RSA NETWITNESS® PLATFORM

Versionshinweise

Für Version 11.2

Kontaktinformationen

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

Marken

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

Lizenzvereinbarung

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

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

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

Drittanbieterlizenzen

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

Hinweis zu Verschlüsselungstechnologien

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

Verteilung

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

Inhalt

Einführung

In diesem Dokument sind Verbesserungen und Korrekturen in RSA NetWitness® Platform 11.2.0.0 aufgeführt. Lesen Sie dieses Dokument vor der Bereitstellung von oder der Aktualisierung auf NetWitness® Platform 11.2.0.0.

Neuheiten

Die RSA NetWitness ® Platform Version 11.2.0.0 bietet neue Funktionen und Verbesserungen für die Untersuchung von Protokollen, Paketen und Endpunkten. Im Rahmen dieser Veröffentlichung wird die Nutzer-und Entitätenverhaltensanalyse eingeführt, mit der sich Angriffe und identitätsbasierte Anomalien erkennen und untersuchen lassen.

NetWitness Analyse des Benutzer- und Entitätsverhaltens (UEBA)

RSA NetWitness® UEBA ist jetzt Teil der RSA NetWitness® Platform. NetWitness UEBA bietet umfassende Analysen vo Benutzer- und Entitätsverhalten, mit denen fortgeschrittene interne Angriffe und identitätsbasierte Anomalien besser erkannt und untersucht werden können und darauf reagiert werden kann.

NetWitness UEBA hat folgende Funktionen: UEBA:

- nutzt dynamische statistische Ausreißeranalysen die Erstellung von Verhaltensbaselines, die Verhaltensmodellierung und die Peer-Group-Analytik zur Aufdeckung anomalen Verhaltens, seitlicher Bewegung, Insiderbedrohungen und Datenexfiltration.
- identifiziert verdächtige verhaltensbasierte Anomalien mithilfe von unbeaufsichtigten Algorithmen des maschinellen Lernens.
- erzeugt ein Identitäts-und Alarmmodell, damit für Indikatoren für hohes Risiko nur der Schweregrad und die Priorität erhöht, und die Warnmeldungsmüdigkeit und falsch positiven Ergebnisse reduziert werden.

NetWitness UEBA Bereitstellung von Services Deployment. NetWitness UEBA kann über den NetWitness Platform-Admin-Server konfiguriert und eingesetzt werden. NetWitness UEBA Server erfasst Windows-Protokolldaten von NetWitness Platform-Services, verarbeitet die Daten und zeigt die Ergebnisse auf der NetWitness-Oberfläche an. Wenn der NetWitness Insights Endpoint-Agent bereitgestellt wird, werden auch die erfassten Windows-Protokolldaten analysiert. Weitere Informationen zur Bereitstellung von UEBA finden Sie im *Handbuch zur Installation physischer Hosts* oder im *Handbuch zur Installation virtueller Hosts*.

In der Version 11.2 unterstützt UEBA nativ eine Vielzahl folgender Windows-Protokollquellen wie:

- Windows/Active Directory
- Windows-Anmelde- und -Authentifizierungsaktivität
- Windows-Dateiserver

Erstellung von Baselines für Identitätsverhalten. Maschinelle Lernmodelle werden auf historische und Echtzeitdaten zur Erstellung von Verhaltensbaselines angewendet. Sie helfen bei der Identifizierung von Ausreißern und geben einen Einblick in organisatorische und individuelle Kennzahlen. Die Standard-Modellierungsrichtlinie wird nach einer 30-tägigen Schulungszeit ausgeführt. Werden darüber hinaus zusätzliche historische Daten gespeichert, kann der Schulungszeitraum so geändert werden, das sie zu einem früheren Zeitrahmen ausgeführt wird. Nur im Vergleich zu dieser Baseline ungewöhnliche Verhaltensweisen führen zu Anomalien oder Infizierungsindikatoren.

Untersuchung der wichtigsten Warnmeldungen und Benutzer mit hohem Risiko. Mithilfe eines vordefinierten Out-of-the-Box (OOTB)-Dashboard und einer Reporting-Funktion können Analysten die wichtigsten Warnmeldungen (Warnmeldung, die durch eine Sequenz von Indikatoren innerhalb einer Stunde (also einer vollen Stunde) ausgelöst werden) und risikoreichen Benutzer (Benutzer mit einer hohen Risikobewertung) untersuchen. Analysten können Benutzer, die sofortige Aufmerksamkeit benötigen, erkennen, tiefere Ermittlungen durchführen und die Risikowerte reduzieren.

NetWitness UEBA-Lizenz. Die NetWitness UEBA-Lizenz basiert auf der Gesamtzahl der Benutzer in Ihrer Organisation. Benutzer sind Personen, die über Netzwerkzugriff und Berechtigungen verfügen. Wenn die Zahl der Benutzer fünf Prozent (5 %) der erworbenen Lizenz übersteigt, müssen Sie neue Lizenzen erwerben. Weitere Informationen erhalten Sie bei Ihrem RSA Account Manager. Weitere Informationen zur Lizenzierung finden Sie im *Leitfaden zum Lizenzierungsmanagement*.

Weitere Informationen zu UEBA finden Sie im *Benutzerhandbuch zu NetWitness Analyse des Benutzer- und Entitätsverhaltens*.

NetWitness Respond

Zugriff auf die Ereignisanalyse direkt aus der Ansicht „Incident-Details“. Sie können nahtlos auf die Ereignisanalyse aus der Investigate-Ansicht im Ablauf des Bereichs „Indikatoren“ eines Incident zugreifen. Zur Untersuchung eines Incident können Sie auf einen Ereignistyp-Hyperlink im Ablauf eines Ereignisses klicken, um die Ereignisanalyse in Respond zu öffnen.

Es wurde die Möglichkeit hinzugefügt, Incidents aus NetWitness Respond an RSA Archer zu senden. Wenn der RSA Archer als Datenquelle im Context Hub konfiguriert ist, können Sie Incidents an Reaktion auf Cyber-Incidents und Sicherheitsverletzungen von RSA Archer senden. Ist diese Option konfiguriert, wird die Schaltfläche „An Archer senden“ sowie „An Archer-Status gesendet“ in NetWitness Respond angezeigt. Sie haben auch die Möglichkeit, die Incident-Liste nach an Archer gesendete Incidents zu filtern. Wenn Sie einen Incident an Archer senden, erstellt das System automatisch einen Eintrag im Journal für den Incident.

Wechseln von Incidents zu RSA Archer. Sie können zu RSA Archer wechseln, um für bestimmte Entitäten Gerätedetails und andere Informationen in RSA Archer® Reaktion auf Cyber-Vorfälle anzuzeigen. Bei diesen Entitäten handelt es sich um IP-Adresse, Host und Mac-Adresse. Im Bereich „Kontextabfrage“ können Sie die Attribute für die unterstrichene Entität anzeigen, z. B. Geschäftseinheitwerte, Gerätenamen, Gerätetyp usw. Weitere Informationen finden Sie im *NetWitness Respond-Benutzerhandbuch*.

Die manuelle Erstellung von Incidents in der Ansicht „Warnmeldungsliste“ wurde verbessert. Sie können eine Priorität, einen Zuweisungsempfänger und Kategorien hinzufügen, wenn Sie einen Incident manuell aus Warnmeldungen heraus erstellen.

Es wurde die Möglichkeit hinzugefügt, Nodes-Typen im Node-Diagramm auszublenden. Damit Sie die Wechselwirkungen zwischen den Entitäten im Node-Diagramm weiter untersuchen können, können Sie die Node-Typen auswählen, die Sie in das Node-Diagramm einfügen möchten. Dies kann besonders hilfreich sein, wenn ein Node-Diagramm über 100 Nodes enthält.

Der Incident-Filter wurde für zugewiesene und nicht zugewiesene Incidents angepasst. Im Feld „Incident-Liste Filter“ können Sie nicht mehr gleichzeitig nach Zuweisungsempfängern und nicht zugewiesenen Incidents filtern. Wenn Sie „Nur nicht zugewiesene Incidents anzeigen“ aktivieren, ist die Drop-down-Liste „Zuweisungsempfänger“ nun deaktiviert. Wenn Sie einen Zuweisungsempfänger aus der Drop-down-Liste auswählen, ist die Option „Nur nicht zugewiesene Incidents anzeigen“ nun deaktiviert.

Die Benutzererfahrung wurde durch die Sortierung der Incident-Liste verbessert. Sie können im Spaltenkopf an eine beliebige Stelle in der Liste klicken, um die Sortierung zu ändern. Sie müssen nicht mehr auf die Pfeile nach oben oder nach unten klicken, um die Liste zu sortieren.

Weitere Informationen finden Sie im *NetWitness Respond – Benutzerhandbuch* und im *Konfigurationsleitfaden zu NetWitness Respond*.

NetWitness Investigate

Kontextinformationen für einen Metawert in der Ereignisanalyse. Der Bereich „Kontextabfrage“, der zuvor in den Ansichten „Navigation“ und „Ereignisse“ verfügbar war, wurde nun auch in der Ansicht „Ereignisanalyse“ hinzugefügt. Im Bereich „Kontextabfrage“ Details zu Elementen angezeigt, die mit einem Ereignis (IP-Adresse, Benutzer, Host, Domain, MAC-Adresse, Dateiname, Datei-Hash) im Context Hub zusammenhängen. Sie können mit den Metawerten eines Ereignisses interagieren, um weitere Einblicke zu erhalten, einschließlich verwandter Incidents, Warnmeldungen, benutzerdefinierter Listen, RSA Archer-Ressourcen, Active Directory-Details und NetWitness Endpoint-Thick-Client. Weitere Informationen finden Sie unter „Anzeigen von zusätzlichem Kontext für einen Datenpunkt“ im *NetWitness-Investigate – Benutzerhandbuch*.

Wechseln aus den Metawerten in die Ansicht „Ereignisanalyse“. Sie können nun von diesen unterstrichenen Entitäten – IP-Adresse, Mac und Host – in die Ansicht „Ereignisanalyse“ von RSA Archer wechseln, um Gerätedetails anzuzeigen.

Freitextabfragen in der Ansicht „Ereignisanalyse“. Der Freitextmodus ist eine Alternative zum Basismodus der Abfragen (geleitet), der in früheren Versionen verfügbar war. Im Freitextmodus können Analysten komplexe Textabfragen eingeben und zwischen Freitextmodus und geleitetem Modus wechseln. Weitere Informationen finden Sie unter „Filtern von Ereignissen in der Ansicht ‚Ereignisanalyse‘“ im *NetWitness Investigate – Benutzerhandbuch*.

Zu den Profilverbesserungen gehören Profilgruppen, neue und aktualisierte Profile sowie die PreQuery für ein Profil in der Brotkrümelnavigation. Weitere Informationen finden Sie unter „Einkapseln von benutzerdefinierten Ansichten mithilfe von Profilen“ im *NetWitness Investigate – Benutzerhandbuch*.

- Mit Profilgruppen können Sie Profile in logische Gruppen organisieren, zum Beispiel verschiedene Profilgruppen für verschiedene Anwendungsfälle oder für verschiedene Benutzer. Sie können bestehende und neue Profile in Profilgruppen verschieben.

- Ein neues Out-of-the-Box-Profil namens RSA Endpoint-Analyse verwendet eine PreQuery in `device.type=nwendpoint` und die Metagruppe und Spaltengruppen der RSA Endpoint-Analyse.
- Im Profil der RSA-Bedrohungsanalyse werden folgende drei Metaschlüssel ersetzt:
  `risk.warning` ist jetzt `behavior of compromise (boc)`
  `risk.suspicious` ist jetzt `indicator of compromise (ioc)`
  `risk.informational` ist jetzt `enabler of compromise (eoc)`
- Wenn ein Profil in der Ansicht „Navigation“ oder „Ereignisse“ ausgewählt wird, wird die PreQuery für das Profil in der Brotkrümelnavigation angezeigt.

Die Konfiguration der Suchoptionen wurde verbessert. Das Menü für die Einstellung von Suchoptionen wurde neu geordnet, damit es übersichtlicher und leichter auszuwählen ist. Weitere Informationen finden Sie unter „Konfigurieren der Ansichten „Navigation“ und „Ereignisse““ im *NetWitness Investigate – Benutzerhandbuch*.

Verbesserungen des Bereichs „Textanalyse“. In der Ansicht „Ereignisanalyse“ wurden mehrere Verbesserungen an der Benutzerfreundlichkeit bei der Betrachtung von Daten vorgenommen.

- Neue Seitenumbruchskontrollen ermöglichen mehr Flexibilität beim Blättern durch eine Liste von Ereignissen.
- Wenn ein rekonstruiertes Ereignis im Bereich „TextanalyseW eine Anfrage oder Antwort hat, die die maximale Anzahl von Bytes überschreitet, zeigt der Header an, dass die Nachricht abgeschnitten wurde. Damit werden für die Ansicht der Textanalyse eines Ereignisses, das für die Darstellung zu lang ist, möglichst viele Daten bereitgestellt.

Ereignisquellenmanagement

Identifizieren von Ereignisquellen im Leerlauf. Dieses neue Attribut zeigt die Anzahl der Tage an, die vergangen sind, seit von jeder Ereignisquelle zuletzt ein Protokoll empfangen wurde. Sie können dieses Attribut für Gruppenereignisquellen verwenden, die für eine bestimmte Zeit (zum Beispiel 90 Tage) zur Überprüfung oder zum Entfernen großer Datenmengen im Leerlauf waren.

Context Hub

Option für Import- oder Exportattribute. Die Attribute im Bereich „Kontextabfrage“ können nun so verwaltet werden, das Benutzer die für RSA Archer-Gerätedetails vorgesehene Attribute anzeigen können. Sie können das Attribut von Interesse aus der Geräteanwendung von RSA Archer konfigurieren und diese Attribute im Kontextfeld anzeigen. Dazu können Sie die vorhandenen Attribute exportieren, das neue Attribut hinzufügen und den aktualisierten Satz von Attributen importieren. Diese Attribute werden in der im Bereich „Kontextabfrage“ importierten Reihenfolge widergespiegelt, wenn Sie den Kontext für einen Incident oder ein Ereignis in der Ansicht „Ereignisanalyse“ anzeigen. Weitere Informationen finden Sie im *Context Hub-Konfigurationsleitfaden*.

Mit dem NetWitness-Server implementierte Services

Neuer Contentdienst. Mit dem neuen **Contentdienst** werden die von RSA zur Verfügung gestellten und vom Benutzer erstellten Parser-Regeln verwaltet. Sie können jetzt Parser-Regeln in der Benutzeroberfläche hinzufügen. Der Contentdienst wird auf der Registerkarte „Protokoll-Parser-Regeln“ verwendet, die später in diesem Dokument im Abschnitt Protokollanalyse beschrieben wird.

Log und Netzwerk-Decoder

Unterstützung für Standard-PCAPNG-Dateien. Mit dem Netzwerk-Decoder können nun Standard-PCAPNG-Dateien geschrieben, damit ein offeneres Datenbankformat zur Verfügung steht. Diese Funktion ist standardmäßig aktiviert, wenn Sie 11.2 direkt installieren. Wenn Sie von einer früheren Version auf 11.2 aktualisieren, müssen Sie PCAPNG-formatierte Datenbankdateien manuell aktivieren, was zu einer Verringerung des Speicherplatzes um ungefähr 4% führen kann (da die PCAPNG-Dateien mehr Platz benötigen als die NWDB-Dateien). Sie können PCAPNG-Format auch mit 10 Gbit/s-Erfassung verwenden, wodurch die Leistung nicht signifikant verringert wird (< 1 %).

So aktivieren Sie den neuen Konfigurations-Node:
`/database/config/packet.file.type = 'netwitness' or 'pcapng'`

Neuer GeoIP2-Parser. Der neue GeoIP2-Parser wandelt IP-Adressen in geografische Standorte um, stellt das neueste Maxmind GeoIP-Paket zur Verfügung und unterstützt IPv6-Adressen sowie IPv4. Der GeoIP2-Parser liest aus `ip.src`, `ip.dst`, `ipv6.src` und `ipv6.dst`, um GeoIP-Informationen zu erzeugen, und ist standardmäßig im Decoder aktiviert. Weitere Informationen finden Sie unter „GeoIP2“ und „GeoIP-Parser“ im *Konfigurationsleitfaden für Decoder und Log Decoder*.

GeoIP-Suchen auf IPv4-/IPv6-Metadaten. Sie können nun GeoIP-Suchen auf allen IPv4-oder IPv6-Metadaten durchführen, so dass Sie geografische Informationen in Szenarien verstehen können, wenn `ip.src` und `ip.dst` nicht im Mittelpunkt der Analyse stehen.

- Es gibt eine neue Lua-API, mit der Lua-Parsern vollständig auf alle GeoIP2-Informationen zugreifen können. Die Lua-API gibt die angeforderten Informationen aus der GeoIP2-Datenbank zurück. Der Parser kann diese Informationen dann nutzen, um Metadaten zu erstellen oder eine eigene Analyse durchzuführen.
- Sie können den nativen GeoIP2-Parser so konfigurieren, dass er GeoIP2-Metadaten für jeden IPv4- oder IPv6-Schlüssel mit dem `config`-Node `parsers.options` erzeugt.

Weitere Informationen finden Sie unter „GeoIP2“ und „GeoIP-Parser“ im *Konfigurationsleitfaden für Decoder und Log Decoder*.

TLS-Zertifikat-Hashes. Der Netzwerk-Decoder kann Hashes von Zertifikaten erzeugen, die im Paketstream zu sehen sind. Diese Hashes sind der SHA-1-Wert eines DER-kodierten Zertifikats, das bei einem TLS-Handshake erkannt wird. Die gehashten Daten werden in den `cert.checksum`-Schlüssel geschrieben. Mithilfe der produzierten Hashes kann der Netzwerkverkehr mit Hashes aus öffentlichen SSL-Blacklists verglichen werden. Weitere Informationen finden Sie unter „TLS-Zertifikat-Hashes“ im *Konfigurationsleitfaden für Decoder und Log Decoder*.

Benutzeroberfläche

Die Registerkarte „Protokoll-Parser-Regeln“ wurde verschoben. Die Registerkarte „Protokoll-Parser-Regeln“ unter „ADMIN > Ereignisquellen“ der Version 11.1 wurde in der Version 11.2 nach „KONFIGURIEREN“ verschoben.

Zusätzliche Sprachunterstützung wurde hinzugefügt. In den Benutzereinstellungen gibt es eine neue Sprachoption, mit der Sie eine andere verfügbare Sprache auswählen können. Die ausgewählte Sprache verändert den Text in ganz NetWitness Platform. Weitere Informationen finden Sie im Handbuch *Erste Schritte mit NetWitness Platform*.

Rebranding für NetWitness. Das NetWitness 11.2-Produkt hat über die gesamte Benutzeroberfläche, Dokumentation und andere relevante Anzeigen folgendes neues Branding erhalten:

1. RSA NetWitness® Suite in RSA NetWitness® Platform
2. RSA NetWitness® Packets in RSA NetWitness® Netzwork
3. RSA NetWitness® Logs und Packets in RSA NetWitness® Logs & Network
4. Paket Hybrid-Hosttyp in Network Hybrid-Hosttyp
5. Packet Decoder-Hosttyp in Network Decoder-Hosttyp
6. RSA NetWitness® SecOps Manager in RSA Archer® Cyber Incident & Breach Response

Administration

Konfigurierbare Kontextmenüaktionen in Investigate. In Investigate verfügbar Kontextmenüaktionen können nun mithilfe der Benutzeroberfläche für Kontextmenüaktionen mit verschiedenen Feldern und Gruppen konfiguriert werden. Sie können neue Kontextmenüaktionen erstellen und diese mit Hilfe der unter „ADMIN > System“ verfügbaren Kontextmenüaktionen verwalten. Die mithilfe der Benutzeroberfläche konfigurierten Kontextmenüaktionen können als Kontextmenüaktion für Metaschlüssel auf der Registerkarte „Ermittlungen“ unter den Ansichten „Navigation“, „Ereignisse“ und „Ereignisanalysen“ angezeigt werden. Auch in der Ereignisanalyse werden Kontextmenü-Aktionen für Metaschlüssel unterstützt.

Verbessertes Anmelde-Bannerverfügbar. Das Anmelde-Banner enthält nun vollständig anpassbaren Text und erhöhte Sicherheitsmaßnahmen.

Protokollanalyse

Die Registerkarte „Protokoll-Parser-Regeln“ wurde verbessert. In RSA wurde die Möglichkeit hinzugefügt, bestehende Protokoll-Parser zu erweitern, benutzerdefinierte Protokoll-Parser hinzuzufügen und Protokoll-Parser-Regeln für Ihre Protokoll-Parser zu aktualisieren. Durch Protokoll-Parser-Regeln ändert sich die Art und Weise, wie Meta-Informationen aus den Ereignisquellen extrahiert werden. Sie können Protokoll-Parser-Regeln hinzufügen, die bestehende Protokoll-Parser in Ihrem System und den Standard-Protokoll-Parser erweitern, der Metadaten aus Nachrichten extrahiert, die anderenfalls als unbekannt aufgeführt werden könnten. Weitere Informationen finden Sie im *Handbuch für Protokollparser-Anpassungen* unter dem RSA-Link. In 11.1 waren die Protokoll-Parser-Regeln schreibgeschützt.

Upgradeanweisungen

Die folgenden Upgradepfade werden für RSA NetWitness® Platform 11.2.0.0 unterstützt:

- RSA NetWitness® Platform 10.6.6.x auf 11.2.0.0
- RSA NetWitness® Platform 11.0.x oder 11.1.x auf 11.2.0.0

Weitere Informationen zum Upgrade auf 11.2.0.0 finden Sie in den Upgradeanweisungen im Abschnitt Installation und Upgrade.

Behobene Probleme

In diesem Abschnitt werden die Probleme aufgeführt, die seit der letzten -Hauptversion behoben wurden.

Sicherheit

Rückverfolgungsnummer	Beschreibung
ASOC-58379	Moderates CentOS 7 glibc Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:0805
ASOC-58373	Sicherheitsaktualisierung für CentOS 7-Kernel https://access.redhat.com/errata/RHSA-2018:1629
ASOC-58376	dhcp-Sicherheitsaktualisierung: https://access.redhat.com/errata/RHSA-2018:1453
ASOC-58374	procps-ng-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:1700
ASOC-58381	ntp-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:0855
ASOC-58384	gcc-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:0849
ASOC-58380	krb5-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:0666
ASOC-50151	openssh-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:0980
ASOC-58367	openjdk-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:1649
ASOC-58377	libvorbis-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:1058

Rückverfolgungsnummer	Beschreibung
ASOC-52448	Authconfig-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2017:2285
ASOC-52439	Libx11-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2017:1865
ASOC-52443	NetworkManager-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2017:2299
ASOC-52444	Bash-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2017:2299
ASOC-52445	Openldap-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2017:1852
ASOC-49815	Systemd-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:0260

Allgemeine Anwendungsprobleme

Rückverfolgungsnummer	Beschreibung
ASOC-46483	Das System meldet inaktive Benutzer in der Ansicht „Reagieren“ und einigen Ansichten von „Investigation“ ab.

Untersuchen

Rückverfolgungsnummer	Beschreibung
ASOC-51011	Drei neue Metagruppen für 11.0 und dieselben Spaltengruppen für 11.1 werden nicht erstellt, wenn Sie ein Upgrade von 10.6.5 auf 11.x durchführen: RSA Endpoint Analysis, RSA Outbound HTTP, RSA Outbound SSL/TLS.
ASOC-50702	Nach dem Upgrade auf 11.1 gibt es nicht übereinstimmende Datentypen zwischen dem Log Decoder- (table-map.xml) und Concentrator-Definitionen (index-concentrator.xml).

Rückverfolgungsnummer	Beschreibung
ASOC-50924	Der Versuch einer direkten Abfrage oder einer Abfrage über den Link, die einen IPv6-Metawert mit nicht unterstützten Sonderzeichen verwendet, generiert einen Fehler in der Ansicht „Ereignisanalyse“ und der Ansicht „Navigation“.
ASOC-50771	Wenn Sie über die Ansicht „Ereignisse“ aus der Ereignisanalyse wechseln, entweder durch Klicken auf den Link „Ereignisanalyse“ oder durch Klicken mit der rechten Maustaste auf eines der Ereignisse, funktionieren die Optionen im Kontextmenü für Metawerte nicht.
ASOC-49854	Das Drehfeld für die Serviceauswahl lädt unendlich.
ASOC-50712	Metaentitäten können bei deaktivierter Option „Optimieren des Ladens der Seite ‚Investigation‘“ nicht zu einer benutzerdefinierten Spaltengruppe hinzugefügt werden.
ASOC-50349	Benutzerdefinierte Spaltengruppen, die Metadaten enthalten, können in der Ansicht „Ereignisse“ erstellt werden, aber wenn die benutzerdefinierte Spaltengruppe in der Ansicht „Ereignisanalyse“ verwendet wird, werden die in der Metaentität enthaltenen Metaschlüssel in den Ergebnissen nicht angezeigt.
ASOC-50041	Wenn Sie in der Ansicht „Ereignisanalyse“ mit der rechten Maustaste auf einen Metawert klicken, der ein Semikolon enthält, und versuchen, den Drill-down in einer neuen Registerkarte in der Ansicht „Navigation“ anzuwenden, wird ein Fehler angezeigt: Visualisierung kann nicht aufgebaut werden.
ASOC-45198	Wenn Sie die URL ändern und die neue URL für ein eingeschränktes Ereignis ist, bleibt der rekonstruierte Inhalt für die vorherige Abfrage in der Ansicht „Ereignisanalyse“ bestehen und es wird keine Fehlermeldung angezeigt.
ASOC-48945	Wenn Sie eine Abfrage für eine Sitzung eingeben, auf die Sie in der Ansicht „Ereignisanalyse“ einen Zugriff haben, werden keine Daten und keine Fehlermeldung angezeigt.
ASOC-48710	Wenn Sie in der Ansicht „Ereignisanalyse“ ermitteln, wird die folgende Fehlermeldung zurückgegeben: „Ein unerwarteter Fehler ist aufgetreten.“

Reagieren

Rückverfolgungsnummer	Beschreibung
ASOC-40749	Der Respond-Administrator kann im Dashboard keine Investigate-Dashlets abfragen oder Live-Dashlets anzeigen.
ASOC-41891	Der Link für Security Analytics Incident Management in NetWitness SecOps Manager 1.3.1.2 ist in NetWitness Suite 11.1.0.0 nicht gültig.
ASOC-46834	„Domain für verdächtige C&C“ und „Domain“ können in der Regelerstellung nicht ausgewählt werden.
ASOC-50911	Die Aggregation wird beendet, nachdem eine erneute Verbindung mit Mongo hergestellt wurde.
ASOC-51480	Endpoint-Ereignisse mit einer Detektor-IP werden nicht durch die Endpoint-Incident-Regel aggregiert und erzeugen keine Incidents mit der Bedingung der aktuellen Standard-Incident-Regel. Weitere Informationen finden Sie unter „Standard-Incident-Regeln“ im *Konfigurationsleitfaden für NetWitness Respond*.

Event Stream Analysis (ESA)

Rückverfolgungsnummer	Beschreibung
ASOC-50201	Wenn Sie neue ESA-Regeln in der Ansicht „Integrität und Zustand“ bereitstellen und eine neue Policy unter Event Stream-Analysen mithilfe der Statistik für die ESA-Regelarbeitsspeichernutzung erstellen, sind keine bereitgestellten ESA-Regeln aufgeführt.

Nicht unterstützte Funktionen

Die folgenden Tabellen enthalten Informationen zu Funktionen, die in RSA NetWitness® Platform 11.1 oder späteren Versionen nicht mehr unterstützt werden.

In 11.1.0.0 oder späteren Versionen nicht unterstützte Funktionen

Nr.	Funktion	Anmerkungen
1	Malware Colo	Malware-Colocation wird in 11.1.0.0 und späteren Versionen nicht unterstützt. Malware Analysis wird als eigenständige Malware Analysis-Instanz unterstützt.
2	All-in-One(AIO)-Bereitstellung	Die All-in-One-Bereitstellung wird nicht unterstützt. Die Neuinstallation von AIO wurde entfernt.
3	Eigenständiger Warehouse Connector	Der eigenständige Warehouse Connector wird nicht unterstützt.
4	Verwaltungsfunktionen	1. Eigenes Passwort vergessen 2. E-Mail-Benachrichtigung an Benutzer, wenn das Passwort abläuft 3. AD-Benutzertest/-suche
5.	Pivotal	Pivotal wird nicht unterstützt.
6.	Warehouse Analytics	Warehouse Analytics wird nicht unterstützt.

In zukünftigen Versionen verfügbare Funktionen

Die folgenden Funktionen sind nicht in 11.2 verfügbar und werden in einer zukünftigen Version zur Verfügung stehen.

Nr.	Funktion	Anmerkungen
1	IPDB-Reporting	Der IPDB Extractor-Service wird in 11.2.0.0 nicht unterstützt und in späteren Versionen verfügbar sein.

Nr.	Funktion	Anmerkungen
2	STIG	Wenn Sie über einen sicherheitsverstärkten STIG-Host verfügen, können kein Upgrade auf Version 11.2.0.0 durchführen, da die Backupskripte dies nicht unterstützen.
3	Unterstützung für mehrere Security Analytics-Server (NetWitness-Server)	Eine Bereitstellung mit mehreren Servern wird nicht unterstützt.
4	PKI-Authentifizierung	Die PKI-Authentifizierungsfunktion ist in Version 11.2.0.0 nicht verfügbar.
6	Endpunktanalyse	Analysen wie der Risikowert oder die IOC-Berechnung werden für Endpunktscandaten nicht unterstützt.
7	Endpunktkorrektur	Funktionen zur Reaktion (Eingrenzung/Blockierung) werden nicht unterstützt.
8	Endpunktnachverfolgung	Die Nachverfolgung von Netzwerkereignissen wird nicht unterstützt.
9	Endpunktkernelmodus	Der Endpoint-Agent arbeitet derzeit im Benutzermodus und bietet keine Unterstützung für die Erkennung im Kernelmodus.
10	Endpunktdateireputation	Abfragen nach der Dateireputation wie OPSWAT, YARA und Reversing Lab werden nicht unterstützt und können Dateien daher nicht in die Whitelist oder Blacklist hinzufügen.

Bekannte Probleme

In diesem Abschnitt werden Probleme beschrieben, die in dieser Version fortbestehen. Sofern ein Workaround verfügbar ist, werden ausführliche Anmerkungen oder Verweise eingefügt.

Bekannte Probleme während des Upgrades auf Version 11.2

Die folgenden bekannten Probleme treten während eines Upgrades von Version 10.6.6 auf Version 11.2 oder einer Aktualisierung von Version 11.1 oder 11.1.x auf 11.2 auf.

Der wiederholte STIX-Feed beim Upgrade von 10.6.6 auf 11.2 schlägt fehl.

Rückverfolgungsnummer: ASOC-61227

Problem: Wenn Sie Security Analytics 10.6.6 auf NetWitness Platform 11.2 aktualisieren, funktioniert der wiederkehrende STIX-Feed, den Sie mit HTTPS URL erstellt haben. Das liegt daran, dass in 10.6.x standardmäßig alle Zertifikate vertrauenswürdig sind. Dies ist in 11.2 jedoch nicht der Fall. In 11.2 wird die Option „Allen Zertifikaten vertrauen“ zur Verfügung gestellt und standardmäßig deaktiviert.

Workaround: Navigieren Sie zu „Konfigurieren“ > „Benutzerdefinierte Feeds“ und bearbeiten Sie den fehlgeschlagenen Feed. Zur Lösung des Problems aktivieren Sie entweder die Option „Allen vertrauen“ oder laden ein gültiges SSL-Zertifikat hoch. Bei weiteren Fragen wenden Sie sich bitte an den RSA-Kundendienst.

Beim Upgrade auf NetWitness Platform 11.2 werden die Lizenzdetails nicht in der AWS-Cloud gespeichert.

Rückverfolgungsnummer: ASOC-61614

Problem: Wenn Sie von Security Analytics 10.6.6 auf NetWitness Platform 11.2 aktualisieren, wird die Lizenzserver-ID nicht gespeichert. Der Adminserver kann daher ndie Lizenzserverdaten nicht aus dem externen Backend-System abrufen und Services können nicht lizenziert werden.

Workaround: Folgen Sie den Schritten unter „Zugriff auf Download Central“ und „Registrieren des Servers (online)“ im *Leitfaden zum Lizenzmanagement*. Hier erfahren Sie, wie Sie die Lizenzdetails aus dem externen Backend-System abrufen und die neue Lizenzserver-ID registrieren.

Offlinelizenzen werden nach einem Upgrade von 10.6.6 auf 11.2.0.0 nicht beibehalten.

Rückverfolgungsnummer: ASOC-41757

Problem: Selbst wenn Sie eine neue Antwort-BIN-Datei aus Download Central hochgeladen haben, funktionieren Offlinelizenzen nicht. Obwohl alte Dateien in `/var/lib/fneserver` wiederhergestellt sind, bleiben die Lizenzen weiterhin deaktiviert.

Workaround: Führen Sie zum Wiederherstellen der Lizenzen die folgenden Schritte aus:

1. Erzeugen Sie eine neue Antwort-BIN-Datei von Download Central.
2. Stellen Sie eine SSH-Verbindung mit einem NetWitness-Serverhost 11.2.0.0 (AdminServer) her.

3. Verschieben Sie RA*-Dateien (3 Dateien) aus `/var/lib/fneserver/`.
4. Melden Sie sich bei der RSA NetWitness 11.2.0.0-Benutzeroberfläche mit Administratorbenutzeranmeldedaten an und navigieren Sie zur Registerkarte **ADMIN** > **System** > **Lizenzdetails**.
5. Klicken Sie auf **Lizenzen aktualisieren**.
6. Laden Sie die Antwortdatei auf Download Central hoch. Navigieren Sie zur Registerkarte **ADMIN** > **System** > **Lizenzierung** > **Einstellungen**.
7. Klicken Sie auf **Antwort hochladen**.

Hinweis: Ein Upgrade mit dem Onlinemodus (RSA NetWitness Suite 11.2.0.0 mit Internetverbindung) funktioniert erfolgreich und alle Lizenzen werden nach dem Upgrade auf 11.2.0.0 wiederhergestellt.

Die Investigation-Links sind für statische Diagramme nach dem Upgrade von 10.6.6 auf 11.2 deaktiviert.

Rückverfolgungsnummer: ASOC-42136

Problem: Der Investigation-Link ist für das statische Diagramm (das Ergebnis des Berichts weist das Diagrammformat auf) deaktiviert, in dem die Datenquelle als NetWitness Suite-Broker vorhanden ist (dieser Service ist standardmäßig verfügbar).

Workaround: Für dieses Problem gibt es zwei Workarounds:

- Die Regeln, die das Ergebnis als ein statisches Diagramm festlegen, können im tabellarischen Format angezeigt werden, und Investigation funktioniert wie erwartet.
- Oder Sie können die folgenden Schritte durchführen, um das Problem zu beheben:
  1. Löschen Sie den NetWitness Suite-Broker und fügen Sie ihn mit demselben Namen erneut als Datenquelle zur Reporting Engine hinzu.
  2. Wenn die Berichte mit einem statischen Diagramm geplante Berichte sind, funktioniert der Investigation-Link bei der nächsten Ausführung wie erwartet.
  3. Wenn der Bericht ein Ad-hoc-Bericht ist, führen Sie den Bericht erneut aus, um die Investigation-Links wiederherzustellen.

Nach dem Upgrade von 10.6.6 auf 11.2 kann das Geomap-Dashlet nicht mithilfe eines vorkonfigurierten Diagramms (OOTB) erstellt werden.

Rückverfolgungsnummer: ASOC-41896

Problem: Wenn Sie ein Upgrade auf NetWitness Suite 11.2.0.0 durchführen, kann das Geomap-Dashlet nicht mithilfe eines vorkonfigurierten Diagramms erstellt werden. Dies geschieht, wenn ein benutzerdefiniertes Dashboard ein Geomap-Dashlet verwendet, das mit einem vorkonfigurierten Diagramm erstellt wird.

Workaround: Die Datenquelle muss für dieses vorkonfigurierte Diagramm, das für die Verwendung im Dashlet mit Geomap erforderlich ist, manuell aktualisiert werden. Oder erstellen Sie ein neues Diagramm mit derselben vorkonfigurierten Regel und verwenden Sie das neue Diagramm im Geomap-Dashlet.

Wenn Sie den Entropy Parser und die Indexierungsnutzlast verwendet haben, müssen Sie nach einem Upgrade von 11.x auf 11.2 das Bucket-Flag zur Indexdatei hinzufügen, damit der Entropy Parser Index-Buckets verwenden kann.

Rückverfolgungsnummer: ASOC-45721

Problem: Wenn Sie ein Upgrade von Version 11.0 auf Version 11.2 durchführen, den Entropy Parser auf dem Decoder (nur Pakete) verwendet haben und die Nutzlast indexieren, müssen Sie das Bucket-Flag zu Ihrer Indexdatei hinzufügen, um die neue Index-Bucket-Funktion nutzen zu können.

Hinweis: Wenn Sie von Version 11.1 oder höher auf Version 11.2 aktualisieren, müssen Sie diese Änderung nicht vornehmen.

Workaround: Fügen Sie das Bucket-Flag wie folgt zur Indexdatei hinzu, damit der Entropy Parser Index-Buckets verwenden kann:

1. Wählen Sie im NetWitness Suite-Menü **ADMIN** > **Services** aus.
   Die Ansicht „Services“ wird angezeigt.
2. Wählen Sie jeden Concentrator-Service aus, der Datenverkehr von den Decodern aggregiert.
3. Wählen Sie unter  (Aktionen) **Ansicht** > **Konfigurieren** und dann die Registerkarte **Dateien** aus.
4. Wählen Sie die `index-concentrator-custom.xml file` aus und legen Sie das `bucket`-Flag auf `true` für `payload.req` und `payload.res` fest. Zum Beispiel:
   ```
   <key description="Payload Size Request" format="UInt 32"
   level="IndexNone" bucket="true" name="payload.req"
   valueMax="500000"/>
   <key description="Payload Size Response" format=UInt32"
   level="IndexNone" bucket="true" name="payload.res"
   valueMaz="500000"/>
   ```
5. Klicken Sie auf **Anwenden**.
6. Damit die Änderungen in der `index-concentrator-custom.xml`-Datei wirksam werden, müssen Sie den Concentrator-Service neu starten:
   ```
   systemctl restart nwconcentrator
   ```

UEBA

Wenn der Proxy konfiguriert ist und es werden Updates durchgeführt, werden die Lizenzdetails nicht automatisch aktualisiert.

Rückverfolgungsnummer: ASOC-52366

Problem: Wenn der Proxy konfiguriert ist und es werden Updates durchgeführt, werden die Lizenzdetails nicht automatisch und auch nicht nach Klicken auf „Aktualisieren“ in der Ansicht „Lizenzdetails“ aktualisiert. Das liegt daran, dass die Kommunikation zum Lizenzserver nicht angegeben ist.

Workaround: Der Administrator muss die Lizenzdetails manuell im Offlinemodus herunterladen und die neuesten Lizenzdetails über die NetWitness Platform-Benutzeroberfläche hochladen. Weitere Informationen finden Sie im *Leitfaden zum Lizenzmanagement*.

Endpoint

Nginx lehnt Post-Anfragen mit einer Anfragegröße von mehr als 1 MB ab.

Rückverfolgungsnummer: ASOC-56236

Problem: Der Nginx-Server wird aktualisiert und die Standardgröße für Nutzdaten wird auf 1 MB eingestellt. Dies führt dazu, dass jede Datenpost-Anfrage, die mehr als 1 MB überschreitet, fehlschlägt.

Workaround: Fügen Sie die folgende Einstellung zur Nginx-Konfigurationsdatei (`/etc/nginx/conf.d/nginx.conf`) hinzu und starten Sie den Nginx-Server neu.

```
client_max_body_size 100M
```

Beim Erzeugen und Kopieren der Datei *nwelcfg-Datei wird der Zeitstempel nicht aktualisiert.

Rückverfolgungsnummer: ASOC-49847

Problem: Wenn der Administrator nach der Installation des Endpoint Insight-Agenten eine neue Konfiguration für die Protokollsammlung über eine der Kopiermethoden oder ein Drittanbieter-Endpunktmanagementtool aktualisieren möchte, ist der Zeitstempel der Konfigurationsdatei weiterhin auf die Endpoint-Serverzeit und nicht auf die Agent-Zeit festgelegt. Daher wird der Zeitstempel, wenn sich der Endpunkt-Agent in einer anderen Zeitzone als der Endpoint-Server befindet, nicht ordnungsgemäß aktualisiert.

Workaround: Führen Sie nach dem Konfigurieren der Datei den folgenden Befehl auf dem Endpoint-Agent aus: `copy /b <filename.nwelcfg> +,,` aus dem Ordner %programdata%\NWEAgent\, in dem die Datei „nwelcfg“ vorhanden ist.

Reagieren

Wenn alle Warnmeldungen für eine Warnmeldungsregel gelöscht werden, wird der Filter für die Regel nicht ordnungsgemäß entfernt.

Rückverfolgungsnummer: ASOC-59243

Problem: In der Ansicht „Warnmeldungsliste“ (Reagieren > Warnmeldungen) können Sie Warnmeldungen nach einem Namen filtern und dann alle Warnmeldungen mit diesem Namen löschen. Wenn Sie den Filter nach Warnmeldungsnamen nach dem Löschen der Warnmeldungen nicht entfernen, ist der Filter beim nächsten Laden der Warnmeldungsliste immer noch vorhanden, aber er wird nicht als Kontrollkästchen im Bereich „Filter“ angezeigt, da alle Warnmeldungen mit diesem Namen gelöscht wurden. Wenn Sie die Ansicht „Warnmeldungsliste“ aufrufen, werden weiterhin keine Ergebnisse angezeigt.

Workaround: Bevor Sie die Ansicht „Warnmeldungsliste“ aktualisieren oder neu laden, können Sie den Filter entfernen. Deaktivieren Sie dazu das Kontrollkästchen mit dem Namen der Warnmeldungen. Wenn Sie die Ansicht „Warnmeldungsliste“ bereits aktualisiert oder neu geladen haben, können Sie den ausgeblendeten Filter nur durch Drücken der Schaltfläche **Filter zurücksetzen** entfernen. Damit werden alle Filter, auch der ausgeblendete Filter für den Warnmeldungsnamen, entfernt.

Incidents werden nicht gekennzeichnet, wenn ein Benutzer Warnmeldungen manuell zu vorhandenen Incidents hinzufügt.

Rückverfolgungsnummer: ASOC-52428

Problem: Wenn Warnmeldungen in „Reagieren“ manuell zu einem Incident hinzugefügt wurden, werden keine Metawerte in Popup-Werten hervorgehoben. Automatisch oder dynamisch zu einem Incident hinzugefügte Warnmeldungen werden hingegen in einem Popup-Fenster angezeigt.

Workaround: Keiner.

Dateinamen für Malwareereignisse mit koreanischen Zeichen werden in der Ansicht „Reagieren“ nicht ordnungsgemäß angezeigt.

Rückverfolgungsnummer: ASOC-40159

Problem: Wenn koreanische Zeichen in einer Warnmeldung vorhanden sind, die von Malware Analysis empfangen wird, werden diese in der Ansicht „Reagieren“ nicht korrekt angezeigt.

Workaround: Keiner.

ESA-Regeln mit dem Schweregrad „Hoch“ oder „Niedrig“ werden nicht in der RSA Archer-Benutzeroberfläche ausgefüllt.

Rückverfolgungsnummer: ARCHER-47101

Problem: Wenn ESA-Warnmeldungen mit dem Schweregrad „Hoch“ oder „Niedrig“ an RSA Archer weitergeleitet werden, wird das Feld „Priorität der Sicherheitswarnmeldung“ in der RSA Archer-Benutzeroberfläche nicht ausgefüllt.

Workaround: Keiner.

wenn RSA Archer Cyber Incident & Breach Response Integration aktiviert ist, sind Incidents und Aufgaben immer noch verfügbar.

Rückverfolgungsnummer: ASOC-39886

Problem: Wenn Archer Cyber Incident & Breach Response (NetWitness SecOps Manager) in den Respond Server-Service integriert sind, werden alle Incidents im Archer Cyber Incident & Breach Response verwaltet. Wenn in früheren Versionen SecOps aktiviert war, waren Incidents und Korrekturaufgaben verborgen. In NetWitness Platform 11.0.0.x können Benutzer weiterhin auf Incidents und Aufgaben in der Ansicht „Reagieren“ („REAGIEREN >Incidents“ und „REAGIEREN > Aufgaben“) zugreifen. Sie werden auch nicht daran gehindert, Incidents in NetWitness Platform zu erstellen. Wenn sie aus der Liste der Warnmeldungen in der Ansicht „Reagieren“ (REAGIEREN > Warnmeldungen) oder aus Investigate Incidents erstellen, werden diese Incidents nicht zu Archer Cyber Incident & Breach Response verschoben.

Workaround: Wenn Sie die Archer Cyber Incident & Breach Response (NetWitness SecOps Manager)-Integration im Respond-Serverservice aktiviert haben, sollten Sie Folgendes in der Ansicht „Reagieren“ nicht verwenden: Ansicht „Incidents-Liste“, Ansicht „Incident-Details“ und Ansicht „Aufgabenliste“. Erstellen Sie Incidents außerdem nicht aus der Liste der Warnmeldungen in der Ansicht „Reagieren“ oder aus „Untersuchen“.

Für migrierte Incidents wird im Bereich „Übersicht“ für die Ereignisanzahl immer 0 angezeigt.

Rückverfolgungsnummer: ASOC-38026

Problem: Im Feld „Katalysatoren“ des Bereichs „Incident-Übersicht“ wird die Anzahl der Ereignisse für migrierte Incidents immer als 0 (null) angezeigt. Dies wird in der NetWitness Platform 11.0.0.x und höher erwartet. (Um auf den Bereich „Übersicht“ zuzugreifen, wechseln Sie „Reagieren > Incidents“. Wenn Sie auf einen Incident in der Liste der Incidents klicken, wird der Bereich „Übersicht“ auf der rechten Seite angezeigt. Wenn Sie auf einen Link im Feld „ID“ oder „NAME“ in der Liste der Incidents klicken, wird die Ansicht „Incident-Details“ mit dem Bereich „Übersicht“ auf der linken Seite geöffnet.)

Workaround: Keiner.

In der Arbeitsspeichertabelle werden keine Erweiterungsinformationen für ESA-Warnmeldungen angezeigt.

Rückverfolgungsnummer: ASOC-37533

Problem: Sie können keine benutzerdefinierten Erweiterungen für ESA-Korrelationsregeln in den Warnmeldungen der Ansicht „Reagieren“ anzeigen.

Workaround: Keiner.

Die Integrationseinstellungen Archer Cyber Incident & Breach Response (NetWitness SecOps Manager) sollten in der Benutzeroberfläche zur Verfügung gestellt werden.

Rückverfolgungsnummer: ASOC-25127

Problem: Die Integrationseinstellungen für das Senden aller Incidents an Archer Cyber Incident & Breach Response (NetWitness SecOps Manager) sollten in der Benutzeroberfläche zur Verfügung gestellt werden.

Workaround: Die Benutzeroberfläche für die partielle Archer Cyber Incident & Breach Response (NetWitness SecOps Manager)-Integration wurde in 11.0.0.x entfernt. Administratoren können die Integration in der Ansicht „Explorer“ des Respond-Serverservice abschließen.

Log Collector

FIPS wird standardmäßig für den Log Collector-Service deaktiviert.

Rückverfolgungsnummer: ASOC-41841

Problem: FIPS wird standardmäßig für den Log Collector-Service deaktiviert, selbst wenn FIPS in 11.2.0.0 aktiviert war.

Hinweis: Selbst wenn FIPS in 11.2.0.0 aktiviert ist, wird es nach der Migration deaktiviert.

Workaround: Führen Sie zum Aktivieren von FIPS auf dem Log Collector-Service die folgenden Schritte aus:

1. Beenden Sie den Log Collector-Service.
2. Öffnen Sie die Datei `/etc/systemd/system/nwlogcollector.service.d/nwlogcollector-opts-managed.conf`.
3. Ändern Sie den Wert der folgenden Variable zu **off**, wie hier beschrieben: zu

   ```
   Environment="OWB_ALLOW_NON_FIPS=on"
   ```
   in
   ```
   Environment="OWB_ALLOW_NON_FIPS=off"
   ```
4. Laden Sie den System-Daemon neu, indem Sie den Befehl `systemctl daemon-reload` ausführen.
5. Starten Sie den Log Collector-Service neu.
6. Legen Sie den FIPS-Modus für den Log Collector-Service in der Benutzeroberfläche fest:

   Hinweis: Dieser Schritt ist nicht erforderlich bei einem Upgrade, wenn FIPS in 11.2.0.0 aktiviert war.

   a. Navigieren Sie zu **ADMINISTRATION** > **Services**.

   b. Wählen Sie den Log Collector-Service aus und navigieren Sie zu **Ansicht** > **Konfiguration**.

   c. Aktivieren Sie im SSL FIPS-Modus das Kontrollkästchen im Bereich „Konfigurationswert“ und klicken Sie auf **Anwenden**.

   Hinweis: Legen Sie zum Aktivieren des Log Decoder und Paket Decoder und Packet in `/sys/config` die Option `ssl.fips` auf „ON“ fest und starten Sie den Service neu.

Untersuchen

Importierte Ermittlungsprofile werden im Drop-Down-Menü nicht angezeigt.

Rückverfolgungsnummer: ASOC-61230

Problem: Wenn Sie Profile über das Dialogfeld „Profile managen“ in die Ansicht „Navigieren“ oder „Ereignisse“ importieren, werden die neu importierten Profile nicht im Drop-down-Menü der Profile hinzugefügt.

Workaround: Aktualisieren Sie das Browserfenster, damit die kürzlich hinzugefügten Profile angezeigt werden.

In der Ansicht „Ereignisanalyse“ werden Protokoll- und Netzwerkereignisse nicht verschachtelt.

Rückverfolgungsnummer: ASOC-60941

Problem: Netzwerk- und Protokollereignisse werden in der Ansicht „Ereignisse“ verschachtelt und in zeitlicher Reihenfolge sortiert, aber in der Ansicht „Ereignisanalyse“ werden die Ereignisse auf andere Weise sortiert. In der Ansicht „Ereignisanalyse“ werden die Ereignisse nicht wie erwartet verschachtelt. Stattdessen werden alle Protokollereignisse in zeitlicher Reihenfolge vor allen in zeitlicher Reihenfolge sortierten Netzwerkereignissen angezeigt.

Workaround: In der Ansicht „Ereignisse“ können Sie Netzwerk- und Protokollereignisse verschachtelt anzeigen.

Wenn ein großer PCAP aus der Ansicht „Ereignisse“ extrahiert wird und die Zeit dafür nach 5 Minuten überschritten ist, wird eine Abfragezeit von 8 Stunden in der Fehlermeldung des Jobabschnitts angezeigt.

Rückverfolgungsnummer: ASOC-60464

Problem: Wenn ein PCAP mit ~ 100000-Sitzungen aus der Ansicht „Ereignisse“ mithilfe von „Exportieren“ > „Alle PCAP exportieren“ exportiert wird, könnte der Download aufgrund der Überschreitung der 5-Minuten-Zeit für den Paketaufruf fehlschlagen. Wenn der Anruf ausfällt, zeigt die Fehlermeldung im Jobabschnitt fälschlicherweise eine Zeitüberschreitung von 8 Stunden (28800000 ms) an.

Workaround: Keiner.

Benutzer mit der Berechtigung für den Investigate-Server* erhalten keine ordnungsgemäße Fehlermeldung mit einer Erklärung dazu, warum sie keinen Zugriff auf die Ansicht „Ereignisanalyse“ haben.

Rückverfolgungsnummer: ASOC-60366

Problem: Wenn der Administrator einem Benutzer keine Investigate-Server*-Berechtigung erteilt hat, sollte der Benutzer beim Versuch, eine Sitzung in der Ansicht „Ereignisanalyse“ anzuzeigen, einen Fehler mit der abgelehnten Berechtigung sehen. Stattdessen wird der interne Serverfehler zurückgegeben.

Workaround: Keiner.

Active Directory-Metawerte in der Ansicht „Ereignisanalyse“, wie z. B. der Benutzername, enthalten möglicherweise Kontextdaten, aber die Metawerte sind nicht als Indikator unterstrichen.

Rückverfolgungsnummer: ASOC-58853

Problem: Analysten, die in der Ansicht „Ereignisanalyse“ arbeiten, erkennen keinen Indikator dafür, dass Active Directory-Metadaten eine Kontextanreicherung verfügen. Sie müssen den Mauszeiger über einen Active Directory-Metawert bewegen und den Bereich „Kontextabfrage“ öffnen, um zu erkennen, diesem Wert Kontext zugeordnet ist.

Workaround: Bewegen Sie den Mauszeiger über einen Metawert oder wählen Sie einen Metawert aus und klicken SIe auf **Kontext anzeigen**, um zu erkennen, ob dem Wert Kontext für Active Directory zugeordnet ist.

Wenn die URL für einen Drill-down-Punkt sehr lang ist und Sie die Abfrage in der Ansicht „Ereignisanalyse“ verwenden, wird ein Fehler (414 Anforderungsfehler) zurückgegeben

Rückverfolgungsnummer: ASOC-50196

Problem: Eine Reihe von Situationen kann zur Erstellung einer sehr langen Abfrage führen, die der Browser nicht verarbeiten kann, insbesondere, wenn Sie Internet Explorer verwenden, der ein viel niedrigeres Zeichenlimit hat als die meisten Browser. Das Wechseln zur Ereignisanalyse von Reporting kann zu einer sehr langen Abfrage führen, ebenso wie eine Reihe von Wechseln in der Ansicht „Navigation“.

Workaround: Setzen Sie das Arbeiten in der Ansicht „Navigation“ oder „Ereignisse“ fort, wenn die URL zu lang wird, um in der Ansicht „Ereignisanalyse“ gerendert zu werden.

Die Abfrageerstellung in der Ansicht „Ereignisanalyse“ reagiert nicht auf Filter, die ein Leerzeichen enthalten.

Rückverfolgungsnummer: ASOC-49427

Problem: Wenn Sie einen Filter hinzufügen und ein zusätzliches Leerzeichen vor <Metaschlüssel>, zwischen <Metaschlüssel> und <Operator> und nach <Operator> einfügen, reagiert die Abfrageerstellung nicht mehr und die Schaltfläche „Abfrageereignisse“ wird deaktiviert, sodass Sie das Hinzufügen von Filtern nicht fortsetzen können.

Workaround: Klicken Sie auf einen vorhandenen Filter und dann auf die Abfrageerstellung. Wenn das nicht funktioniert, aktualisieren Sie die Seite.

Benutzerdefinierte Feeds

Der Status der Fortschrittsleiste des STIX-Feeds ist unvollständig

Rückverfolgungsnummer: ASOC-40642

Problem: Manchmal ist der Status der Fortschrittsleiste für einige der STIX-Feeds unvollständig, selbst wenn die Feeds erfolgreich an die Decoder übertragen werden.

Workaround: Keiner.

Event Stream Analysis (ESA)

ESA-CH-Regeln werden während des Upgrades oder des ESA-Host-Neustarts deaktiviert.

Rückverfolgungsnummer: ASOC-60511

Problem: Wenn der ESA-Host neu gestartet wird und die Context-Hub-Regeln auf der ESA bereitgestellt werden, können die Regeln des Context Hub deaktiviert werden. Dies geschieht als Ergebnis der Konkurrenz zwischen dem Context Hub und dem Start des Event Stream Analysis-Service auf dem ESA-Host.

Workaround: Führen Sie eine der folgenden Aktionen aus, um das Problem zu beheben:

- Navigieren Sie zur Registerkarte **KONFIGURIEREN > ESA-Regeln > Services** und aktivieren Sie je nach Context Hub die deaktivierten Regeln.
- Starten Sie den Event Stream Analysis-Server neu.

ESA-Regeln mit benutzerdefinierten Metawerten werden nicht auf dem ESA-Server bereitgestellt.

Rückverfolgungsnummer: ASOC-60367

Problem: Wenn Sie in 11.2 neue eigene Metaschlüssel hinzufügen, können die ESA-Regeln, die diese Metaschlüssel verwenden, werden diese Metaschlüssel möglicherweise nicht bereitgestellt.. Dies geschieht, weil der Event Stream Analysis-Service Informationen vom Concentrator benötigt.

Workaround: So stellen Sie eine ESA-Korrelationsregel mit benutzerdefinierten Metawerten bereit:

1. Fügen Sie der Datei index-concentrator-custom.xml hinzu („ADMIN“ > „Services“ > Concentrator auswählen und dann „Aktionen“ > „Ansicht“ > „Konfigurieren“ > „Dateien“ auswählen).
2. Starten Sie den Concentrator neu („ADMIN“ > „Services“ > Concentrator auswählen und dann „Aktionen“ > „Neustart“ auswählen).
3. Stellen Sie sicher, dass der Concentrator als Datenquelle für den Event Stream Analysis-Service konfiguriert ist („ADMIN“ > „Services“ > Event Stream Analysis-Service auswählen und dann „Aktionen“ > „Ansicht“ > „Konfigurieren“ > Registerkarte „Datenquellen“ auswählen).
4. Starten Sie den Event Stream Analysis-Server neu („Aktionen“ > „Neustart“).
5. Stellen Sie sicher, dass die neuen Metaschlüssel in den Metaschlüsselreferenzen aufgeführt sind („KONFIGURIEREN“ > „ESA-Regeln“ > Registerkarte „Einstellungen“ > „Metaschlüsselreferenzen“).
6. Stellen Sie die ESA-Regel mit eigenen Metawerten bereit.

Die ESA-Regel kann mit Arraymetadaten in der Erweiterung nicht bereitgestellt werden.

Rückverfolgungsnummer: ASOC-47584

Problem: Wenn ein Benutzer eine In-Memory-Tabelle als Erweiterungsquelle in ESA konfiguriert, in der eine Tabellenspalte den Typ Zeichenfolge aufweist, eine ESA-Regel mit einer Whitelist-Bedingung erstellt und die Zeichenfolgenlistenspalte einem Zeichenfolgen-Arrayereignis-Metaschlüssel zuordnet, wird die Regel bei der Bereitstellung deaktiviert, da die Konvertierung des Datentyps von Zeichenfolge[] zu Zeichenfolge nicht zulässig ist.

Workaround: Keiner.

Für ESA-Regeln, die Erweiterungsquellen verwenden, funktioniert die Option „Groß-/Kleinschreibung ignorieren“ nicht für die erste Anweisung.

Rückverfolgungsnummer: ASOC-49906

Problem: Wenn bei der Erstellung einer ESA-Regel, die eine Erweiterungsquelle verwendet, die Option „Groß-/Kleinschreibung ignorieren“ in der ersten Erweiterungsanweisung aktiviert ist, werden keine Ergebnisse zurückgegeben. Beachten Sie, dass dieses Problem nicht für Anweisungen nach der ersten Anweisung gilt (d. h. Unteranweisungen).

Workaround: Beim Erstellen einer neuen Regel ist die Option „Groß-/Kleinschreibung ignorieren“ jetzt deaktiviert. Für vorhandene Regeln, bei denen die Option „Groß-/Kleinschreibung ignorieren“ für eine Erweiterungsanweisung aktiviert ist, ist die Option immer noch aktiviert, aber Benutzer werden aufgefordert, die Option zu deaktivieren, wenn Sie die Regel in ESA öffnen, und dann die aktualisierte Regel zu speichern.

Die ESA-Komprimierungsstufe kann nicht wie in anderen Appliances festgelegt werden.

Rückverfolgungsnummer: ASOC-26481

Problem: Administratoren können die Komprimierungsstufe in ESA nicht wie mit anderen Appliances festlegen, auch nicht bei Verwendung der Ansicht „Explorer“.

Workaround: Löschen Sie die Concentrator-Quelle aus ESA und fügen Sie sie erneut hinzu, damit die Änderungen der Komprimierungsstufe dargestellt werden:

1. Entfernen Sie die Concentrator-Datenquelle aus ESA. (Wechseln Sie zu „ADMIN > Services“, wählen Sie den Event Stream Analysis-Service aus und wählen Sie dann aus dem Menü „Aktionen“ die Optionen „Ansicht > Konfigurieren“ aus. Entfernen Sie auf der Registerkarte „Datenquellen“ der Ansicht „Konfigurieren“ die Concentrator-Datenquelle.)
2. Legen Sie die Komprimierungsstufe in ESA fest. (Wechseln Sie zur Ansicht „Durchsuchen“, navigieren Sie in der Node-Liste zu „Workflow/Source/nextgenAggregationSource“ und legen Sie „CompressionLevel“ fest.)
3. Fügen Sie die Concentrator-Datenquelle wieder zu ESA hinzu. (Kehren Sie zur Registerkarte „Datenquellen“ der Ansicht „Konfigurieren“ zurück und fügen Sie die Concentrator-Datenquelle hinzu.)

Der Event Stream Analysis-Service reagiert nicht mehr bei Verwendung der abfragebasierten Aggregation für die automatisierte Bedrohungserkennung für Protokolle.

Rückverfolgungsnummer: ASOC-25174

Problem: Event Stream Analysis reagiert möglicherweise nicht aufgrund von hohem Ressourcenverbrauch und die Konfiguration des Wrapper muss angepasst werden.

Workaround: Sie müssen möglicherweise die Einstellungen der Ping-Zeit in der Datei `wrapper.conf` ändern. Führen Sie folgende Schritte durch:

1. Wechseln Sie zu **Administration > Services> Event Stream Analysis> Explorer** und navigieren Sie zum Ordner **`/opt/rsa/esa/conf/`**.
2. Ändern Sie die Einstellungen in die folgenden Werte:
   `wrapper.ping.timeout=300`
3. Fügen Sie die folgenden Zeilen am Ende der Datei hinzu:
   `wrapper.restart.delay=40`
   `wrapper.ping.timeout.action=RESTART`
4. Starten Sie den Event Stream Analysis-Server neu.

ESA zeigt Warnung für Array-Operatoren an

Rückverfolgungsnummer: ASOC-14157

Problem: Beim Schreiben einer erweiterten Regel schlagen Array-Operatoren wie AnyOf fehl. Beispiel:

```
SELECT * FROM
Event(
alias_host.anyOf(i => i.length()>50)
);
```

führt zu einem Fehler ähnlich dem folgenden:

```
Logger name:
com.espertech.esper.epl.enummethod.dot.PropertyExprEvaluatorScalarArray
Thread: pipeline-sessions-0
Level : WARN
Message : Expected array-type input from property 'alias_host' but received class
java.util.Vector
```

Workaround: Um einen unscharfen Vergleich zu erhalten, müssen Sie zunächst das Array in eine Zeichenfolge konvertieren. Beispiel:

SELECT * from Event **(cast(alias_host, string)**LIKE '%TESTHOST%');

Hinweis: Wenn Sie Array-Operatoren in EPL in den Versionen 10.5, 10.5.0.1 und 10.6 verwendet haben, müssen Sie EPL mithilfe des oben genannten Workarounds ändern.

Die Bereitstellung schlägt fehl, wenn der Server ausfällt, auf dem eine externe Datenbank gehostet wird.

Rückverfolgungsnummer: ASOC-9011

Problem: Sie können eine Datenbankverbindung so konfigurieren, dass die Datenbank als eine Erweiterungsquelle für eine Regel verwendet wird. Ein Verweis auf die Datenbank wird in allen ESA bereitgestellt, auch wenn die ESA keine Regeln bereitstellt, die die Datenbank verwenden. Wenn der Server, der die Datenbank hostet, ausfällt, wird jede neue Bereitstellung fehlschlagen.

Workaround: Starten Sie den Server, der die Datenbank hostet, neu.

Reporting

Die Optionen „Ausblenden“ und „Untersuchen“ werden in den Browsern Google Chrome und Mozilla Firefox im Windows 10-Betriebssystem nicht unterstützt

Rückverfolgungsnummer: ASOC-37590

Problem: Wenn Sie den Browser Chrome oder Firefox in einem Windows 10-Betriebssystem verwenden und auf einen Diagrammdatenpunkt klicken, werden die Optionen „Ausblenden“ und „Untersuchen“ nicht angezeigt. Diese Optionen sind bei Verwendung des Internet Explorer-Browsers jedoch verfügbar.

Workaround: Deaktivieren Sie die Touchfunktion in Chrome und Firefox. Wenden Sie zum Deaktivieren dieser Option in Chrome das folgende Verfahren an:

1. Navigieren Sie in Chrome oder Firefox zu chrome://flags/.
2. Wählen Sie die Option „Deaktivieren“ für das Flag „Touch Events API“ aus.
3. Starten Sie den Browser neu.

Wenden Sie zum Deaktivieren dieser Option in Firefox das folgende Verfahren an:

1. Navigieren Sie zu „about:config“.
2. Klicken Sie auf „Ich bin mir der Gefahren bewusst“.
3. Suchen Sie nach dem Einstellungsnamen „dom.w3c_touch_events.enabled“.
4. Aktualisieren Sie die Spalte „Wert“ auf 0.
5. Starten Sie den Browser neu.

Ereignisquellenmanagement

Das Fenster "Parser-Zuordnungen verwalten" hat einen leeren Anzeigenamen für Log Parser, wenn die Ereignisquelle manuell erstellt wurde.

Rückverfolgungsnummer: ASOC-53914

Problem: Wenn Sie das Fenster "Parser-Zuordnungen verwalten" aus der Ansicht „ADMIN“ > „Ereignisquellen“ > „Erkennung“ öffnen, ist der Anzeigename für zugeordnete Ereignisquellen, die manuell erstellt wurden, leer.

Workaround: Schließen Sie das Zuordnungsfenster und öffnen Sie es wieder.

Für automatisch zugeordnete Adressen werden nicht alle Typen angezeigt.

Rückverfolgungsnummer: ASOC-48328

Problem: Wenn eine neue Anwendung zu einer vorhandenen, automatisch zugeordnete Ereignisquelle hinzugefügt wird, kann es zu einer Verzögerung bei der Anzeige des Typs in der Ansicht „Ereignisquellenerkennung“ kommen. Auch könnte die Aufhebung der automatischen Zuordnung später angezeigt werden.

Workaround: Keiner.

SMS-Service stürzt mit Speicherfehler ab.

Rückverfolgungsnummer: ASOC-62575

Problem: Bei Systemen mit einer großen Anzahl von aktiven Ereignisquellen kann der SMS-Dienst mit einem **java.lang.OutOfMemoryError:-Fehler abstürzen, wenn das System mit der Verarbeitung von Protokollstatistik-Nachrichten nicht Schritt halten kann. Java Heap Space**-Fehler.

Workaround: Wenn dieses Problem auftritt, wenden Sie sich an den RSA-Support. Hier erhalten Sie weitere Informationen zur Lösung dieses Problems.

Core-Services

Das Kontrollkästchen „SSL FIPS-Modus“ in der Ansicht „Services > Konfigurieren“ sollte für Brokers, Concentrators und Archivers deaktiviert werden, da eine Änderung des Wertes für das Kontrollkästchen die FIPS-Durchsetzung für den Service nicht deaktiviert

Rückverfolgungsnummer: ASOC-41902

Problem: In 11.0.0.x oder höher wird für den Broker, Concentrator und Archiver immer FIPS durchgesetzt und der Administrator hat nicht die Option, zwischen FIPS und Nicht-FIPS zu wechseln. Der Administrator kann das Kontrollkästchen „SSL FIPS-Modus“ verwenden, um den FIPS-Modus auf einem Log Decoder, Packet Decoder oder Log Collector ein- und auszuschalten.

Workaround: Keiner.

Fehler aufgrund einer ungültigen XML-Datei für mehrere MetaCallback bei der Option „Erweitert“ der benutzerdefinierte Feedkonfiguration.

Rückverfolgungsnummer: ASOC-40867

Problem: NetWitness Platform bietet keine Unterstützung für das Hochladen von Feeds für die XML-Dateien, in denen mehrere Callbacks vorhanden sind.

Workaround: Der Ad-hoc-Feed kann über NwConsole oder direkt über die REST-URL des Decoder hochgeladen werden. Das gilt nicht für den wiederkehrenden Feed.

Produktdokumentation

Die folgende Dokumentation ist im Lieferumfang der Version enthalten.

Dokumentation	Standort-URL
RSA NetWitness Platform 11.2 Onlinedokumentation	https://community.rsa.com/community/products/netwitness/112
RSA NetWitness Platform 11.2 – Anweisungen für das Upgrade	https://community.rsa.com/community/products/netwitness/112/content?filterID=contentstatus%5Bpublished%5D~category%5Binstallation-upgrade%5D
RSA NetWitness Platform 11.2 – Checklisten für das Upgrade	Virtueller Host – Upgradecheckliste (10.6.6.x auf 11.2) Physischer Host – Upgradecheckliste (10.6.6.x auf 11.2)
RSA NetWitness Platform – Handbücher für die Hardwarekonfiguration	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA-Inhalt für RSA NetWitness Platform	https://community.rsa.com/community/products/netwitness/rsa-content

Kontaktieren der Kundenbetreuung

Wenn Sie sich mit dem Kundendienst in Verbindung setzen, sollten Sie sich an Ihrem Computer befinden. Halten Sie die folgenden Informationen bereit:

- Die Versionsnummer des verwendeten RSA NetWitness Platform-Produkts oder der Appliance.
- Typ der verwendeten Hardware

Verwenden Sie die folgenden Kontaktinformationen, wenn Sie Fragen haben oder Unterstützung benötigen.

RSA Link	https://community.rsa.com Im Hauptmenü klicken Sie auf **Meine Fälle**.
Tel.	1-800-995-5095, Option 3
Internationale Kontakte	http://germany.emc.com/support/rsa/contact/phone-numbers.htm
Community	https://community.rsa.com/community/support
Basis-Support	Der technische Support für Ihre technischen Probleme ist von montags bis freitags von 08:00 bis 17:00 Uhr Ortszeit erreichbar.
Enhanced Support	Der technische Support ist nur für Fehler des Schweregrads 1 und 2 telefonisch an 365 Tagen im Jahr rund um die Uhr verfügbar.

Revisionsverlauf

Version	Datum	Beschreibung
1,0	15. August 2018	Betriebsfreigabe