezeigter Name	Gibt den in den Ansichten von Investigation für den Schlüssel angezeigten Namen an. Wird durch die Eigenschaft `description` definiert, die für den Schlüssel in der benutzerdefinierten Indexdatei für den Service enthalten ist.
Schlüsselname	Gibt den in der benutzerdefinierten Indexdatei für den Service festgelegten `name` des Metaschlüssels an.

Funktion	Beschreibung
Ansicht	Gibt die Ansicht an, die für den Metaschlüssel festgelegt ist. Sie können die Ansicht mithilfe einer der folgenden Methoden ändern: • Klicken Sie in der Spaltenüberschrift „Ansicht“ auf **v** und wählen Sie dann eine Ansicht aus, um alle Metaschlüsselansichten zu ändern. • Klicken Sie in der Spalte „Ansicht“ auf einen Metaschlüssel. Öffnen Sie dann das Drop-down-Menü, in dem alle verfügbaren Ansichten enthalten sind, um die Ansicht für einen einzelnen Metaschlüssel zu ändern.

Dialogfeld „Profile managen“

Mit Profilen können Sie benutzerdefinierte Ansichten in den Ansichten „Navigation“ und „Ereignisse“ einrichten. Nach der Neuinstallation sind im Dialogfeld „Profile managen“ OOTB-Profile verfügbar. Zur Identifizierung wird den OOTB-Profilen, die dupliziert, aber nicht gelöscht werden können, das Präfix RSA vorangestellt. Im Dialogfeld „Profile managen“ können Sie Profile konfigurieren, hinzufügen, löschen, importieren und exportieren. Ab Version 11.2 können Sie Profile in Profilgruppen organisieren.

Um dieses Dialogfeld zu öffnen, wählen Sie in der Symbolleiste der Ansicht **Investigation > Navigieren** oder **Ereignisse Profil > Profile managen** aus.

Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Konfigurieren von Profilen für die Ansichten „Navigation“ und „Ereignisse“*	Einkapseln von benutzerdefinierten Ansichten mithilfe von Profilen

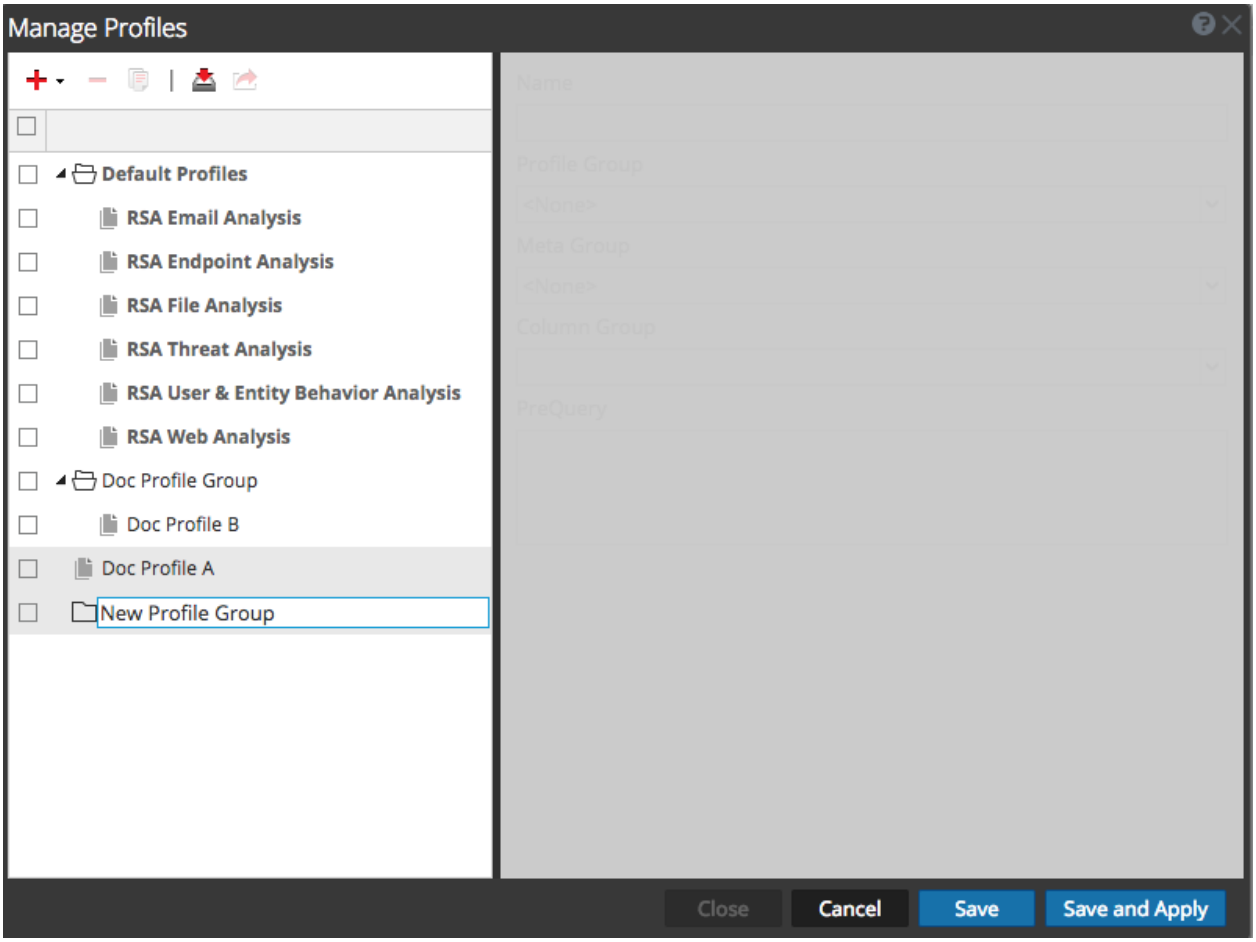
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Navigation“
- Ansicht „Ereignisse“

Überblick

Dies ist ein Beispiel des Dialogfelds „Profile managen“ mit mehreren Profilgruppen.



Das Dialogfeld „Profile managen“ hat zwei Bereiche. Im unteren Teil des Dialogfelds befindet sich eine Reihe mit Schaltflächen. Die Schaltflächen werden in der folgenden Tabelle beschrieben.

Feld	Beschreibung
Schließen	Schließt das Dialogfeld.
Abbrechen	Bricht alle Änderungen ab.
Speichern	Speichert alle Änderungen.
Speichern und übernehmen	Speichert und übernimmt alle Änderungen sofort.

Im Bereich „Profil“ auf der linken Seite des Dialogfelds werden die verfügbaren Profile angezeigt. Hier können Sie Profile hinzufügen, löschen, importieren und exportieren. In der folgenden Tabelle werden die Felder im Bereich „Profil“ beschrieben.

Feld	Beschreibung
	Fügt über den Bereich „Einstellungen“ auf der rechten Seite des Dialogfelds „Profile managen“ ein Profil hinzu.
	Löscht das ausgewählte Profil. Vor dem Löschen des Profils wird ein Bestätigungsdialogfeld angezeigt.
	Zeigt das Dialogfeld „Profilimport“ an, in dem Sie eine Datei hochladen können.
	Exportiert das ausgewählte Profil auf Ihren Computer.
Profilname	Listet alle Profilnamen auf.

Im Bereich „Einstellungen“ auf der rechten Seite des Dialogfelds werden Optionen zum Konfigurieren von Profilen angezeigt. Er kann nur verwendet werden, wenn ein Profil ausgewählt ist. In der folgenden Tabelle werden die Felder im Bereich „Einstellungen“ beschrieben.

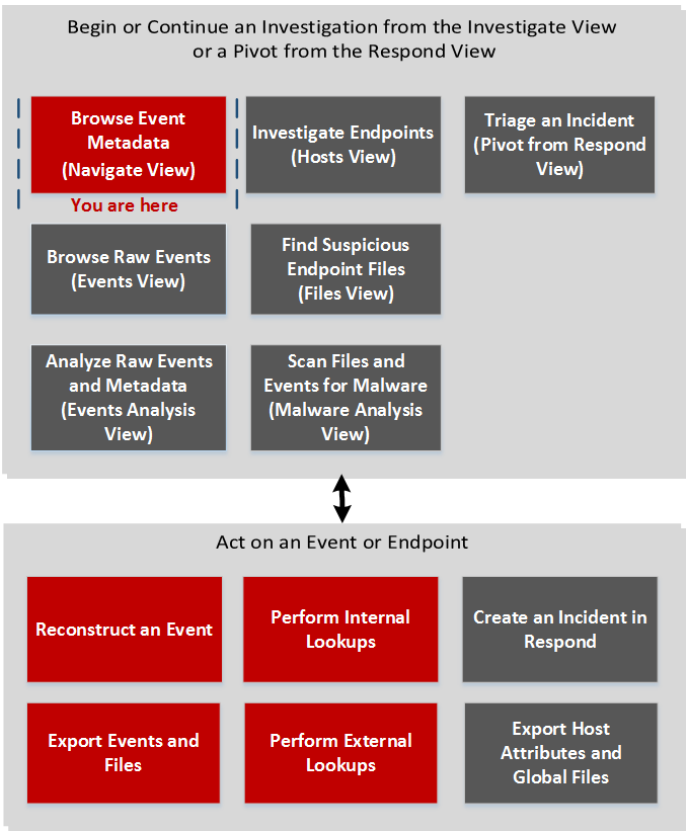
Funktion	Beschreibung
Name	Zeigt den Namen des Profils an.
Metagruppe	Zeigt ein Drop-down-Menü mit einer Liste der verfügbaren Metagruppen an.
Spaltengruppe	Zeigt ein Drop-down-Menü mit einer Liste der verfügbaren Spaltengruppen an. Standardmäßig sind drei Gruppen verfügbar: • Listenansicht • Detailansicht • Protokollansicht
Vorabfrage	Definiert eine einschränkende Abfrage zur Filterung von Investigation-Ergebnissen. Diese Abfrage wird verwendet, wenn das zugehörige Profil aktiviert ist und die Vorabfrage auf Abfragen zutrifft, die in den Ansichten „Investigation > Navigieren“ und „Ereignisse“ verwendet werden. Dies ist ein Beispiel für eine Vorabfrage: `'service=80,25,110'`.

Ansicht „Navigation“

Die Ansicht „Navigation“ (**Ermittlung** > Navigieren) zeigt Ereignismetadaten an – die Metaschlüssel und Metawerte –, die in erfassten Daten für den ausgewählten Service gefunden wurden. Die Daten werden in Übereinstimmung mit den Optionen, die Sie für Profil, Zeitbereich, Metagruppe und Abfrage festgelegt haben, gefiltert und angezeigt. Sie können auch einen Drill-down in die Daten durchführen, indem Sie auf Metaschlüssel und Metawerte klicken. Die Ansicht „Navigation“ ist der Standardeinstiegspunkt in NetWitness Investigate. Sie können den Standardeinstiegspunkt in den Profilvoreinstellungen zu einer der anderen Ansichten ändern.

Workflow

Die Abbildung unten zeigt den allgemeinen Workflow für die Untersuchung von Ereignismetadaten.



Hierbei handelt es sich um die Aufgaben, die Sie in der Ansicht „Navigation“ durchführen können:

- Auswählen eines Services zum Untersuchen und Laden von Daten.
- Anzeigen der Abfrageergebnisse und Filtern nach „Zeitbereich“, „Profil“, „Metagruppe“.
- Sortieren der Ergebnisse und Auswählen einer Quantifizierungsmethode.
- Ereignisse speichern, Wechseln zu einem Ereignis anhand der Ereignis-ID, Anzeigen eines Ereignisses und Drucken des Ereignisses.

- Anzeigen zusätzlicher Kontextdaten für bestimmte Metaschlüssel und Werte.
- Navigieren Sie zu Ansicht „Ereignisse“ oder zur Ansicht „Ereignisanalyse“, wo Sie eine chronologische Liste der Ereignisse anzeigen, ein Ereignis rekonstruieren und eine interaktive Analyse eines Ereignisses durchführen können. Beim Anzeigen und Analysieren von Ereignissen können Sie Ereignisse, Dateien und Protokolle in Ihr lokales Dateisystem exportieren.

Was möchten Sie tun?

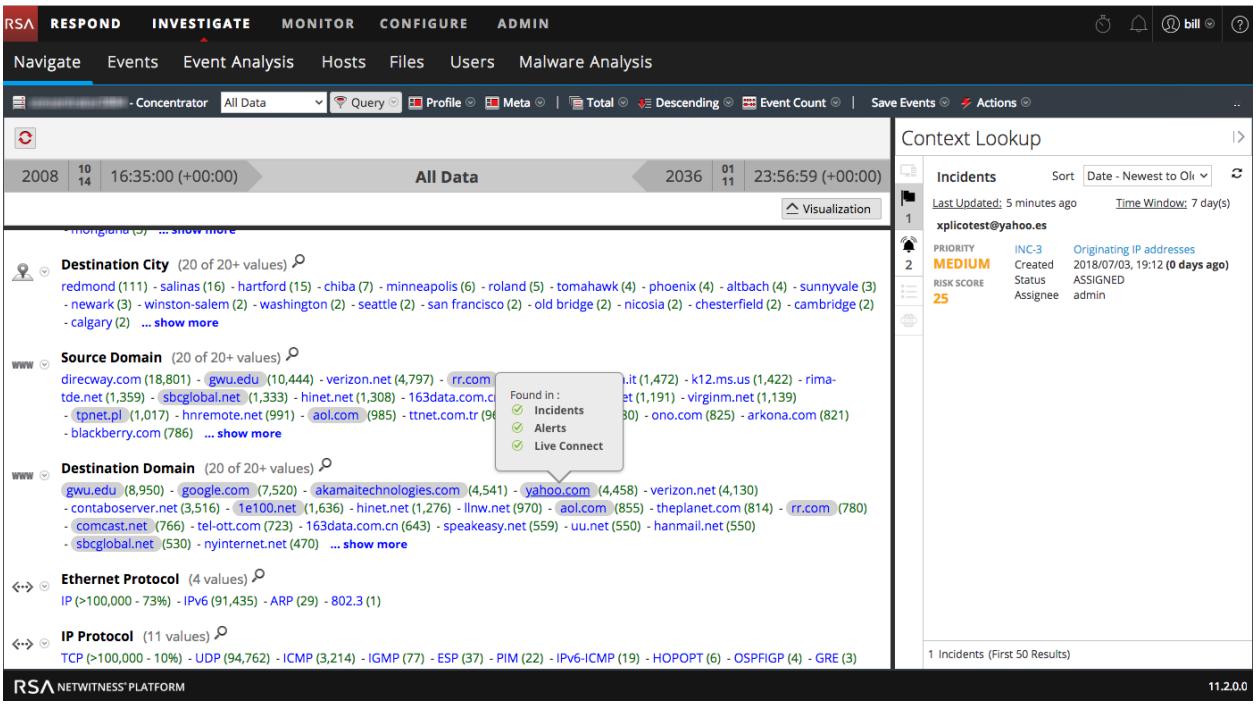
Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten*	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen*	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Nutzereinstellungen für die Ansicht „Navigation“ festlegen*	Konfigurieren der Ansichten „Navigation“ und „Ereignisse“
Threat Hunter	eine Abfrage senden oder eine nähere Analyse der Datenmenge vornehmen*	Untersuchen von Metadaten in der Ansicht „Navigation“
Threat Hunter	Abfrage-Ergebnisse verfeinern*	Abfragen von und Reagieren auf Daten in den Ansichten „Navigation“ und „Ereignisse“
Threat Hunter	Durchführen interner Suchen*	Suchen von weiteren Kontexten in den Ansichten „Navigation“ und „Ereignisse“
Threat Hunter	Durchführen externer Suchen*	Starten einer externen Suche eines Metaschlüssels

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Ereignisse“
- Ansicht „Ereignisanalyse“
- Ansicht „Malware Analysis“

Überblick



Die Ansicht „Navigation“ umfasst folgende Funktionen:

- Symbolleiste
- Schaltfläche zum Anhalten/Neuladen und Brotkrümelnavigation
- Zeitbanner
- (Optional) Debug-Informationen
- Ausblendbarer Visualisierungsbereich
- Bereich „Werte“
- Bereich „Kontextabfrage“
- Kontextmenüs

Symbolleiste

Über die Symbolleiste können Sie:

- den zu untersuchenden Service ändern.
- den angezeigten Datenbereich steuern: Sie können Nutzungsprofile auswählen, einen Zeitbereich festlegen, Metagruppen verwenden und auf die Daten anzuwendende Abfragen erstellen.
- die Quantifizierungs- und Sortiermethode für Daten im Bereich „Werte“ festlegen
- Aktionen für die Ergebnisse ausführen. Sie können Ergebnisse exportieren und drucken, ein Ereignis öffnen, dessen Ereignis-ID Sie in der Ansicht „Ereignisse“ oder „Ereignisanalyse“ haben, und eine Abfrage an Informer übergeben.
- Ermittlungseinstellungen konfigurieren, ohne dazu die Investigate-Ansichten verlassen zu müssen

Bei einigen Symbolleistenoptionen wird der Standardwert oder der ausgewählte Wert und nicht der Name der Option angezeigt. Für die Zeitbereichsoption im Beispiel oben wird z. B. **Letzte 5 Minuten** angezeigt, was für den aktuell ausgewählten Wert steht. Dies sind die Optionen der Symbolleiste.

Option	Beschreibung
	Zeigt neben dem Symbol den Namen des ausgewählten Services an. Durch Klicken auf das Symbol wird das Dialogfeld „Service ermitteln“ geöffnet, in dem Sie einen zu untersuchenden Service auswählen und den zu untersuchenden Standardservice festlegen können (siehe Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“). Wenn Sie den Service ändern, werden die Daten nicht neu geladen.

Option	Beschreibung
Zeitbereich	Zeigt die Zeitbereichsoptionen an. Die derzeit ausgewählte Option wird in der Symbolleiste angezeigt (siehe Filtern von Ergebnissen in der Ansicht „Navigation“). Sie haben folgende Auswahlmöglichkeiten: • Alle Daten • Letzte 5, 10, 15 oder 30 Minuten • Letzte Stunde, letzte 3, 6, 12 oder 24 Stunden • Letzte 2 oder 5 Tage • Morgen • Vormittag • Nachmittag • Abend • Den ganzen Tag • Gestern • Diese Woche • Letzte Woche • Nutzerdefiniert **Hinweis:** Wenn Sie die benutzerdefinierte Start- oder Endzeit in Sekunden angeben, wird der Wert für die Startzeit in Sekunden standardmäßig immer auf „:00“ und der Wert für die Endzeit in Sekunden standardmäßig immer auf „:59“ festgelegt. Wenn Sie beispielsweise einen Drill-Down in ein Problem durchführen, wird die Drill-down-Zeit als `HH:MM:00 - HH:MM:59` interpretiert. Sekunden werden in diesem Format in Untersuchungsfunktionen angezeigt.
Abfrage	Zeigt das Dialogfeld „Abfrage“ an, in dem Sie eine benutzerdefinierte Abfrage direkt eingeben können, anstatt ein Drill-down in die Daten durchzuführen. Eine Beschreibung des Dialogfelds finden Sie unter Dialogfeld „Abfrage“.
Profil	Zeigt das Menü Profil an; das aktuell ausgewählte Profil wird in der Symbolleiste angezeigt. Ein Profil erlaubt Ihnen, Profile zu verwalten und zu verwenden, die angepasste Metagruppen, eine Standard-Spaltengruppe und eine beginnende Abfrage enthalten können. Die Profile gelten für die Ansicht Navigieren (Metagruppen und Abfragen) und die Ansicht Ereignisse (Spaltengruppen und Abfragen). Weitere Informationen finden Sie unter Einkapseln von benutzerdefinierten Ansichten mithilfe von Profilen.

Option	Beschreibung
Meta	Zeigt das Menü Metagruppe an. Sie können Standardmetaschlüssel oder eine benutzerdefinierte Metagruppe verwenden. Sie haben außerdem die Möglichkeit, Änderungen an beiden Gruppentypen vorzunehmen (siehe Metagruppen managen).
Sortierfeld	Zeigt das Menü Sortierfeld an. Die aktuell ausgewählte Option wird in der Symbolleiste angezeigt. Das Menü hat zwei Optionen: „Nach Gesamtsumme ordnen“ und „Nach Wert ordnen“. Das Sortierfeld ist eine Ergänzung der Option „Sortierreihenfolge“. Die Daten für die Metaschlüssel werden basierend auf der Gesamtsumme (grüne Zahl) oder dem Metawert (blauer Text) sortiert (siehe Filtern von Ergebnissen in der Ansicht „Navigation“).
Sortierreihenfolge	Zeigt das Menü „Sortierreihenfolge“ an. Die aktuell ausgewählte Option wird in der Symbolleiste angezeigt. Das Menü hat zwei Optionen: „In aufsteigender Reihenfolge sortieren“ und „In absteigender Reihenfolge sortieren“. Die Sortierreihenfolge ist eine Ergänzung der Option „Sortierfeld“; das ausgewählte Feld für die einzelnen Metaschlüssel wird in aufsteigender oder absteigender Reihenfolge sortiert (siehe Filtern von Ergebnissen in der Ansicht „Navigation“).
Quantifizierungsmethode	Zeigt das Menü „Quantifizierungsmethode“ an. Die aktuell ausgewählte Option wird in der Symbolleiste angezeigt. Die Quantifizierungsmethode gilt nur für die Metaschlüsselergebnisse im Bereich „Werte“. Sie gilt nicht für die Zeitachse. Das Drop-down-Menü enthält drei Optionen zum Berechnen der angezeigten Anzahl (grüne Zahl in Klammern) für einen Metawert: „Nach Ereignisanzahl quantifizieren“, „Nach Ereignisgröße quantifizieren“ und „Nach Paketanzahl quantifizieren“ (siehe Filtern von Ergebnissen in der Ansicht „Navigation“). Diese geben je nach angezeigtem Datentyp unterschiedliche Werte zurück. Bei Paketdaten: • „Nach Ereignisanzahl quantifizieren“ zeigt die Anzahl der Sitzungen an. • „Nach Ereignisgröße quantifizieren“ zeigt die Größe in Byte an. • „Nach Paketanzahl quantifizieren“ zeigt die Anzahl der Pakete an. Bei Protokolldaten: • „Nach Ereignisanzahl quantifizieren“ zeigt die Anzahl der Protokolle an. • „Nach Ereignisgröße quantifizieren“ zeigt die Größe in Byte an. • „Nach Paketanzahl quantifizieren“ zeigt die Anzahl der Protokolle an.

Option	Beschreibung
Ereignisse speichern	Zeigt das Menü „Ereignisse speichern“ an, in dem Optionen für folgende Aufgaben zur Verfügung stehen: Extrahieren von mit einem Ereignis zusammenhängenden Dateien, Exportieren des aktuellen Drill-down-Punkts als PCAP-Datei und Exportieren des aktuellen Drill-down-Punkts als Protokolldatei (siehe „Exportieren eines Drill-down-Punkts“).
Aktionen	Das Menü "Aktionen" enthält Aktionen, die Sie in der Ansicht „Navigation“ ausführen können (siehe Untersuchen von Metadaten in der Ansicht „Navigation“). In Version 11.0.0.x sind folgende Optionen verfügbar: „Visualisieren“, „Zu Ereignis wechseln“ und „Drucken“. Ab Version 11.1 sind die Optionen „Visualisieren“, „In Ereignisrekonstruktion zu Ereignis wechseln“, „In Ereignisanalyse zu Ereignis wechseln“ und „Drucken“ verfügbar.
Ereignisse suchen	Ermöglicht Ihnen, nach Textmustern im aktuellen Satz von Ereignissen zu suchen. Wenn Sie auf das Suchfeld klicken, wird ein Drop-down-Menü mit Suchoptionen angezeigt. Wenn Sie auf „Anwenden“ klicken, werden die ausgewählten Optionen gespeichert und die Suchoptionen in der Ansicht „Ereignisse“ und im Profil „Untersuchen“ aktualisiert (siehe Suchen nach Textmustern).
Einstellungen	Zeigt die Einstellungen für die Ansicht „Navigation“ an (die auch in der Ansicht „Profil“ bearbeitet werden können), sodass Sie die Einstellungen für Investigate ändern können, ohne die Ansicht „Navigation“ verlassen zu müssen. Wenn Sie eine Einstellung in der Ansicht „Navigation“ ändern, wird die Einstellung auch in der Ansicht „Profil“ geändert (siehe Konfigurieren der Ansichten „Navigation“ und „Ereignisse“).

Schaltfläche zum Anhalten/Neuladen und Brotkrümelnavigation

In der Brotkrümelnavigation werden die einzelnen Abfragen nachverfolgt, die während des Drill-down durch die Metadaten für einen Service durchgeführt wurden. Die Abfragen werden jeweils mit einem Drop-down-Menü angezeigt und sind durch ein Pipe-Zeichen voneinander getrennt. Der letzte Punkt ist der aktuelle Punkt, auch als Spitze bezeichnet. Über das Symbol vor der Brotkrümelnavigation können Sie das Laden von Metawerten anhalten bzw. die Metawerte neu laden.

Die Brotkrümelnavigation zeigt den Servicenamen nicht an und wird nur angezeigt, wenn eine Abfrage aktiv ist. Wenn zu viele Drill-down-Punkte zum Anzeigen zur Verfügung stehen, wird ein Überlauf in Form von zwei spitzen Klammern (>>) am Ende der Brotkrümelnavigation angezeigt.

Die Drop-down-Menüs in der Brotkrümelnavigation unterscheiden sich nur je nach Position des Crumb und sind ansonsten identisch.

In der folgenden Tabelle werden die Steuerelemente und Menüoptionen in der Brotkrümelnavigation beschrieben.

Funktion	Beschreibung
	Schaltfläche „Anhalten und neu laden“ Steuert das Laden von Daten in der Ansicht. Drei Funktionen sind möglich: Laden anhalten, Laden fortführen und neu laden.

Funktion	Beschreibung
Hierhin navigieren	Öffnet den ausgewählten Drill-down-Punkt im aktuellen Bereich „Werte“.
Hierhin navigieren (neue Registerkarte)	Öffnet den ausgewählten Drill-down-Punkt in einer neuen Registerkarte.
Einfügen vor	Fügt vor dem aktuellen Drill-down-Punkt eine Abfrage ein. Das Dialogfeld „Filter erstellen“ wird angezeigt, in dem Sie eine benutzerdefinierte Abfrage definieren können, die in der Brotkrümelnavigation eingefügt werden soll (siehe Erstellen einer angepassten Abfrage).
Anfügen	Fügt nach dem aktuellen Drill-down-Punkt eine Abfrage an. Das Dialogfeld „Filter erstellen“ wird angezeigt, in dem Sie eine benutzerdefinierte Abfrage definieren können, die an das Ende der Brotkrümelnavigation angefügt werden soll (siehe „Erstellen einer angepassten Abfrage“).
Entfernen	Entfernt den ausgewählten Drill-down-Punkt aus der Brotkrümelnavigation.
Bearbeiten	Öffnet den ausgewählten Drill-down-Punkt im Dialogfeld „Filter erstellen“, sodass Sie die Abfrage bearbeiten können.
>>	Durch Klicken auf die spitzen Klammern wird ein Drop-down-Menü mit dem Überlauf der Brotkrümelnavigation geöffnet.

(Optional) Debug-Informationen

Wenn Sie die Einstellung „Debuginformationen anzeigen“ aktiviert haben und der Service, durch den Sie navigieren, ein Broker der Version 10.4 oder höher ist, zeigt NetWitness Platform Debug-Informationen unter der Brotkrümelnavigation an.

Die Debug-Informationen sind die `where` -Klausel der aktuellen Abfrage. Es ist nur dann keine `where` -Klausel vorhanden, wenn sich der Zeitbereich auf alle Daten bezieht und keine Drill-down-Punkte vorhanden sind. Wenn der Broker über mindestens einen Aggregatservice verfügt, der offline ist, werden in den Debug-Informationen auch die Offlineservices angezeigt.

Beispiel:

```
(attachment exists)&&(tcp.dstport = '80')&&(risk.info exists)$$time='2014-05-04 18:50:00"-"2014-05-09 18:59:59(attachment exists) && (tcp.dstport = '80') && (risk.info exists) && time="2014-05-04 18:50:00"-"2014-05-09 18:50:59"
```

Außerdem wird im Bereich „Werte“ am Ende jedes Metaschlüssels die Ladedauer angezeigt.

Zeitbanner

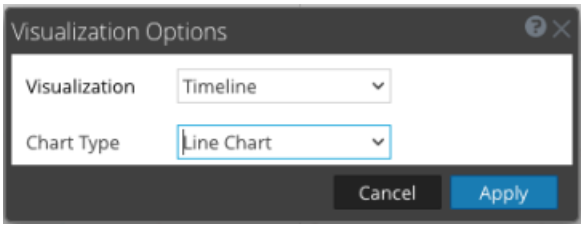
Genau unter der Brotkrümelnavigation und den Debug-Informationen (sofern vorhanden) wird im Zeitbanner der Zeitbereich angezeigt, der für die Diagrammerstellung verwendet wurde.

Visualisierungen

Im oberen Bereich der Ansicht „Navigation“ wird eine Visualisierung des aktuellen Drill-down-Punkts angezeigt. Sie können über den Bereich „Visualisierung“ einen Drill-down in die Daten durchführen (siehe Filtern von Ergebnissen in der Ansicht „Navigation“). Sie können die Visualisierung ein- oder ausblenden und eine der folgenden Visualisierungsoptionen wählen: „Zeitachse“ oder „Koordinaten“. Als Visualisierung wird zunächst die zuletzt gespeicherte Visualisierung geöffnet.

Zeitachsendiagramm

Die Zeitachse ist die Anzahl der Ereignisse, die zu einer bestimmten Instanz auftreten. Die Zeitachse bietet Ereigniszählungen, sodass Sie sehen können, wenn sich die Anzahl der Ereignisse zu einem bestimmten Zeitpunkt drastisch erhöht. Die Zeitachse zeigt die Aktivitäten für den ausgewählten Service und Zeitbereich als Liniendiagramm oder Balkendiagramm an, je nachdem, was Sie im Menü „Optionen“ ausgewählt haben. In der zweiten Abbildung wird ein Liniendiagramm und in der dritten ein Balkendiagramm dargestellt.



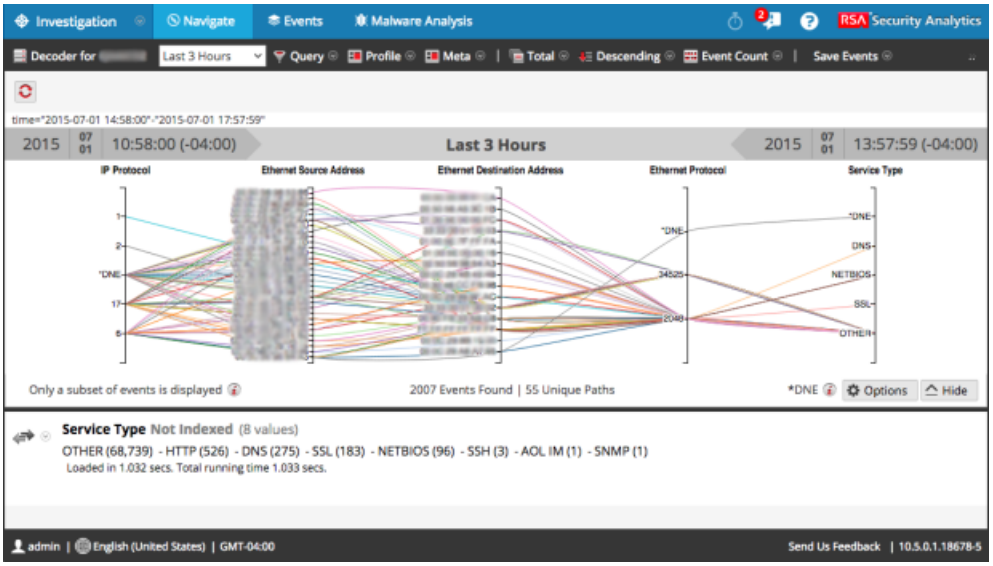
Die Zeitachse zeigt die Aktivitäten für den ausgewählten Service und Zeitbereich als Liniendiagramm oder Balkendiagramm an, je nachdem, was Sie im Menü „Optionen“ ausgewählt haben.

Funktion	Beschreibung
Anzahl der Ereignisse (Zeitachse)	Die Y-Achse des Diagramms mit der Anzahl der Ereignisse (in Tausend).
Zeitachse (Zeitachse)	Die X-Achse des Diagramms, die den Zeitpunkt der Ereignisse angibt.
Ereignispunkt (Zeitachse)	Wenn Sie sich einen bestimmten Abschnitt genauer anschauen möchten, wählen Sie diesen Bereich einfach im Diagramm aus. Der neue Zeitbereich wird nun im Diagramm dargestellt.
Ermitteln (Zeitachse)	Zeigt die Metawerte für die ausgewählte Teilmenge an.

Funktion	Beschreibung
Zoom zurücksetzen (Zeitachse)	Um zum ursprünglichen Zeitbereich zurückzukehren, klicken Sie auf „Zoom zurücksetzen“.
Optionen	Zeigt das Dialogfeld „Visualisierungsoptionen“ an. Datenpunkte können als Liniendiagramm (Standard), Balkendiagramm oder Koordinatendiagramm angezeigt werden. Wenn ein Diagrammtyp ausgewählt ist, werden die relevanten Optionen angezeigt.
Ausblenden	Blendet das Diagramm aus.

Parallelkoordinatendiagramm

Das Parallelkoordinatendiagramm ist eine der Auswahlmöglichkeiten im Menü „Optionen“ zum Visualisieren des aktuellen Drill-down-Punkts. Wenn im Dialogfeld „Visualisierungsoptionen“ die Option „Koordinaten“ ausgewählt ist, können Sie die anzuzeigenden Metadaten auswählen (siehe Visualisieren von Metadaten als Parallelkoordinaten).



Funktion	Beschreibung
Achsen	Jede Achse ist ein Metaschlüssel. Die Anzahl der Metaschlüssel wirkt sich auf die Ladezeit des Diagramms aus. Alle Metaschlüssel werden geladen, aber die Anzahl von Ereignissen pro Metaschlüssel ist begrenzt.
Linien	Die Linien stellen Ereignisse dar und verbinden Werte auf den Achsen, um die Korrelation zwischen mehreren Metaschlüsseln zu zeigen.
Optionen	Zeigt das Dialogfeld „Visualisierungsoptionen“ an. Datenpunkte können als Liniendiagramm (Standard), Balkendiagramm oder Koordinatendiagramm angezeigt werden. Wenn ein Diagrammtyp ausgewählt ist, werden die relevanten Optionen angezeigt.

Funktion	Beschreibung
Nur eine Teilmenge der Ereignisse wird angezeigt.	Mit dieser Meldung werden Sie darüber benachrichtigt, dass nicht alle Ereignisse im Bereich „Werte“ in das Diagramm übernommen werden. Um alle Ereignisse anzuzeigen, kann es hilfreich sein, Achsen zu entfernen oder die Daten im Bereich „Werte“ zu filtern.
Gefundene Ereignisse | Eindeutige Pfade	Zeigt die Gesamtanzahl von Ereignissen im Diagramm im Vergleich zur Anzahl der eindeutigen Pfade im Diagramm an. Durch Aktivieren der Option „Alle Metaschlüssel müssen in einem Ereignis vorhanden sein“ wird das Diagramm erneut gezeichnet und dadurch besser ausgerichtet und lesbarer.
DNE	Gibt an, dass für diesen Metaschlüssel in dem Ereignis keine Werte vorhanden sind.

Sie können im Dialogfeld Visualisierungsoptionen für Koordinaten die Metaschlüssel auswählen, die dargestellt werden sollen.

Funktion	Beschreibung
Visualisierungsauswahl	Zeigt eine Drop-down-Liste mit Visualisierungstypen an: Zeitachse und Koordinaten
Alle Metaschlüssel müssen in einem Ereignis vorhanden sein	Begrenzt die in der Visualisierung dargestellten Daten auf ausschließlich solche Ereignisse, die alle ausgewählten Metaschlüssel enthalten. Dabei ist das Ziel, eine übersichtliche, besser ausgerichtete Visualisierung zu erhalten.
	Zeigt das Dialogfeld „Schlüssel zur Parallelkoordinatenvisualisierung hinzufügen“ an, damit Sie der Visualisierung Achsen hinzufügen können. Diese Option ist nützlich, wenn Sie nach Beziehungen zwischen den Standardmetaschlüsseln und einigen zusätzlichen Metaschlüsseln suchen.
	Löscht die ausgewählten Schlüssel, sodass sie nicht als Achsen in der Visualisierung angezeigt werden. Die Visualisierung wird dadurch übersichtlicher und kann mehr Datenpunkte enthalten.
	Stellt die Standardmetaschlüssel für die Visualisierung wieder her, d. h. alle Metaschlüssel in dem aktuellen Drill-down-Punkt.
	Steuert die Anzeige von zusätzlichen Informationen zur Anzahl der ausgewählten Achsen im Vergleich zur empfohlenen Anzahl. Hiermit werden Ihnen mögliche Performanceverbesserungen durch Entfernen von Achsen aufgezeigt.
Achsen	Listet die Metaschlüssel auf, die als Achsen in der Visualisierung ausgewählt wurden.
Abbrechen	Verwirft alle an den Visualisierungsoptionen vorgenommenen Änderungen.
Anwenden	Speichert die Änderungen an den Visualisierungsoptionen und wendet sie auf die aktuelle Visualisierung an.

Im Dialogfeld „Schlüssel zur Parallelkoordinatenvisualisierung hinzufügen“ können Sie die Metaschlüssel oder Metagruppen auswählen, die als Achsen in der Parallelkoordinatenvisualisierung verwendet werden sollen.

Funktion	Beschreibung
Visualisierungsauswahl	Schlüssel auswählen: Die folgenden zwei Optionen dienen zur Auswahl von Metaschlüsseln: • Aus Standardmetaschlüsseln • Aus Metagruppen Jede Option stellt eine Drop-down-Liste zur Auswahl bereit.
Mit den ausgewählten Metaschlüsseln ...	Mit den Optionen für die Methode zum Hinzufügen von Metaschlüsseln können Sie Folgendes ausführen: • Aktuelle Schlüsselliste ersetzen • An aktuelle Schlüsselliste anhängen • Am Anfang der aktuellen Schlüsselliste einfügen
Abbrechen	Schließt das Dialogfeld, ohne Schlüssel hinzuzufügen.
Hinzufügen	Schließt das Dialogfeld und fügt die ausgewählten Schlüssel wie angegeben hinzu.

Bereich „Werte“

Die Hauptfunktion der Ansicht „Navigation“ ist der Bereich „Werte“, in dem Sie Daten analysieren können (siehe Filtern von Ergebnissen in der Ansicht „Navigation“).

Die Standardansicht bezieht sich auf die letzten 3 Stunden der Sammlung, wobei die standardmäßigen Metaschlüssel und die nicht indizierten geschlossenen Metaschlüssel verwendet werden. Die Metaschlüssel in den Metagruppen werden in der Reihenfolge angezeigt, in der NetWitness Platform die Schlüssel abfragt. Beim Laden der Daten in den Bereich „Werte“ wird NetWitness Platform optimiert, um Teilergebnisse, den Ladefortschritt und den Servicestatus anzuzeigen.

Das Ladeverhalten wird durch verschiedene Konfigurationseinstellungen bestimmt. Die Einstellungen auf höchster Ebene werden vom Administrator für jeden Nutzer festgelegt. und zwar:

- Die maximal zulässige Dauer einer Abfrage dieses Nutzers (Timeout für Abfrage)
- Der Schwellenwert, bis zu dem NetWitness Platform die Anzahl an Metawerten in einer Sitzung zählt (Sitzungsschwellenwert). Wenn ein Schwellenwert für eine Sitzung festgelegt ist, werden in der Ansicht „Navigation“ das Erreichen des Schwellenwerts sowie der Prozentsatz der geladenen Ergebnisse angezeigt. Jede Sitzung, für die kein Prozentsatz angezeigt wird, ist korrekt und wurde bis zum Abschluss verarbeitet. Wenn ein vorhandener Prozentsatz gibt an, wie viel der Verarbeitung abgeschlossen wurde. Der angezeigte Prozentsatz wird durch Extrapolieren aus dem Wert zum Zeitpunkt des Abschlusses der Verarbeitung unter Berücksichtigung der verbleibenden Arbeit geschätzt. Höhere Prozentwerte sind in der Regel genauer, da sie weniger Extrapolation erfordern.

- Der Schwellenwert, bis zu dem NetWitness Platform die Anzahl an Metawerten in einer Sitzung zählt (Sitzungsschwellenwert). Wenn ein Schwellenwert für eine Sitzung festgelegt ist, werden in der Ansicht „Navigation“ das Erreichen des Schwellenwerts sowie der Prozentsatz der Abfragezeit, der zum Erreichen des Schwellenwertes verwendet wurde, angezeigt.

Hinweis: Der Ladevorgang für die Werte nicht indizierter Metaschlüssel im Bereich „Werte“ dauert länger. Zum Optimieren des Ladevorgangs öffnet NetWitness Platform nicht indizierte Metaschlüssel standardmäßig nicht. Detaillierte Informationen über nicht indizierte Metaschlüssel in Investigation erhalten Sie unter „Verwalten und Anwenden von Standardmetaschlüsseln in einer Ermittlung“.

Wenn Sie die Ermittlung für einen Service gestartet haben, zeigt NetWitness Platform die Ergebnisse im Bereich „Werte“ an.

1. NetWitness Platform lädt Metaschlüssel und Metawerte im Bereich „Werte“. Für jeden Ladevorgang von Metaschlüsseln gibt es folgende Phasen:
   a. **Warten auf Ladevorgang** oder **Geschlossen**. Lautet die Phase Geschlossen, werden keine Daten für diesen Schlüssel geladen.
   b. **Laden**
      i. **Ladefortschritt**: NetWitness Platform empfängt und zeigt Fortschrittsmeldungen an.
      ii. **Teilergebnisse**: NetWitness Platform empfängt Meldungen zu Werten und zeigt Teilergebnisse im Bereich „Werte“ an.
   c. **Ladevorgang abgeschlossen**: Alle Ergebnisse wurden geladen.
2. Nach jedem Abschluss eines Metaschlüssel-Ladevorgangs und dem Anzeigen endgültiger Werte wird mit dem nächsten Metaschlüssel fortgefahren. Die Anzahl der Werte, die für jeden Metaschlüssel ausgegeben werden, wird durch den Wert Threads rendern in den Ermittlungseinstellungen festgelegt. Der Ladevorgang wird fortgesetzt, bis alle erforderlichen Schlüssel geladen wurden.
3. Falls **Debuginformationen anzeigen** aktiv ist und der betreffende Service ein Broker der Version 10.4 oder höher ist, zeigt NetWitness Platform unter den Werten für jeden Metaschlüssel die Ladedauer und zusätzliche Ladeinformationen für die aggregierten Services an. NetWitness Platform blendet außerdem die Debug-Informationen unter der Brotkrümelnavigation ein.

Iterative Ergebnisse

Iterative Ergebnisse liefern Feedback zum Status von Abfragen in den Schnittstellen, um eine Einschätzung zur Ladedauer zu geben und fehlende Servicedaten zu melden. Wenn Sie z. B. einen Broker abfragen, der Daten von zwei Concentrators aggregiert, werden in NetWitness Platform die Ergebnisse vom ersten Concentrator angezeigt, sobald sie verfügbar sind, auch wenn der zweite Concentrator noch auf Ergebnisse wartet.

Iterative Ergebnisse umfassen auch Benachrichtigungen bei fehlenden Servicedaten, wenn der Service nicht erreichbar ist.

Teilergebnisse

Wenn vom Core-Service Teilergebnisse zurückgegeben werden, wird am Ende der Metaschlüsselliste eine Meldung mit dem aktuellen Fortschritt des Ladevorgangs der Werte angezeigt. Zum Beispiel: Zurzeit werden 38 ip.src-Werte geprüft, 71 % gibt an, dass das Laden der Werte für den Metaschlüssel zu 71 % abgeschlossen ist.

Debug-Informationen

Wenn die Einstellung „Debuginformationen anzeigen“ aktiviert ist, wird am Ende der Werte ein Feld mit dem Status für die verschiedenen Systeme angezeigt, für die Sie in NetWitness Platform Abfragen ausführen. Wenn Sie z. B. Abfragen für einen 10.4-Broker ausführen, der Daten von mehreren Concentrators abruft, zeigt NetWitness Platform den Status der Abfragen pro Concentrator an, sodass die relative Geschwindigkeit des Datenladevorgangs bei jedem Concentrator sichtbar ist. Für jeden Service, der Teil der Abfrage war, wird die verstrichene Gesamtzeit für die Abfrage aufgeführt.

Für jeden Service, der Teil der Abfrage war, wird die verstrichene Gesamtzeit für die Abfrage aufgeführt. Im Beispiel oben haben zwei Services die Ergebnisse innerhalb von 3,207 Sekunden zurückgegeben, localhost:50005 brauchte dagegen nur 2 Sekunden zum Zurückgeben der Ergebnisse. Außerdem wird die „Where“-Klausel der Abfrage unter der Brotkrümelnavigation angezeigt. Sie können diese Syntax direkt in eine Anwendungsregel oder in eine „Where“-Klausel einer Regel für die Reporting kopieren.

Ladevorgang abgeschlossen

Für jeden Metaschlüssel wird eine Liste mit Werten (blauer Text) und der jeweiligen Anzahl (grüner Text) angezeigt, die aus dem aktuellen Drill-down-Punkt stammt. Wenn Sie auf einen Wert klicken, um einen Drill-down in eine Teilmenge der aktuell ausgewählten Daten durchzuführen, wird die Anzeige aktualisiert, und der neue Drill-down-Punkt wird in der Brotkrümelnavigation wiedergegeben. Sie können die Sortierungs- und Quantifizierungsmethoden für die Werteliste über die Optionen der Symbolleiste festlegen.

Hinweis: Für den Titel, die Werte und die Zählangaben nicht indizierter Metaschlüssel kann kein Drill-down durchgeführt werden; entsprechende Werte und Zählangaben werden in Schwarz angezeigt.

Funktion	Beschreibung
Metaschlüssel	Der Name des aufgeführten Metaschlüssels; **Servicetyp** ist z. B. ein Metaschlüssel.
Anzahl der gerenderten Werte und Anzahl der zum Laden verfügbaren Werte	Die Anzahl der gerenderten Werte wird durch den Wert „Threads rendern“ in den Ermittlungseinstellungen festgelegt. Im Beispiel oben lautet der Metaschlüssel **Servicetyp** und 20 von 20+ Werten werden zurzeit angezeigt. Sie können weitere Werte anzeigen, indem Sie auf **...Mehr anzeigen** klicken.

Funktion	Beschreibung
🔍	Durch Klicken auf 🔍 für einen indizierten Metaschlüssel wird das Suchdialogfeld geöffnet, in das Sie einen Filter für den aktuellen Metaschlüssel eingeben können. Die Suchfunktion steht nicht für nicht indizierte Metaschlüssel zur Verfügung und basiert auf dem tatsächlichen Metawert und nicht auf dem Alias. Drill-downs mit dem Suchdialogfeld werden mit Aliasen nicht unterstützt. HINWEIS: Fragen Sie Ihren Administrator nach einer Liste von Aliasen, die für einen Metaschlüssel in Investigation verwendet werden. Wenn ein Alias verwendet wird, liefert das Suchdialogfeld keine Ergebnisse. Stattdessen müssen Sie eine Abfrage für den Metaschlüssel per Rechtsklick oder über das Dialogfeld „Abfrage“ durchführen.
Offlineservices: xxx.xxx.xxx.xxx:50004	Führt die Offlineservices auf, die von einem 10.4-Broker abgefragt werden.
Metaanzahl, zum Beispiel (3)	Die Anzahl an Instanzen, die für ein bestimmtes Metaelement in der Sitzung gefunden wurde.
Metawert, zum Beispiel: other src	Der Name, der mit dem gefundenen Metaelement verknüpft ist.
...Mehr anzeigen	Wenn die Anzahl an Metawerten begrenzt wurde (z. B. auf 20), werden durch Klicken auf diesen Link zusätzliche Metawerte für den ausgewählten Metaschlüssel angezeigt.
In 0,418 Sek. geladen. Gesamtlaufzeit 0,434 Sek. (localhost:50005 in 1 Sek. geladen...	Debug-Statistiken zeigen die Ladedauer basierend auf der Einstellung „Debuginformationen anzeigen“ an.

Drop-down-Menüs „Metaschlüssel“

Die Metaschlüssel im Bereich „Werte“ weisen Drop-down-Menüs auf. Neben jedem Metanamen wird ein Drop-down-Pfeil mit Optionen angezeigt, die auf dieses Element zutreffen. Sie können diese Optionen nutzen, um die Darstellung der Ergebnisse für den Metaschlüssel in der aktuellen Ansicht zu ändern. Änderungen an Metaschlüsseln bleiben in der aktuellen Ansicht angezeigt, bis Sie die Seite aktualisieren oder einen neuen Service in der Symbolleiste der Ansicht „Navigation“ auswählen. Siehe Drill-down zu Daten im Bereich „Werte“

Durch eine Aktualisierung wird die Darstellung der Metaschlüssel wieder auf die Standardeinstellung zurückgesetzt, die im Dialogfeld „Standardmetaschlüssel managen“ definiert wurde (siehe „Verwalten und Anwenden von Standardmetaschlüsseln in einer Ermittlung“). Wenn Sie im Dialogfeld „Standardmetaschlüssel managen“ bisher keine Änderungen vorgenommen haben, stellt NetWitness Platform die standardmäßigen Metaschlüssel vom Core-Service wieder her.

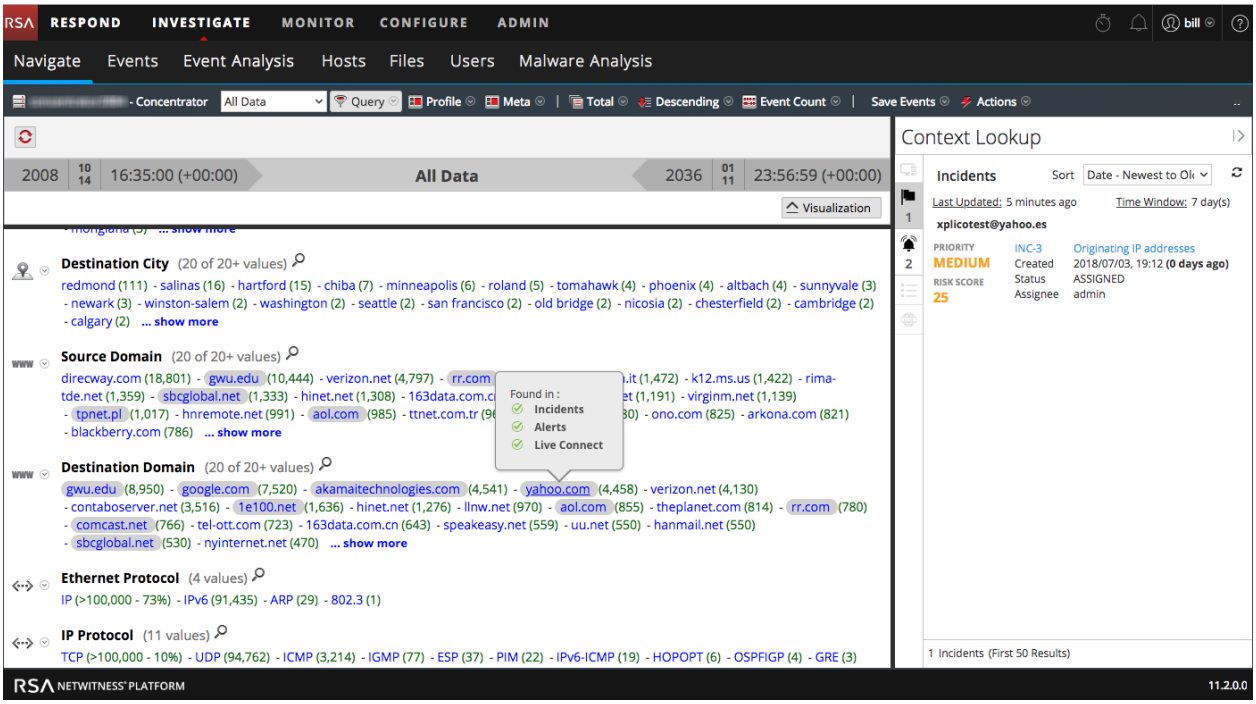
- Mehr Ergebnisse
- Max. Ergebnisse
- Ergebnisse ausblenden

- Metaschlüsselinformationen
- Als CSV-Datei anzeigen (Version 11.0.0.x) oder Werte exportieren (ab Version 11.1)

Bereich „Kontextabfrage“

In den Ansichten „Navigation“ und „Ereignisse“ befindet sich rechts der Bereich „Kontextabfrage“. Der Kontextabfragebereich wird nur angezeigt, wenn der Context-Hub-Service installiert und konfiguriert wurde. Weitere Informationen zum Konfigurieren des Context-Hub-Services finden Sie im *Context-Hub-Konfigurationsleitfaden*.

Im Bereich „Kontextabfrage“ werden die relevanten Daten angezeigt, wenn ein Analyst Kontextdaten für einen Metawert im Bereich „Werte“ abfragt.

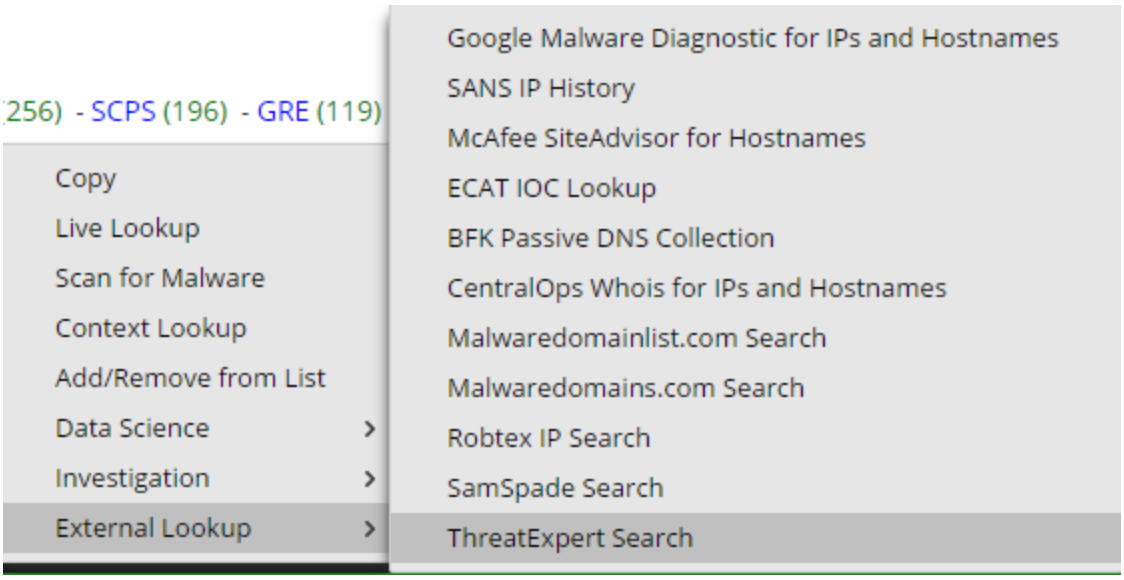


Nachdem der Administrator den Context-Hub-Service konfiguriert hat, können Sie die Kontextinformationen für die Metawerte in der Ansicht „Navigation“ und der Ansicht „Ereignisse“ anzeigen. Weitere Informationen zum Konfigurieren des Context-Hub-Services finden Sie im *Context-Hub-Konfigurationsleitfaden*. Informationen zur Durchführung von Kontextabfragen für Metawerte finden Sie unter Suchen von weiteren Kontexten in den Ansichten „Navigation“ und „Ereignisse“.

Der Context-Hub-Service ist mit einer Standardzuordnung von Metadatentypen und Metaschlüsseln vorkonfiguriert. Informationen über die Zuordnung des Context-Hub-Metawerts zum Investigation-Metaschlüssel finden Sie unter „Managen der Metadatentyp- und Metaschlüsselzuordnung“ im *Context-Hub-Konfigurationsleitfaden*.

Sie können den Typ der Kontextdaten anzeigen, die für einen hervorgehobenen Metawert verfügbar sind, indem Sie den Mauszeiger über einen hervorgehobenen Metawert bewegen. Eine Inline-Anzeige zeigt an, welcher Typ von Kontextdaten für den Metawert zur Verfügung steht: Endpunkt, Incidents, Warnmeldungen oder Listen.

Wenn Sie mit der rechten Maustaste auf einen Metawert klicken, wird ein Menü mit der Option „Kontextabfrage“ geöffnet. Die folgende Abbildung zeigt die Option „Kontextabfrage“, wenn Sie mit der rechten Maustaste auf einen Metawert klicken.



Für Metaschlüssel, wie IP-, Host- und Mac-Adresse, werden die Details der mit einem Flag versehenen Werte aus Endpunkt, Incident, Warnmeldungen und Listen erfasst.

Für Metaschlüssel, wie Datei, Datei-Hash, Domain, Nutzer, werden die Details der mit einem Flag versehenen Werte aus Incident, Warnmeldungen und Listen erfasst.

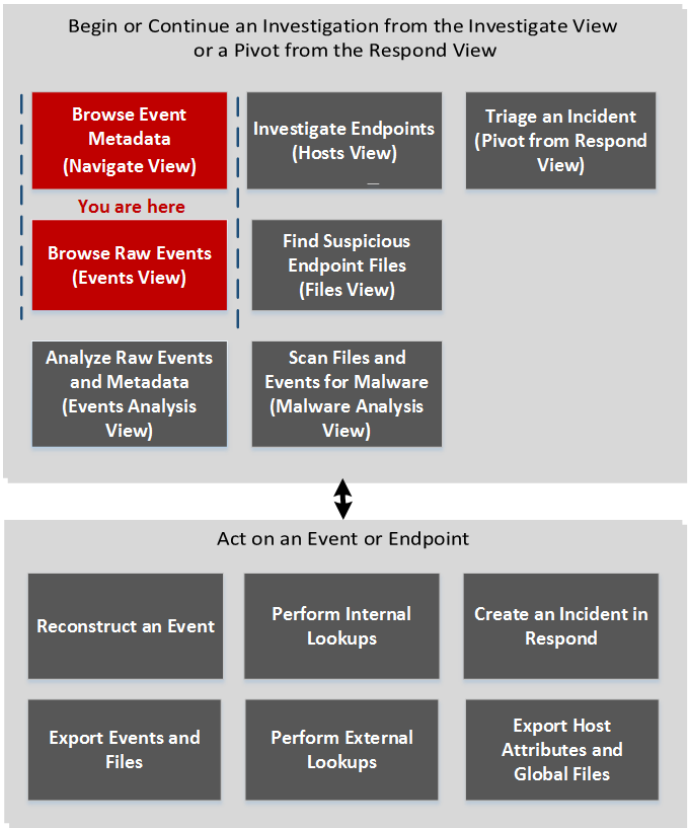
Die Daten werden im Bereich „Kontext“ nur angezeigt, wenn Daten verfügbar sind.

Weitere Informationen über die Ergebnisse der Suche und Kontextinformationen für verschiedene Datenquellen finden Sie unterBereich „Kontextabfrage“.

Dialogfeld „Abfrage“

Sie können in der Ansicht „Navigation“ oder „Ereignisse“ eine Abfrage erstellen, anstatt durch die Metaschlüssel und Werte zu klicken, um einen Drill-down in die Metadaten auszuführen. Die Dialogfelder zum Erstellen einer Abfrage bieten Syntaxhilfe mit Drop-down-Listen der anwendbaren Metaschlüssel und Operanden. Um auf dieses Dialogfeld über die Symbolleiste der Ansicht **Navigieren** oder **Ereignisse** zuzugreifen, klicken Sie auf **Abfrage**.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten*	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen*	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“

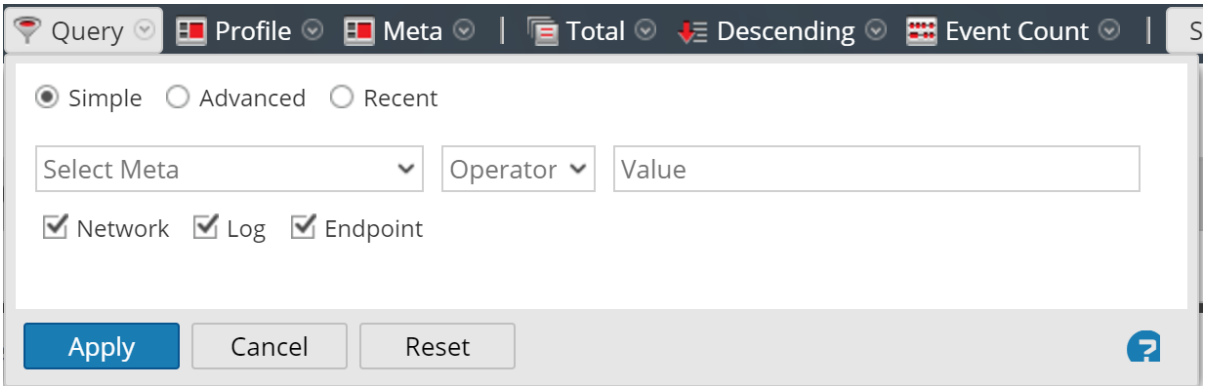
Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	eine angepasste Abfrage erstellen*	Erstellen einer angepassten Abfrage

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Navigation“
- Ansicht „Ereignisse“

Überblick

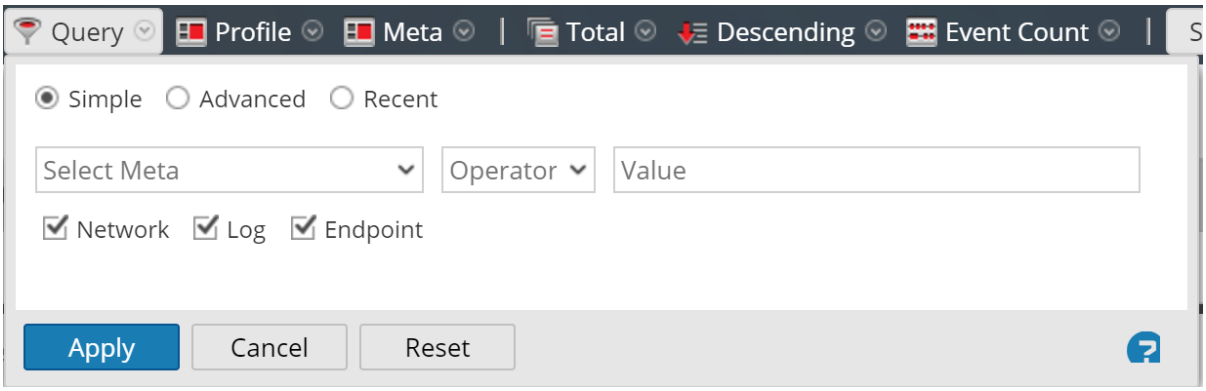


Das Dialogfeld „Abfrage“ umfasst drei Ansichten:

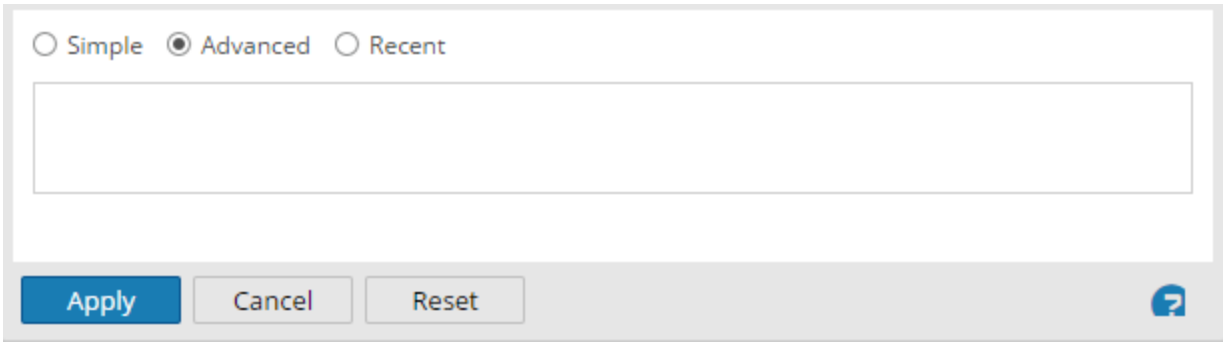
- Einfach
- Erweitert
- Zuletzt verwendet

In der Ansicht Einfach können Sie mithilfe der im Dialogfeld angezeigten Optionen eine Abfrage erstellen. In der Ansicht „Erweitert“ können Sie ohne Anleitung eine Abfrage erstellen. In der Ansicht Aktuell können Sie eine Abfrage aus einer Drop-down-Liste aktueller Abfragen auswählen.

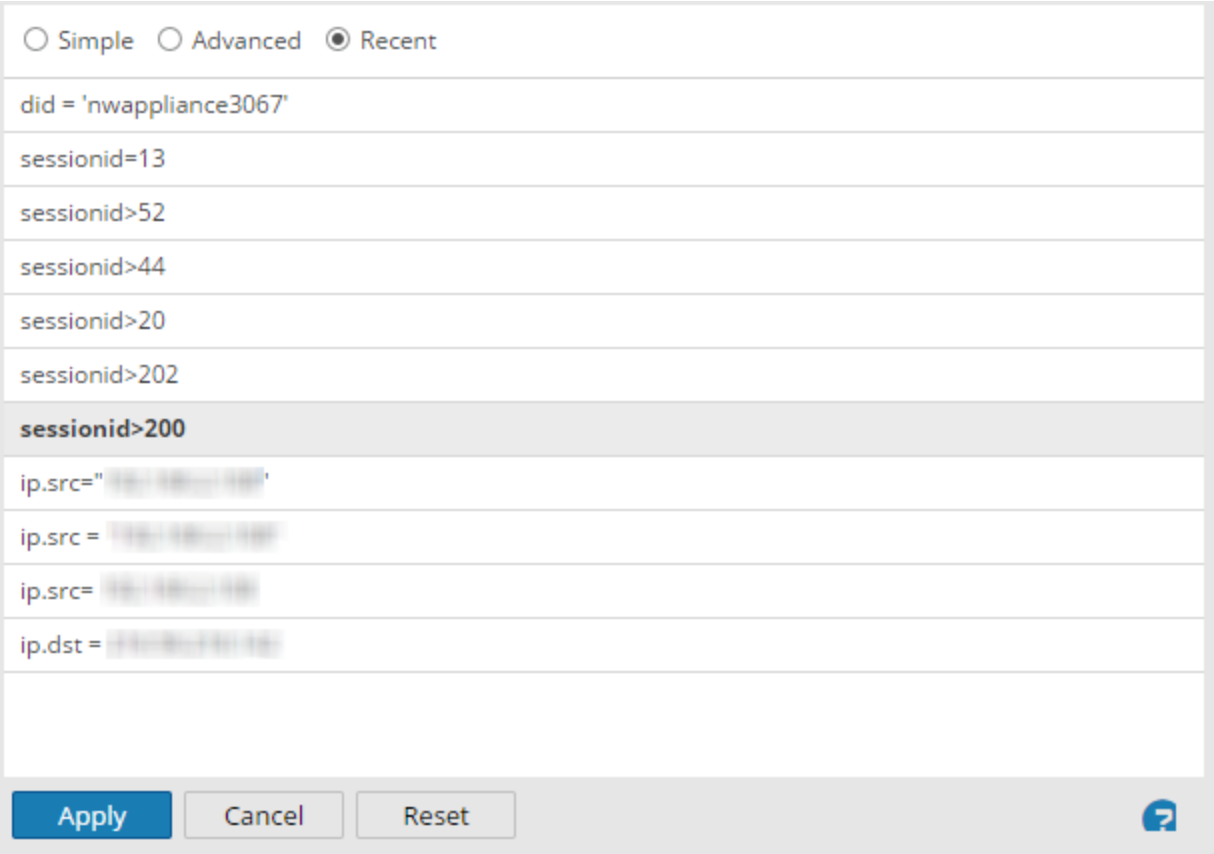
Ansicht „Einfach“



Ansicht „Erweitert“



Ansicht „Aktuell“



In der folgenden Tabelle sind die Funktionen des Dialogfelds „Abfrage“ beschrieben.

Funktion	Beschreibung
Metadaten auswählen	Zeigt eine Drop-down-Liste der Metagruppen an
Operator	Zeigt eine Drop-down-Liste mit den Operatoren `(=,NetWitness Platform!=,NetWitness Platformexists,NetWitness Platform!exists)` an.
Wert	Ermöglicht das Eingeben eines Werts zum Abschließen der Abfrage
Netzwerk	Begrenzt die Abfrage auf Pakete, wenn Protokoll nicht ausgewählt ist
Protokoll	Begrenzt die Abfrage auf Pakete, wenn Netzwerk nicht ausgewählt ist
Feld „Abfrage“	Ermöglicht das Eingeben eine Abfrage in der Ansicht „Erweitert“. Wenn Sie zu tippen beginnen, wird eine Drop-down-Liste der verfügbaren Metaschlüssel für den Service angezeigt, danach wird beim Tippen eine Drop-down-Liste der Operatoren angezeigt. Wenn der aktuell eingegebene Ausdruck im Feld Abfrage ungültig ist, wird eine Warnung in der Nähe des Felds angezeigt. Wenn die Abfrage gültig ist, wird die Warnung ausgeblendet.

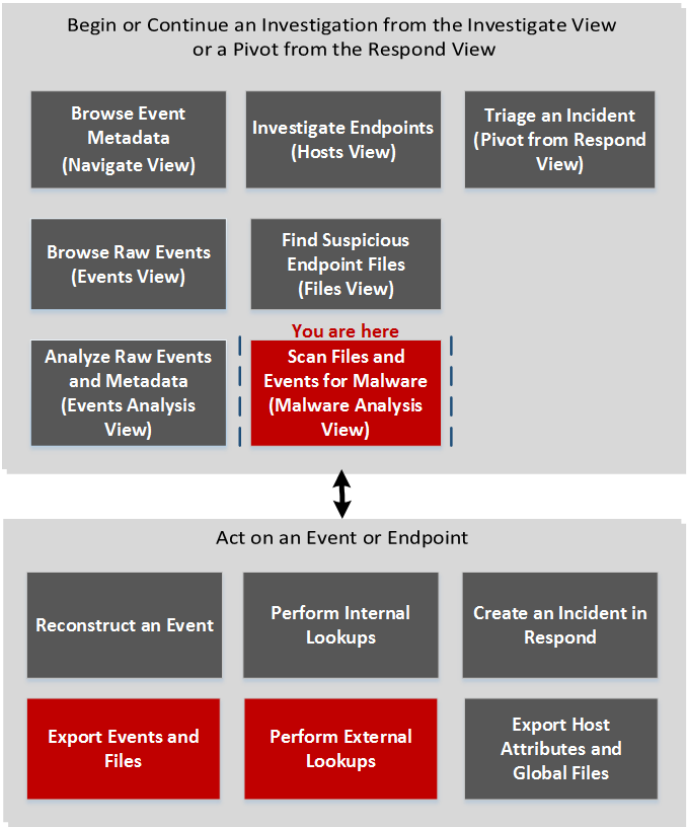
Funktion	Beschreibung
Abfrageliste	Ermöglicht das Auswählen einer Abfrage aus einer Liste aktueller Abfragen in der Ansicht „Aktuell“. Durch Doppelklicken auf eine Abfrage wird diese Option automatisch angewendet.
Anwenden	Wendet die neue Abfrage auf die aktuelle Investigation-Ansicht an
Abbrechen	Schließt das Dialogfeld, ohne die Änderungen anzuwenden.
Zurücksetzen	Setzt alle Felder zurück.

Dialogfeld „Auf Schadsoftware scannen“

Im Dialogfeld „Auf Schadsoftware scannen“ können Malware Analysis-Analysten Dateien für die Untersuchung in Malware Analysis hochladen.

Um auf dieses Dialogfeld zuzugreifen, navigieren Sie zur Ansicht **Malware Analysis**. Wählen Sie im Dialogfeld **Malware Analysis Service auswählen** im linken Bereich einen Service aus und klicken Sie dann im rechten Bereich auf Scan Files.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen*	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*

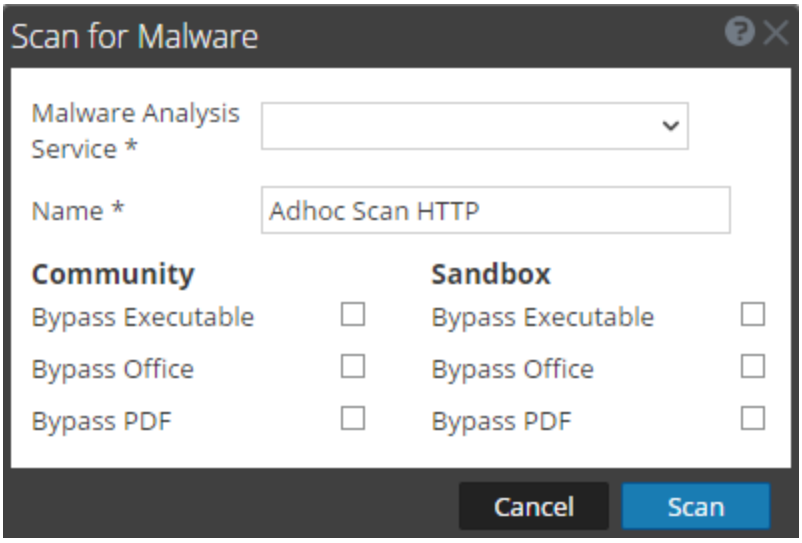
* Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Beginnen einer Schadsoftwareanalyse-Ermittlung
- Starten eines Malware Analysis-Scans in der Ansicht „Navigation“

Überblick

Die folgende Abbildung zeigt das Dialogfeld „Auf Schadsoftware scannen“ und in der folgenden Tabelle sind die in diesem Dialogfeld verfügbaren Funktionen beschrieben.

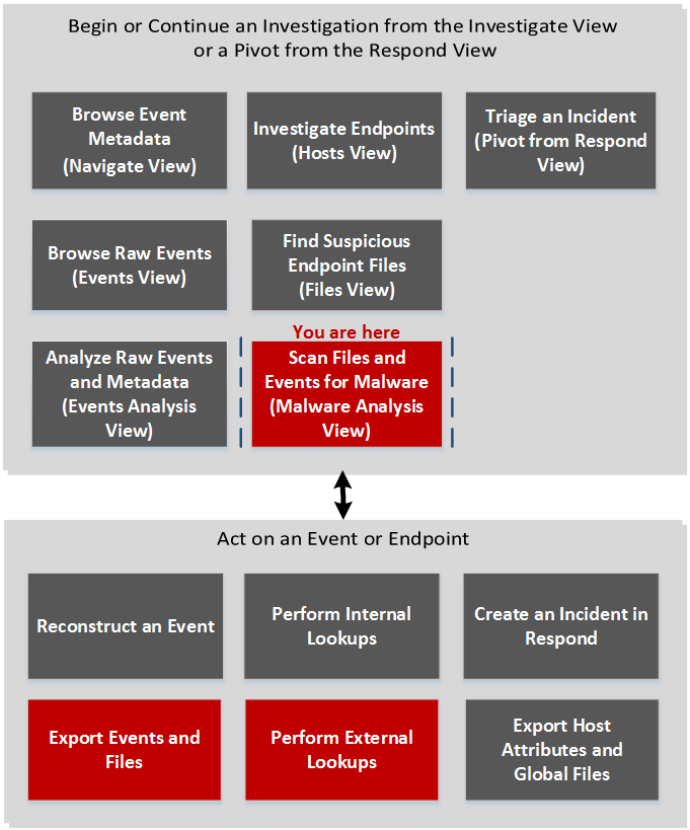


Funktion	Beschreibung
+	Lädt eine Datei von Ihrem Computer hoch.
−	Löscht eine Datei aus der Liste.
Dateiname	Zeigt die Namen der Dateien an, die der Liste hinzugefügt wurden.
Name	Hier können Sie einen Namen für den Scanjob eingeben.
Community	Zeigt Optionen für Community für das Umgehen oder Ignorieren bestimmter Dateitypen an: • Ausführbare Datei umgehen • Office umgehen • PDF umgehen
Sandbox	Zeigt Optionen für Sandbox für das Umgehen oder Ignorieren bestimmter Dateitypen an: • Ausführbare Datei umgehen • Office umgehen • PDF umgehen
Abbrechen	Schließt das Dialogfeld, ohne dass Aktionen durchgeführt wurden.
Scan	Scannt die hochgeladenen Dateien.

Dialogfeld „Malware Analysis Service auswählen“

Das Dialogfeld „Malware Analysis Service auswählen“ kann von der Ansicht „Malware Analysis“ aus aufgerufen werden. In diesem Dialogfeld können Malware Analysis-Analysten den zu untersuchenden Service auswählen, einen Scan für diesen zu untersuchenden Service festlegen, eine zu untersuchende Datei hochladen und einen fortlaufenden Scan für diesen Service starten.

Workflow



Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“

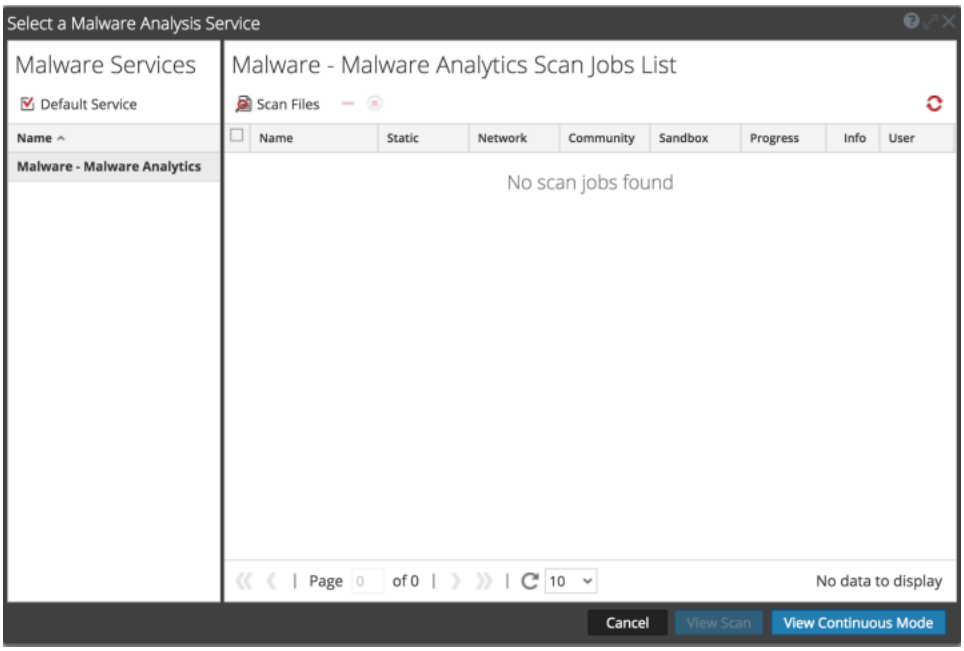
Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen*	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*

* Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Beginnen einer Schadsoftwareanalyse-Ermittlung
- Starten eines Malware Analysis-Scans in der Ansicht „Navigation“

Überblick



Das Dialogfeld „Malware Analysis Service auswählen“ besteht aus dem Bereich „Schadsoftwareservices“ links und dem Bereich „Liste der Scanjobs“ rechts. Im Bereich „Liste der Scanjobs“ befinden sich eine Symbolleiste, eine Liste sowie Schaltflächen zum Anzeigen von Scans.

Im Bereich „Schadsoftwareservices“ wird eine Liste der für die Schadsoftwareanalyse verfügbaren Services angezeigt. In diesem Bereich können Sie den zu untersuchenden Service auswählen und über das Symbol Standardservice einen Standardservice festlegen. Wenn Sie einen Service auswählen, werden die verfügbaren Scanjobs für diesen Service in der Liste der Scanjobs angezeigt.

Dies sind die Funktionen in der Symbolleiste „Liste der Scanjobs“.

Funktion	Beschreibung
Scan Files	Zeigt das Dialogfeld „Auf Schadsoftware scannen“ an, in dem Sie eine Datei zum Scannen in den Service hochladen können.
Scanjob(s) löschen ( )	Löscht einen oder mehrere ausgewählte Scanjobs. NetWitness Platform zeigt vor dem Löschen von Scanjobs ein Bestätigungsdialogfeld an.
Scanjob(s) abbrechen ( )	Pausiert bzw. setzt einen oder mehrere Scanjobs fort.
Aktualisieren ( )	Aktualisiert die Liste der Scanjobs.

Die Liste der Scanjobs enthält folgende Spalten. Diese Liste steht auch im Dashlet „Schadsoftware-Scanjobs“ zur Verfügung.

Funktion	Beschreibung
Name	Zeigt den Namen des Jobs an.
Statisch, Netzwerk, Community, Sandbox	Filtert die Ergebnisse basierend auf den Punktzahlen für jedes Bewertungsmodul.
Progress	Zeigt den aktuellen Fortschritt des Jobs an. • Grün: Der Job ist abgeschlossen. • Schwarz: Der Job wird noch ausgeführt. • Rot: Ein Fehler ist aufgetreten.
Info	Liefert zusätzliche Informationen. Zeigt die Abfrage für den Job an. Ist der Job noch nicht abgeschlossen, werden hier auch ausführlichere Beschreibungen des Status angezeigt.
Nutzer	Zeigt den Namen des Nutzers an, der den Job erstellt hat.
Events	Zählt die Anzahl der Ereignisse für den Job.
Fallengelassen	Zählt die Anzahl an Dateien/Ereignissen im Job, die verworfen wurden, weil ihre Bewertungen unter dem konfigurierten Schwellenwert lagen.
Ereignistyp	Gibt den Jobtyp an: Manuell hochladen, Nach Bedarf oder Erneut übermitteln.
Geplant	Gibt Datum und Uhrzeit der Ausführung des Jobs an.

Folgende Aktionen stehen im Dialogfeld zur Verfügung.

Funktion	Beschreibung
Schaltfläche Abbrechen	Bricht den ausgewählten Scanjob ab.
Schaltfläche Scan anzeigen	Zeigt die Ereigniszusammenfassung für den ausgewählten Scan mit den standardmäßigen Dashlets an.
Schaltfläche Fortlaufenden Modus anzeigen	Zeigt die Ereigniszusammenfassung für den ausgewählten Scan mit den standardmäßigen Dashlets an.

Dialogfelder „Einstellungen“ für Investigate-Ansichten

In NetWitness PlatformVersion 11.0 gibt es zwei Dialogfelder „Einstellungen“, eines für die Ansicht „Navigation“ und eines für die Ansicht „Ereignisse“. Mit dem Hinzufügen des Dialogfelds „Einstellungen“ für die Ansicht „Ereignisanalyse“ in Version 11.1 Investigate drei Dialogfelder „Einstellungen“.

Die Einstellungen in den Dialogfelder „Einstellungen“ in den Ansichten „Navigation“ und „Ereignisse“ stellen eine Untermenge der Investigation-Einstellungen dar, die unter „Profile“ > Bereich „Einstellungen“ > Registerkarte „Investigation“ vorgenommen werden können. Durch die Bereitstellung der Einstellungen innerhalb der Ansicht „Investigation“ wird das Arbeiten in NetWitness Platform für Analysten beschleunigt. Wenn Sie eine Einstellung hier ändern, wird diese Einstellung auch in der Ansicht „Profile“ geändert und umgekehrt.

Um auf dieses Dialogfeld zuzugreifen, wechseln Sie zur Ansicht **Navigieren** oder **Ereignisse** und klicken in der Symbolleiste auf die Option **Einstellungen**.

Die Einstellungen in der Ansicht „Ereignisanalyse“ haben keine entsprechenden Einstellungen im Bereich „Profile“ > „Einstellungen“.

Was möchten Sie tun?

Nutzerrolle	Ziel	Details anzeigen
Threat Hunter	Durchsuchen von Ereignismetadaten	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Durchsuchen von Raw-Ereignissen	Starten einer Ermittlung in der Ansicht „Navigation“ oder „Ereignisse“
Threat Hunter	Analyse von Raw-Ereignissen und Metadaten	Starten einer Ermittlung in der Ansicht „Ereignisanalyse“
Threat Hunter	Untersuchen von Endpunkten (Version 11.1)	Untersuchen von Hosts
Threat Hunter	Verdächtige Endpunktdateien finden (Version 11.1)	Untersuchen von Dateien
Threat Hunter	Dateien und Ereignisse auf Schadsoftware scannen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Priorisieren eines Incident in „Untersuchen“	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Einstellungen für Investigate konfigurieren*	Konfigurieren von Ansichten und Voreinstellungen von NetWitness Investigate

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

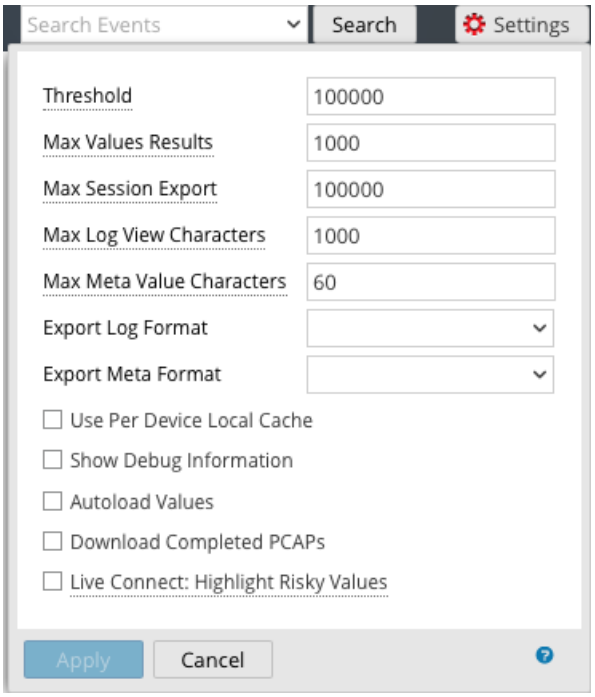
Verwandte Themen

- Wie funktioniert NetWitness Investigate?

Überblick

Die Dialogfelder „Einstellungen“ in den Ansichten „Navigation“ und „Ereignisse“ enthalten viele gemeinsame Komponenten.

Verschiedene Investigation-Einstellungen in der Ansicht „Navigation“ beeinflussen beim Laden von Werten im Bereich „Werte“ die Performance. Die Standardwerte basieren auf der gängigen Verwendung und einzelne Analysten können diese Einstellungen für ihre eigenen Ermittlungen anpassen. Die nachstehende Abbildung zeigt ein Beispiel des Dialogfelds und in der folgenden Tabelle sind die Funktionen beschrieben.



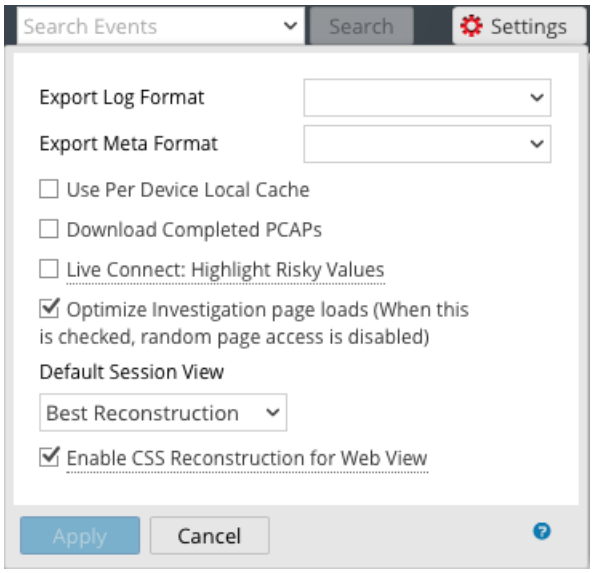
Funktion	Beschreibung
Schwellenwert	Legt den Schwellenwert für die maximale Anzahl der für einen Metaschlüsselwert geladenen Sitzungen im Bereich „Werte“ fest. Ein höherer Schwellenwert ermöglicht genauere Zählerangaben für einen Wert, verursacht aber auch längere Ladezeiten. Der Standardwert ist **100.000**.
Max. Wertergebnisse	Legt die maximale Anzahl von Werten fest, die in der Ansicht Navigieren geladen werden, wenn im Metaschlüsselmenü die Option Max. Ergebnisse für einen offenen Metaschlüssel ausgewählt ist. Der Standardwert ist **1.000**.
Max. Sitzungsexport	Legt die maximale Anzahl von Sitzungen fest, die exportiert werden können. Der Standardwert ist **100.000**.

Funktion	Beschreibung
Exportprotokollformat	Legt das Dateiformat der exportierten Protokolle fest. Vier Formate sind möglich: • Text • SML • CSV • JSON
Format exportierte Metadaten	Legt das Dateiformat der exportierten Metawerte fest. Vier Formate sind möglich: • Text • SML • CSV • JSON
Lokaler Cache pro Gerät	Wenn diese Option deaktiviert ist, sendet Investigate eine neue Abfrage an die Datenbank anstatt im Cache gespeicherten Daten in den Investigation-Ansichten nach dem Laden anzuzeigen. Wenn diese Option aktiviert ist, verwendet Investigate die Daten aus dem lokalen Cache.
Debuginformationen anzeigen	Diese Option steuert die Anzeige der `where`-Klausel unterhalb der Brotkrümelnavigation in der Ansicht „Navigation“ sowie der verstrichenen Ladezeit für jeden aggregierten Service für einen Broker. Wenn diese Option aktiviert ist, werden die Debug-Informationen angezeigt. Der Standardwert ist **Aus** (deaktiviert)**.**
Ereignisse in Ereignisbereich anhängen	Diese Option wirkt sich auf das Paging im Bereich „Ereignisse“ aus. Wenn diese Option aktiviert ist, wird die nächste Gruppe von Ereignissen an die bereits angezeigten Ereignisse angehängt. Wenn diese Option deaktiviert ist, wird die vorherige Seite mit Ereignissen durch die nächste Seite ersetzt. Der Standardwert ist **Aus** (deaktiviert).
Werte automatisch laden	Wenn diese Option aktiviert ist, werden die Werte für den ausgewählten Service automatisch in die Ansicht „Navigation“ geladen. Wenn diese Option aktiviert ist, werden bei der Auswahl eines zu untersuchenden Services Werte automatisch geladen. Wurde diese Option nicht aktiviert, zeigt Investigate die Schaltfläche **Werte laden** an, über die Sie Optionen ändern können. Der Standardwert ist **Aus**.
Abgeschlossene PCAPs herunterladen	Diese Einstellung automatisiert das Herunterladen von extrahierten PCAPs im Modul Investigation, damit extrahierte PCAP-Dateien nicht manuell heruntergeladen und in einer Anwendung zum Anzeigen von PCAP-Daten, z. B. Wireshark, geöffnet werden müssen.

Funktion	Beschreibung
Live Connect: Riskante IPs markieren	Wenn diese Option deaktiviert ist, werden alle Metawerte, die in Live Connect verfügbaren Kontext haben, im Bereich „Werte“ der Ansicht „Navigation“ hervorgehobenen. Wenn die Option aktiviert ist, werden unter allen Werten, die in Live Connect Kontext haben, nur die Werte, die von der Community als „Riskant/Verdächtig/Unsicher“ erachtet werden, hervorgehoben. Diese Option ist standardmäßig deaktiviert (**Aus**).
Anwenden	Setzt die Einstellungen sofort in Kraft. Diese sind auch beim nächsten Laden von Werten sichtbar. Dieselben Änderungen werden auch in der Ansicht Profile angewendet.
Abbrechen	Bricht den Bearbeitungsvorgang ab und schließt das Dialogfeld mit unveränderten Einstellungen.

Dialogfeld „Einstellungen“ der Ansicht „Ereignisse“

Die nachstehende Abbildung zeigt ein Beispiel des Dialogfelds für die Ansicht „Ereignisse“ und in der folgenden Tabelle sind die Funktionen beschrieben.

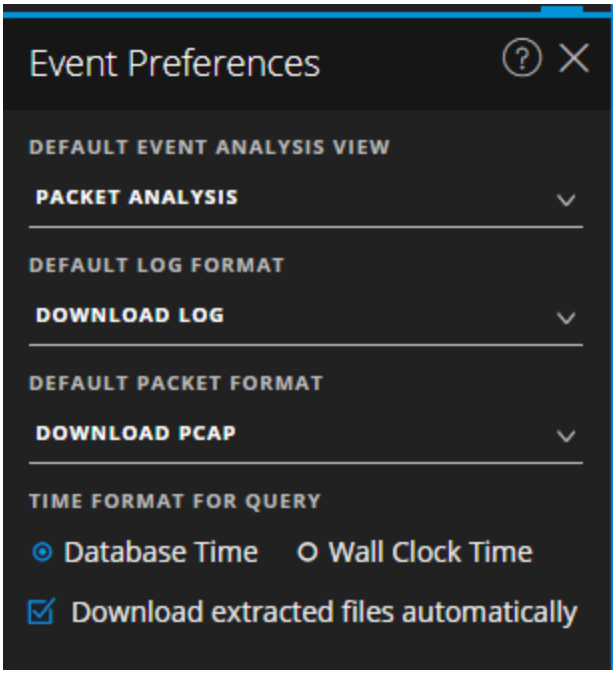


Funktion	Beschreibung
Exportprotokollformat	Legt das Dateiformat der exportierten Protokolle fest. Vier Formate sind möglich: • Text • SML • CSV • JSON

Funktion	Beschreibung
Format exportierte Metadaten	Legt das Dateiformat der exportierten Metawerte fest. Vier Formate sind möglich: • Text • SML • CSV • JSON
Abgeschlossene PCAPs herunterladen	Diese Einstellung automatisiert das Herunterladen von extrahierten PCAPs im Modul Investigation, damit extrahierte PCAP-Dateien nicht manuell heruntergeladen und in einer Anwendung zum Anzeigen von PCAP-Daten, z. B. Wireshark, geöffnet werden müssen.
Live Connect: Riskante IPs markieren	Wenn diese Option aktiviert ist, verwendet Investigate einen Filter, um nur die IP-Adressen abzurufen, die von der RSA-Community als riskant betrachtet werden. Wenn diese Option nicht aktiviert ist, zeigt NetWitness Platform alle IP-Adressen an. Diese Option ist standardmäßig deaktiviert (**Aus**).
Optimieren des Ladens der Seite „Investigation“	Legt eine Auslagerungsoption fest. Wenn optimiert, werden die Ergebnisse so schnell wie möglich zurückgegeben. Dabei geht die ursprüngliche Möglichkeit verloren, zu einer bestimmten Seite der Ereignisliste zu wechseln. Durch die Deaktivierung dieses Kontrollkästchens wird die Paginierung der Ereignislisten geändert, damit Sie auf eine bestimmte Seite in der Liste (oder auf die letzte Seite) springen können. Der Standardwert ist **aktiviert**.
Standardsitzungsansicht	Wählt den Standardrekonstruktionstyp für die anfängliche Rekonstruktion in der Ansicht Ereignisse aus. Der Standardwert ist **Beste Rekonstruktion**, bei dem die Ereignisse mithilfe der am besten für das Ereignis geeigneten Rekonstruktionsmethode wiederhergestellt werden.
CSS-Rekonstruktion für Webansicht ermöglichen	Diese Einstellung steuert, wie die Rekonstruktion von Webinhalten durchgeführt wird. Wenn die Einstellung aktiviert ist, werden bei der Webrekonstruktion auch Cascaded Style-Sheet-Stilvorlagen (CSS) und Bilder mit einbezogen, sodass die Darstellung der Originalansicht in einem Webbrowser entspricht. Dies schließt das Scannen und Rekonstruieren von verbundenen Ereignissen sowie das Suchen nach Stylesheets und Bildern ein, die im Zielereignis verwendet werden. Diese Option ist standardmäßig aktiviert. Deaktivieren Sie die Option, wenn Probleme beim Anzeigen bestimmter Websites auftreten.
Anwenden	Setzt die Einstellungen sofort in Kraft. Diese sind auch beim nächsten Anzeigen von Ereignissen sichtbar. Dieselben Änderungen werden auch in der Ansicht Profile angewendet.
Abbrechen	Bricht den Bearbeitungsvorgang ab und schließt das Dialogfeld mit unveränderten Einstellungen.

Bereich „Einstellungen“ der Ansicht „Ereignisanalyse“

Ab Version 11.1 hat die Ansicht „Ereignisanalyse“ Nutzereinstellungen, die Sie in der Ansicht „Ereignisanalyse“ > Bereich „Ereigniseinstellungen“ konfigurieren können. Diese Einstellungen bleiben erhalten, sodass sie jedes Mal, wenn Sie sich anmelden und zur Ansicht „Ereignisanalyse“ wechseln, angewendet werden. Die nachstehende Abbildung zeigt ein Beispiel des Dialogfelds und in der Tabelle darunter sind die Optionen beschrieben.



Funktion	Beschreibung
Standardmäßige Ansicht „Ereignisanalyse“	Wählt die Standardansicht „Ereignisanalyse“ aus, die jedes Mal angezeigt wird, jedes Mal, wenn Sie die Ansicht „Ereignisanalyse“ öffnen. Wenn Sie zum Beispiel „Dateianalyse“ auswählen, wird der Bereich „Dateianalyse“ hervorgehoben und jedes Mal angezeigt, wenn Sie ein Ereignis in der Ansicht „Ereignisanalyse“ untersuchen. Folgende Optionen stehen zur Verfügung: • **Textanalyse**: Anzeigen und Analysieren der Rohtextnutzlast eines Ereignisses. • **Paketanalyse**: Anzeigen und interaktive Analyse der Pakete und der Nutzlast eines Ereignisses. • **Dateianalyse**: Anzeigen einer Liste von Dateien und Herunterladen einer oder mehrerer Dateien in einem Ereignis.

Funktion	Beschreibung
Standardmäßiges Protokollformat	Wählt das Standardformat für das Herunterladen von Protokollen aus: • **Protokoll herunterladen**: Raw-Protokoll (Protokoll) mit dieser Option. • **CSV herunterladen**: Kommagetrennte Werte (CSV) mit dieser Option. • **XML herunterladen**: Die XML-Datei (Extensible Markup Language) mit dieser Option. • **JSON herunterladen**: Die JSON-Datei (JavaScript Object Notation) mit dieser Option.
Standardmäßiges Paketformat	Wählt das Standardpaketformat für das Herunterladen von Paketen aus: • **PCAP herunterladen**: Zum Herunterladen des gesamten Ereignisses als eine Paketerfassungsdatei (*.pcap). • **Alle Nutzdaten herunterladen**: Zum Herunterladen der Nutzdaten als eine *.payload-Datei. • **Anforderungsnutzdaten herunterladen**: Zum Herunterladen der Anforderungsnutzdaten als eine *.payload1-Datei. • **Antwortnutzdaten herunterladen**: Zum Herunterladen der Antwortnutzdaten als eine *.payload2-Datei.
Zeitformat für Abfrage	Die Ansicht „Ereignisanalyse“ kann Ergebnisse basierend auf der Datenbankzeit oder der aktuellen Uhrzeit anzeigen. Die Standardeinstellung für diese Einstellung ist „Datenbankzeit“. Dieses Zeitformat wird auch zur Anzeige von Abfrageergebnissen in den Ansichten „Navigation“ und „Ereignisse“ verwendet. Wenn **Datenbankzeit** ausgewählt ist, basieren Start- und Endzeit für eine Abfrage auf der Zeit, zu der das Ereignis gespeichert wurde. Wenn **Uhrzeit** ausgewählt ist, wird die Abfrage mit der Endzeit basierend auf der aktuellen Browserzeit ausgeführt; die Startzeit wird basierend auf dieser Endzeit und dem Zeitraum berechnet.
Extrahierte Dateien automatisch herunterladen	Ermöglicht das automatische Herunterladen von Dateien, wenn sie in dem Standardformat sind, das in den Feldern **Standardmäßiges Protokollformat** und **Standardpaketformat** im Bereich „Ereigniseinstellungen“ ausgewählt ist. Wählen Sie das Kontrollkästchen aus, um das automatische Herunterladen des ausgewählten Formats in den lokalen Ordner zu aktivieren. Andernfalls geht der Auftrag zum Herunterladen in die Jobwarteschlange und Sie können ihn manuell herunterladen.