RSA NETWITNESS® SUITE

NetWitness Respond – Benutzerhandbuch

für Version 11,1

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

Drittanbieterlizenzen

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

Hinweis zu Verschlüsselungstechnologien

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

Verteilung

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

Juli 2018

Inhalt

NetWitness Respond-Prozess

NetWitness Suite Respond sammelt Warnmeldungen aus mehreren Quellen, die in logische Gruppen unterteilt werden können. Durch Anstoßen eines Incident-Reaktions-Workflows werden die aufgekommenen Sicherheitsprobleme dann untersucht und behoben.NetWitness Suite Respond ermöglicht es Ihnen, Regeln für die Aggregation von Warnmeldungen in Vorfällen zu konfigurieren. Die Warnmeldungen werden vom System in ein allgemeingültiges Format normalisiert, um eine einheitliche Ansicht der Regelkriterien unabhängig von der Datenquelle zu ermöglichen. Auf Grundlage der Warnmeldungsdaten können Sie Abfragekriterien erstellen, um solche Felder abzufragen, die häufig in Datenquellen vorkommen und für diese spezifisch sind.

Die Regel-Engine ermöglicht die Gruppierung ähnlicher Warnmeldungen in ein Incident, damit der Ermittlungs- und Behebungworkflow auf mehrere Gruppen mit ähnlichen Warnmeldungen angewendet werden kann. Mithilfe von Regeln, die Sie erstellen, können Sie abhängig von einem gemeinsamen Wert für ein oder zwei Attribute (Beispiel: Quellenhostname) Warnmeldungen in Incidents gruppieren. Eine solche Gruppe kann auch anhand dessen erstellt werden, ob die Warnmeldungen innerhalb eines bestimmten Zeitfensters aufgetreten sind (Beispiel: Warnmeldungen mit einem Abstand von jeweils weniger als 4 Stunden zueinander).

Wenn eine Warnmeldung von einer Regel erfasst wird, wird anhand der Kriterien ein Incident erstellt. Wenn ein vorhandener Incident mit den entsprechenden Kriterien erstellt wurde und der Incident noch nicht ausgeführt wird, werden diesem Incident weiterhin neu auftretende Warnmeldungen hinzugefügt. Wenn für die Werte der Gruppe (beispielsweise ein bestimmter Hostname) oder für das Zeitfenster noch kein Incident vorhanden ist, wird ein neuer Incident erstellt und die Warnmeldung wird diesem Incident hinzugefügt.

Es können mehrere Incident-Regeln verwendet werden. Mit diesen Regeln können entweder Warnmeldungen in Incidents gruppiert oder Warnmeldungen unterdrückt werden, damit sie nicht mit Regeln abgeglichen werden. Regeln werden von oben nach unten nacheinander abgearbeitet. Wenn eine eingehende Warnmeldung einer Regel entspricht, wird diese Warnmeldung dem entsprechenden Incident zugeordnet und keine weitere Regel wird auf sie angewendet. Durch Incidents wird ein Kontext für Warnmeldungen gegeben, es werden Tools zum Erfassen des Ermittlungsstatus bereitgestellt und der Fortschritt zugehöriger Aufgaben kann nachverfolgt werden.

Die Phasen des NetWitness Respond-Prozesses sind:

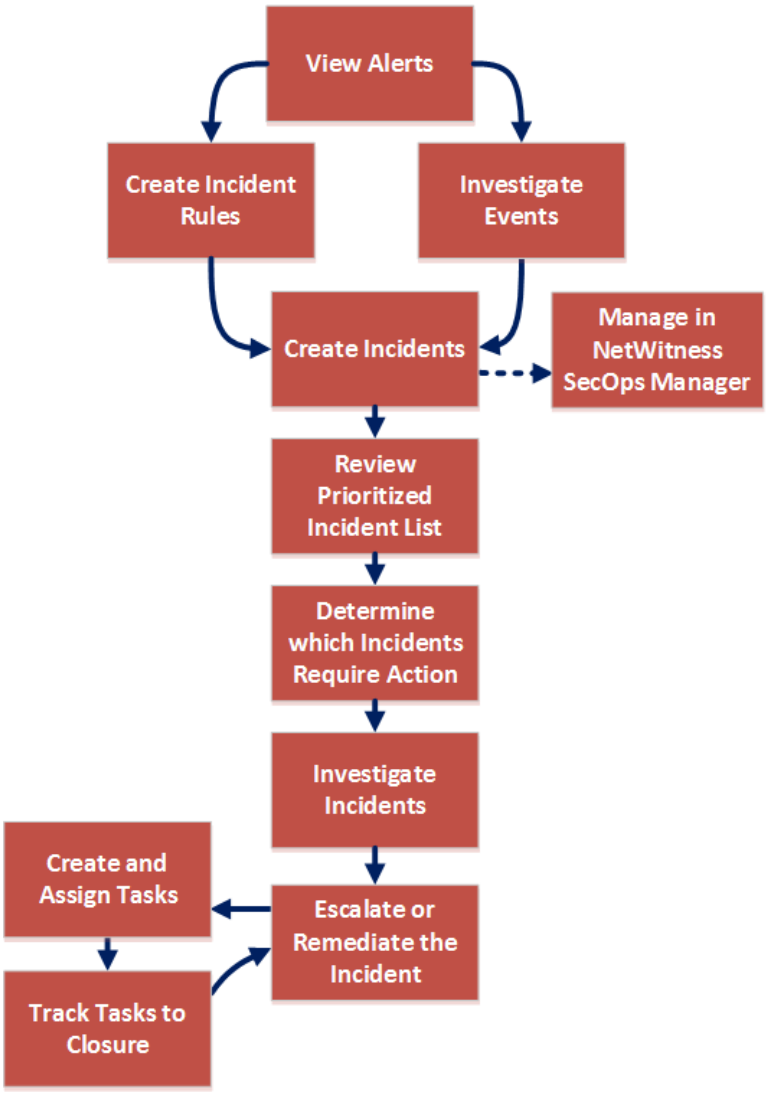
- Überprüfen von Warnmeldungen
- Erstellen von Incidents
- Reagieren auf Incidents:
  - Überprüfen der Liste mit priorisierten Incidents
  - Bestimmen, welche Incidents eine Aktion erfordern

- Untersuchen von Incidents
- Eskalieren oder korrigieren Sie den Incident (dies umfasst das Erstellen und Zuweisen von Aufgaben sowie das Nachverfolgen von Aufgaben bis zum Abschluss).

Sie haben auch die Möglichkeit, Incidents in RSA NetWitness® SecOps Manager anstelle von NetWitness Respond zu managen.

NetWitness Respond-Workflow

Die folgende Abbildung zeigt den allgemeinen NetWitness Respond-Workflow-Prozess.



Reagieren auf Incidents

Ein *Incident* ist ein Satz logisch gruppierter Warnmeldungen, die automatisch von der Incident-Aggregations-Engine erstellt und nach bestimmten Kriterien gruppiert werden. Über einen Incident, der in der Ansicht „Reagieren“ zur Verfügung steht, können Analysten diese Gruppen der Warnmeldungen priorisieren, untersuchen und beheben. Incidents können zwischen Benutzern verschoben, mit Anmerkungen versehen und in einem Node-Diagramm untersucht werden. Incidents sorgen dafür, dass Benutzer das volle Ausmaß eines Angriffs oder eines Ereignisses in ihrem NetWitness Suite-System verstehen und dann Maßnahmen ergreifen können.

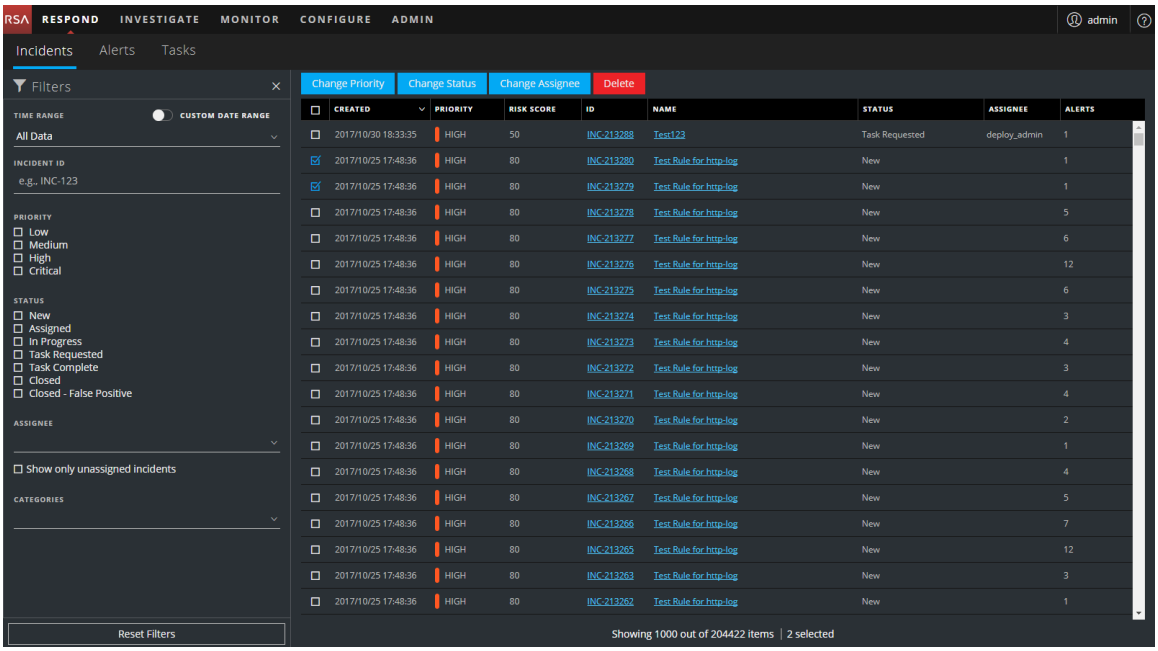
Die Ansicht **Reagieren** soll Ihnen helfen, die noch nicht behobenen Probleme in Ihrem Netzwerk schnell zu identifizieren und diese Probleme mit anderen Analysten zusammen schnell zu lösen.

In der Ansicht „Reagieren“ wird Incident-Experten eine Warteschlange mit Incidents in der Reihenfolge des Schweregrads angezeigt. Wenn Sie einen Incident in der Warteschlange auswählen, erhalten Sie relevante zugehörige Daten, damit Sie den Incident untersuchen können. So können Sie den Umfang des Incident ermitteln und ihn nach Bedarf eskalieren oder korrigieren.

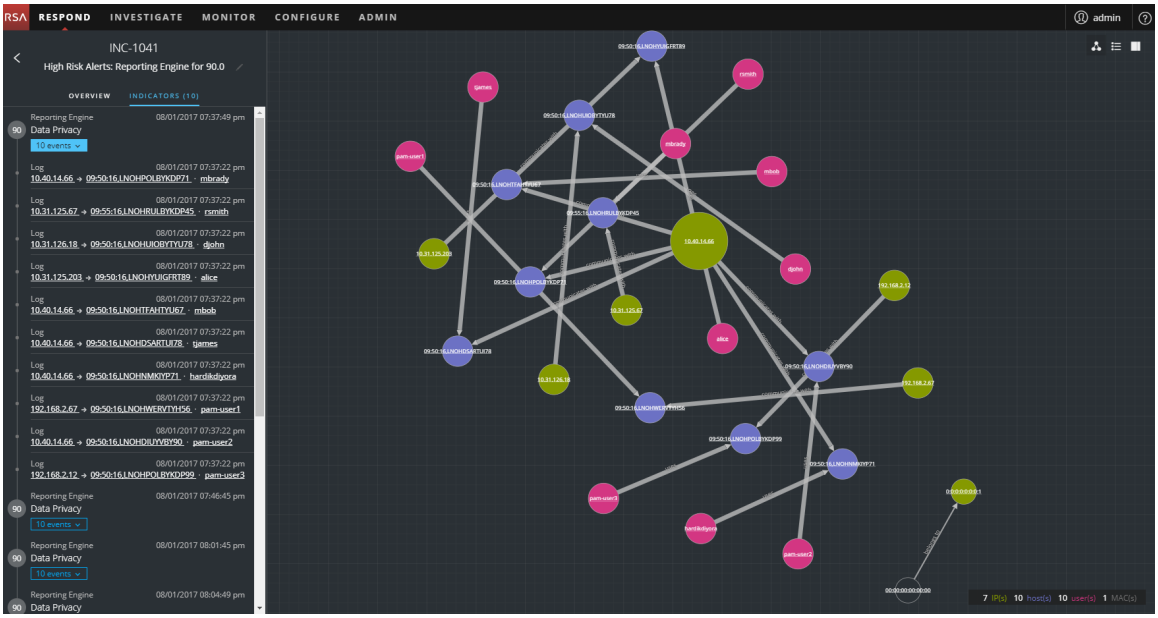
In der Ansicht „Reagieren“ werden Incidents, Warnmeldungen und Aufgaben angezeigt:

- **Incidents**: Ermöglicht es Ihnen, auf Incidents zu reagieren und sie zu managen.
- **Warnmeldungen**: Ermöglicht es Ihnen, Warnmeldungen aus allen Quellen zu managen, die von NetWitness Suite empfangen werden, und zu ausgewählten Warnmeldungen Incidents zu erstellen.
- **Aufgaben**: Ermöglicht es Ihnen, die vollständige Liste der Aufgaben anzuzeigen und zu managen, die für alle Incidents erstellt wurde.

Wenn Sie zu „REAGIEREN“ > „Incidents“ navigieren, können Sie die Ansicht „Incident-Liste“ sehen. Von dort aus können Sie auf die Ansicht „Incident-Details“ für einen ausgewählten Incident zugreifen. Hierbei handelt es sich um die Hauptansichten, die Sie verwenden, um auf Incidents zu reagieren. Auf der folgenden Abbildung ist die Liste der priorisierten Incidents in der Ansicht **Incident-Liste** zu sehen.



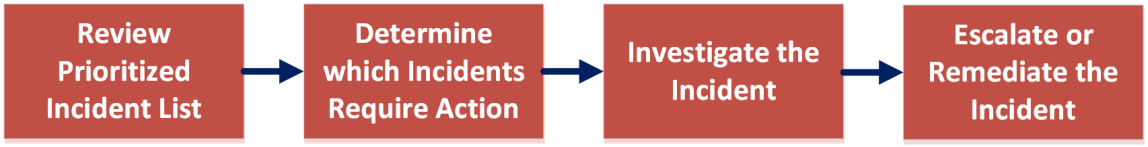
Die nächste Abbildung zeigt ein Beispiel für Details, die in der Ansicht **Incident-Details** verfügbar sind.



Die Ansicht „Reagieren“ soll die Bewertung von Incidents, die Kontextualisierung von Daten, die Zusammenarbeit mit anderen Analysten und bei Bedarf den Wechsel zu einer detaillierten Untersuchung vereinfachen.

Reagieren auf Incidents-Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess, anhand dessen Incident-Experten in NetWitness Suite auf Incidents reagieren.



Sie müssen zunächst die Liste der priorisierten Incidents überprüfen, in der grundlegende Informationen zu allen Incidents stehen, und herausfinden, für welche Aktionen erforderlich sind. Sie können einen Link in einem Incident anklicken, um zugehörige Details in der Ansicht „Incident-Details“ anzuzeigen. Von dort können Sie den Incident genauer untersuchen. Dann können Sie bestimmen, wie Sie auf den Incident reagieren, indem sie ihn eskalieren oder korrigieren.

Dies sind die grundlegenden Schritte zum Reagieren auf einen Incident:

1. Überprüfen der Liste mit priorisierten Incidents
2. Ermitteln, welche Incidents eine Aktion erfordern
3. Untersuchen des Incident
4. Eskalieren oder Korrigieren des Incident

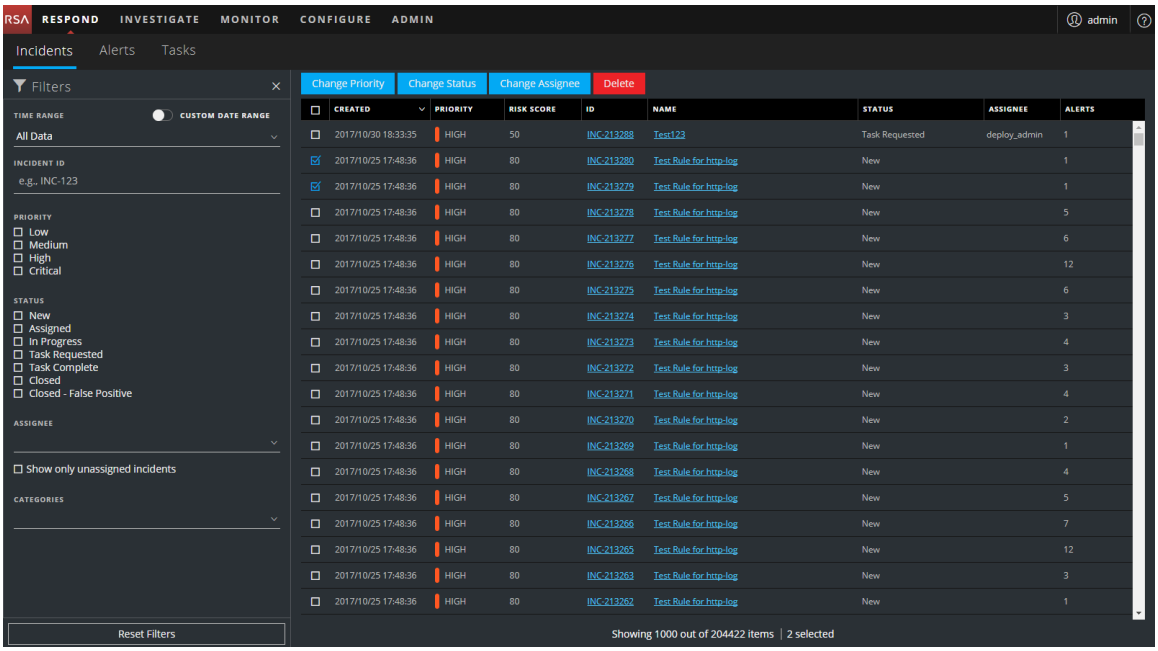
Überprüfen der Liste mit priorisierten Incidents

In der Ansicht „Reagieren“ können Sie die Liste der priorisierten Incidents anzeigen. In der Incident-Liste werden sowohl aktive als auch geschlossene Incidents angezeigt.

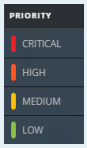
Aufrufen der Incident-Liste

Nach der Anmeldung bei NetWitness Suite wird den meisten Incident-Experten die Ansicht „Reagieren“ angezeigt, da sie als Standardansicht festgelegt ist. Wenn für Sie eine andere erste Ansicht eingestellt ist, können Sie zur Ansicht „Reagieren“ navigieren.

1. Melden Sie sich in NetWitness Suite an.
   In der Ansicht „Reagieren“ wird die Liste der Incidents angezeigt, die auch als Ansicht „Incident-Liste“ bezeichnet wird.



2. Wenn Sie die Incident-Liste in der Ansicht „Reagieren“ nicht sehen, navigieren Sie zu **Reagieren > Incidents**.
3. Blättern Sie durch die Incident-Liste, in der grundlegende Informationen zu jedem Incident wie in der folgenden Tabelle beschrieben angezeigt werden.

Spalte	Beschreibung
CREATED	Zeigt das Erstellungsdatum des Incident an.
PRIORITÄT	Zeigt die Priorität des Incident an. Die Priorität kann „Kritisch“, „Hoch“, „Mittel“ oder „Niedrig“ sein. Für die Priorität wird ein Farbcode verwendet: Rot kennzeichnet einen Incident als **Kritisch**, Orange steht für Incidents mit der Risikobewertung **Hoch**, Gelb für Incidents mit der Risikobewertung**Mittel** und Grün für Incidents mit der Risikobewertung **Niedrig**. Beispiel: 

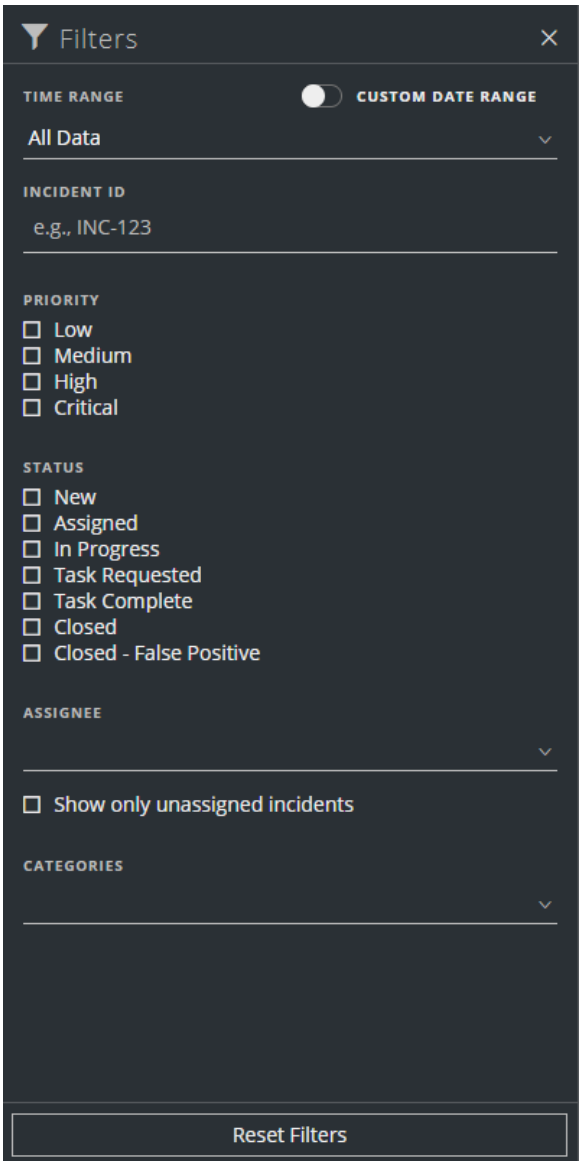
Spalte	Beschreibung
Risikowert	Zeigt den Risikowert des Incident an. Der Risikowert gibt das Risikopotenzial des Incident an. Er wird mittels eines Algorithmus berechnet und liegt zwischen 0 und 100. 100 ist der höchste Risikowert.
ID	Zeigt die automatisch erstellte Incident-Nummer an. Jedem Incident wird eine eindeutige Nummer zugewiesen, anhand derer Sie den Incident nachverfolgen können.
NAME	Zeigt den Namen des Incident an. Der Incident-Name leitet sich aus der Regel ab, die den Incident ausgelöst hat. Durch Klicken auf den Link können Sie die Detailansicht des jeweils ausgewählten Incident aufrufen.
STATUS	Zeigt den Status des Incident an. Mögliche Status sind: **Neu**, **Zugewiesen**, **Läuft**, **Aufgabe angefordert**, **Aufgabe abgeschlossen**, **Geschlossen** und **Geschlossen – falsch positives Ergebnis**.
ZUWEISUNGSEMPFÄNGER	Zeigt das Teammitglied an, dem der Incident derzeit zugewiesen ist.
WARNMELDUNGEN	Zeigt an, wie viele Warnmeldungen dem Incident zugeordnet sind. Ein Incident kann viele Warnmeldungen enthalten. Eine große Anzahl von Warnmeldungen kann auf einen großflächigen Angriff hindeuten.

Am unteren Rand der Liste sehen Sie die Anzahl der Incidents auf der aktuellen Seite, die Gesamtzahl der Incidents und die Anzahl der ausgewählten Incidents. Beispiel: **1.000 von 1.115 Elementen werden angezeigt | 3 ausgewählt**. Es können maximal 1.000 Incidents gleichzeitig angezeigt werden.

Filtern der Incident-Liste

Die Anzahl der Incidents in der Ansicht „Incident-Liste“ kann sehr groß sein, sodass es schwierig ist, bestimmte Incidents zu finden. Mit dem Filter können Sie die Incidents angeben, die Sie anzeigen möchten. Sie können auch den Zeitraum auswählen, in dem diese Incidents aufgetreten sind. Nehmen wir an, Sie möchten alle neuen kritischen Incidents anzeigen, die in der letzten Stunde aufgetreten sind.

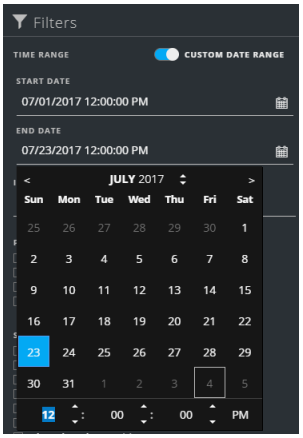
1. Stellen Sie sicher, dass der Bereich „Filter“ links neben der Liste mit Incidents angezeigt wird. Sollte der Bereich „Filter“ nicht angezeigt werden, klicken Sie in der Symbolleiste der Ansicht „Incident-Liste“ auf , um den Bereich „Filter“ zu öffnen.



2. Wählen Sie im Bereich „Filter“ eine oder mehrere Optionen zum Filtern der Incident-Liste aus:

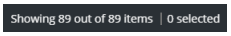
   - **ZEITBEREICH**: Sie können einen bestimmten Zeitraum in der Drop-down-Liste „Zeitbereich“ auswählen. Der Zeitbereich basiert auf dem Erstellungsdatum der Incidents. Wenn Sie zum Beispiel „Letzte Stunde“ auswählen, werden die Incidents angezeigt, die innerhalb der letzten 60 Minuten erstellt wurden.

- **BENUTZERDEFINIERTER DATUMSBEREICH**: Sie können einen bestimmten Datumsbereich anstelle der Option „Zeitbereich“ auswählen. Klicken Sie dazu auf den weißen Kreis vor „Benutzerdefinierter Datumsbereich“, damit die Felder „Startdatum“ und „Enddatum“ angezeigt werden. Wählen Sie die Datums- und Zeitangaben im Kalender aus.



- **INCIDENT-ID**: Hier können Sie die Incident-ID des Incident eingeben, den Sie suchen, zum Beispiel „INC-1050“.
- **PRIORITÄT**: Wählen Sie die Prioritäten aus, die Sie anzeigen möchten.
- **STATUS**: Wählen Sie einen oder mehrere Incident-Status aus. Wenn Sie beispielsweise „Geschlossen – falsch positives Ergebnis“ auswählen, werden nur falsch positive Incidents angezeigt, also Incidents, die zunächst als verdächtigt eingestuft, dann aber als sicher bestätigt wurden.
- **ZUWEISUNGSEMPFÄNGER**: Hier können Sie einen oder mehrere Zuweisungsempfänger auswählen, deren Incidents Sie anzeigen möchten. Sollen beispielsweise nur die Incidents angezeigt werden, die Cale oder Stanley zugewiesen sind, wählen Sie „Cale“ und „Stanley“ in der Drop-down-Liste „Zuweisungsempfänger“ aus. Lassen Sie die Auswahl unter „Zuweisungsempfänger“ frei, wenn die Incidents unabhängig von ihrem Zuweisungsempfänger angezeigt werden sollen.
  (Verfügbar in Version 11.1 und neueren Versionen) Wenn Sie nur Incidents anzeigen möchten, die nicht zugewiesen sind, wählen Sie **Nur nicht zugewiesene Incidents anzeigen** aus.
- **KATEGORIEN**: In dieser Drop-down-Liste können Sie eine oder mehrere Kategorien auswählen. Wenn Sie beispielsweise nur Incidents der Kategorien „Backdoor“ oder „Rechtemissbrauch“ anzeigen möchten, müssen Sie „Backdoor“ und „Rechtemissbrauch“ auswählen.

In der Incident-Liste wird eine Liste der Incidents angezeigt, die Ihre Auswahlkriterien erfüllen. Sie finden die Anzahl der Incidents in der gefilterten Liste am unteren Rand der Incident-Liste.



3. Klicken Sie auf ×, um den Bereich „Filter“ zu schließen und zur Ansicht „Incident-Liste“ zurückzukehren, in der nun Ihre gefilterten Incidents angezeigt werden.

Entfernen meiner Filter aus der Ansicht „Incident-Liste“

NetWitness Suite speichert Ihre Filterauswahl in der Ansicht „Incident-Liste“. Sie können Ihre Filterauswahl entfernen, wenn Sie sie nicht mehr benötigen. Wenn Sie beispielsweise nicht die erwartete Anzahl an Incidents sehen oder alle Incidents in der Incident-Liste anzeigen möchten, können Sie Ihre Filter zurücksetzen.

1. Klicken Sie auf der Symbolleiste der Ansicht „Incident-Liste“ auf ▼.
   Der Bereich „Filter“ erscheint links neben der Incident-Liste.
2. Klicken Sie am unteren Rand des Bereichs „Filter“ auf **Filter zurücksetzen**.

Anzeigen eigener Incidents

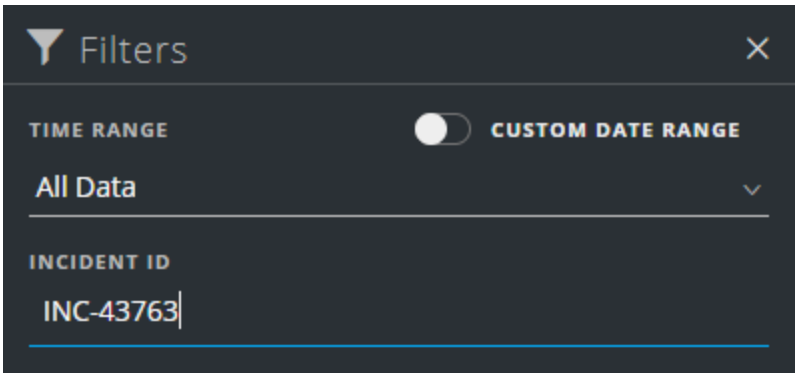
Sie können Ihre Incidents anzeigen, indem Sie die Incidents nach Ihrem Benutzernamen filtern.

1. Wenn Sie den Bereich „Filter“ nicht sehen können, klicken Sie auf der Symbolleiste der Ansicht „Incident-Liste“ auf ▼.
2. Wählen Sie im Bereich „Filter“ unter „ZUWEISUNGSEMPFÄNGER“ Ihren Benutzernamen aus der Drop-down-Liste aus.
   In der Incident-Liste werden die Incidents angezeigt, die Ihnen zugewiesen sind.

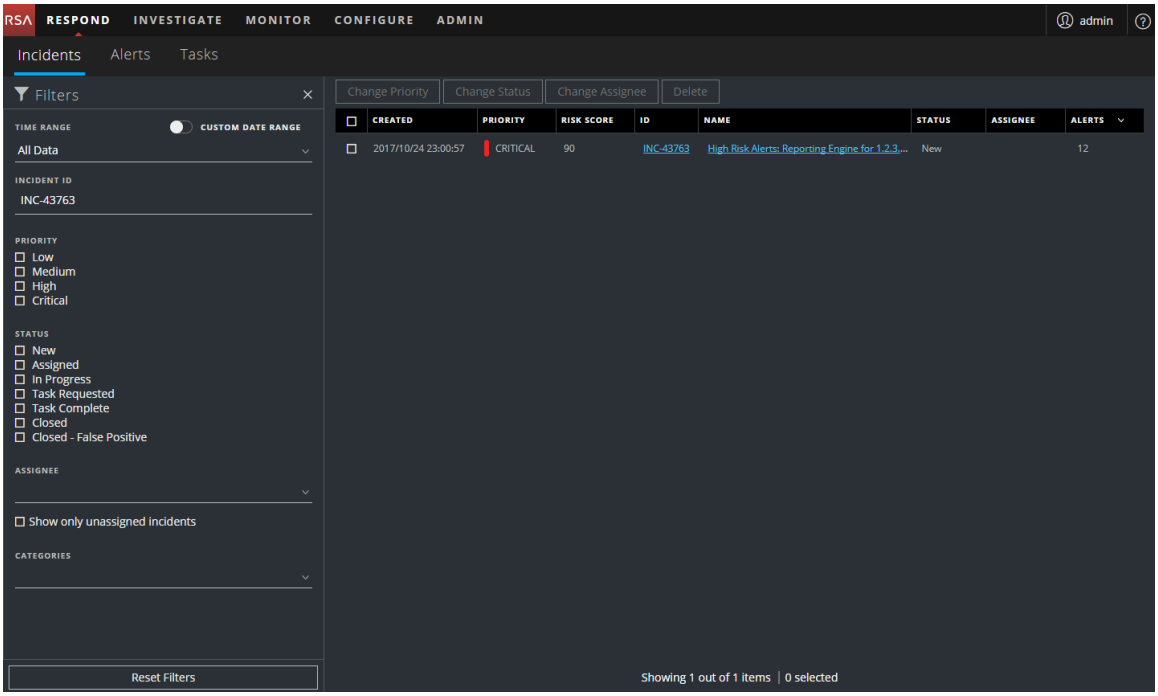
Suchen von Incidents

Wenn Sie die Incident-ID kennen, können Sie einen Incident schnell mithilfe des Filters suchen. Beispiel: Sie möchten einen bestimmten Incident in Tausenden von Incidents suchen.

1. Navigieren Sie zu **Reagieren > Incidents**.
   Der Bereich „Filter“ wird links neben der Liste mit Incidents angezeigt. Sollte der Bereich „Filter“ nicht angezeigt werden, klicken Sie in der Symbolleiste der Ansicht „Incident-Liste“ auf ▼, um den Bereich „Filter“ zu öffnen.

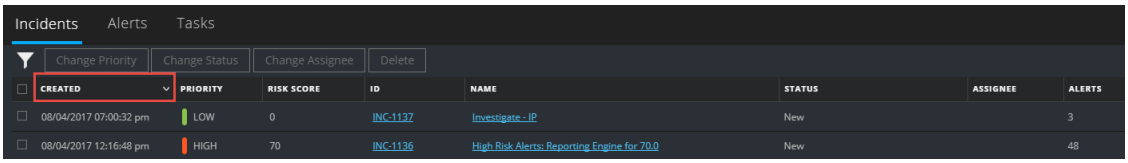


2. Geben Sie in das Feld „Incident-ID“ die Incident-ID für den Incident ein, nach dem Sie suchen möchten, z. B. INC-43763.
   Der angegebene Incident wird in der Incident-Liste angezeigt. Wenn keine Ergebnisse angezeigt werden, versuchen Sie, die Filter zurücksetzen.



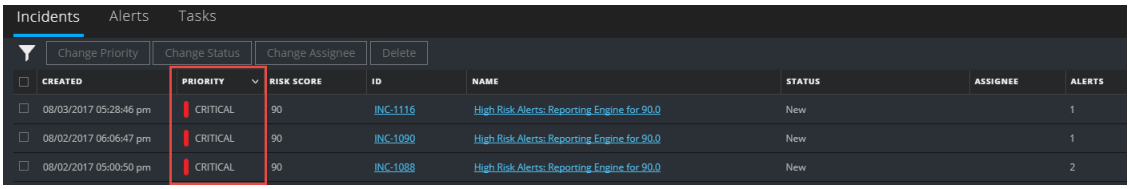
Sortieren der Incident-Liste

Die Sortierung der Incident-Liste erfolgt standardmäßig nach dem Erstellungsdatum in absteigender Reihenfolge (neueste oben).

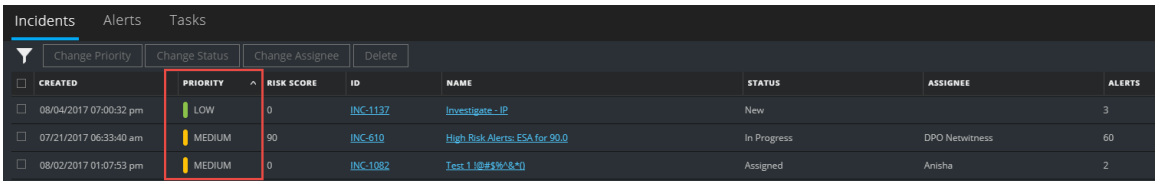


Sie können die Sortierreihenfolge der Incident-Liste ändern, indem Sie auf eine Spalte in der Liste klicken.

Wenn Sie Ihre Incidents zum Beispiel priorisieren möchten, können Sie sie anhand der Spalte „Priorität“ sortieren. Bewegen Sie dazu den Mauszeiger über die Spalte „Priorität“ und klicken Sie auf den Abwärtspfeil (▼). Die Incident-Liste wird nach Priorität und in absteigender Reihenfolge sortiert (höchste Priorität zuerst), wie auf der folgenden Abbildung zu sehen.



Sie können nach „Priorität“ in aufsteigender Reihenfolge sortieren (niedrigste Priorität oben), indem Sie auf den Aufwärtspfeil (▲) klicken, wie auf der folgenden Abbildung dargestellt.

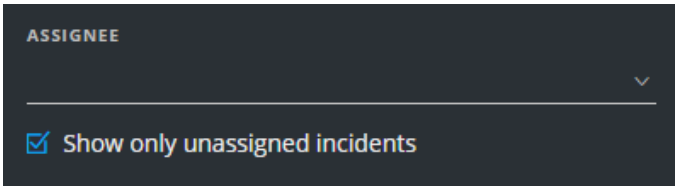


Nicht zugewiesene Vorfälle

Diese Option ist nur für Version 11.1 und höher verfügbar.

Mithilfe des Filters können Sie nicht zugewiesene Incidents anzeigen.

1. Wenn Sie den Bereich „Filter“ nicht sehen können, klicken Sie auf der Symbolleiste der Ansicht „Incident-Liste“ auf ▼.
2. Wählen Sie im Bereich „Filter“ unter ZUWEISUNGSEMPFÄNGER die Option **Nur nicht zugewiesene Incidents anzeigen** aus.

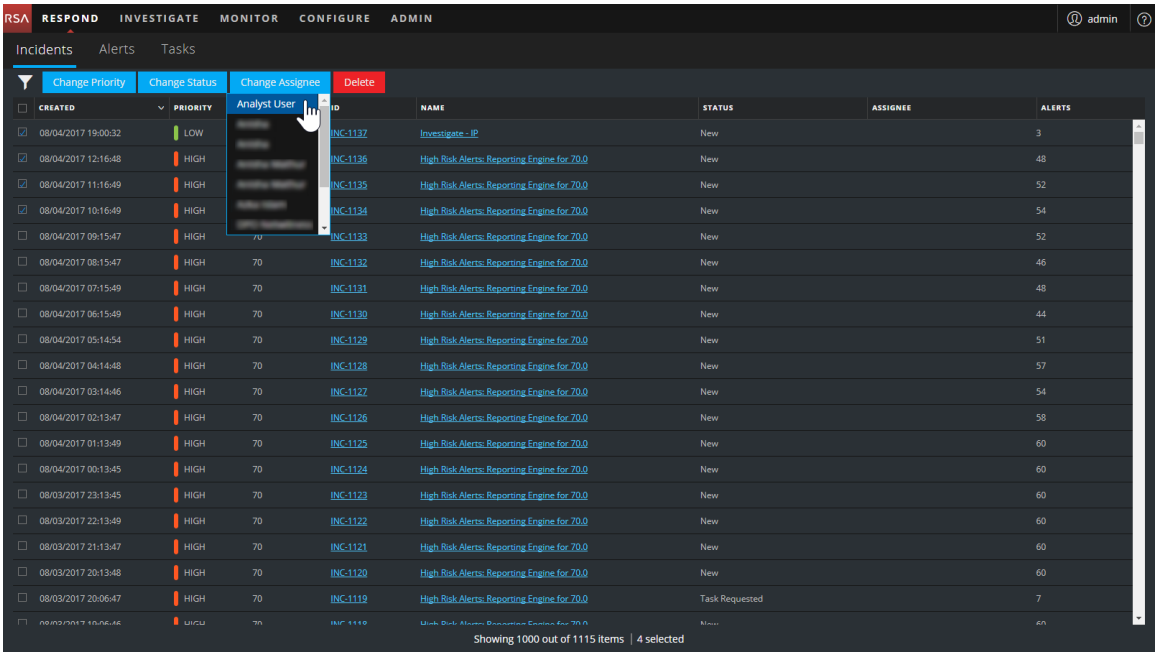
   

   Die Liste der Incidents wird so gefiltert, dass nur noch nicht zugewiesenen Incidents angezeigt werden.

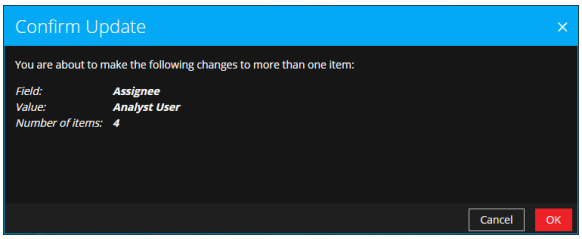
Zuweisen von Incidents an sich selbst

1. Wählen Sie in der Ansicht „Incident-Liste“ einen oder mehrere Incidents aus, die Sie sich selbst zuweisen möchten.

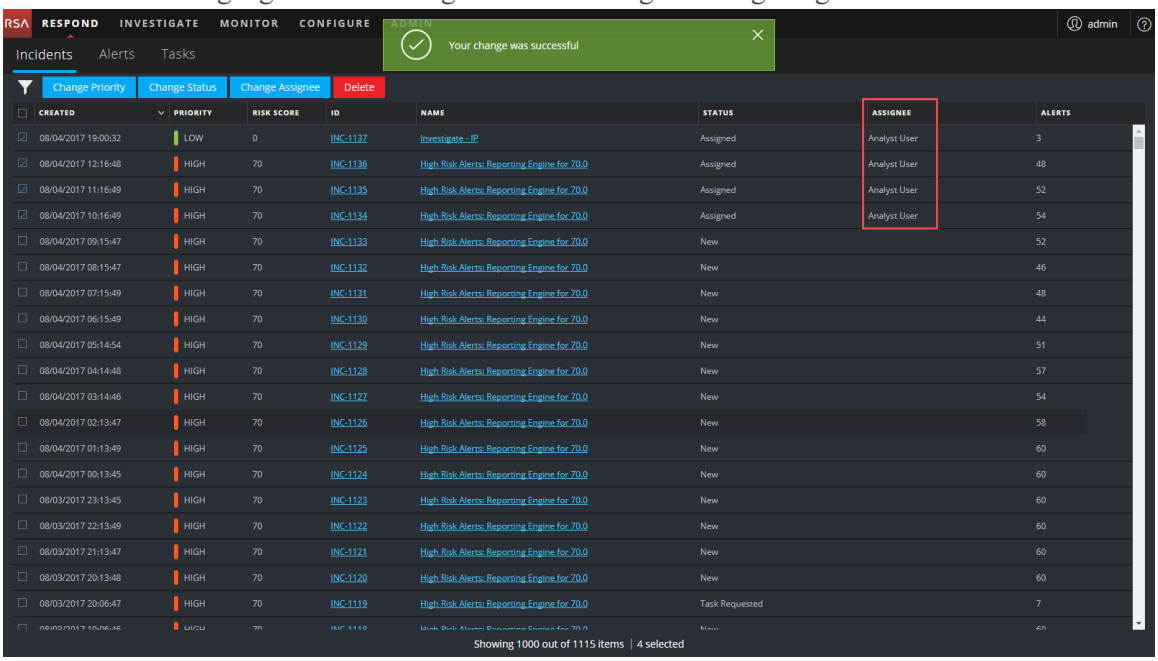
2. Klicken Sie auf **Zuweisungsempfänger ändern** und wählen Sie in der Drop-down-Liste Ihren Benutzernamen aus.



3. Bei Auswahl von mehr als einem Incident klicken Sie im Dialogfeld „Aktualisierung bestätigen“ auf **OK**.

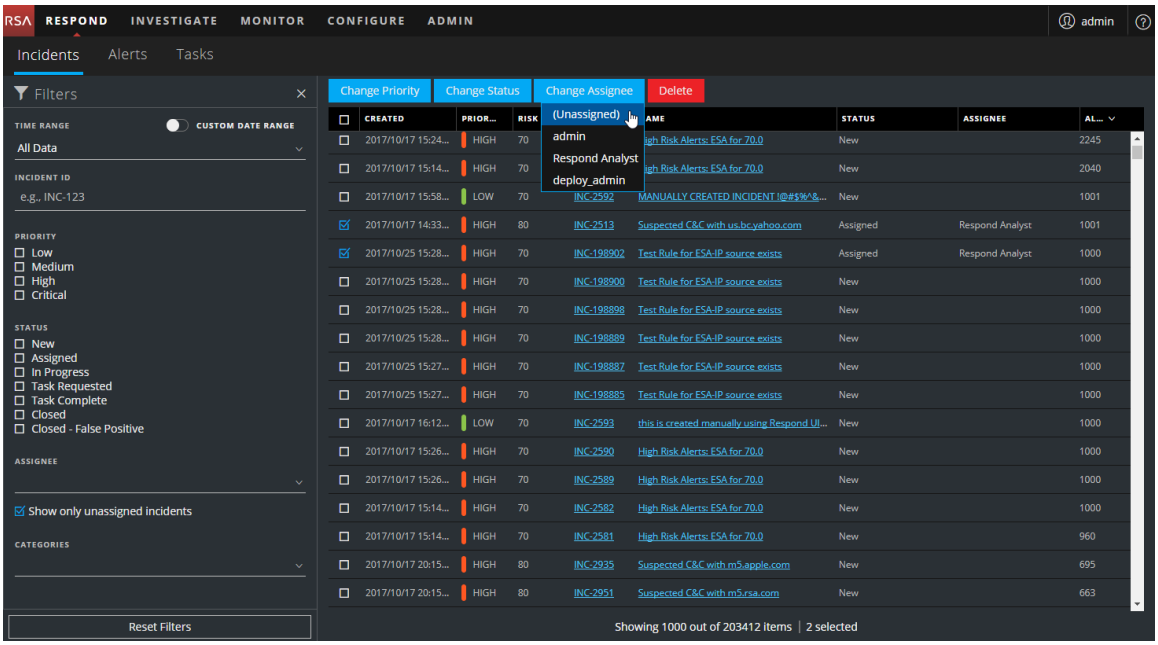


Eine Benachrichtigung über die erfolgreiche Änderung wird angezeigt.

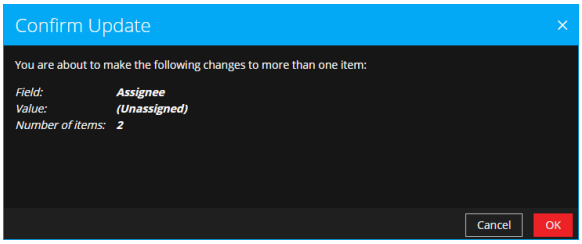


Aufheben der Zuweisung eines Incidents

1. Wählen Sie in der Ansicht „Incident-Liste“ einen oder mehrere Incidents aus, für die Sie die Zuweisung aufheben möchten.
2. Klicken Sie auf **Zuweisungsempfänger ändern** und wählen Sie in der Drop-down-Liste **(Nicht zugewiesen)** aus.



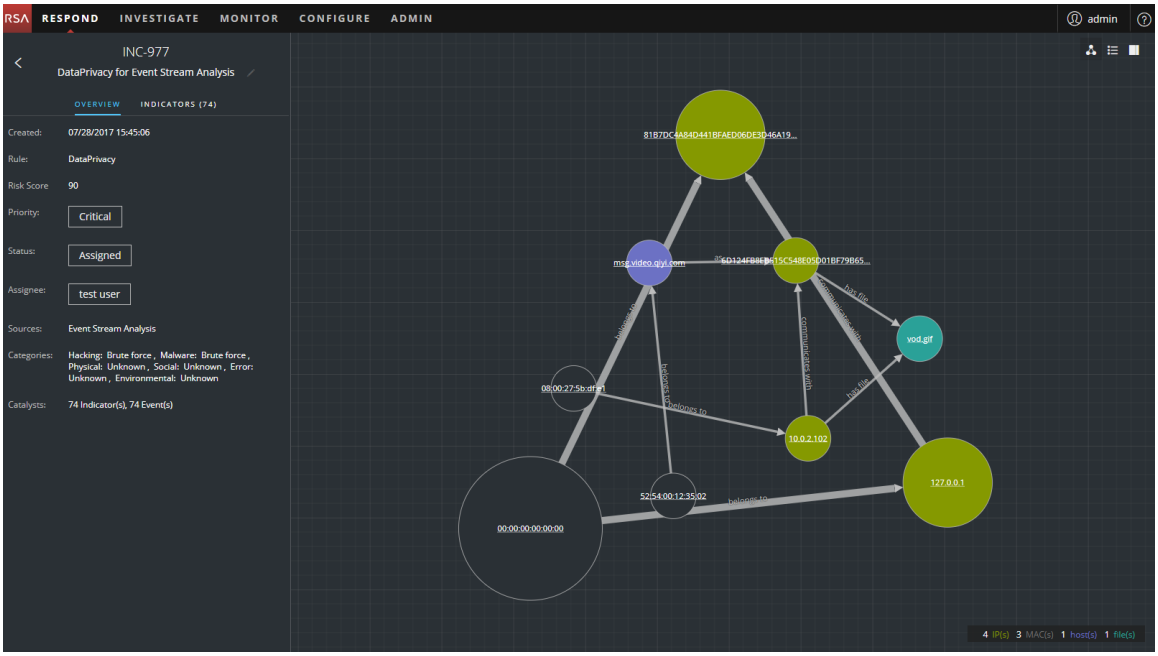
3. Bei Auswahl von mehr als einem Incident klicken Sie im Dialogfeld „Aktualisierung bestätigen“ auf **OK**.



4. Überprüfen Sie, ob der Status weiterhin korrekt ist, und nehmen Sie die erforderlichen Änderungen vor. Um den Status zu ändern, wählen Sie einen oder mehrere Incidents aus, klicken Sie auf **Status ändern** und wählen Sie einen neuen Status aus.
   Wenn Sie einen Incident beispielsweise versehentlich sich selbst zugewiesen haben, können Sie die Zuweisung des Incident aufheben und den Status von „Zugewiesen“ wieder zu „Neu“ ändern.

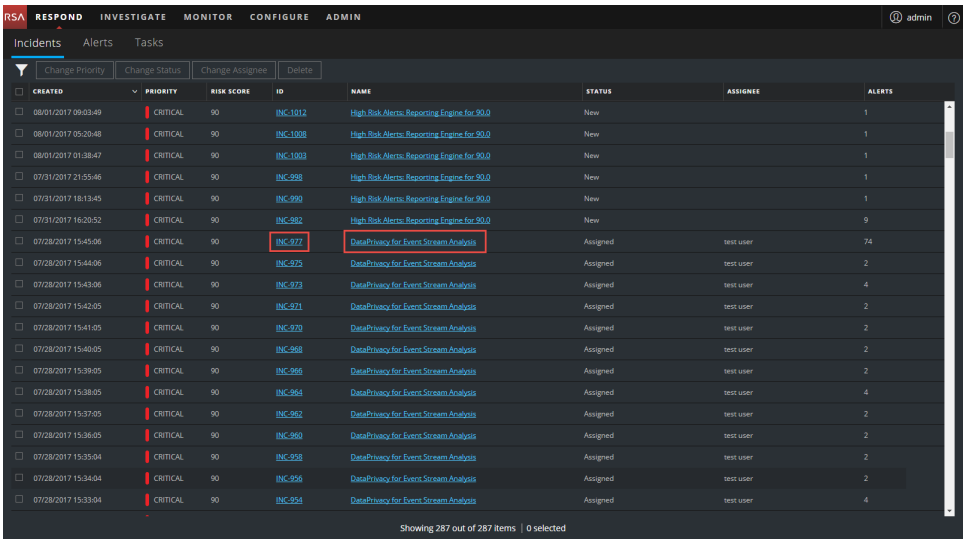
Ermitteln, welche Incidents eine Aktion erfordern

Sobald Sie die allgemeinen Informationen über den Incident aus der Ansicht „Incident-Liste“ erhalten haben, können Sie in die Ansicht „Incident-Details“ wechseln, um weitere Informationen zur Bestimmung der erforderlichen Aktion zu erhalten.

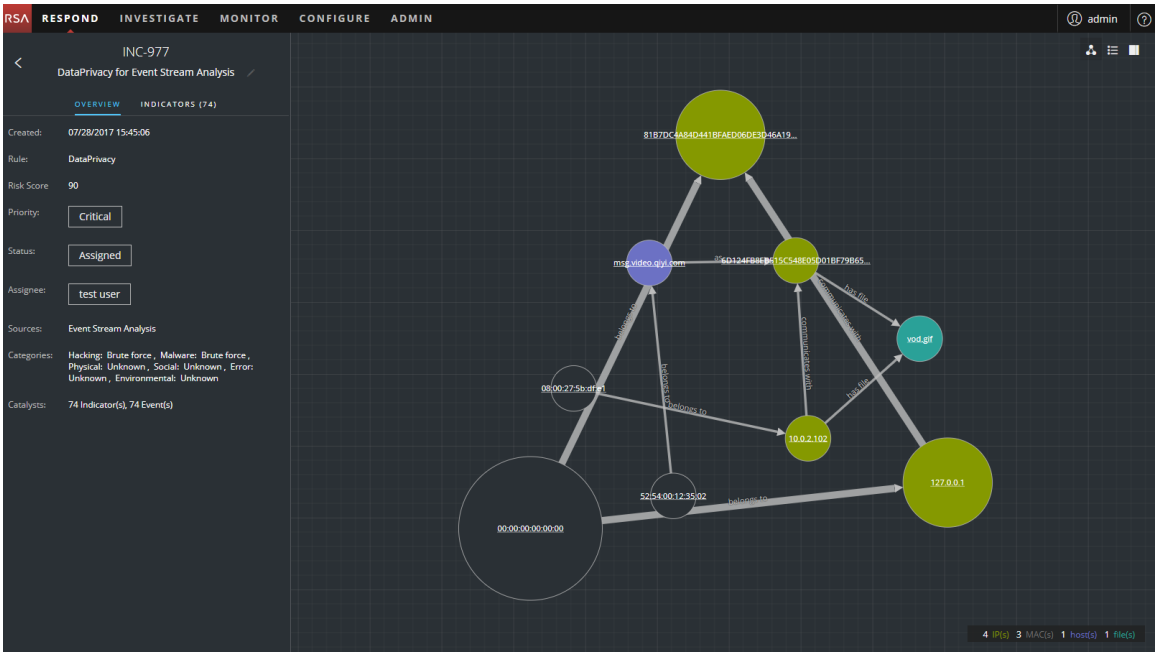


Anzeigen von Details des Incident

Um Details für einen Incident anzuzeigen, wählen Sie in der Incident-Listenansicht einen Incident zur Ansicht aus und klicken Sie dann auf den Link in der Spalte „ID“ oder „Name“ für diesen Incident.



Die Ansicht „Incident-Details“ für den ausgewählten Incident wird mit dem Bereich „Überblick“ und dem Node-Diagramm angezeigt.

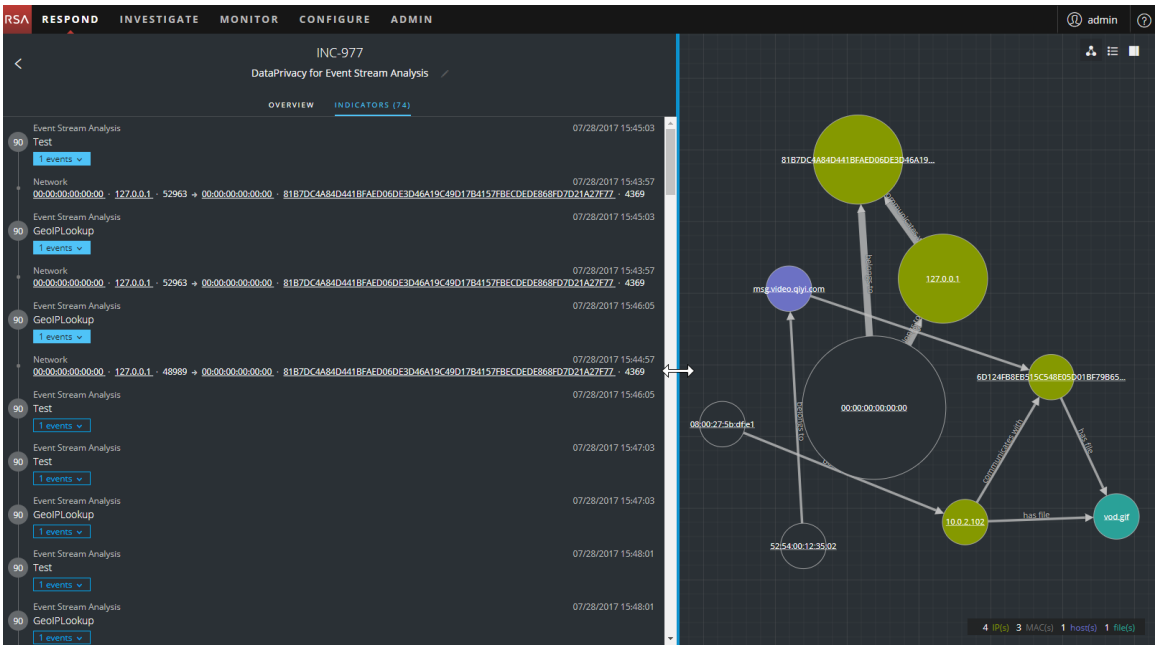


Die Ansicht „Incident-Details“ umfasst folgende Bereiche:

- **ÜBERSICHT**: Das Übersichtsfenster für den Incident enthält zusammengefasste allgemeine Informationen zu dem Incident, wie die Bewertung, die Priorität, Warnmeldungen und Status. Sie haben die Möglichkeit, Priorität, Status und Zuweisungsempfänger für den Incident zu ändern.

- **INDIKATOREN**: Der Bereich „Indikatoren“ enthält eine chronologische Liste der Indikatoren. ***Indikatoren*** sind Warnmeldungen, z. B. eine ESA-Warnmeldung oder eine NetWitness Endpoint-Warnmeldung. Diese Liste hilft Ihnen, Indikatoren und wichtige Daten zueinander in Beziehung zu setzen. Beispiel: Eine mit einem Befehl und einer Kommunikations-ESA-Warnmeldung verbundene IP-Adresse kann auch eine NetWitness Endpoint-Warnmeldung oder andere verdächtige Aktivitäten ausgelöst haben.
- **Node-Diagramm**: Das Node-Diagramm ist eine interaktive Grafik, die die Beziehung zwischen den am Incident beteiligten Entitäten anzeigt. Eine *Entität* ist ein angegebener Teil Metadaten, z. B. IP-Adresse, MAC-Adresse, Benutzer, Host, Domain, Dateinamen oder Datei-Hash.
- **Ereignisse**: Im Bereich „Ereignisse“, auch bekannt als Tabelle „Ereignisse“, werden die mit dem Incident verbundenen Events aufgeführt. Dort werden auch die Quell- und Zielinformationen für das Ereignis sowie zusätzliche Informationen je nach Ereignistyp angezeigt. Sie können auf ein Ereignis in der Liste klicken, um die detaillierten Daten für dieses Ereignis anzuzeigen.
- **JOURNAL**: Im Bereich „Journal“ können Sie auf das Journal für den ausgewählten Incident zugreifen, sodass Sie mit anderen Analysten kommunizieren und zusammenarbeiten können. Sie können Hinweise in einem Journal veröffentlichen, Ermittlungsmeilensteintags (Aufklärung, Bereitstellung, Ausnutzung, Installation, Befehl und Kontrolle) hinzufügen und den Verlauf der Aktivität für den Incident anzeigen.
- **AUFGABEN**: Im Bereich „Aufgaben“ werden alle Aufgaben angezeigt, die für den Incident erstellt wurden. Sie können von hier aus auch zusätzliche Aufgaben erstellen.
- **VERWANDT**: Der Bereich „Verwandte Indikatoren“ ermöglicht es Ihnen, die NetWitness Suite-Warnmeldungsdatenbank zu durchsuchen, um Warnmeldungen zu finden, die mit diesem Incident in Verbindung stehen. Sie können auch verwandte Warnmeldungen, die Sie finden, zum Incident hinzufügen.

Um weitere Informationen im linken Bereich anzuzeigen, ohne einen Bildlauf durchzuführen, können Sie den Mauszeiger über den rechten Rand bewegen und die Linie ziehen, um die Größe des Bereichs wie in der folgenden Abbildung dargestellt zu ändern:

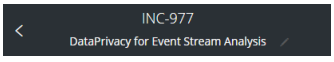


Anzeigen grundlegender zusammenfassender Informationen zum Incident

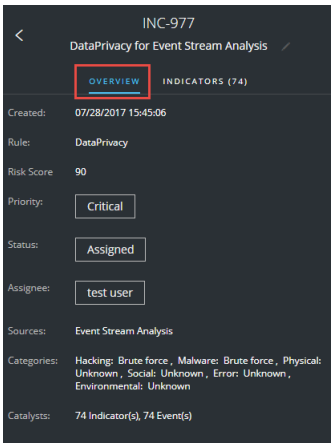
Sie können grundlegende zusammenfassende Informationen über einen Incident im Bereich „Übersicht“ anzeigen.

Über dem Bereich „Übersicht“ werden die folgenden Informationen angezeigt:

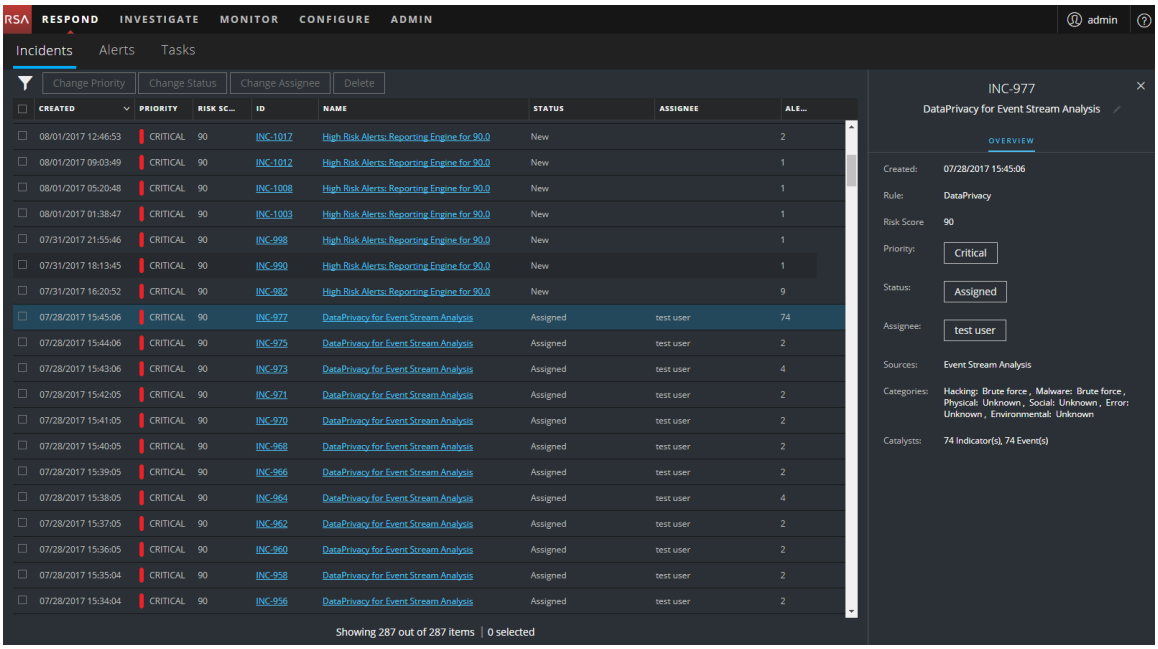
- **Incident-ID**: Dies ist eine automatisch erstellte eindeutige ID, die dem Incident zugewiesen wird.
- **Name**: Der Incident-Name leitet sich aus der Regel ab, die den Incident ausgelöst hat.



Um den Bereich „Übersicht“ über die Ansicht „Details für Incident“ anzuzeigen, wählen Sie im linken Bereich **ÜBERSICHT**.



Um den Bereich „Übersicht“ von der Liste der Incidents aus anzuzeigen, klicken Sie auf einen Incident in der Liste. Das Übersichtsfenster wird auf der rechten Seite angezeigt.



Die Übersicht enthält grundlegende zusammenfassende Informationen über den ausgewählten Incident:

- **Erstellt**: Zeigt Datum und Uhrzeit der Erstellung des Incident an.
- **Regel/Von**: Zeigt den Namen der Regel, die den Incident erstellt hat, oder den Namen der Person, die den Incident erstellt hat.
- **Risikowert**: Gibt das Risiko des Incidents an, das über einen Algorithmus berechnet wird und zwischen 0 und 100 liegt. 100 ist der höchste Risikowert.

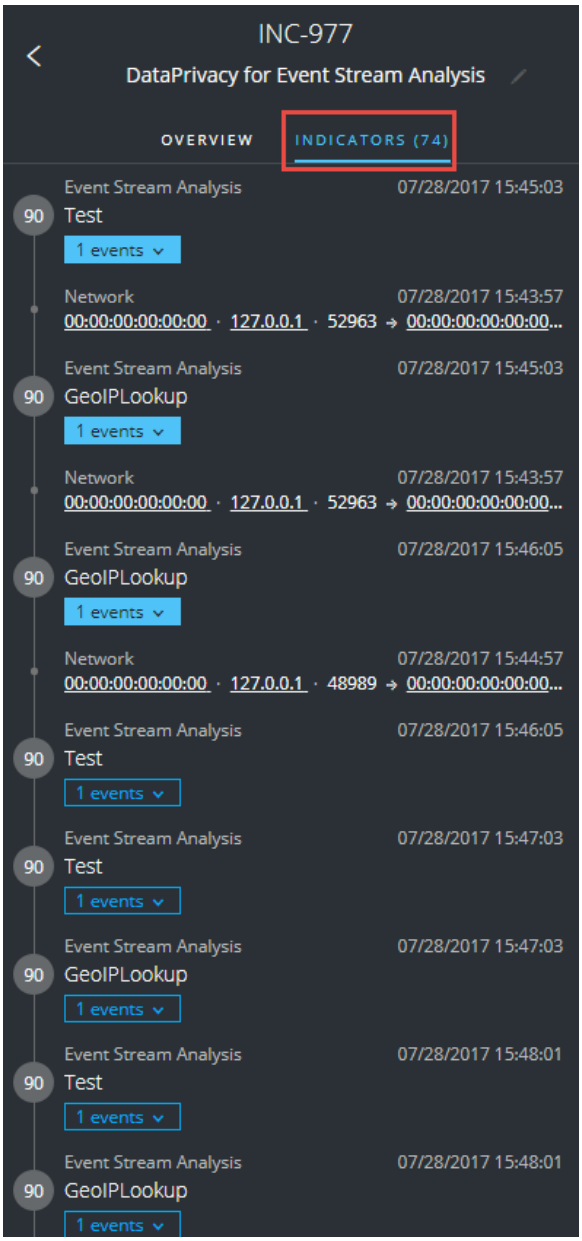
- **Priorität**: Zeigt die Incident-Priorität. Die Priorität kann „Kritisch“, „Hoch“, „Mittel“ oder „Niedrig“ sein.
- **Status**: Zeigt den Incident-Status. Der Status kann „Neu“, „Zugewiesen“, „Läuft“, „Aufgabe angefordert“, „Aufgabe abgeschlossen“, „Geschlossen“ und „Geschlossen – falsch positives Ergebnis“ lauten. Nachdem Sie eine Aufgabe erstellt haben, ändert sich der Status auf „Aufgabe angefordert“.
- **Zuweisungsempfänger**: Zeigt das Teammitglied, das derzeit dem Incident zugewiesen ist.
- **Quellen:** Gibt die Datenquellen an, die verwendet werden, um die verdächtige Aktivität zu suchen.
- **Kategorien**: Zeigt die Kategorien der Incident-Ereignisse.
- **Katalysatoren**: Zeigt die Anzahl der Indikatoren, die zu dem Incident geführt haben.

Anzeigen der Indikatoren und Erweiterungen

Hinweis: *Indikatoren* sind Warnmeldungen, z. B. eine ESA-Warnmeldung oder eine NetWitness Endpoint-Warnmeldung.

Indikatoren, Ereignisse und Erweiterungen finden Sie im Bereich „Indikatoren“. Der Bereich „Indikatoren“ ist eine chronologische Liste der Indikatoren, die Ihnen dabei hilft, Erweiterungen und Ereignisse im Zusammenhang mit dem auslösenden Indikator zu finden. Zum Beispiel kann ein Indikator eine Command-and-Control-Warnmeldung (C2), eine NetWitness Endpoint-Warnmeldung, eine Warnmeldung über eine verdächtige Domain oder eine Warnmeldung aus einer Regel für Event Stream Analysis (ESA) sein. Im Bereich „Indikatoren“ können Sie diese Indikatoren (Warnmeldungen) aus verschiedenen Systemen aggregieren und ordnen, damit Sie sehen können, wie sie zueinander in Beziehung stehen, und einen Zeitplan für einen bestimmten Angriff erstellen können.

Klicken Sie zum Öffnen des Bereichs „Indikatoren“ im linken Bereich der Incident-Detailansicht auf **INDIKATOREN**.



Indikatoren sind Warnmeldungen, z. B. ESA-Warnmeldungen oder NetWitness Endpoint-Warnmeldungen. Diese Liste hilft Ihnen, Indikatoren und wichtige Daten zueinander in Beziehung zu setzen. Beispielsweise können Indikatoren die Daten anzeigen, die durch Ihre Regeln gefunden wurden. Im Bereich „Indikatoren“ wird der Risikowert für einen Indikator in einem vollfarbigen Kreis angezeigt.

Informationen zur Datenquelle werden unter den Namen der Indikatoren angezeigt. Sie können auch das Datum und die Uhrzeit der Erstellung des Indikators und die Anzahl der Ereignisse im Indikator anzeigen. Wenn Daten verfügbar sind, können Sie die Anzahl der Erweiterungen anzeigen. Durch Klick auf die Schaltflächen „Ereignis“ und „Erweiterung“ können Sie Details anzeigen.

Anzeigen und Untersuchen der Ereignisse

Sie können die Ereignisse im Zusammenhang mit dem Incident über den Bereich „Ereignisse“ anzeigen und untersuchen. Er zeigt Informationen zu den Ereignissen, z. B. die Uhrzeit des Ereignisses, Quell-IP, Ziel-IP, Detektor-IP, Quellbenutzer, Zielbenutzer und Dateiinformationen zu den Ereignissen. Wie viele Informationen aufgeführt werden, hängt vom Typ des jeweiligen Ereignisses ab.

Es gibt zwei Typen von Ereignissen:

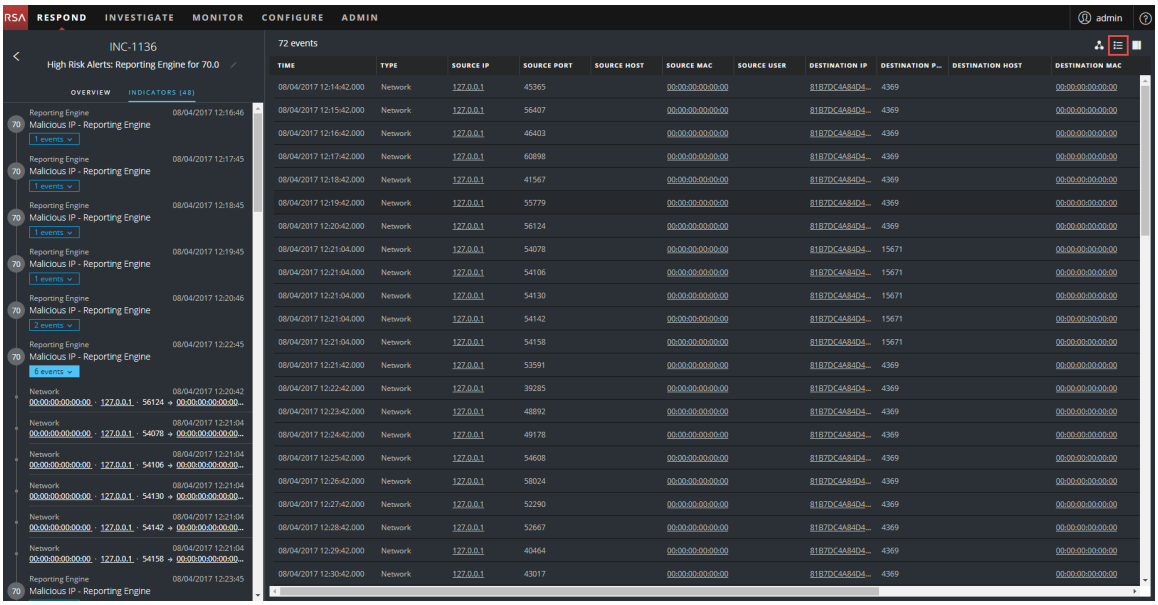
- Eine Transaktion zwischen zwei Rechnern (eine Quelle und ein Ziel)
- Eine auf einem einzelnen Rechner erkannte Anomalie (ein Detektor)

Einige Ereignisse haben nur einen Detektor. Mit NetWitness Endpoint wird z. B. Malware auf dem Rechner gefunden. Andere Ereignisse haben eine Quelle und ein Ziel. Paketdaten zeigen beispielsweise die Kommunikation zwischen Ihrem Rechner und einer Command-and-Control-Domain (C2).

Sie können einen Drill-down in ein Ereignis durchführen, um detaillierte Daten über das Ereignis zu erhalten.

So zeigen Sie Ereignisse an und untersuchen sie:

1. Um den Bereich „Ereignisse“ anzuzeigen, klicken Sie in der Symbolleiste der Ansicht „Incident-Details“ auf .



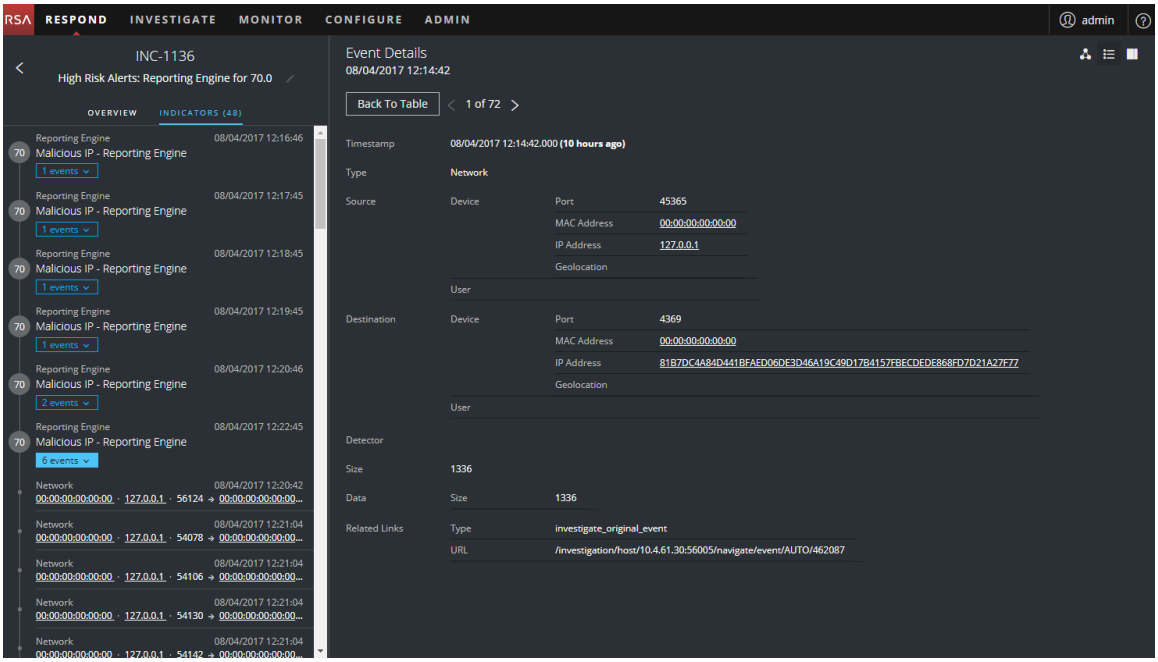
Der Bereich „Ereignisse“ zeigt eine Liste von Informationen zu jedem Ereignis an, wie in der folgenden Tabelle gezeigt wird.

Spalte	Beschreibung
ZEIT	Zeigt an, wann das Ereignis eingetreten ist.
TYP	Zeigt den Typ der Warnmeldung an, z. B. „Protokoll“ oder „Netzwerk“.
QUELL-IP	Zeigt die Quell-IP-Adresse an, wenn eine Transaktion zwischen zwei Computern erfolgt ist.
QUELLPORT	Zeigt den Quellport der Transaktion an. Quellport und Zielport können dieselbe IP-Adresse haben.
QUELLHOST	Zeigt den Quellhost, auf dem das Ereignis stattgefunden hat.
QUELL-MAC	Zeigt die MAC-Adresse des Quellcomputers an.
QUELLBENUTZER	Zeigt den Benutzer des Quellcomputers an.

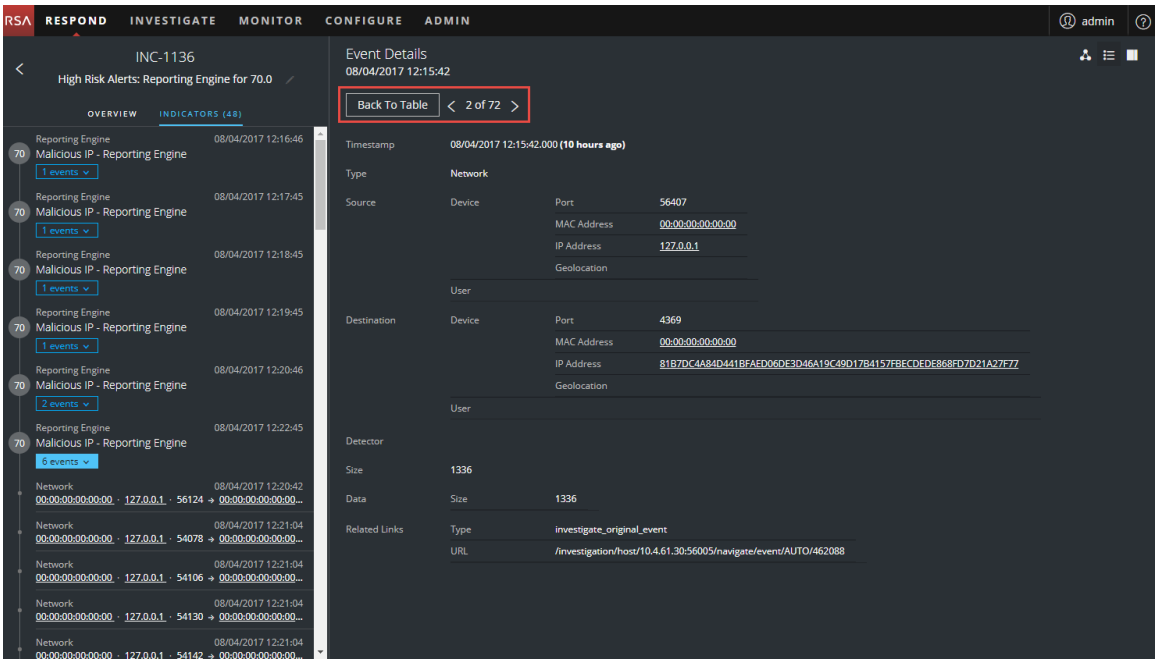
Spalte	Beschreibung
ZIEL-IP	Zeigt die Ziel-IP-Adresse an, wenn eine Transaktion zwischen zwei Computern erfolgt ist.
ZIELPORT	Zeigt den Zielport der Transaktion an. Quellport und Zielport können dieselbe IP-Adresse haben.
ZIELHOST	Zeigt den Zielhost, auf dem das Ereignis stattgefunden hat.
ZIEL-MAC	Zeigt die MAC-Adresse des Zielcomputers an.
ZIELBENUTZER	Zeigt den Benutzer des Zielcomputers an.
DETEKTOR-IP	Zeigt die IP-Adresse des Computers an, auf dem eine Anomalie erkannt wurde.
DATEINAME	Zeigt den Dateinamen an, falls eine Datei in das Ereignis involviert ist.
DATEI-HASH	Zeigt einen Hash der Dateiinhalte an.

Wenn nur ein Ereignis in der Liste vorhanden ist, werden die Ereignisdetails für das betreffende Ereignis anstelle einer Liste angezeigt.

2. Klicken Sie auf ein Ereignis in der Ereignisliste, um die Ereignisdetails anzuzeigen.
   Dieses Beispiel zeigt die Ereignisdetails für das erste Ereignis in der Liste.



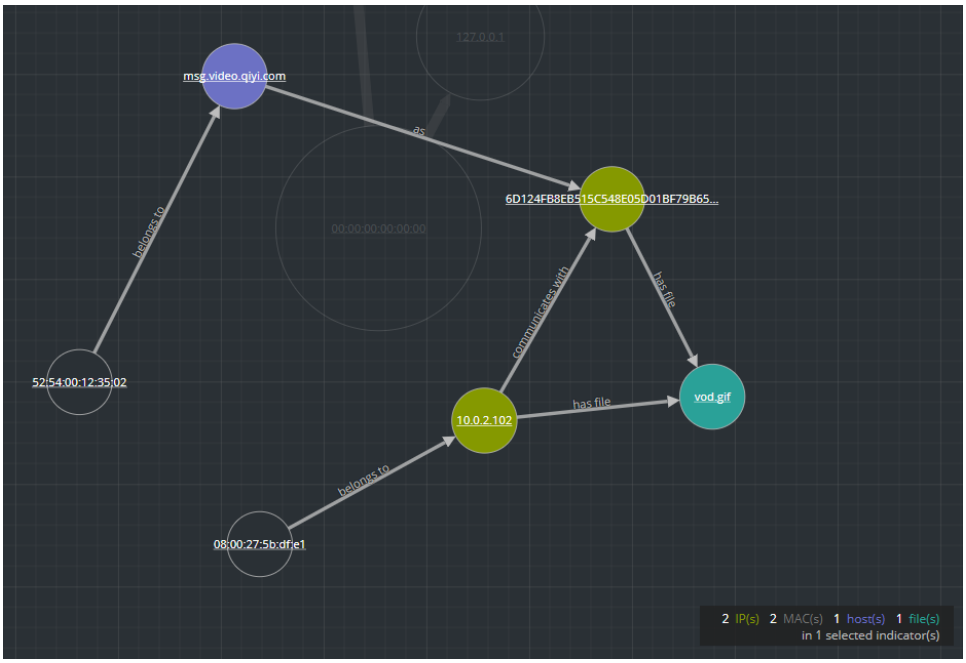
3. Verwenden Sie die Ereignisdetails-Navigation, um Details für zusätzliche Ereignisse anzuzeigen.
   Dieses Beispiel zeigt das zweite Ereignis in der Liste.



Anzeigen und Untersuchen der an den Ereignissen beteiligten Entitäten

Eine *Entität* ist eine IP-Adresse, eine MAC-Adresse, ein Benutzer, ein Host, eine Domain, ein Dateinamen oder ein Datei-Hash. Das Node-Diagramm ist eine interaktive Grafik, die Sie verschieben können, um ein besseres Verständnis davon zu erhalten, wie die an den Ereignissen beteiligten Entitäten miteinander in Bezug stehen. Die Node-Diagramme sehen unterschiedlich aus, je nach Typ des Ereignisses, der Anzahl der beteiligten Rechner und in Abhängigkeit davon, ob die Rechner Benutzern zugeordnet sind und ob Dateien mit dem Ereignis verknüpft sind.

Die folgende Abbildung zeigt ein beispielhaftes Node-Diagramm mit sechs Nodes.



Wenn Sie sich das Node-Diagramm genau ansehen, sehen Sie Kreise, die Nodes darstellen. Ein Node-Diagramm kann einen oder mehrere der folgenden Typen von Nodes enthalten:

- **IP-Adresse** (Wenn das Ereignis eine erkannte Anomalie ist, wird eine Detektor-IP angezeigt. Wenn das Ereignis eine Transaktion ist, wird eine Ziel-IP und eine Quell-IP angezeigt.)
- **MAC-Adresse** (Möglicherweise wird für jede Art von IP-Adresse eine MAC-Adresse angezeigt.)
- **Benutzer** (Wenn der Rechner mit einem Benutzer verknüpft ist, wird ein Benutzer-Node angezeigt.)
- **Host**
- **Domain**
- **Dateiname** (Wenn das Ereignis Dateien betrifft, wird ein Dateiname angezeigt.)
- **Datei-Hash** (Wenn das Ereignis Dateien betrifft, wird möglicherweise ein Datei-Hash angezeigt.)

Die Legende im unteren Bereich des Node-Diagramms zeigt die Anzahl der Nodes für jeden Typ und die Farbcodierung der Nodes.

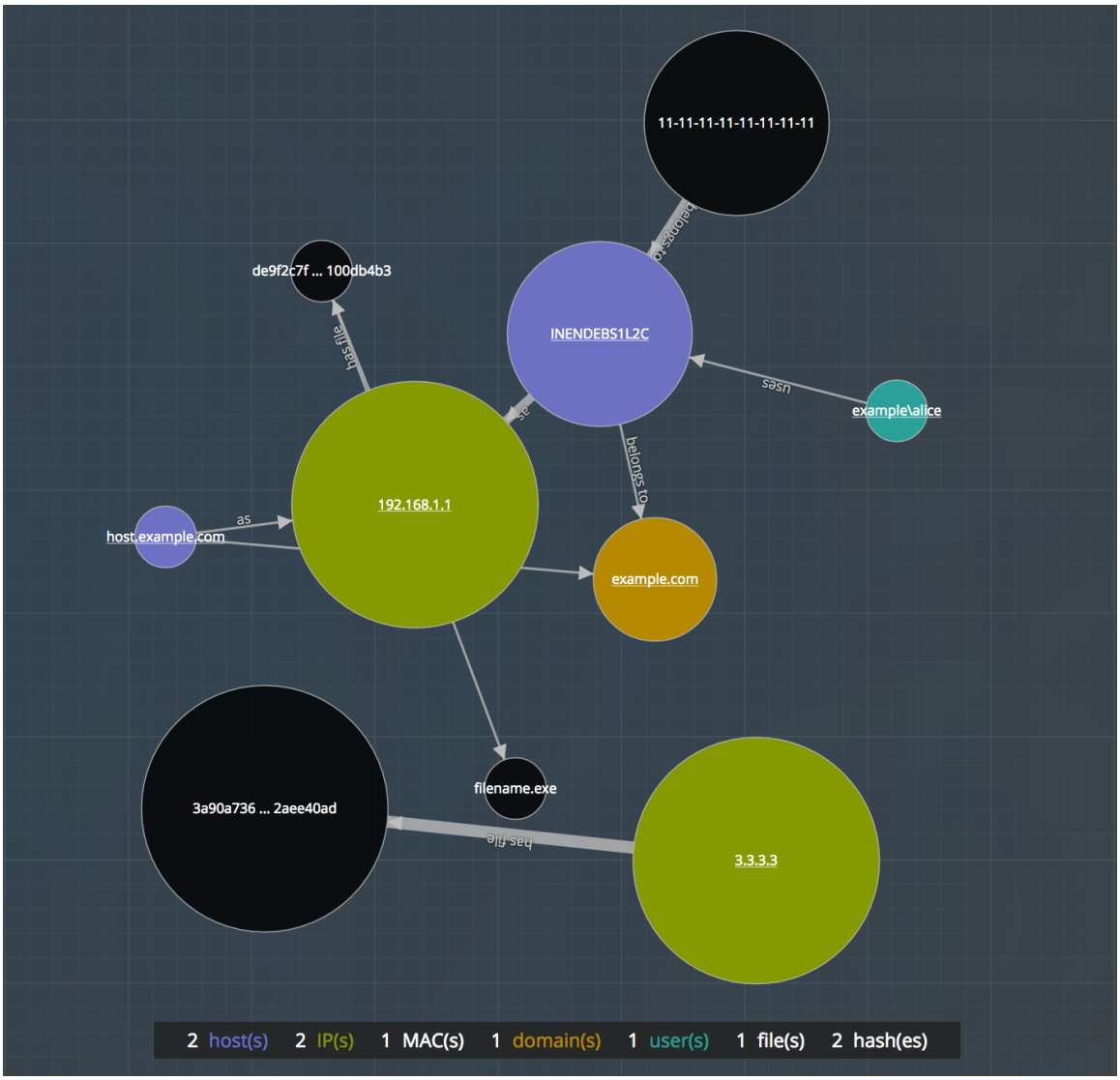
Sie können auf einen beliebigen Node klicken und ihn wie gewünscht ziehen.

Die Pfeile zwischen den Nodes bieten zusätzliche Informationen über die Beziehungen der Entitäten:

- **Kommuniziert mit**: Ein Pfeil zwischen einem Quellrechner-Node (IP-Adresse oder MAC-Adresse) und einem Zielrechner-Node mit der Beschriftung „Kommuniziert mit“ zeigt die Richtung der Kommunikation.
- **Als**: Ein Pfeil zwischen Nodes mit der Beschriftung „Als“ bietet zusätzliche Informationen über die IP-Adresse, auf die der Pfeil zeigt. Im obigen Beispiel gibt es einen Pfeil aus dem Host-Node-Kreis, der auf einen Node mit einer gehashten IP-Adresse zeigt und mit „Als“ beschriftet ist. Dies weist darauf hin, dass der Name auf dem Host-Node-Kreis der Hostname dieser IP-Adresse ist und keine andere Entität.
- **Hat Datei**: Ein Pfeil zwischen einem Rechner-Node (IP-Adresse, MAC-Adresse oder Host) und einem Datei-Hash-Node mit der Beschriftung „Hat“ gibt an, dass die IP-Adresse diese Datei hat.
- **Verwendet**: Ein Pfeil zwischen einem Benutzer-Node und einem Rechner-Node (IP-Adresse, MAC-Adresse oder Host) mit der Beschriftung „Verwendet“ zeigt den Rechner, den der Benutzer während des Ereignisses verwendet hat.
- **Heißt**: Ein Pfeil von einem Datei-Hash-Node zu einem Dateinamen-Node mit der Beschriftung „Heißt“ gibt an, dass der Datei-Hash einer Datei mit diesem Namen entspricht.
- **Gehört zu**: Ein Pfeil zwischen zwei Nodes mit der Beschriftung „Gehört zu“ gibt an, dass sie zu dem gleichen Node gehören. Zum Beispiel bedeutet ein Pfeil zwischen einer MAC-Adresse und einem Host mit der Beschriftung „Gehört zu“, dass es sich um die MAC-Adresse für den Host handelt.

Pfeile mit stärkerer Linie weisen auf eine stärkere Kommunikation zwischen den Nodes hin. Größere Nodes (Kreise) weisen mehr Aktivität auf als kleinere Nodes. Die größeren Nodes sind die häufigsten Entitäten, die in den Ereignissen erwähnt werden.

Das folgende Beispiel eines Node-Diagramms verfügt über zehn Nodes.

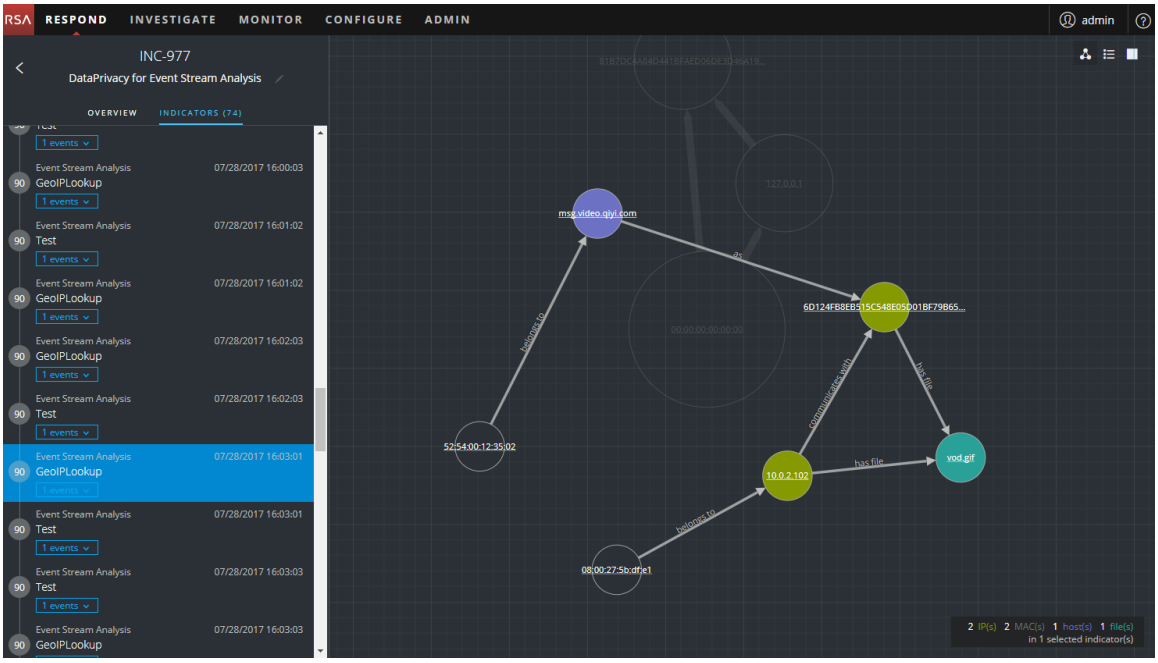


In diesem Beispiel sehen Sie zwei IP-Nodes mit einem hohen Maß an Aktivität. Beide verfügen über Dateien, aber sie kommunizieren nicht miteinander. Die IP-Adresse oben (192.168.1.1) stellt einen Rechner mit zwei Hostnamen (host.example.com und INENDEBS1L2C) in der Domain „example.com“ dar. Die MAC-Adresse des Rechners lautet 11-11-11-11-11-11-11-11-11-11 und Alice verwendet ihn.

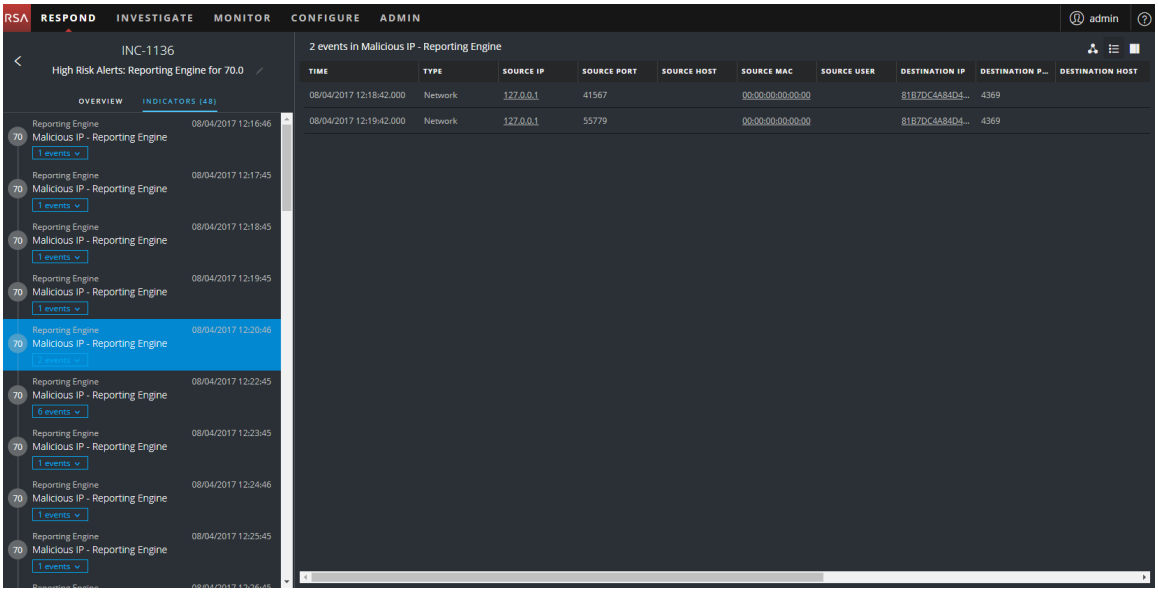
Filtern der Daten in der Ansicht „Incident-Details“

Sie können auf Indikatoren im Bereich „Indikatoren“ klicken, um die Anzeige im Node-Diagramm und in der Ereignisliste zu filtern.

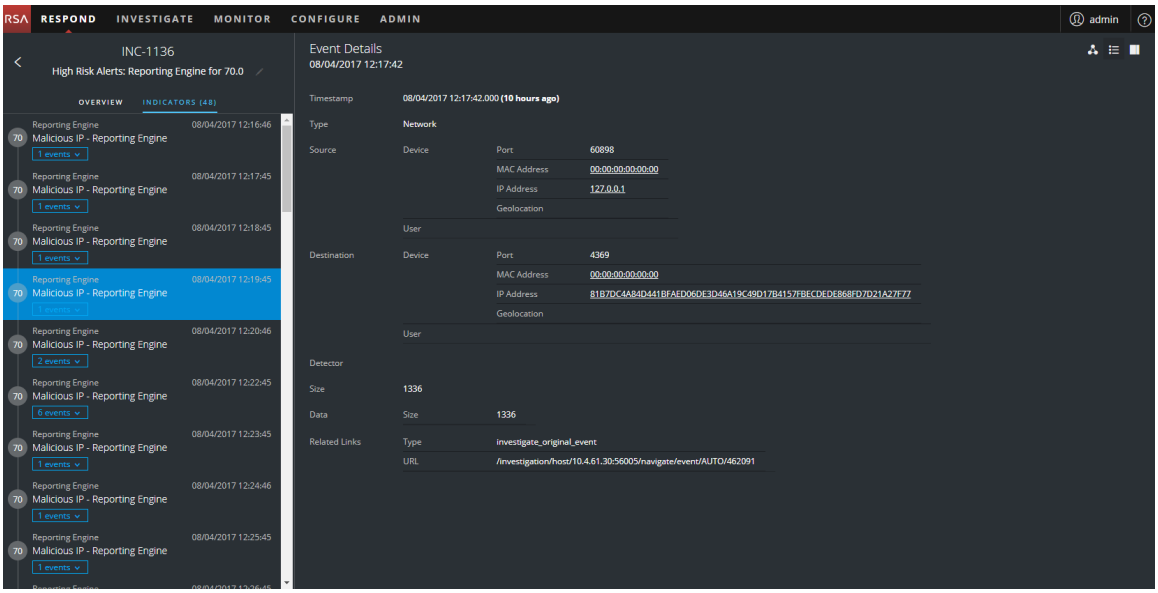
Wenn Sie einen Indikator zum Filtern des Node-Diagramms auswählen, werden Daten, die nicht Bestandteil Ihrer Auswahl sind, abgeblendet. Sie befinden sich aber immer noch in der Ansicht, wie in der folgenden Abbildung gezeigt.



Wenn Sie einen Indikator zum Filtern der Ereignisliste auswählen, werden nur die Ereignisse für diesen Indikator in der Liste angezeigt. Die folgende Abbildung zeigt einen ausgewählten Indikator, der zwei Ereignisse enthält. Die gefilterte Ereignisliste zeigt diese beiden Ereignisse.



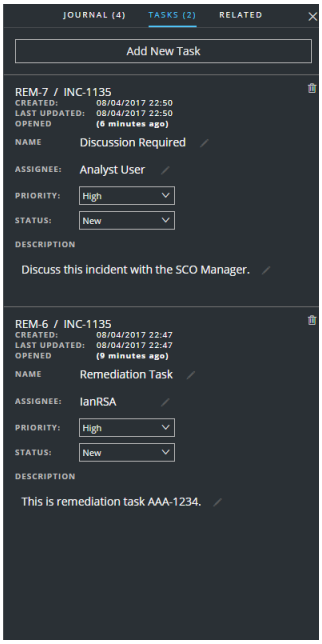
Wenn Sie einen Indikator zum Filtern der Ereignisliste auswählen und es nur ein Ereignis für diesen Indikator gibt, sehen Sie die Ereignisdetails für dieses Ereignis wie in der folgenden Abbildung gezeigt.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
INC-1136
High Risk Alerts: Reporting Engine for 70.0
OVERVIEW
INDICATORS (48)
Reporting Engine
Malicious IP - Reporting Engine
08/04/2017 12:16:46
1 events
08/04/2017 12:17:45
08/04/2017 12:18:45
08/04/2017 12:19:45
08/04/2017 12:20:46
2 events
08/04/2017 12:22:45
6 events
08/04/2017 12:23:45
08/04/2017 12:24:46
08/04/2017 12:25:45
Event Details
08/04/2017 12:17:42
Timestamp
08/04/2017 12:17:42.000 (10 hours ago)
Type
Network
Source
Device
Port
60898
MAC Address
00:00:00:00:00:00
IP Address
127.0.0.1
Geolocation
User
Destination
4369
81B7DC4A84D441BFAED06DE3D46A19C49D17B4157FBECDEDE868FD7D21A27F77
Detector
Size
1336
Data
Related Links
Type
investigate_original_event
URL
/investigation/host/10.4.61.30:56005/navigate/event/AUTO/462091

Anzeigen der Aufgaben im Zusammenhang mit einem Incident

Threat-Experten und andere Analysten können Aufgaben für einen Incident erstellen und diese Aufgaben bis zum Abschluss nachverfolgen. Dies kann sehr hilfreich sein, wenn Sie beispielsweise Aktionen für Incidents von Teams außerhalb Ihrer Sicherheitsabläufe benötigen. Sie können die Aufgaben im Zusammenhang mit einem Incident in der Ansicht „Incident-Details“ anzeigen.

1. Navigieren Sie zu **Reagieren > Incidents** und suchen Sie den Incident, den Sie in der Liste „Incidents“ anzeigen möchten.
2. Klicken Sie auf den Link im Feld **ID** oder **NAME** des Incident, um die Ansicht mit den Incident-Details aufzurufen.
3. Klicken Sie in der Symbolleiste der Ansicht „Incident-Details“ auf ◻.
   Der Bereich „Journal“ wird geöffnet.
4. Klicken Sie auf die Registerkarte **AUFGABEN**.
   Im Bereich „Aufgaben“ werden alle Aufgaben für den Incident angezeigt.

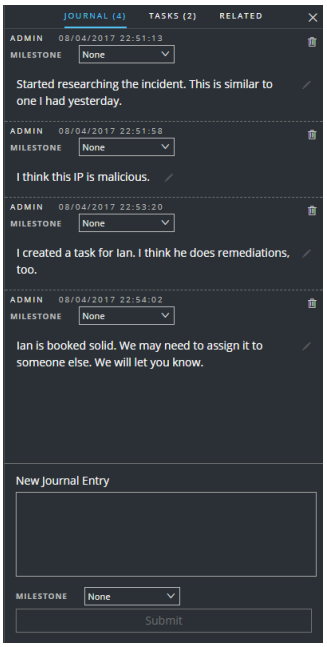


Weitere Informationen zu Aufgaben finden Sie unter Aufgaben-Listenansicht, Anzeigen aller Incident-Aufgaben und Erstellen einer Aufgabe.

Anzeigen von Incident-Anmerkungen

Im Incident-Journal können Sie den Verlauf der Aktivitäten für Ihren Incident anzeigen. Sie können Journaleinträge von anderen Analysten anzeigen und mit ihnen kommunizieren und zusammenarbeiten.

1. Navigieren Sie zu **Reagieren > Incidents** und suchen Sie den Incident, den Sie in der Liste „Incidents“ anzeigen möchten.
2. Klicken Sie auf den Link im Feld **ID** oder **NAME** des Incident, um die Ansicht mit den Incident-Details aufzurufen.
3. Klicken Sie in der Symbolleiste der Ansicht „Incident-Details“ auf ◘.
   Im Bereich „Journal“ werden alle Journaleinträge für den Incident angezeigt.

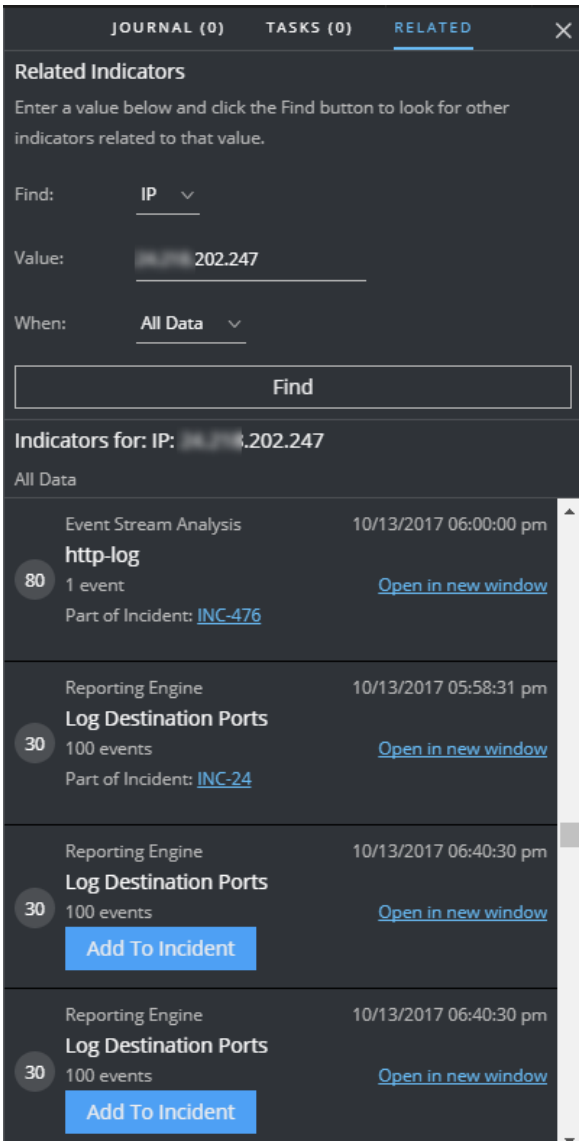


Suchen verwandter Indikatoren

Verwandte Indikatoren sind Warnmeldungen, die ursprünglich nicht Teil des ausgewählten Incident waren, aber irgendwie mit dem Incident verknüpft sind. Die Beziehung kann, muss aber nicht, offensichtlich sein. Beispielsweise können verwandte Indikatoren eine oder mehrere Entitäten aus dem Incident umfassen, aber sie können auch aufgrund von Intelligenz außerhalb von NetWitness Suite verknüpft sein.

Im Bereich „Verwandt“ in der Ansicht „Incident-Details“ können Sie in anderen Warnmeldungen außerhalb des aktuellen Incident nach einer Entität (z. B. IP, MAC, Host, Domain, Benutzer, Dateiname oder Hash) suchen.

1. Navigieren Sie zu **Reagieren > Incidents** und suchen Sie den Incident, den Sie in der Liste „Incidents“ anzeigen möchten.
2. Klicken Sie auf den Link im Feld **ID** oder **NAME** des Incident, um die Ansicht mit den Incident-Details aufzurufen.
3. Klicken Sie in der Symbolleiste der Ansicht „Incident-Details“ auf ◻.
   Der Bereich „Journal“ wird auf der rechten Seite geöffnet.
4. Klicken Sie auf die Registerkarte **VERWANDT**.



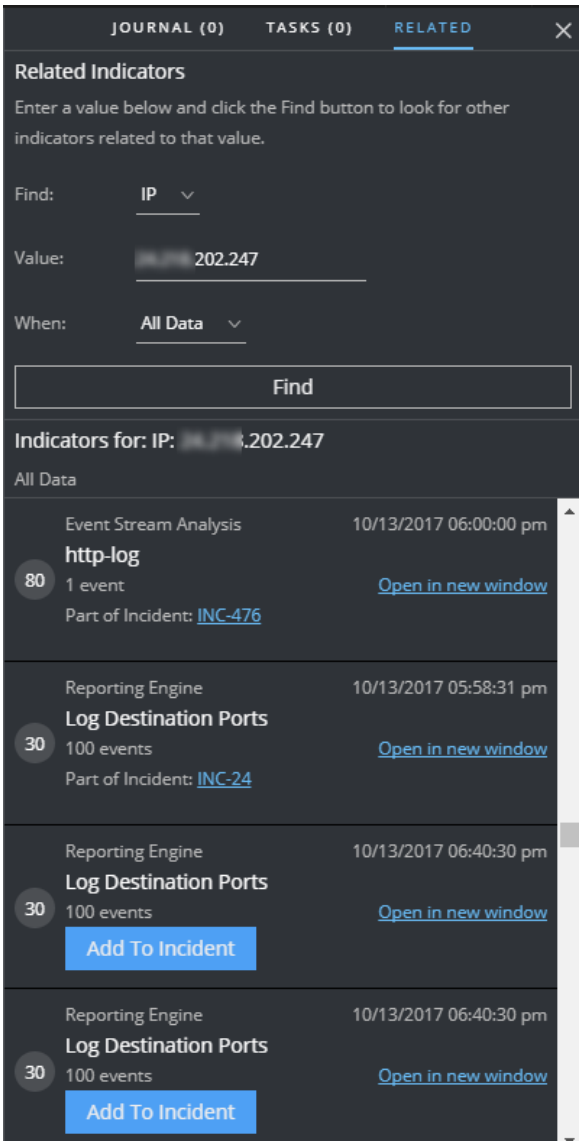
5. Klicken Sie auf **Suchen**.
   Eine Liste der verwandten Indikatoren (Warnmeldungen) wird unter der Schaltfläche **Suchen** im Abschnitt **Indikatoren für** angezeigt. Wenn eine Warnmeldung nicht mit einem anderen Incident verknüpft ist, können Sie den verwandten Indikator (Warnmeldung) durch

Klicken auf die Schaltfläche **Einem Incident hinzufügen** zum aktuellen Incident hinzufügen. Siehe Hinzufügen verwandter Indikatoren zum Incident unten.

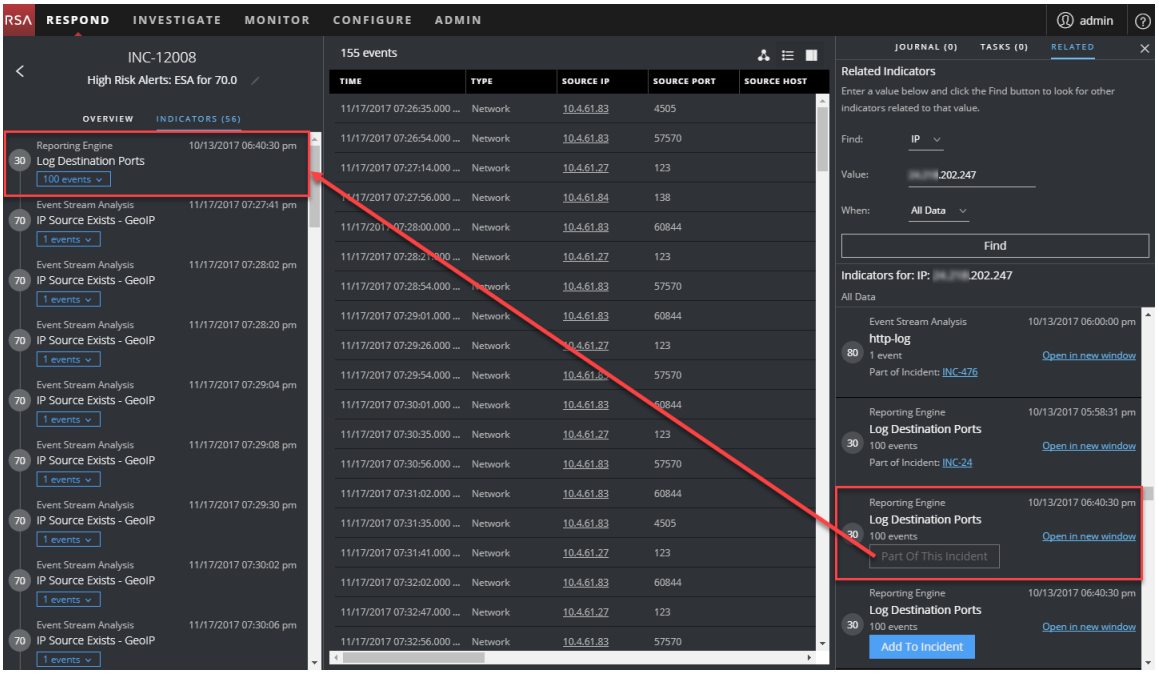
Hinzufügen verwandter Indikatoren zum Incident

Sie können dem aktuellen Incident im Bereich „Verwandte Indikatoren“ verwandte Indikatoren (Warnmeldungen) hinzufügen. Ein Indikator, der bereits mit einem Incident verknüpft ist, kann nicht mit einem anderen Incident verknüpft werden. Wenn eine Warnmeldung nicht bereits mit einem Incident verknüpft ist, wird in den Suchergebnissen eine Schaltfläche **Einem Incident hinzufügen** für sie angezeigt.

1. Führen Sie im Bereich **VERWANDT** (verwandte Indikatoren) eine Suche aus, um verwandte Indikatoren zu suchen. Siehe Suchen verwandter Indikatoren oben.



2. Überprüfen Sie die Warnmeldungen in den Suchergebnissen. Im Bereich **Indikatoren für** (unter der Schaltfläche „Suchen“) werden die verwandten Indikatoren (Warnmeldungen)angezeigt.
3. Um die Details einer Warnmeldung zu prüfen, bevor Sie sie als verwandten Indikator hinzufügen, können Sie auf den Link **In neuem Fenster öffnen** klicken, um die Warnmeldungsdetails für diesen Indikator anzuzeigen.
4. Klicken Sie für jede Warnmeldung, die Sie als verwandten Indikator zum aktuellen Incident hinzufügen möchten, auf die Schaltfläche **Einem Incident hinzufügen**.
   Der ausgewählte verwandte Indikatoren wird dem Bereich „Indikatoren“ auf der linken Seite hinzugefügt. Die Schaltfläche im Bereich „Verwandte Indikatoren“ auf der rechten Seite zeigt jetzt **Zu Incident gehörig**.



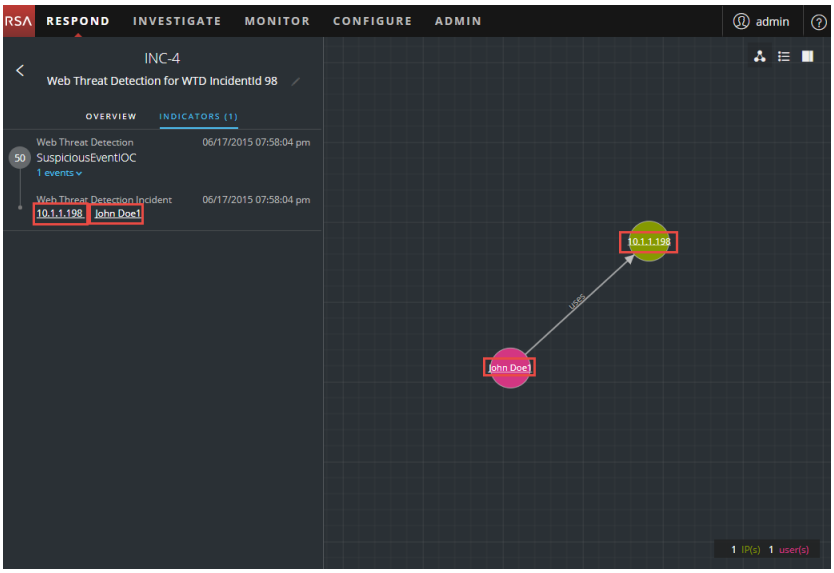
Untersuchen des Incident

Um einen Incident in der Ansicht „Incident-Details“ weiter zu untersuchen, finden Sie Links, über die Sie zu zusätzlichen Kontextinformationen zum Incident gelangen, wenn diese verfügbar sind. Dieser zusätzliche Kontext kann Ihnen zusätzlichen technischen Kontext und Unternehmenskontext zu einer bestimmten Entität im Incident verständlich machen. Sie können auch zusätzliche Informationen erhalten, die Sie untersuchen können, um sicherzustellen, dass Sie den vollen Umfang des Incident verstehen.

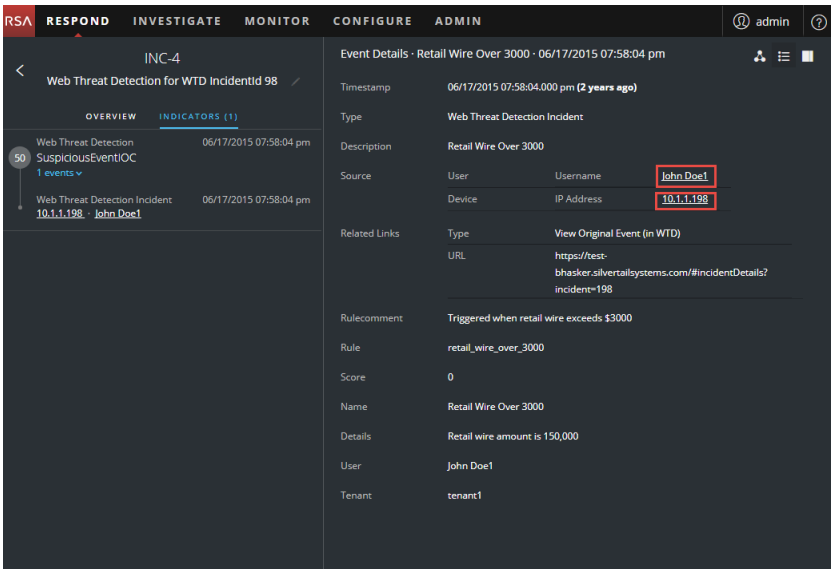
Anzeigen von kontextbezogenen Informationen

In den Bereichen „Indikatoren“, „Ereignisliste“ und „Ereignisdetails“ sowie im Node-Diagramm sehen Sie unterstrichene Entitäten. Wenn eine Entität unterstrichen ist, werden Informationen zu diesem Entitätentyp in Context Hub von NetWitness Suite aufgefüllt. Möglicherweise sind zusätzliche Informationen zu dieser Entität im Context Hub verfügbar.

Die folgende Abbildung zeigt unterstrichene Entitäten im Bereich „Indikatoren“ und im Node-Diagramm.



Die folgende Abbildung zeigt unterstrichene Entitäten im Bereich „Ereignisdetails“.

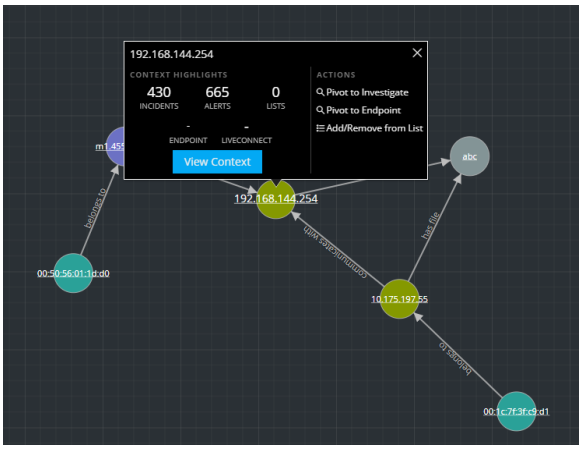


Der Context Hub ist mit Metadatenfeldern vorkonfiguriert, die den Entitäten zugeordnet sind. NetWitness Respond und Investigation nutzen diese Standardzuordnungen für die Kontextabfrage. Informationen zum Hinzufügen von Metaschlüsseln finden Sie unter „Konfigurieren von Einstellungen für eine Datenquelle“ im *Context Hub-Konfigurationsleitfaden*.

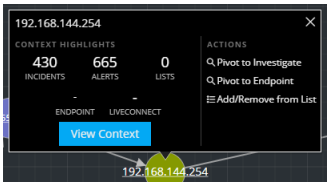
Achtung: Damit die Kontextabfrage in den Ansichten „Reagieren“ und „Untersuchen“ ordnungsgemäß funktioniert, empfiehlt RSA, dass Sie beim Zuordnen von Metaschlüsseln unter **ADMIN > SYSTEM > Ermittlung > Kontextabfrage** den Metaschlüsselzuordnungen nur Metaschlüssel hinzufügen, nicht Felder der MongoDB. Zum Beispiel ist „ip.address“ ein Metaschlüssel und „ip_address“ ist kein Metaschlüssel (es ist ein Feld in der MongoDB).

So zeigen Sie kontextbezogene Informationen an:

1. Bewegen Sie den Mauszeiger in den Bereichen „Indikatoren“, „Ereignisliste“ und „Ereignisdetails“ oder im Node-Diagramm über eine unterstrichene Entität.
   Eine Kontext-Kurzinformation wird mit einer kurzen Übersicht über den Typ der Kontextdaten, die für die ausgewählte Entität verfügbar sind, angezeigt.



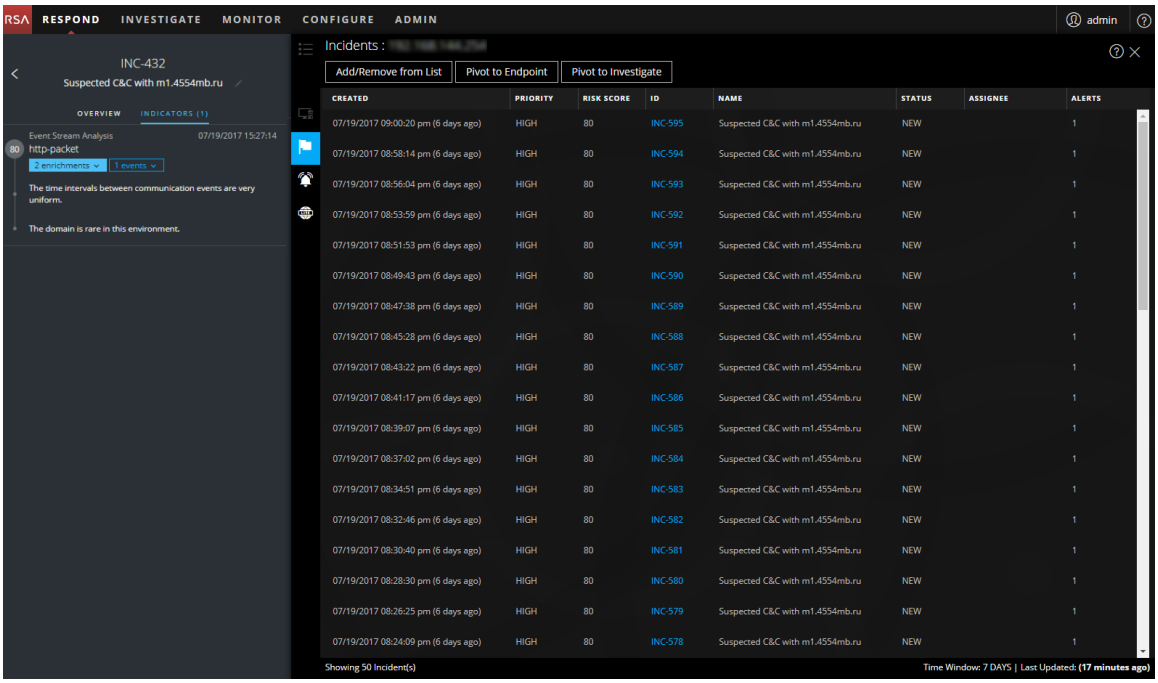
Die Kontext-Kurzinformation besteht aus zwei Abschnitten: Kontexthighlights und -aktionen.



Die Informationen im Abschnitt **Kontexthighlights** helfen Ihnen, die Aktionen zu bestimmen, die Sie durchführen möchten. Es können verwandte Daten für Incidents, Warnmeldungen, Listen, Endpoint und Live Connect angezeigt werden. Abhängig von Ihren Daten können Sie möglicherweise auf diese Elemente klicken, um weitere Informationen anzuzeigen. Das obige Beispiel zeigt 430 verwandte Incidents, 665 Warnmeldungen, 0 Listen und keine Informationen in NetWitness Endpoint oder Live Connect an, die die IP-Adressentität 192.168.144.254 erwähnen.

Im Abschnitt **Aktionen** werden die verfügbaren Aktionen aufgeführt. Im obigen Beispiel sind die Optionen „Zu Ermittlungen wechseln“, „Zu Endpoint wechseln“ und „Zu Liste hinzufügen/Aus Liste entfernen“ verfügbar. Weitere Informationen finden Sie unter Zu Ermittlungen wechseln, Wechseln zum NetWitness Endpoint, und Hinzufügen einer Entität zu einer Whitelist.

2. Um weitere Details über die ausgewählte Entität anzuzeigen, klicken Sie auf die Schaltfläche **Kontext anzeigen**.
   Der Bereich „Kontextabfrage“ wird geöffnet und zeigt alle Informationen im Zusammenhang mit der Entität.
   Das folgende Beispiel zeigt kontextbezogene Informationen für eine ausgewählte Quell-IP-Adresse. Es werden alle Incidents aufgeführt, die die IP-Adresse erwähnen.

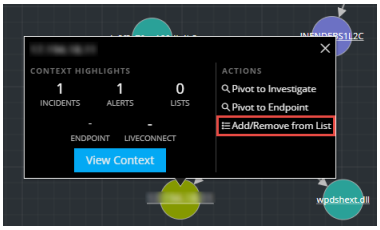


Weitere Informationen zum Verständnis der verschiedenen Ansichten im Bereich „Context Hub-Abfrage“ finden Sie unter Bereich „Kontextabfrage“ – Ansicht „Reagieren“ .

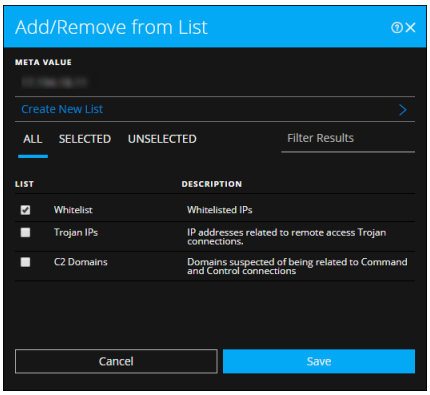
Hinzufügen einer Entität zu einer Whitelist

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

1. Bewegen Sie den Mauszeiger in den Bereichen „Indikatoren“, „Ereignisliste“ und „Ereignisdetails“ oder im Node-Diagramm über die unterstrichene Entität, die Sie einer Context Hub-Liste hinzufügen möchten.
   Eine Kontext-Kurzinformation wird geöffnet und zeigt die verfügbaren Aktionen.



2. Klicken Sie im Abschnitt **AKTIONEN** der Kurzinformation auf **Zu Liste hinzufügen/Aus Liste entfernen**.
   Das Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ zeigt die verfügbaren Listen.



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

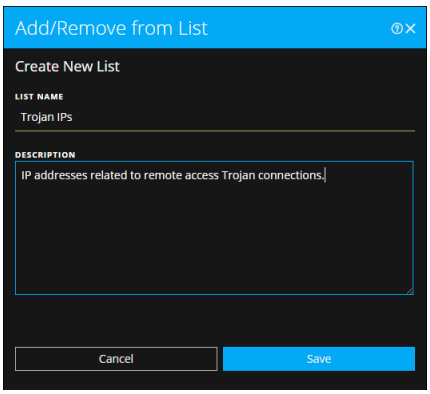
Eine Liste erstellen

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

So erstellen Sie eine Liste in Context Hub:

1. Bewegen Sie den Mauszeiger in den Bereichen „Indikatoren“, „Ereignisliste“ und „Ereignisdetails“ oder im Node-Diagramm über die unterstrichene Entität, die Sie einer Context Hub-Liste hinzufügen möchten.
   Eine Kontext-Kurzinformation wird geöffnet und zeigt die verfügbaren Aktionen.
2. Klicken Sie im Abschnitt **AKTIONEN** der Kurzinformation auf **Zu Liste hinzufügen/Aus Liste entfernen**.

3. Klicken Sie im Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ auf **Neue Liste erstellen**.



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

Wechseln zum NetWitness Endpoint

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

1. Bewegen Sie den Mauszeiger in den Bereichen „Indikatoren“, „Ereignisliste“ und „Ereignisdetails“ oder im Node-Diagramm über eine unterstrichene Entität, um eine Kontext-Kurzinformation aufzurufen.
2. Wählen Sie im Abschnitt **AKTIONEN** der Kurzinformation **Zu Endpoint wechseln**.
   Die NetWitness Endpoint-Thick-Clientanwendung wird außerhalb des Webbrowsers geöffnet.

Weitere Informationen zum Thick-Client finden Sie im *Benutzerhandbuch* für *NetWitness Endpoint*.

Zu Ermittlungen wechseln

Für eine eingehendere Untersuchung des Incident können Sie die Ansicht „Untersuchen“ aufrufen.

1. Bewegen Sie den Mauszeiger in den Bereichen „Indikatoren“, „Ereignisliste“ und „Ereignisdetails“ oder im Node-Diagramm über eine unterstrichene Entität, um eine Kontext-Kurzinformation aufzurufen.
2. Wählen Sie im Abschnitt **AKTIONEN** der Kurzinformation **Zu Ermittlungen wechseln**. Die Ansicht „Untersuchen“ > „Navigation“ wird geöffnet, in der Sie eine umfassendere Untersuchung durchführen können.

Weitere Informationen finden Sie im *NetWitness Investigate – Benutzerhandbuch*.

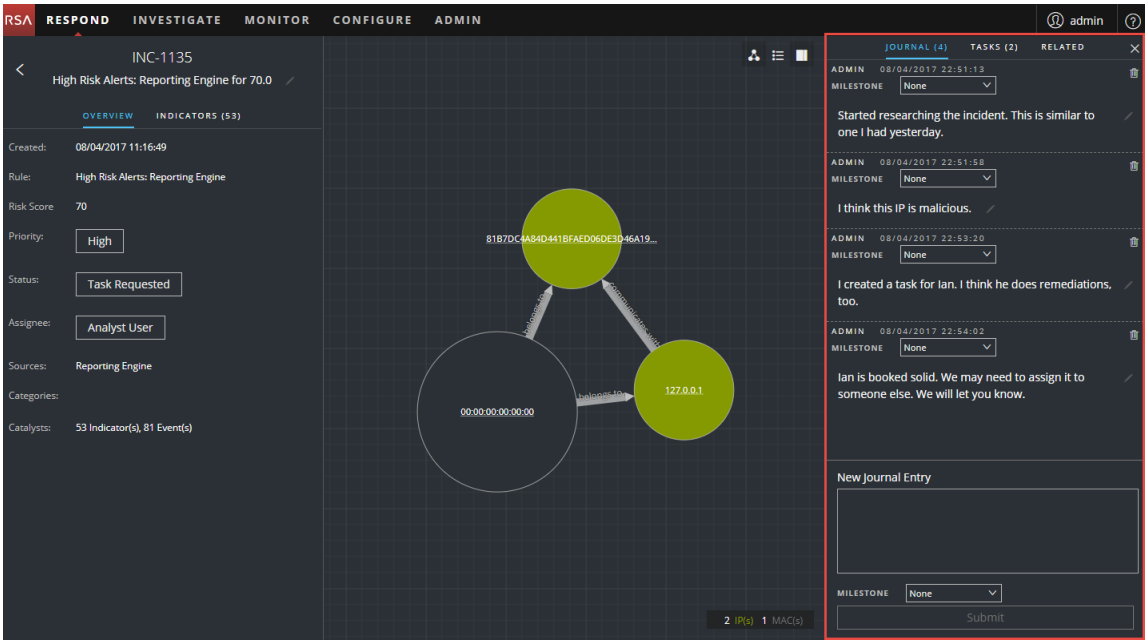
Dokumentmaßnahmen außerhalb von NetWitness

Das Journal zeigt Hinweise, die von Analysten hinzugefügt wurden, und ermöglicht es Ihnen, mit Kollegen zusammenzuarbeiten. Sie können Hinweise in einem Journal veröffentlichen, Ermittlungsmeilensteintags (Aufklärung, Bereitstellung, Ausnutzung, Installation, Befehl und Kontrolle) hinzufügen und den Verlauf der Aktivitäten für den Incident anzeigen.

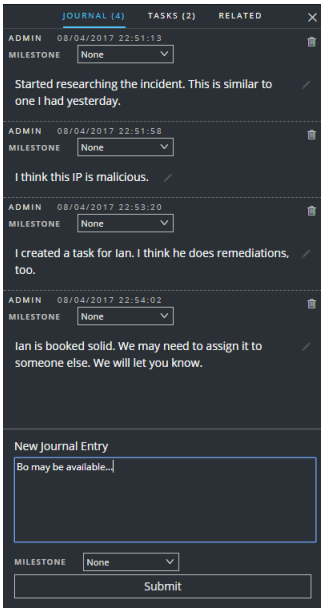
Anzeigen von Journaleinträgen für einen Incident

Klicken Sie in der Symbolleiste der Ansicht „Incident-Details“ auf ■ .

Das Journal wird auf der rechten Seite der Ansicht „Incident-Details“ angezeigt.



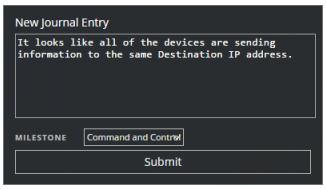
Das Journal zeigt den Verlauf der Aktivitäten für einen Incident. Für jeden Journaleintrag sehen Sie den Autor und die Uhrzeit des Eintrags.



Hinweis hinzufügen

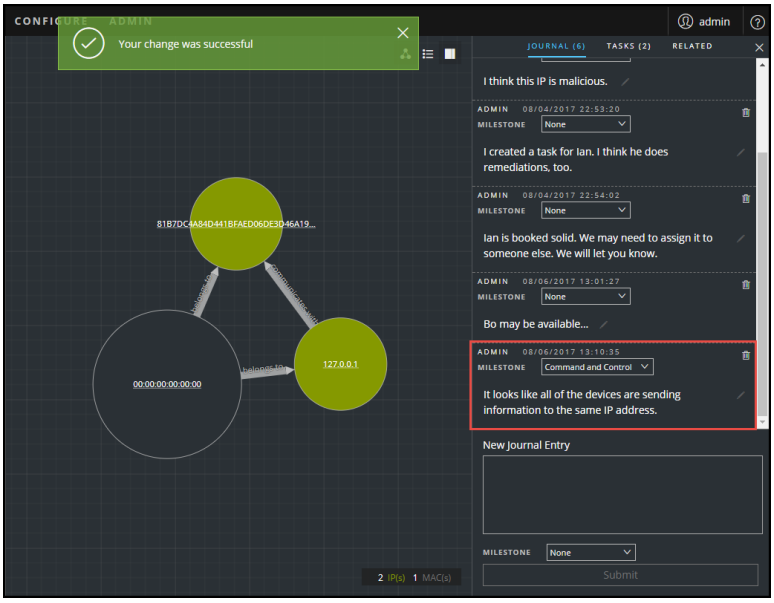
In der Regel werden Sie einen Hinweis hinzufügen wollen, damit ein anderer Analyst den Incident verstehen kann, oder einen Hinweis für die Nachwelt, damit Ihre Ermittlungsschritte dokumentiert werden.

1. Geben Sie unten im Bereich „Journal“ Ihren Hinweis in das Feld **Neuer Journaleintrag** ein.



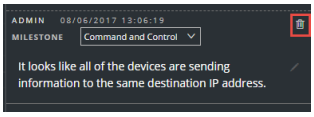
2. (Optional) Wählen Sie einen Ermittlungsmeilenstein aus der Drop-down-Liste (Aufklärung, Bereitstellung, Ausnutzung, Installation, Befehl und Kontrolle, Aktion für Ziel, Eindämmung, Behebung und Abschluss).

3. Nachdem Sie die Notiz abgeschlossen haben, klicken Sie auf **Senden**.
   Ihr neuer Journaleintrag wird im Journal angezeigt.



Löschen eines Hinweises

1. Suchen Sie im Bereich „Journal“ nach dem Journaleintrag, den Sie löschen möchten.
2. Klicken Sie auf das Papierkorb-Symbol (löschen) neben dem Journaleintrag.



3. Klicken Sie im angezeigten Bestätigungsdialogfeld auf **OK**, um zu bestätigen, dass Sie den Journaleintrag löschen möchten. Diese Aktion kann nicht rückgängig gemacht werden.

Eskalieren oder Korrigieren des Incident

Möglicherweise möchten Sie Incidents einem andere Analysten zuweisen oder den Status und die Priorität eines Incident ändern, wenn Sie weitere Informationen über ihn erfassen. Dies ist hilfreich, wenn Sie z. B. die Priorität eines Incident von **Mittel** auf **Hoch** erhöhen, nachdem Sie erkannt haben, dass der Incident eine Sicherheitsverletzung darstellt.

Aktualisieren eines Incident

Sie können einen Incident von verschiedenen Stellen aus aktualisieren. Sie können die Priorität, den Status oder den Zuweisungsempfänger in der Incident-Listenansicht und der Ansicht „Incident-Details“ ändern. Wenn Sie z. B. Analyst sind, möchten Sie sich möglicherweise selbst einen Fall aus der Incident-Listenansicht zuweisen, wenn Sie sehen, dass dieser mit einem anderen Fall verknüpft ist, an dem Sie arbeiten. Wenn Sie ein SOC-Manager oder Administrator sind, möchten Sie möglicherweise nicht zugewiesene Incidents aus der Incident-Listenansicht anzeigen und die Incidents bei Ihrem Eingang zuweisen. SOC-Manager und Administratoren können Massenaktualisierungen an Priorität, Status oder Zuweisungsempfänger vornehmen, anstatt jeweils nur einen Incident zu aktualisieren.

In der Ansicht „Details“ können Sie den Status auf „Läuft“ ändern, sobald Sie beginnen, an einem Incident zu arbeiten, und ihn anschließend nach Behebung des Problems auf „Geschlossen“ oder „Geschlossen – falsch positives Ergebnis“ aktualisieren. Oder Sie können die Priorität des Incident auf „Mittel“ oder „Hoch“ ändern, wenn Sie die Details des Vorgangs bestimmen.

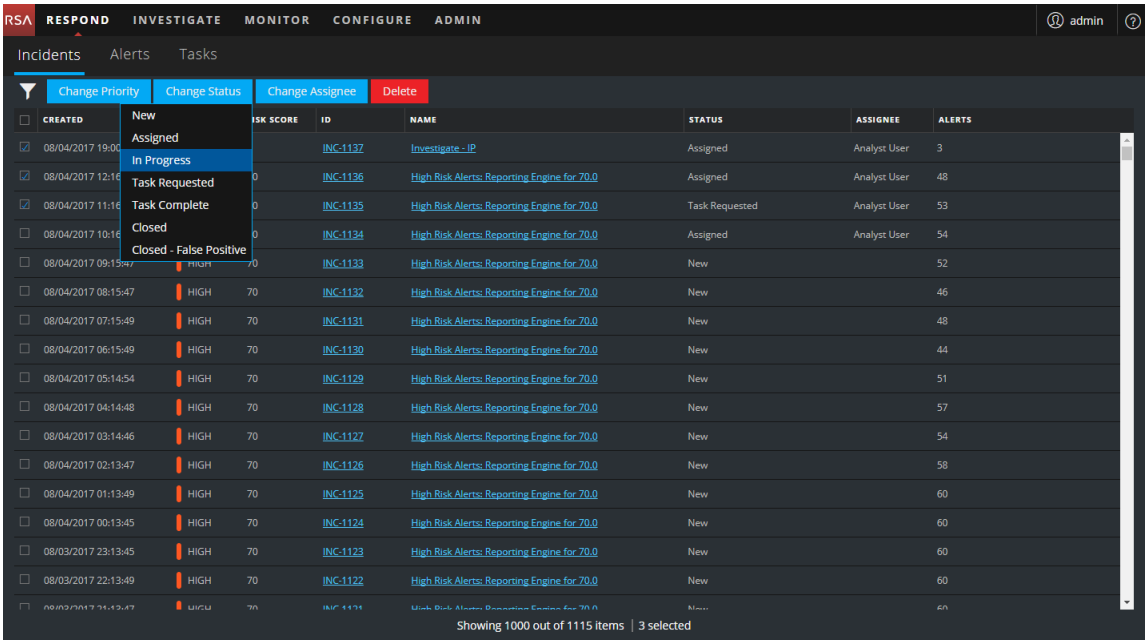
Ändern des Incident-Status

Wenn ein Incident das erste Mal in der Incident-Liste angezeigt wird, hat er den anfänglichen Status „Neu“. Sie können den Status entsprechend aktualisieren, wenn Sie am Incident arbeiten. Folgende Status sind verfügbar:

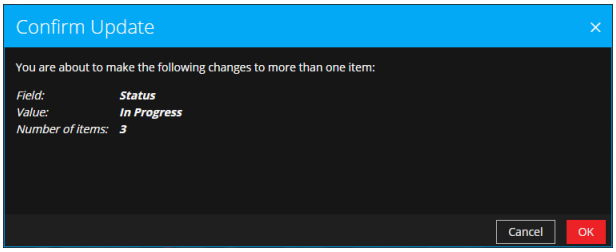
- Neu
- Zugewiesen
- Läuft
- Aufgabe angefordert
- Aufgabe abgeschlossen
- Abgeschlossen
- Geschlossen – falsch positives Ergebnis

So aktualisieren Sie den Status mehrerer Incidents:

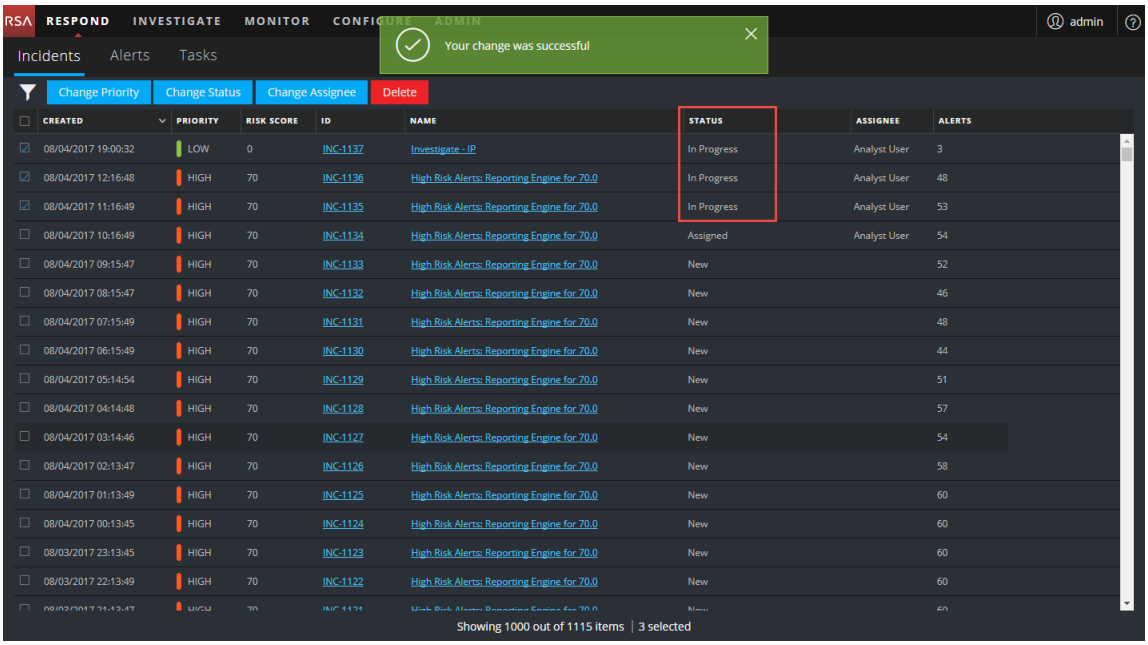
1. Wählen Sie in der Incident-Listenansicht einen oder mehrere Incidents, die Sie ändern möchten. Um alle Incidents auf der Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile der Incident-Liste. Die Anzahl der ausgewählten Incidents wird in der Fußzeile der Incident-Liste angezeigt.
2. Klicken Sie auf **Status ändern** und wählen Sie in der Drop-down-Liste einen Status aus. In diesem Beispiel lautet der aktuelle Status „Zugewiesen“, aber der Analyst möchte ihn für die ausgewählten Incidents auf „Läuft“ ändern.



3. Bei Auswahl von mehr als einem Incident im Dialogfeld **Aktualisierung bestätigen** klicken Sie auf **OK**.

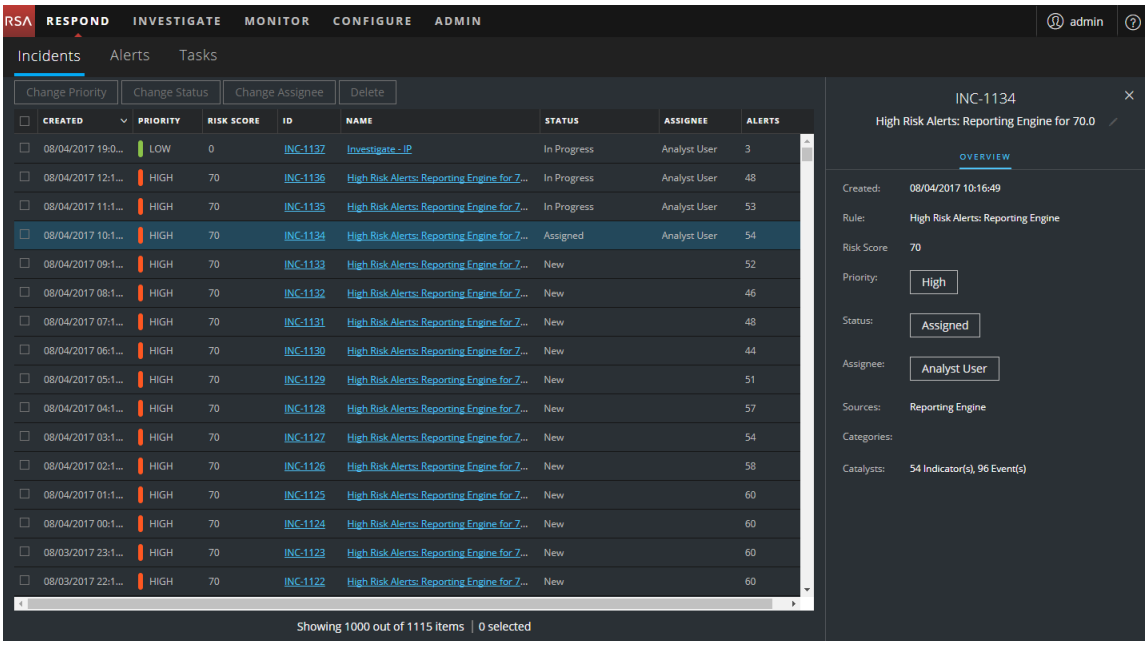


Eine Benachrichtigung über die erfolgreiche Änderung wird angezeigt. In diesem Beispiel lautet der Status der aktualisierten Incidents jetzt „Läuft“.

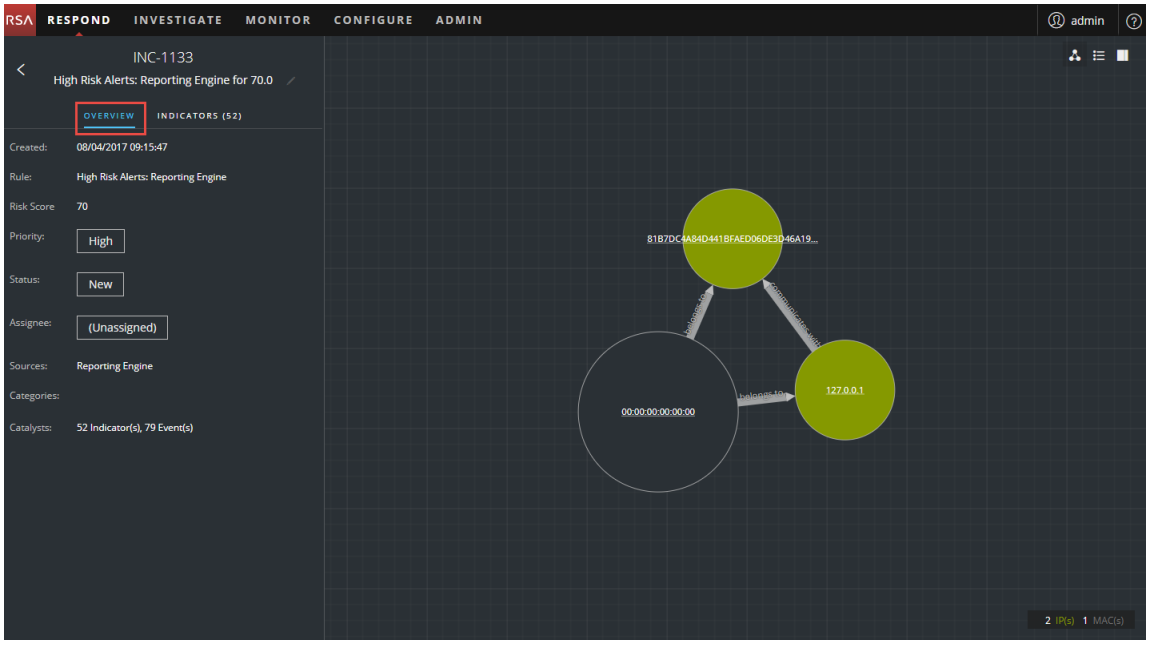


So ändern Sie den Status eines einzelnen Incident über den Bereich „Übersicht“:

1. Um den Bereich „Übersicht“ zu öffnen, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Incident-Listenansicht auf einen Incident, dessen Status aktualisiert werden muss.

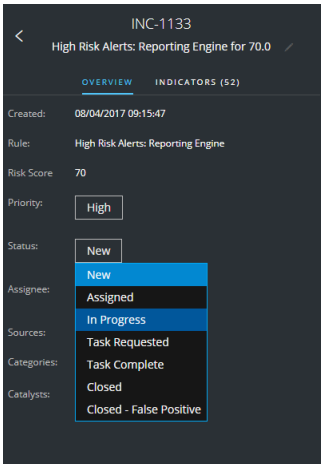


- Klicken Sie in der Ansicht „Incident-Details“ auf die Registerkarte **ÜBERSICHT**.



Im Bereich „Übersicht“ zeigt die Schaltfläche „Status“ den aktuellen Status des Incident.

2. Klicken Sie auf die Schaltfläche **Status** und wählen Sie in der Drop-down-Liste einen Status aus.



Eine Benachrichtigung über die erfolgreiche Änderung wird angezeigt.

Ändern der Incident-Priorität

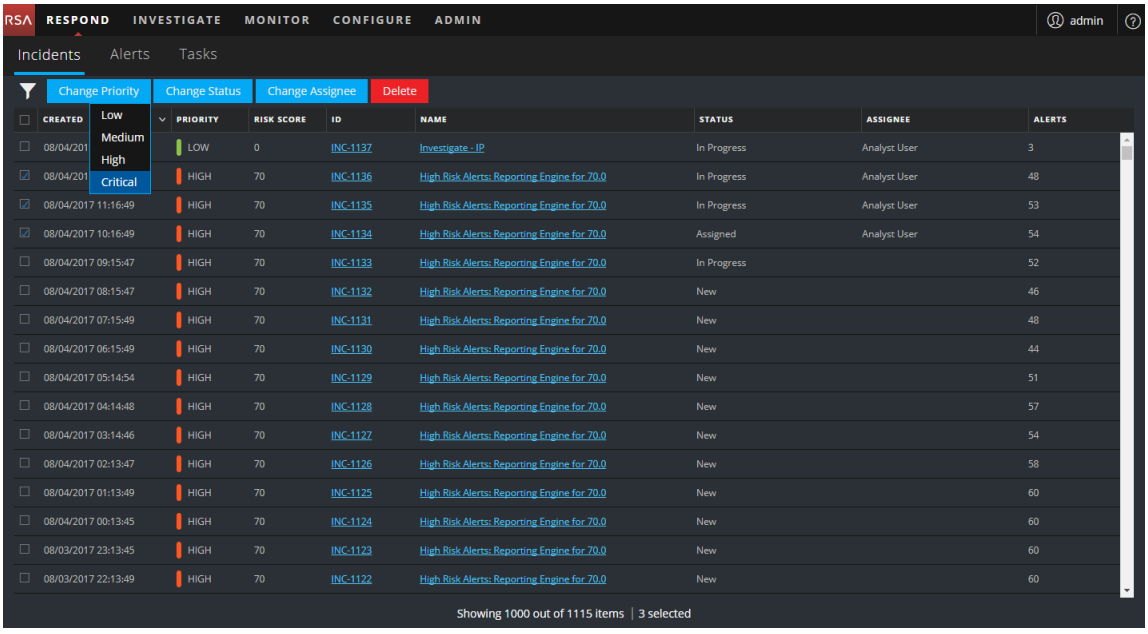
Die Incident-Liste ist standardmäßig nach Priorität sortiert. Sie können die Priorität aktualisieren, wenn Sie die Details des Falls untersuchen. Die folgenden Prioritäten sind verfügbar:

- Kritisch
- High
- Mittel
- Niedrig

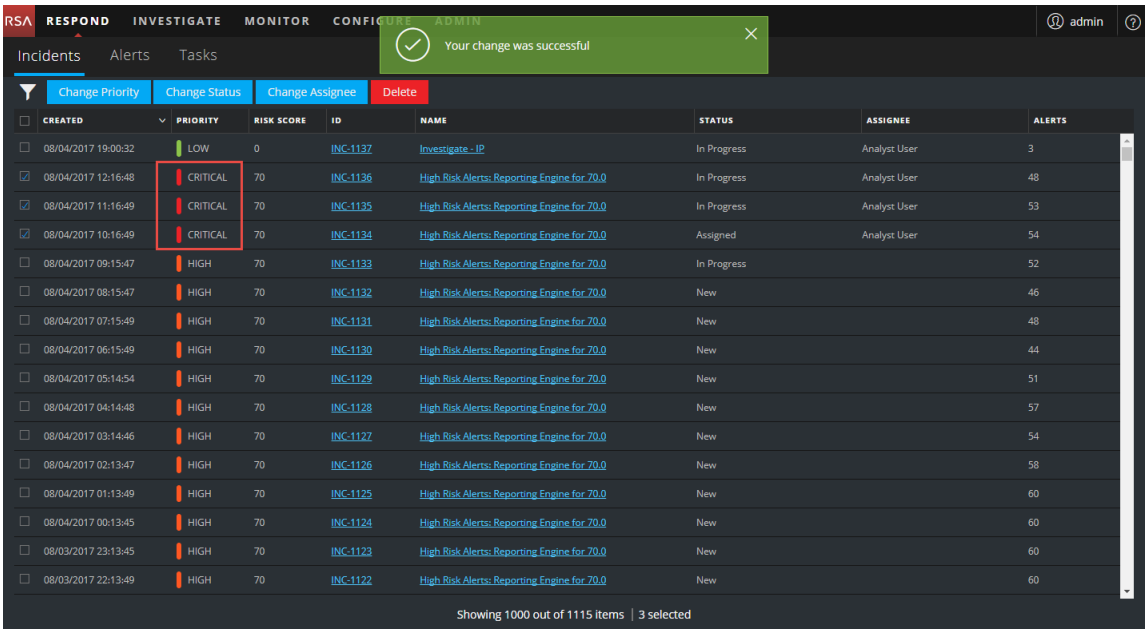
Hinweis: Sie können die Priorität eines geschlossenen Incident nicht ändern.

So aktualisieren Sie die Priorität mehrerer Incidents:

1. Wählen Sie in der Incident-Listenansicht einen oder mehrere Incidents, die Sie ändern möchten. Um alle Incidents auf der Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile der Incident-Liste. Die Anzahl der ausgewählten Incidents wird in der Fußzeile der Incident-Liste angezeigt.
2. Klicken Sie auf **Priorität ändern** und wählen Sie aus der Drop-down-Liste eine Priorität aus. In diesem Beispiel lautet die aktuelle Priorität „Hoch“, aber der Analyst möchte sie für die ausgewählten Incidents auf „Kritisch“ ändern.

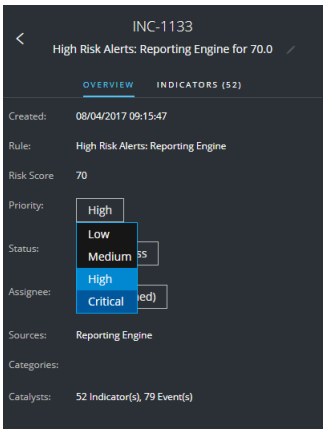


3. Bei Auswahl von mehr als einem Incident im Dialogfeld **Aktualisierung bestätigen** klicken Sie auf **OK**.
   Eine Benachrichtigung über die erfolgreiche Änderung wird angezeigt. In diesem Beispiel lautet der Status der aktualisierten Incidents jetzt „Kritisch“.



So ändern Sie die Priorität eines einzelnen Incident über den Bereich „Übersicht“

1. Um den Bereich „Übersicht“ zu öffnen, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Incident-Listenansicht auf einen Incident, dessen Priorität aktualisiert werden muss.
   - Klicken Sie in der Ansicht „Incident-Details“ auf die Registerkarte **ÜBERSICHT**. Die Schaltfläche „Priorität“ im Bereich „Übersicht“ zeigt die aktuelle Priorität des Incident an.
2. Klicken Sie auf die Schaltfläche **Priorität** und wählen Sie in der Drop-down-Liste einen Status aus.



Eine Benachrichtigung über die erfolgreiche Änderung wird angezeigt. Die Schaltfläche „Priorität“ ändert sich und zeigt die neue Incident-Priorität an.

Zuweisen von Incidents an andere Analysten

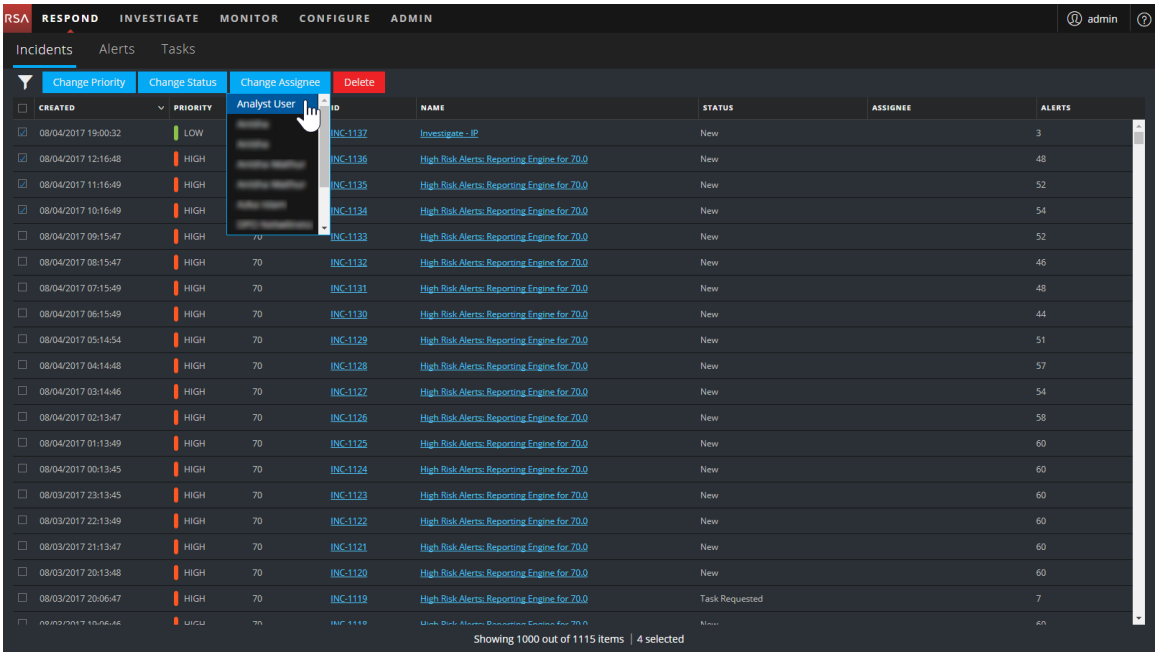
Sie können Incidents anderen Analysten auf die gleiche Weise zuweisen, wie Sie sie sich selbst zuweisen. SOC-Manager und Administratoren können einem Benutzer gleichzeitig mehrere Incidents zuweisen.

Hinweis: Sie können den Zuweisungsempfänger eines geschlossenes Incident nicht ändern.

So weisen einem Benutzer mehrere Incidents zu:

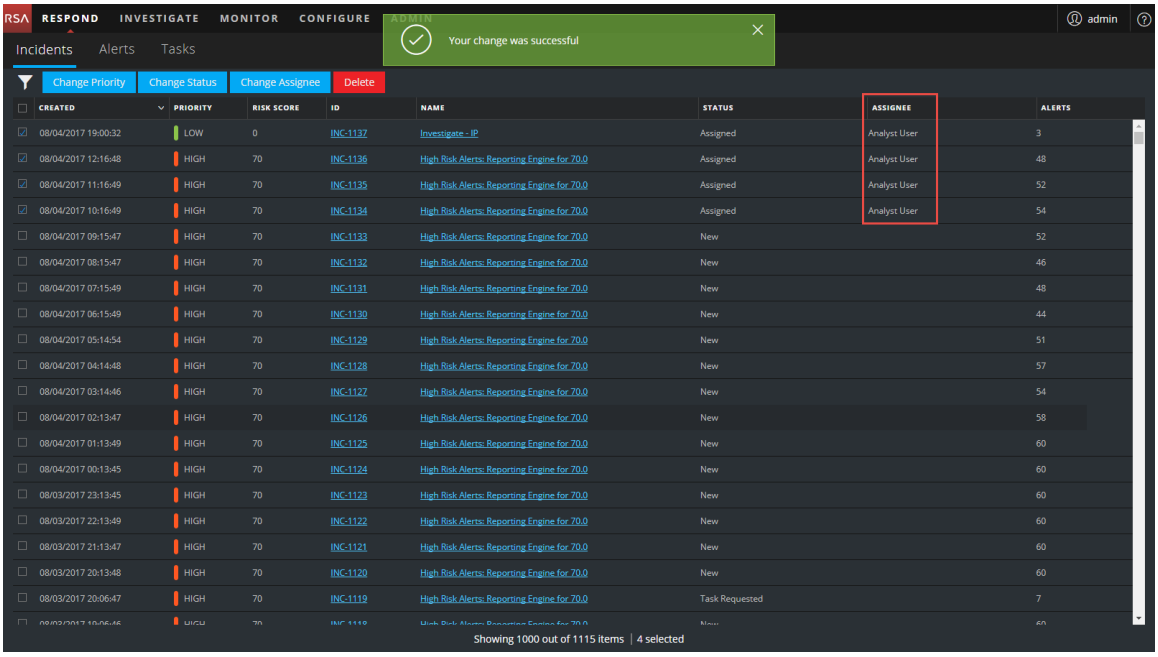
1. Wählen Sie in der Incident-Listenansicht die Incidents, die Sie einem Benutzer zuweisen möchten. Um alle Incidents auf der Seite auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile der Incident-Liste. Die Anzahl der ausgewählten Incidents wird in der Fußzeile der Incident-Liste angezeigt.
2. Klicken Sie auf **Zuweisungsempfänger ändern** und wählen Sie in der Drop-down-Liste einen Benutzer aus. In diesem Beispiel sind die Incidents nicht zugewiesen, sie sollten

jedoch einem Analysten zugewiesen sein.



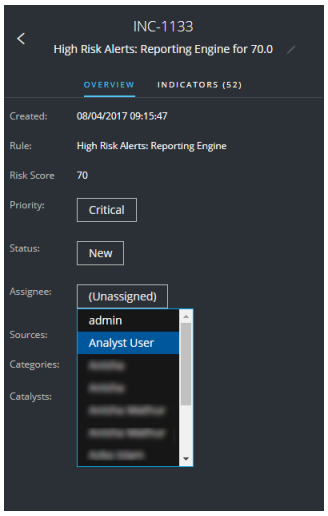
3. Bei Auswahl von mehr als einem Incident im Dialogfeld **Aktualisierung bestätigen** klicken Sie auf **OK**.

   Eine Benachrichtigung über die erfolgreiche Änderung wird angezeigt. Der Zuweisungsempfänger wird auf den ausgewählten Benutzer geändert.



So weisen Sie einen Benutzer über den Bereich „Übersicht“ einem Incident zu:

1. Um den Bereich „Übersicht“ zu öffnen, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Incident-Listenansicht auf einen Incident, dessen Priorität aktualisiert werden muss.
   - Klicken Sie in der Ansicht „Incident-Details“ auf die Registerkarte **ÜBERSICHT**.
     Im Bereich „Übersicht“ zeigt die Schaltfläche „Priorität“ die aktuelle Priorität des Incident. Im folgenden Beispiel hat die Schaltfläche „Zuweisungsempfänger“ den aktuellen Status „Nicht zugewiesen“.



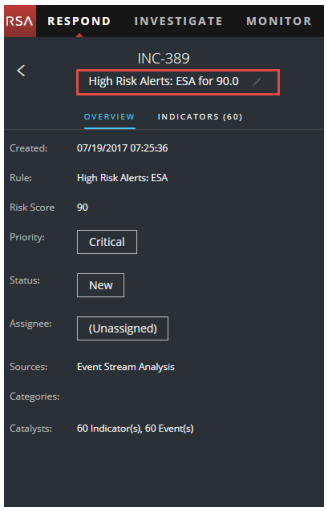
2. Klicken Sie auf die Schaltfläche **Zuweisungsempfänger** und wählen Sie in der Drop-down-Liste einen Benutzer aus.
   Eine Benachrichtigung über die erfolgreiche Änderung wird angezeigt. Die Schaltfläche „Zuweisungsempfänger“ ändert sich und zeigt den zugewiesenen Benutzer an.

Umbenennen eines Incident

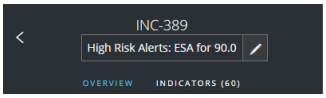
Sie können einen Incident aus dem Bereich „Übersicht“ in der Incident-Listenansicht und der Ansicht „Incident-Details“ umbenennen. Möglicherweise möchten Sie einen Incident zur Klärung des Problems umbenennen, insbesondere, wenn mehrere Incidents denselben Namen haben.

1. Navigieren Sie zu **Reagieren > Incidents**.
2. Um den Bereich „Übersicht“ zu öffnen, führen Sie einen der folgenden Schritte aus:

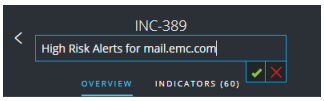
- Klicken Sie in der Incident-Listenansicht auf einen Incident, dessen Name geändert werden muss.
  Der Bereich „Übersicht“ wird geöffnet.
- Navigieren Sie in der Ansicht „Incident-Details“ zum Bereich **ÜBERSICHT**.
  In der Kopfzeile über dem Bereich „Übersicht“ sehen Sie die Incident-ID und den Namen des Incident.



3. Klicken Sie auf den Incident-Namen in der Kopfzeile, um einen Text-Editor zu öffnen.

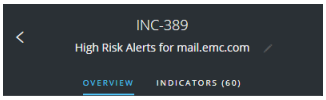


4. Geben Sie einen neuen Namen für den Incident in den Text-Editor ein und klicken Sie auf das Häkchen, um die Änderung zu bestätigen.



   Sie können z. B. „Warnmeldungen mit hohem Risiko: ESA für 90.0“ zur Verdeutlichung in „Warnmeldungen für mail.emc.com“ ändern.
   Eine Benachrichtigung über die erfolgreiche Änderung wird angezeigt.

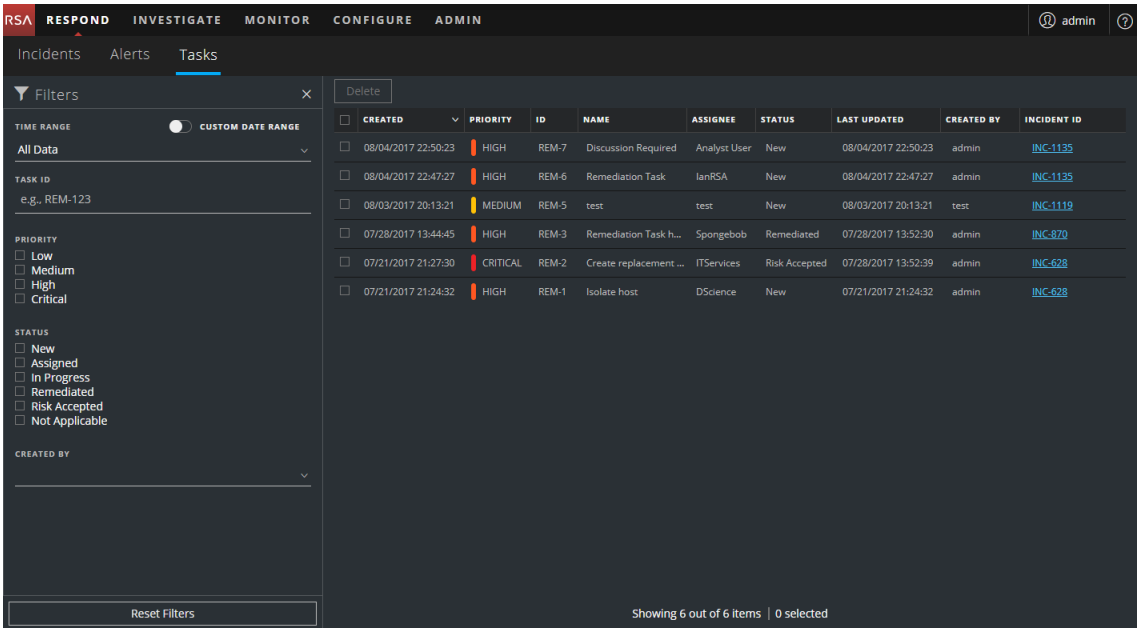
   Im Feld „Incident-Name“ wird der neue Name angezeigt.



Anzeigen aller Incident-Aufgaben

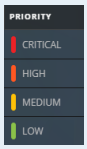
Wenn zusätzliche Arbeiten für einen Incident erforderlich sind, können Sie Aufgaben für den Incident erstellen und den Fortschritt , dieser Aufgaben nachverfolgen. Dies ist hilfreich, wenn Sie beispielsweise Arbeiten außerhalb der Sicherheitsabläufe durchführen oder eine Anforderung für die Erstellung eines neuen Image für den Rechner vornehmen. In der Ansicht „Aufgabenliste“ können Sie die Aufgaben managen und bis zum Abschluss nachverfolgen.

1. Navigieren Sie zu **Reagieren > Aufgaben**.
   In der Ansicht „Aufgabenliste“ wird eine Liste aller Incident-Aufgaben angezeigt.



2. Blättern Sie durch die Aufgabenliste, in der grundlegende Informationen zu jeder Aufgabe angezeigt werden, wie in der folgenden Tabelle beschrieben ist.

Spalte	Beschreibung
CREATED	Zeigt das Datum an, an dem die Aufgabe erstellt wurde.

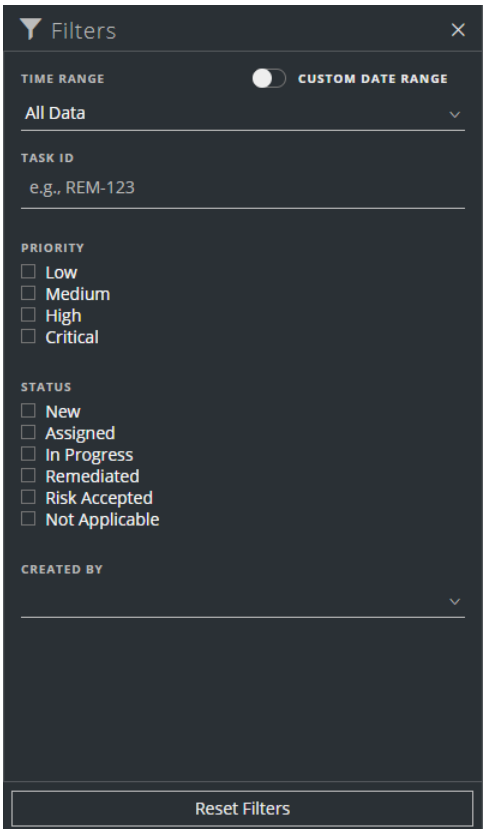
Spalte	Beschreibung
PRIORITÄT	Zeigt die Priorität an, die der Aufgabe zugewiesen wurde. Die Priorität kann eine der Folgenden sein: Kritisch, Hoch, Mittel oder Niedrig. Die Priorität ist auch farbcodiert, wobei Rot **Kritisch** bedeutet, Orange **hohes** Risiko, Gelb **mittleres** Risiko und Grün **geringes** Risiko, wie in der folgenden Abbildung dargestellt ist: 
ID	Zeigt die Aufgaben-ID.
NAME	Zeigt den Aufgabennamen an.
ZUWEISUNGSEMPFÄNGER	Zeigt den Namen des Benutzers an, der der Aufgabe zugewiesen wurde.
STATUS	Zeigt den Status der Aufgabe an: „Neu“, „Zugewiesen“, „Läuft“, „Korrigiert“, „Risiko akzeptiert“ und „Nicht zutreffend“.
LETZTE AKTUALISIERUNG	Zeigt das Datum und die Uhrzeit der letzten Aktualisierung der Aufgabe an.
ERSTELLT VON	Zeigt den Benutzer an, der die Aufgabe erstellt hat.
Incident-ID	Zeigt die ID des Incident an, für den die Aufgabe erstellt wurde. Klicken Sie auf die ID, um die Details des Incident anzuzeigen.

Am unteren Rand der Liste sehen Sie die Anzahl der Aufgaben auf der aktuellen Seite, die Gesamtzahl der Aufgaben und die Anzahl der ausgewählten Aufgaben. Beispiel: **6 von 6 Elementen werden angezeigt | 2 ausgewählt**.

Filtern der Aufgabenliste

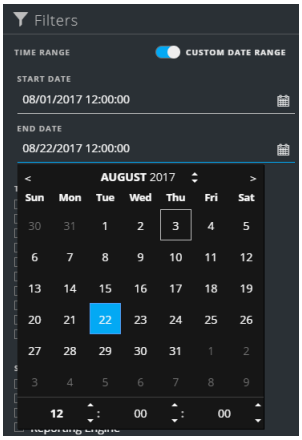
Die Anzahl der Aufgaben in der Aufgabenliste kann sehr groß sein, sodass es schwierig ist, bestimmte Aufgaben zu finden. Mit dem Filter können Sie die Aufgaben angeben, die Sie anzeigen möchten, etwa Aufgaben, die in den letzten 7 Tagen erstellt wurden. Sie können auch nach einer spezifischen Aufgabe suchen.

1. Navigieren Sie zu **Reagieren > Aufgaben**.
   Der Bereich „Filter“ wird auf der linken Seite der Aufgabenliste angezeigt. Sollte der Bereich „Filter“ nicht angezeigt werden, klicken Sie in der Symbolleiste der Ansicht „Aufgabenliste“ auf , woraufhin der Bereich „Filter“ geöffnet wird.



2. Wählen Sie im Bereich „Filter“ eine oder mehrere Optionen zum Filtern der Liste „Incidents“:
   - **ZEITBEREICH**: Sie können einen bestimmten Zeitraum aus der Drop-down-Liste „Zeitbereich“ auswählen. Der Zeitbereich basiert auf dem Erstellungsdatum der Aufgaben. Wenn Sie zum Beispiel „Letzte Stunde“ auswählen, werden die Aufgaben angezeigt, die innerhalb der letzten 60 Minuten erstellt wurden.

- **BENUTZERDEFINIERTER DATUMSBEREICH**: Sie können einen bestimmten Datumsbereich anstelle der Option „Zeitbereich“ auswählen. Klicken Sie dazu auf den weißen Kreis vor „BENUTZERDEFINIERTER DATUMSBEREICH“, um die Felder „Startdatum“ und „Enddatum“ anzuzeigen. Wählen Sie die Datums- und Zeitangaben im Kalender aus.



- **AUFGABEN-ID**: Geben Sie die Aufgaben-ID für eine Aufgabe ein, die Sie suchen möchten, z. B. REM-123.
- **PRIORITÄT**: Wählen Sie die Prioritäten aus, die Sie anzeigen möchten.
- **STATUS**: Wählen Sie einen oder mehrere Incident-Status aus. Wählen Sie beispielsweise „Korrigiert“ aus, um abgeschlossene Korrekturaufgaben anzuzeigen.
- **ERSTELLT VON**: Wählen Sie den Benutzer, der die Aufgaben erstellt hat, die Sie anzeigen möchten. Wenn Sie beispielsweise nur die Aufgaben anzeigen möchten, die von Edwardo erstellt wurden, wählen Sie „Edwardo“ aus der Drop-down-Liste „ERSTELLT VON“ aus. Wenn Sie Aufgaben unabhängig von der Person, die sie erstellt hat, anzeigen möchten, treffen Sie unter „ERSTELLT VON“ keine Auswahl.

In der Aufgabenliste wird eine Liste der Aufgaben angezeigt, die Ihre Auswahlkriterien erfüllen. Sie finden die Anzahl der Elemente in der gefilterten Liste am unteren Rand der Aufgabenliste.
Beispiel: **6 von 6 Elementen werden angezeigt**

3. Wenn Sie den Bereich „Filter“ schließen möchten, klicken Sie auf **X**. Ihre Filter werden beibehalten, bis Sie sie entfernen.

Entfernen meiner Filter aus der Aufgabenliste

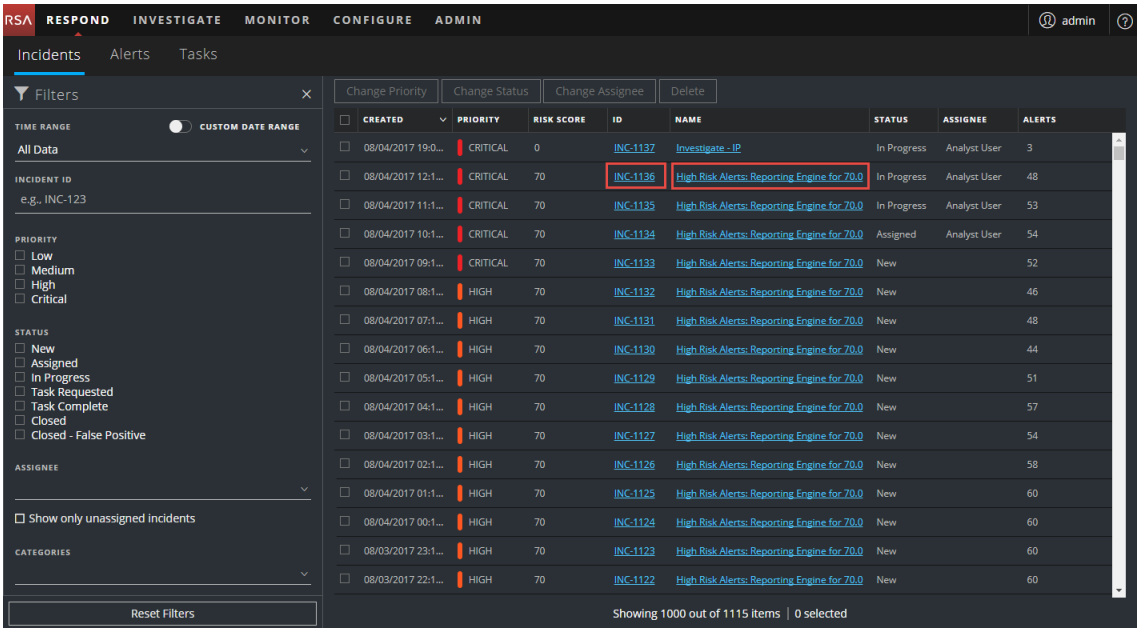
NetWitness Suite erinnert sich an Ihre Filterauswahl in der Ansicht „Aufgabenliste“. Sie können Ihre Filterauswahl entfernen, wenn Sie sie nicht mehr benötigen. Wenn Sie beispielsweise nicht die erwartete Anzahl an Aufgaben sehen oder Sie alle Aufgaben in der Aufgabenliste anzeigen möchten, können Sie Ihre Filter zurücksetzen.

1. Navigieren Sie zu **Reagieren > Aufgaben**.
   Der Bereich „Filter“ wird auf der linken Seite der Aufgabenliste angezeigt. Sollte der Bereich „Filter“ nicht angezeigt werden, klicken Sie in der Symbolleiste der Ansicht „Aufgabenliste“ auf ▼, woraufhin der Bereich „Filter“ geöffnet wird.
2. Klicken Sie am unteren Rand des Bereichs „Filter“ auf **Filter zurücksetzen**.

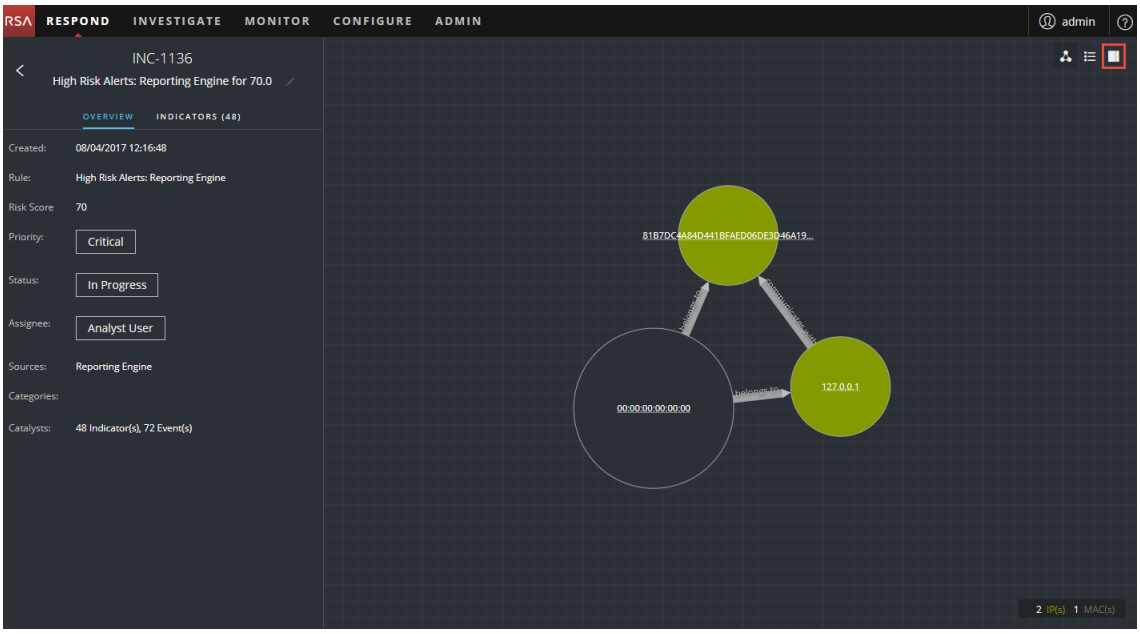
Erstellen einer Aufgabe

Nachdem Sie einen Incident untersucht haben und mehr über ihn wissen, können Sie eine Aufgabe erstellen, sie einem Benutzer zuweisen und bis zum Abschluss nachverfolgen. Sie können Aufgaben in der Ansicht „Incident-Details“ erstellen.

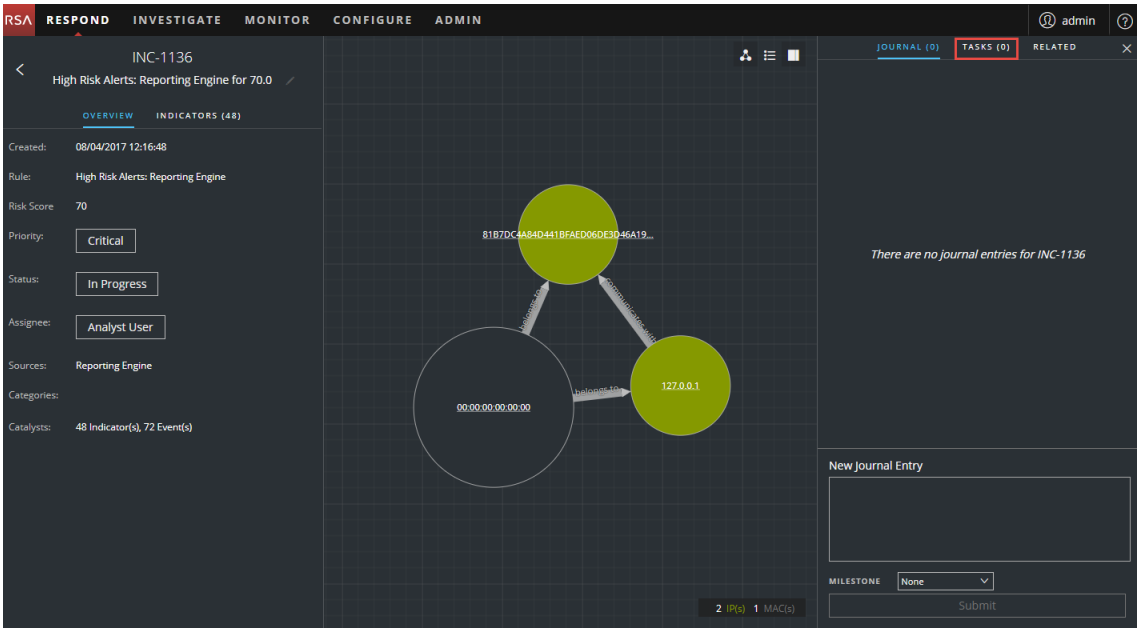
1. Navigieren Sie zu **Reagieren > Incidents**.
   In der Ansicht „Incident-Liste“ wird eine Liste aller Incidents angezeigt.



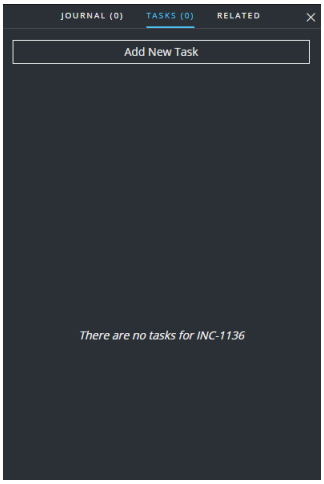
2. Suchen Sie den Incident, der eine Aufgabe benötigt, und klicken Sie auf den Link im Feld **ID** oder **NAME**.
   Die Ansicht „Incident-Details“ wird geöffnet.



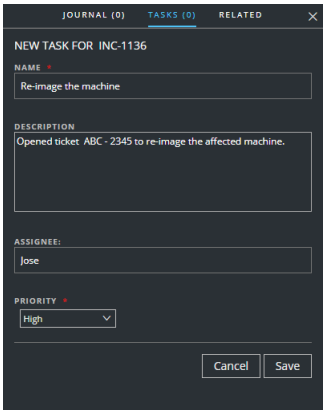
3. Wählen Sie in der Symbolleiste oben rechts in der Ansicht „Incident-Details“ ▣ aus.
   Der Bereich „Journal“ wird geöffnet.



4. Wählen Sie die Registerkarte **AUFGABEN** aus.



5. Klicken Sie im Bereich „Aufgaben“ auf **Neue Aufgabe hinzufügen.**
   Die Felder für die neue Aufgabe werden angezeigt.

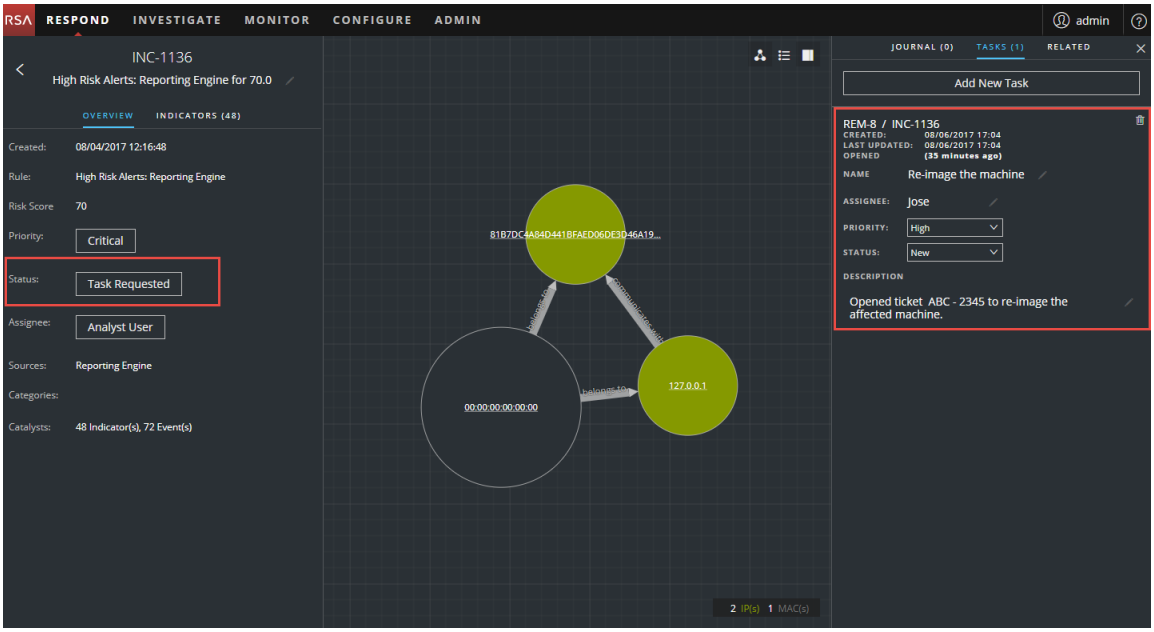


   Wenn der Incident den Status „Geschlossen“ aufweist („Geschlossen“ oder „Geschlossen – falsch positives Ergebnis“), ist die Schaltfläche „Neue Aufgabe hinzufügen“ deaktiviert.

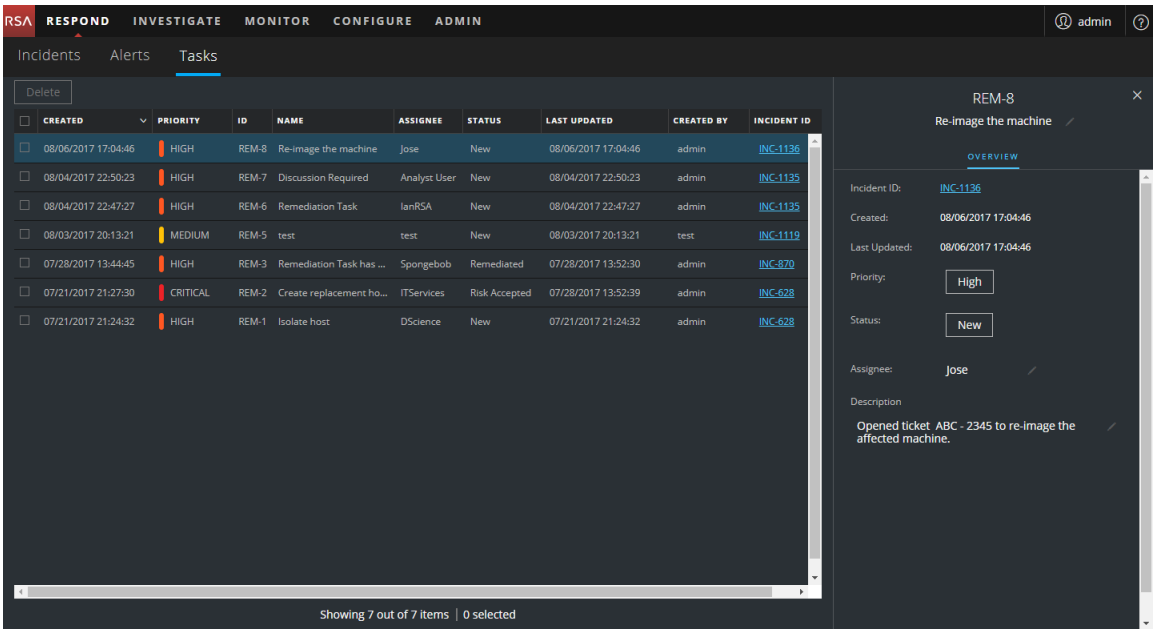
6. Stellen Sie folgende Informationen bereit:
   - **Name**: Name der Aufgabe. Beispiel: Neues Image für den Rechner erstellen.
   - **Beschreibung**: (Optional) Geben Sie eine Beschreibung für die Aufgabe ein. Sie können geltende Referenznummern einbeziehen.
   - **Zuweisungsempfänger**: (Optional) Geben Sie den Namen des Benutzers ein, dem die Aufgabe zugewiesen werden soll.
   - **Priorität**: Klicken Sie auf die Schaltfläche „Priorität“ und wählen Sie eine Priorität für die Aufgaben aus der Drop-down-Liste: „Niedrig“, „Mittel“, „Hoch“ oder „Kritisch“.

7. Klicken Sie auf **Speichern**.
   Sie sehen eine Bestätigung, dass Ihre Änderung erfolgreich war. Der Status des Incident

ändert sich zu **Aufgabe angefordert**. Die Aufgabe wird im Bereich „Aufgaben“ für diesen Incident angezeigt.



Außerdem wird Sie in der Liste der Aufgaben (Reagieren > Aufgaben) in einer Liste aller Incident-Aufgaben angezeigt.

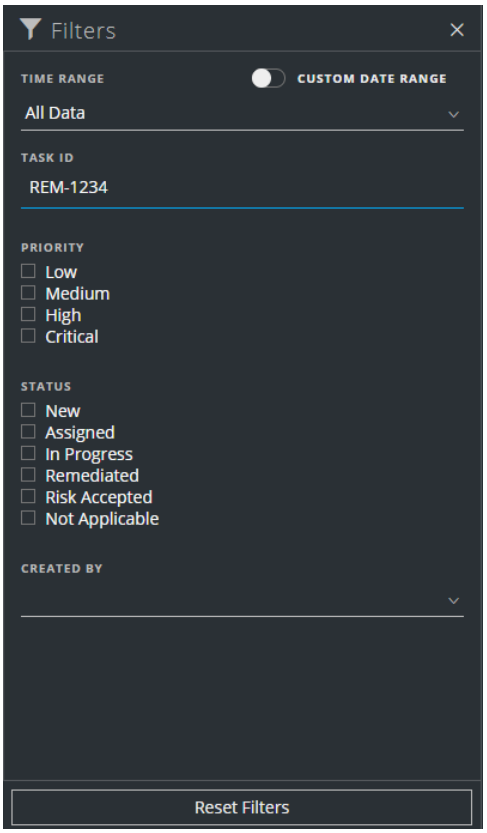


Hinweis: Sollte sich der Status nicht ändern, müssen Sie möglicherweise Ihren Internetbrowser aktualisieren.

Suchen einer Aufgabe

Wenn Sie die Aufgaben-ID kennen, können Sie eine Aufgabe schnell mithilfe des Filters suchen. Beispiel: Sie möchten eine bestimmte Aufgabe in Tausenden von Aufgaben suchen.

1. Navigieren Sie zu **Reagieren > Aufgaben**.
   Der Bereich „Filter“ wird auf der linken Seite der Aufgabenliste angezeigt. Sollte der Bereich „Filter“ nicht angezeigt werden, klicken Sie in der Symbolleiste der Ansicht „Aufgabenliste“ auf , woraufhin der Bereich „Filter“ geöffnet wird.



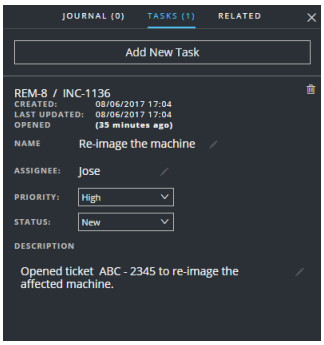
2. Geben Sie im Feld „AUFGABEN-ID“ die Aufgaben-ID für eine Aufgabe ein, die Sie suchen möchten, z. B. REM-1234.
   Die angegebene Aufgabe wird in der Aufgabenliste angezeigt. Wenn keine Ergebnisse angezeigt werden, versuchen Sie, die Filter zurücksetzen.

Ändern einer Aufgabe

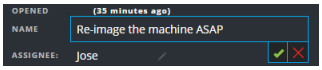
Sie können eine Aufgabe von innerhalb eines Incident und in der Aufgabenliste ändern. Möglicherweise möchten Sie als Status der Aufgabe „Läuft“ anzeigen und einige zusätzliche Informationen zur Aufgabe hinzufügen. Wenn die Aufgabe den Status „Geschlossen“ (Nicht zutreffend, Risiko akzeptiert oder Korrigiert) aufweist, können Sie weder Priorität noch Zuweisungsempfänger ändern.

So ändern Sie eine Aufgabe innerhalb eines Incident:

1. Navigieren Sie zu **Reagieren > Incidents**.
   In der Incident-Listenansicht wird eine Liste aller Incidents angezeigt.
2. Suchen Sie den Incident, der eine Aufgabenaktualisierung benötigt, und klicken Sie auf den Link im Feld **ID** oder **NAME**.
   Die Ansicht „Incident-Details“ wird geöffnet.
3. Wählen Sie in der Symbolleiste oben rechts in der Ansicht ◻ aus.
   Der Bereich „Journal“ wird geöffnet.
4. Wählen Sie die Registerkarte **AUFGABEN** aus.
5. Im Bereich „Aufgaben“ gibt ein Bleistiftsymbol ein Textfeld an, das Sie ändern können. Eine Schaltfläche weist auf eine Drop-down-Liste hin, in der Sie eine Auswahl treffen können.

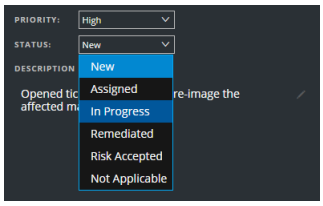


6. Sie können die folgenden Felder bearbeiten:
   - **NAME**: Klicken Sie auf den aktuellen Aufgabennamen, um einen Text-Editor zu öffnen.

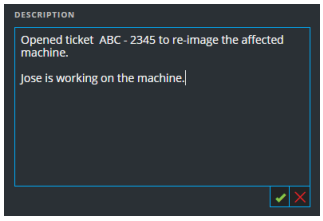


     Klicken Sie auf das Häkchen, um die Änderung zu bestätigen. Sie können beispielsweise „Neues Image für den Rechner erstellen“ zu „So bald wie möglich neues Image für den Rechner erstellen“ ändern.

- **ZUWEISUNGSEMPFÄNGER**: Klicken Sie auf „(Nicht zugewiesen)“ oder den Namen des vorherigen Zuweisungsempfängers, um einen Text-Editor zu öffnen. Geben Sie den Namen des Benutzers ein, dem die Aufgabe zugewiesen werden soll.
  Klicken Sie auf das Häkchen, um die Änderung zu bestätigen.
- **PRIORITÄT**: Klicken Sie auf die Schaltfläche „Priorität“ und wählen Sie eine Priorität für die Aufgabe aus der Drop-down-Liste: „Niedrig“, „Mittel“, „Hoch“ oder „Kritisch“.
- **STATUS**: Klicken Sie auf die Schaltfläche „Status“ und wählen Sie in der Drop-down-Liste einen Status für die Aufgabe aus: „Neu“, „Zugewiesen“, „Läuft“, „Korrigiert“, „Risiko akzeptiert“ und „Nicht zutreffend“. Beispielsweise können Sie den Status auf „Läuft“ ändern.



- **BESCHREIBUNG**: Klicken Sie auf den Text unter der Beschreibung, um einen Text-Editor zu öffnen.

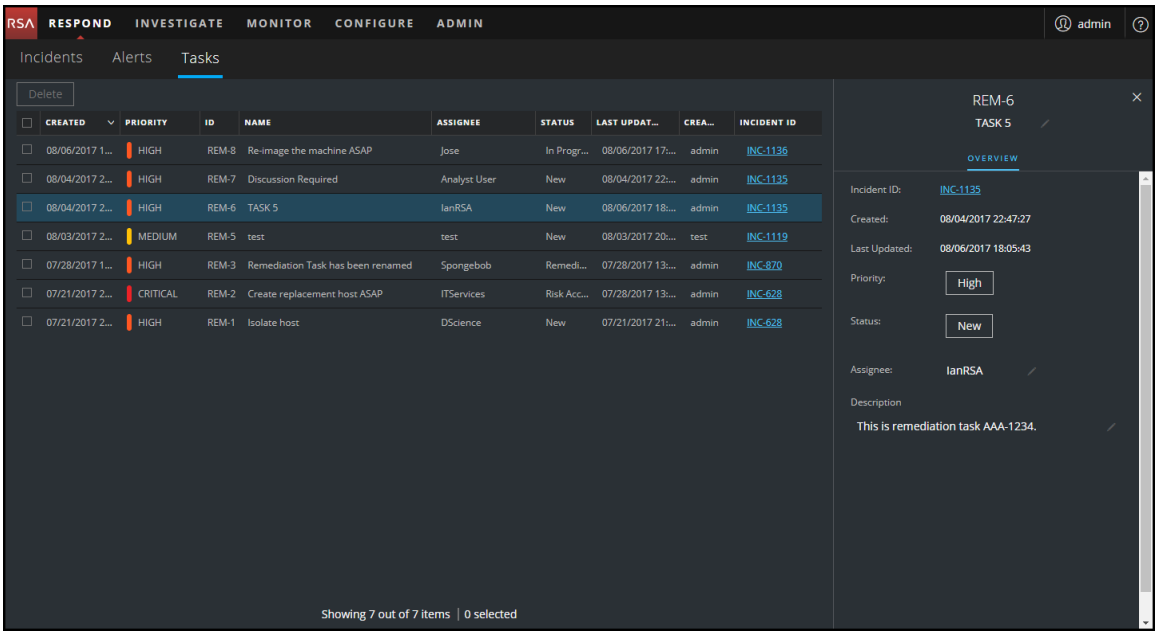


  Ändern Sie den Text und klicken Sie auf das Häkchen, um die Änderung zu bestätigen.

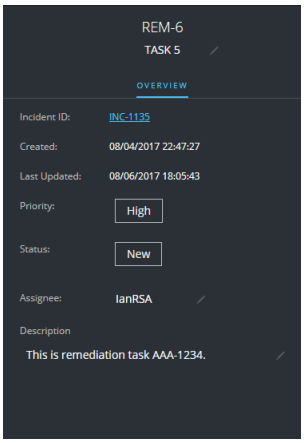
Für jede vorgenommene Änderung sehen Sie eine Bestätigung darüber, dass Ihre Änderung erfolgreich war.

So ändern Sie eine Aufgabe aus der Liste der Aufgaben:

1. Navigieren Sie zu **Reagieren > Aufgaben**.
   In der Ansicht „Aufgabenliste“ wird eine Liste aller Incident-Aufgaben angezeigt.
2. Klicken Sie in der Aufgabenliste auf die Aufgabe, die Sie aktualisieren möchten.
   Der Bereich „Übersicht“ für Aufgaben wird rechts neben der Liste der Aufgaben angezeigt.

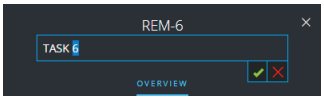


Im Bereich „Übersicht“ für Aufgaben gibt ein Bleistiftsymbol ein Textfeld an, das Sie ändern können. Eine Schaltfläche weist auf eine Drop-down-Liste hin, in der Sie eine Auswahl treffen können.



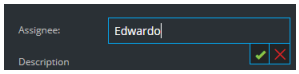
3. Sie können die folgenden Felder bearbeiten:

   - **<Aufgabenname>**: Klicken Sie am oberen Rand des Bereichs „Übersicht“ für Aufgaben unter der Aufgaben-ID auf den Namen der aktuellen Aufgabe, um einen Text-Editor zu öffnen.

     Klicken Sie auf das Häkchen, um die Änderung zu bestätigen. Beispielsweise können Sie „AUFGABE 5“ in „AUFGABE 6“ ändern.

- **Priorität**: Klicken Sie auf die Schaltfläche „Priorität“ und wählen Sie eine Priorität für die Aufgabe aus der Drop-down-Liste: „Niedrig“, „Mittel“, „Hoch“ oder „Kritisch“.
- **Status**: Klicken Sie auf die Schaltfläche „Status“ und wählen Sie in der Drop-down-Liste einen Status für die Aufgabe aus: „Neu“, „Zugewiesen“, „Läuft“, „Korrigiert“, „Risiko akzeptiert“ und „Nicht zutreffend“.
- **Zuweisungsempfänger**: Klicken Sie auf „(Nicht zugewiesen)“ oder den Namen des vorherigen Zuweisungsempfängers, um einen Text-Editor zu öffnen. Geben Sie den Namen des Benutzers ein, dem die Aufgabe zugewiesen werden soll.

  Klicken Sie auf das Häkchen, um die Änderung zu bestätigen.
- **Beschreibung**: Klicken Sie auf den Text unter der Beschreibung, um einen Text-Editor zu öffnen.

  Ändern Sie den Text und klicken Sie auf das Häkchen, um die Änderung zu bestätigen.

Für jede vorgenommene Änderung sehen Sie eine Bestätigung darüber, dass Ihre Änderung erfolgreich war.

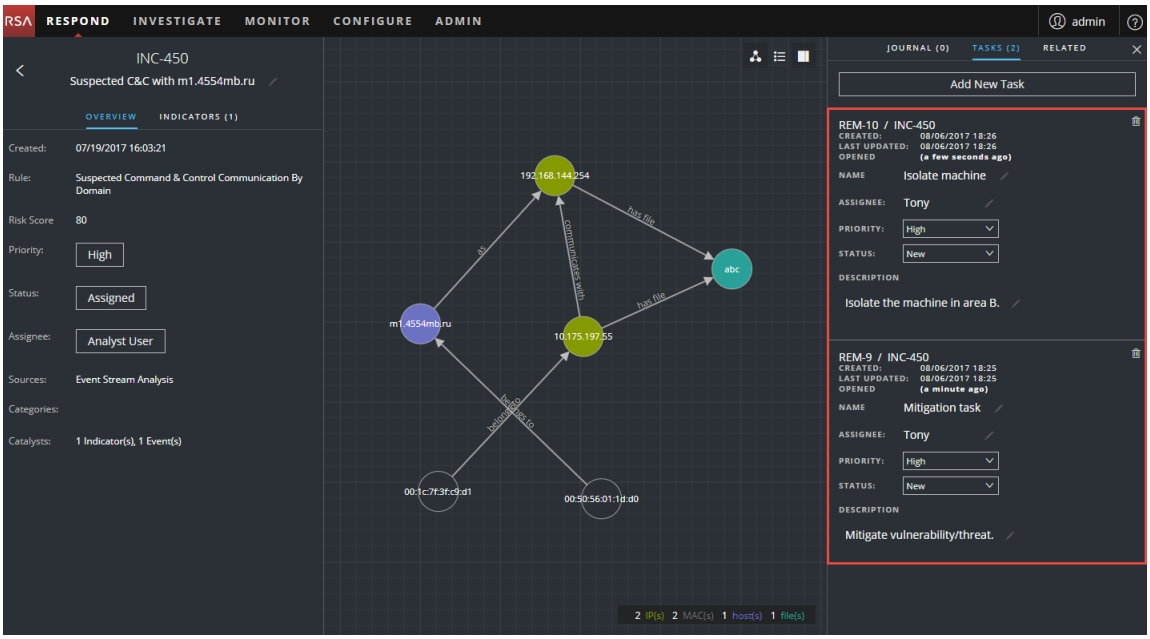
Löschen einer Aufgabe

Sie können eine Aufgabe löschen, wenn Sie sie z. B. irrtümlich erstellt haben oder Sie feststellen, dass sie nicht benötigt wird. Sie können eine Aufgabe von innerhalb eines Incident und in der Ansicht „Aufgabenliste“ löschen. In der Ansicht „Aufgabenliste“ können Sie mehrere Aufgaben gleichzeitig löschen.

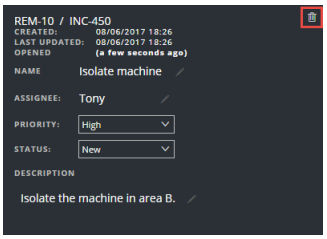
So löschen Sie eine Aufgabe innerhalb eines Incident:

1. Navigieren Sie zu **Reagieren > Incidents**.
   In der Incident-Listenansicht wird eine Liste aller Incidents angezeigt.
2. Suchen Sie den Incident, der eine Aufgabenaktualisierung benötigt, und klicken Sie auf den Link im Feld **ID** oder **NAME**.
   Die Ansicht „Incident-Details“ wird geöffnet.

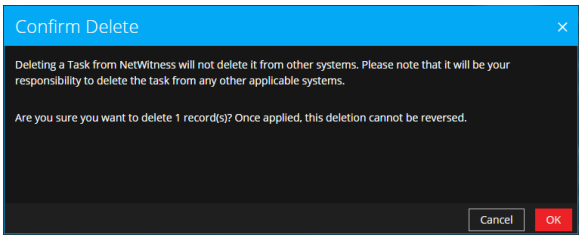
3. Wählen Sie in der Symbolleiste oben rechts in der Ansicht ■ aus.
   Der Bereich „Journal“ wird geöffnet.
4. Wählen Sie die Registerkarte „AUFGABEN“ aus.
5. Im Bereich „Aufgaben“ können Sie die Aufgaben sehen, die für den Incident erstellt wurden.



6. Klicken Sie auf 🗑 rechts neben der Aufgabe, die Sie löschen möchten.



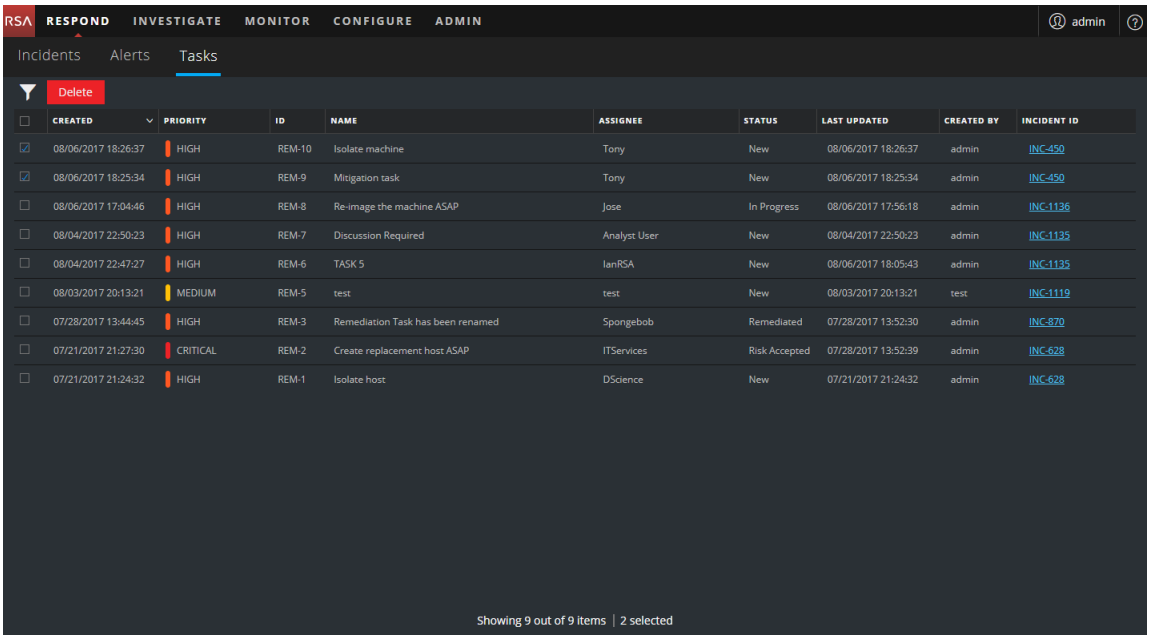
7. Bestätigen Sie, dass Sie die Aufgabe löschen möchten, und klicken Sie auf **OK**.



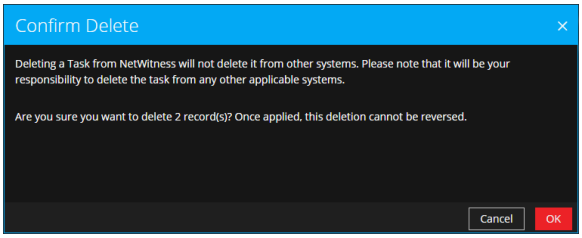
Die Aufgabe wird aus NetWitness Suite gelöscht. Durch das Löschen von Aufgaben aus NetWitness Suite werden sie nicht von anderen Systemen gelöscht.

So löschen Sie Aufgaben aus der Aufgabenliste:

1. Navigieren Sie zu **Reagieren > Aufgaben**.
   In der Ansicht „Aufgabenliste“ wird eine Liste aller Incident-Aufgaben angezeigt.
2. Wählen Sie in der Liste der Aufgaben die Aufgaben aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.



3. Bestätigen Sie, dass Sie die Aufgaben löschen möchten, und klicken Sie auf **OK**.



Die Aufgaben werden aus NetWitness Suite gelöscht. Durch das Löschen von Aufgaben aus NetWitness Suite werden sie nicht von anderen Systemen gelöscht.

Schließen eines Incident

Nachdem Sie einen Incident untersucht, das Problem behandelt und eine Lösung gefunden haben, schließen Sie den Incident.

1. Navigieren Sie zu **Reagieren > Incidents**.
2. Wählen Sie in der Incident-Listenansicht den Incident, den Sie schließen möchten, und klicken Sie auf **Status ändern**.
3. Wählen Sie aus der Drop-down-Liste **Geschlossen** aus.
   Eine Benachrichtigung über die erfolgreiche Änderung wird angezeigt. Der Incident ist jetzt geschlossen. Sie können die Priorität oder den Zuweisungsempfänger eines geschlossenen Incident nicht ändern.

Hinweis: Sie können einen Incident auch im Bereich „Übersicht“ schließen. In der Incident-Listenansicht können Sie mehrere Incidents gleichzeitig schließen. Unter Ändern des Incident-Status finden Sie zusätzliche Details.

Überprüfen von Warnmeldungen

NetWitness Suite ermöglicht es Ihnen, eine konsolidierte Liste von Warnmeldungen zu Bedrohungen, die aus mehreren Quellen erzeugt wurden, an einem zentralen Ort anzuzeigen. Sie finden diese Warnmeldungen in der Ansicht „RESPOND > Warnmeldungen“. Die Quelle der Warnmeldungen können ESA-Korrelationsregeln, ESA Analytics, NetWitness Endpoint, Malware Analysis, Reporting Engine und viele andere sein. Sie können die ursprüngliche Quelle der Warnmeldungen, den Schweregrad der Warnmeldung und zusätzliche Warnmeldungsdetails anzeigen.

Hinweis: Warnmeldungen zu ESA-Korrelationsregeln finden Sie NUR in der Ansicht „RESPOND > Warnmeldungen“.

Um eine große Anzahl von Warnmeldungen besser managen zu können, haben Sie die Möglichkeit, die Liste der Warnmeldungen basierend auf von Ihnen angegebenen Kriterien wie Schweregrad, Zeitbereich und Warnmeldungsquelle zu filtern. Beispielsweise können Sie die Warnmeldungen so filtern, dass nur Warnmeldungen mit einem Schweregrad zwischen 90 und 100 angezeigt werden, die nicht bereits Teil eines Incident sind. Sie können dann eine Gruppe von Warnmeldungen auswählen, um einen Incident zu erstellen oder sie zu einem vorhandenen Incident hinzuzufügen.

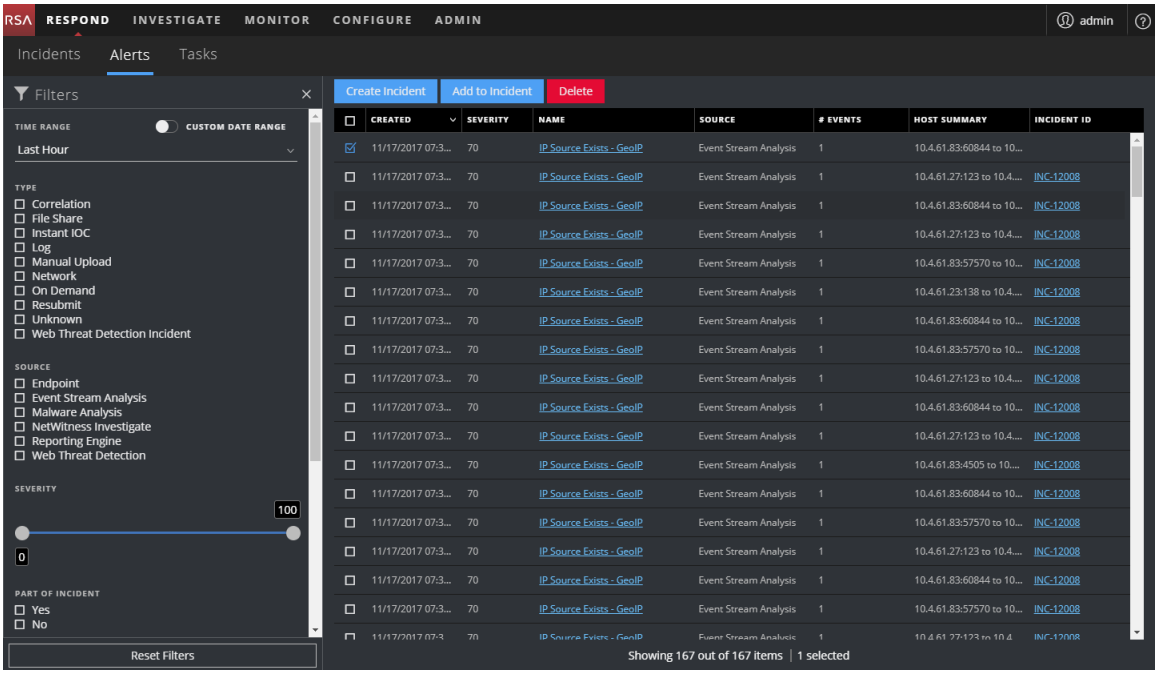
Sie können die folgenden Verfahren durchführen, um Warnmeldungen zu überprüfen und zu managen:

- Anzeigen von Warnmeldungen
- Filtern der Warnmeldungsliste
- Entfernen meiner Filter aus der Warnmeldungsliste
- Anzeigen von Übersichtsinformationen zu Warnmeldungen
- Anzeigen von Ereignisdetails für eine Warnmeldung
- Untersuchen von Ereignissen
- Manuelles Erstellen eines Incident
- Warnmeldungen zu einem Incident hinzufügen
- Löschen von Warnmeldungen

Anzeigen von Warnmeldungen

In der Listenansicht der Warnmeldungen können Sie verschiedene Warnmeldungen aus mehreren Quellen durchsuchen, diese filtern und gruppieren, um Incidents zu erstellen. Dieses Verfahren zeigt Ihnen, wie Sie auf die Liste der Warnmeldungen zugreifen.

1. Navigieren Sie zu **Reagieren > Warnmeldungen**.
   Die Ansicht „Warnmeldungsliste“ zeigt eine Liste aller NetWitness Suite-Warnmeldungen.



2. Blättern Sie durch die Warnmeldungsliste, in der grundlegende Informationen zu jeder Warnmeldung angezeigt werden, wie in der folgenden Tabelle beschrieben ist.

Spalte	Beschreibung
CREATED	Zeigt das Datum und die Uhrzeit der Aufzeichnung der Warnmeldung im Quellsystem an.
SCHWEREGRAD	Zeigt den Schweregrad der Warnmeldung an. Der Wert kann zwischen 1 und 100 liegen.
NAME	Zeigt eine grundlegende Beschreibung der Warnmeldung an.
QUELLE	Zeigt die ursprüngliche Quelle der Warnmeldung an. Die Quelle der Warnmeldungen können NetWitness Endpoint, Malware Analysis, Event Stream Analysis (ESA-Korrelationsregeln), ESA Analytics, Reporting Engine, Web Threat Detection und viele andere sein.

Spalte	Beschreibung
EREIGNISANZAHL	Zeigt die Anzahl an Ereignissen, die in einer Warnmeldung enthalten sind. Diese Zahl variiert je nach Quelle der Warnmeldung. NetWitness Endpoint- und Malware Analysis-Warnmeldungen haben zum Beispiel immer nur ein Ereignis. Für bestimmte Arten von Warnmeldungen bedeutet eine große Anzahl an Ereignissen, dass die Warnmeldung riskanter ist.
HOSTZUSAMMENFASSUNG	Zeigt Details des Hosts an, wie zum Beispiel den Hostnamen, von dem die Warnmeldung ausgelöst wurde. Die Details können Informationen zu den Quell- und Zielhosts in einer Warnmeldung enthalten. Manche Warnmeldungen können Ereignisse über mehr als einen Host beschreiben.
Incident-ID	Zeigt die Incident-ID der Warnmeldung. Gibt es keine Incident-ID, gehört die Warnmeldung zu keinem Incident und Sie können einen Incident erstellen, um die Warnmeldung hinzuzufügen. Alternativ kann die Warnmeldung einem vorhandenen Incident hinzugefügt werden.

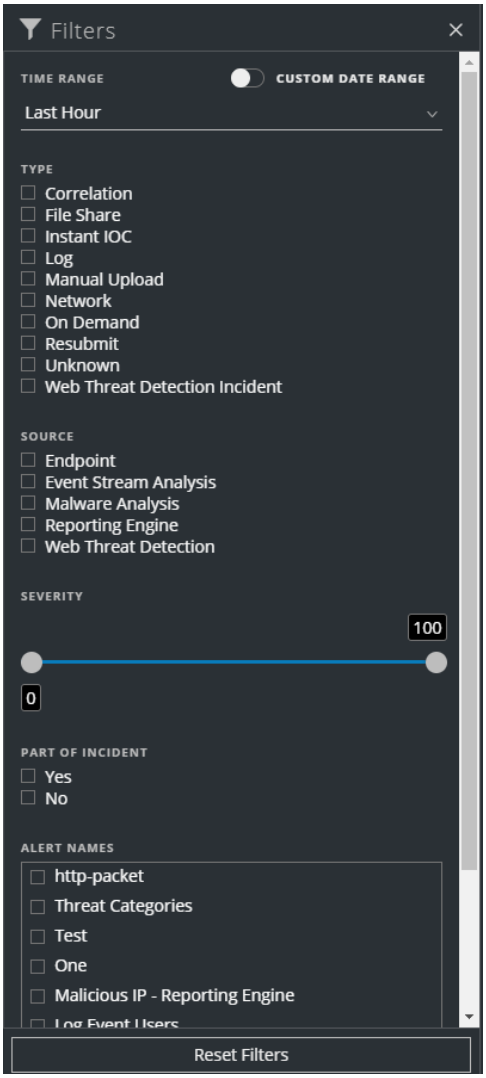
Am unteren Rand der Liste sehen Sie die Anzahl der Warnmeldungen auf der aktuellen Seite und die Gesamtzahl der Warnmeldungen. Beispiel: **377 von 377 Elementen werden angezeigt**

Filtern der Warnmeldungsliste

Die Anzahl der Warnmeldungen in der Liste der Warnmeldungen kann sehr groß sein, sodass es schwierig ist, bestimmte Warnmeldungen zu finden. Über den Filter können Sie die gewünschten Warnmeldungen anzeigen, beispielsweise Warnmeldungen aus einer bestimmten Quelle, Warnmeldungen mit einem bestimmten Schweregrad oder Warnmeldungen, die nicht Teil eines Incident sind usw.

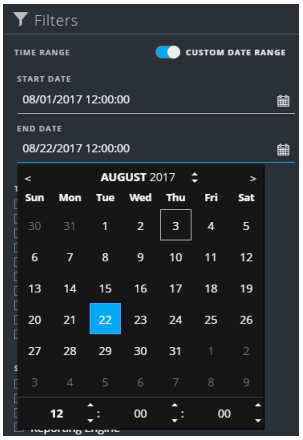
1. Navigieren Sie zu **Reagieren > Warnmeldungen**.
   Der Bereich „Filter“ wird auf der linken Seite der Warnmeldungsliste angezeigt. Sollte der

Bereich „Filter“ nicht angezeigt werden, klicken Sie in der Symbolleiste der Listenansicht der Warnmeldungen auf , woraufhin der Bereich „Filter“ geöffnet wird.



2. Wählen Sie im Bereich „Filter“ eine oder mehrere Optionen zum Filtern der Liste „Warnmeldungen“:
   - **ZEITBEREICH**: Sie können einen bestimmten Zeitraum aus der Drop-down-Liste „Zeitbereich“ auswählen. Der Zeitbereich basiert auf dem Datum, an dem die Warnmeldungen empfangen wurden. Wenn Sie zum Beispiel „Letzte Stunde“ auswählen, werden die Warnmeldungen angezeigt, die innerhalb der letzten 60 Minuten empfangen wurden.
   - **BENUTZERDEFINIERTER DATUMSBEREICH**: Sie können einen bestimmten Datumsbereich anstelle der Option „Zeitbereich“ auswählen. Klicken Sie dazu auf den weißen Kreis vor „BENUTZERDEFINIERTER DATUMSBEREICH“, um die Felder

„Startdatum“ und „Enddatum“ anzuzeigen. Wählen Sie die Datums- und Zeitangaben im Kalender aus.



- **TYP**: Wählen Sie den Ereignis-Typ der Warnmeldung aus, um zum Beispiel Protokolle, Netzwerksitzungen usw. anzuzeigen.
- **QUELLE**: Wählen Sie eine oder mehrere Quellen aus, um die von diesen Quellen ausgelösten Warnmeldungen anzuzeigen. Zum Beispiel: Möchten Sie lediglich die NetWitness Endpoint-Warnmeldung anzeigen, wählen Sie „Endpoint“ als Quelle aus.
- **SCHWEREGRAD**: Wählen Sie den Schweregrad der anzuzeigenden Warnmeldungen aus. Die Werte liegen zwischen 1 und 100. Um sich beispielsweise zunächst auf die Warnmeldungen mit dem höchsten Schweregrad zu konzentrieren, können Sie nur die Warnmeldungen mit einem Schweregrad von 90 bis 100 anzeigen.
- **ZUM INCIDENT GEHÖRIG**: Wählen Sie **Nein** aus, um nur Warnmeldungen anzuzeigen, die nicht Teil eines Incident sind. Wählen Sie **Ja** aus, um nur Warnmeldungen anzuzeigen, die Teil eines Incident sind. Wenn Sie beispielsweise bereit sind, einen Incident aus einer Gruppe von Warnmeldungen zu erstellen, können Sie „Nein“ auswählen, um nur die Warnmeldungen anzeigen, die derzeit nicht Teil eines Incident sind.
- **WARNMELDUNGSNAMEN**: Wählen Sie den Namen der anzuzeigenden Warnmeldung aus. Sie können diesen Filter verwenden, um nach allen Warnmeldungen zu suchen, die durch eine bestimmte Regel oder Quelle erzeugt wurden, z. B. schädliche IP - Reporting Engine.

In der Warnmeldungsliste wird eine Liste der Warnmeldungen angezeigt, die Ihre Auswahlkriterien erfüllen. Sie finden die Anzahl der Elemente in der gefilterten Liste am unteren Rand der Warnmeldungsliste.
Beispiel: **30 von 30 Elementen werden angezeigt**

3. Wenn Sie den Bereich „Filter“ schließen möchten, klicken Sie auf **X**. Ihre Filter werden beibehalten, bis Sie sie entfernen.

Entfernen meiner Filter aus der Warnmeldungsliste

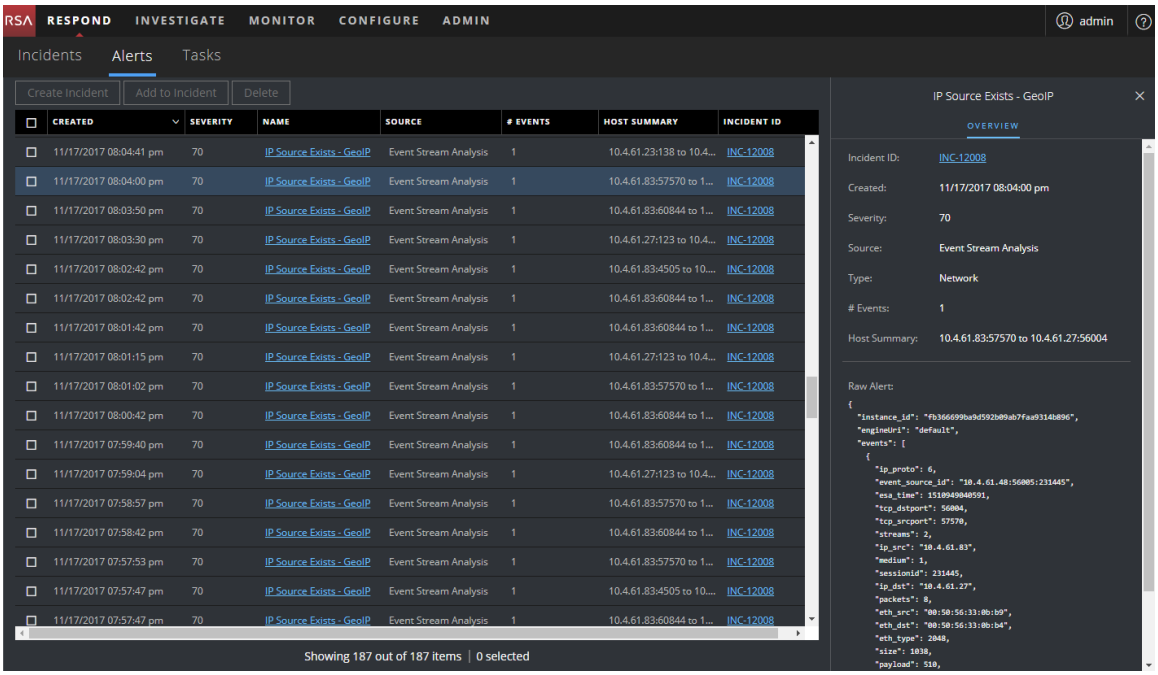
NetWitness Suite erinnert sich an Ihre Filterauswahl in der Listenansicht „Warnmeldungen“. Sie können Ihre Filterauswahl entfernen, wenn Sie sie nicht mehr benötigen. Wenn Sie beispielsweise nicht die erwartete Anzahl an Warnmeldungen sehen oder Sie alle Warnmeldungen in der Warnmeldungsliste anzeigen möchten, können Sie Ihre Filter zurücksetzen.

1. Navigieren Sie zu **Reagieren > Warnmeldungen**.
   Der Bereich „Filter“ wird auf der linken Seite der Warnmeldungsliste angezeigt. Sollte der Bereich „Filter“ nicht angezeigt werden, klicken Sie in der Symbolleiste der Listenansicht der Warnmeldungen auf , woraufhin der Bereich „Filter“ geöffnet wird.
2. Klicken Sie am unteren Rand des Bereichs „Filter“ auf **Filter zurücksetzen**.

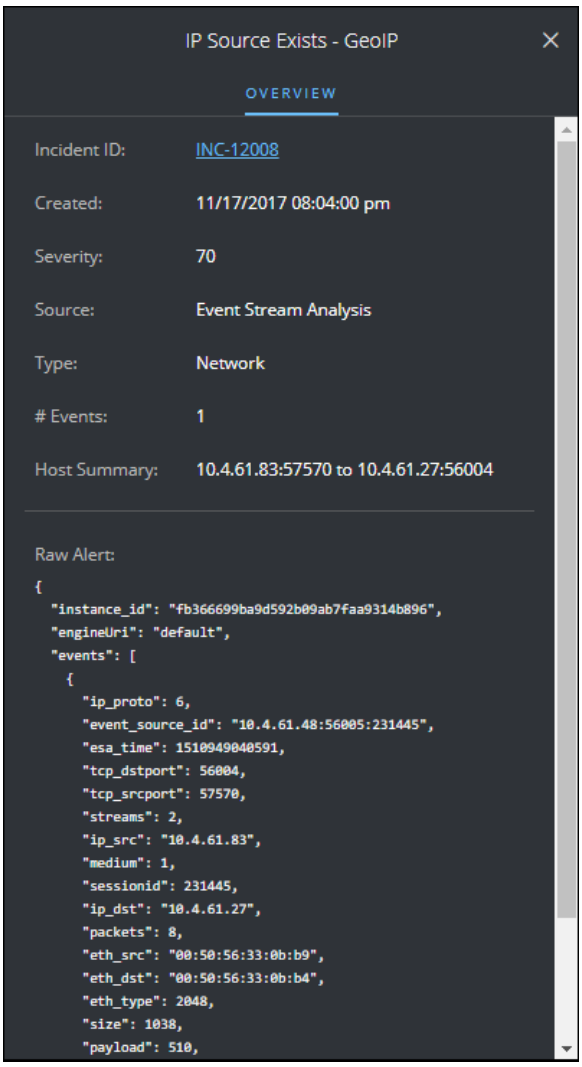
Anzeigen von Übersichtsinformationen zu Warnmeldungen

Zusätzlich zum Anzeigen von grundlegenden Informationen zu einer Warnmeldung können Sie auch Rohwarnmeldungs-Metadaten im Bereich „Übersicht“ anzeigen.

1. Klicken Sie in der Liste der Warnmeldungen auf die Warnmeldung, die Sie anzeigen möchten.
   Der Bereich „Übersicht über Warnmeldungen“ wird rechts neben der Liste der Warnmeldungen angezeigt.

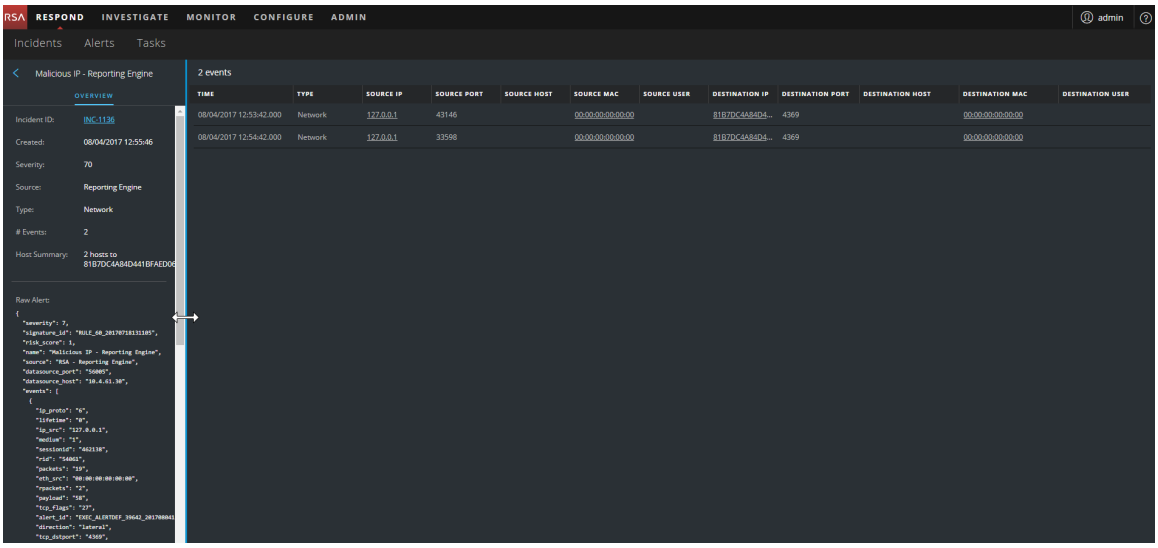

RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Incidents
Alerts
Tasks
Create Incident
Add to Incident
Delete
CREATED
SEVERITY
NAME
SOURCE
EVENTS
HOST SUMMARY
INCIDENT ID
11/17/2017 08:04:41 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.23:138 to 10.4... INC-12008
11/17/2017 08:04:00 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:57570 to 1... INC-12008
11/17/2017 08:03:50 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:60844 to 1... INC-12008
11/17/2017 08:03:30 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.27:123 to 10.4... INC-12008
11/17/2017 08:02:42 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:4505 to 10.... INC-12008
11/17/2017 08:02:42 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:60844 to 1... INC-12008
11/17/2017 08:01:42 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:60844 to 1... INC-12008
11/17/2017 08:01:15 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.27:123 to 10.4... INC-12008
11/17/2017 08:01:02 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:57570 to 1... INC-12008
11/17/2017 08:00:42 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:60844 to 1... INC-12008
11/17/2017 07:59:40 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:60844 to 1... INC-12008
11/17/2017 07:59:04 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.27:123 to 10.4... INC-12008
11/17/2017 07:58:57 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:57570 to 1... INC-12008
11/17/2017 07:58:42 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:60844 to 1... INC-12008
11/17/2017 07:57:53 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:57570 to 1... INC-12008
11/17/2017 07:57:47 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:4505 to 10.... INC-12008
11/17/2017 07:57:47 pm 70 IP Source Exists - GeoIP Event Stream Analysis 1 10.4.61.83:60844 to 1... INC-12008
Showing 187 out of 187 items | 0 selected
IP Source Exists - GeoIP
OVERVIEW
Incident ID: INC-12008
Created: 11/17/2017 08:04:00 pm
Severity: 70
Source: Event Stream Analysis
Type: Network
Events: 1
Host Summary: 10.4.61.83:57570 to 10.4.61.27:56004
Raw Alert:
{
"instance_id": "fb366699ba9d592b09ab7faa9314b896",
"engineUri": "default",
"events": [
{
"ip_proto": 6,
"event_source_id": "10.4.61.48:56005:231445",
"esa_time": 1510949040591,
"tcp_dstport": 56004,
"tcp_srcport": 57570,
"streams": 2,
"ip_src": "10.4.61.83",
"medium": 1,
"sessionid": 231445,
"ip_dst": "10.4.61.27",
"packets": 8,
"eth_src": "00:50:56:33:8b:b9",
"eth_dst": "00:50:56:33:8b:b4",
"eth_type": 2048,
"size": 1038,
"payload": 510,

2. Im Abschnitt „Rohwarnmeldung“ können Sie blättern, um die Rohwarnmeldungs-Metadaten anzuzeigen.



Anzeigen von Ereignisdetails für eine Warnmeldung

Nachdem Sie die allgemeinen Informationen über die Warnmeldung aus der Listenansicht „Warnmeldungen“ geprüft haben, können Sie in die Ansicht „Warnmeldungsdetails“ wechseln, um genauere Informationen zur Bestimmung der erforderlichen Aktion zu erhalten. Eine Warnmeldung enthält ein oder mehrere Ereignisse. In der Ansicht „Warnmeldungsdetails“ können Sie einen Drill-down in eine Warnmeldung durchführen, um zusätzliche Ereignisdetails zu erhalten und die Warnmeldung weiter zu untersuchen. Die folgende Abbildung zeigt ein Beispiel für die Ansicht „Warnmeldungsdetails“.



Der Bereich „Übersicht“ auf der linken Seite enthält dieselben Informationen für eine Warnmeldung wie der Bereich „Übersicht“ in der Ansicht „Warnmeldungsliste“.

Der Bereich „Ereignisse“ auf der rechten Seite zeigt Informationen zu den Ereignissen in der Warnmeldung, z. B. die Uhrzeit des Ereignisses, Quell-IP, Ziel-IP, Detektor-IP, Quellbenutzer, Zielbenutzer und Dateiinformationen zu den Ereignissen. Wie viele Informationen aufgeführt werden, hängt vom Typ des jeweiligen Ereignisses ab.

Es gibt zwei Typen von Ereignissen:

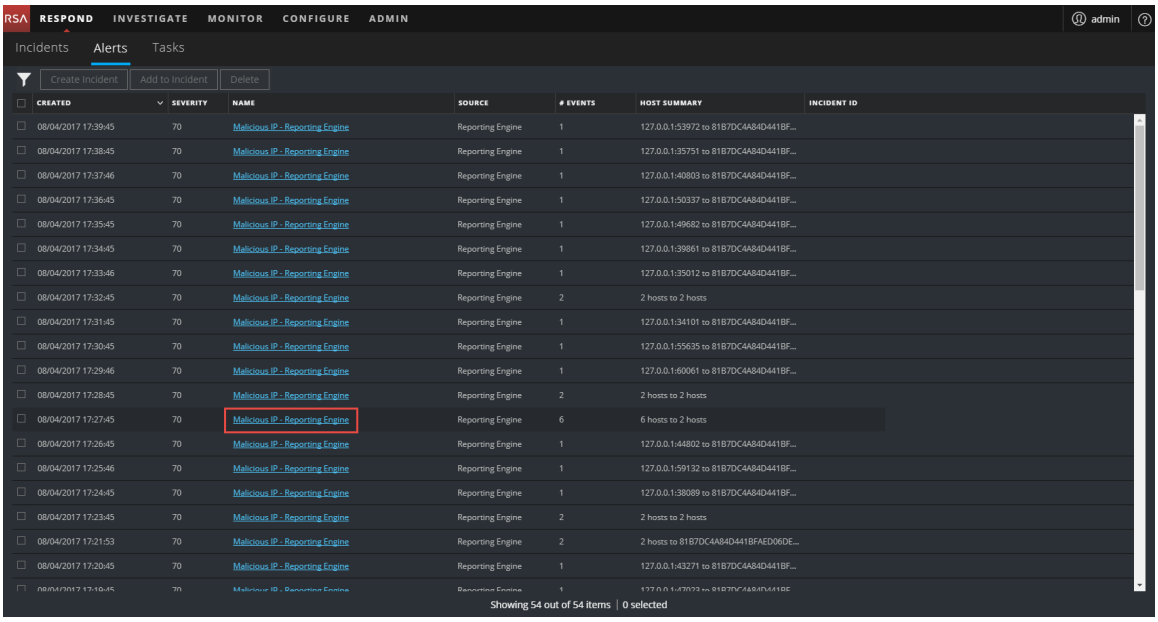
- Eine Transaktion zwischen zwei Rechnern (eine Quelle und ein Ziel)
- Eine auf einem einzelnen Rechner erkannte Anomalie (ein Detektor)

Einige Ereignisse haben nur einen Detektor. Mit NetWitness Endpoint wird z. B. Malware auf dem Rechner gefunden. Andere Ereignisse haben eine Quelle und ein Ziel. Paketdaten zeigen beispielsweise die Kommunikation zwischen Ihrem Rechner und einer Command-and-Control-Domain (C2).

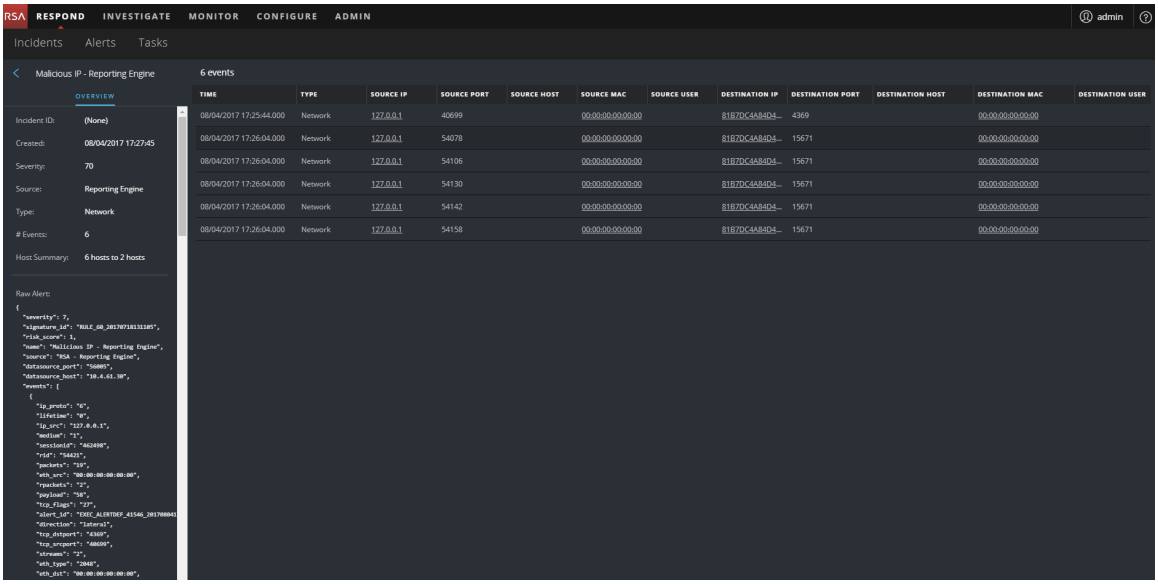
Sie können einen Drill-down in ein Ereignis durchführen, um detaillierte Daten über das Ereignis zu erhalten.

So zeigen Sie Ereignisdetails für eine Warnmeldung an:

1. Um Ereignisdetails für eine Warnmeldung anzuzeigen, wählen Sie in der Ansicht „Warnmeldungsliste“ eine anzuzeigende Warnmeldung aus und klicken Sie dann auf den Link in der Spalte „NAME“ für diese Warnmeldung.



Die Ansicht „Warnmeldungsdetails“ zeigt den Bereich „Übersicht“ auf der linken Seite und den Bereich „Ereignisse“ auf der rechten Seite.



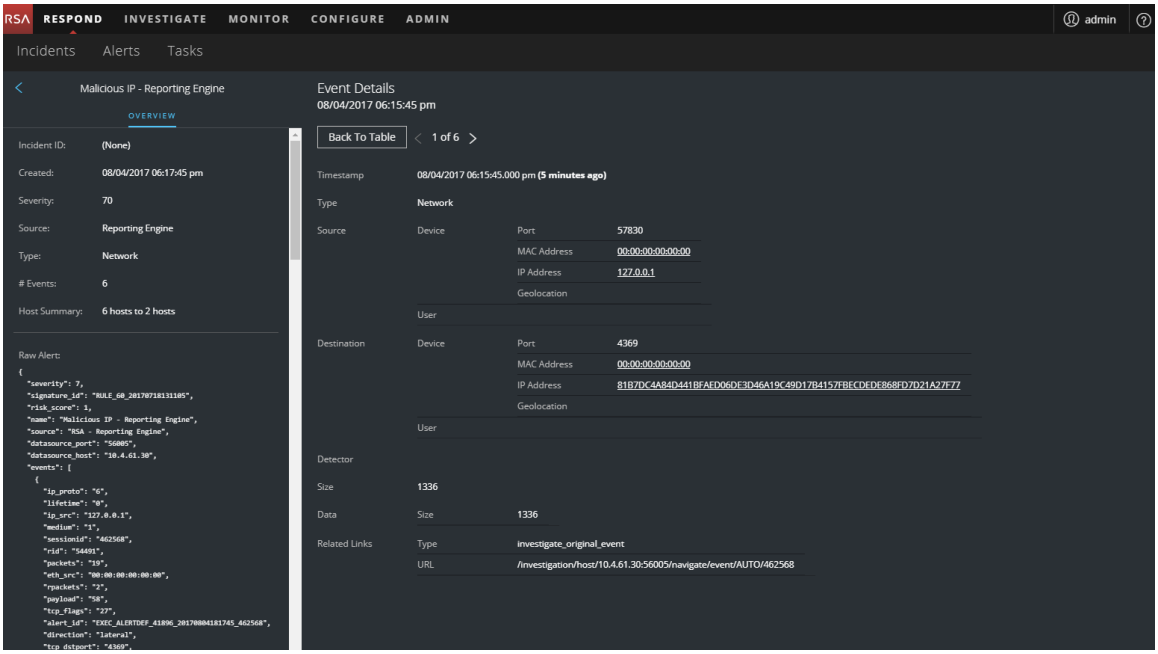
Der Bereich „Ereignisse“ zeigt eine Liste von Ereignissen mit Informationen zu jedem Ereignis. In der folgende Tabelle sehen Sie einige der Spalten, die in der Liste der Ereignisse (Ereignistabelle) angezeigt werden können.

Spalte	Beschreibung
ZEIT	Zeigt an, wann das Ereignis eingetreten ist.

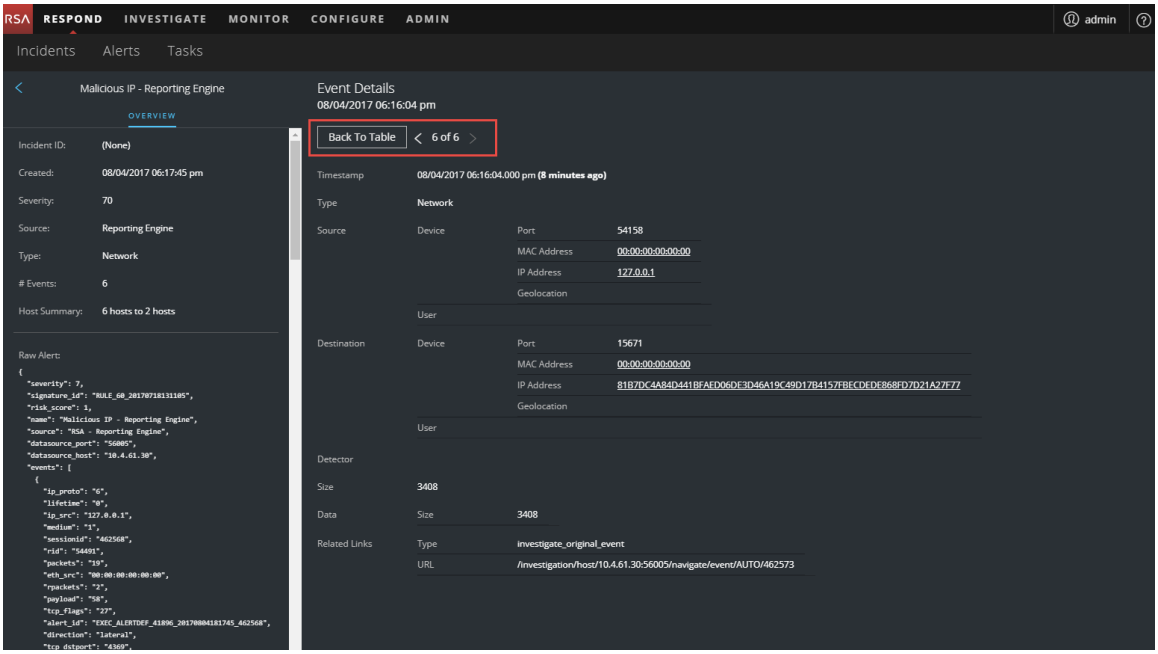
Spalte	Beschreibung
TYP	Zeigt den Typ der Warnmeldung an, z. B. „Protokoll“ oder „Netzwerk“.
QUELL-IP	Zeigt die Quell-IP-Adresse an, wenn eine Transaktion zwischen zwei Rechnern erfolgt ist.
Ziel-IP	Zeigt die Ziel-IP-Adresse an, wenn eine Transaktion zwischen zwei Rechnern erfolgt ist.
DETEKTOR-IP	Zeigt die IP-Adresse des Rechners an, auf dem eine Anomalie erkannt wurde.
QUELLBENUTZER	Zeigt den Benutzer des Quellrechners an.
ZIELBENUTZER	Zeigt den Benutzer des Zielrechners an.
DATEINAME	Zeigt den Dateinamen an, falls eine Datei in das Ereignis involviert ist.
DATEI-HASH	Zeigt einen Hash der Dateiinhalte an.

Wenn nur ein Ereignis in der Liste vorhanden ist, werden die Ereignisdetails für das betreffende Ereignis anstelle einer Liste angezeigt.

2. Klicken Sie auf ein Ereignis in der Ereignisliste, um die Ereignisdetails anzuzeigen. Dieses Beispiel zeigt die Ereignisdetails für das erste Ereignis in der Liste.



3. Verwenden Sie die Seitennavigation rechts neben der Schaltfläche „Zurück zu Tabelle“, um andere Ereignisse anzuzeigen. Dieses Beispiel zeigt die Ereignisdetails für das letzte Ereignis in der Liste.



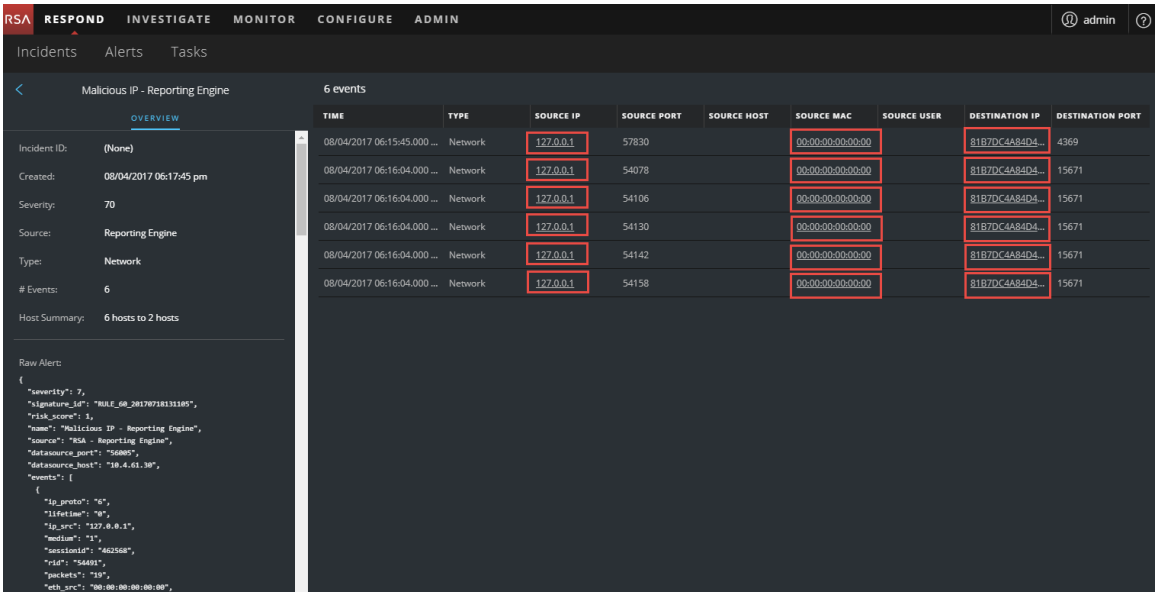
Detaillierte Informationen zu den Ereignisdaten im Bereich „Warnmeldungsdetails“ finden Sie unter Ansicht „Warnmeldungsdetails“.

Untersuchen von Ereignissen

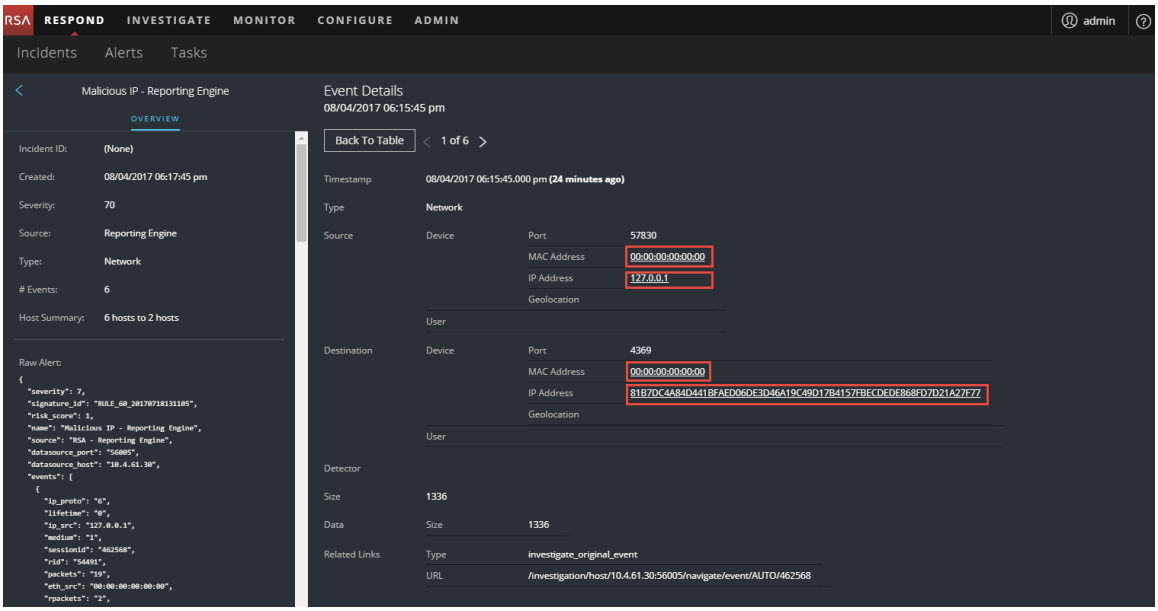
Um die Ereignisse näher zu untersuchen, finden Sie Links, die Sie zu zusätzlichen Kontextinformationen weiterleiten. Von dort stehen je nach Ihrer Auswahl Optionen zur Verfügung.

Anzeigen von kontextbezogenen Informationen

In der Ansicht „Warnmeldungsdetails“ sehen Sie unterstrichene Entitäten im Bereich „Ereignisse“. Eine unterstrichene Entität wird als eine Entität im Context Hub betrachtet und bietet zusätzliche verfügbare Kontextinformationen. Die folgende Abbildung zeigt unterstrichene Entitäten in der Ereignisliste.



Die folgende Abbildung zeigt unterstrichene Entitäten in den Ereignisdetails.

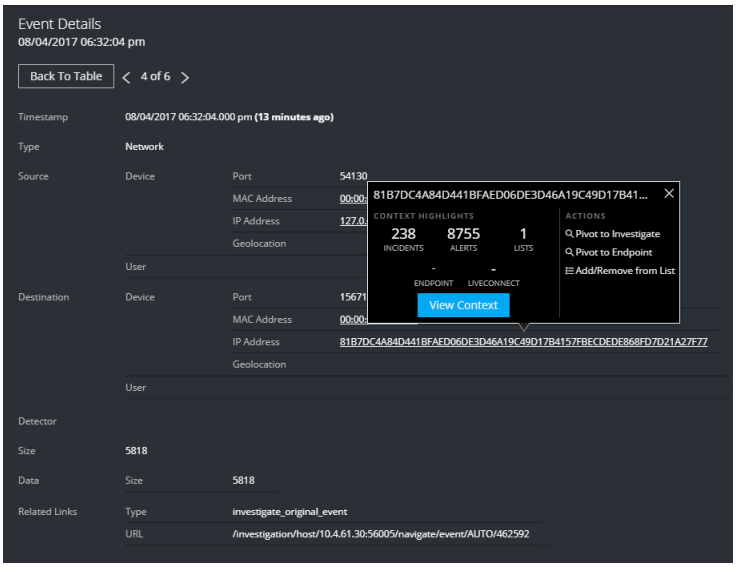


Der Context Hub ist mit Metadatenfeldern vorkonfiguriert, die den Entitäten zugeordnet sind. NetWitness Respond und Investigation nutzen diese Standardzuordnungen für die Kontextabfrage. Informationen zum Hinzufügen von Metaschlüsseln finden Sie unter „Konfigurieren von Einstellungen für eine Datenquelle“ im *Context Hub-Konfigurationsleitfaden*.

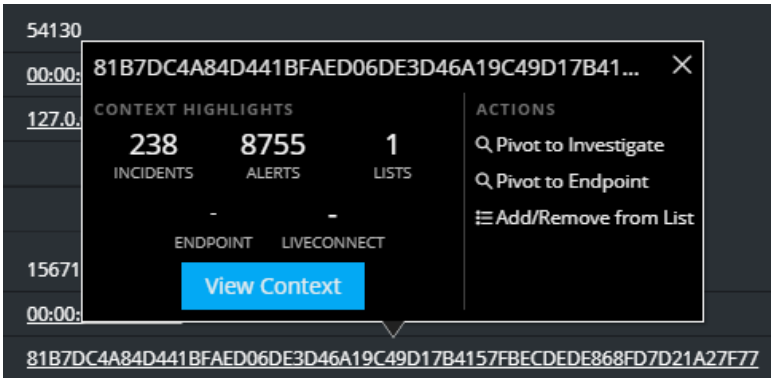
Achtung: Damit die Kontextabfrage in den Ansichten „Reagieren“ und „Untersuchen“ ordnungsgemäß funktioniert, empfiehlt RSA, dass Sie beim Zuordnen von Metaschlüsseln unter **ADMIN > SYSTEM > Ermittlung > Kontextabfrage** den Metaschlüsselzuordnungen nur Metaschlüssel hinzufügen, nicht Felder der MongoDB. Zum Beispiel ist „ip.address“ ein Metaschlüssel und „ip_address“ ist kein Metaschlüssel (es ist ein Feld in der MongoDB).

So zeigen Sie kontextbezogene Informationen an:

1. Bewegen Sie in der Ansicht „Warnmeldungsdetails“ in der Ereignisliste oder den Ereignisdetails die Maus über eine unterstrichene Entität.
   Eine Kontext-Kurzinformation wird mit einer kurzen Übersicht über den Typ der Kontextdaten, die für die ausgewählte Entität verfügbar sind, angezeigt.



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



Die Informationen im Abschnitt **Kontexthighlights** helfen Ihnen, die Aktionen zu bestimmen, die Sie durchführen möchten. Sie zeigen die Anzahl der verwandten Warnmeldungen und Incidents. Abhängig von Ihren Daten können Sie möglicherweise auf diese nummerierten Elemente klicken, um weitere Informationen anzuzeigen. Im obigen Beispiel werden 238 verwandte Incidents und 8.755 verwandte Warnmeldungen sowie 1 verwandte Context Hub-Liste angezeigt.

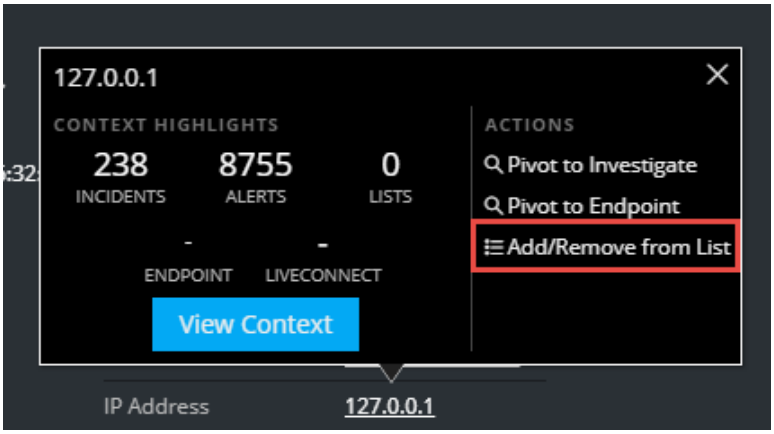
Im Abschnitt **Aktionen** werden die verfügbaren Aktionen aufgeführt. Im obigen Beispiel sind die Optionen „Zu Ermittlungen wechseln“, „Zu Endpoint wechseln“ und „Zu Liste hinzufügen/Aus Liste entfernen“ verfügbar.

2. Um weitere Details über die ausgewählte Entität anzuzeigen, klicken Sie auf die Schaltfläche **Kontext anzeigen**.
   Der Bereich „Kontext“ wird geöffnet und zeigt alle Informationen im Zusammenhang mit der Entität.
   Bereich „Kontextabfrage“ – Ansicht „Reagieren“ bietet zusätzliche Informationen.

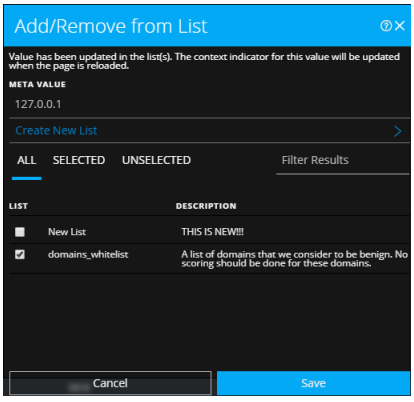
Hinzufügen einer Entität zu einer Whitelist

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

1. Bewegen Sie in der Ansicht „Warnmeldungsdetails“ in der Ereignisliste oder den Ereignisdetails die Maus über die unterstrichene Entität, die Sie einer Context Hub-Liste hinzufügen möchten.
   Eine Kontext-Kurzinformation wird geöffnet und zeigt die verfügbaren Aktionen.



2. Klicken Sie im Abschnitt **Aktionen** der Kurzinformation auf **Zu Liste hinzufügen/Aus Liste entfernen**.
   Im Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ werden die verfügbaren Listen angezeigt.



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

Erstellen einer Whitelist

Sie können eine Whitelist im Context Hub auf die gleiche Weise wie in der Ansicht „Incident-Details“ erstellen. Siehe Eine Liste erstellen.

Wechseln zum NetWitness Endpoint

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

1. Bewegen Sie in der Ereignisliste oder den Ereignisdetails in der Ansicht „Warnmeldungsdetails“ die Maus über eine unterstrichene Entität, um auf eine Kontext-Kurzinformation zuzugreifen.
2. Wählen Sie im Abschnitt **AKTIONEN** der Kurzinformation **Zu Endpoint wechseln**. Die NetWitness Endpoint-Thick-Clientanwendung wird außerhalb des Webbrowsers geöffnet.

Weitere Informationen zum Thick-Client finden Sie im *Benutzerhandbuch* für *NetWitness Endpoint*.

Zu Ermittlungen wechseln

Für eine eingehendere Untersuchung des Incident können Sie die Ansicht „Untersuchen“ aufrufen.

1. Bewegen Sie in der Ereignisliste oder den Ereignisdetails in der Ansicht „Warnmeldungsdetails“ die Maus über eine unterstrichene Entität, um auf eine Kontext-Kurzinformation zuzugreifen.
2. Wählen Sie im Abschnitt **AKTIONEN** der Kurzinformation **Zu Ermittlungen wechseln**. Die Ansicht „Untersuchen“ > „Navigation“ wird geöffnet, in der Sie eine umfassendere Untersuchung durchführen können.

Weitere Informationen finden Sie im *NetWitness Investigate – Benutzerhandbuch*.

Manuelles Erstellen eines Incident

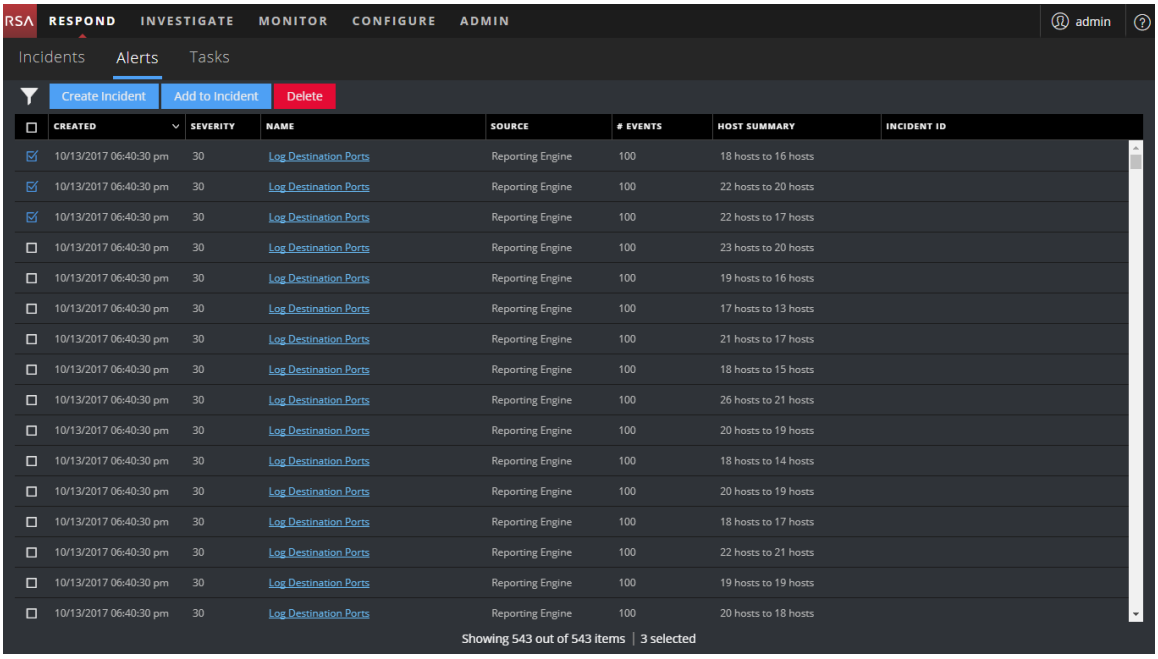
Sie können Incidents manuell aus Warnmeldungen in der Ansicht „Warnmeldungsliste“ erstellen. Die Warnmeldungen, die Sie auswählen, können nicht Teil eines anderen Incident sein. Incidents, die manuell aus Warnmeldungen erstellt wurden, erhalten standardmäßig niedrige Priorität, Sie können die Priorität jedoch nach der Erstellung ändern. Sie können keine Kategorien zu manuell erstellten Incidents hinzufügen.

Hinweis: Incidents können manuell oder automatisch erstellt werden. Eine Warnmeldung kann nur einem Incident zugeordnet werden. Sie können Incident-Regeln erstellen, mit denen die gesammelten Warnmeldungen abhängig von diesen Regeln in Incidents gruppiert werden. Weitere Informationen finden Sie im Thema „Erstellen einer Incident-Regel für Warnmeldungen“ im *NetWitness Respond – Konfigurationsleitfaden*.

So erstellen Sie einen Incident manuell:

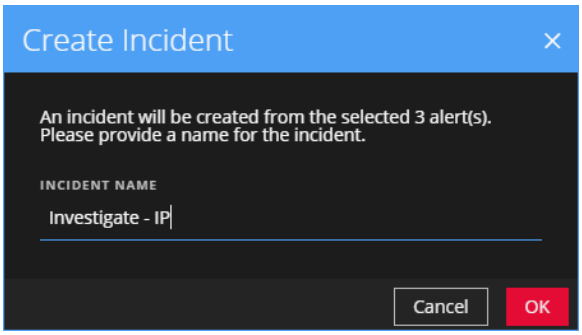
1. Navigieren Sie zu **Reagieren > Warnmeldungen**.
2. Wählen Sie eine oder mehrere Warnmeldungen in der Liste der Warnmeldungen aus.

   Hinweis: Durch das Auswählen von Warnmeldungen, die keine Incident-IDs besitzen, wird die Schaltfläche **Incident erstellen** aktiviert. Wenn die Warnmeldung bereits mit einem Incident verknüpft ist, wird die Schaltfläche deaktiviert. Sie können Warnmeldungen filtern, die nicht mit einem Incident verknüpft sind. Stellen Sie hierzu im Bereich „Filter“ die Option **ZUM INCIDENT GEHÖRIG** auf **Nein** ein.

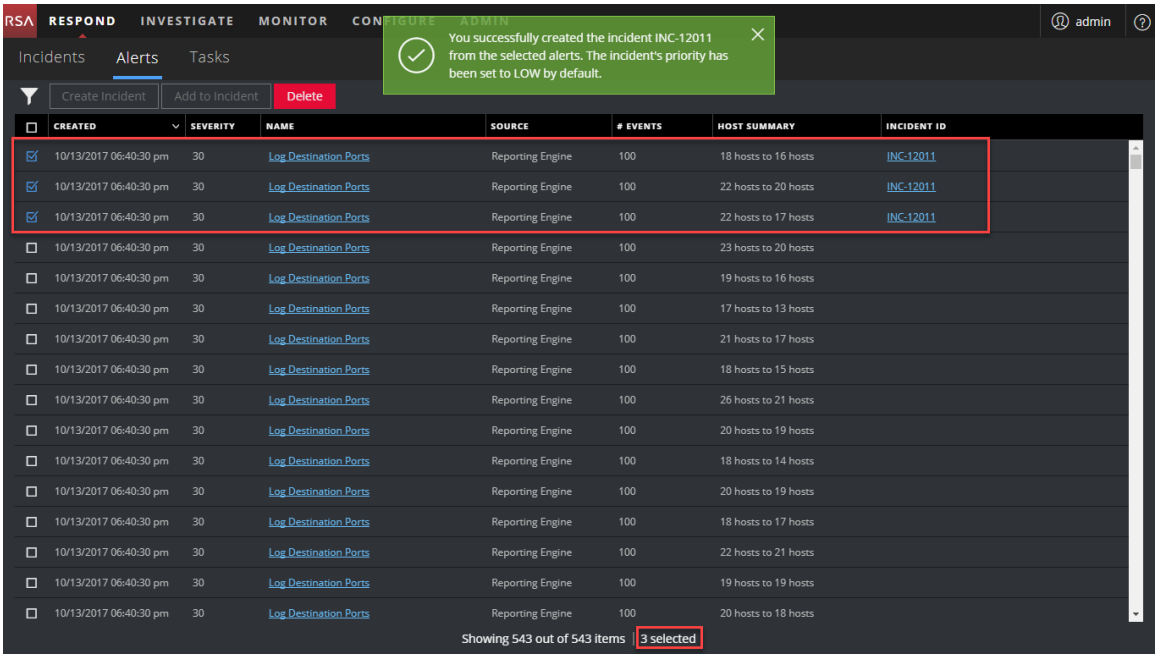


3. Klicken Sie auf **Incident erstellen**.

   Das Dialogfeld **Incident erstellen** wird angezeigt.



4. Geben Sie im Feld **INCIDENT-NAME** einen Namen zur Identifizierung des Incident ein. Zum Beispiel „Untersuchen – IP“.
5. Klicken Sie auf **OK**.



Sie sehen eine Bestätigungsmeldung darüber, dass ein Incident aus den ausgewählten Warnmeldungen erstellt wurde. Die neue Incident-ID wird als Link in der Spalte „INCIDENT-ID“ der ausgewählten Warnmeldungen angezeigt. Wenn Sie auf den Link klicken, gelangen Sie zu der Ansicht „Incident-Details“ für diesen Incident, in der Sie Informationen aktualisieren können, beispielsweise die Priorität von niedrig zu hoch ändern.

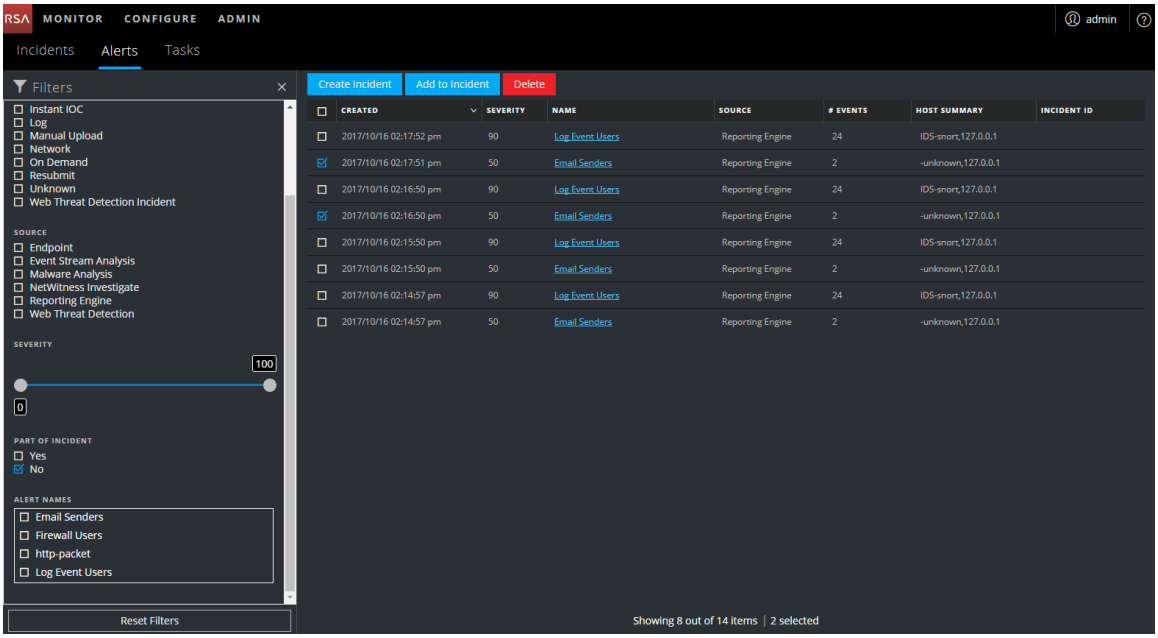
Warnmeldungen zu einem Incident hinzufügen

Hinweis: Diese Option ist nur für Version 11.1 und höher verfügbar.

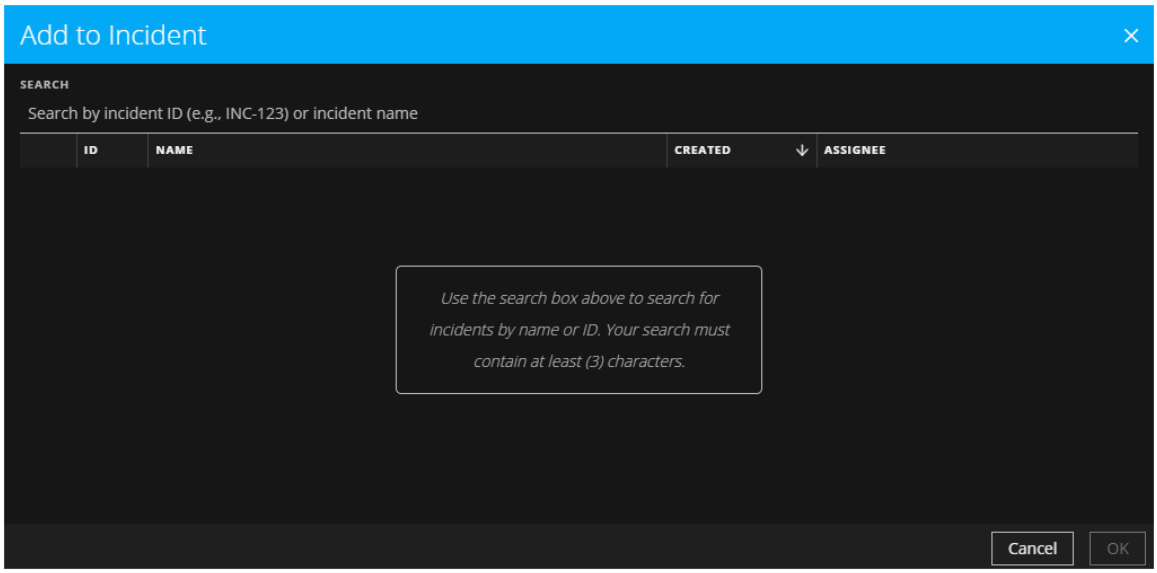
Wenn Sie Warnmeldungen haben, die zu einem bestimmten vorhandenen Incident passen, müssen Sie keinen neuen Incident erstellen. Stattdessen können Sie aus der Ansicht „Warnmeldungsliste“ Warnmeldungen zu diesem Incident hinzufügen. Die Warnmeldungen, die Sie auswählen, können nicht Teil eines anderen Incident sein.

1. Navigieren Sie zu **Reagieren > Warnmeldungen**.
2. Wählen Sie in der Liste der Warnmeldungen eine oder mehrere Warnmeldungen aus, die Sie zu einem Incident hinzufügen möchten, und klicken Sie auf **Einem Incident hinzufügen**.

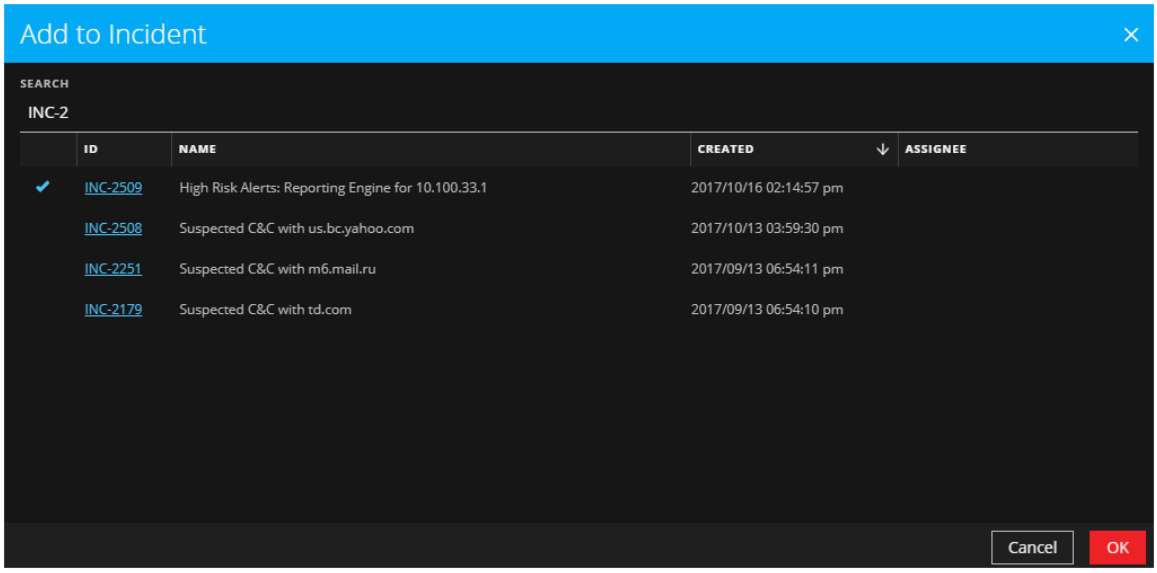
Hinweis: Durch das Auswählen von Warnmeldungen, die keine Incident-IDs besitzen, wird die Schaltfläche **Einem Incident hinzufügen** aktiviert. Wenn die Warnmeldung bereits mit einem Incident verknüpft ist, wird die Schaltfläche deaktiviert. Sie können Warnmeldungen filtern, die nicht mit einem Incident verknüpft sind. Stellen Sie hierzu im Bereich „Filter“ die Option **ZUM INCIDENT GEHÖRIG** auf **Nein** ein.



3. Geben Sie im Dialogfeld **Einem Incident hinzufügen** im Feld **Suchen** mindestens drei Zeichen ein, um über den **Namen** oder die **Incident-ID** nach dem Incident zu suchen.



4. Wählen Sie in der Ergebnisliste den Incident aus, der die ausgewählten Warnmeldungen empfangen soll, und klicken Sie auf **OK**.

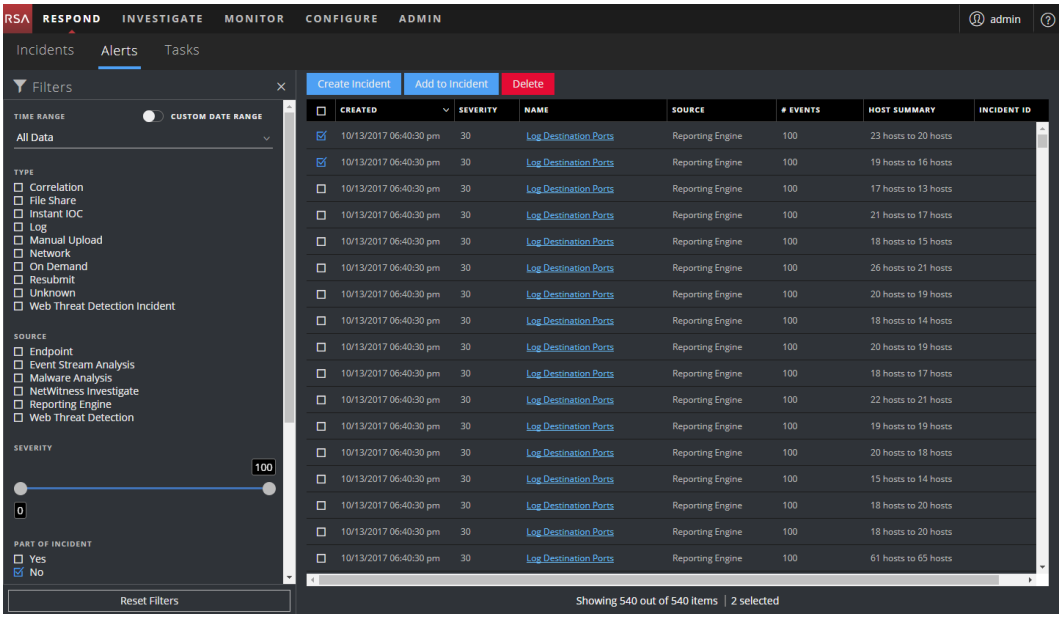


Die ausgewählten Warnmeldungen gehören nun zum ausgewählten Incident und besitzen dessen Incident-ID.

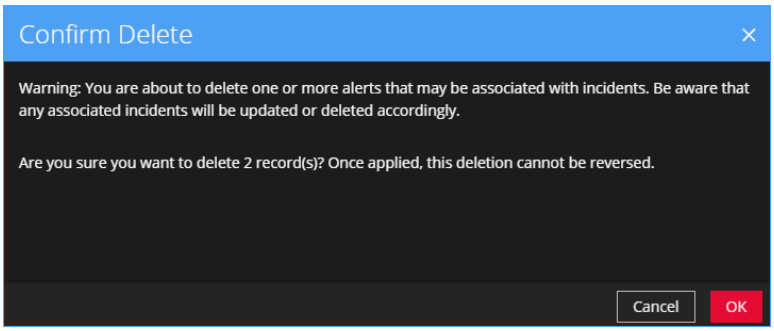
Löschen von Warnmeldungen

Benutzer mit den entsprechenden Berechtigungen, wie Administratoren und Datenschutzbeauftragte, können Warnmeldungen löschen. Dieses Verfahren ist hilfreich, wenn Sie unnötige oder nicht relevante Warnmeldungen entfernen möchten. Wenn Sie diese Warnmeldungen löschen, wird mehr Festplattenspeicher frei.

1. Navigieren Sie zu **Reagieren > Warnmeldungen**.
   Die Ansicht „Warnmeldungsliste“ zeigt eine Liste aller NetWitness Suite-Warnmeldungen.
2. Wählen Sie in der Liste der Warnmeldungen die Warnmeldungen aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.



   Wenn Sie keine Berechtigung zum Löschen von Warnmeldungen haben, wird die Schaltfläche „Löschen“ nicht angezeigt.
3. Bestätigen Sie, dass Sie die Warnmeldungen löschen möchten, und klicken Sie auf **OK**.



   Die Warnmeldungen werden aus NetWitness Suite gelöscht. Wenn eine gelöschte Warnmeldung die einzige in einem Incident war, wird der Incident ebenfalls gelöscht. Wenn

mehrere gelöschte Warnmeldungen in einem Incident vorhanden waren, wird der Incident entsprechend aktualisiert.

NetWitness Respond-Referenzinformationen

Die Benutzeroberfläche der Ansicht „Reagieren“ bietet Zugriff auf NetWitness Respond-Funktionen. Dieses Thema enthält Beschreibungen der Benutzeroberflächen sowie andere Referenzinformationen zum besseren Benutzerverständnis der Funktionen von NetWitness Respond.

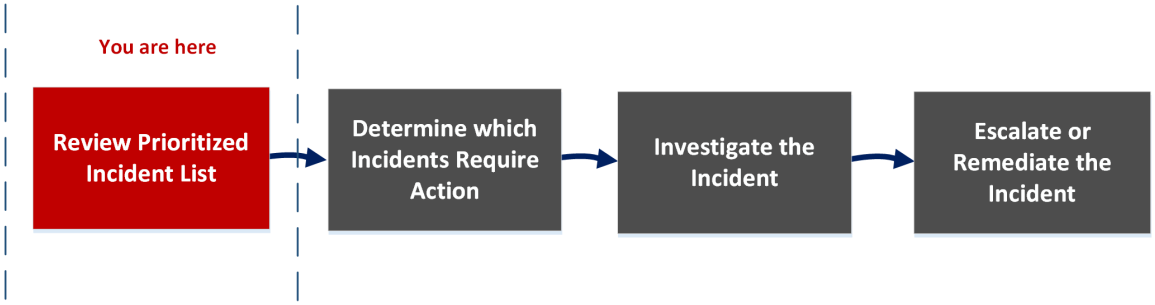
Themen

Incidents-Listenansicht

Die Incidents-Listenansicht (REAGIEREN > Incidents) gibt Incident-Experten und anderen Analysten eine priorisierte Ergebnisliste mit Incidents an die Hand, die von verschiedenen Quellen erstellt wurden. Ihre Ergebnisliste könnte beispielsweise Incidents enthalten, die auf Basis von ESA-Regeln, von NetWitness Endpoint oder von ESA Analytics-Modulen für Automatic Threat Detection erstellt wurden (z. B. C2 für Pakete oder Protokolle). Über die Incidents-Listenansicht haben Sie einfachen Zugriff auf alle nötigen Informationen, um Incidents schnell zu sichten, zu managen und endgültig zu beheben.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess, anhand dessen Incident-Experten in NetWitness Suite auf Incidents reagieren.



In der Ansicht „Incident-Liste“ können Sie die Liste priorisierter Incidents überprüfen. Dort finden Sie auch grundlegende Informationen zu den einzelnen Incidents. Sie haben zudem die Möglichkeit, Zuweisungsempfänger, Priorität und Status der Incidents zu ändern. Da die Incidents-Liste sehr viele Incidents enthalten kann, lassen sich die Incidents nach Zeitbereich, Incident-ID, benutzerdefiniertem Datumsbereich, Status, Zuweisungsempfänger und Kategorie filtern.

Was möchten Sie tun?

Rolle	Ziel	Anleitung
Incident-Experten, Analysten und SOC-Manager	Priorisierte Incidents anzeigen*	Überprüfen der Liste mit priorisierten Incidents
Incident-Experten, Analysten und SOC-Manager	Incident-Liste filtern und sortieren*	Filtern der Incident-Liste
Incident-Experten, Analysten	Eigene Incidents anzeigen*	Anzeigen eigener Incidents
Incident-Experten, Analysten	Sich selbst Incidents zuweisen	Zuweisen von Incidents an sich selbst
Incident-Experten, Analysten und SOC-Manager	Incidents suchen*	Suchen von Incidents
Incident-Experten, Analysten und SOC-Manager	Incident aktualisieren*	Eskalieren oder Korrigieren des Incident
Incident-Experten, Analysten	Incident-Details anzeigen	Ermitteln, welche Incidents eine Aktion erfordern
Incident-Experten, Analysten	Incident eingehender untersuchen	Untersuchen des Incident
Incident-Experten, Analysten und SOC-Manager	Aufgabe erstellen	Eskalieren oder Korrigieren des Incident

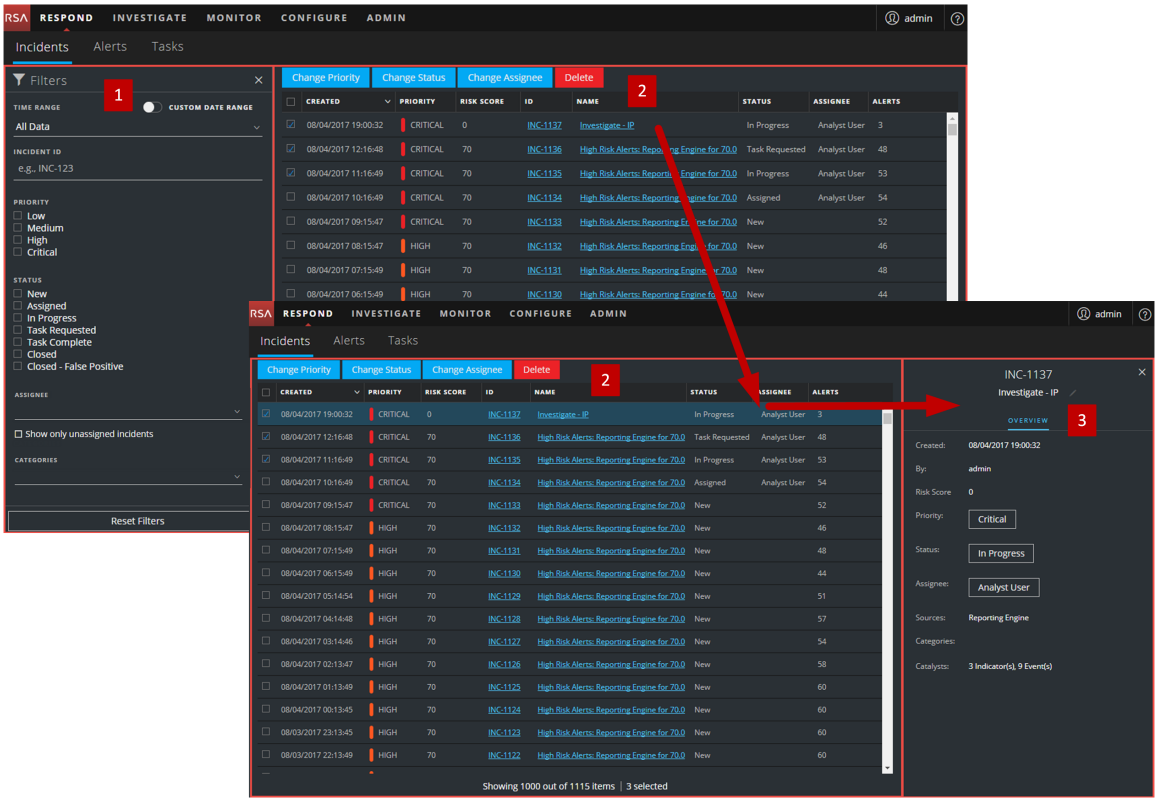
* Sie können diese Aufgaben in der aktuellen Ansicht (d. h. in der Incidents-Listenansicht) durchführen.

Verwandte Themen

- Incident-Detailansicht
- Reagieren auf Incidents

Überblick

Das folgende Beispiel zeigt die anfängliche Incidents-Listenansicht mit dem Bereich „Filter“. Durch Klicken auf einen Incident in der Incident-Liste können Sie den Bereich „Übersicht“ für den betreffenden Incident öffnen.



1 Bereich „Filter“

2 Incidents-Liste

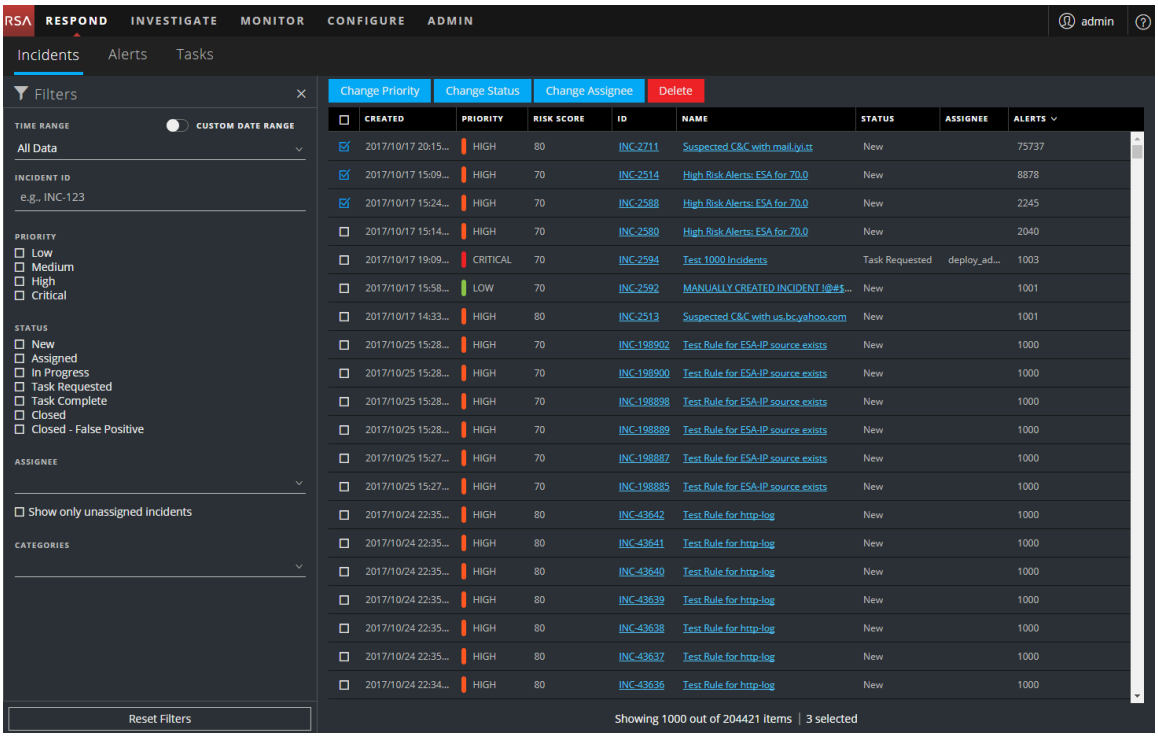
3 Bereich „Übersicht“

Durch Klicken auf die Links in den Spalten „ID“ und „NAME“ können Sie direkt aus der Incidents-Liste heraus die Detailansicht eines Incident aufrufen. Der Bereich „Übersicht“ steht auch in der Incident-Detailansicht zur Verfügung. Weitere Informationen über die Incident-Detailansicht finden Sie unter Incident-Detailansicht.

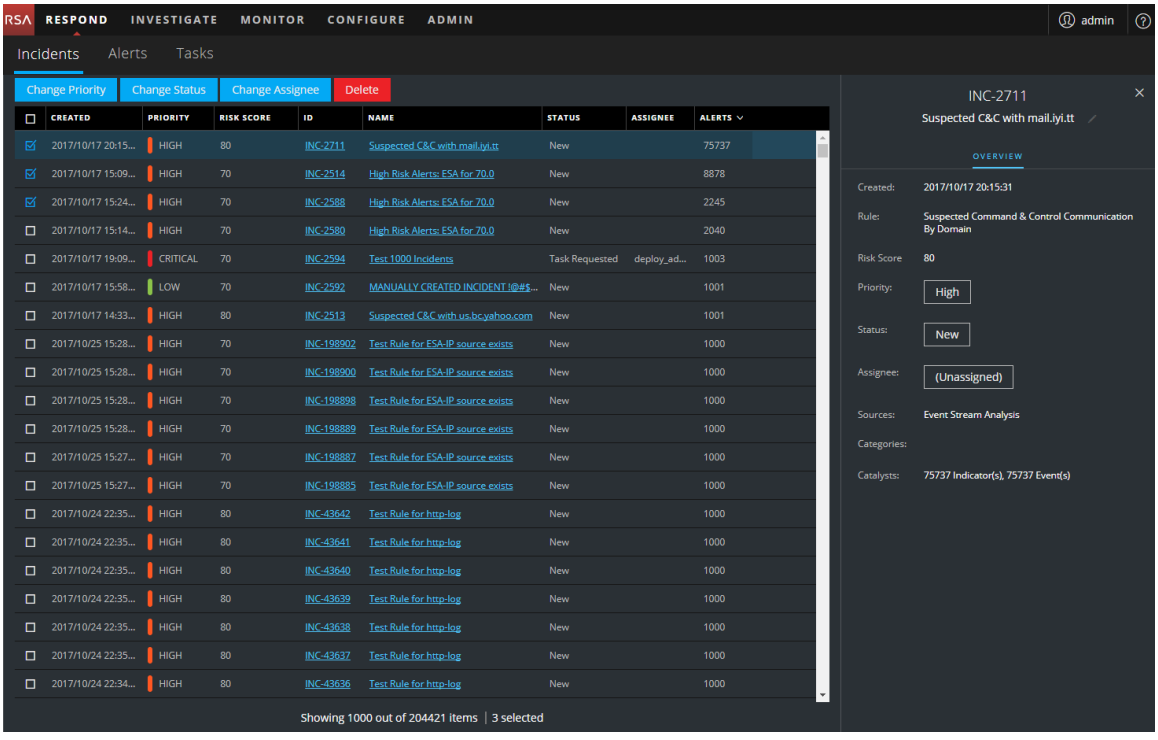
Incidents-Listenansicht

Zum Öffnen der Incidents-Listenansicht klicken Sie auf **Reagieren > Incidents**. In der Incidents-Listenansicht wird eine Liste sämtlicher Incidents angezeigt. Die Incidents-Listenansicht besteht aus dem Bereich „Filter“, einer Liste von Incidents und einem Bereich „Übersicht“ für die einzelnen Incidents.

Auf der Abbildung unten sehen Sie links den Bereich „Filter“ und rechts die Incident-Liste.

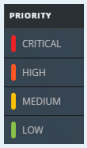


Auf der Abbildung unten sehen Sie links die Incident-Liste und rechts den Bereich „Incident-Übersicht“.



Incidents-Liste

In der Incidents-Liste werden alle priorisierten Incidents aufgeführt. Sie können diese Liste so filtern, dass nur die Incidents angezeigt werden, die für Sie von Interesse sind.

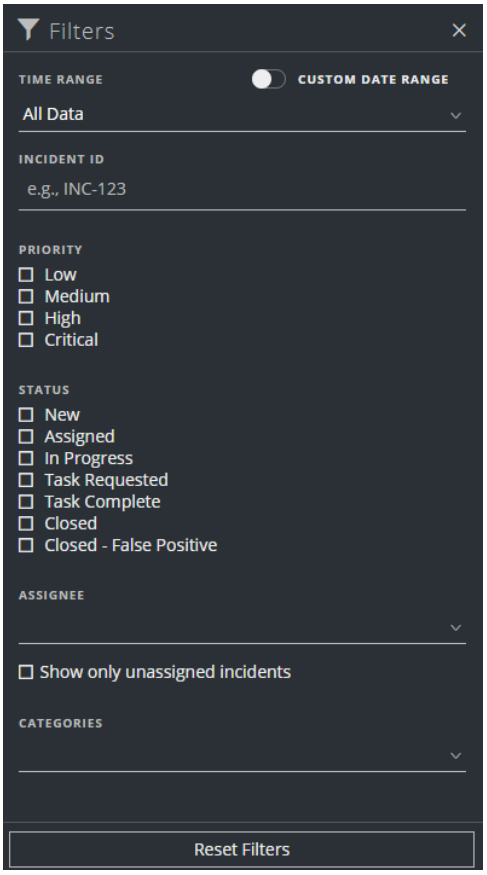
Spalte	Beschreibung
CREATED	Zeigt das Erstellungsdatum des Incident an.
PRIORITÄT	Zeigt die Priorität des Incident an. Die Priorität kann „Kritisch“, „Hoch“, „Mittel“ oder „Niedrig“ sein. Für die Priorität wird ein Farbcode verwendet: Rot kennzeichnet einen Incident als **Kritisch**, Orange steht für Incidents mit der Risikobewertung **Hoch**, Gelb für Incidents mit der Risikobewertung**Mittel** und Grün für Incidents mit der Risikobewertung **Niedrig**. Beispiel: 
RISIKOWERT	Zeigt den Risikowert des Incident an. Der Risikowert gibt das Risikopotenzial des Incident an. Er wird mittels eines Algorithmus berechnet und liegt zwischen 0 und 100. 100 ist der höchste Risikowert.
ID	Zeigt die automatisch erstellte Incident-Nummer an. Jedem Incident wird eine eindeutige Nummer zugewiesen, anhand derer Sie den Incident nachverfolgen können.
NAME	Zeigt den Namen des Incident an. Der Incident-Name leitet sich aus der Regel ab, die den Incident ausgelöst hat. Durch Klicken auf den Link können Sie die Detailansicht des jeweils ausgewählten Incident aufrufen.
STATUS	Zeigt den Status des Incident an. Mögliche Status sind: „Neu“, „Zugewiesen“, „Läuft“, „Aufgabe angefordert“, „Aufgabe abgeschlossen“, „Geschlossen“ und „Geschlossen – falsch positives Ergebnis“.

Spalte	Beschreibung
ZUWEISUNGSEMPFÄNGER	Zeigt das Teammitglied an, dem der Incident derzeit zugewiesen ist.
WARNMELDUNGEN	Zeigt an, wie viele Warnmeldungen dem Incident zugeordnet sind. Ein Incident kann viele Warnmeldungen enthalten. Eine große Anzahl von Warnmeldungen kann auf einen großflächigen Angriff hindeuten.

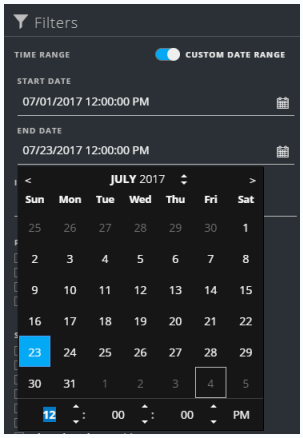
Am unteren Rand der Liste sehen Sie die Anzahl der Incidents auf der aktuellen Seite, die Gesamtzahl der Incidents und die Anzahl der ausgewählten Incidents. Beispiel: **1.000 von 2.517 Elementen werden angezeigt | 2 ausgewählt**. Es können maximal 1.000 Incidents gleichzeitig angezeigt werden.

Bereich „Filter“

Auf der Abbildung unten sehen Sie die im Bereich „Filter“ verfügbaren Filter.



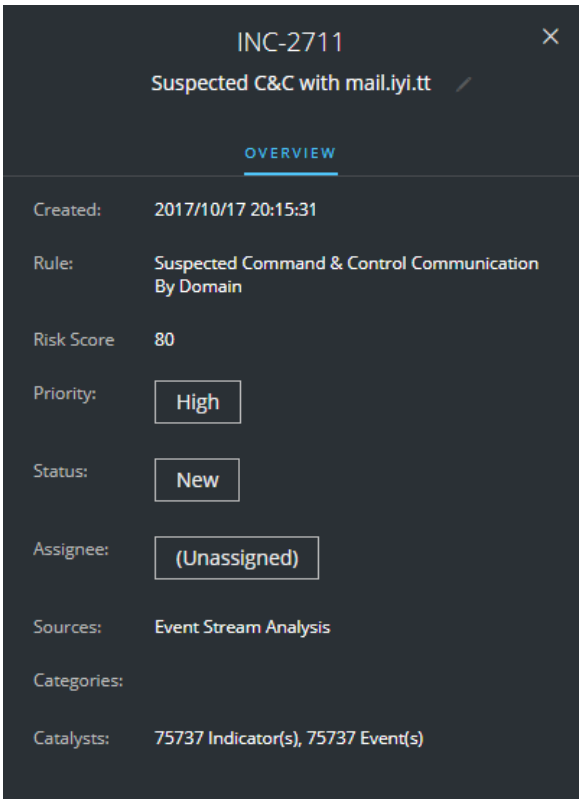
Im Bereich „Filter“ links neben der Ansicht „Incident-Liste“ stehen Optionen zur Verfügung, mit denen Sie die Incident-Liste filtern können. Wenn Sie den Bereich „Filter“ verlassen, werden die ausgewählten Filter für die Incidents-Listenansicht beibehalten.

Option	Beschreibung
ZEITBEREICH	Sie können einen bestimmten Zeitraum aus der Drop-down-Liste „Zeitbereich“ auswählen. Der Zeitbereich basiert auf dem Datum, an dem die Warnmeldungen empfangen wurden. Wenn Sie zum Beispiel „Letzte Stunde“ auswählen, werden die Warnmeldungen angezeigt, die innerhalb der letzten 60 Minuten empfangen wurden.
BENUTZERDEFINIERTER DATUMSBEREICH	Sie können einen bestimmten Datumsbereich anstelle der Option „Zeitbereich“ auswählen. Klicken Sie dazu auf den weißen Kreis vor „Benutzerdefinierter Datumsbereich“, damit die Felder „Startdatum“ und „Enddatum“ angezeigt werden. Wählen Sie die Datums- und Zeitangaben im Kalender aus. 
Incident-ID	Hier können Sie die Incident-ID des Incident eingeben, den Sie suchen, zum Beispiel „INC-1050“.
PRIORITÄT	Hier können Sie festlegen, Incidents welcher Priorität angezeigt werden sollen.

Option	Beschreibung
STATUS	Hier können Sie einen oder mehrere Incident-Status auswählen. Wenn Sie beispielsweise „Geschlossen – falsch positives Ergebnis“ auswählen, werden nur falsch positive Incidents angezeigt, also Incidents, die zunächst als verdächtigt eingestuft, dann aber als sicher bestätigt wurden.
ZUWEISUNGSEMPFÄNGER	Hier können Sie einen oder mehrere Zuweisungsempfänger auswählen, deren Incidents Sie anzeigen möchten. Sollen beispielsweise nur die Incidents angezeigt werden, die Cale oder Stanley zugewiesen sind, wählen Sie „Cale“ und „Stanley“ in der Drop-down-Liste „Zuweisungsempfänger“ aus. Lassen Sie die Auswahl unter „Zuweisungsempfänger“ frei, wenn die Incidents unabhängig von ihrem Zuweisungsempfänger angezeigt werden sollen. (Verfügbar in Version 11.1 und neueren Versionen) Wenn Sie nur Incidents anzeigen möchten, die nicht zugewiesen sind, wählen Sie **Nur nicht zugewiesene Incidents anzeigen** aus.
KATEGORIEN	Aus dieser Drop-down-Liste können Sie eine oder mehrere Kategorien auswählen. Wenn Sie beispielsweise nur Incidents der Kategorien „Backdoor“ oder „Rechtemissbrauch“ anzeigen möchten, müssen Sie „Backdoor“ und „Rechtemissbrauch“ auswählen.
Filter zurücksetzen	Entfernt die Filterauswahl.

Bereich „Übersicht“

Im Bereich „Übersicht“ finden Sie grundlegende Übersichtsinformationen zu dem jeweils ausgewählten Incident. In der Incident-Liste haben Sie die Möglichkeit, einen Incident anzuklicken, um auf den Bereich „Übersicht“ zuzugreifen. Der Bereich „Übersicht“ in der Ansicht „Incident-Details“ enthält dieselben Informationen.



In der folgenden Tabelle sind die Felder im Bereich „Incident-Übersicht“ aufgelistet.

Feld	Beschreibung
<Incident-ID>	Zeigt die ID des Incident an.
<Incident-Name>	Zeigt den Namen des Incident an. Klicken Sie auf den Incident-Namen, wenn Sie ihn ändern möchten. Regeln beispielsweise erstellen unter Umständen viele Incidents mit identischem Namen. Dann können Sie die Namen der Incidents, um sie eindeutiger zu kennzeichnen.
Erstellt	Zeigt Datum und Uhrzeit der Erstellung des Incident an.
Regel/Von	Zeigt den Namen der Regel an, die den Incident erstellt hat, oder den Namen der Person, die den Incident erstellt hat.

Feld	Beschreibung
Risikowert	Gibt das Risikopotenzial des Incidents an. Es wird mittels eines Algorithmus berechnet und liegt zwischen 0 und 100. 100 ist der höchste Risikowert.
Priorität	Zeigt die Priorität des Incident an. Die Priorität kann „Kritisch“, „Hoch“, „Mittel“ oder „Niedrig“ sein. Wenn Sie die Priorität ändern möchten: Klicken Sie auf die Schaltfläche der Priorität und wählen Sie eine neue Priorität aus der Drop-down-Liste aus.
Status	Zeigt den Status des Incident an. Der Status kann „Neu“, „Zugewiesen“, „Läuft“, „Aufgabe angefordert“, „Aufgabe abgeschlossen“, „Geschlossen“ und „Geschlossen – falsch positives Ergebnis“ lauten. Wenn Sie den Status ändern möchten: Klicken Sie auf die Schaltfläche des Status und wählen Sie einen neuen Status aus der Drop-down-Liste aus.
Zuweisungsempfänger	Zeigt das Teammitglied an, dem der Incident derzeit zugewiesen ist. Wenn Sie den Zuweisungsempfänger ändern möchten: Klicken Sie auf die Schaltfläche des Zuweisungsempfängers und wählen Sie einen neuen Zuweisungsempfänger aus der Drop-down-Liste aus.
Quellen	Zeigt die Datenquellen, die zur Lokalisierung der verdächtigen Aktivität verwendet wurden.
Kategorien	Zeigt die Kategorien der Incident-Ereignisse an.
Katalysatoren	Zeigt an, wie viele Indikatoren zur Erfassung des Incidents geführt haben.

Symbolleistenaktionen

In dieser Tabelle werden die Aktionen aufgeführt, die in der Symbolleiste der Incidents-Listenansicht verfügbar sind.

Option	Beschreibung
	Öffnet den Bereich „Filter“, in dem Sie festlegen können, welche Incidents in der Incident-Liste angezeigt werden sollen
	Schließt den Bereich
Schaltfläche **Priorität ändern**	Ermöglicht die Änderung der Prioität eines oder mehrerer ausgewählter Incidents in der Incidents-Liste.
Schaltfläche **Status ändern**	Ermöglicht die Änderung des Status eines oder mehrerer ausgewählter Incidents.
Schaltfläche **Zuweisungsempfänger ändern**	Ermöglicht die Änderung des Zuweisungsempfängers eines oder mehrerer ausgewählter Incidents.
Schaltfläche **Löschen**	Löscht die ausgewählten Incidents, die entsprechenden Berechtigungen vorausgesetzt (z. B. Administrator oder Datenschutzbeauftragter).

Incident-Detailansicht

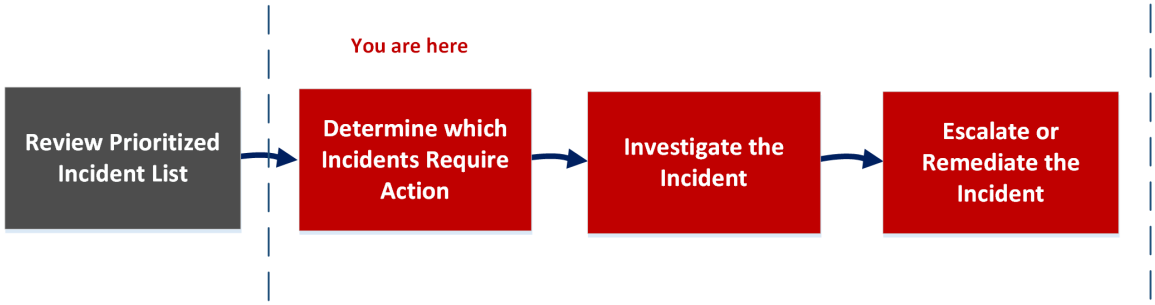
In der Incident-Detailansicht haben Sie Zugriff auf umfassende Details zu einem Incident (Zugriff: „REAGIEREN“ > „Incidents“ > Klick auf den gewünschten Link in der Spalte „ID“ oder „NAME“ der Incident-Liste). Die Incident-Detailansicht besteht aus verschiedenen Bereichenmit unterschiedlichen Informationen:

- **Übersicht**: Hier finden Sie eine Zusammenfassung des Incident und können ihn aktualisieren.
- **Indikatoren**: Hier finden Sie alle zu dem betreffenden Incident gehörenden Indikatoren (Warnmeldungen) sowie die Ereignisse in diesen Warnmeldungen und die verfügbaren Erweiterungsinformationen.
- **Node-Diagramm**: Hier finden Sie eine Visualisierung der Größe von Entitäten (IP-Adresse, MAC-Adresse, Benutzer, Host, Domain, Dateiname oder Datei-Hash) sowie ihrer Interaktionen.
- **Ereignisdatenblatt**: Hier findenn Sie die Ereignisse, die dem Incident zugeordnet sind.
- **Journal**: Hier können Sie Hinweise vermerken und mit anderen Analysten zusammenarbeiten.
- **Aufgaben**: Hier können Sie Incident-Aufgaben erstellen und bis zu ihrem Abschluss nachverfolgen.
- **Zugehörige Indikatoren**: Hier finden Sie mit dem Incident in Zusammenhang stehende Indikatoren (Warnmeldungen). Indikatoren, die noch keinem Incident zugeordnet sind, lassen sich hier zu einem Incident hinzufügen.

Die Daten in der Detailansicht eines Incident lassen sich auch filtern, sodass Sie sich nur auf die Indikatoren und Entitäten beschränken können, die für Sie von Interesse sind.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess, anhand dessen Incident-Experten in NetWitness Suite auf Incidents reagieren.



Anhand der ausführlichen Incident-Informationen, die in der Incident-Detailansicht angezeigt werden, können Sie herausfinden, welche Incidents ein Eingreifen erfordern. Hier stehen alle nötigen Informatione und Tools zur Verfügung, um einen Incident zu untersuchen und anschließend zu eskalieren oder zu korrigieren.

Was möchten Sie tun?

Rolle	Ziel	Anleitung
Incident-Experten, Analysten und SOC-Manager	Priorisierte Incidents anzeigen, Incident-Liste filtern und sortieren, Incidents suchen, eigene Incidents anzeigen und sich selbst Incidents zuweisen	Überprüfen der Liste mit priorisierten Incidents
Incident-Experten, Analysten	Incident-Details anzeigen*	Anzeigen von Details des Incident
Incident-Experten, Analysten	Warnmeldungen und Erweiterungen anzeigen*	Anzeigen der Indikatoren und Erweiterungen
Incident-Experten, Analysten	Ereignisse anzeigen*	Anzeigen und Untersuchen der Ereignisse
Incident-Experten, Analysten	Grafische Darstellung der in Ereignisse involvierten Entitäten anzeigen*	Anzeigen und Untersuchen der an den Ereignissen beteiligten Entitäten
Incident-Experten, Analysten	Incident-Daten filtern*	Filtern der Daten in der Ansicht „Incident-Details“
Incident-Experten, Analysten	Incident-Anmerkungen anzeigen und hinzufügen*	Anzeigen von Incident-Anmerkungen und Dokumentmaßnahmen außerhalb von NetWitness
Incident-Experten, Analysten	Aufgaben anzeigen und erstellen*	Anzeigen der Aufgaben im Zusammenhang mit einem Incident und Erstellen einer Aufgabe
Incident-Experten, Analysten	Zugehörige Warnmeldungen anzeigen und dem Incident hinzufügen*	Suchen verwandter Indikatoren und Hinzufügen verwandter Indikatoren zum Incident

Rolle	Ziel	Anleitung
Incident-Experten, Analysten	Kontextbezogene Informationen aus Context Hub für einen Incident anzeigen*	Anzeigen von kontextbezogenen Informationen
Incident-Experten, Analysten	Entität zur Whitelist hinzufügen, um die Anzahl falsch positiver Ergebnisse zu reduzieren	Hinzufügen einer Entität zu einer Whitelist
Incident-Experten, Analysten	In das Modul „Investigation“ wechseln*	Zu Ermittlungen wechseln
Incident-Experten, Analysten	Zu NetWitness Endpoint wechseln*	Wechseln zum NetWitness Endpoint
Incident-Experten, Analysten	Incident aktualisieren oder schließen*	Aktualisieren eines Incident und Schließen eines Incident
Incident-Experten, Analysten und SOC-Manager	Alle Aufgaben anzeigen	Eskalieren oder Korrigieren des Incident
Incident-Experten, Analysten und SOC-Manager	Massenaktualisierung von Incidents und Aufgaben durchführen	Eskalieren oder Korrigieren des Incident

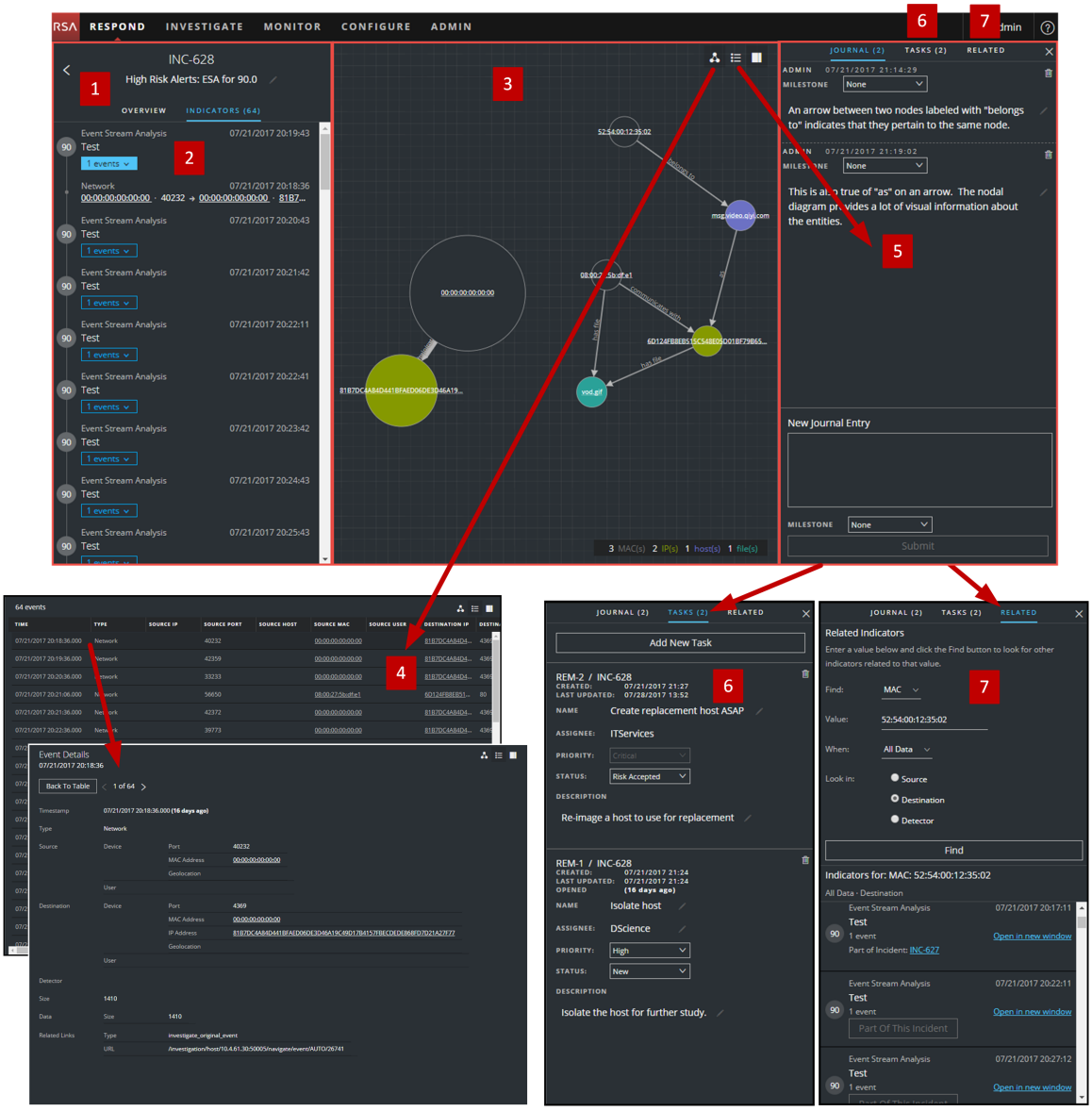
* Sie können diese Aufgaben in der aktuellen Ansicht (d. h. in der Incident-Detailansicht) durchführen.

Verwandte Themen

- Incidents-Listenansicht
- Ermitteln, welche Incidents eine Aktion erfordern
- Untersuchen des Incident
- Eskalieren oder Korrigieren des Incident

Überblick

Das folgende Beispiel zeigt, wo Sie die Bereich der Incident-Detailansicht finden.

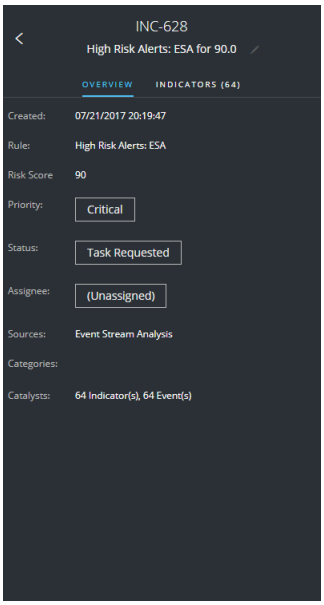


1	Bereich „Übersicht“ (Klicken Sie auf die Registerkarte „ÜBERSICHT“, um den Bereich aufzurufen.)
2	Bereich „Indikatoren“
3	Node-Diagramm
4	Ereignisdatenblatt (Klicken Sie auf ein Ereignis in der Ereignisliste, um die Ereignisdetails aufzurufen.)

5	Bereich „Journal“
6	Bereich „Aufgaben“ (Klicken Sie auf die Registerkarte „AUFGABEN“, um den Bereich aufzurufen.)
7	Bereich „Verwandte Indikatoren“ (Klicken Sie auf die Registerkarte „VERWANDT“, um den Bereich aufzurufen.)

Bereich „Übersicht“

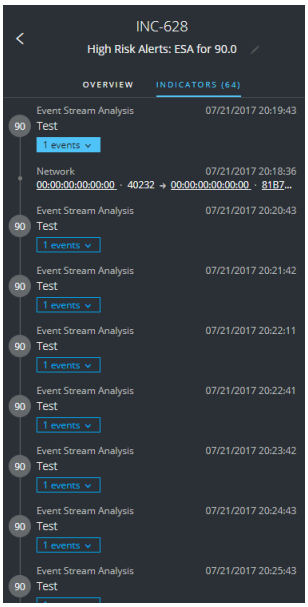
Im Bereich „Übersicht“ finden Sie grundlegende Übersichtsinformationen zu dem jeweils ausgewählten Incident. Hier können Sie außerdem den Namen des Incident ändern sowie die Incident-Priorität, den Incident-Status und den Zuweisungsempfänger für den Incident aktualisieren. Der Bereich „Übersicht“ in der Incident-Listenansicht enthält dieselben Informationen. Details hierzu finden Sie im Thema „Incident-Listenansicht“ im Abschnitt Bereich „Übersicht“.



Bereich „Indikatoren“

Der Bereich „Indikatoren“ enthält eine chronologische Liste aller Indikatoren. *Indikatoren* sind Warnmeldungen, z. B. ESA-Warnmeldungen oder NetWitness Endpoint-Warnmeldungen. (Es handelt sich hierbei nicht um eine Zeitleiste, die den zeitlichen Verlauf der Ereignisse in einem Incident visuell darstellt.) Diese Liste hilft Ihnen, Indikatoren und wichtige Daten zueinander in Beziehung zu setzen. Beispiel: Eine mit einer ESA-Command-and-Conquer-Warnmeldung in Zusammenhang stehende IP-Adresse könnte gleichzeitig auch eine NetWitness Endpoint-Warnmeldung oder andere verdächtige Aktivitäten ausgelöst haben.

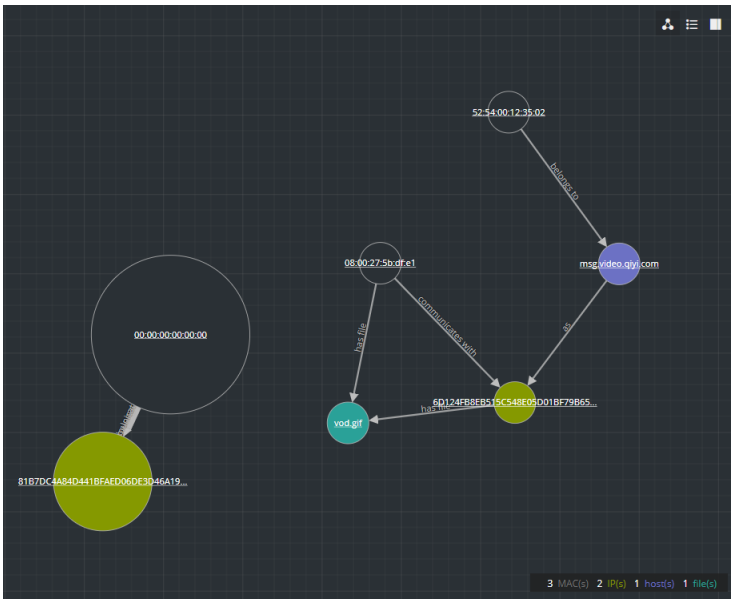
Klicken Sie zum Öffnen des Bereichs „Indikatoren“ im linken Bereich der Incident-Detailansicht auf **INDIKATOREN**.



Informationen zur Datenquelle werden unter den Namen der Indikatoren angezeigt. Ebenfalls angegeben sind Datum und Uhrzeit der Indikator-Erstellung und die Anzahl von Ereignissen in dem betreffenden Indikator.

Node-Diagramm

Das Node-Diagramm ist eine interaktive Grafik, in der die in einen Incident involvierten Entitäten abgebildet werden. Eine *Entität* ist ein angegebener Teil Metadaten, z. B. IP-Adresse, MAC-Adresse, Benutzer, Host, Domain, Dateinamen oder Datei-Hash.



Nodes

Nodes werden im Node-Diagramm als Kreise dargestellt. In der folgenden Tabelle werden die verschiedenen Node-Typen in Node-Diagrammen beschrieben.

Node	Beschreibung
IP-Adresse	Handelt es sich bei einem Ereignis um eine erkannte Anomalie, wird die Detektor-IP angezeigt. Handelt es sich bei einem Ereignis um eine Transaktion, werden die Ziel-IP und die Quell-IP angezeigt.
MAC-Adresse	Möglicherweise wird für jeden erkantenn Typ von IP-Adresse eine MAC-Adresse angezeigt.
Benutzer	Ist der Computer einem Benutzer zugeordnet, wird ein Benutzer-Node angezeigt.
Host	Bei Hosts kann es sich um physische Geräte oder virtuelle Maschinen handeln, auf denen Services installiert sind. Hosts werden mit ihrem vollständig qualifizierten Domainnamen (FQDN) oder ihrer IP-Adresse angegeben.
Domain	
Dateiname	Wenn in das Ereignis Dateien involviert sind, werden die entsprechenden Dateinamen angezeigt.
Datei-Hash	Wenn in das Ereignis Dateien involviert sind, werden möglicherweise die entsprechenden Datei-Hashes angezeigt.

Die Legende im unteren Bereich des Node-Diagramms zeigt die Anzahl der Nodes jeden Typs und die Farbcodierung der Nodes. Sie hilft auch bei der Lokalisierung von Entitäten, wenn die Werte (z. B. IP-Adressen) gehasht sind.

Alle Nodes können per Drag-and-Drop beliebig verschoben werden.

Pfeile

Die Pfeile zwischen den Nodes bieten zusätzliche Informationen über die Beziehungen der Entitäten. In der folgenden Tabelle werden die verschiedenen Pfeil-Typen in Node-Diagrammen beschrieben.

Pfeil	Beschreibung
Kommuniziert mit	Ein Pfeil zwischen einem Quellrechner-Node (IP-Adresse oder MAC-Adresse) und einem Zielrechner-Node mit der Beschriftung „Kommuniziert mit“ bildet die Richtung der Kommunikation ab.
Gleich	Ein Pfeil mit „Gleich“ beschrifteter Pfeil zwischen zwei Nodes liefert zusätzliche Informationen über die IP-Adresse, auf die der Pfeil zeigt. Beispiel: Zeigt ein mit „Gleich“ beschrifteter Pfeil vom Host-Node-Kreis auf einen IP-Adress-Node, bedeutet das, dass der im Host-Node-Kreis abgebildete Name der Hostname dieser IP-Adresse ist und es sich nicht um eine separate Entität handelt.
Hat Datei	Ein mit „Hat Datei“ beschrifteter Pfeil zwischen einem Computer-Node (IP-Adresse, MAC-Adresse oder Host) und einem Datei-Hash-Node bedeutet, dass die IP-Adresse diese Datei hat.
Verwendet	Ein mit „Verwendet“ beschrifteter Pfeil zwischen einem Benutzer-Node und einem Computer-Node (IP-Adresse, MAC-Adresse oder Host) bedeutet, dass der Benutzer diesen Computer verwendet hat, als das Ereignis eingetreten ist.
Heißt	Ein mit „Heißt“ beschrifteter Pfeil von einem Datei-Hash-Node zu einem Dateinamen-Node bedeutet, dass der Datei-Hash einer Datei mit diesem Namen entspricht.
Gehört zu	Ein mit „Gehört zu“ beschrifteter Pfeil zwischen zwei Nodes bedeutet, dass sie zum selben Node gehören. Beispiel: Ein mit „Gehört zu“ beschrifteter Pfeil zwischen einer MAC-Adresse und einem Host bedeutet, dass die MAC-Adresse zu diesem Host gehört.

Je dicker ein Pfeil dargestellt ist, desto intensiver ist die Kommunikation zwischen den betreffenden Nodes. Größere Nodes (Kreise) weisen mehr Aktivität auf als kleinere Nodes. Die größeren Nodes sind die Entitäten, die am häufigsten in den Ereignissen erwähnt wurden.

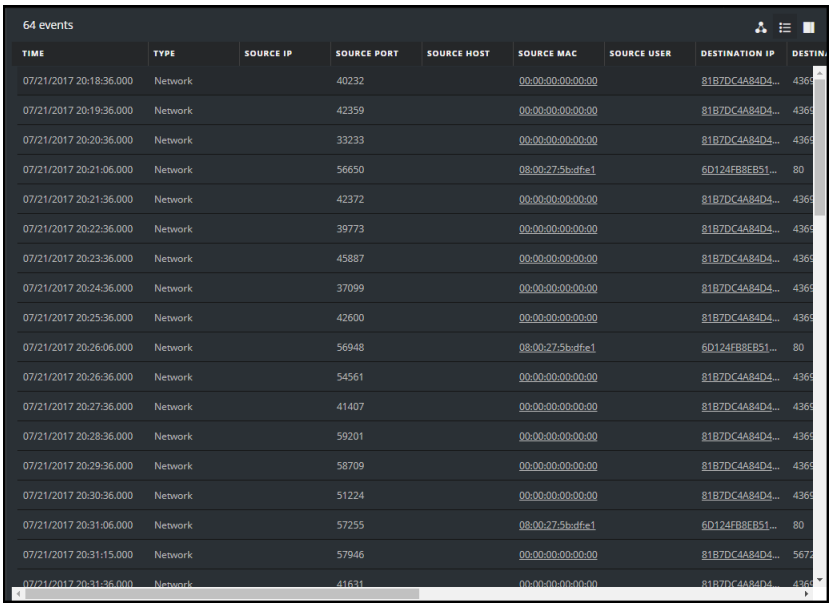
Ereignisdatenblatt

Im Ereignisdatenblatt sind die einem Incident zugeordneten Ereignisse aufgeführt. Es liefert Informationen zu den Ereignissen, z. B. den Zeitpunkt des Ereigniseintritts, die Quell-IP, die Ziel-IP, die Detektor-IP, den Quellbenutzer, den Zielbenutzer und Dateiinformationen im Zusammehang mit den Ereignissen. Wie viele Informationen aufgeführt werden, hängt vom Typ des jeweiligen Ereignisses ab.

Im Ereignisdatenblatt werden entweder mehrere Ereignisse in Form einer Ereignisliste angezeigt oder Ereignisdetails zu einem einzigen Ereignis.

Ereignisliste

Die folgende Abbildung zeigt die Ereignisliste.



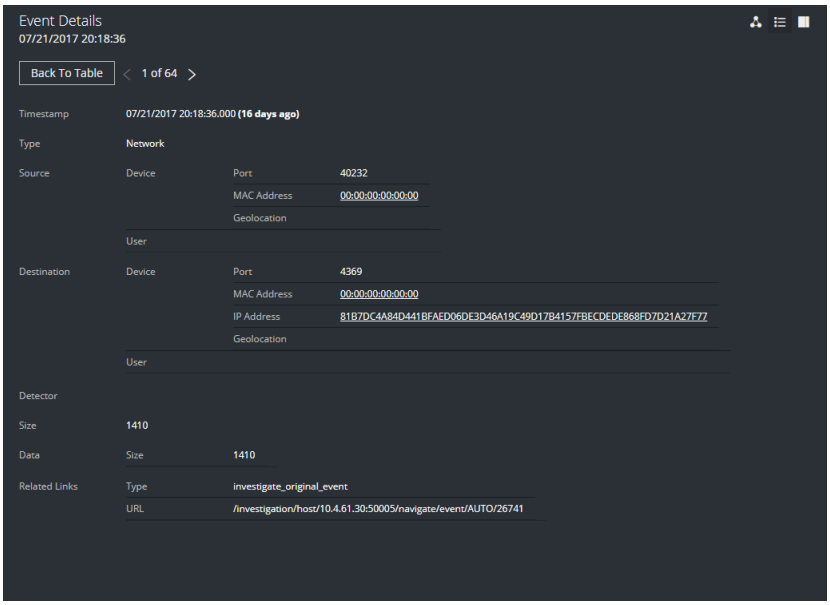
In der folgenden Tabelle werden die Spalten in der Ereignisliste beschrieben.

Spalte	Beschreibung
ZEIT	Zeigt an, wann das Ereignis eingetreten ist.
TYP	Zeigt den Typ der Warnmeldung an, z. B. „Protokoll“ oder „Netzwerk“.
QUELL-IP	Zeigt die Quell-IP-Adresse an, wenn eine Transaktion zwischen zwei Computern erfolgt ist.

Spalte	Beschreibung
QUELLPORT	Zeigt den Quellport der Transaktion an. Quellport und Zielport können dieselbe IP-Adresse haben.
QUELLHOST	Zeigt den Zielhost an, auf dem das Ereignis eingetreten ist.
QUELL-MAC	Zeigt die MAC-Adresse des Quellcomputers an.
QUELLBENUTZER	Zeigt den Benutzer des Quellcomputers an.
ZIEL-IP	Zeigt die Ziel-IP-Adresse an, wenn eine Transaktion zwischen zwei Computern erfolgt ist.
ZIELPORT	Zeigt den Zielport der Transaktion an. Quellport und Zielport können dieselbe IP-Adresse haben.
ZIELHOST	Zeigt den Hostnamen des Zielcomputers an.
ZIEL-MAC	Zeigt die MAC-Adresse des Zielcomputers an.
ZIELBENUTZER	Zeigt den Benutzer des Zielcomputers an.
DETEKTOR-IP	Zeigt die IP-Adresse des Computers an, auf dem eine Anomalie erkannt wurde.
DATEINAME	Zeigt den Dateinamen an, falls eine Datei in das Ereignis involviert ist.
DATEI-HASH	Zeigt einen Hash der Dateiinhalte an.

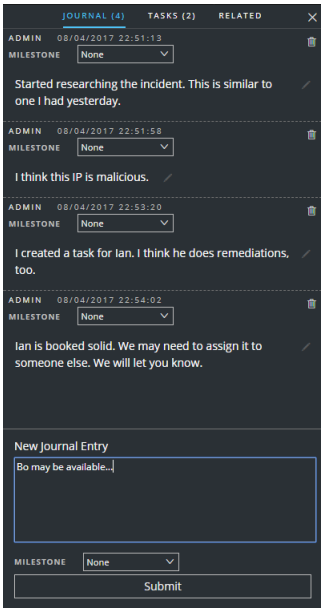
Ereignisdetails

Zum Anzeigen der Details eines Ereignisses klicken Sie in der Ereignisliste auf das gewünschte Ereignis. Wenn nur ein Ereignis in der Liste vorhanden ist, werden anstelle einer Liste nur die Ereignisdetails für dieses Ereignis angezeigt.



Bereich „Journal“

Das Incident-Journal zeigt den zeitlichen Verlauf aller einen Incident betreffenden Aktivitäten.



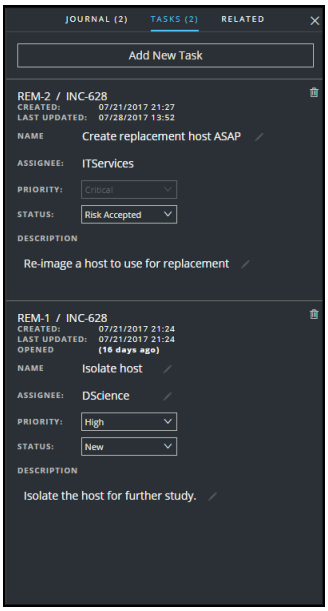
In der folgenden Tabelle werden die Optionen für neue Journaleinträge beschrieben.

Feld	Beschreibung
Neuer Journaleintrag	In dieses Feld geben Sie Ihre Anmerkungen ein.

Feld	Beschreibung
Meilenstein	Option. Wählen Sie falls zutreffend einen Meilenstein aus. Anhand dieses Felds werden bedeuten Ereignisse eines Incident nachverfolgt.
Schaltfläche **Absenden**	Klicken Sie auf „Absenden“, um den Eintrag zum Journal hinzuzufügen. Ihre Journaleinträge sind für alle Benutzer sichtbar, die den Incident aufrufen.

Bereich „Aufgaben“

Im Bereich „Aufgaben“ können Sie Incident-Aufgaben managen und bis zu ihrem Abschluss nachverfolgen.



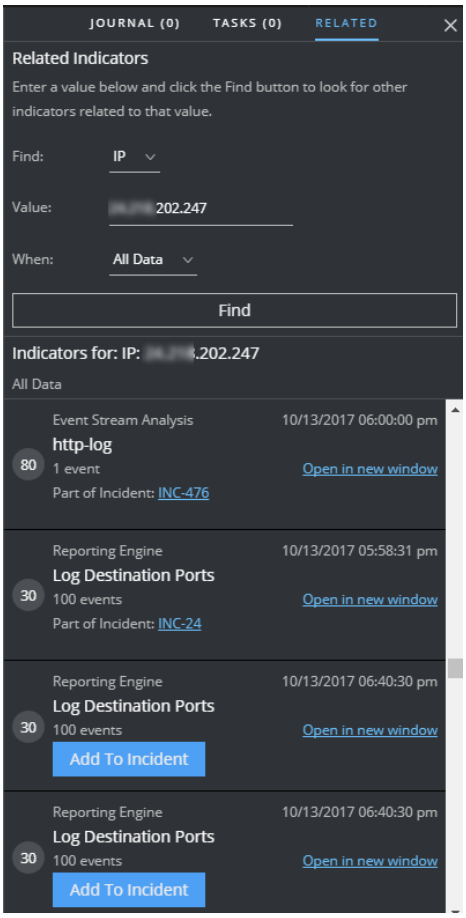
In der folgenden Tabelle werden die verschiedenen Felder einer Aufgabe beschrieben.

Feld	Beschreibung
<Aufgaben-ID>/<Incident-ID>	Automatisch erzeugte Aufgaben-ID/Incident, der der Aufgabe zugeordnet ist
ERSTELLT	Erstellungsdatum der Aufgabe
Letzte Aktualisierung	Datum, an dem die Aufgabe zuletzt geändert wurde
GEÖFFNET	Verstrichene Zeit seit dem Öffnen der Aufgabe (Beispiel: „Vor 3 Minuten“ oder „Vor 2 Tagen“)

Feld	Beschreibung
NAME	Name der Aufgabe. Beispiel: Neues Image auf den Computer aufspielen. Klicken Sie in das Feld, wenn Sie es bearbeiten möchten.
ZUWEISUNGSEMPFÄNGER	Der Benutzername des Benutzers, dem die Aufgabe zugewiesen ist. Klicken Sie in das Feld, wenn Sie es bearbeiten möchten.
PRIORITÄT	Die Priorität der Aufgabe: „Niedrig“, „Mittel“, „Hoch“ oder „Kritisch“. Wenn Sie auf die Prioritätsschaltfläche klicken, kännen Sie aus der Drop-down-Liste eine neue Priorität für die Aufgabe auswählen.
STATUS	Status der Aufgabe: „Neu“, „Zugewiesen“, „Läuft“, „Korrigiert“, „Risiko akzeptiert“ und „Nicht zutreffend“. Wenn Sie auf die Statusschaltfläche klicken, können Sie aus der Drop-down-Liste einen neuen Status für die Aufgabe auswählen.
DESCRIPTION	Hier können Sie eine Beschreibung der Aufgabe eingeben. Es empfiehlt sich, hier alle zugehörigen Referenznummern einzutragen. Klicken Sie in das Feld, wenn Sie es bearbeiten möchten.

Bereich „Verwandte Indikatoren“

Im Bereich „Verwandte Indikatoren“ können Sie die NetWitness Suite-Warnmeldungsdatenbank nach Warnmeldungen durchsuchen, die zu dem jeweiligen Incident in Beziehung stehen. Gefunden Warnmeldungen lassen sich dem Incident hinzufügen, falls sie noch keinem Incident zugeordnet sind.



In der folgenden Tabelle werden die Felder im Suchabschnitt oben in dem Bereich beschrieben.

Feld	Beschreibung
Suchen	Wählen Sie die Entität aus, nach denen Sie die Warnmeldungen durchsuchen möchten. (Beispiel: „IP“)
Wert	Geben Sie den Wert der Entität ein. (Beispiel: IP-Adresse der Entität)
Zeitraum	Wählen Sie aus, aus welchem Zeitraum die Ergebnisse der Warnmeldungssuche stammen sollen. Zum Beispiel: „Letzte 24 Stunden“.
Schaltfläche **Suchen**	Startet die Suche. Eine Liste der verwandten Indikatoren wird unter der Schaltfläche **Suchen** im Abschnitt **Indikatoren für** angezeigt.

In der folgenden Tabelle werden die Optionen im Abschnitt **Indikatoren für** (Ergebnisse) unten im Bereich beschrieben.

Option	Beschreibung
Indikatoren für:	Zeigt die Suchergebnisse an.
Link **In neuem Fenster öffnen**	Zeigt Warnmeldungsdetails zu dem betreffenden Indikator an.
Schaltfläche **Einem Incident hinzufügen**	Fügt den verwandten Indikator dem betreffenden Incident hinzu. Der verwandte Indikator wird dann im Bereich „Indikatoren“ angezeigt.
Schaltfläche **Zum Incident gehörig**	Zeigt an, dass der Indikator dem betreffenden Incident bereits zugeordnet.

Symbolleistenaktionen

Option	Beschreibung
	(Zurück zu Incidents) Führt zurück zur Incident-Listenansicht.
	Schließt den Bereich.
	Löscht den Eintrag (z. B. einen Journaleintrag oder eine Aufgabe).
Schaltfläche **Priorität**	(Im Bereich „Übersicht) Ermöglicht die Änderung der Priorität eines oder mehrerer ausgewählter Incidents in der Incident-Liste.
Schaltfläche **Status**	(Im Bereich „Übersicht) Ermöglicht die Änderung des Status eines oder mehrerer ausgewählter Incidents.
Schaltfläche **Zuweisungsempfänger**	(Im Bereich „Übersicht) Ermöglicht die Änderung des Zuweisungsempfängers für einen oder mehrere ausgewählte Incidents.
 (Anzeigen: Diagramm)	Öffnet das Node-Diagramm.

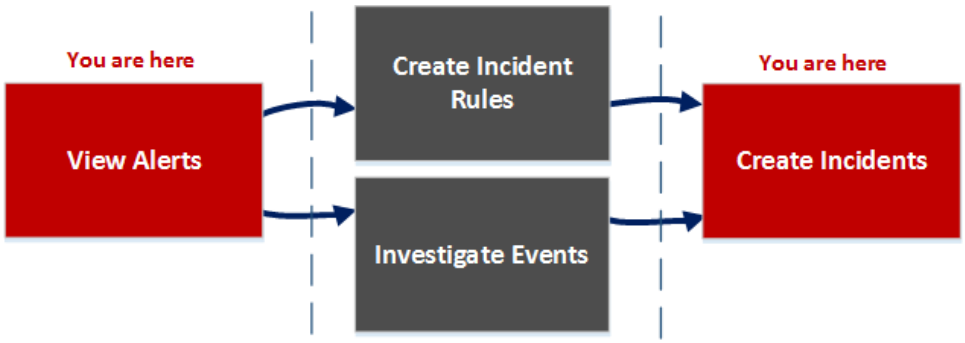
Option	Beschreibung
 (Anzeigen: Datenblatt)	Öffnet das Ereignisdatenblatt. Hier werden entweder mehrere Ereignisse in Form einer Ereignisliste angezeigt oder Ereignisdetails zu einem einzigen Ereignis.
 („Journal“, „Aufgaben“ und „Verwandt“)	Öffnet die Bereiche „Journal“, „Aufgaben“ und „Verwandte Indikatoren“.

Warnmeldungsliste

Die Warnmeldungsliste („REAGIEREN“ > „Warnmeldungen“) gibt Ihnen einen zentralen Überblick über sämtliche Bedrohungswarnmeldungen und Indikatoren, die NetWitness Suite empfängt. Die Warnmeldungen können aus ESA-Korrelationsregeln, ESA Analytics, Malware Analysis, Reporting Engine, NetWitness Endpoint sowie vielen weiteren Quellen stammen. Sie können die in der Warnmeldungsliste aufgeführten Warnmeldungen durchsuchen, filtern und zur Erstellung von Incidents auch zusammenfassen.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess, anhand dessen Analysten Warnmeldungen überprüfen und Incidents erstellen.



Die Listenansicht der Warnmeldungen ist eine quellenübergreifende Liste aller Warnmeldungen, die NetWitness Suite empfangen hat. Sie können die einzelnen Warnmeldungen untersuchen und Incidents aus ihnen erstellen. Außerdem haben Sie die Möglichkeit, Incident-Regeln für die Erstellung von Incidents zu definieren.

Hinweis: Mithilfe von NetWitness Suite Automated Threat Detection können Sie Incidents erstellen, ohne erst manuell Regeln definieren zu müssen.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Incident-Experten, Analysten	Alle Warnmeldungen in NetWitness Suite anzeigen*	Anzeigen von Warnmeldungen
Incident-Experten, Analysten	Warnmeldungen filtern*	Filtern der Warnmeldungsliste

Rolle	Ziel	Details anzeigen
Incident-Experten, Analysten	Übersichtsinformationen zu Warnmeldungen sowie Metadaten zu Rohwarnmeldungen anzeigen*	Anzeigen von Übersichtsinformationen zu Warnmeldungen
Incident-Experten, Analysten	Incidents aus Warnmeldungen erstellen*	Manuelles Erstellen eines Incident
Incident-Experten, Analysten	(verfügbar ab Version 11.1) Warnmeldungen zu einem vorhandenen Incident hinzufügen.*	Warnmeldungen zu einem Incident hinzufügen
Administratoren, Datenschutzbeauftragte	Warnmeldungen löschen*	Löschen von Warnmeldungen
SOC-Manager, Administratoren	Incident-Regeln erstellen	Siehe „Erstellen einer Incident-Regel für Warnmeldungen“ im *NetWitness Respond-Konfigurationsleitfaden*.
Incident-Experten, Analysten	Ereignisse in einer Warnmeldung untersuchen	Anzeigen von Ereignisdetails für eine Warnmeldung und Untersuchen von Ereignissen
Incident-Experten, Analysten	Einem bereits vorhandenen Incident Warnmeldungen hinzufügen	Hinzufügen verwandter Indikatoren zum Incident

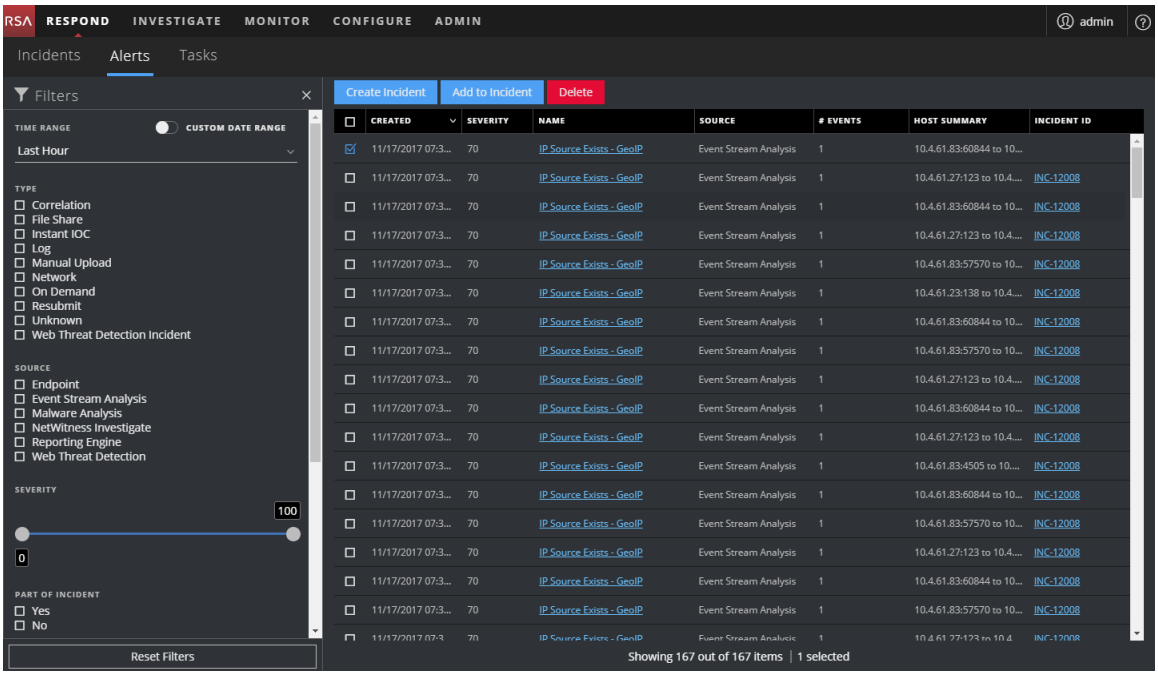
* Sie können diese Aufgaben in der aktuellen Ansicht (d. h. in der Warnmeldungsliste) durchführen.

Verwandte Themen

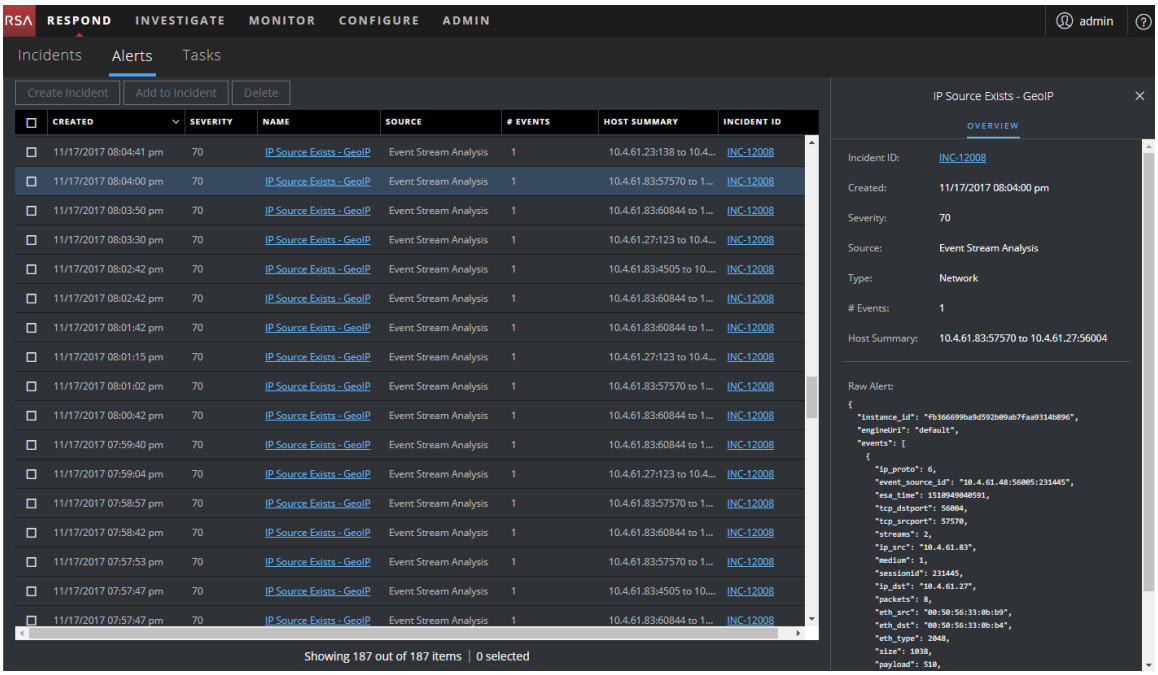
- Ansicht „Warnmeldungsdetails“
- Überprüfen von Warnmeldungen

Warnmeldungsliste

Zum Aufrufen der Warnmeldungsliste klicken Sie auf **Reagieren > Warnmeldungen**. In der Warnmeldungsliste werden sämtliche Warnmeldungen und Indikatoren aufgelistet, die von der Antwortserver-Datenbank in NetWitness Suite empfangen wurden. Auf der Abbildung unten sehen Sie links den Bereich „Filter“.

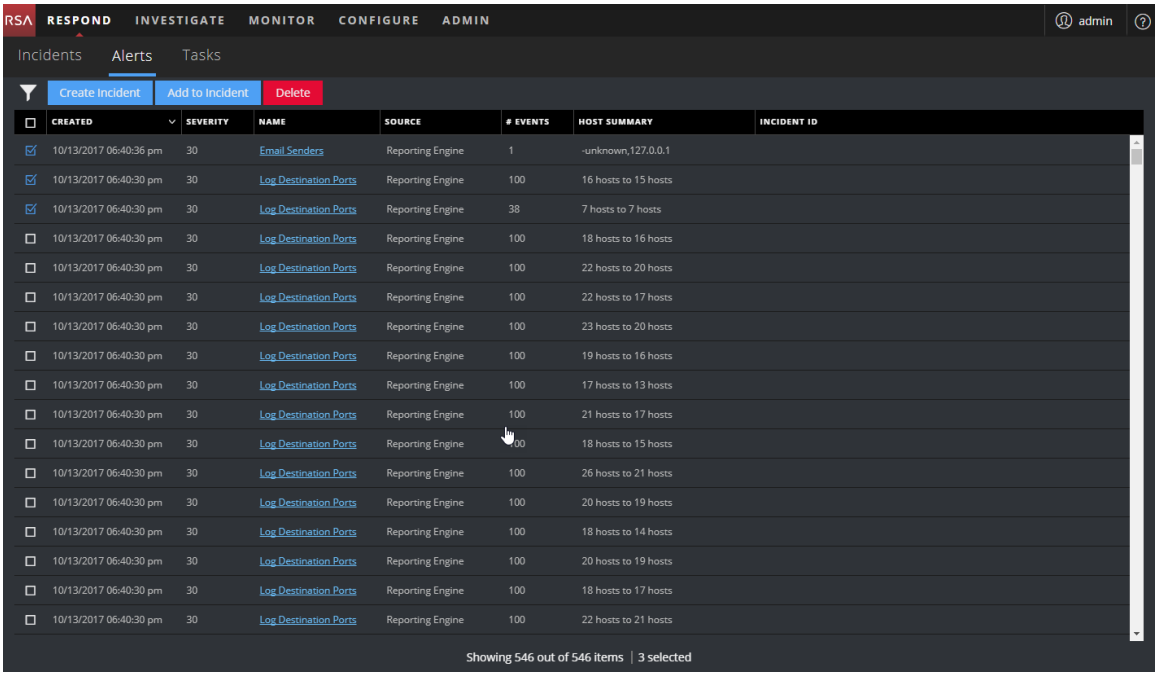


Die Listenansicht unter „Warnmeldungen“ besteht aus einem „Filter“-Bereich, einer Liste mit Warnmeldungen und einem „Übersicht“-Bereich für die einzelnen Warnmeldungen. Wenn Sie auf eine Warnmeldung in der Warnmeldungsliste klicken, wird rechts der Bereich „Übersicht“ für die betreffende Warnmeldung angezeigt.



Warnmeldungsliste

In der Warnmeldungsliste sind sämtliche Warnmeldungen in NetWitness Suite aufgeführt. Sie können diese Liste so filtern, dass nur die Warnmeldungen angezeigt werden, die für Sie von Interesse sind.



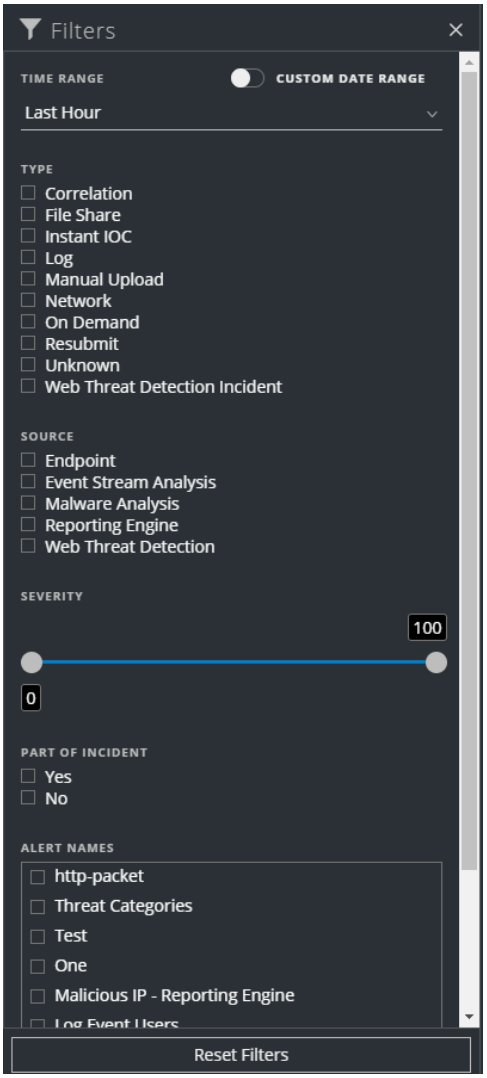
Spalte	Beschreibung
	Erlaubt die Auswahl einer oder mehrerer Warnmeldungen, um sie anschließend zu Löschen. Warnmeldungen können von Benutzern mit den entsprechenden Berechtigungen gelöscht werden, wie Administratoren und Datenschutzbeauftragten.
CREATED	Zeigt an, an welchem Datum und zu welcher Uhrzeit die Warnmeldung im Quellsystem erfasst wurde.
SCHWEREGRAD	Zeigt den Schweregrad der Warnmeldung an. Möglich sind Werte von 1 bis 100.
NAME	Zeigt eine grundlegende Beschreibung der Warnmeldung an.

Spalte	Beschreibung
QUELLE	Zeigt die ursprüngliche Quelle der Warnmeldung an. Mögliche Warnmeldungsquellen sind unter anderem NetWitness Endpoint, Malware Analysis, ESA-Korrelationsregeln, ESA Analytics und Reporting Engine.
EREIGNISANZAHL	Zeigt die Anzahl an Ereignissen, die in einer Warnmeldung enthalten sind. Diese Zahl variiert je nach Quelle der Warnmeldung. NetWitness Endpoint- und Malware Analysis-Warnmeldungen haben zum Beispiel immer nur ein Ereignis. Für bestimmte Arten von Warnmeldungen bedeutet eine große Anzahl an Ereignissen, dass die Warnmeldung riskanter ist.
HOSTZUSAMMENFASSUNG	Zeigt Details des Hosts an, wie zum Beispiel den Hostnamen, von dem die Warnmeldung ausgelöst wurde. Die Details können Informationen zu den Quell- und Zielhosts in einer Warnmeldung enthalten. Manche Warnmeldungen können Ereignisse über mehr als einen Host beschreiben.
Incident-ID	Zeigt die Incident-ID einer Warnmeldung an. Ist keine Incident-ID aufgeführt, gehört die Warnmeldung zu keinem Incident und Sie können einen Incident erstellen, der dann diese Warnmeldung enthält. Alternativ kann die Warnmeldung einem vorhandenen Incident hinzugefügt werden.

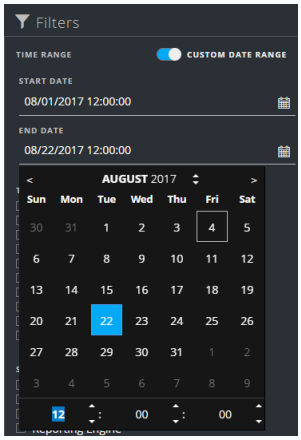
Unter der Liste sehen Sie die Anzahl von Warnmeldungen auf der aktuellen Seite sowie die Gesamtzahl aller Warnmeldungen und die Anzahl ausgewählter Warnmeldungen. Beispiel: **377 von 377 Elementen werden angezeigt | 3 ausgewählt**

Bereich „Filter“

Auf der Abbildung unten sehen Sie die im Bereich „Filter“ verfügbaren Filter.



Im Bereich „Filter“ links neben der Warnmeldungsliste stehen Optionen zur Verfügung, mit denen Sie die Warnmeldungsliste filtern können. Wenn Sie den Bereich „Filter“ verlassen, werden die ausgewählten Filter für die Warnmeldungsliste beibehalten.

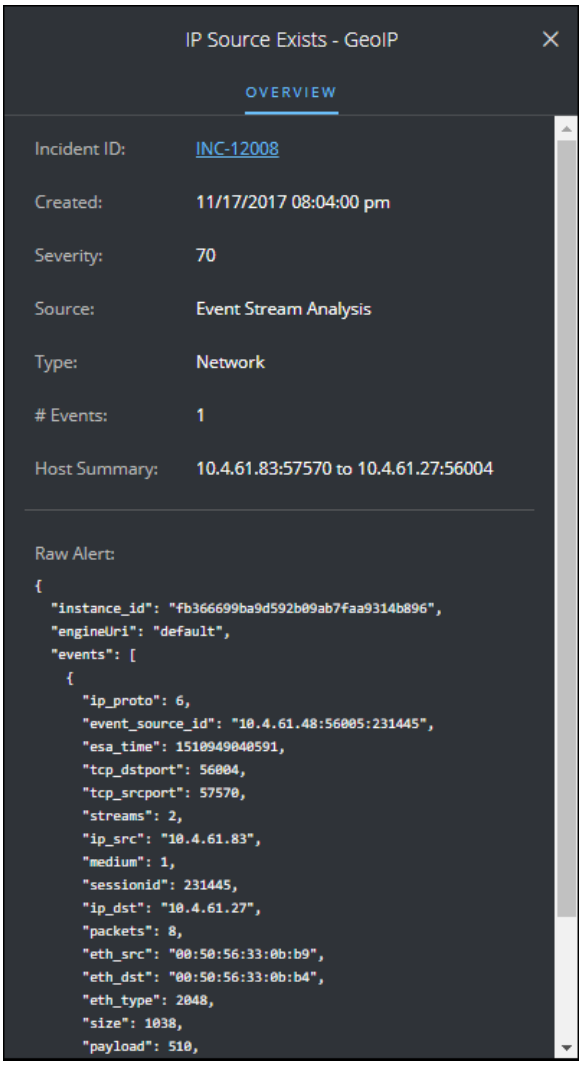
Option	Beschreibung
ZEITBEREICH	Sie können einen bestimmten Zeitraum aus der Drop-down-Liste „Zeitbereich“ auswählen. Der Zeitbereich basiert auf dem Datum, an dem die Warnmeldungen empfangen wurden. Wenn Sie zum Beispiel „Letzte Stunde“ auswählen, werden die Warnmeldungen angezeigt, die innerhalb der letzten 60 Minuten empfangen wurden.
BENUTZERDEFINIERTER DATUMSBEREICH	Sie können einen bestimmten Datumsbereich anstelle der Option „Zeitbereich“ auswählen. Klicken Sie dazu auf den weißen Kreis vor „Benutzerdefinierter Datumsbereich“, damit die Felder „Startdatum“ und „Enddatum“ angezeigt werden. Wählen Sie die Datums- und Zeitangaben im Kalender aus. 
TYP	Zeigt den Ereignis-Typ der Warnmeldung an, zum Beispiel Protokolle, Netzwerksitzungen usw.
QUELLE	Zeigt die ursprüngliche Quelle der Warnmeldung an. Mögliche Warnmeldungsquellen sind unter anderem NetWitness Endpoint, Malware Analysis, Event Stream Analysis (ESA-Korrelationsregeln), ESA Analytics, Reporting Engine und Web Threat Detection.

Option	Beschreibung
SCHWEREGRAD	Zeigt den Schweregrad der Warnmeldung an. Der Wert kann zwischen 1 und 100 liegen.
ZU INCIDENT GEHÖRIG?	Gibt an, ob die Warnmeldung einem Incident zugeordnet ist. Wählen Sie **Ja** aus, um alle Warnmeldungen anzuzeigen, die zu einem Incident gehören. Wählen Sie **Nein** aus, um alle Warnmeldungen anzuzeigen, die zu keinem Incident gehören. Vor der Erstellung eines Incident aus einer Warnmeldung sollten Sie beispielsweise die Option „Nein“ auswählen, damit nur die Warnmeldungen angezeigt werden, die noch nicht zu einem Incident gehören.
WARNMELDUNGSNAMEN	Zeigt den Namen der Warnmeldung an. Sie können diesen Filter verwenden, um nach allen Warnmeldungen zu suchen, die durch eine bestimmte Regel oder Quelle erzeugt wurden, z. B. nach Meldungen mit dem Namen „Schädliche IP - Reporting Engine“.
Filter zurücksetzen	Entfernt die Filterauswahl.

In der Warnmeldungsliste wird eine Liste aller Warnmeldungen angezeigt, die Ihre Auswahlkriterien erfüllen. Die Anzahl der Elemente in der gefilterten Liste finden Sie am unteren Rand der Warnmeldungsliste. Beispiel: **30 von 30 Elementen werden angezeigt**

Bereich „Übersicht“

Im Bereich „Übersicht“ finden Sie grundlegende Übersichtsinformationen zu der jeweils ausgewählten Warnmeldung sowie die Metadaten der zugehörigen Rohwarnmeldung. Der Bereich „Übersicht“ in der Ansicht „Warnmeldungsdetails“ enthält dieselben Informationen, lässt sich jedoch um zusätzliche Informationen erweitern.



In der folgenden Tabelle sind die Felder im „Übersicht“-Bereich einer Warnmeldung aufgeführt.

Feld	Beschreibung
<Name der Warnmeldung>	Zeigt den Namen der Warnmeldung an.
Incident-ID	Zeigt die Incident-ID an, die der Warnmeldung zugeordnet ist. Mit einem Klick auf den Incident-ID-Link können Sie die Detailansicht des zugeordneten Incident aufrufen. Gibt es keine Incident-ID, gehört die Warnmeldung zu keinem Incident. Dann können Sie einen Incident für die Warnmeldung erstellen oder sie einem bereits vorhandenen Incident hinzufügen.

Feld	Beschreibung
Erstellt	Zeigt an, an welchem Datum und zu welcher Uhrzeit die Warnmeldung erstellt wurde.
Schweregrad	Zeigt den Schweregrad der Warnmeldung an. Der Wert kann zwischen 1 und 100 liegen.
Quelle	Zeigt die ursprüngliche Quelle der Warnmeldung an. Mögliche Warnmeldungsquellen sind unter anderem NetWitness Endpoint, Malware Analysis, ESA-Korrelationsregeln, ESA Analytics und Reporting Engine.
Typ	Zeigt den Ereignistyp der Warnmeldung an, zum Beispiel Protokolle, Netzwerksitzungen usw.
Ereignisanzahl	Zeigt die Anzahl an Ereignissen, die in einer Warnmeldung enthalten sind. Diese Zahl variiert je nach Quelle der Warnmeldung. NetWitness Endpoint- und Malware Analysis-Warnmeldungen haben zum Beispiel immer nur ein Ereignis. Für bestimmte Arten von Warnmeldungen bedeutet eine große Anzahl an Ereignissen, dass die Warnmeldung riskanter ist.
Rohwarnmeldung	Zeigt die Metadaten der Rohwarnmeldung an.

Symbolleistenaktionen

In dieser Tabelle werden die Aktionen aufgeführt, die in der Symbolleiste der Warnmeldungsliste verfügbar sind.

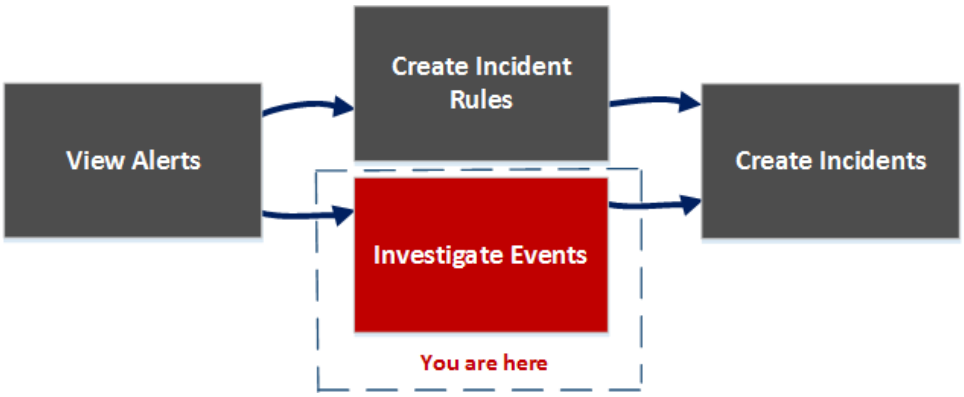
Option	Beschreibung
	Öffnet den Bereich „Filter“, in dem Sie festlegen können, welche Incidents in der Incident-Liste angezeigt werden sollen
	Schließt den Bereich
Schaltfläche **Incident erstellen**	Erlaubt die Erstellung von Incidents aus Warnmeldungen. Die Warnmeldungen dürfen nicht zu einem Incident gehören. Zum Aufrufen einer Liste aller Warnmeldungen ohne Incident können Sie die Warnmeldungsliste filtern: Wählen Sie dazu im Abschnitt „ZU INCIDENT GEHÖRIG?“ die Option „Nein“ aus.
Schaltfläche **Einem Incident hinzufügen**	(Diese Option ist in Version 11.1 und höher verfügbar.) Damit können Sie ausgewählte Warnmeldungen zu einem Incident hinzufügen. Die Warnmeldungen dürfen nicht zu einem Incident gehören. Zum Aufrufen einer Liste aller Warnmeldungen ohne Incident können Sie die Warnmeldungsliste filtern. Wählen Sie im Abschnitt „Zum Incident gehörig“ die Option „Nein“ aus.
Schaltfläche **Löschen**	Erlaubt das Löschen von Warnmeldungen.

Ansicht „Warnmeldungsdetails“

In der Ansicht „Warnmeldungsdetails“ finden Sie Übersichtsinformationen zu der Warnmeldung, beispielsweise ihre Quelle, die Anzahl von in ihr enthaltenen Ereignissen und Angabe dazu, ob sie zu einem Incident gehört. (Zugriff: „REAGIEREN“ > „Warnmeldungen“ > Klick auf den Link in „NAME“-Spalte der Warnmeldungsliste) Außerdem können Sie hier detaillierte Informationen zu den Ereignissen in der Warnmeldung sowie die Ereignismetadaten einsehen.

Workflow

Dieser Workflow veranschaulicht den allgemeinen Prozess, anhand dessen Analysten Warnmeldungen überprüfen und Incidents erstellen.



Sobald Sie die Warnmeldungsliste in der Ansicht „Warnmeldungsdetails“ durchgesehen haben, können Sie Warnmeldungen von Interesse in der zugehörigen Detailansicht näher untersuchen und Incidents aus ihnen erstellen. Unter Konfigurieren > „Incident-Regeln“ können Sie Incident-Regeln erstellen, auf deren Grundlage Incidents erstellt werden sollen.

Hinweis: Sie können auch NetWitness Suite Automated Threat Detection nutzen. Mit diesem Service können Sie Incidents erstellen, ohne erst manuell Regeln definieren zu müssen.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Incident-Experten, Analysten	Alle Warnmeldungen in NetWitness Suite anzeigen	Anzeigen von Warnmeldungen

Rolle	Ziel	Details anzeigen
SOC-Manager, Administratoren	Incident-Regeln erstellen	Siehe „Erstellen einer Incident-Regel für Warnmeldungen“ im *NetWitness Respond-Konfigurationsleitfaden*.
Incident-Experten, Analysten	Liste aller Ereignisse in einer Warnmeldung anzeigen*	Anzeigen von Ereignisdetails für eine Warnmeldung
Incident-Experten, Analysten	Ereignismetadaten für jedes Ereignis in einer Warnmeldung anzeigen*	Anzeigen von Ereignisdetails für eine Warnmeldung
Incident-Experten, Analysten	Ereignisse in einer Warnmeldung eingehender untersuchen*	Untersuchen von Ereignissen
Incident-Experten, Analysten	Einem bereits vorhandenen Incident Warnmeldungen hinzufügen	Warnmeldungen zu einem Incident hinzufügen Hinzufügen verwandter Indikatoren zum Incident
Incident-Experten, Analysten	Incidents aus Warnmeldungen erstellen	Manuelles Erstellen eines Incident
Datenschutzbeauftragte, Administratoren	Warnmeldungen löschen	Löschen von Warnmeldungen

* Sie können diese Aufgaben in der aktuellen Ansicht (d. h. in der Detailansicht der Warnmeldung) durchführen.

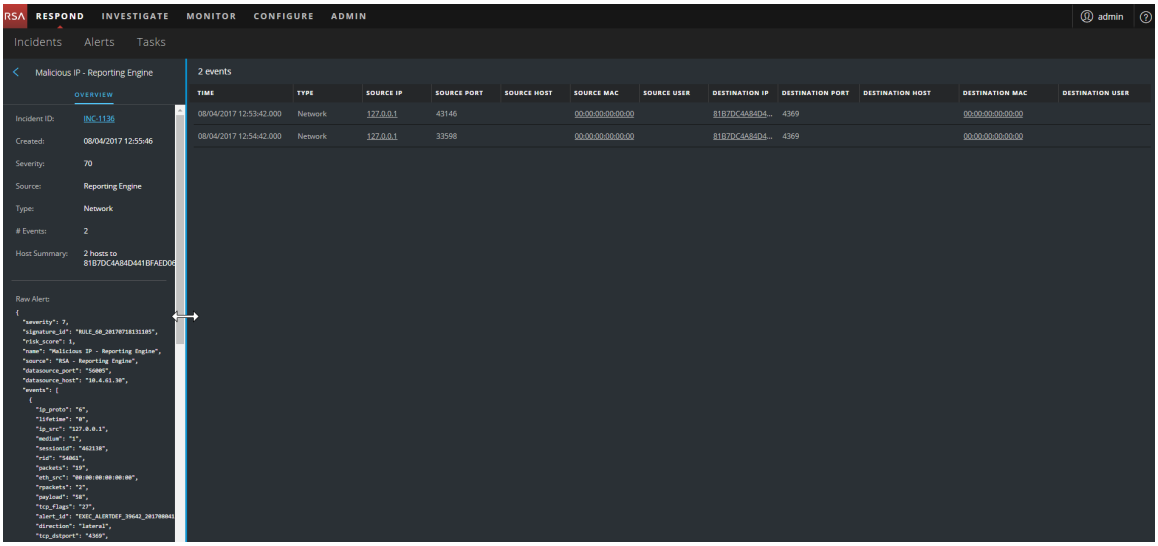
Verwandte Themen

- Warnmeldungsliste
- Überprüfen von Warnmeldungen

Ansicht „Warnmeldungsdetails“

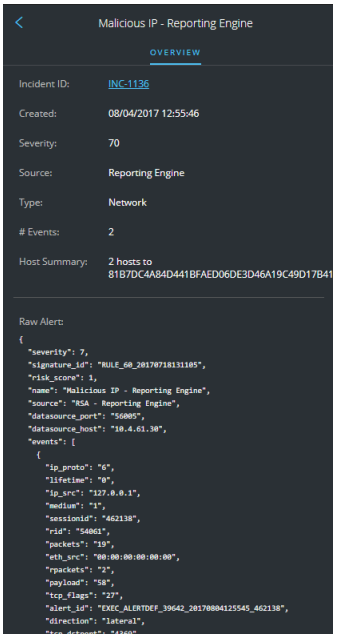
1. Navigieren Sie zum Aufrufen der Ansicht „Warnmeldungsdetails“ zu **Reagieren** > **Warnmeldungen**.

2. Wählen Sie aus der Warnmeldungsliste die Warnmeldung aus, deren Details Sie einsehen möchten, und klicken Sie in der Spalte „NAME“ auf den Link dieser Warnmeldung.
   Die Ansicht „Warnmeldungsdetails“ besteht aus dem Bereich „Übersicht“ links und dem Ereignisbereich rechts. Sie können die Größe der Bereiche anpassen, um mehr Informationen zu sehen (siehe Abbildung unten).



Bereich „Übersicht“

Im Bereich „Übersicht“ finden Sie grundlegende Übersichtsinformationen zu der jeweils ausgewählten Warnmeldung. Der Bereich „Übersicht“ in der Warnmeldungsliste enthält dieselben Informationen. Details hierzu finden Sie im Thema „Warnmeldungsliste“ im Abschnitt Bereich „Übersicht“.

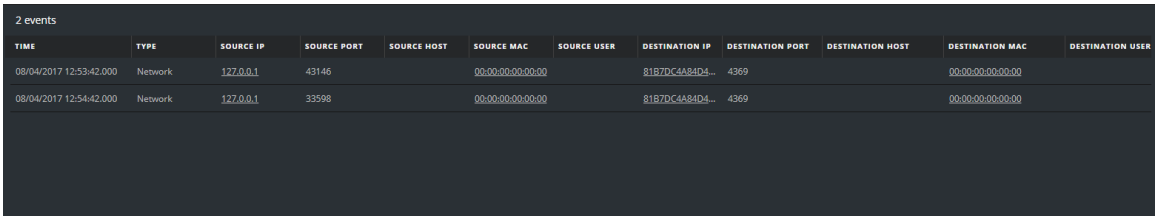


Ereignisbereich

Enthält die Warnmeldung mehr als ein Ereignis, wird im Ereignisbereich eine Liste der Ereignisse angezeigt. Enthält die Warnmeldung nur ein einziges Ereignis, werden im Ereignisbereich die Ereignisdetails angezeigt. Diese können Sie auch aufrufen, indem Sie in der Ereignisliste auf ein Ereignis klicken.

Ereignisliste

In der Ereignisliste für eine ausgewählte Warnmeldung werden sämtliche in der betreffenden Warnmeldung enthaltenen Ereignisse aufgeführt.



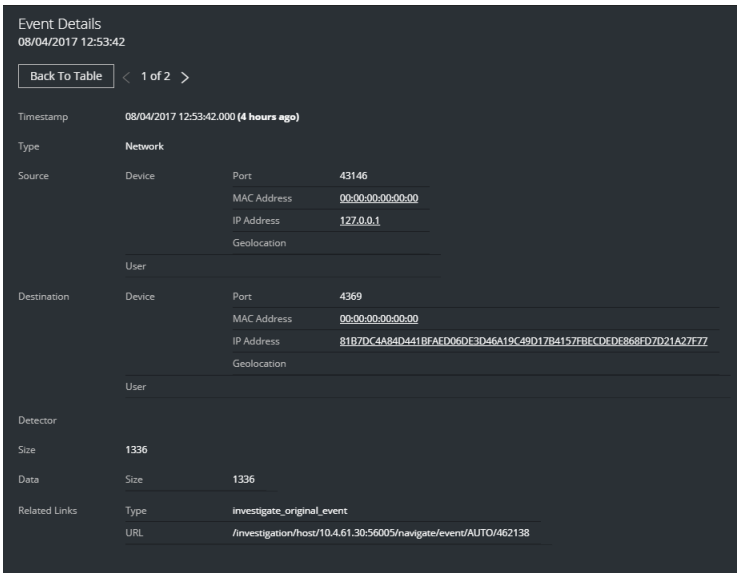
In der nachfolgenden Tabelle sind die Spalten der Ereignisliste aufgeführt. Sie liefern einen Überblick über das jeweilige Ereignis.

Spalte	Beschreibung
ZEIT	Zeigt an, wann das Ereignis eingetreten ist.
TYP	Zeigt den Typ der Warnmeldung an, z. B. „Protokoll“ oder „Netzwerk“.
QUELL-IP	Zeigt die Quell-IP-Adresse an, wenn eine Transaktion zwischen zwei Rechnern erfolgt ist.
Ziel-IP	Zeigt die Ziel-IP-Adresse an, wenn eine Transaktion zwischen zwei Rechnern erfolgt ist.
DETEKTOR-IP	Zeigt die IP-Adresse des Rechners an, auf dem eine Anomalie erkannt wurde.
QUELLBENUTZER	Zeigt den Benutzer des Quellrechners an.
ZIELBENUTZER	Zeigt den Benutzer des Zielrechners an.
DATEINAME	Zeigt den Dateinamen an, falls eine Datei in das Ereignis involviert ist.

Spalte	Beschreibung
DATEI-HASH	Zeigt einen Hash der Dateiinhalte an.

Ereignisdetails

In den Ereignisdetails im Bereich „Ereignisse“ finden Sie die Ereignismetadaten aller Ereignisse in der betreffenden Warnmeldung.



Ereignismetadaten

In der folgenden Tabelle sind einige der Abschnitte und Unterabschnitte der Ereignismetadaten aufgeführt, die in den ersten beiden Spalten der Ereignisdetails aufgeführt werden. Diese Liste ist nicht vollständig.

Abschnitt	Unterabschnitt	Beschreibung
Daten		Zeigt Informationen zu den in das Ereignis involvierten Daten an, beispielsweise die involvierten Dateien. In ein Ereignis können 0 oder mehr Dateien involviert sein.
	Dateiname	Zeigt den Dateinamen an, falls eine Datei in das Ereignis involviert ist.
	Hash	Zeigt einen Hash der Dateiinhalte an, beispielsweise MD5 oder SHA1.

Abschnitt	Unterabschnitt	Beschreibung
	Größe	Zeigt die Größe der in das Ereignis involvierten Übertragung oder Datei an.
Beschreibung		Zeigt eine allgemeine Beschreibung des Ereignisses an.
Ziel		Zeigt das Zielgerät und dessen Benutzer an.
	Gerät	Zeigt Informationen über das Zielgerät an. Siehe Attribute von Ereignisquellen und Zielgeräten unten.
	Benutzer	Zeigt Informationen über den oder die Benutzer des Zielgeräts an. Siehe Attribute von Ereignisquellen und Zielbenutzern unten.
Detektor		Zeigt den Host oder das Softwareprodukt an, von dem das Problem erkannt wurde. Diese Angabe ist die wichtigste für Schadsoftwarescanner und Protokolle.
	Geräteklasse	Zeigt die Geräteklasse des Produkts an, das die Warnmeldung erkannt hat.
	IP-Adresse	Zeigt die IP-Adresse des Produkts an, das die Warnmeldung erkannt hat.
	Produktname	Zeigt den Namen des Produkts an, das die Warnmeldung erkannt hat.
Domain		Zeigt die dem Ereignis zugeordnete Domain an.
Erweiterung		Zeigt alle zur Erweiterung verfügbaren Informationen an.
Verwandte Links		Zeigt sofern verfügbar einen Link zurück zur Benutzeroberfläche des Quellprodukts an
	Typ	Zeigt den Typ des Ereignisses an, z. B. „investigate_original_event“.
	URL	Zeigt die URL zurück zur Benutzeroberfläche des Quellprodukts an.

Abschnitt	Unterabschnitt	Beschreibung
Größe		Zeigt die Größe der involvierten Übertragung oder Datei an.
Quelle		Zeigt das Quellgerät und dessen Benutzer an.
	Gerät	Zeigt Informationen zum Quellrechner an. Siehe Attribute von Ereignisquellen und Zielgeräten unten.
	Benutzer	Zeigt Informationen zum Benutzer bzw. zu den Benutzern des Quellrechners an. Siehe Attribute von Ereignisquellen und Zielbenutzern unten.
Zeitstempel		Zeigt die Uhrzeit an, zu der das Ereignis eingetreten ist.
Typ		Zeigt den Typ der Warnmeldung an, beispielsweise „Protokoll“, „Netzwerk“, „Korrelation“, „Neuübermittlung“, „Manuell hochladen“, „On demand“, „Dateifreigaben“ oder „IOC-Sofortwarnmeldung“.

Attribute von Ereignisquellen und Zielgeräten

In der folgenden Tabelle sind die in den Ereignisdetails verfügbaren Attribute von Ereignisquellen oder Zielgeräten aufgeführt.

Name	Beschreibung
Asset-Typ	Zeigt den Gerätetyp an, zum Beispiel „Desktop“, „Laptop“, „Server“, „Netzwerksystem“ oder „Tablet“.
Geschäftseinheit	Zeigt den Geschäftsbereich an, dem das Gerät zugeordnet ist.
Compliancerating	Zeigt das Compliancerating des Geräts an. Mögliche Werte sind „Niedrig“, „Mittel“ und „Hoch“.
Bedeutung	Zeigt an, wie wichtig (geschäftskritisch) das Gerät für das Unternehmen ist.
Anlage	Zeigt den Standort des Geräts an.

Name	Beschreibung
Geolocation	Zeigt den geografischen Standort des Hosts an. Folgende Attribute können enthalten sein: „Stadt“, „Land“, „Breitengrad“, „Längengrad“, „Organisation“ und „Domain“.
IP-Adresse	Zeigt die IP-Adresse des Geräts an.
MAC-Adresse	Zeigt die MAC-Adresse des Geräts an.
NetBIOS-Name	Zeigt den NetBIOS-Namen des Geräts an.
Port	Zeigt den TCP-Port, den UDP-Port oder den IP Src-Port (erster verfügbarer) für Verbindungen zum und vom Host an.

Attribute von Ereignisquellen und Zielbenutzern

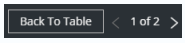
In der folgenden Tabelle sind die in den Ereignisdetails verfügbaren Attribute von Ereignisquellen oder Zielbenutzern aufgeführt.

Attributname	Beschreibung
AD-Domain	Zeigt die Active Directory-Domain an.
AD-Benutzername	Zeigt den Active Directory-Benutzernamen an.
E-Mail-Adresse	Zeigt die E-Mail-Adresse des Benutzers an.
Benutzername	Zeigt einen allgemeinen Namen an, falls die Quelle des Benutzernamens unbekannt ist, beispielsweise UNIX oder den Benutzernamen aus einem bestimmten System.

Symbolleistenaktionen

In dieser Tabelle werden die Aktionen aufgeführt, die in der Symbolleiste der Ansicht „Warnmeldungsdetails“ verfügbar sind.

Option	Beschreibung

Option	Beschreibung
	(Zurück zu Warnmeldungen) Bringt den Benutzer zurück zur Warnmeldungsliste.
	Klicken Sie auf die Pfeile, um durch die Ereignismetadetails der Ereignisse in einer Warnmeldung zu navigieren. Die Zahlen geben an, welches Ereignis gerade angezeigt wird (z. B. „1 von 2“). Klicken Sie auf **Zurück zu Tabelle**, um zur Ereignisliste zurückzukehren. Sie wird auch als Ereignistabelle bezeichnet.

Aufgaben-Listenansicht

Sobald Sie einen Incident untersucht haben, können Sie in der Aufgaben-Listenansicht („REAGIEREN“ > „Aufgaben“) Incident-Aufgaben erstellen und nachverfolgen. Erfordert ein Incident beispielsweise Maßnahmen durch ein Team außerhalb Ihres eigenen Sicherheitsteams, können Sie Korrekturaufgaben erstellen. Innerhalb der Aufgaben können Sie externe Ticketnummern vermerken. Anschließend können Sie die Tasks bis zu ihrem Abschluss nachverfolgen. Außerdem haben Sie die Möglichkeit, Aufgaben bei Bedarf zu ändern oder zu löschen, je nach Ihren Benutzerberechtigungen.

Was möchten Sie tun?

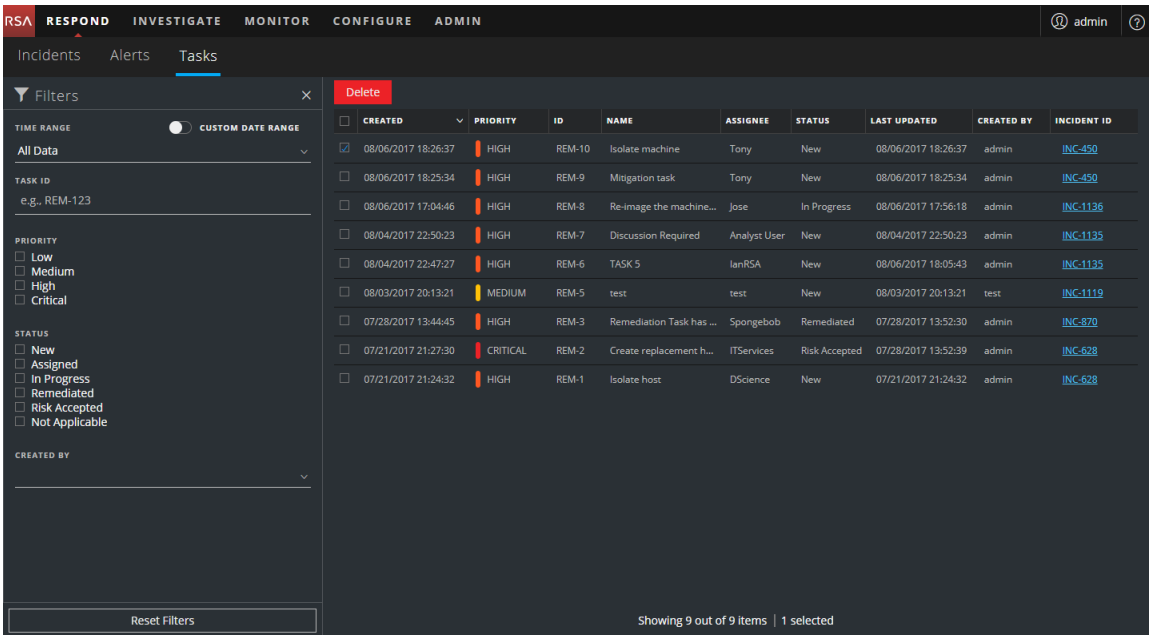
Rolle	Ziel	Details anzeigen
Incident-Experten, Analysten	Aufgaben anzeigen	Anzeigen aller Incident-Aufgaben und Anzeigen der Aufgaben im Zusammenhang mit einem Incident
Incident-Experten, Analysten	Aufgaben filtern	Filtern der Aufgabenliste
Incident-Experten, Analysten	Aufgabe erstellen	Erstellen einer Aufgabe
Incident-Experten, Analysten	Aufgaben suchen und ändern	Suchen einer Aufgabe und Ändern einer Aufgabe
Incident-Experten, Analysten	Aufgabe schließen (Status ändern in „Korrigiert“, „Risiko akzeptiert“ oder „Nicht zutreffend“)	Ändern einer Aufgabe
Incident-Experten, Analysten und SOC-Manager	Aufgabe löschen	Löschen einer Aufgabe

Verwandte Themen

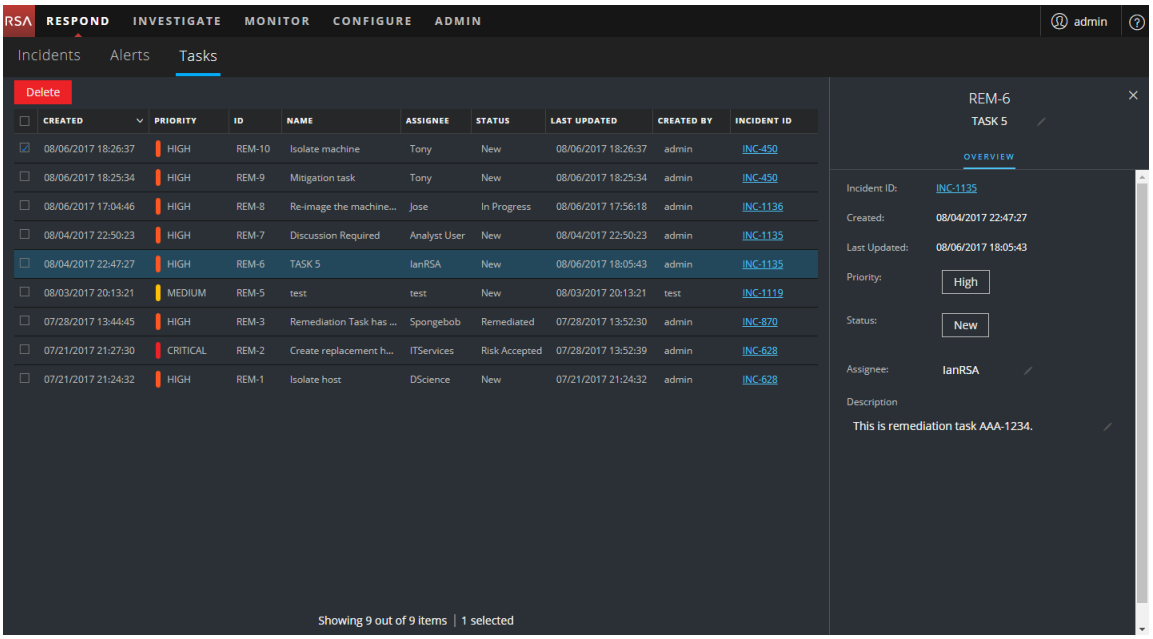
- Incident-Detailansicht
- Eskalieren oder Korrigieren des Incident

Aufgabenliste

Klicken Sie zum Öffnen der Aufgaben-Listenansicht auf **Reagieren > Aufgaben**. In der Aufgaben-Listenansicht wird eine aller Incident-Aufgaben aufgeführt.



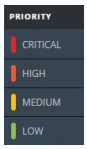
Die Aufgaben-Listenansicht besteht aus dem Bereich „Filter“, der Aufgabenliste und einem Bereich „Übersicht“ für die einzelnen Aufgaben. Die folgende Abbildung zeigt die Aufgabenliste und den Bereich „Übersicht“.



Aufgabenliste

In der Aufgabenliste werden alle Incident-Aufgaben aufgeführt. Sie können diese Liste so filtern, dass nur die Aufgaben angezeigt werden, die für Sie von Interesse sind.

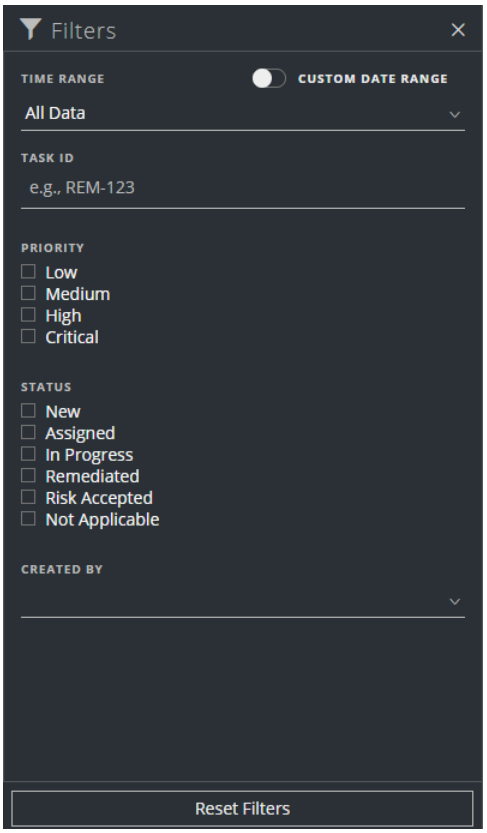
Spalte	Beschreibung
	Erlaubt die Auswahl einer oder mehrerer Aufgaben zwecks anschließendem Ändern oder Löschen. Benutzer mit entsprechenden Berechtigungen (z. B. SOC-Manager) können Massenaktualisierungen durchführen und Aufgaben löschen. Beispiel: Ein SOC-Manager möchte einem Benutzer mehrere Aufgaben gleichzeitig zuweisen.
ERSTELLT	Zeigt das Datum an, an dem die Aufgabe erstellt wurde.

Spalte	Beschreibung
PRIORITÄT	Zeigt die Priorität an, die der Aufgabe zugewiesen wurde. Die Priorität kann eine der Folgenden sein: Kritisch, Hoch, Mittel oder Niedrig. Die Priorität ist auch farbcodiert, wobei Rot **Kritisch** bedeutet, Orange **hohes** Risiko, Gelb **mittleres** Risiko und Grün **geringes** Risiko, wie in der folgenden Abbildung dargestellt ist: 
ID	Zeigt die Aufgaben-ID.
NAME	Zeigt den Aufgabennamen an.
ZUWEISUNGSEMPFÄNGER	Zeigt den Namen des Benutzers an, der der Aufgabe zugewiesen wurde.
STATUS	Zeigt den Status der Aufgabe an: „Neu“, „Zugewiesen“, „Läuft“, „Korrigiert“, „Risiko akzeptiert“ und „Nicht zutreffend“.
LETZTE AKTUALISIERUNG	Zeigt das Datum und die Uhrzeit der letzten Aktualisierung der Aufgabe an.
ERSTELLT VON	Zeigt den Benutzer an, der die Aufgabe erstellt hat.
Incident-ID	Zeigt die ID des Incident an, für den die Aufgabe erstellt wurde. Klicken Sie auf die ID, um die Details des Incident anzuzeigen.

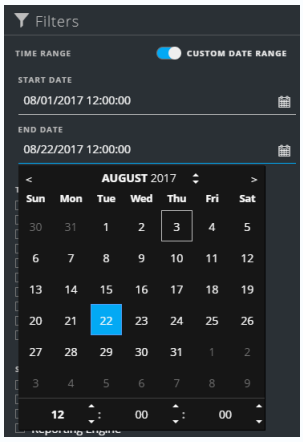
Am unteren Rand der Liste sehen Sie die Anzahl der Aufgaben auf der aktuellen Seite sowie die Gesamtzahl aller Aufgaben. Beispiel: **„23 von 23 Elementen werden angezeigt“.**

Bereich „Filter“

Auf der Abbildung unten sehen Sie die im Bereich „Filter“ verfügbaren Filter.


Filters
TIME RANGE
CUSTOM DATE RANGE
All Data
TASK ID
e.g., REM-123
PRIORITY
Low
Medium
High
Critical
STATUS
New
Assigned
In Progress
Remediated
Risk Accepted
Not Applicable
CREATED BY
Reset Filters

Im Bereich „Filter“ links der Aufgaben-Listenansicht stehen Optionen zur Verfügung, mit denen Sie die Incident-Aufgaben filtern können.

Option	Beschreibung
ZEITBEREICH	Sie können einen bestimmten Zeitraum aus der Drop-Down-Liste „Zeitbereich“ auswählen. Der Zeitbereich basiert auf dem Erstellungsdatum der Aufgaben. Wenn Sie zum Beispiel „Letzte Stunde“ auswählen, werden die Aufgaben angezeigt, die innerhalb der letzten 60 Minuten erstellt wurden.
BENUTZERDEFINIERTER DATUMSBEREICH	Sie können einen bestimmten Datumsbereich anstelle der Option „Zeitbereich“ auswählen. Klicken Sie dazu auf den weißen Kreis vor „Benutzerdefinierter Datumsbereich“, damit die Felder „Startdatum“ und „Enddatum“ angezeigt werden. Wählen Sie die gewünschten Daten und Uhrzeiten aus dem Kalender aus. 
AUFGABEN-ID	Hier können Sie die ID einer Aufgabe eingeben, die Sie suchen, z. B. „REM-123“.

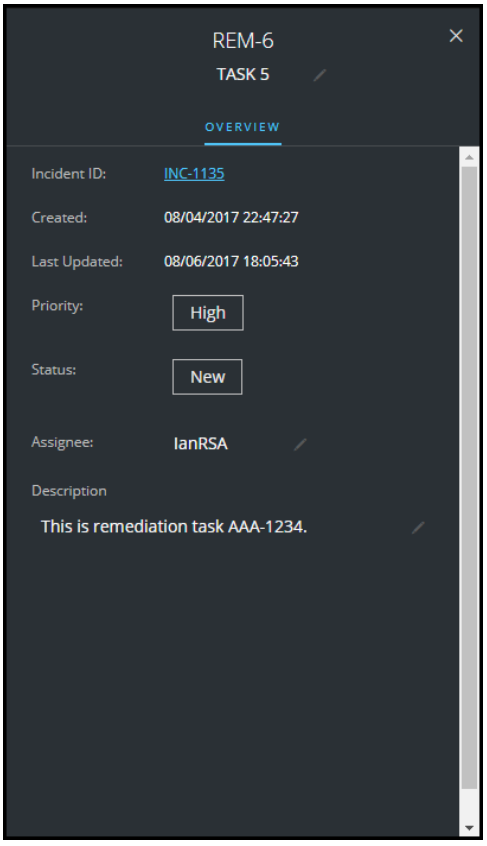
Option	Beschreibung
PRIORITÄT	Hier können Sie festlegen, Aufgaben welcher Priorität angezeigt werden sollen. Wenn Sie eine oder mehrere Prioritäten auswählen, werden in der Aufgabenliste nur die Aufgaben angezeigt, denen eine der ausgewählten Prioritäten zugewiesen ist. Beispiel: Wenn Sie „Kritisch“ auswählen, werden in der Aufgabenliste nur Aufgaben angezeigt, denen die Priorität „Kritisch“ zugewiesen wurde.
STATUS	Hier können Sie festlegen, dass nur die Aufgaben mit dem gewünschten Status angezeigt werden sollen. Wenn Sie eine oder mehrere Status auswählen, werden in der Aufgabenliste nur die Aufgaben angezeigt, denen einer der ausgewählten Status zugewiesen ist. Beispiel: Wenn Sie „Zugewiesen“ auswählen, werden im Bereich „Aufgaben“ nur Aufgaben angezeigt, die Benutzern zugewiesen wurden.
ERSTELLT VON	Hier können Sie den Benutzer auswählen, der die Aufgaben erstellt hat, die Sie anzeigen möchten. Wenn Sie beispielsweise nur die Aufgaben anzeigen möchten, die von Edwardo erstellt wurden, wählen Sie „Edwardo“ aus der Drop-down-Liste „ERSTELLT VON“ aus. Wenn Sie Aufgaben unabhängig von der Person, die sie erstellt hat, anzeigen möchten, treffen Sie unter „ERSTELLT VON“ keine Auswahl.
Filter zurücksetzen	Entfernt die Filterauswahl.

In der Aufgabenliste wird eine Liste der Aufgaben angezeigt, die Ihre Auswahlkriterien erfüllen. Die Gesamtanzahl von Elementen in der gefilterten Liste wird unter der Aufgabenliste angezeigt. Beispiel: **„18 von 18 Elementen werden angezeigt“.**

Bereich „Übersicht“ für Aufgaben

So greifen Sie auf den Bereich „Übersicht“ für eine Aufgabe zu:

1. Navigieren Sie zu **Reagieren > Aufgaben**.
2. Klicken Sie in der Aufgabenliste auf die Aufgabe, die Sie anzeigen möchten.
   Der Bereich „Übersicht“ für die Aufgabe wird rechts neben der Aufgabenliste angezeigt.



In der folgenden Tabelle sind die Felder im Bereich „Übersicht“ einer Aufgabe aufgelistet.

Feld	Beschreibung
<Aufgaben-ID>	Zeigt die ID an, die der Aufgabe automatisch zugewiesen wurde.

Feld	Beschreibung
<Aufgabenname>	Zeigt den Namen der Aufgabe an. Hierbei handelt es sich um ein bearbeitbares Feld. Wenn Sie den Namen der Aufgabe ändern möchten, können Sie durch Klicken auf den aktuellen Aufgabennamen einen Texteditor öffnen. Beispielsweise können Sie den Aufgabennamen von „Neues Image auf Laptop aufspielen“ in „Neues Image auf Server aufspielen“ ändern.
Incident-ID	Zeigt die ID des Incident an, für den die Aufgabe erstellt wurde. Klicken Sie auf die ID, um die Details des Incident anzuzeigen.
Erstellt	Zeigt Details zu Datum und Uhrzeit der Aufgabenerstellung an
Letzte Aktualisierung	Zeigt das Datum und die Uhrzeit der letzten Aktualisierung der Aufgabe an.
Priorität	Zeigt die Priorität der Aufgabe an: „Niedrig“, „Mittel“, „Hoch“ oder „Kritisch“. Wenn Sie die Priorität ändern möchten: Klicken Sie auf die Schaltfläche der Priorität und wählen Sie aus der Drop-down-Liste eine Priorität für die Aufgabe aus.
Status	Zeigt den Status der Aufgabe an: „Neu“, „Zugewiesen“, „Läuft“, „Korrigiert“, „Risiko akzeptiert“ und „Nicht zutreffend“. Wenn Sie den Status ändern möchten: Klicken Sie auf die Schaltfläche des Status und wählen Sie aus der Drop-down-Liste einen Status für die Aufgabe aus.
Zuweisungsempfänger	Zeigt den Benutzer an, der der Aufgabe zugewiesen wurde. Wenn Sie der Aufgabe einen anderen Benutzer zuweisen möchten, können Sie durch Klicken auf „(Nicht zugewiesen)“ oder den Namen des bisherigen Zuweisungsempfängers einen Texteditor öffnen.

Feld	Beschreibung
Beschreibung	Zeigt Details zur Aufgabe an. Wenn Sie die Beschreibung ändern möchten, können Sie durch Klicken auf den Text unter der Beschreibung einen Texteditor öffnen.

Symbolleistenaktionen

In dieser Tabelle werden die Aktionen aufgeführt, die auf der Symbolleiste Aufgaben-Listenansicht verfügbar sind.

Option	Beschreibung
	Öffnet den Bereich „Filter“, in dem Sie festlegen können, welche Aufgaben in der Aufgabenliste angezeigt werden sollen.
	Schließt den Bereich.
Schaltfläche **Löschen**	Löscht die ausgewählten Aufgaben.

Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“

Im Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ können Sie Entities oder Metawerte zu vorhandenen Listen hinzufügen, sie aus vorhandenen Listen entfernen oder neue Listen erstellen. Beispiel: Wenn Sie eine IP-Adresse abfragen und sie als verdächtig oder interessant bewerten, können Sie sie zu einer relevanten Liste hinzufügen, die als Datenquelle hinzugefügt wurde. Das verbessert die Sichtbarkeit der verdächtigen IP-Adresse. Sie können Entities oder Metawerte auch zu mehreren unterschiedlichen Listen hinzufügen. Beispielsweise können Sie sie einerseits zu einer Liste mit verdächtigen Domains im Zusammenhang mit Command-and-Control-Verbindungen hinzufügen und andererseits zu einer weiteren Liste mit für Remotezugriff verwendeten IP-Adressen mit Trojanerverbindung. Ist keine Liste verfügbar, können Sie eine erstellen. Sie können Entities und Metawerte außerdem aus Listen löschen.

Hinweis: Das Hinzufügen und das Entfernen von Entities und Metawerten über das Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ werden nur für als Datenquelle hinzugefügte einspaltige Listen unterstützt, nicht für mehrspaltige Listen. Wenn Sie eine Liste oder einen Wert in einer Liste über die Knotenansicht oder die Ansicht „Kontextabfrage“ bearbeiten, müssen Sie die Webseite aktualisieren, damit die aktualisieren Daten angezeigt werden.

Was möchten Sie tun?

Rolle	Ziel	Details anzeigen
Incident-Experten, Analysten	Entity zu einer Liste hinzufügen	Über die Incident-Detailansicht: Siehe Hinzufügen einer Entität zu einer Whitelist. Über die Ansicht „Warnmeldungsdetails“: Siehe Hinzufügen einer Entität zu einer Whitelist.
Incident-Experten, Analysten	Whitelist, Blacklist oder andere Liste erstellen	Eine Liste erstellen
Administratoren	Context Hub-Liste als Datenquelle hinzufügen	Siehe „Konfigurieren von Listen als Datenquelle“ im *Context Hub-Konfigurationsleitfaden*.
Administratoren	Liste für Context Hub importieren oder exportieren	Siehe „Importieren oder Exportieren von Listen für Context Hub“ im *Context Hub-Konfigurationsleitfaden*.

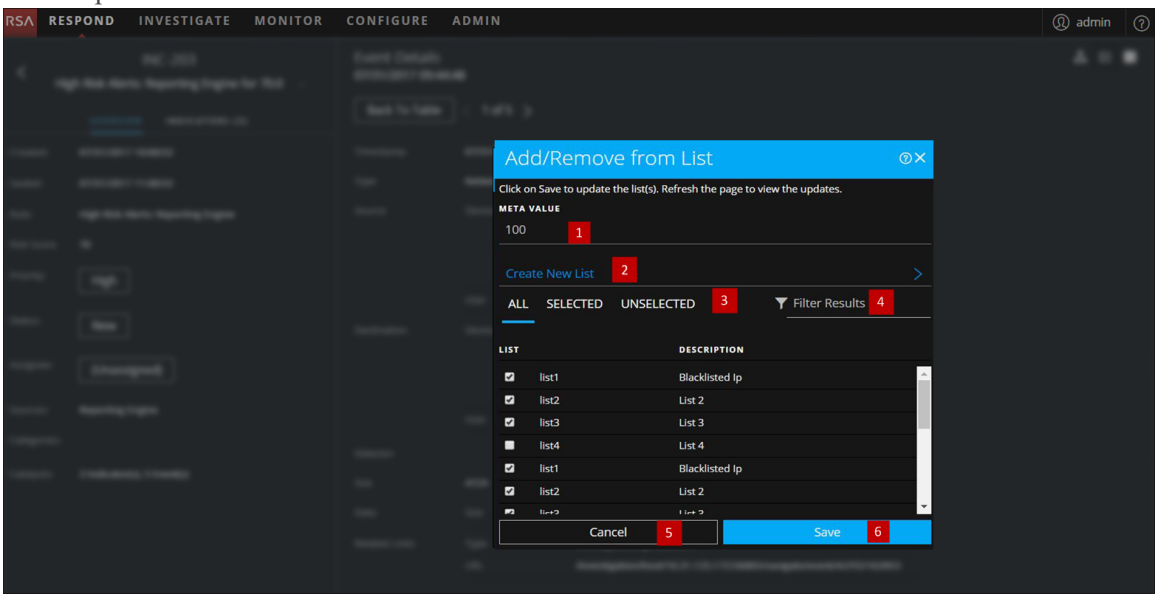
Verwandte Themen

- Untersuchen des Incident
- Überprüfen von Warnmeldungen
- Anzeigen von kontextbezogenen Informationen (Incident-Detailansicht)
- Anzeigen von kontextbezogenen Informationen (Ansicht „Warnmeldungsdetails“)

Hinweis: Listen lassen sich nicht löschen. Sie können jedoch Werte aus einer Liste löschen.

Überblick

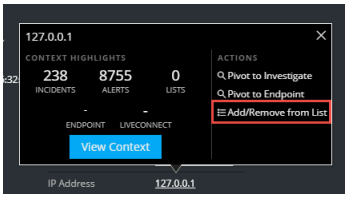
Unten sehen Sie ein Beispiel für das Dialogfeld **Zu Liste hinzufügen/Aus Liste entfernen** in der Respond-Ansicht.



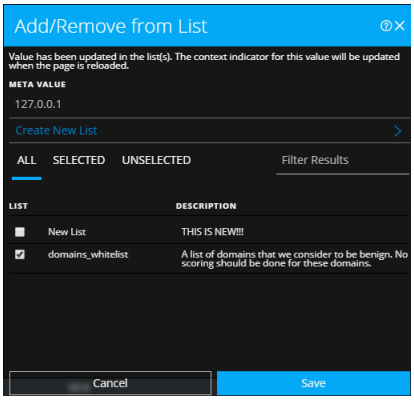
1	Hinzuzufügende oder zu entfernende Entities oder Metawerte
2	Erstellen einer neuen Liste mit den ausgewählten Metawerten
3	Auswählbare Registerkarten: „Alle“, „Ausgewählt“ und „Nicht ausgewählt“
4	Suche nach Listenname oder Listenbeschreibung
5	Abbrechen der Aktion
6	Speichern zur Aktualisierung einer Liste oder zur Erstellung einer neuen Liste

Zu Liste hinzufügen/Aus Liste entfernen

Wenn Sie das Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ aufrufen möchten: Platzieren Sie den Mauszeiger in der Incident-Detailansicht oder in der Ansicht „Warnmeldungsdetails“ auf der unterstrichenen Entity, die Sie zu einer Context Hub-Liste hinzufügen bzw. aus einer Context Hub-Liste entfernen möchten. Eine Kontext-Kurzinformation wird geöffnet und zeigt die verfügbaren Aktionen.



Klicken Sie im Abschnitt „Aktionen“ der Kurzinformation auf „Zu Liste hinzufügen/Aus Liste entfernen“. Im Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ werden die verfügbaren Listen angezeigt.



In der folgenden Tabelle sind die Optionen im Dialogfeld „Zu Liste hinzufügen/Aus Liste entfernen“ aufgeführt.

Option	Beschreibung
METAWERT	Zeigt die Entity oder den Metawert an, die/der zum Hinzufügen zu oder Entfernen aus einer oder mehreren Listen ausgewählte wurde. Sie können auch eine neue Liste mit dem ausgewählten Wert erstellen.
Neue Liste erstellen	Wenn Sie auf diese Option klicken, wird ein Dialogfeld zur Erstellung einer neuen Liste mit dem ausgewählten Metawert angezeigt.

Option	Beschreibung
ALLE	Zeigt alle verfügbaren Context Hub-Listen an. Listen, die die ausgewählte Entity bzw. den ausgewählten Wert enthalten, sind bereits ausgewählt. Aktivieren Sie das entsprechende Kontrollkästchen, um eine Entity oder einen Metawert zu einer Liste hinzuzufügen. Deaktivieren Sie das entsprechende Kontrollkästchen, um einen Wert oder eine Entity aus der Liste zu entfernen.
AUSGEWÄHLT	Zeigt nur die Listen an, in denen die ausgewählte Entity oder der ausgewählte Metawert enthalten ist. (Alle Listen sind ausgewählt.)
NICHT AUSGEWÄHLT	Zeigt nur die Listen an, in denen die ausgewählte Entity oder der ausgewählte Metawert nicht enthalten ist. (Keine Liste ist ausgewählt.)
Filtern von Ergebnissen	Geben Sie hier den Namen oder die Beschreibung einer bestimmten Liste ein, um sie unter mehreren Listen zu finden.
LISTE	Zeigt den Namen aller Listen an.
DESCRIPTION	Zeigt Informationen zur ausgewählten Liste an. In diesem Dialogfeld wird die Beschreibung angezeigt, die Sie bei der Erstellung einer Liste angeben. Beispiel: Diese Liste enthält alle IP-Adressen in der Blacklist.
Abbrechen	Bricht den Vorgang ab.
Speichern	Speichert die Änderungen.

Bereich „Kontextabfrage“ – Ansicht „Reagieren“

Der Context-Hub-Service konsolidiert kontextbezogene Informationen aus verschiedenen Datenquellen in der Ansicht „Reagieren“, damit Analysten während ihrer Untersuchungen bessere Entscheidungen treffen und die richtigen Maßnahmen ergreifen können. Der zentrale Überblick über die Entitäten, Metawerte und kontextbezogenen Informationen hilft Analysten, Schwerpunktbereiche zu ermitteln und zu priorisieren. Beispielsweise werden kürzlich erzeugte Incidents und Warnmeldungen aus der Ansicht „Reagieren“, in die eine bestimmte Entität oder ein bestimmter Metawert involviert ist, angezeigt, wenn ein Analyst zusätzliche Informationen zu der betreffenden Entität bzw. dem betreffenden Metawert abfragt. Im Bereich „Kontextabfrage“ werden kontextbezogene Informationen zu den ausgewählten Entitäten oder Metawerten angezeigt, darunter beispielsweise IP-Adresse, Benutzer, Host, Domain, Dateiname oder Datei-Hash. Welche Daten verfügbar sind, hängt von den im Context Hub konfigurierten Quellen ab.

Im Bereich „Kontextabfrage“ werden die kontextbezogenen Informationen basierend auf den Daten angezeigt, die in den konfigurierten Quellen im Context Hub verfügbar sind.

Was möchten Sie tun?

Rolle	Ziel	Anleitung
Incident-Experten, Analysten, Threat Hunters	Bereich „Kontextabfrage“ aufrufen	Über die Incident-Dateilansicht: Siehe Anzeigen von kontextbezogenen Informationen . Über die Ansicht „Warnmeldungsdetails“: Siehe Anzeigen von kontextbezogenen Informationen .
Incident-Experten, Analysten, Threat Hunters	Im Bereich „Kontextabfrage“ angezeigte Informationen zu einer bestimmten Entität verstehen	Siehe die Informationen in diesem Thema.
Administrator	Datenquellen für Context Hub konfigurieren	Siehe „Konfigurieren von Datenquellen für Context Hub“ im *Context Hub-Konfigurationsleitfaden*.

Rolle	Ziel	Anleitung
Administrator	Context Hub-Einstellungen konfigurieren	Siehe „Konfigurieren der Einstellungen von Datenquellen für den Context Hub“ im *Context Hub-Konfigurationsleitfaden*.

Verwandte Themen

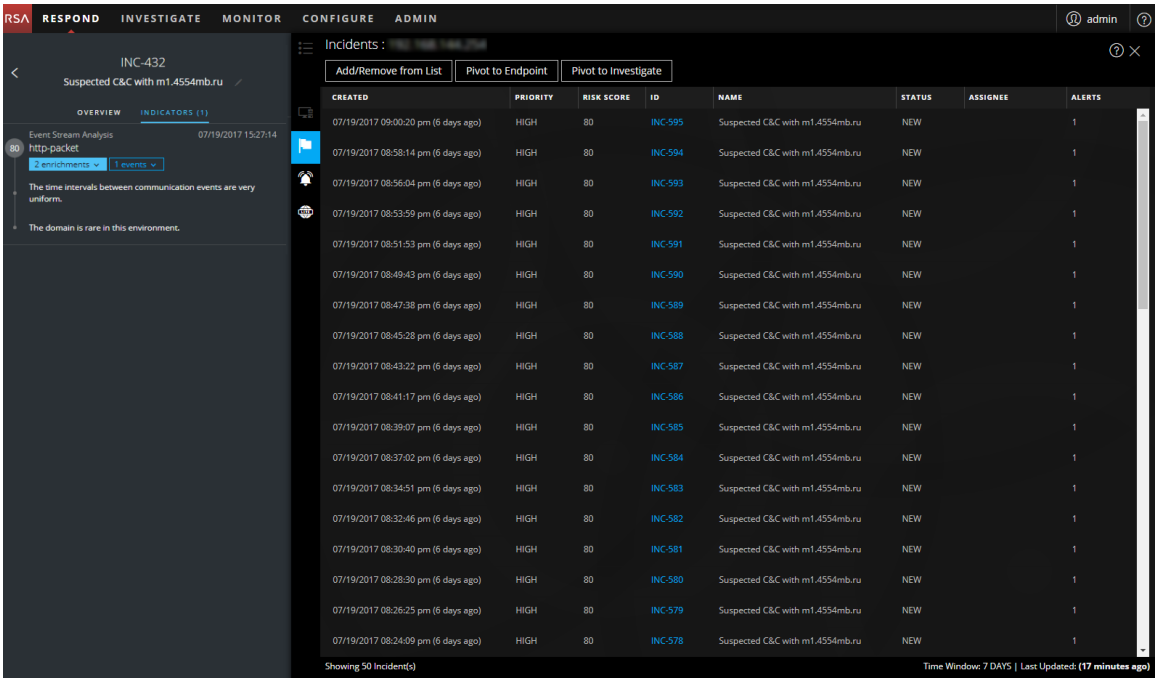
- Untersuchen des Incident
- Überprüfen von Warnmeldungen

Kontextbezogene Informationen im Bereich „Kontextabfrage“

Welche kontextbezogenen Informationen oder Abfrageergebnisse im Bereich „Kontextabfrage“ angezeigt werden, hängt von der ausgewählten Einheit und den ihr zugeordneten Datenquellen ab.

Für jede Datenquelle wird im Bereich „Kontextabfrage“ eine separate Registerkarte angezeigt. Die Registerkarte „Listendatenquelle“ wird dabei an erster Stelle im Kontextbereich angezeigt, gefolgt von den Registerkarten „Archer“, „Endpoint“, „Incidents“, „Warnmeldungen“ und „Live Connect“.

Die folgende Abbildung zeigt den Bereich „Kontextabfrage“ für eine ausgewählte Entität in der Incident-Detailansicht. Zu sehen ist die Registerkarte „Incidents“ im Bereich „Kontextabfrage“.



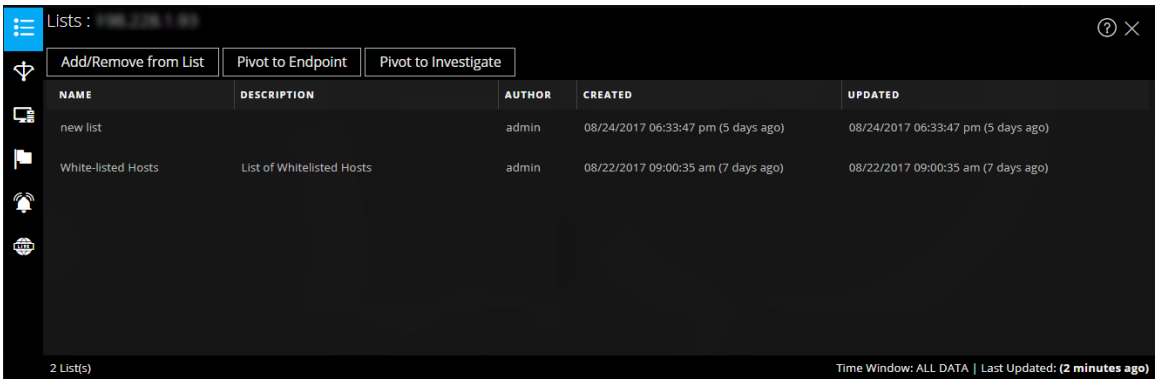
In der folgenden Tabelle sind die auf den verschiedenen Registerkarten verfügbaren Daten und die unterstützten Entitäten beschrieben.

Registerkarte	Beschreibung	Unterstützte Entitäten
(Listen)	Zeigt alle Listendaten an, die der ausgewählten Entität bzw. dem ausgewählten Metawert zugeordnet sind. Die Ergebnisse werden beginnend ab der zuletzt aktualisierten Liste angezeigt.	Alle Entitäten
(Archer)	Zeigt Informationen zu Ressourcen sowie Wichtigkeitsratings an, basierend auf der Archer-Datenquelle.	IP und Host
(Active Directory)	Zeigt alle Benutzerinformationen für den ausgewählten Benutzer an.	Benutzer

Registerkarte	Beschreibung	Unterstützte Entitäten
 (NetWitness Endpoint)	Zeigt die aus der NetWitness Endpoint-Datenquelle abgerufenen Informationen zu der ausgewählten Entität bzw. zu dem ausgewählten Metawert an, inklusive der Angaben „Rechner“, „Module“ und „IIOC-Stufen“. Module werden auf Basis des IOC-Werts sortiert (vom höchsten Wert zum niedrigsten Wert), IIOC-Stufen von der höchsten Stufe zur niedrigsten Stufe.	IP, MAC-Adresse und Host
 (Incidents)	Zeigt eine Liste aller Incidents an, die der ausgewählten Entität bzw. dem ausgewählten Metawert zugeordnet sind. Die Ergebnisse werden beginnend ab dem neuesten Incident sortiert.	Alle Entitäten
 (Warnmeldungen)	Zeigt eine Liste aller Warnmeldungen an, die der ausgewählten Entität bzw. dem ausgewählten Metawert zugeordnet sind. Die Ergebnisse werden beginnend ab der neuesten Warnmeldung sortiert.	Alle Entitäten
 (Live Connect)	Zeigt Live Connect-Informationen an.	IP, Domain und Datei-Hash

Listen

Auf der Registerkarte „Listen“ im Bereich „Kontextabfrage“ werden alle Listen angezeigt, die der ausgewählten Entität bzw. dem ausgewählten Metawert zugeordnet sind. Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Listen“ im Kontextbereich.

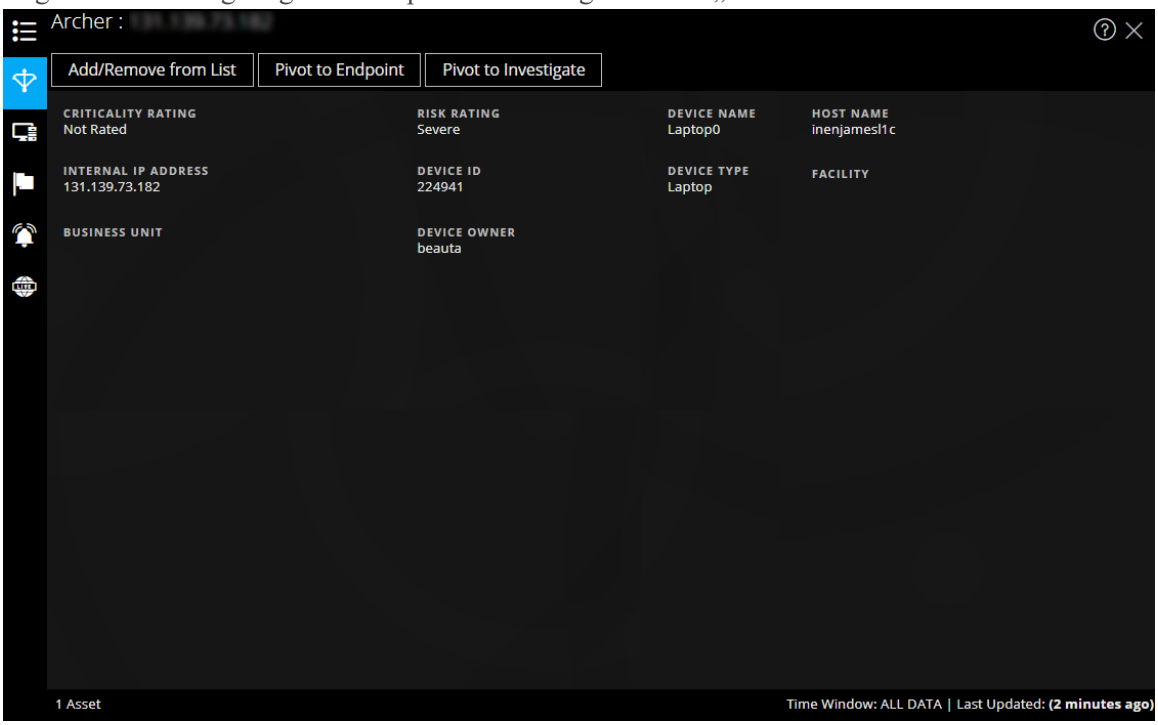


Für Listen werden die folgenden Informationen werden angezeigt:

Feld	Beschreibung
Name	Name der Liste (definiert bei der Erstellung der Liste)
Beschreibung	Beschreibung der Liste (definiert bei der Erstellung der Liste)
Verfasser	Eigentümer, der die Liste erstellt hat
Erstellt	Datum der Listenerstellung
Updated	Datum, an dem die Liste zuletzt aktualisiert oder geändert wurde
Anzahl	Anzahl der Listen, in denen die ausgewählte Entität bzw. der ausgewählte Metawert aufgeführt werden
Zeitfenster	Basiert auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfenster „Antworten konfigurieren“ festgelegt wurde. Standardmäßig werden alle Listendaten abgerufen.
Letzte Aktualisierung	Zeitpunkt, zu dem Context Hub die Abfragedaten abgerufen und im Cache gespeichert hat

Archer

Auf der Registerkarte „Archer“ im Bereich „Kontextabfrage“ werden Informationen zu Ressourcen sowie Wichtigkeitsratings angezeigt. Hierfür wird auf die Archer-Datenquellen zurückgegriffen, die den IP- und Hostentitäten bzw. den Metawerten zugeordnet sind. Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Archer“ im Kontextbereich.



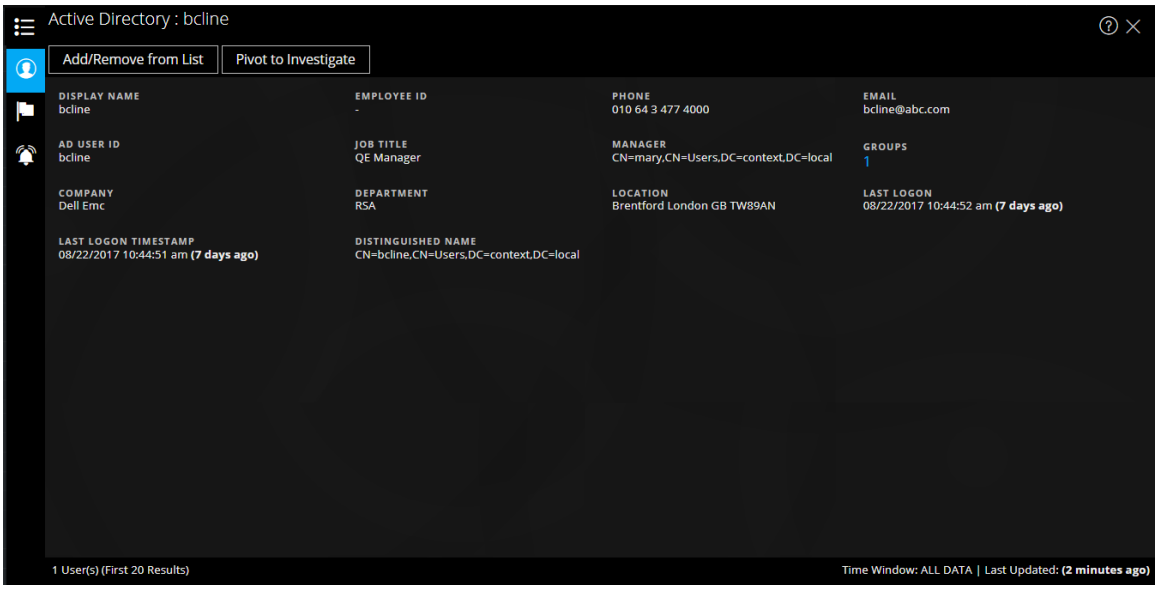
Auf der Registerkarte „Archer“ werden die nachfolgend aufgeführten Informationen angezeigt.

Feld	Beschreibung
Wichtigkeitsrating	Zeigt die operative Wichtigkeit des Geräts an, basierend auf den Anwendungen, die es unterstützt. Mögliche Wichtigkeitsratings sind „Ohne Rating“, „Niedrig“, „Mittelniedrig“, „Mittel“, „Mittelhoch“ oder „Hoch“.
Geräte-ID	Zeigt einen automatisch eingesetzten Wert an, der den Datensatz in allen Anwendungen innerhalb des Systems eindeutig identifiziert.
Gerätename	Zeigt den eindeutigen Namen des Geräts an.
Device-Eigentümer	Zeigt die Eigentümer des Geräts an, die für es verantwortlich sind. Sie sind zum Lesen und Aktualisieren des Datensatzes berechtigt.

Feld	Beschreibung
Hostname	Zeigt den Hostnamen des Geräts an.
Anlagen	Zeigt Links zu Datensätzen der Anwendung „Anlagen“ an, die mit dem Gerät in Verbindung stehen.
Geschäftsbereich	Zeigt Links zu Datensätzen der Anwendung „Geschäftsbereich“ an, die mit dem Gerät in Verbindung stehen.
Risikorating	Berechnet das Risikorating des Geräts auf Basis der letzten Bewertung und des durchschnittlichen Risikoratings aller Anlagen, in denen das Gerät eingesetzt wird. Mögliche Risikoratings sind „Schwerwiegend“, „Hoch“, „Mittel“, „Niedrig“ oder „Minimal“.
Typ	Zeigt den Gerätetyp an, z. B. Server, Laptop oder Desktop.
IP-Adresse	Zeigt die primäre interne IP-Adresse des Geräts an.
Anzahl	Zeigt die Anzahl der verfügbaren Ressourcen an.
Zeitfenster	Basiert auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfenster „Antworten konfigurieren“ festgelegt wurde. Standardmäßig werden alle Archer-Daten abgerufen.
Letzte Aktualisierung	Zeitpunkt, zu dem Context Hub die Abfragedaten abgerufen und im Cache gespeichert hat

Active Directory

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Active Directory“ im Kontextbereich.



Auf der Registerkarte „Active Directory“ im Bereich „Kontextabfrage“ werden sämtliche Informationen zu einem Benutzer sowie alle ihm zugeordneten Incidents und Warnmeldungen aufgeführt. Abfragen können die folgenden Formate haben:

- Benutzerprinzipalname
- Domain/Benutzername
- SAM-Konto-Name

Existiert ein Benutzer in mehreren Domains oder Gesamtstrukturen, werden alle verfügbaren Kontextinformationen zu dem Benutzer angezeigt.

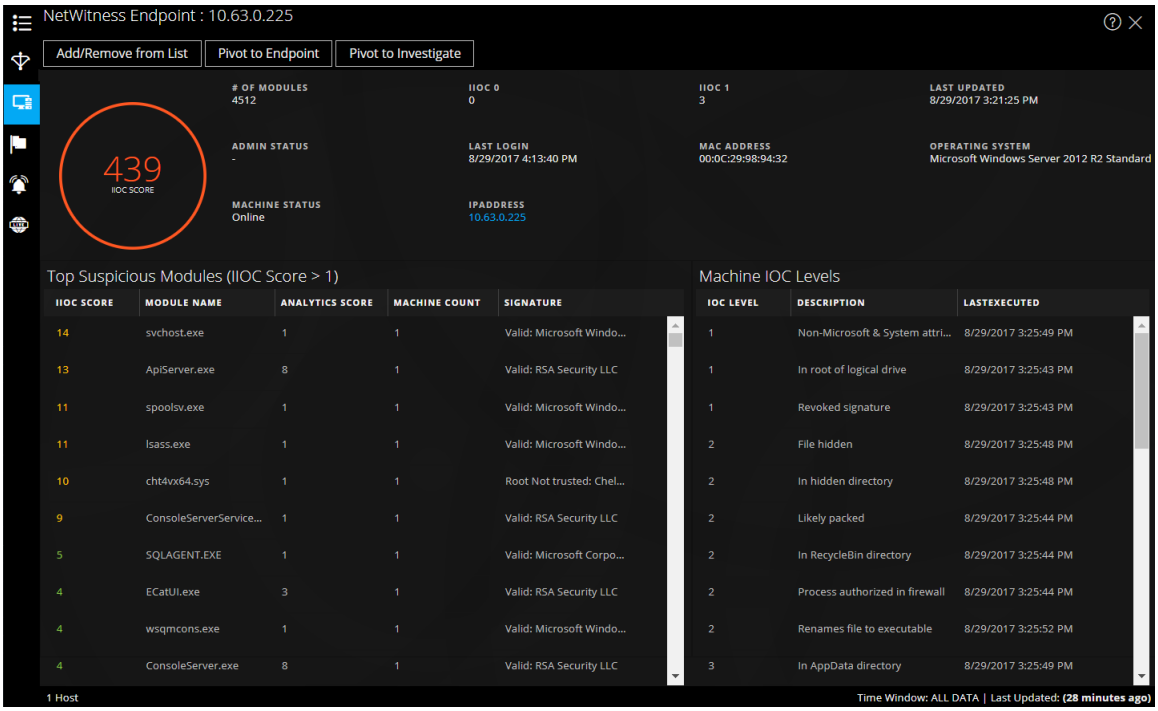
Auf der Registerkarte „Active Directory“ werden die nachfolgend aufgeführten Informationen angezeigt.

Feld	Beschreibung
Angezeigter Name	Zeigt den Namen des Benutzers an.
Mitarbeiterkennung	Zeigt die Mitarbeiterkennung des Benutzers an.
Telefon	Zeigt die Telefonnummer des Benutzers an.
E-Mail	Zeigt die E-Mail-Kennung des Benutzers an.
AD-Benutzer-ID	Zeigt die eindeutige Kennung des Benutzers innerhalb seiner Organisation an.
Position	Zeigt die Stellenbezeichnung des Benutzers an.
Manager	Zeigt den Namen des für den Benutzer zuständigen Managers an.

Feld	Beschreibung
Gruppen	Listet die Gruppen auf, in denen der Benutzer Mitglied ist.
Unternehmen	Zeigt den Namen des Unternehmens an, für das der Benutzer arbeitet.
Abteilung	Zeigt den Namen der Organisationsabteilung an, zu der der Benutzer gehört.
Standort	Zeigt den Standort des Benutzers an.
Letzte Anmeldung	Zeigt an, wann der Benutzer sich letztmals beim System angemeldet hat (nur bei Definition des globalen Katalogs).
Zeitstempel letzte Anmeldung	Zeigt an, wann sich der Benutzer beim System angemeldet hat.
Distinguished Name	Zeigt den eindeutigen Namen an, der dem Benutzer zugewiesen wurde.
Anzahl	Zeigt die Anzahl der Benutzer an.
Zeitfenster	Basiert auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfenster „Einstellungen der Datenquelle konfigurieren“ festgelegt wurde. Standardmäßig werden alle Active Directory-Daten abgerufen.
Letzte Aktualisierung	Zeitpunkt, zu dem Context Hub die Abfragedaten abgerufen und im Cache gespeichert hat

NetWitness Endpoint

Auf der Registerkarte „NetWitness Endpoint“ im Bereich „Kontextabfrage“ werden die nachfolgend aufgeführten Informationen angezeigt.



Es werden die nachfolgend aufgeführten IIOC-Informationen angezeigt.

Feld	Beschreibung
Modulanzahl	Zeigt an, wie viele Module abgefragt wurden.
Administratorstatus	Zeigt den Administratorstatus an (falls verfügbar).
Letzte Aktualisierung	Zeigt an, wann die Daten zuletzt aktualisiert wurden.
Letzte Anmeldung	Zeigt an, wann sich der Benutzer letztmals angemeldet hat.
MAC-Adresse	MAC-Adresse des Computers
Betriebssystem	Auf dem NetWitness Endpoint-Computer installierte Betriebssystemversion
Computerstatus	Zeigt den Status des abgefragten Moduls an: „Online“, „Offline“, „Aktiv“ oder „Inaktiv“.
IP-Adresse	Zeigt die IP-Adresse des betreffenden Moduls an.

Es werden die nachfolgend aufgeführten Modulinformationen angezeigt.

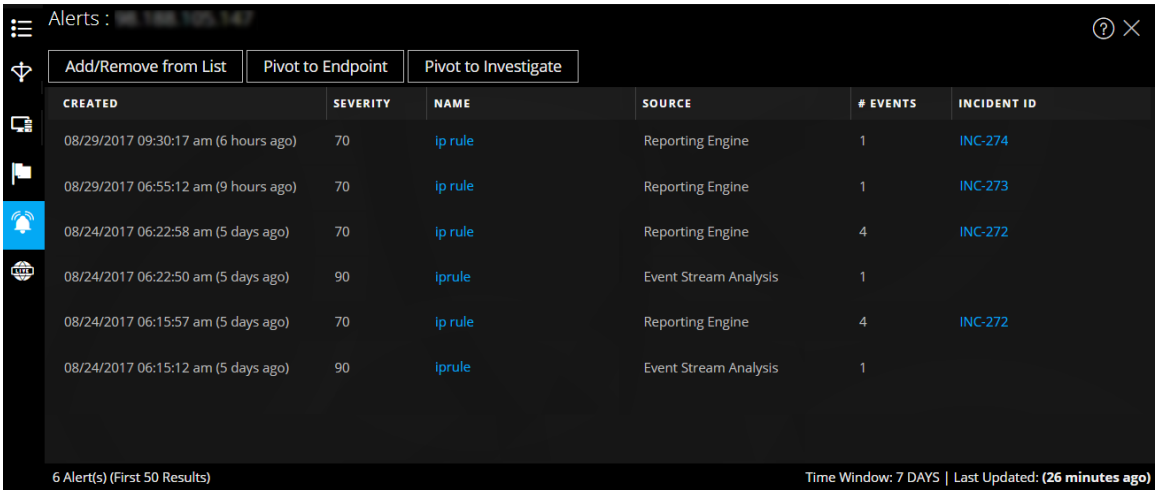
Feld	Beschreibung
IIOC-Wert	Der IIOC-Wert eines Computers ist der aus den Modulwerten aggregierte Wert. Er basiert auf dem Wert, der im Feld „IIOC-Mindestwert“ im Dialogfeld „Einstellungen für Context Hub-Datenquellen“ festgelegt wurde. Der Standardwert für „IIOC-Mindestwert“ lautet „500“. Siehe Thema „Konfigurieren der Einstellungen von Datenquellen für den Context Hub“ im *Context Hub-Konfigurationsleitfaden*.
Modulname	Name des abgefragten Moduls
Analysewert	Anzahl der aktiven Dateien für den ausgewählten Computer.
Rechneranzahl	Gibt an, wann die Scanergebnisse zuletzt in der NetWitness Endpoint-Datenbank aktualisiert wurden.
Signatur	Gibt an, ob die Datei signiert oder unsigniert bzw. gültig oder ungültig ist. Ebenfalls angegeben sind Informationen zum Unterzeichner (z. B. Google oder Apple).

Für Computer werden die nachfolgend aufgeführten Informationen angezeigt.

Feld	Beschreibung
IOC-Ebene	Zeigt die IOC-Ebenen an.
Beschreibung	Zeigt die Beschreibung der IOC-Ebene an (falls verfügbar).
Letzte Ausführung	Zeigt an, wann die Aktion ausgeführt wurde.
Anzahl	Zeigt an, wie viele Hosts abgefragt wurden.
Zeitfenster	Basiert auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfeld „Einstellungen der Datenquelle konfigurieren“ festgelegt wurde. Standardmäßig werden alle NetWitness Endpoint-Daten abgerufen.
Letzte Aktualisierung	Gibt an, wann die Scanergebnisse zuletzt in der NetWitness Endpoint-Datenbank aktualisiert wurden.

Warnmeldungen

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Warnmeldungen“ im Kontextbereich. Die Ergebnisse werden zuerst nach Eingang der Warnmeldung (neu nach alt) und dann nach Schweregrad sortiert.



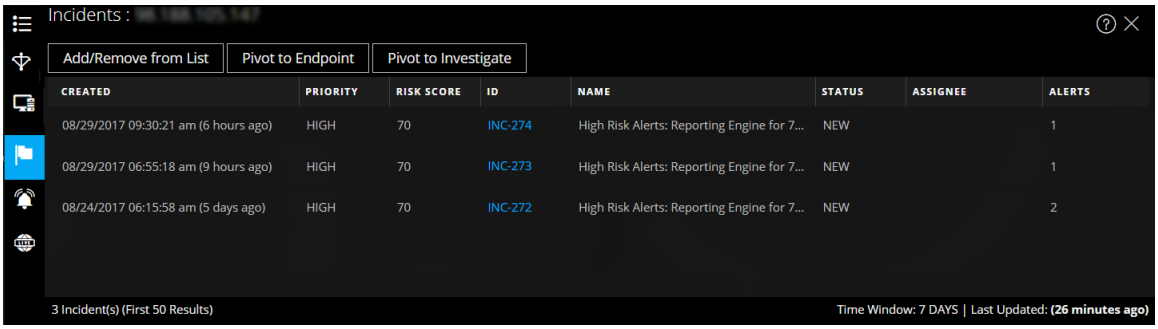
Auf der Registerkarte „Warnmeldungen“ im Bereich „Kontextabfrage“ werden die nachfolgend aufgeführten Informationen angezeigt.

Feld	Beschreibung
Erstellt	Datum und Uhrzeit der Erstellung der Warnmeldung
Schweregrad	Schweregradwert der Warnmeldungen
Name	Name der Warnmeldung. Klicken Sie auf den Namen, um die Details der Warnmeldung einzusehen.
Quelle	Name der Warnmeldungsquelle, die die Warnmeldung ausgelöst hat
Ereignisanzahl	Anzahl der Ereignisse, die der Warnmeldung zugeordnet sind
Incident-ID	Dies ist die ID des Incident, dem die Warnmeldung zugeordnet ist (falls zutreffend). Klicken Sie auf die ID, um die Details der Warnmeldung einzusehen.
Anzahl	Zeigt die Anzahl der Warnmeldungen an. Standardmäßig werden nur die ersten 100 Warnmeldungen angezeigt. Weitere Informationen zur Konfiguration der Einstellungen finden Sie im Thema „Konfigurieren der Einstellungen von Datenquellen für den Context Hub“ im *Context Hub-Konfigurationsleitfaden*.

Feld	Beschreibung
Zeitfenster	Basiert auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfeld „Einstellungen der Datenquelle konfigurieren“ festgelegt wurde. Standardmäßig werden die Warnmeldungsdaten der letzten 7 Tage abgerufen.
Letzte Aktualisierung	Gibt an, wann zuletzt kontextbezogene Daten aus der Datenquelle abgerufen wurden.

Incidents

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Incidents“ im Kontextbereich. Die Ergebnisse werden zuerst nach Eingang des Incidents (neu nach alt) und dann nach Prioritätsstatus sortiert.



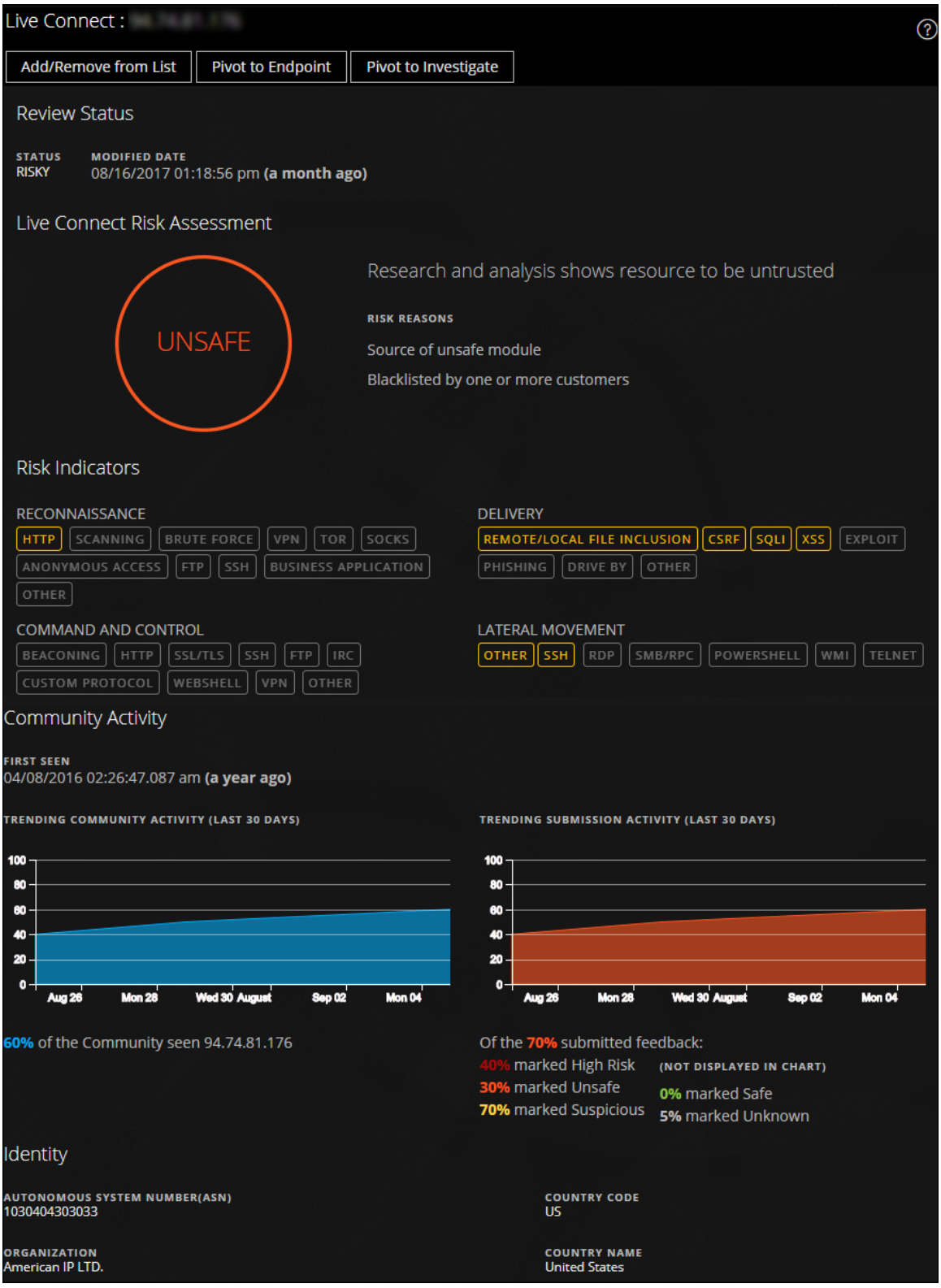
Auf der Registerkarte „Incidents“ im Bereich „Kontextabfrage“ werden die nachfolgend aufgeführten Informationen angezeigt.

Feld	Beschreibung
Erstellt	Datum der Erstellung des Incident
Priorität	Prioritätsstatus der Incidents
Risikowert	Risikowert der Incidents
ID	Incident-ID des Incident. Durch Klicken auf eine Incident-ID können Sie weitere Details zu dem betreffenden Incident einsehen.
Name	Incident-Name
Status	Status des Incident

Feld	Beschreibung
Zuweisungsempfänger	Aktueller Eigentümer des Incident
Warnmeldungen	Anzahl der Warnmeldungen, die dem Incident zugeordnet sind
Anzahl	Zeigt die Anzahl von Incidents an. Standardmäßig werden nur die ersten 100 Warnmeldungen angezeigt. Weitere Informationen zur Konfiguration der Einstellungen finden Sie im Thema „Konfigurieren der Einstellungen von Datenquellen für den Context Hub“ im *Context Hub-Konfigurationsleitfaden*.
Zeitfenster	Basiert auf dem Wert, der im Feld „Abfrage der letzten“ im Dialogfenster „Einstellungen der Datenquelle konfigurieren“ festgelegt wurde. Standardmäßig werden die Warnmeldungsdaten der letzten 7 Tage abgerufen.
Letzte Aktualisierung	Gibt an, wann zuletzt kontextbezogene Daten aus der Datenquelle abgerufen wurden.

Live Connect

Die folgende Abbildung zeigt ein Beispiel für die Registerkarte „Live Connect“ im Kontextbereich.


Live Connect :
Add/Remove from List
Pivot to Endpoint
Pivot to Investigate
Review Status
STATUS
RISKY
MODIFIED DATE
08/16/2017 01:18:56 pm (a month ago)
Live Connect Risk Assessment
UNSAFE
Research and analysis shows resource to be untrusted
RISK REASONS
Source of unsafe module
Blacklisted by one or more customers
Risk Indicators
RECONNAISSANCE
HTTP SCANNING BRUTE FORCE VPN TOR SOCKS ANONYMOUS ACCESS FTP SSH BUSINESS APPLICATION OTHER
DELIVERY
REMOTE/LOCAL FILE INCLUSION CSRF SQLI XSS EXPLOIT PHISHING DRIVE BY OTHER
COMMAND AND CONTROL
BEACONING HTTP SSL/TLS SSH FTP IRC CUSTOM PROTOCOL WEBSHELL VPN OTHER
LATERAL MOVEMENT
OTHER SSH RDP SMB/RPC POWERSHELL WMI TELNET
Community Activity
FIRST SEEN
04/08/2016 02:26:47.087 am (a year ago)
TRENDING COMMUNITY ACTIVITY (LAST 30 DAYS)
100
80
60
40
20
0
Aug 26
Mon 28
Wed 30 August
Sep 02
Mon 04
TRENDING SUBMISSION ACTIVITY (LAST 30 DAYS)
100
80
60
40
20
0
Aug 26
Mon 28
Wed 30 August
Sep 02
Mon 04
60% of the Community seen 94.74.81.176
Of the 70% submitted feedback:
40% marked High Risk
30% marked Unsafe
70% marked Suspicious
(NOT DISPLAYED IN CHART)
0% marked Safe
5% marked Unknown
Identity
AUTONOMOUS SYSTEM NUMBER(ASN)
1030404303033
ORGANIZATION
American IP LTD.
COUNTRY CODE
US
COUNTRY NAME
United States

Im Bereich „Live Connect“ werden die folgenden Informationen angezeigt:

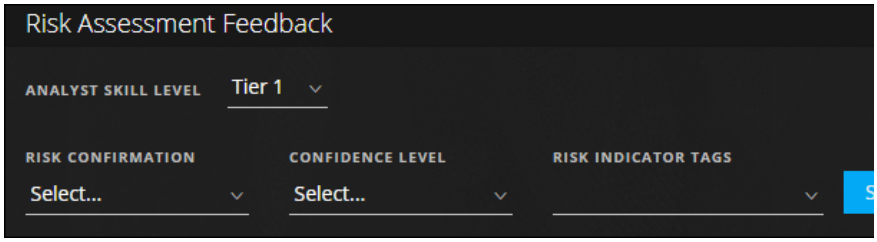
- Prüfstatus
- Live Connect-Risikobewertung
- Risikoindikatoren
- Community-Aktivität
- WHOIS
- Verwandte Dateien, Domains und IPs
- Identität
- Zertifikatinformationen

Auf der Registerkarte „Live Connect“ im Bereich „Kontextabfrage“ werden die nachfolgend aufgeführten Informationen angezeigt.

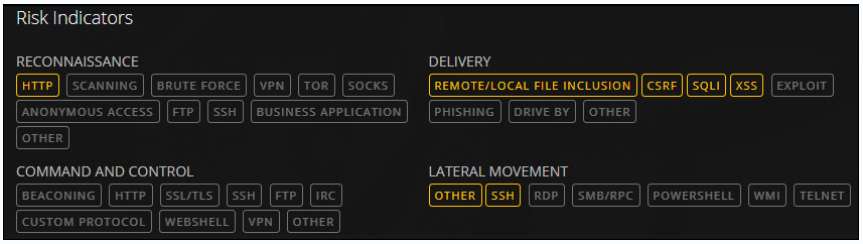
Feld	Beschreibung
Prüfstatus	Zeigt den Überprüfungsstatus der ausgewählten Live Connect-Entität an (IP, Datei oder Domain), basierend auf der Analystenaktivität. Das ermöglicht Transparenz hinsichtlich der Analystenaktivität innerhalb eines Unternehmens. **Status** Nachfolgend sind die verschiedenen Statustypen aufgeführt: • **Neu:** Wenn Abfrageergebnisse für eine IP-Adresse erstmals innerhalb des Unternehmens abgerufen werden. • **Angezeigt:** Wenn die Abfrageergebnisse für eine IP-Adresse bereits von Analysten innerhalb des Unternehmens abgerufen wurden. • **Als sicher markiert:** Wenn ein Analyst innerhalb des Unternehmens die Suchergebnisse für eine IP-Adresse bereits abgerufen und die IP-Adresse als sicher markiert hat. • **Als riskant markiert:** Wenn ein Analyst innerhalb des Unternehmens die Suchergebnisse bereits angezeigt und die IP-Adresse als riskant markiert hat.

Feld	Beschreibung
Risikobewertung	Zeigt die Risikobewertung für die ausgewählte Live Connect-Entität an (IP, Datei oder Domain), basierend auf der Live Connect-Analyse und Feedback von Analysten. Die Kategorien der Risikobewertung lauten: • **Sicher:** Die Live Connect-Entität gilt als sicher. • **Unbekannt:** In Live Connect liegen nicht genügend Informationen zu der Entität vor, um das Risiko berechnen zu können. • **Hohes Risiko**: Basierend auf der Analyse und den Risikogründen der Community mit „Hohes Risiko“ gekennzeichnet. Die mit „Hohes Risiko“ gekennzeichneten Entitäten erfordern sofortige Maßnahmen. • **Verdächtig**: Basierend auf der Analyse und den Risikogründen der Community als „Verdächtig“ gekennzeichnet. Die Analyse deutet auf eine potenziell bedrohliche Aktivität hin, die Maßnahmen erfordert. • **Unsicher:** Basierend auf der Analyse und den Risikogründen der Community als „Verdächtig“ gekennzeichnet. Die Entität wurde als „Hohes Risiko“, „Verdächtig“ oder „Unsicher“ eingestuft. Die entsprechenden Risikogründe werden angezeigt.

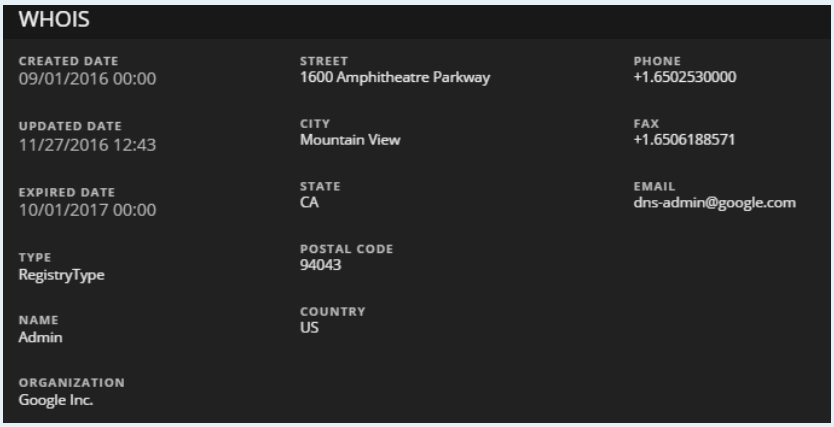
Feld	Beschreibung
Feedback zur Risikobewertung	Über das Feedback zur Risikobewertung können Analysten Threat Intelligence-Feedback zu einer Entität an den Live Connect-Server übermitteln. • **Kompetenzebene des Analysten** Nachfolgend sind die möglichen Kompetenzebenen eines Analysten aufgeführt: ◦ **Tier 1:** Analysten auf dieser Kompetenzebene definieren in der Regel Korrekturverfahren und entscheiden, ob ein Incident an andere Stellen innerhalb des SOC (Security Operations Center) eskaliert werden soll. Dies ist der Standardwert. ◦ **Tier 2:** Analysten auf dieser Kompetenzebene untersuchen Incidents, dokumentieren die Untersuchung und leiten ihr Feedback an die anderen SOC-Workflows weiter. ◦ **Tier 3:** Analysten auf dieser Kompetenzebene leiten die Untersuchungsergebnisse an die SOC-Teams weiter. Sie sind im Allgemeinen für das Incident-Management verantwortlich und verfügen über umfassende, fundierte Fähigkeiten in Bezug auf die Incident-Reaktion und den Umgang mit den zugehörigen Tools. **Hinweis:** Bei der Erstellung eines neuen NetWitness Suite-Benutzers (Analysten) sollten Administratoren angeben, ob es sich um einen Tier-1-, Tier-2- oder Tier-3-Analysten handelt. • **Risikobestätigung:** die Risikobestätigung für die ausgewählte Live Connect-Entität (IP, Datei oder Domain). Es existieren folgende Kategorien für die Risikobestätigung: ◦ **Sicher**: Die Live Connect-Entität gilt als sicher. ◦ **Unbekannt**: Dem Analysten liegen nicht genügend Informationen für eine Risikobestätigung vor. ◦ **Hohes Risiko**: Basierend auf der Analyse und den Risikogründen der Community mit „Hohes Risiko“ gekennzeichnet. Die mit „Hohes Risiko“ gekennzeichneten Entitäten erfordern sofortige Maßnahmen. ◦ **Verdächtig**: Basierend auf der Analyse und den Risikogründen

Feld	Beschreibung
	der Community als „Verdächtig“ gekennzeichnet. Die Analyse deutet auf eine potenziell bedrohliche Aktivität hin, die Maßnahmen erfordert. ◦ **Unsicher**: Basierend auf der Analyse und den Risikogründen der Community als „Unsicher“ gekennzeichnet. • **Konfidenzniveau:** das Konfidenzniveau, das ein Analyst seinem Feedback zur Live Connect-Entität beimisst. Es existieren folgende Kategorien für das Konfidenzniveau: ◦ Hoch ◦ Mittel ◦ Niedrig • **Risikoindikatortags:** Hier können Sie eine Tagkategorie auswählen, basierend auf der Analyse. 

Feld	Beschreibung
Community-Aktivität	Community-Aktivitäten wie: • Datum, an dem die Community das Problem erstmals bemerkt hat • Verstrichene Zeit, seitdem die Community die IP/Datei/Domain erstmals bemerkt hat (aktueller Zeitpunkt - Zeitpunkt des ersten Bemerkens) **Trending-Community-Aktivität:** Wenn die IP-Adresse innerhalb der RSA-Community bekannt ist, wird eine grafische Darstellung des Community-Aktivitätstrends für folgende Parameter angezeigt: • Benutzer (in %), von denen die IP-Adresse in der Live Connect-Community im Lauf der Zeit angezeigt wurde • Benutzer (in %), die Feedback für die IP-Adresse übermittelt haben. • Benutzer (in %), von denen die IP-Adresse im Lauf der Zeit als „Unsicher“ markiert wurde

Feld	Beschreibung
Risikoindikatoren	Risikoindikatoren werden basierend auf den Tags hervorgehoben, die den Entitäten (IPs, Dateien oder Domains) von der Community zugewiesen werden.  Die Tags werden wie folgt kategorisiert: • Aufklärung • Lieferung • Command and Control • Laterale Bewegung • Rechteerweiterung • Verpackung und Exfiltration Diese Tags sind Muster und variieren je nach den Eingaben aus der Community, die auf dem Live Connect-Server eingehen. Der Analyst kann die entsprechenden Risikoindikatortags auswählen, während er Prüfungsfeedback verfasst. Hervorgehobene Tags bedeuten, dass die ausgewählte Entität der betreffenden Kategorie und dem betreffenden Tag zugeordnet ist. Durch Klicken auf ein hervorgehobenes Tag können Sie die Beschreibung des Tags einsehen.

Feld	Beschreibung
Identität	Zeigt die folgenden Identitätsinformationen für die ausgewählte Entität bzw. den ausgewählten Metawert an: Für IP-Adressen: • Autonomous System Number (ASN) • Präfix • Ländercode und Name des Landes • Registrierter Benutzer (Organisation) • Datum Für Datei-Hashes: • Dateiname • Dateigröße • MD5 • SH1 • SH256 • Kompilierzeit • MIME-Typ Für Domains: • Domainname • Zugeordnete IP-Adresse
Zertifikatinformationen	Zeigt die folgenden Zertifikatinformationen für den ausgewählten Datei-Hash an • Aussteller des Zertifikats • Gültigkeit des Zertifikats • Signaturalgorithmus • Seriennummer des Zertifikats

Feld	Beschreibung
WHOIS-Informationen	Die **WHO IS**-Informationen geben Details bezüglich des Eigentums für eine bestimmte Domain an.  Die folgenden Informationen zum Domaineigentümer werden angezeigt: • Erstellungsdatum • Aktualisierungsdatum • Ablaufdatum • Typ (Registrierungstyp) • Name • Organisation • Adresse mit Postleitzahl • Land • Telefonnummer • Fax • E-Mail-Adresse

Feld	Beschreibung
Verwandte Dateien	Verwandte Dateien werden für Entitäten der Typen „IP“ und „Domain“ angezeigt. Eine Liste der bekannten zugehörigen Dateien wird zusammen mit den folgenden Informationen angezeigt: • Live Connect-Risikorating („Sicher“, „Riskant“ oder „Unbekannt“) • Dateiname • MD5 • Kompilierzeit und Kompilierdatum • Import-Hash der API-Funktion • MIME-Typ
Verwandte Domains	Verwandte Domains werden für Entitäten der Typen „IP“ und „Dateien“ angezeigt. Eine Liste der bekannten zugehörigen Domains wird zusammen mit den folgenden Informationen angezeigt: • Live Connect-Risikorating („Sicher“, „Riskant“ oder „Unbekannt“) • Domainname • Name des Landes • Registrierungsdatum • Ablaufdatum • E-Mail-Adresse des Registranten

Feld	Beschreibung
Verwandte IPs	Verwandte IPs werden für Entitäten der Typen „Domain“ und „Dateien“ angezeigt. Eine Liste der bekannten zugehörigen IPs wird zusammen mit den folgenden Informationen angezeigt: • Live Connect-Risikorating („Sicher“, „Riskant“ oder „Unbekannt“) • IP-Adresse • Domainname • Ländercode und Name des Landes • Name des Landes • Registrierungsdatum • Ablaufdatum • E-Mail-Adresse des Registranten