RSA NETWITNESS® PLATFORM

NetWitness Investigate – Quickstart-Handbuch

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 Dell 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 Dell 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 Nutzer 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

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

Juni 2019

Was ist NetWitness® Investigate?

NetWitness Platform prüft und überwacht den gesamten Datenverkehr in einem Netzwerk. Ein Servicetyp, ein Decoder, kümmert sich um die Aufnahme, Analyse und Speicherung der Pakete, Protokolle und Endpunktdaten, die über das Netzwerk übertragen werden. Mit den konfigurierten Parsern und Feeds auf dem Decoder werden *Metadaten* erstellt, die Analysten zum Untersuchen der aufgenommenen Protokolle und Pakete verwenden können. Ein anderer Servicetyp, der als Concentrator bezeichnet wird, indiziert und speichert die Metadaten. NetWitness Investigate bietet die Datenanalysefunktionen, die in RSA NetWitness® Platform verfügbar sind, mit denen Analysten Paket-, Protokoll- und Endpunktdaten analysieren und mögliche interne oder externe Bedrohungen für die Sicherheit und die IP-Infrastruktur erkennen können.

Informationen zu diesem Handbuch

Dieses Benutzerhandbuch bietet End-to-End-Guidelines für alle Mitglieder des SOC-Teams, um NetWitness Investigate zu konfigurieren und um Protokoll- und Netzwerkereignisse zu untersuchen. Die End-to-End-Guidelines für die Untersuchung von Endpunkten und das Verhalten von Nutzerentitäten mithilfe von NetWitness Investigate werden in separaten Dokumenten bereitgestellt:

- *NetWitness Endpoint – Quickstart-Handbuch*
- *NetWitness UEBA – Quickstart-Handbuch*

RSA NetWitness Platform 11.3 – Dokumentation in RSA Link

Die Produktdokumentation für NetWitness Platform ist nach funktionalen Gesichtspunkten aufgebaut. Wenn Sie nach einem bestimmten Benutzerhandbuch oder nach einer bestimmten Version suchen, gehen Sie zum Masterinhaltsverzeichnis der Version 11.x.

Verwenden Sie diese Links, um die Dokumentation der RSA NetWitness Platform 11.3 anzuzeigen. Beide Links stellen die gleiche Dokumentation in diesen beiden Formaten bereit:

- HTML-Benutzerhandbücher enthalten die neuesten Informationen zu derzeit unterstützten Versionen von 11.x: RSA NetWitness Platform 11.x Dokumentation.
- PDF-Benutzerhandbücher enthalten die Informationen für eine bestimmte Version: RSA NetWitness Platform 11.3 PDFs.

Verwenden Sie diese Links, um auf Dokumentationen zuzugreifen, die sich nicht auf eine bestimmte Version der Software beziehen:

- Benutzerhandbücher zur Hardwarekonfiguration: https://community.rsa.com/community/products/netwitness/hardware-setup-guides
- Dokumentation für RSA-Inhalte wie Feeds, Parser, Anwendungsregeln und Berichte: https://community.rsa.com/community/products/netwitness/rsa-content.

Erste Schritte

Die folgenden Aufgaben können in beliebiger Reihenfolge durchgeführt werden und gelten für das gesamte SOC-Team.

Beschreibung	Referenzen
	
Anzeigen von Informationen zu Produktaktualisierungen, Verbesserungen und bekannten Problemen	*Veröffentlichungshinweise für RSA NetWitness Platform 11.3*
Verstehen, wie NetWitness Investigate funktioniert	„So funktioniert NetWitness Investigate“ im *NetWitness Investigate – Benutzerhandbuch*

Setup, Installation oder Upgrade

Für Investigate sind keine speziellen Setup-, Installations- oder Upgrade-Aufgaben erforderlich; es ist Teil von NetWitness Platform for Logs and Network. Das Setup ist jedoch für mehrere Komponenten erforderlich, mit denen NetWitness Investigate arbeitet, wenn Sie diese Art der Analyse planen. Diese Aufgaben sind für den Administrator bestimmt, und der SOC-Manager möchte möglicherweise das Setup verstehen.

Beschreibung	Referenzen
	
Installation und Einrichtung von Malware Analysis (eigenständig oder Service)	Konfigurationsleitfaden Malware Analysis
Installation und Einrichtung von NetWitness Endpoint (eigenständig oder Service)	NetWitness Endpoint – Quickstart-Handbuch
Installation und Einrichtung von NetWitness UEBA (eigenständig oder Service)	NetWitness UEBA – Quickstart-Handbuch

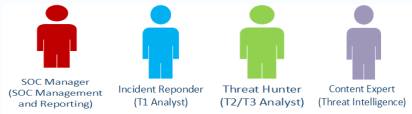
Konfiguration auf Systemebene

Administratoren konfigurieren die Einstellungen auf Systemebene für NetWitness Ermittlung. Die folgenden Aufgaben sind für den Administrator und die Aufgaben können in beliebiger Reihenfolge durchgeführt werden. SOC-Manager sollten die möglichen Konfigurationsoptionen kennen.

Beschreibung	Referenzen
	
Konfigurieren einer rollenbasierten Zugriffskontrolle (RBAC) für Analysten, die Investigate verwenden werden. Diese Komponenten verfügen über Berechtigungen für Investigate: Investigate (Ansicht „Navigation“ und „Ereignisse“), Investigate-Server (Ansicht „Ereignisanalyse“), Malware (Ansicht „Malware Analysis“), Endpoint-Broker-Server und Endpoint-Server.	„Rollenberechtigungen“ im Handbuch Systemsicherheit und Nutzerverwaltung
Konfigurieren von Investigate, um die Inhalte einzuschränken, die für verschiedene Nutzerrollen verfügbar sind (preQueries).	„Überprüfen von Abfrage- und Sitzungsattributen pro Rolle“ im Handbuch Systemsicherheit und Nutzerverwaltung
Konfigurieren der Standardeinstellungen und Limits für NetWitness Investigate auf Systemebene.	„Konfigurieren von Investigation-Einstellungen“ im Systemkonfigurationsleitfaden

Konfiguration der Nutzerpräferenz

Die folgenden Aufgaben gelten für Threat Hunters, Contentexperten und Incident-Experten sowie SOC-Manager. Die Aufgaben können in beliebiger Reihenfolge durchgeführt werden.

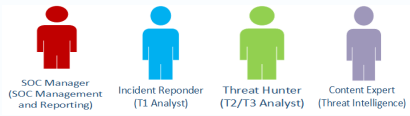
Beschreibung	Referenzen
	
Konfigurieren der Einstellungen für die Ansichten „Navigation“ und „Ereignisse“.	„Konfigurieren der Ansichten „Navigation“ und „Ereignisse““ im *NetWitness Investigate – Benutzerhandbuch*
Konfigurieren der Einstellungen für die Ansicht „Ereignisanalyse“.	„Konfigurieren der Ansicht „Ereignisanalyse““ im *NetWitness Investigate – Benutzerhandbuch*

Beschreibung	Referenzen
Konfigurieren der Einstellungen für die Ansicht „Malware Analysis“.	„Konfigurieren von Malware Analysis“ im *Malware-Analyse – Benutzerhandbuch*.

Investigation

Verschiedene Arten von Ermittlungen können von Analysten mit unterschiedlichen Kompetenzstufen und Zielen bearbeitet werden.

- Incident-Experten (T1-Analysten) wechseln typischerweise zu Investigate von NetWitness Respond, um detaillierte Informationen über einen Incident zu erhalten, damit Sie auf Incidents reagieren und diese beheben können.
- Threat Hunters (T2/T3-Analysten) durchsuchen typischerweise Ereignisse, Metadaten und Rohinhalte, damit sie Probleme zur Behebung empfehlen und Probleme beheben können.
- Contentexperten (Threat Intelligence) durchsuchen typischerweise Ereignisse, Metadaten, Rohinhalte, Nutzer- und Hostdaten sowie UEBA-Daten, um neue Bedrohungsinformationen zu untersuchen, neue Feeds zu bewerten und zu erstellen und Korrelationsregeln für die Kennzeichnung von Kompromissindikatoren zu erstellen.
- SOC- Manager müssen die Anwendungsbeispiele verstehen.

Beschreibung	Referenzen
	
Informationen zu praktischen Anwendungsbeispielen	„Anwendungsbeispiele für NetWitness Investigate“ im *NetWitness Investigate – Benutzerhandbuch*
Untersuchen von Metadaten und Raw-Ereignissen in Protokollen und Netzwerkdatenverkehr	„Starten einer Ermittlung“ im *NetWitness Investigate – Benutzerhandbuch*
Untersuchen möglicher Malware	Leitfaden zur Malware Analysis
Untersuchen von Endpunkten	NetWitness Endpoint – Benutzerhandbuch
Durchführen von Analysen des Nutzer- und Entitätsverhaltens	NetWitness UEBA – Benutzerhandbuch

Wartung

Der Administrator kann die folgenden Aufgaben in beliebiger Reihenfolge ausführen.

Beschreibung	Referenzen
	
Verwalten der Liste der Abfragen und Analysieren der Abfragemuster anderer Nutzer des NetWitness Platform-Systems.	„Verwalten von Abfragen mithilfe von URL-Integration“ im Leitfaden Systemwartung
Optimieren der Konfigurationseinstellungen auf Systemebene, um die Performance zu verbessern oder den Zugriff auf Daten zu beschränken.	„Überprüfen von Abfrage- und Sitzungsattributen pro Rolle“ im Handbuch Systemsicherheit und Nutzerverwaltung „Konfigurieren von Investigation-Einstellungen“ im Systemkonfigurationsleitfaden