RSA NETWITNESS® PLATFORM

Versionshinweise

für RSA NetWitness Platform 11.3

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 müssen 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

Einleitung

In diesem Dokument sind Verbesserungen und Korrekturen in RSA NetWitness® Platform 11.3.0.0 aufgeführt. Lesen Sie dieses Dokument vor der Bereitstellung von oder der Aktualisierung auf RSA NetWitness® Platform 11.3.0.0.

Neuheiten

RSA NetWitness® Platform 11.3.0.0 bietet neue Funktionen und Verbesserungen für jede Rolle im Security Operation Center. Dazu gehören:

- Zusätzliche Funktionen für die Analyse von Hosts und Dateien für bösartige oder verdächtige Aktivitäten.
- Verbesserungen der Bedienbarkeit, um die Arbeit für Incident Responders und Threat Hunters zu erleichtern.
- Richtlinien- und Lizenzierungsverbesserungen, damit Administratoren ihre Umgebungen effizienter managen können.

NetWitness Endpoint

Endpunkt-Agent

In Version 11.3 unterstützt der Agent die EDR-Funktionen (Endpoint Detection and Response, Endpunkterkennung und Reaktion) sowie die Windows-Protokollsammlung.

Der erweiterte (lizenzierte) Agent bietet EDR-Funktionen mit kontinuierlichem Monitoring der Aktivitäten auf dem Host für umfassende Transparenz sowie Analysen aller Verhaltensweisen und Prozesse auf dem Endpunkt. Der Agent zeichnet Daten zu jeder kritischen Aktion auf, z. B. Prozesse, Dateien, Änderungen an der Registrierung und Netzwerkverbindungen, und sendet diese als Ereignisse nahezu in Echtzeit an den Server. Der Agent kann Anomalien wie z. B. Bild-Hooks, Kernel-Hooks, Registrierungsdiskrepanzen und verdächtige Threads erkennen. Darüber hinaus erfasst er Windows-Protokolle. Weitere Informationen finden Sie im *NetWitness Endpoint-Benutzerhandbuch*.

Im Folgenden sind die wichtigsten Funktionen aufgeführt:

- Interaktionen mit der Nutzerkonsole, die für die Untersuchung von Schadsoftwareangriffen, die legitime Windows-Dateien wie `cmd.exe` oder `powershell.exe` verwenden, unerlässlich sind, um Befehle auf einem infizierten Host ausführen zu können.

- Einblicke in vollständige Befehlszeilenargument-Zeichenfolgen, die für forensische Untersuchungen und Ermittlungen wichtig sind.
- Erkennung von dateibasierten Skripten oder Skripten ohne Dateien durch das Reporting von Skripten direkt für Prozessereignisse anstatt für Skript-Engines. Zu den derzeit unterstützten Engines gehören `powershell`, `cmd`, `cscript`, `wscript`, `rundll32`, `mshtml` und `javascript`.
- Einmischsicherer Agent: Registrierungsschlüssel sowie `.exe`- und `.sys`-Dateien von Agents im Nutzer- und Kernelmodus sind geschützt.

Endpunkt-Agents können je nach Richtlinienkonfiguration in einem Insights-Modus oder im erweiterten Modus ausgeführt werden. Weitere Informationen finden Sie im *Konfigurationsleitfaden für NetWitness Endpoint*.

Wichtige Verbesserungen der 11.3-Agents im Vergleich zu NetWitness Endpoint-Legacy-Agents

- Entkoppelte Abhängigkeiten mit internen Kernel-Strukturen.
- Performanceverbesserungen bei der Dateiblockierung mit einer enormen Zunahme der Anzahl von Hashes, die blockiert werden können.
- Höhere Grenzwerte für die Erfassung von Ereignissen. Ereignisse sind nicht mehr an ausführbarem Hash gebunden, sondern an die gesamte Erstellungskette.
- Bessere Kompatibilität und Interoperabilität mit Anwendungen von Drittanbietern.

Unterstützte Agent-Betriebssysteme

Folgende Betriebssysteme werden nun unterstützt:

- Windows 2019 Server
- Windows 10 (32- und 64-Bit) (bis Version 1809)
- Red Hat Linux 7.x
- Mac OS 10.13 (High Sierra)
- Mac OS 10.14 (Mojave)

Agents können auch auf einer virtuellen Desktopinfrastruktur (VDI) in VMware-Umgebungen installiert werden. Weitere Informationen finden Sie in der *Installationsanleitung zu NetWitness Endpoint Agent*.

Skalierbare und verteilte Bereitstellungen

Abhängig von der Anzahl, dem Speicherort, der Verteilung der Agents und den Daten, die von Endpunkten erfasst werden, können Sie Ihre Bereitstellung durch Hinzufügen mehrerer Endpoint Log Hybride skalieren. Installieren Sie Endpunkt-Broker, um eine konsolidierte Ansicht aller Endpunktserver in Ihrer Bereitstellung zu erhalten. Weitere Informationen finden Sie im *NetWitness Endpoint-Benutzerhandbuch* und im *Konfigurationsleitfaden zu NetWitness Endpoint*.

Gruppen und Richtlinien

Um Endpunkt-Agentkonfigurationen effizient zu managen und zu aktualisieren, können Administratoren Agents gruppieren und ihr Verhalten mithilfe von Policies managen. Administratoren können entweder standardmäßige oder kundenspezifische Richtlinien verwenden. Sie können die Windows-Protokollkonfiguration über die Windows-Protokollrichtlinie aktivieren, statt sie über den Agent-Packager zu erzeugen. Weitere Informationen finden Sie im *Konfigurationsleitfaden für NetWitness Endpoint*.

Analysieren von Dateien und Hosts mithilfe der Risikobewertung

Analysten können eine Datei oder einen Host mithilfe von Risikobewertungen von 1 bis 100 untersuchen. Der detaillierte Kontext von Risikotreibern (Warnmeldungen und Ereignisse) ist verfügbar, um Sie bei der schnellen Ermittlung verdächtiger oder bösartiger Aktivitäten zu unterstützen. Weitere Informationen finden Sie im *NetWitness Endpoint-Benutzerhandbuch*.

Prozessvisualisierung

Zur besseren Bedienung durch Analysten während der Prozessermittlung gibt es nun eine intuitive Benutzeroberfläche, die Ihnen Folgendes erleichtert:

- Verstehen der gesamten Prozessereigniskette sowie Verarbeiten der Beziehungen zwischen über- und untergeordneten Elementen und aller zugehörigen Ereignisse in einer Zeitachsenansicht.
- Analysieren von wichtigen Prozessattributen, z. B. Nutzername, Startargumente, Reputation, Dateistatus, Signaturgeber, Signatur und Dateipfad.

Weitere Informationen finden Sie im *NetWitness Endpoint-Benutzerhandbuch*.

Dateianalyse und -reaktion

Analysten können:

- Dateien mithilfe der Dateireputation (z. B. „erwiesenermaßen fehlerfrei“, „ungültig“, „verdächtig“) anhand des Context Hub, der Risikobewertung und des Zertifikatstatus analysieren.
- Eine externe Suche mithilfe von Google oder VirusTotal durchführen.
- Eine Datei herunterladen und eine genauere Dateianalyse durchführen, z. B. Zeichenfolgensuche und Textinhalte für Skripte.

Nach der Ermittlung können Analysten:

- Den Dateien Status zuweisen, um sie als Blacklist, Whitelist usw. zu kategorisieren.
- Bedrohungen durch das Blockieren bösartiger oder infizierter Dateien beseitigen.

Weitere Informationen finden Sie im *NetWitness Endpoint-Benutzerhandbuch*.

Anwendungsregeln für vorhandene IIOCs

Die vorhandenen IIOCs aus NetWitness Endpoint 4.4.0. x stehen als vordefinierte Anwendungsregeln in NetWitness Platform 11.3 zur Verfügung. Weitere Informationen finden Sie im *Konfigurationsleitfaden für NetWitness Endpoint*.

Hinzugefügte Regeln für die Endpunktrisikobewertung für ESA

Zusätzlich zu den ESA-Beispielregeln enthält NetWitness Platform nun ein Endpunktrisikobewertungspaket mit ungefähr 400 Regeln. Diese Regeln erzeugen Warnmeldungen, die zum Berechnen von Risikobewertungen für verdächtige Dateien und Hosts verwendet werden, die die festgelegten Schwellenwerte der Risikobewertungen überschreiten. Wenn Sie über NetWitness Endpoint verfügen, können Sie dieses Regelpaket einer Bereitstellung von ESA-Regeln auf die gleiche Weise hinzufügen wie eine ESA-Regel. Sie müssen jedoch Endpunktdatenquellen (Concentrator) während der Bereitstellung von ESA-Regeln angeben. Weitere Informationen finden Sie im *ESA-Konfigurationsleitfaden*.

Aktualisierungen der Ansicht „Ermittlung > Ereignisanalyse“ für Endpunktereignisse

- Textanalysen für Endpunktereignisse bieten aussagekräftigen Text, der das Ereignis erklärt. Sie können auch Metadaten mit Werten größer als 255 Zeichen anzeigen.
- Für jede Sitzung können Sie das Ereignis in der Prozessanalyse anzeigen oder die Details des mit dem Ereignis verknüpften Hosts einsehen, indem Sie zur Ansicht „Details zum Host“ wechseln.

NetWitness Respond

Neu konzipierte Ereignisliste für NetWitness Endpoint-Ereignisse

Zur besseren Bedienung durch Analysten und zum Integrieren von Endpunktereignissen in NetWitness Respond verfügt die neu konzipierte Ereignisliste über ein flexibles Layout, das unterschiedliche Daten besser darstellt. Die neu konzipierte Liste ermöglicht es Analysten, Ereignisse mit einer besser durchsuchbaren Ereignisvorschau schnell zu verstehen und zu priorisieren, die für NetWitness Endpoint- und Inline-Ereignisdetails kundenspezifisch angepasst wurde. Weitere Informationen finden Sie im *NetWitness Respond-Benutzerhandbuch*.

Verbesserter Warnmeldungslistenfilter für NetWitness Endpoint

Beim Filtern der Warnmeldungsliste nach der Endpunktquelle enthält Sie sowohl NetWitness Endpoint 4.4.x- als auch NetWitness Endpoint 11.x-Warnmeldungen.

Hinzugefügte UEBA-Incident-Regel

Es ist eine neue standardmäßige UEBA-Incident-Regel (User Entity Behavior Analytics) verfügbar, die das Verhalten von Nutzerentitäten gruppiert nach Klassifizierungs-ID erfasst, um Incidents aus Warnmeldungen zu erstellen.

Aktualisierte Incident-Regel in NetWitness Endpoint

Wenn Sie über NetWitness Endpoint verfügen, erfasst die standardmäßige Incident-Regel „Warnmeldungen mit hohem Risiko: NetWitness Endpoint“ die von NetWitness Endpoint mit einer Risikobewertung von „hoch“ oder „kritisch“ erzeugten Warnmeldungen. Diese Regel gruppiert nun Warnmeldungen in Incidents nach Hostname. Weitere Informationen finden Sie im *Konfigurationsleitfaden für NetWitness Respond*.

Hinzugefügte Funktion zur automatischen Erstellung von Incidents für Endpunktrisikobewertungen

Wenn Sie über NetWitness Endpoint verfügen, können Sie die Einstellungen für den Schwellenwert der Endpunktrisikobewertung so konfigurieren, dass automatisch Risikobewertungs-Incidents für verdächtige Dateien und Hosts erstellt werden, die die festgelegten Schwellenwerte der Risikobewertungen überschreiten. Weitere Informationen zur Konfiguration der Einstellungen für den Risikobewertungsschwellenwert finden Sie im *Konfigurationsleitfaden für NetWitness Respond*. Weitere Informationen zu NetWitness Endpoint finden Sie im *Konfigurationsleitfaden für NetWitness Endpoint*.

Wechseln zu „Ermittlung“ > Ansichten „Hosts“ und „Dateien“ aus der Ansicht „Respond“

Für eine detaillierte Untersuchung eines Incident können Analysten über kontextbezogene Kurzinformationen in der Ansicht „Respond“ auf „Ermittlung“ > Ansichten „Hosts“ und „Dateien“ zugreifen.

Suchen nach Dateireputationsstatus und -informationen aus der Ansicht „Respond“

In der Ansicht „Respond“ und den Ansichten „Ermittlung“, in denen Context Hub in NetWitness Platform integriert ist, können Analysten den Mauszeiger über eine Datei-Hash-Einheit bewegen, um eine kontextbezogene Kurzinformation zu öffnen, in der der Reputationsstatus der Datei angezeigt wird. Analysten können auch auf die Schaltfläche „Kontext anzeigen“ klicken, die den Bereich „Kontextabfrage“ mit zusätzlichen Dateiinformationen öffnet.

NetWitness UEBA

Erweiterte Analysen mithilfe von RSA NetWitness Endpoint

UEBA ist in NetWitness Endpoint integriert, um die aktuelle Erkennungsabdeckung in NetWitness Platform zu verbessern. Der Zweck dieser Integration besteht darin, potenzielle Aktivität von Angreifern zu identifizieren. Der Schwerpunkt liegt auf zwei primären Datenquellen:

- Prozessausführungen
- Registrierungsänderungen

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

Zugriff auf die Ansichten „Hostdetails“ oder „Prozess analysieren“ aus der Ansicht „Nutzerprofil“

Ein Analyst kann aus der Ansicht „Nutzerprofil“ zur Ansicht „Hostdetails“ oder „Prozess analysieren“ navigieren, um nach detaillierteren Informationen zu einem ungewöhnlichen Prozess oder einem Host zu suchen, der mit dem Nutzerrisiko zusammenhängt. Weitere Informationen finden Sie im *NetWitness UEBA – Benutzerhandbuch*.

Unterstützung für zusätzliche Datenquelle

NetWitness UEBA unterstützt nun die RSA SecurID-Datenquelle.

NetWitness Investigate

Analysten können eine große Anzahl von Ereignissen gleichzeitig in der Ereignisliste der Ansicht „Ereignisanalyse“ anzeigen

Bis zu 50.000 Ereignisse werden in aufsteigender Reihenfolge basierend auf der Erfassungszeit in die Ereignisliste geladen. Eine Zeilennummernanzeige alle 100 Zeilen erleichtert die Navigation durch die Liste. Die Benutzeroberflächenfunktionen erleichtern Ihnen das Verständnis zur Sortierreihenfolge sowie dazu, was derzeit angezeigt wird. Weitere Informationen finden Sie unter „Analysieren von Ereignissen in der Ansicht ‚Ereignisanalyse‘“ im *NetWitness Investigate – Benutzerhandbuch*.

Analysten können den detaillierten Status einer Abfrage in der Ansicht „Ereignisanalyse“ anzeigen.

Wenn Sie in der Ansicht „Ereignisanalyse“ auf das Informationssymbol () klicken, öffnet die Abfrageerstellung die Abfragekonsole – eine neue Benutzeroberflächenfunktion, die eine Statusleiste, Warnungen, Fehlermeldungen und andere Details dazu enthält, was während der Ausführung einer Abfrage geschieht. Wenn eine Abfrage abgeschlossen wurde, werden in der Abfragekonsole der Zeitbereich, die Abfrage, die abgefragten Services, alle Services, die nicht abgefragt werden konnten, sowie die Zeitdauer angezeigt, die der jeweilige Service für die Suche nach Ergebnissen und das Abrufen von Ereignissen basierend auf der Abfrage benötigte. Sie können die vollständige Abfrage als Text kopieren. Weitere Informationen finden Sie unter „Filtern von Daten in der Ansicht ‚Ereignisanalyse‘“ im *NetWitness Investigate – Benutzerhandbuch*.

Verbesserter Workflow für Analysten in den Ansichten „Navigation“, „Ereignisse“ und „Ereignisanalyse“

Um die Durchführung von Ermittlungen für Analysten zu erleichtern, wurden diese Verbesserungen implementiert:

- Wenn Sie in der Ansicht „Ereignisse“ zwischen den Seiten wechseln, werden Protokollereignisse aufgrund des Zwischenspeicherns von Abfrageergebnissen schneller geladen.
- Der in der Navigation genutzte Zeitbereich wird beim Wechseln in die Ansicht „Ereignisse“ verwendet.

- In der Ansicht „Navigation“ wird eine leicht verständliche Metaschlüsselbeschreibung neben dem Namen des Metaschlüssels angezeigt. Weitere Informationen finden Sie unter „Ansicht ‚Navigation‘“ im *NetWitness Investigate – Benutzerhandbuch*.
- In der Ansicht „Ereignisanalyse“ wurde eine benutzerdefinierte Zeitbereichseingabe hinzugefügt. Zusätzlich zu den vordefinierten Zeitfenstern können Sie einen benutzerdefinierten Zeitbereich eingeben und dann auf den Monat, den Tag, das Jahr, die Stunde und die Minute klicken, um den Zeitbereich direkt in der Brotkrümelnavigation zu bearbeiten. Weitere Informationen finden Sie unter „Filtern von Daten in der Ansicht ‚Ereignisanalyse‘“ im *NetWitness Investigate – Benutzerhandbuch*.

Weitere Informationen zu geladenen Ereignissen in der Ansicht „Ereignisse“ werden in der Fußzeile eingeblendet

Anhand der Nachricht in der Fußzeile können Analysten verstehen, was in der Ansicht „Ereignisse“ angezeigt wird. Wenn keine Ereignisse geladen werden, wird diese Meldung angezeigt: „0 Ereignisentsprechungen“. In anderen Meldungen werden Sie darüber informiert, ob der vom Administrator festgelegte Scan- oder Ergebnisgrenzwert erreicht wurde und für welche Services Ergebnisse angezeigt werden. Beispielsweise erfahren Sie in der folgenden Meldung, dass der Scangrenzwert erreicht wurde und weitere Daten zum Scannen verfügbar sind: „1 bis 25 von 100.000+ Ereignisentsprechungen werden angezeigt (Scangrenzwert von 100.000 Ereignissen wurde erreicht)“. Weitere Informationen finden Sie unter „Ansicht ‚Ereignisse‘“ im *NetWitness Investigate – Benutzerhandbuch*.

Schnellere Such- und Abfragegeschwindigkeit in den Ansichten „Navigation“ und „Ereignisse“

Wenn in der Ansicht „Navigation“ arbeitende Analysten einen Broker oder Concentrator abfragen, geben nachfolgende Abfragen, die alle oder einige der Kriterien einer vorherigen Abfrage gemeinsam nutzen, die Ergebnisse schneller zurück, indem neue Zwischenspeicherungsfunktionen in die Services integriert werden. In der Ansicht „Ereignisse“ werden Abfragen zwischengespeichert, die komplexe Vorgänge mit Textwerten verwenden, sodass nachfolgende Abfragen, die alle oder einige der Kriterien einer vorherigen Abfrage gemeinsam nutzen, die Ergebnisse schneller zurückgeben.

Neue Abfrageerstellungsfunktionen in der Ansicht „Ereignisanalyse“

- Sie können komplexe Filter in der Abfrageerstellung im geleiteten Modus erstellen, indem Sie den Filter „Freitext“ im Untermenü „Erweiterte Optionen“ verwenden, der sich in allen Drop-down-Menüs des geleiteten Modus befindet. Der Freitextmodus ist zum Einfügen einer langen, komplexen Abfrage weiterhin verfügbar.
- Wenn Sie eine Abfrage mit Freitextfiltern senden, werden diese serverseitig vor der Ausführung validiert. Wenn einer der Filter ungültig ist, wird die Abfrage nicht ausgeführt.
- Während der Ausführung einer Abfrage können Sie diese abbrechen. Wenn eine Abfrage abgebrochen wird, geben die Ereignisanzahl im Bereich „Ereignisse“, die Fußzeilennachricht und die Abfragekonsole die Anzahl der abgerufenen Ereignisse und nicht die Gesamtanzahl der gefundenen Ereignisse an.

Weitere Informationen finden Sie unter „Filtern von Ereignissen in der Ansicht ‚Ereignisanalyse'" im *NetWitness Investigate – Benutzerhandbuch*.

Aktualisierte Metaschlüssel in der Spaltengruppe „Endpunktanalyse"

Die Spaltengruppe „Endpunktanalyse" wurde aktualisiert und enthält nun neue Metaschlüssel für die Endpunktermittlung. Diese werden eingeblendet, wenn Sie ein Endpunktereignis in den Ansichten „Ereignisse" und „Ereignisanalyse" anzeigen.

Neue Voreinstellungsoption zur Steuerung der automatischen Aktualisierung des Zeitbereichs in der Brotkrümelnavigation

In der Ansicht „Ereignisanalyse" wird durch eine neue Voreinstellung im Dialogfeld „Ereignisvoreinstellung" die automatische Aktualisierung des Zeitbereichs in der Brotkrümelnavigation gesteuert. Während Sie die Ergebnisse für einen bestimmten Zeitbereich anzeigen, wird der Service im Minutentakt abgefragt, um festzustellen, ob neue Ergebnisse vorhanden sind. Es werden jedoch keine neuen Ergebnisse in die aktuelle Ansicht geladen. Standardmäßig bleibt das Zeitbereichsfenster in der Brotkrümelnavigation mit der aktuellen Suche synchronisiert. Sie können festlegen, dass das Zeitbereichsfenster in der Brotkrümelnavigation automatisch aktualisiert wird, wenn der Service darauf hinweist, dass die neuesten aktualisierten Ergebnisse vorhanden sind. Aktivieren Sie dazu das Kontrollkästchen **Zeitfenster automatisch aktualisieren**. Wenn der Zeitbereich aktualisiert wurde und Sie auf die Schaltfläche „Abfrage senden" klicken, können Sie die neuesten aktualisierten Ergebnisse abrufen.

Zugriff auf UEBA über „Ermittlung" > Ansicht „Hostdetails"

Wenn NetWitness UEBA installiert ist, können Sie die Risiken im Zusammenhang mit den auf dem Host angemeldeten Nutzern analysieren, indem Sie zur Ansicht „Nutzer" navigieren. Weitere Informationen finden Sie im *NetWitness UEBA – Benutzerhandbuch*.

Event Stream Analysis (ESA)

Neuer verbesserter ESA-Korrelationsservice für ESA-Korrelationsregeln

Der ESA-Korrelationsservice in NetWitness Platform 11.3 ersetzt den Event Stream Analysis-Service vorheriger Versionen. Wie der Event Stream Analysis-Service wird auch der ESA-Korrelationsservice auf den Hosttypen „ESA Primary" und „ESA Secondary" installiert.

Es gibt zwei ESA-Services, die auf einem ESA-Host ausgeführt werden können:

- ESA-Korrelation (ESA-Korrelationsregeln)
- Event Stream Analytics Server (ESA Analytics)

Der Service „Context Hub-Server", der Anreicherungsabfragefunktionen in den Ansichten „Respond" und „Ermittlung" bereitstellt, wird nur auf einem ESA Primary-Host ausgeführt.

Unterstützung für verschiedene Datenquellen für Ihre ESA-Korrelationsregeln

Anstatt Datenquellen (z. B. Concentrator) dem gesamten Service hinzuzufügen, können Sie für jede Bereitstellung von ESA-Regeln verschiedene Datenquellen festlegen. Sie können beispielsweise Concentrator mit HTTP-Paketdaten in einer Bereitstellung und Concentrator mit HTTP-Protokolldaten in einer anderen Bereitstellung verwenden. Weitere Informationen finden Sie im *Warnmeldungen mit ESA-Korrelationsregeln – Benutzerhandbuch*.

Überlegungen zum Upgrade für Bereitstellungen von ESA-Regeln finden Sie in den entsprechenden Upgrade- und Aktualisierungsanweisungen sowie im *ESA-Konfigurationsleitfaden*.

Unterstützung für die Anpassung der Komprimierungsebene für Concentrator auf ESA

Wenn Sie eine Bereitstellung von ESA-Regeln einrichten und einen Concentrator zur Verwendung als Datenquelle konfigurieren, haben Sie die Möglichkeit, die Datenkomprimierungsebene für den Concentrator auf ESA festzulegen. Weitere Informationen finden Sie im *Warnmeldungen mit ESA-Korrelationsregeln – Benutzerhandbuch*.

Aktivieren oder Deaktivieren der Weiterleitung von Warnmeldungen zu einzelnen ESA-Regeln an die Ansicht „Respond“

Sie können Warnmeldungen für einzelne ESA-Regeln aktivieren oder deaktivieren. Weitere Informationen finden Sie im *ESA-Konfigurationsleitfaden*.

ESPER-Version 5.3 aktualisiert auf Version 7.1

ESPER wurde auf die neueste Version 7.1 aktualisiert.

Log Collector

Sortierte Liste mit Log Collector (LC) und Virtual Log Collector (VLC)

Für die Log Collector-Services „Local Collector“ und „Remote Collector“ werden die Drop-down-Menüs alphabetisch sortiert, damit Sie den anzuzeigenden Collector leichter auffinden können:

- Auf einem Local Collector wird auf der Registerkarte „Remote Collector“ das Feld „Remote Collector“ im Dialogfeld „Quelle hinzufügen“ sortiert.
- Auf einem Virtual Log Collector weist die Registerkarte „Local Collector“ sortierte Felder für Ziele und Quellen auf.

Sortierte Liste mit Log Collector und Log Decoder

Die Drop-down-Menüs „Log Collector“ und „Log Decoder“ in der Ansicht „ADMINISTRATION“ > „Integrität und Zustand“ > „Ereignisquellenüberwachung“ werden alphabetisch sortiert, damit Sie die anzuzeigenden Elemente leichter auffinden können.

Syslog-Ports für lokale Log Collector

In Version 11.3 können lokale Log Collector (Log Collector, die sich auf Log Decoder-Appliances befinden) Syslog auf anderen Ports als 514 und 6514 empfangen, um den Empfang von Syslog-Nachrichten mit unterschiedlichen Codierungen zu unterstützen, z. B. EUC-KR, ISO8897-9 usw. Der Log Decoder-Service ist nach wie vor die Sammelstelle für den Empfang von ASCII/UTF-8-Protokollen auf Ports 514 und 6514.

Verbesserte Pass-Through-Logik für nicht konformes Syslog

Remote Log Collector akzeptieren nun alle nicht konformen Syslog-Meldungen, mit Ausnahme derer, die eine leere Kopfzeile oder einen leeren Nachrichtentext haben. Unerwünschte Meldungen sollten bei der Syslog-Erfassung mithilfe von Ereignisfiltern herausgefiltert werden. Weitere Informationen finden Sie im Abschnitt „Konfigurieren von Ereignisfiltern für einen Collector“ im *Protokollsammlungs-Leitfaden*. Weitere Informationen zum Syslog-Format können Sie „Syslog RFC3164“ und „Syslog RFC5424“ entnehmen (https://www.ietf.org/standards/rfcs/).

Core-Services

Snort-Parser mit UDM-Unterstützung

Die Unterstützung für Snort-Parser wurde mit der neuen Option `udm=true` aktualisiert, die den ausgerichteten UDM-Schlüsselsatz (Unified Data Model) verwendet. Weitere Informationen finden Sie unter „Snort-Parser“ im *Konfigurationsleitfaden für Decoder und Log Decoder*.

Entschlüsselung von Secure SMTP

NetWitness Platform unterstützt die opportunistische SSL/TLS-Entschlüsselung, die in „RFC 3207“ (https://Tools.ietf.org/html/rfc3207) behandelt wird. Sie können eine HTTPS-Parser-Option hinzufügen, die eine CSV-formatierte Liste (durch Trennzeichen getrennte Werte) mit Zielports der Sitzung enthält, in der der STARTTLS-Befehl gesucht wird, wobei mindestens ein Chiffrierschlüssel hochgeladen wurde. Dadurch wird die STARTTLS-Funktion aktiviert. Weitere Informationen finden Sie unter „Entschlüsselung von Secure SMTP“ im *Konfigurationsleitfaden für Decoder und Log Decoder*.

GeoIP-Parser wird nicht mehr unterstützt und wurde durch GeoIP2-Parser ersetzt

Der ursprüngliche GeoIP-Parser wird nicht mehr unterstützt. Er wurde durch den in Version 11.2 eingeführten neuen GeoIP2-Parser vollständig ersetzt. Der GeoIP2-Parser unterstützt alle vorherigen Funktionen sowie das neue Maxmind-Paket, einschließlich IPv4-und IPv6-Konvertierungen.

Einschränken der Abfragespeichernutzung mit dem SDK-Parameter „max.query.memory“

Mit dem Parameter `max.where.clause.sessions` wird die Anzahl der Sitzungen begrenzt, die durch eine einzige Abfrage gescannt werden können. Beispiel: Wenn ein Benutzer alle Metadaten einer Datenbank auswählt, beendet die Datenbank die Verarbeitung der Ergebnisse, sobald die Anzahl der Sitzungslesevorgänge für die Abfrage diesen Konfigurationswert erreicht. Dieser Parameter wird in einer zukünftigen Version nicht mehr unterstützt. Verwenden Sie den Parameter`max.query.memory`, um die Gesamtspeichernutzung der Abfrage zu begrenzen.

PowerVault-SEDs kann für den externen Speicher verwendet werden.

Sie können nun PowerVault-SEDs (selbstverschlüsselnde Festplatten) für die Verwendung als externen Speicher konfigurieren, um Protokolle und Paketdaten für den Abruf zu speichern.

N-Gram-Indizes haben eine bessere Performance als in Version 11.2 mit verbesserten Volltext-Suchvorgängen

Es wurden Verbesserungen an der Einfügerate von N-Gram-Indizes für Volltext-Suchvorgänge vorgenommen. N-Gram-Modusindizes sind für Aktualisierungen etwa doppelt so schnell, was bedeutet, dass sie in mehreren Concentrators genutzt werden können, ohne dass sich dies auf die Performance der Aggregation auswirkt. Standardmäßig ist diese Funktion deaktiviert. Weitere Informationen zu N-Gram-Indizes finden Sie unter „Indexanpassung“ im *Core-Datenbank-Tuning-Leitfaden für NetWitness Platform*.

Neue `avglen`-Funktion in der Datenbank-Abfragesyntax

Die `avglen`-Funktion wurde zur Abfragesyntax hinzugefügt. Sie gibt einen einzelnen Wert zurück, d. h. die durchschnittliche Länge eines Metawerts innerhalb einer Funktion.

Administration

Möglichkeit zur Konfiguration von Hybridkomponenten auf Core-Appliances (ermöglicht die Verwendung von mehreren PowerVaults für Hybridkomponenten)

Sie können Hybridkategorien wie Log Hybrid- und Network (Packet) Hybrid-Servicekategorien auf einem physischen Host der Serie 6 (R640) installieren. So haben Sie die Möglichkeit, mehrere externe PowerVault-Speichergeräte an den physischen Host der Serie 6 (R640) anzuhängen.

PKI-Authentifizierung (Public Key Infrastructure)

Durch die PKI-Authentifizierung können sich Nutzer authentifizieren und mithilfe von digitalen Zertifikaten auf die NetWitness Platform-Benutzeroberfläche zugreifen. Weitere Informationen finden Sie unter „PKI-Authentifizierung“ im *Handbuch zur Systemsicherheit und Benutzerverwaltung*.

DISA STIG-Unterstützung

In Version 11.3 unterstützt RSA alle Auditregeln der DISA STIG-Kontrollgruppe (Defense Information Systems Agency Security Technical Implementation Guide). Weitere Informationen zur STIG-Unterstützung in Version 11.3 finden Sie im *Leitfaden Systemwartung*.

Befehl „Zertifikat erneut ausgeben“

RSA hat den Befehl `cert-reissue` und die zugehörigen Argumente hinzugefügt, damit Sie Hostzertifikate erneut ausgeben können. Nachdem Sie alle Hosts auf 11.3 aktualisiert haben, sollten Sie für alle so bald wie möglich Zertifikate erneut ausgeben, um zu verhindern, dass Sie ablaufen. Wenn die Zertifikate ablaufen, wird Ihre NetWitness-Bereitstellung in einen nicht wiederherstellbaren Zustand versetzt. Weitere Informationen zum erneuten Ausstellen von Zertifikaten in Version 11.3 finden Sie im *Systemkonfigurationsleitfaden*.

Aktiver Stand-by-NW-Serverhost (für Failover/hohe Verfügbarkeit) – nur physischer Host

Der aktive Stand-by-NW-Server dupliziert die kritischen Komponenten und Konfigurationen des aktiven NW-Serverhosts, um die Zuverlässigkeit zu erhöhen. Der aktive Stand-by-NW-Server kann so konfiguriert werden, dass er im Stand-by-Modus verbleibt und in regelmäßigen Abständen Backups des aktiven NW-Serverhosts empfängt. Wenn der aktive NW-Server ausfällt (in den Offlinezustand wechselt), kann das Failover-Verfahren ausgeführt werden und der Stand-by-NW-Server wird aktiv. Weitere Informationen zum Einrichten und Managen eines aktiven Stand-by-NW-Servers in Version 11.3 finden Sie im NetWitness Platform *Leitfaden zur Bereitstellung*.

Neues Tool zur Konsolidierung von Host- und Servicekonfigurationsdaten in einer einzelnen Instanz

Das NW-Konsolidierungstool steht ausgewählten 10.6.6-Kunden zur Verfügung, die die Konfiguration und die Daten von Version 10.6.6 zu NetWitness Platform 11.3 migrieren möchten. Dieses Tool kann verwendet werden, wenn Ihre Bereitstellung mehrere Security Analytics- und Reporting Engine-Instanzen aufweist und Sie die Host- und Serviceskonfiguration und -daten in einer einzelnen Instanz konsolidieren möchten. Sie können auch die Daten im Zusammenhang mit Nutzern, Gruppen, Rollen, Feeds und Berichten konsolidieren.

Lizenzierung

Unterstützung für die Lizenzierung von Endpoint und ESA-Korrelationsservern sowie die Konsolidierung aller Berechtigungen für Durchsatzlizenzen

Die erweiterte Benutzeroberfläche für die Lizenzierung erleichtert Administratoren die Anzeige der Lizenzinformationen. Auf der Seite „Lizenzierungsdetails“ wird die Nutzung des gebündelten Durchsatzes für verschiedene Berechtigungen mit Trends bei der Durchsatznutzung angezeigt. Administratoren können alle Lizenzen in der Bereitstellung anzeigen, einschließlich der für Endpoint und den ESA-Korrelationsserver. Darüber hinaus können Administratoren die Lizenzen für mehrere NetWitness-Server sowie für Hot- und Warm-Server konfigurieren. Weitere Informationen finden Sie im *Leitfaden zum Lizenzmanagement*.

Bedrohungsbasierte Authentifizierung

NetWitness Platform-Integration mit RSA SecurID Access

Die NetWitness Platform-Integration in RSA SecurID Access ermöglicht es Ihnen, verdächtige Nutzer in der NetWitness Platform zu identifizieren und die Zugriffsebenen zu erhöhen oder die Nutzer in RSA SecurID Access zu blockieren, basierend auf der Sicherheitsstufe und den in SecurID definierten SecurID-Richtlinien. Der NetWitness Respond-Server sendet E-Mail-Kennungen verdächtiger Nutzer von Incidents an RSA SecurID Access. Weitere Informationen zum Konfigurieren dieser Integration auf dem Respond-Server finden Sie im *Respond – Konfigurationsleitfaden*.

Behobene Probleme

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

Sicherheit

Rückverfolgungsnummer	Beschreibung
ASOC-59254	Kernel-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:1965
ASOC-58383	policycoreutils-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:0913
ASOC-58382	Openssl-Sicherheitsaktualisierung https://access.redhat.com/errata/RHSA-2018:0998

Ermittlung

Rückverfolgungsnummer	Beschreibung
ASOC-61230	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.
ASOC-60941	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.
ASOC-50196	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	Beschreibung
ASOC-49427	Die Abfrageerstellung in der Ansicht „Ereignisanalyse“ reagiert nicht auf Filter, die ein Leerzeichen enthalten.

Reagieren

Rückverfolgungsnummer	Beschreibung
ASOC-59243	Wenn alle Warnmeldungen für eine Warnmeldungsregel gelöscht werden, wird der Filter für die Regel nicht ordnungsgemäß entfernt.
ASOC-37533	Wenn eine benutzerdefinierte In-Memory-Tabelle erstellt und als Erweiterungsquelle in ESA hinzugefügt wird, werden diese Informationen nicht für ESA-Warnmeldungen angezeigt.

Event Stream Analysis (ESA)

Rückverfolgungsnummer	Beschreibung
ASOC-60511	ESA-CH-Regeln werden während des Upgrades oder des Neustarts von ESA-Hosts deaktiviert.
ASOC-60367	ESA-Regeln mit benutzerdefinierten Metaschlüsseln werden nicht auf dem ESA-Server bereitgestellt.
ASOC-26481	Die ESA-Komprimierungsstufe kann nicht wie in anderen Appliances festgelegt werden.
ASOC-14157	ESA zeigt Warnung für Array-Operatoren an.

Core-Services

Rückverfolgungsnummer	Beschreibung
ASOC-41902	Das Kontrollkästchen „SSL FIPS-Modus“ muss für Broker, Concentrator und Archiver deaktiviert werden.

Upgrade

Rückverfolgungsnummer	Beschreibung
ASOC-49843	Während des Upgrades auf Version 11.x werden Auditprotokollvorlagen nicht in der Logstash-Ausgabekonfigurationsdatei aktualisiert.
ASOC-42136	Aktivität nach dem Upgrade, die Investigation-Links sind für statische Diagramme deaktiviert.

Hinweise zum Upgrade

Die folgenden Upgradepfade werden für RSA NetWitness® Platform 11.3.0.0 unterstützt:

- RSA NetWitness® Platform 10.6.6.x auf 11.3.0.0
- RSA NetWitness® Platform 11.0.x, 11.1.x oder 11.2.x auf 11.3.0.0

Weitere Informationen zur Installation von und zum Upgrade auf Version 11.3.0.0 finden Sie in den Installations- und Upgradehandbüchern auf https://community.rsa.com/community/products/netwitness/113 > Installations- und Upgradehandbücher.

Produktdokumentation

Die folgende Dokumentation ist im Lieferumfang der Version enthalten.

Dokumentation	Standort-URL
RSA NetWitness Platform 11.3 – Onlinedokumentation	https://community.rsa.com/community/products/netwitness/documentation
RSA NetWitness Platform 11.3 – Anweisungen für das Upgrade	https://community.rsa.com/community/products/netwitness/documentation

Dokumentation	Standort-URL
RSA NetWitness Platform – Handbücher für die Hardwarekonfiguration	https://community.rsa.com/community/products/netwitness/hardware-setup-guides
RSA-Inhalte für RSA NetWitness Platform	https://community.rsa.com/community/products/netwitness/rsa-content

Bekannte Probleme

Probleme, die in dieser Version noch nicht gelöst wurden, sind auf der folgenden Website dokumentiert: https://community.rsa.com/community/products/netwitness/documentation/known-issues. Sofern ein Workaround verfügbar ist, werden ausführliche Anmerkungen oder Verweise eingefügt.

Feedback zur Produktdokumentation

Sie können eine E-Mail an sahelpfeedback@rsa.com senden, um Feedback zu den Dokumentation der RSA NetWitness Platform zu geben.

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.

Nr.	Funktion	Anmerkungen
7.	Einige Funktionen des Event Stream Analysis-Services von Version 11.2 und älter	Funktionen des Event Stream Analysis-Services (11.2 und älter), die sich nicht im ESA-Korrelationsservice 11.3 befinden: 1. Speicher-Snapshot für Testregeln 2. Benachrichtigungsmethode für ESA-SNMP 3. Datenbank als Erweiterungsquelle (durch Context Hub-Liste ersetzt) 4. Warehouse Analytics als Erweiterungsquelle (durch Context Hub-Liste ersetzt) 5. Database Connection als Erweiterungsquelle (durch Context Hub-Liste ersetzt) 6. Sortierung nach Erfassungszeit 7. Arbeitsspeicherpool
8.	Endpoint Hybrid	Der Typ „Endpoint Hybrid-Host“ wird in 11.3.0.0 und neueren Versionen nicht unterstützt.

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

Wenn Sie Fragen haben oder Unterstützung benötigen, befolgen Sie die Anweisungen auf der folgenden Website: https://community.rsa.com/docs/DOC-1294

Revisionsverlauf

Version	Datum	Beschreibung
1,0	13. März 2019	Betriebsfreigabe