RSA NETWITNESS® PLATFORM

Guía de inicio rápido de NetWitness Investigate

para RSA NetWitness® Platform 11.3

Información de contacto

RSA Link en https://community.rsa.com contiene una base de conocimientos que responde a las preguntas comunes y brinda soluciones para problemas conocidos, documentación de productos, análisis de la comunidad y administración de casos.

Marcas comerciales

Para obtener una lista de las marcas comerciales de RSA, visite mexico.emc.com/legal/emc-corporation-trademarks.htm#rsa (visite el sitio web de su país correspondiente).

Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de Dell, se suministran bajo licencia, y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con el aviso de copyright mencionado a continuación. No se puede suministrar a ninguna persona, ni poner a su disposición de cualquier otra manera, este software ni la documentación, o cualquier copia de estos elementos.

Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal.

Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por Dell.

Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. El texto de los acuerdos de licencia que se aplican al software de otros fabricantes en este producto puede encontrarse en la página de documentación del producto en RSA Link. Al usar este producto, el usuario acepta regirse totalmente por los términos de los acuerdos de licencia.

Nota sobre tecnologías de cifrado

Es posible que este producto contenga tecnologías de cifrado. Muchos países prohíben o limitan el uso, la importación o la exportación de las tecnologías de cifrado, y las regulaciones actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

Distribución

Dell considera que la información de esta publicación es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

junio 2019

¿Qué es NetWitness® Investigate?

NetWitness Platform audita y monitorea todo el tráfico de una red. Un tipo de servicio, un Decoder, recopila, analiza y almacena los paquetes, los registros y los datos de terminales que recorren la red. Los analizadores y los feeds configurados en el Decoder crean *metadatos* que los analistas pueden usar para investigar los registros y los paquetes recopilados. Otro tipo de servicio, denominado un Concentrator, indexa y almacena los metadatos. NetWitness Investigate ofrece funcionalidades de análisis de datos en RSA NetWitness® Platform de modo que los analistas puedan analizar datos de paquetes, registros y terminales, e identificar posibles amenazas internas o externas a la seguridad y la infraestructura de IP.

Acerca de esta guía

En esta guía se proporcionan reglas de punto a punto para todos los miembros del equipo del SOC a fin de configurar NetWitness Investigate y investigar eventos de registro y de red. Las reglas de punto a punto para investigar las terminales y el comportamiento de las entidades de usuario mediante NetWitness Investigate se proporciona en otra documentación:

- *Guía de inicio rápido de NetWitness Endpoint*
- *Guía de inicio rápido de NetWitness UEBA*

Documentación de RSA NetWitness Platform 11.3 en RSA Link

La documentación del producto de NetWitness Platform está organizada en líneas funcionales. Si se busca una versión o una guía específica, vaya a la Tabla de contenido principal de la versión 11.x.

Utilice estos enlaces para ver la documentación de RSA NetWitness Platform 11.3. Ambos enlaces proporcionan la misma documentación en estos dos formatos:

- Las guías HTML incluyen la información más reciente acerca de las versiones 11.x que se soportan actualmente: Documentación de RSA NetWitness Platform 11.x.
- Las guías PDF proporcionan la información correspondiente a una versión específica: PDF de RSA NetWitness Platform 11.3

Utilice estos enlaces para obtener acceso a documentación que no está relacionada con una versión específica del software:

- Guías de configuración de hardware: https://community.rsa.com/community/products/netwitness/hardware-setup-guides
- Documentación de contenido de RSA, como feeds, analizadores, reglas de aplicación e informes: https://community.rsa.com/community/products/netwitness/rsa-content.

Introducción

Las siguientes tareas se pueden realizar en cualquier secuencia y aplican para todo el equipo del SOC.

Descripción	Referencias
	
Ver información acerca de las actualizaciones del producto, las mejoras y los problemas conocidos	*Notas de la versión de NetWitness Platform 11.3*
Cómo funciona NetWitness Investigate	"Cómo funciona NetWitness Investigate" en la *Guía del usuario de NetWitness Investigate*.

Configuración, instalación o actualización

No se requieren tareas especiales de configuración, instalación ni actualización para Investigate. es parte de NetWitness Platform para los registros y la red. Sin embargo, se requiere la configuración de varios componentes con los cuales NetWitness Investigate funciona si planea realizar este tipo de análisis. Estas tareas son para el administrador y es posible que el administrador del SOC desee comprender la configuración.

Descripción	Referencias
	
Instalar y configurar Malware Analysis (independiente o servicio)	Guía de configuración de Malware Analysis
Instalar y configurar NetWitness Endpoint (independiente o servicio)	Guía de inicio rápido de NetWitness Endpoint
Instalar y configurar NetWitness UEBA (independiente o servicio)	Guía de inicio rápido de NetWitness UEBA

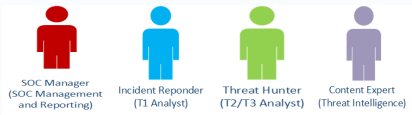
Configuración de nivel de sistema

Los administradores configuran las preferencias de nivel de sistema para NetWitness Investigate. Las siguientes tareas son para el administrador y se pueden ejecutar en cualquier secuencia. Los administradores del SOC deben comprender las posibles opciones de configuración.

Descripción	Referencias
	
Configurar el control de RBAC (acceso basado en funciones) para los analistas que utilizarán Investigate. Los siguientes componentes tienen permisos relacionados con Investigate: investigate (vista Navegar y vista Eventos), investigate-server (vista Análisis de eventos), malware (vista Malware Analysis), endpoint-broker-server y endpoint-server.	"Permisos de función" en la Guía de administración de usuarios y de la seguridad del sistema de
Configurar Investigate para limitar el contenido disponible para las diferentes funciones de usuario (consultas preexistentes).	"Verificar atributos de consultas y sesiones por función" en la Guía de administración de usuarios y de la seguridad del sistema de
Configurar los ajustes y límites predeterminados de NetWitness Investigate en el nivel del sistema.	"Configurar los ajustes de investigación" en la Guía de configuración del sistema

Configuración de preferencias de usuario

Las siguientes tareas están asociadas al trabajo de los buscadores de amenazas, expertos en contenido, encargados de respuesta ante incidentes y administradores del SOC. Las tareas se pueden realizar en cualquier secuencia.

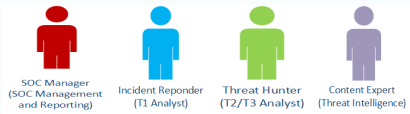
Descripción	Referencias
	
Configurar las preferencias de la vista Navegar y la vista Eventos.	Para obtener más información, consulte "Configurar la vista Navegar y la vista Eventos" en la *Guía del usuario de NetWitness Investigate*.
Configurar las preferencias de la vista Análisis de eventos.	"Configurar la vista Análisis de eventos" en la *Guía del usuario de NetWitness Investigate*

Descripción	Referencias
Configurar las preferencias de la vista Malware Analysis.	"Configurar Malware Analysis" en la *Guía del usuario de Malware Analysis*.

Investigation

Los analistas pueden manejar distintos tipos de investigaciones con diferentes niveles de habilidades y objetivos.

- Los encargados de respuesta ante incidentes (analistas T1) suelen cambiar a Investigate de NetWitness Respond para buscar información detallada acerca de un incidente a fin de responder y corregir incidentes.
- Los Buscadores de amenazas (analistas de T2/T3) por lo general se remiten a los eventos, los metadatos y el contenido crudo para entregar recomendaciones acerca de problemas que deben resolverse, además de resolver problemas.
- Los Expertos en contenido (inteligencia de amenazas) por lo general estudian los eventos, los metadatos, el contenido crudo, los datos de usuarios y de hosts y los datos de UEBA, de modo de investigar nueva inteligencia de amenazas, evaluar y crear feeds nuevos y crear reglas de correlación para marcar indicadores de vulnerabilidad.
- Los Administradores del SOC deben comprender los casos de uso.

Descripción	Referencias
	
Obtenga más información acerca de los casos de uso prácticos	"Solución de problemas de NetWitness Investigate" en la *Guía del usuario de NetWitness Investigate*
Investigar los metadatos y los eventos crudos en los registros y el tráfico de red	"Comenzar una investigación" en la *Guía del usuario de NetWitness Investigate*
Investigar posible malware	Guía del usuario de Malware Analysis
Investigar terminales	Guía del usuario de NetWitness Endpoint
Realizar UEBA (User and Entity Behavior Analysis)	Guía del usuario de NetWitness UEBA

Mantenimiento

El administrador puede ejecutar las siguientes tareas en cualquier secuencia.

Descripción	Referencias
	
Mantener la lista de consultas y analizar los patrones de consulta de otros usuarios del sistema de NetWitness Platform.	"Mantenimiento de consultas mediante la integración de URL" en la Guía de mantenimiento del sistema
Ajustar los ajustes de configuración en el nivel del sistema para mejorar el rendimiento o limitar el acceso a los datos.	"Verificar atributos de consultas y sesiones por función" en la Guía de administración de usuarios y de la seguridad del sistema de "Configurar los ajustes de Investigación" en la Guía de configuración del sistema