RSA NETWITNESS® SUITE

Guía de detección de amenazas automatizadas

para la versión 11.0

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 EMC, 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 EMC.

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

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

febrero 2018

Contenido

Detección de amenazas automatizadas de NetWitness Suite

Detección de amenazas automatizadas de RSA NetWitness® Suite usa módulos preconfigurados de ESA Analytics para identificar tipos de amenazas específicos. Un módulo ESA Analytics es una canalización que consta de objetos de actividad que enriquecen un evento con información adicional a través de cálculos matemáticos. Los módulos ESA Analytics residen dentro de los servicios ESA Analytics. Los servicios ESA Analytics utilizan agregación basada en consultas (QBA) para recopilar eventos filtrados para los módulos desde Concentrators. Solo los datos que requiere un módulo se transfieren entre el Concentrator y el sistema ESA Analytics.

Hay dos servicios de ESA que se pueden ejecutar en un host de ESA:

- Event Stream Analysis (ESA Correlation Rules)
- Event Stream Analytics Server (ESA Analytics)

El primer servicio es Event Stream Analysis, un servicio que crea alertas a partir de reglas de ESA, también conocido como ESA Correlation Rules, las cuales se crean manualmente o se descargan desde Live. El segundo servicio es ESA Analytics, un servicio que se utiliza para Detección de amenazas automatizadas. Dado que el servicio ESA Analytics usa módulos preconfigurados para Detección de amenazas automatizadas, no es necesario crear ni descargar reglas para utilizarla.

En Detección de amenazas automatizadas de NetWitness Suite están disponibles actualmente dos módulos Suspicious Domains, Command and Control (C2) for Packets y C2 for Logs.

Debido a que cada módulo ESA Analytics tiene distintos requisitos de datos, asegúrese de que se cumplan todos los requisitos específicos de cada módulo antes de implementar un módulo para Detección de amenazas automatizadas.

Detección de amenazas automatizadas para Suspicious Domains

Los módulos Suspicious Domains examinan el tráfico HTTP para detectar dominios que posiblemente sean servidores de comando y control de malware que se conectan a su ambiente. Una vez que Detección de amenazas automatizadas para Suspicious Domains de NetWitness Suite examina el tráfico HTTP, genera puntajes según diversos aspectos del comportamiento del tráfico (como la frecuencia y la regularidad con las cuales se establece contacto con un dominio determinado). Si estos puntajes alcanzan un umbral establecido, se genera una alerta de ESA. Esta alerta de ESA se reenvía a la vista Respond. La alerta en la vista Respond se enriquece con datos que ayudan a interpretar los puntajes para determinar los pasos de moderación que se deben seguir.

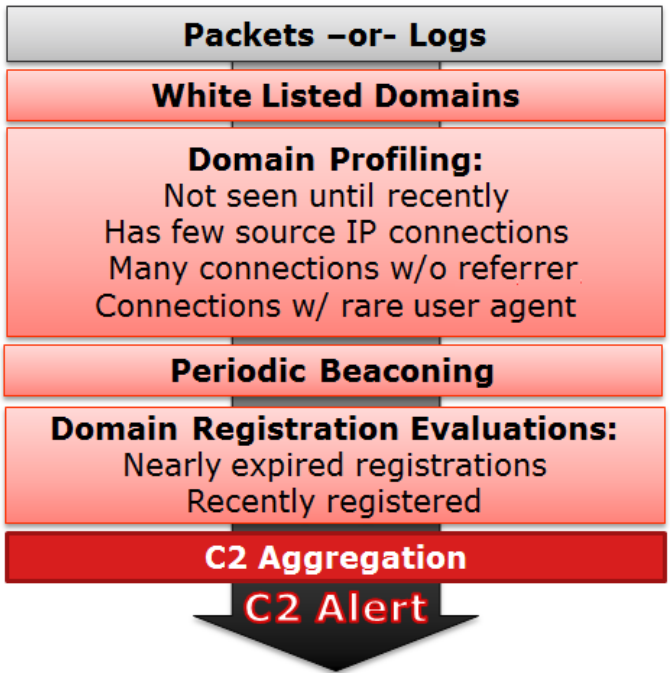
Los módulos Suspicious Domain de Detección de amenazas automatizadas proporcionan un puntaje para detectar las comunicaciones de comando y control. Las comunicaciones de comando y control se producen cuando el malware ha puesto en riesgo un sistema y envía datos a un origen. A menudo, el malware de comando y control se puede detectar a través de un comportamiento de Beacon. La señalización ocurre cuando el malware envía comunicaciones periódicas al servidor de comando y control para informarle que se ha puesto en riesgo una máquina y que espera más instrucciones. La capacidad de detectar el malware en esta etapa de riesgo puede evitar que se produzcan daños a la máquina en riesgo y se considera una etapa crítica en la "cadena de ataques".

Detección de amenazas automatizadas de NetWitness Suite resuelve varios problemas comunes que se producen cuando se busca malware:

- **Capacidad de usar algoritmos en lugar de firmas**. Debido a que muchos creadores de malware han comenzado a usar segmentos de código polimórfico o cifrado para los cuales es muy difícil crear una firma, es posible que en ocasiones este enfoque no detecte el malware. Debido a que Detección de amenazas automatizadas de NetWitness Suite usa un algoritmo basado en comportamiento, puede detectar el malware de forma más rápida y eficaz.
- **Capacidad de automatizar la búsqueda.** La búsqueda manual en los datos es un método eficaz de encontrar malware, pero también es extremadamente lento. La automatización de este proceso permite que un analista use su tiempo con mayor eficacia.
- **Capacidad de buscar un ataque rápidamente**. En lugar de la creación de lotes y el posterior análisis de los datos, Detección de amenazas automatizadas los analiza a medida que NetWitness Suite los recopila, lo cual permite la detección de los ataques casi en tiempo real.

Flujo de trabajo del módulo Suspicious Domains

Detección de amenazas automatizadas de NetWitness Suite funciona de manera muy similar a un sistema de filtrado. Comprueba si se produce un comportamiento determinado (o si existen ciertas condiciones) y, si se produce ese comportamiento o condición, continúa con el paso siguiente del proceso. Esto ayuda a hacer que el sistema sea eficiente y libera recursos, de modo que los eventos que no se consideran amenazas no se mantengan en la memoria. En el siguiente diagrama se proporciona una versión simplificada del flujo de trabajo del módulo Suspicious Domains.



1.) **Los paquetes o los registros se enrutan a ESA**. Los paquetes o los registros HTTP se analizan en el Decoder o en el Log Decoder y se envían al host de ESA.

2.) **Se comprueba la lista blanca**. Si creó una lista blanca mediante Context Hub, ESA comprueba esta lista para descartar dominios. Si un dominio del evento está en la lista blanca, se ignora el evento.

3.) **Se comprueba el perfil de dominio**. Detección de amenazas automatizadas comprueba si el dominio se vio recientemente (aproximadamente tres días), si tiene pocas conexiones de IP de origen, muchas conexiones sin un remitente o conexiones con un agente de usuario poco frecuente. Si una o varias de estas condiciones son verdaderas, se comprueba el Beacon periódico en el dominio.

4.) **Se comprueba el Beacon periódico del dominio**. La señalización ocurre cuando el malware envía comunicaciones periódicas al servidor de comando y control para informarle que se ha puesto en riesgo una máquina y que espera más instrucciones. Si el sitio muestra un comportamiento de Beacon, se comprueba la información de registro del dominio.

5.) **Se comprueba la información de registro del dominio**. Se usa el servicio Whois para ver si el dominio se registró recientemente o si está por vencer. Los dominios que poseen una vida útil muy breve a menudo son aspectos distintivos del malware.

6.) **Puntajes de agregados de Command and Control (C2)**. Cada uno de los factores anteriores genera un puntaje independiente, el cual se pondera para indicar diversos niveles de importancia. Los puntajes ponderados determinan si se debe generar una alerta. Si se genera una alerta, las alertas agregadas aparecen en la vista Respond y, posteriormente, se pueden investigar más a fondo desde ahí. Una vez que las alertas comienzan a aparecer en la vista Respond, continúan agregándose bajo el incidente asociado. Esto facilita ordenar los volúmenes de alertas que pueden generarse para un incidente de comando y control.

Los analistas pueden ver las alertas en la vista Respond.

Detección de amenazas automatizadas para Suspicious Domains en paquetes frente a registros de proxy web

RSA NetWitness Suite brinda la capacidad de realizar la Detección de amenazas automatizadas para Suspicious Domains mediante paquetes o registros de proxy web. Aunque los datos de paquetes se pueden transmitir del cable a la instalación de NetWitness Suite y analizar directamente, si tiene la capacidad de usar un proxy web en la instalación, su uso puede ser de gran utilidad. Debido a que algunas instalaciones utilizan traducción de red o cifrado SSL, la dirección IP de origen real de una conexión saliente se puede enmascarar si la observa en el nivel de los paquetes. Mediante el uso de un proxy web, obtiene el beneficio de su capacidad de acelerar y descifrar el tráfico SSL, así como de rastrear las direcciones IP de origen reales del tráfico que monitorea.

Tanto Dominios sospechosos para paquetes (C2 para paquetes) como Dominios sospechosos para registros (C2 para registros) deben producir los mismos resultados. Desde un punto de vista de resultados, usar uno sobre el otro no representa ninguna ventaja real.

Configuración de Detección de amenazas automatizadas para Suspicious Domains

En este tema se indica a los administradores y los analistas cómo configurar un módulo Suspicious Domains para Detección de amenazas automatizadas de NetWitness Suite. La funcionalidad Detección de amenazas automatizadas permite analizar los datos que residen en uno o más Concentrators mediante módulos preconfigurados de ESA Analytics. Por ejemplo, con el uso de un módulo Suspicious Domains, un servicio ESA Analytics puede examinar el tráfico HTTP para determinar la probabilidad de que exista actividad maliciosa en el ambiente.

En NetWitness Suite están disponibles dos tipos de módulos Suspicious Domains preconfigurados: Comando y control (C2) para paquetes y C2 para registros. El módulo Suspicious Domains define un subconjunto de eventos, y las actividades ejecutadas en ellos, para identificar los dominios C2 sospechosos.

Antes de que implemente un módulo ESA Analytics para Detección de amenazas automatizadas, es importante destacar que hay muchas configuraciones de instalación posibles que se pueden instalar en ESA, incluidas las siguientes: ESA Analytics, ESA Correlation Rules y Context Hub. Cada una de estas puede ocupar recursos, por lo que es importante considerar el dimensionamiento antes de implementar la Detección de amenazas automatizadas en ESA.

Requisitos previos

- Si utiliza datos de paquetes, debe haber configurado un Decoder para datos de paquetes HTTP y un analizador HTTP Lua o Flex.
- Si utiliza datos del registro de proxy web, debe haber configurado el Log Decoder correspondiente con el analizador correcto para el proxy web.
- Si utiliza datos del registro de proxy web, debe haber actualizado a los analizadores de registros más recientes. Se admiten los siguientes analizadores: Blue Coat Cache Flow (cacheflowelff), Cisco IronPort WSA (ciscoiportwsa) y Zscaler (zscalernss).
- Si utiliza datos del registro de proxy web, para obtener los mejores resultados, debe configurar todos los proxies web del mismo modo (configúrelos en la misma zona horaria, utilice el mismo método de recopilación [syslog o lote] y, si usa lote, utilice la misma cadencia de lotes).

- Debe haber una conexión abierta desde el host de ESA al servicio Whois (misma ubicación que cms:netwitness.com:443 de RSA Live) en el puerto 443. Verifique con el administrador del sistema que esto se haya establecido.
- Para ingresar un dominio a la lista blanca, debe habilitar el servicio Context Hub.

Importante: Detección de amenazas automatizadas requiere un período de "preparación" en el cual el algoritmo de puntaje se ajuste al tráfico de la red. Debe planear la configuración de Detección de amenazas automatizadas, de modo que el período de preparación tenga lugar durante el tráfico normal. Por ejemplo, el inicio de Detección de amenazas automatizadas un martes a las 08:00 h en la zona horaria que contiene la mayor cantidad de usuarios permite que el módulo analice con exactitud un día de tráfico normal.

Configurar Detección de amenazas automatizadas para Suspicious Domains

Este procedimiento proporciona los pasos necesarios para configurar un módulo Suspicious Domains de ESA Analytics para Detección de amenazas automatizadas. Los módulos ESA Analytics, como Suspicious Domains, se consideran preconfigurados porque usted no necesita crear reglas de ESA manualmente para ellos.

Los pasos básicos necesarios son:

1. **Configurar ajustes de registro (solo para registros)**. Antes de poder usar Detección de amenazas automatizadas para los registros, debe configurar varios ajustes. Omita este paso si piensa usar Detección de amenazas automatizadas para paquetes.
2. **Crear una lista blanca (opcional) mediante el servicio Context Hub**. La creación de una lista blanca permite garantizar que los sitios web de acceso frecuente se excluyan del puntaje de Detección de amenazas automatizadas.
3. **Configurar el servicio Búsqueda de WhoIs**. El servicio Whois permite obtener datos exactos acerca de los dominios a los cuales se conecta. A fin de garantizar un puntaje eficaz, es importante configurar el servicio Búsqueda de Whois. Verifique que se pueda acceder al servicio Whois desde su ambiente.
4. **Mapear orígenes de datos a los módulos ESA Analytics**. Defina la manera en que Detección de amenazas automatizadas de NetWitness Suite debe detectar automáticamente las amenazas avanzadas mediante el mapeo de un módulo ESA Analytics preconfigurado a varios orígenes de datos, como Concentrators, y a un servicio ESA Analytics.

5. **Verificar que la regla de incidentes C2 esté habilitada y monitorear la actividad**. Después de mapear el módulo Suspicous Domains, se requiere un tiempo para la preparación del algoritmo de puntaje. Después del período de preparación, verifique que la regla C2 esté habilitada en las Reglas de incidentes y monitoree para ver si la regla se activa.
6. **Verificar que las reglas de incidentes estén configuradas correctamente**. Cuando observa incidentes en la vista Respond, es útil si estos se agrupan por Sospecha de C&C.

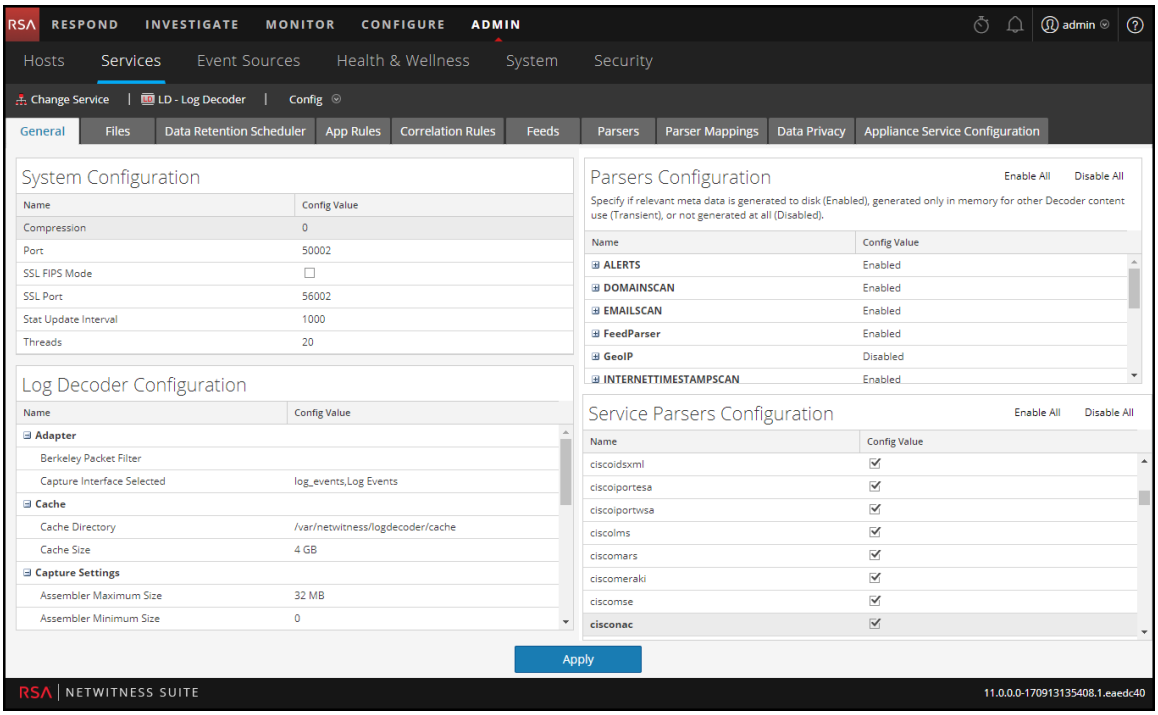
Paso 1: (Solo para registros) Configurar ajustes de registro

Para configurar Detección de amenazas automatizadas para registros, debe realizar algunos pasos de configuración adicionales:

- Verifique que los analizadores compatibles estén habilitados para el Log Decoder.
- Obtenga las versiones más recientes del analizador de proxy web correspondiente en RSA Live.
- Actualice el mapeo en el archivo de configuración de Envision. Este archivo se requiere para actualizar el Log Decoder de modo que funcione con los metadatos nuevos disponibles a través de los analizadores.
- Verifique que el archivo table-map.xml se haya actualizado correctamente.
- Verifique que los índices se hayan actualizado correctamente.

Para verificar que los analizadores estén en ejecución en el Log Decoder:

1. Vaya a **ADMIN** > **Servicios**.
2. Seleccione el Log Decoder y elija  **> Ver > Configuración**.
   La sección Configuración de analizadores de servicio muestra una lista de los analizadores habilitados.
3. Verifique que el analizador de proxy web adecuado esté habilitado.

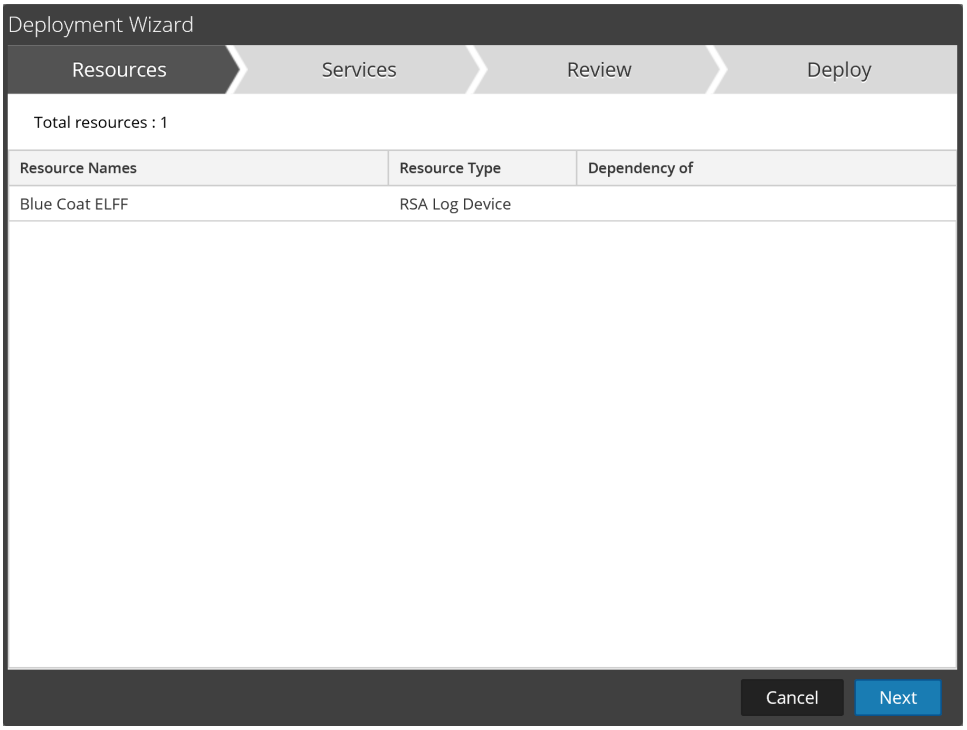


Para obtener los analizadores más recientes desde RSA Live:

1. Vaya a **CONFIGURAR** > **Live Content**.
2. Ingrese un término de búsqueda para uno de los analizadores de proxy web compatibles.
3. Seleccione el analizador de proxy web adecuado (por ejemplo, el analizador Blue Coat ELFF [cacheflowelff]).

> **Nota:** Debe haber realizado los pasos de configuración del registro para que este se realice correctamente en el analizador de proxy web.

4. Haga clic en **Implementar**.
   Se abre el Asistente de implementación.

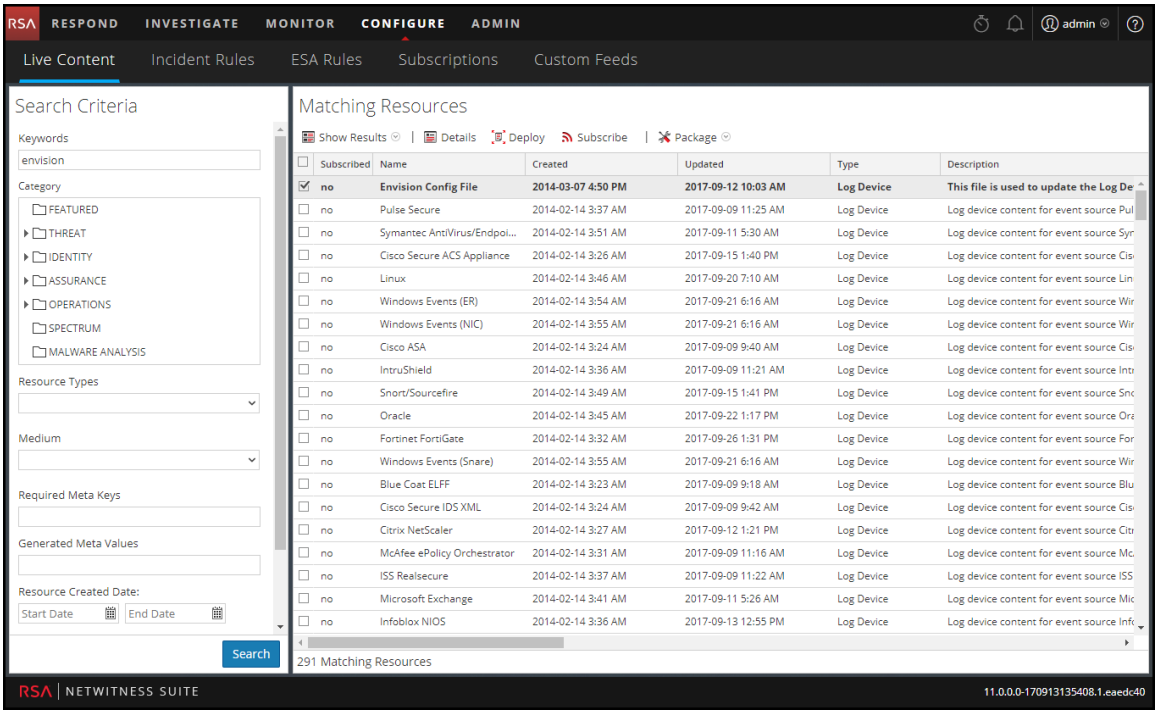


5. En **Servicios**, seleccione el Log Decoder como el servicio.
6. Haga clic en **Implementar** para implementar el analizador en el Log Decoder.

Para obtener el archivo de configuración de Envision más reciente:

1. Vaya a **CONFIGURAR** > **Live Content**.
2. Ingrese **envision** como la palabra clave para la búsqueda.

3. Seleccione el archivo de configuración de Envision más reciente y haga clic en **Implementar**.



4. En el Asistente de implementación, bajo **Servicios**, seleccione el Log Decoder.
5. Haga clic en **Implementar** para implementar el archivo de configuración de Envision en el Log Decoder.

Para verificar que el archivo de configuración de Envision se haya actualizado correctamente:

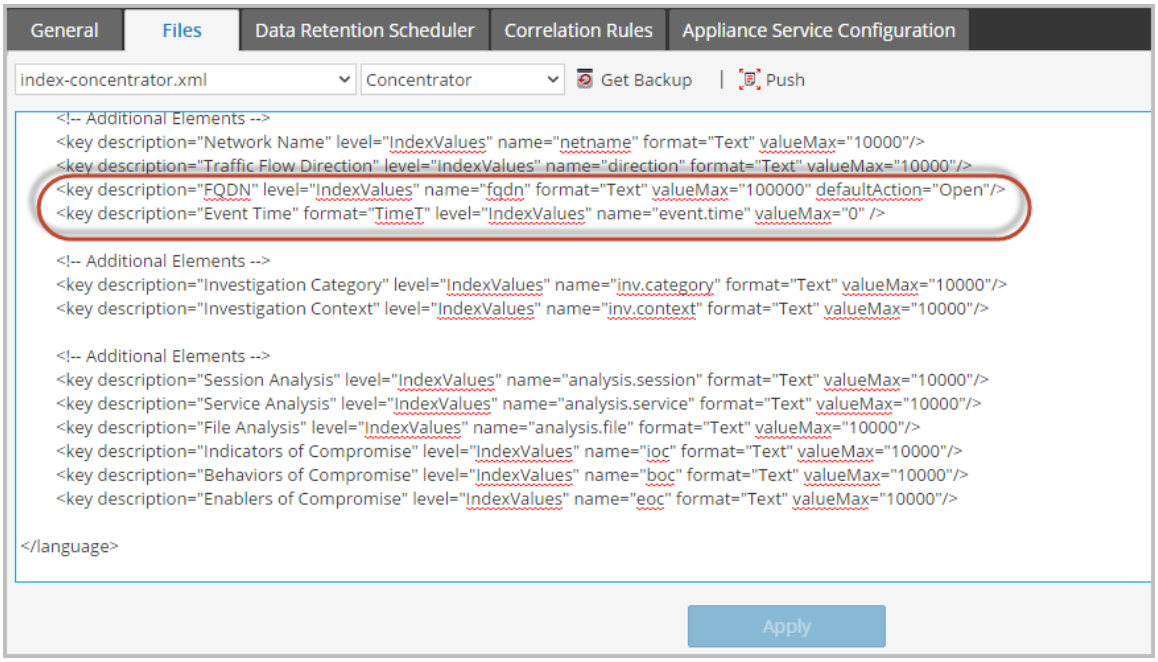
1. Vaya a **ADMIN > Servicios**, seleccione el Log Decoder y, a continuación, elija  > **Ver > Configuración > pestaña Archivos**.
   Puede ver el archivo **table-map.xml**. Este archivo se modifica cuando usted actualiza el archivo de configuración de Envision.
2. Busque el término *event.time*. Ahora, el campo debe indicar *"event.time" flags ="None"*. Esto significa que ahora los metadatos event.time se incluyen en el mapeo. De manera similar, la marca fqdn se debe configurar en “None”.

Para verificar que los índices para el archivo index-concentrator.xml se hayan actualizado:

Debe verificar que el archivo **index-concentrator.xml** incluya los metadatos event.time y fqdn.

1. Vaya a **ADMIN** > **Servicios**, seleccione el Concentrator y, a continuación, elija > **Ver** > **Configuración**.
2. En la pestaña Archivos, busque el archivo **index-concentrator.xm**.
3. Verifique que exista la siguiente entrada en el archivo index-concentrator.xml. Si no es así, debe asegurarse de actualizar el Concentrator a la versión correcta:

```
<key description="FQDN" level="IndexValues" name="fqdn" format="Text"
valueMax="100000" defaultAction="Open"/><key description="Event Time"
format="TimeT" level="IndexValues" name="event.time" valueMax="0" />
```



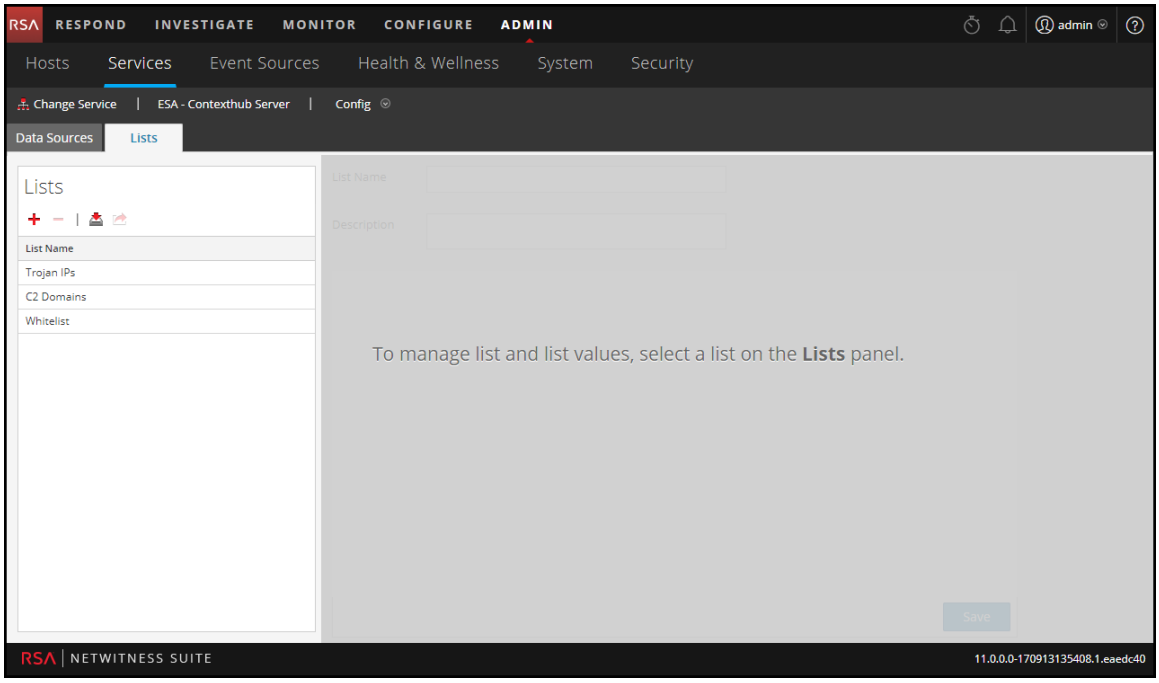
Paso 2: Crear una lista blanca de dominios (opcional)

Este procedimiento se utiliza cuando se trabaja con Detección de amenazas automatizadas a fin de garantizar que determinados dominios no activen un puntaje de amenazas. En ocasiones, un dominio al que se accede habitualmente puede activar un puntaje de Detección de amenazas automatizadas. Por ejemplo, un servicio de clima podría tener un comportamiento de Beacon similar a una comunicación de comando y control, y podría activar un puntaje negativo no justificado. Cuando esto sucede, se denomina un falso positivo. Para impedir la activación de un falso positivo con un dominio específico, puede agregar el dominio a una lista blanca. La mayoría de los dominios no necesita estar en una lista blanca, porque la solución solo alerta sobre comportamientos muy sospechosos. Los dominios que tal vez desee incluir en la lista blanca son servicios automatizados válidos que no tienen muchas conexiones de host.

Nota: Para las migraciones desde la versión 10.6.x, si su lista de blanca de Detección de amenazas automatizadas anterior (Dominios en lista blanca) aparece en la pestaña Listas, puede cambiar su nombre a **domains_whitelist** para usarla con los módulos Suspicious Domains.

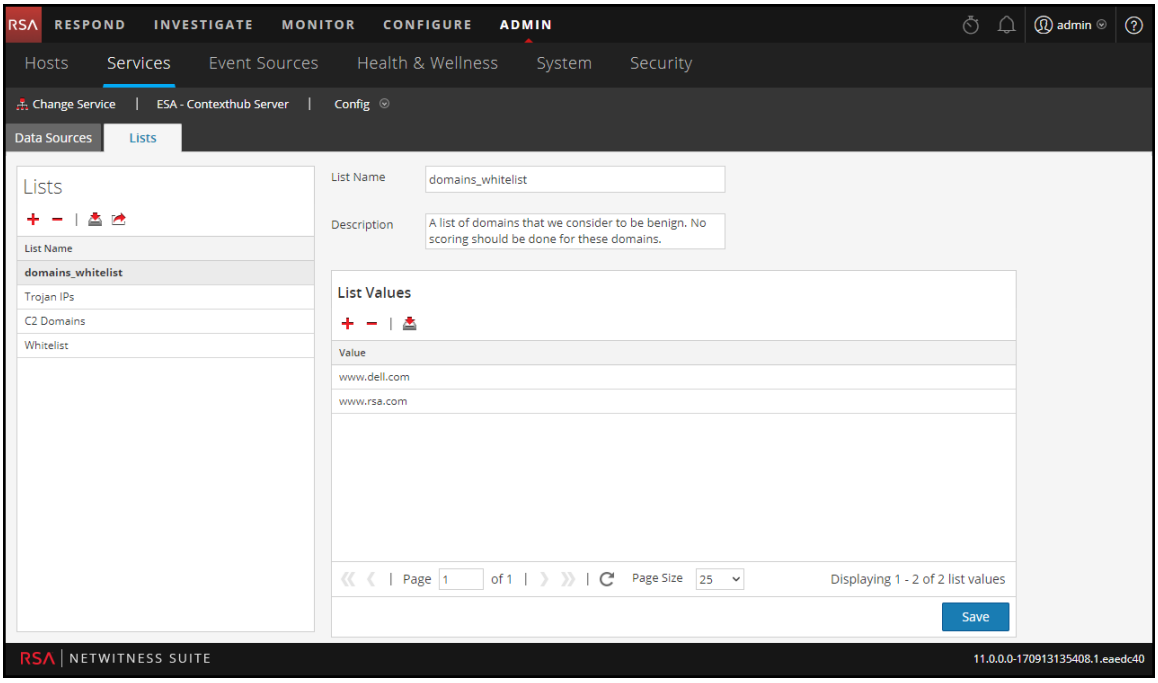
1. Cree una lista blanca de dominios en Context Hub con el nombre **`domains_whitelist:`**

   a. Vaya a **ADMIN > Servicios**, seleccione el servicio Servidor de Context Hub y, a continuación, seleccione la pestaña **Ver > Configuración > Listas**.
   La pestaña Listas muestra las listas actuales en Context Hub.



   b. En el panel Listas, haga clic en + para agregar una lista. En el campo **Nombre de lista**, escriba **`domains_whitelist`**. Debe usar este nombre para que el módulo lo

reconozca.



2. Agregue dominios manualmente a la lista o importe un archivo .CSV que contenga una lista de dominios.
   Puede ingresar dominios completos o puede utilizar un comodín para incluir todos los subdominios de un dominio determinado. Por ejemplo, puede ingresar *.gov para incluir todas las direcciones IP del Gobierno en la lista blanca. Sin embargo, no puede usar otras funciones de regex, como [a-z]*.gov. Esto se debe a que el uso de *.gov reemplaza una cadena completa, por ejemplo, www.irs.gov.

   a. Para agregar dominios manualmente, en la sección **Valores de lista**, haga clic en + .

   b. Para eliminar un dominio, selecciónelo y haga clic en − .

   c. Para importar un archivo .CSV, en la sección **Valores de lista**, haga clic en y, en el cuadro de diálogo **Importar valores de lista**, navegue al archivo .CSV. Seleccione uno de los siguientes delimitadores: Coma, LF (salto de línea) y CR (retorno de carro), según cómo separa los valores en el archivo. Haga clic en **Cargar**.

3. Haga clic en **Guardar**.
   domains_whitelist aparece en el panel Listas. Los analistas pueden agregar elementos a esta lista desde la vista Respond y desde otras partes de Investigation. En la *Guía de configuración de Context Hub* se proporciona información adicional.

Paso 3: Configurar el servicio Búsqueda de Whois

Consulte el tema "Configurar el servicio Búsqueda de Whois" en la *Guía de configuración de ESA*.

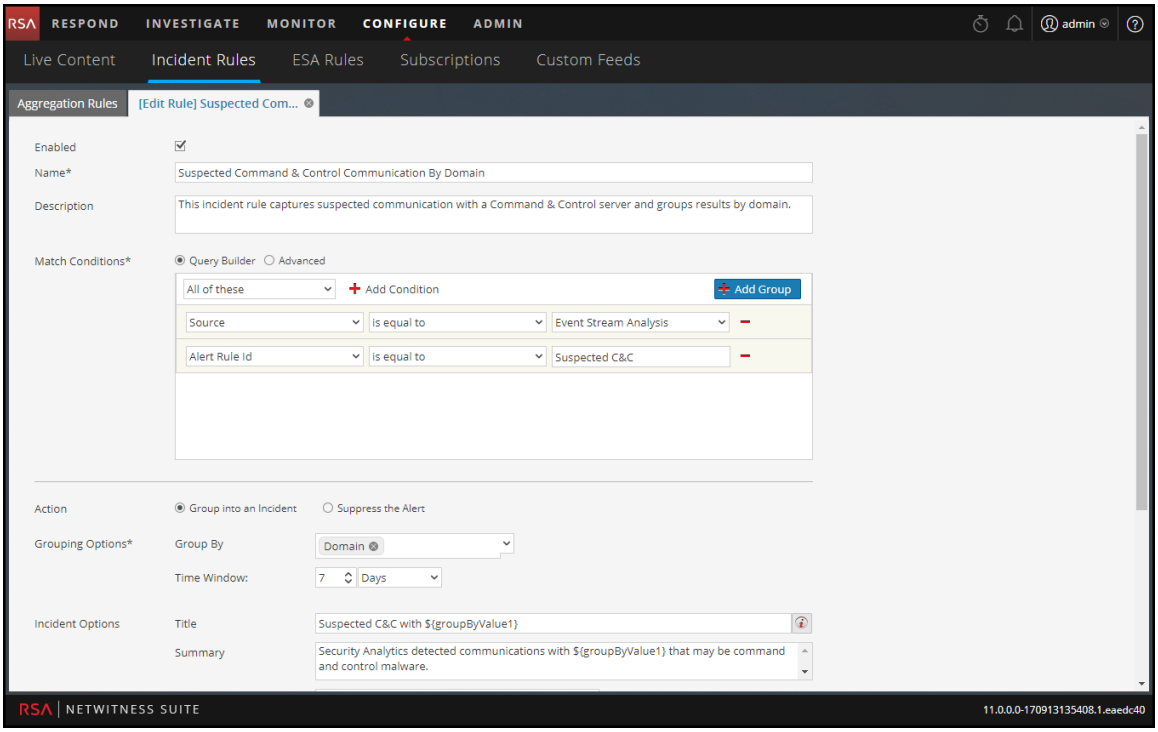
Paso 4: Mapear orígenes de datos a los módulos ESA Analytics

Consulte el tema "Mapeo de orígenes de datos de ESA a módulos Analytics" de la *Guía de configuración de ESA*.

Paso 5: Verificar que la regla Sospecha de comando y control por dominio esté habilitada y monitorear la regla

Verifique la regla Sospecha de comando y control por dominio en las Reglas de incidentes.

1. Vaya a **CONFIGURAR** > **Reglas de incidentes** > **Reglas de agregación**.
2. Seleccione la regla **Comunicación de comando y control sospechosa por dominio** y haga doble clic en ella para abrirla.



3. Verifique que la opción **Habilitado** esté seleccionada.

La regla muestra un botón Habilitado en verde una vez que se habilita.

Resultado

Después de la implementación del mapeo del módulo Suspicous Domains de ESA Analytics para Detección de amenazas automatizadas, ESA comenzará a ejecutar analítica en el tráfico HTTP. Puede ver información detallada de cada incidente en la vista Respond.

Paso 6: Verificar que el incidente se agrupe por Sospecha de C&C

Para agrupar los incidentes correctamente en la vista Respond, configure la condición Agrupar por en Dominio.

1. Vaya a **CONFIGURAR** > **Reglas de incidentes** > **Reglas de agregación**.
2. Seleccione la regla **Comunicación de comando y control sospechosa por dominio** y haga doble clic en ella para abrirla.
3. Verifique que el campo **Agrupar por** esté configurado en *Dominio*.

   Esto agregará alertas y se crearán incidentes para “Sospecha de C&C”.

Próximos pasos

Monitoree la vista Respond para ver si la regla se activa. En la *Guía del usuario de NetWitness Respond* se proporciona información adicional.

Solución de problemas de Detección de amenazas automatizadas de NetWitness Suite

Detección de amenazas automatizadas de NetWitness Suite es un motor de analítica que examina los datos de HTTP. También utiliza otros componentes, como los servicios Whois y Context Hub, los cuales pueden agregar complejidad a la instalación. En este tema se proporcionan sugerencias para ayudarlo a detectar problemas si la implementación de Detección de amenazas automatizadas no proporciona los resultados previstos.

Posibles problemas

Problema	Causas posibles	Soluciones
Veo demasiadas alertas (falsos positivos).	Varias	Una causa posible es que el servicio Búsqueda de Whois presenta fallas o no está configurado. La búsqueda de Whois es útil para determinar si una URL es válida y, si la conexión falla o no está configurada correctamente, puede generar falsos positivos. Consulte el tema "Configurar el servicio Búsqueda de Whois" en la *Guía de configuración de ESA*.
		Puede ser necesario ingresar direcciones URL en la lista blanca. En ocasiones, el comportamiento legítimo de una URL activa una alerta. Una manera de evitarlo es agregar la URL a la lista blanca. Consulte el tema "Agregar una entidad a una lista blanca" de la *Guía del usuario* de *NetWitness Respond*.

Problema	Causas posibles	Soluciones
No se ven las alertas.	El host de ESA requiere un período de “preparación” cuando se implementa un mapeo del módulo ESA Analytics para Detección de amenazas automatizadas.	Cuando implementa un mapeo del módulo ESA Analytics para Detección de amenazas automatizadas, hay un período de “preparación” durante el cual no se ven alertas. Cada tipo de módulo tiene un período de preparación predeterminado y usted debe esperar hasta que este período se complete. Para obtener más información, consulte el tema “Mapeo de orígenes de datos de ESA a módulos Analytics” de la *Guía de configuración de ESA*.
Veo problemas de rendimiento (más uso de recursos o una caída de rendimiento).	Varias	Si tiene problemas de rendimiento en un host de ESA que está ejecutando Detección de amenazas automatizadas (ESA Analytics) y reglas de ESA, siga los pasos de solución de problemas correspondientes a las reglas. Para obtener estos pasos de solución de problemas, vaya a “Solucionar problemas de ESA” en la *Guía de alertas mediante ESA*.