RSA NETWITNESS® SUITE

Ermittlung und Malware-Analyse – Benutzerhandbuch

für Version 11.0

Kontaktinformationen

Der RSA-Link unter https://community.rsa.com enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, 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

Diese Software und die zugehörige Dokumentation sind Eigentum von EMC und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden.

Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens EMC ausgelegt werden.

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

EMC 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 2018

Inhalt

Wie funktioniert NetWitness Investigate? 9

Daten und Metadaten 9
Analysemethoden 9
Auslöser für eine Ermittlung 10
Workflow einer Ermittlung 11
Ansicht „Navigation“ 11
Ansicht Ereignisse 12
Ansicht „Malware Analysis“ 14
Kontextbezogene Informationen für ein Ereignis 14
Ereignisrekonstruktion und Ereignisanalyse 15
Malware Analysis-Funktionen 17
Funktionsübersicht 17
Analysemethode 19
Bewertungsmethode: 20
Bereitstellung 20
Schadsoftware-Auswertungsmodule 21
Netzwerk 21
Statische Analyse 22
Community 22
Sandbox 22
Rollen und Berechtigungen für Malware-Analysten. 23
Erforderliche Rollen und Berechtigungen 23

Konfigurieren von Ermittlungsansichten und -einstellungen 27

Konfigurieren der Schadsoftware-Ansicht Ereigniszusammenfassung 28
Hinzufügen eines Dashlet 29
Ändern oder Löschen eines Dashlet mithilfe von Symbolleistenoptionen 29
Anwenden des Schwellenwertfilters auf mehrere Dashlets 29
Einstellen des Titels und der Kategorieoptionen für ein Dashlet 30
Dashlets anordnen 31
Wiederherstellen von Standard-Dashlets 32
Konfigurieren von Navigationsansicht und Ereignisansicht 33

Zugriff auf die Investigation-Einstellungen 33
Kalibrieren der Werte der Ladeparameter in der Ansicht „Navigation“ 36
Konfigurieren des PCAP-Downloadverhaltens in Investigation 37
Konfigurieren des Standard-Exportprotokollformats in Investigation 37
Konfigurieren des Standard-Metaexportformats in Investigation 38
Kalibrieren des Abrufs und der Standardrekonstruktion in der Ansicht „Ereignisse“ 38
Aktivieren oder Deaktivieren der Cascading Style Sheet-Darstellung in Rekonstruktionen von Webinhalt 39
(Optional) Konfigurieren von Suchoptionen 39

Durchführen einer Ermittlung 41

Starten einer Untersuchung für einen Service oder eine Sammlung 43
Beginnen einer Untersuchung in der Ansicht „Navigation“ (ohne Standardservice) 44
Einrichten oder Löschen des Standardservices 45
Starten einer Ermittlung (Standardservice angegeben) 47
Ändern des zu untersuchenden Services oder der Sammlung 48
Untersuchen von Workbench-Wiederherstellungssammlungen 51
Einschränken der in der Ansicht „Navigation“ angezeigten Ergebnisse 53
Metagruppen managen 53
Verwalten und Anwenden von Standardmetaschlüsseln in einer Ermittlung 61
Suchen nach Textmustern in der Ansicht „Untersuchen“ 65
Optionen zum Steuern des Suchverhaltens 66
Syntax für die Suche nach regulären Ausdrücken 68
Rohtext-Schlüsselwortsuche 69
Suchen in der Ansicht „Navigation“ 69
Suchen in der Ansicht „Ereignisse“ 69
Einstellen der Quantifizierungsmethode und Sortierreihenfolge von Metaschlüsselergebnissen 70
Einstellen des Zeitbereichs für eine Ermittlung 72
Einkapseln von benutzerdefinierten Ansichten mithilfe von Ermittlungsprofilen 74
Visualisieren von Metadaten als Parallelkoordinaten 77
Abfragen von Daten in der Ansicht „Navigation“ 91
Erstellen einer angepassten Abfrage 91
Zeitdiagramm des Drill-down in die Daten in der Ansicht „Navigation“ 96

Drill-down zu Daten im Bereich „Werte“ 98
Anzeigen und Ändern von Abfragen mithilfe von URL-Integration 105
Alle Aktivitäten am 03/12/2013 zwischen 5:00 und 6:00 Uhr mit einem registrierten Hostnamen 107
Alle Aktivitäten am 03/12/2013 zwischen 17:00 und 17:10 Uhr mit Http-Datenverkehr zu und von der IP-Adresse 10.10.10.3 107
Aktionen zu Drill-down-Punkten in der Ansicht „Navigation“ 108
Exportieren eines Drill-Punkts 108
Starten einer externen Suche eines Metaschlüssels 109
Starten eines Schadsoftwareanalyse-Scans in der Navigationsansicht 114
Managen von Context Hub-Listen und -Listenwerten in Investigate 116
Öffnen der Ereignisliste 118
Ausdrucken des aktuellen Drill-down-Punkts 119
Visualisieren des aktuellen Drill-Punkts in Informer 120
Anzeigen von zusätzlichem Kontext für einen Datenpunkt 121
Untersuchen von Ereignissen 124
Filter und Suchergebnisse in der Ansicht Ereignisse 124
Kombinieren von Ereignissen aus geteilten Sitzungen 128
Managen von Spaltengruppen in der Ereignisansicht 133
Rekonstruieren eines Ereignisses 135
Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“ 140
Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion 175
Exportieren von Ereignissen 177
Durchführen von Schadsoftwareanalysen 179
Beginnen einer Schadsoftwareanalyse-Ermittlung 180
Starten einer Schadsoftwareermittlung von einem Malware Analysis-Dashlet aus 181
Beginnen einer Malware Analysis Investigation (ohne Standardservice) 182
Einrichten oder Löschen des Standardservices 184
Hochladen und Scannen von Dateien 185
Starten einer Ermittlung (Standardservice angegeben) 185
Anwenden von Zeitparameterfilter auf Ergebnisse 186
Anwenden eines Schwellenwertfilters auf Ergebnisse von Scans im kontinuierlichen Modus 186
Löschen oder erneutes Übermitteln eines Scans nach Bedarf mit neuen 187

Umgehungseinstellungen
Anzeigen der Dateiliste 188
Anzeigen der Ereignisliste 189
Implementieren von angepassten YARA-Inhalten 191
Voraussetzungen 191
YARA-Version und -Ressourcen 191
Metaschlüssel in YARA-Regeln 192
YARA-Inhalte 193
Hinzufügen von benutzerdefinierten YARA-Regeln 194
Überprüfen von Scandateien und Ereignissen in Listenform 196
Sortieren der Datei- bzw. Ereignisliste 197
Filtern der Liste nach Dateinamen oder MD5-Datei-Hash 197
Löschen von Ereignissen aus dem Scan 199
Rückkehr zur Ereigniszusammenfassung 199
Öffnen der detaillierten Analyse für ein Ereignis 199
Filtern der Dashlet-Daten in der Ansicht Ereigniszusammenfassung 200
Konfiguration des Dashlet „Punktezahlrad“ 200
Konfiguration des Dashlet „Meta-Treemap“ 202
Konfiguration des Dashlet „Meta-Strukturen“ 203
Konfiguration des Dashlet „Ereigniszeitachse“ 204
Konfiguration des Dashlet „Top-Liste höchst verdächtiger Schadsoftware“ 204
Konfiguration des Dashlet „Schadsoftware mit IOCs mit hoher Wahrscheinlichkeit und hohen Werten“ 205
Konfiguration des Dashlet „Top-Liste möglicher Zero-Day-Schadsoftware“ 206
Hochladen von Dateien für Malware Analysis-Scans 207
Manuelles Hochladen von Dateien 207
Hochladen von Dateien aus einem beobachteten Ordner 209
Anzeigen der detaillierten Schadsoftwareanalyse eines Ereignisses 212
Anzeigen der Schadsoftwareanalyse-Details für ein Ereignis 212
Pivotieren der Netzwerkanalyse-Ergebnisse 213
Verwenden der Option Dateiaktionen in der Ansicht Statische Analyseergebnisse 214
Anzeigen der Details der Communityanalyseergebnisse 215
Anzeige der Sandbox-Analyseergebnisse in der ThreatGrid-Benutzeroberfläche 216

Ermittlungs-Referenzmaterialien 217

Dialogfeld „Ereignisse zu einem Incident hinzufügen“ 219
Dialogfeld „Zur Liste hinzufügen/Aus Liste entfernen“ 223

Bereich „Kontextabfrage“ 227
Abfrageergebnisse 229
Dialogfeld „Incident erstellen“ 232
Ansicht „Ereignisanalyse“ 235
Ansicht „Ereignisanalyse“ – Bereich „Dateianalyse“ 239
Ansicht „Ereignisanalyse“ – Bereich „Paketanalyse“ 242
Ansicht „Ereignisanalyse“ – Bereich „Textanalyse“ 246
Ansicht „Ereignisrekonstruktion“ 249
Ansicht Ereignisse 253
Dialogfeld „Untersuchen“ 260
Registerkarte „Investigation“ – Bereich „Benutzereinstellungen“ 264
Dialogfeld „Standardmetaschlüssel managen“ 271
Malware Analysis-Ereignisliste und -Dateiliste 276
Dialogfeld „Spaltengruppen managen“ 283
Dialogfeld „Metagruppen managen“ 288
Dialogfeld „Profile managen“ 292
Ansicht „Malware Analysis“ 296
Ansicht „Navigieren“ 304
Symbolleiste 307
Schaltfläche zum Anhalten/Neuladen und Breadcrumb 313
(Optional) Debug-Informationen 314
Zeitbanner 315
Visualisierungen 315
Bereich „Werte“ 320
Dialogfeld „Abfrage“ 326
Dialogfeld „Auf Schadsoftware scannen“ 331
Dialogfeld „Malware Analysis Service auswählen“ 334
Einstellungsdialogfeld für die Ansichten „Navigieren“ und „Ereignisse“ 338

Wie funktioniert NetWitness Investigate?

Investigate bietet die Datenanalysefunktionen, die in RSA NetWitness® Suite 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.

Daten und Metadaten

RSA NetWitness Suite 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. Die konfigurierten Parser und Feeds auf dem Decoder erstellen Metadaten, die Analysten verwenden können, um die aufgenommenen Protokolle und Pakete zu untersuchen. Ein anderer Servicetyp, der als Concentrator bezeichnet wird, indiziert und speichert die Metadaten.

Analysten fragen in der Regel den Concentrator ab, um Bedrohungen zu erkennen. Der Concentrator verarbeitet Abfragen. Sie gehen erst dann zum Decoder, wenn eine vollständige Rekonstruktion von Sitzungen, Endpunktereignissen 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.

Analysemethoden

Analysten können erfasste Daten untersuchen, Ergebnisse von anderen NetWitness Suite-Ansichten in Investigate öffnen und Daten aus anderen Sammlungsquellen importieren. Im Laufe einer Ermittlung können Analysten problemlos zwischen den drei Ansichten im Modul „Investigation“ umschalten: Ansicht „Navigation“, Ansicht „Ereignisse“ und Ansicht „Malware Analysis“.

Analysten verwenden Investigate, um Ereignisse zu suchen, die den Workflow für die Reaktion auf Incidents voranbringen oder um strategische Analysen durchzuführen, nachdem ein anderes Tool ein Ereignis erzeugt hat. Ein Incident-Experte, der an einem Incident in NetWitness Respond arbeitet, kann den Incident in NetWitness Investigate öffnen und Ereignisse zum Incident hinzufügen. Ein Threat Hunter, die in NetWitness Investigate arbeitet, kann ein Ereignis zu einem vorhandenen Incident hinzufügen oder einen neuen Incident in NetWitness Respond erstellen. In beiden Fällen führt der Analyst ein Drill-down oder ein Pivot in die Metadaten durch, um die Anzahl der Protokolle und Pakete zu filtern und verdächtige Ereignisse anzuzeigen, während er sich auf bestimmte Kombinationen von Metadaten konzentriert, die zu einem Incident führen.

Hinweis: Spezifische Benutzerrollen und -berechtigungen werden von einem Benutzer benötigt, damit dieser Ermittlungen und Schadsoftwareanalysen in NetWitness Suite 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.

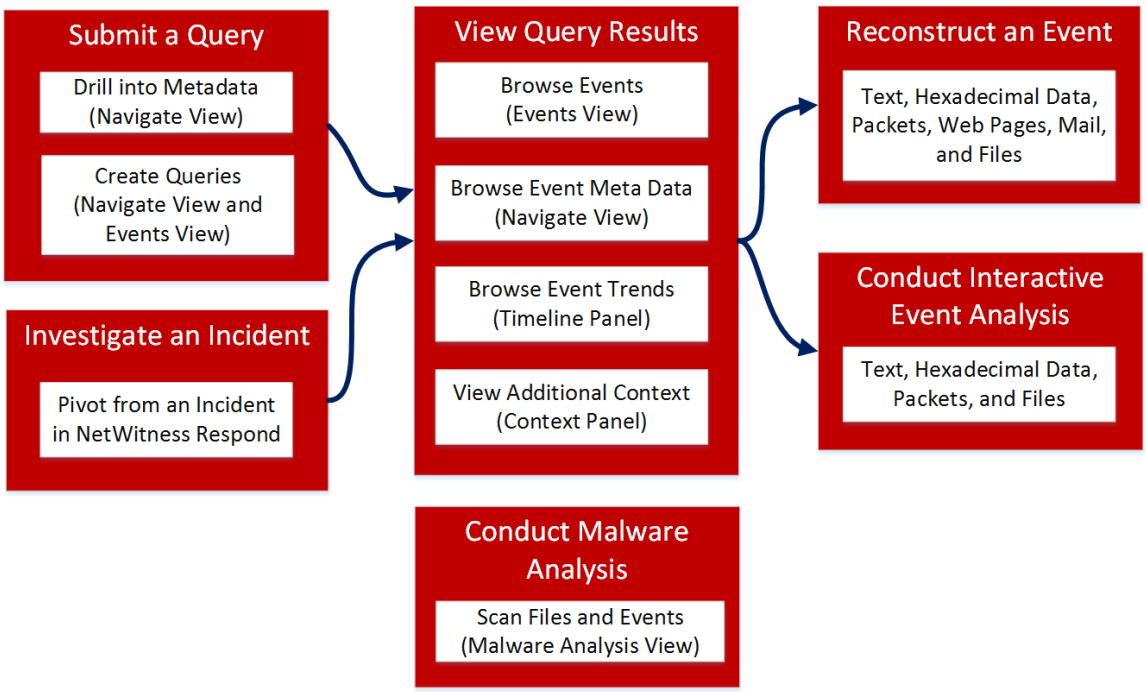
Auslöser für eine Ermittlung

Es folgen einige Beispiele für Auslöser einer Ermittlung:

- Sie erhalten Informationen von einem Dritten zu einem neuen Active Directory-Hack. Sie verwenden diese, um eine Suche über all Ihre Active Directory-Rohprotokolldaten für die letzten 24 Stunden durchzuführen.
- Sie werden vom SOC-Manager gebeten, aufgrund der derzeitigen Beliebtheit von Pokemon Go diesbezügliche Malware zu finden. Sie erstellen 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 seltsamen Indikatoren in Bezug auf einen Host zeigt. Sie stellen eine Verknüpfung mit diesem Host her, um spezifische Details zu finden.
- Sie suchen den nächsten Zero-Day-Angriff und navigieren durch Netzwerkmetadaten, um ungewöhnliche automatisierte Sitzungen zu finden, die das Unternehmen verlassen.
- Sie werden von Ihrem SOC-Manager gebeten, Informationen im Zusammenhang mit Benutzer `jarvis` zu finden, einem Mitarbeiter, der gerade entlassen wurde. Sie führen eine Abfrage für die letzte Woche für diesen Benutzernamen durch.

Workflow einer Ermittlung

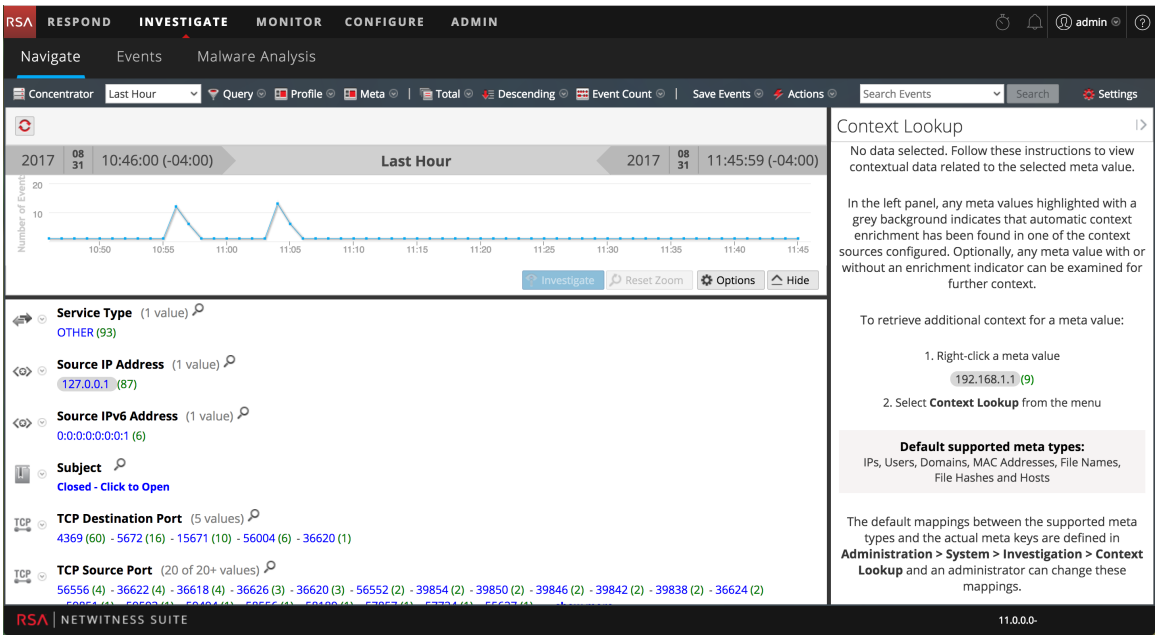
Diese Abbildung zeigt den allgemeinen Workflow einer Ermittlung. An einem normalen Tag führt der Analyst die Schritte im allgemeinen Workflow kreislaufförmig aus. Sie beginnen in der Regel mit der Ausführung einer Abfrage, filtern dann eine Teilmenge der Ereignisse heraus, rekonstruieren oder analysieren ein Ereignis und wiederholen dann die Schritte, um ein anderes Ereignis zu rekonstruieren oder analysieren. 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 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 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.



Nachdem Sie eine Abfrage eingegeben oder eine Ermittlung von NetWitness Respond gestartet haben, werden definierte Metaschlüssel abgefragt und die Inhalte der erfassten Pakete, Protokolle und Endpunktereignisse werden in der Ansicht „Navigation“ angezeigt.

Ansicht „Navigation“

Diese Abbildung zeigt die Ansicht Navigieren.



Die Ansicht „Navigation“ bietet die Möglichkeit, einen Drill-down und eine Abfrage für Daten auf einem Broker, Concentrator oder Decoder vorzunehmen, wobei das Untersuchen eines Decoder nicht typisch ist. Jede Situation ist einzigartig in Bezug auf die Art der Informationen, die der Analyst sucht. Ermittlungen präsentieren die Inhalte der erfassten Pakete, Protokolle und Endpunktereignisse als eine Sammlung extrahierter Daten in der Ansicht „Navigation“. Die definierten Metaschlüssel werden abgefragt und Werte werden mit der Anzahl der Ereignisse zurückgegeben. Wenn Sie auf einem beliebigen Level auf einen Wert klicken, werden die Ergebnisse detailliert angezeigt.

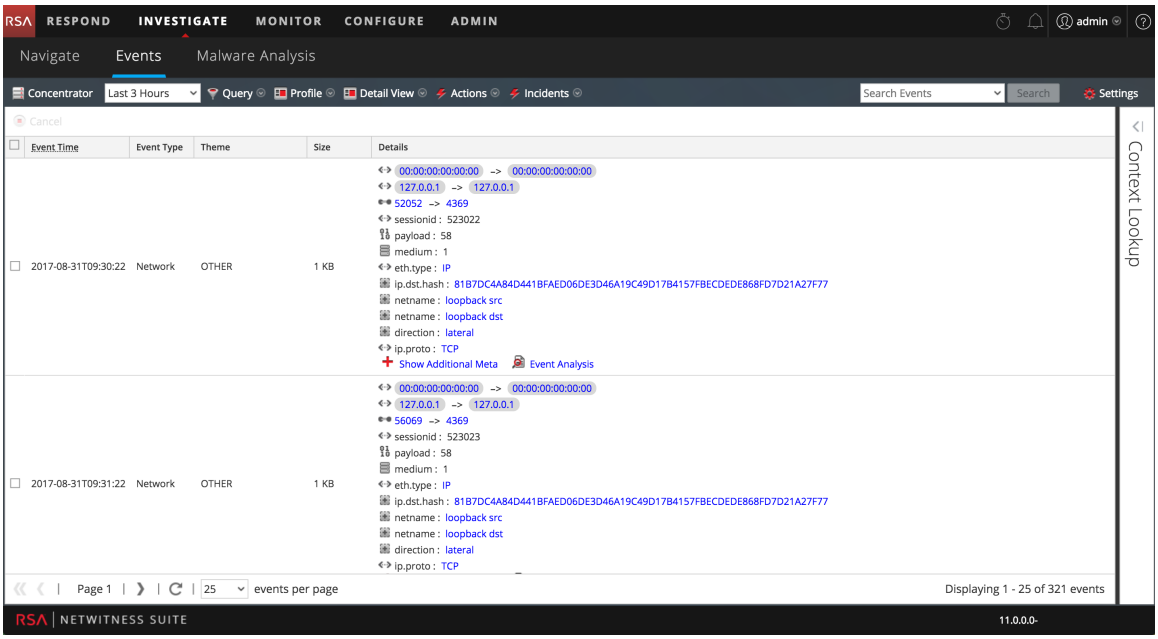
In der Ansicht „Navigation“ können Sie mit dem Context Hub für bestimmte konfigurierte Metaschlüssel wie IP-Adresse oder Hostname nach zusätzlichen Kontextinformationen rund um einen Wert suchen. Der zusätzliche Kontext kann Incidents, Warnmeldungen und andere Quellen umfassen, in denen der Wert erwähnt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

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.

Die Ansicht „Navigation“ bietet auch eine sequenzielle Visualisierung der Daten auf einer Zeitachse. Hier können Sie einen ausgewählten Zeitraum vergrößern.

Ansicht Ereignisse

Diese Abbildung zeigt die 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 an einem aktuellen Drill-down-Punkt von der Ansicht „Navigation“ aus öffnen. 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 Suite Core-Service zugreifen können, ohne zuerst ein Drill-down durch Metadaten durchführen zu müssen.

Die Ansicht „Ereignisse“ präsentiert Ereignisinformationen in drei Standardformen, eine einfache Auflistung von Ereignissen in Rasterform, eine detaillierte Auflistung von Ereignissen und eine Protokollansicht. Zusätzlich zu den Standardformularen können Sie eine angepasste Spaltengruppe ausgewählter Metaschlüssel erstellen, dann die angepasste Spaltengruppe einem angepassten Profil zuweisen, um die Ereignisliste anzuzeigen. Sobald sie erstellt sind, können angepasste Spaltengruppen und Profile aus einer Drop-down-Liste ausgewählt werden.

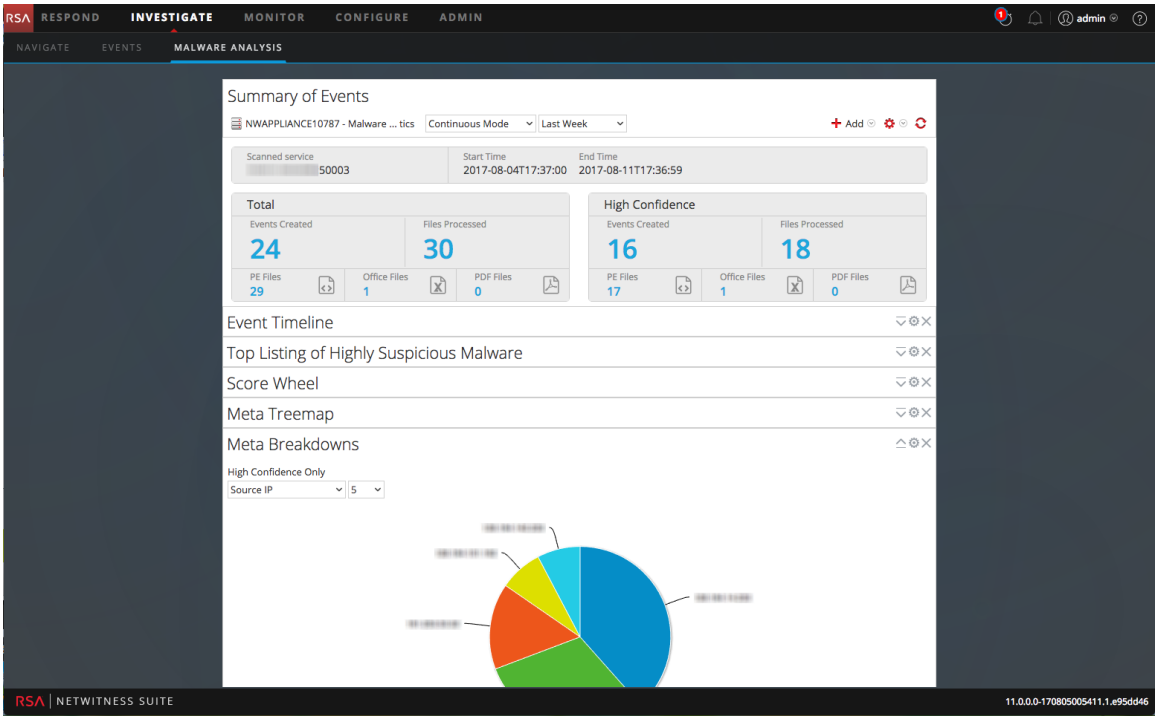
In der Ansicht Ereignisse können Sie:

- Ein Ereignis von der Ereignisliste wiederherstellen Zwei Rekonstruktionsschnittstellen können in der Ansicht „Ereignisse“ aufgerufen werden: Ereignisrekonstruktion und Ereignisanalyse.
- Ermittlungsprofile verwenden, um verschiedene Ermittlungseinstellungen in auswählbare Sätze zusammenzubinden, Ermittlungsmetagruppen zu importieren und zu exportieren, Ermittlungsspaltengruppen zu importieren und zu exportieren
- Ereignisse und zugeordnete Dateien exportieren

- Einen Incident aus einem Ereignis erstellen oder einen Incident bearbeiten, um Ereignisse hinzuzufügen oder zu entfernen

Ansicht „Malware Analysis“

Diese Abbildung zeigt die 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. Sie können die Ansicht „Malware Analysis“ direkt öffnen oder eine Kontextmenüaktion verwenden, um von einem Metawert in einem aktuellen Drill-down-Punkt in der Navigationsansicht nach Schadsoftware zu scannen. Der Schadsoftwareanalyst kann die Multi-Level-Auswertungsmodule nutzen, um die enorme Anzahl an erfassten Dateien zu priorisieren, von denen potenziell die größte Gefahr ausgeht.

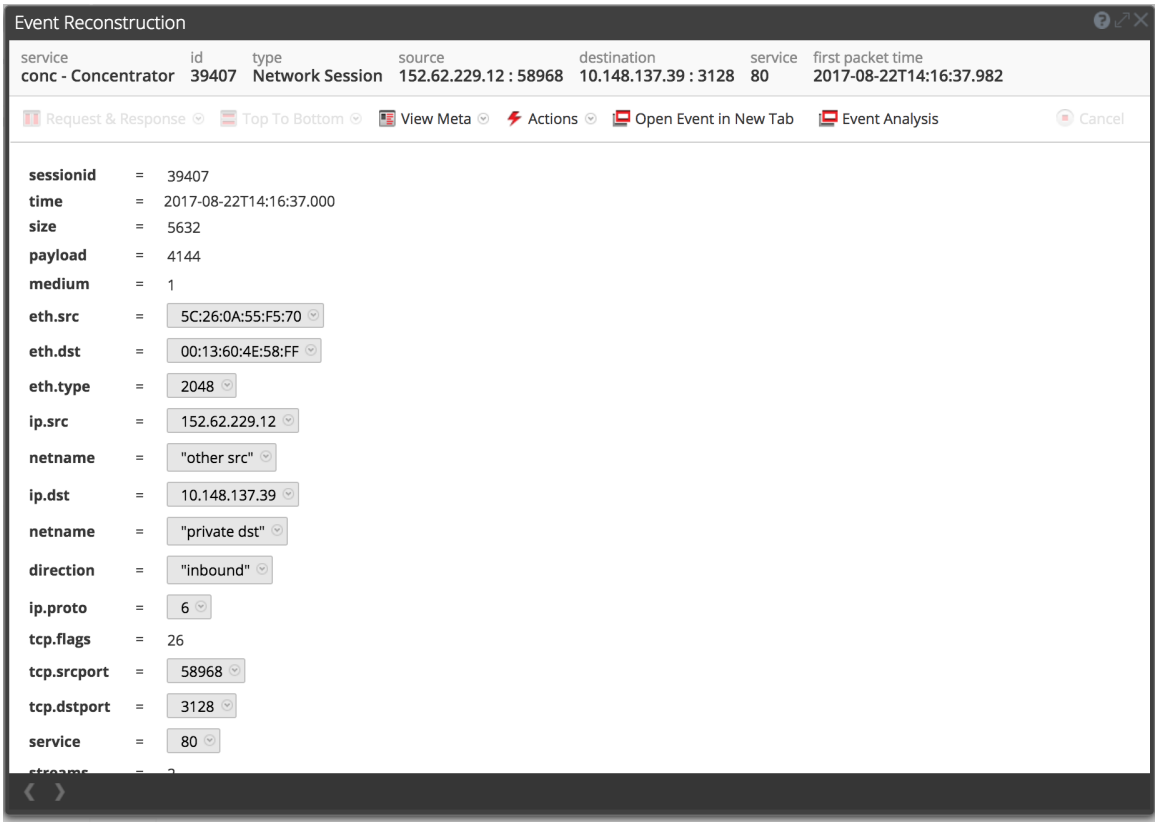
Kontextbezogene Informationen für ein Ereignis

Aus den Ansichten „Navigation“ und „Ereignis“ können Sie Details zu Elementen nachschlagen, die mit einem Ereignis (IP-Adresse, Benutzer, Host, Domain, MAC-Adresse, Dateiname, 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. Im Context Hub können Sie auf einen Datenpunkt klicken, um zurück zur Ansicht „Navigation“ zu gelangen.

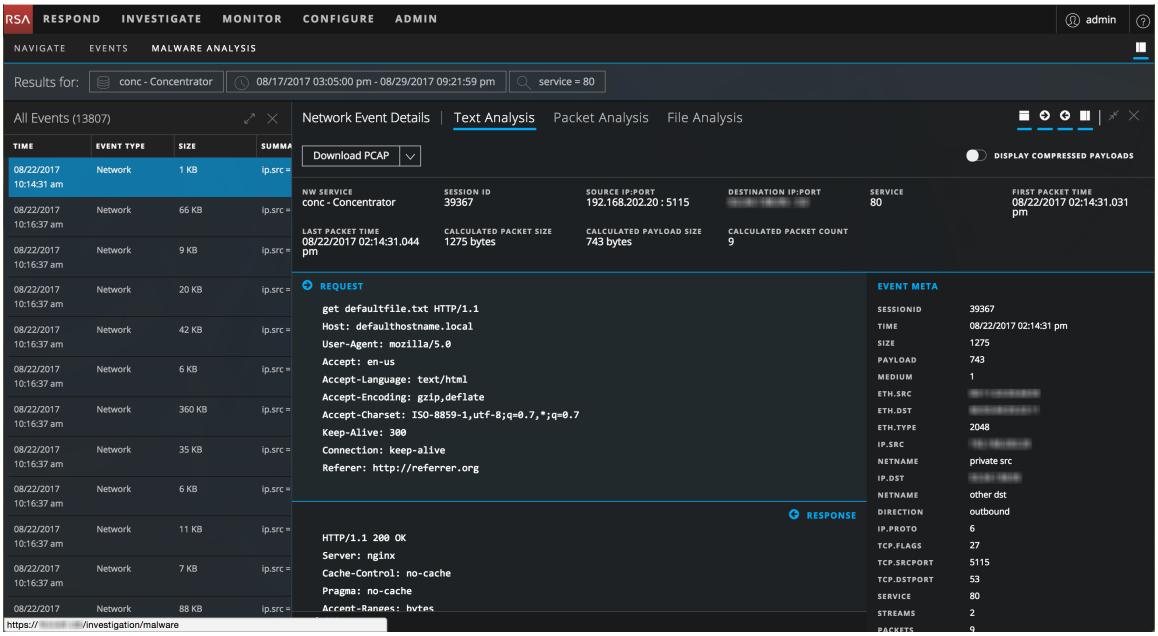
Ereignisrekonstruktion und Ereignisanalyse

Wenn Sie ein Ereignis ermitteln, das zusätzliche Untersuchungen verdient, können Sie ein Ereignis mit Ereignisrekonstruktion oder interaktiver Ereignisanalyse bedenkenlos 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“ wird in einem Fenster über der Ansicht „Ereignisse“ geöffnet. Sie sehen die Metaschlüssel und Metawerte in einer Liste und auf einer Seite, um das nächste Ereignis in dieser Form 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. Diese Abbildung ist ein Beispiel für die Ereignisrekonstruktion.



Die Ansicht „Ereignisanalyse“ ist ein interaktives Tool, das Analysten hilft, Pakete, Text, oder Dateien in einem Ereignis mit visuellen Hinweisen für bestimmte Arten von Informationen anzuzeigen. Je nach Typ der Rekonstruktion, z. B. Pakete, Text oder Dateien, sind unterschiedliche Informationen relevant. 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“.



Malware Analysis-Funktionen

NetWitness Suite 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.

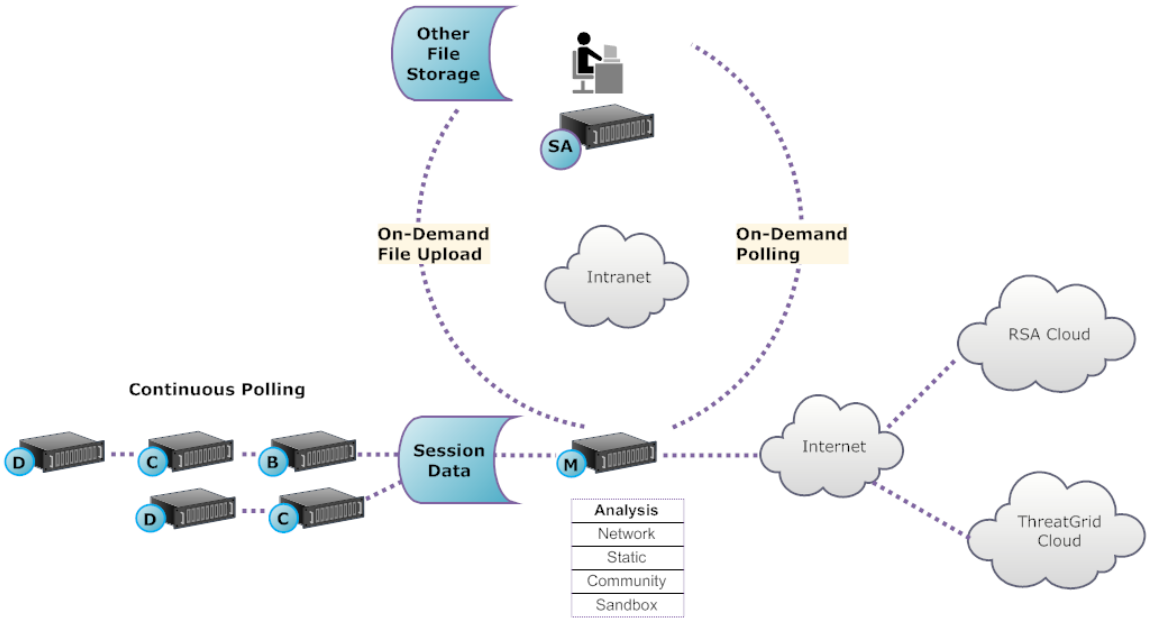
Zusätzlich zu den integrierten Indikatoren für eine Infizierung unterstützt Malware Analysis auch in YARA geschriebene Indikatoren für eine Infizierung. YARA ist eine Regelsprache, die es Schadsoftwareforschern ermöglicht, Schadsoftwaremuster zu identifizieren und zu klassifizieren. Dies ermöglicht es 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.

Daily Quota (Number of Files)	Free	Standard	Enterprise
Malware Analysis	100	unlimited	unlimited
ThreatGrid Analysis	5	1000	5000



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 Suite-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 Suite 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 Suite 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 Suite 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.

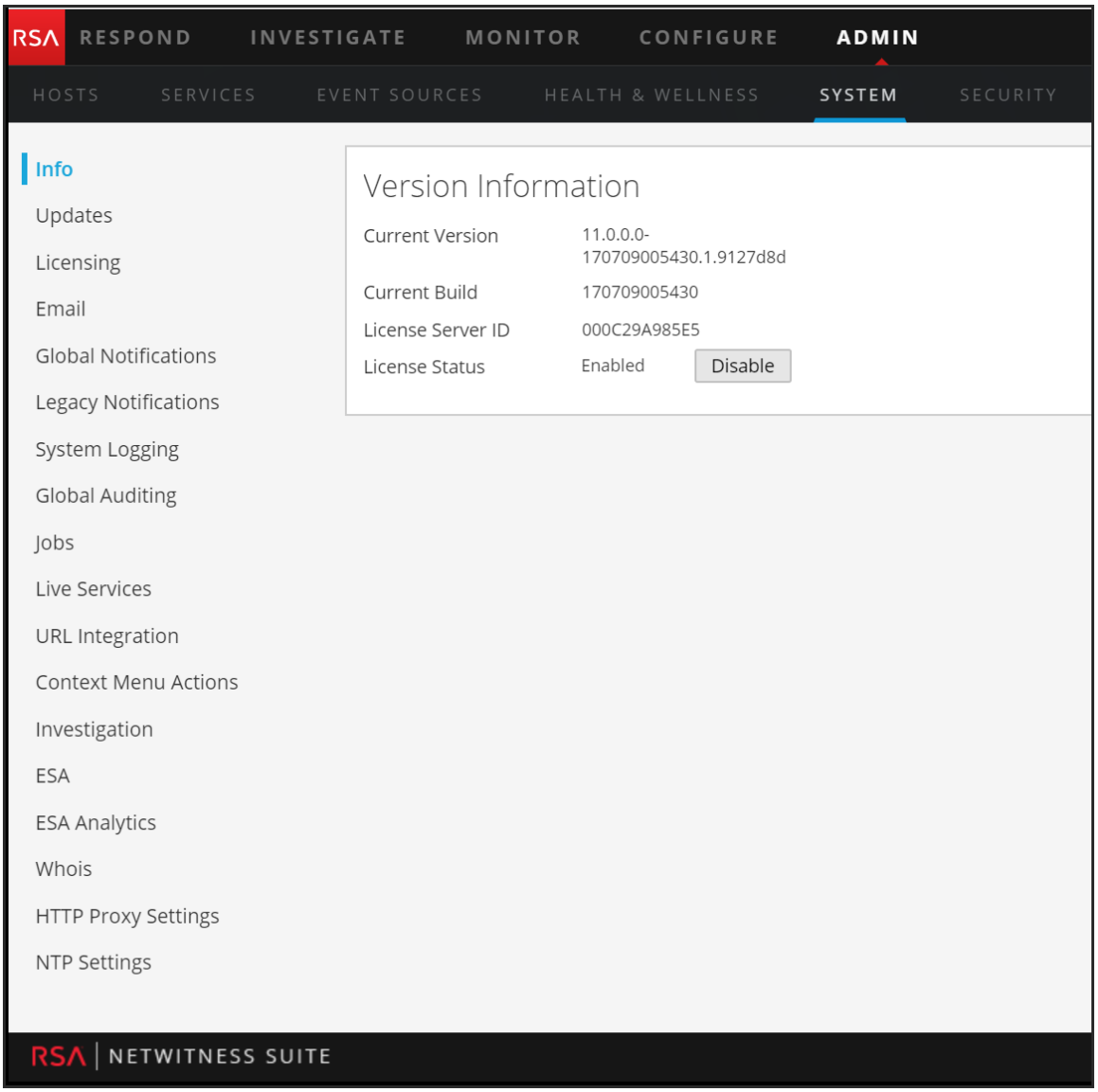
Rollen und Berechtigungen für Malware-Analysten.

In diesem Thema werden die Benutzerrollen und Berechtigungen erläutert, die für einen Benutzer zum Durchführen einer Schadsoftwareanalyse in NetWitness Suite erforderlich sind. 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.

Erforderliche Rollen und Berechtigungen

RSA NetWitness Suite managt die Sicherheit durch Gewähren des Zugriffs auf Ansichten und Funktionen mithilfe von Systemberechtigungen und Berechtigungen für individuelle Services.

Auf der Systemebene in der Ansicht „Administration > System“ muss dem Benutzer eine Systemrolle zugewiesen werden, die Zugriff auf bestimmte Ansichten und Funktionen gewährt.



Der standardmäßigen Rolle `Malware_Analysts` in NetWitness Suite 11.0 werden alle unten aufgeführten Berechtigungen zugewiesen. Falls erforderlich, kann ein Administrator eine benutzerdefinierte Rolle mit mehreren der folgenden Berechtigungen erstellen:

- Auf Investigation-Modul zugreifen (erforderlich)
- Investigation – Navigieren durch Ereignisse
- Investigation – Navigieren durch Werte
- Auf Incident-Modul zugreifen
- Incidents anzeigen und managen
- Anzeigen von Schadsoftwareereignissen (zum Anzeigen von Ereignissen)

- Dateidownload (zum Herunterladen von Dateien aus dem Malware Analysis-Service)
- Initiieren eines Schadsoftwarescans (zum Initiieren eines einmaligen Servicescans oder eines einmaligen Dateiuploads)
- Dashlet-Berechtigungen aus praktischen Gründen: Dashlet – Untersuchen der Top-Werte, Dashlet – Untersuchen der Servicelisten, Dashlet – Untersuchen der Jobs, Dashlet – Untersuchen der Verknüpfung.

Ein Anwendungsbeispiel für die Erstellung einer benutzerdefinierten Rolle ist die Rolle eines Assistenten des Schadsoftwareanalysten mit eingeschränkten Berechtigungen, die nicht die Berechtigungen zum Herunterladen von Dateien umfassen.

Für bestimmte Services muss ein Schadsoftwareanalyst der Gruppe **Analysten** oder einer anderen Gruppe angehören, die die zwei Standardberechtigungen der Gruppe „Analysten“ aufweist: **sdk.meta** und **sdk.content**. Benutzer mit diesen Berechtigungen können zum Zwecke der Analyse für den Service bestimmte Anwendungen verwenden, Abfragen ausführen und Inhalte anzeigen.

Konfigurieren von Ermittlungsansichten und -einstellungen

Analysten können einige Merkmale der Ansichten und des Verhaltens von NetWitness Suite Investigation konfigurieren. Sie können die Art anpassen, in der die Investigation-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 Investigation 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 Malware-Analysten. beschrieben.

Diese Themen enthalten weitere Informationen:

- Konfigurieren von Navigationsansicht und Ereignisansicht
- Konfigurieren der Schadsoftware-Ansicht Ereigniszusammenfassung

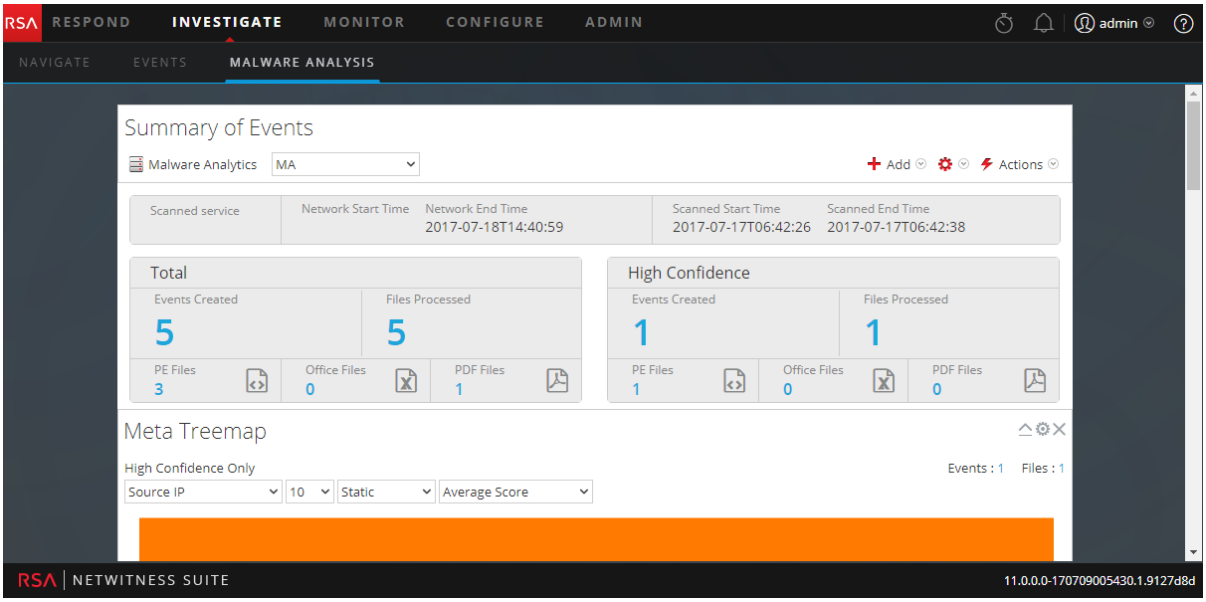
Konfigurieren der Schadsoftware-Ansicht

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.

Hinzufügen eines Dashlet

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: Ergebnisrad, Meta-Treemap, Meta-Strukturen und Ereigniszeitachse. Die anderen drei Dashlets sind die gleichen Dashlets, die im Dashboard „NetWitness Suite“ 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 Suite.
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.

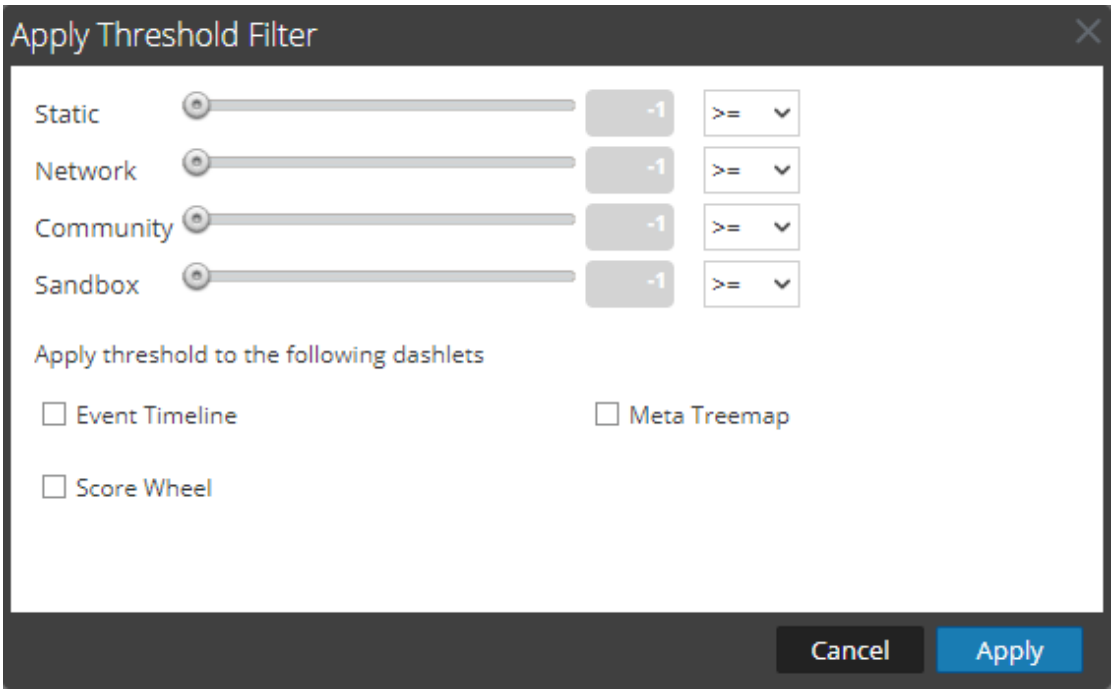
So verwenden Sie die Symbolleistenoptionen:

- 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.

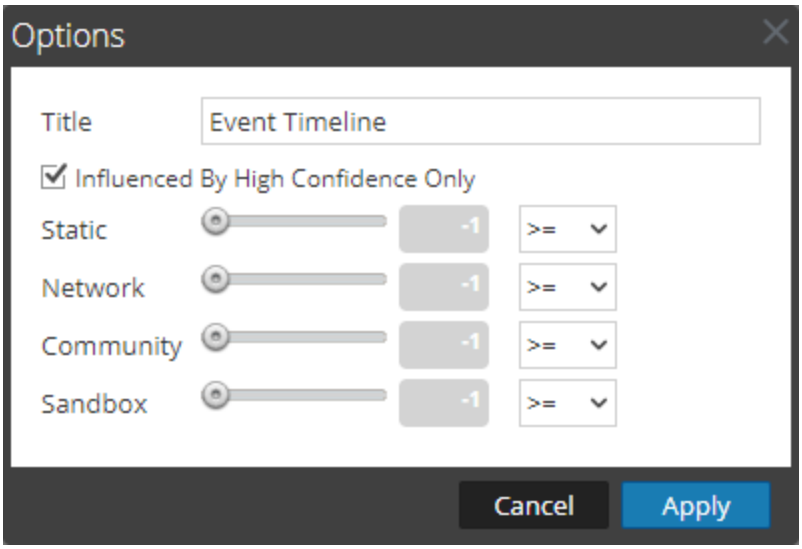
1. Wählen Sie in der Symbolleiste > **Schwellenwertfilter anwenden** aus.
   Das Dialogfeld „Schwellenwertfilter anwenden“ wird angezeigt.



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.

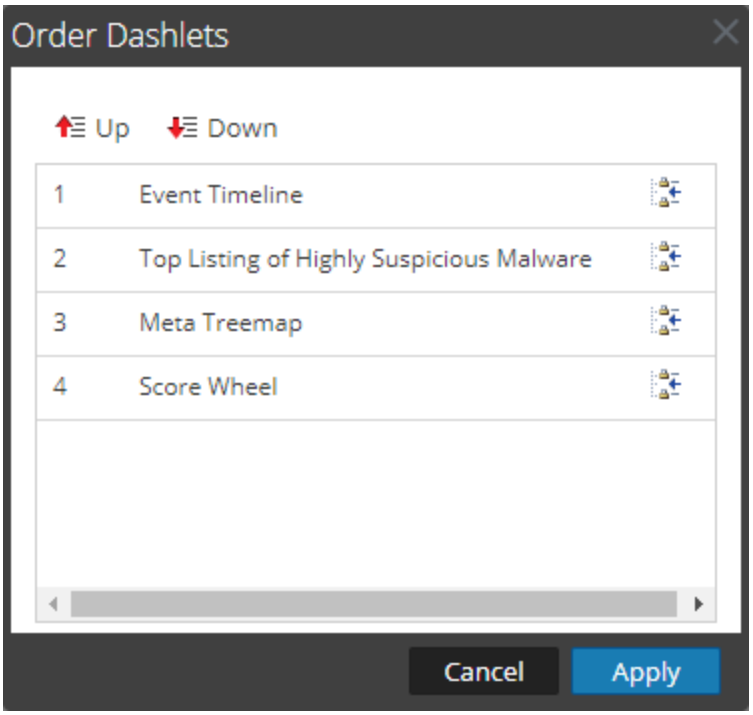


2. Geben Sie einen neuen Titel für das Dashlet in das Feld **Titel** ein.
3. Wenn Sie nur Ereignisse sehen möchten, die von dem Tag Hohe Wahrscheinlichkeit beeinflusst sind, was bedeutet, dass eine hohe Wahrscheinlichkeit besteht, dass das Ereignis gefährlichen Code enthält, aktivieren Sie die Optionen **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.

Konfigurieren von Navigationsansicht und Ereignisansicht

Analysten können Einstellungen festlegen, die die Performance und das Verhalten von NetWitness Suite beim Analysieren von Daten in den Ansichten „Investigate > Navigation“ und „Investigate > Ereignisse“ beeinflussen.

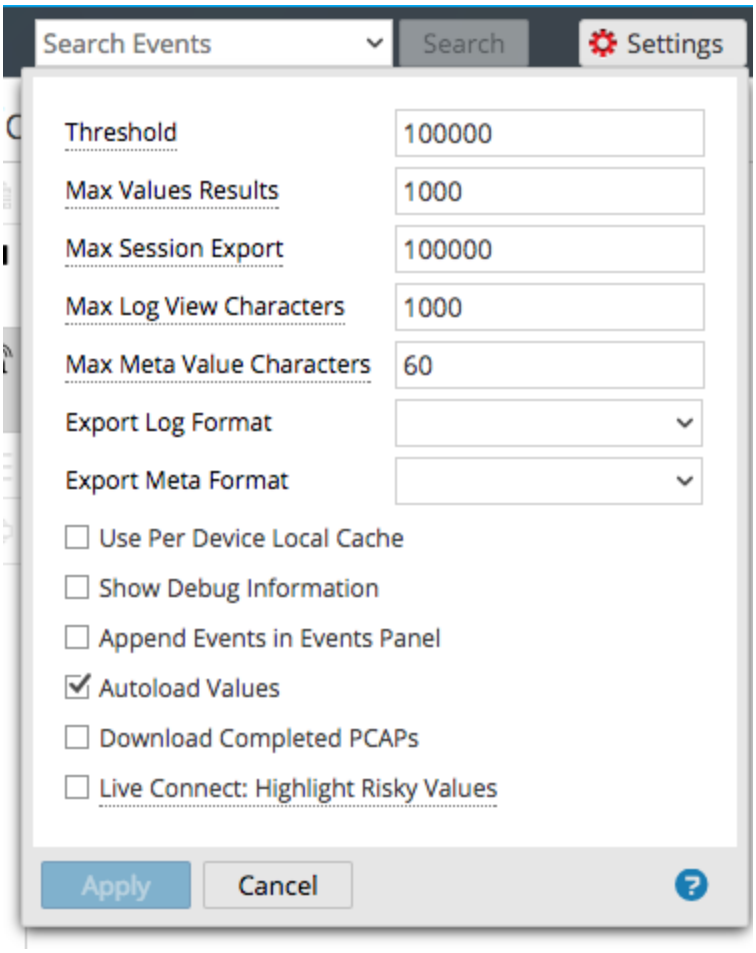
Diese Einstellungen sind an zwei Stellen in NetWitness Suite verfügbar. Änderungen, die an der einen Stelle vorgenommen werden, werden auch in der anderen Ansicht angewendet:

- Ansicht „Untersuchen“ > Dialogfeld „Einstellungen“ und Suchfeld der Ansichten „Navigation“ und „Ereignisse“.
- Registerkarte „Profile“ > Bereich „Einstellungen“ > „Investigation“

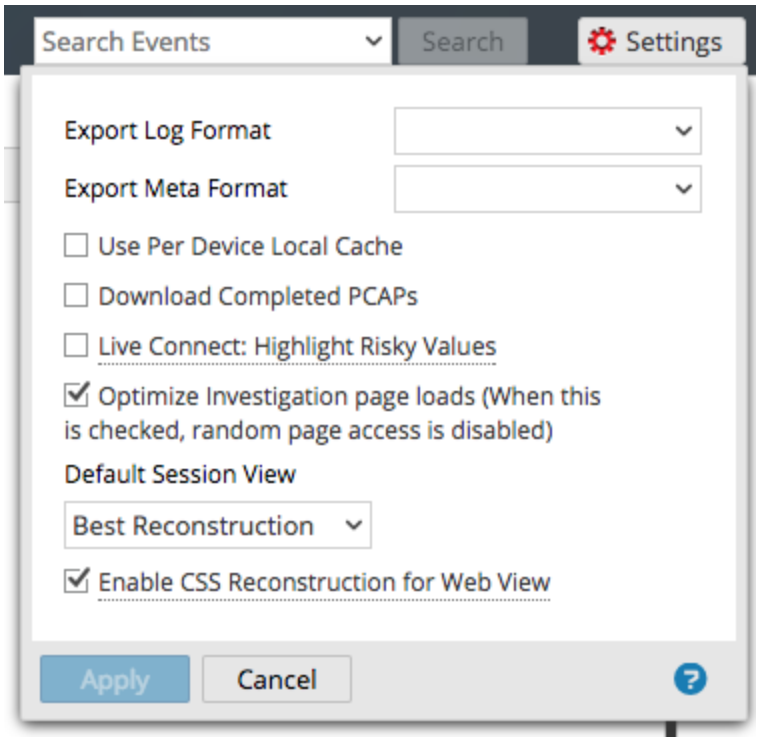
Zugriff auf die Investigation-Einstellungen

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.

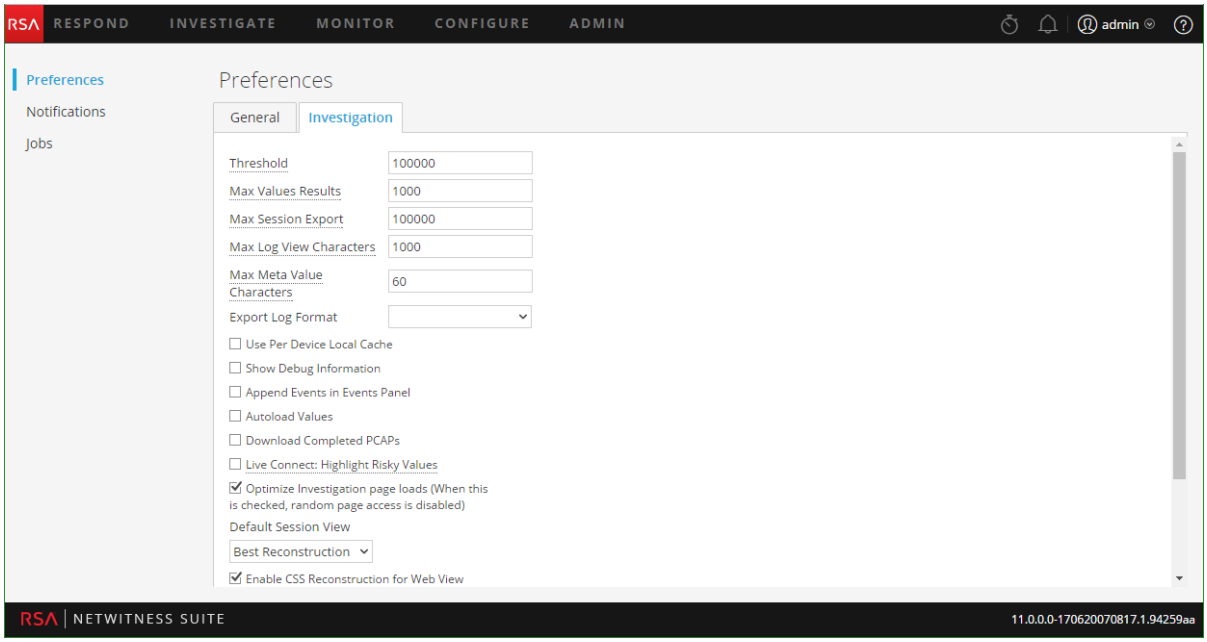


- Wählen Sie in der Symbolleiste der Ansicht **Ereignisse** die Option **Einstellungen** aus.
  Das Dialogfeld „Einstellungen“ der Ansicht „Ereignisse“ wird angezeigt.



- Wählen Sie in der oberen rechten Ecke von NetWitness Suite die Option **Profil** aus dem Drop-Down-Menü „Benutzer“ und klicken Sie auf **Voreinstellungen**. Klicken Sie auf die Registerkarte **Investigation**.

  Die Registerkarte „Investigation“ wird angezeigt.



Kalibrieren der Werte der Ladeparameter in der Ansicht „Navigation“

Verschiedene Investigation-Einstellungen beeinflussen die Performance von NetWitness Suite 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 **Investigation** oder zum Dialogfeld **Einstellungen** der Ansicht „Navigieren“.
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 **Investigation > Ereignisse > Protokolltext** angezeigt werden sollen. Der Standardwert ist **1000**.
- Debuginformationen anzeigen: Wenn Sie möchten, dass NetWitness Suite 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**.
- Werte automatisch laden: Wenn Sie möchten, dass NetWitness Suite automatisch Werte für den ausgewählten Service in der Navigationsansicht lädt, aktivieren Sie diese Option. Wurde diese Option nicht ausgewählt, zeigt NetWitness Suite die Schaltfläche **Werte laden** an, über die Sie die Optionen ändern können. Der Standardwert ist **Aus**.
- Live Connect: Riskante IPs markieren: Wenn Sie möchten, dass NetWitness Suite 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 Suite alle IP-Adressen an. Diese Option ist standardmäßig deaktiviert (**Aus**).

3. Klicken Sie auf **Anwenden**.

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

Konfigurieren des PCAP-Downloadverhaltens in Investigation

Sie können den Download extrahierter PCAPs im Modul Investigation automatisieren, damit der Browser die extrahierten PCAPs herunterlädt und in der Standardanwendung zum Öffnen von PCAP-Dateien, beispielsweise Wireshark, öffnet.

So konfigurieren Sie dies:

1. Stellen Sie sicher, dass eine Anwendung zum Öffnen von PCAP-Dateien auf Ihrem lokalen Dateisystem installiert ist und dass die Anwendung als Standardanwendung für PCAP-Dateiformate konfiguriert ist.
2. Navigieren Sie zur Registerkarte **Investigation** oder zum Dialogfeld **Einstellungen** der Ansicht „Navigieren“ oder der Ansicht „Ereignisse“.
3. Aktivieren Sie die Option **Abgeschlossene PCAPs herunterladen**.
4. Klicken Sie auf **Anwenden**.
   Die Einstellung wird sofort wirksam.

Konfigurieren des Standard-Exportprotokollformats in Investigation

Sie können Protokolle aus Investigation in unterschiedliche Formate exportieren. Die verfügbaren Optionen sind: Text, XML, CSV, JSON. Es gibt keinen integrierten Standardwert für das Protokollexportformat. Wenn Sie hier kein Format auswählen, zeigt NetWitness Suite ein Auswahldialogfenster an, wenn Sie einen Protokollexport aufrufen.

So wählen Sie das Format der exportierten Protokolle aus:

1. Navigieren Sie zur Registerkarte **Investigation** oder zum Dialogfeld **Einstellungen** der Ansicht „Navigieren“.
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 in Investigation

Sie können Metawerte aus Investigation in unterschiedliche Formate exportieren. Die verfügbaren Optionen sind: Text, XML, CSV, JSON. Es gibt keinen integrierten Standardwert für das Metaexportformat. Wenn Sie hier kein Format auswählen, zeigt NetWitness Suite ein Auswahldialogfeld an, wenn Sie einen Export von Metawerten aufrufen.

So wählen Sie das Format der exportierten Metawerte aus:

1. Navigieren Sie zur Registerkarte **Investigation** oder zum Dialogfeld **Einstellungen** der Ansicht „Navigieren“.
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 Suite Ereignisse abruft und in der Ansicht „Ereignisse“ rekonstruiert. Gehen Sie wie folgt vor:

1. Navigieren Sie zur Registerkarte **Investigation** 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 bestimmte Seite der Ereignisliste zu wechseln. Durch die Deaktivierung dieses Kontrollkästchens wird die Paginierung der Liste „Ereignisse“ geändert, damit Sie auf eine bestimmte Seite in der Liste (oder auf die letzte Seite) springen können. Der Standardwert ist **aktiviert**.
- **Ereignisse in Ereignisbereich anhängen**: Wenn diese Option ausgewählt ist, werden die Ereignisse, die im **Bereich „Ereignisse“** angezeigt werden, inkrementell hinzugefügt. Beispielsweise wird bei jedem Klicken auf das Symbol für die nächste Seite das nächste Inkrement der Ereignisse hinzugefügt. Zuerst werden 1 bis 25 angezeigt, dann 1 bis 50, dann 1 bis 75 und so weiter. Diese Option ist nur verfügbar, wenn die Option „Optimieren des Ladens der Seite Investigation“ aktiviert ist.
- **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. 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 (Cascaded Style-Sheet) 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.

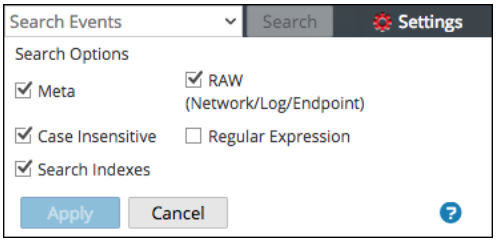
Hinweis: Die Darstellung des rekonstruierten Inhalts stimmt eventuell nicht genau mit der ursprünglichen Webseite überein, wenn die entsprechenden Bilder und Formatvorlagen nicht gefunden werden oder aus dem Cache des Webbrowsers geladen wurden. Zudem werden Layouts oder Formate, die dynamisch über das 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. Navigieren Sie zur Registerkarte **Investigation**.
2. Klicken Sie auf 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.

(Optional) Konfigurieren von Suchoptionen

1. Klicken Sie in das Feld **Suche**, um das Drop-down-Menü „Ereignisse suchen“ anzuzeigen.



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

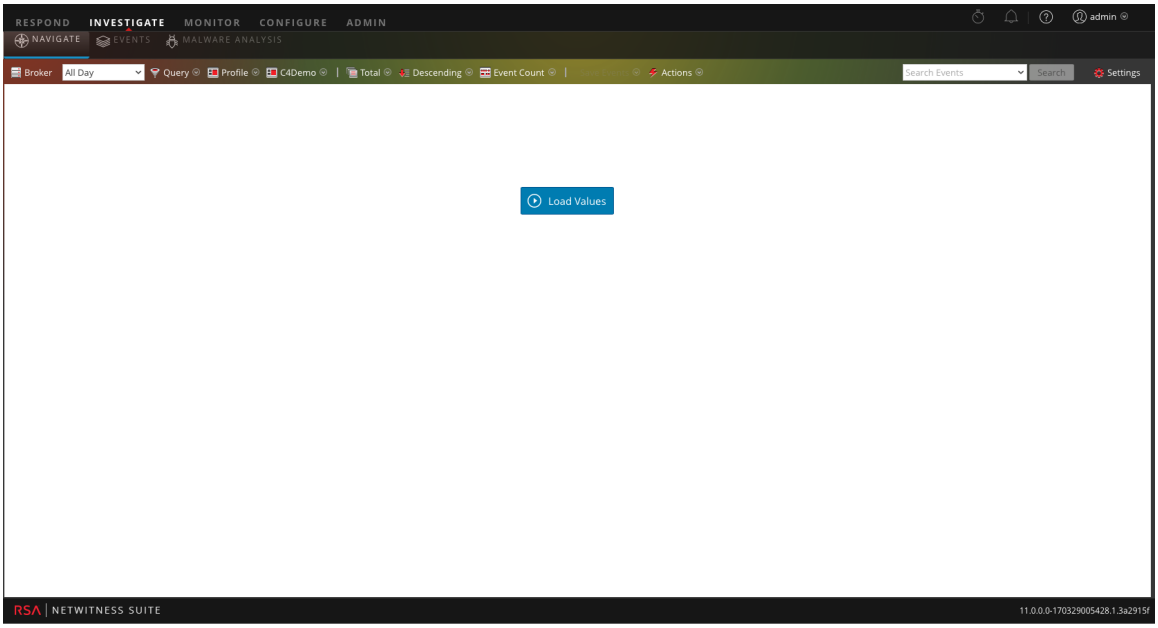
Durchführen einer Ermittlung

Sie können auf verschiedene Weise eine Ermittlung in NetWitness Suite beginnen. Angaben zum detaillierten Verfahren finden Sie unter Starten einer Untersuchung für einen Service oder eine Sammlung. Wenn Sie eine Ermittlung beginnen, gibt es keine bestimmte Reihenfolge, in der die Ermittlung durchzuführen ist. Stattdessen bietet NetWitness Suite verschiedene Methoden für das Anzeigen, Filtern und Abfragen der Daten, für Aktionen zu einem Drill-down-Punkt und das Untersuchen bestimmter Ereignisse.

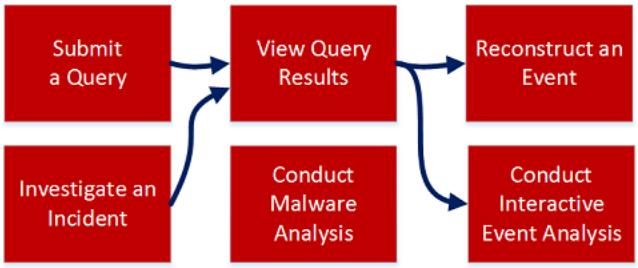
Für Analysten, die NetWitness Suite Investigation verwenden, müssen die entsprechenden Systemrollen und Berechtigungen in den Benutzerkonten eingerichtet werden. Siehe Rollen und Berechtigungen für Malware-Analysten.. Ein Administrator muss die Rollen und Berechtigungen konfigurieren.

Hinweis: Wenn Sie einen Service der Version 10.6 von einem NetWitness-Server der Version 11.0 aus untersuchen, variiert das Downloadverhalten für Dateien, PCAP-Dateien, Protokolle, Nutzlasten und Metawerte. Möglicherweise wird eine Ereignisnutzlast in einem 10.6-Service angezeigt, für den Sie keine Berechtigung haben, aber Sie werden nicht in der Lage sein, Dateien oder Nutzlasten herunterzuladen.

Um eine Ermittlung durchzuführen, melden Sie sich bei NetWitness Suite an und wechseln Sie zu Ermittlung. Die Ansicht „Untersuchen“ wird mit den Feldern geöffnet, in denen Sie Service, Zeitraum und eine optionale Abfrage für bestimmte Metadaten auswählen. Wählen Sie einen Service aus und klicken Sie auf **LoadValues**.



Dies sind die grundlegenden Schritte für die Durchführung von Ermittlungen.



1. Von einer Respond-Entität aus können Sie eine Abfrage senden oder zu Ermittlung wechseln (siehe Starten einer Untersuchung für einen Service oder eine Sammlung).
2. Abfrageergebnisse können Sie in der Ansicht „Navigation“ (siehe Einschränken der in der Ansicht „Navigation“ angezeigten Ergebnisse) und der Ansicht „Ereignisse“ (siehe Untersuchen von Ereignissen) anzeigen.
3. Rekonstruieren Sie ein Ereignis (siehe Rekonstruieren eines Ereignisses) oder zeigen Sie die interaktive Ereignisanalyse eines Ereignisses an (siehe Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“).
4. Reagieren Sie auf einen Drill-down-Punkt oder ein Ereignis (siehe Aktionen zu Drill-down-Punkten in der Ansicht „Navigation“ und Untersuchen von Ereignissen). Möglich ist beispielsweise das Anzeigen von zusätzlichem Kontext für einen Datenpunkt, Starten eines Schadsoftwareanalyse-Scans in der Navigationsansicht oder Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion.

Starten einer Untersuchung für einen Service oder eine Sammlung

Analysten können eine Untersuchung von Daten für NetWitness Suite-Services oder -Sammlungen beginnen, die das Laden von Werten zur Folge hat.

Hinweis: Spezifische Benutzerrollen und -berechtigungen werden von einem Benutzer benötigt, damit dieser Untersuchungen in NetWitness Suite vornehmen 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.

Um eine Ermittlung in NetWitness Suite zu starten, muss ein Service angegeben werden.

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

Hinweis: Der Archiver-Service wird nicht in der Ansicht „Navigation“ angezeigt, damit Benutzer während einer Untersuchung keine Beeinträchtigung der Leistung erfahren. Der Archiver ist in der Ansicht „Ereignisse“ zum Exportieren von Protokollen und für erweiterte Suchfunktionen verfügbar.

Sobald ein Service oder eine Sammlung ausgewählt wurde, ist NetWitness Suite bereit, Daten für den Service oder die Sammlung zu laden. Mehrere Einstellungen im Dialogfeld „Einstellungen“ der Ansichten „Navigieren“ und „Ereignisse“ oder auf der Registerkarte „Profile“ > Bereich „Einstellungen“ > „Untersuchungen“ wirken sich auf den Ladevorgang aus: „Schwellenwert“, „Max. Wertergebnisse“, „Debuginformationen anzeigen“, „Werte automatisch laden“ und „Optimieren des Ladens der Seite »Untersuchen«“ (siehe Konfigurieren von Ermittlungsansichten und -einstellungen).

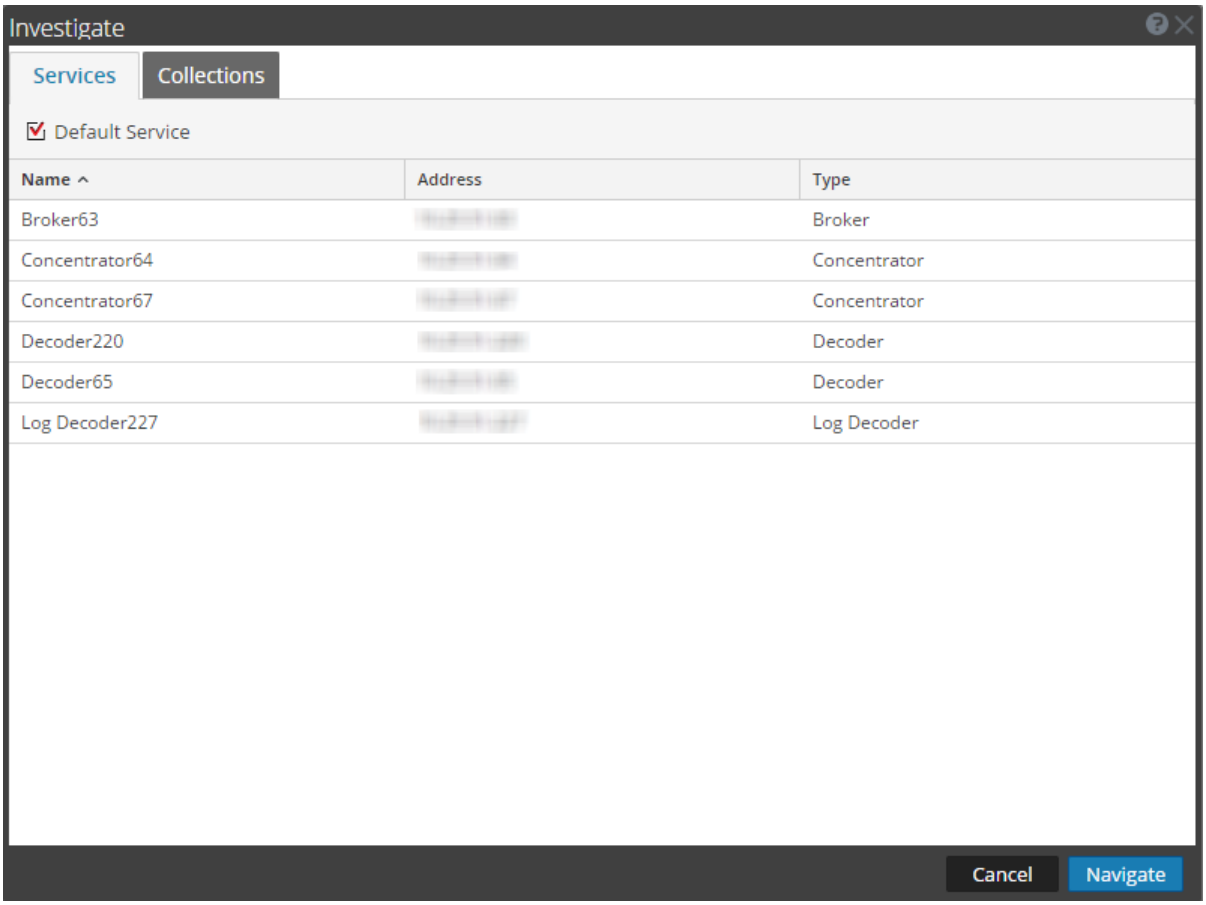
Hinweis: Wenn Sie „Werte automatisch laden“ angegeben haben, aktualisiert NetWitness Suite die Daten automatisch. Andernfalls müssen Sie auf die Schaltfläche „Werte laden“ klicken. NetWitness Suite aktualisiert die Metadaten im Bereich „Werte“ in der Ansicht „Navigation“ und die Ergebnisse werden sofort 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 Untersuchung zu einer Sammlung durchführen.

Beginnen einer Untersuchung in der Ansicht „Navigation“ (ohne Standardservice)

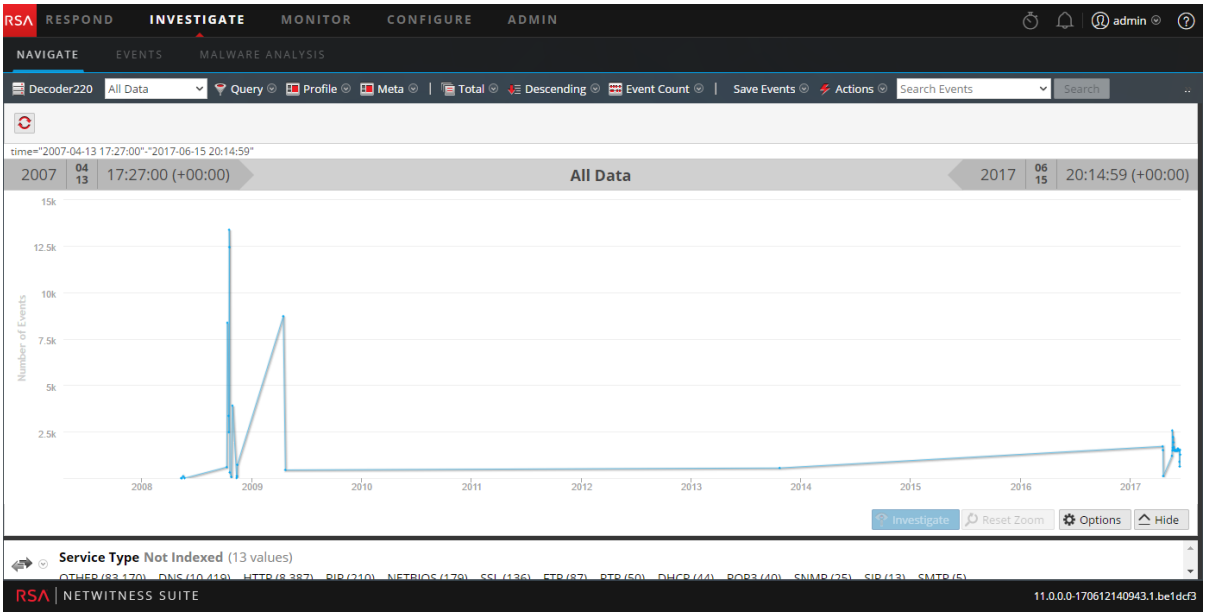
1. Wechseln Sie zu **UNTERSUCHEN > Navigation**.
   Das Dialogfeld „Untersuchen“ wird angezeigt.



2. Doppelklicken Sie auf einen Service oder wählen Sie einen Service, in der Regel einen Concentrator, aus und klicken Sie auf **Navigation**.
   Der daraufhin angezeigte Bereich enthält die Aktivität für den ausgewählten Service.
3. 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

Einschränken der in der Ansicht „Navigation“ angezeigten Ergebnisse beschrieben. Sie können während der Untersuchung auch jederzeit Optionen ändern.

4. Wenn Sie fertig sind, klicken Sie auf Load Values.
   Der Vorgang zum Laden der Daten des ausgewählten Service beginnt.

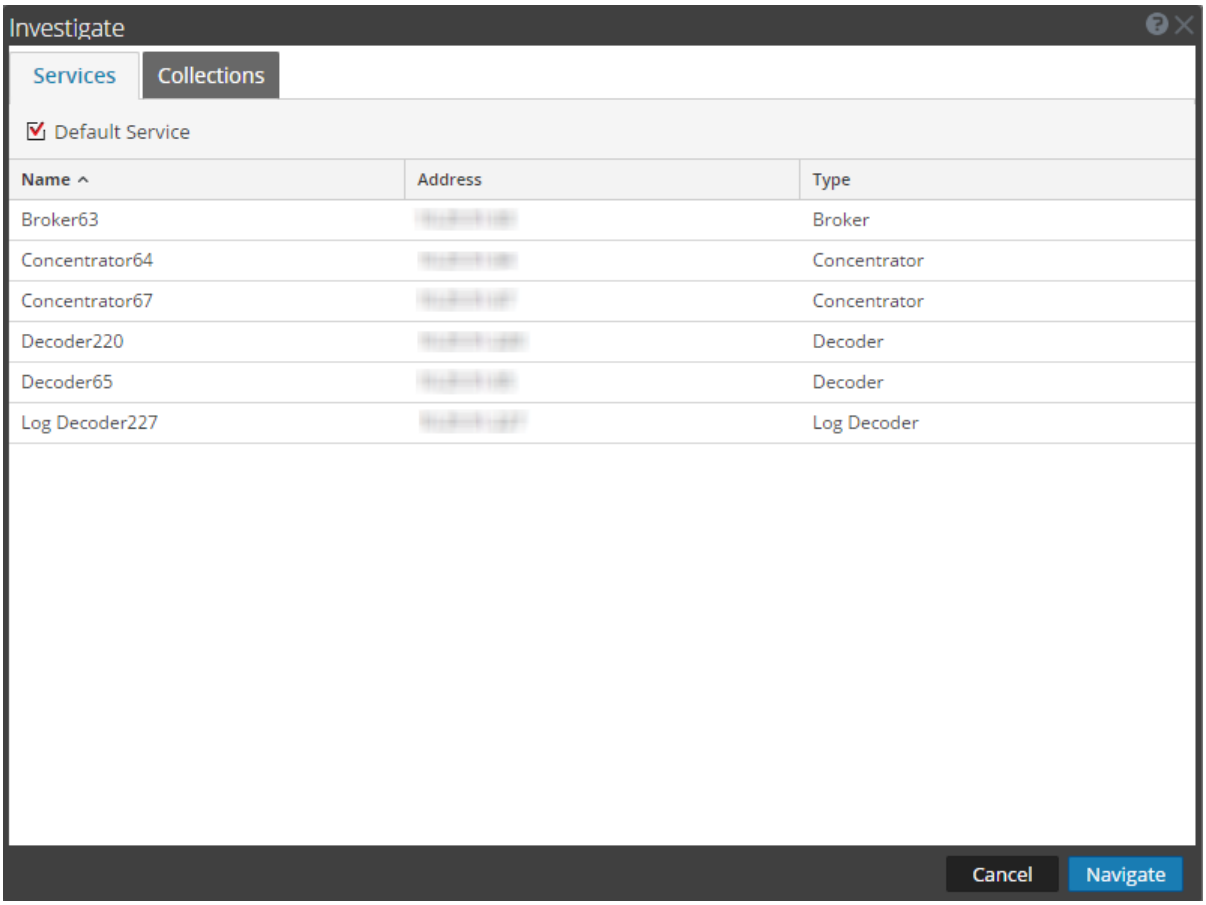


   Wenn der Service ausgewählt ist und die Daten geladen sind, können Sie mit dem Analysieren der Daten beginnen.

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.



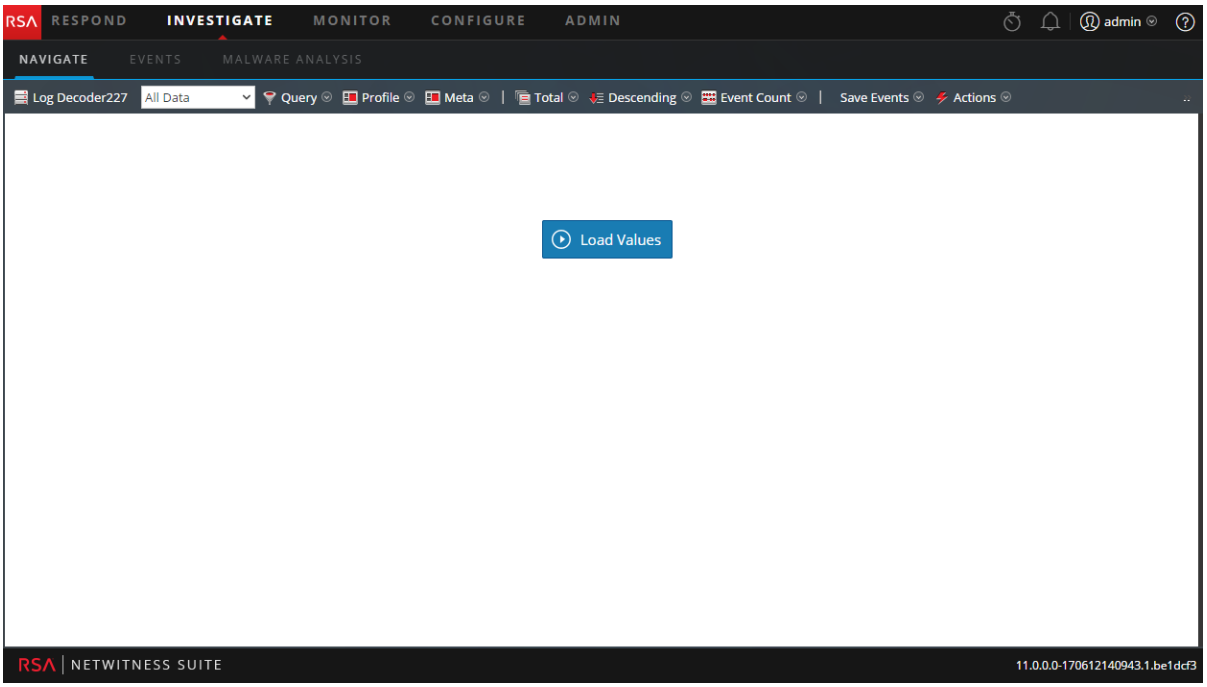
2. Wählen Sie im Raster **Services** einen Service aus und klicken Sie auf Default Service. Der Service wird als Standard eingestellt (angezeigt durch **Standard** in Klammern hinter dem Servicenamen).

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.

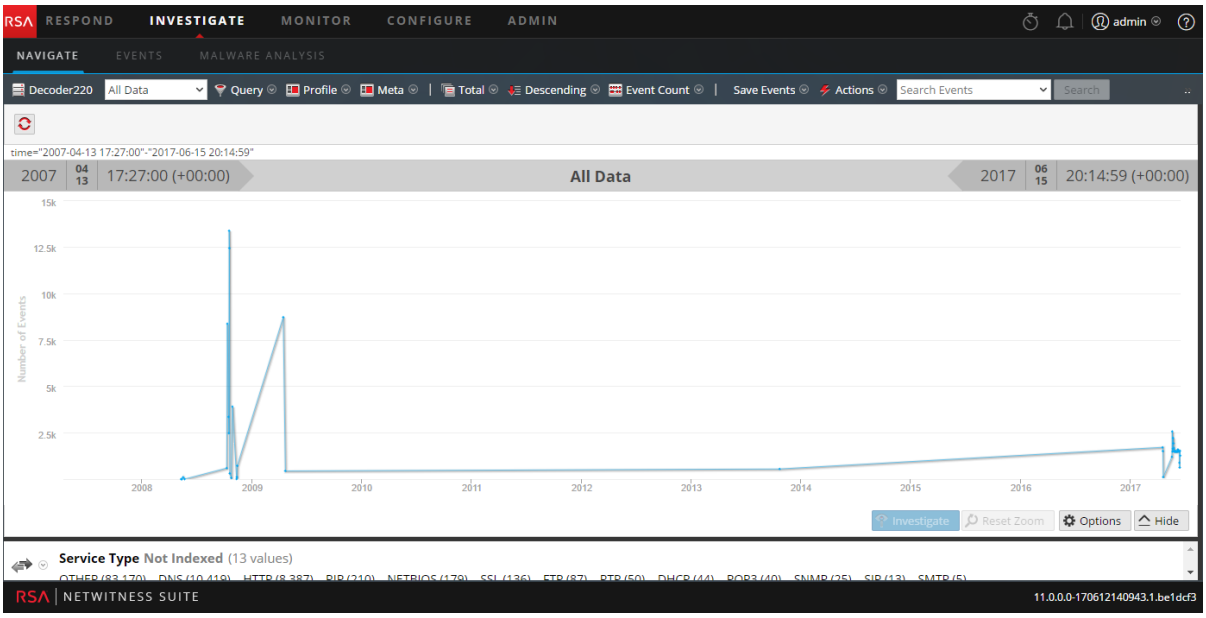
   Hinweis: Durch die Schaltfläche „Abbrechen“ wird die Auswahl des Standardservice nicht aufgehoben. Es wird lediglich das Dialogfeld geschlossen, ohne im Raster zum aktuell ausgewählten Service zu navigieren. Durch das Einrichten eines Standardservices, der sich vom aktuell einer Ermittlung unterzogenen 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 > Navigation**.
   Wenn die Einstellung „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.



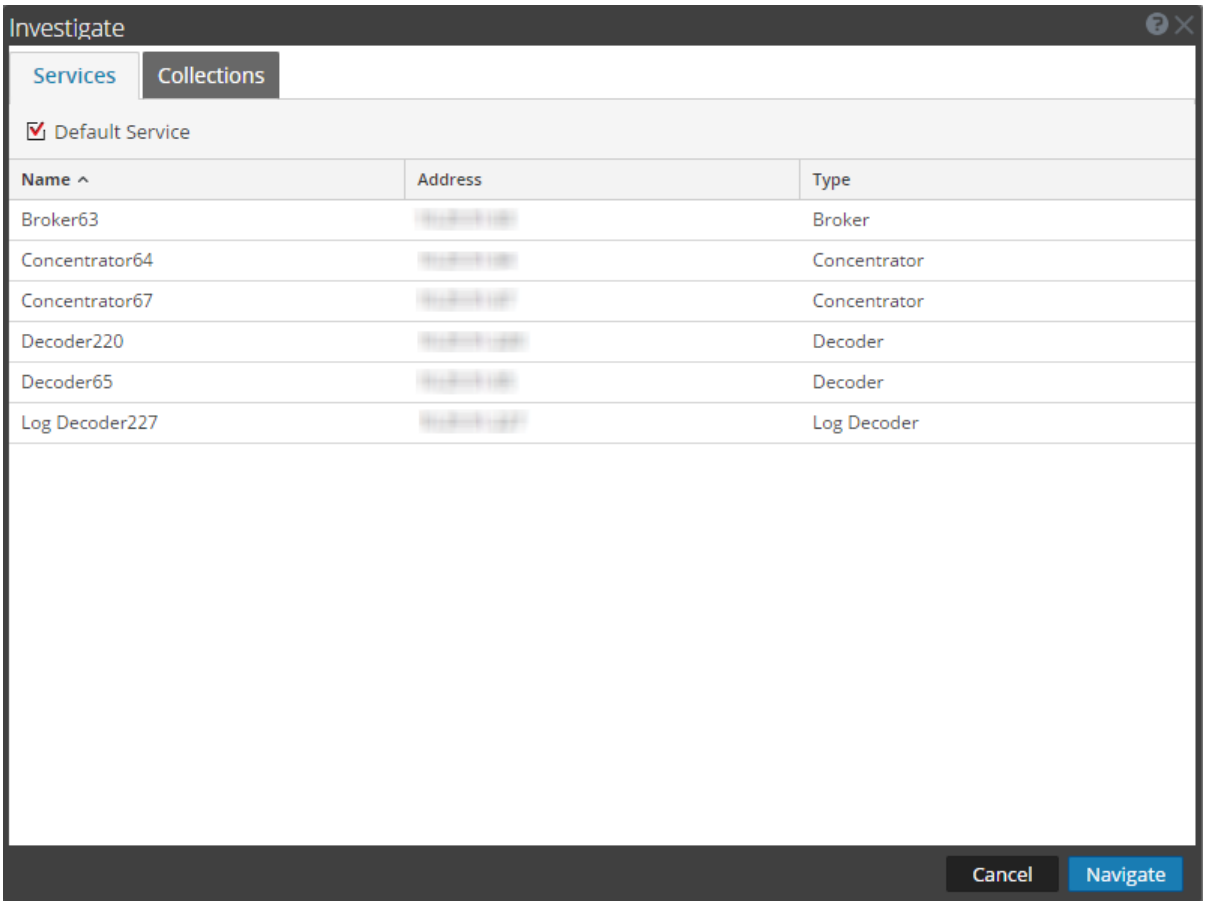
2. Wenn Sie die Ermittlungsoptionen vor dem Laden ändern möchten, können Sie z. B. ein benutzerdefiniertes Profil erstellen oder ändern, einen anderen Zeitraum anwenden, eine Metagruppe erstellen oder anwenden und eine benutzerdefinierte Abfrage ausführen.
3. Wenn Sie fertig sind, klicken Sie auf Load 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.

Ändern des zu untersuchenden Services oder der Sammlung

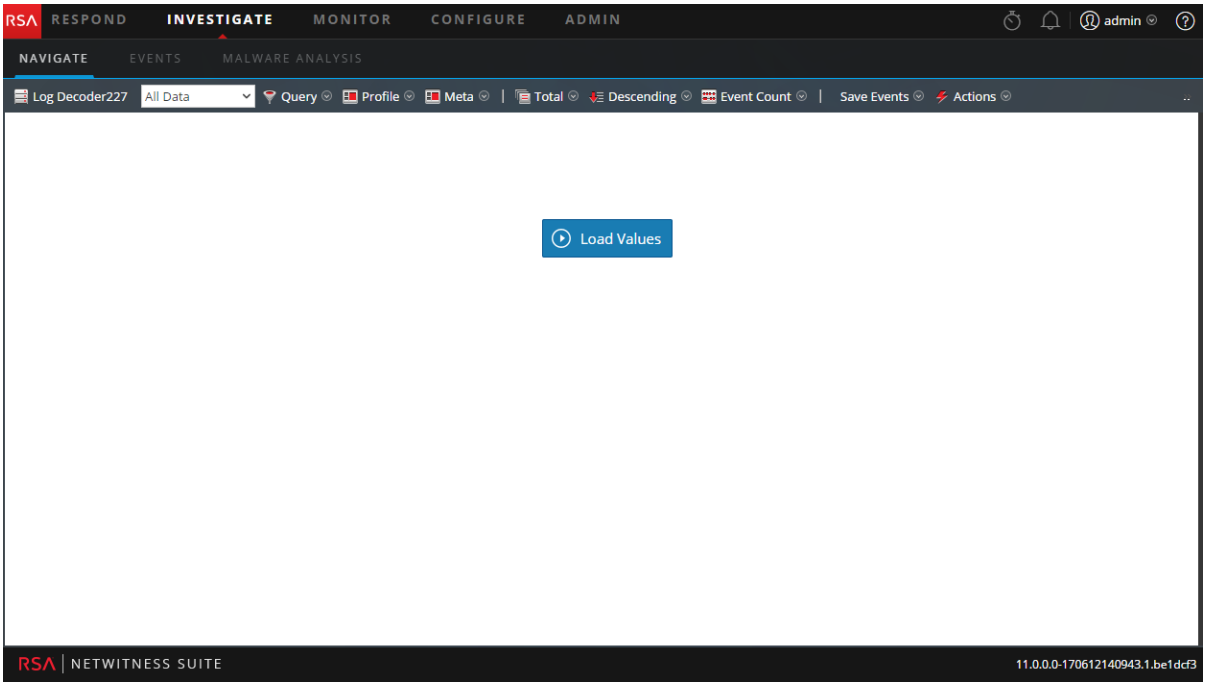
1. Klicken Sie in der Ansicht „Navigation“ auf den Servicenamen ganz oben im Bereich „Optionen“.
   Das Dialogfeld „Untersuchen“ wird angezeigt.



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.



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.

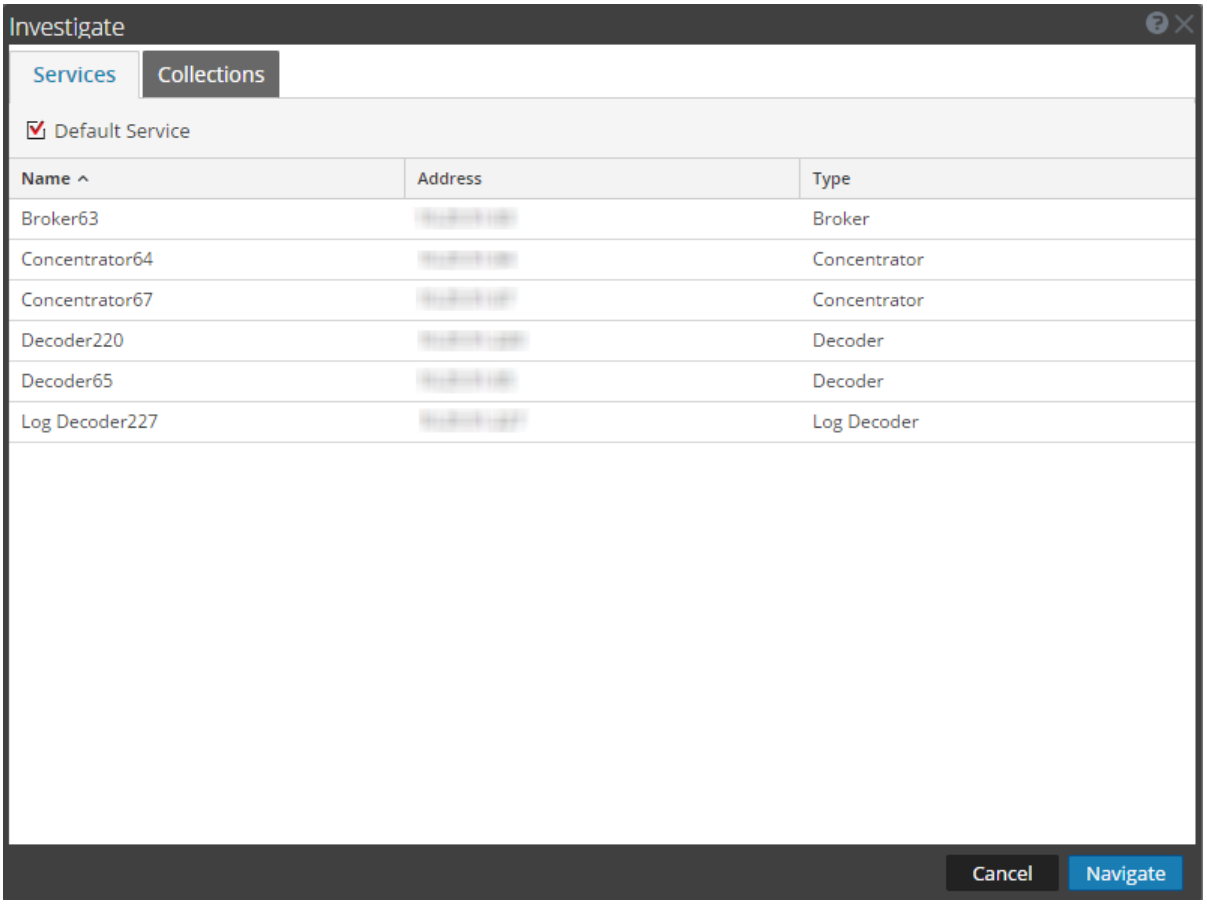
Untersuchen von Workbench-Wiederherstellungssammlungen

Dieses Verfahren ermöglicht Administratoren das Auswählen von Inhalten aus einer bestehenden Sammlung zur erneuten Verarbeitung für eine tiefergehende Untersuchung. 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 > Navigation**.
   Das Dialogfeld „Untersuchen“ wird angezeigt.



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

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

Einschränken der in der Ansicht „Navigation“ angezeigten Ergebnisse

Im Zuge von Ermittlungen in NetWitness Suite können die angezeigten Ergebnisse beim Laden von Metaschlüsselwerten in der Ansicht „Navigieren“ mithilfe von mehreren Methoden verfeinert werden. Analysten können:

- Einstellen des Zeitbereichs für eine Ermittlung (Ansicht „Navigation“ oder Ansicht „Ereignisse“)
- Einstellen der Quantifizierungsmethode und Sortierreihenfolge von Metaschlüsselergebnissen (Ansicht „Navigation“)
- Verwalten und Anwenden von Standardmetaschlüsseln in einer Ermittlung (Ansicht „Navigation“)
- Metagruppen managen (Ansicht„Navigation“)
- Visualisieren von Metadaten als Parallelkoordinaten(Ansicht „Navigation“)
- Einkapseln von benutzerdefinierten Ansichten mithilfe von Ermittlungsprofilen (Ansicht „Navigation“ und Ansicht „Ereignisse“)

Metagruppen managen

Eine Metagruppe kombiniert ausgewählte Metaschlüssel in einer Gruppe, um nur Daten anzuzeigen, in denen die Metaschlüssel gefunden wurden. In der Ansicht „Untersuchen > Navigation“ können Metagruppen zum Filtern der in einer Ermittlung angezeigten Daten verwendet werden. Eine Neuinstallation von NetWitness Suite umfasst Out-of-the-Box(OOTB)-Metagruppen, die RSA-Inhaltsentwickler entwickelt haben, damit Sie interessante Datasets in Ermittlung finden können. Zur Identifizierung wird den OOTB-Metagruppen, die dupliziert, aber nicht bearbeitet oder 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 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 hinzufügen, indem sie die benutzerdefinierte Indexdatei eines Service bearbeiten, sind die neuen Gruppen für Investigation verfügbar, nachdem der Service von Neuem 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

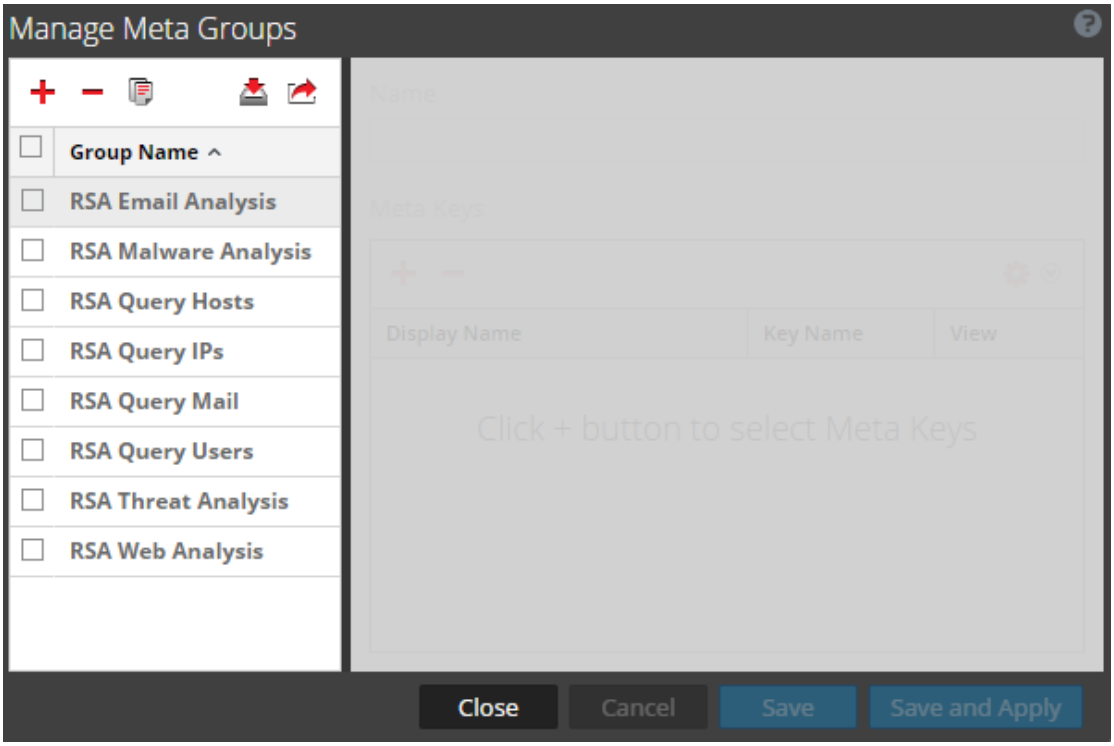
Die OOTB-Metagruppen sind in die RSA NetWitness Suite integriert. Die Standard-Metagruppen sind nützlich, um den Fokus einer Ermittlung auf typische Anwendungsbeispiele zu setzen und die Bedrohungserkennung anhand des RSA Hunting Pack zu unterstützen.

Dies sind die OOTB-Metagruppen:

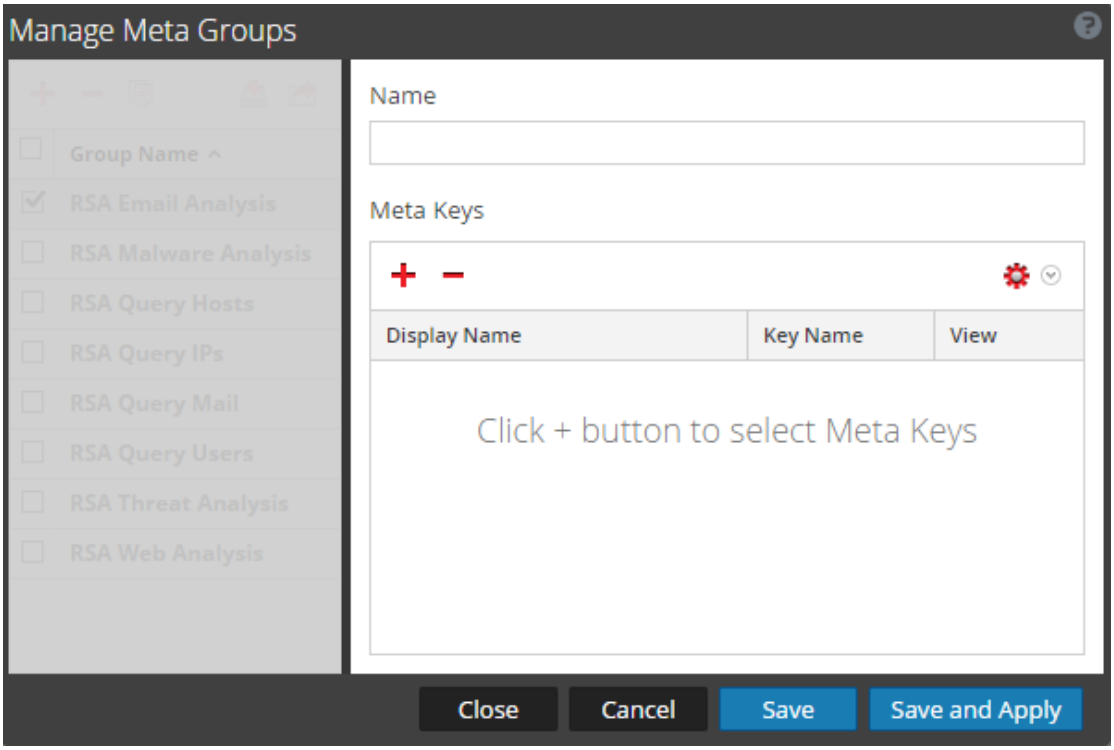
- RSA-E-Mail-Analyse umfasst Metaschlüssel, die E-Mail-Aktivitäten beschreiben.
- RSA-Endpunktanalyse enthält Metaschlüssel, die einen Einblick in die Prozesse, die Dateien, die Benutzer und die Verbindungen von NetWitness Endpoint-Hosts (NWE) bieten.
- RSA Malware Analysis umfasst Metaschlüssel, die 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-Webanalyse umfasst Metaschlüssel, die Anomalien im Webdatenverkehr markieren.

Erstellen von Metagruppen und Hinzufügen von Metaschlüsseln

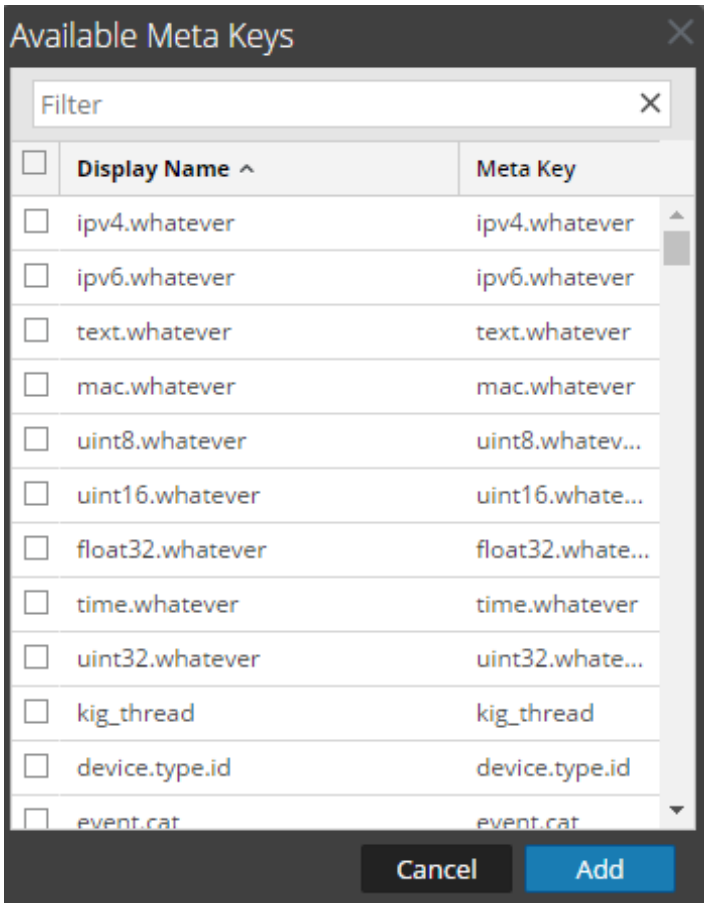
1. Wenn Sie einen Service in der Ansicht **Untersuchen > Navigation** untersuchen möchten, wählen Sie in der Symbolleiste **Metadaten > Metagruppen managen** aus.
   Das Dialogfeld „Metagruppen managen“ wird angezeigt. Zu Beginn sind nur OOTB-Gruppen für einen Service konfiguriert und unter „Gruppenname“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



2. Klicken Sie in der Rastersymbolleiste auf +.
   Oben im Raster „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.

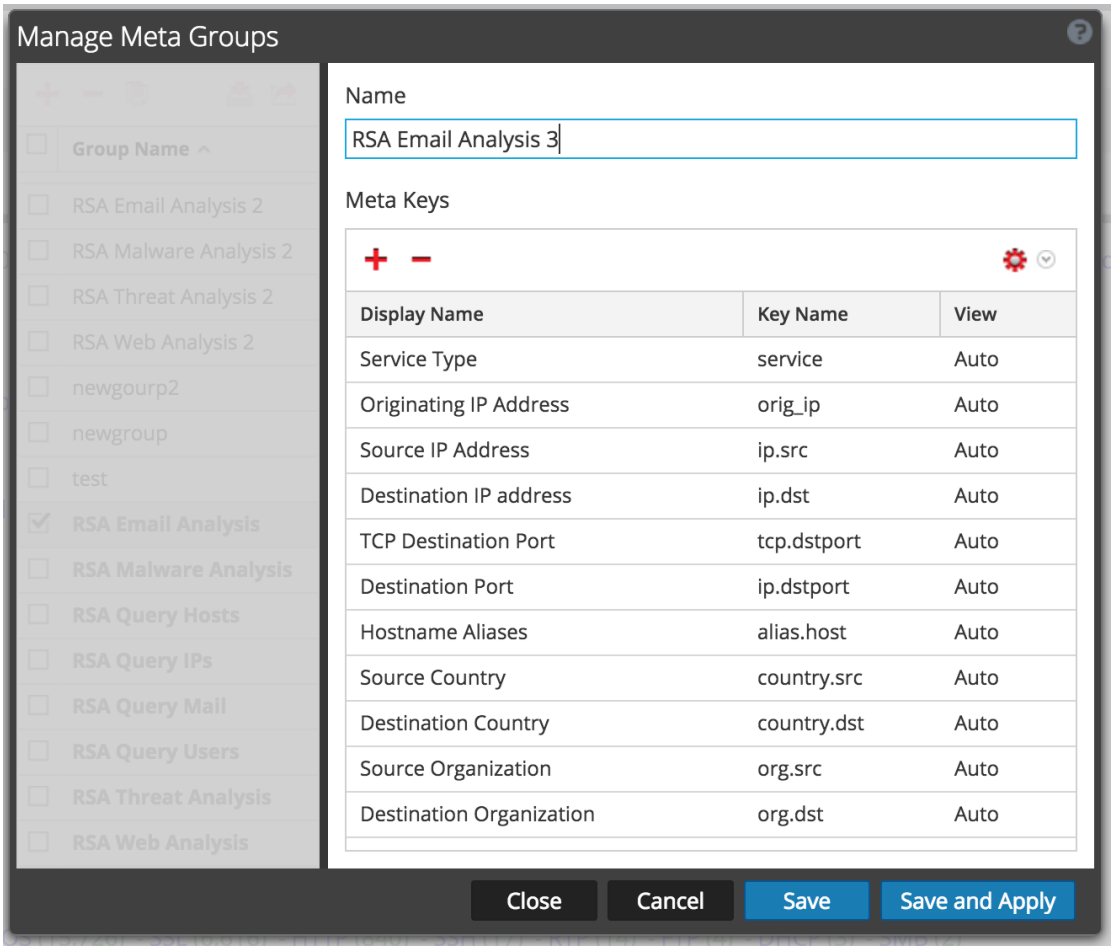
10. Klicken Sie auf **Schließen**.

Duplizieren und Bearbeiten einer Out-of-the-Box-Metagruppe

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

1. Wählen Sie eine OOTB-Metagruppe aus dem Raster „Metagruppen“ aus und klicken Sie auf .

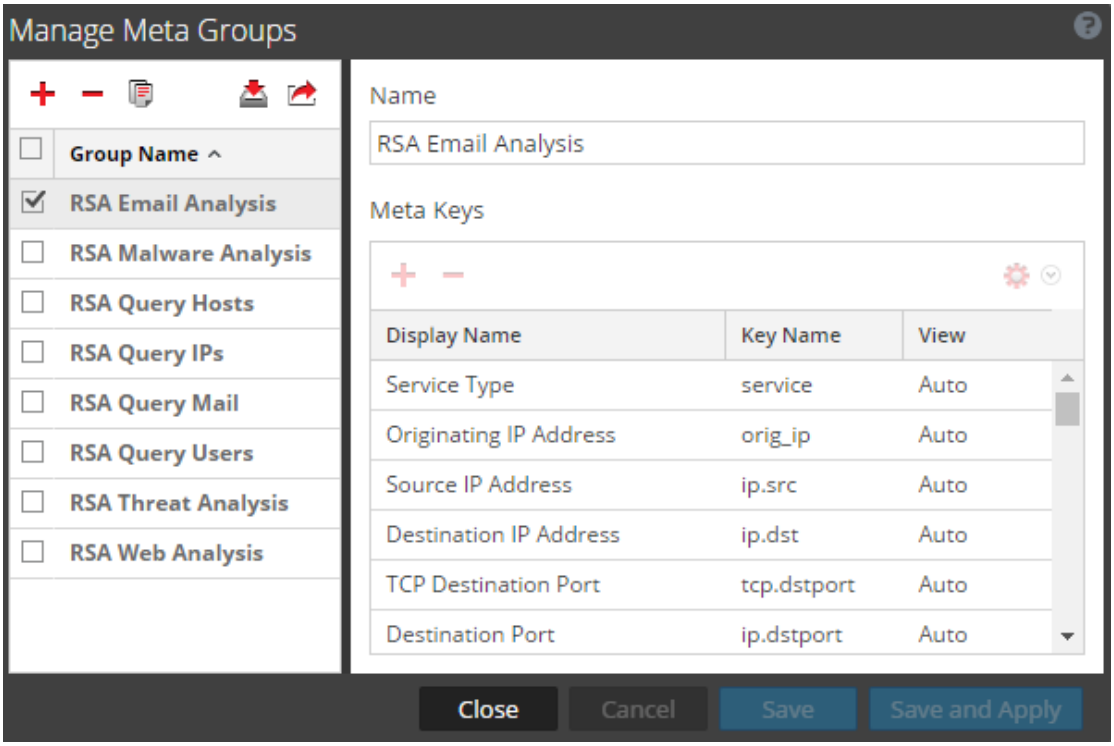
   Das Formular rechts wird zur Bearbeitung geöffnet und enthält alle Metaschlüssel, da sie sich in der OOTB-Gruppe befinden.



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 im Raster **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. Um die Änderungen auf die aktuelle Navigationsansicht anzuwenden, klicken Sie auf **Speichern und übernehmen**.

Löschen von Metagruppen

1. Wählen Sie die zu entfernende Gruppe im Raster **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 im Raster **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 in NetWitness Suite zeigt NetWitness Suite eine Fehlermeldung an, wenn 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 im Raster **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 zum Raster 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.

Verwalten und Anwenden von Standardmetaschlüsseln in einer Ermittlung

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.

Wenn keine benutzerdefinierten Metagruppen aktiv sind, wird die Ansicht Navigieren mit der Metaschlüssel-Sichtbarkeit, die im Dialogfeld Standardmetaschlüssel angegeben ist, angezeigt. Um das Laden von Metaschlüsseln in der Ansicht „Navigation“ > Bereich „Werte“ zu optimieren, werden von NetWitness Suite nicht indizierte Metaschlüssel nicht standardmäßig geöffnet. Wenn Sie einen nicht indizierten Metaschlüssel in der Ansicht „Werte“ öffnen, beginnt NetWitness Suite, 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.

Um die anzuwendenden Metaschlüssel für Ihre Ermittlung auszuwählen, können Sie:

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

Hinweis: 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 auf diesem 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.

Standardmetaschlüssel verwenden

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

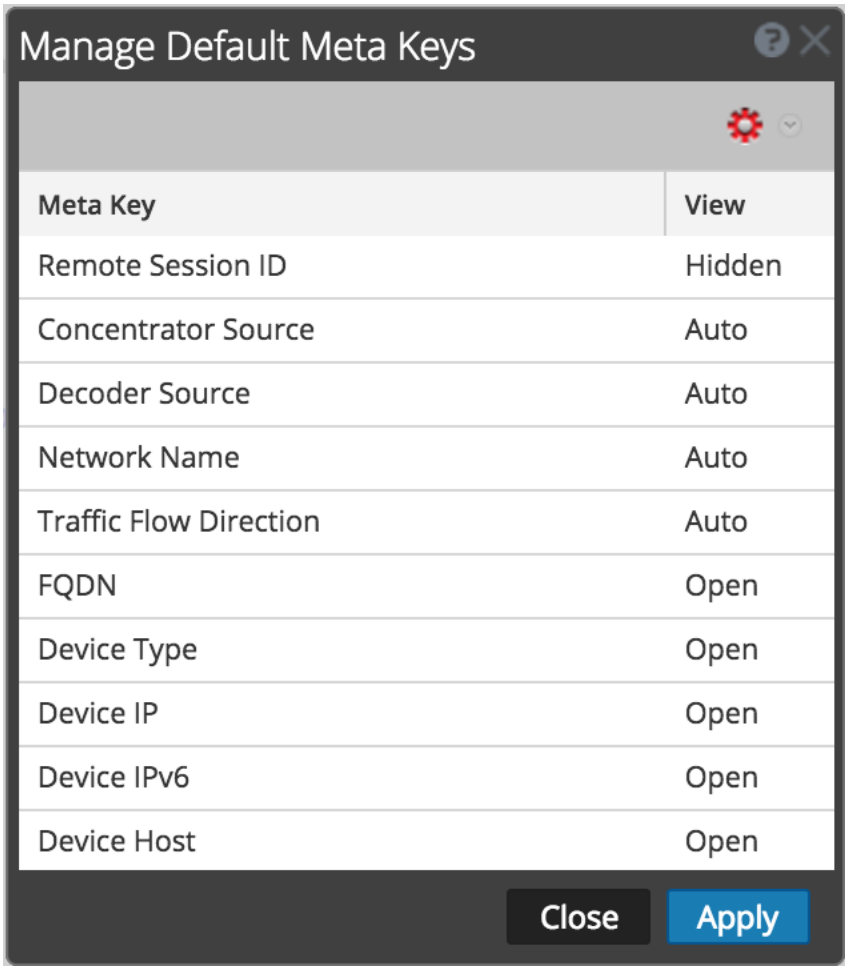
1. Navigieren Sie zu Ermittlung **> Navigation.**
2. Wählen Sie einen Service aus und wählen Sie dann **Navigieren** aus.

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.

Konfiguration von Standardmetaschlüsseln

So konfigurieren Sie die Standardansicht der Standardmetaschlüssel in der Ansicht „Investigation > Navigieren“:

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 Standardmetaschlüssel 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 standardgemäß geladen, Sie können aber einzelne Metaschlüssel in der Ansicht Navigieren manuell laden.

Suchen nach Textmustern in der Ansicht „Untersuchen“

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

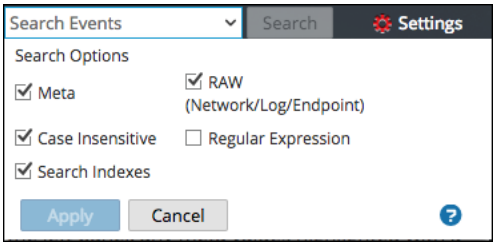
So greifen Sie auf das Suchfeld und die Suchoptionen in den Ansichten „Navigieren“ oder „Ereignisse“ zu.

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 diesem Feld ausgewählten Optionen ändern die Ausführung der Suche. Der Standardmodus für die Suche ist, die Suchindizes für Textschlüsselwörter in Meta- und Rohdaten zu verwenden.

Hinweis: Da das Kontrollkästchen „Suchindizes“ standardmäßig aktiviert ist, 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 „Suchindizes“. Die Suche dauert länger, gibt jedoch einen umfassenderen Satz von Daten zurück.

In der folgenden Tabelle werden die Investigation-Suchoptionen beschrieben.

Funktion	Beschreibung
Suchindizes	Durchsucht die Indizes zuerst, bevor die Metadaten oder Rohdaten durchsucht werden. 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:** – Die Indexsuche gibt nur Ergebnisse aus indizierten Daten zurück. – 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.
Meta	Durchsucht die Metadaten. Ihr Schlüsselwort oder Regex-Muster wird mit allen geparsten Metadaten verglichen.
RAW (Netzwerk/Protokoll/Endpunkt)	Durchsucht den Protokoll- oder Ereignistext. 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.
Groß-/Kleinschreibung ignorieren	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.

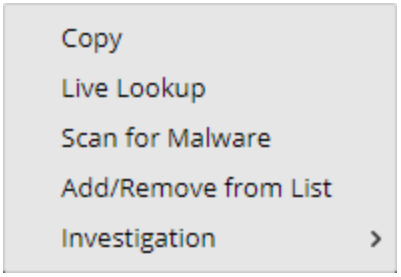
Suchbeispiele

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. Um einen Drill-down in die Daten durchzuführen, klicken Sie auf einen Metawert, z. B. HTTP, im Bereich „Navigation“.



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 „Ereignisses“ 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.

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 Ereignisansicht zurückzukehren, klicken Sie im Suchfeld auf das **X**.

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 „Ermittlung > Navigation“ in einer Reihenfolge sortiert werden.

Jeder Metaschlüsselabschnitt in der Ansicht „Ermittlung > 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 „Navigieren“.)

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**.

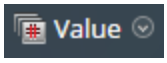
So wählen Sie die Quantifizierungsmethode für die Metaschlüsselanzahl und die Sortierung der Metaschlüsselergebnisse aus, die in der Ansicht „Navigieren“ angezeigt werden:

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.

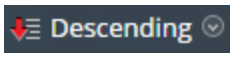
   Die aktuelle Ansicht wird gemäß Ihrer Auswahl erneut geladen.

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.

Einstellen des Zeitbereichs für eine Ermittlung

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

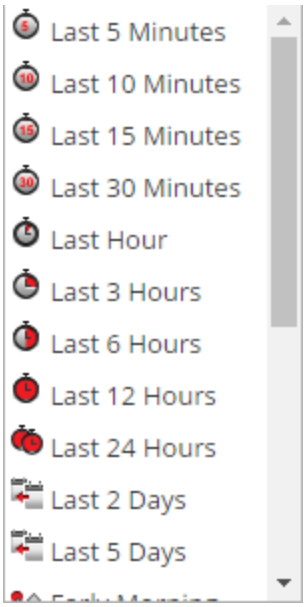
- Ein Zeitbereich relativ zur Sammlung. Zeitbereiche relativ zur Sammlung basieren auf dem letzten Datenerfassungszeitbereich.
- Ein Zeitbereich relativ zum Kalender.
- Ein angepasster Datumsbereich.
- Alle Daten.

Der ausgewählte Zeitbereich (Typ) wird in der Symbolleiste der Ansicht „Navigation“ unter der Bezeichnung „Zeitbereich“ angezeigt; standardmäßig lautet die Bezeichnung **Letzte 3 Stunden**. Die Ansicht „Zeitbereich“ zeigt den ersten und letzten Zeitstempel für den Datumsbereich, der für die Metadaten verwendet wird.

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

Auswählen eines integrierten Zeitbereichs für die Ermittlung

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**, **Den ganzen Tag** oder einen Tagesabschnitt wie **Morgen**, **Vormittag**, **Nachmittag** oder **Abend**.
   - 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.

Festlegen eines angepassten Zeitbereichs für die Ermittlung

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“, „Minute“ und „Sekunde“aus oder klicken Sie auf **Jetzt**. Die Uhrzeitauswahl wird standardmäßig auf die aktuelle Uhrzeit eingestellt.

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 zum Beispiel ein Drill-down in ein Problem durchführen, wird die Zeit für diesen Drill-down als „HH:MM:00 - HH:MM:59“ interpretiert. Sekunden werden in diesem Format in den Funktionen unter **Investigation > Navigation** angezeigt.

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

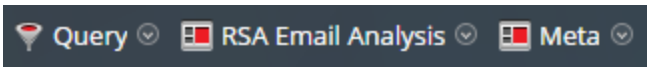
Einkapseln von benutzerdefinierten Ansichten mithilfe von Ermittlungsprofilen

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 Suite-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.

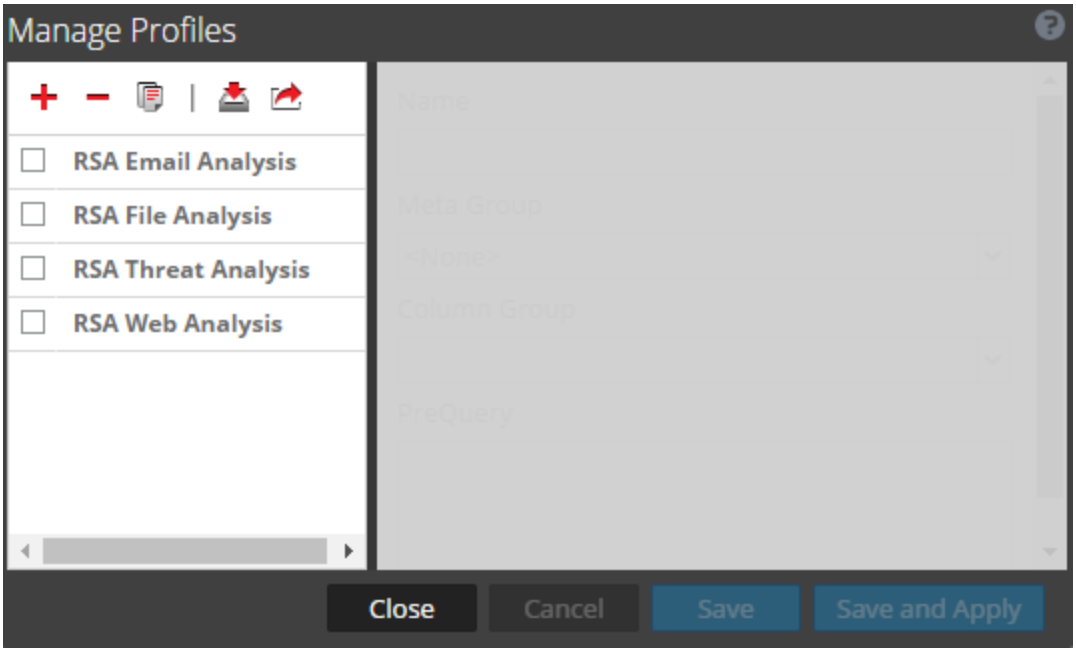
Die folgende Abbildung illustriert dies in der Navigationsansicht. Der Profilname wird zwischen Abfrage und Metadaten angezeigt. In der Ansicht „Ereignisse“ wird der Profilname zwischen Abfrage und Ansicht angezeigt.



Navigieren Sie zum Dialogfeld „Profile managen“.

1. Navigieren Sie zu **Ermittlung > Navigation** oder Ermittlung **> Ereignisse**.
2. Wenn das Dialogfeld **Ermitteln** angezeigt wird, wählen Sie einen Service aus und klicken Sie auf **Navigieren**.

3. Wählen Sie in der Symbolleiste **Profile > Profile managen**.
   aus.Das Dialogfeld „Profile managen“ wird angezeigt.



Profile erstellen und bearbeiten

1. Wählen Sie im Dialogfeld **Profile managen** entweder ein bestehendes Profil aus, indem Sie auf das Kontrollkästchen neben dem Namen klicken, oder klicken Sie auf +, um ein neues Profil zu erstellen.
   Der rechte Bereich ist verfügbar.
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. Wählen Sie eine Metagruppe aus der Drop-down-Liste **Metagruppe** aus. Sie können benutzerdefinierte Metagruppen hinzufügen, wie unter Metagruppen managen beschrieben ist.
4. Wählen Sie eine Spaltengruppe für die Drop-down-Liste **Spaltengruppe** aus. Sie können benutzerdefinierte Spaltengruppen hinzufügen, wie beschrieben in Managen von Spaltengruppen in der Ereignisansicht.
5. Geben Sie Abfragen zum Filtern von Ergebnissen in das Feld **Vorabfrage** ein. Vorabfrage folgt der gleichen Syntax wie die Abfrageerstellung. Die Vorabfrage in der Abbildung verwendet eine Metagruppe namens **crypto exists**.
6. 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 Bestätigungsdialog angezeigt, bevor das ausgewählte Profil als aktiv festgelegt wird.

Wechseln des aktiven Profils

Wenn Sie nicht genügend Ergebnisse oder die richtigen Ergebnisse in der Navigations- oder Ereignisansicht sehen, haben Sie eventuell ein Profil aktiviert. 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 die Maus 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.

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.

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.

Das Parallelkoordinatendiagramm ist eine Möglichkeit zur Visualisierung des aktuellen Drill-down-Punkts in Investigation, um mehr als zwei Metaschlüssel gleichzeitig zu 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 „Navigieren“, 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 in NetWitness Suite zeigt NetWitness Suite eine Fehlermeldung an, wenn 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 Suite 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“ festlegen.

RSA-Metagruppen für Parallelkoordinaten – Anwendungsbeispiele

Eine Reihe von vordefinierten Metagruppen ist im Lieferumfang von NetWitness Suite 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:

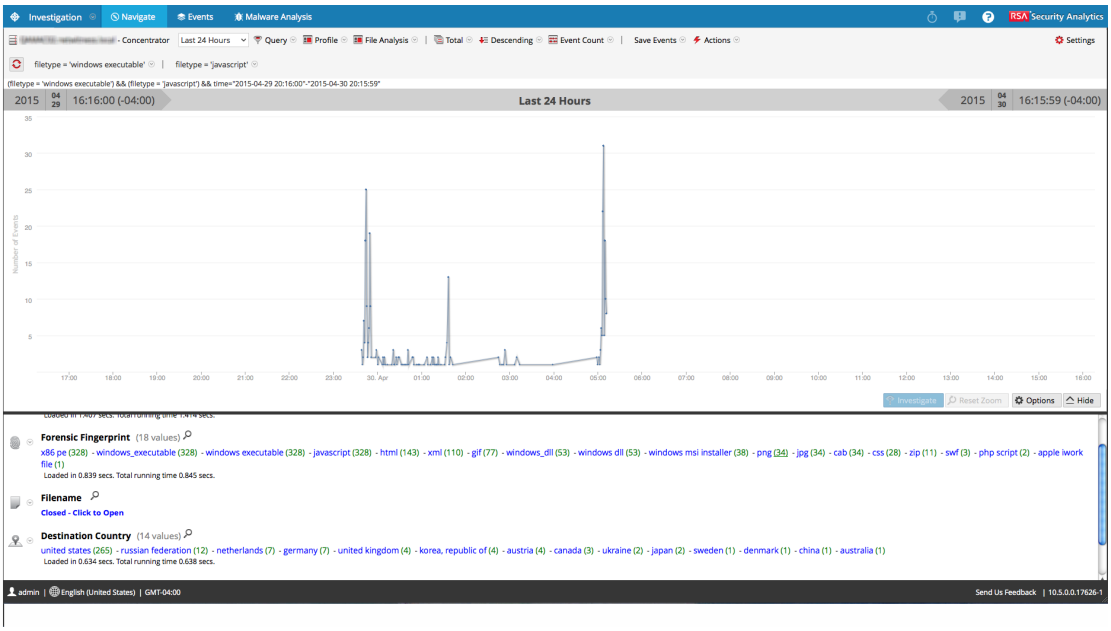
- Botnet Beaconing
- Verdeckte Kanäle
- E-Mail
- Verschlüsselte Sitzungen
- Endpunktanalyse
- Dateianalyse
- Malware Analysis
- Ausgehender HTTP
- Ausgehendes SSL/TLS
- SQL-Injektionsangriffe
- Bedrohungsanalyse
- Webanalyse

Anzeigen einer Parallelkoordinatenvisualisierung

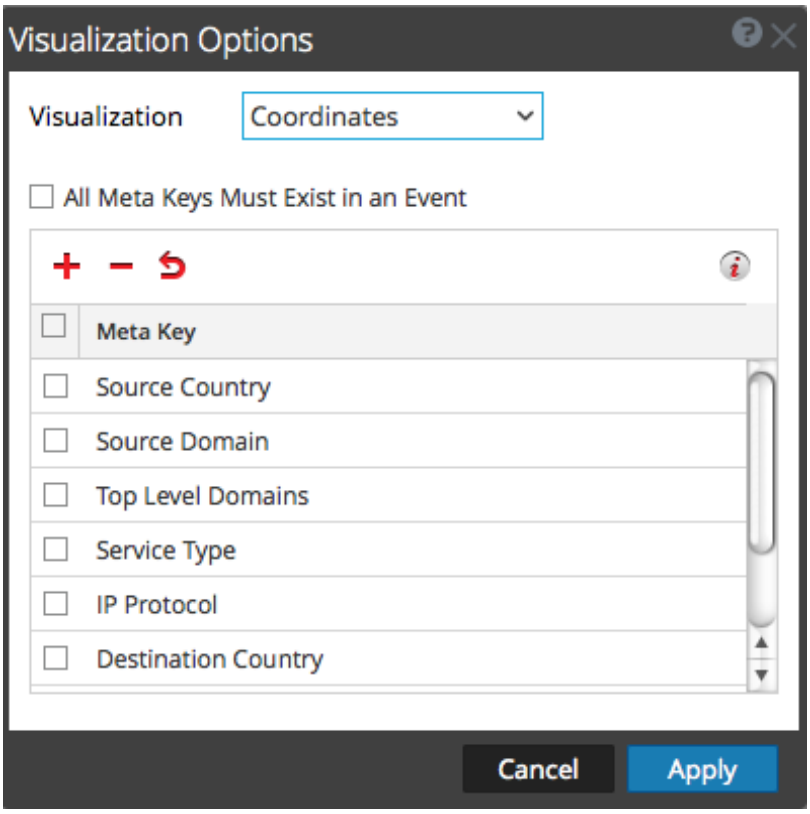
Von einer Ermittlung in der Ansicht „Investigation > Navigation“:

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

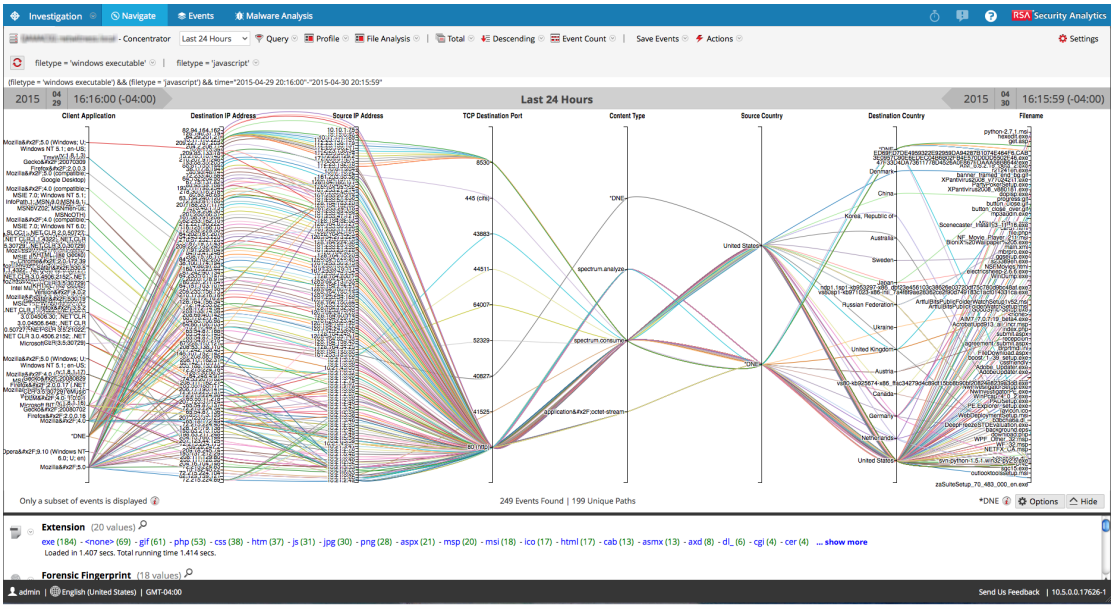
4. Als Zeitachse wird eine Standardvisualisierung für den aktuellen Drill-down-Punkt angezeigt.



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**.



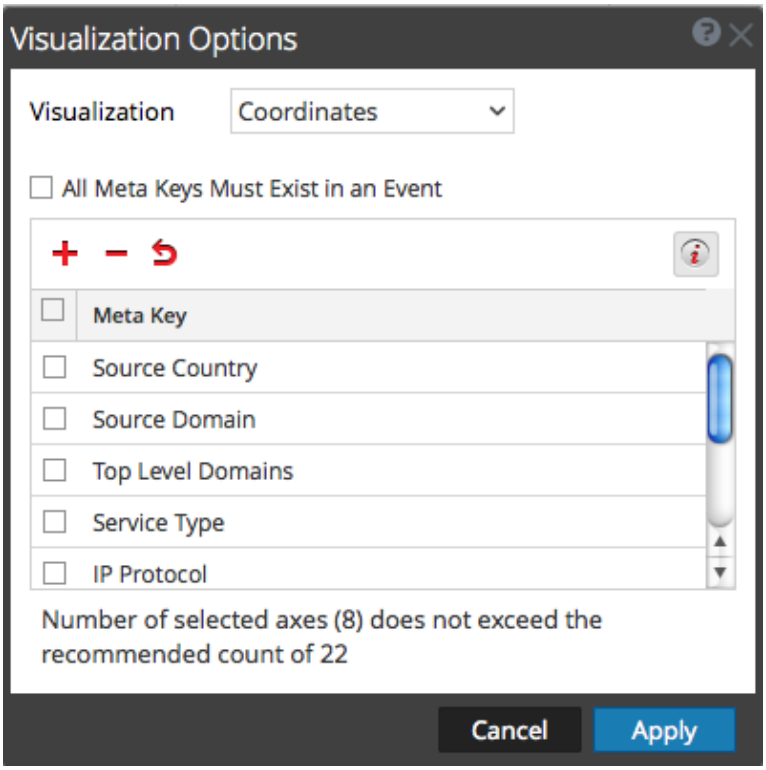
Die Visualisierung wird geladen. In diesem Beispiel wurden 249 Ereignisse gefunden und es werden 199 eindeutige Pfade visualisiert.



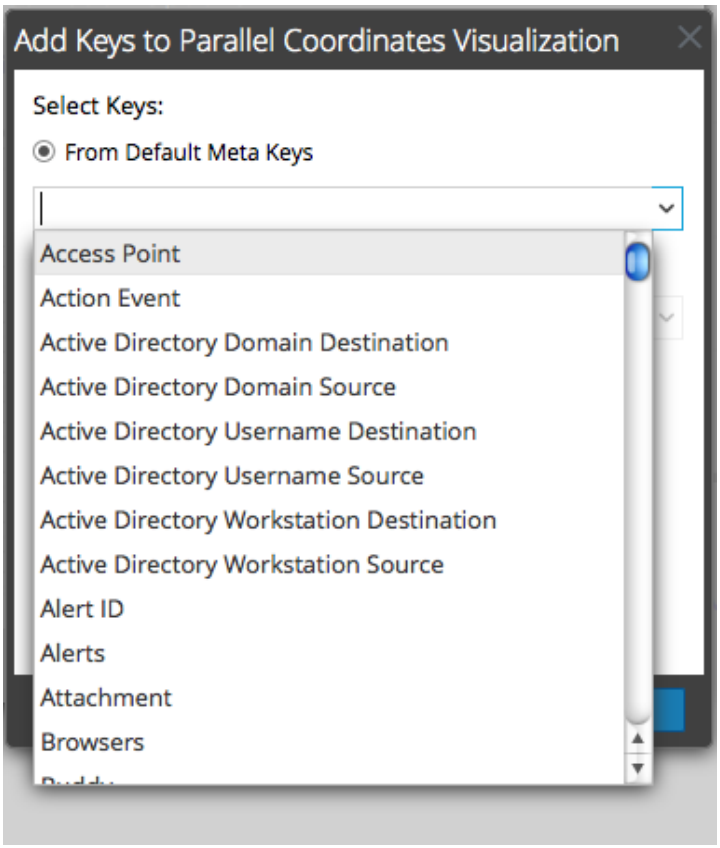
Auswählen der Metaschlüssel für eine Parallelkoordinatenvisualisierung

Gehen Sie bei geöffneter Parallelkoordinatenvisualisierung wie folgt vor:

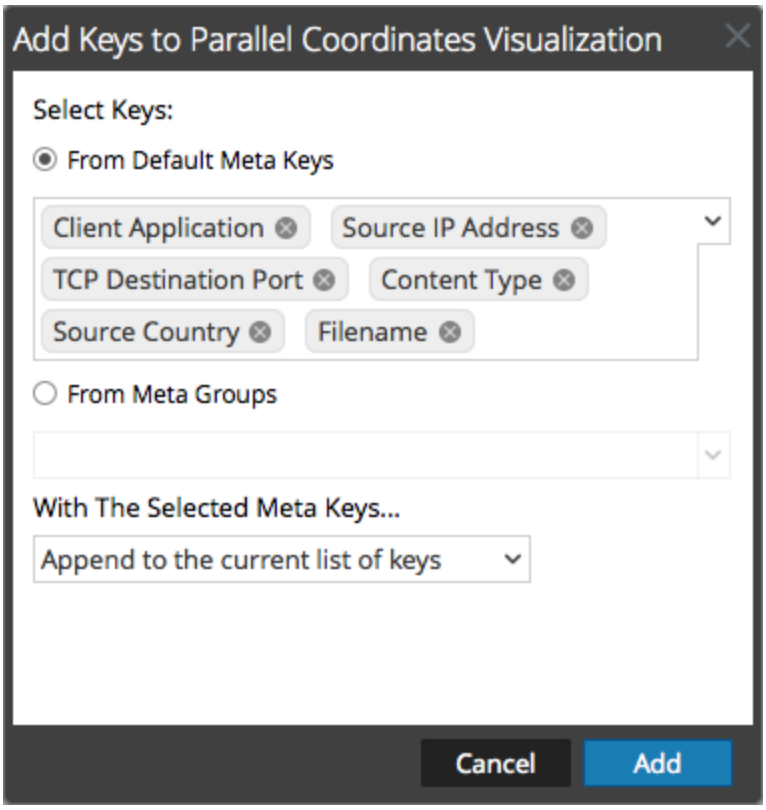
1. Wählen Sie im Bereich „Visualisierung“ den Punkt **Optionen** aus.
   Das Dialogfeld „Visualisierungsoptionen“ wird angezeigt. Klicken Sie in der Symbolleiste auf , um die empfohlene Anzahl an Achsen für eine lesbare Visualisierung anzuzeigen.
   Wenn eine empfohlene Anzahl an Schlüsseln angezeigt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



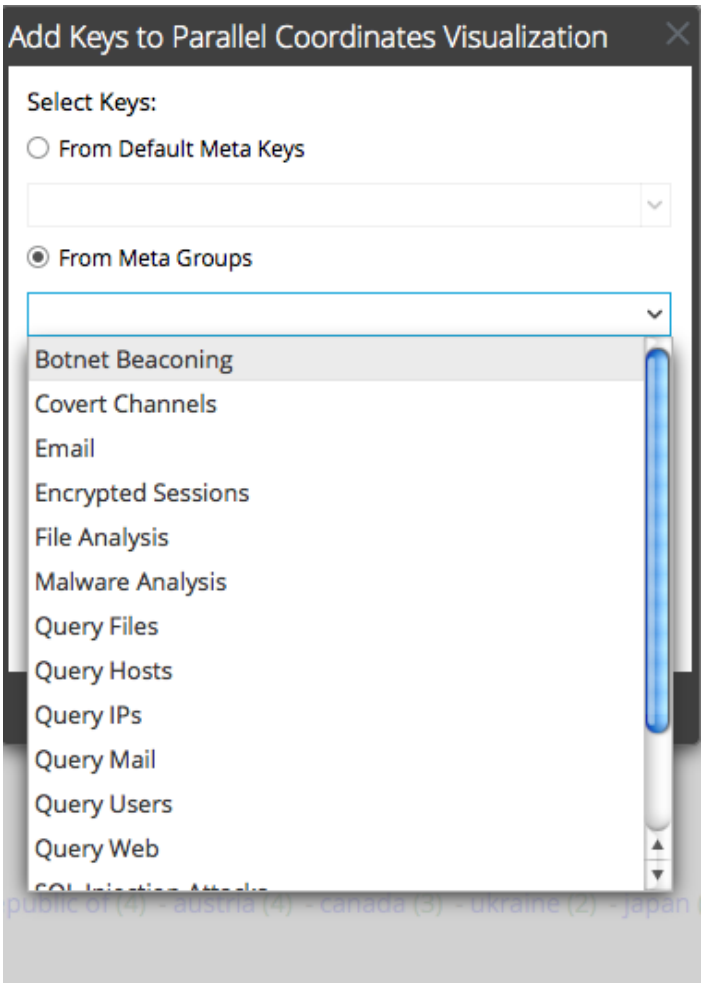
2. Wenn Sie die Reihenfolge der Metaschlüssel ändern möchten, ziehen Sie die Metaschlüssel in die gewünschte Reihenfolge nach oben oder unten.
3. Wenn Sie Metaschlüssel löschen möchten, klicken Sie in das Auswahlfeld und klicken Sie auf .
   Die Metaschlüssel werden entfernt, aber die Änderung wurde 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.

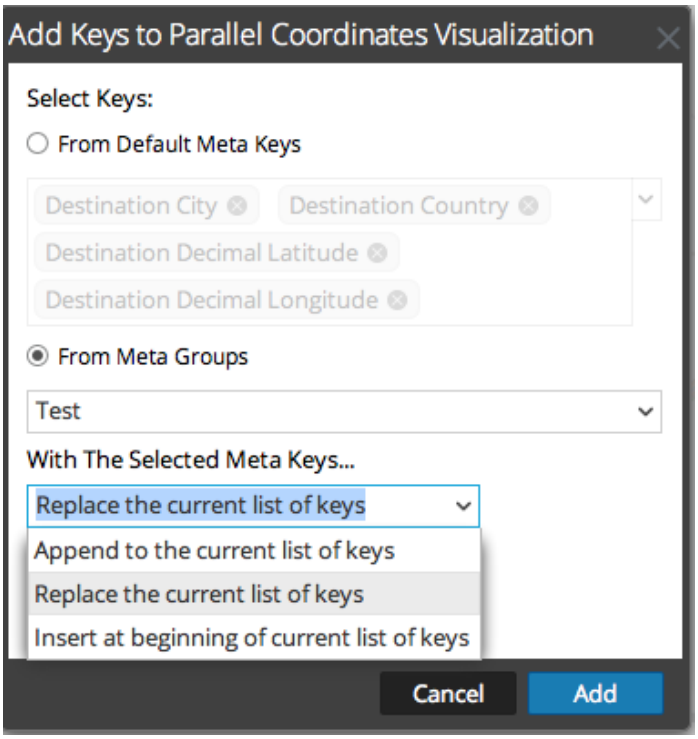


6. Wenn Sie alle Schlüssel einer Metagruppe hinzufügen möchten, können Sie keine einzelnen Schlüssel hinzufügen. Wählen Sie **Aus Metagruppen** aus und wählen Sie in der Drop-down-Liste eine Gruppe aus.



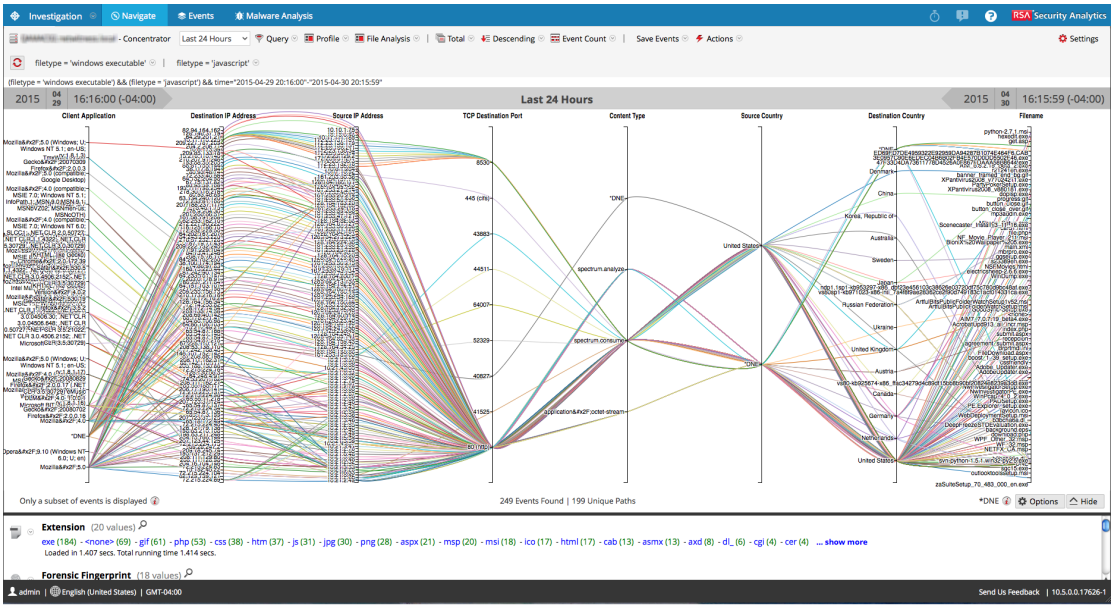
Die ausgewählten Metagruppen werden in dem Feld aufgelistet.

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.**



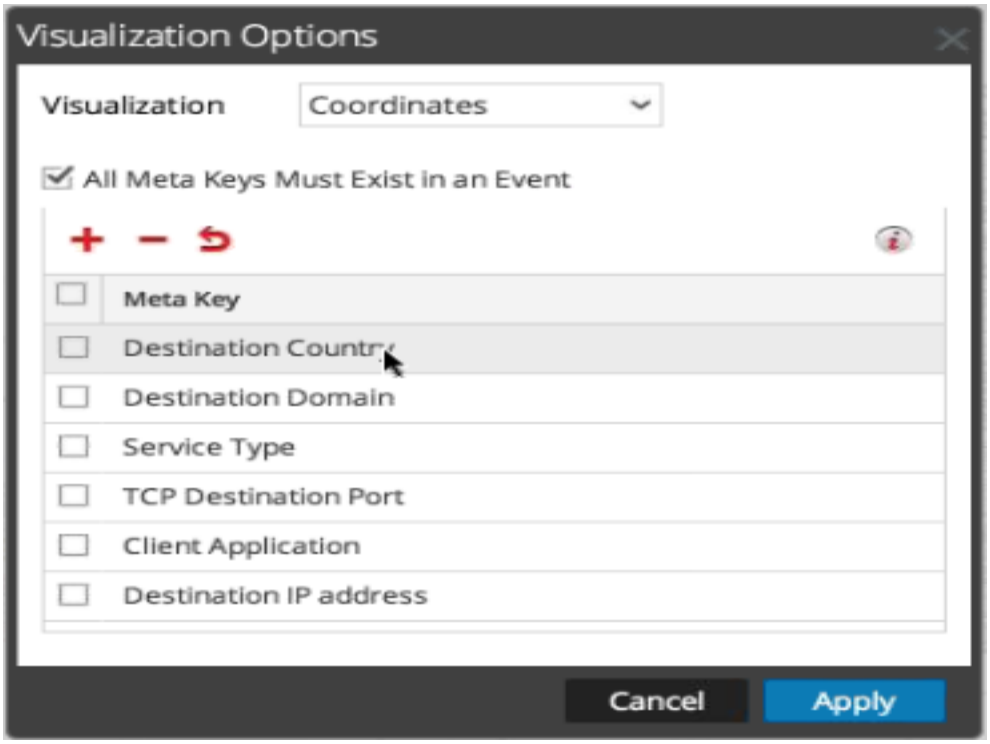
8. Klicken Sie auf **Hinzufügen**, um das Verfahren abzuschließen.
   Das Dialogfeld „Visualisierungsoptionen“ wird mit den ausgewählten Metaschlüsseln oder -gruppen angezeigt.

9. Klicken Sie zum Anzeigen des neuen Visualisierungsdiagramms auf **Anwenden**.

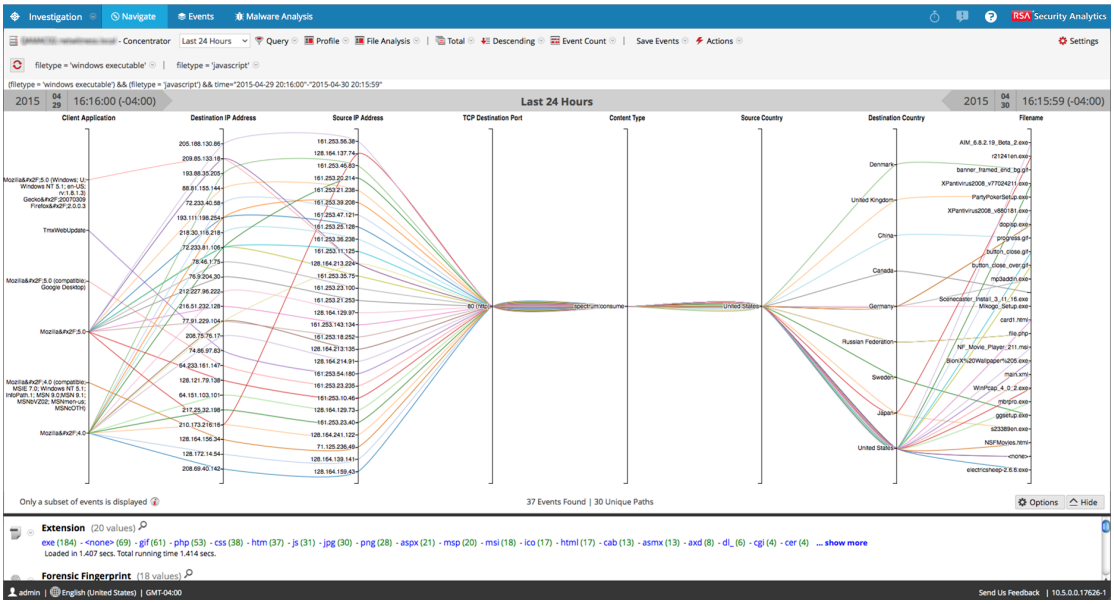


Optimieren einer Parallelkoordinatenvisualisierung

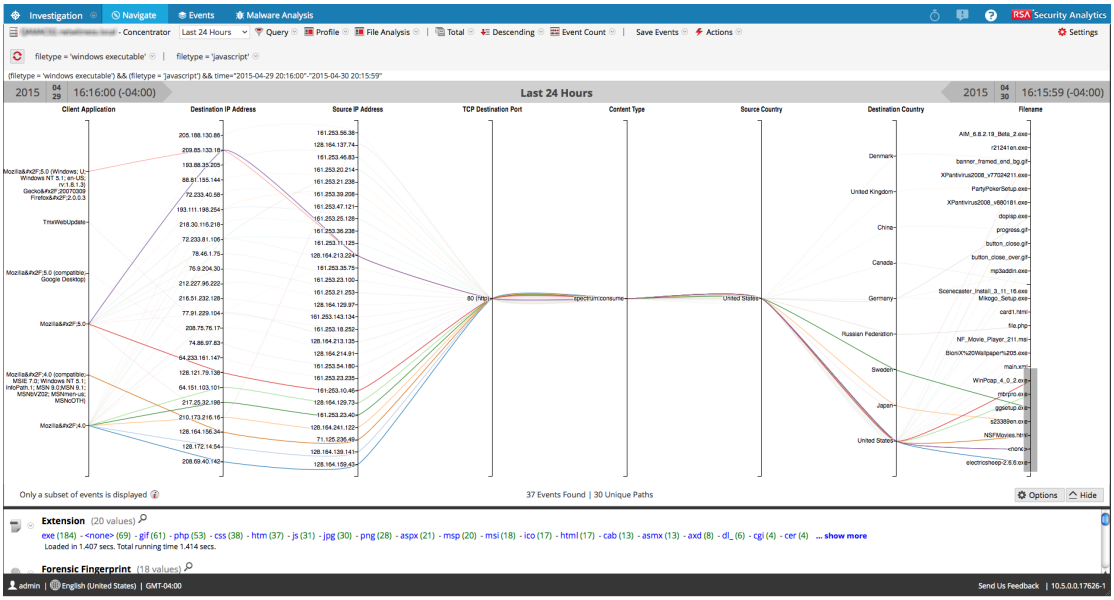
1. Wählen Sie zum Optimieren der Visualisierung durch Entfernen der Ereignisse, in denen nicht alle Metaschlüssel enthalten sind, **Optionen** aus.



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 normalerweise 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.



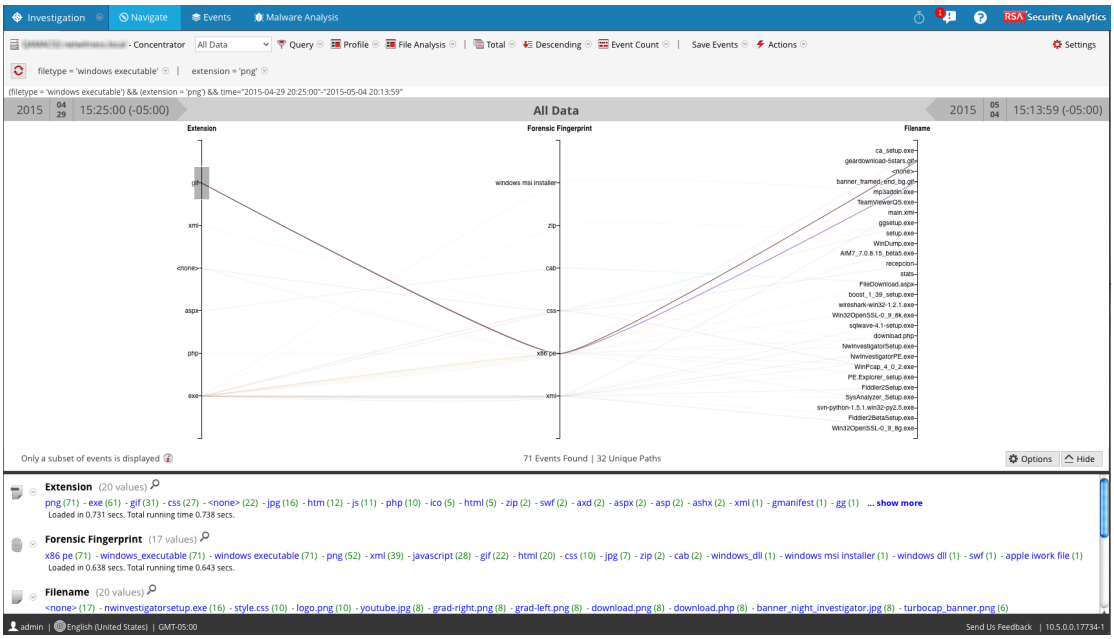
4. Wenn Sie die Visualisierung vergrößern möchten, ziehen Sie die untere Ecke des Bereichs nach unten und ziehen Sie die rechte Ecke des Browserfensters breiter.

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“. Entlang jeder Achse sind Werte aufgetragen. 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`.

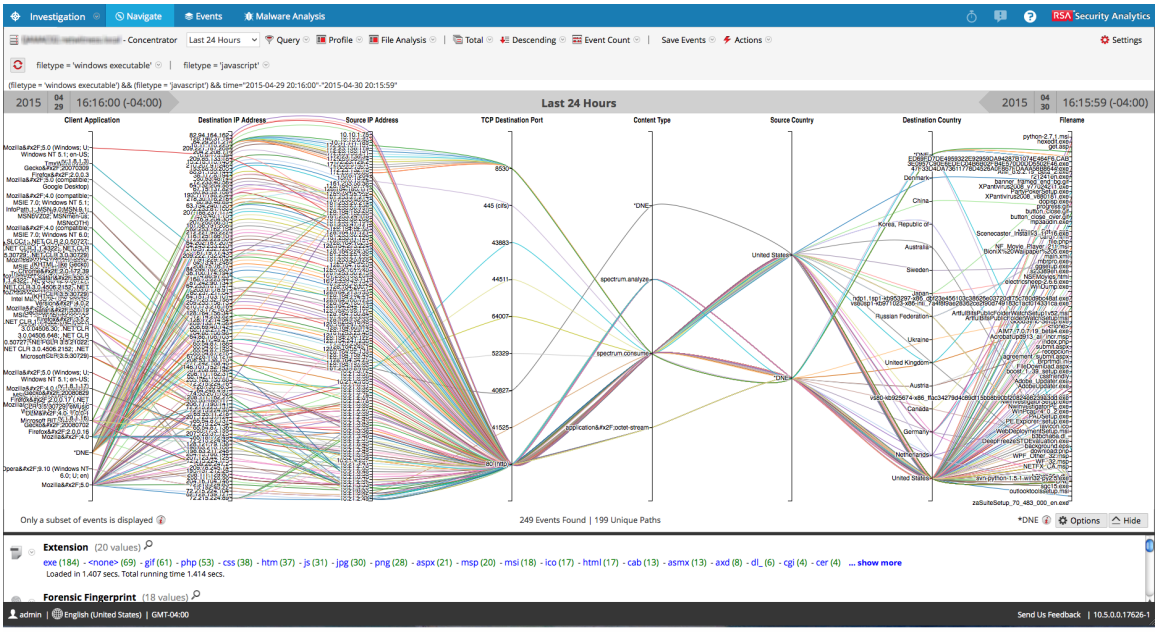


Beispielvisualisierung eines großen Datensatzes

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 Suite 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 Suite 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 Suite 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 Suite 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 Suite 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.

Abfragen von Daten in der Ansicht „Navigation“

In diesem Thema werden die Methoden zur Abfrage von Daten in der Ansicht „Investigation > Navigation“ beschrieben.

Wenn Sie eine Ermittlung in NetWitness Suite durchführen, stehen Ihnen verschiedene Methoden zur Ergebnisabfrage und zur Drill-down-Analyse eines Bereichs von Interesse in der Ansicht „Navigieren“ zur Verfügung. Analysten können:

- Erstellen einer angepassten Abfrage, anstatt durch Metaschlüssel und Werte zu klicken (Ansicht „Navigation“ und „Ereignisse“).
- Zeitdiagramm des Drill-down in die Daten in der Ansicht „Navigation“ (Ansicht „Navigation“)
- Drill-down zu Daten im Bereich „Werte“ (Ansicht „Navigation“)
- Anzeigen und Ändern von Abfragen mithilfe von URL-Integration(Ansicht „Navigation“ und „Ereignisse“)

Erstellen einer angepassten Abfrage

Sie können eine Abfrage im Optionsbereich der Ansicht „Untersuchen“ > „Navigation“ 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. 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.

Wenn Sie eine Metagruppe ausgewählt haben, erzeugt NetWitness Suite 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:

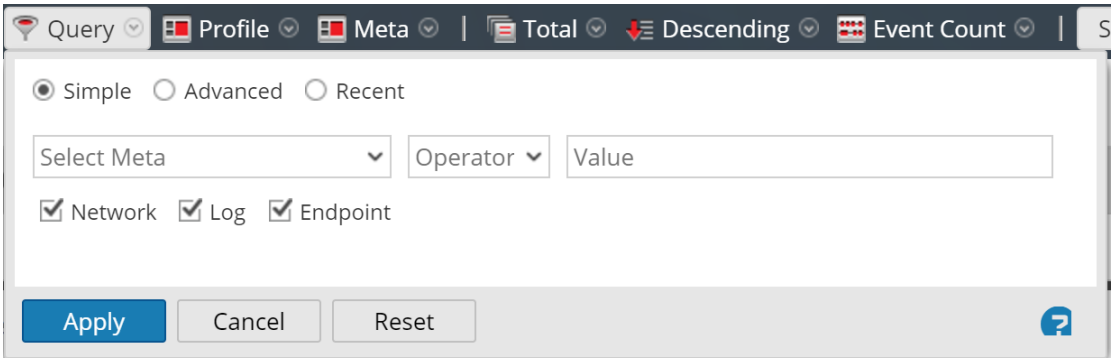
```
action exists
action = 'get'
alias.host = '10.25.55.115'
```

```
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 Suite Drop-down-Listen von Metadaten und Operatoren.

1. Wählen Sie in der Symbolleiste **Ansicht Navigieren** 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**.

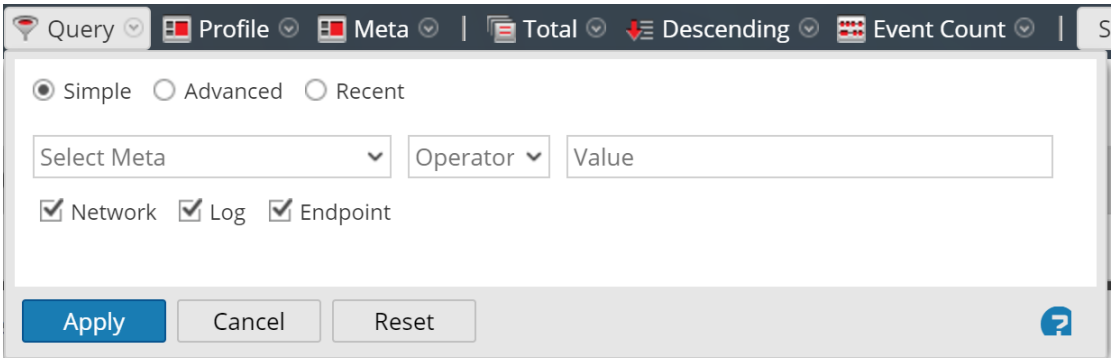
Das Fenster wird geschlossen und die Ansicht wird mit den Ergebnissen der neuen Abfrage aktualisiert. Die Abfrage wird im Breadcrumb angezeigt.

b. Klicken Sie auf **Abbrechen**.

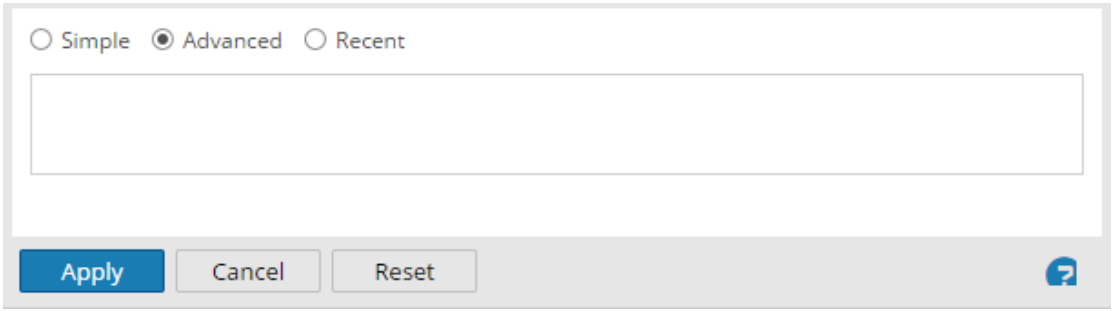
Das Fenster wird geschlossen und es werden keine Änderungen an der Ansicht oder aktuellen Abfrage vorgenommen.

Erstellen einer Abfrage mithilfe der erweiterten Methode

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

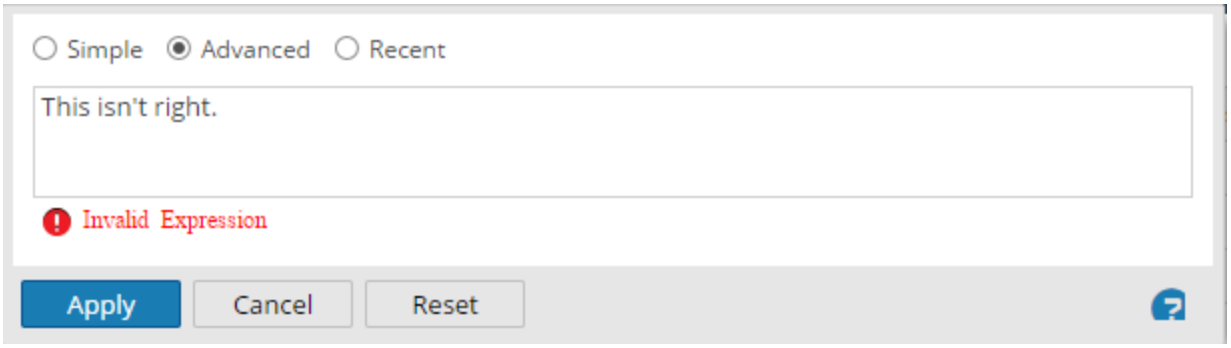


2. Wählen Sie die Option **Erweitert** aus.
   Das Feld „Erweiterte Abfrage“ wird angezeigt.



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.



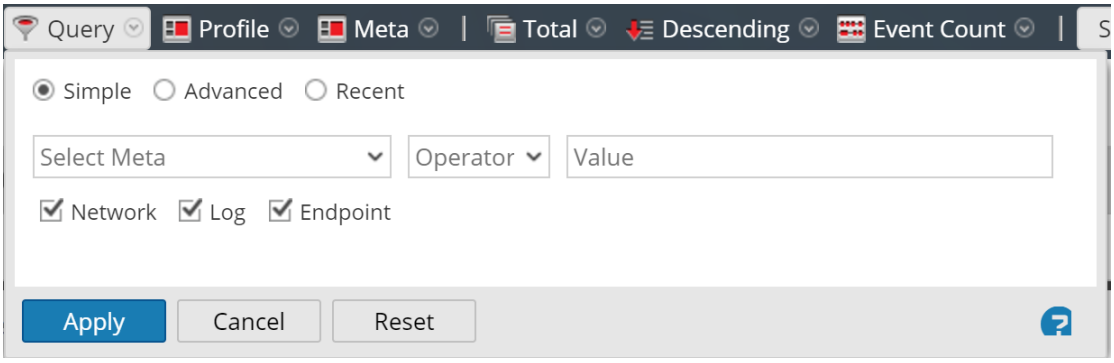
6. Führen Sie einen der folgenden Schritte aus:

   - 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

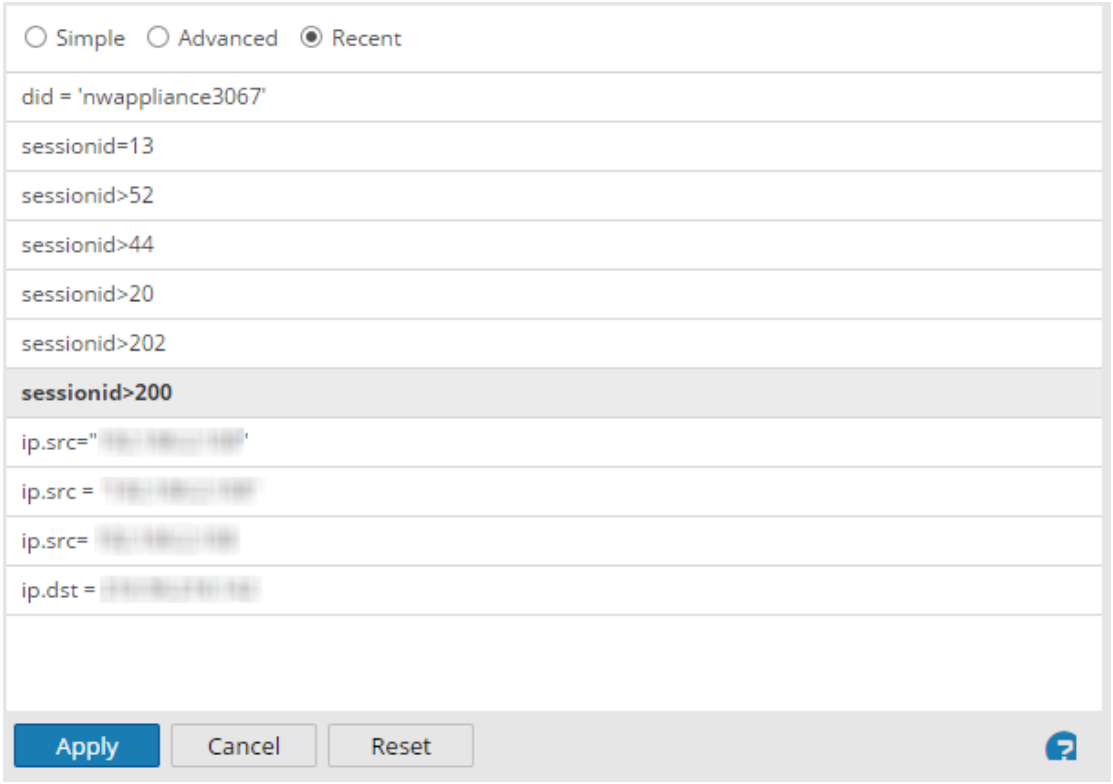
Sie können zuletzt verwendete Abfragen anzeigen und eine auswählen, um sie auf den aktuell untersuchten Service anzuwenden. So wählen Sie eine zuletzt verwendete Abfrage aus:

1. Wählen Sie in der Symbolleiste **Ansicht Navigieren** 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.



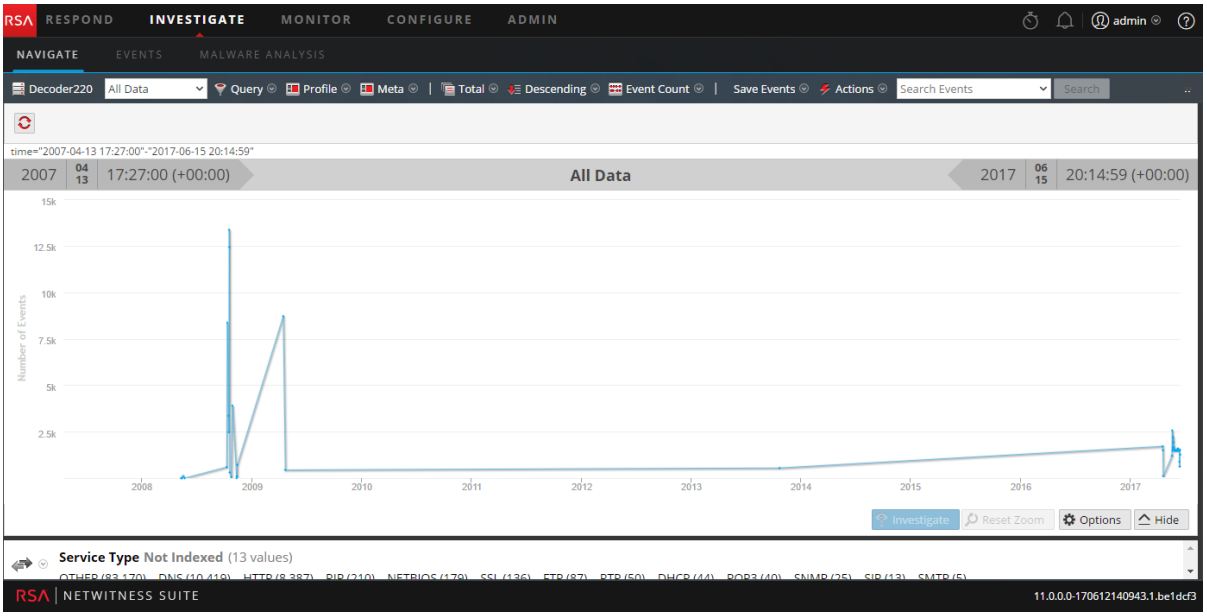
3. Klicken Sie in die Liste der zuletzt verwendeten Abfragen, um eine Abfrage auszuwählen.
4. Führen Sie einen der folgenden Schritte aus:
   - Doppelklicken Sie auf eine Abfrage.
   - Wählen Sie eine Abfrage aus und klicken Sie auf **Anwenden**.
     Das Fenster wird geschlossen und die Ansicht wird 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.

Zeitdiagramm des Drill-down in die Daten in 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.



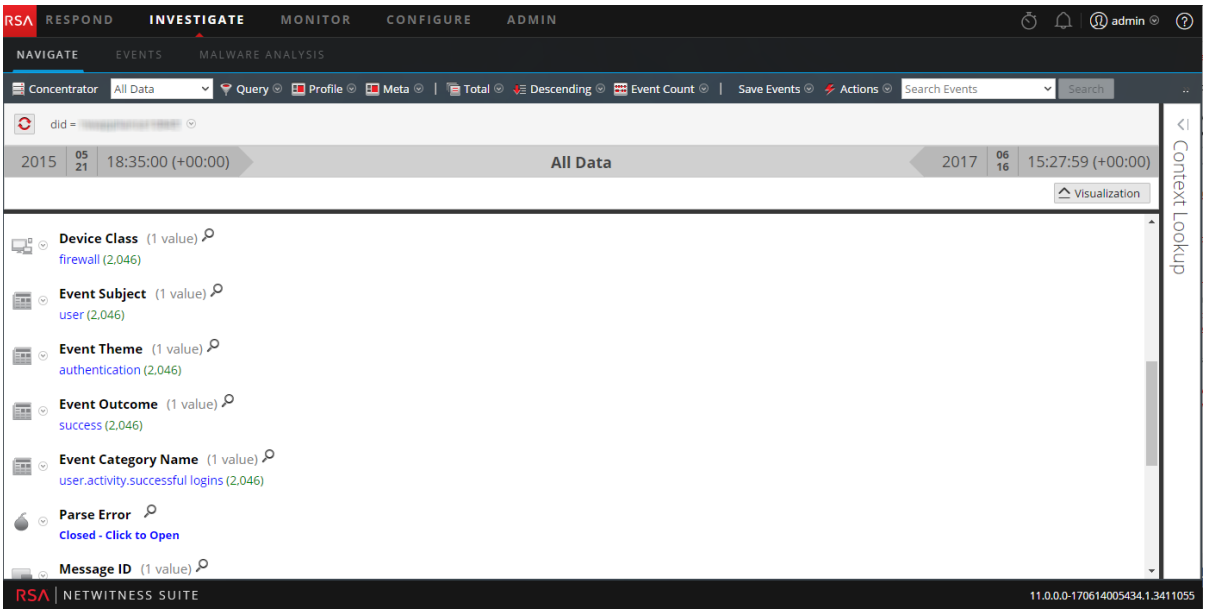
2. Zur Markierung eines Zeitbereichs im Zeitdiagramm klicken Sie auf den gewünschten Zeitbereich und ziehen Sie die Maus.
   Das Zeitdiagramm wird für den ausgewählten Zeitbereich neu gezeichnet, die Metawerte bleiben jedoch unverändert.
3. Zum Drill-down in die Daten für den ausgewählten Zeitbereich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

Drill-down in einer Untermenge der Metadaten

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

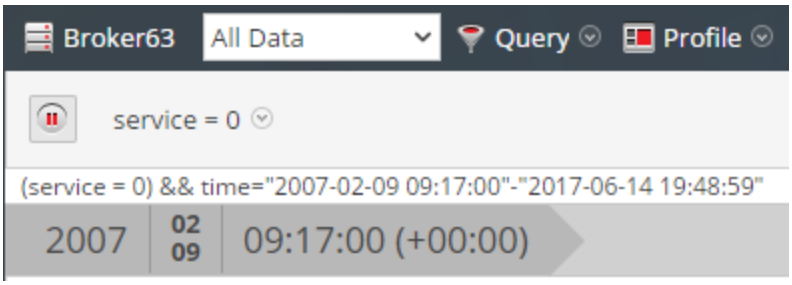


2. Um einen Drill-down in den Metadaten durchzuführen, führen Sie eine der folgenden Aktionen aus:

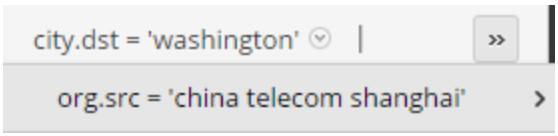
   a. Klicken Sie auf einen **Metaschlüssel**, zum Beispiel „Quellland“ oder „Zielland“.

   b. Klicken Sie auf einen **Metawert**. Dies ist der blaue Text in den Ergebnissen. Beispiel: Italien.

   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 Überlauf-Symbol und auf eine Abfrage in der Drop-down-Liste.

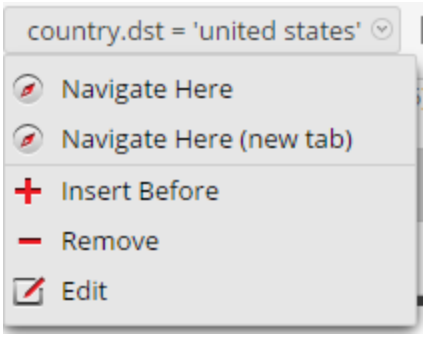


Hinzufügen einer Abfrage in die Breadcrumb-Navigation

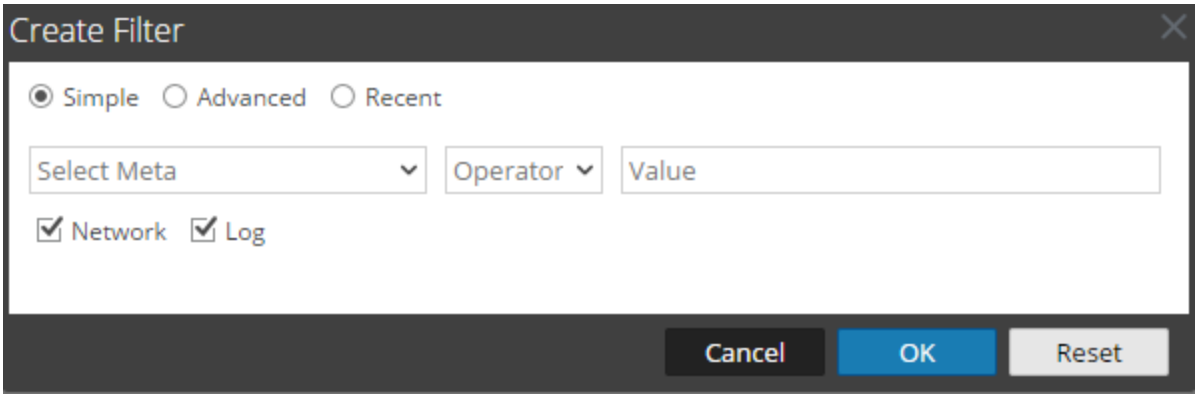
Sie können auf eines der Breadcrumb-Elemente klicken, um das Menü Abfrage anzuzeigen. Sie können vor einem Breadcrumb-Element eine neue Abfrage einfügen und am Ende des Breadcrumbs eine neue Abfrage anfügen. Nach jeder Bearbeitung im Breadcrumb aktualisiert NetWitness Suite die Ergebnisse.

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.



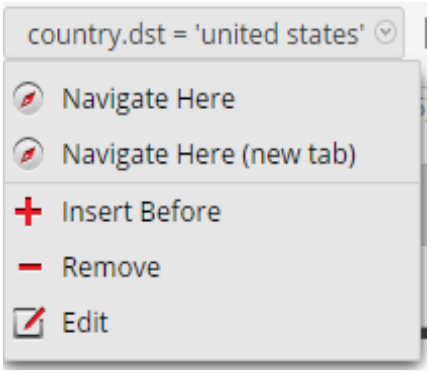
3. Erstellen Sie die Abfrage wie unter Erstellen einer angepassten Abfrage beschrieben.

Bearbeiten einer Abfrage im Breadcrumb

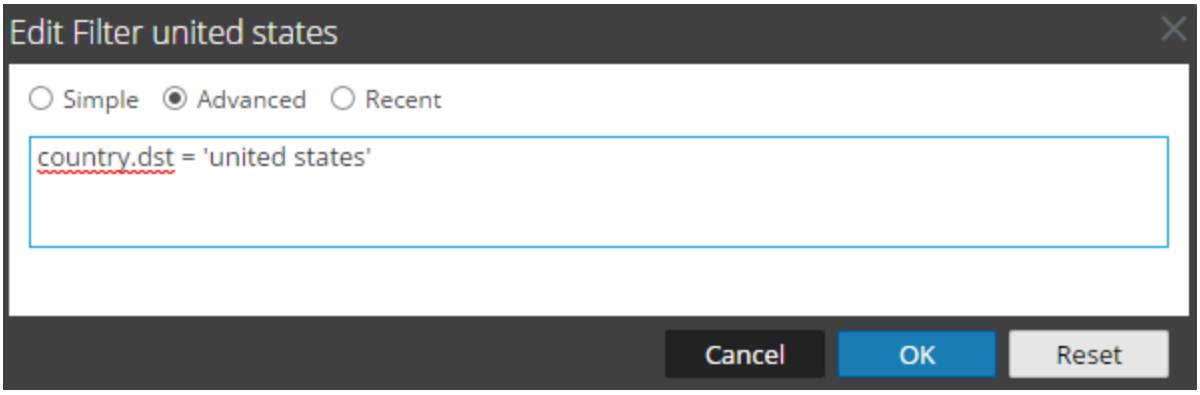
Sie können auf eines der Breadcrumb-Elemente klicken, um das Menü Abfrage anzuzeigen. Sie können ein Breadcrumb-Element löschen und eine Abfrage in einem Breadcrumb-Element bearbeiten. Nach jeder Bearbeitung im Breadcrumb aktualisiert NetWitness Suite die Ergebnisse.

So arbeiten Sie mit Abfragen in einem Breadcrumb:

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



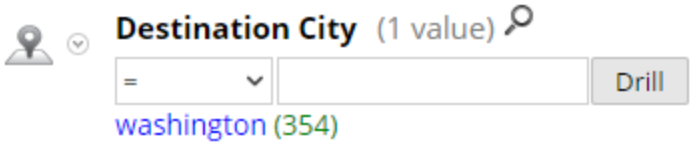
2. Um eine Abfrage im Breadcrumb zu bearbeiten, klicken Sie auf **Bearbeiten**.
   Das Dialogfeld „Erstellen“ wird angezeigt und die ausgewählte Abfrage wird zur Bearbeitung geöffnet.



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

Schnellsuche innerhalb eines Metaschlüssels

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.

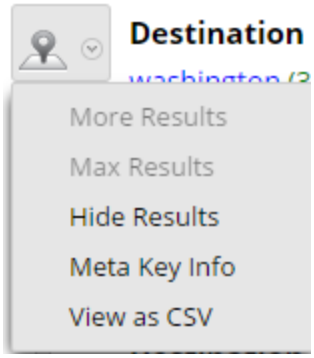


2. (Optional) Zum Schließen des Suchformulars klicken Sie nochmals auf die Lupe.
3. Wählen Sie den Vorgang aus der Drop-down-Liste auf der linken Seite aus und geben Sie den zu suchenden Textwert ein. Klicken Sie anschließend auf **Drill**, um die Ausführung zu starten.
   Die Metadaten für diesen Metaschlüssel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

Anzeige der Metaschlüssel-Informationen in der Ansicht Navigieren

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.



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

Anzeige von Ereignissen, die dem Metawert zugeordnet sind

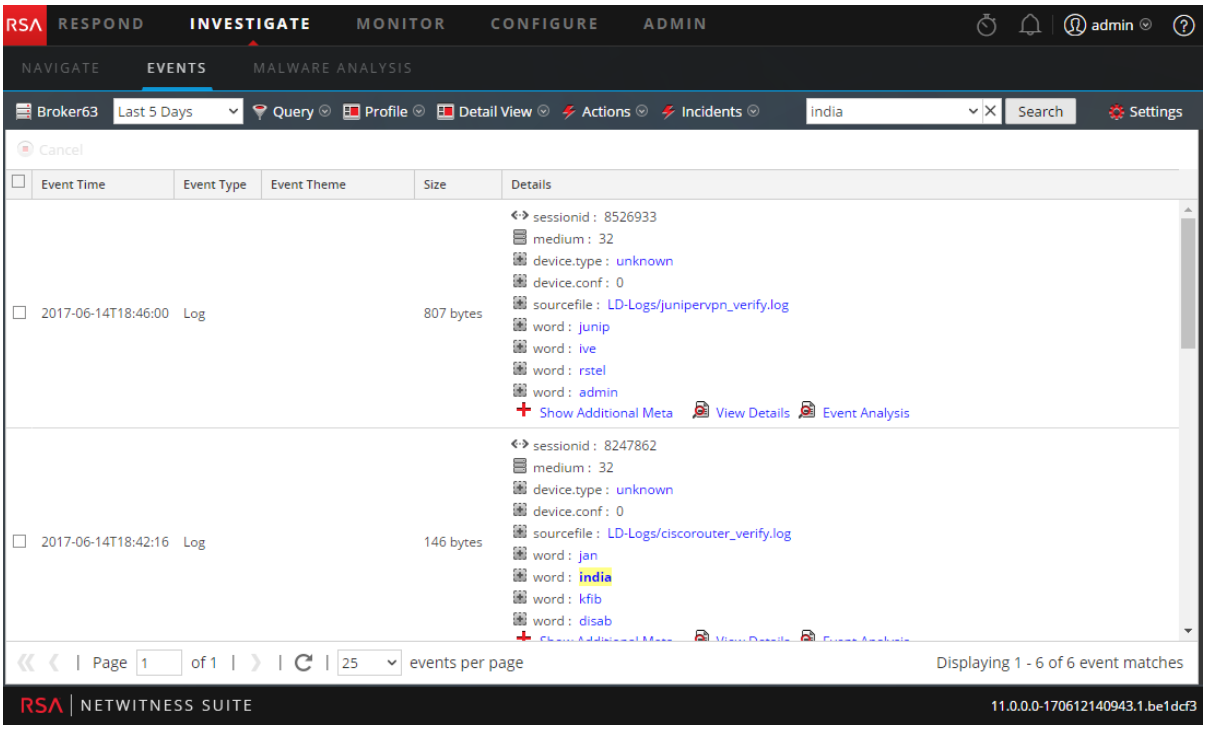
Die Ansicht Ereignisse bietet zwei unterschiedliche Ansichtsmöglichkeiten für zusätzliche Ereignisinformationen: Die Ereignisliste und die Detailansicht.

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 im Menüpunkt Untersuchen von Ereignissen beschrieben.

Suchen nach bestimmten Ereignissen im Zusammenhang mit einem Metawert

1. Führen Sie in der Ansicht „Navigieren“ 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).

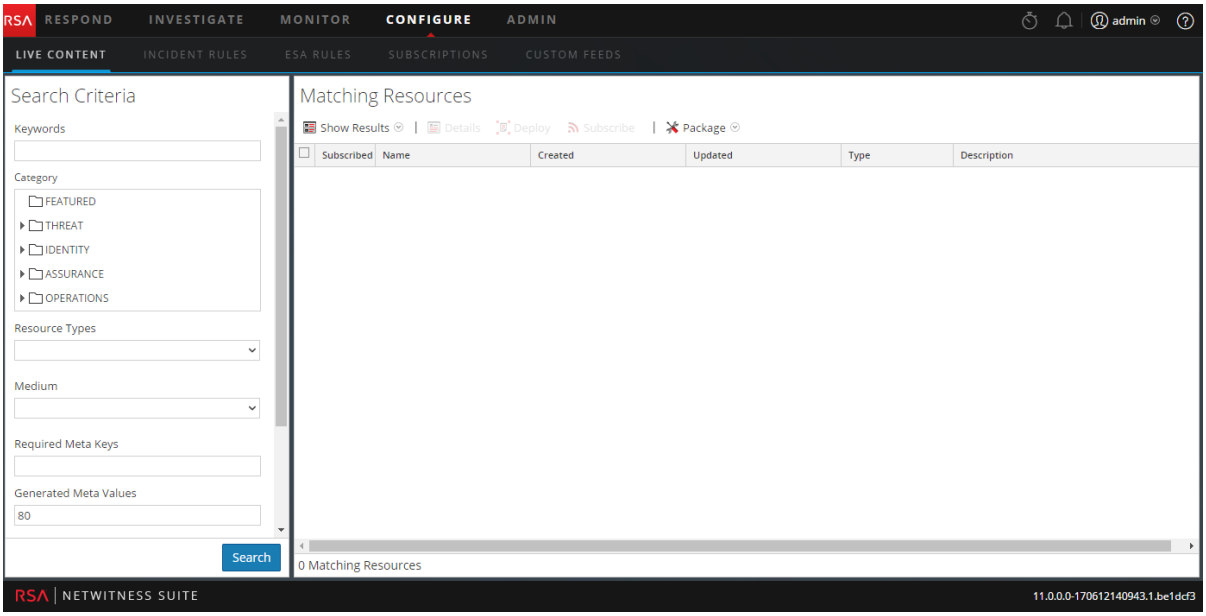
2. Geben Sie eine Suchzeichenfolge in das Suchfeld ein und drücken Sie die **Eingabetaste** oder klicken Sie auf **Suche**.
   Sie können Ihre Suchmoduseinstellungen für Ihre Suchen auch auswählen und festlegen. Detaillierte Suchinformationen finden Sie unter Suchen nach Textmustern in der Ansicht „Untersuchen“.
   Die Ansicht „Ereignisse“ wird in einer neuen Registerkarte geöffnet und zeigt die Suchergebnisse an. Ihre Zeitbereichsauswahl und Drill-Downs (Abfragen) werden in die Ansicht „Ereignisse“ übertragen.



Anzeige eines ausgewählten Metawerts in Live

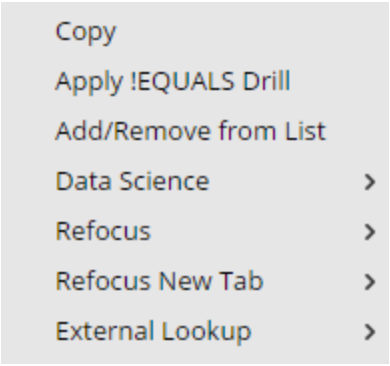
1. Führen Sie in der Ansicht Navigieren einen Drill-down zu den Metadaten durch, die den Schwerpunkt Ihrer Ermittlungen bilden sollen.
2. Klicken Sie mit der rechten Maustaste auf einen Metawert (den Text in Blau).
   Das Drop-down-Menü Metawert wird angezeigt.
3. Um den Metawert in NetWitness Suite 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.



Neufokussierung der Ermittlung in einem Drill-down-Punkt

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.

Betrachten eines spezifischen Zählers in einer neuen Registerkarte

So können Sie einen Zähler für einen Metawert in einer neuen Registerkarte oder eine Geomap der Speicherorte für den ausgewählten Metawert anzeigen lassen.

1. Klicken Sie mit der rechten Maustaste auf einen Zähler für einen Metawert (die grüne Nummer, die nach dem blauen Metawert steht).
   Das Kontextmenü wird angezeigt.

2. (Optional) Um eine separate Ermittlung für den spezifischen Metawert zu öffnen, wählen Sie **In neuer Registerkarte öffnen** aus.
3. (Optional) Um eine Geomap mit den Speicherorten anzuzeigen, von denen der ausgewählte Metawert stammt, klicken Sie auf **Geomap-Orte in neuer Registerkarte**.

Anzeigen und Ändern von Abfragen mithilfe von URL-Integration

Die externe URL-Integration ermöglicht über die Suche in der NetWitness Suite-Architektur die Integration von Drittanbieterprodukten. 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 „Investigation“ in NetWitness Suite wechseln. Diese Integration ermöglicht eine interne Darstellung 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 Suite definiert. Kann NetWitness Suite 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>
```

Dabei gilt Folgendes

- `<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 Suite-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 Suite 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 Suite-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 ist `<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>
```

Dabei gilt Folgendes

- `<sa host: port>` ist die IP-Adresse oder das DNS, mit oder ohne einem 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>`** ist Host und Port eines in der NetWitness Suite-Instanz definierten Service für den abzufragenden Service. NetWitness Suite versucht, Host und Port als eine in NetWitness Suite definierte Service-ID aufzulösen.
- `<encoded query>` steht dabei für die URL-kodierte NetWitness Suite-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 ist `<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 SA-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.

Aktionen zu Drill-down-Punkten in der Ansicht „Navigation“

In diesem Thema werden die Aktionen beschrieben, die Analysten zur Verfügung stehen, die einen Drill-down-Punkt an ein Ausgabeformat senden oder den Drill-down-Punkt von einer anderen Perspektive in der Ansicht „Navigation“ anzeigen möchten.

Wenn eine Ermittlung in NetWitness Suite durchgeführt wird, sind verschiedene Aktionen verfügbar, sobald ein Drill-down-Punkt in der Navigationsansicht erreicht wurde. Analysten können:

- Exportieren eines Drill-Punkts (Ansicht „Navigation“ und Ansicht „Ereignisse“)
- Ausdrucken des aktuellen Drill-down-Punkts (Ansicht „Navigation“)
- Öffnen der Ereignisliste für einen Metawert (Ansicht „Navigation“)
- Starten einer externen Suche eines Metaschlüssels (Ansicht „Navigation“)
- Starten eines Schadsoftwareanalyse-Scans in der Navigationsansicht
- Anzeigen von zusätzlichem Kontext für einen Datenpunkt (Ansicht „Navigation“ und Ansicht „Ereignisse“)
- Managen von Context Hub-Listen und -Listenwerten in Investigate (Ansicht „Navigation“ und Ansicht „Ereignisse“)
- Visualisieren des aktuellen Drill-Punkts in Informer (Ansicht „Navigation“)

Exportieren eines Drill-Punkts

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

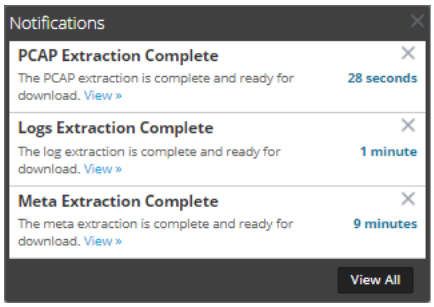
- Dateien aus einer Sitzung extrahieren und den Typ der zu extrahierenden Dateien wählen: Archive, Audio-BitTorrent, Dokumente, ausführbare Dateien, Bilder, andere, Video und Web.
- den Drill-down-Punkt als Paketerfassungsdatei (PCAP), Protokolldatei oder Metadatendatei exportieren.

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 Suite 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 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. Wenn die geplante Datei-Extrahierung abgeschlossen ist, wird sie im Jobbenachrichtigungsbereich angezeigt.



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

Starten einer externen Suche eines Metaschlüssels

Dieses Thema enthält Anweisungen für die Verwendung sofort einsatzfähiger Investigation-Plug-ins, um mithilfe von NetWitness Suite-externen Tools eine externe Suche bestimmter Metaschlüssel zu starten, während Daten in der Navigationsansicht oder der Ereignisansicht ermittelt werden.

Analysten können sofort einsatzfähige externe Suchen mit NetWitness Suite Investigation 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 Suite integriert:

- Google Malware: Öffnet eine Google Malware-Suche in einer neuen Registerkarte.
- McAfee SiteAdvisor: Öffnet eine McAfee SiteAdvisor-Suche in einer neuen Registerkarte.
- BFK-passive DNS-Erfassung: Öffnet eine BFK-passive DNS-Erfassung-Suche in einer neuen Registerkarte.
- CentralOps WHOIS für IP-Adressen und Hostnamen: Öffnet eine CentralOps Whois-Suche nach IP-Adressen und Hostnamen
- Suche auf Malwaredomainlist.com: Öffnet eine Suche auf Malwaredomainlist.com in einer neuen Registerkarte.
- Suche auf Malwaredomains.com: Öffnet eine Suche auf Malwaredomains.com in einer neuen Registerkarte.
- Robtex IP-Suche: Öffnet eine Robtex IP-Suche in einer neuen Registerkarte.
- SamSpade-Suche: Öffnet eine SamSpade-Suche in einer neuen Registerkarte.
- ThreatExpert-Suche: Öffnet eine ThreatExpert-Suche in einer neuen Registerkarte.
- UrlVoid-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.

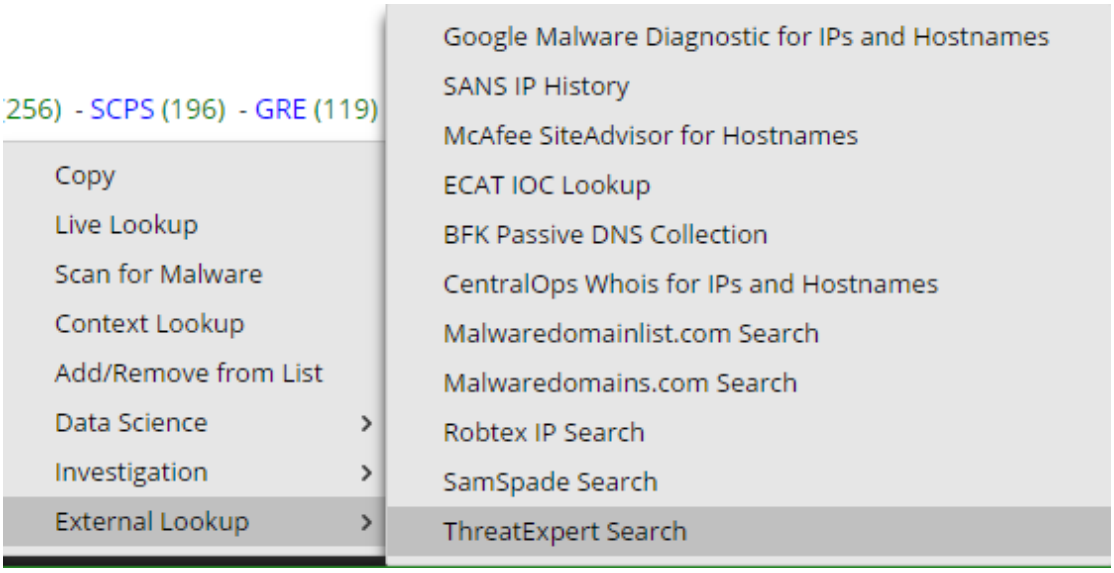
Für den Metaschlüssel `client` öffnet die ECAT-Lookup-Option einen ECAT-Client in einer neuen Registerkarte, sofern der ECAT-Client auf dem gleichen System installiert ist, auf dem der Browser verwendet wird.

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

Eine ECAT IOC-Suche starten

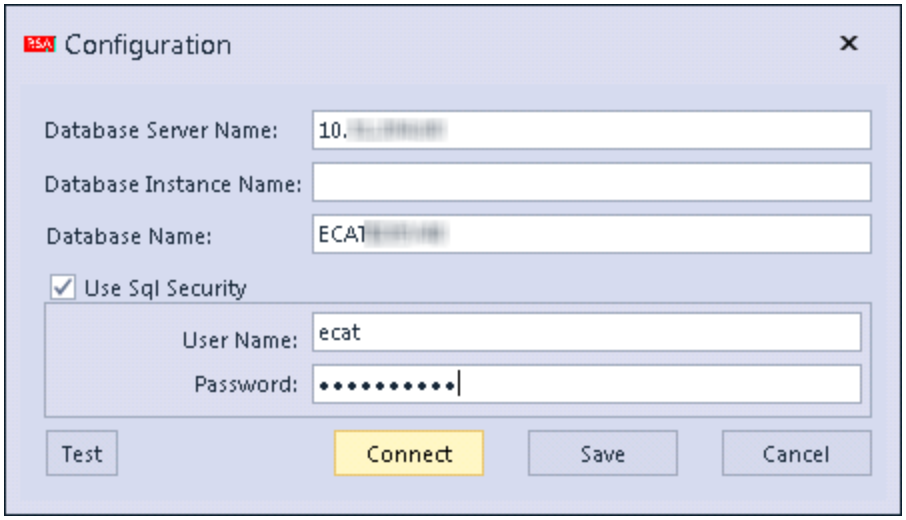
So starten Sie einen ECAT-Suche von Daten aus der Ansicht „Investigation > Navigieren“:

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.

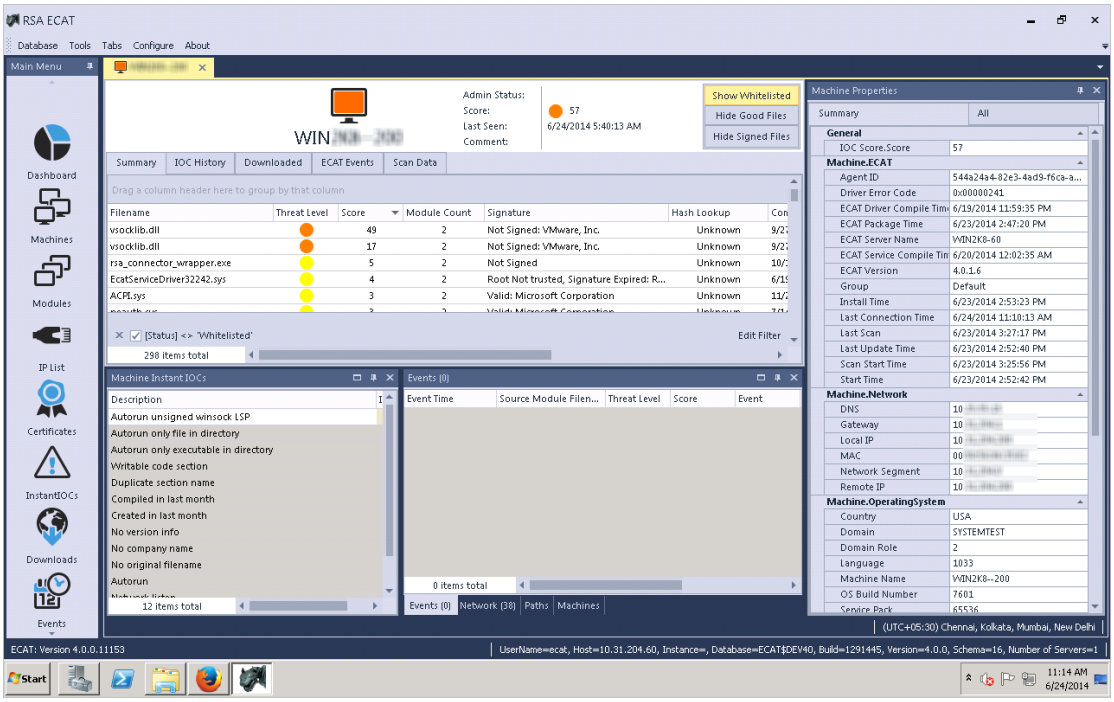


3. Wählen Sie **ECAT IOC-Suche** aus.
   Ein Dialogfeld fordert Sie auf, eine Anwendung auszuwählen.

4. Wählen Sie ECAT aus und klicken Sie auf **OK**.
   Das Dialogfeld „RSA ECAT-Konfiguration“ wird angezeigt.



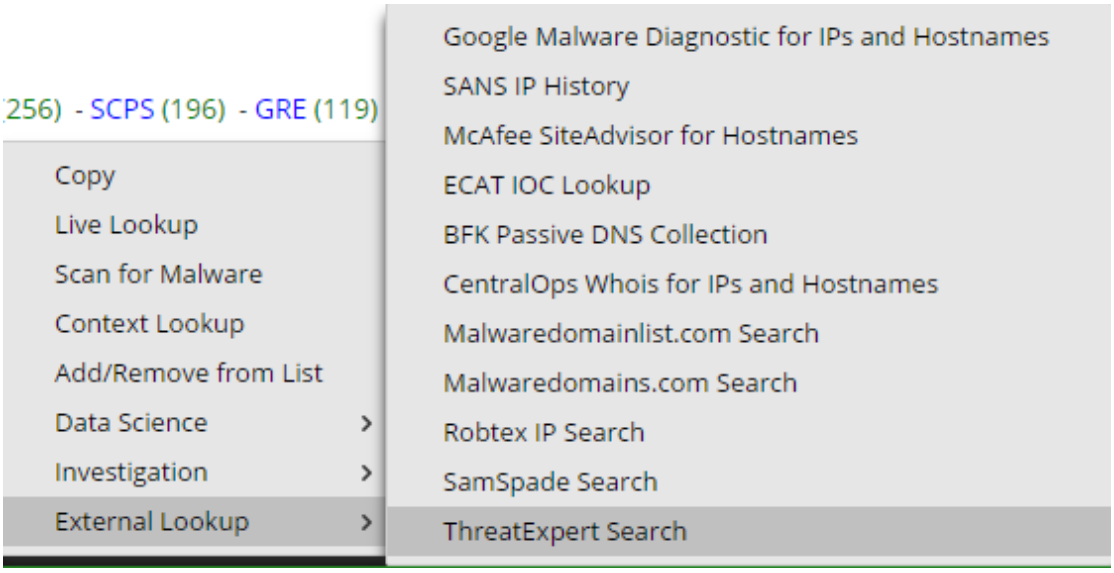
5. Geben Sie die den Benutzernamen und das Passwort ein, die für die Anmeldung am ECAT-Client erforderlich sind, und klicken Sie auf **Verbinden**
   . Der Drill-down-Punkt wird in RSA ECAT geöffnet.



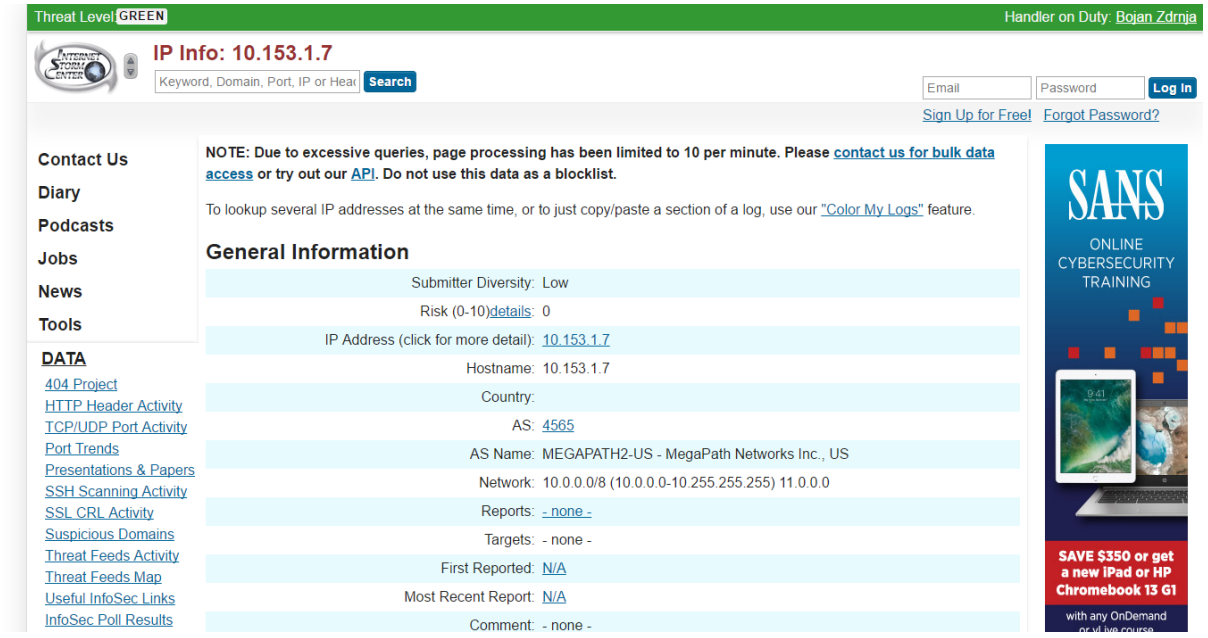
Starten weiterer externer Suchen

So starten Sie eine externe Suche (einen anderen als ECAT IOC) von Daten aus der Ansicht „Investigation > Navigieren“:

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.

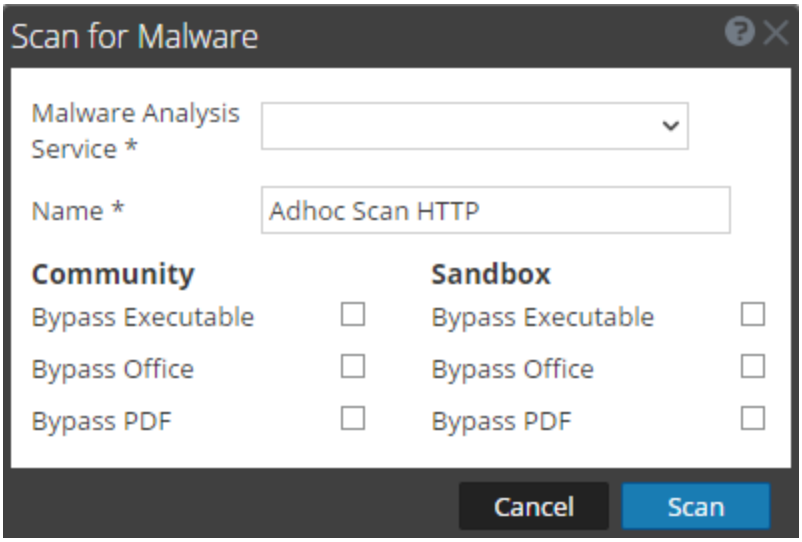


Starten eines Schadsoftwareanalyse-Scans in der Navigationsansicht

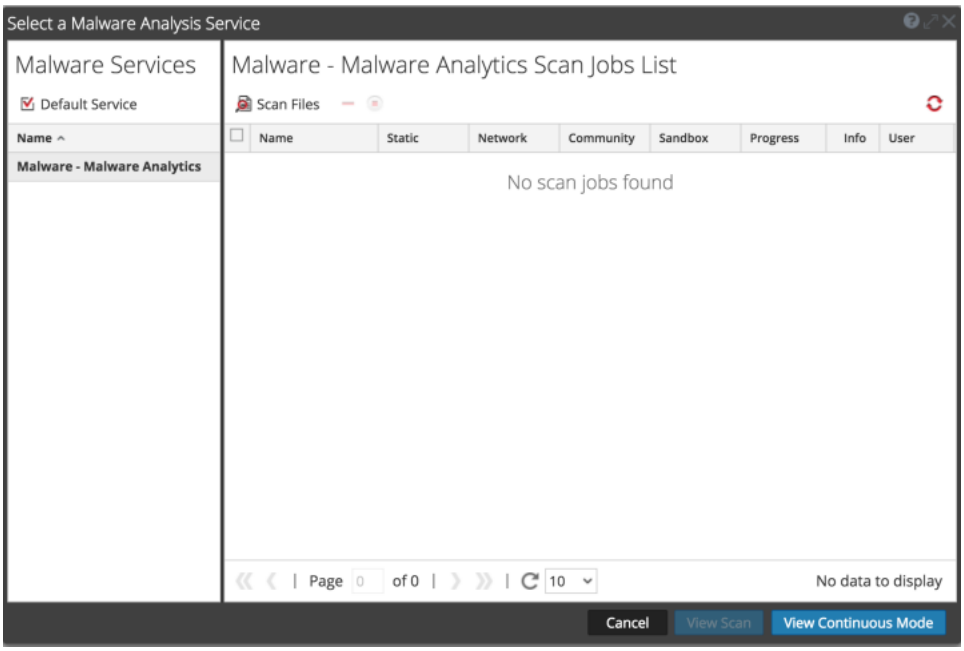
Analysten können aus Investigation heraus einen Malware Analysis-Scan nach Bedarf starten, indem sie einen Service und einen Metawert und dann eine Option aus dem Kontextmenü auswählen. Wenn die Abfrage abgeschlossen ist, stehen die gescannten Daten für die Schadsoftwareanalyse zur Verfügung.

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

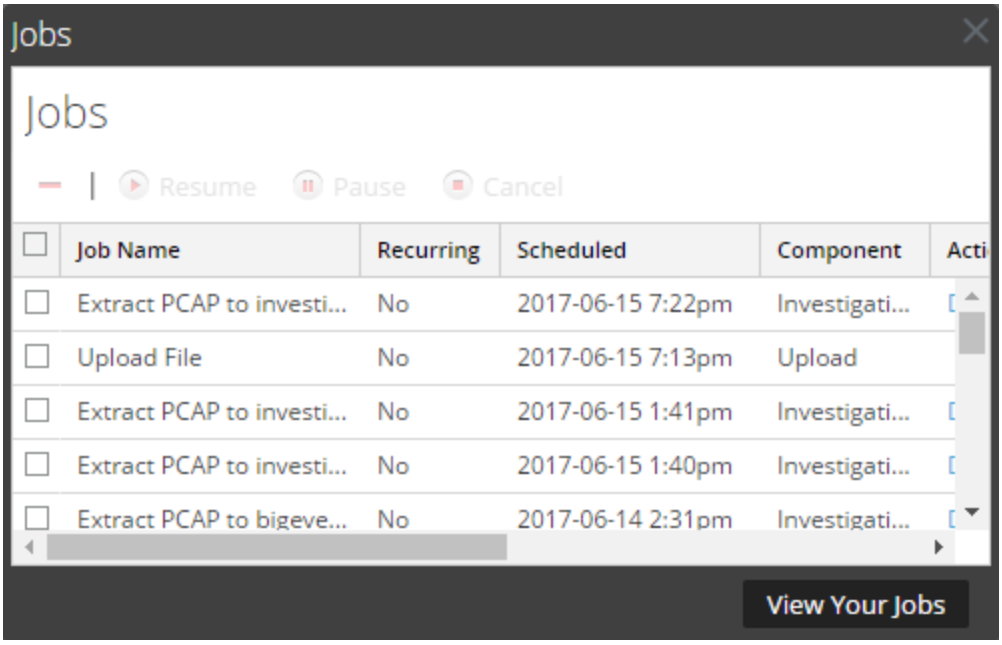
1. Klicken Sie mit der rechten Maustaste auf einen Metawert (zum Beispiel OTHER, DNS oder FTP) und wählen Sie im Kontextmenü **Auf Schadsoftware scannen** aus.
   Das Dialogfeld „Auf Schadsoftware scannen“ wird mit einem vorgeschlagenen Namen für den Scan nach Bedarf und ohne ausgewählten Service angezeigt.
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 Suite-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.

Managen von Context Hub-Listen und -Listenwerten in Investigate

Analysten können Listen und Listenwerte für die Context Hub-Erweiterung in den Ansichten „Navigation“ und „Ereignisse“ hinzufügen. Wenn der Service „Context Hub“ aktiviert und konfiguriert ist, stellt NetWitness Suite 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 „Investigation“-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.

Voraussetzungen

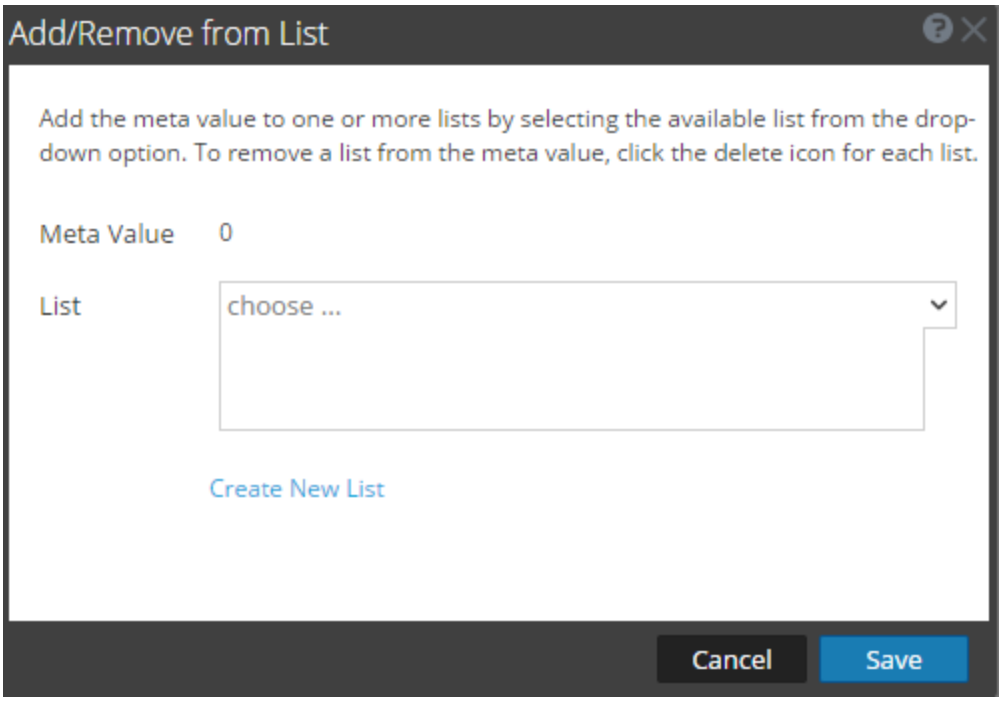
Damit ein Analyst Listen in „Investigation“ managen kann, muss der Administrator Folgendes tun:

- Den Service „Context Hub“ 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 in „Investigation“

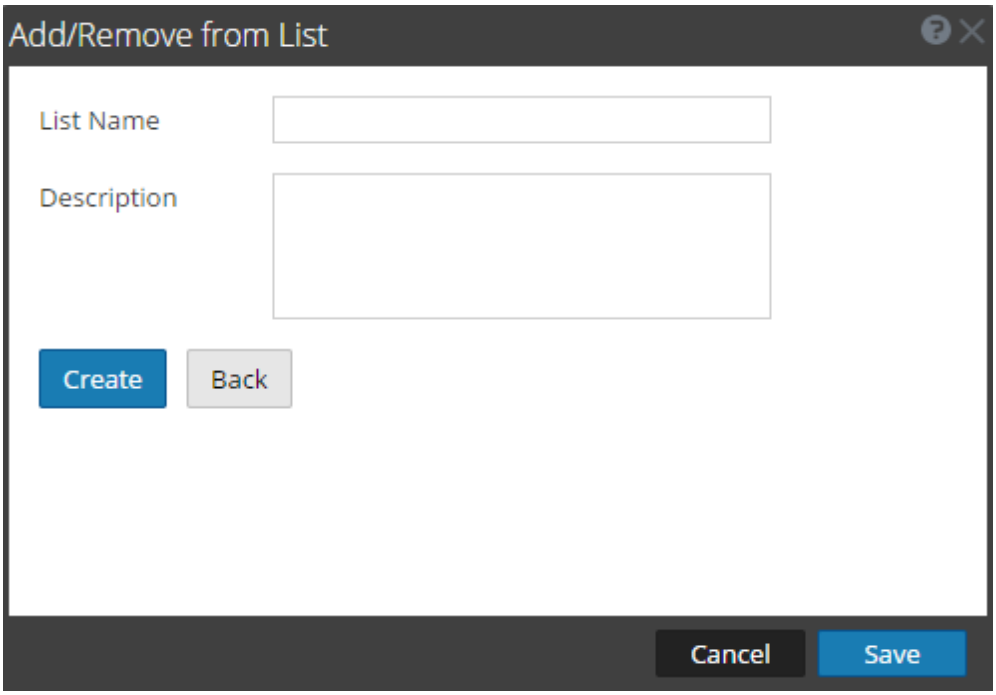
So entfernen Sie einen Metawert aus einer Liste:

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 in „Investigation“

So erstellen eine Context Hub-Liste in „Investigation“:

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.

Öffnen der Ereignisliste

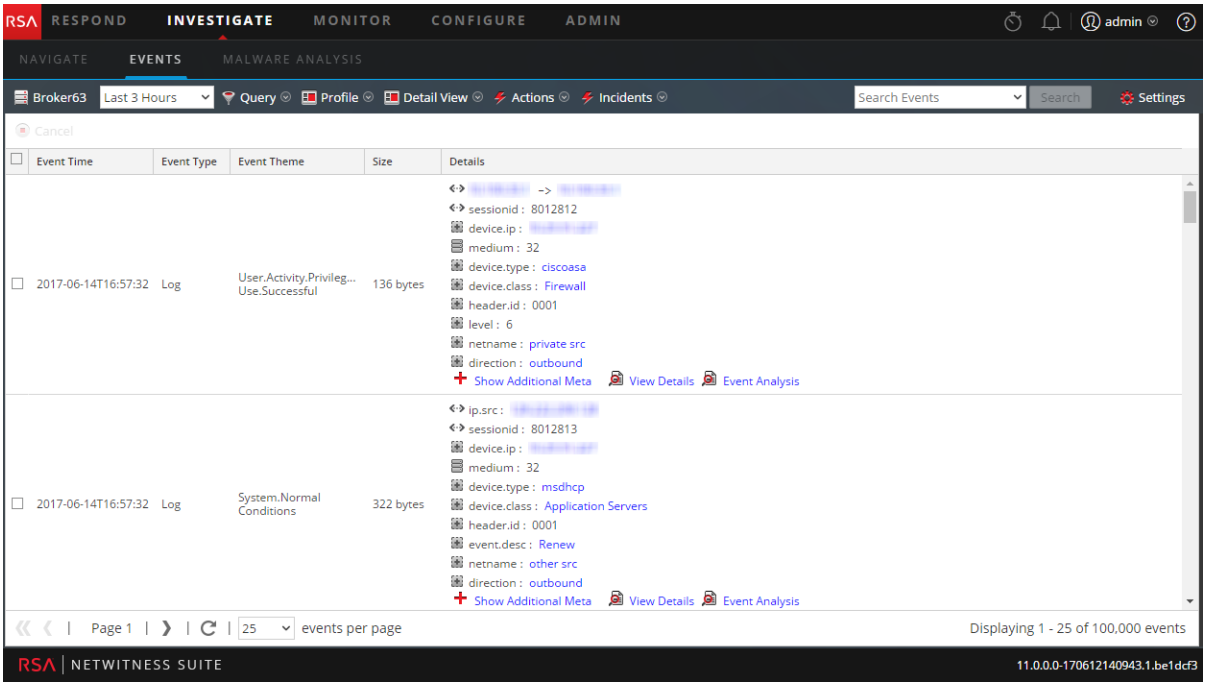
Analysten können in den Ansichten „Untersuchen“ > „Ereignisse“ .

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

1. Navigieren Sie zu **Untersuchen** > **Ereignisse**, um die Standardabfrage für den Standardservice zu verwenden.
   NetWitness Suite 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. Durch die Standardabfrage werden alle Ereignisse ausgewählt und in der Ansicht „Ereignisse“ erscheinen Ereignisse des ausgewählten Service, mit den ältesten Ereignissen zuerst.

2. Zeigen Sie die Ereignisse für einen bestimmten Metawert an, indem Sie zu **Untersuchen > Navigation** wechseln und auf einen Metawert unter einem Metaschlüssel klicken (der Wert erscheint als blauer Text), nachdem die Ereignisse im Bereich „Werte“ geladen wurden. In der Ansicht „Ereignisse“ werden die Ereignisse für den ausgewählten Metawert angezeigt.

Diese Abbildung zeigt ein Beispiel für die Detailansicht.



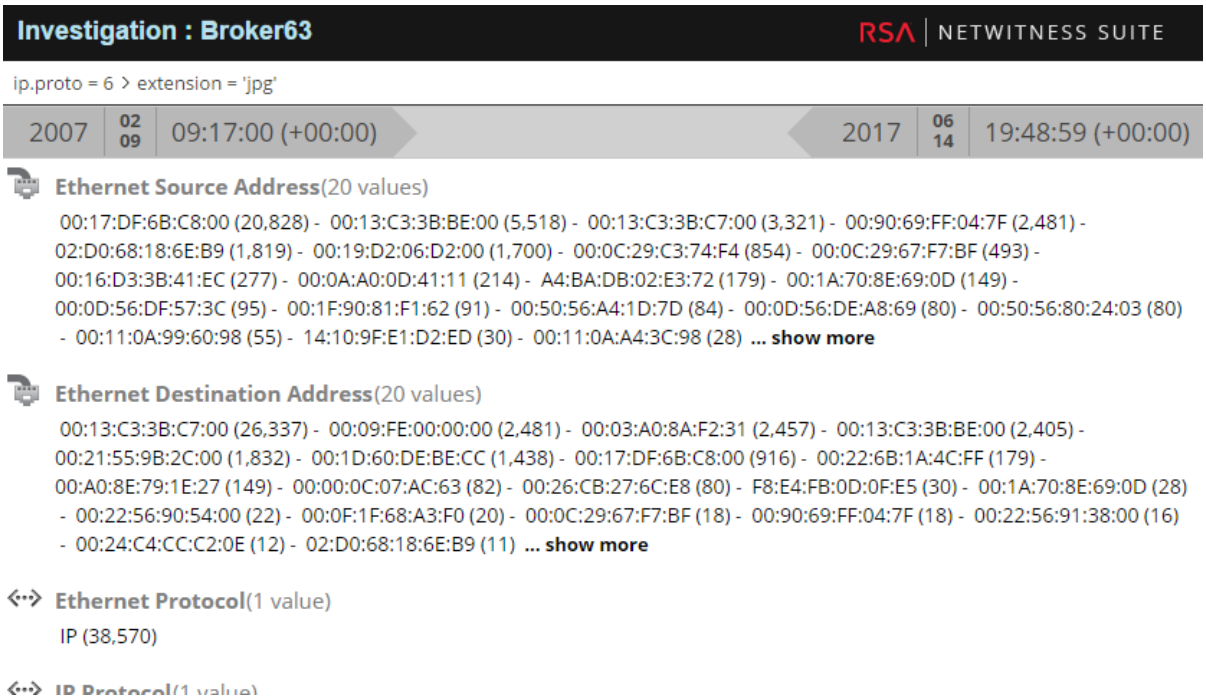
Sie können Abfragen, die Zeitbereicheinstellung und Profile verwenden, um die Ereignisse zu filtern, die in der Ereignisansicht aufgeführt sind. Von jedem der Ereignistypen in der Ereignisansicht aus können Sie Dateien extrahieren, Ereignisse exportieren, Protokolle exportieren und den Bereich Ereignisrekonstruktion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

Ausdrucken des aktuellen Drill-down-Punkts

In der Ansicht „Untersuchen > 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 **Untersuchen > 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.

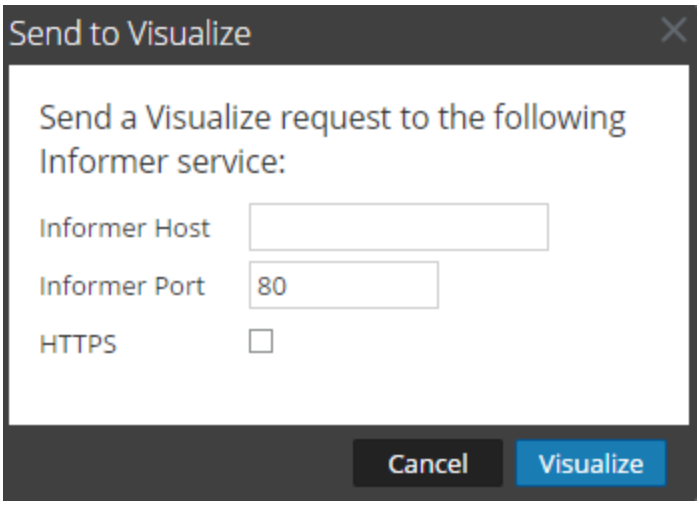
Visualisieren des aktuellen Drill-Punkts in Informer

Dieses Thema bietet Anweisungen zum Senden eines Drill-down-Punkts in der Ansicht „Ermittlung > 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 Suite 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 Suite-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.

Anzeigen von zusätzlichem Kontext für einen Datenpunkt

Aus einer Ereignisrekonstruktion oder dem Bereich „Werte“ in der Ansicht „Untersuchen“ können Sie Details und Informationen zu Elementen nachsehen, die im Zusammenhang mit einem Ereignis im Context Hub stehen. Die Daten aus konfigurierten Quellen wie RSA NetWitness Endpoint können Ihnen helfen, die Vorfälle zu verstehen.

Diese Elemente oder Entitäten sind Kennungen, z. B. eine IP-Adresse, ein Benutzername, ein Hostname, ein Domain-Name, ein Dateiname oder ein Datei-Hash. Zum Abrufen externer Informationen zu einer bestimmten Entität verwendet NetWitness Suite den Context Hub. 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. Z. B. kann Ihnen der Context Hub sagen, ob eine bestimmte Entität in Incidents, Warnmeldungen, Feeds oder Veröffentlichungen von Communityinformationen erwähnt wurde.

Bei Rechtsklick auf die Entität in Investigate fragt der Context Hub die konfigurierten Datenquellen nach relevanten Informationen ab. Der Bereich „Kontext“ wird auf der rechten Seite des Browser-Fensters geöffnet. Der Bereich „Kontext“ wird mit den Informationen aus dem Context Hub gefüllt, sobald diese verfügbar sind.

Um eine weitere Suche ausführen, klicken Sie mit der rechten Maustaste auf eine andere Entität und der Bereich „Kontext“ wird mit den Informationen zu dieser Entität aktualisiert.

Um den Bereich „Kontext“ zu schließen, klicken Sie auf das .

Im Bereich „Kontextabfrage“ können Sie einzelne Datenquellen anzeigen und weiter durchsuchen. Wenn Sie beispielsweise auf einen bestimmten Incident-Wert klicken, werden die spezifischen Incident-Details in der Ansicht „Incident Respond“ angezeigt.

Eine detaillierte Beschreibung der Informationen, die für jede Datenquelle im Bereich „Kontextabfrage“ angezeigt werden, finden Sie unter Bereich „Kontextabfrage“.

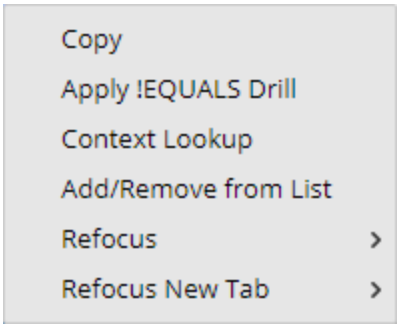
Bevor ein Analyst kontextbezogenen Informationen anzeigen kann, muss der Administrator Folgendes tun:

- Sicherstellen, dass der Analyst eine Rolle mit der Berechtigung `Context Lookup` hat, wie unter „Rollenberechtigungen“ und „Mangen von Benutzern mit Rollen und Berechtigungen“ im *Handbuch Systemsicherheit und Benutzerverwaltung* beschrieben wird.
- Fügen Sie den Context Hub-Service in RSA NetWitness Suite hinzu.
- Konfigurieren Sie Datenquellen für den Service „Context Hub“, wie im *Context Hub-Konfigurationsleitfaden* beschrieben.

Hinweis: Navigieren Sie zu Master Table of Contents für Version 11.0, um Dokumente zu NetWitness Suite 11.0 zu suchen.

So zeigen Sie Informationen im Bereich „Kontextübersicht“ an:

1. Suchen Sie in der Ansicht „Navigation“ oder „Ereignisse“ einen Metawert, für den Sie zusätzlichen Kontext anzeigen möchten, und bewegen Sie den Mauszeiger über den Metawert.
   Der Bereich **Kontexthighlights** wird mit einer kurzen Übersicht über den Typ der Kontextdaten angezeigt, die für die Datenquelle verfügbar sind: NetWitness Endpoint, Incidents, Warnmeldungen, Hosts, Dateien, Feeds und Live Connect.
2. Klicken Sie mit der rechten Maustaste auf einen Metawert und klicken Sie auf **Kontextabfrage**, um den Bereich „Kontextabfrage“ zu öffnen.

   Der Bereich „Kontextübersicht“ wird auf der rechten Seite des Browser-Fensters geöffnet. Der Bereich „Kontextübersicht“ wird mit den Informationen aus dem Context Hub gefüllt, sobald diese verfügbar sind.
3. Um Aktionen aus dem Bereich „Kontext“ auszuführen, klicken Sie auf eine Entität, z. B. IP-Adresse, und klicken Sie mit der rechten Maustaste.
   Folgende Optionen sind verfügbar: „Link in neuer Registerkarte öffnen“, „In Investigate abfragen“, „Link kopieren“, „Einfügen“, „Google-Abfrage“, VirusTotal-Abfrage“ und „In Endpoint abfragen“.

Untersuchen von Ereignissen

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

- Analysten, die Analysen mit NetWitness Suite 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 „Investigation > 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:

- Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion
- Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
- Kombinieren von Ereignissen aus geteilten Sitzungen
- Exportieren von Ereignissen
- Filter und Suchergebnisse in der Ansicht Ereignisse
- Managen von Spaltengruppen in der Ereignisansicht
- Rekonstruieren eines Ereignisses

Filter und Suchergebnisse in der Ansicht Ereignisse

Analysten können die Ereignisse in der Ansicht „Ereignisse“ filtern und, indem sie nach Ereignissen suchen oder den Service auswählen, auf dem Ereignisse angezeigt werden sollen, den Zeitbereich festlegen und Metadaten abfragen.

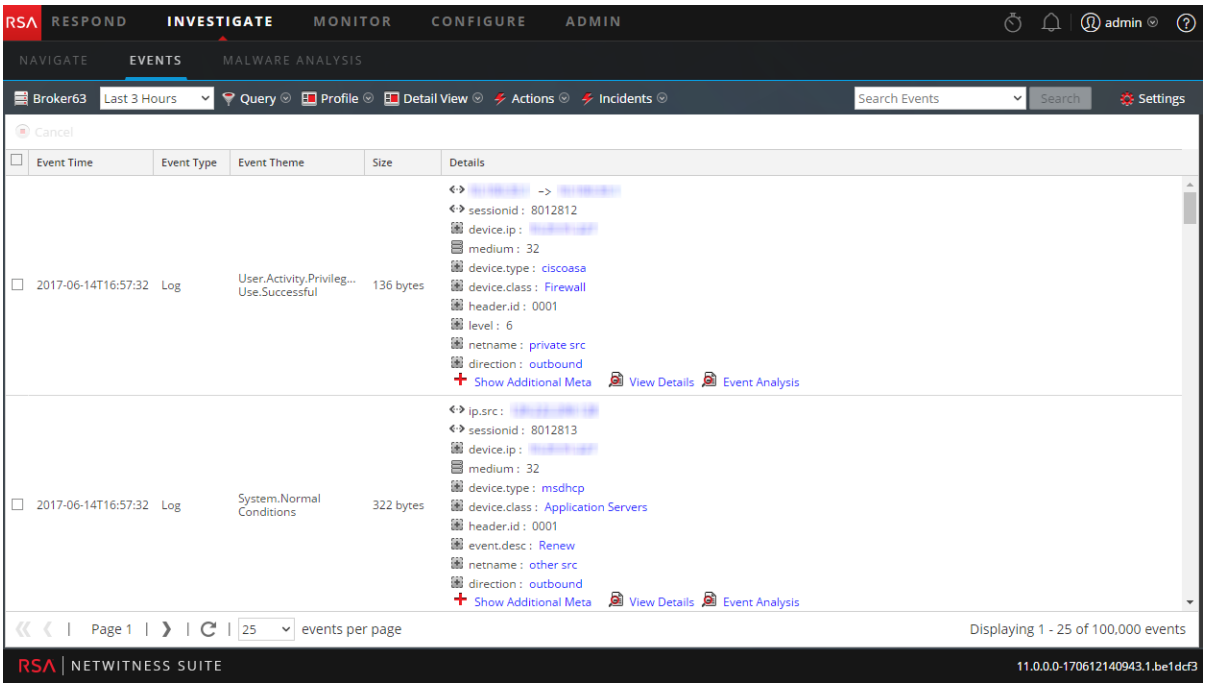
Wenn Sie die Ansicht „Ereignisse“ von einem Drill-down-Punkt der Ansicht „Navigation“ aus geöffnet haben, wird sie standardmäßig in der „Details“-Ansicht der Ereignisse geöffnet. Analysten, die nicht über die Berechtigungen zum Verwenden der Ansicht Navigieren verfügen, können die Services direkt in 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

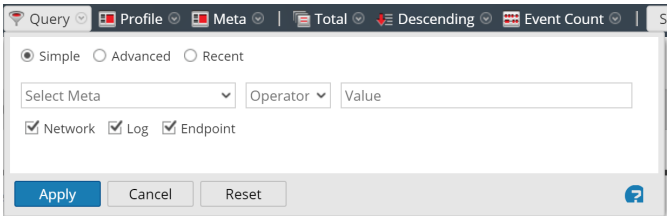
So filtern Sie die in der Ansicht „Ereignisse“ angezeigten Daten:

1. Wählen Sie in der Ansicht **Untersuchen** die Ansicht **Ereignisse** aus.
   Die Ansicht „Ereignisse“ wird angezeigt.

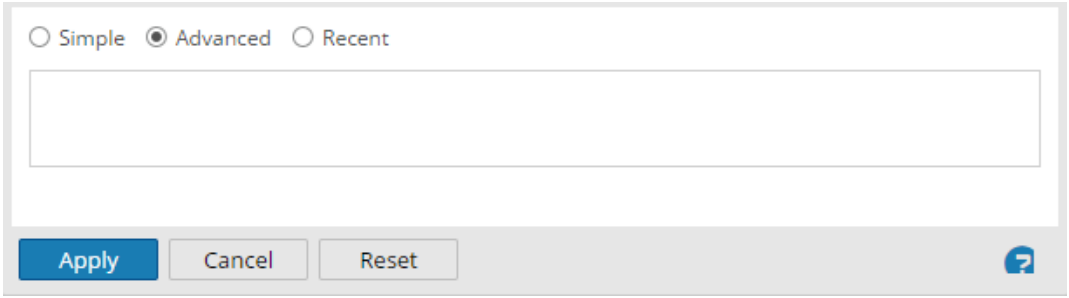


2. Wählen Sie einen anderen Zeitraum als den Standardzeitraum (**Letzte 3 Stunden**) aus, indem Sie auf der Symbolleiste in das Feld „Zeitraum“ klicken und einen Wert auswählen. Zum Beispiel **Letzte Stunde**.
   Die Ansicht „Ereignisse“ wird mit dem ausgewählten Zeitraum aktualisiert.

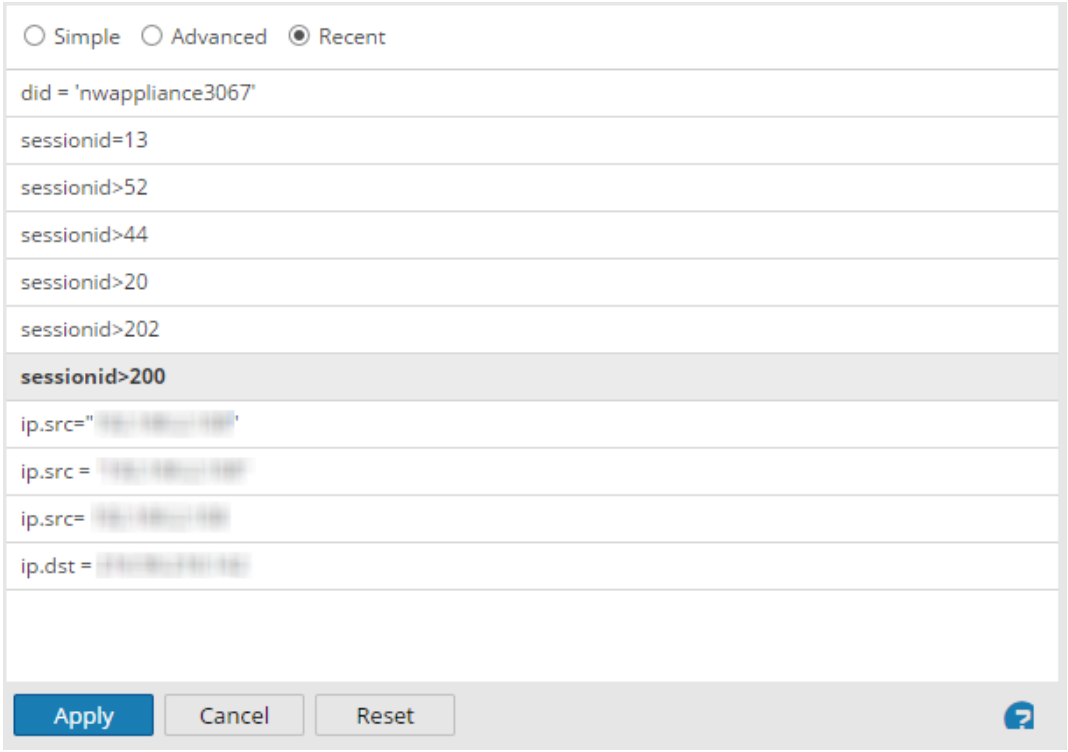
3. Klicken Sie zum Eingeben einer Abfrage für den ausgewählten Service und Zeitraum auf der Symbolleiste auf **Abfrage**.
   Das Dialogfeld „Abfrage“ wird mit ausgewählter Option „Einfach“ angezeigt.



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 Suite die Ergebnisse.

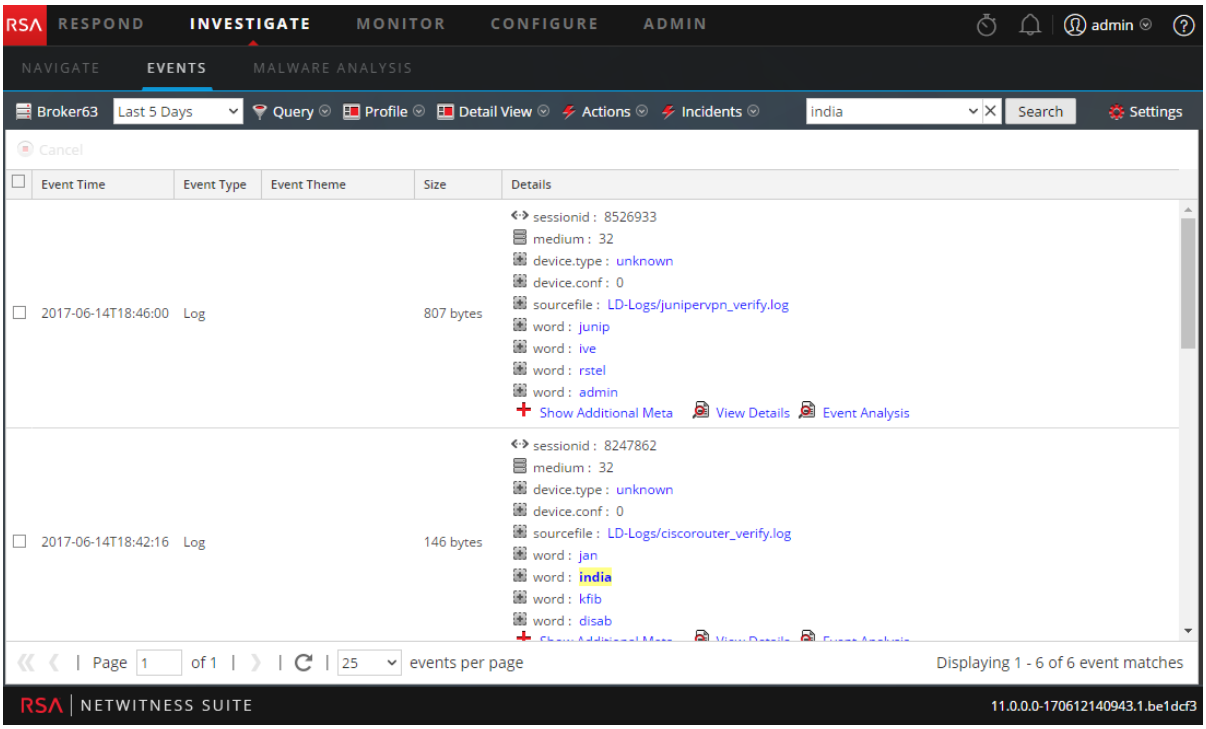
Suchen nach Ereignissen in der Ansicht „Ereignisse“

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. Beachten Sie, dass die Treffer der Suche bei Ereignisrekonstruktionen nicht markiert werden.



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 Ereignisansicht zurückzukehren, klicken Sie im Suchfeld auf das **X**.

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 Suite 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

In NetWitness Suite 10.5 und höher beendet der Decoder 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.

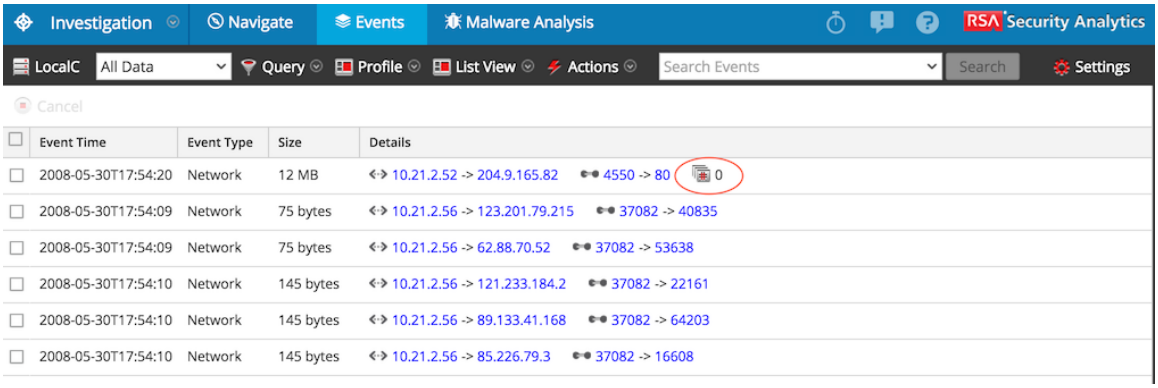
Hervorhebung von Sitzungsfragmenten

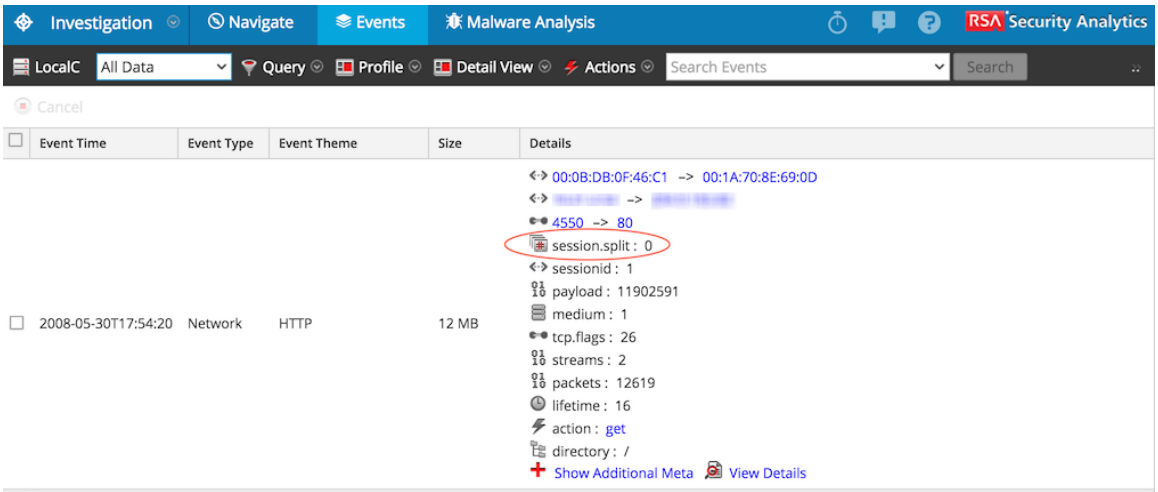
Jedes Sitzungsfragment verfügt über zusätzliche Metadaten: `session.split`. Der Wert der `session.split`-Metadaten eines bestimmten Sitzungsfragments gibt an, wie viele Fragmente vor diesem Fragment existieren. Beim Anzeigen einer Sitzung in der Ansicht „Ereignisse“ identifizieren die `session.split`-Metadaten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

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`-Metadaten 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 Zahlen unten zeigen die Ereignislistenansicht und die Detailansicht der Ereignisse 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:

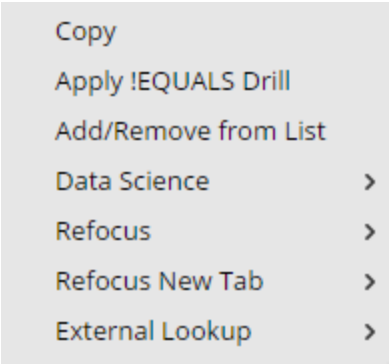
1. Identifizieren von Sitzungen, die Fragmente einer Netzwerksitzung sind.
2. Anzeigen aller Sitzungsfragmente einer bestimmten Netzwerksitzung oder eines einzigen Sitzungsfragments.
3. Exportieren der Pakete für die gesamte Netzwerksitzung als eine einzige PCAP-Datei.

Suchen und Kombinieren von Fragmenten

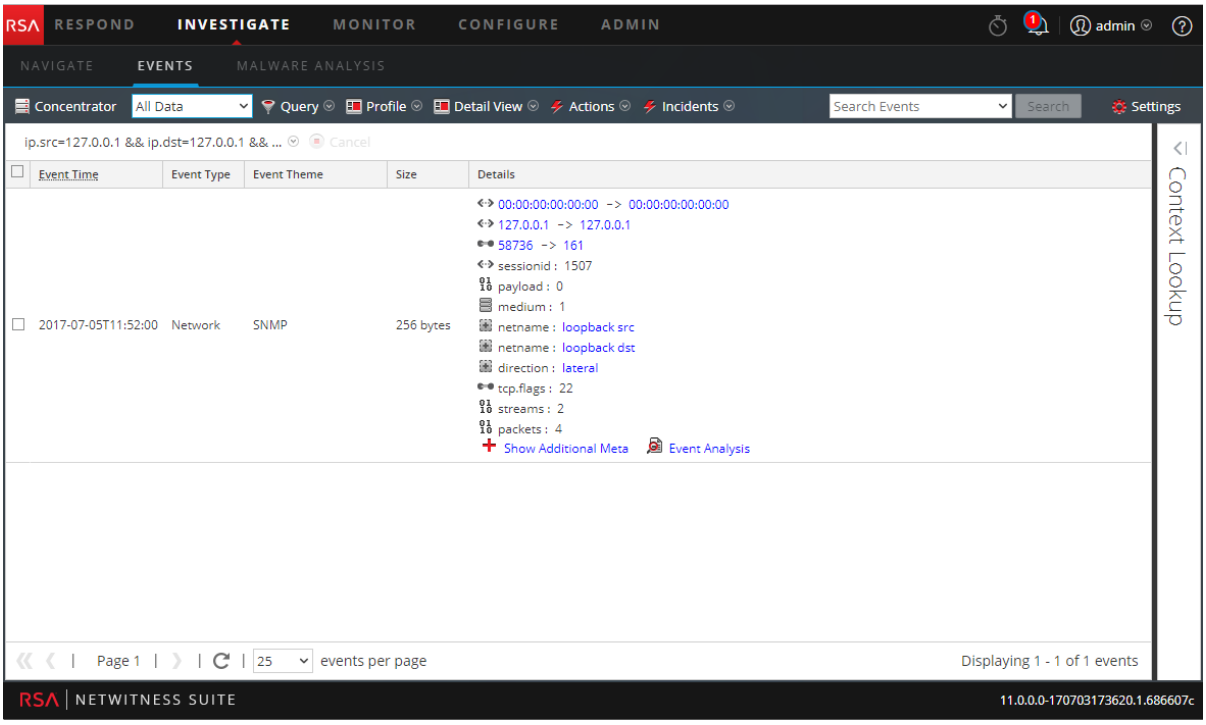
Innerhalb der Ansicht „Ereignisse“ können Sie nach Sitzungsfragmenten suchen, indem Sie die Kontextmenüoptionen „Neu fokussieren > Sitzungsfragmente finden“ verwenden. NetWitness Suite erstellt mithilfe der Quell- und Zieladressen und -ports der ausgewählten Sitzung eine Abfrage und zeigt alle Sitzungen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

So suchen Sie Sitzungsfragmente:

1. Klicken Sie in der Ansicht **Investigation > 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`.
   Das Kontextmenü wird angezeigt.



2. Wählen Sie **Neu fokussieren > Sitzungsfragmente finden** oder **Neue Registerkarte neu fokussieren > Sitzungsfragmente suchen** aus.
   NetWitness Suite füllt die Liste „Ereignisse“ 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.

Managen von Spaltengruppen in der Ereignisansicht

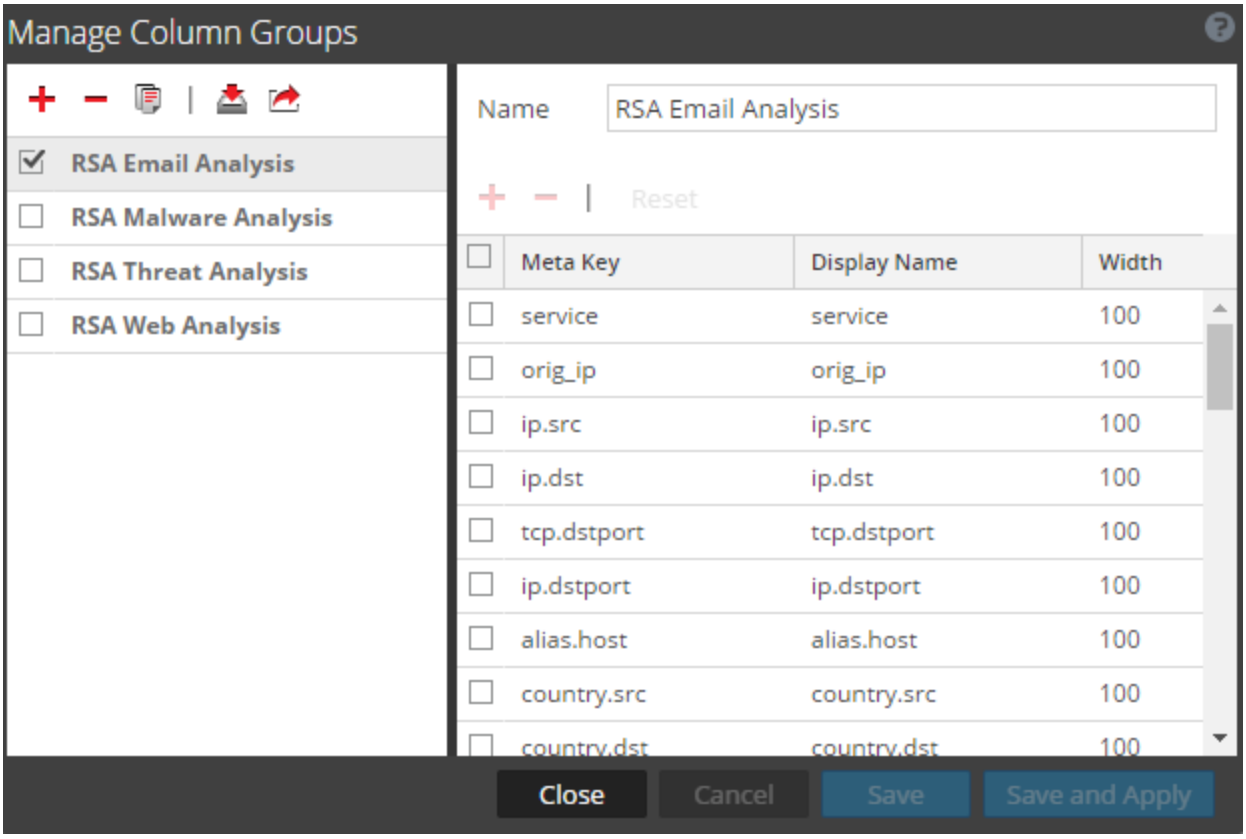
In diesem Thema erhalten Sie Anweisungen zum Erstellen und Managen von benutzerdefinierten Spaltengruppen für die Anzeige von Daten in der Ansicht „Ereignisse“.

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: 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. Wählen Sie in der Ansicht **Ermittlung** die Ansicht **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.

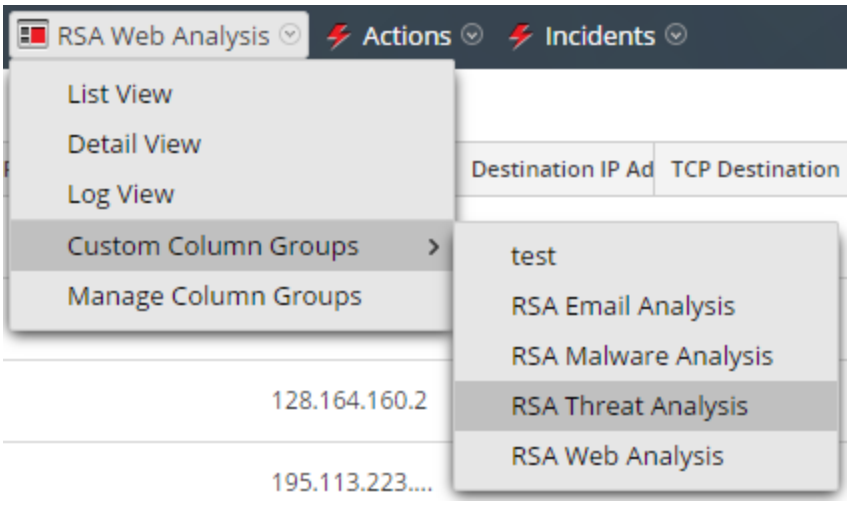


3. Klicken Sie zum Hinzufügen einer neuen Spaltengruppe im Bereich „Spaltengruppe“ auf + und geben Sie den Namen der Spaltengruppe im angezeigten Feld ein.
4. Auf der rechten Seite wird der Bereich für die Spaltendefinition geöffnet, in dem der Gruppenname bereits ausgefüllt ist. Sie können den Gruppennamen bearbeiten.
5. Klicken Sie zum Hinzufügen einer Spalte zur Gruppe auf +. Klicken Sie dann im leeren Feld **Metaschlüssel**, um die Drop-down-Liste **Metaschlüssel** anzuzeigen.
6. Wählen Sie ein Metadatenschlüsselfeld aus der Liste aus und wiederholen Sie diesen Schritt solange, bis die Spalte vollständig ist.
7. (Optional) Klicken Sie zum Löschen eines Metadatenschlüssels aus der Spaltengruppe auf −.
8. (Optional) Wenn Sie die Reihenfolge ändern möchten, in der die Spalten in der Ereignisliste angezeigt werden, ziehen Sie die Metadatenschlüssel an die gewünschte Position.
9. (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.

10. (Optional) Klicken Sie auf **Zurücksetzen**, um die vorherigen Spalteneinstellungen wiederherzustellen und alle Änderungen rückgängig zu machen.
11. 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 benutzerdefinierten Spaltengruppe

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 benutzerdefinierten Gruppen aus dem Untermenü aus.
   Die Ereignisansicht wird aktualisiert und zeigt die benutzerdefinierte Spaltengruppe an.

Rekonstruieren eines Ereignisses

Beim Anzeigen einer Ereignisliste in der Ansicht „Ereignisse“ können Sie zuverlässig eine Rekonstruktion des Ereignisse in einem lesbaren Format 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.

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

> **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.

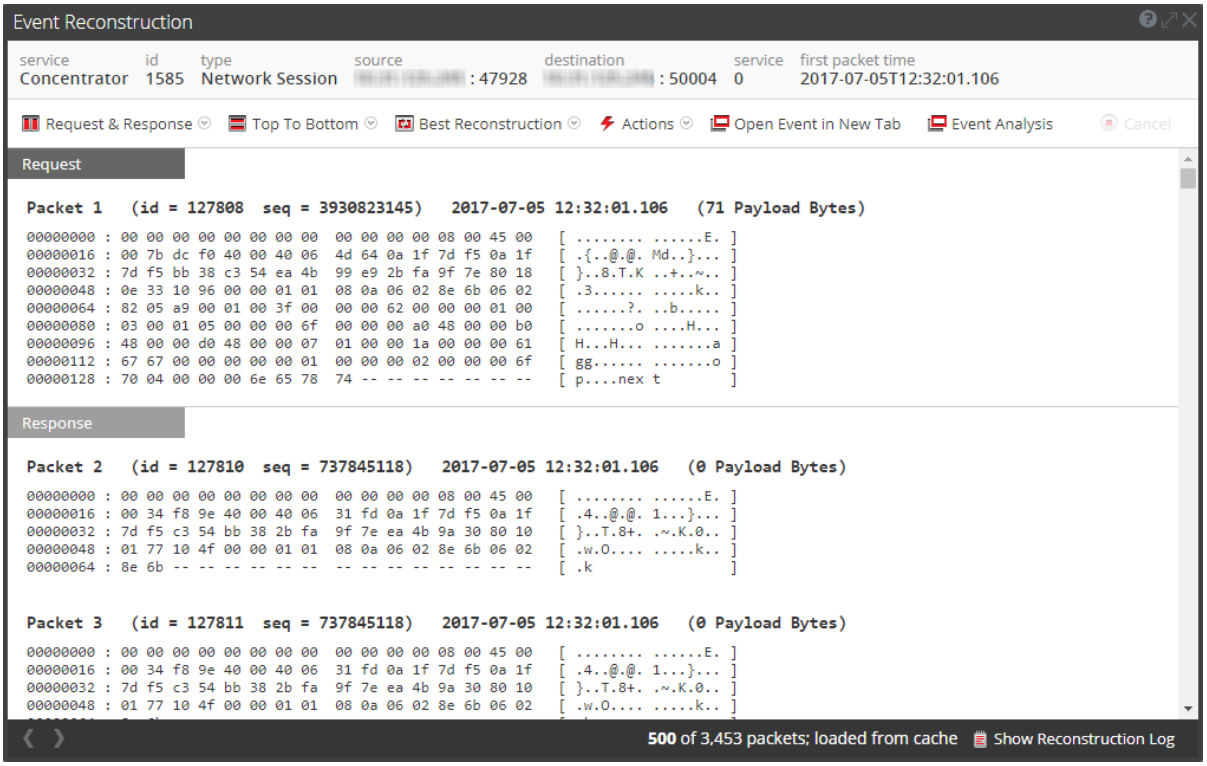
- das Ereignis in einem separaten Fenster oder auf einer separaten Registerkarte anzeigen (je nach Browserkonfiguration)
- Wenn Sie die Rekonstruktion als Vorschau in der aktuellen Ansicht anzeigen, können Sie mithilfe der Navigationsschaltflächen unten links zum nächsten Ereignis vor- bzw. zum vorherigen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

Hinweis: Die Rekonstruktionseinstellungen und die Rekonstruktionscacheeinstellungen ermöglichen es einem Administrator, die Anwendungsperformance für das Modul „Investigation“ zu verwalten. Da Analysten Sitzungen, die sie untersuchen, rekonstruieren, können sich zwei Situationen auf Leistung 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 Suite alle 24 Stunden den Cache, dessen Daten älter als ein 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

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, indem Sie ein zu rekonstruierendes Ereignis und dann **Aktionen > Ereignis anzeigen > Inline-Vorschau** auswählen.

   Das Dialogfeld „Ereignisrekonstruktion“ wird in der gleichen Ansicht in einem Pop-up-Fenster geöffnet. Standardmäßig wird in NetWitness Suiteentweder 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 auf der Symbolleiste „Ereignisrekonstruktion“ können Sie die Rekonstruktionsmethode ändern, Ergebnisse nebeneinander anzeigen, ein Ereignis exportieren, einen E-Mail-Anhang öffnen, Dateien extrahieren und das Ereignis auf 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.

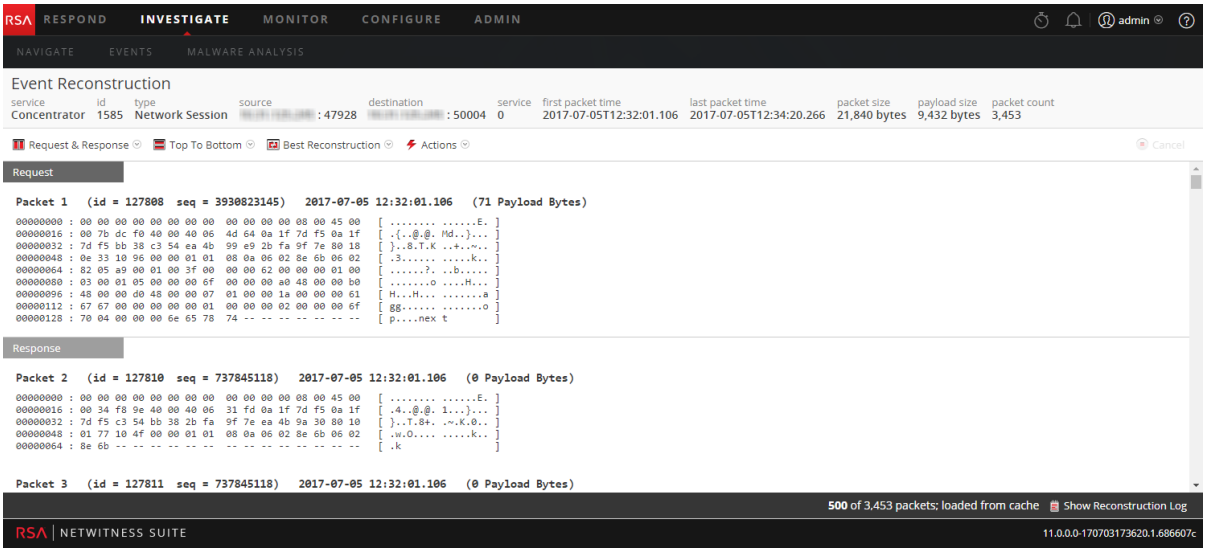


4. Um eine Rekonstruktion des nächsten Ereignisses in einer Vorschau anzuzeigen, klicken Sie auf . Um eine Rekonstruktion des vorherigen Ereignisses anzuzeigen, klicken Sie auf .
5. Führen Sie einen der folgenden Schritte aus, um eine Ereignisrekonstruktion in einer neuen Registerkarte zu öffnen:

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 auf 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 auf der Symbolleiste **Ereignisrekonstruktion** auf **Beste Rekonstruktion**.
2. Wählen Sie im 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 auf 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 auf der Symbolleiste des Abschnitts **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:

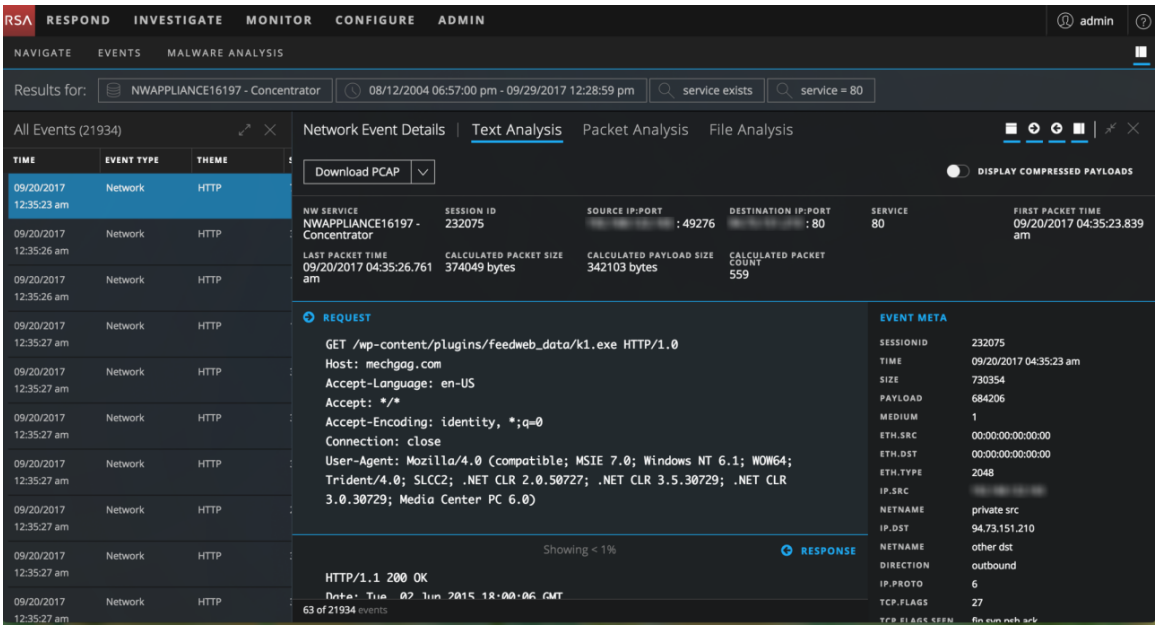
1. Klicken Sie auf der Symbolleiste des Abschnitts **Ereignisrekonstruktion** auf **Aktionen**.
2. Klicken Sie auf **Dateien extrahieren**.
   Das Dialogfeld „Dateiextraktion“ wird angezeigt.
3. Wählen Sie die Typen der zu extrahierenden Dateien aus und klicken Sie auf **OK**.
4. Der Job wird geplant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

Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“

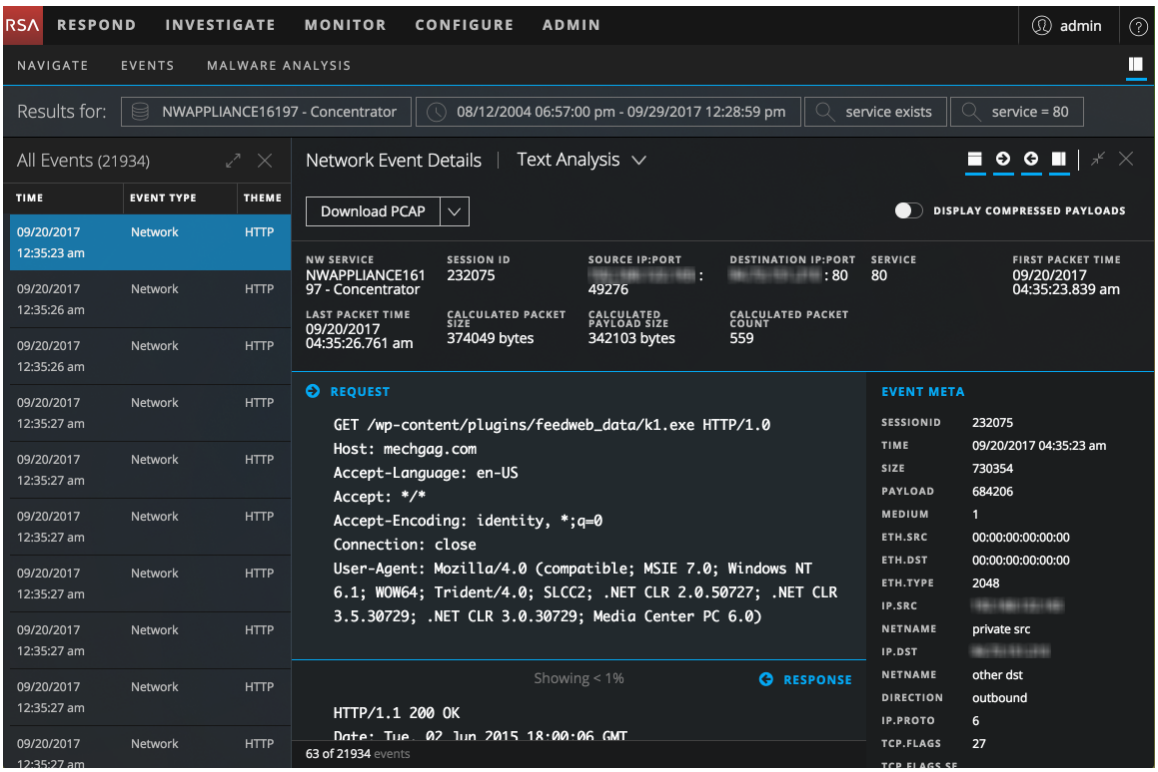
Bei der Suche nach möglichen Bedrohungen in erfassten Netzwerkdaten können Sie Drill-downs an verschiedenen interessanten Punkte in den Daten durchführen. Wenn eine bestimmte Sitzung verdächtige Ereignisse enthält, können Sie die Liste der Ereignisse für die Sitzung untersuchen und Sie können auch eine Rekonstruktion des Ereignisses mit Funktionen, mit denen Sie Muster identifizieren können, sicher anzeigen. (Die verschiedenen Methoden des Zugriffes auf die Ansicht „Ereignisanalyse“ finden Sie unter Untersuchen von Ereignissen) Dieses Kapitel enthält Anweisungen für das Arbeiten in der Ansicht „Ereignisanalyse“.

In der Ansicht „Ereignisanalyse“ können Sie das Format für die Rekonstruktion auswählen: Paketanalyse, Dateianalyse oder Textanalyse. Wenn der Metaschlüssel `medium` ein Ereignis als Protokollereignis oder Endpunktereignis markiert (abfragen als `medium=32`), ist nur die Textanalyse verfügbar. Die Standardrekonstruktion für Netzwerkereignisse ist Textanalyse. Jedoch überschreibt bei einem Netzwerkereignis das zuletzt geöffnete Rekonstruktionsformat die Standardeinstellung.

Diese Abbildung ist ein Beispiel für den Bereich „Netzwerkereignisdetails: Paketanalyse“ 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.



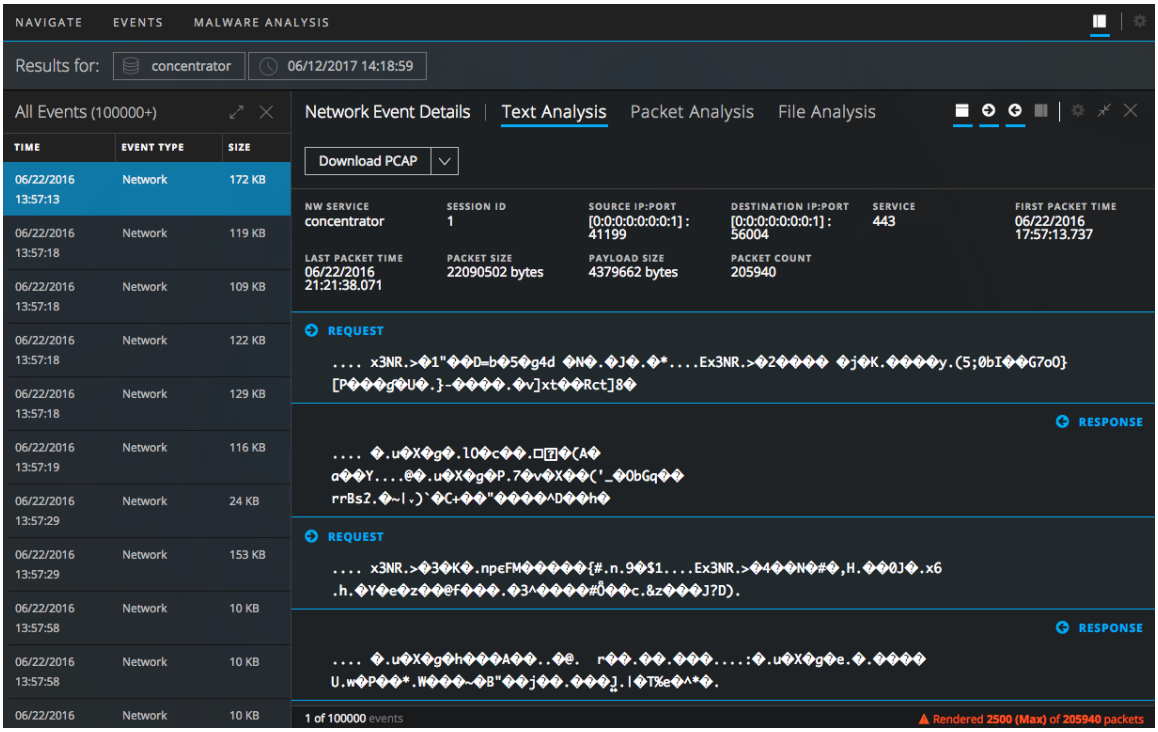
Innerhalb jeder Analyseart sind viele Einstellungen für die Optimierung Ihrer Analyse verfügbar. Wenn Sie eine Einstellung ändern, wird die Einstellung zwischen Browseraktualisierungen und Anmeldungen im selben Browser beibehalten. Dies sind die beibehaltenen Einstellungen:

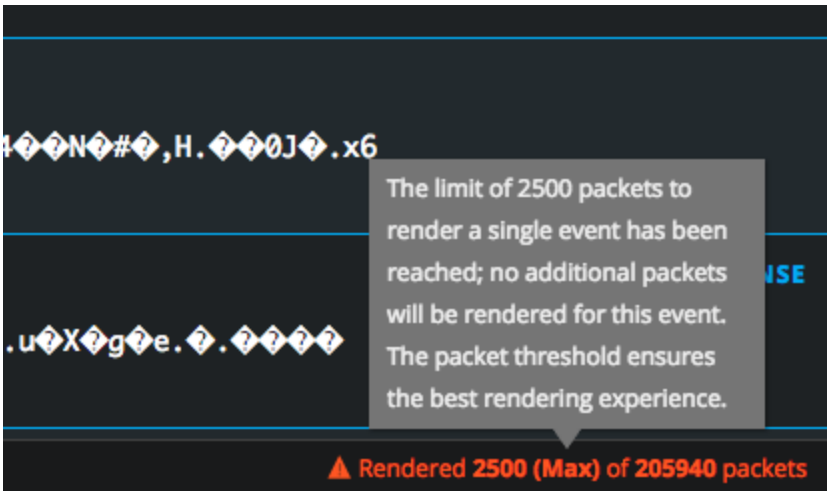
- Die aktuell ausgewählte Rekonstruktion: Textanalyse, Paketanalyse oder Dateianalyse.
- Ob der Bereich „Ereignis-Metadaten“ offen oder geschlossen ist.
- Ob der Ereignis-Header offen oder geschlossen ist.
- Ob die Anforderung oder die Antwort oder beide angezeigt werden.
- Ob Paketnutzlasten im Bereich Paketanalyse angezeigt werden.
- Ob schattierte Byte im Bereich Paketanalyse angezeigt werden.
- Ob andere gängige Dateitypen im Bereich Paketanalyse hervorgehoben sind.
- 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.

Der Bereich Textanalyse für einige Netzwerkereignisse kann sehr groß sein. Um die beste Wiedergabe sicherzustellen, ist die Anzahl der Pakete, die in einem einzigen Ereignis dargestellt werden können, auf 2500 beschränkt. Wenn im Bereich Textanalyse nicht alle Pakete angezeigt werden, ist in der Fußzeile angegeben, dass das Limit der 2500 Pakete erreicht wurde. Für dieses Ereignis werden keine zusätzlichen Pakete dargestellt. Diese Abbildung zeigt eine Rekonstruktion, die 205940 Pakete besitzt, wobei nur 2500 Pakete dargestellt werden. Für diese Rekonstruktion werden keine weiteren Pakete dargestellt.





Hinweis: Einige Netzwerkereignisse weisen eine große Anzahl von Paketen auf, aber eine sehr kleine Nutzlast. Wenn die gesamte Nutzlast in den ersten 2500 Paketen enthalten ist, wird in diesem Fall die Definition der Anzeige aller Pakete erfüllt. Es wird keine Meldung angezeigt, dass nicht alle Pakete angezeigt werden.

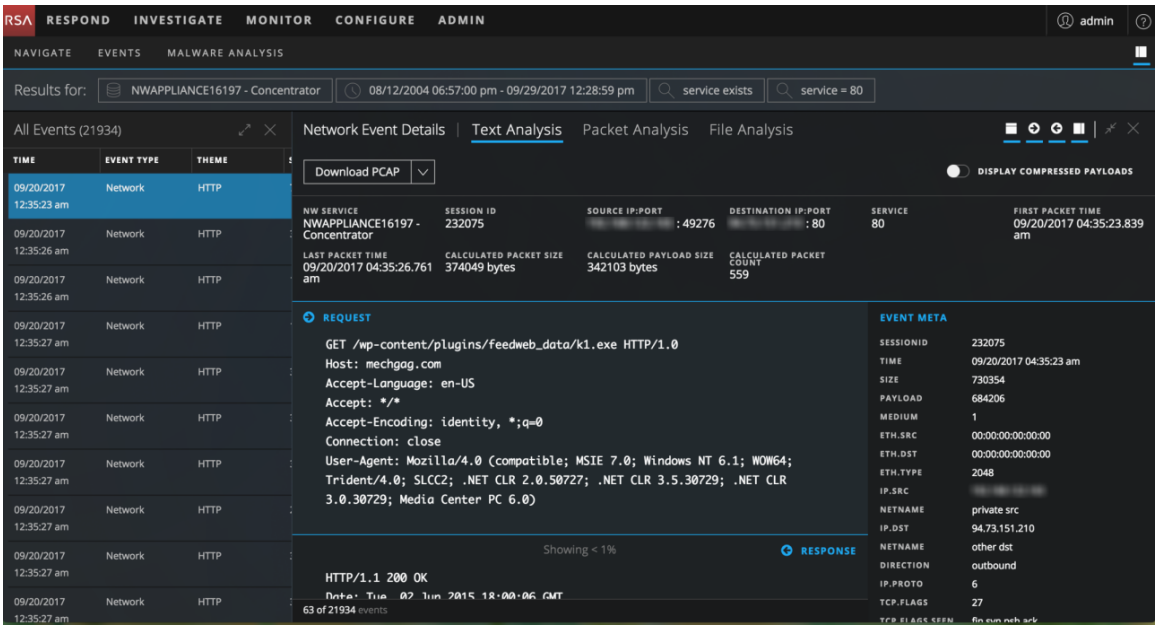
Im Bereich Textanalyse werden Netzwerkereignisse, Protokollereignisse und Endpunktereignisse unterschiedlich angezeigt.

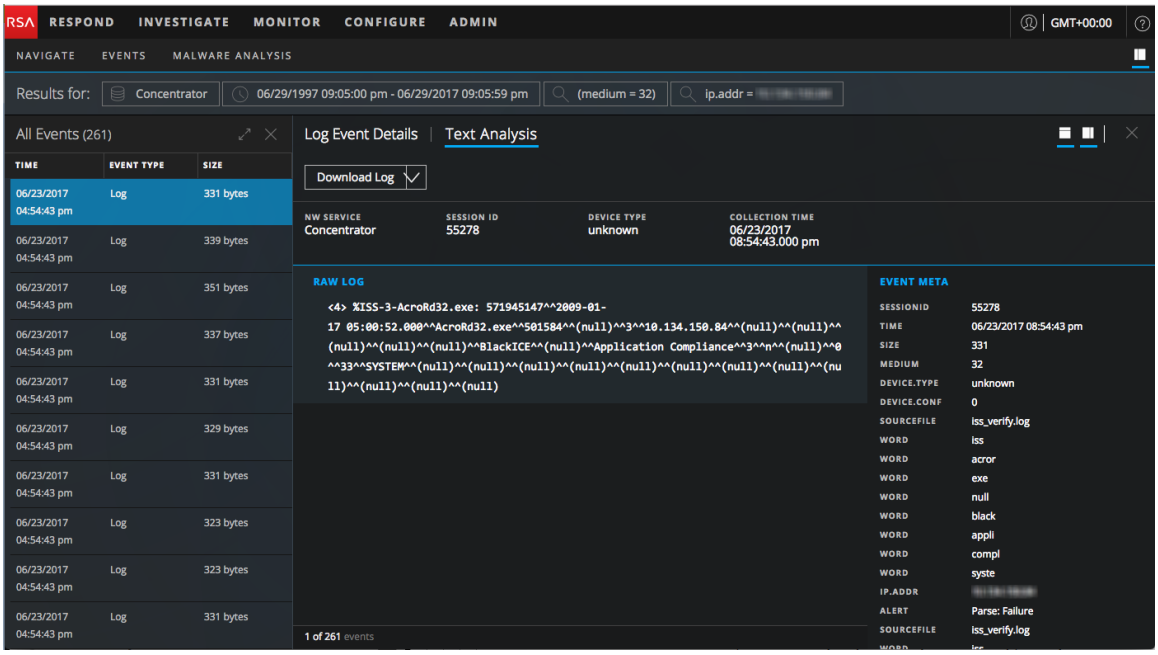
- Für Netzwerkereignisse stellt Investigate die Richtung des Pakets (Anforderung oder Antwort) und die Inhalte jedes Pakets im Textformat bereit. Wenn Sie ein Netzwerkereignis rekonstruieren, ist der BereichTextanalyse scrollbar. Wenn Sie einen Bildlauf durchführen, bleiben die Informationen zur Identifizierung des Texts sowie die Anforderungs- und Antwortbezeichnungen sichtbar, anstatt dass aus der Ansicht herausgescrollt wird.
- Protokollereignisse, (filtern nach `medium = 32` und `nwe.callback_id does not exist`) und Endpunktereignisse (filtern nach `medium = 32` und `nwe.callback_id exists`) haben keine Anforderung oder Antwort. Nur das Rohereignis wird im Bereich Textanalyse angezeigt.

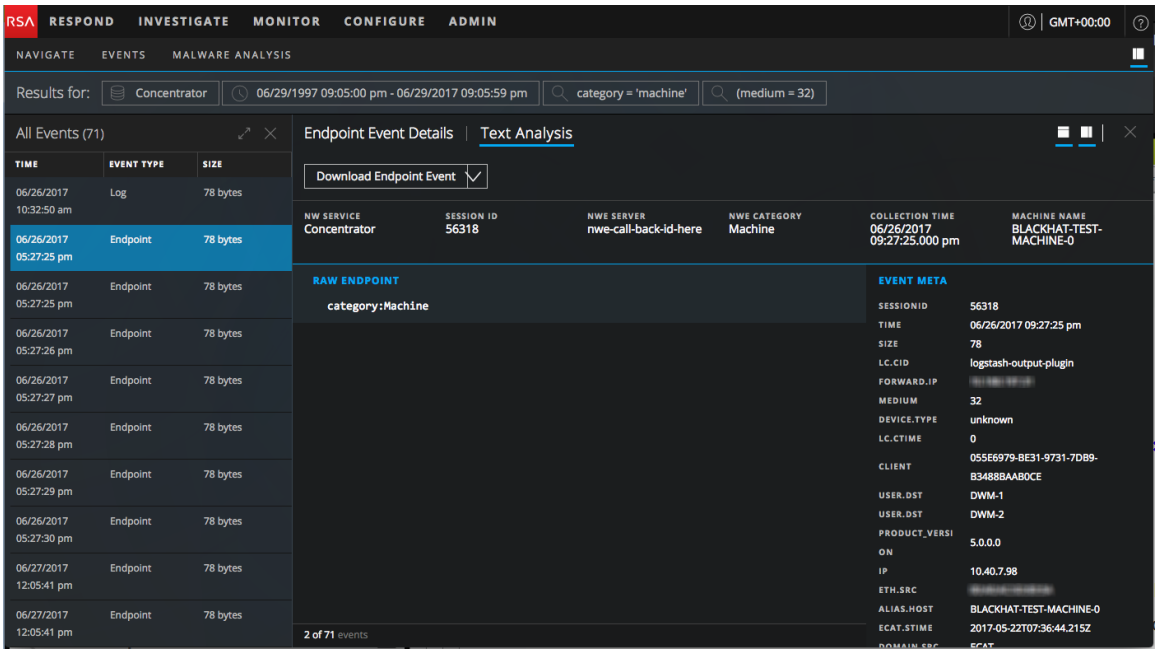
Für jeden Ereignistyp (Netzwerk, Protokoll oder Endpunkt) gibt es einige Unterschiede:

- 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.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
NAVIGATE
EVENTS
MALWARE ANALYSIS
Results for:
NWAPPLIANCE16197 - Concentrator
08/12/2004 06:57:00 pm - 09/29/2017 12:28:59 pm
service exists
service = 80
All Events (21934)
TIME
EVENT TYPE
THEME
Network Event Details
Text Analysis
Packet Analysis
File Analysis
Download PCAP
DISPLAY COMPRESSED PAYLOADS
NW SERVICE
NWAPPLIANCE16197 - Concentrator
SESSION ID
232075
SOURCE IP:PORT
: 49276
DESTINATION IP:PORT
: 80
SERVICE
80
FIRST PACKET TIME
09/20/2017 04:35:23.839 am
LAST PACKET TIME
09/20/2017 04:35:26.761 am
CALCULATED PACKET SIZE
374049 bytes
CALCULATED PAYLOAD SIZE
342103 bytes
CALCULATED PACKET COUNT
559
REQUEST
GET /wp-content/plugins/feedweb_data/k1.exe HTTP/1.0
Host: mechgag.com
Accept-Language: en-US
Accept: */*
Accept-Encoding: identity, *;q=0
Connection: close
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Showing < 1%
RESPONSE
HTTP/1.1 200 OK
63 of 21934 events
EVENT META
SESSIONID 232075
TIME 09/20/2017 04:35:23 am
SIZE 730354
PAYLOAD 684206
MEDIUM 1
ETH.SRC 00:00:00:00:00:00
ETH.DST 00:00:00:00:00:00
ETH.TYPE 2048
NETNAME private src
IP.DST 94.73.151.210
NETNAME other dst
DIRECTION outbound
IP.PROTO 6
TCP.FLAGS 27

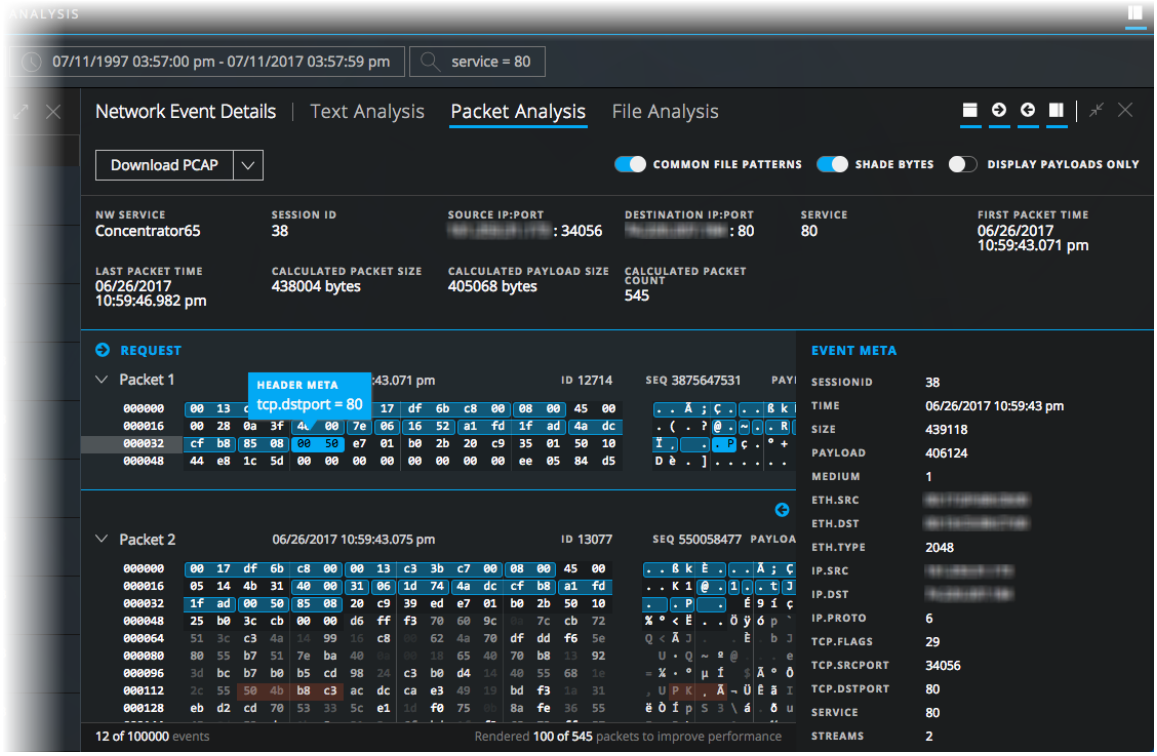

RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
GMT+00:00
NAVIGATE
EVENTS
MALWARE ANALYSIS
Results for:
Concentrator
06/29/1997 09:05:00 pm - 06/29/2017 09:05:59 pm
(medium = 32)
ip.addr =
All Events (261)
TIME
EVENT TYPE
SIZE
Log Event Details
Text Analysis
Download Log
NW SERVICE
Concentrator
SESSION ID
55278
DEVICE TYPE
unknown
COLLECTION TIME
06/23/2017 08:54:43.000 pm
RAW LOG
<4> %ISS-3-AcroRd32.exe: 571945147^^2009-01-17 05:00:52.000^^AcroRd32.exe^^501584^^(null)^^3^^10.134.150.84^^(null)^^(null)^^(null)^^(null)^^(null)^^BlackICE^^(null)^^Application Compliance^^3^^n^^(null)^^0^^33^^SYSTEM^^(null)^^(null)^^(null)^^(null)^^(null)^^(null)^^(null)^^(null)^^(null)^^(null)^^(null)
1 of 261 events
EVENT META
SESSIONID 55278
TIME 06/23/2017 08:54:43 pm
SIZE 331
MEDIUM 32
DEVICE.TYPE unknown
DEVICE.CONF 0
SOURCEFILE iss_verify.log
WORD iss
WORD acror
WORD exe
WORD null
WORD black
WORD appli
WORD compl
WORD syste
ALERT Parse: Failure
SOURCEFILE iss_verify.log



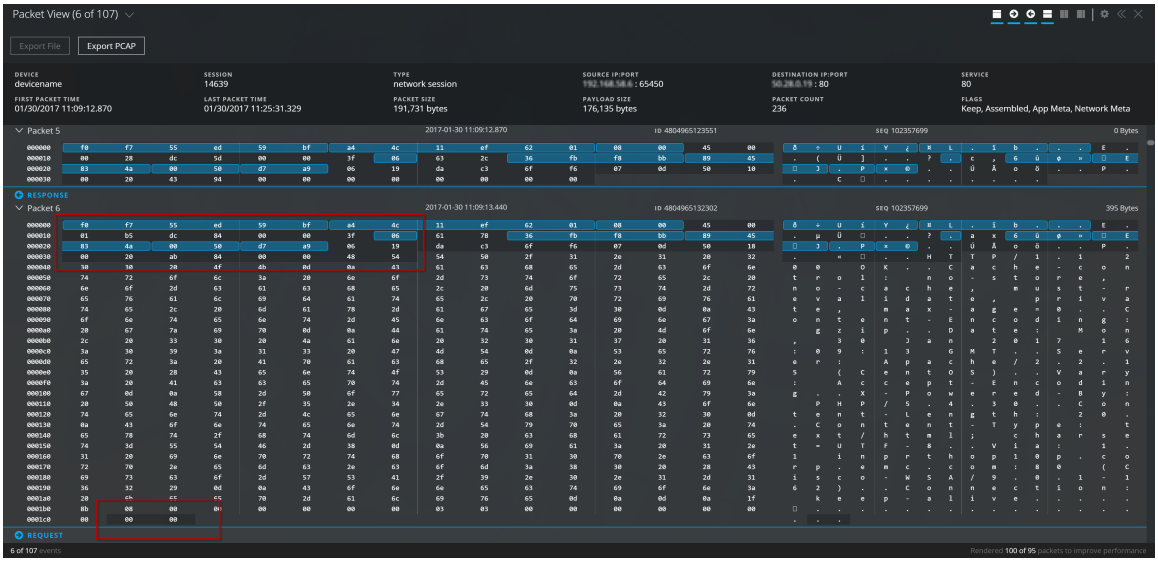
Hinweis: Die berechnete Paketanzahl, berechnete Paketgröße und berechnete Nutzdatengröße im Ereignis-Header kann sich von derselben Statistik im Bereich „Ereignis-Metadaten“ unterscheiden, da die Metadaten gelegentlich bereits vor Abschluss der Ereignisanalyse geschrieben werden und daher duplizierte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

Der Bereich „Paketanalyse“

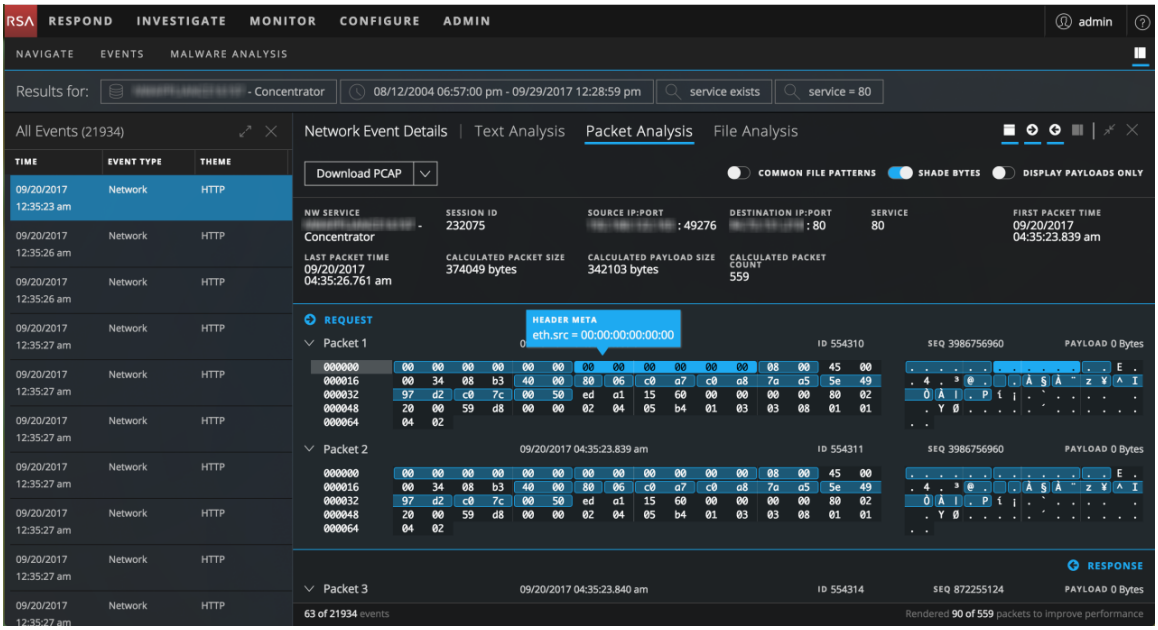
Der Bereich Paketanalyse ist nur für Netzwerkereignisse bestimmt. Der Bereich Paketanalyse ist scrollbar und die Informationen zur Identifizierung des Pakets sowie die Anforderungs- und Antwortbezeichnungen bleiben sichtbar, anstatt dass aus der Ansicht herausgescrollt wird.



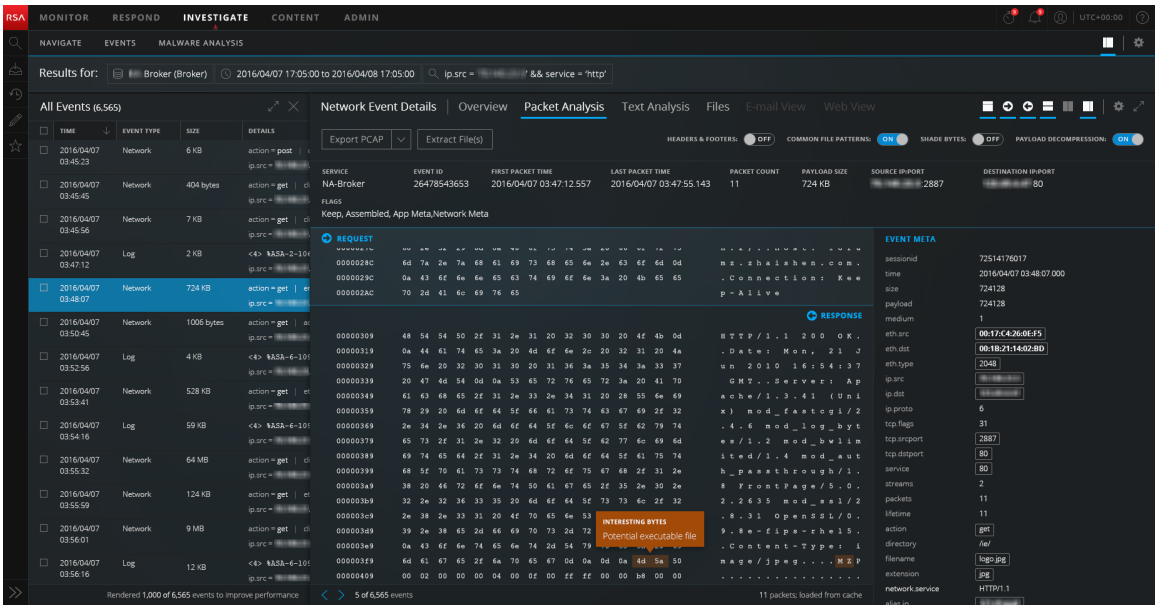
Im Bereich Paketanalyse geben die Überschriften die Richtung des Pakets (Anforderung oder Antwort), die Anzahl der Pakete, die Startzeit des Pakets, die Paket-ID und die Reihenfolge sowie die Nutzlastgröße an. Alle Pakete beginnen mit einer Kopfzeile und einige Pakete haben eine Fußzeile. Einige Pakete haben eine Nutzlast. In der Paketanalyse haben die Kopfzeile und Fußzeile einen dunkleren Hintergrund, damit sie von der Nutzlast des Pakets zu unterscheiden sind. Der dunklere Hintergrund für die Kopf- und Fußzeile wird im hexadezimalen und im ASCII-Format angezeigt.



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.

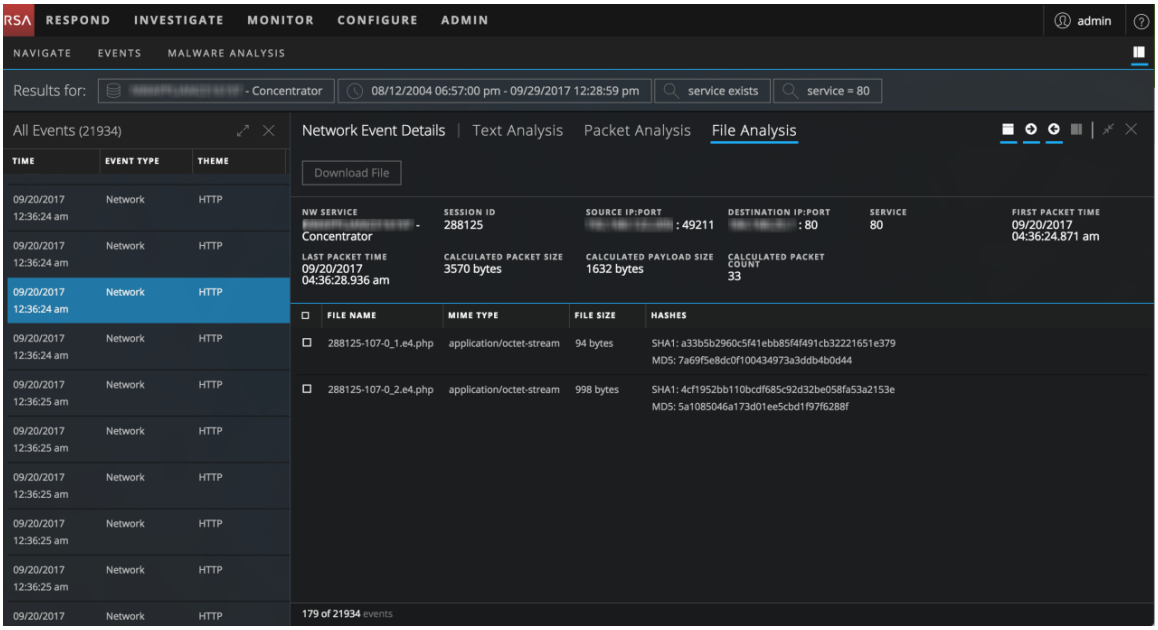


Gebräuchliche Dateisignaturen sind mit einem orangefarbenen Hintergrund hervorgehoben. Wenn Sie den Cursor über den hervorgehobenen Text bewegen, wird die Beschreibung des Dateityps in einem Kasten mit Hover-Effekt angezeigt.

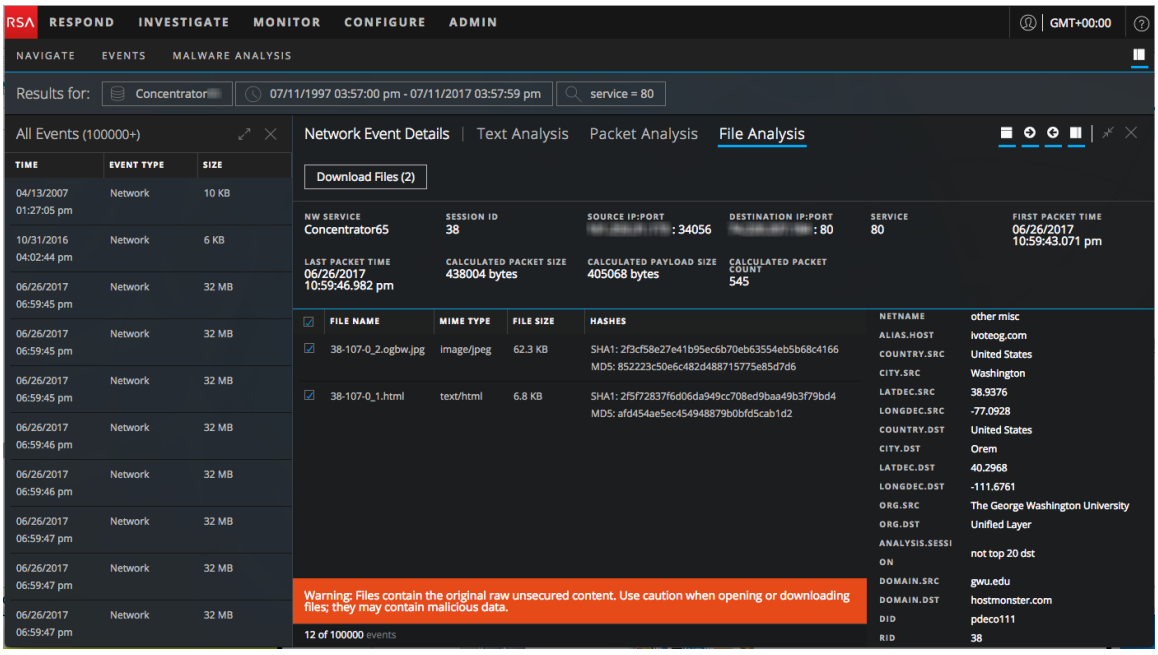


Der Bereich „Dateianalyse“

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“ aktiv und gibt die Anzahl der ausgewählten Dateien. an.



Achtung: Vorsicht ist beim Entpacken und Öffnen von Dateien geboten, die mit einer Standardanwendung verknüpft sind; 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	√		
Anzeigen oder Ausblenden des Ereignis-Headers im Bereich „Textanalyse“	√	√	√

Aktion	Netzwerkereignis	Ereignis protokollieren	Endpunktereignis
Erweitern abgeschnittener Texteinträge im Bereich „Textanalyse“	√		
Wechseln zwischen einer komprimierten und dekomprimierten Ansicht der Nutzlasten im Bereich „Textanalyse“	√		
Anzeigen hervorgehobener Bytes im Bereich „Paketanalyse“	√		
Markieren 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“	√		

Aktion	Netzwerkereignis	Ereignis protokollieren	Endpunktereignis
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“	√		
Herunterladen der Datei für ein Protokollereignis im Bereich „Textanalyse“		√	

Aktion	Netzwerkereignis	Ereignis protokollieren	Endpunktereignis
Herunterladen der Datei für ein Endpunktereignis im Bereich „Textanalyse“			√
Öffnen des aktuellen Endpunktereignisses im Bereich „NetWitness Endpoint“			√

Auswählen des Typs der Ereignisanalyse

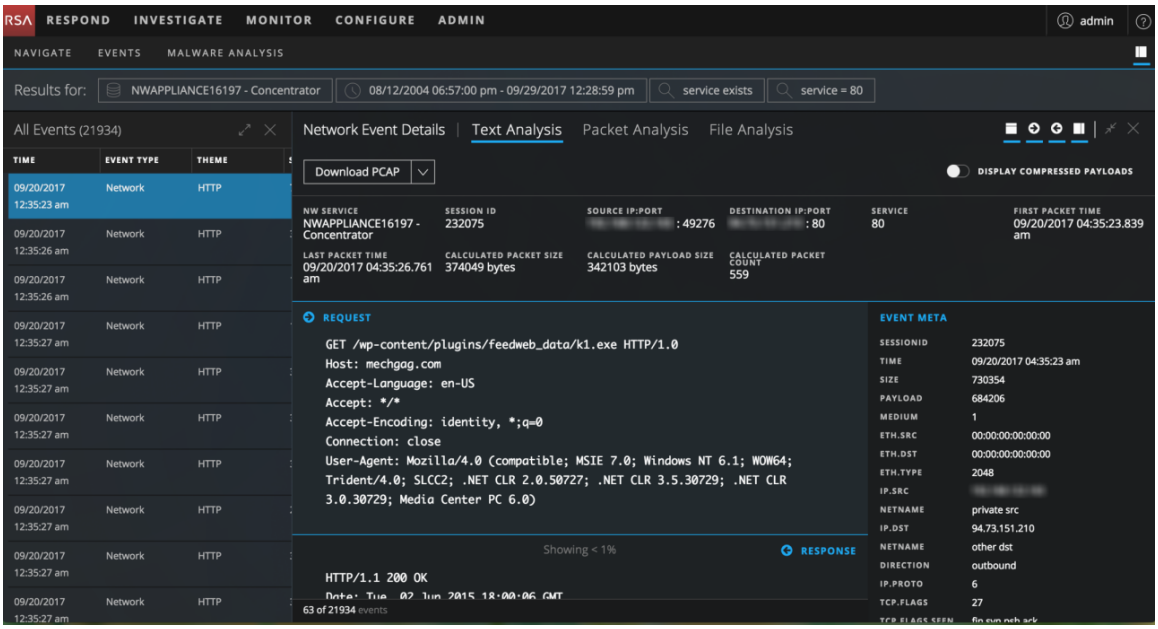
Um den Typ der Ereignisanalyse für ein Ereignis auszuwählen, führen Sie einen der folgenden Schritte aus:

1. Klicken Sie in der Symbolleiste der **Ansicht „Ereignisanalyse“** auf das Menü „Analysetyp“ in der oberen linken Ecke.
2. Wählen Sie im Drop-down-Menü den Typ der Analyse: **Paketanalyse, Dateianalyse** oder **Textanalyse**.
   Die Ansicht wird mit geöffnetem Bereich „Paketanalyse“, „Dateianalyse“ oder „Textanalyse“ aktualisiert.

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 auf der linken Seite geöffnet und der Bereich „Netzwerkdetails“, „Protokolldetails“ oder „Endpunktdetails“ wird auf der rechten Seite geöffnet. Sie können auf ein Ereignis in der Ereignisliste klicken, um eine andere Rekonstruktion anzuzeigen. Zunächst belegt der Bereich „Netzwerkdetails“, „Protokolldetails“ oder „Endpunktdetails“ standardmäßig 75 % der Fensterbreite.



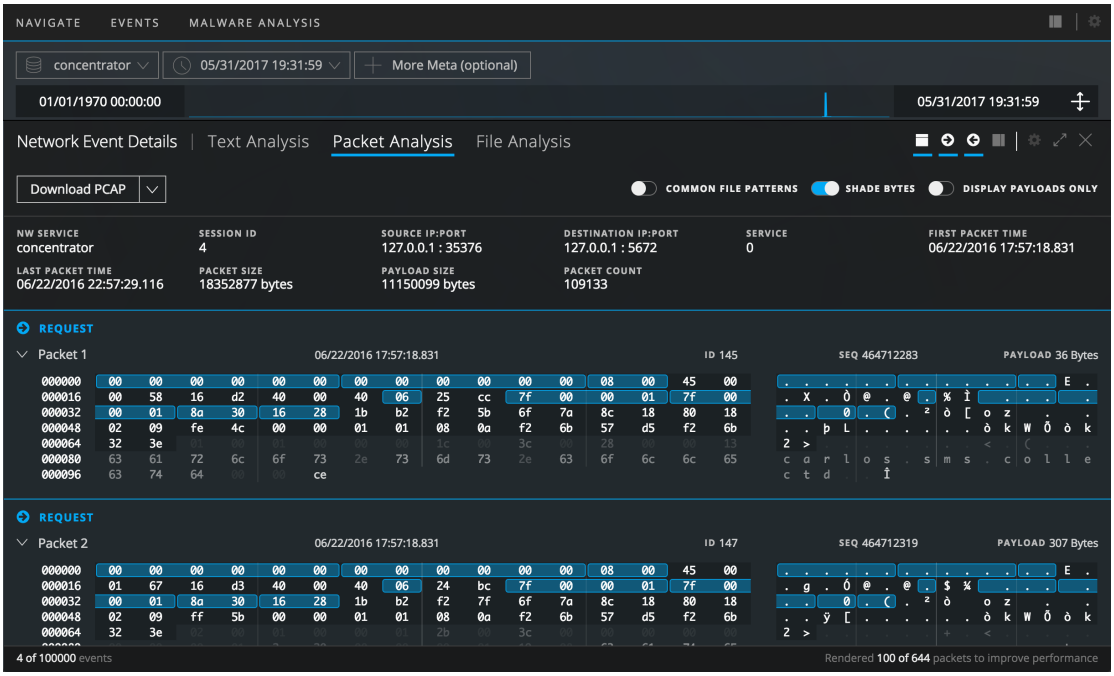
Sie können das Größenverhältnis der beiden Bereiche anpassen, um die Lesbarkeit zu verbessern, indem Sie einen der Bereiche erweitern, einen der Bereiche verkleinern und einen der Bereiche schließen. Nach dem Schließen eines Bereichs können Sie diesen erneut öffnen. Das Verhältnis, das Sie auswählen, 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“.

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.

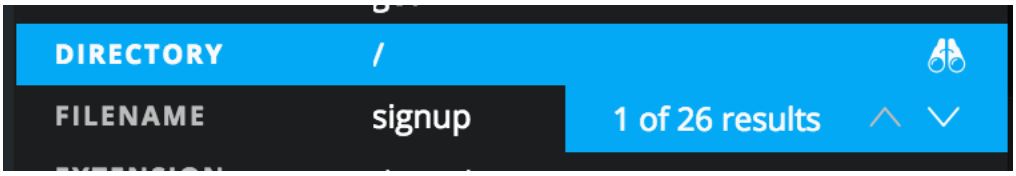
Um auszuwählen, welche Seite des Gesprächs angezeigt werden soll – Anforderung, Antwort oder beide –, klicken Sie auf eines der Richtungssymbole oder auf beide.  . Die Rekonstruktion wird anhand der ausgewählten Informationen aktualisiert.

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.



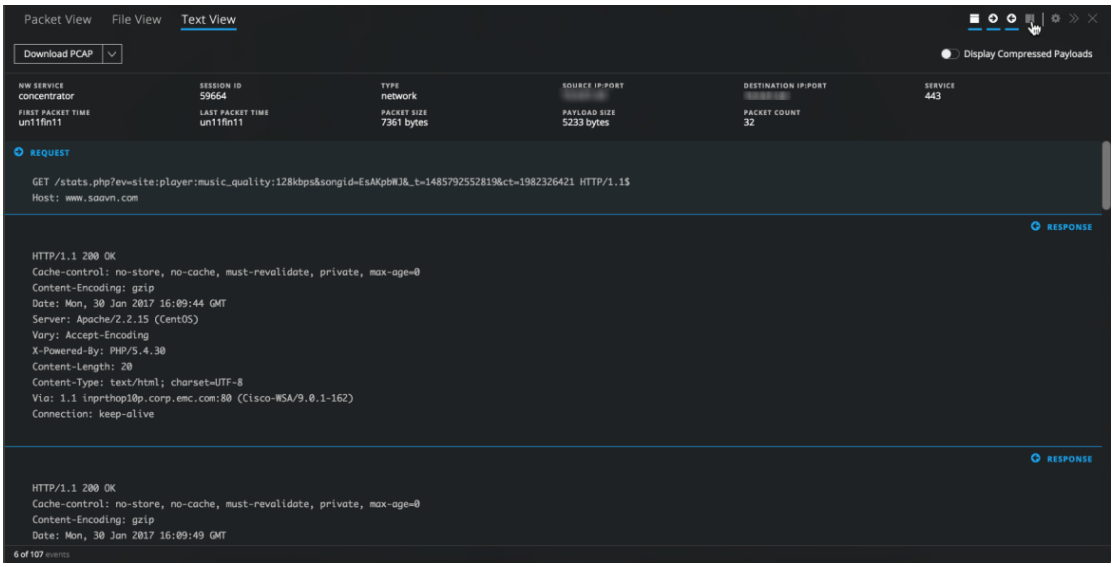
Durch Klicken auf das Symbol wird eine Suche nach dem Metaschlüssel-/Metawert-Paar (ohne Beachtung der Groß- und Kleinschreibung) im Bereich Textanalyse ausgelöst und jede Instanz wird hervorgehoben. Im Bereich „Ereignis-Metadaten“ werden in der hervorgehobenen Zeile die Anzahl der Ergebnisse und ein 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.

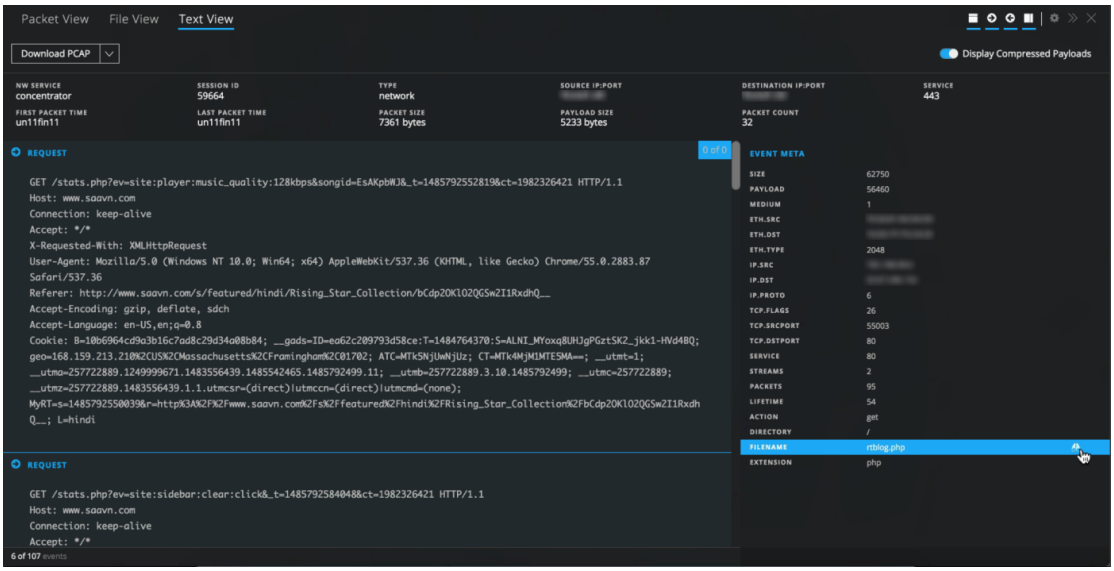
So durchsuchen Sie den unformatierten Text nach Metawerten, die einen Metaschlüssel ausgelöst haben:

1. Öffnen Sie ein Netzwerkereignis im Bereich Textanalyse.

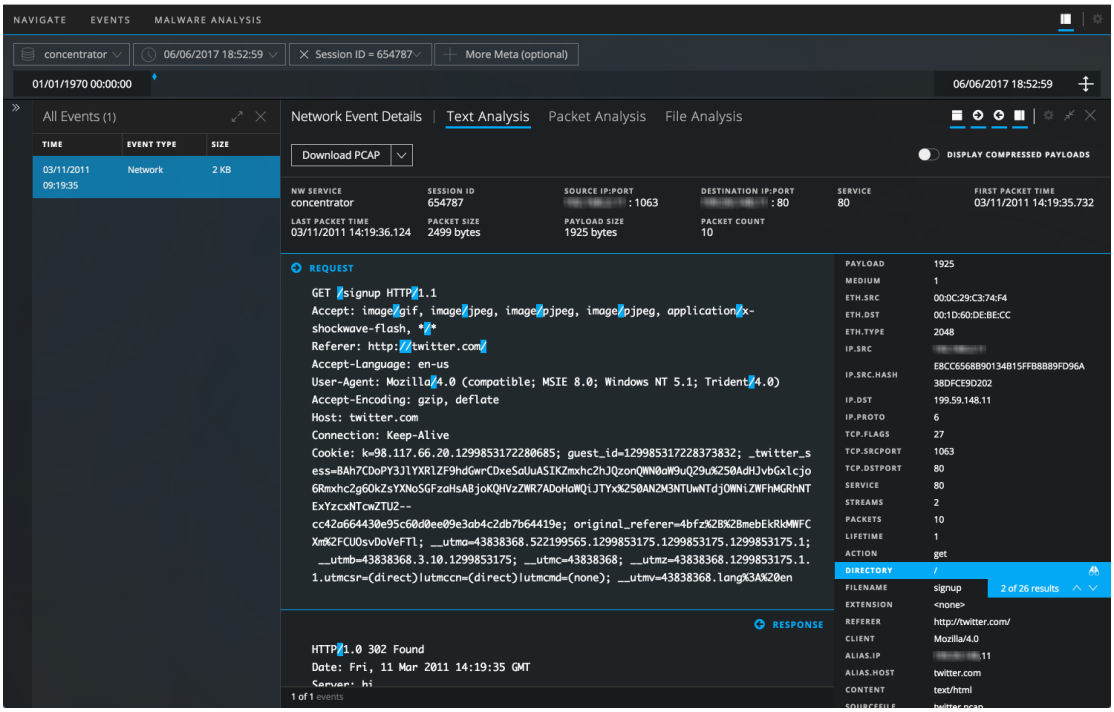


2. Klicken Sie in der Symbolleiste auf , um das den Bereich „Ereignis-Metadaten“ zu öffnen. Wenn Sie den Mauszeiger über die Metaschlüssel-/Wert-Paare in der Liste bewegen, identifiziert ein Fernglas-Symbol Werte, die im Bereich Textanalyse durchsucht werden können.

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.



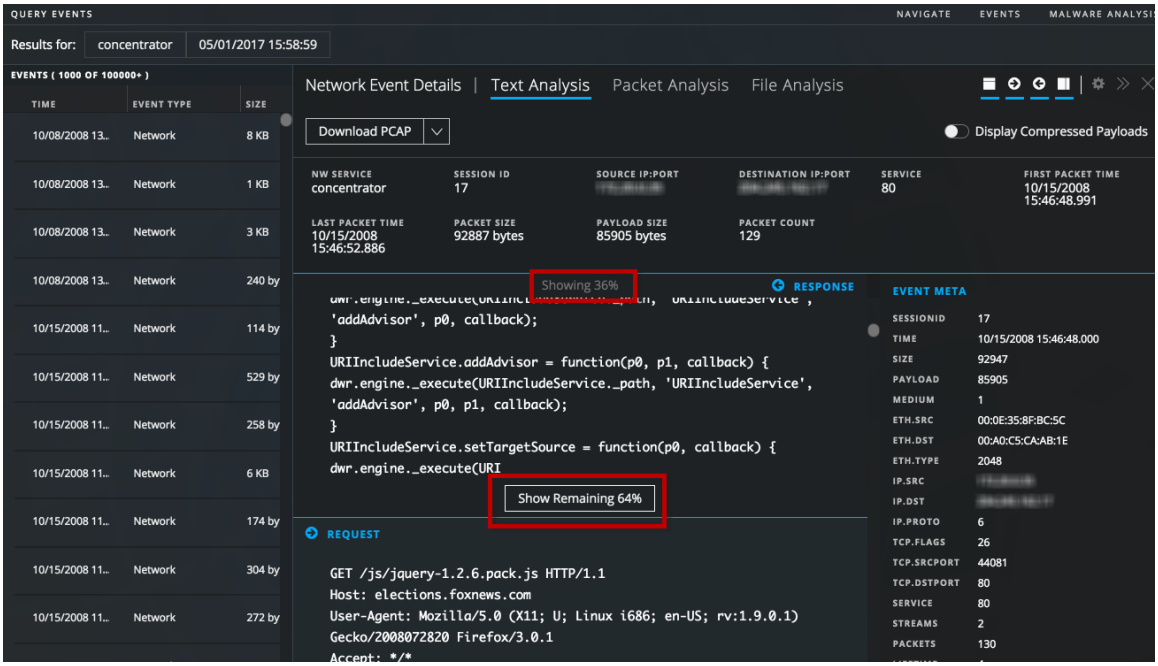
4. Um die Hervorhebung zu entfernen, schließen Sie den Bereich „Ereignis-Metadaten“, klicken Sie auf das gleiche Metaschlüssel-/Metawert-Paar im Bereich „Ereignis-Metadaten“ oder klicken Sie auf ein anderes Metaschlüssel-/Metawert-Paar im Bereich „Ereignis-Metadaten“.
   Die Hervorhebung wird aus dem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

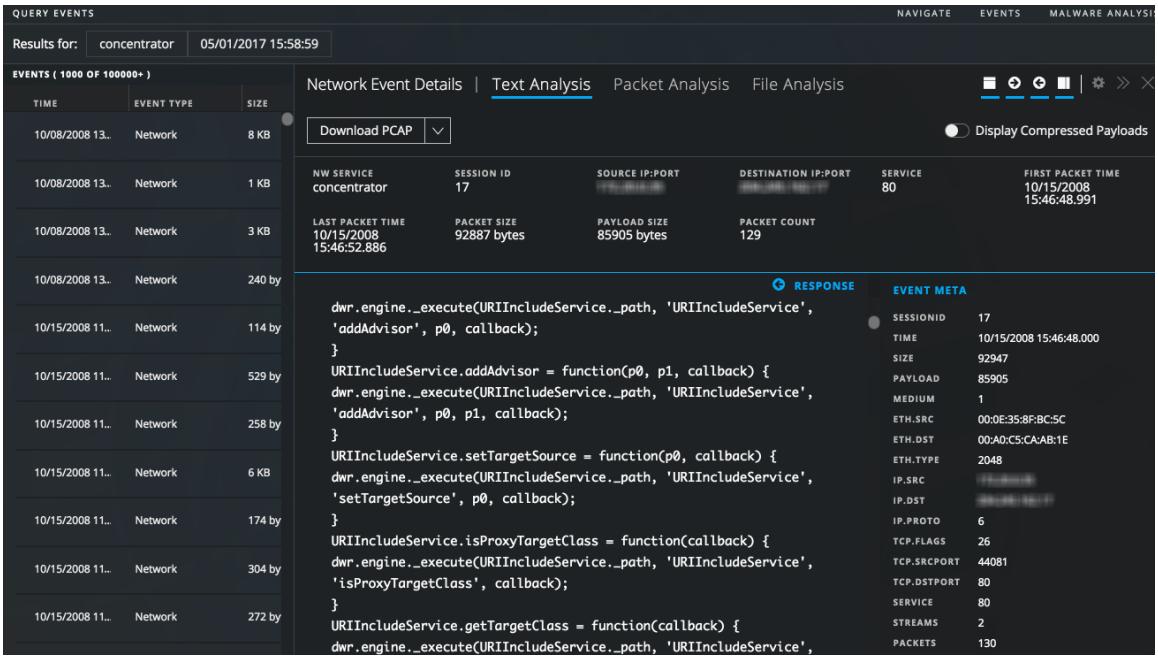
Erweitern abgeschnittener Texteinträge im Bereich „Textanalyse“

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 36 % der Zeichen (die ersten 2000) angezeigt werden. Klicken Sie auf **Verbleibende 64 % anzeigen**, um den Rest des Eintrags anzuzeigen.



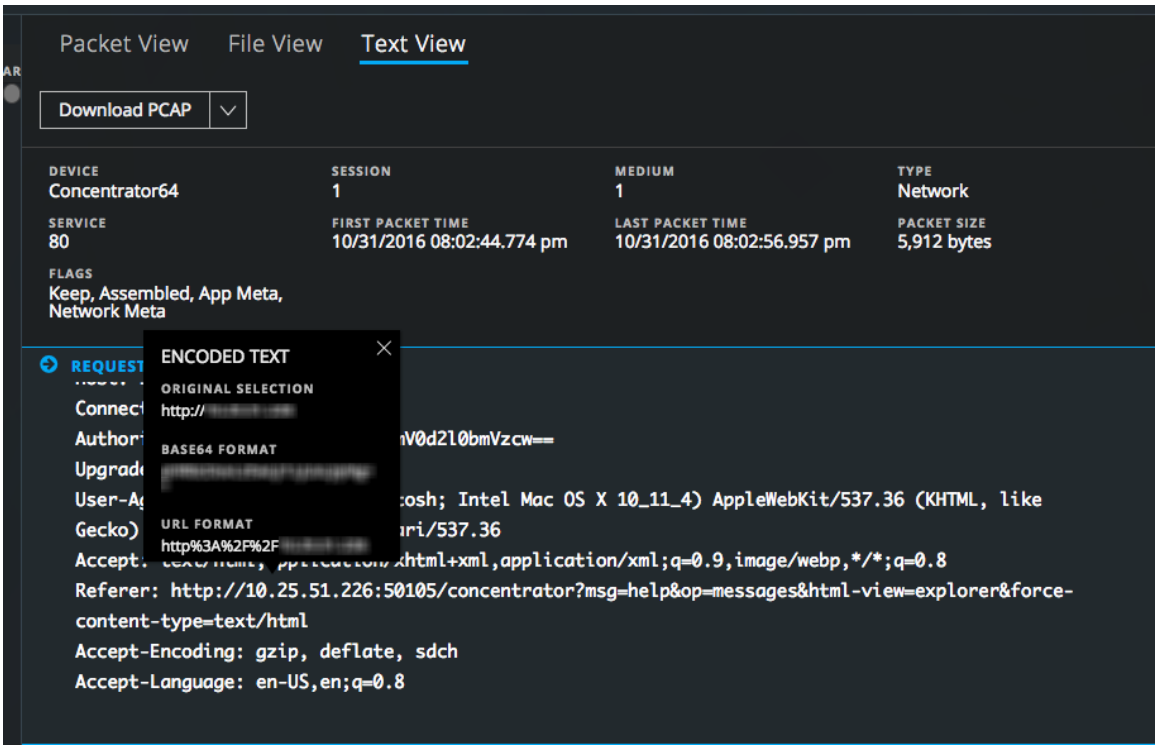
Wenn Sie im Bereich „Ereignis-Metadaten“ nach Metadaten suchen, während Text im Bereich Textanalyse gekürzt wird, wird der abgeschnittene Text durchsucht. Wenn die Metadaten in ausgeblendetem Text vorhanden sind, wird der Texteintrag erweitert, um den Text mit den gefundenen Metadaten anzuzeigen.

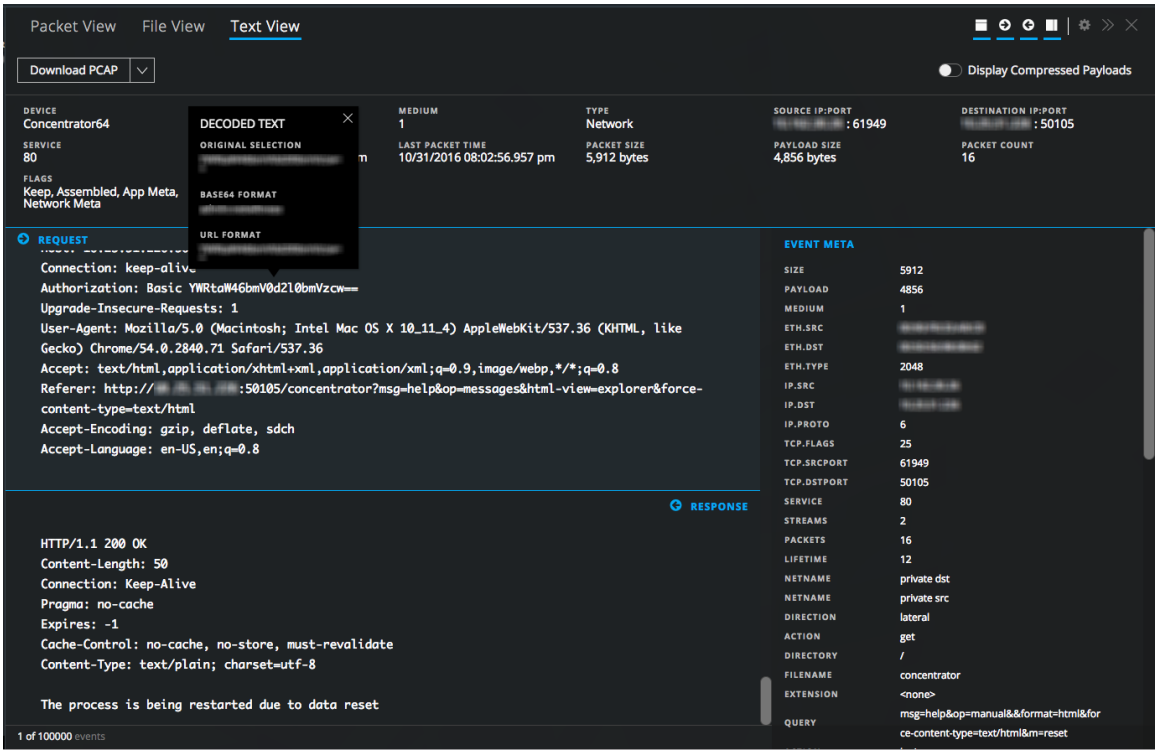
Durchführen von URL- und Base64-Codierung und -Decodierung im Bereich „Textanalyse“

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.

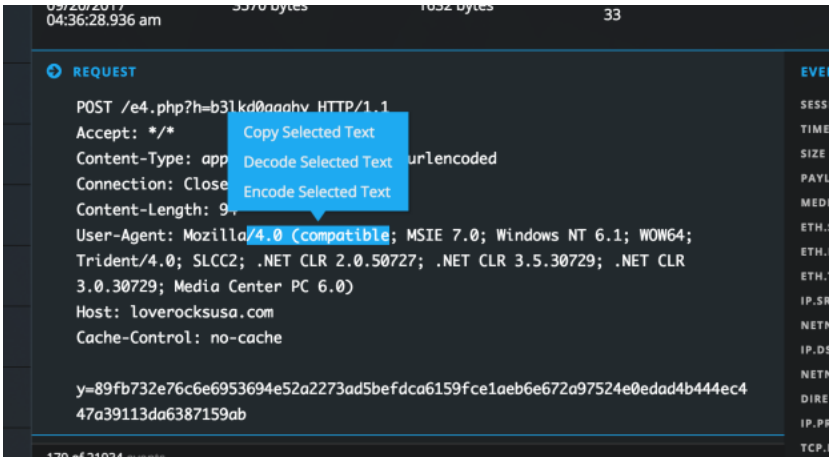




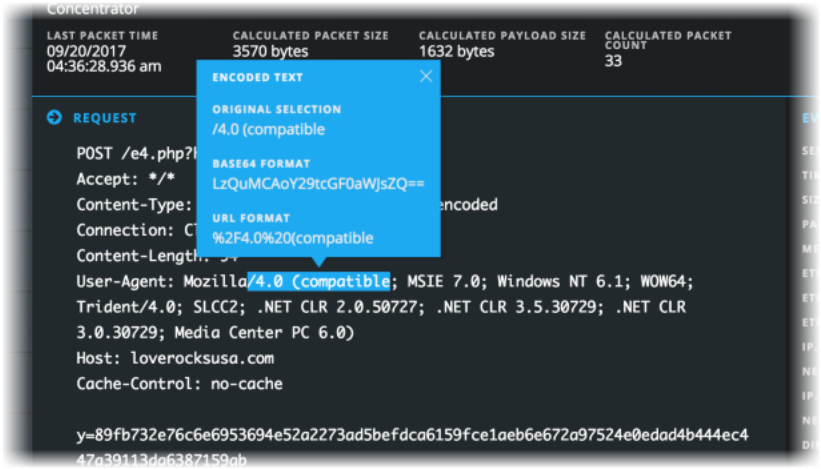
Durchführen von Codierung bzw. Decodierung im Bereich Textanalyse:

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.



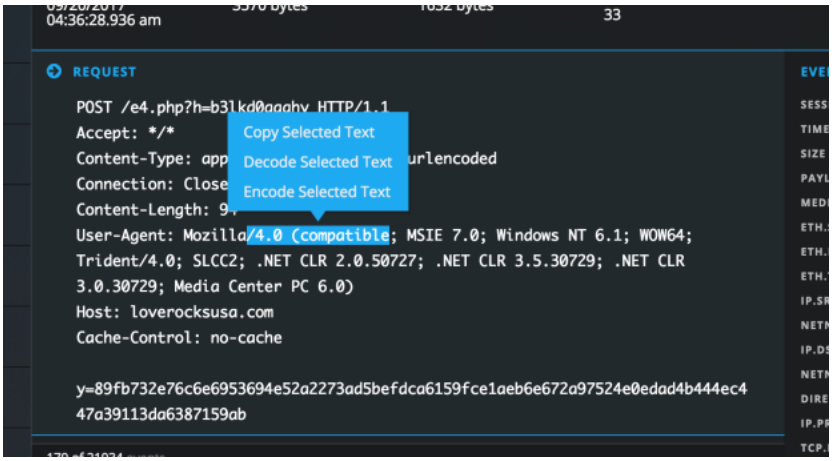
3. Klicken Sie auf **Ausgewählten Text codieren.**
   Der codierte Text wird in einem Feld mit Hover-Effekt angezeigt, das beibehalten wird, bis Sie auf das ⊠ klicken, anderen Text im Bereich Textanalyse wählen, den Bereich Bereich „Ereignisse“ schließen, ein anderes Ereignis für die Rekonstruktion auswählen 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. Ziehen Sie die Maustaste, um Text auszuwählen, klicken Sie mit der rechten Maustaste und wählen Sie **Ausgewählten Text kopieren** im Pop-up-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 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“

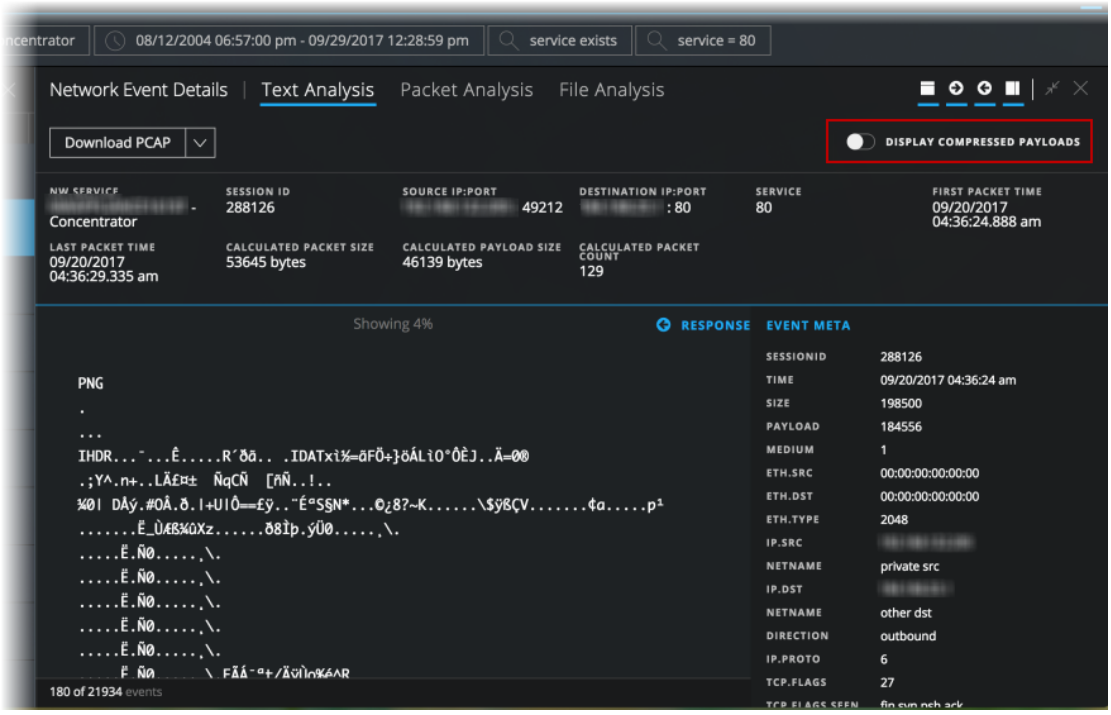
Wenn der Inhalt einer HTTP-Netzwerksitzung komprimiert wird und Sie den Bereich Textanalyse anzeigen, zeigt NetWitness Suite standardmäßig dekomprimierten Inhalt. Dies hilft Ihnen, zu bestimmen, ob Muster vorhanden sind, und Sie können die besten lesbaren Zeichen anzeigen. Sie können zwischen einer komprimierten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

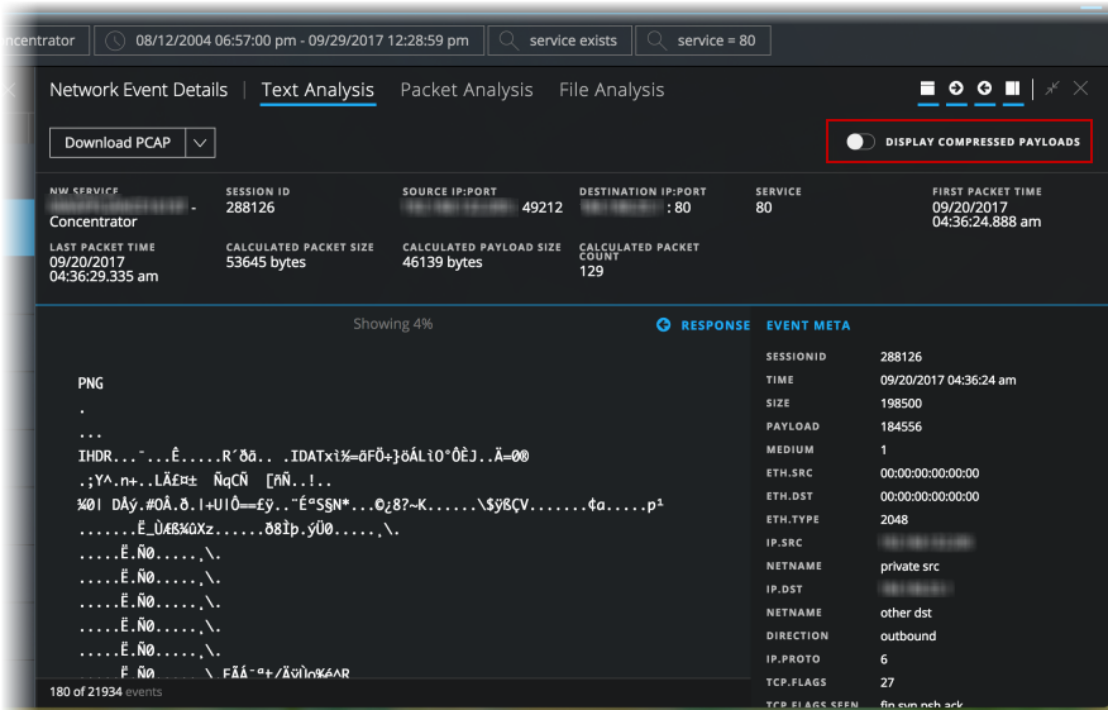
1. Öffnen Sie den Bereich Textanalyse einer HTTP-Sitzung, der komprimierten Content enthält.

   Standardmäßig wird die Sitzung mit dem dekomprimierten Text rekonstruiert und über der Rekonstruktion befindet sich der Umschalter **Komprimierte Nutzlasten 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.

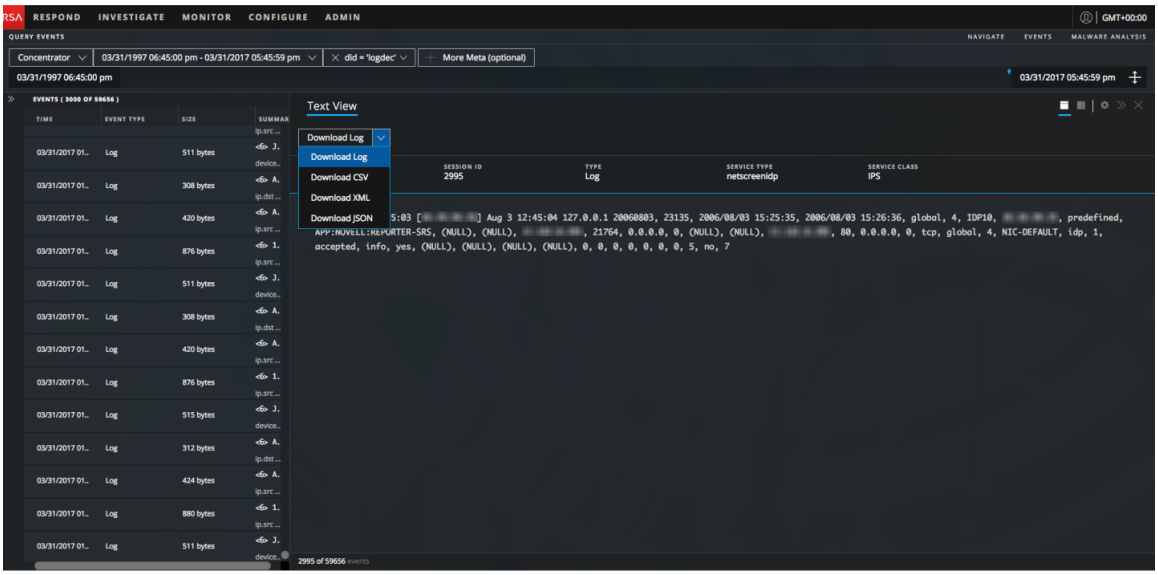
Herunterladen eines Protokolls im Bereich „Textanalyse“

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**

Hinweis: 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.

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



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.

Hinweis: Dateien, die über längere Zeiträume ausgeführt oder in der Vergangenheit heruntergeladen wurden, können nicht heruntergeladen werden.

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>`

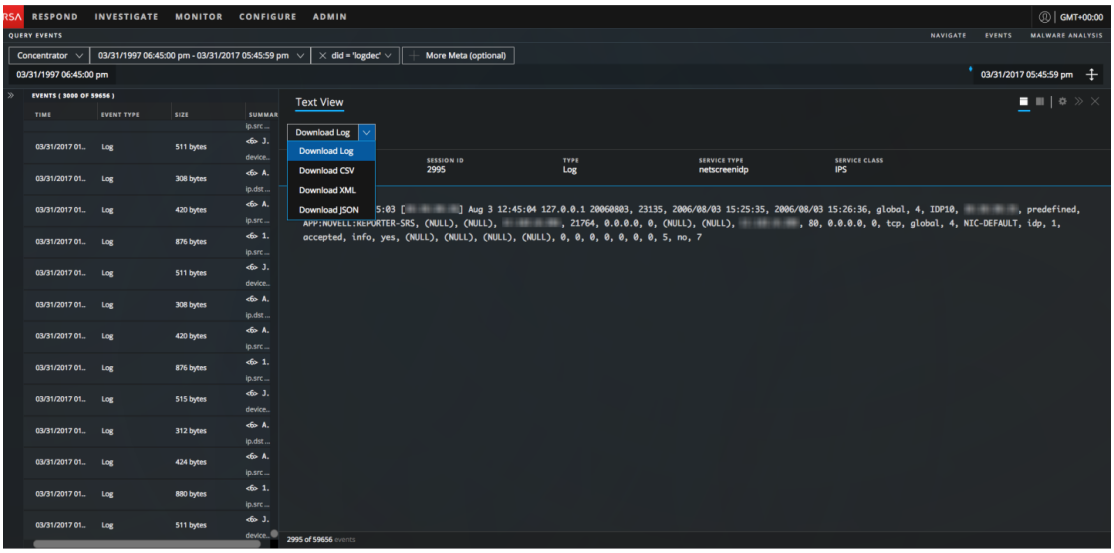
Hierbei gilt:

- `<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 der 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="10.4.30.65".`

So laden Sie das Protokoll für eine Sitzung herunter:

1. 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.

Herunterladen von Netzwerk-Datendateien 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 Nutzlasten 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:

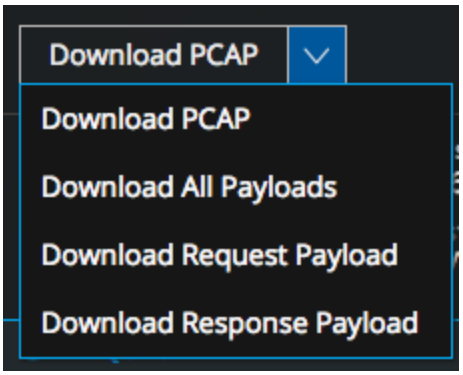
- `<service-ID or host name>` ist der Name des Services (z. B. ein Concentrator oder Broker), in dem die Sitzung gespeichert wurde.
- `SID<n>` ist die Sitzungs-ID-Nummer.
- `<filetype>` ist pcap, payload, payload1 oder payload2.

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:

1. 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.



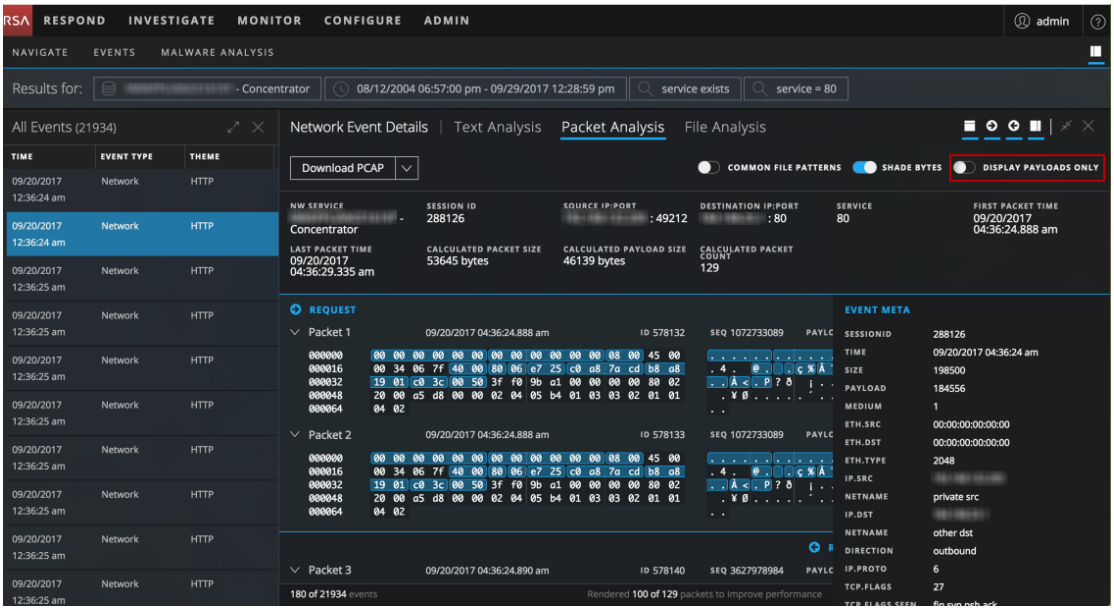
Die Netzwerkdatendatei wird im angegebenen Format auf Ihr lokales Dateisystem heruntergeladen.

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.

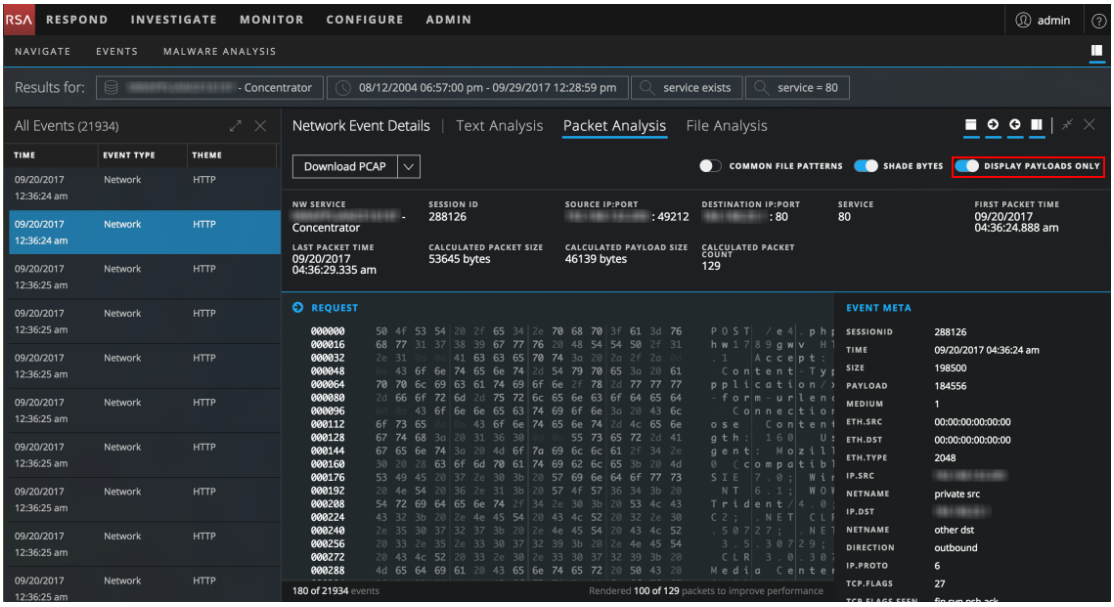
- Bei deaktivierter Option „Nur Nutzdaten anzeigen“ werden die Anzahl der Pakete, Paket-Kopfzeile, Packet-Fußzeile und Nutzdaten angezeigt.
- Bei aktivierter Option „Nur Nutzdaten anzeigen“ werden keine Kopf- und Fußzeilen-Bytes angezeigt. Nur die Paketinhalte von 16 hexadezimalen Bytes pro Zeile und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

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.



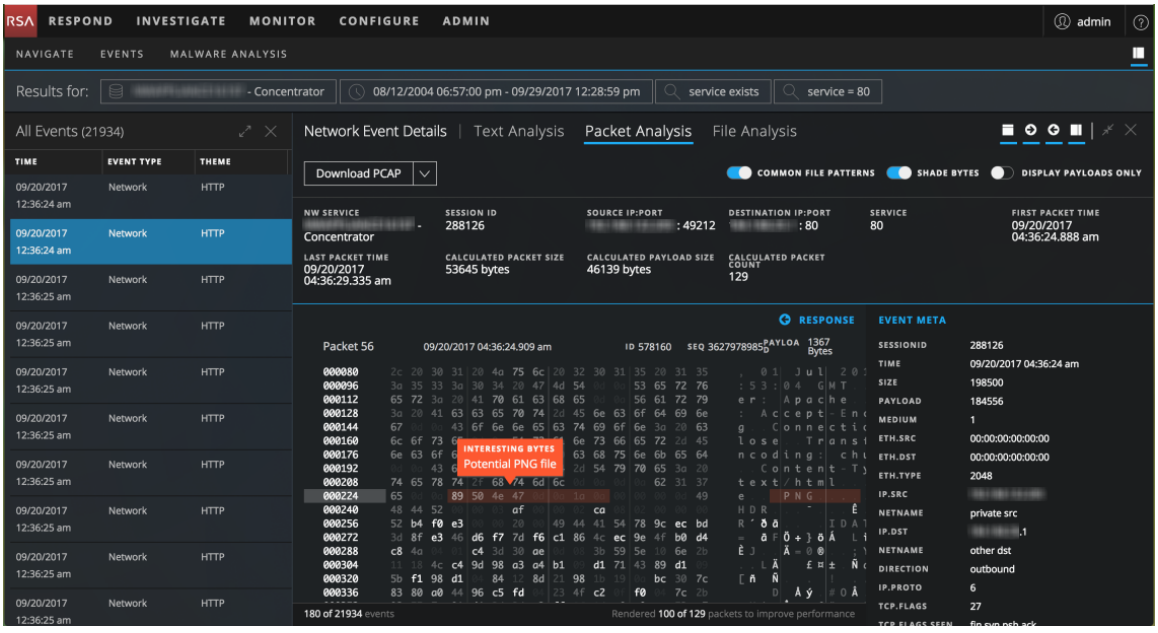
2. Um die Ansicht zu ändern und nur die Nutzlast für jedes Paket anzuzeigen, klicken Sie auf den Umschalter **Nur Nutzdaten anzeigen**.
   Die Ansicht ändert sich, sodass nur die Nutzlast sichtbar ist und zusammenhängende Pakete

auf der gleichen Seite verkettet werden, um die Nutzlast besser lesbar und verständlich zu machen.

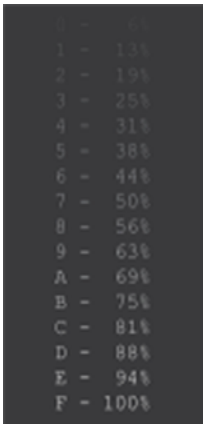


Anzeigen hervorgehobener Bytes im Bereich „Paketanalyse“

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.



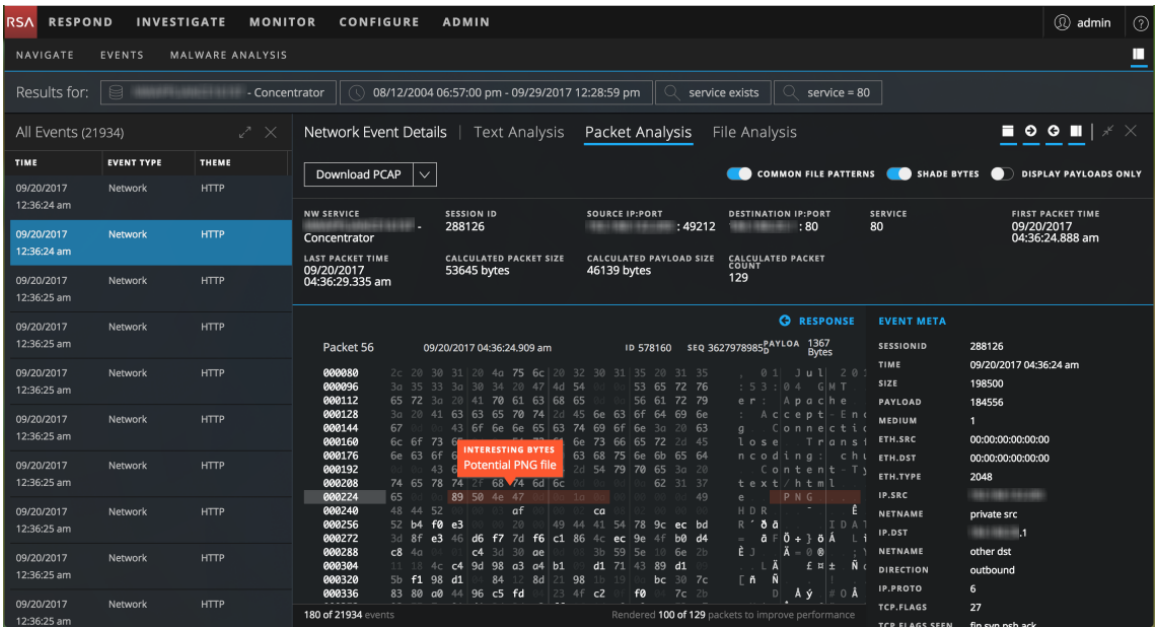
Mit der Option „Byte schattieren“ wird eine Schattierung zum Identifizieren der verschiedenen hexadezimalen Bytes (00 bis FF) mithilfe unterschiedlich starker Hervorhebung hinzugefügt. Bytes nahe dem unteren Bereich sind transparenter und Bytes, die sich 255 annähern, sind undurchsichtiger. Hexadezimal- 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
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

Dateityp	Hexadezimale Signatur	ASCII-Codierung
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:

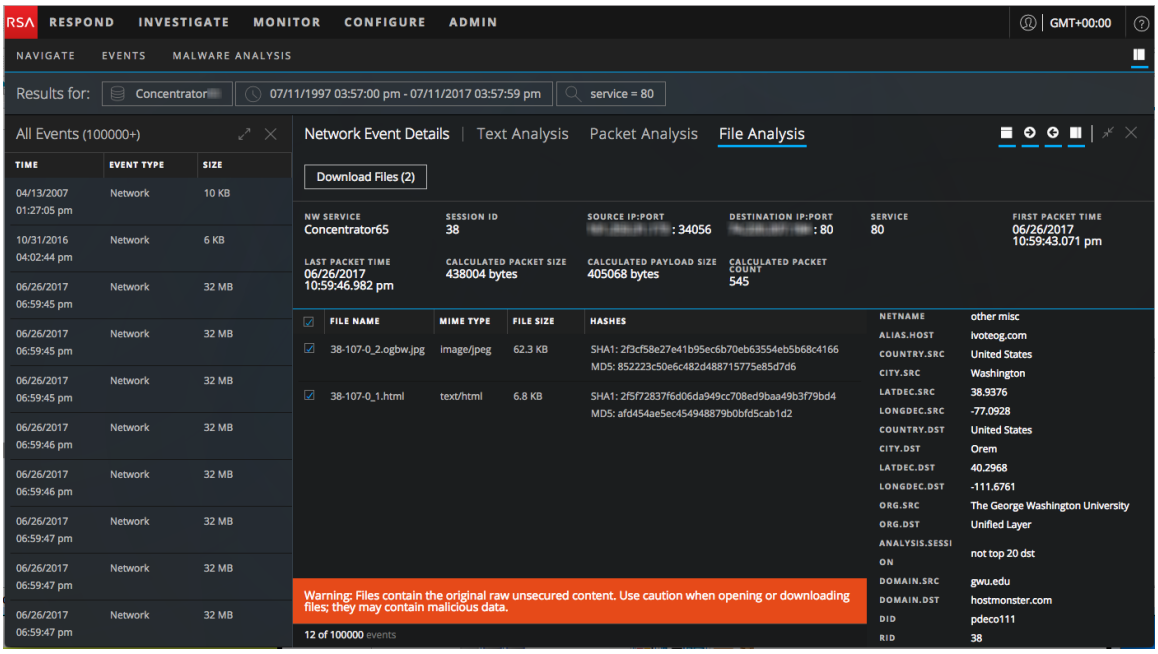
1. Navigieren Sie zum Bereich „Paketanalyse“ und aktivieren Sie die Option **Gebräuchliche Dateimuster**.
   Wenn es mehr als eine Hervorhebung in der Ansicht gibt, werden alle angezeigt.
2. Um das Feld mit Hover-Effekt anzuzeigen, platzieren Sie den Mauszeiger über der Hervorhebung.

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 diesem Formular wird Folgendes sichergestellt:

- 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`

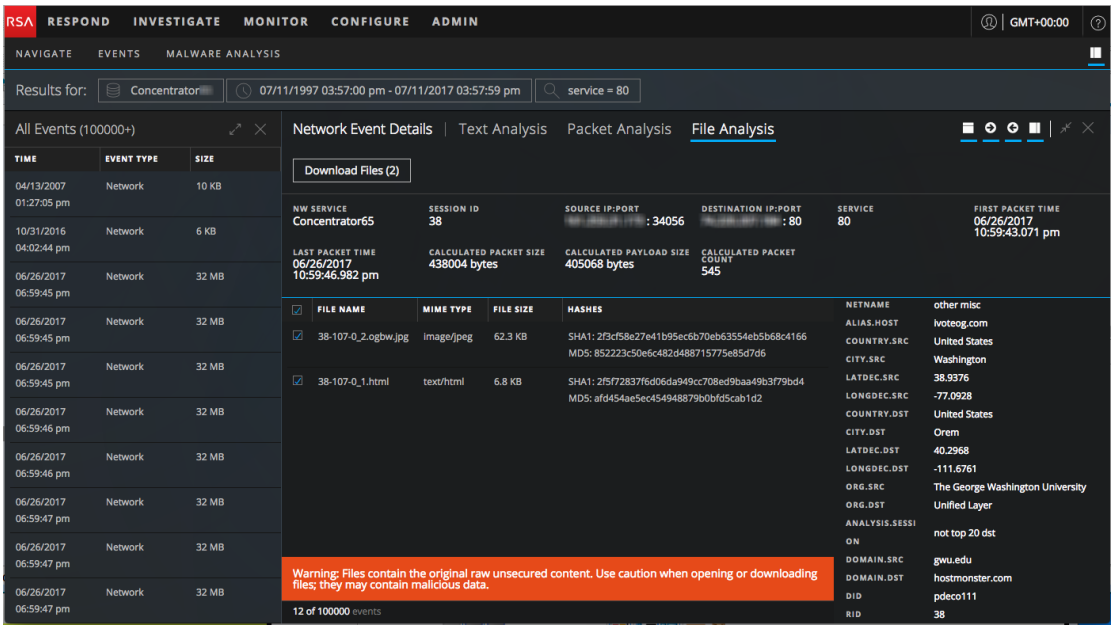
Hierbei gilt:

- `<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: Vorsicht ist beim Entpacken und Öffnen von Dateien geboten, die mit einer Standardanwendung verknüpft sind; 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`.

Öffnen eines Endpunktereignisses in der NetWitness Endpoint-Anwendung

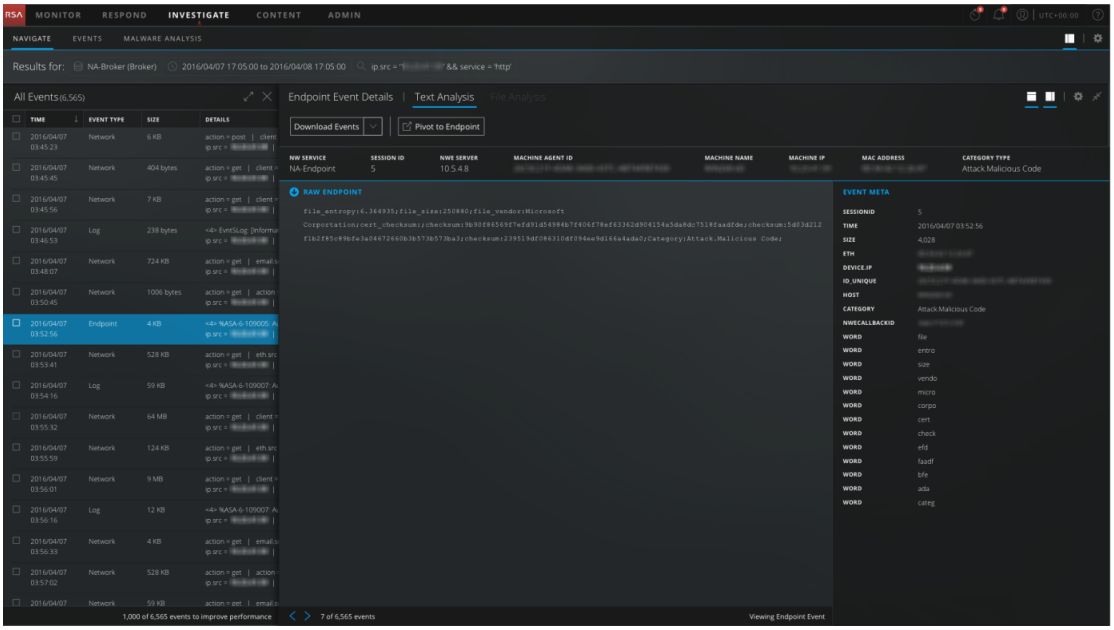
Beim Anzeigen eines Endpunktereignisses im Bereich „Textanalyse“ können Sie zur Analyse des gleichen Ereignisses in NetWitness Endpoint wechseln.

Hinweis: 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.

So öffnen Sie ein Ereignis in NetWitness Endpoint:

1. Um nach Endpunktereignissen zu suchen, wählen Sie **Abfrage** in der Symbolleiste der Ansicht „Navigation“.

2. Wählen Sie im Dialogfeld **Abfrage** die Option **Erweitert** und geben Sie eine der folgenden Abfragen ein: `nwe.callback_id exists` oder `device.type='nwendpoint'` Endpunktdaten werden im Bereich „Werte“ angezeigt.
3. Klicken Sie mit der rechten Maustaste auf ein Ereignis und wählen Sie im Kontextmenü **Ereignisanalyse**.
   Die Ereignisanalyse wird unter Anzeige des ausgewählten Ereignisses 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.

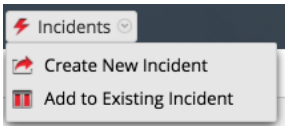
Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion

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

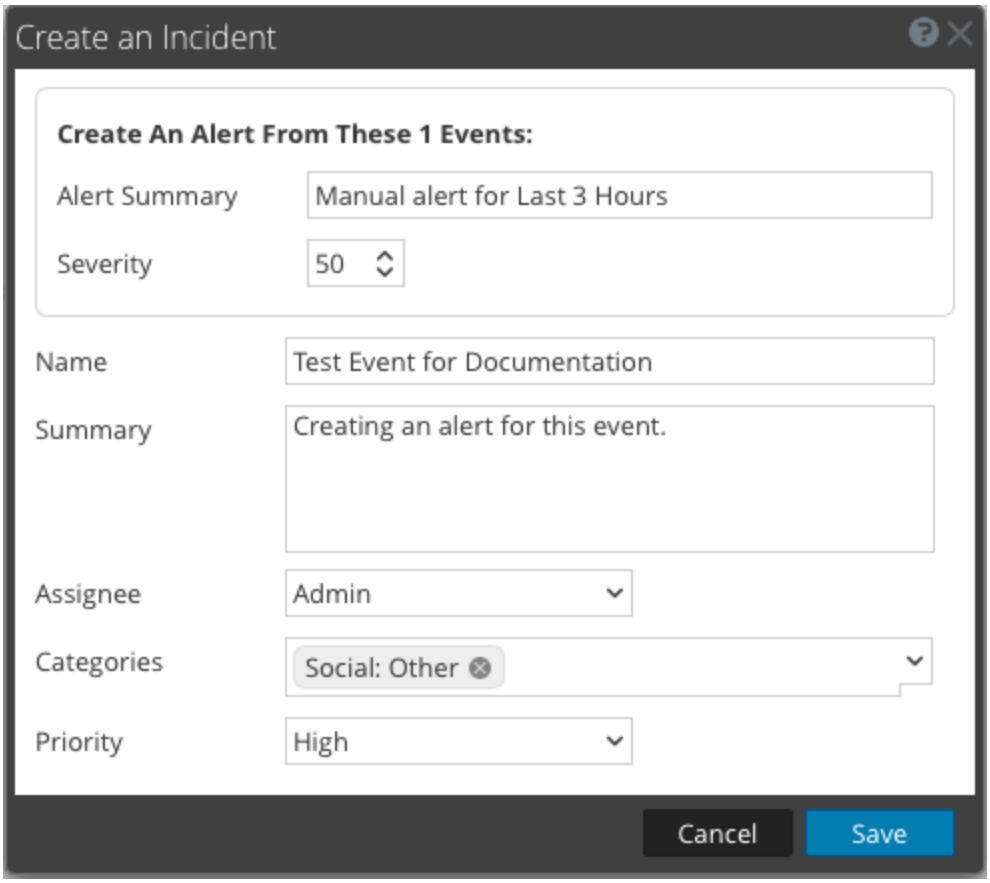
Hinweis: Ein Administrator muss die erforderlichen Rollen und Berechtigungen konfigurieren, wie in „Rollenberechtigungen“ und „Managen von Benutzern mit Rollen und Berechtigungen“ im *Handbuch Systemsicherheit und Benutzerverwaltung* beschrieben ist.

1. Navigieren Sie mithilfe einer der unter Untersuchen von Ereignissen beschriebenen Methoden zu Ansicht „Ereignisse“.

2. Wählen Sie in der Ansicht „Ereignisse“ ein oder mehrere Ereignisse aus und 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 in der Ansicht „Ereignisse“ zu einem Incident hinzuzufügen, wählen Sie ein oder mehrere Ereignisse und dann **Incidents > Zu vorhandenem Incident hinzufügen**.

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.

Exportieren von Ereignissen

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.

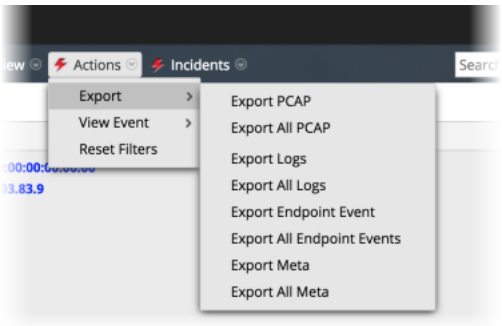
Bei der Exportfunktion wird der Service auf alle Sitzungen für den ausgewählten Zeitbereich und Drill-down-Punkt abgefragt, um die Inhalte jeder Sitzung zu extrahieren. Die zu exportierenden Detailinformationen werden sowohl durch den Zeitbereich als auch durch den Drill-down-Punkt zum Zeitpunkt des 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 Suite 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 aus.
   In einer Meldung werden Sie informiert, dass PCAP heruntergeladen wird.

Durchführen von Schadsoftwareanalysen

Analysten können den RSA NetWitness Suite Malware Analysis-Service zur Erkennung von Schadsoftware in ausgewählten Daten und Dateien nutzen.

Für Analysten, die Analysen mithilfe von NetWitness Suite Malware Analysis durchführen, müssen die entsprechenden Systemrollen und Berechtigungen in den Benutzerkonten eingerichtet werden. Siehe Rollen und Berechtigungen für Malware-Analysten..

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

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 Suite 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 Suite-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 Schadsoftwareanalyse-Scans in der Navigationsansicht.

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. Ermittlung 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.

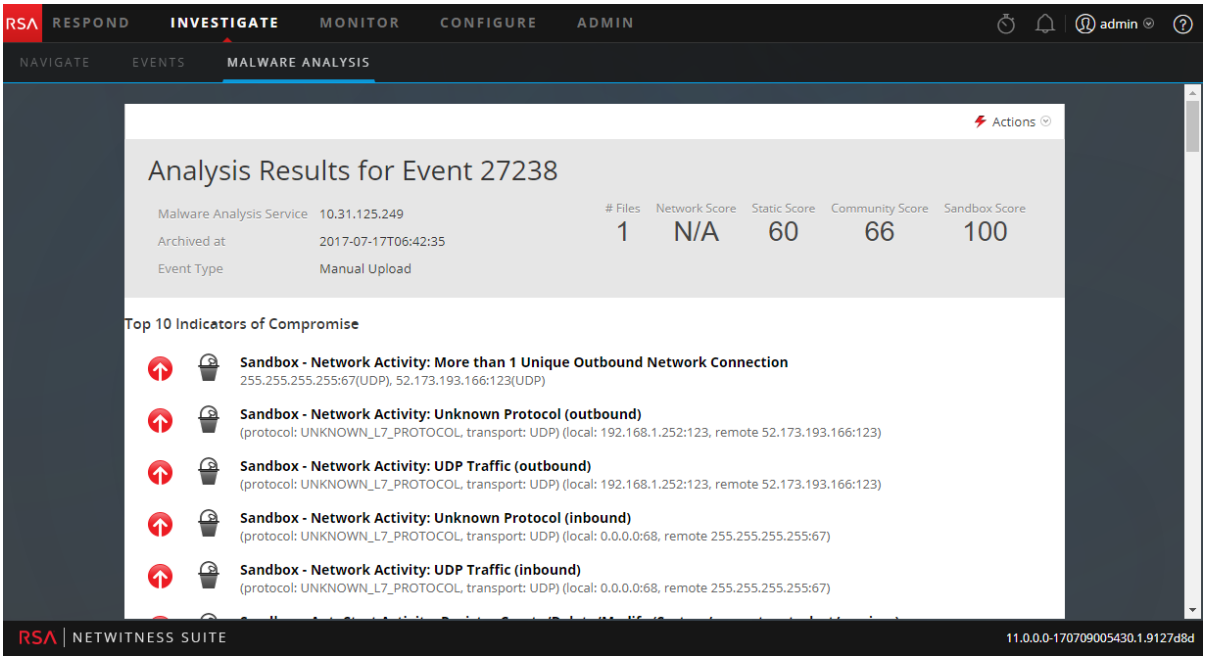
Starten einer Schadsoftwareermittlung von einem Malware Analysis-Dashlet aus

Eine Vorbedingung für dieses Verfahren ist, dass eines der folgenden Dashlets im NetWitness Suite-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 Suite 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 Suite*.

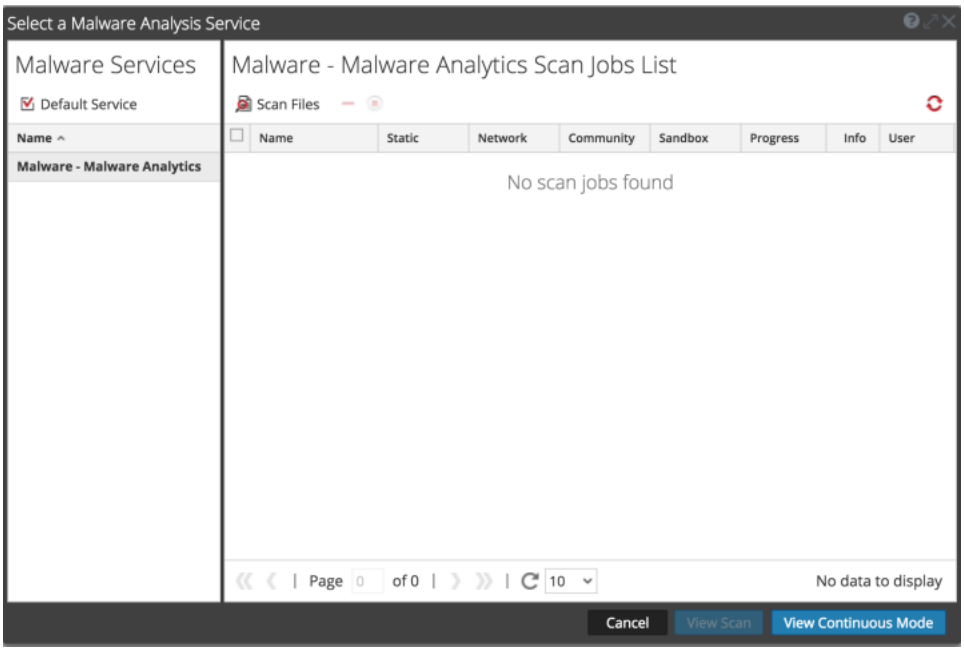
Weitere Informationen über Methoden, Informationen in Dashlets in der Malware Analysis-Ansicht zu konfigurieren und zu filtern, finden Sie unter Filtern der Dashlet-Daten in der Ansicht Ereigniszusammenfassung.

Weitere Informationen über die Aktionen, die Sie in den Analyseergebnissen durchführen können, finden Sie unter Anzeigen der detaillierten Schadsoftwareanalyse eines Ereignisses.

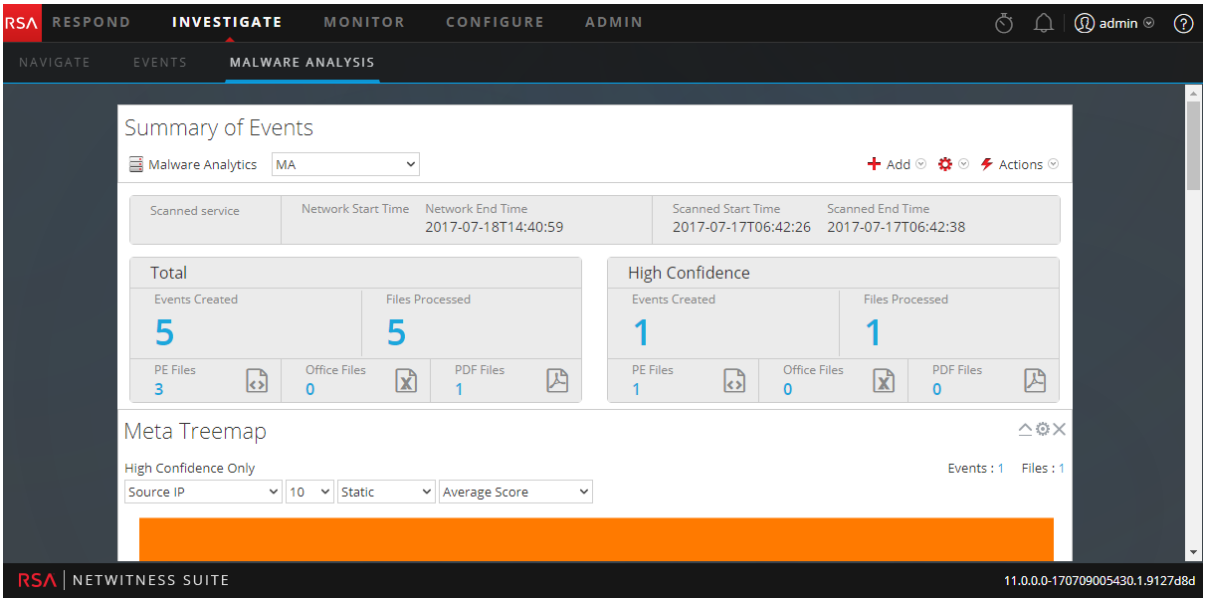
Beginnen einer Malware Analysis Investigation (ohne Standardservice)

So starten Sie eine Ermittlung ohne angegebenen Standardservice:

1. Wählen Sie **Investigation > Malware Analysis**.
   Das Dialogfeld „Malware Analysis Service auswählen“ wird mit verfügbaren Malware Analysis-Hosts und -Services für den aktuellen Benutzer 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 Schadsoftwareanalyse-Scans in der Navigationsansicht).
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.

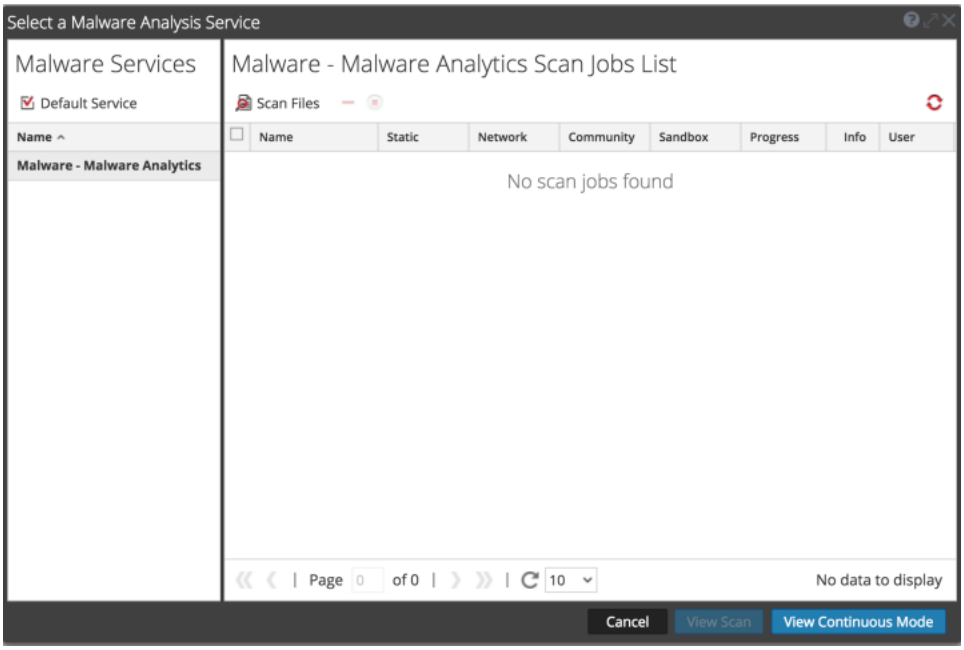


Einrichten oder Löschen des Standardservices

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

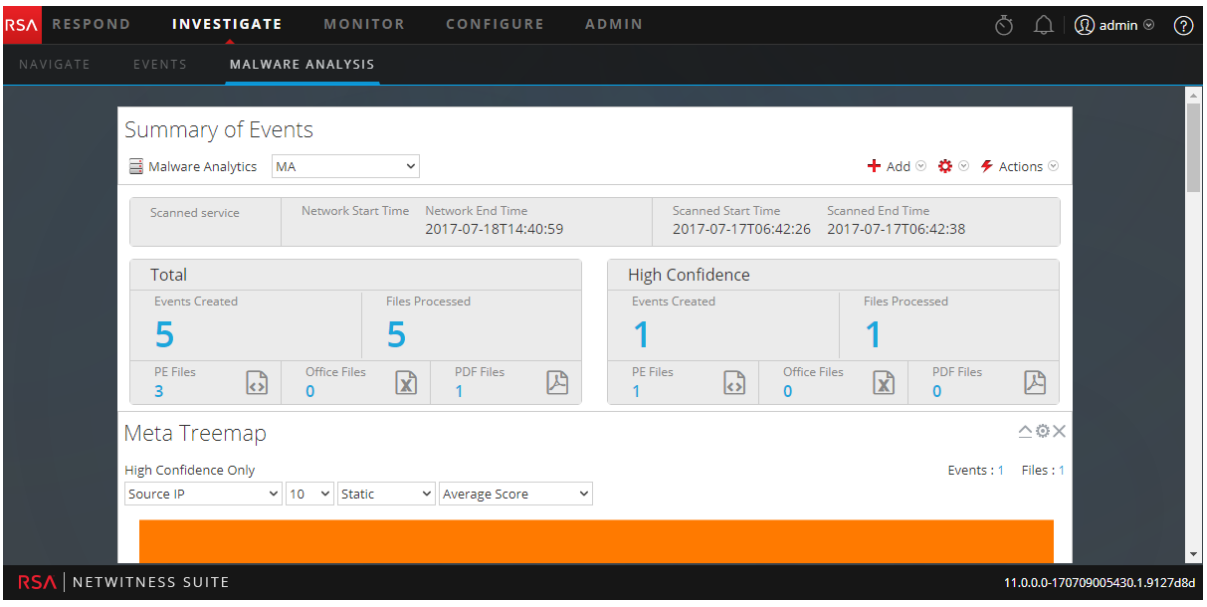
Ein Schadsoftwareanalyst mit der Berechtigung für `Initiate Malware Analysis Scan` kann zu scannende Dateien mithilfe der Option „Dateien scannen“ des Dialogfelds „Malware Analysis Service auswählen“ hochladen (siehe Hochladen von Dateien für Malware Analysis-Scans). Ein Administrator kann Paketerfassungsdateien zu einem Decoder für Malware Analysis in der Ansicht „Services-System“ hochladen, wie beschrieben in „Paketerfassungsdatei hochladen“ im *Konfigurationsleitfaden für Decoder und Log Decoder*.

Starten einer Ermittlung (Standardservice angegeben)

So starten Sie eine Ermittlung mit angegebenem Standardservice:

1. Wählen Sie **Investigation > Malware Analysis**.

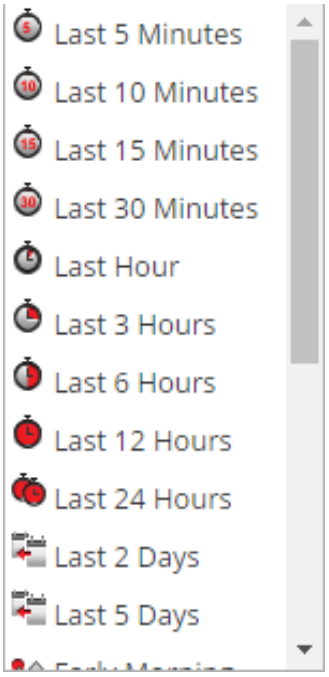
   Die Ereigniszusammenfassung für den kontinuierlichen Scan des ausgewählten Services wird mit den geöffneten Standard-Dashlets angezeigt. Jeder Benutzer kann Standard-Dashlets hinzufügen, ändern und löschen, die für verschiedene Scanermittlungen persistent sind. Benutzer können außerdem Standard-Dashlets 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 .

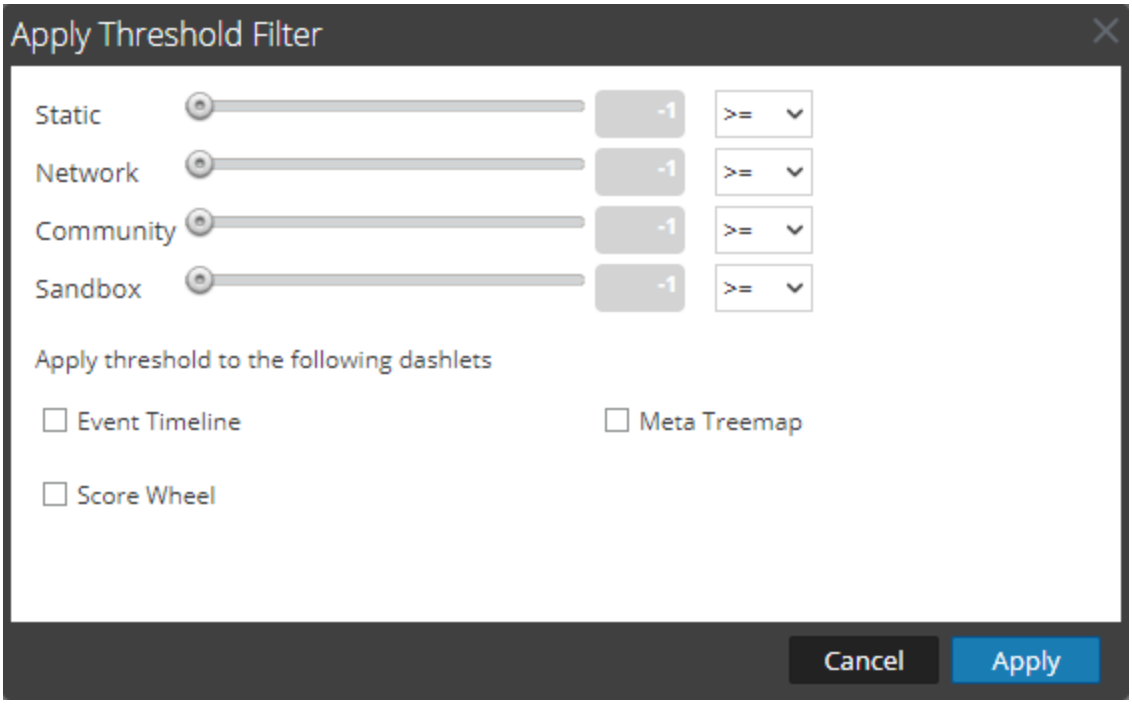
Anwenden eines Schwellenwertfilters auf Ergebnisse von Scans im kontinuierlichen Modus

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

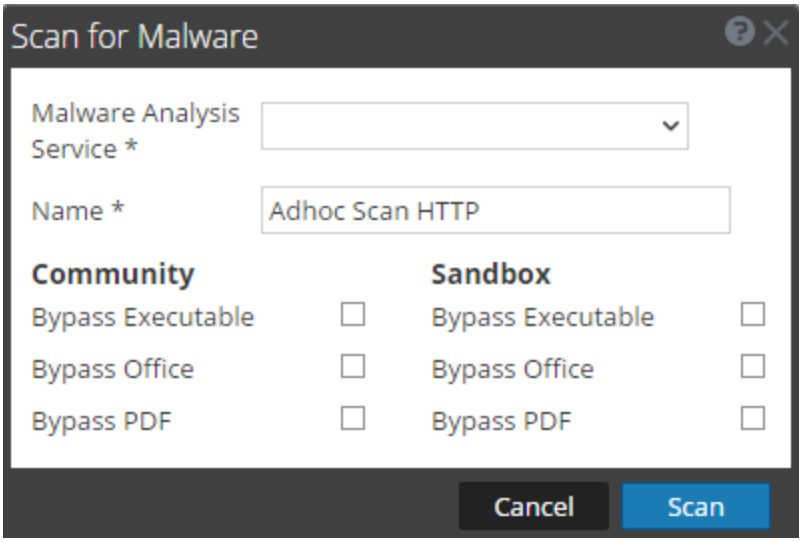
Sie können einen Scan nach Bedarf löschen oder ihn mit anderen Umgehungseinstellungen als denjenigen, die in der Servicekonfigurationsansicht für einen Malware Analysis-Service angegeben sind, erneut übermitteln.

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.

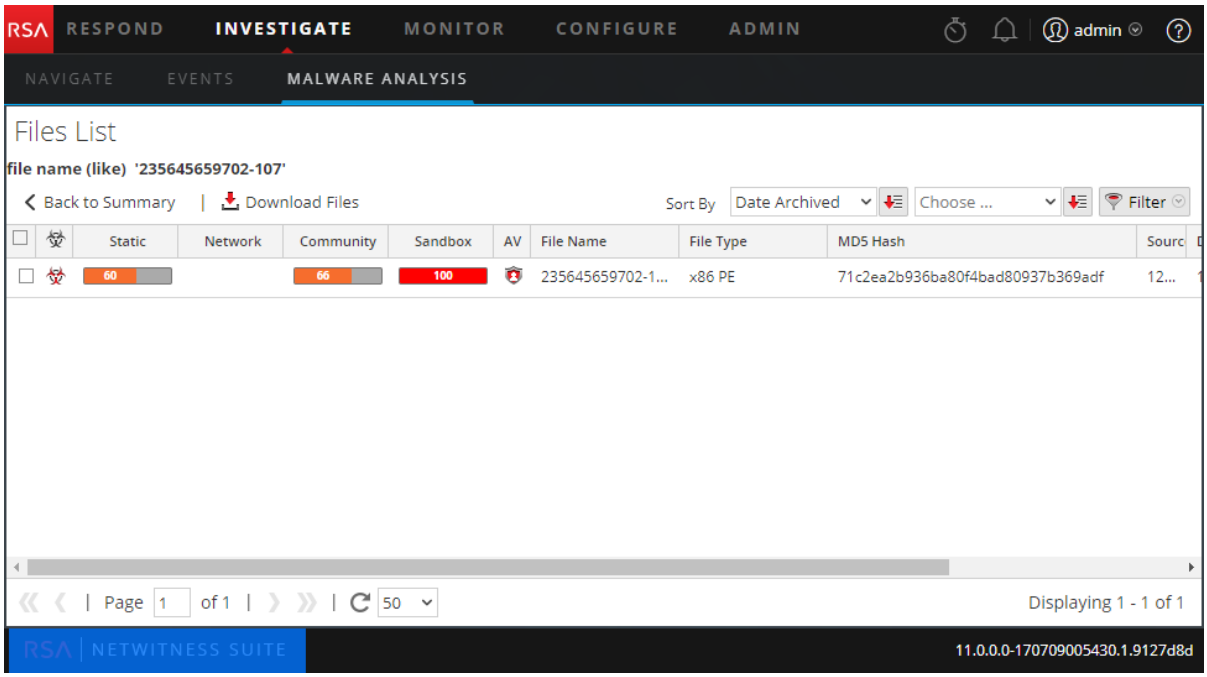
Anzeigen der Dateiliste

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.

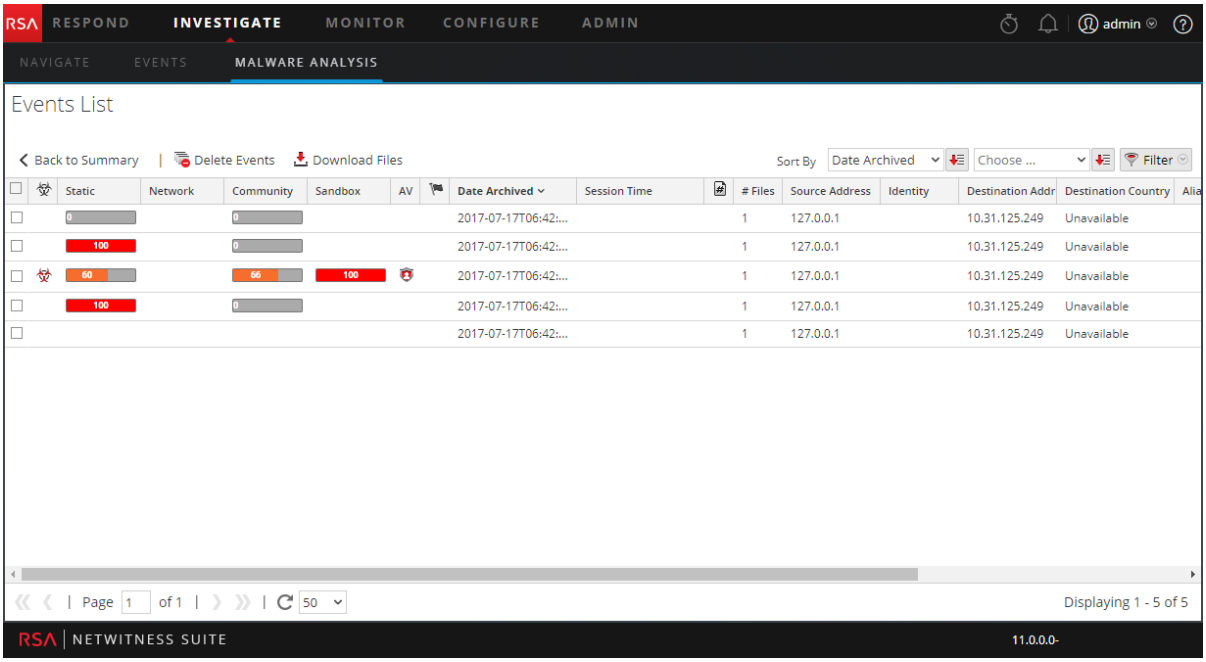
Um zur Ereigniszusammenfassung zurückzukehren, klicken Sie auf **Zurück zur Zusammenfassung**.

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.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
NAVIGATE
EVENTS
MALWARE ANALYSIS
Events List
Back to Summary
Delete Events
Download Files
Sort By
Date Archived
Choose ...
Filter
Static
Network
Community
Sandbox
AV
Date Archived
Session Time
Files
Source Address
Identity
Destination Addr
Destination Country
2017-07-17T06:42:...
1
127.0.0.1
10.31.125.249
Unavailable
Page 1 of 1
50
Displaying 1 - 5 of 5
RSA | NETWITNESS SUITE
11.0.0.0-

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. Um Updates zu erhalten, 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 1.7 (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 1.7 (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 Regelname 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“.

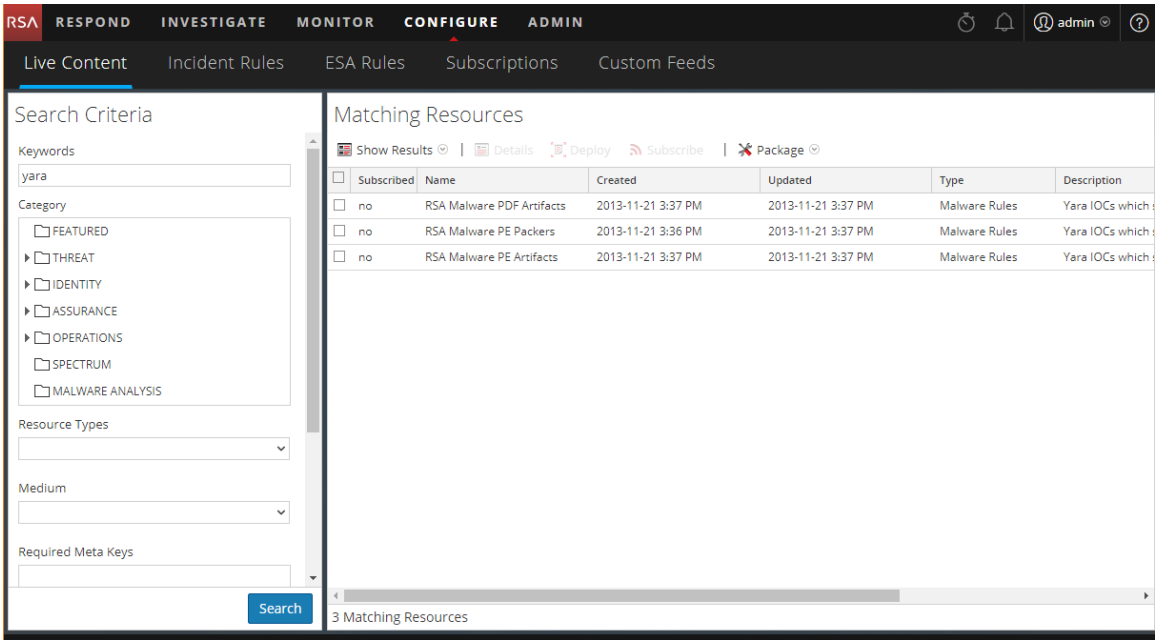
Hinweis: Weitere Informationen zu YARA-Ressourcen erhalten Sie unter der folgenden URL: https://code.google.com/p/yara-project/downloads/list. NetWitness Suite nutzt YARA 1.7, nicht YARA 2.0.

YARA-Inhalte

RSA Live beinhaltet drei Arten von YARA-Regeln:

- PE Packers
- PDF Artifacts
- PE Artifacts

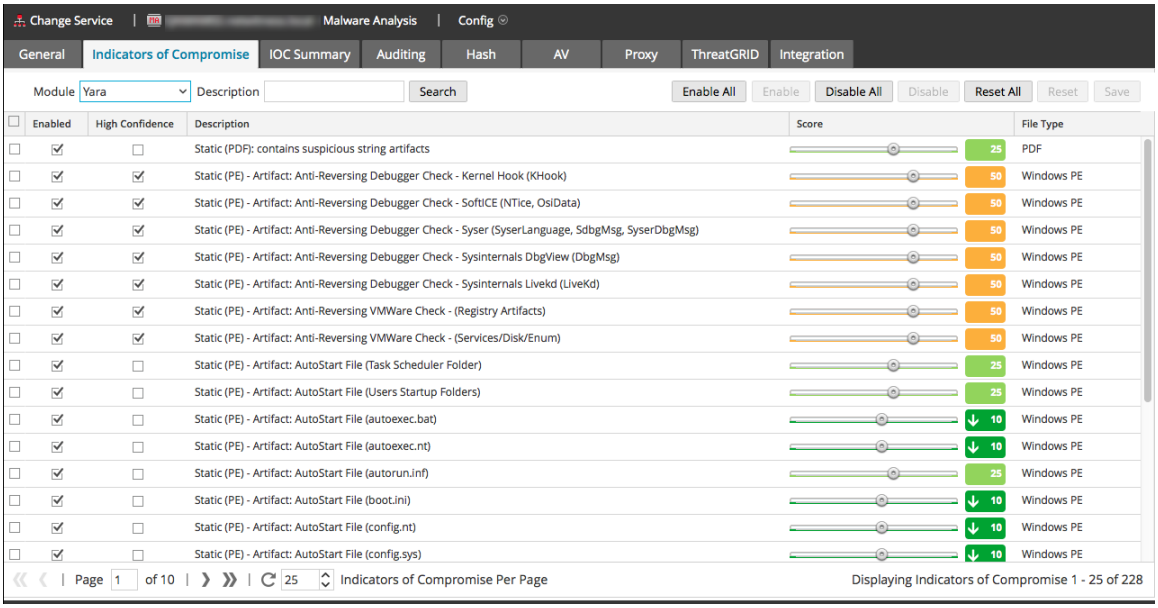
Die folgende Abbildung zeigt YARA-Inhalte verfügbar als YARA-Regeln in NetWitness Suite Live.



Auf dem Malware Analysis-Host befinden sich die YARA-Regeln in `/var/lib/rsamalware/spectrum/yara`, wie im folgenden Beispiel gezeigt.

```
[root@TESTHOST yara]# pwd
 /var/lib/rsamalware/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/rsamalware/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/rsamalware/spectrum/yara/watch`
   Die Datei wird innerhalb einer Minute verarbeitet.
   Sobald die Datei verarbeitet wurde, wird sie von NetWitness Suite 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 Suite 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 Suite 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.

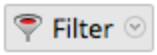
So sortieren Sie die Liste:

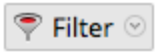
1. Wählen Sie in der ersten Drop-down-Liste **Sortieren nach** einen Spaltennamen und die Sortierreihenfolge aus:  für die absteigende oder  für die aufsteigende Reihenfolge.
2. (Optional) Wählen Sie in der zweiten Drop-down-Liste **Sortieren nach** einen Spaltennamen und die Sortierreihenfolge aus:  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 

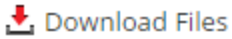
. Wenn das Dialogfeld „Filter“ angezeigt wird, klicken Sie auf **Zurücksetzen**.

Herunterladen von Dateien aus der Dateiliste

In NetWitness Suite 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 Suite 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).

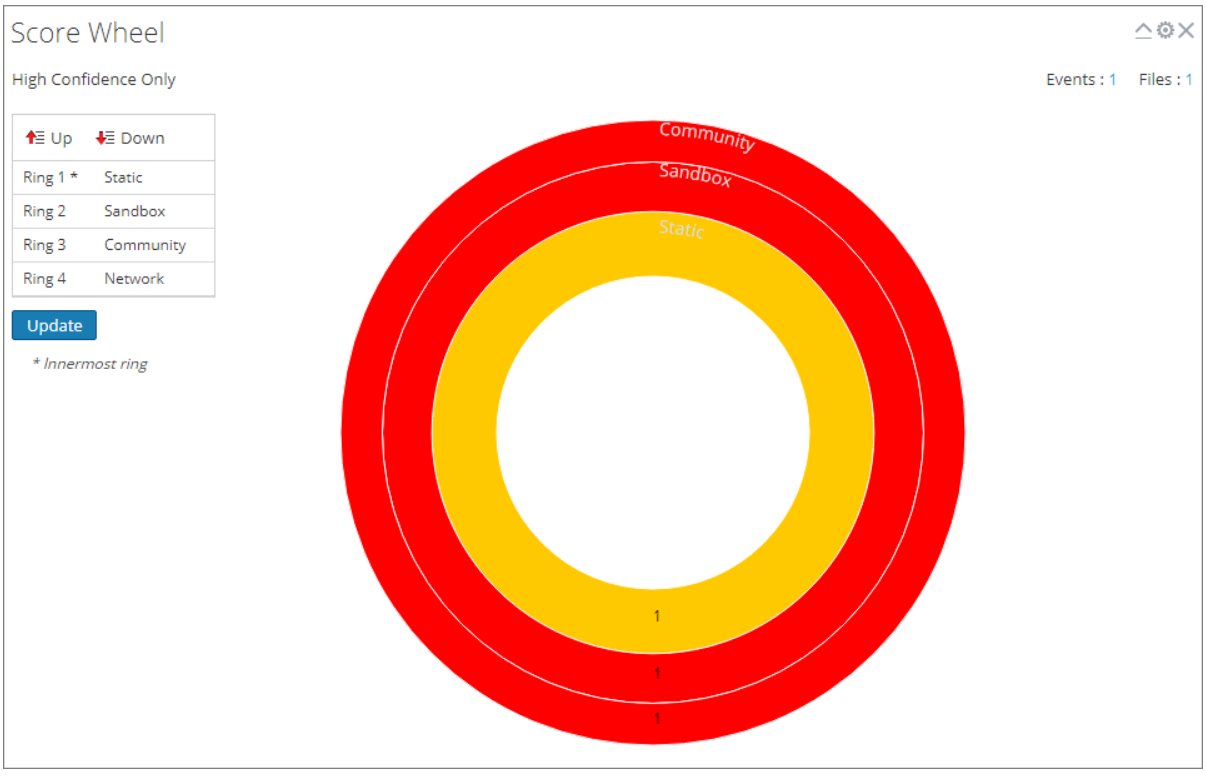
Filtern der Dashlet-Daten in der Ansicht Ereigniszusammenfassung

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 „Punktezahlrad“

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 Punktezahlrad 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.

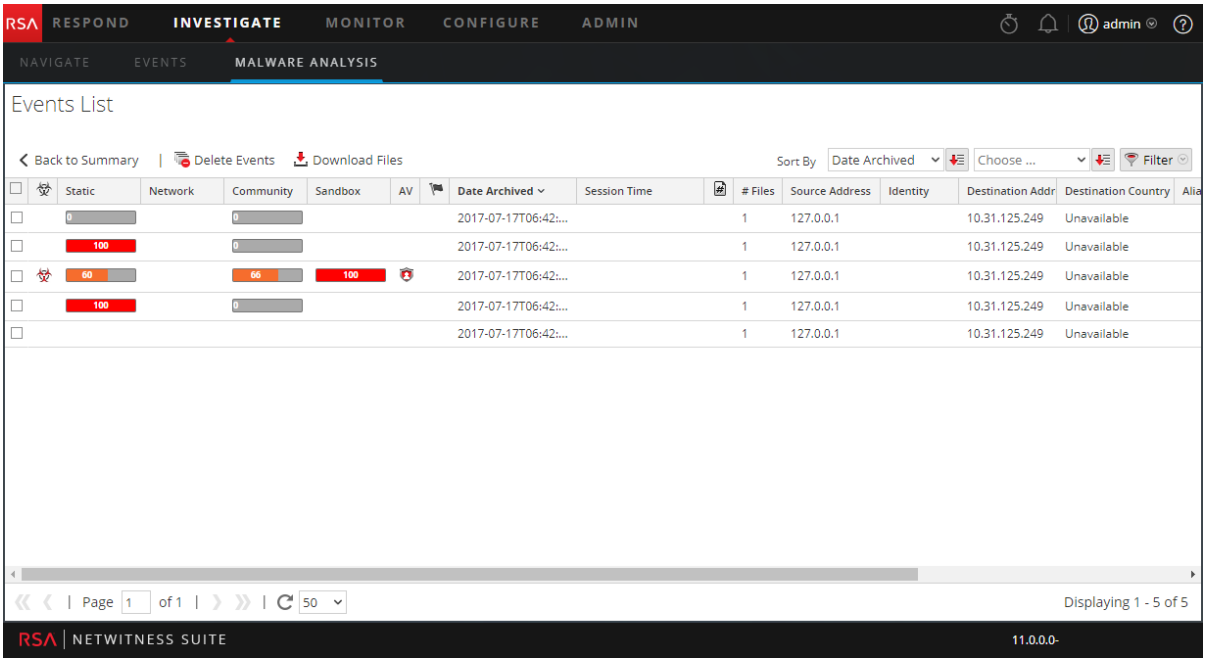


Sie können die Reihenfolge der Ringe ändern, um Indikatoren für eine Infizierung hervorzuheben, die nur in einer der Kategorien gekennzeichnet wurden. Das Vergleichen derselben Ergebnisse in unterschiedlichen Reihenfolgen der Ringe liefert Einblicke in zusätzliche Anfälligkeiten während einer Sitzung 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 Punktzahlrads 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 Punktzahlrads 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

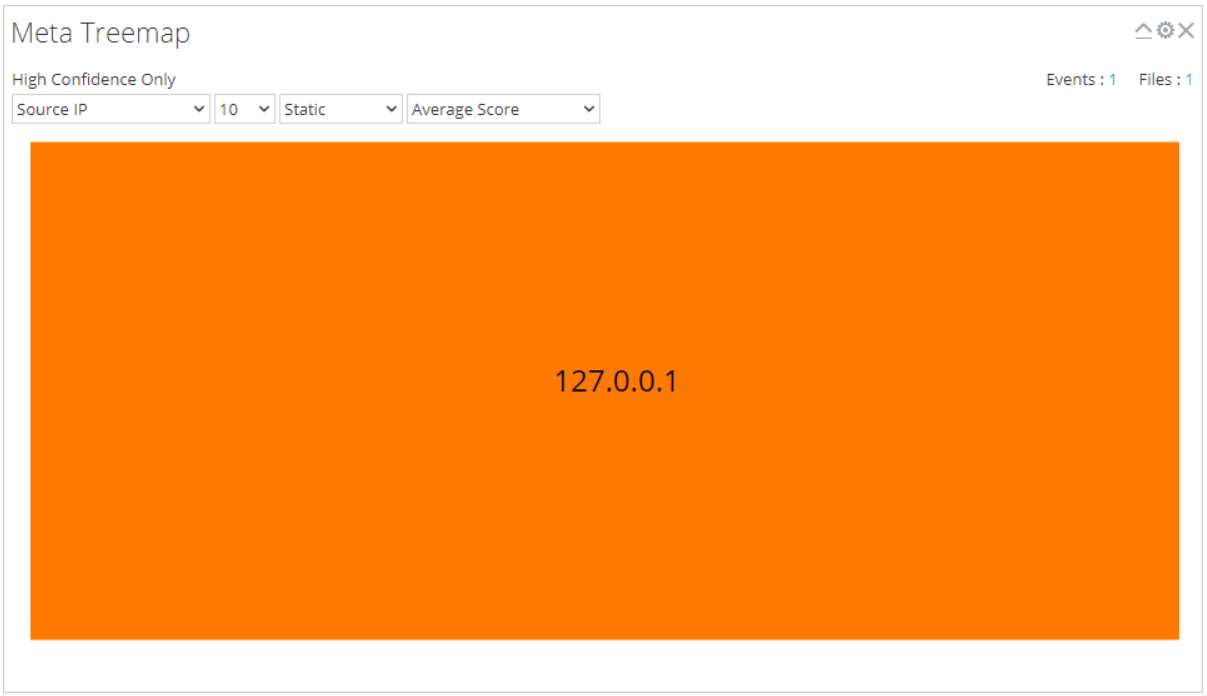
Im Punktezahlrad können Sie die Reihenfolge der Bereiche nach dem Bewertungsmodul ordnen. Zunächst ist die Reihenfolge der Bereiche von innen nach außen wie folgt: Statisch, Netzwerk, Community, und Sandbox.

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 Punktzahlrad wird mit der neuen Reihenfolge aktualisiert.

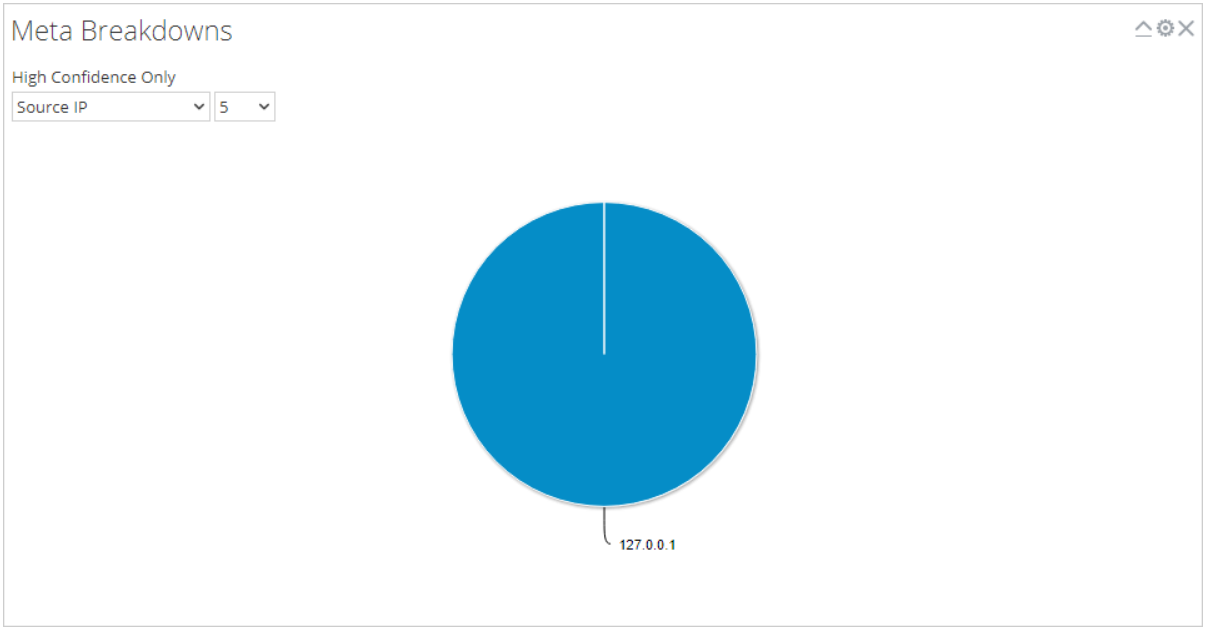
Konfiguration des Dashlet „Meta-Treemap“

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.



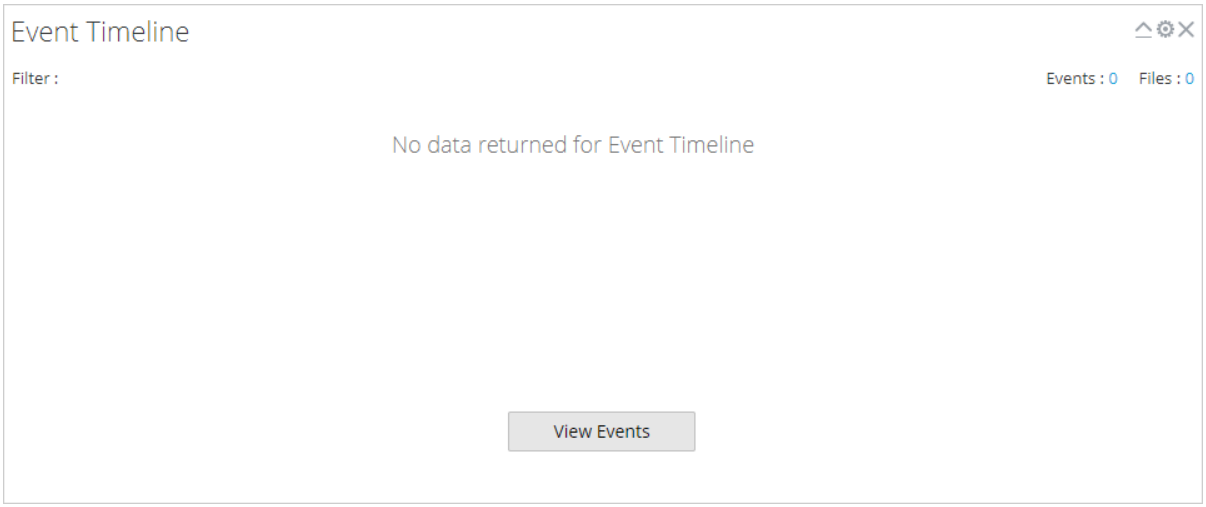
Konfiguration des Dashlet „Meta-Strukturen“

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.

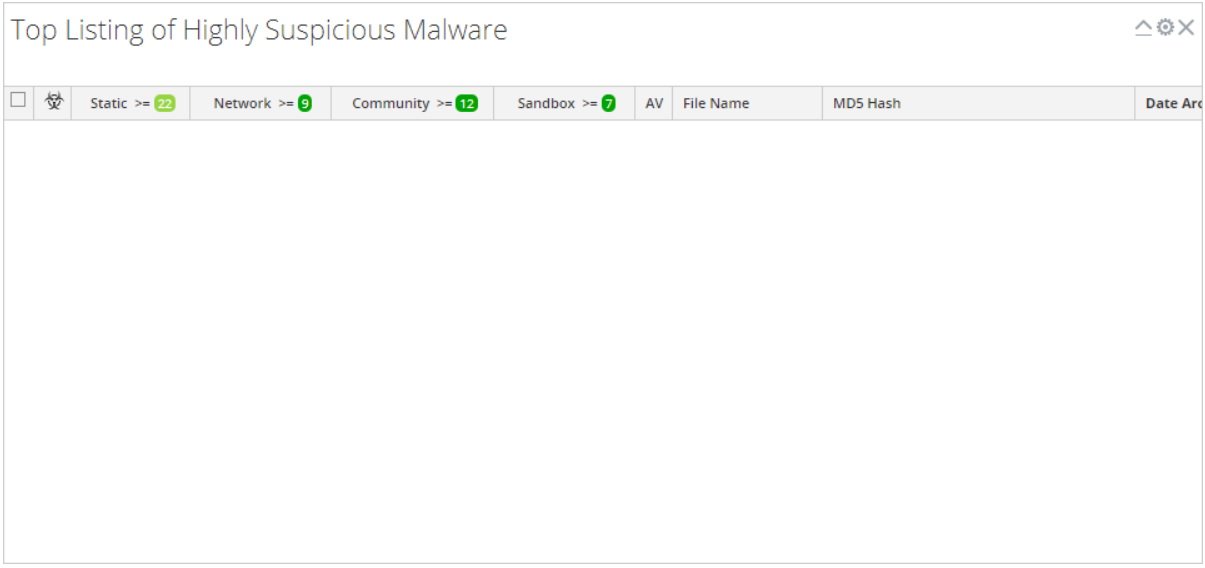


Öffnen aller Ereignisse in der Ereignisliste

Von der Ereigniszeitachse aus können Sie in der Ereignisliste die gesamte Liste der Ereignisse öffnen. Klicken Sie dazu auf View Events. 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.

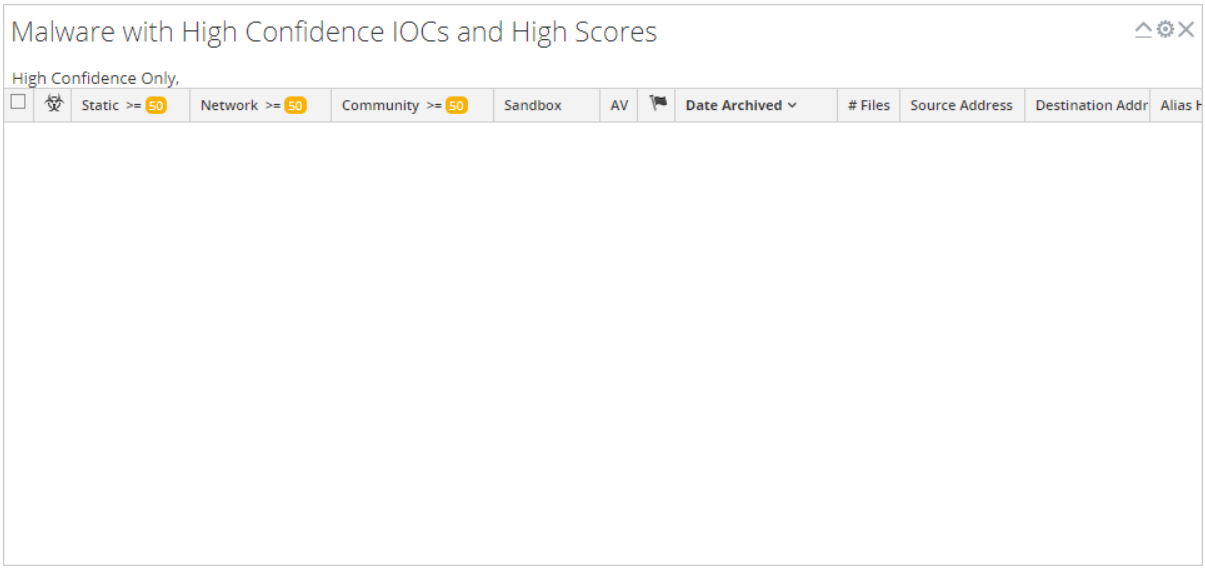
Konfiguration des Dashlet „Top-Liste höchst verdächtiger Schadsoftware“

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.



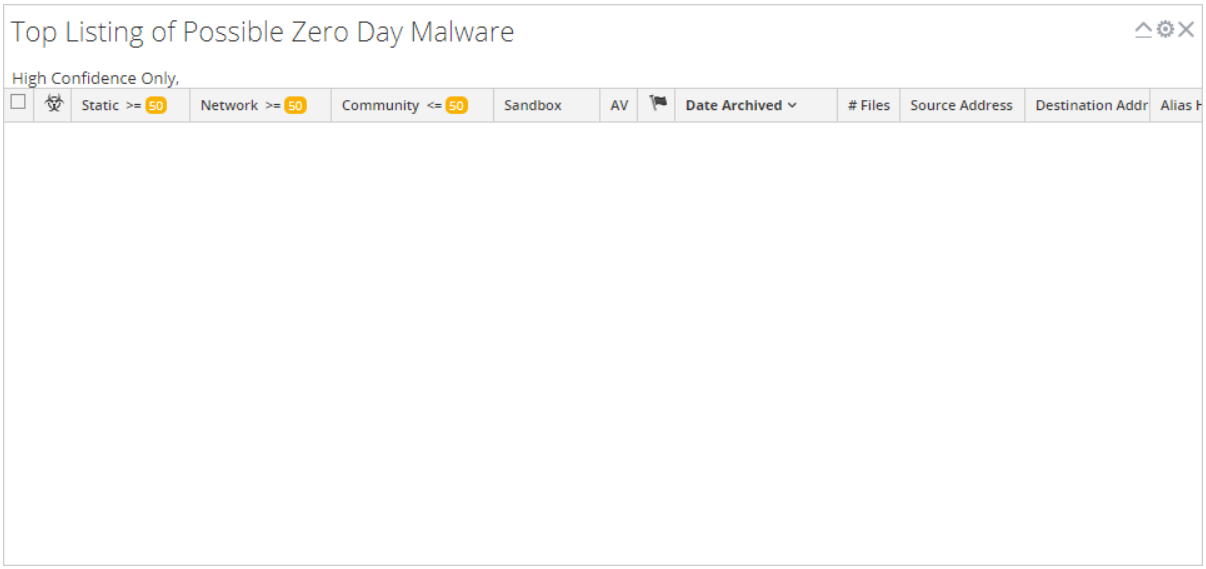
Konfiguration des Dashlet „Schadsoftware mit IOCs mit hoher Wahrscheinlichkeit und hohen Werten“

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.

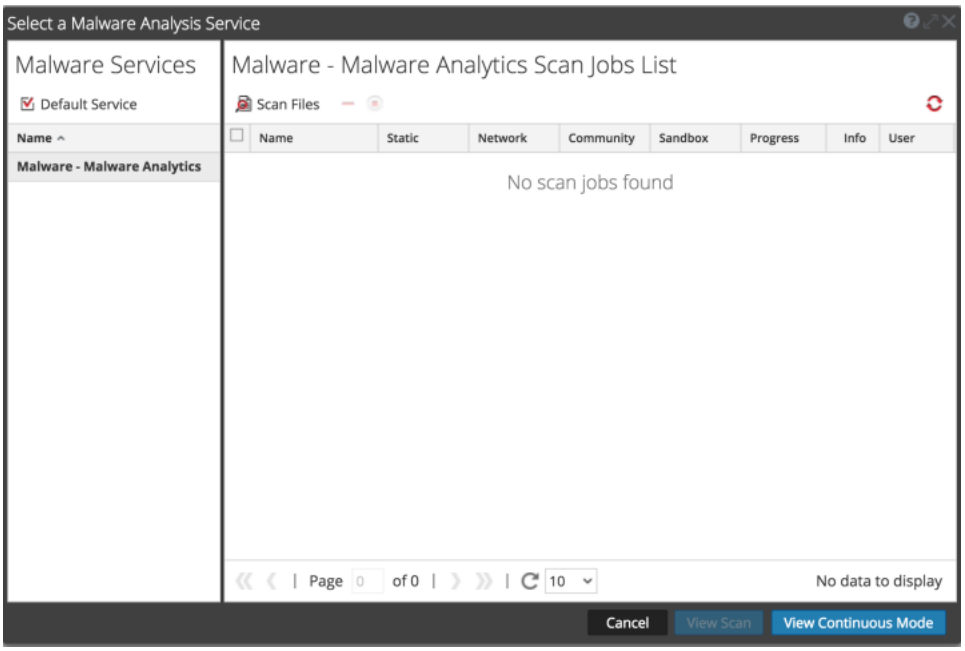
Es ist außerdem möglich, eine Datei zum Scannen mithilfe einer beobachteten Dateifreigabe hochzuladen.

Manuelles Hochladen von Dateien

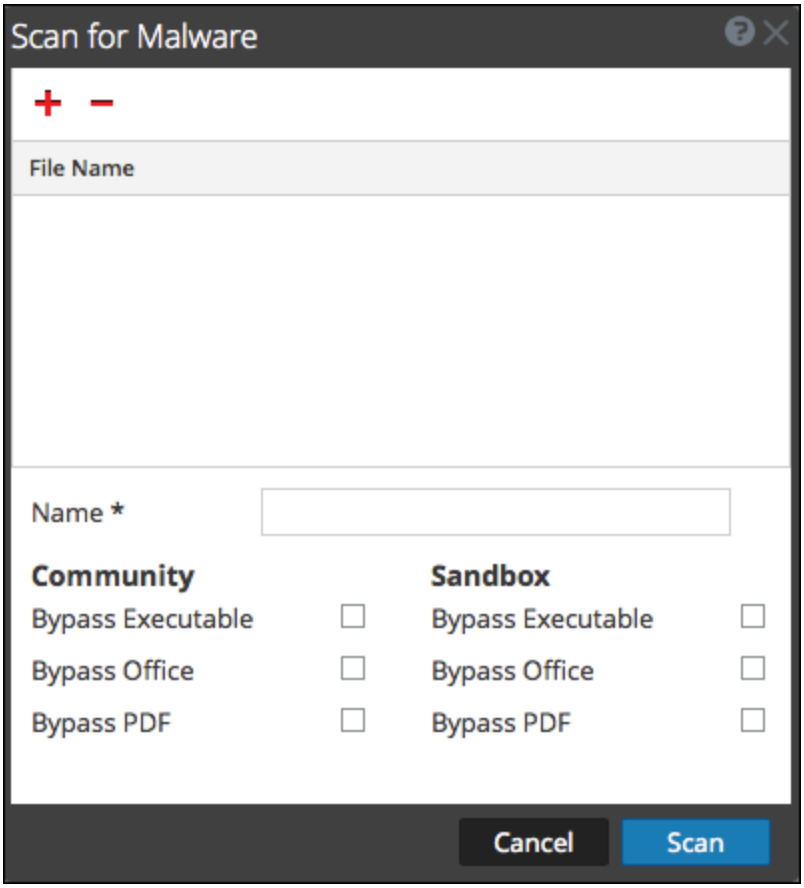
Dieses Thema beinhaltet Anweisungen zum Einleiten eines Scans von einer hochgeladenen Datei nach Bedarf. Wenn Sie eine Datei zum Scannen hochladen, startet NetWitness Suite den Uploadjob und fügt diesen der Jobwarteschlange hinzu. Wenn der Job beendet wurde, können Sie den Scan in Malware Analysis aufrufen.

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 Suite-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 Suite 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 wird für den ausgewählten Scan 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/rsamalware/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 Suite 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`.

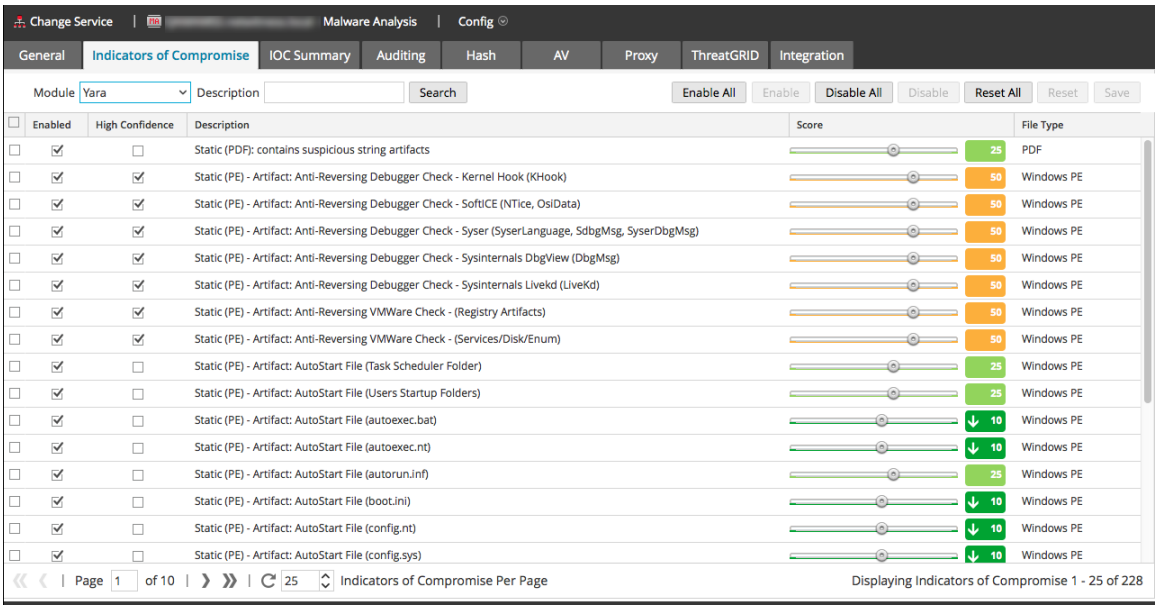
d. Verarbeitete Dateien werden aus dem Verzeichnis hashWatch nicht entfernt.

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/rsamalware/spectrum/yara/watch`
Die Datei wird innerhalb einer Minute verarbeitet.
Sobald die Datei verarbeitet wurde, wird sie von NetWitness Suite 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.

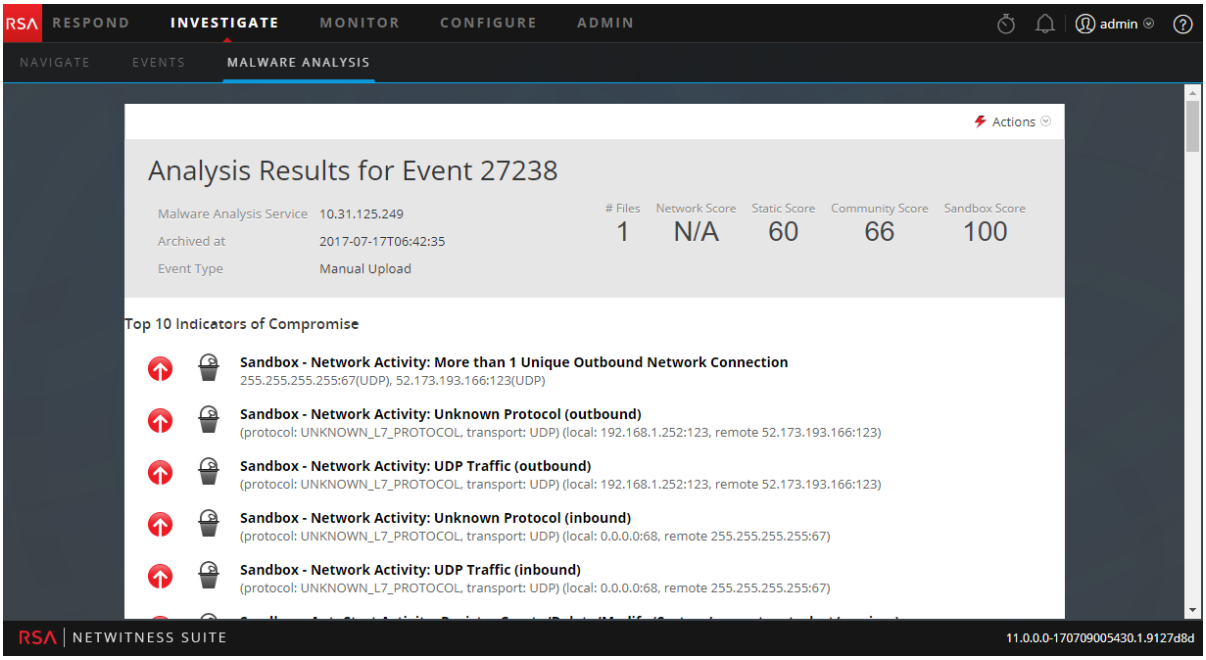
1. Komprimieren Sie, wenn Sie als Administrator angemeldet sind, die zu verarbeitenden Dateien in einer ZIP-Datei mit dem Passwort `infected` und speichern Sie sie unter `/var/lib/rsamalware/spectrum/infectedZipWatch/watch`. Innerhalb von ein oder zwei Minuten verarbeitet Malware Analysis das Archiv 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 Schadsoftwareanalyse-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.

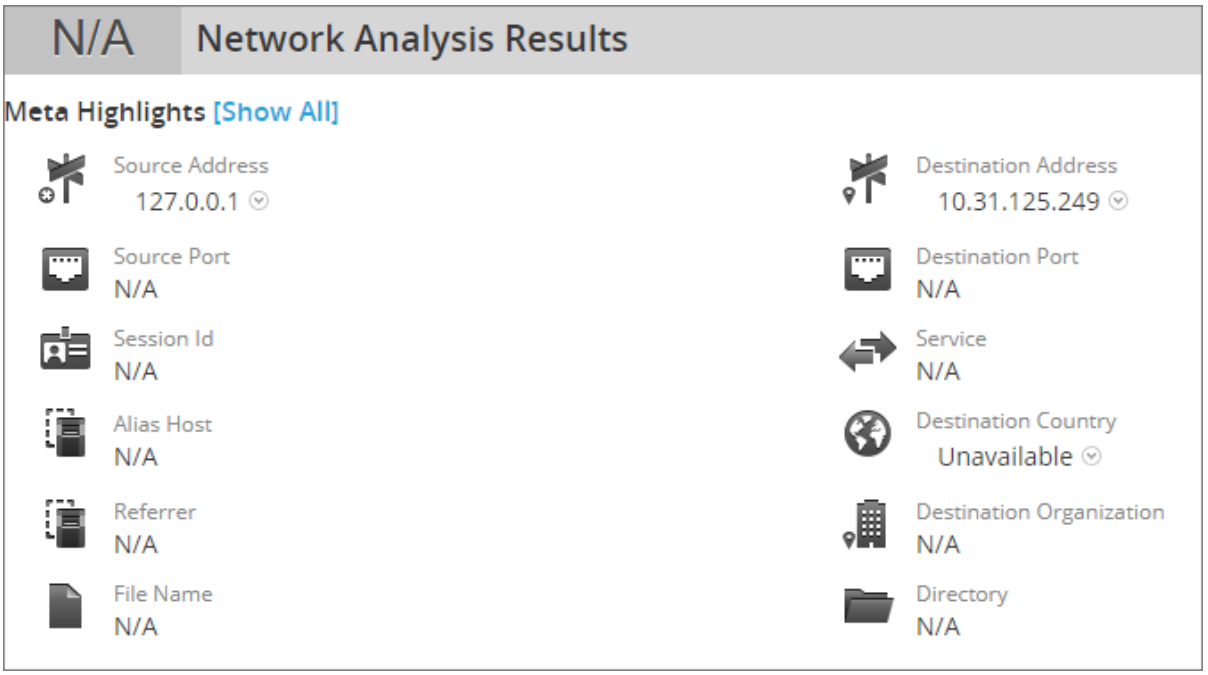


4. (Optional) Wenn Sie ein Ereignis löschen möchten, wählen Sie **Aktionen > Ereignis löschen**.
5. Wenn Sie eine Rekonstruktion der Netzwerksitzung anzeigen möchten, wählen Sie **Aktionen > Netzwerksitzung anzeigen**.
   Die Sitzung wird in der Ansicht „Navigieren“ > „Ereignisrekonstruktion“ angezeigt.

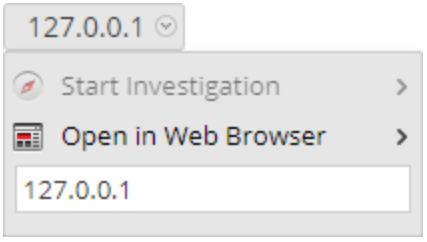
Pivotieren der Netzwerkanalyse-Ergebnisse

Sie können die Netzwerkanalyse-Ergebnisse auf mehreren Wegen pivotieren.

1. Blättern Sie nach unten zu den Netzwerkanalyse-Ergebnissen.



2. Bewegen Sie die Maus über einen Metawert und klicken Sie mit der linken Maustaste.
   Das Kontextmenü wird angezeigt.

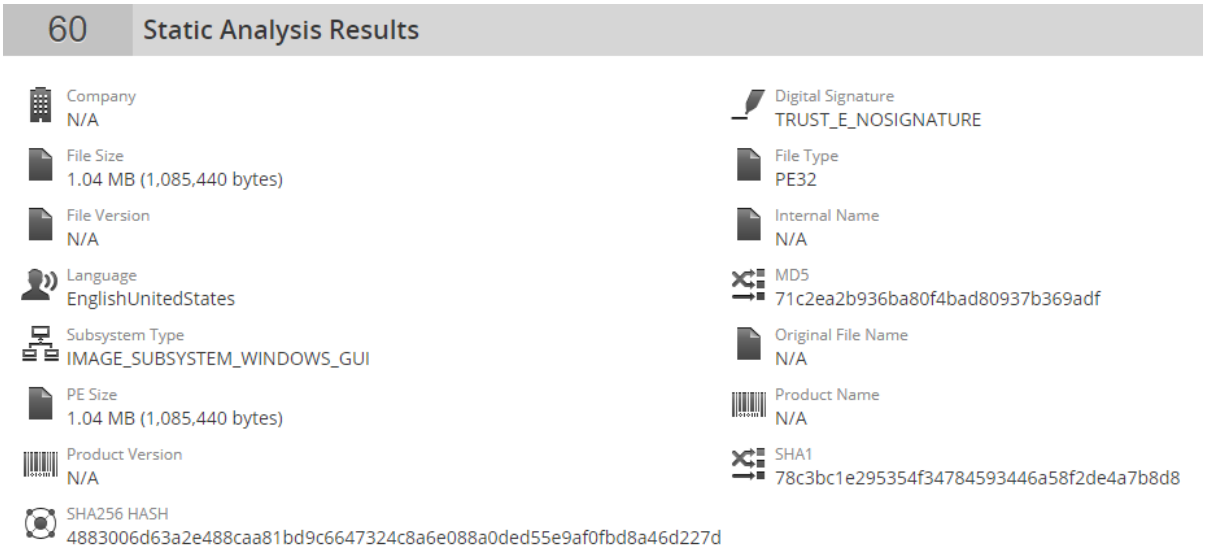


3. Um den ausgewählten Metawert in der Ansicht **Navigieren** anzuzeigen, wählen Sie **Ermittlungen starten** und eine Zeitoption aus.

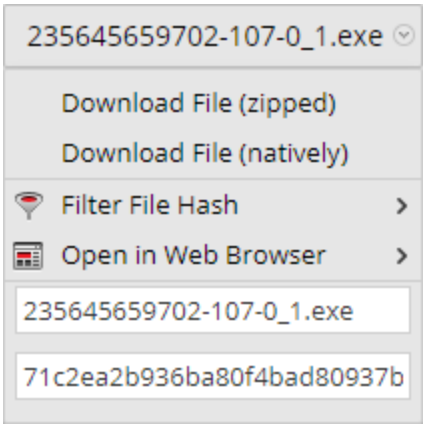
4. Um den ausgewählten Metawert in einem Browser anzuzeigen, wählen Sie **In Webbrowser öffnen > In Google öffnen**.

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

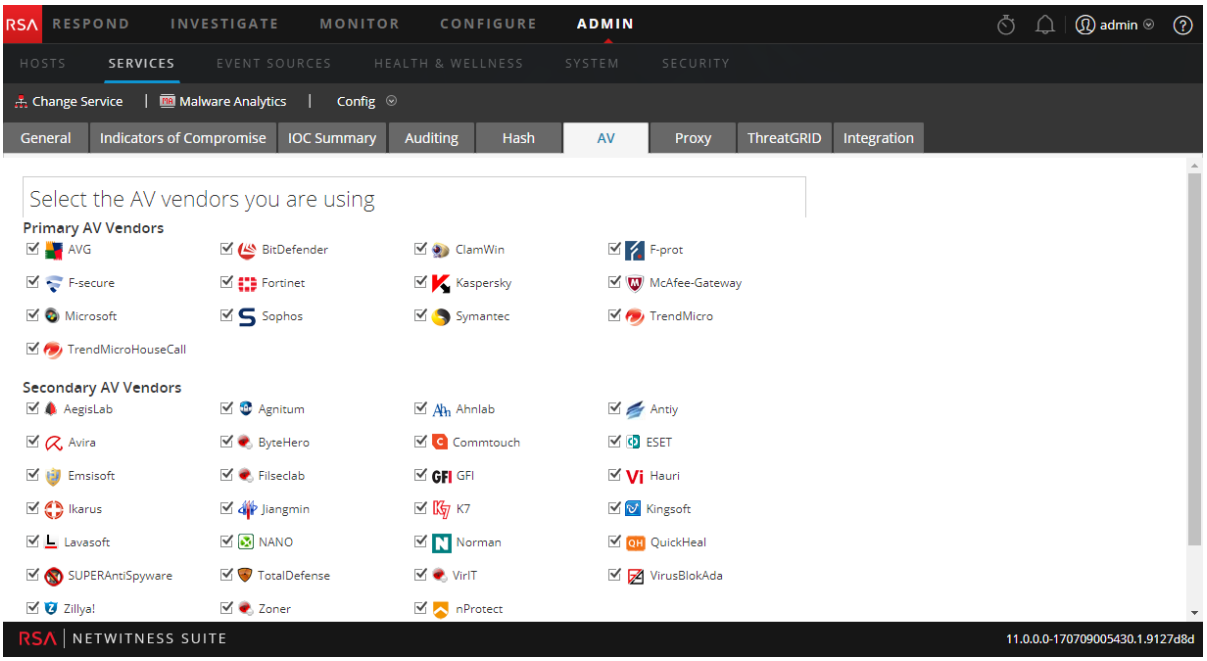
Die Community-Analyseergebnisse fassen Ergebnisse zusammen, die Indikatoren für eine Infizierung identifizieren, die als Risiko oder als harmlos markiert wurden.

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.

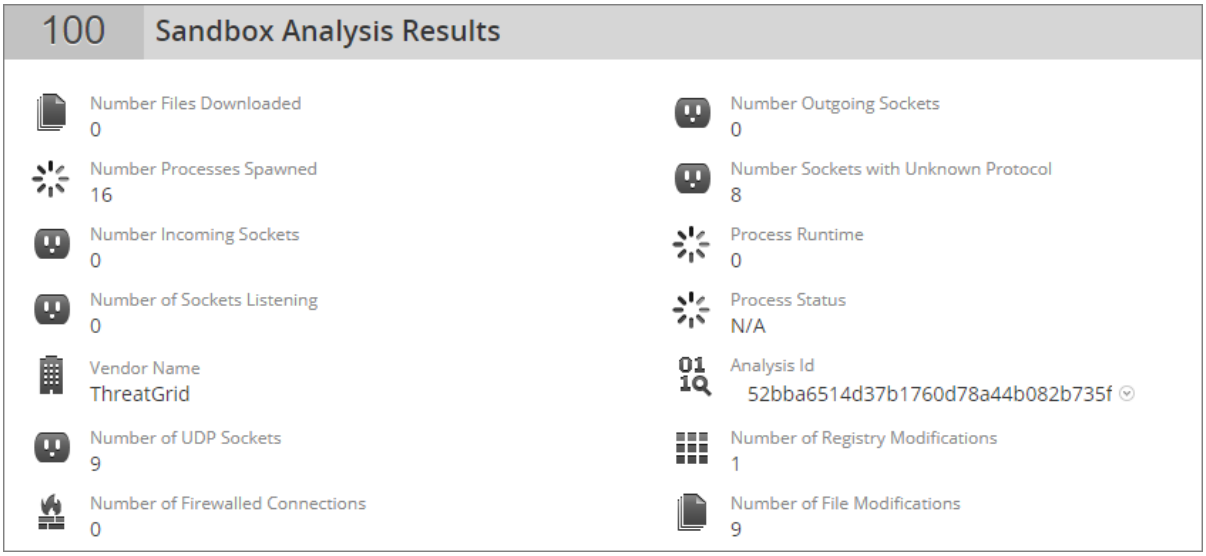
Wenn keine eingesetzten AV-Anbieter für den aktuellen Malware Analysis-Service konfiguriert wurden, wird folgende Meldung angezeigt: Es wurden keine AV-Anbieter als „Eingesetzt“ markiert. Rufen Sie die Seite „Malware Analysis-Servicekonfiguration“ auf, um die eingesetzten AV-Anbieter zu identifizieren.



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.

Ermittlungs-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.

- Ansicht „Navigieren“
- Ansicht Ereignisse
- Ansicht „Malware Analysis“
- Dialogfeld „Zur Liste hinzufügen/Aus Liste entfernen“
- Dialogfeld „Ereignisse zu einem Incident hinzufügen“
- Bereich „Kontextabfrage“
- Dialogfeld „Incident erstellen“
- Ansicht „Ereignisanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Textanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Paketanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Dateianalyse“
- Ansicht „Ereignisrekonstruktion“
- Dialogfeld „Untersuchen“
- Registerkarte „Investigation“ – Bereich „Benutzereinstellungen“
- Dialogfeld „Standardmetaschlüssel managen“
- Malware Analysis-Ereignisliste und -Dateiliste
- Dialogfeld „Spaltengruppen managen“
- Dialogfeld „Profile managen“
- Ansicht „Navigieren“
- Dialogfeld „Abfrage“
- Dialogfeld „Auf Schadsoftware scannen“

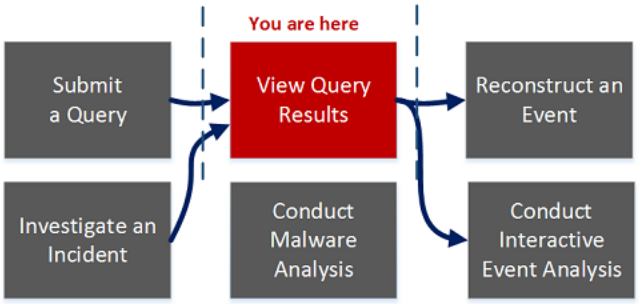
- Dialogfeld „Malware Analysis Service auswählen“
- Einstellungsdialogfeld für die Ansichten „Navigieren“ und „Ereignisse“

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 „Investigation > Ereignisse“ auf der Symbolleiste auf **Incidents > Zu vorhandenem Incident hinzufügen**.

Workflow



Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Ein oder mehrere Ereignisse zu einem vorhandenen Incident oder einem neuen Incident hinzufügen*	Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion
Threat Hunter	Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen*	Durchführen einer Ermittlung
Threat Hunter	Ereignis rekonstruieren	Rekonstruieren eines Ereignisses

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Interaktive Ereignisanalyse durchführen	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Incident-Experte	Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Schadsoftwareanalyse durchführen	Durchführen von Schadsoftwareanalysen

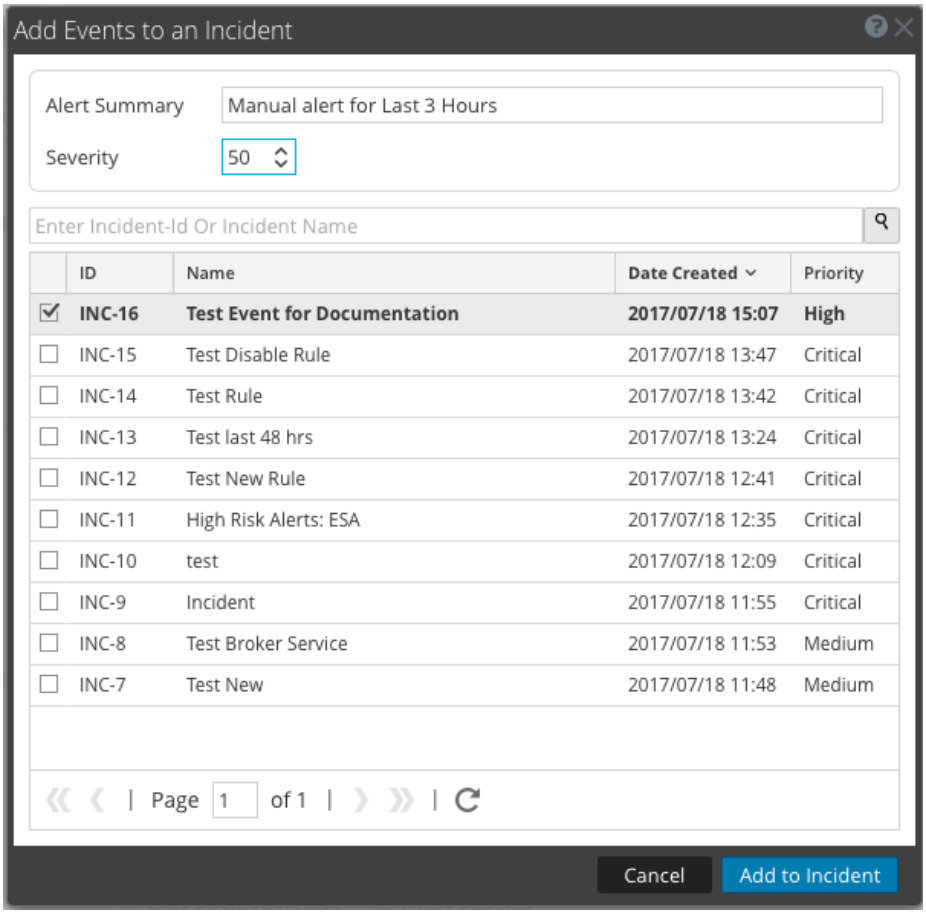
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Untersuchen von Ereignissen
- 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 „Ereignisse 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.

Funktion	Beschreibung
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.
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.

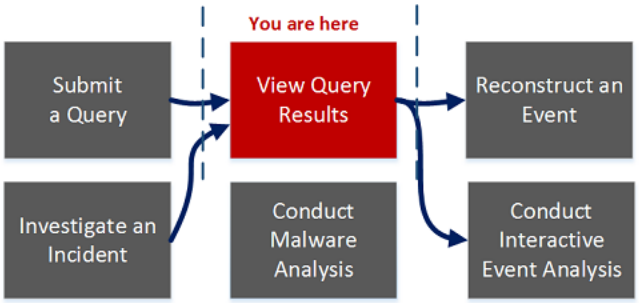
Dialogfeld „Zur Liste hinzufügen/Aus Liste entfernen“

Wenn Sie in Ermittlung arbeiten, können Sie IP-Adressen oder Benutzernamen in den Ansichten „Navigieren“ und „Ereignisse“ aufrufen. Im Dialogfeld „Zur Liste hinzufügen/Aus Liste entfernen“ können Sie einer bestehenden Context Hub-Liste Metawerte für die Metaschlüssel `Source IP`, `Destination IP` oder `Username` hinzufügen oder eine neue Liste mit den Metawerten erstellen. Wenn Sie einer Liste Metawerte hinzufügen, können Sie nach zusätzlichem Kontext für diese Metawerte suchen.

Rufen Sie das Dialogfeld auf, indem Sie unter `Source IP`, `Destination IP`, oder `Username` mit der rechten Maustaste auf einen Metawert klicken und im Kontextmenü **Zur Liste hinzufügen/Aus Liste entfernen** auswählen.

Workflow

Das folgende Workflowdiagramm zeigt den allgemeinen Workflow für „Untersuchen“. Die Position der aktuellen Aktivität ist hervorgehoben.



Was möchten Sie tun?

Benutzerrolle	Ich möchte…	Dokumentation
Threat Hunter	einer Context Hub-Liste Metawerte hinzufügen.*	Managen von Context Hub-Listen und -Listenwerten in Investigate
Threat Hunter	eine Context Hub-Liste erstellen.	Managen von Context Hub-Listen und -Listenwerten in Investigate

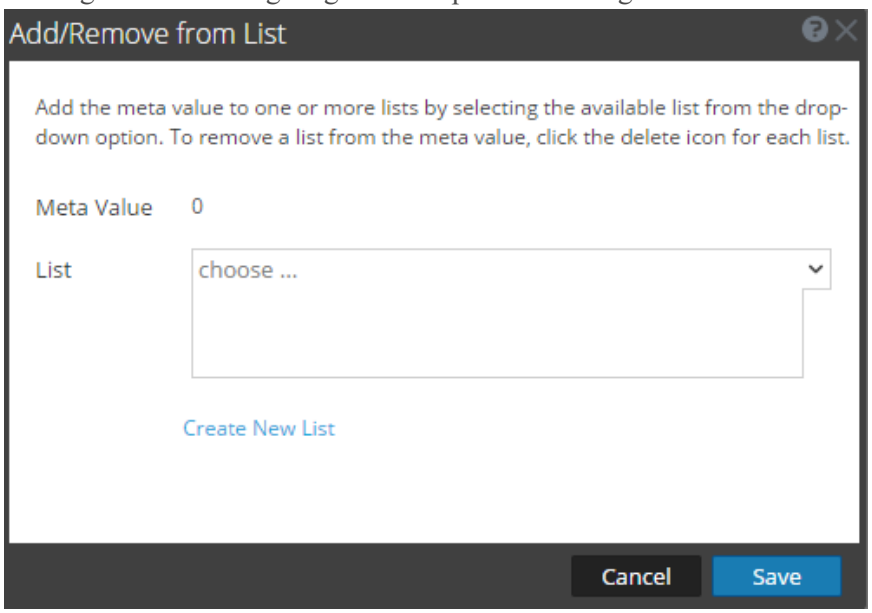
Benutzerrolle	Ich möchte…	Dokumentation
Threat Hunter	eine Abfrage senden.	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen.	Durchführen einer Ermittlung
Threat Hunter	ein Ereignis rekonstruieren.	Rekonstruieren eines Ereignisses
Threat Hunter	ein Ereignis analysieren.*	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Incident-Experte	einen Incident untersuchen.	*NetWitness Respond – Benutzerhandbuch*

Verwandte Themen

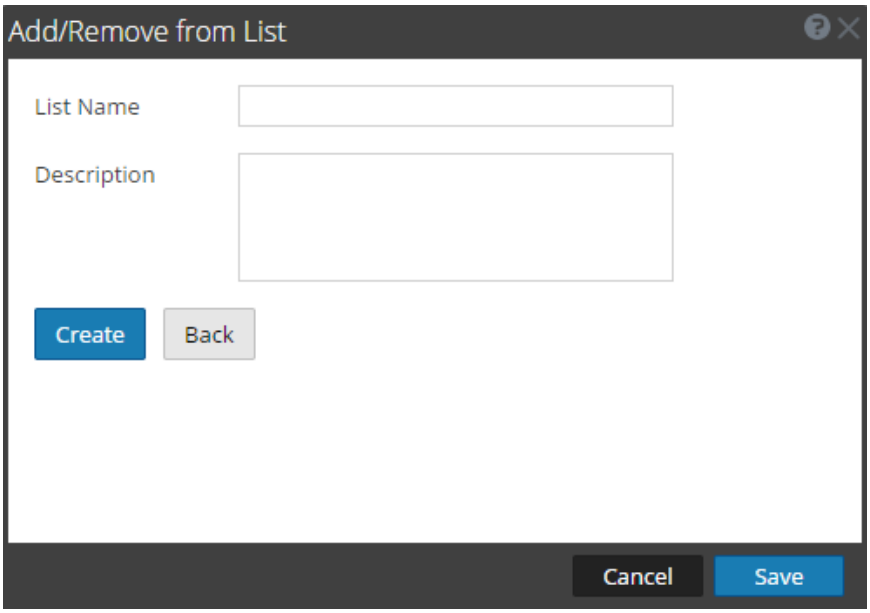
- Anzeigen von zusätzlichem Kontext für einen Datenpunkt
- Untersuchen von Ereignissen
- Ansicht Ereignisse

Überblick

Die folgende Abbildung zeigt ein Beispiel des Dialogfelds beim ersten Öffnen.



Die folgende Abbildung zeigt das Dialogfeld, wenn Sie „Neue Liste erstellen“ auswählen.



Die folgende Tabelle beschreibt die Funktionen der Dialogfelder „Zur 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.

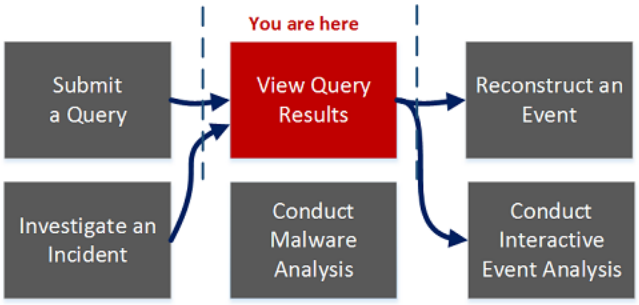
Funktion	Beschreibung
Liste	Die Liste, zu der der ausgewählte Metawert hinzugefügt werden muss. Ein Drop-down-Menü bietet eine Liste der verfügbaren Listen an, denen Sie den Metawert hinzufügen können.
Neue Liste erstellen	Öffnet ein neues Dialogfeld, in dem Sie eine neue Liste für den ausgewählten Metawert erstellen können.
Listenname	Der Name der neuen Liste
Beschreibung	Die Beschreibung der neuen Liste
Erstellen	Erstellen Sie 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.

Bereich „Kontextabfrage“

Sobald ein Administrator den Context Hub-Service konfiguriert hat, werden die Kontextinformationen der Metawerte in der Ansicht **Navigieren** und der Ansicht **Ereignisse** von Investigate angezeigt. 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 „Navigieren“ und der Ansicht „Ereignisse“ des Moduls Investigation angezeigt. Metawerte, die einer Context Hub-Liste hinzugefügt wurden, sind im Bereich „Werte“ der Ansicht „Navigieren“ grau hervorgehoben. 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.

Workflow



Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Metwawerte untersuchen*	Anzeigen von zusätzlichem Kontext für einen Datenpunkt
Threat Hunter	Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Abfrageergebnisse anzeigen*	Durchführen einer Ermittlung
Threat Hunter	Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	Interaktive Ereignisanalyse durchführen	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Incident-Experte	Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

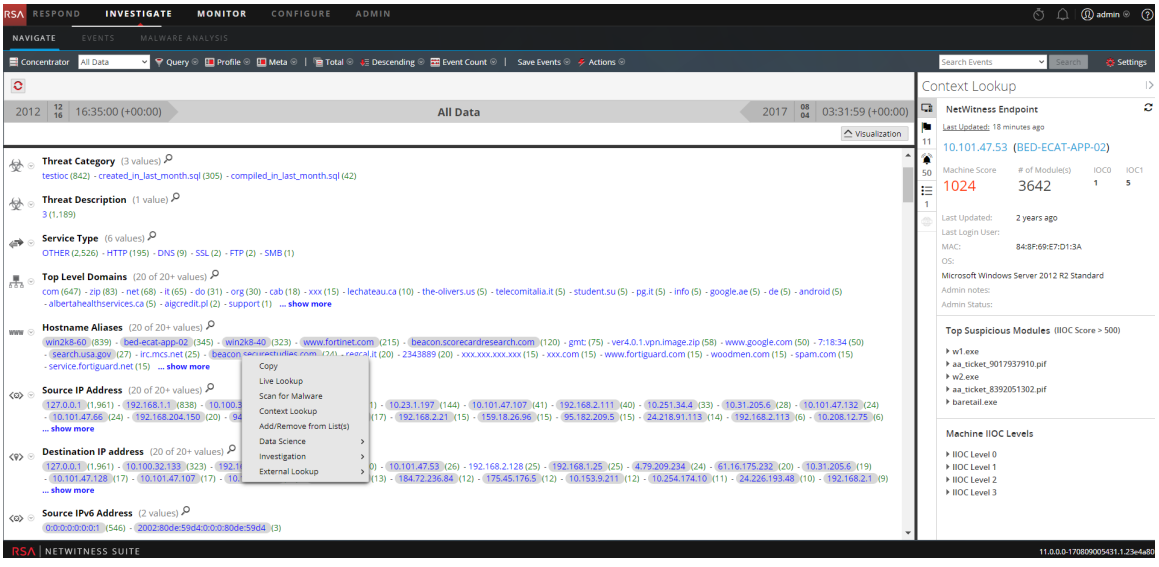
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Ansicht Ereignisse
- Ansicht „Navigieren“
- „NetWitness-Feedback und Datenfreigabe“ im *Handbuch Live-Services-Management*
- Anzeigen von zusätzlichem Kontext für einen Datenpunkt

Überblick

Die folgende Abbildung zeigt ein Beispiel für den Bereich „Kontextabfrage“. Die Steuerelemente und Funktionen werden 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
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 (Ergebnisse der ersten n)	Die Fußzeile enthält die Anzahl der Gesamtzahl von Ergebnissen sowie die Anzahl der derzeit angezeigten Ergebnisse. Beispiel: 50 Warnmeldungen (erste 50 Warnmeldungen).

Abfrageergebnisse

Wenn Sie Kontextdaten aus den konfigurierten Quellen abrufen, werden im Bereich „Kontextabfrage“ die nachfolgend aufgeführten Informationen angezeigt.

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
- Zuletzt aktualisiert: 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
- Zuletzt aktualisiert: 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:

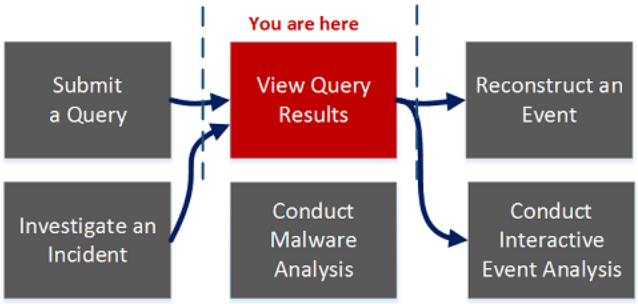
- Computername und IP-Adresse des Computers.
  Durch Klicken auf die IP-Adresse oder den Endpoint-Rechernamen werden Sie zur Endpoint-Benutzeroberfläche weitergeleitet, wo Sie weitere Untersuchungen vornehmen können.
- Zuletzt aktualisiert: Gibt an, wann zuletzt kontextbezogene Daten aus der Datenquelle 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.
- Zuletzt aktualisiert: Gibt an, wann die Scanergebnisse zuletzt in der Endpoint-Datenbank aktualisiert wurden.
- Zuletzt angemeldeter Benutzer
- 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

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?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Incident erstellen oder einem Incident Ereignisse hinzufügen*	Hinzufügen von Ereignissen zu einem Incident zwecks Reaktion
Threat Hunter	Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen*	Durchführen einer Ermittlung
Threat Hunter	Ereignis rekonstruieren	Rekonstruieren eines Ereignisses

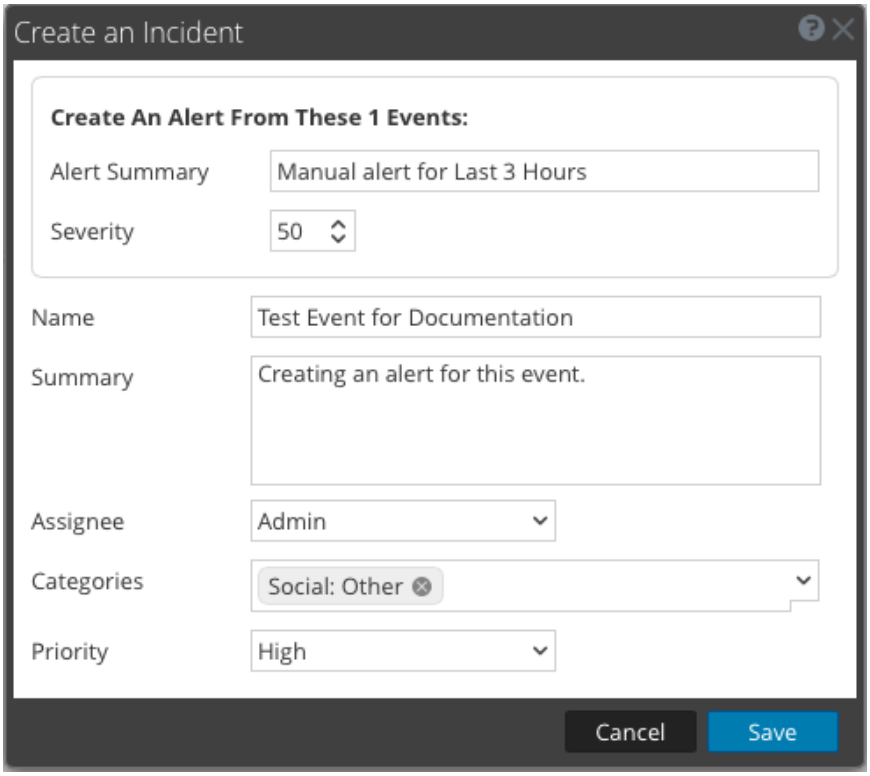
Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Interaktive Ereignisanalyse durchführen	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Incident-Experte	Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- 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 Benutzer 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.
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“

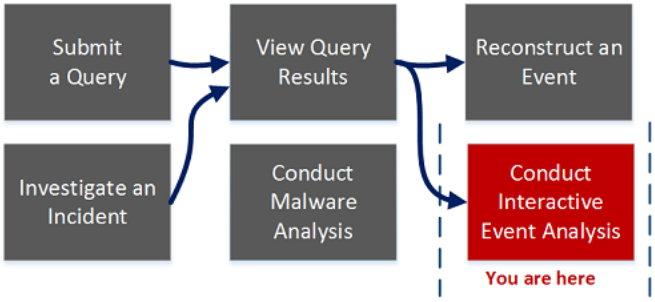
In der Ansicht „Ereignisanalyse“ stehen Ihnen interaktive Funktionen zur Verfügung, die Ihnen helfen, bedeutsame Datenmuster zu identifizieren. Diese Ansicht ist eine Alternative zur statischen Ansicht „Ereignisrekonstruktion“. Analysten, denen eine Benutzerrolle mit Zugriff auf die Ansicht „Ereignisanalyse“ zugewiesen ist, können Netzwerk-, Protokoll- und Endpunktereignisse in der Ansicht „Ereignisanalyse“ untersuchen. Dabei haben Sie die Wahl zwischen dieser Ansicht und der Ansicht „Ereignisrekonstruktion“.

In der Ansicht „Ereignisanalyse“ werden die Ereignisse im Zusammenhang mit dem aktuellen Drill-down-Punkt in der Ansicht „Navigation“ aufgelistet, geordnet nach Uhrzeit. Wenn Sie auf ein Ereignis klicken, wird im selben Browserfenster entweder der Bereich „Netzwerkereignisdetails“, der Bereich „Protokollereignisadetails“ oder der Bereich „Endpunktereignisdetails“ geöffnet. Für jeden Ereignistyp stehen ein oder mehrere Analysetypen zur Verfügung: Textanalyse, Paketanalyse und Dateianalyse.

Öffnen können Sie dieses Fenster wie folgt:

- Klicken Sie in der Ansicht „Ereignisse“ bei geöffneter Detailansicht unten im Ereignis auf **Ereignisanalyse**.
- Klicken Sie auf der Symbolleiste im Bereich „Ereignisrekonstruktion“ auf **Ereignisanalyse**.

Workflow



Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Abfrageergebnisse anzeigen	Durchführen einer Ermittlung
Threat Hunter	Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	Ereignis analysieren*	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Schadsoftwareanalyse durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

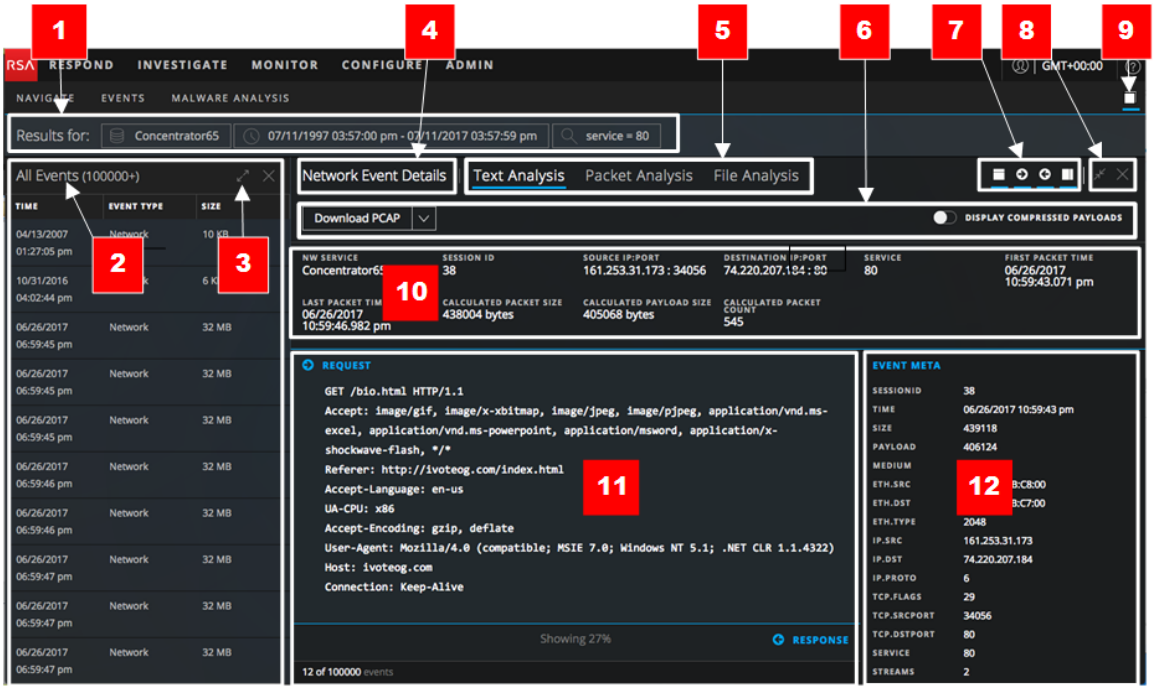
Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Ereignisanalyse“ – Bereich „Paketanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Textanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Dateianalyse“

Überblick

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 1.000 Ereignisse (Paketereignisse, Protokollereignisse und Endpunktereignisse) werden in die Ereignisliste geladen. In den Spalten der Ereignisliste werden der Zeitpunkt des Ereigniseintritts, der Ereignistyp (Netzwerk, Protokoll oder Endpunkt), die Ereignisgröße und eine Übersicht aufgeführt. Sie können:

- durch die Liste scrollen und durch Klicken auf **Weitere laden** die nächsten 100.000 Ereignisse anzeigen.
- die Spaltenreihenfolge per Drag-and-Drop ändern.
- die Spaltenbreite anpassen.
- die Ereignisanalyse eines Ereignisses anzeigen.



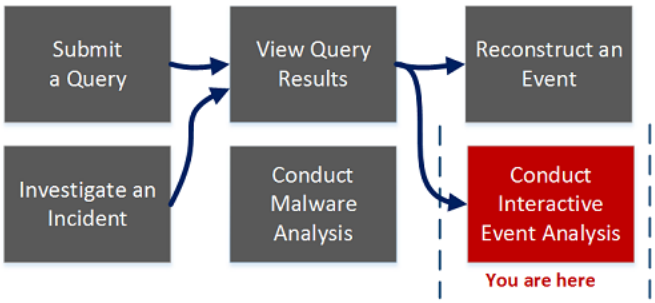
1	Die schreibgeschützte Brotkrümelnavigation zeigt die Abfrage, über die das Dataset generiert wurde. Alle Abfragen werden in der Ansicht „Navigieren“ oder in der Ansicht „Ereignisse“ ausgeführt.
2	Eine schreibgeschützte Liste aller Ereignisse, zusammengestellt auf Basis der Abfrage aus der Ansicht „Navigieren“ oder der Ansicht „Ereignisse“. In der Ereignisliste wird die Gesamtanzahl der Ereignisse angezeigt. Reihenfolge und Breite der Spalten lassen sich anpassen. Sie können bis zum Ende der Liste scrollen und dort weitere Ereignisse laden (siehe Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“).
3 und 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 Analysieren 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 Analysieren 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 Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“ beschrieben.  Klicken Sie auf dieses Symbol, um den Ereignis-Header auszublenden oder einzublenden. Durch Ausblenden der Kopfzeile steht mehr Platz für die Paketliste zur Verfügung und Sie müssen weniger scrollen, wenn Sie weitere Pakete sehen möchten.  Klicken Sie auf dieses Symbol, um den Bereich „Ereignis-Metadaten“ für das Ereignis in einem anderen Bereich anzuzeigen.
9	Öffnet die Ereignisliste oder den Bereich „Ereignis-Metadaten“ wieder, falls sie geschlossen wurden.
10	Ereignis-Header mit 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 Analysieren 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, das Ihnen in der Ansicht „Navigieren“ oder in der Ansicht „Ereignisse“ aufgefallen ist.

Workflow



Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen	Durchführen einer Ermittlung
Threat Hunter	Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	Ereignis analysieren*	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Dateien aus einem Ereignis exportieren*	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Schadsoftwareanalyse durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

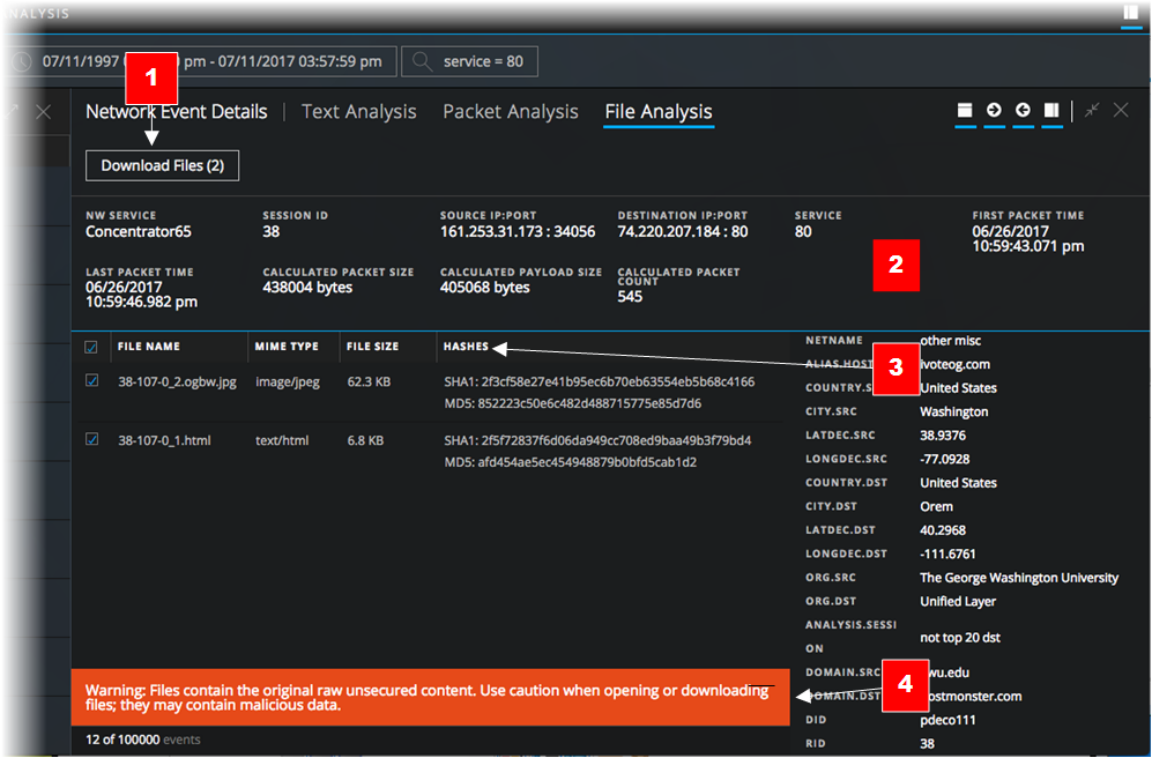
Verwandte Themen

- 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.

Unten sehen Sie ein Beispiel für einen Dateianalyse.

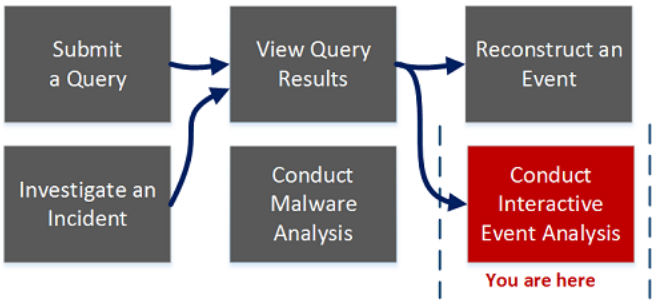


1	Klicken Sie auf diese Schaltfläche, um eine oder mehrere ausgewählte Dateien herunterzuladen.
2	Im Ereignis-Header sind Übersichtsinformationen zu dem Netzwerkereignis aufgeführt, das die Dateien enthält.
3	Scrollbare Liste mit allen dem Ereignis zugeordneten Dateien, die sich jeweils auswählen und 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, das Ihnen in der Ansicht „Navigieren“ oder in der Ansicht „Ereignisse“ aufgefallen ist.

Workflow



Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen	Durchführen einer Ermittlung
Threat Hunter	Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	Ereignis analysieren*	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Dateien aus einem Ereignis exportieren*	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Schadsoftwareanalyse durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

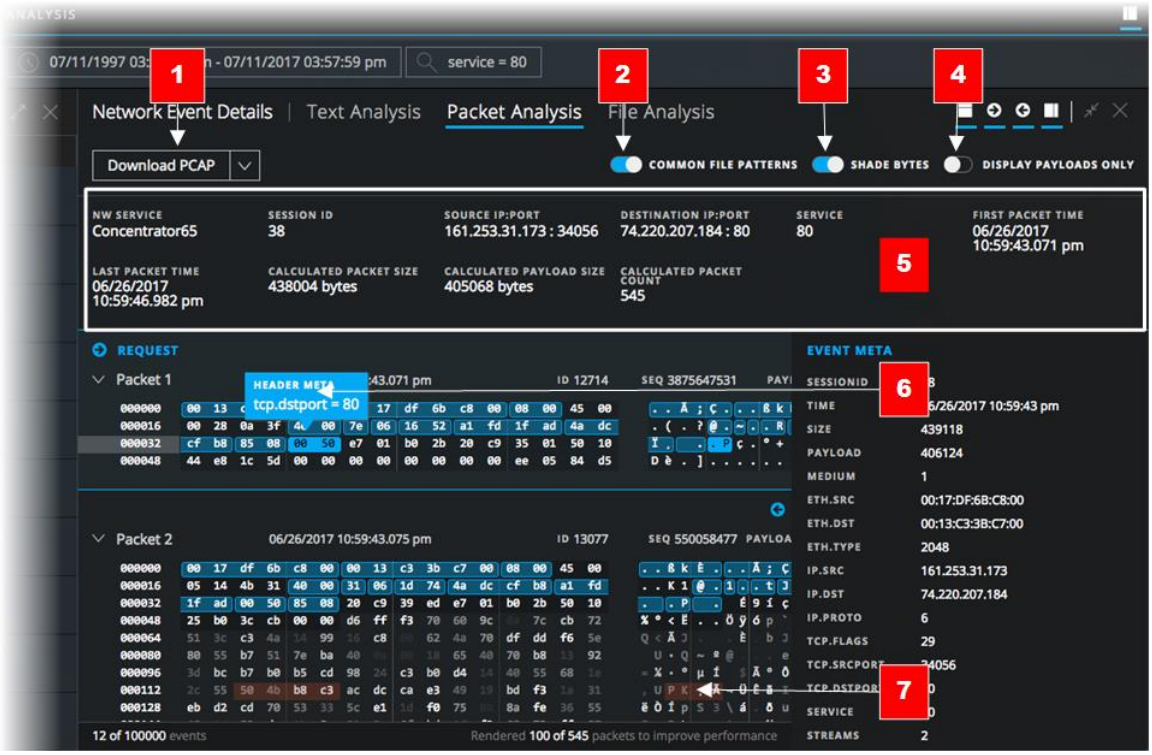
- Wie funktioniert NetWitness Investigate?
- Ansicht „Ereignisanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Textanalyse“
- Ansicht „Ereignisanalyse“ – Bereich „Dateianalyse“

Überblick

Im Bereich Paketanalyse können ausschließlich Netzwerkereignisse analysiert werden. Im Bereich Paketanalyse werden alle Pakete in einem Ereignis aufgeführt. Für jedes Paket werden die Paketnummer, die Richtung (Anforderung oder Antwort) und der Paketinhalt angezeigt, Letzterer links im Binärformat, in der Mitte im hexadezimalen Format und rechts im Textformat. 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.

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.

Unten sehen Sie ein Beispiel für den Bereich „Paketanalyse“.



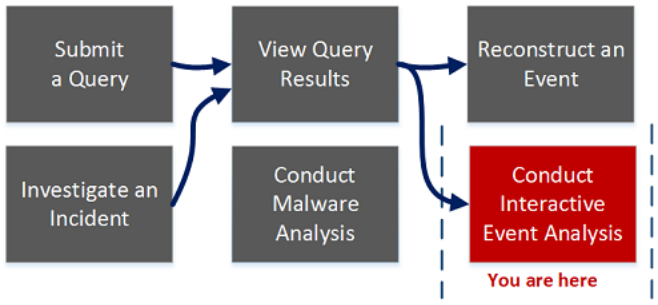
1	Optionen zum Exportieren eines Netzwerkereignisses. Sie können zwecks eingehenderer Analyse oder Weiterleitung an Dritte wahlweise eine PCAP-Datei, alle Nutzlasten, Anforderungsnutzlasten oder Antwortnutzlasten exportieren.
2	Die Option zur Identifizierung häufig vorkommender Dateisignaturen ist standardmäßig aktiviert. Häufig vorkommende Dateisignaturen sind orangefarben hervorgehoben (7). 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. Beispiel: **Header Meta ip.proto=6** ist eine Kurzinformation für hervorgehobene Metadaten in der Hexadezimal- und der Binärdarstellung des Paket-Headers.

7 Häufig vorkommende Dateisignaturen werden orangefarben hervorgehoben. Wenn Sie den Mauszeiger auf dem Bereich platzieren, wird ein Pop-up-Feld mit dem möglichen Dateityp angezeigt.

Ansicht „Ereignisanalyse“ – Bereich „Textanalyse“

Im Bereich Textanalyse (**Ereignisanalyse > Textanalyse)** können Sie die Rohtext-Nutzdaten eines Ereignisses aus der Ansicht Navigieren oder der Ansicht Events, 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?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen	Untersuchen von Ereignissen
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	ein Ereignis analysieren*	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Dateien aus einem Ereignis exportieren*	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Schadsoftwareanalysen durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

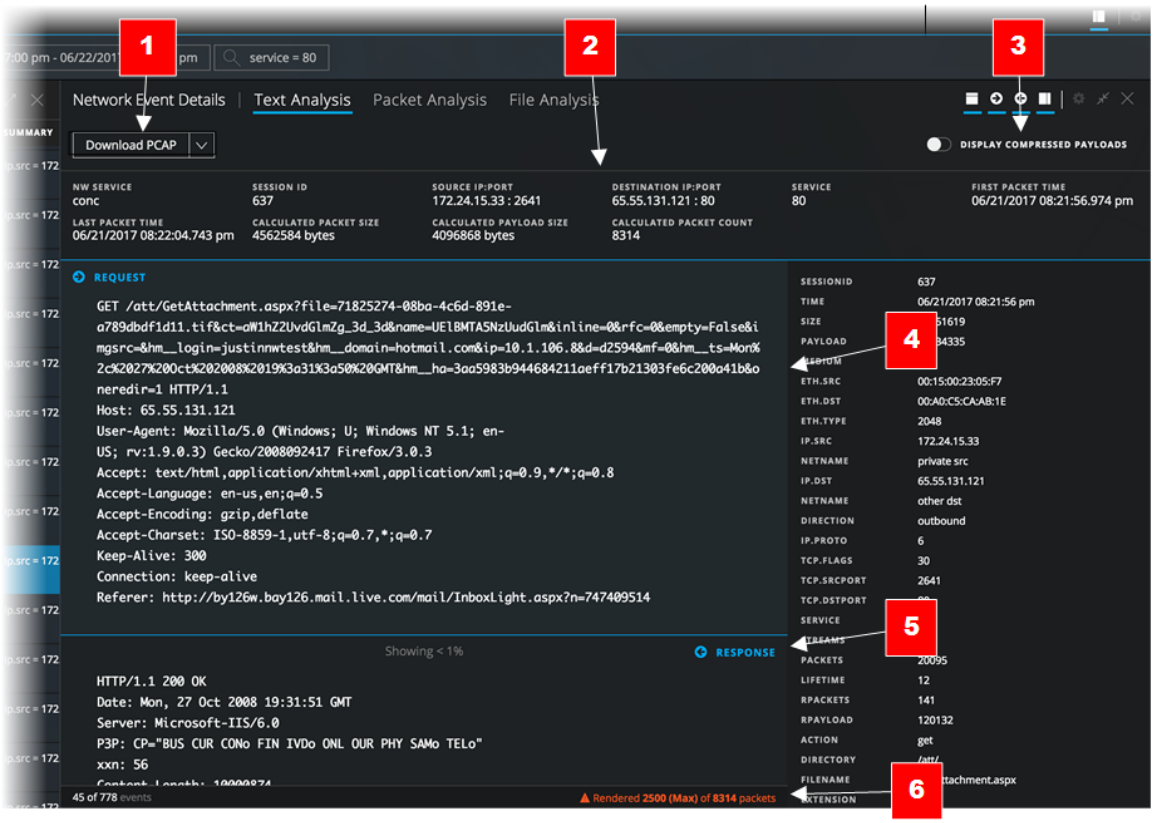
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

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.



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	Klicken Sie, um die Netzwerk-Nutzlast in komprimierter oder dekomprimierter Form anzuzeigen.
4	Die Nutzdaten für ein Netzwerkereignis umfassen Anforderungen und Antworten. Dies ist der Anforderungsseite des Pakets.
5	Dies ist der Antwortseite des Pakets. Nur 1 % der Antwort wird angezeigt, da die Anzeige abgeschnitten wurde, damit mehr Pakete angezeigt werden können. Wenn Sie einen Bildlauf nach unten durchführen, können Sie auf eine Option klicken, um den Rest der Nutzdaten anzuzeigen.
6	Diese Meldung wird angezeigt, wenn der Schwellenwert der 2.500 Pakete erreicht ist, eine Messgröße zur Optimierung der Performance. Zusätzliche Pakete werden nicht angezeigt. Sie können das Ereignis herunterladen, um alle Pakete anzuzeigen.

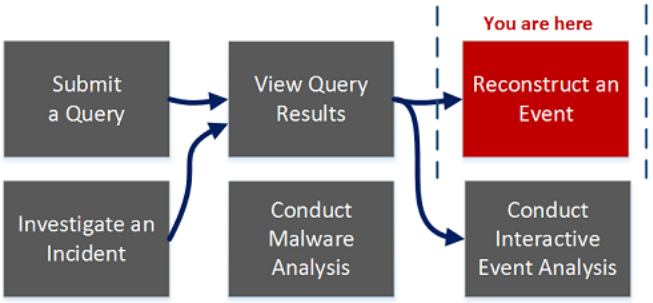
Ansicht „Ereignisrekonstruktion“

In der Ansicht „Ereignisrekonstruktion“ finden Sie eine Rekonstruktion eines ausgewählten Ereignisses aus der Ansicht „Ereignisse“. Standardmäßig wird inNetWitness Suite 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**.

Workflow



Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Abfrageergebnisse anzeigen	Durchführen einer Ermittlung
Threat Hunter	Rekonstruktion eines Ereignisses anzeigen*	Rekonstruieren eines Ereignisses
Threat Hunter	Interaktive Ereignisanalyse anzeigen	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Dateien aus einem Ereignis exportieren*	Rekonstruieren eines Ereignisses
Threat Hunter	Schadsoftwareanalyse durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

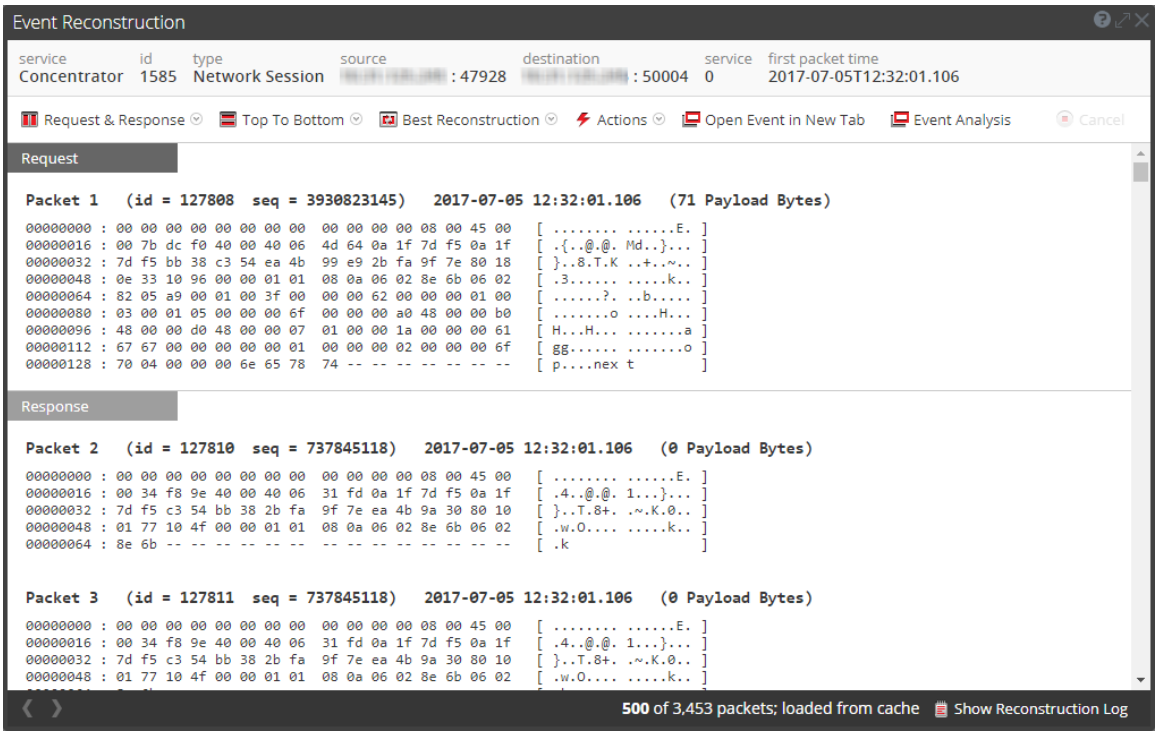
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

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.

Funktion	Beschreibung
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.

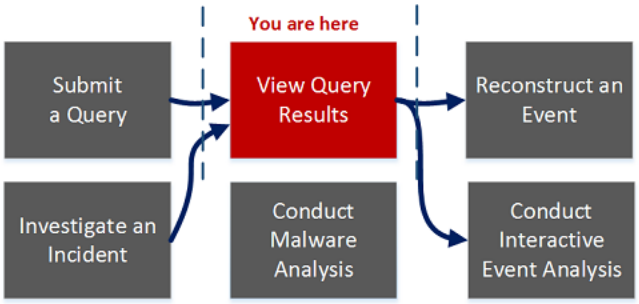
Funktion	Beschreibung
❮	Zeigt das vorherige Ereignis an.
❯	Zeigt das nächste Ereignis an.
Rekonstruktionsprotokoll anzeigen	Zeigt das Rekonstruktionsprotokoll unten in der Ansicht an. Sobald Sie auf diese Schaltfläche klicken, wird sie in „Rekonstruktionsprotokoll ausblenden“ geändert.

Ansicht Ereignisse

In der **Ansicht „Ereignisse“** finden Sie eine Liste aller Ereignisse, die einer Sitzung zugeordnet sind. Es gibt zwei Möglichkeiten, die Ansicht Ereignisse anzuzeigen:

- Klicken Sie auf **Untersuchen > Ereignisse**. NetWitness Suite 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.
- Klicken 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 „Navigieren“.

Workflow



Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Abfrage senden*	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Benutzereinstellungen für die Ansicht „Ereignisse“ festlegen*	Konfigurieren von Navigationsansicht und Ereignisansicht

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Ergebnisse in der Ansicht „Ereignisse“ filtern und durchsuchen*	Untersuchen von Ereignissen
Threat Hunter	Ereignisse aus geteilten Sitzungen kombinieren*	Kombinieren von Ereignissen aus geteilten Sitzungen
Threat Hunter	Ereignisse zwecks Reaktion einem Incident hinzufügen*	Durchführen einer Ermittlung
Threat Hunter	Ereignis rekonstruieren*	Rekonstruieren eines Ereignisses
Threat Hunter	Interaktive Ereignisanalyse anzeigen*	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Dateien aus einem Ereignis exportieren*	Exportieren von Ereignissen
Threat Hunter	Spaltengruppen managen*	Managen von Spaltengruppen in der Ereignisansicht
Threat Hunter	Zusätzlichen Kontext zu einem Metawert abrufen*	Anzeigen von zusätzlichem Kontext für einen Datenpunkt
Threat Hunter	Schadsoftwareanalyse durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

*Diese Aufgabe lässt sich in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Untersuchen von Ereignissen
- Ansicht „Navigieren“

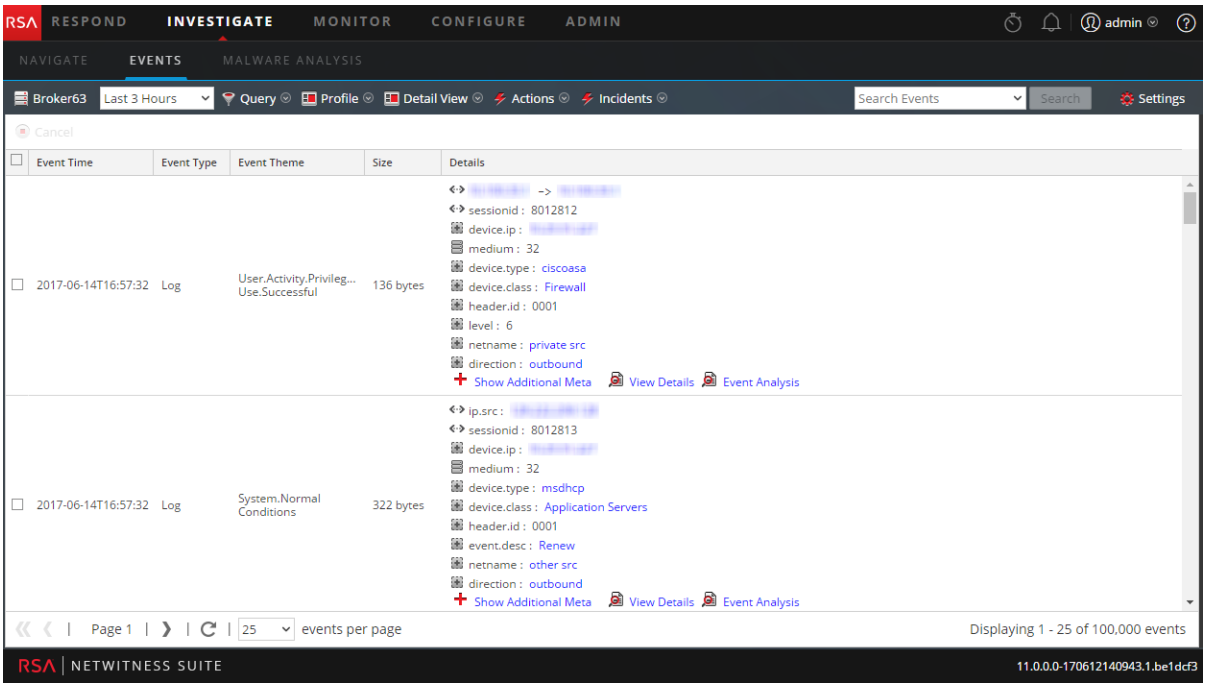
Überblick

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.

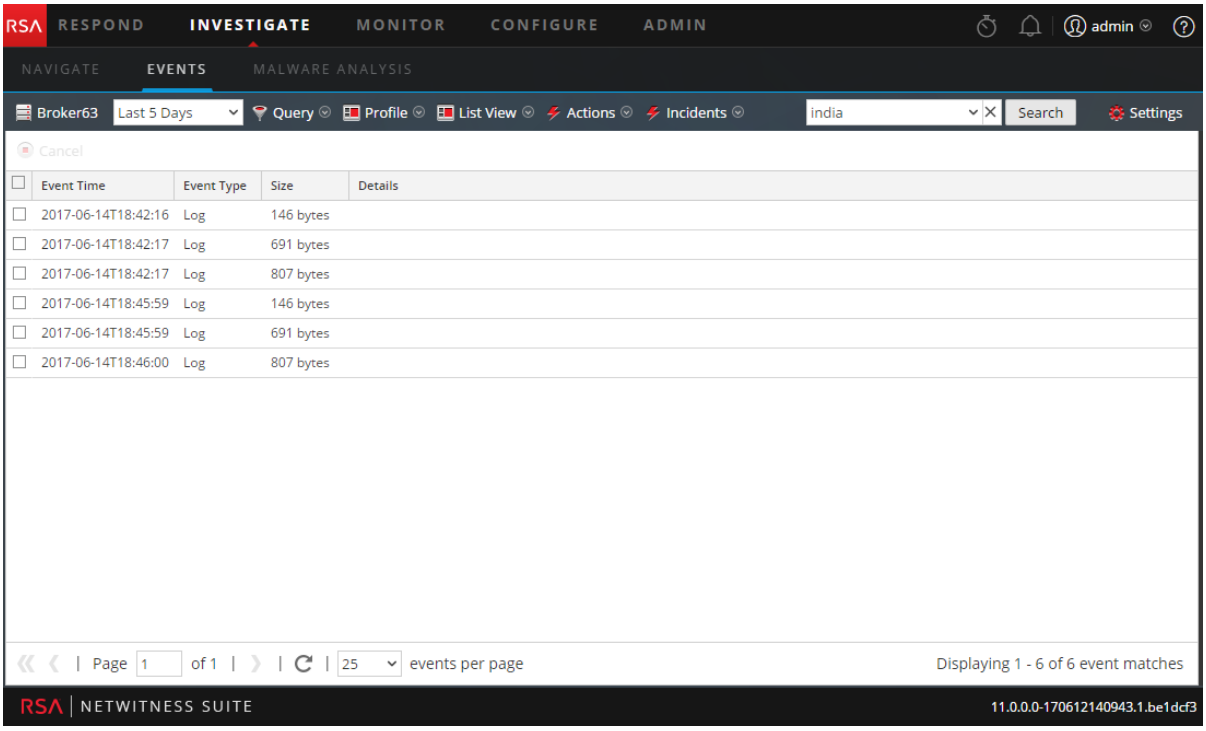
- In der Listenansicht werden die einander entsprechenden Quellen- und Zieladressen sowie Portinformationen zu Ereignissen in zusammengefasster Form in einem Raster dargestellt.
- Die Detailansicht enthält alle zum Ereignis gesammelten Metadaten in Seitenform.
- Die Protokollansicht ist für die Anzeige 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.

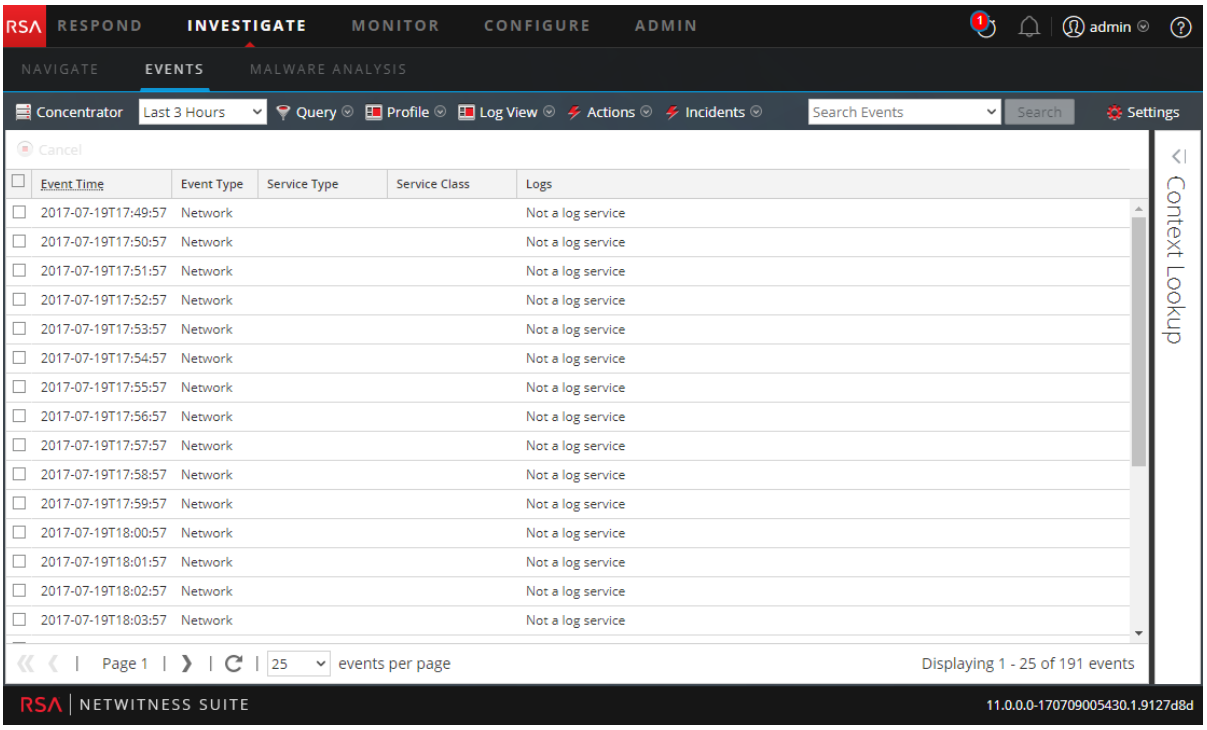
Die folgende Abbildung ist ein Beispiel für Ereignisse in der Detailansicht. Der Bereich „Kontextabfrage“ ist nur sichtbar, wenn der Service „Context Hub“ konfiguriert ist.



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).

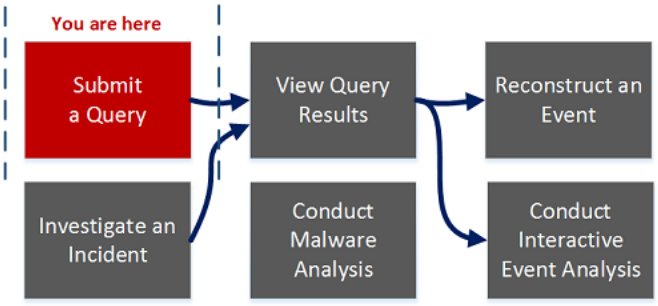
Funktion	Beschreibung
Profil	Zeigt das Menü Profil verwenden an; das aktuell ausgewählte Profil wird in der Symbolleiste angezeigt. Ein Profil erlaubt Ihnen, Profile zu verwalten und zu verwenden, die angepasste Metagruppen, eine Standard-Spaltengruppe und eine beginnende Abfrage enthalten können. Die 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 Benutzerdefinierte 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.
Suche	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 in der Ansicht „Untersuchen“ 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 von Navigationsansicht und Ereignisansicht).

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 „Navigieren“ 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?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	einen Standard-Service einrichten oder ändern*	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	einen Service oder eine Sammlung untersuchen*	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen	Durchführen einer Ermittlung

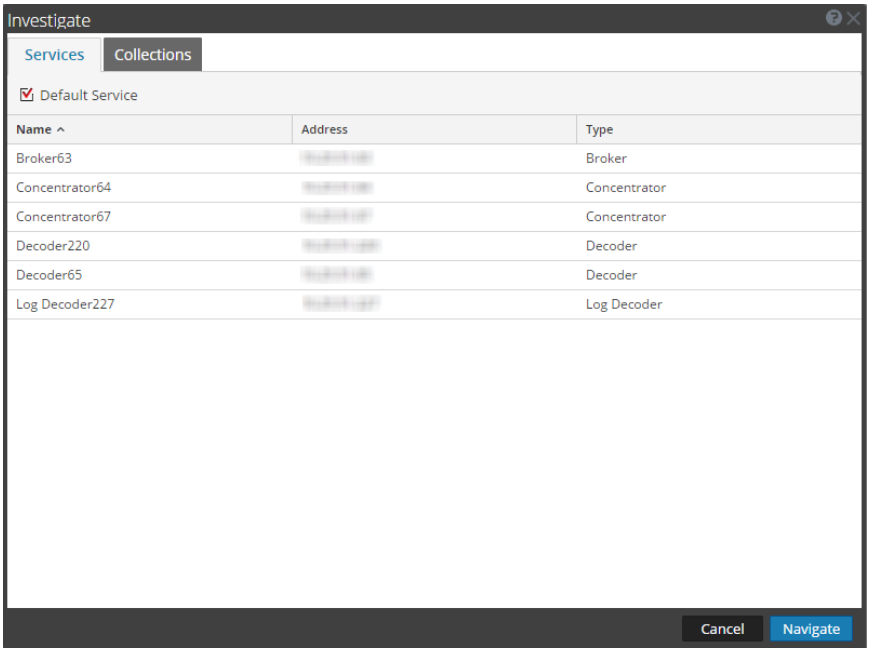
Benutzerrolle	Ziel	Dokumentation
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	eine interaktive Ereignisanalyse durchführen	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Schadsoftwareanalysen durchführen	Durchführen von Schadsoftwareanalysen

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?

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 „Navigieren“ 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 „Navigieren“ 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.

Funktion	Beschreibung
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 „Benutzereinstellungen“

In der Ansicht „Profil“ > Bereich „Einstellungen“ > Registerkarte „Investigation“ können Benutzer verschiedene Einstellungen festlegen, die die Performance und das Verhalten von NetWitness Suite bei der Datenanalyse sowie bei der Anzeige und Rekonstruktion von Ereignissen in Investigation beeinflussen. Um auf diese Registerkarte zuzugreifen, wählen Sie  > Profile. Wenn die Ansicht „Profil“ angezeigt wird, wählen Sie die Registerkarte Einstellungen > Investigation aus. Sie können Benutzereinstellungen in NetWitness Suite zu jedem beliebigen Zeitpunkt ändern.

Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Benutzereinstellungen für Investigate anzeigen und ändern*	Konfigurieren von Navigationsansicht und Ereignisansicht
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen	Durchführen einer Ermittlung
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	eine interaktive Ereignisanalyse durchführen	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*
Threat Hunter	Schadsoftwareanalysen durchführen	Durchführen von Schadsoftwareanalysen

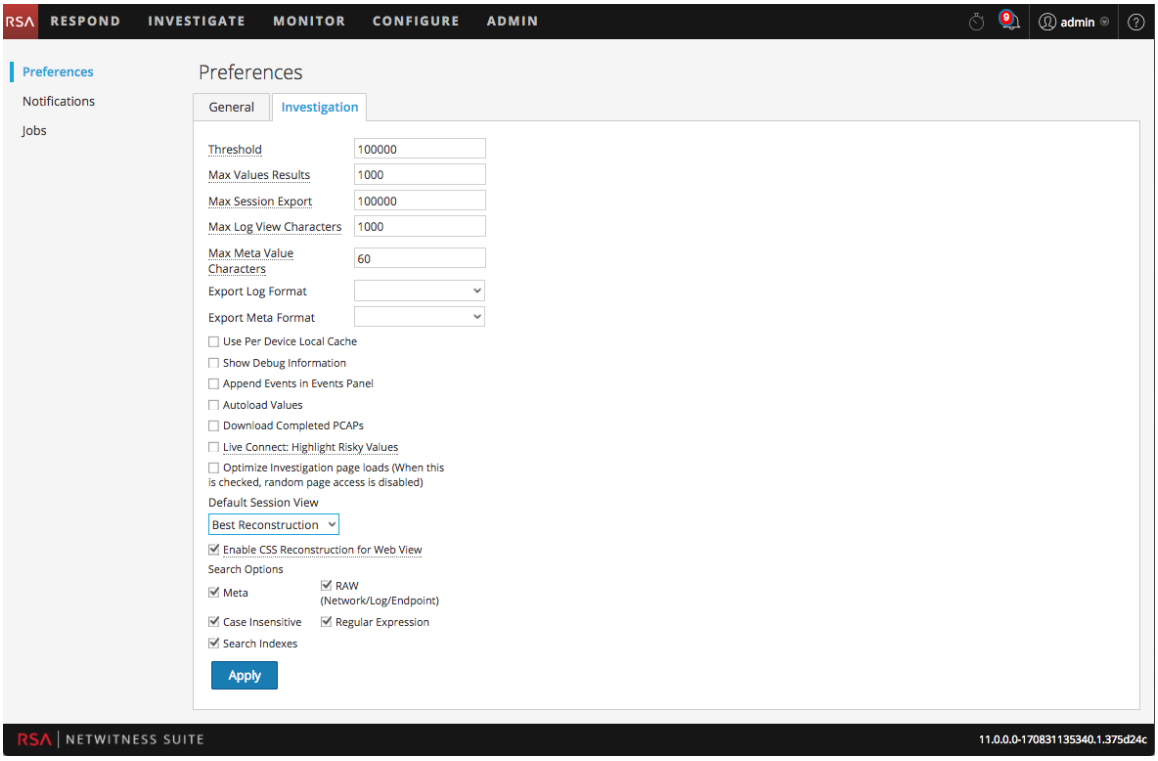
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Ansicht „Navigieren“
- Ansicht Ereignisse

Überblick

Diese Abbildung ist ein Beispiel der Registerkarte „Investigation“ und in der folgenden Tabelle sind die Investigation-Einstellungen beschrieben.



Funktion	Beschreibung
Schwellenwert	Diese Einstellung steuert den Zähler, der während des Ladens für den Wert Metaschlüssel in der Ansicht „Navigieren“ 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 Suite 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 „Navigieren“ 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**.
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**.

Funktion	Beschreibung
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 Suite 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 Suite 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 Suite die `where`-Klausel unter der Breadcrumb-Navigation in der Ansicht „Navigieren“ 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**.

Funktion	Beschreibung
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 Suite eine Schaltfläche **Werte laden** an, über die der Benutzer 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.
Live Connect: Riskante Werte markieren	

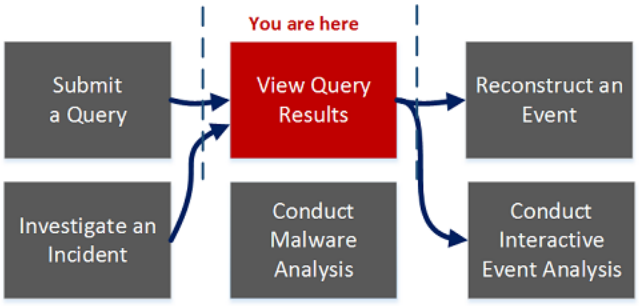
Funktion	Beschreibung
Optimieren des Ladens der Seite „Investigation“	Diese Option ist standardmäßig aktiviert und legt fest, wie in der Ereignisansicht Ereignisse abgerufen werden. Im Optimalfall werden Ergebnisse so schnell wie möglich zurückgegeben. Dadurch entfällt die ursprüngliche Möglichkeit, 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.

Funktion	Beschreibung
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 Formatvorlagen und 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 „Navigieren“ und „Ereignisse“ festgelegt. Unter Suchen nach Textmustern in der Ansicht „Untersuchen“ finden Sie detaillierte Informationen.
Anwenden	Speichert Ihre Einstellungen und macht sie sofort wirksam.

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?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Standardmetaschlüssel für einen Service konfigurieren*	Verwalten und Anwenden von Standardmetaschlüsseln in einer Ermittlung
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen*	Durchführen einer Ermittlung
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	ein Ereignis analysieren	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Schadsoftwareanalysen durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

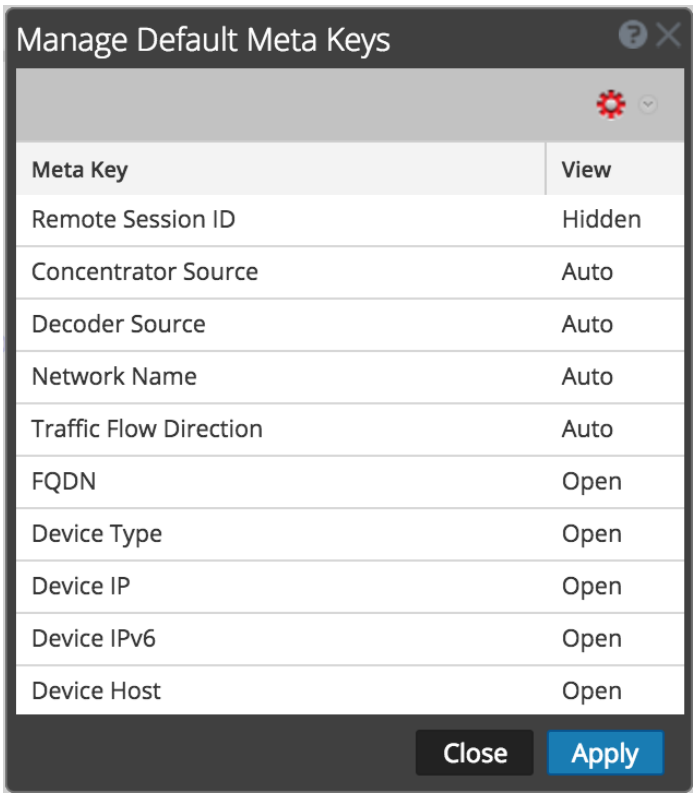
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Metagruppen managen
- Wie funktioniert NetWitness Investigate?

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.

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.

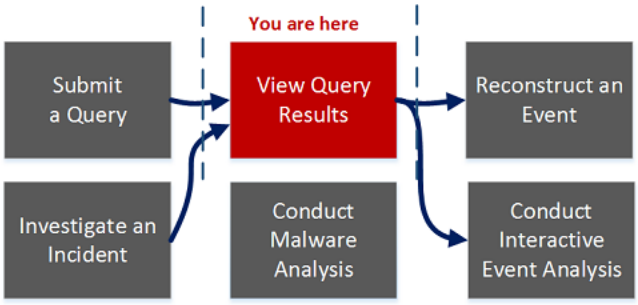
Malware Analysis-Ereignisliste und -Dateiliste

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?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	detaillierte Schadsoftware-Analysedaten für Dateien oder Ereignisse anzeigen*	Überprüfen von Scandateien und Ereignissen in Listenform
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Abfrageergebnisse anzeigen	Durchführen einer Ermittlung
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	ein Ereignis analysieren	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Schadsoftwareanalysen durchführen*	Durchführen von Schadsoftwareanalysen
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

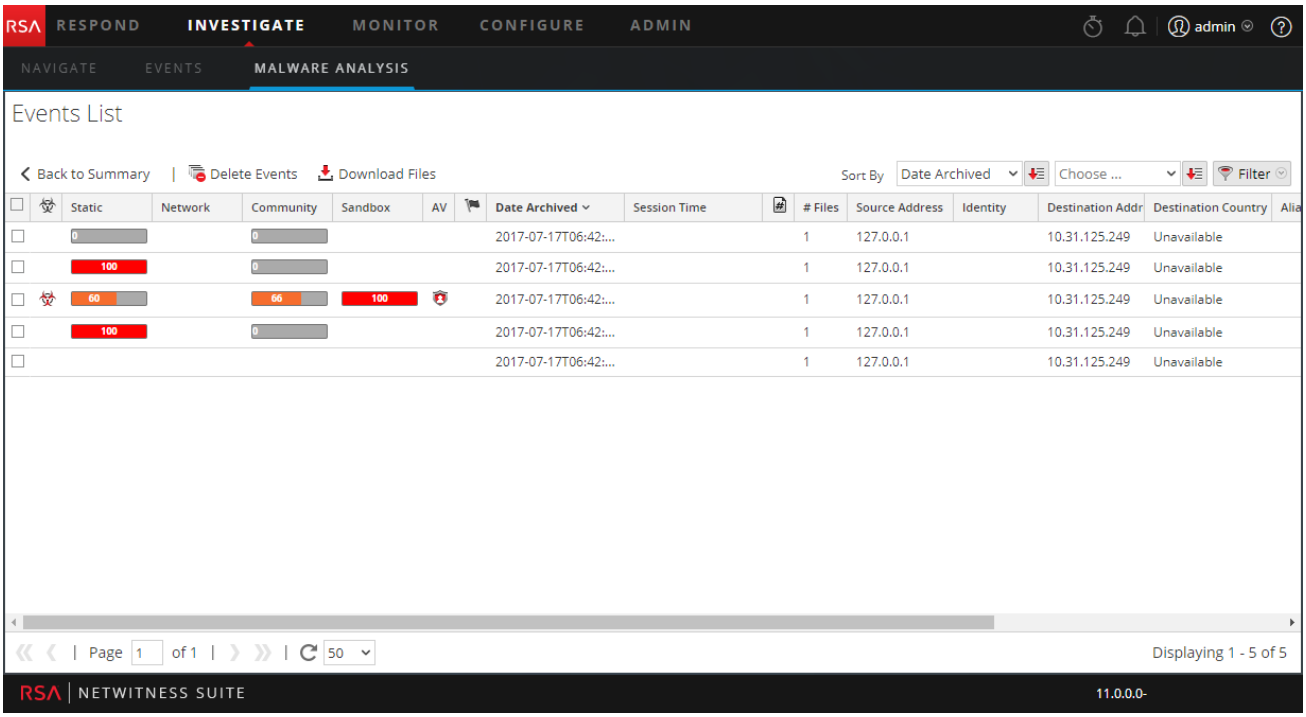
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

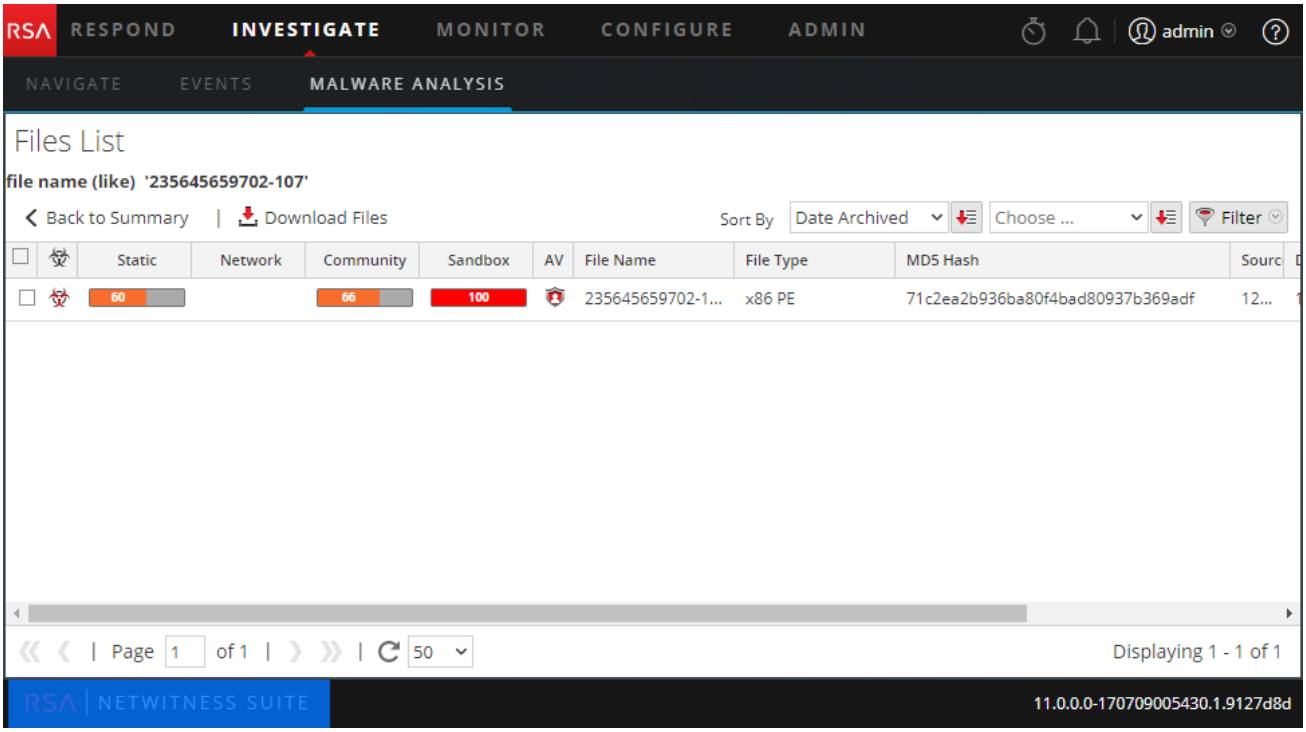
- Wie funktioniert NetWitness Investigate?

Überblick

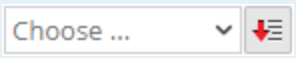
Dies ist ein Beispiel für die Ereignislistenansicht.

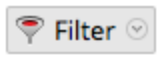


Dies ist ein Beispiel für die Ansicht „Dateiliste“.



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.

Funktion	Beschreibung
	Zeigt ein Drop-down-Menü an, aus dem Sie eine zweite Sortierreihenfolge auswählen können. Dieses Menü enthält auch die OptionNetWitness Suite**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.
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.

Funktion	Beschreibung
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, Manueller Upload.
Service	Zeigt den Service an, auf dem das Ereignis geschah.
Zielorganisation	Zeigt die Organisation des Ziels an.

Das Dateilistenraster verfügt über folgende Funktionen.

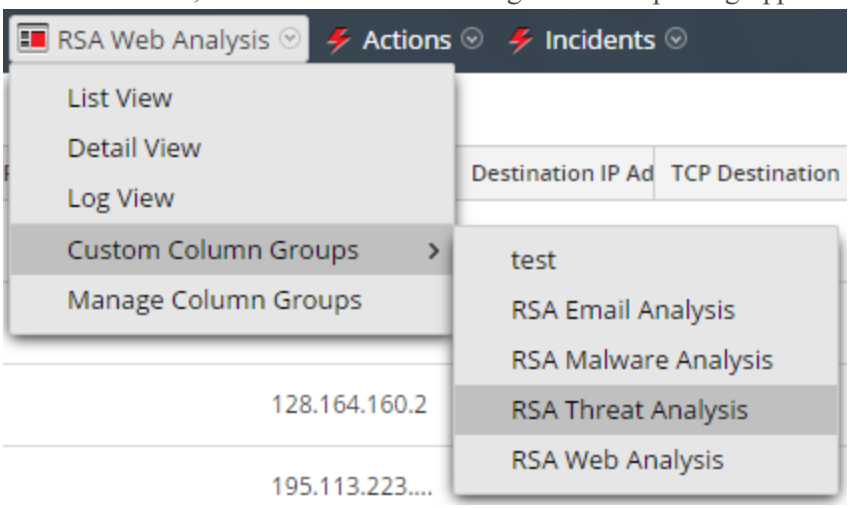
Funktion	Beschreibung
	Zeigt an, ob das Ereignis durch die Kennzeichnung Hohe Wahrscheinlichkeit beeinflusst ist.
Statisch, Netzwerk, Community, Sandbox	Zeigt die Bewertungen für jedes Bewertungsmodul an.
AV	Zeigt an, ob das Virenschutzprogramm dieses Ereignis als verdächtig gekennzeichnet hat.
Dateiname	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.
Archivierungsdatum	Zeigt Datum und Uhrzeit der Archivierung der Datei an.

Funktion	Beschreibung
Größe	Zeigt die Größe der Datei an.

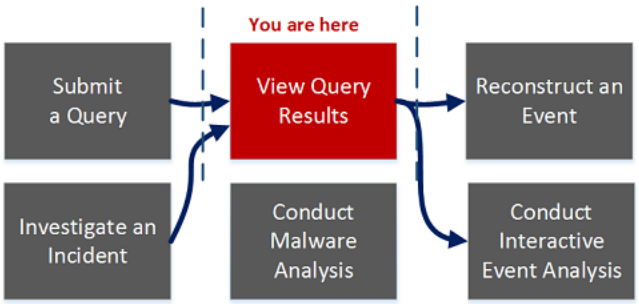
Dialogfeld „Spaltengruppen managen“

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 > Ansicht „Ereignisse“** und wählen in der Drop-Down-Liste „Ansicht“ **Spaltengruppen managen** aus. Die Option „Anzeigen“ wird nach dem aktuellen Wert benannt, z. B. Detailansicht, Listenansicht, Protokollansicht, oder nach der aktuell ausgewählten Spaltengruppe.



Workflow



Was möchten Sie tun?

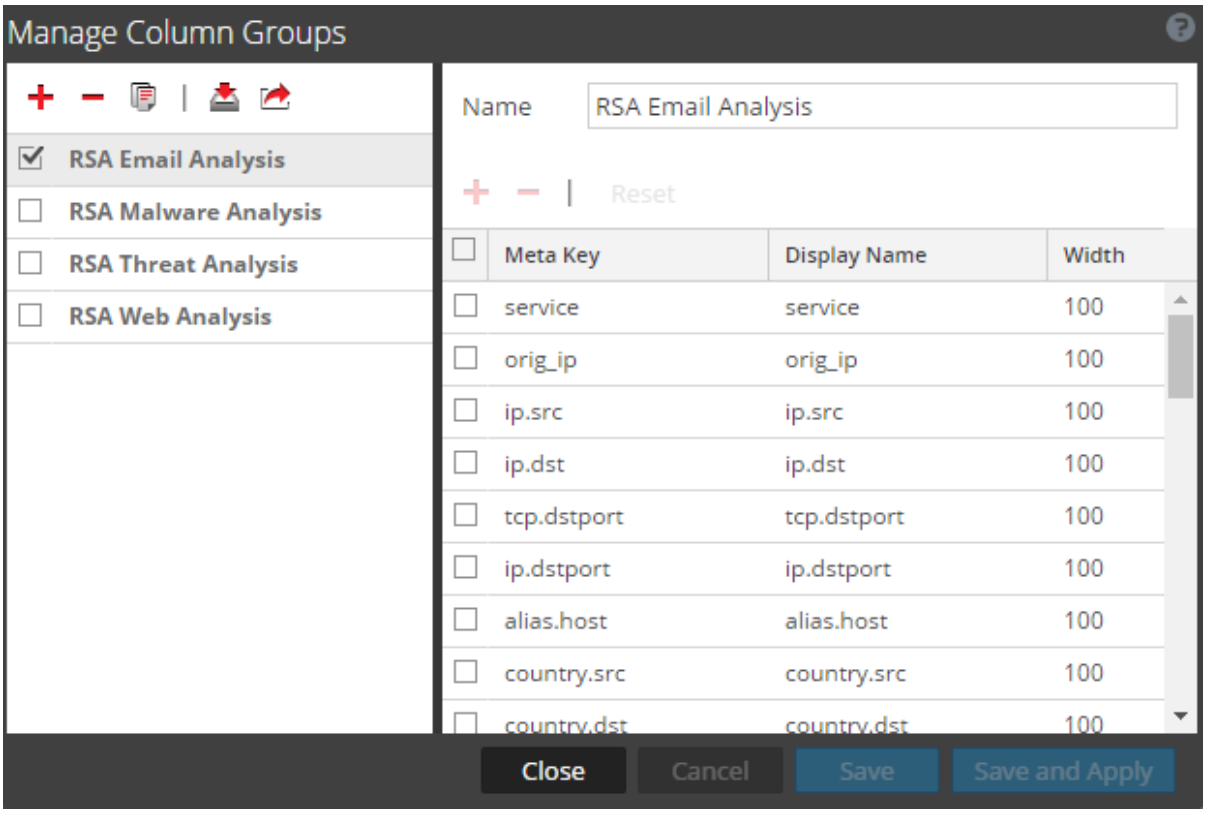
Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Spaltengruppen managen*	Managen von Spaltengruppen in der Ereignisansicht
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen*	Durchführen einer Ermittlung
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	ein Ereignis analysieren	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Schadsoftwareanalysen durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?

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.

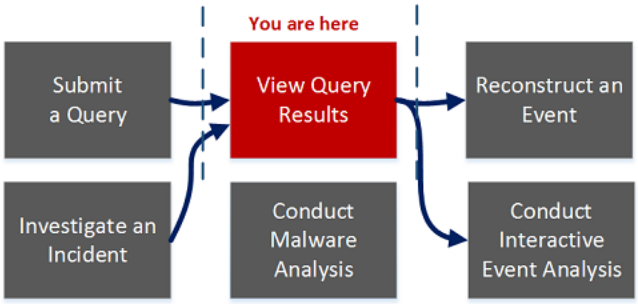
Funktion	Beschreibung
Breite	Legt die Breite der Spalte jedes Metaschlüssels fest. Als Grenze können Sie einen Wert zwischen **10** und **1.000** verwenden. Die Standardbreite ist **100**.

Dialogfeld „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?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Metagruppen hinzufügen, bearbeiten und löschen*	Metagruppen managen
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen*	Durchführen einer Ermittlung
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	ein Ereignis analysieren	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“

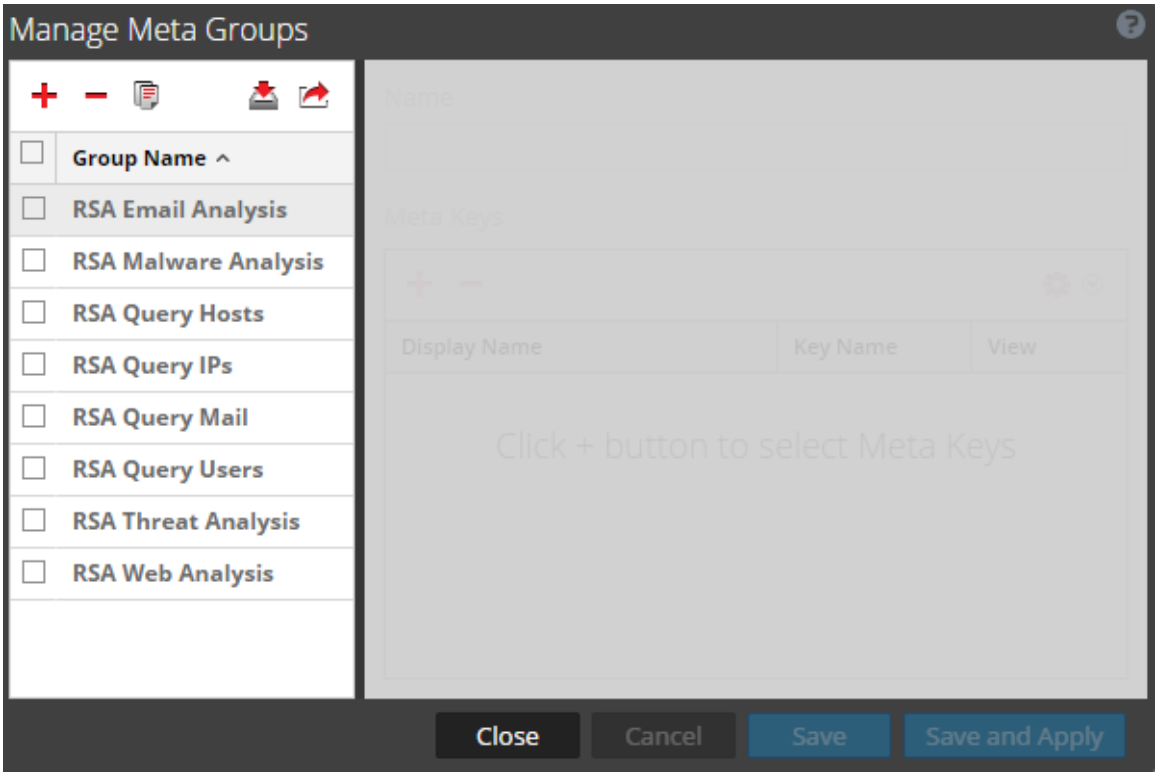
Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Schadsoftwareanalysen durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Verwalten und Anwenden von Standardmetaschlüsseln in einer Ermittlung
- Wie funktioniert NetWitness Investigate?

Überblick



Das Dialogfeld „Metagruppen managen“ hat zwei Bereiche. In der folgenden Tabelle werden die Schaltflächen unten im Dialogfeld beschrieben.

Funktion	Beschreibung

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.

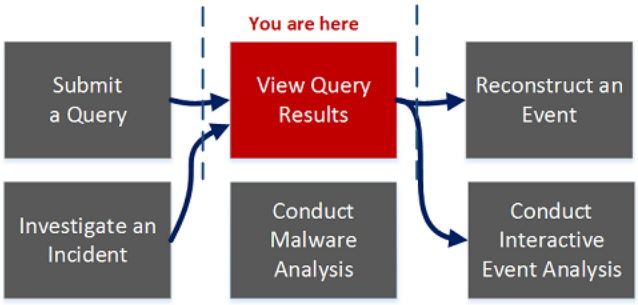
Funktion	Beschreibung
	Löscht die ausgewählten Metaschlüssel.
	Zeigt ein Drop-down-Menü an, in dem Sie die Ansicht für alle Metaschlüssel auswählen können. Es gibt vier Optionen, denen die möglichen Werte der Eigenschaft `defaultAction` zugrunde liegen, die zur Definition eines Schlüssels in der benutzerdefinierten 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.
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 „Navigieren“ 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.

Um dieses Dialogfeld zu öffnen, wählen Sie in der Symbolleiste der Ansicht **Investigation > Navigieren** oder **Ereignisse Profil > Profile managen** aus.

Workflow



Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Profile konfigurieren*	Einkapseln von benutzerdefinierten Ansichten mithilfe von Ermittlungsprofilen
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen*	Durchführen einer Ermittlung
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	ein Ereignis analysieren	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Schadsoftwareanalysen durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

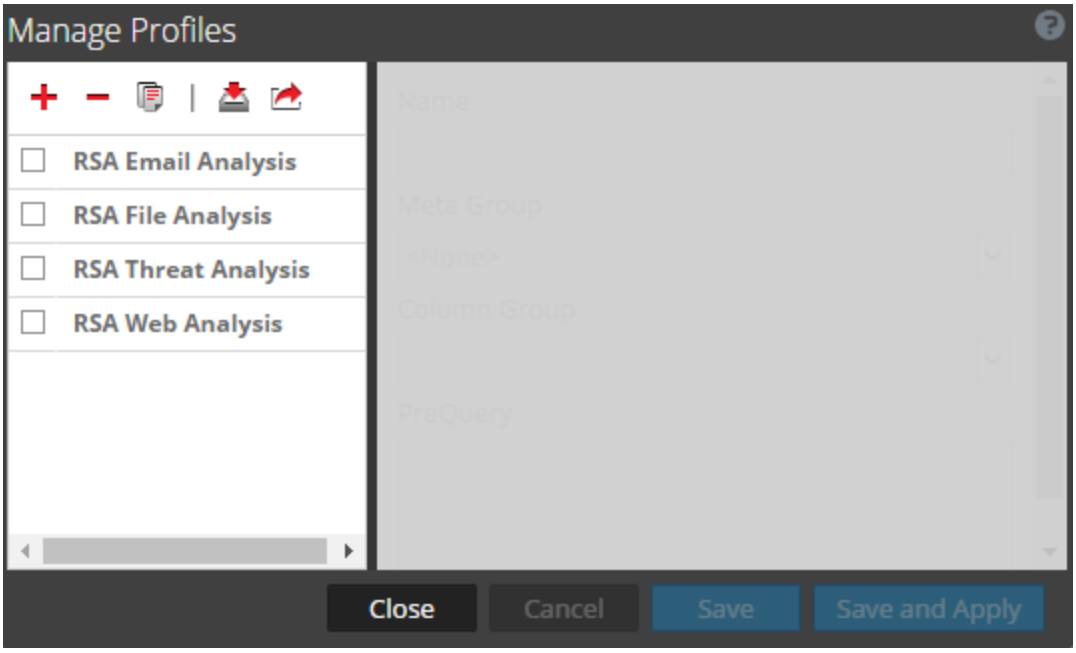
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Metagruppen managen
- Wie funktioniert NetWitness Investigate?

Überblick

Dies ist ein Beispiel des Dialogfelds „Profile managen“.



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.

Funktion	Beschreibung
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'.`

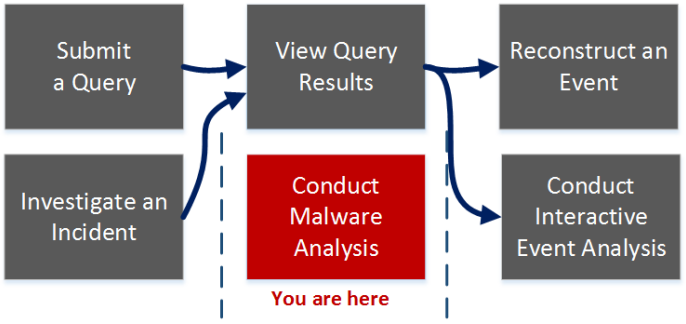
Ansicht „Malware Analysis“

In NetWitness Suite 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 Benutzerrolle (Administration oder Analyst) und Benutzeranpassungen 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 diese auf Ansicht zuzugreifen, wählen Sie **Ermittlung > Malware Analysis** aus.

Wählen Sie in Netwitness **Investigation > 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?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen	Durchführen einer Ermittlung

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	ein Ereignis analysieren	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Schadsoftwareanalysen durchführen*	Durchführen von Schadsoftwareanalysen
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

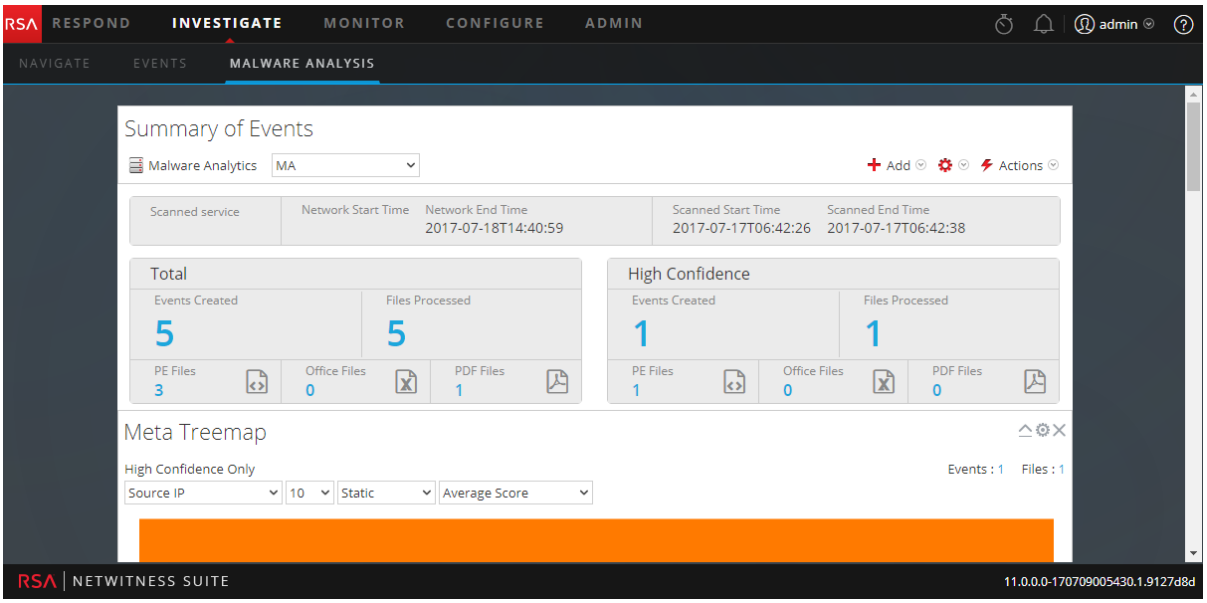
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Starten eines Schadsoftwareanalyse-Scans in der Navigationsansicht

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 im NetWitness Suite-Dashboard sind ebenfalls verfügbar und werden im Thema „Dashlets“ unter RSA Content für die RSA NetWitness® Suite 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.
	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“.

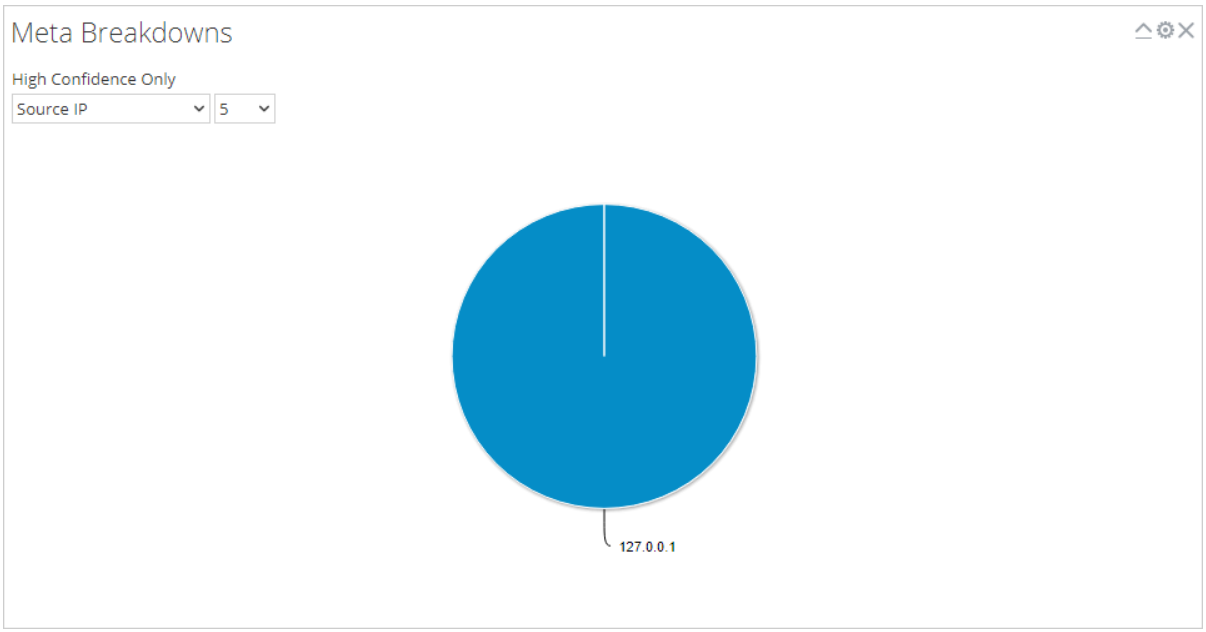
Dialogfeld „Optionen“

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.

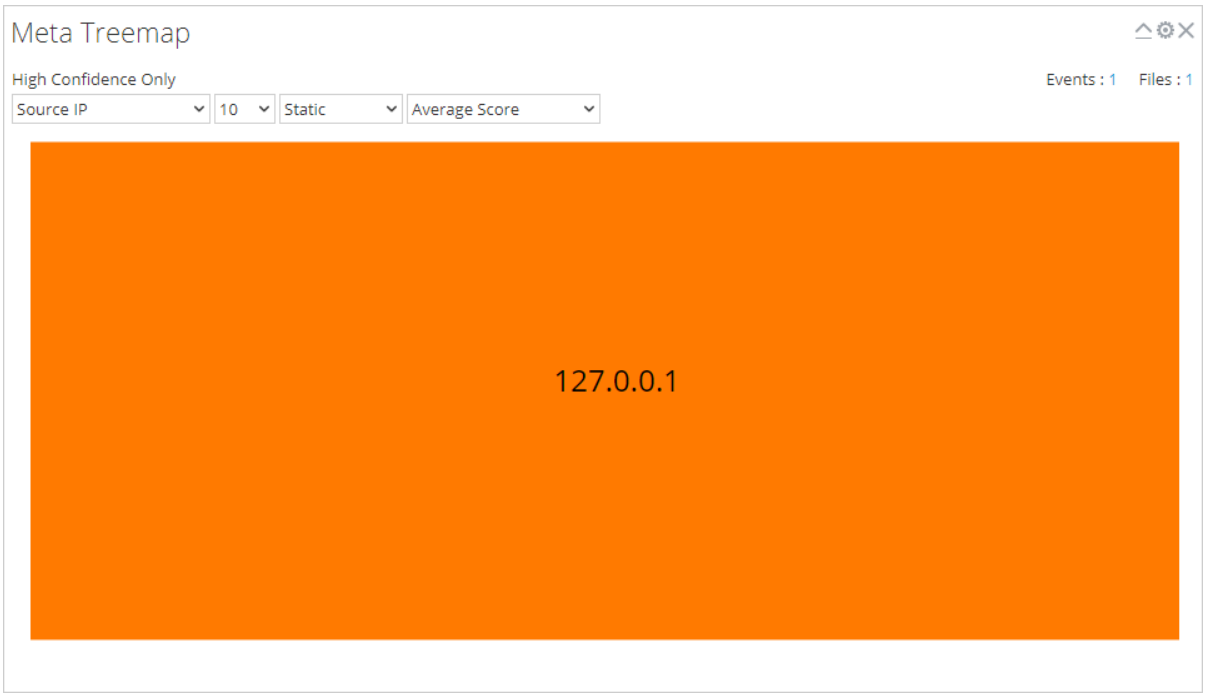


In der folgenden Tabelle sind die Optionen im Dashlet „Meta-Strukturen“ beschrieben.

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.

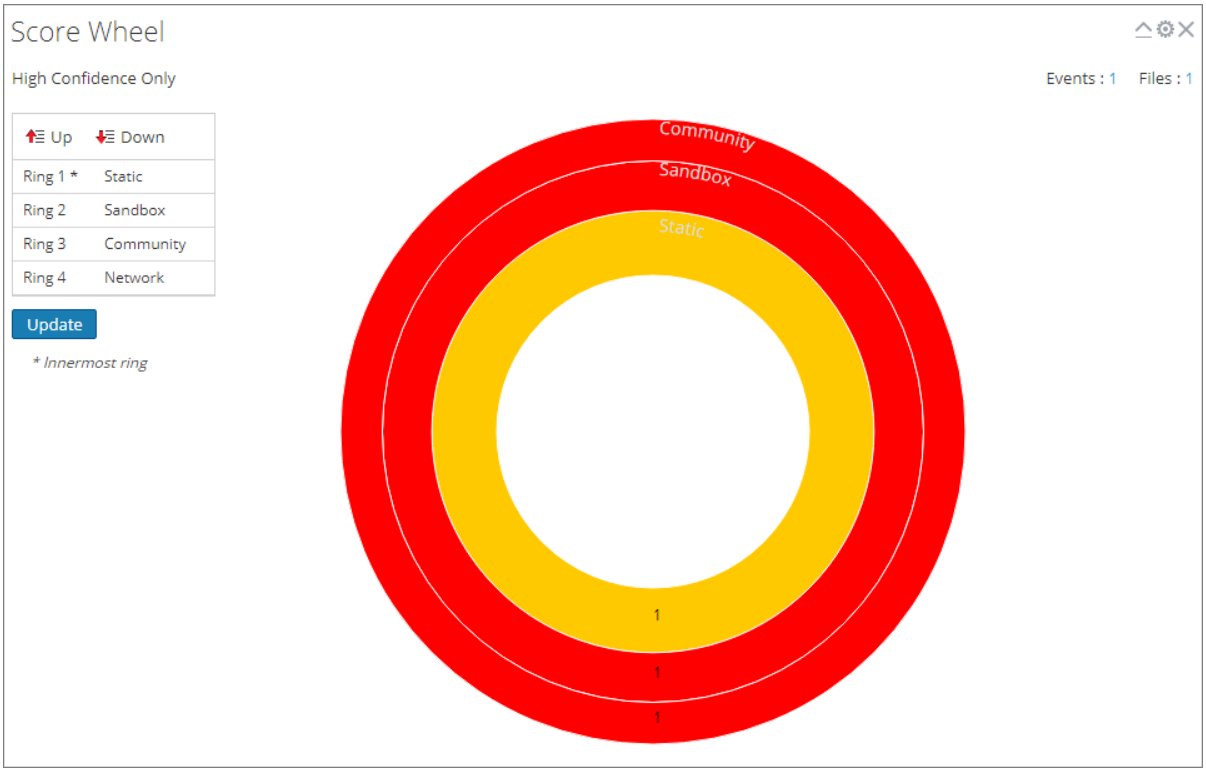


In der folgenden Tabelle sind die Optionen im Dashlet „Meta-Treemap“ beschrieben.

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.

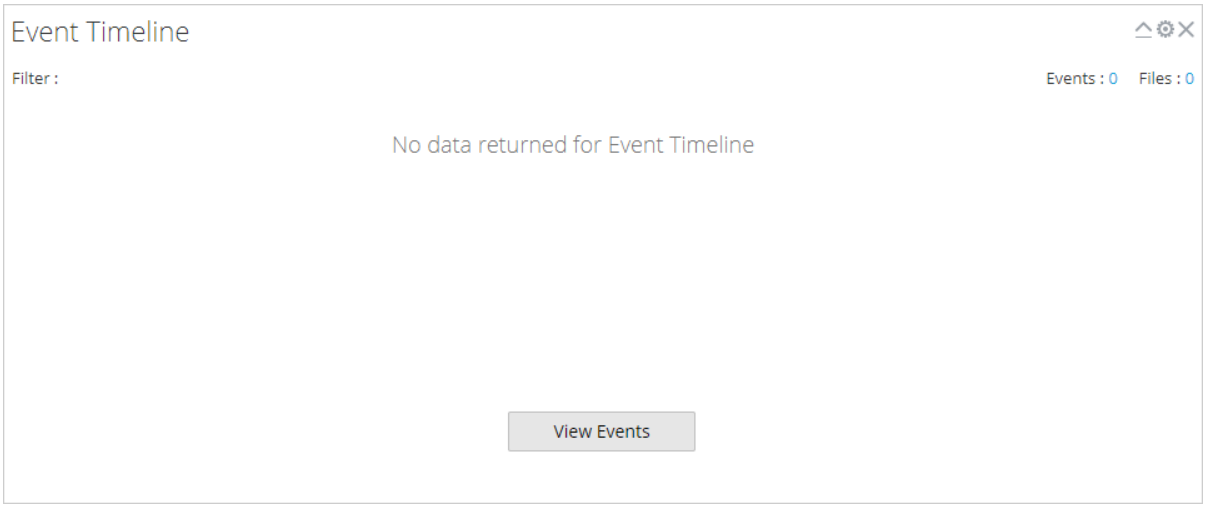


In der folgenden Tabelle sind die Funktionen im Dashlet „Punktzahlrad“ beschrieben.

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.

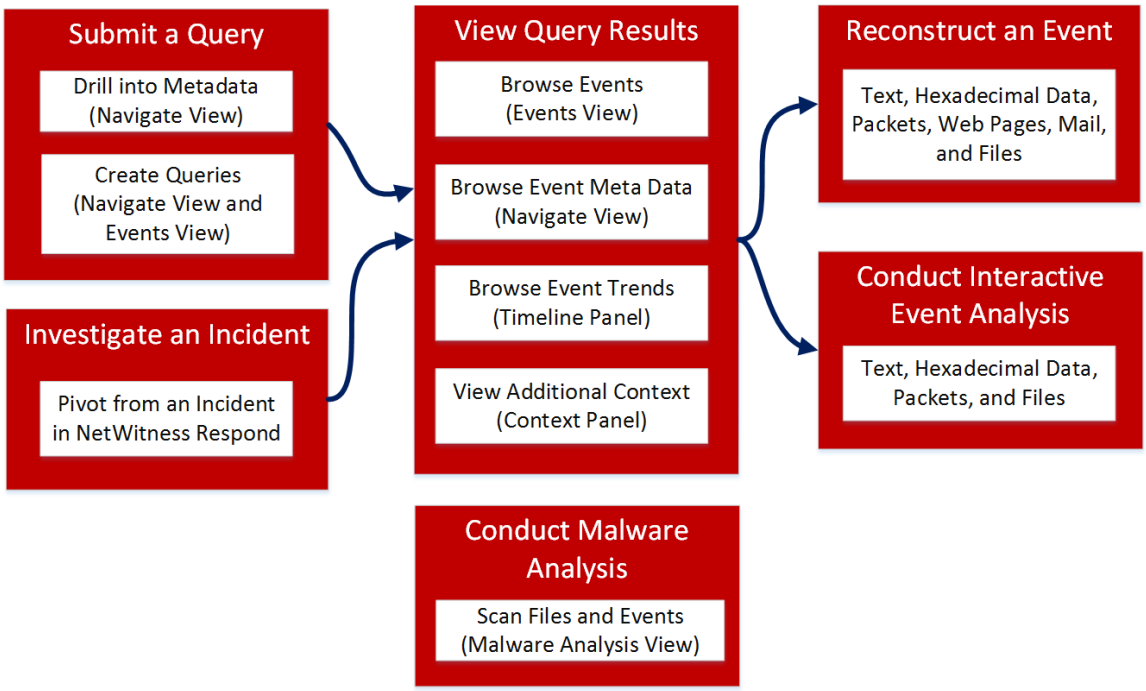
Funktion	Beschreibung
Nur hohe Wahrscheinlichkeit	Gibt an, ob die Ergebnisse auf Ereignisse beschränkt sind, die als hoch vertraulich markiert sind. Wenn die Ergebnisse nicht eingeschränkt sind, wird diese Zeile nicht angezeigt.
Ereignisse anzeigen	Zeigt die Ansicht „Investigation > Ereignisse“ an.

Ansicht „Navigieren“

Ansicht „Navigation“ (**Ermittlung** > Navigieren) ist der primäre Einstiegspunkt in NetWitness .Investigate. In der Ansicht „Navigieren“ werden die Aktivitäten und Werte für den ausgewählten Service in Übereinstimmung mit den festgelegten Investigation-Optionen angezeigt: „Profil“, „Zeitbereich“, „Metagruppe“ und „Abfrage“. In den Ermittlungsdaten zu den Ereignissen sind die Metaschlüssel und -werte zu sehen.

Workflow

Der Workflow unten zeigt die allgemeinen Schritte und Unteraufgaben zur Untersuchung von Ereignissen.



Hierbei handelt es sich um die Aufgaben, die Sie in 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.
- Speichern der Ereignisse, Wechseln zu einem Ereignis anhand der Ereignis-ID, Anzeigen eines Ereignisses und Drucken des Ereignisses.
- Anzeigen zusätzlicher Kontextdaten für bestimmte Metaschlüssel und Werte.

- Navigieren zu Ansicht „Ereignisse“ (enthält eine chronologische Liste der Ereignisse), Rekonstruieren eines Ereignisses und Durchführen einer interaktiven Analyse eines Ereignisses. Beim Anzeigen und Analysieren von Ereignissen können Sie Ereignisse, Dateien und Protokolle in Ihr lokales Dateisystem exportieren.

Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	eine Abfrage senden oder eine nähere Analyse der Datenmenge vornehmen*	Abfragen von Daten in der Ansicht „Navigation“
Threat Hunter	Benutzereinstellungen für Investigate festlegen*	Konfigurieren von Ermittlungsansichten und -einstellungen
Threat Hunter	Abfrage-Ergebnisse verfeinern*	Einschränken der in der Ansicht „Navigation“ angezeigten Ergebnisse
Threat Hunter	einen Drill-down-Punkt in der Ansicht „Ereignisse“ öffnen*	Öffnen der Ereignisliste
Threat Hunter	ein Ereignis visualisieren*	Zeitdiagramm des Drill-down in die Daten in der Ansicht „Navigation“
Threat Hunter	einen Drill-down-Punkt exportieren oder drucken, eine externe Suche oder Malware Analysis-Scan starten*	Aktionen zu Drill-down-Punkten in der Ansicht „Navigation“
Threat Hunter	zusätzlichen Kontext für ein Ereignis suchen*	Anzeigen von zusätzlichem Kontext für einen Datenpunkt

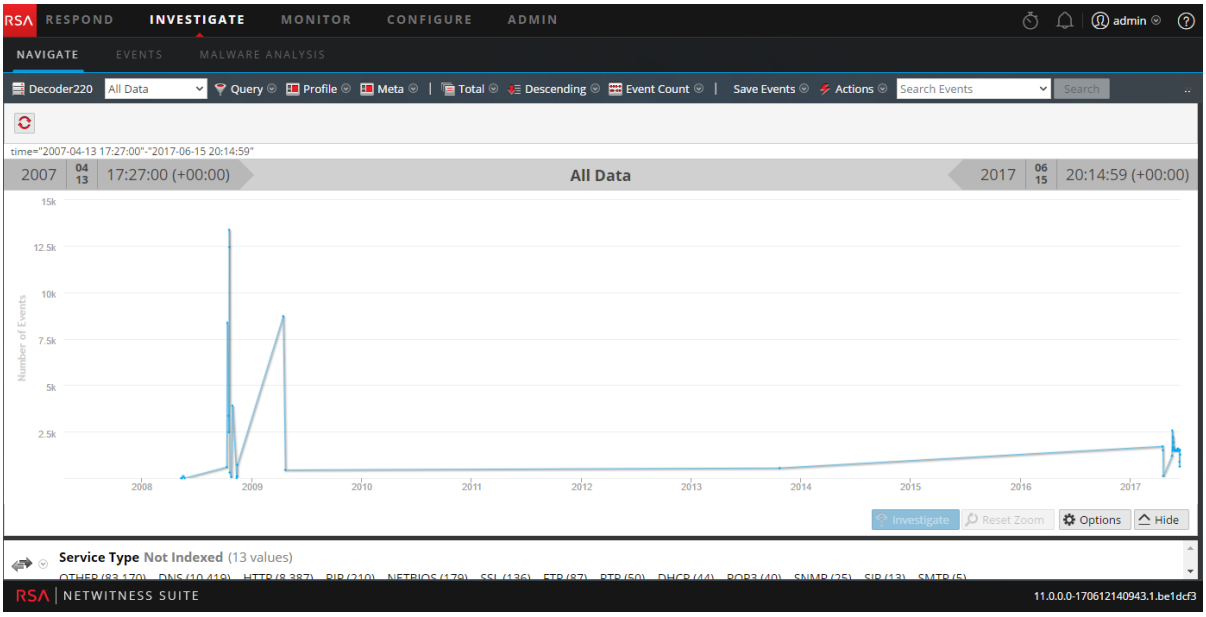
Benutzerrolle	Ziel	Dokumentation
Threat Hunter	eine Rekonstruktion eines Ereignisses anzeigen	Rekonstruieren eines Ereignisses
Threat Hunter	eine Ereignisanalyse anzeigen	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Schadsoftwareanalysen durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Durchführen einer Ermittlung
- Ansicht Ereignisse
- Ansicht „Malware Analysis“

Überblick



Die Ansicht „Navigieren“ umfasst folgende Funktionen:

- Symbolleiste
- Schaltfläche zum Anhalten/Neuladen und Breadcrumb
- 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, zu einem Ereignis navigieren, dessen Ereignis-ID Sie kennen, und eine Abfrage an Informer übergeben.
- Ermittlungseinstellungen konfigurieren, ohne dazu die Investigation-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 Untersuchung für einen Service oder eine Sammlung). 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 Einstellen des Zeitbereichs für eine Ermittlung). 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 • Benutzerdefiniert **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 anhand der Zeit 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 Funktionen von „Investigation > Navigieren“ 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“.

Option	Beschreibung
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 Ermittlungsprofilen.
Meta	Zeigt das Menü Metagruppe an. Sie können standardmäßige Metaschlüssel 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 Einstellen der Quantifizierungsmethode und Sortierreihenfolge von Metaschlüsselergebnissen).

Option	Beschreibung
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 Einstellen der Quantifizierungsmethode und Sortierreihenfolge von Metaschlüsselergebnissen).

Option	Beschreibung
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 Einstellen der Quantifizierungsmethode und Sortierreihenfolge von Metaschlüsselergebnissen). 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.
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“).

Option	Beschreibung
Aktionen	Das Menü „Aktionen“ enthält verschiedene Aktionen („Visualisieren“, „Zu Ereignis wechseln“ und „Drucken“), die Sie in der Ansicht „Navigieren“ ausführen können (siehe Aktionen zu Drill-down-Punkten in der Ansicht „Navigation“).
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 „Investigations“ aktualisiert (siehe Suchen nach Textmustern in der Ansicht „Untersuchen“).
Einstellungen	Zeigt die Investigation-Einstellungen für die Ansicht „Navigieren“ an (die auch in der Ansicht „Profil“ bearbeitet werden können), sodass Sie die Einstellungen für Investigation ändern können, ohne die Ansicht „Navigieren“ verlassen zu müssen. Wenn Sie eine Einstellung in der Ansicht „Navigieren“ ändern, wird die Einstellung auch in der Ansicht „Profil“ geändert (siehe Konfigurieren von Navigationsansicht und Ereignisansicht).

Schaltfläche zum Anhalten/Neuladen und Breadcrumb

Im Breadcrumb 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 dem Breadcrumb können Sie das Laden von Metawerten anhalten bzw. die Metawerte neu laden.

Der Breadcrumb 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 des Breadcrumb angezeigt.

Die Drop-down-Menüs im Breadcrumb unterscheiden sich nur je nach Position des Crumb und sind ansonsten identisch.

In der folgenden Tabelle werden die Steuerelemente und Menüoptionen im Breadcrumb beschrieben.

Funktion	Beschreibung
Pause	Schaltfläche „Anhalten und neu laden“ Steuert das Laden von Daten in der Ansicht. Drei Funktionen sind möglich: Laden anhalten, Laden fortführen und neu laden.
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 den Breadcrumb 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 des Breadcrumb angefügt werden soll (siehe „Erstellen einer angepassten Abfrage“).
Entfernen	Entfernt den ausgewählten Drill-down-Punkt aus dem Breadcrumb.
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 Breadcrumb-Überlauf 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 Suite Debug-Informationen unter der Breadcrumb-Navigation 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

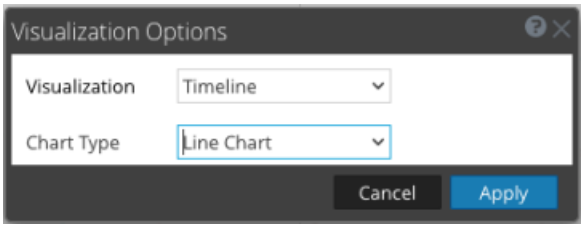
Genau unter dem Breadcrumb und den Debug-Informationen (sofern vorhanden) wird im Zeitbanner der Zeitbereich angezeigt, der für die Diagrammerstellung verwendet wurde.

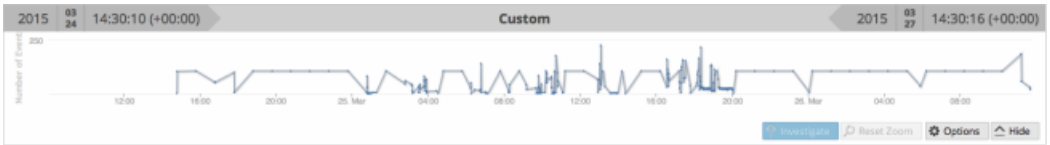
Visualisierungen

Im oberen Bereich der Ansicht „Navigieren“ wird eine Visualisierung des aktuellen Drill-down-Punkts angezeigt. Sie können über den Bereich „Visualisierung“ einen Drill-down in die Daten durchführen (siehe Zeitdiagramm des Drill-down in die Daten 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.



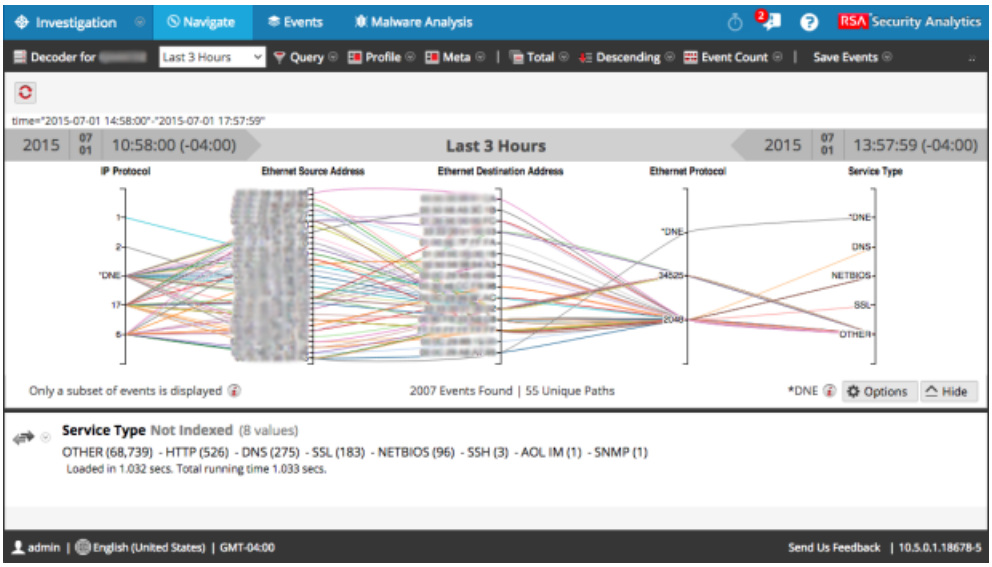


Die Zeitachse zeigt die Aktivitäten für den ausgewählten Service und Zeitbereich als Liniendiagramm oder Balkendiagramm an, je nachdem, was Sie im Menü „Optionen“ ausgewählt haben.

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.
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.
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.

Funktion	Beschreibung
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.

Funktion	Beschreibung
	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 „Navigieren“ ist der Bereich „Werte“, in dem Sie Daten analysieren können (siehe Drill-down zu Daten im Bereich „Werte“).

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 Suite die Schlüssel abfragt. Beim Laden der Daten in den Bereich „Werte“ wird NetWitness Suite 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 Benutzer festgelegt. und zwar:

- Die maximal zulässige Dauer einer Abfrage dieses Benutzers (Abfragetimeout)
- Der Schwellenwert, bis zu dem NetWitness Suite die Anzahl an Metawerten in einer Sitzung zählt (Sitzungsschwellenwert). Wenn ein Schwellenwert für eine Sitzung festgelegt ist, werden in der Navigationsansicht 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 Suite die Anzahl an Metawerten in einer Sitzung zählt (Sitzungsschwellenwert). Wenn ein Schwellenwert für eine Sitzung festgelegt ist, werden in der Navigationsansicht 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 Suite 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 Suite die Ergebnisse im Bereich „Werte“ an.

1. NetWitness Suite 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 Suite empfängt und zeigt Fortschrittsmeldungen an.

ii. **Teilergebnisse**: NetWitness Suite 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 Suite unter den Werten für jeden Metaschlüssel die Ladedauer und zusätzliche Ladeinformationen für die aggregierten Services an. NetWitness Suite blendet außerdem die Debug-Informationen unter der Breadcrumb-Navigation 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 Suite 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 Suite Abfragen ausführen. Wenn Sie z. B. Abfragen für einen 10.4-Broker ausführen, der Daten von mehreren Concentrators abruft, zeigt NetWitness Suite 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 dem Breadcrumb 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 im Breadcrumb 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. Detaillierte Informationen über nicht indizierte Metaschlüssel in Investigation erhalten Sie unter Verwalten und Anwenden von Standardmetaschlüsseln in einer Ermittlung.

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.

Kontextmenüs für Metaschlüssel

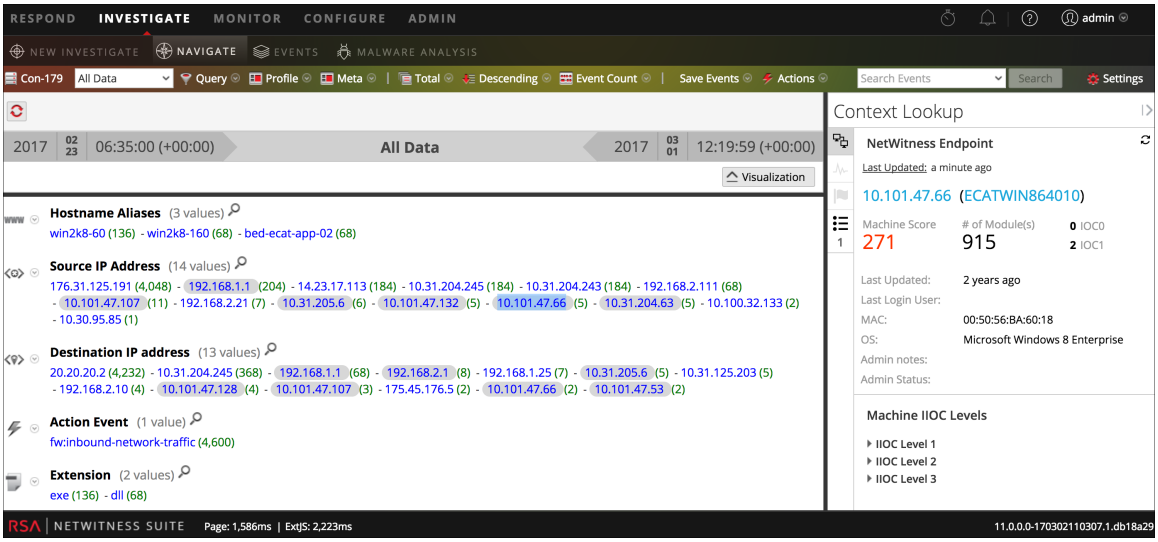
Die Metaschlüssel im Bereich „Werte“ weisen Kontextmenüs auf. Neben jedem Metanamen wird ein Drop-down-Pfeil mit Optionen angezeigt, die auf dieses Element zutreffen. Sie können diese Optionen nutzen, um die Darstellung der Ergebnisse für den Metaschlüssel in der aktuellen Ansicht zu ändern. Änderungen an Metaschlüsseln werden in der aktuellen Ansicht mit den bestehenden Drill-down-Punkten angezeigt, bis Sie die Seite aktualisieren oder einen neuen Service in der Symbolleiste der Ansicht „Navigieren“ auswählen. Durch eine Aktualisierung mit Verwalten und Anwenden von Standardmetaschlüsseln in einer Ermittlung wird die aktuelle Darstellung der Metaschlüssel wieder auf die im Dialogfeld „Standardmetaschlüssel managen“ definierte Ansicht zurückgesetzt (siehe „Verwalten und Anwenden von Standardmetaschlüsseln in einer Ermittlung“). Wenn Sie im Dialogfeld „Standardmetaschlüssel managen“ bisher keine Änderungen vorgenommen haben, stellt NetWitness Suite die standardmäßigen Metaschlüssel vom Core-Service wieder her.

- Mehr Ergebnisse
- Max. Ergebnisse
- Ergebnisse ausblenden
- Metaschlüsselinformationen

Bereich „Kontextabfrage“

In der Ansicht „Navigieren“ und der Ansicht „Ereignisse“ befindet sich rechts der Bereich „Kontextabfrage“. Der Kontextabfragebereich wird nur angezeigt, wenn der Service „Context Hub“ 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.

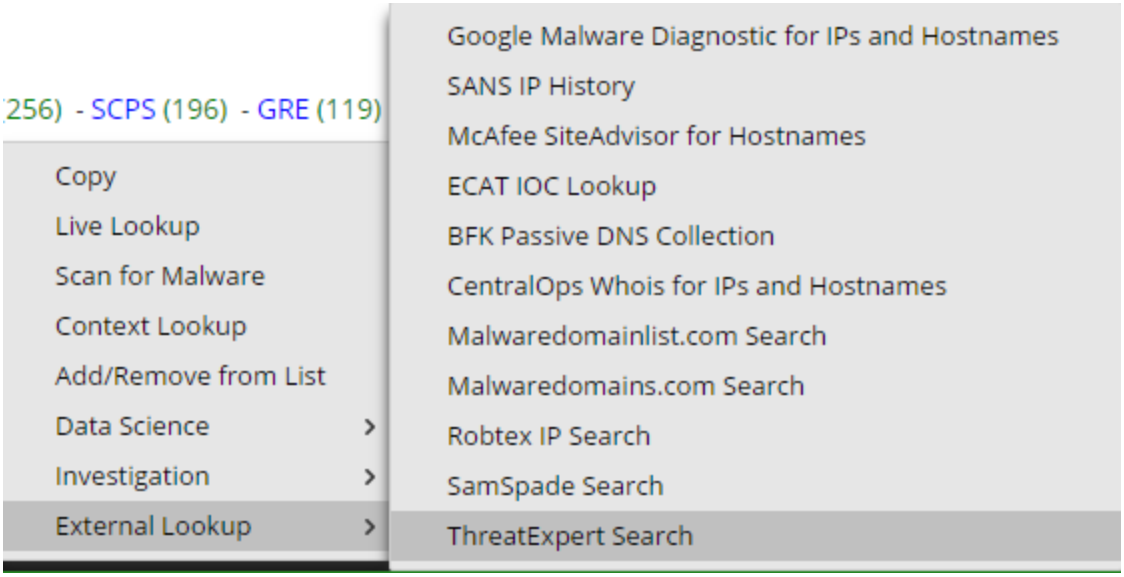


Nachdem der Administrator den Context Hub-Service konfiguriert hat, können Sie die Kontextinformationen für die Metawerte in der Ansicht „Navigieren“ und der Ansicht „Ereignisse“ anzeigen. Weitere Informationen zum Konfigurieren des Context Hub-Services finden Sie im *Context Hub-Konfigurationsleitfaden*. Informationen zur Durchführung von Kontextabfragen für Metawerte finden Sie unterAnzeigen von zusätzlichem Kontext für einen Datenpunkt.

Der Context Hub-Service ist mit einer Standardzuordnung von Metadatentyp und Metaschlüssel 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, Benutzer, werden die Details der mit einem Flag versehenen Werte aus Incident, Warnmeldungen und Listen erfasst.

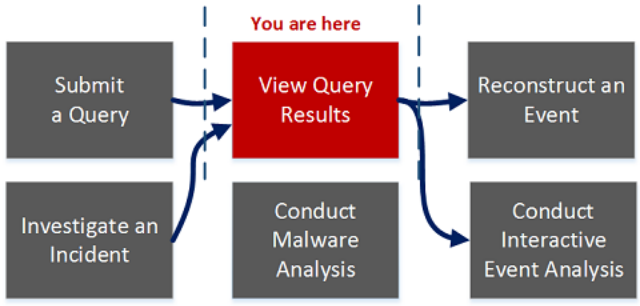
Die Daten werden im Bereich „Kontext“ nur angezeigt, wenn Daten verfügbar sind.

Weitere Informationen über die Ergebnisse der Suche und Kontextinformationen für verschiedene Datenquellen finden Sie unterBereich „Kontextabfrage“.

Dialogfeld „Abfrage“

Sie können in der Ansicht „Navigieren“ 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?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	eine angepasste Abfrage erstellen*	Erstellen einer angepassten Abfrage
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen	Durchführen einer Ermittlung
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses
Threat Hunter	ein Ereignis analysieren	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“

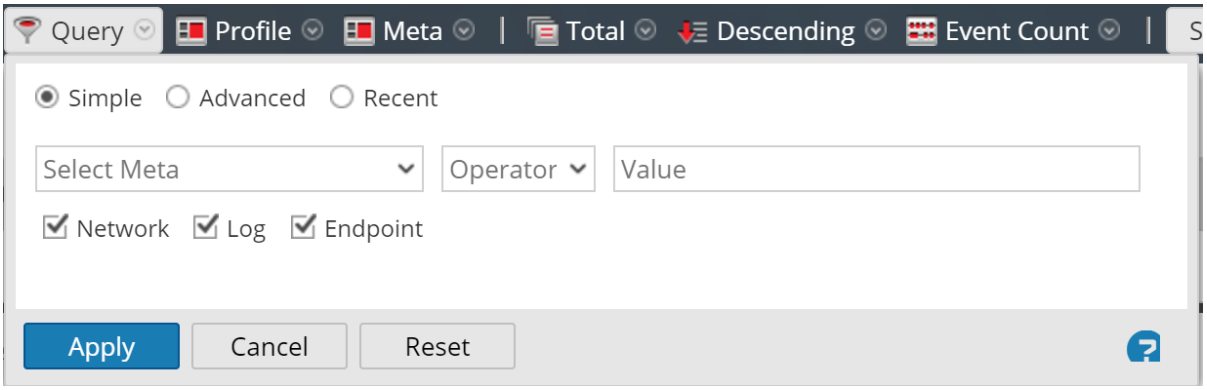
Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Schadsoftwareanalysen durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?

Überblick

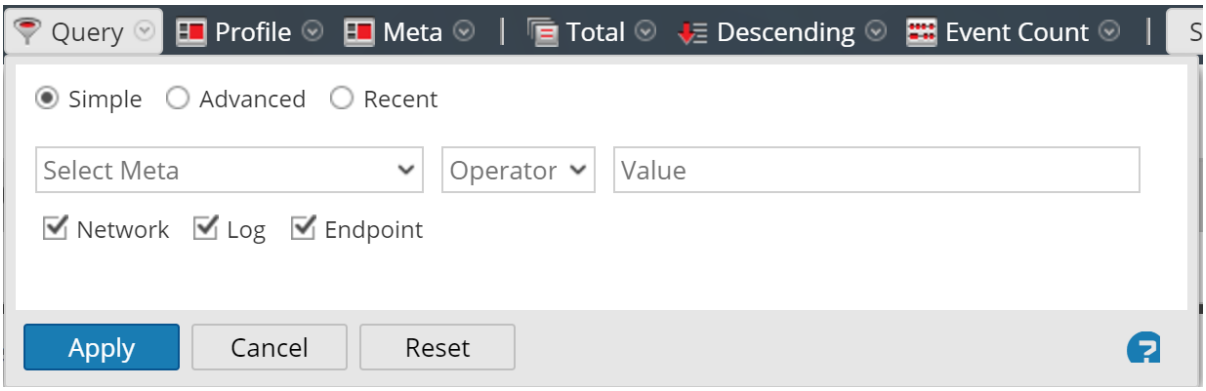


Das Dialogfeld „Abfrage“ umfasst drei Ansichten:

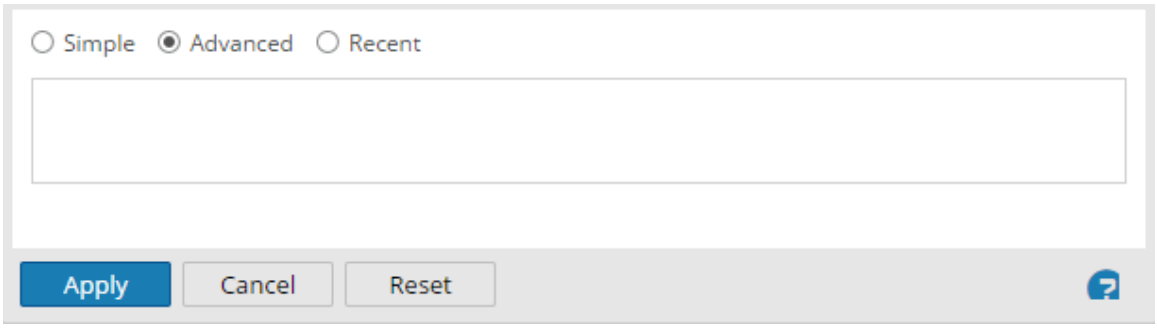
- Einfach
- Erweitert
- Zuletzt verwendet

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.

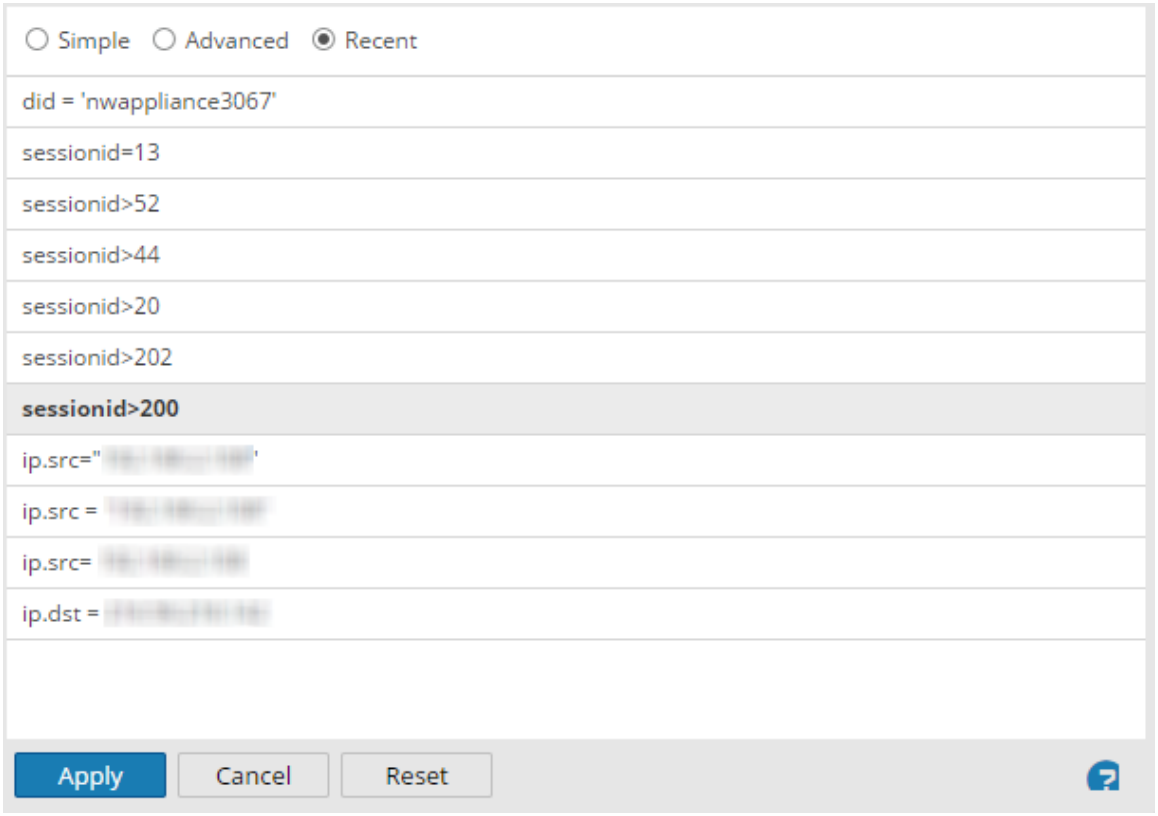
Ansicht „Einfach“



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 Suite!=,NetWitness Suiteexists,NetWitness Suite!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

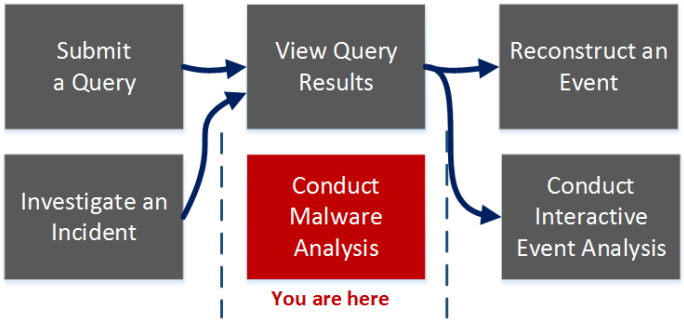
Funktion	Beschreibung
Feld „Abfrage“	Ermöglicht das Eingeben eine Abfrage in der Ansicht „Erweitert“. Wenn Sie zu tippen beginnen, wird eine Drop-down-Liste der verfügbaren Metaschlüssel für den Service angezeigt, danach wird beim Tippen eine Drop-down-Liste der Operatoren angezeigt. Wenn der aktuell 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.
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?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	eine Datei zum Scannen auf Schadsoftware senden*	Hochladen von Dateien für Malware Analysis-Scans
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen	Durchführen einer Ermittlung
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	ein Ereignis analysieren	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Schadsoftwareanalysen durchführen*	Durchführen von Schadsoftwareanalysen
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

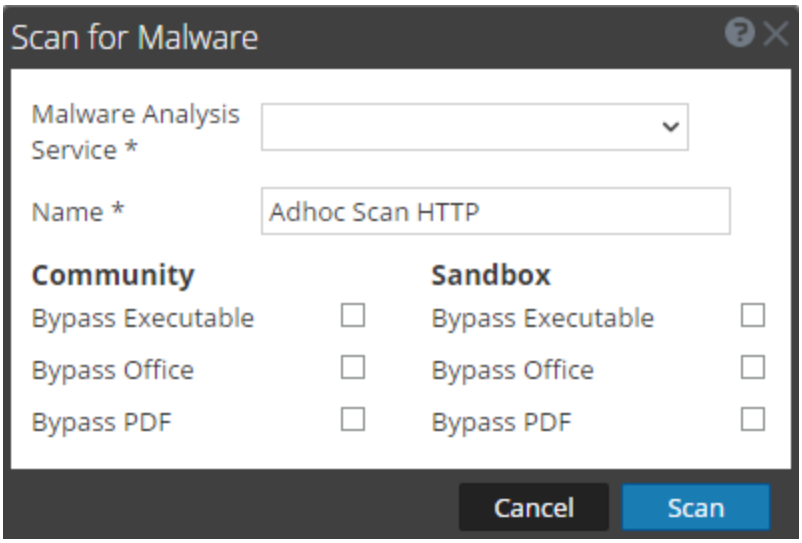
*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Beginnen einer Schadsoftwareanalyse-Ermittlung
- Starten eines Schadsoftwareanalyse-Scans in der Navigationsansicht

Überblick

Die folgende Abbildung zeigt das Dialogfeld „Auf Schadsoftware scannen“ und in der folgenden Tabelle sind die in diesem Dialogfeld verfügbaren Funktionen beschrieben.

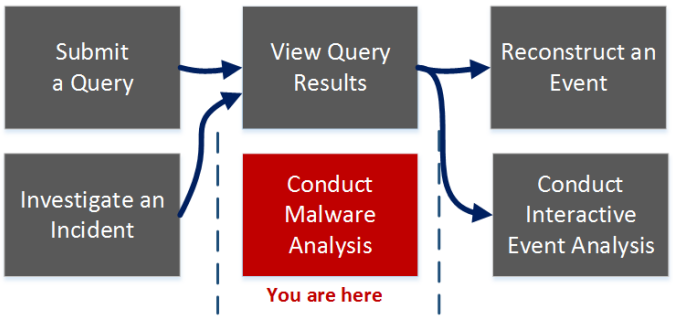


Funktion	Beschreibung
	Lädt eine Datei von Ihrem Computer hoch.
	Löscht eine Datei aus der Liste.
Dateiname	Zeigt die Namen der Dateien an, die der Liste hinzugefügt wurden.
Name	Hier können Sie einen Namen für den Scanjob eingeben.
Community	Zeigt Optionen für Community für das Umgehen oder Ignorieren 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 in der Ansicht „Malware Analysis“ aufgerufen werden. In diesem Dialogfeld können Malware Analysis-Analysten den zu untersuchenden Service auswählen, einen Scan für diesen festlegen, eine zu untersuchende Datei hochladen und einen fortlaufenden Scan für den Service starten.

Workflow



Was möchten Sie tun?

Benutzerrolle	Ich möchte…	Dokumentation
Threat Hunter	eine Datei zum Scannen auf Schadsoftware senden.*	Hochladen von Dateien für Malware Analysis-Scans
Threat Hunter	eine Abfrage senden.	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen.	Durchführen einer Ermittlung
Threat Hunter	ein Ereignis rekonstruieren.	Rekonstruieren eines Ereignisses
Threat Hunter	ein Ereignis analysieren.	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“

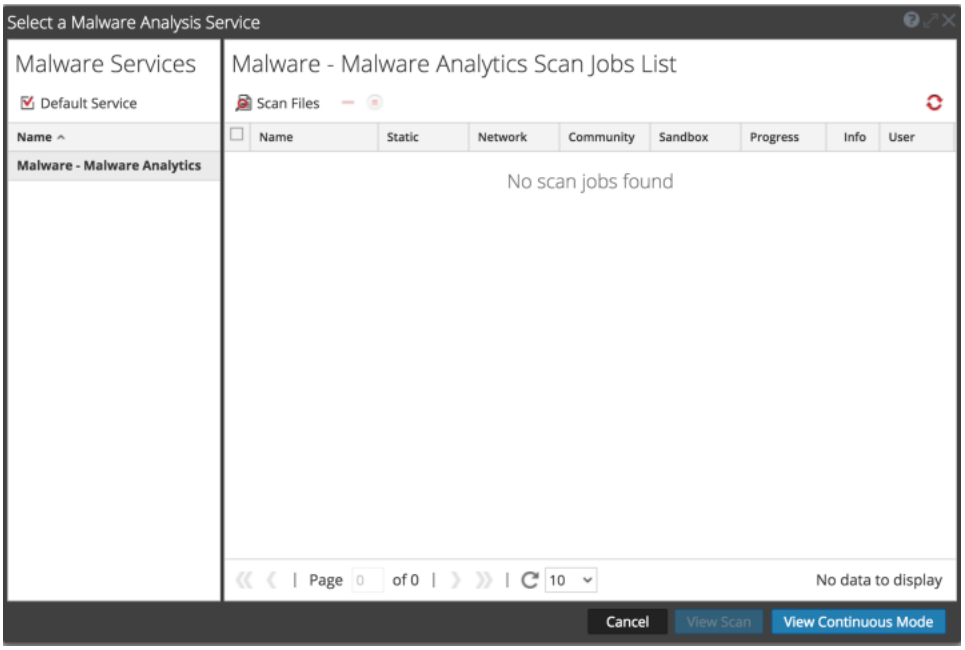
Benutzerrolle	Ich möchte…	Dokumentation
Threat Hunter	Schadsoftwareanalysen durchführen.*	Durchführen von Schadsoftwareanalysen
Incident-Experte	Untersuchen eines Incident	*NetWitness Respond – Benutzerhandbuch*

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

Verwandte Themen

- Wie funktioniert NetWitness Investigate?
- Beginnen einer Schadsoftwareanalyse-Ermittlung
- Starten eines Schadsoftwareanalyse-Scans in der Navigationsansicht

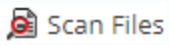
Überblick



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 Aufrufen 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 auf der Symbolleiste „Liste der Scanjobs“.

Funktion	Beschreibung
	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 Suite 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.

Funktion	Beschreibung
Benutzer	Zeigt den Namen des Benutzers an, der den Job erstellt hat.
Ereignisse	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.

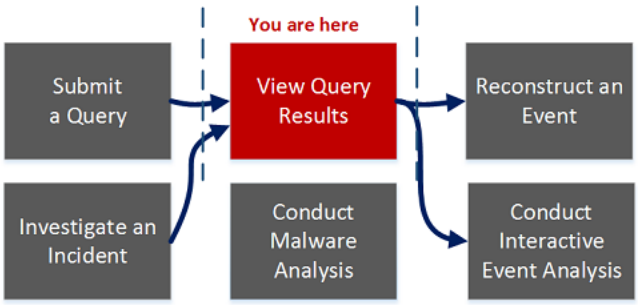
Funktion	Beschreibung
Schaltfläche Abbrechen	Bricht den ausgewählten Scanjob ab.
Schaltfläche Scan anzeigen	Zeigt die Ereigniszusammenfassung für den ausgewählten Scan mit den standardmäßigen Dashlets an.
Schaltfläche Fortlaufenden Modus anzeigen	Zeigt die Ereigniszusammenfassung für den ausgewählten Scan mit den standardmäßigen Dashlets an.

Einstellungsdialogfeld für die Ansichten „Navigieren“ und „Ereignisse“

Die Einstellungen in den Dialogfelder „Einstellungen“ in den Ansichten „Navigieren“ 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 Suite 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**.

Workflow



Was möchten Sie tun?

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	Einstellungen für Ermittlung konfigurieren*	Konfigurieren von Navigationsansicht und Ereignisansicht
Threat Hunter	eine Abfrage senden	Starten einer Untersuchung für einen Service oder eine Sammlung
Threat Hunter	Abfrageergebnisse anzeigen*	Durchführen einer Ermittlung
Threat Hunter	ein Ereignis rekonstruieren	Rekonstruieren eines Ereignisses

Benutzerrolle	Ziel	Dokumentation
Threat Hunter	ein Ereignis analysieren	Analysieren von Ereignissen in der Ansicht „Ereignisanalyse“
Threat Hunter	Schadsoftwareanalysen durchführen	Durchführen von Schadsoftwareanalysen
Incident-Experte	einen Incident untersuchen	*NetWitness Respond – Benutzerhandbuch*

*Sie können diese Aufgabe in der aktuellen Ansicht durchführen.

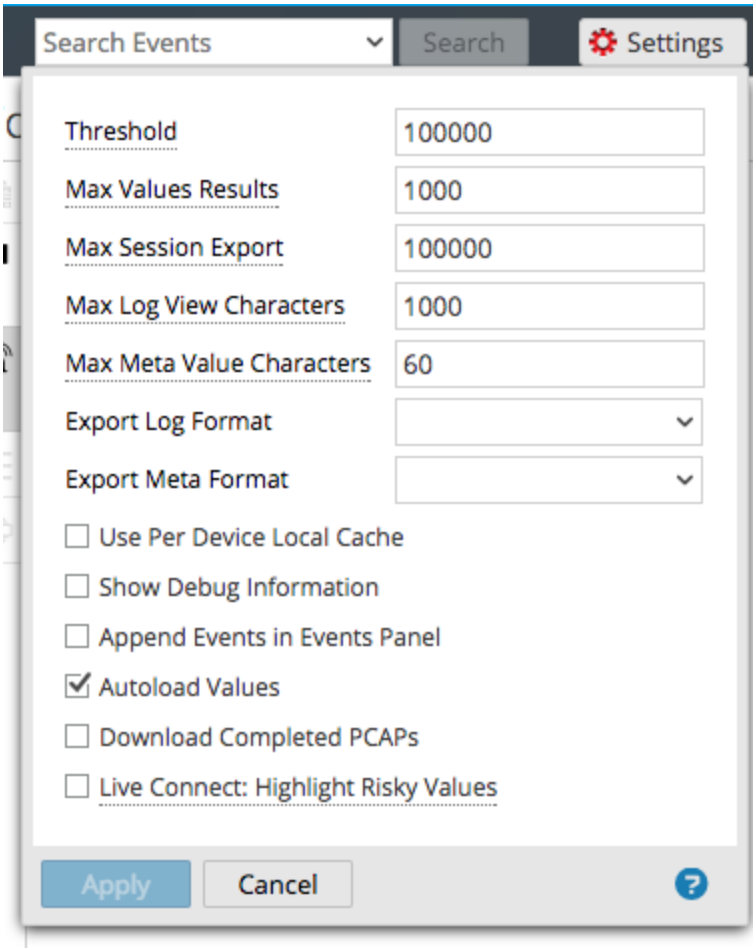
Verwandte Themen

- Wie funktioniert NetWitness Investigate?

Überblick

Die Dialogfelder „Einstellungen“ in den Ansichten „Navigieren“ und „Ereignisse“ enthalten viele gemeinsame Komponenten.

Verschiedene Investigation-Einstellungen in der Ansicht „Navigieren“ 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**.

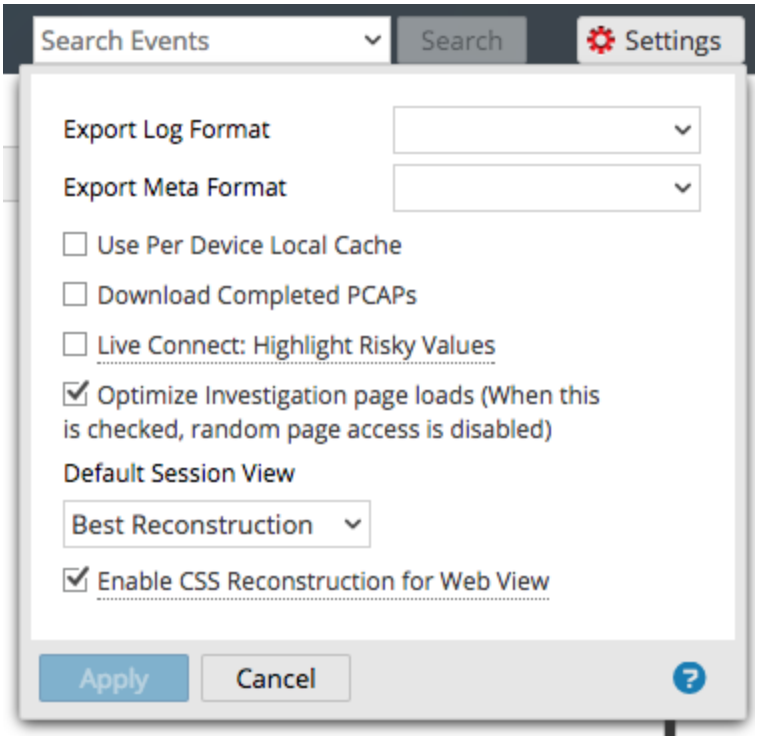
Funktion	Beschreibung
Max. Wertergebnisse	Legt die maximale Anzahl von Werten fest, die in der Ansicht Navigieren geladen werden, wenn im Metaschlüsselmenü die Option Max. Ergebnisse für einen offenen Metaschlüssel ausgewählt ist. Der Standardwert ist **1.000**.
Max. Sitzungsexport	Legt die maximale Anzahl von Sitzungen fest, die exportiert werden können. Der Standardwert ist **100.000**.
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.

Funktion	Beschreibung
Debuginformationen anzeigen	Diese Option steuert die Anzeige der `where`-Klausel unterhalb der Breadcrumb-Navigation in der Ansicht „Navigieren“ 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 „Navigieren“ 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 „Navigieren“ 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
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 aktiviert ist, zeigt NetWitness Suite alle IP-Adressen an. Diese Option ist standardmäßig deaktiviert (**Aus**).

Funktion	Beschreibung
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.