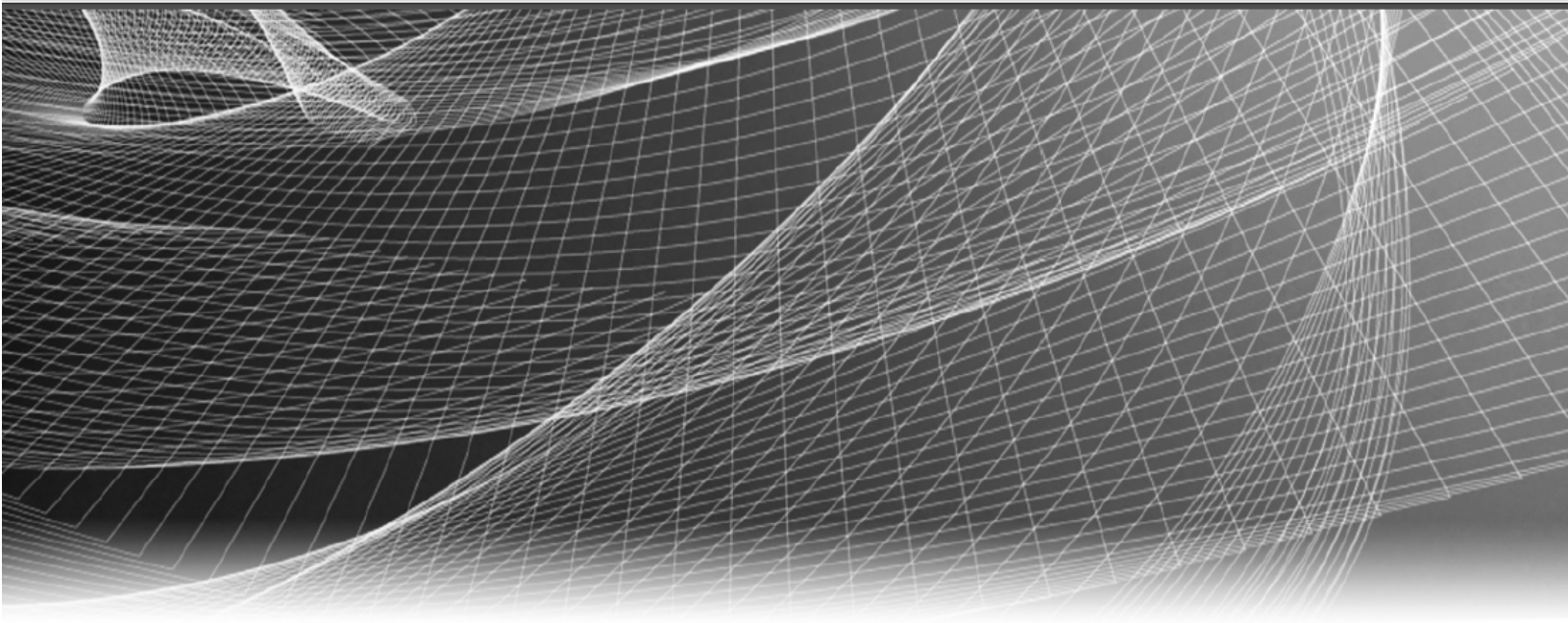


RSA Security Analytics

Guía de introducción de Security Analytics

para la versión 10.6

RSA EMC²

Marcas comerciales

Acuerdo de licencia

Licencias de otros fabricantes

Nota sobre tecnologías de cifrado

Distribución

Contenido

Presentación de Security Analytics

RSA Security Analytics es un sistema distribuido y modular que permite el uso de arquitecturas de implementación altamente flexibles que escalan con las necesidades de la organización. Security Analytics permite que los administradores recopilen dos tipos de datos desde la infraestructura de la red, los datos de paquetes y los datos del registro. Los aspectos clave de la arquitectura son:

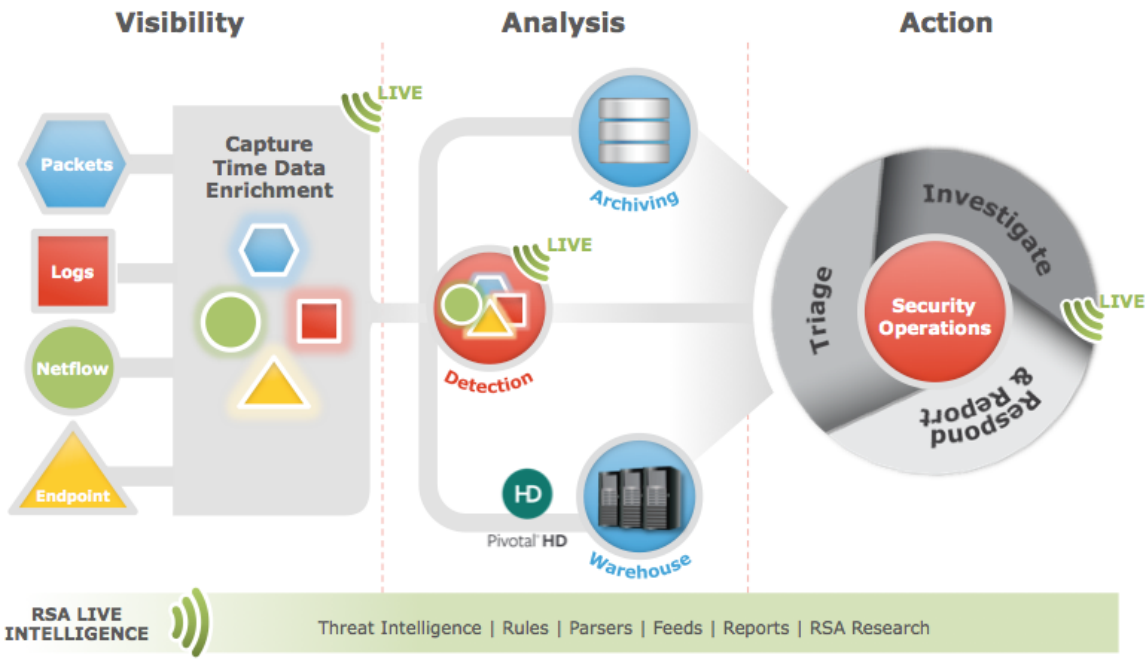
- **Recopilación de datos distribuidos**. Los datos de paquetes se recopilan con un dispositivo denominado **Decoder**, mientras que **Log Decoder** recopila eventos de registros. Decoder captura, analiza y reconstruye todo el tráfico de red de las capas 2 a la 7 o los datos de registros y eventos de cientos de dispositivos y orígenes de eventos. **Concentrator** indexa metadatos extraídos de los datos de red o de registros y los pone a disposición para la analítica en tiempo real y la creación de consultas de toda la empresa, a la vez que facilita la creación de informes y alertas. **Broker** agrega datos que capturan otros dispositivos y orígenes de eventos. Los Brokers agregan datos de Concentrators configurados; los Concentrators agregan datos de Decoders. Por lo tanto, un Broker conecta las distintas áreas de almacenamiento de datos en tiempo real ubicadas en varios pares de Decoder/Concentrator a lo largo de la infraestructura.
- **Analítica en tiempo real**. El host de Security Analytics **Event Stream Analysis (ESA)** proporciona analítica de flujo avanzada, como correlación y procesamiento de eventos complejos, a alto rendimiento y baja latencia. Puede procesar grandes volúmenes de datos de eventos dispares que provienen de Concentrators. ESA utiliza un lenguaje de procesamiento de eventos avanzado que permite a los analistas expresar filtrado, agregación, combinaciones, reconocimiento de patrones y correlación en múltiples flujos de eventos dispares. Event Stream Analysis ayuda a realizar detección de incidentes y alertas eficaces.

  RSA Analytics Warehouse. Un sistema de cómputo distribuido basado en hadoop, que recopila, administra y permite la analítica y la creación de informes sobre conjuntos de datos de seguridad a largo plazo, por ejemplo, meses o años. Warehouse puede estar conformado por tres o más nodos según los requisitos de analítica, archiving y resistencia de la organización.

  Servidor de Security Analytics. Aloja Reporting, Investigation, Administration y otros aspectos de la interfaz del usuario. También permite la creación de informes sobre datos que se encuentran en el dispositivo Warehouse.
- **Capacidad**. Security Analytics cuenta con una arquitectura de capacidad modular, habilitada para capacidad de conexión directa (DAC) o redes de almacenamiento SAN, que se adapta a

las necesidades de investigación a corto plazo y de retención de datos y analítica a más largo plazo de la organización.

Security Analytics ofrece gran flexibilidad de implementación. En el diseño de su arquitectura, puede usar varias docenas de hosts físicos o un único host físico en función de los detalles específicos de los requisitos de rendimiento y seguridad del cliente. Además, todo el sistema Security Analytics se ha optimizado para su ejecución en infraestructuras virtualizadas. En la siguiente imagen se ilustra la arquitectura funcional de Security Analytics:



La arquitectura del sistema incluye estos componentes principales: Decoders, Brokers y Concentrators, Archivers, ESA, Warehouse Connectors y RSA Warehouse. Los componentes de Security Analytics se pueden usar en conjunto como un sistema o de manera individual.

- En una implementación de información de seguridad y administración de eventos (SIEM), la configuración básica requiere estos componentes: Log Decoder, Concentrator, Broker, Event Stream Analysis (ESA) y el servidor de Security Analytics.
- En una implementación de análisis forense, la configuración básica requiere estos componentes: Decoder, Concentrator, Broker, ESA y Malware Analysis. Un componente opcional es el servicio Incident Management, el cual reside en el sistema ESA y se usa para dar prioridad a las alertas.

La tabla proporciona una sinopsis de cada componente principal:

Componente del sistema	Descripción
Decoder/Log Decoder	• Security Analytics recopila dos tipos de datos: datos de paquetes y datos del registro. • Los datos de paquetes, es decir, paquetes de red, se recopilan mediante Decoder a través del puerto TAP o SPAN de la red, el cual normalmente se determina que es un punto de salida en la red de una organización. • Un Log Decoder puede recopilar cuatro tipos de registro diferentes: syslog, ODBC, eventos de Windows y archivos planos. • Eventos de Windows se refiere a la metodología de recopilación de Windows 2008 y los archivos planos puede obtenerse a través de SFTP. • Ambos tipos de Decoders recopilan datos transaccionales crudos que se enriquecen, cierran y agregan a Warehouse o a otros componentes de Security Analytics. • El proceso de recopilación y análisis de datos transaccionales es una plataforma dinámica y abierta.
Concentrator/Broker	• Cualquier dato que se puede indexar en el Decoder pasa por el filtro del Concentrator respectivo. • Una vez que los datos se almacenan en el Concentrator, se transmiten en forma de metadatos a RSA Analytics Warehouse.
Archivers	• Archiver es un host que permite el archiving de registros a largo plazo mediante la indexación y la compresión de datos del registro y su envío a almacenamiento de archiving. • El almacenamiento de archiving se optimiza para la retención de datos a largo plazo y los informes de cumplimiento de normas. • Archiver almacena registros crudos y metadatos de registros de Log Decoders para la retención a largo plazo y utiliza capacidad de conexión directa (DAC) para el almacenamiento. **Nota:** Los paquetes crudos y los metadatos de paquetes no se almacenan en el Archiver.

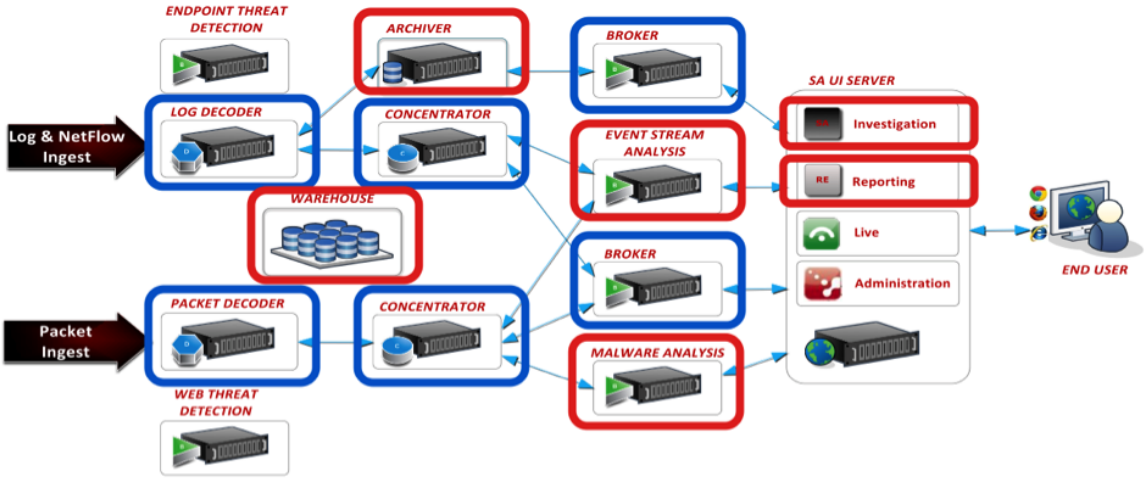
Componente del sistema	Descripción
Event Stream Analysis (ESA)	• Este host de ESA proporciona analítica de flujo de eventos, como correlación y procesamiento de eventos complejos, a alto rendimiento y baja latencia. Puede procesar grandes volúmenes de datos de eventos dispares que provienen de Concentrators. • ESA utiliza un lenguaje de procesamiento de eventos avanzado que permite a los usuarios expresar filtrado, agregación, combinaciones, reconocimiento de patrones y correlación en múltiples flujos de eventos dispares. • ESA ayuda a ejecutar detección de incidentes y alertas eficaces.
Warehouse Connectors	• Warehouse Connector permite recopilar metadatos y eventos de Decoders y escribirlos en formato Avro en un sistema de procesamiento distribuido basado en Hadoop. • Puede configurar Warehouse Connector como un servicio en Log Decoders o Decoders existentes o se puede ejecutar como un host virtual en el ambiente virtual. • Warehouse Connector tiene los siguientes componentes: origen de datos, destino y flujo de datos.

Componente del sistema	Descripción
RSA Analytics Warehouse	• RSA Analytics Warehouse proporciona la funcionalidad de archiving de datos a más largo plazo a través de un sistema de procesamiento distribuido basado en Hadoop que recopila, administra y permite la analítica y la creación de informes de datos de seguridad. • RSA Analytics Warehouse requiere un servicio denominado Warehouse Connector para recopilar metadatos y eventos de Decoder y Log Decoder, y escribirlos en formato Avro en un sistema de procesamiento distribuido basado en Hadoop. • Cualquier dato entrante en Log Decoder y Concentrator se reenvía finalmente a Warehouse. • Generalmente un Warehouse se compone de dos unidades: nodos de almacenamiento y capacidad de conexión directa (DAC). • Los datos completos (no solo los metadatos) se almacenan en RSA Analytics Warehouse y están disponibles para Security Analytics cuando es necesario.

Componentes principales frente a descendentes

En Security Analytics, los servicios Core recopilan y analizan datos, generan metadatos y agregan los metadatos generados con los datos crudos. En la siguiente figura, los servicios Core se resaltan en azul; estos son Decoder, Log Decoder, Concentrator y Broker. Los sistemas descendentes usan los datos almacenados en los servicios Core para analítica. Por lo tanto, las operaciones de los servicios descendentes dependen de los servicios de Security Analytics Core. Los sistemas descendentes se resaltan en rojo; estos son Archiver, Warehouse, ESA, Malware Analysis, Investigation y Reporting.

Aunque los servicios de Security Analytics Core pueden funcionar y proporcionar una buena solución de analítica sin los sistemas descendentes, los componentes descendentes ofrecen funciones de analítica adicionales. ESA proporciona correlación en tiempo real entre sesiones y eventos, y también entre distintos tipos de eventos, como datos de paquetes y registros. Investigation brinda la capacidad de desglosar a datos, examinar eventos y archivos, y reconstruir eventos en un ambiente seguro. El servicio de Malware Analysis ofrece inspección automatizada en tiempo real de actividad maliciosa en sesiones de red y archivos asociados.



Interfaz del usuario de Security Analytics

De manera muy general, Security Analytics ejecuta dos funciones:

- Proporciona una interfaz del usuario basada en navegador gráfico para administrar la arquitectura, las configuraciones y los permisos para los servicios de Security Analytics.
- Adquiere los datos de Warehouse, Decoders y Concentrators, realiza análisis y ejecuta alertas e informes.
- Todos los módulos de Security Analytics comparten un enfoque común en la presentación de datos y las opciones de configuración con el uso de diferentes tableros, vistas, cuadrículas y cuadros de diálogo. Esto permite a los usuarios navegar de una forma comprensible, fácil y sin problemas. Después de familiarizarse con la interfaz del usuario, los usuarios pueden mejorar más su productividad mediante la creación de tableros para propósitos específicos. Por ejemplo, un conjunto de tableros personalizados puede presentar información de diferentes regiones o distintos tipos de amenazas.

Módulos de Security Analytics

Security Analytics organiza las tareas administrativas, analíticas y de creación de informes en módulos que representan agrupamientos lógicos de funciones y tareas para servicios:

- El tablero es el punto de entrada para todos los módulos de Security Analytics y ofrece un portal a funciones de otros módulos para comodidad del usuario.
- El módulo Administration es la interfaz del usuario para administrar y monitorear hosts, dispositivos/orígenes de eventos y servicios. Cuando están configurados, los hosts, los

dispositivos/orígenes de eventos y los servicios están disponibles para otros módulos de Security Analytics.

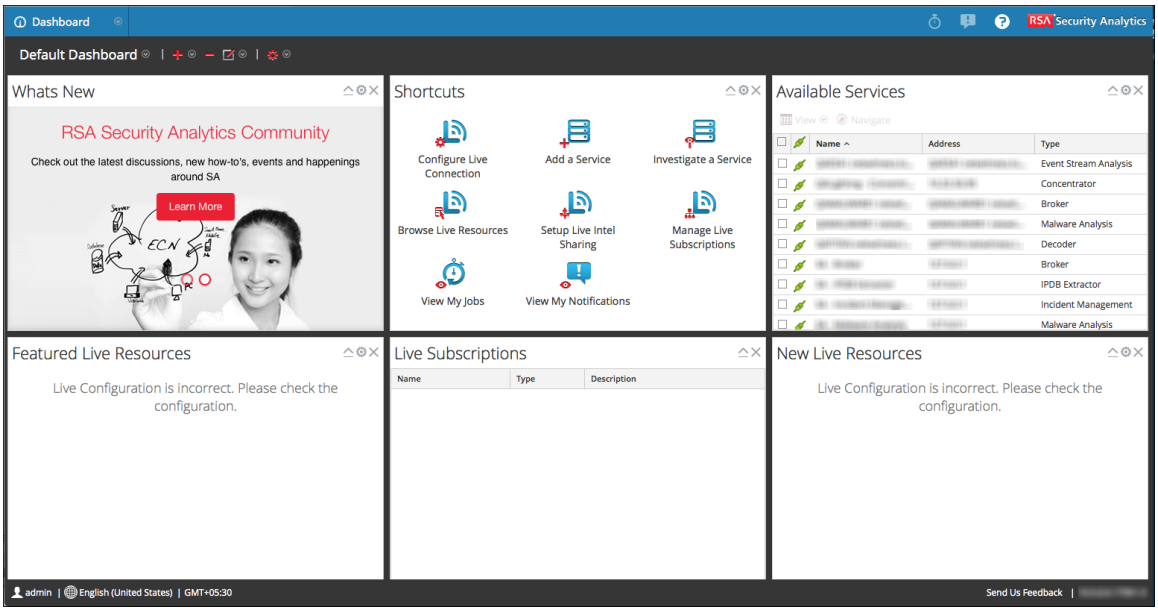
- El módulo Investigation es la interfaz del usuario que permite la visualización de los paquetes que capturan los hosts de Security Analytics. Malware Analysis es la interfaz del usuario para el análisis de malware automatizado.
- El módulo Live es la interfaz del usuario para acceder y administrar los recursos disponibles para los clientes a través del sistema de administración de contenidos de Live.
- Los módulos Informes y Alertas proporcionan la interfaz del usuario para funciones de creación de informes y alertas automatizadas.
- El módulo Incidentes proporciona la función de administración de incidentes en Security Analytics. La función de administración de incidentes es una manera fácil de hacer un seguimiento del proceso de respuesta a incidentes y proporciona las siguientes funcionalidades:
  - Rastree la respuesta ante incidentes de manera coherente.
  - Automatice el proceso de creación de incidentes de seguridad útiles a partir de alertas entrantes.
  - Proporcione contexto de negocios y herramientas de investigación para ayudar al equipo a descubrir las causas raíz.
  - Rastree el proceso de corrección de forma automatizada mediante la integración de un sistema de help desk de otros fabricantes.
  - Rastree la respuesta ante incidentes de manera coherente.
  - Automatice el proceso de creación de incidentes de seguridad útiles a partir de alertas entrantes.
  - Proporcione contexto de negocios y herramientas de investigación para ayudar al equipo a descubrir las causas raíz.
  - Rastree el proceso de corrección de forma automatizada mediante la integración de un sistema de help desk de otros fabricantes.

Elementos comunes en una ventana del navegador

Security Analytics contiene algunos elementos básicos en cada ventana del navegador. Estas funciones se incluyen en todas las vistas de Security Analytics.

Para mostrar esta vista, realice una de las opciones siguientes:

- Inicie sesión en Security Analytics en **https://<SA-IP>**, donde <SA-IP> es la dirección IP del servidor de Security Analytics.
- En el menú de **Security Analytics**, seleccione **Tablero**.



Características

Cada ventana del navegador que accede a Security Analytics incluye estos elementos:

- El menú de Security Analytics
- La barra de herramientas de Security Analytics
- El pie de página

Barra de herramientas de Security Analytics

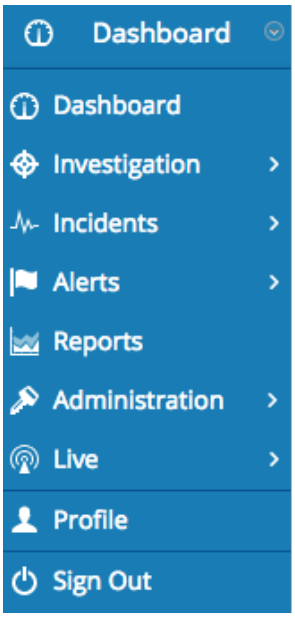
En la parte superior de todos los tableros de Security Analytics, se encuentra la barra de herramientas de Security Analytics. Diferentes módulos tienen distinto contenido según las vistas disponibles. Aquí se presentan dos ejemplos de la barra de herramientas de Security Analytics.

Estas son las funciones de la barra de herramientas de Security Analytics.

Característica	Descripción
Menú de Security Analytics	Contiene opciones para acceder a los módulos, Ayuda, Perfil y Cerrar sesión. Algunos módulos tienen un submenú de vistas.
Opciones de vista de los módulos	Muestra una vista. La opción de la vista que se muestra actualmente aparece resaltada.
Menú de Security Analytics	Muestra el módulo actual como título. Haga clic para abrir un menú desplegable en el cual puede ver un módulo, ver el perfil o cerrar la sesión de Security Analytics.
Botón Trabajos 	Muestra la Bandeja de trabajos, que ofrece información sobre los trabajos de un usuario.
Botón Notificaciones 	Muestra la Bandeja de notificaciones, que ofrece información sobre las notificaciones de un usuario.
Botón Ayuda 	Muestra la ayuda en línea de Security Analytics.

Menú de Security Analytics

El menú de Security Analytics se encuentra en el lado izquierdo de la barra de herramientas de Security Analytics.



Estas son las opciones del menú de Security Analytics.

Opción de menú	Descripción
Tablero	Muestra el tablero de Security Analytics.
Investigation	Muestra el módulo Investigation con la vista Navegar abierta. El submenú tiene una opción que muestra la vista Navegar, la vista Eventos y la vista Malware Analysis.
Incidentes	Muestra el módulo Incident Management. El submenú tiene una opción para mostrar la vista Línea de espera, la vista Alertas, la vista Corrección y la vista Configurar
Alertas	Muestra el módulo Alerts con la vista Configurar abierta. El submenú tiene opciones de acceso directo a las vistas: Resumen y Configurar.
Reports	Muestra el módulo Reports con la vista Informes abierta.
Administración	Muestra el módulo Administration con la vista Servicios abierta. El submenú tiene opciones de acceso directo a las vistas de Administration: Hosts, Servicios, Orígenes de eventos, Estado y condición, Sistema o Seguridad.
En vivo	Muestra el módulo Live con la vista Configurar abierta. El submenú tiene opciones para tener acceso directo a las vistas de Live: Buscar, Configurar y Feeds.
Perfil	Muestra el perfil para configurar preferencias de usuario y ver notificaciones y trabajos.

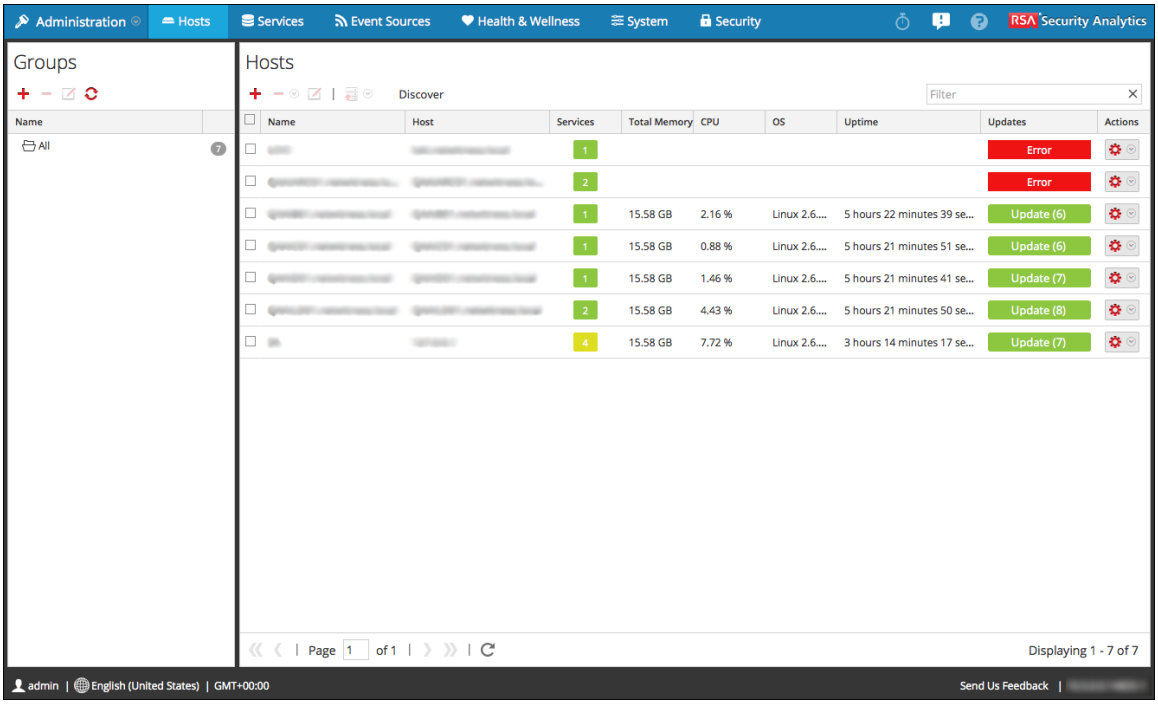
Opción de menú	Descripción
Cerrar sesión	Cierra la sesión de Security Analytics.

Elementos comunes en una vista

Los módulos de Security Analytics que se enumeran en el menú de Security Analytics (Administration, Investigation, Live, Alerts, Reports, etc.) se denominan vistas, y cada vista ofrece funciones adaptadas al módulo. Además, hay una vista Perfil, con acceso directo desde el menú de Security Analytics, que presenta opciones para las preferencias de usuario.

Para mostrar una vista, seleccione un módulo en el menú de **Security Analytics**. Por ejemplo, **Security Analytics, Administration**, **Investigation** o **Live**. A medida que pasa el cursor sobre el módulo, puede seleccionar una vista en el menú de opciones. Desde dentro del módulo, puede seleccionar una vista alternativa en la barra de herramientas de Security Analytics. Por ejemplo, **Administration** tiene seis vistas: **Hosts, Servicios, Orígenes de eventos, Estado y condición, Sistema y Seguridad**.

En este ejemplo de la vista Hosts de Administration se ilustran algunas de las funciones de una vista.



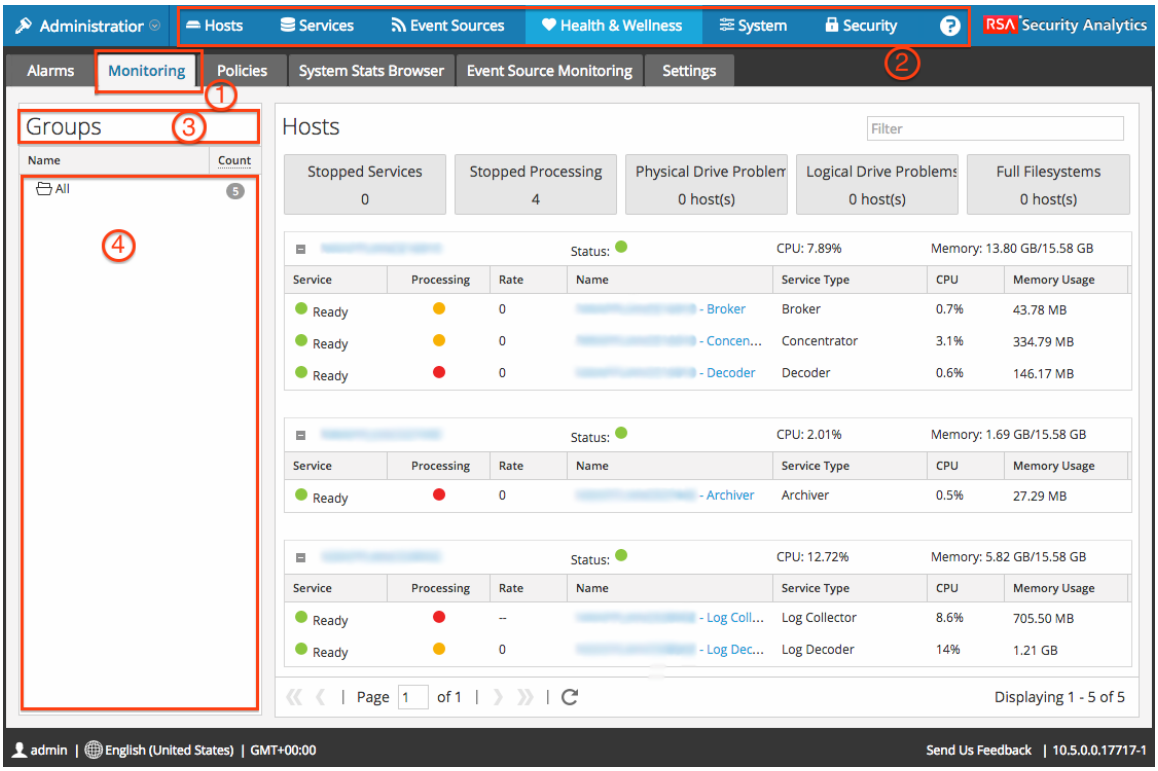
Características

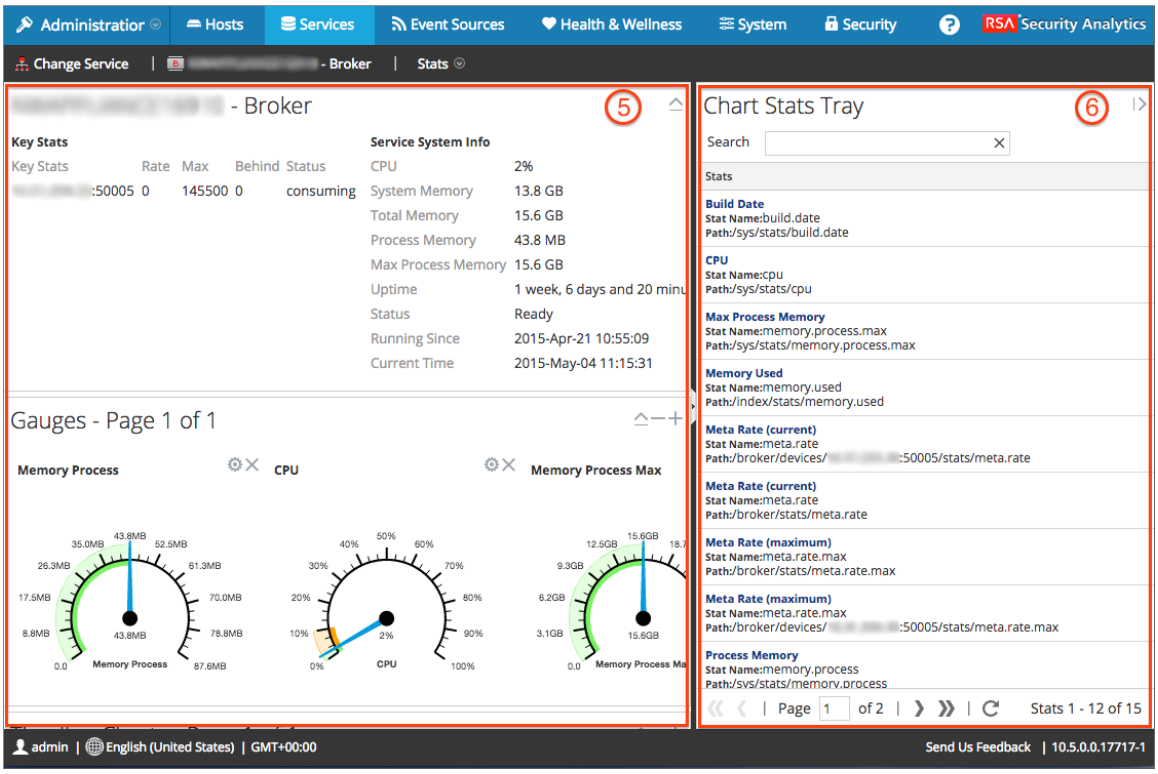
Cada vista tiene funcionalidades diferentes. Cualquier combinación de estas funcionalidades es posible en una vista:

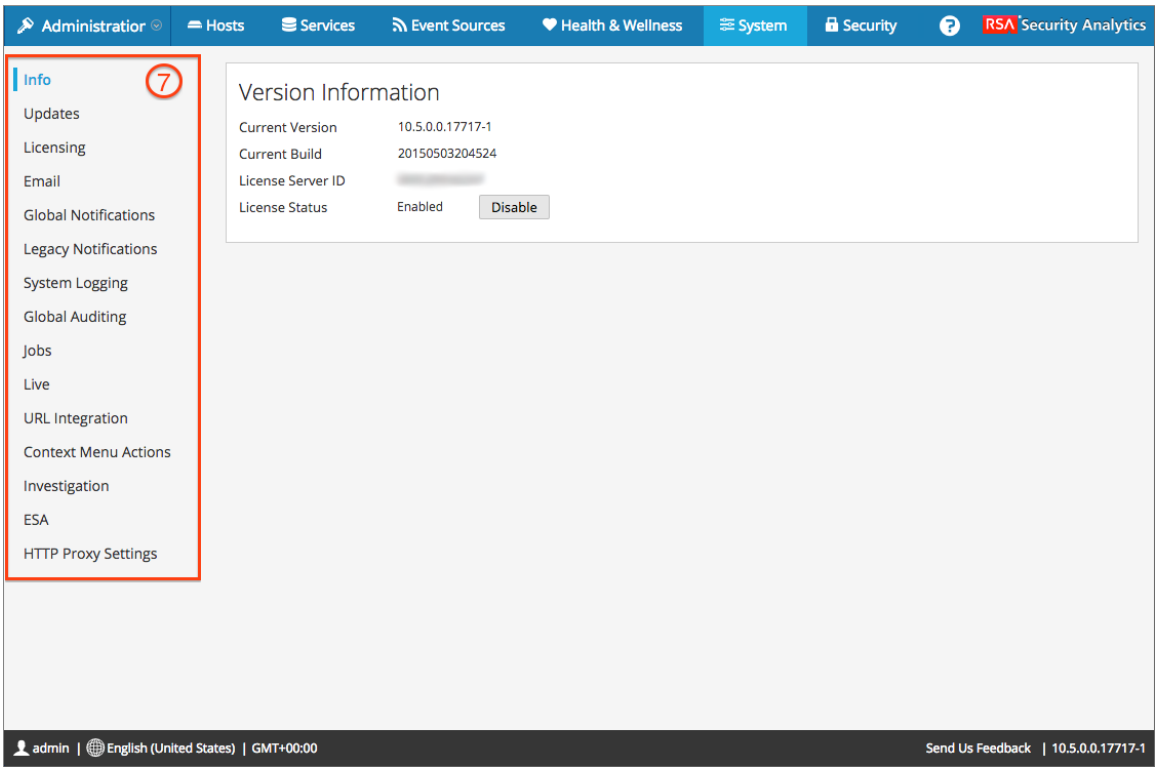
- Barras de herramientas
- Secciones

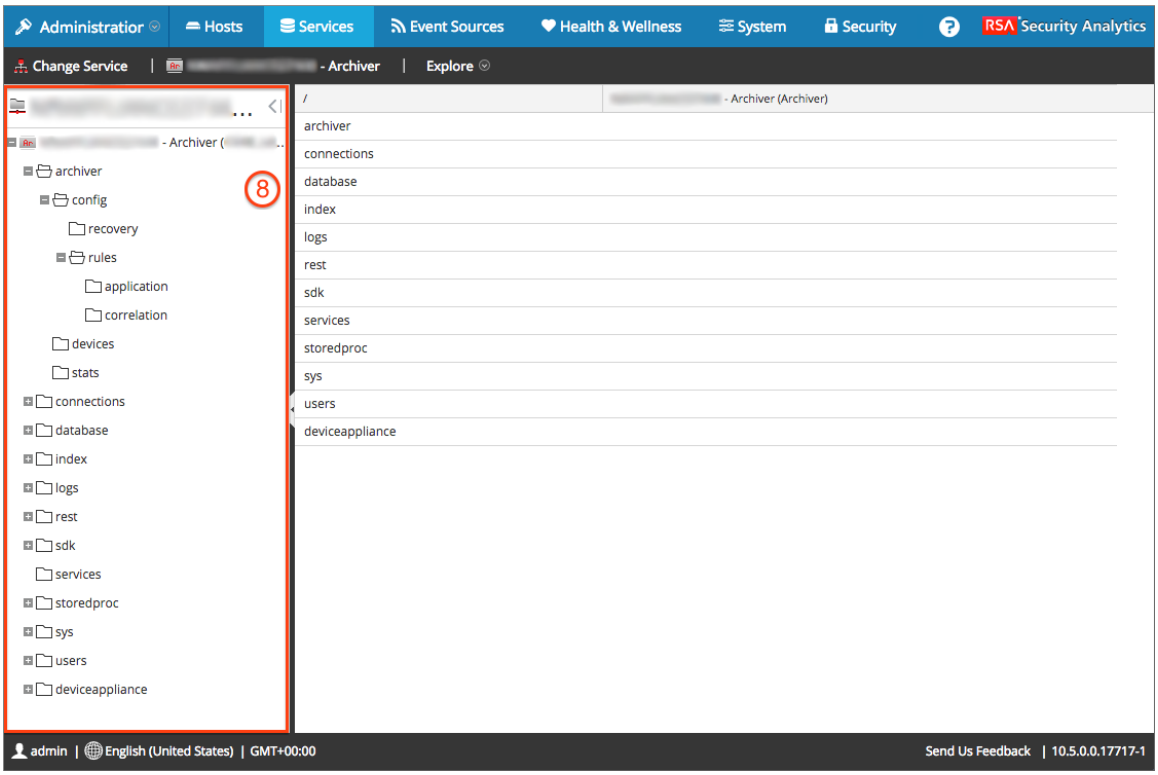
- Paneles: hay dos tipos distintos de paneles especializados, el panel de opciones y el árbol de nodos
- Pestañas
- Rutas de navegación
- Cuadrículas o tablas
- Menús contextuales

En las siguientes figuras se etiquetan las partes generales de una vista.




Administration
Hosts
Services
Event Sources
Health & Wellness
System
Security
RSA Security Analytics
Change Service
- Broker
Stats
- Broker
5
Key Stats
Key Stats Rate Max Behind Status
:50005 0 145500 0 consuming
Service System Info
CPU 2%
System Memory 13.8 GB
Total Memory 15.6 GB
Process Memory 43.8 MB
Max Process Memory 15.6 GB
Uptime 1 week, 6 days and 20 minu
Status Ready
Running Since 2015-Apr-21 10:55:09
Current Time 2015-May-04 11:15:31
Gauges - Page 1 of 1
Memory Process
CPU
Memory Process Max
Chart Stats Tray
6
Search
Stats
Build Date
Stat Name:build.date
Path:/sys/stats/build.date
CPU
Stat Name:cpu
Path:/sys/stats/cpu
Max Process Memory
Stat Name:memory.process.max
Path:/sys/stats/memory.process.max
Memory Used
Stat Name:memory.used
Path:/index/stats/memory.used
Meta Rate (current)
Stat Name:meta.rate
Path:/broker/devices/:50005/stats/meta.rate
Meta Rate (current)
Stat Name:meta.rate
Path:/broker/stats/meta.rate
Meta Rate (maximum)
Stat Name:meta.rate.max
Path:/broker/stats/meta.rate.max
Meta Rate (maximum)
Stat Name:meta.rate.max
Path:/broker/devices/:50005/stats/meta.rate.max
Process Memory
Stat Name:memory.process
Path:/sys/stats/memory.process
Page 1 of 2
Stats 1 - 12 of 15
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.5.0.0.17717-1


Administration
Hosts
Services
Event Sources
Health & Wellness
System
Security
RSA Security Analytics
Info
7
Updates
Licensing
Email
Global Notifications
Legacy Notifications
System Logging
Global Auditing
Jobs
Live
URL Integration
Context Menu Actions
Investigation
ESA
HTTP Proxy Settings
Version Information
Current Version 10.5.0.0.17717-1
Current Build 20150503204524
License Server ID
License Status Enabled Disable
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.5.0.0.17717-1



En la siguiente tabla se proporcionan descripciones de las funciones etiquetadas anteriormente.

Clave	Característica	Descripción
1	pestañas	Organice las funciones de un panel en grupos de fácil visualización y acceso de modo que no tenga que desplazarse hacia abajo en la página para ver todo. Si un panel tiene muchas opciones, las pestañas facilitan la navegación al grupo de opciones correcto en un panel.
2	barra de herramientas	Una barra de herramientas puede aplicarse a toda una vista, a una sección o a un panel.

Clave	Característica	Descripción
3, 4	secciones (de arriba abajo)	En un panel, algunos tableros tienen secciones que organizan información de arriba abajo; por ejemplo, la vista **Información del servicio** tiene dos secciones en el panel **Servicio**, la sección **Servicio** en la parte superior y la sección **Información de sesión** en la parte inferior. Puede que algunas veces deba desplazarse hacia abajo para ver una sección cerca de la parte inferior del panel.
5, 6	paneles (de izquierda a derecha)	En una vista, la mayoría de los tableros tiene paneles que organizan información de izquierda a derecha; por ejemplo, la vista **Estadísticas del servicio** tiene dos paneles, el panel principal a la izquierda y el panel **Bandeja de estadísticas de gráfico** a la derecha. La **Bandeja de estadísticas de gráfico** no es el enfoque principal, de modo que se expande para dejar más espacio en el panel principal.
7	panel de opciones	En el panel de opciones se muestran las opciones disponibles en una vista. A menudo, el panel de opciones no tiene un título. Una lista de selecciones sin un encabezado se denomina opciones.
8	árbol de nodos	Un árbol de nodos es una lista de nodos con carpetas expandibles y contraíbles.

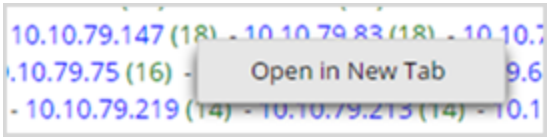
Rutas de navegación

Las rutas de navegación muestran las opciones seleccionadas para llegar a esta vista. Haga clic en una ruta de navegación para volver a la vista o al menú. En algunos módulos, las rutas de navegación tienen funciones adicionales. Por ejemplo, en Investigation, una ruta de navegación representa una secuencia de consultas que se utilizan para llegar al punto de desglose actual y es posible editar la consulta directamente desde la ruta de navegación.

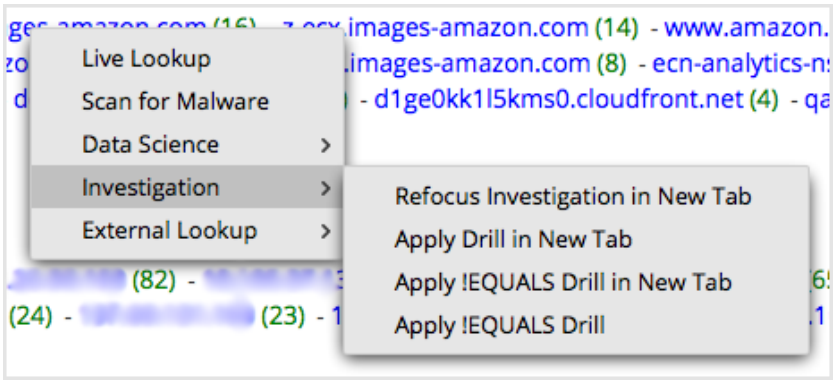
Menús contextuales

Los menús contextuales ofrecen opciones que pertenecen específicamente al contexto actual. En ciertas vistas, al colocar el cursor sobre un elemento y hacer clic con el botón secundario del mouse, se muestran las opciones que pueden aplicarse a ese elemento. En la documentación de Security Analytics, los menús contextuales se analizan en los módulos y las vistas correspondientes.

Un buen ejemplo de un menú contextual se muestra en la vista **Navegación**. Cuando hace clic con el botón secundario en el conteo de un valor de metadatos (el número verde entre paréntesis), el menú ofrece una opción: abrir el desglose en una nueva pestaña.



Si hace clic con el botón secundario en el valor de metadatos (texto azul), se muestra un menú contextual diferente. En este contexto, existen opciones para escanear en busca de malware, buscar el valor en Investigation y ver el mismo desglose en una nueva pestaña, aplicar lo opuesto de este desglose (!EQUALS) en la misma pestaña o aplicar lo opuesto de este desglose en una nueva pestaña.



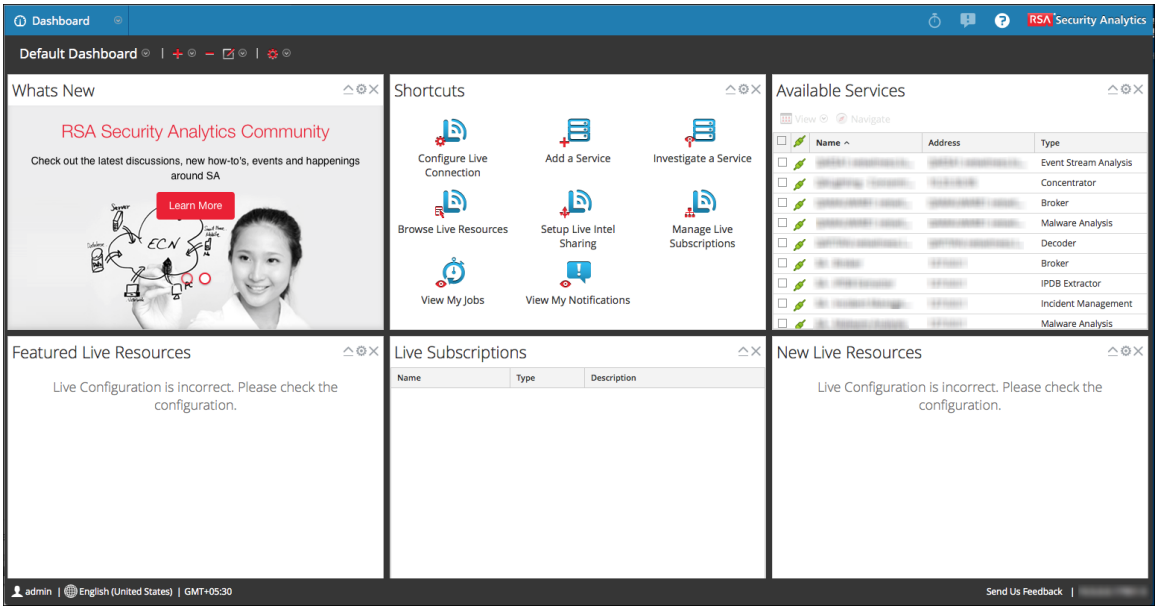
Tableros

Un tablero es un grupo de dashlets que brinda la capacidad de ver en un solo espacio snapshots clave de los diferentes módulos que se consideran importantes. En Security Analytics, puede crear tableros para obtener información general y métricas que retratan todo el panorama de una implementación de Security Analytics, en los cuales se muestra solo la información más pertinente a las operaciones diarias.

De manera predeterminada, el tablero de Security Analytics se muestra cuando inicia sesión en Security Analytics. Incluye algunos dashlets útiles que le permiten comenzar a hacer sus propias personalizaciones. Los dashlets de todos los módulos de Security Analytics se encuentran disponibles para agregarlos al tablero predeterminado o a un tablero personalizado de Security Analytics.

Para ver el tablero de **Security Analytics**, realice una de las siguientes acciones:

- Inicie sesión en Security Analytics. La aplicación se abre en el tablero de Security Analytics.
- En el menú de **Security Analytics**, seleccione **Dashboard**.



El tablero predeterminado

El tablero predeterminado está configurado para mostrar dashlets específicos en posiciones específicas. El tablero predeterminado sirve como ejemplo de la composición de tableros y como punto de inicio para la personalización.

- Para personalizar la información del tablero predeterminado, puede editar, agregar, transferir, maximizar y eliminar dashlets.
- Después de modificar el tablero predeterminado, puede restablecerlo a su diseño original.
- El tablero predeterminado no se puede eliminar

Tableros personalizados

Puede crear tableros personalizados para desempeñar un propósito determinado, por ejemplo, para representar un área geográfica o funcional específica de la red. Cada tablero personalizado se agrega a la lista de selección de tableros.

Después de crear tableros personalizados, puede:

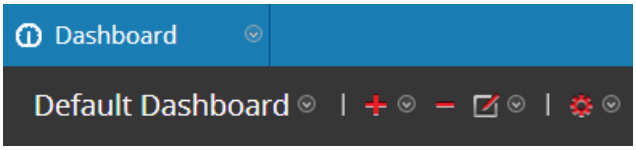
- Cambiar entre tableros mediante la selección de una opción en la lista de selección de tableros
- Eliminar cualquier tablero personalizado
- Importar o exportar un tablero

Cada tablero tiene:

- La barra de herramientas del tablero
- El título del tablero y la lista de selección de tableros
- Ninguno o más dashlets

Barra de herramientas del tablero

Junto al título del tablero actual se encuentra la barra de herramientas del tablero. La barra de herramientas del tablero permite realizar varias operaciones en los tableros y los dashlets.

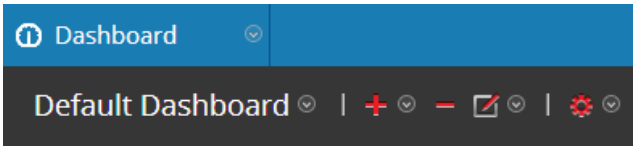


Opción	Descripción
Agregar dashlet	Muestra el cuadro de diálogo Agregar un dashlet, en el cual puede agregar un dashlet al tablero actual.
Eliminar tablero	Elimina un tablero personalizado. El tablero predeterminado no se puede eliminar.

Opción	Descripción
Cambiar diseño del tablero	Muestra el cuadro de diálogo Cambiar diseño del tablero, en el cual puede cambiar el diseño del tablero a una de cinco opciones.
Crear nuevo tablero	Muestra el cuadro de diálogo Crear un tablero, donde puede definir un tablero personalizado.
Cambiar el nombre del tablero	Muestra el cuadro de diálogo Cambiar el nombre del tablero, en el cual puede cambiar el título del tablero.
Restaurar tablero predeterminado	Restaura el tablero predeterminado a su apariencia original, con los dashlets predeterminados en sus posiciones originales.
Exportar tablero	Crear un archivo .cfg que contiene la estructura del tablero actual.
Importar tablero	Agrega un tablero según el archivo .cfg exportado anteriormente.

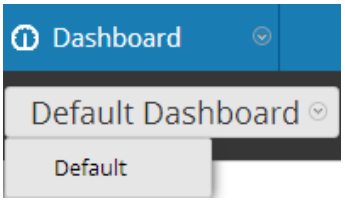
Título de tablero

El título del tablero indica el módulo actual; por ejemplo, Dashboard.



Lista de selección de tableros

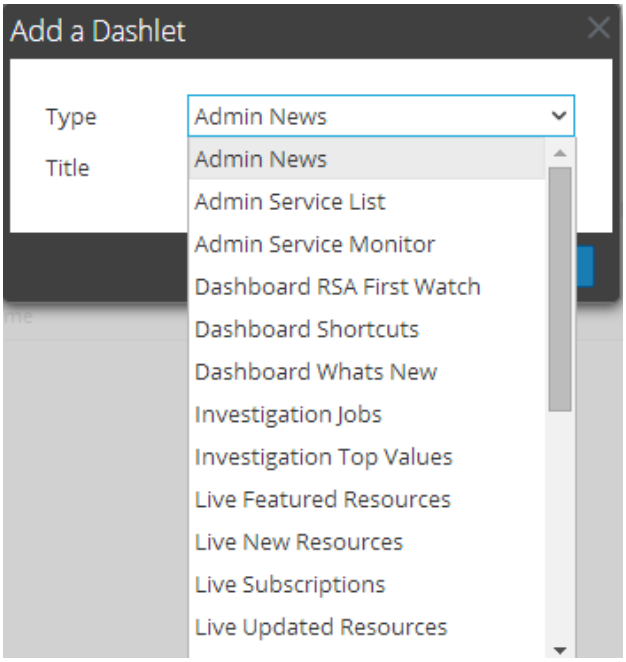
Puede obtener acceso a tableros personalizados en la lista de selección de tableros. Cuando selecciona un tablero personalizado, su título se muestra debajo de la barra de herramientas de Security Analytics.



Dashlets

Security Analytics utiliza dashlets para mostrar subconjuntos centrados de información del sistema, servicios, trabajos, recursos, suscripciones, reglas, actividad de la línea de espera de incidentes, actividad de analistas de incidentes y otra información.

Los módulos de Security Analytics pueden mostrar solo los dashlets que se presentan en el cuadro de diálogo Agregar un dashlet. El tablero principal ofrece todos los dashlets de Security Analytics. Este es un ejemplo de los dashlets actualmente disponibles.



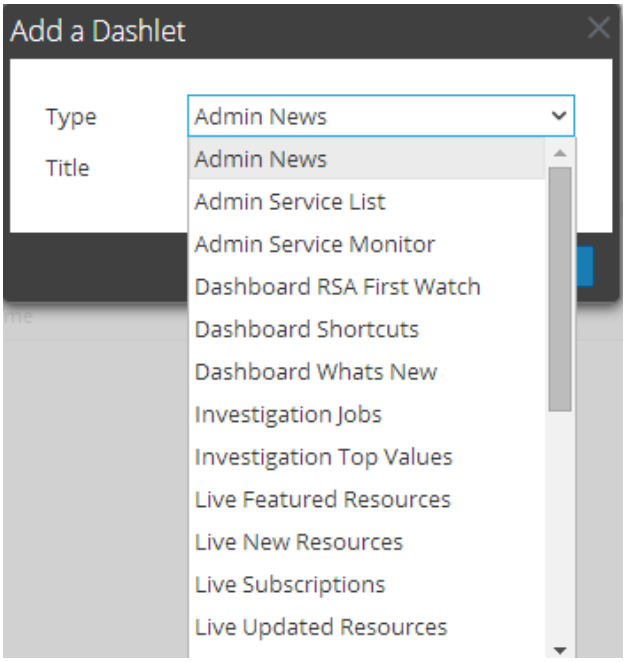
Los controles para un dashlet están en la barra de título. Todos los dashlets utilizan un conjunto de controles común y solo aquellos que se aplican al dashlet específico se muestran en la barra de título.

Ícono	Nombre	Descripción
	Contraer verticalmente	Contrae el dashlet de forma vertical para que solo el título sea visible.
	Expandir verticalmente	Expande el dashlet a su tamaño original.
❯	Avanzar página	En dashlets con más de una página, avanza a la página siguiente.
❮	Retroceder página	En dashlets con más de una página, retrocede a la página anterior.
❯❯	Última página	En dashlets con más de una página, avanza a la última página.

Ícono	Nombre	Descripción
	Primera página	En dashlets con más de una página, retrocede a la primera página.
	Recargar	Vuelve a cargar el dashlet.
	Configuración	Muestra ajustes configurables para el dashlet.
	Maximizar	En algunos dashlets con contenido que no cabe horizontalmente en el ancho del dashlet, maximiza un gráfico o un dashlet a pantalla completa.
	Delete	Elimina el dashlet del tablero.

Dashlets

Los dashlets de todos los módulos de Security Analytics se encuentran disponibles para agregarlos al tablero predeterminado o a un tablero personalizado de Security Analytics. Todos los dashlets tienen en común un conjunto de controles que se describen en Tableros. Este es un ejemplo de algunos de los dashlets actualmente disponibles.



Algunos dashlets tienen parámetros de configuración y controles adicionales; por ejemplo, el dashlet Gráfica en tiempo real de Reports, el dashlet Lista del malware altamente sospechoso principal de Malware y el dashlet Monitor de servicios de Administration. Para obtener más información sobre estos controles adicionales, lea la información relacionada específicamente con ese dashlet.

Terminología

A

Término	Descripción
Módulo Administration	El módulo Administration es la interfaz del usuario para administrar y monitorear dispositivos y servicios. Cuando están configurados, los dispositivos y los servicios están disponibles para otros módulos de Security Analytics.
Alertas	El módulo Security Analytics Alerts es la interfaz del usuario para las funciones automatizadas de alertas.
Datos anonimizados	"Los datos se anonimizan cuando se eliminan todos los elementos de identificación de un conjunto de datos personales. En la información no puede quedar ningún elemento que pudiera, si se hace un esfuerzo razonable, servir para volver a identificar a las personas involucradas. Cuando los datos de anonimizan correctamente, dejan de ser datos personales". (Fuente: EU_DP_LAW_HANDBOOK) Este término se define como parte de la solución de privacidad de datos de Security Analytics.
anonimización	El Privacy Technology Focus Group define la anonimización como una tecnología que convierte datos de texto no cifrado en una forma no legible por humanos e irreversible, incluidos, entre otros, hashes unidireccionales y técnicas de cifrado en las cuales se descartó la clave de descifrado. Este término se define como parte de la solución de privacidad de datos de Security Analytics.
Archiver	RSA Archiver es un dispositivo que permite el archiving de registros a largo plazo mediante la indexación y la compresión de datos del registro y su envío a almacenamiento de archiving.

B

Término	Descripción

Término	Descripción
Broker	RSA Broker es un dispositivo y un servicio en la red de Security Analytics. Los Brokers agregan los datos que capturan los Concentrators configurados, y los Concentrators agregan datos de Decoders. Por lo tanto, un Broker conecta las distintas áreas de almacenamiento de datos en tiempo real ubicadas en varios pares de Decoder/Concentrator a lo largo de la infraestructura.

C

Término	Descripción
capacidad	Security Analytics cuenta con una arquitectura de capacidad modular, habilitada para capacidad de conexión directa (DAC) o redes de almacenamiento SAN, que se adapta a las necesidades de investigación a corto plazo y de retención de datos y analítica a más largo plazo de la organización.
recopilaciones	Las recopilaciones son conjuntos de retención de registros para almacenar datos del registro. Para cada recopilación, puede especificar la cantidad de espacio de almacenamiento total que se usará y los días durante los cuales se conservarán los registros en la recopilación. Las recopilaciones se configuran en Archiver.
Concentrator	RSA Concentrator es un dispositivo y un servicio en la red de Security Analytics. Los Concentrators indexan metadatos extraídos de los datos de red o de registros y los ponen a disposición para la analítica en tiempo real y la creación de consultas de toda la empresa, a la vez que facilitan la creación de informes y alertas.
Base de datos Core	Se refiere a la combinación de datos de paquetes, metadatos, sesiones e índice.
Servicios principales	En Security Analytics, los servicios Core recopilan y analizan datos, generan metadatos y agregan los metadatos generados con los datos crudos. Entre los servicios Core se incluyen Decoder, Log Decoder, Concentrator y Broker.

D

Término	Descripción
tablero	El tablero de Security Analytics es la interfaz del usuario que se muestra en un navegador cuando se inicia sesión en Security Analytics. También se puede mencionar como el tablero en sentido genérico. Por ejemplo: Puede crear tableros personalizados en el tablero de Security Analytics. En el sentido específico, “tablero de Security Analytics” reemplaza a “tablero unificado”.
Decoder	RSA Decoder es un dispositivo y un servicio en la red de Security Analytics. En la red de Security Analytics, los datos de paquetes se recopilan con un dispositivo denominado Decoder, mientras que el Log Decoder recopila eventos de registros. Decoder captura, analiza y reconstruye todo el tráfico de red de las capas 2 a 7 o los datos de registros y eventos de cientos de dispositivos.
sistema y componentes descendentes	En oposición a los componentes principales, los sistemas descendentes usan datos almacenados en servicios Core para analítica. Por lo tanto, las operaciones de los servicios descendentes dependen de los servicios de Security Analytics Core. Los sistemas descendentes son Archiver, Warehouse, ESA, Malware Analysis, Investigation y Reporting.
punto de desglose	Conjunto de datos en los cuales se centró un analista mediante filtros y consultas en la vista Investigation. En efecto, el analista desglosa a los datos capturados para buscar datos interesantes que puedan alojar archivos o código perjudiciales.

E

Término	Descripción
Event Stream Analysis (ESA)	El dispositivo RSA Event Stream Analysis (ESA) proporciona analítica de flujo avanzada, como correlación y procesamiento de eventos complejos, a alto rendimiento y baja latencia. Puede procesar grandes volúmenes de datos de eventos dispares que provienen de Concentrators. ESA utiliza un lenguaje de procesamiento de eventos avanzado que permite a los analistas expresar filtrado, agregación, combinaciones, reconocimiento de patrones y correlación en múltiples flujos de eventos dispares. Event Stream Analysis ayuda a realizar detección de incidentes y alertas eficaces.
EVP	Eventos por segundo es una medida de la capacidad de procesamiento para un host de RSA que consume datos.

F

Término	Descripción
implementación de análisis forense	En una implementación de análisis forense, la configuración básica de Security Analytics requiere estos componentes: Decoder, Concentrator, Broker, ESA y Malware Analysis. Un componente opcional es el servicio Incident Management, el cual reside en el sistema ESA y se usa para dar prioridad a las alertas.

G

Término	Descripción
Registro de auditoría global	El registro de auditoría global proporciona a los auditores de Security Analytics visibilidad consolidada en tiempo real de las actividades de los usuarios dentro de Security Analytics desde una ubicación centralizada. Esta visibilidad incluye registros de auditoría recopilados desde el sistema Security Analytics y desde los distintos servicios de toda la infraestructura de Security Analytics.

H

Término	Descripción
aplicación de hash	Método de ocultamiento que se usa para proteger datos confidenciales.
host	Equipo físico o máquina virtual, que se designa con un nombre de dominio calificado o una dirección IP, en los cuales está instalado cualquier servicio de Security Analytics [es decir, el servidor de Security Analytics y los servicios Appliance, Archiver, Broker, Concentrator, Decoder (Packets y Logs), Hybrid, Malware Analysis, Event Stream Analysis, Log Collector, Security Analytics Warehouse, Workbench, Reporting Engine e IPDB Extractor].

I

Término	Descripción
Término	Descripción
identificabilidad	“Una persona se identifica en esta información; o bien, si en esta información se describe a una persona, aunque no se la identifique, de una manera que permita descubrirla mediante investigación adicional”. (Fuente: EU_DP_LAW_HANDBOOK) Este término se usa cuando se analiza la solución de privacidad de datos de Security Analytics.
Servicio Incident Management	El servicio Incident Management reside en el sistema ESA y se usa para dar prioridad a las alertas.
Módulo Incidentes	El módulo Incidentes proporciona la función de administración de incidentes en Security Analytics. La función de la administración de incidentes ofrece una manera sencilla de rastrear el proceso de respuesta ante incidentes.
index	El índice es una recopilación de archivos que proporciona una forma de buscar ID de sesión con el uso de valores de metadatos.

Término	Descripción
Módulo Investigation	El módulo Investigation es la interfaz del usuario de Security Analytics que permite la visualización y la reconstrucción de paquetes y registros que capturan los dispositivos de Security Analytics.

J

Término	Descripción
sistema de trabajos	El sistema de trabajos de Security Analytics le permite comenzar una tarea de ejecución prolongada y continuar utilizando otras partes de Security Analytics mientras el trabajo está ejecutándose. No solo puede monitorear el progreso de la tarea, sino que también puede recibir notificaciones cuando la tarea haya finalizado y si el resultado fue exitoso o falló. Mientras esté trabajando en Security Analytics, puede abrir una vista rápida de los trabajos desde la barra de herramientas.

L

Término	Descripción
Módulo Live	El módulo Live es la interfaz del usuario de Security Analytics para acceder y administrar los recursos disponibles para los clientes a través del sistema de administración de contenido de Live.
Log Decoder	Un Log Decoder es un tipo de Decoder que recopila registros en lugar de paquetes. Puede recopilar cuatro tipos de registros diferentes: syslog, ODBC, eventos de Windows y archivos planos.

M

Término	Descripción
Malware Analysis	Malware Analysis es un dispositivo y un servicio que comparte ubicación en Security Analytics. El servicio se usa para el análisis automatizado de malware y está disponible a través del módulo Investigation.

Término	Descripción
Recopilación de mensajes	Usa una función de hash unidireccional para convertir una cantidad arbitraria de bytes en una secuencia de bytes de longitud fija. Esto se usa como parte de una solución de privacidad de datos.
Base de datos de metadatos	la base de datos de metadatos contiene información que un Decoder o Log Decoder extrae del flujo de datos crudos. Los analizadores, las reglas o los feeds pueden generar elementos de metadatos.
ID de meta-datos	número que se usa para identificar exclusivamente un elemento de metadatos en la base de datos de metadatos.
datos de metadatos o elementos de metadatos	Un Decoder recopila y analiza datos crudos, con lo cual crea elementos de metadatos (metadatos) en el proceso.
clave de metadatos	nombre que se utiliza para clasificar el tipo de cada elemento de metadatos. Las claves de metadatos comunes incluyen ip.src, time o service.
valor de metadatos	cada elemento de metadatos contiene un valor. El valor es lo que genera cada analizador, feed o regla.
licencia medida	La licencia medida es un método de licencia de Security Analytics que se basa en un rendimiento por día de registros (SIEM) o paquetes de red (monitoreo de red y malware de red), junto con la compra por separado del hardware necesario para implementar el sistema y satisfacer los requisitos de retención de los clientes.

N

Término	Descripción
Dispositivo NetWitness o NextGen	Un servicio RSA Broker, Concentrator, Decoder, Log Decoder o Log Collector. Si ve los términos dispositivo NextGen o dispositivo NetWitness, cámbielo a dispositivo Core.

O

Término	Descripción
licencia de prueba de uso inmediato	Security Analytics 10.5 incluye una licencia de prueba de uso inmediato predeterminada que permite a los clientes usar el producto con funcionalidad completa durante 90 días. El periodo de 90 días comienza cuando la interfaz del usuario de Security Analytics se configura y se usa por primera vez.
Anuncios de incumplimiento de normas	Durante el inicio de sesión se muestra un anuncio rojo si la licencia venció o si se superó el uso asignado. También puede ver un anuncio rojo si la licencia tiene errores internos. Un anuncio rojo no se puede descartar. Durante el inicio de sesión se muestra un anuncio amarillo si se aproxima el vencimiento de la licencia o si está cerca del uso asignado. Puede descartar este anuncio amarillo si hace clic en el botón Descartar.

P

Término	Descripción
ID de paquete	Número que se usa para identificar exclusivamente un paquete o un registro en una base de datos de paquete.
Base de datos de paquete	La base de datos de paquete contiene los datos crudos capturados. En un Decoder, la base de datos de paquete contiene paquetes que se capturan de la red. Los Log Decoders utilizan la base de datos de paquete para almacenar registros crudos. Es posible acceder a los datos crudos almacenados en la base de datos de paquete mediante ID de paquete; sin embargo, generalmente este ID nunca es visible para el usuario final.
datos personales	“De acuerdo con la ley de la UE, los datos personales se definen como información relacionada con una persona natural identificada o identificable, es decir, información sobre una persona cuya identidad se manifiesta claramente o puede al menos establecerse con la obtención de información adicional”. (Fuente: EU_DP_LAW_HANDBOOK)

R

Término	Descripción
RSA Analytics Warehouse	Un sistema de cómputo distribuido basado en hadoop, que recopila, administra y permite la analítica y la creación de informes sobre conjuntos de datos de seguridad a largo plazo, por ejemplo, meses o años. Warehouse puede estar conformado por tres o más nodos según los requisitos de analítica, archiving y resistencia de la organización. Requiere un servicio denominado Warehouse Connector para recopilar metadatos y eventos de Decoder y Log Decoder, y los escribe en formato Avro en un sistema de procesamiento distribuido basado en Hadoop.
Módulo Reports	El módulo Reports es la interfaz del usuario de Security Analytics para las funciones automatizadas de creación de informes.
funciones	En Security Analytics, las funciones determinan lo que pueden hacer los usuarios. Una función tiene permisos asignados y usted debe asignar una función a cada usuario. El usuario tiene entonces permiso para hacer lo que la función le permite.

S

Término	Descripción
Security Analytics Core (anteriormente NextGen)	Los siguientes productos forman parte de la suite de Security Analytics Core: Decoder, Log Decoder, Concentrator, Broker, Archiver y Workbench.
Servidor de Security Analytics	El servidor web para creación de informes, investigación, administración y otros aspectos de la interfaz del analista. También permite la creación de informes sobre datos que se encuentran en el dispositivo Warehouse.

Término	Descripción
datos confidenciales	Las disposiciones normativas de algunos lugares, como la Unión Europea (UE), exigen que los sistemas de información cuenten con medios de protección de datos cuando usan datos confidenciales. Todos los datos que puedan representar directa o indirectamente "quién hizo qué y cuándo" se pueden considerar como datos confidenciales o de identificación personal.
Servicio	Un servicio se ejecuta en un host y realiza una función única, como recopilar registros o archivar datos. Los servicios de Security Analytics incluyen Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Incident Management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector y Workbench.
licencia basada en servicios	Esta es una licencia de Security Analytics permanente por servicio que no tiene fecha de vencimiento. La compatibilidad con la licencia basada en servicios se aplica a todos los dispositivos que requieren una licencia.
sesión	En un Packet Decoder, una sesión representa un único flujo de red lógica. Por ejemplo, una conexión TCP/IP es una sesión. En un Log Decoder, cada evento de un registro es una sesión. Cada sesión contiene referencias a todos los ID de paquete e ID de metadatos que hacen referencia a la sesión.
ID de sesión	Número que se utiliza para identificar de manera única una sesión en la base de datos de sesiones.
Base de datos de sesión	la base de datos de sesión contiene información que vincula el paquete y los elementos de metadatos juntos en sesiones.
Implementación de SIEM	En una implementación de información de seguridad y administración de eventos (SIEM), la configuración básica de Security Analytics requiere estos componentes: Log Decoder, Concentrator, Broker, Event Stream Analysis (ESA) y el servidor de Security Analytics.

Término	Descripción
licencia de suscripción	Las licencias de suscripción para Security Analytics se ofrecen por un período específico que varía entre 12 y 36 meses. Una vez que se obtienen, las licencias de suscripción no se pueden cancelar ni degradar.

T

Término	Descripción
Datos transitorios	En Security Analytics, los datos transitorios no se almacenan en disco. Cuando una clave de metadatos se marca como transitoria en el archivo de índice personalizado o en la vista Configuración de servicios donde se configuran los analizadores para el servicio, el Decoder y el Log Decoder no guardan la clave de metadatos en disco, sino que la mantienen en memoria, donde se puede analizar hasta que se sobrescribe.

V

Término	Descripción
host virtual	(Formalmente, dispositivo virtual) Máquina virtual, que se designa con un nombre de dominio calificado o una dirección IP, en la cual se ejecuta cualquier servicio de Security Analytics [es decir, los servicios Appliance, Archiver, Broker, Concentrator, Decoder (Packets y Logs), Hybrid, Malware Analysis, Event Stream Analysis, Log Collector, Security Analytics Warehouse, Workbench, Reporting Engine e IPDB Extractor]. Una instancia virtual de un dispositivo Security Analytics.

W

Término	Descripción
Warehouse Connector	Warehouse Connector recopila metadatos y eventos de Decoders y los escribe en formato Avro en un sistema de procesamiento distribuido basado en Hadoop. Puede configurar Warehouse Connector como un servicio en Log Decoders o Decoders existentes o se puede ejecutar como un dispositivo virtual en el ambiente virtual.
Eventos de Windows	Eventos de Windows tiene relación con Log Decoders y se refiere a la metodología de recopilación de Windows 2008 y a los archivos planos que se pueden obtener a través de SFTP.

Procedimientos

En Security Analytics, los usuarios deben abrir un navegador e iniciar sesión. Para aprovechar Security Analytics al máximo, debe saber cómo administrar trabajos y notificaciones, configurar tableros y cuadrículas, personalizar los ajustes de las aplicaciones, como el idioma y la zona horaria, y cambiar su contraseña.

Estos procedimientos están dirigidos a todos los usuarios que aprenden a trabajar en Security Analytics.

Acceso a Security Analytics

El acceso a Security Analytics puede variar en función del ambiente. Puede tener una cuenta de usuario interna o una cuenta de usuario externa de Security Analytics. Las cuentas de usuario internas son locales para Security Analytics y los usuarios internos pueden iniciar sesión en Security Analytics y recibir permisos basados en funciones. Las cuentas de usuario externas se autentican fuera de Security Analytics y se mapean a funciones de Security Analytics. Si es un usuario externo y no puede acceder a Security Analytics ni ver la información que necesita dentro de Security Analytics, póngase en contacto con el administrador del sistema. El administrador puede asignar las funciones apropiadas a su cuenta.

Nota: Si inicia sesión en Security Analytics desde una ventana del navegador Internet Explorer 10, se puede mostrar el siguiente error: `The page can't be displayed.` Debe habilitar el protocolo TLS 1.1 en el navegador de la siguiente manera: Navegue a **Opciones de Internet > Opciones avanzadas > Configuración > Seguridad**. Además de los otros protocolos, asegúrese de que el protocolo TLS 1.1 esté habilitado. Haga clic en **Aplicar**. Vuelva a cargar la página.

Cuando intenta iniciar sesión en Security Analytics, la cuenta puede estar en uno de los siguientes estados:

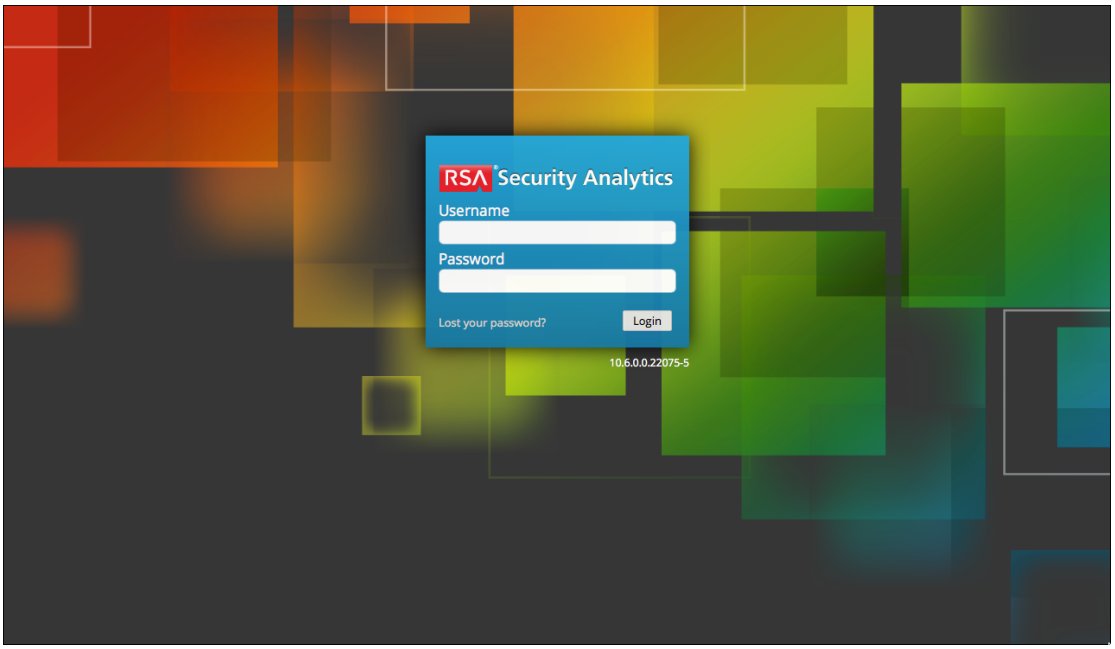
- **Válido:** Puede iniciar sesión correctamente en Security Analytics.
- **Bloqueado:** no puede iniciar sesión debido a que hubo demasiados intentos de inicio de sesión en su cuenta con credenciales incorrectas. Esto es temporal. Póngase en contacto con el administrador para obtener ayuda.
- **Expirado:** Puede autenticarse en Security Analytics, pero debe cambiar la contraseña antes de acceder a Security Analytics.

1. Use un ícono de Security Analytics que proporcionó el administrador o escriba lo siguiente en el navegador web:

   `https://<hostname or IP address>/login`

Donde `<hostname or IP address>` es el nombre de host o la dirección IP del servidor de Security Analytics.

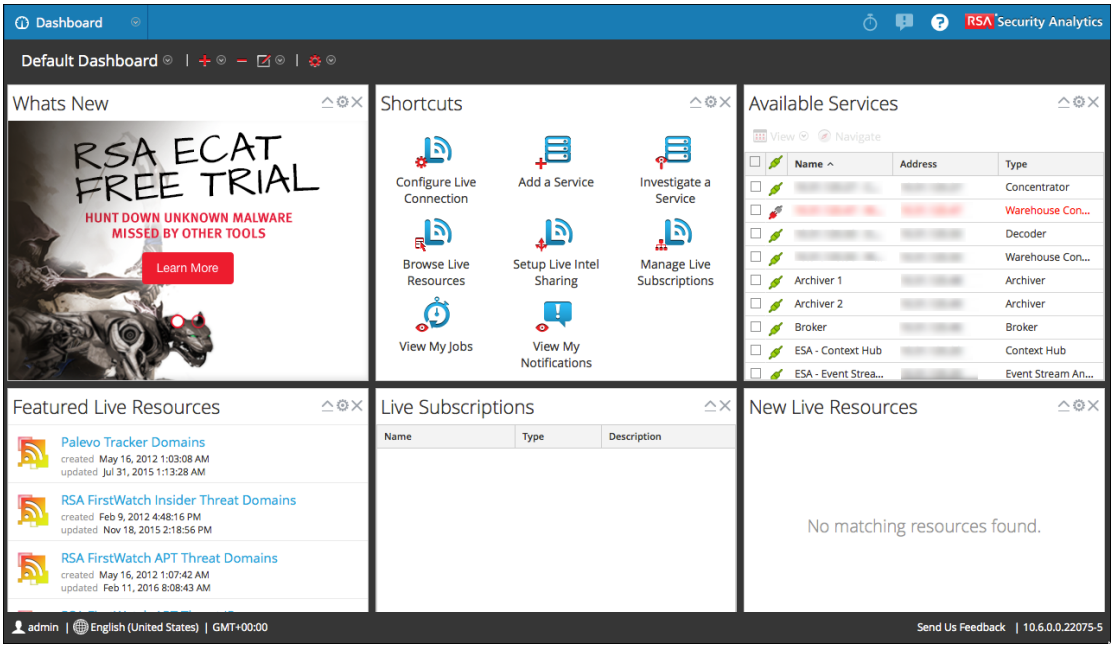
Aparece la pantalla de inicio de sesión de Security Analytics.



2. Escriba el nombre de usuario y la contraseña, y haga clic en **Inicio de sesión**.

   Si el inicio de sesión se realiza correctamente, se abrirá una vista inicial de acuerdo con las preferencias del perfil de usuario.

   En la siguiente figura se muestra un ejemplo del tablero predeterminado de Security Analytics.

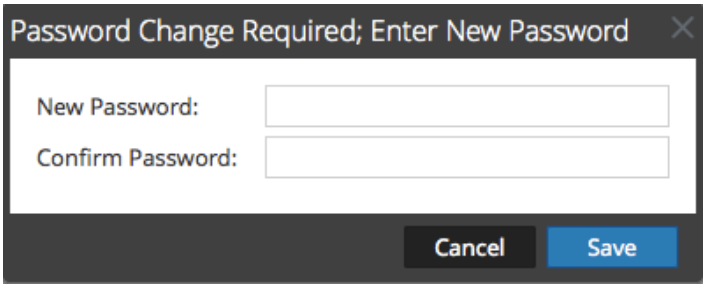


Si la cuenta está bloqueada:

Si hace demasiados intentos de inicio de sesión con un nombre de usuario o una contraseña incorrectos, la cuenta se bloqueará. Póngase en contacto con el administrador para que desbloquee la cuenta.

Si la cuenta venció:

1. En el cuadro de diálogo, escriba una nueva contraseña, confírmela y haga clic en **Guardar**.

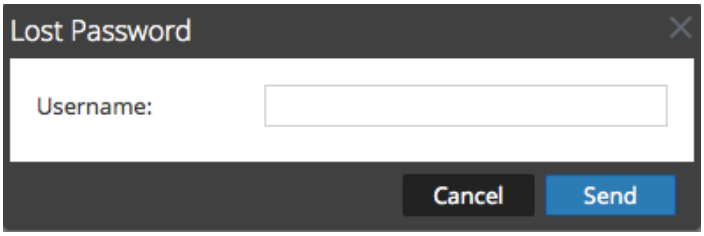


2. Haga clic en **Aceptar** para confirmar que la contraseña se cambió correctamente.
   Tiene un máximo de cinco minutos para ingresar la contraseña nueva. El tiempo de espera de la sesión se podría agotar antes según la configuración de seguridad de la sesión y del tiempo de inactividad que estableció el administrador. Si el tiempo de espera de la sesión se agota, vuelva a iniciar sesión con la contraseña antigua y cambie la contraseña.

Si olvidó la contraseña:

1. En la pantalla de inicio de sesión de Security Analytics, haga clic en el vínculo **¿Perdió su contraseña?**.

2. En el cuadro de diálogo **Contraseña perdida**, escriba su nombre de usuario y haga clic en **Enviar**.



Debe recibir un correo electrónico con instrucciones. Si no recibe un correo electrónico, póngase en contacto con el administrador para que agregue una dirección de correo electrónico a su cuenta.

Si no dispone del acceso apropiado a Security Analytics:

Si puede iniciar sesión correctamente en Security Analytics, pero no puede ver la información que necesita, es posible que requiera que se asigne una función de usuario a su cuenta de usuario. Póngase en contacto con el administrador para obtener ayuda.

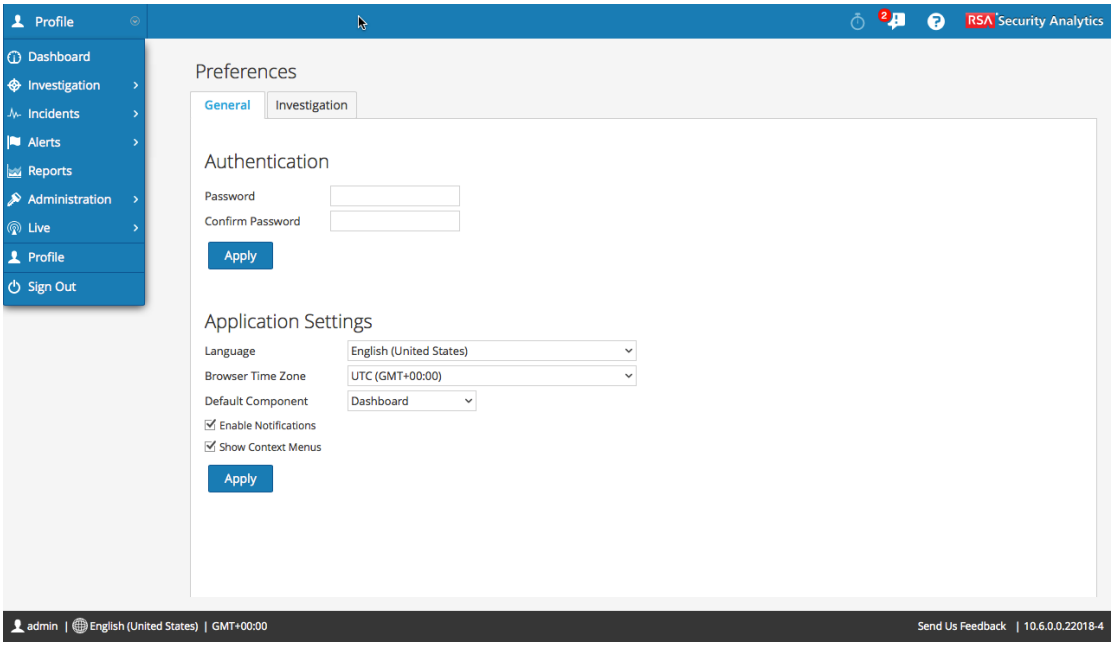
Cambio de la contraseña

Los usuarios pueden cambiar la contraseña que usan para autenticarse en Security Analytics en la vista Perfil > panel Preferencias. La contraseña del usuario se actualiza en los servicios de Security Analytics Core, a menos que se trate del usuario administrador. La contraseña del usuario administrador no se propaga a los servicios principales. Después de cambiar la contraseña, el usuario debe cerrar sesión y volver a iniciarla para comunicarse con los servicios principales.

Nota: Para los servicios principales, esto se aplica solo a conexiones que no son de confianza. Cuando un servicio principal usa una conexión de confianza, el usuario no ingresa una contraseña, de modo que no se requiere una actualización.

Para cambiar la contraseña de Security Analytics:

1. En el menú de **Security Analytics**, seleccione **Perfil.**
2. En el panel de opciones, seleccione **Preferencias**.
   El panel Preferencias se muestra con la pestaña General abierta.



3. En la sección **Autenticación**, escriba una nueva contraseña en el campo **Contraseña**.
4. En el campo **Confirmar contraseña**, vuelva a escribir la nueva contraseña.
5. Haga clic en **Aplicar**.
   La contraseña nueva entra en vigor inmediatamente y se solicita la próxima vez que inicia sesión en Security Analytics.
6. Para cerrar sesión y volver a iniciarla con las nuevas credenciales:
   a. En el menú de **Security Analytics**, seleccione **Cerrar sesión**.
   b. Vuelva a iniciar sesión en Security Analytics con la credencial nueva.

Configuración de las preferencias de la aplicación

En esta sección se documentan las preferencias de usuario válidas para la aplicación Security Analytics en general. Las preferencias que se aplican específicamente a Investigation se describen en el tema **Configurar la vista Navegar y la vista Eventos** de la *Guía de Investigation y Malware Analysis*.

Puede ver y administrar preferencias de diferentes usuarios en el panel Preferencias. Puede:

- Configurar el idioma de la aplicación
- Configurar la zona horaria del navegador
- Configurar el componente predeterminado

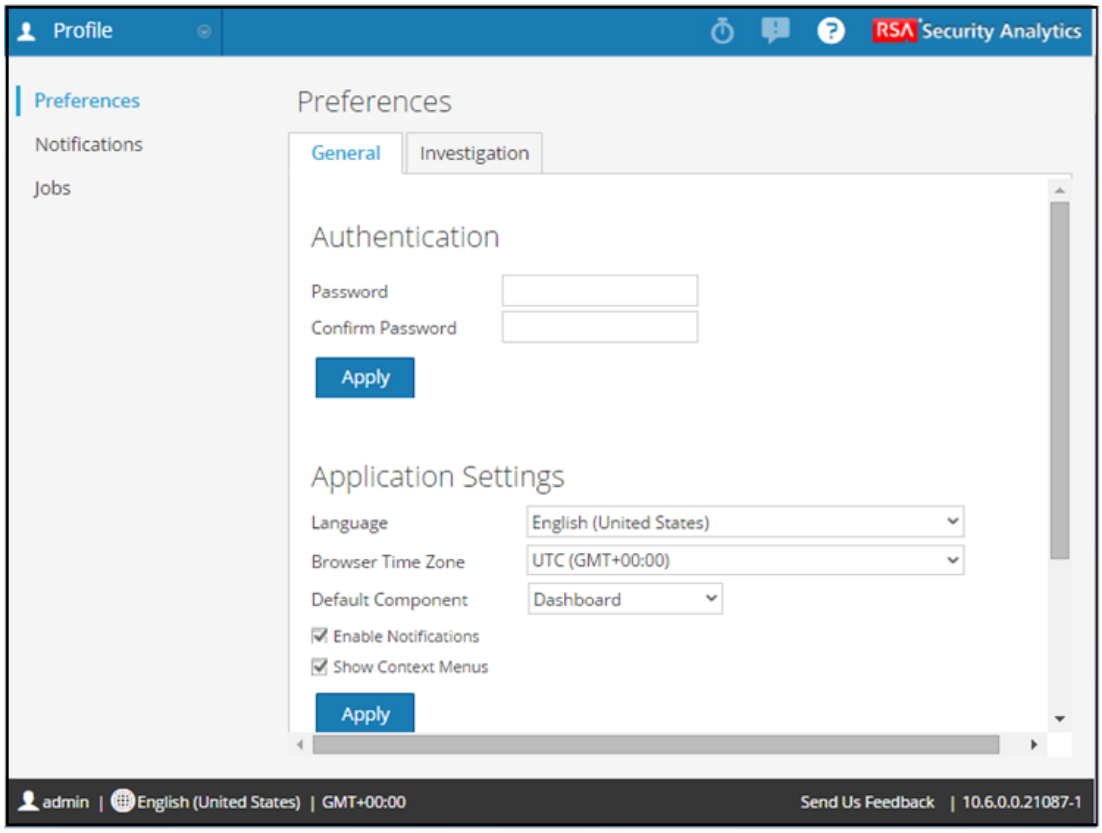
- Habilitar notificaciones
- Habilitar menús contextuales

Estas preferencias se aplican a su propio perfil.

Ver las preferencias de usuario

Para ver preferencias de usuario:

1. En el menú de **Security Analytics**, seleccione **Perfil.**
2. En el panel de opciones, seleccione **Preferencias**.



Configurar el idioma, la zona horaria del navegador y el componente predeterminado para Security Analytics

El idioma predeterminado para todos los tableros, dashlets, vistas y cuadros de diálogo que ve es el idioma recomendado que envía su navegador. Si Security Analytics no está traducido a ese idioma, el idioma predeterminado es inglés (Estados Unidos). Puede cambiar el idioma a otros a los que Security Analytics está traducido. Estos ajustes se pueden configurar en la sección **Configuración de aplicación**.

Para cambiar el idioma, la zona horaria del navegador y el componente predeterminado de Security Analytics:

1. Seleccione una localización en la lista desplegable **Idioma**.
2. Seleccione una zona horaria en la lista desplegable **Zona horaria del navegador**.
3. Seleccione el componente que cumple la función de vista inicial cuando inicia sesión en Security Analytics en la lista desplegable **Componente predeterminado**.
4. Haga clic en **Aplicar**.
   Las configuraciones seleccionadas entran en vigencia de inmediato.

Habilitar o inhabilitar las notificaciones del sistema para la cuenta de usuario

De manera predeterminada, las notificaciones del sistema de Security Analytics se habilitan cuando se crea una cuenta de usuario nueva. Cada usuario puede realizar este cambio según su preferencia. Para activar o desactivar notificaciones para su cuenta de usuario:

1. En la sección **Configuración de aplicación**, haga clic en la casilla de verificación **Habilitar notificaciones**.
2. Haga clic en **Aplicar**.
   La nueva preferencia se aplica de inmediato.

Activar o desactivar menús contextuales para su cuenta de usuario

De manera predeterminada, los menús contextuales de Security Analytics se habilitan cuando se crea una cuenta de usuario nueva. Los menús contextuales proporcionan funciones adicionales para vistas específicas cuando hace clic con el botón secundario en una vista. Cada usuario puede realizar este cambio según su preferencia. Para activar o desactivar menús contextuales para su cuenta de usuario:

1. En la sección **Configuración de aplicación**, haga clic en la casilla de verificación **Mostrar menús contextuales**.
2. Haga clic en **Aplicar**.
   La nueva preferencia se aplica de inmediato.

Visualización de la ayuda en la aplicación

Estos procedimientos son útiles cuando usted busca ayuda mientras trabaja en Security Analytics. Hay distintas maneras de obtener ayuda mientras usa Security Analytics. Entre las opciones, se incluyen: ayuda en pantalla, mensajes de globo y vínculos de ayuda.

Ver la ayuda en pantalla

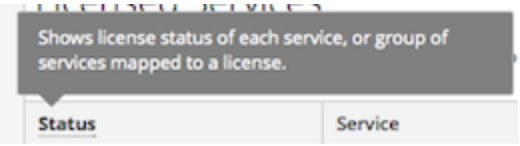
En la ayuda en línea se proporciona información adicional sobre lo que se debe hacer en las secciones o los campos que ve en la interfaz del usuario de Security Analytics. Para mostrar la ayuda en pantalla, coloque el cursor sobre . La ayuda en pantalla muestra una descripción breve del elemento.

Ejemplo de la ayuda en pantalla:

Ver mensajes de globo

Los mensajes de globo son una manera rápida de ver una descripción del texto o información adicional sobre una acción, un campo o un parámetro. Los mensajes de globo aparecen como texto subrayado. Para mostrar el mensaje de globo y ver una descripción breve del término, mantenga el mouse sobre el texto subrayado.

Ejemplo de un mensaje de globo:



Ver la ayuda en línea

Los vínculos de la ayuda en línea lo llevan fuera de Security Analytics a la documentación en línea de RSA. Este sitio tiene un conjunto de documentación completo para Security Analytics y los vínculos llevan al usuario directamente al tema que describe la parte de la interfaz del usuario que está activa en la vista.

Para ver el tema de la ayuda en línea correspondiente a la ubicación actual, haga clic en en la barra de herramientas de Security Analytics o en un cuadro de diálogo. El tema de ayuda pertinente se muestra en una ventana del navegador por separado. En él se describen las características y las funciones de la vista o el cuadro de diálogo actuales. Desde ese tema, puede navegar rápidamente a los procedimientos relacionados.

La siguiente figura es un ejemplo del ícono de la ayuda en línea en la barra de herramientas de Security Analytics.

Configuración de los tableros

A medida que se familiarice con Security Analytics, habrá tipos de información que deseará ver rápida y fácilmente en el tablero. Puede obtener grandes beneficios si configura sus tableros para que muestren la información que apoya su flujo de trabajo.

Las operaciones que pertenecen a los tableros son:

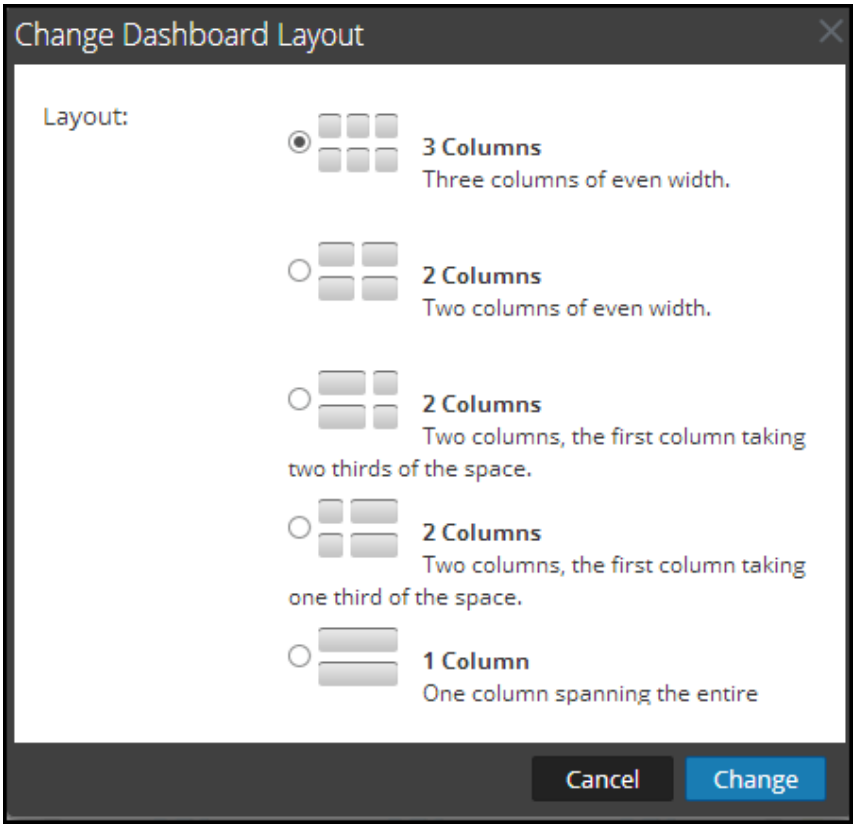
- Creación y eliminación de tableros
- Restauración del tablero predeterminado
- Cambio del diseño de un tablero
- Cambio entre tableros
- Adición, eliminación, transferencia, edición y maximización de dashlets en un tablero
- Importación y exportación de tableros

Organización del diseño del tablero

Para personalizar las vistas en Security Analytics, puede cambiar el diseño del tablero de **Security Analytics** o de un tablero personalizado.

1. Navegue a cualquier tablero.
2. En la barra de herramientas del tablero, haga clic en el menú desplegable **Editar** () y seleccione **Cambiar diseño del tablero**.

Se muestra el cuadro de diálogo Cambiar diseño del tablero.



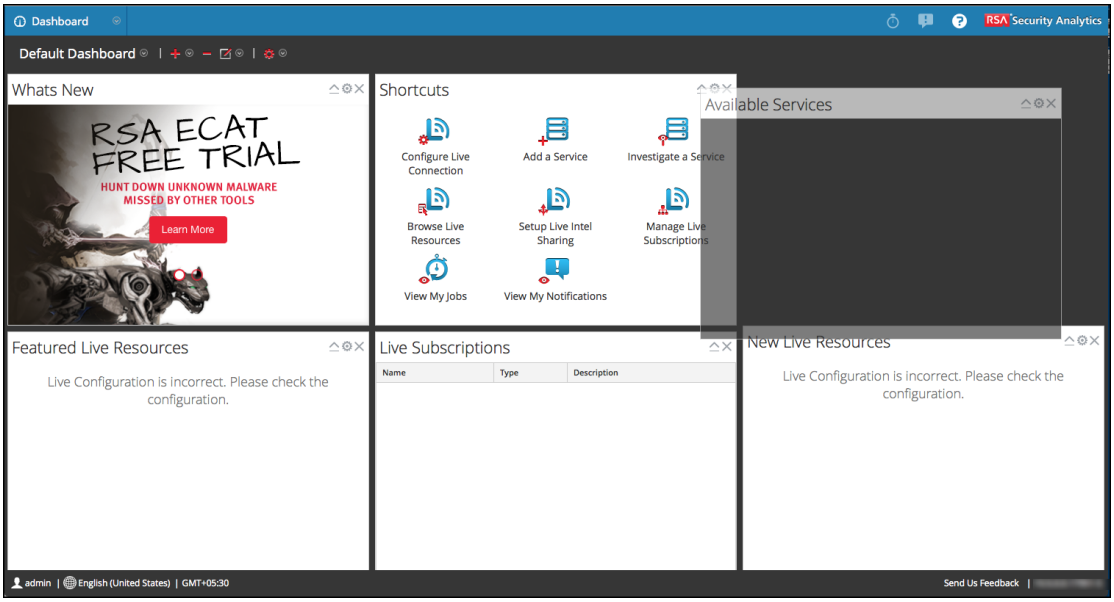
3. Escoja un diseño para el tablero y haga clic en **Cambiar**.
   El diseño del tablero se cambia al diseño seleccionado.

Mover un dashlet a otra posición

Puede organizar los dashlets según su preferencia. Para esto, debe arrastrarlos y soltarlos en otro orden en el tablero.

1. Para mover un dashlet, mantenga el cursor sobre el encabezado del dashlet que desea mover.
   El cursor de dirección aparece sobre el dashlet. Haga clic y mantenga presionado el encabezado del dashlet que desee mover.
2. Siga presionando el botón del mouse izquierdo y arrastre la ventana hacia la nueva ubicación.
   En la siguiente imagen se muestra el dashlet Nuevos recursos de Live a medida que se

desplaza de la parte inferior de la columna 1 a la parte superior de la columna 3.

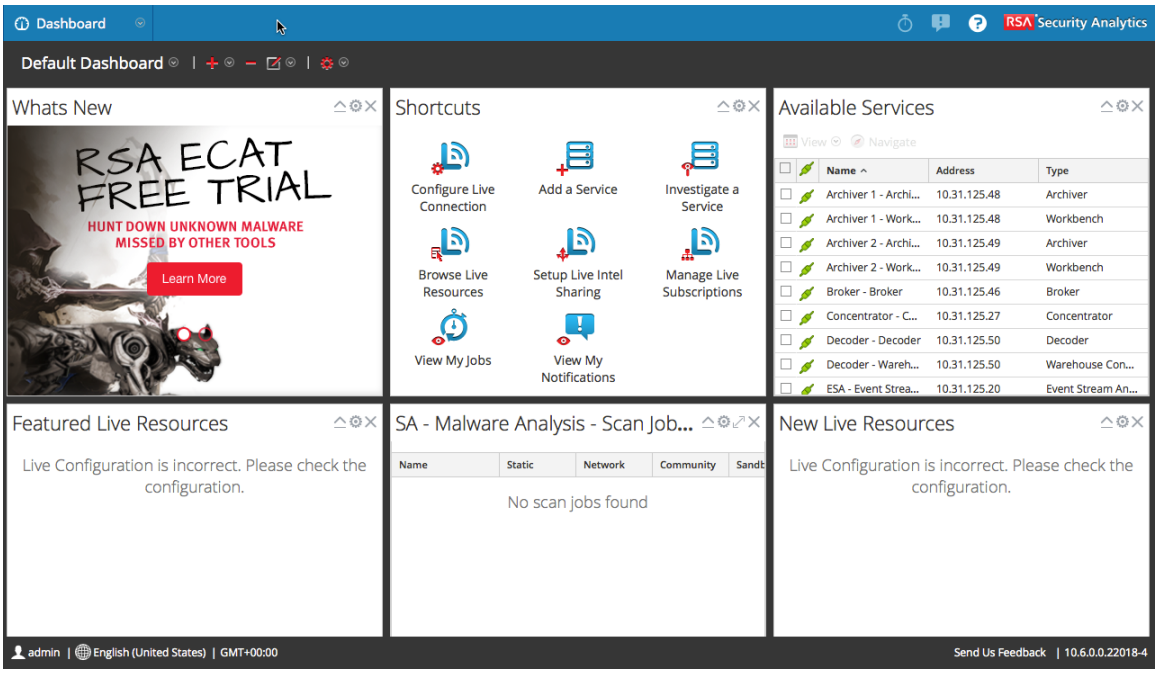


3. Suelte el botón del mouse cuando el dashlet esté en la ubicación deseada.

   El dashlet que ocupa actualmente esa posición se desplaza hacia abajo.

Maximizar un único dashlet

En este tema se explica cómo abrir un dashlet en el área completa del tablero principal de Security Analytics con el mismo título del dashlet. Por ejemplo, el dashlet Trabajos de escaneo de la siguiente figura se puede ver en el área completa del tablero de Security Analytics. Es más fácil ver los dashlets que tienen una gran cantidad de columnas o gráficos, por ejemplo, algunos dashlets de Reporting, cuando están maximizados. Esto permite ver todo el contenido sin necesidad de desplazarse.

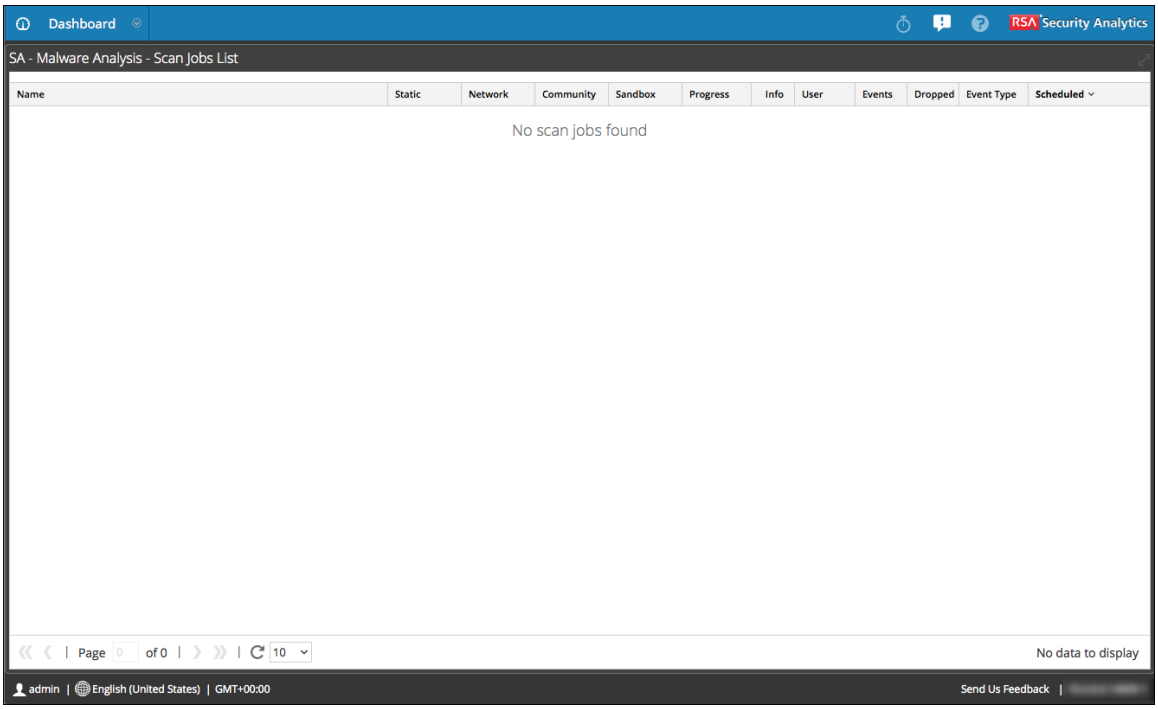


1. Para maximizar un dashlet, haga clic en el ícono de control de maximización de la barra de título del dashlet: ⤢

   El dashlet se muestra en pantalla completa.

2. Para maximizar un dashlet, haga clic en el ícono de control de maximización de la barra de título del dashlet: ⤢

   El dashlet se muestra en pantalla completa.



Restaurar el tablero predeterminado

Después de personalizar el tablero de **Security Analytics** predeterminado, puede revertirlo al diseño original de los dashlets mediante la opción **Restaurar tablero predeterminado** del menú desplegable **Acciones** (). Para realizar esta reversión, se debe mostrar el tablero de un módulo.

1. Navegue al tablero de **Security Analytics** que se personalizó.
2. En la barra de herramientas del tablero, haga clic en el menú desplegable **Acciones** () y seleccione **Restaurar tablero predeterminado**.
   Se restaura el diseño original del tablero predeterminado.

Adición y administración de dashlets

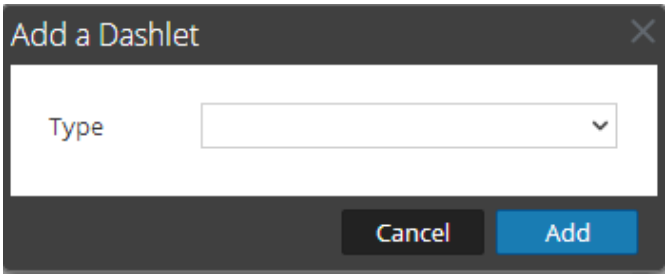
Puede agregar dashlets al tablero predeterminado o crear un tablero personalizado con su propio conjunto de dashlets útil para que el flujo de trabajo sea más eficiente. Algunos dashlets tienen opciones de configuración para adaptar la apariencia o el contenido del dashlet.

Agregar un dashlet

Para personalizar las vistas de Security Analytics, puede agregar dashlets al tablero de Security Analytics o a un tablero personalizado. El tablero de Security Analytics, como indica el nombre, ofrece todos los dashlets de Security Analytics. El cuadro de diálogo Agregar un dashlet proporciona una forma de definir el nombre y los parámetros configurables para un nuevo dashlet.

1. Para agregar un dashlet, navegue a cualquier tablero.
2. En la barra de herramientas del tablero, haga clic en y seleccione **Agregar dashlet** en el menú desplegable.

   Se muestra el cuadro de diálogo Agregar un dashlet.

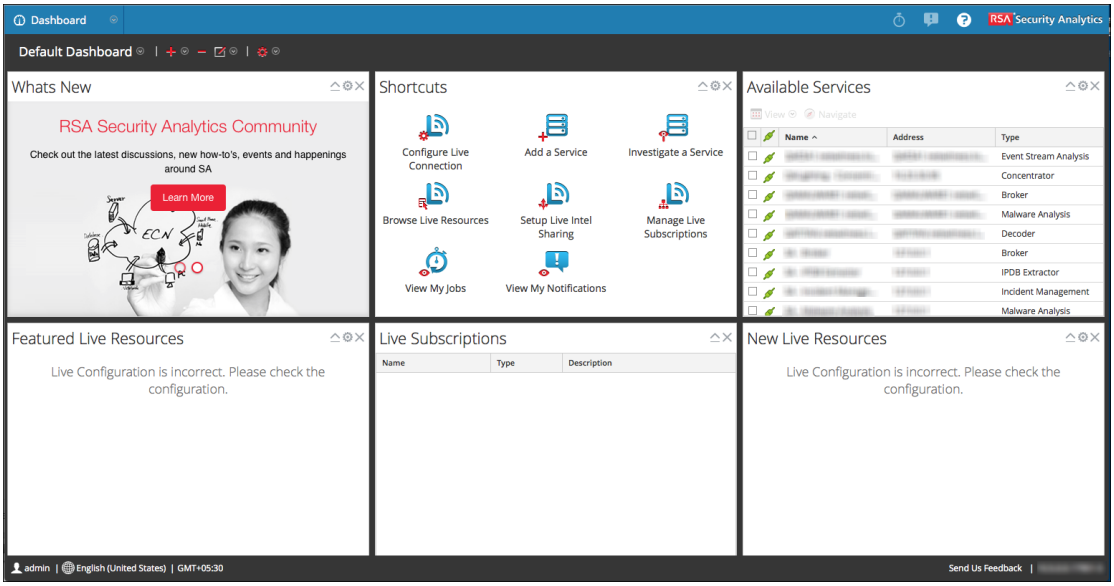


3. Haga clic en la lista de selección **Tipo** para ver los tipos de dashlets disponibles y seleccione el tipo de dashlet que desea agregar; por ejemplo, Monitor de servicios de administración.

Otros campos configurables quedan disponibles en el cuadro de diálogo **Agregar un dashlet**; estos varían según el dashlet. Por ejemplo, en un dashlet **Monitor de servicios de administración**, usted define el título del dashlet y el tipo de servicio que se monitoreará. Todos los dashlets tienen un título.

4. Ingrese un título para el dashlet. Puede escribir letras, nombres, caracteres especiales y espacios para el nombre. Por ejemplo, el título podría ser **Dashlet Monitor de servicios**.
5. Si hay campos configurables disponibles para el dashlet, configure los valores correspondientes. Puede seleccionar más de un tipo de servicio.
6. Cuando se hayan configurado todos los campos obligatorios, haga clic en **Agregar**.

   El dashlet se agrega al tablero.



Editar las propiedades de un dashlet

Algunos dashlet son de solo lectura y las propiedades no son configurables. Otros dashlets son configurables para que los usuarios puedan personalizar algunos aspectos de los datos que se muestran en ese dashlet. Un dashlet con propiedades editables tiene un ícono de configuración que muestra la hoja de propiedades para edición.

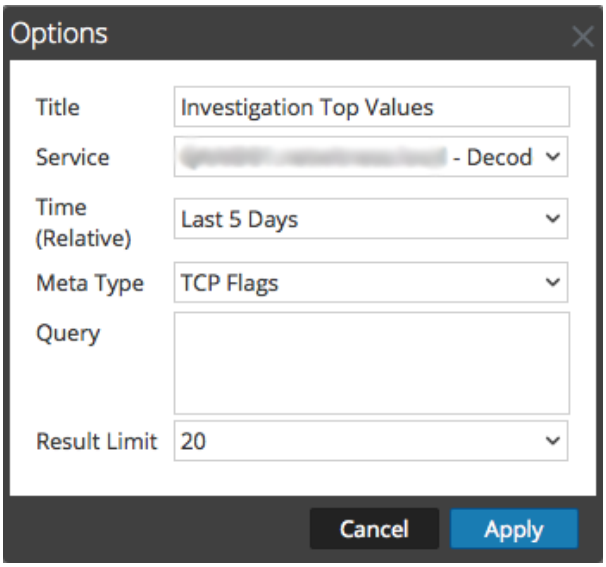
Un dashlet sin propiedades editables, como el dashlet Suscripciones de Live, no muestra el ícono de configuración en la barra de título.

Muchos dashlets tienen un título editable. Un ejemplo de un dashlet con propiedades configurables adicionales es el dashlet Monitor de servicios de administración, en el cual puede editar las siguientes propiedades:

- Título de la pantalla del dashlet.
- Tipo de servicios que se monitorearán; por ejemplo, puede monitorear solo Decoders o Decoders y Concentrators.

Otros dashlets tienen parámetros que puede definir para especificar el tipo y la cantidad de información que desea ver en el dashlet. El tablero de investigación personalizado tiene tres dashlets. Cada uno de los tres muestra el ícono de configuración.

1. Para mostrar y modificar las opciones de un dashlet, haga clic en el ícono de configuración en una barra de título del dashlet.
   Se muestra el cuadro de diálogo **Opciones**.



2. Cambie cualquiera de las propiedades mostradas. Por ejemplo, en un dashlet Valores principales de Investigation, puede cambiar el Límite de resultado de 20 a 40.
3. Haga clic en **Aplicar**.
   Se aplican los cambios.

Eliminar un dashlet

1. Haga clic en el ícono de control de eliminación en la barra de título del dashlet:
   El cuadro de diálogo **Eliminar dashlet** solicita confirmar la intención de eliminar el dashlet.
2. Si desea eliminarlo, haga clic en **Sí**. El dashlet se quita del tablero.
   Si decide no eliminarlo, haga clic en **No**.

Trabajo con tableros personalizados

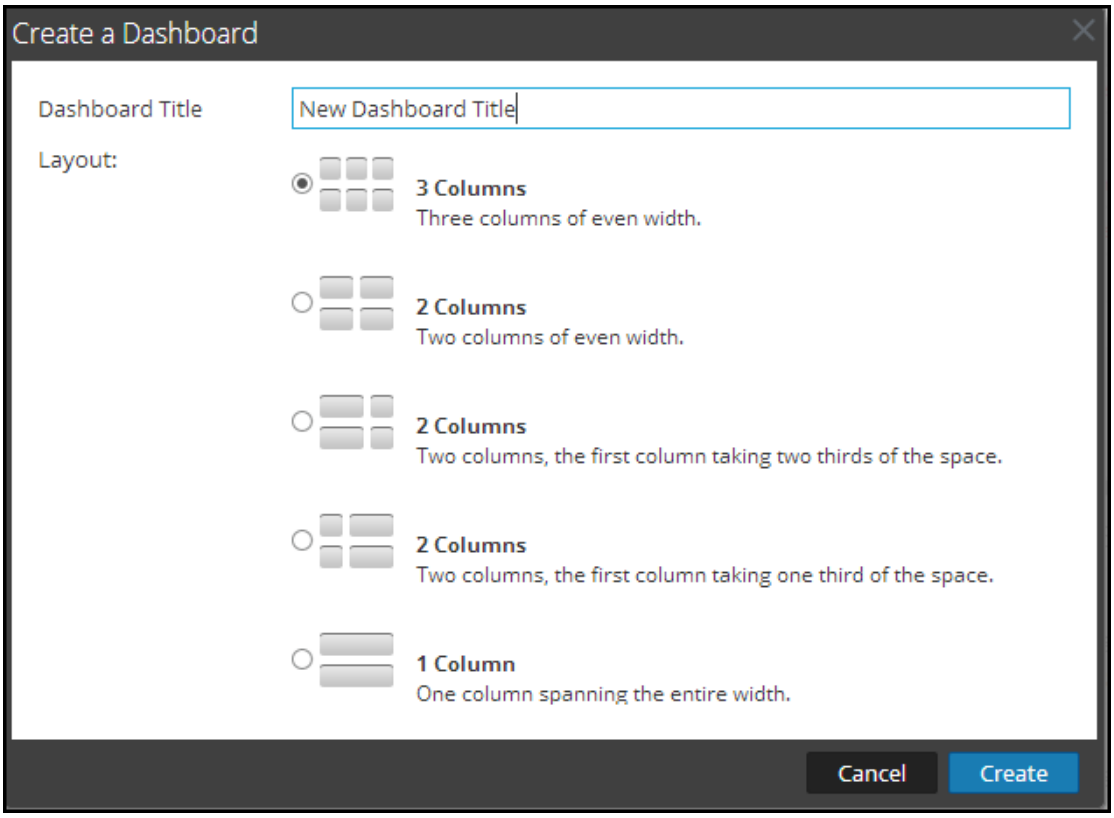
Para adaptar Security Analytics a fin de brindarle un mejor servicio a su sitio y sus métodos, puede crear tableros personalizados. Algunas razones para crear tableros personalizados son:

- Consolidar funcionalidad relacionada en un único tablero.
- Crear un tablero Unified con una recopilación de dashlets para todos los módulos.
- Crear un tablero para consolidar dashlets de diferentes ubicaciones de red.
- Crear una vista general de las funcionalidades de un módulo determinado.
- Consolidar dashlets que se apliquen a un escenario específico.

Crear tableros personalizados

1. En el tablero de **Security Analytics**, seleccione  **> Crear nuevo tablero**.

   Se muestra el cuadro de diálogo Crear un tablero.



2. Escriba el título del nuevo tablero. Puede escribir letras, nombres, caracteres especiales y espacios para el nombre. La longitud permitida para el nombre es 255 caracteres.
3. Seleccione una opción de diseño para el nuevo tablero.

   Se crea el tablero y se agrega a la lista de selección de tableros

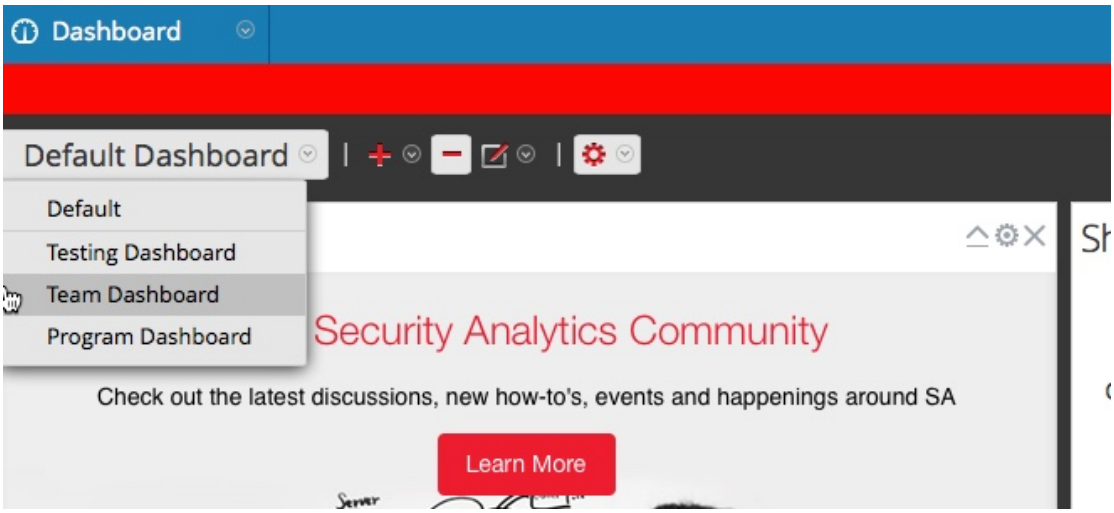
Ahora que creó un tablero, puede:

- Agregue dashlets al tablero.
- Exporte el tablero.
- Elimine el tablero.
- Cambiar el nombre del tablero.

Seleccionar un tablero

1. Para cambiar entre tableros en un módulo de Security Analytics, haga clic en la **Lista de selección de tableros**.

   Se muestra la Lista de selección de tableros.



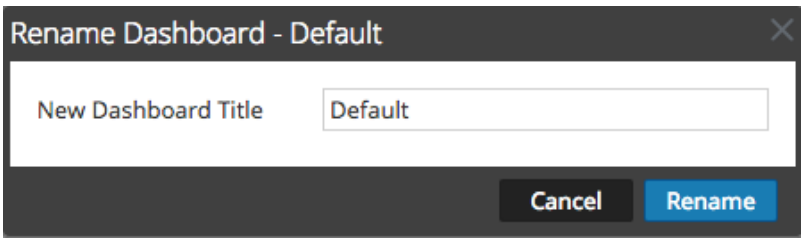
2. Seleccione el tablero que desea ver.

   Se muestra el tablero seleccionado.

Cambiar el nombre de un tablero personalizado

1. En la barra de herramientas del tablero, seleccione  > **Cambiar el nombre del tablero**.

   Se muestra el cuadro de diálogo Cambiar el nombre del tablero.



2. En el campo **Título de tablero nuevo**, ingrese un nuevo título para el tablero.

3. Haga clic en **Rename**.

   El tablero se actualiza con el nuevo título.

Eliminar un tablero personalizado

Si encuentra que la Lista de selección de tableros en Security Analytics incluye tableros personalizados que ya no son necesarios, puede quitar los tableros no deseados. Debe mostrarse el tablero que se eliminará. El tablero predeterminado no puede eliminarse.

Nota: Si desea que el tablero esté disponible en el futuro, puede exportarlo antes de quitarlo, como se describe en Importación y exportación de tableros.

1. En la **Lista de selección de tableros**, seleccione el tablero no deseado; por ejemplo, **Región 3**.

   Se muestra el tablero.

2. En la barra de herramientas del tablero, seleccione .

   Un cuadro de diálogo solicita confirmar la intención de eliminar el tablero.

3. Para confirmar la eliminación del tablero, haga clic en **Sí**.

   Se elimina el tablero de la Lista de selección de tablero.

Importación y exportación de tableros

La capacidad para exportar tableros personalizados según las diferentes circunstancias y condiciones podría llevar a tener una gran cantidad de tableros que no se necesitan diariamente. En lugar de reinventar la rueda cada vez que desee volver a crear un determinado tablero personalizado, puede exportar los tableros que no se estén utilizando actualmente. Cuando esté listo para utilizar un tablero exportado anteriormente, impórtelo a Security Analytics.

Exportar un tablero

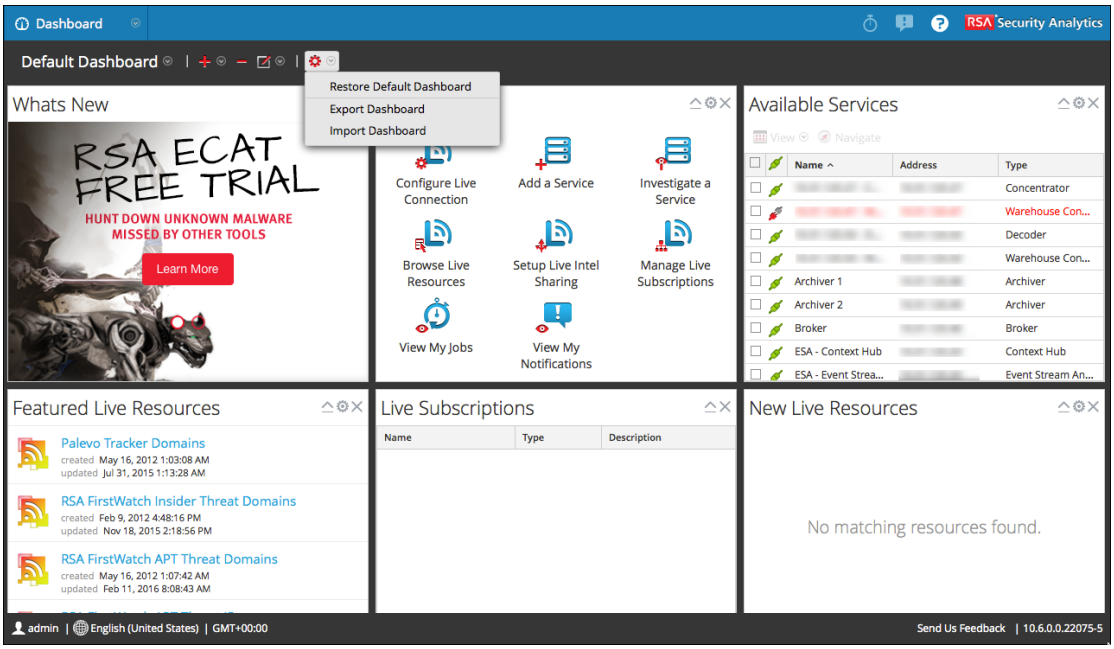
Los tableros exportados están diseñados para funcionar dentro de la misma instancia de Security Analytics. También es posible compartir los tableros personalizados con otros usuarios de la organización, siempre y cuando tengan permisos equivalentes.

Para exportar un tablero, este debe estar abierto de modo que se pueda acceder a la opción Exportar tablero del menú desplegable Editar en la barra de herramientas del tablero.

Nota: Cuando exporta el tablero Gráficas en tiempo real de Reporter, también debe exportar los gráficos utilizados en los dashlets Gráfica en tiempo real de Reports puesto que no se exportan de forma predeterminada. Cuando importa el tablero, debe importar manualmente los gráficos dependientes utilizados en el dashlet Gráfica en tiempo real de Reporter.

1. Vaya al tablero que desea exportar. Todos los tableros existentes aparecen en la **lista de selección de tableros** desplegable en el tablero mostrado actualmente.

2. Haga clic en el menú desplegable **Acciones** ( ) en la barra de herramientas del tablero y seleccione **Exportar tablero**.



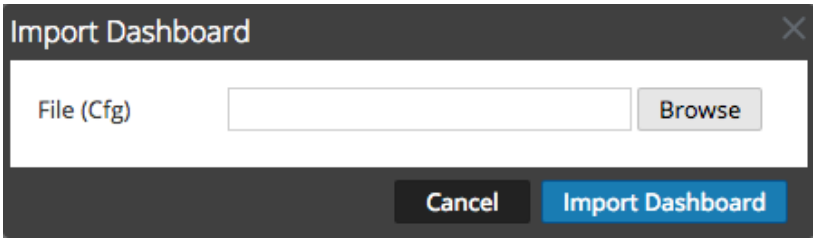
3. En la parte inferior de la pantalla aparece un mensaje de advertencia indicando que los archivos descargados pueden dañar su equipo. Si este es el tablero que desea exportar, haga clic en **Mantener**.

4. Guarde el archivo exportado en formato .cfg.

Importar un tablero

Nota: debe importar el tablero Gráficas en tiempo real de Reporter y sus gráficos relacionados en la misma instancia del servidor de Security Analytics y Reporting Engine desde donde se exportó. Debe asegurarse de que los orígenes de datos configurados para el Reporting Engine sean los mismos que en la instancia de Security Analytics desde donde se importaron. Si importa el tablero y los gráficos relacionados en otra instancia del servidor de Security Analytics, debe asegurarse de que el nombre del origen de datos esté actualizado en los gráficos.

1. En la barra de herramientas del tablero, seleccione **Importar tablero** en el menú desplegable **Acciones** ( ).



2. Navegue al archivo de tablero en el cuadro de diálogo **Importar tablero**. Solo son compatibles los archivos .cfg.
3. Haga clic en **Importar tablero**.
   El tablero se muestra en Security Analytics.

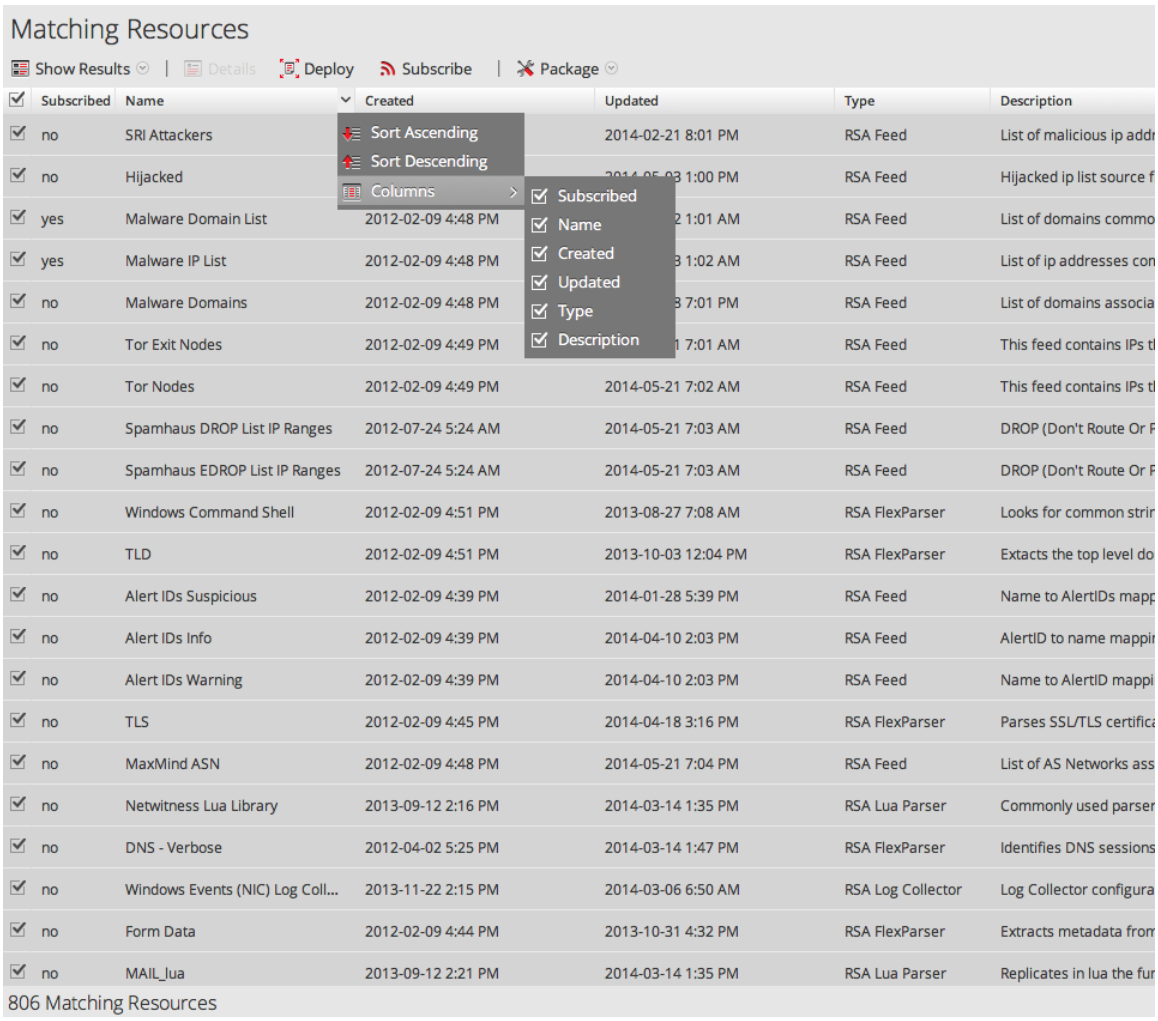
Configuración de cuadrículas

La mayor parte de la información que se muestra en los tableros y dashlets de Security Analytics se aprecia mejor en filas y columnas. A esto se lo denomina cuadrículas, y todas las cuadrículas se pueden personalizar de diversas maneras. Puede:

- Seleccionar las columnas que desea ver.
- Ordenar cada columna en forma ascendente o descendente
- Cambiar el ancho de las columnas.

El dashlet Monitor de servicios de administración tiene una función única que permite bloquear una columna en su posición en la cuadrícula dentro del dashlet, con lo cual puede desplazarse hacia la derecha sin perder de vista esa columna.

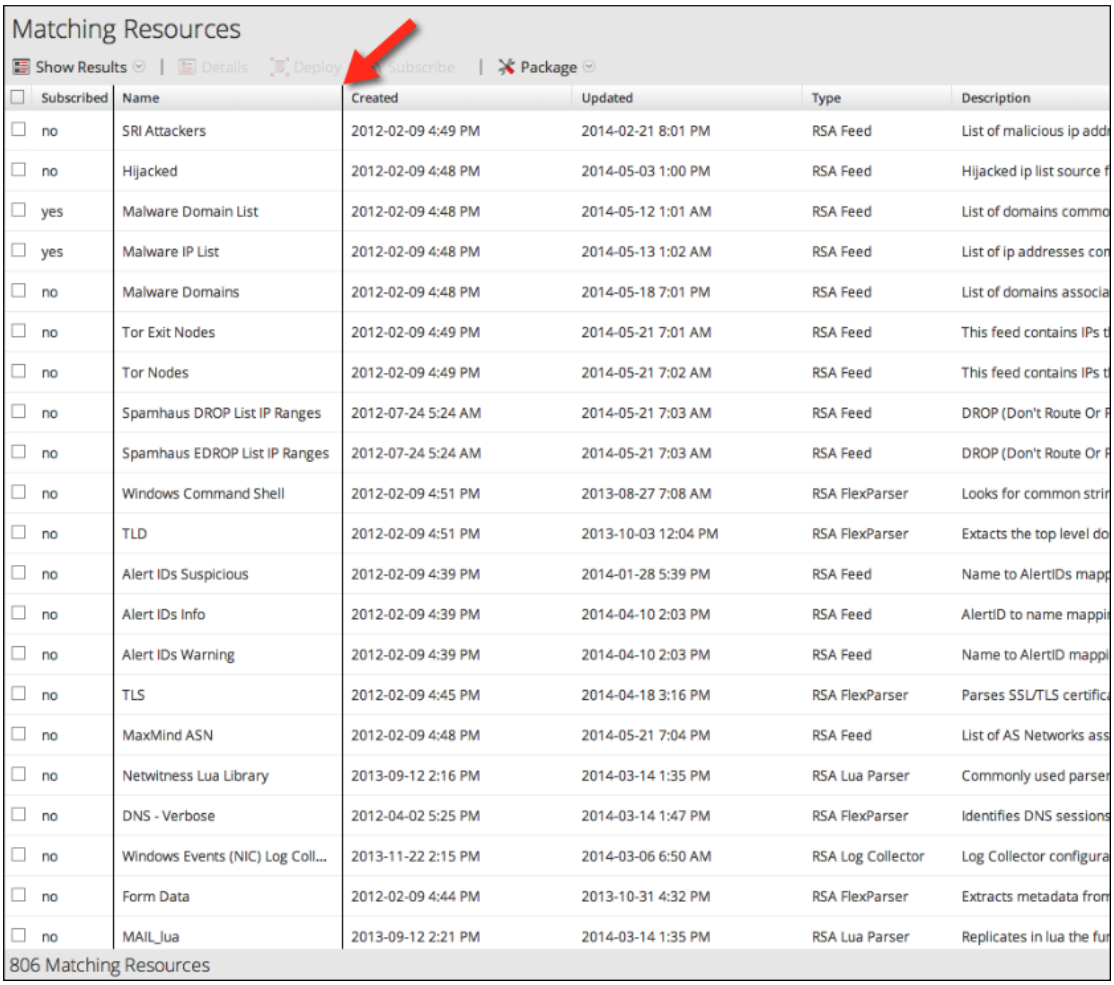
Este es un ejemplo de una cuadrícula (la cuadrícula Coincidencias de recursos de la vista Buscar en Live).



Cambiar el ancho de una columna

Puede cambiar el ancho de una columna para que las columnas sean más angostas o más anchas que su ajuste predeterminado. Por ejemplo, si una columna es demasiado angosta para mostrar todo su contenido, puede ensancharla.

1. Coloque el cursor sobre la barra de título en el borde derecho del título.
2. Cuando el cursor cambie al cursor de cambio de tamaño de la columna (una línea corta vertical con flechas apuntando hacia la derecha e izquierda), haga clic y arrastre la línea para ampliar o angostar la columna. Este es un ejemplo del cambio de tamaño de la columna Nombre en curso.



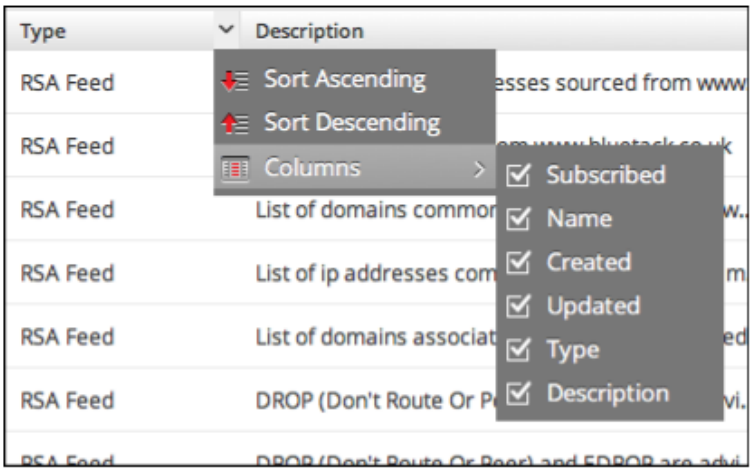
Subscribed	Name	Created	Updated	Type	Description
no	SRI Attackers	2012-02-09 4:49 PM	2014-02-21 8:01 PM	RSA Feed	List of malicious ip add
no	Hijacked	2012-02-09 4:48 PM	2014-05-03 1:00 PM	RSA Feed	Hijacked ip list source f
yes	Malware Domain List	2012-02-09 4:48 PM	2014-05-12 1:01 AM	RSA Feed	List of domains commo
yes	Malware IP List	2012-02-09 4:48 PM	2014-05-13 1:02 AM	RSA Feed	List of ip addresses cor
no	Malware Domains	2012-02-09 4:48 PM	2014-05-18 7:01 PM	RSA Feed	List of domains associa
no	Tor Exit Nodes	2012-02-09 4:49 PM	2014-05-21 7:01 AM	RSA Feed	This feed contains IPs t
no	Tor Nodes	2012-02-09 4:49 PM	2014-05-21 7:02 AM	RSA Feed	This feed contains IPs t
no	Spamhaus DROP List IP Ranges	2012-07-24 5:24 AM	2014-05-21 7:03 AM	RSA Feed	DROP (Don't Route Or F
no	Spamhaus EDROP List IP Ranges	2012-07-24 5:24 AM	2014-05-21 7:03 AM	RSA Feed	DROP (Don't Route Or F
no	Windows Command Shell	2012-02-09 4:51 PM	2013-08-27 7:08 AM	RSA FlexParser	Looks for common strin
no	TLD	2012-02-09 4:51 PM	2013-10-03 12:04 PM	RSA FlexParser	Extacts the top level do
no	Alert IDs Suspicious	2012-02-09 4:39 PM	2014-01-28 5:39 PM	RSA Feed	Name to AlertIDs mapp
no	Alert IDs Info	2012-02-09 4:39 PM	2014-04-10 2:03 PM	RSA Feed	AlertID to name mappi
no	Alert IDs Warning	2012-02-09 4:39 PM	2014-04-10 2:03 PM	RSA Feed	Name to AlertID mappi
no	TLS	2012-02-09 4:45 PM	2014-04-18 3:16 PM	RSA FlexParser	Parses SSL/TLS certifica
no	MaxMind ASN	2012-02-09 4:48 PM	2014-05-21 7:04 PM	RSA Feed	List of AS Networks ass
no	Netwitness Lua Library	2013-09-12 2:16 PM	2014-03-14 1:35 PM	RSA Lua Parser	Commonly used parser
no	DNS - Verbose	2012-04-02 5:25 PM	2014-03-14 1:47 PM	RSA FlexParser	Identifies DNS sessions
no	Windows Events (NIC) Log Coll...	2013-11-22 2:15 PM	2014-03-06 6:50 AM	RSA Log Collector	Log Collector configura
no	Form Data	2012-02-09 4:44 PM	2013-10-31 4:32 PM	RSA FlexParser	Extracts metadata from
no	MAIL_lua	2013-09-12 2:21 PM	2014-03-14 1:35 PM	RSA Lua Parser	Replicates in lua the fu

3. Cuando el ancho sea el correcto, suelte el botón del mouse.

Seleccionar las columnas que desea ver

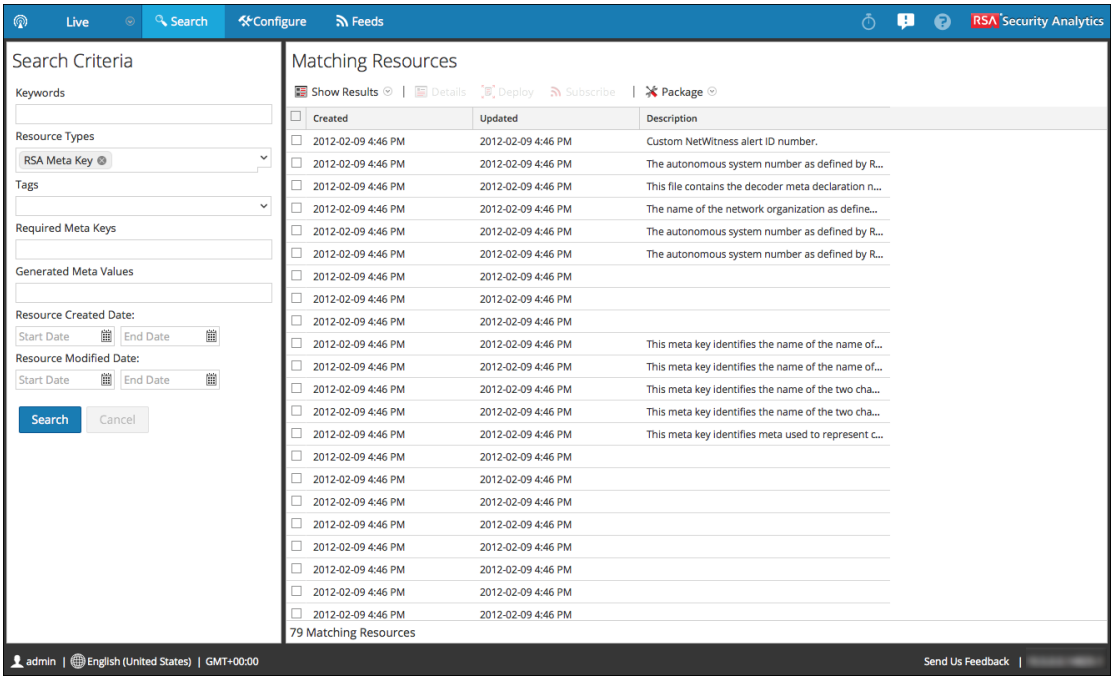
1. Coloque el cursor sobre la barra de título en el borde derecho del título.
2. Cuando el cursor cambie al ícono de lista de selección ( ), haga clic para ver la lista.
3. En la parte inferior de la lista, seleccione **Columnas**.

Se muestra una lista de columnas disponibles con una marca de verificación para cada columna incluida actualmente en la cuadrícula.



4. Seleccione un nombre de columna para seleccionarlo o deseleccionarlo.

   Cuando deselecciona un nombre de columna, esa columna se elimina de la cuadrícula. Cuando selecciona un nombre de columna, esa columna se agrega a la cuadrícula. Este es un ejemplo de la cuadrícula Coincidencias de recursos después de la deselección de varias columnas.



Organizar el contenido de una columna

Para adaptar una cuadrícula de modo que cumpla mejor su propósito, puede elegir cómo se ordena el contenido de cada una de sus columnas.

1. Coloque el cursor sobre la barra de título en el borde derecho del título.
2. Cuando el cursor cambie al ícono de lista de selección ( ), haga clic para ver el menú.

   El menú muestra una lista de las opciones de organización disponibles.
3. Seleccione una de las opciones de organización; por ejemplo, Orden ascendente u Orden descendente.

   La cuadrícula se ordena según su selección.

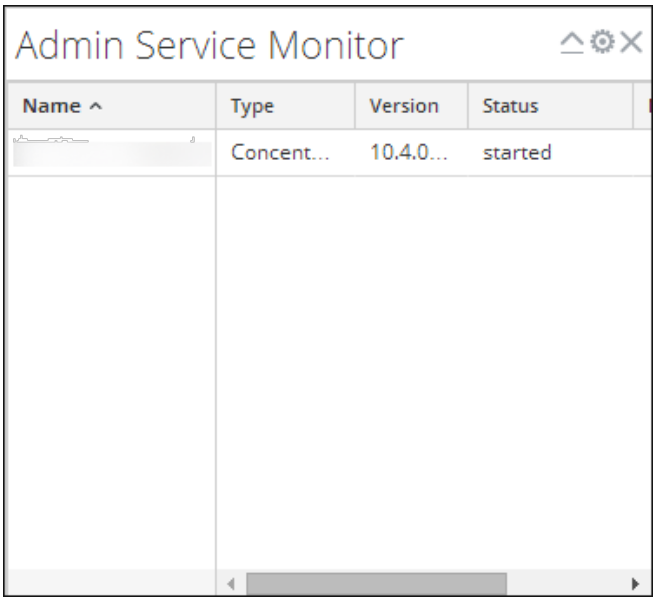
Bloquear una columna (solo el dashlet Monitor de servicios de administración)

En el dashlet Monitor de servicios de administración, la cuadrícula dentro del dashlet incluye la opción de bloquear una columna en su lugar, lo cual permite desplazarse hacia la derecha sin perder de vista esa columna.

1. Para mantener una columna en la vista durante el desplazamiento a la derecha, haga clic en el ícono del menú desplegable ( ) en el título de cualquier columna.

   Se muestra el menú contextual de la columna.
2. Seleccione **Bloquear**.

   La columna que seleccionó se mueve hacia el lado izquierdo de la cuadrícula y permanece ahí cuando otras columnas se desplazan horizontalmente. En este ejemplo, la columna Nombre se mantiene visible incluso el usuario cuando se desplaza hacia la derecha. Tenga en cuenta que parte de la columna Tipo se desplazó hacia la izquierda, pero la columna Nombre sigue en el mismo lugar.



3. Cuando desee desbloquear la columna, haga clic en el ícono del menú desplegable ( ) y seleccione **Desbloquear**.

Administración de trabajos

Inevitablemente, existen tareas, ad hoc o programadas, en Security Analytics que tardan algunos minutos en finalizar. El sistema de trabajos de Security Analytics le permite comenzar una tarea de ejecución prolongada y continuar utilizando otras partes de Security Analytics mientras el trabajo está ejecutándose. No solo puede monitorear el progreso de la tarea, sino que también puede recibir notificaciones cuando la tarea haya finalizado y si el resultado fue exitoso o falló.

Mientras esté trabajando en Security Analytics, puede abrir una vista rápida de sus trabajos desde la barra de herramientas de Security Analytics. Puede verla en cualquier momento, pero cuando el estado de un trabajo ha cambiado, el ícono de Trabajos ( ) se marca con la cantidad de trabajos en ejecución. Una vez que todos los trabajos se han completado, el número desaparece.

También puede ver los trabajos en estas dos vistas.

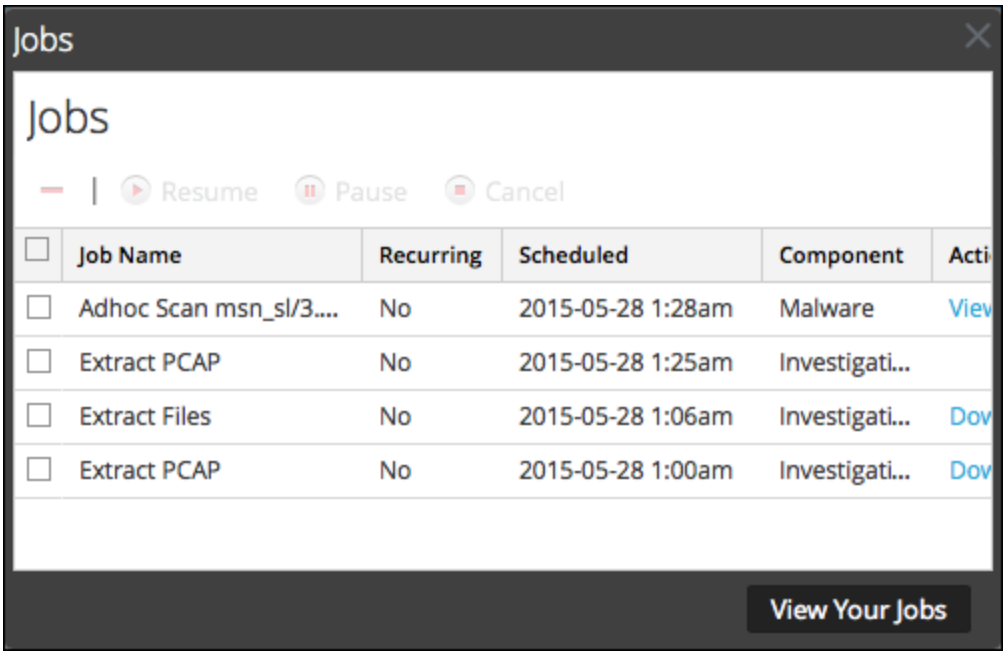
- En la vista Perfil, puede ver los mismos trabajos en un panel completo. Estos son trabajos solamente.
- En la vista Sistema, los usuarios con privilegios administrativos pueden ver y administrar todos los trabajos de todos los usuarios en un único panel de trabajos.

La estructura del panel de trabajos es igual en todas las vistas.

Mostrar la Bandeja de trabajos

En la barra de herramientas de **Security Analytics**, haga clic en el ícono Trabajos: .

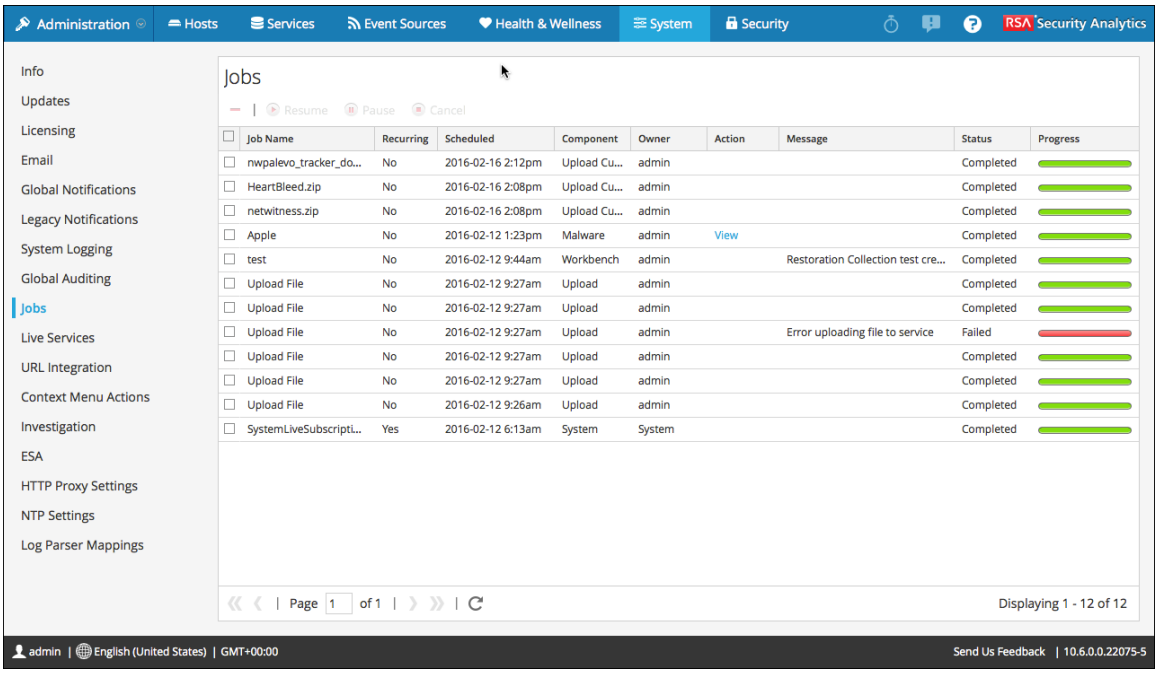
Se muestra la Bandeja de trabajos.



La Bandeja de trabajos muestra todos sus trabajos, recurrentes y no recurrentes, utilizando un subconjunto de las columnas disponibles en el panel Trabajos. Por lo demás, la Bandeja de trabajos y la vista Perfil > panel Trabajos son lo mismo. En la vista Sistema de Administration, el panel Trabajos muestra información acerca de todos los trabajos de Security Analytics de todos los usuarios.

Ver los trabajos en la vista Perfil > panel Trabajos

Para ver una vista más grande de sus trabajos, haga clic en **Ver sus trabajos**.
Se muestra la vista Perfil > panel Trabajos.



Pausar y reanudar ejecución programada de un trabajo recurrente

Las opciones Pausar y Reanudar se aplican solo a los trabajos recurrentes. Sin embargo, cuando pausa un trabajo recurrente que está en ejecución, la ejecución no se ve afectada. La próxima ejecución (si se asume que el trabajo sigue en pausa) se omite.

1. Para detener la próxima ejecución de un trabajo recurrente, en cualquier panel **Trabajos**, seleccione el trabajo y haga clic en **Pausar**.

   La siguiente ejecución del trabajo se omite y el programa se mantiene en pausa hasta que se hace clic en Reanudar.

2. Para reiniciar la ejecución de trabajos recurrentes en pausa, seleccione el trabajo y haga clic en **Reanudar**.

   La siguiente ejecución del trabajo se realiza según lo calendarizado y el calendario para el trabajo se reanuda.

Cancelar un trabajo

Para cancelar trabajos que estén en ejecución o en línea de espera para ejecutarse:

1. En la **Bandeja de trabajos** o en el panel **Trabajos**, seleccione uno o más trabajos.
2. Haga clic en **Cancelar**.

   Se muestra un cuadro de diálogo de confirmación.

3. Haga clic en **Sí**.

   Los trabajos se cancelan y las entradas permanecen en la cuadrícula con un estado de **cancelado**.

   Si cancela un trabajo recurrente, se cancela esa ejecución del trabajo. La próxima vez que el trabajo se programe para ejecución, se ejecutará de manera normal.

Eliminar un trabajo

Precaución: Cuando elimina un trabajo, el trabajo se elimina de forma instantánea de la cuadrícula. No aparece un diálogo de confirmación. Si elimina un trabajo recurrente, también se eliminan todas las ejecuciones futuras.

Los usuarios pueden eliminar sus propios trabajos antes, durante o después de la ejecución. Los usuarios con la función ADMIN pueden eliminar cualquier trabajo. Para eliminar trabajos:

1. Seleccione uno o más trabajos.
2. Haga clic en **Eliminar**.
3. Los trabajos se eliminan de la cuadrícula.

Descargar un trabajo

Cuando un trabajo tiene el estado Descargar en la columna Acción, puede descargar el resultado del trabajo. Si está trabajando en el módulo Investigation y extrae los datos de paquete para una sesión como un archivo PCAP o extrae los archivos de carga (por ejemplo, documentos de Word e imágenes) de una sesión, se crea un archivo. Para descargar el archivo a su sistema local, haga clic en **Descargar**.

Visualización y eliminación de notificaciones

Mientras trabaja en Security Analytics, puede ver las notificaciones recientes del sistema sin salir del módulo en el cual está trabajando. Puede abrir una vista rápida de las notificaciones en la barra de herramientas de Security Analytics. Puede verla en cualquier momento, pero cuando recibe una notificación nueva, se marca el ícono Notificaciones.

Algunos ejemplos de notificaciones son:

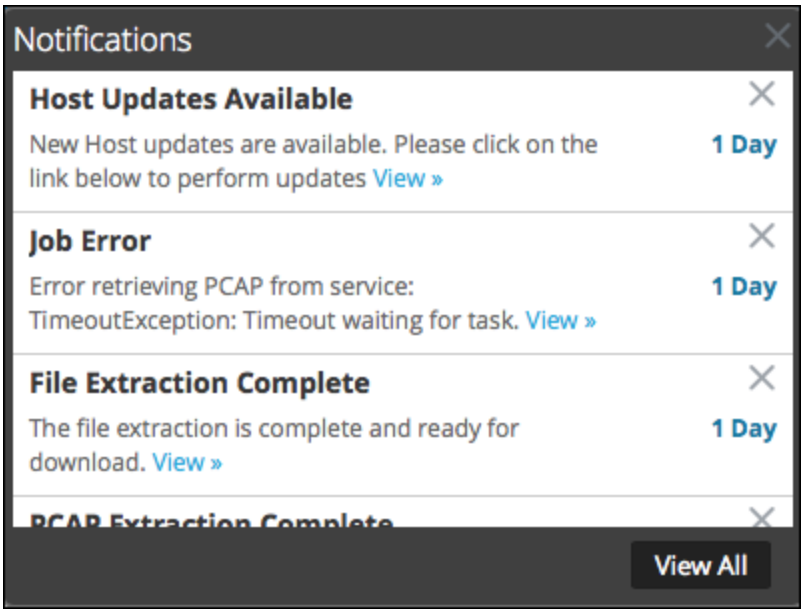
- Se completó una actualización del host.
- Una migración de analizador a decodificador que se ha completado.
- Hay disponible una versión de software más reciente.

En estas dos vistas, puede ver todas las notificaciones en un panel Notificaciones completo.

- En la vista Perfil, puede ver solo sus notificaciones.
- En la vista Sistema, los usuarios con privilegios administrativos pueden ver y administrar todas las notificaciones de todos los usuarios en un único panel.

Ver notificaciones

Para visualizar la bandeja Notificaciones, en la barra de herramientas de Security Analytics, haga clic en el ícono Notificaciones ().



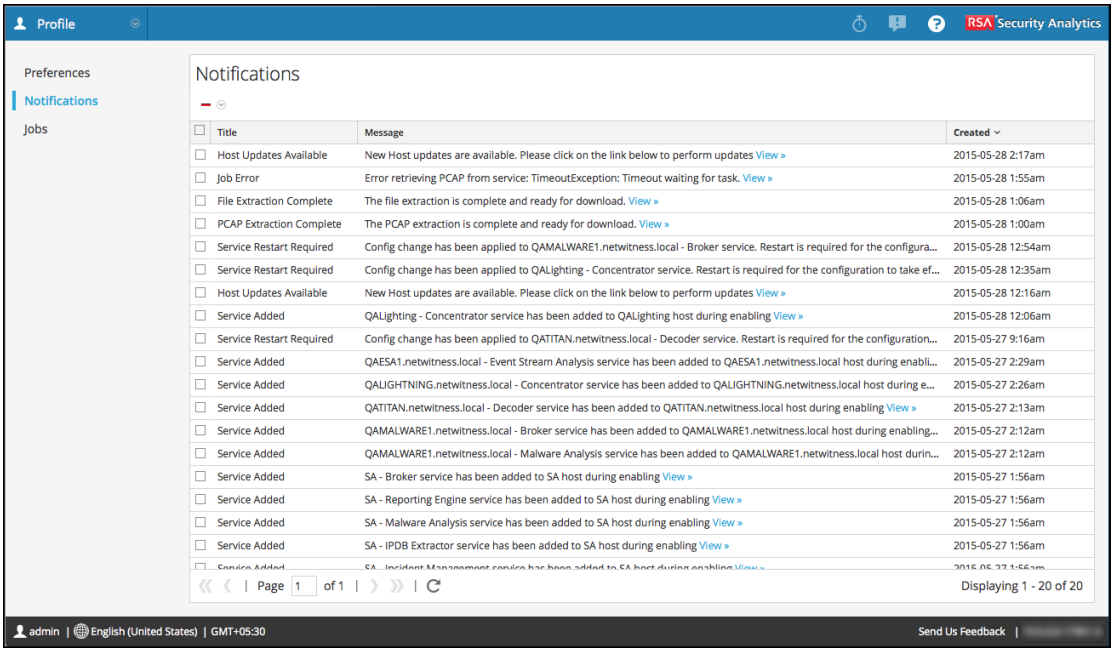
Ver todas las notificaciones

Para ver todas las notificaciones, realice una de las siguientes acciones:

1. En el menú de **Security Analytics**, seleccione **Perfil** y, a continuación, en el panel de opciones de la vista Perfil, seleccione **Notificaciones**.
2. En el menú de **Security Analytics**, seleccione **Administration > Sistema** y, a continuación, en el panel de opciones de la vista Sistema, seleccione **Notificaciones**.
3. En la barra de herramientas de **Security Analytics**, haga clic en para abrir la bandeja Notificaciones y, a continuación, haga clic en **Ver todo** en esta bandeja.

   Se muestra el panel Notificaciones. Aquí aparecen todas las notificaciones y el formato es

diferente al formato de la Bandeja de notificaciones.



Eliminar registros de notificaciones

Para eliminar registros de notificaciones:

1. En la cuadrícula **Notificaciones de perfil**, seleccione las notificaciones que desea eliminar.
2. Haga clic en Delete .

   Las notificaciones seleccionadas se eliminan de esta cuadrícula y de la Bandeja de notificaciones.

Referencias

La interfaz del usuario de Security Analytics incluye funciones como las siguientes:

- La vista Perfiles
- La bandeja de trabajos
- La bandeja de notificaciones
- Ventanas del navegador
- Tableros
- Menús contextuales
- Cuadrículas
- Dashlets

Esta sección incluye un ejemplo de cada una de ellas. Los ejemplos de los dashlets pueden resultarle útiles cuando debe decidir cómo personalizar los tableros.

Panel Trabajos y Bandeja de trabajos

Varios módulos de Security Analytics inician trabajos; por ejemplo, el módulo Live puede descargar recursos de CMS, el módulo Administration puede cargar un feed en un servicio y el módulo Investigation puede analizar y reconstruir paquetes en archivos de captura de paquetes.

En la vista Sistema de Administration, los usuarios del grupo ADMIN pueden administrar todos los trabajos de Security Analytics en el panel Trabajos. Otros usuarios no administrativos pueden ver sus propios trabajos en la vista Perfil.

Además, mientras esté trabajando en Security Analytics, puede abrir una vista rápida de los trabajos desde la barra de herramientas. Cuando el estado de un trabajo ha cambiado, el ícono de Trabajos () se marca con la cantidad de trabajos en ejecución. Una vez que todos los trabajos se han completado, el número desaparece.

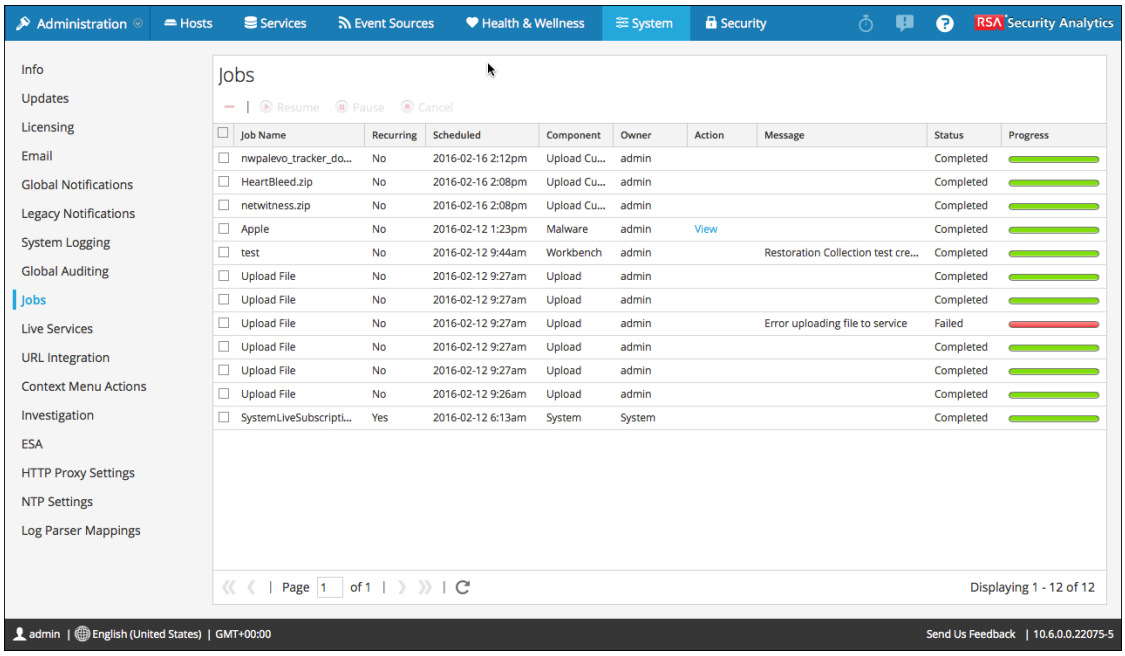
En el panel Trabajos, puede:

- Ver y ordenar los trabajos
- Pausar o reanudar un trabajo
- Cancelar un trabajo
- Eliminar un trabajo
- Descargar un trabajo

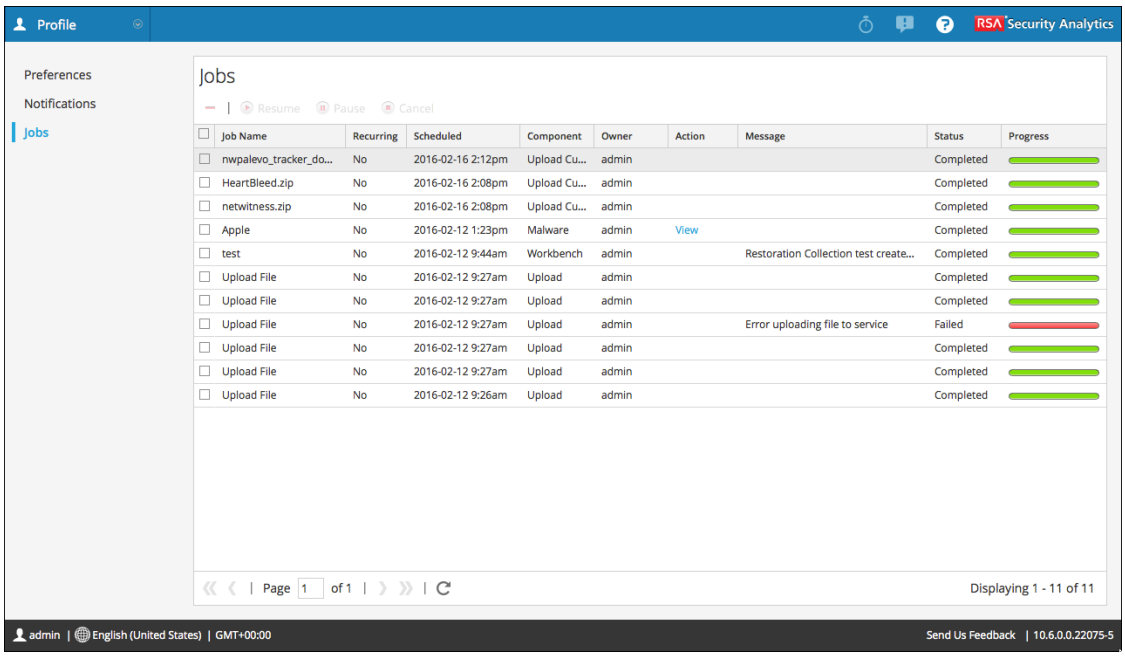
La estructura del panel de trabajos es igual en todas las vistas. Los procedimientos asociados con el panel Trabajos y la Bandeja de trabajos se describen en Administración de trabajos.

Para acceder al panel Trabajos, realice una de las siguientes acciones:

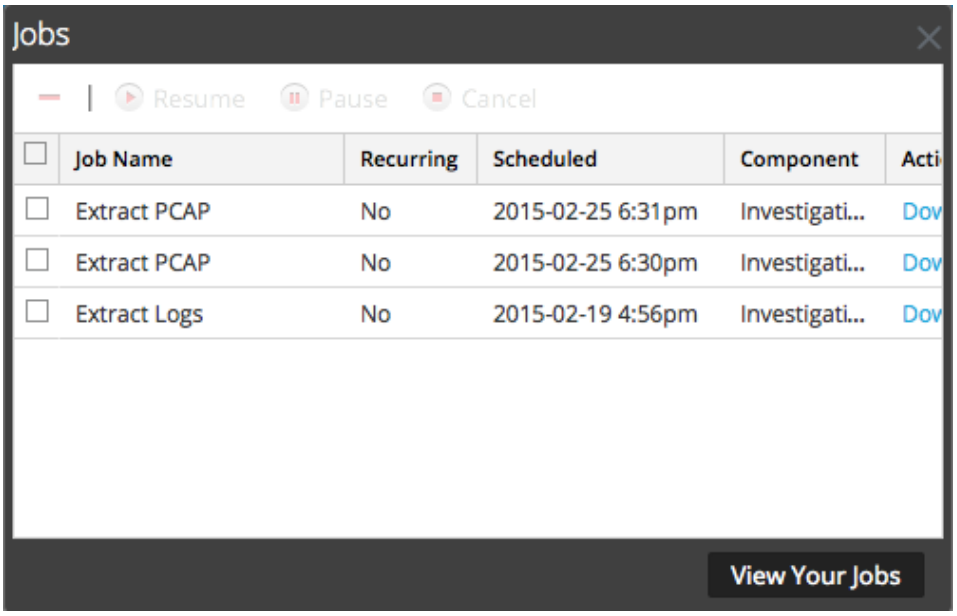
- En el menú de **Security Analytics**, seleccione **Administration > Sistema**, y en el panel de opciones, seleccione **Trabajos**.



- En el menú de **Security Analytics**, seleccione **Perfil**, y en el panel de opciones, seleccione **Trabajos**.



Para ver la Bandeja de trabajos, en la barra de herramientas de Security Analytics, haga clic en el ícono **Trabajos**  .



El panel Trabajos organiza la información acerca de los trabajos en una cuadrícula. Las columnas presentan una barra de progreso del trabajo, el nombre del trabajo, una indicación de que el trabajo es recurrente o no recurrente, el módulo de Security Analytics que está controlando el trabajo, el propietario del trabajo, el estado, cualquier mensaje asociado y un botón de descarga que permite descargar archivos de captura de paquete o archivos de carga.

Características

La Bandeja de trabajos muestra todos sus trabajos, recurrentes y no recurrentes, mediante un subconjunto de las columnas disponibles en el panel **Trabajos**. Por lo demás, la Bandeja de trabajos y la vista Perfil > panel Trabajos son lo mismo. En la vista Sistema de Administration, el panel Trabajos muestra información acerca de todos los trabajos de Security Analytics de todos los usuarios.

En esta tabla se enumeran las opciones de la barra de herramientas del panel Trabajos.

Característica	Descripción
Resume	La opción Reanudar se aplica solo a los trabajos recurrentes que están en pausa. Cuando reanuda un trabajo pausado, la próxima ejecución del trabajo se ejecuta como calendarizada.
Pause	La opción Pausar se aplica solamente a los trabajos recurrentes. Cuando pausa un trabajo recurrente que está en ejecución, la ejecución no se ve afectada. La próxima ejecución (si se asume que el trabajo sigue en pausa) se omite.

Característica	Descripción
	Cancela un trabajo recurrente o no recurrente. Puede cancelar un trabajo mientras está en ejecución. Si cancela un trabajo recurrente, se cancela esa ejecución del trabajo. La próxima vez que el trabajo se calendarice para ejecución, se ejecutará de manera normal.
	Elimina un trabajo recurrente o no recurrente del panel **Trabajos**. Cuando elimina un trabajo, este se elimina instantáneamente del panel Trabajos. No aparece un diálogo de confirmación. Si elimina un trabajo recurrente, también se eliminan todas las ejecuciones futuras.

Esta tabla describe las funcionalidades de la Bandeja de trabajos y el panel Trabajos.

Característica	Descripción
Cuadro de selección	Haga clic en este cuadro para seleccionar uno o más trabajos.
Progreso	Muestra el porcentaje completado de un trabajo.
Nombre del trabajo	Muestra el nombre del trabajo; por ejemplo, **Extraer archivos** o **Actualizar servicio**.
Recurrente	Indica si el trabajo es recurrente o no recurrente. **Sí** = recurrente, **No** = no recurrente.
Componente	Indica el componente en el cual se originó el trabajo; por ejemplo, **Investigation** o **Administration**.
Propietario	Indica el propietario del trabajo. El propietario del trabajo no está incluido en la **Bandeja de trabajos** predeterminada, ya que solo se muestran aquí los trabajos del usuario actual. La columna está disponible para agregarla.
Status	Indica el estado del trabajo. Los valores comunes para el estado son **En pausa**, **En ejecución**, **Cancelado**, **Fallido**, **Completado**, mientras que también es posible tener otros valores de estado.

Característica	Descripción
Mensaje	Muestra información adicional sobre el trabajo; por ejemplo, **Extracción de archivos** o **No se encontraron sesiones**.
Acción	Visualiza trabajos en las vistas Investigation y Malware Analysis, o descarga archivos de trabajos para el trabajo en el directorio **Descargas** predeterminado del sistema local. Solo los trabajos completados correctamente tienen el vínculo **Ver** en la columna **Acción**. Solo los trabajos que crean un archivo tienen el vínculo **Descargar** en la columna **Acción**.
Ver sus trabajos	Muestra trabajos en la **vista Perfil > panel Trabajos**.
Programado	Indica la fecha y hora en la que se calendarizó el inicio del trabajo.

Panel Notificaciones y Bandeja de notificaciones

Security Analytics proporciona notificaciones del sistema para informar a los usuarios acerca de ciertas acciones o condiciones.

- Se completó una actualización del host.
- Una migración de analizador a decodificador que se ha completado.
- Un servicio quedó inactivo (registro crítico de un tipo específico).
- Finalizó una visualización.
- Finalizó un informe.
- Hay disponible una versión de software más reciente.

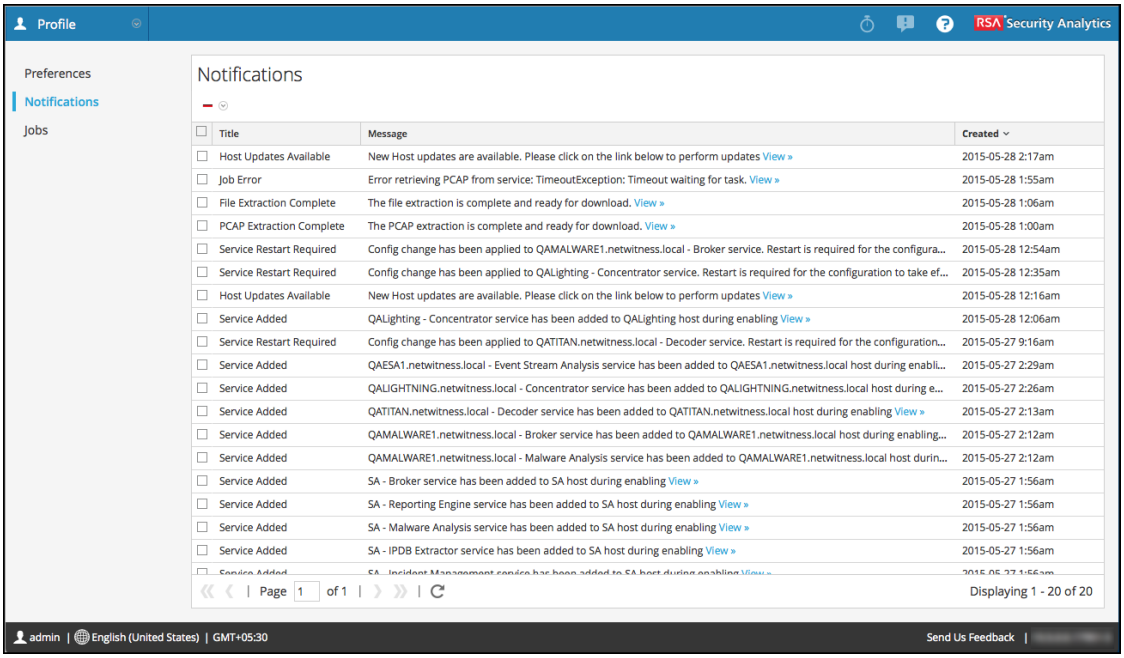
Mientras trabaja en Security Analytics, puede ver las notificaciones recientes del sistema sin salir del módulo en el cual está trabajando. Puede abrir una vista rápida de las notificaciones en la barra de herramientas de Security Analytics. Puede verla en cualquier momento, pero cuando recibe una notificación nueva, se marca el ícono Notificaciones.

Cuando vea notificaciones en la Bandeja de notificaciones, solo aparecerán las notificaciones recientes. Puede ver todas las notificaciones en un formato de cuadrícula en la vista Perfil o en la vista Sistema. Los procedimientos para ver notificaciones se presentan en Visualización y eliminación de notificaciones.

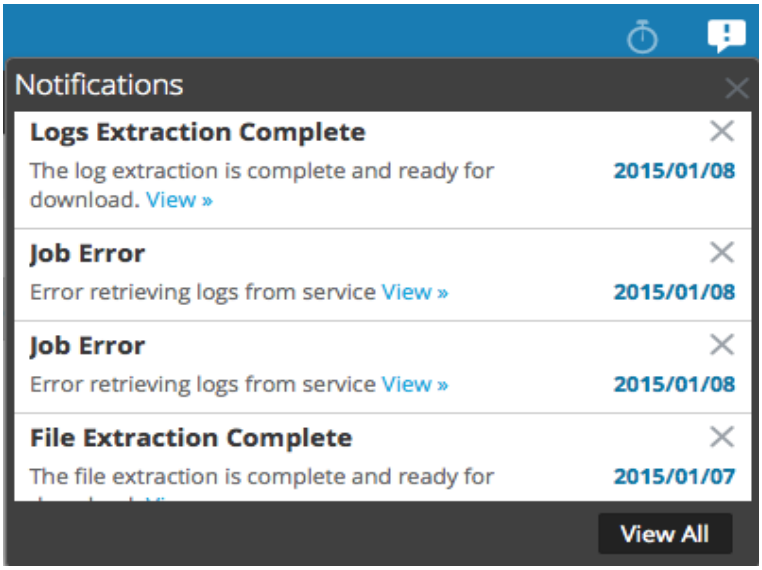
Para acceder al panel Notificaciones, realice una de las siguientes acciones:

- En el menú de **Security Analytics**, seleccione **Perfil** y, a continuación, en el panel de opciones de la vista Perfil, seleccione **Notificaciones.**

- En el menú de **Security Analytics**, seleccione Administration > Sistema y, a continuación, en el panel de opciones de la vista Sistema, seleccione **Notificaciones.**



- En la barra de herramientas de **Security Analytics**, haga clic en  y, a continuación, haga clic en **Ver todo** en la Bandeja de notificaciones.



Características

El panel Notificaciones y la bandeja tienen una barra de herramientas y una cuadrícula. La Bandeja de notificaciones es un subconjunto de la información que se presenta en el panel Notificaciones. En la siguiente tabla se describen las funciones del panel Notificaciones.

Característica	Descripción
	Muestra un menú desplegable que permite eliminar los registros de notificación seleccionados o todos los registros de notificación en la cuadrícula **Notificaciones** y en la Bandeja de notificaciones.
Título	El título de la notificación, por ejemplo, **Extracción de archivo completa**.
Mensaje	Todo el mensaje, por ejemplo, **La extracción de archivo está completa y lista para descarga.**
Ver	Algunos mensajes incluyen un vínculo que muestra una vista en la que puede tomar medidas. Por ejemplo, si hay un archivo para descargar, cuando se hace clic en este vínculo, se abre el panel Trabajos que muestra la vista donde puede descargar el archivo.
Created	La fecha y la hora en que se creó la notificación. En la bandeja Notificaciones, esta columna es la cantidad de días desde que se creó la notificación.
Ver todo	Muestra la cuadrícula de notificaciones de la vista Perfil.

Vista Perfil > panel Preferencias

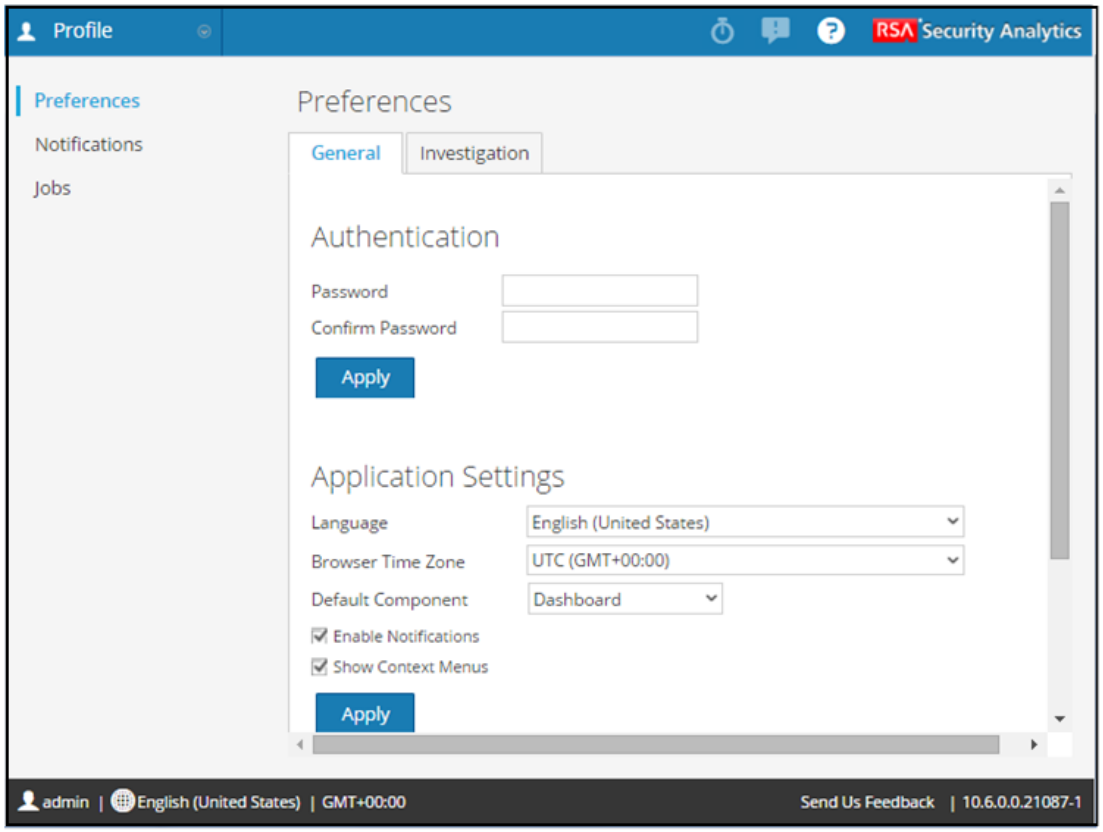
Los usuarios pueden establecer diversas preferencias que tienen prioridad sobre las preferencias del sistema que establece el administrador del sistema. Entre estas se incluyen:

- Preferencias generales para Security Analytics y ajustes para la aplicación Security Analytics en conjunto (se describe más abajo)
- Preferencias que se aplican a Investigation y que pueden afectar las vistas iniciales y el tiempo de carga
- Preferencias que se aplican a Reporter.

Para acceder a este panel:

1. En el menú de **Security Analytics**, seleccione **Perfil**.
2. En el panel de opciones de la vista **Perfil**, seleccione **Preferencias**.

   El panel se muestra con la pestaña General seleccionada.



Características

El panel Preferencias > pestaña General tiene dos secciones: autenticación y configuración de aplicación.

Autenticación

En la siguiente tabla se describen las opciones de la sección Autenticación. El procedimiento relacionado se describe en Cambio de la contraseña.

Característica	Descripción
Contraseña y Confirmar contraseña	La contraseña debe tener al menos ocho caracteres y puede incluir letras mayúsculas y minúsculas, números, caracteres especiales y espacios.
Aplicar	Actualiza el perfil de usuario con la nueva contraseña. La nueva contraseña entra en vigor inmediatamente y se solicita la próxima vez que inicia sesión en Security Analytics. El cambio de contraseña se aplica al inicio de sesión en el sistema y en todos los servicios de Security Analytics en los cuales se agregó la cuenta.

Configuración de aplicación

En la siguiente tabla se describen las opciones de la sección Configuración de aplicación. Los procedimientos relacionados se describen en Configuración de las preferencias de la aplicación.

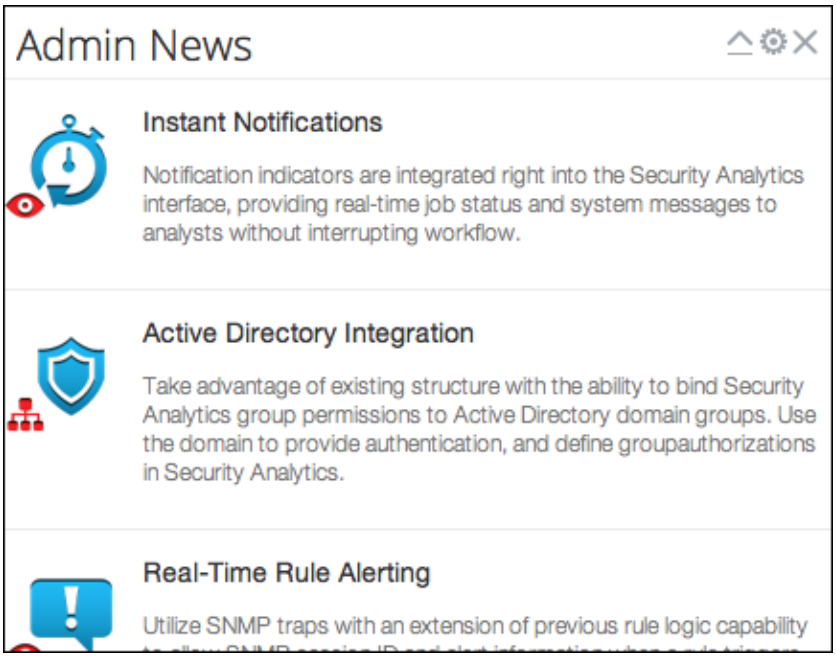
Característica	Descripción
Idioma	Muestra una lista desplegable de idiomas disponibles para usar en Security Analytics.
Zona horaria del navegador	Muestra una lista desplegable de zonas horarias disponibles para usar en Security Analytics.
Componente predeterminado	Este campo tiene una lista desplegable para seleccionar el componente que actúa como la vista inicial cuando inicia sesión en Security Analytics.

Característica	Descripción
Habilitar notificaciones	Esta casilla de verificación activa o desactiva notificaciones para su cuenta de usuario. De manera predeterminada, las notificaciones del sistema de Security Analytics se habilitan cuando se crea una cuenta de usuario nueva.
Mostrar menús contextuales	Esta casilla de verificación activa o desactiva menús contextuales para su cuenta de usuario. De manera predeterminada, los menús contextuales de Security Analytics se habilitan cuando se crea una nueva cuenta de usuario. Los menús contextuales proporcionan funciones adicionales para vistas específicas cuando hace clic con el botón secundario en una vista.
Aplicar	Actualiza la configuración de la aplicación y los cambios se aplican de inmediato.

Dashlet Novedades de administración

Este dashlet presenta información del producto y actualizaciones para el módulo Administration.

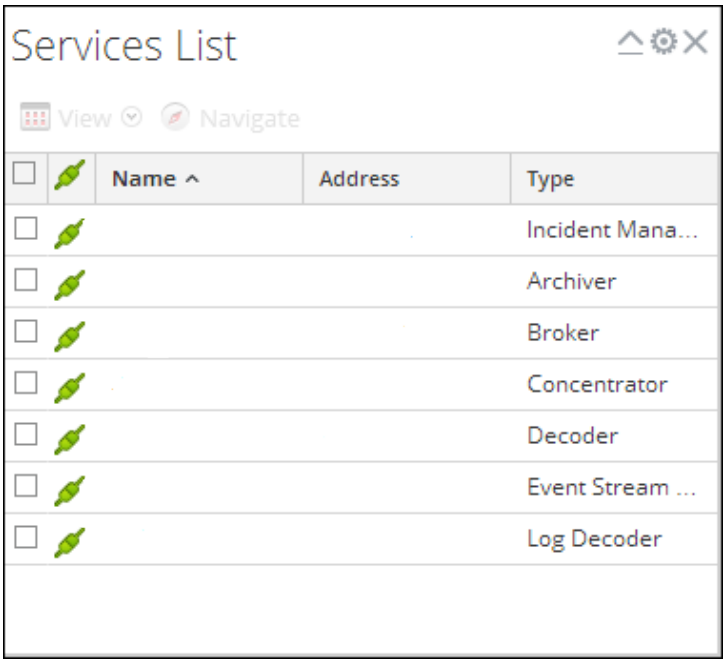
Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, seleccione  > **Agregar un dashlet** en la barra de herramientas del tablero y elija **Novedades de administración**.



Dashlet Lista de servicios de administración

El dashlet Lista de servicios de Administration es una lista de servicios disponibles en Security Analytics con vínculos a tareas administrativas que se pueden realizar en esos servicios. De hecho, este dashlet es un subconjunto centrado de la**Vista Hosts de Administration** (consulte el tema en la *Guía de introducción de hosts y servicios*.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, seleccione > **Agregar dashlet** en la barra de herramientas del tablero y elija **Lista de servicios de administración**.



Características

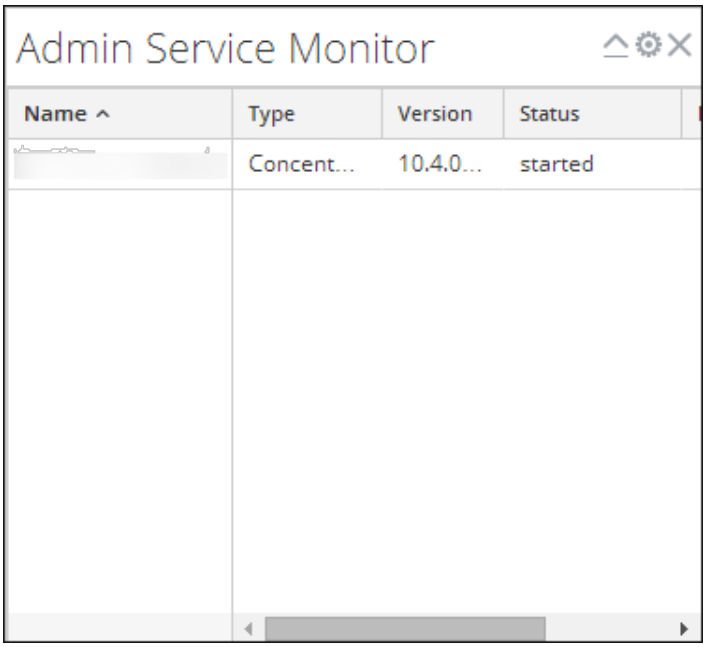
- La opción ( ) del menú Ver es un enlace rápido al menú Ver de la vista Servicios de Administration. Seleccione un servicio y haga clic aquí para seleccionar una vista.
- La opción Navegar es un enlace rápido a la vista Navegar del módulo Investigation.
- La cuadrícula Servicios tiene un subconjunto de las columnas de la cuadrícula de la vista Hosts de Administration. En la siguiente tabla se proporcionan descripciones de las columnas que se presentan en el dashlet

Columna	Descripción
	Casilla de verificación de selección. Haga clic en el encabezado para seleccionar o deseleccionar todos los servicios en la lista.
Connection Status  	Los íconos de conexión indican si la conexión al servicio es buena (verde) o mala (rojo y gris). Si la fila completa aparece en texto rojo, también indica un mal estado de conexión.
Nombre	El nombre del servicio; por ejemplo, **HQ-Decoder** o **10.26.22.44-Decoder**.
Dirección	La dirección IP del servicio de NextGen; por ejemplo, **10.26.22.44**.
Tipo	Tipo de servicio. Los posibles valores son Broker, Concentrator, Decoder, Log Decoder, Log Collector, Archiver, Workbench, Warehouse Collector, Event Stream Analysis, IPDB Extractor, Reporting Engine, Malware Analysis e Incident Management.

Dashlet Monitor de servicios de administración

El dashlet Monitor de servicios de administración resume la versión del servicio y la información de estado que aparece en la vista Servicios de Administration. Este es un subconjunto de las columnas de la vista Hosts.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Monitor de servicios de administración**. El cuadro de diálogo Agregar un dashlet incluye una opción para seleccionar el tipo de servicio para el nuevo dashlet.



Características

Este dashlet incluye este subconjunto de las columnas de la vista **Hosts**:

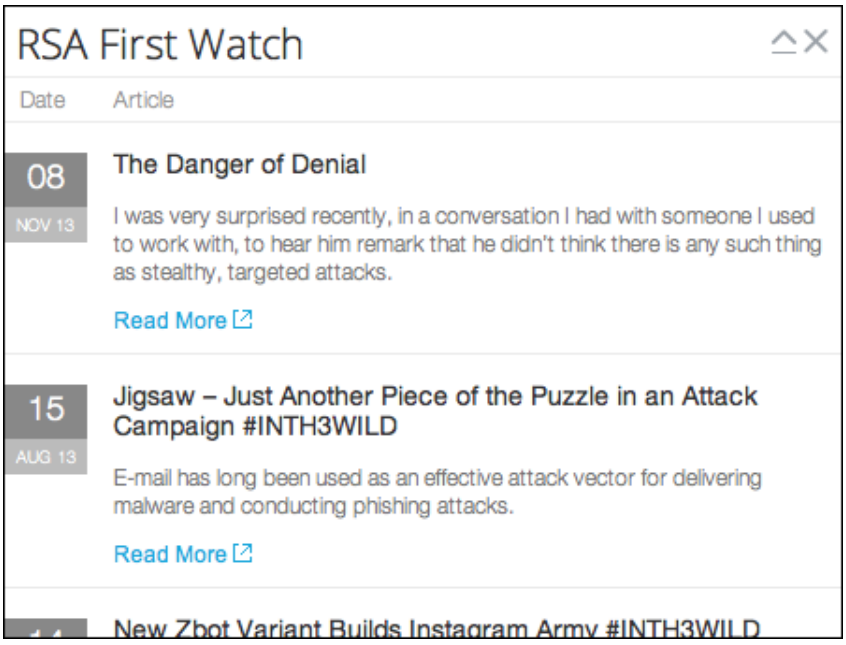
- Nombre
- Tipo
- Versión
- Status
- Uso de la memoria
- CPU

Para obtener más detalles acerca de la **vista Hosts**, consulte la *Guía de introducción de hosts y servicios*.

Dashlet RSA First Watch de Dashboard

El dashlet Dashboard RSA First Watch proporciona reconocimiento de la situación e inteligencia de amenazas de toda la comunidad de investigación de RSA y de respuesta a incidentes. Proporciona a los clientes la inteligencia para prepararse, responder y mitigar amenazas informáticas avanzadas. Los equipos de RSA First Watch, Respuesta a incidentes y Centro de respuesta ante incidentes computacionales (CIRC) rastrean millones de direcciones IP y dominios, así como docenas de orígenes de amenazas únicas y actores de amenazas.

Para mostrar este dashlet en el tablero Unified o como parte de un tablero personalizado, haga clic en  > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Dashboard RSA First Watch**.



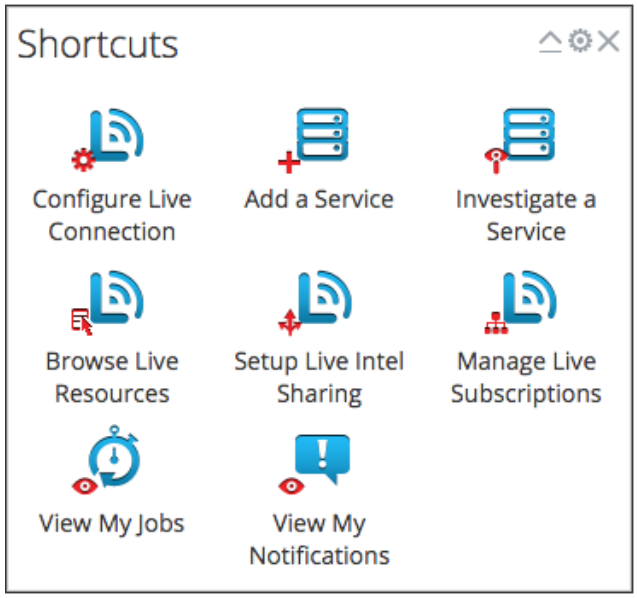
Características

Columna	Descripción
Fecha	La fecha en que se publicó el artículo.
Artículo	El título del artículo, una muestra del artículo y un vínculo “Lea más” al artículo completo.

Dashlet Accesos directos de Dashboard

El dashlet Accesos directos de Dashboard ofrece enlaces rápidos a tareas comunes en otras áreas de Security Analytics. Es una buena herramienta para usuarios principiantes que están intentando familiarizarse con el sistema.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en  > **Agregar dashlet** en la barra de herramientas del tablero y seleccione el dashlet **Accesos directos de Dashboard**.



Características

Además de los controles de dashlet estándar, este dashlet tiene opciones que se vinculan a tareas comunes de Security Analytics.

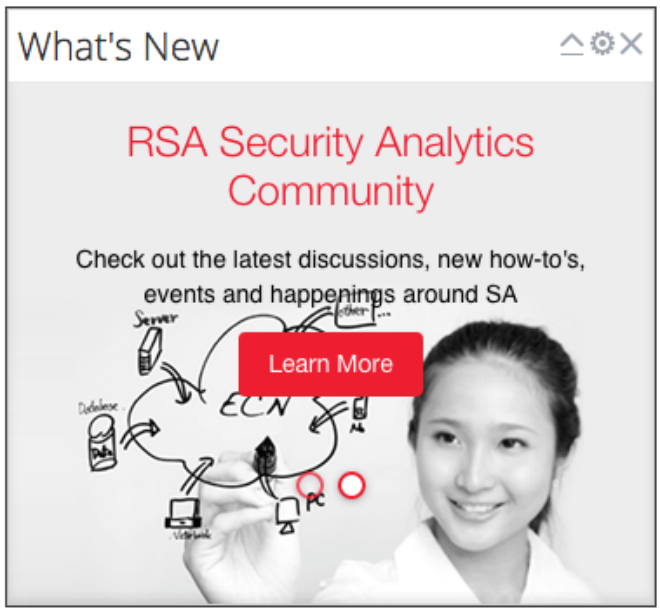
Opción	Descripción
Configurar conexión de Live	Establece un vínculo a la vista Sistema de Administration >panel Configuración de Live, donde puede configurar la conexión con el sistema de administración de contenido de Live.
Agregar un servicio	Establece un vínculo a la vista Servicios.

Opción	Descripción
Investigar un servicio	Establece un vínculo a la pestaña Navegar de la vista Navegar, donde puede seleccionar un servicio para navegar desde una lista de servicios disponibles.
Navegar en recursos de Live	Establece un vínculo a la vista Buscar en Live, donde puede buscar recursos en la biblioteca de recursos de Live.
Configurar Live Intelligence Sharing	Establece un vínculo a la vista Sistema de Administration, donde puede optar por participar en el uso compartido de inteligencia de Live.
Administrar suscripciones de Live	Establece un vínculo a la vista Configurar de Live, donde puede ver y editar suscripciones e implementaciones.
Ver Mis trabajos	Establece un vínculo al panel Trabajos (vista Perfil), donde puede ver trabajos de Security Analytics.
Ver Mis notificaciones	Establece un vínculo al panel Notificaciones (vista Perfil), donde puede ver notificaciones del sistema.

Dashlet Novedades de Dashboard

El dashlet Novedades de Dashboard muestra los anuncios y la información de los productos más recientes para todos los productos de Security Analytics.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en  > **Agregar dashlet** en la barra de herramientas del tablero y seleccione el dashlet **Novedades de Dashboard**.

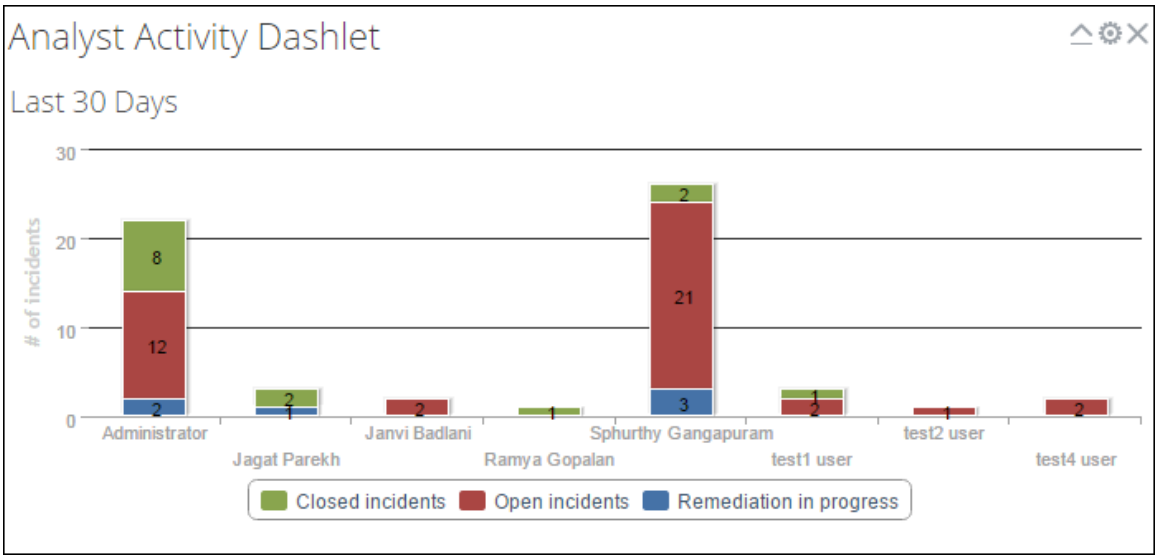


Dashlet Actividad de analistas de incidentes

El dashlet Actividad de analista de incidentes muestra la cantidad y el estado de los incidentes por analista en un rango de tiempo. Muestra tres categorías:

- Incidentes cerrados
- Incidentes abiertos
- Corrección en curso

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en > **Agregar dashlet** en la barra de herramientas del tablero. Seleccione **Actividad de analistas de incidentes** en el menú desplegable y configure un rango de tiempo para la actividad.



Nota: Cuando contrae el dashlet con la opción , las barras tardan cierto tiempo en volver a mostrarse. Puede actualizar el navegador para ver el gráfico rápidamente.

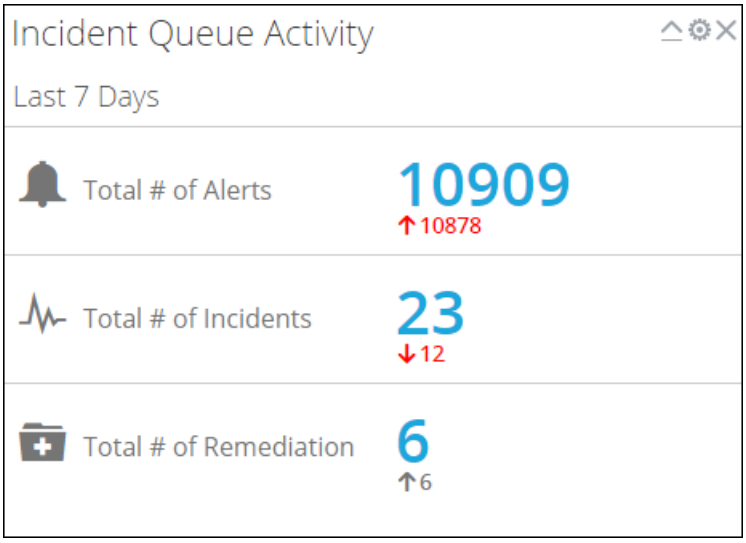
Característica	Descripción
Gráfico de barras	Cuando coloca el cursor del mouse sobre una parte del gráfico de barras, la cantidad y el estado de los incidentes se muestran como texto.
Categorías de incidentes	En la leyenda de la parte inferior se muestran las categorías de incidentes. Cuando hace clic en una categoría, esta se elimina del gráfico. Si vuelve a hacer clic en la categoría, esta se muestra nuevamente en el gráfico.

Dashlet Actividad de la línea de espera de incidentes

El dashlet Actividad de la línea de espera de incidentes muestra la cantidad total de alertas, incidentes y tareas de corrección para un rango de tiempo seleccionado.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Actividad de la línea de espera de incidentes**. En el cuadro de diálogo Agregar un dashlet, ingrese un título para el dashlet y seleccione un rango de tiempo para los resultados.

La siguiente figura es un ejemplo del dashlet con información de los últimos siete días.

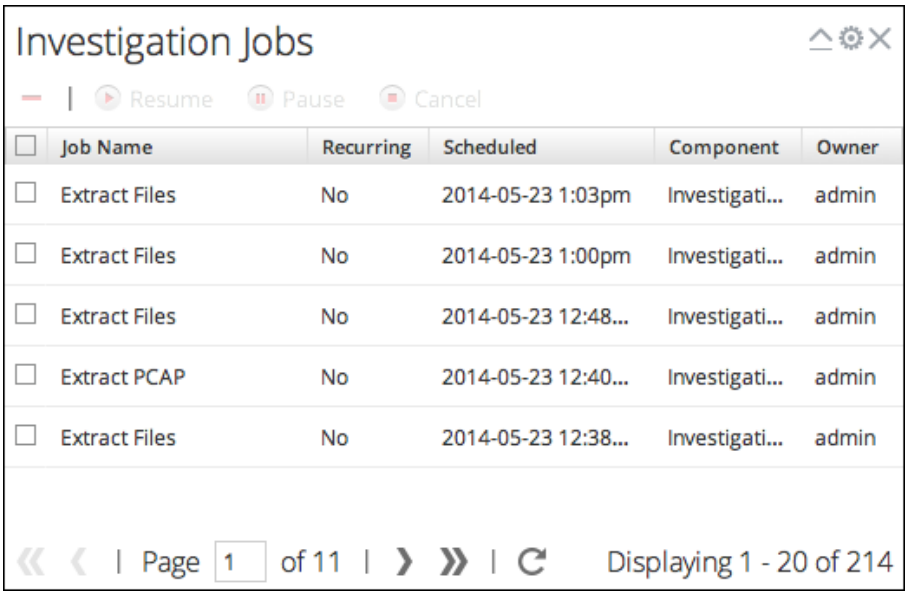


Característica	Descripción
Totales	Filas independientes muestran los totales de alertas, incidentes y corrección. Si hace clic en un total, se abre la pestaña correspondiente a alertas, incidentes o corrección.
Aumento y disminución	El número debajo del total es la cantidad de aumento o disminución. Un total que cambió más de un 33 % aparece en rojo. Un total que cambió menos de un 33 % aparece en gris.

Dashlet Trabajos de investigación

El dashlet Trabajos de investigación muestra el estado de todos los trabajos en el módulo Investigation. Los procedimientos de administración de la barra de herramientas, la cuadrícula y los trabajos se describen en Bandeja de trabajos.

Para mostrar este dashlet en el tablero predeterminado o como parte de un tablero personalizado, haga clic en > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Trabajos de investigación**.



Características

El dashlet Trabajos de investigación muestra todos los trabajos que posee, recurrentes y no recurrentes, y le permite monitorear su progreso.

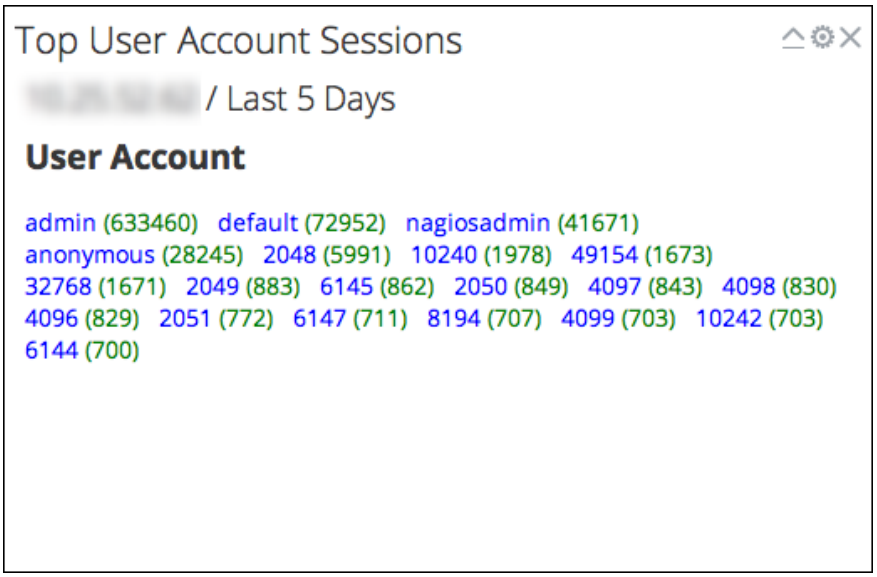
Característica	Descripción
Resume	La opción Reanudar se aplica solo a los trabajos recurrentes que están en pausa. Cuando reanuda un trabajo pausado, la próxima ejecución del trabajo se ejecuta como calendarizada.
Pause	La opción Pausar se aplica solamente a los trabajos recurrentes. Cuando pausa un trabajo recurrente que está en ejecución, la ejecución no se ve afectada. La próxima ejecución (si se asume que el trabajo sigue en pausa) se omite.

Característica	Descripción
Cancel	Cancela un trabajo recurrente o no recurrente. Puede cancelar un trabajo mientras está en ejecución. Si cancela un trabajo recurrente, se cancela esa ejecución del trabajo. La próxima vez que el trabajo se calendarice para ejecución, se ejecutará de manera normal.
—	Elimina un trabajo recurrente o no recurrente del panel Trabajos. Cuando elimina un trabajo, este se elimina instantáneamente del panel Trabajos. No aparece un diálogo de confirmación. Si elimina un trabajo recurrente, también se eliminan todas las ejecuciones futuras.

Dashlet Valores principales de Investigation

El dashlet Valores principales de Investigation permite inspeccionar los valores principales de un período específico y de un tipo de metadatos determinado en un dispositivo dado. Los metadatos y los parámetros de consulta se definen en el cuadro de diálogo Agregar un dashlet.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Valores principales de Investigation**.



Características

Puede definir los metadatos y parámetros de consulta en el cuadro de diálogo **Agregar un dashlet**.

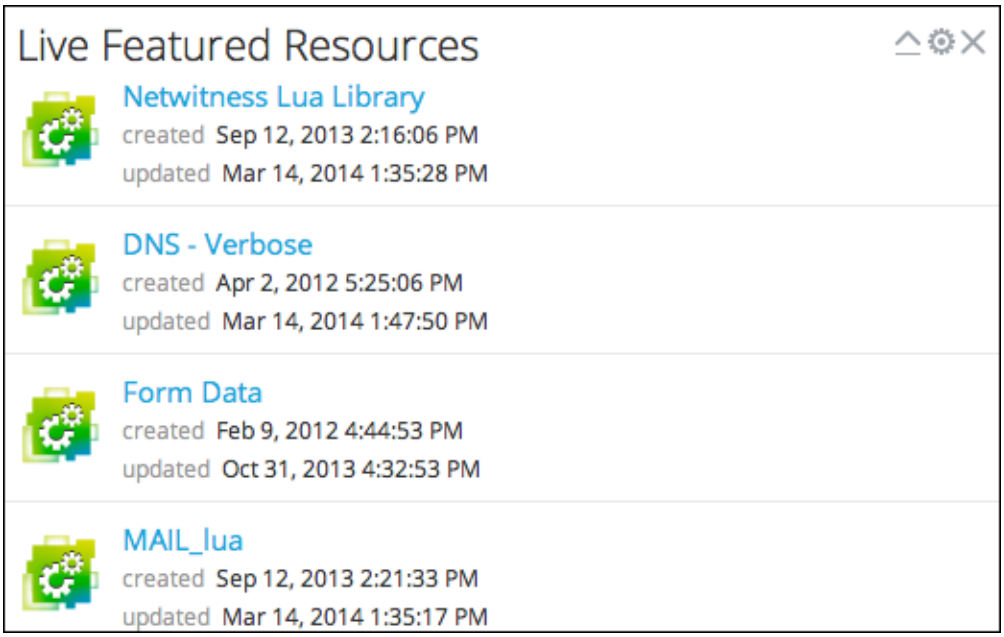
Característica	Descripción
Título	El título del dashlet.
Servicio	El nombre o la dirección IP del servicio objetivo.

Característica	Descripción
Tiempo (relativo)	Últimos cinco minutos Últimos 10 minutos Últimos 15 minutos Últimos 30 minutos Last Hour Últimas 3 horas Últimas seis horas Últimas 12 horas Last 24 Hours Últimos 2 días Últimos 5 días
Tipo de metadatos	Seleccione el tipo de metadatos en la lista desplegable.
Consulta	Complete la consulta para definir los resultados de forma más detallada
Límite de resultado	Seleccione la cantidad de resultados que se mostrarán en la lista desplegable.

Dashlet Recursos destacados de Live

El dashlet Recursos destacados de Live muestra la lista de recursos de Live que están etiquetados como destacados para el servidor del sistema de administración de contenido (CMS) configurado.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Recursos destacados de Live**.



Características

Este dashlet tiene una vista de página de los recursos destacados de Live y proporciona la siguiente información acerca de cada recurso.

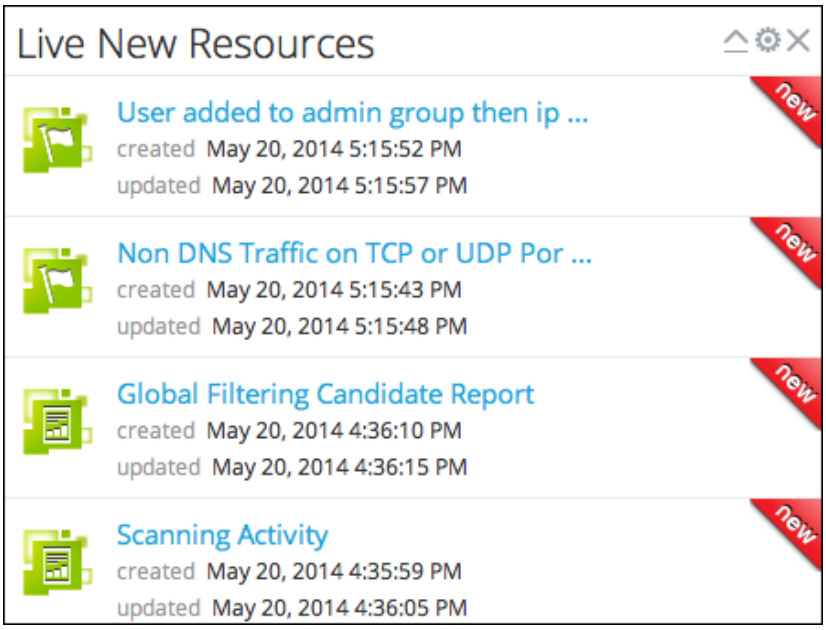
Valor	Descripción
(Ícono Tipo de recurso)	Cada tipo de recursos de Live se representa con un ícono. Por ejemplo, el ícono en la captura de pantalla representa un feed del analizador. Si hace clic en el ícono Tipo de recurso, se abre una nueva pestaña del navegador con la vista detallada del recurso en la vista Recurso de Live.

Valor	Descripción
Nombre del recurso	El nombre del recurso, por ejemplo, **Direcciones IP de amenazas APT de NetWitness**. Si hace clic en **Nombre del recurso**, se muestra la vista detallada del recurso en la vista Recurso de Live. La vista se abre en la pestaña actual del navegador.
Fecha de creación	La fecha en que se creó el recurso.
Fecha de la última actualización	La fecha en que el recurso se actualizó por última vez.

Dashlet de los recursos nuevos de Live

El dashlet Nuevos recursos de Live muestra una lista de los recursos de Live CMS que están etiquetados como nuevos para el servidor del sistema de administración de contenido (CMS) configurado. Puede hacer clic en un nombre de recurso para ir a la vista detallada del recurso.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Nuevos recursos de Live**.



Características

Este dashlet tiene una vista de página de los recursos nuevos de Live y proporciona la siguiente información acerca de cada recurso.

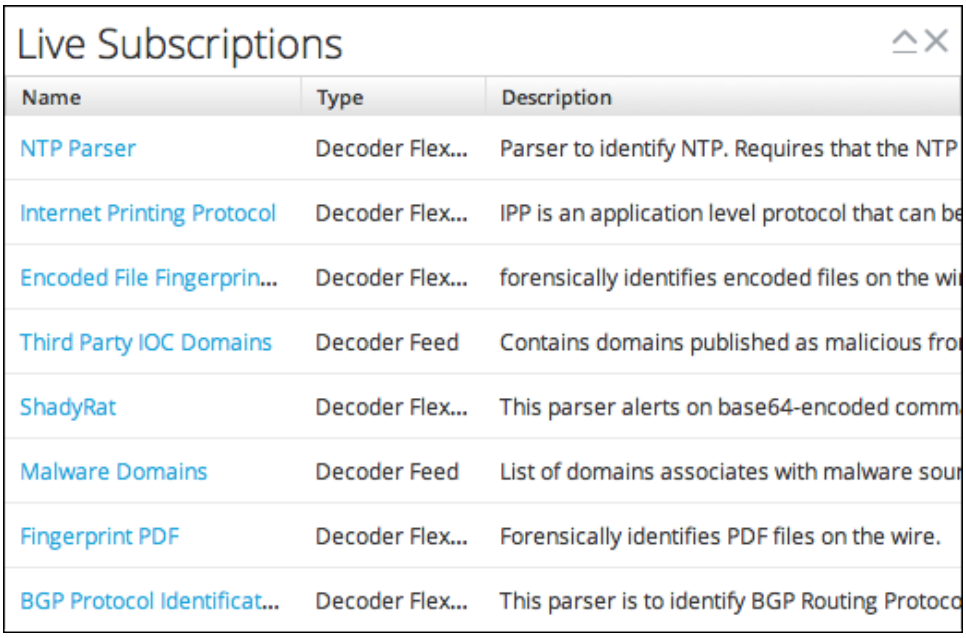
Valor	Descripción
 Ícono Tipo de recurso	Cada tipo de recursos de Live se representa con un ícono. Por ejemplo, el ícono de la izquierda representa un FlexParser de Decoder. Si hace clic en el ícono Tipo de recurso, se abre una nueva pestaña del navegador con la vista detallada del recurso en la vista Recurso de Live.

Valor	Descripción
Nombre del recurso	El nombre del recurso, por ejemplo, **Gh0st Protocol Parser**. Si hace clic en Nombre del recurso, se muestra la vista detallada del recurso en la vista Recurso de Live. La vista se abre en la pestaña actual del navegador.
Fecha de creación	La fecha en que se creó el recurso.
Fecha de la última actualización	La fecha en que el recurso se actualizó por última vez.

Dashlet de las suscripciones de Live

El dashlet Suscripciones de Live presenta una lista de todos los recursos de Live a los cuales se encuentra suscrita esta instancia de Security Analytics. Esta es sencillamente una lista de referencia rápida. Si necesita administrar suscripciones, utilice la pestaña Suscripciones en la vista Administrar de Live.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Suscripciones de Live**.



Características

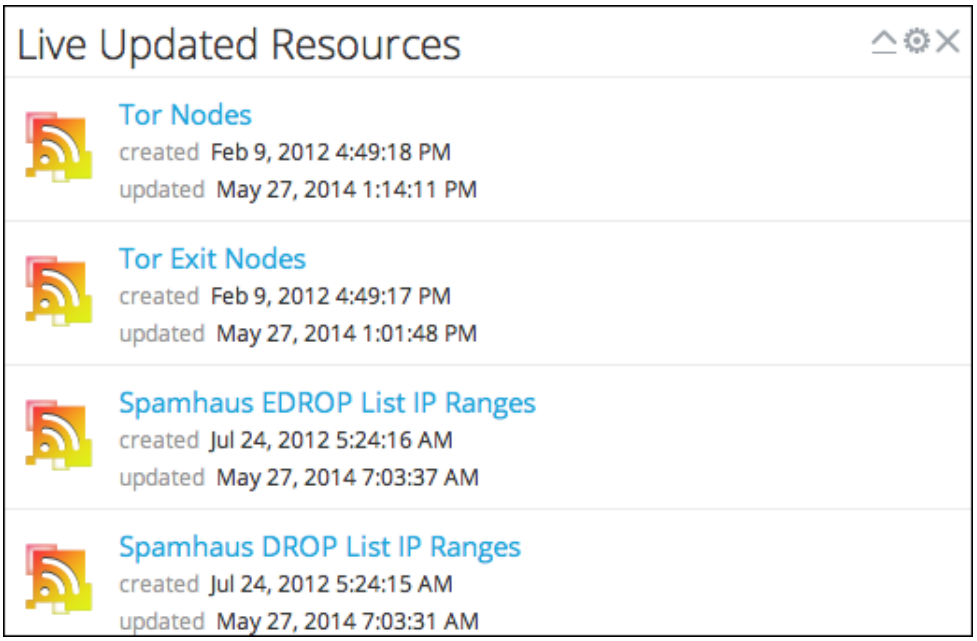
La cuadrícula es un subconjunto de la cuadrícula de suscripciones en la vista Administrar Live.

Valor	Descripción
Nombre	Muestra el nombre de la suscripción.
Tipo	Especifica el tipo de suscripción.
Descripción	Describe el tipo de información que proporciona la suscripción.

Dashlet de los recursos actualizados de Live

El dashlet Recursos actualizados de Live muestra una lista de los recursos de Live CMS que están etiquetados como actualizados para el servidor del sistema de administración de contenido (CMS) configurado. Puede hacer clic en el título de recurso para ir a una vista detallada del recurso.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en  > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Recursos actualizados de Live**.



Características

Este dashlet tiene una vista de página de los recursos actualizados de Live y proporciona la siguiente información acerca de cada recurso.

Este dashlet tiene una vista de página de los recursos destacados de Live y proporciona la siguiente información acerca de cada recurso.

Valor	Descripción
 Ícono Tipo de recurso	Cada tipo de recursos de Live se representa con un ícono. Por ejemplo, el ícono en la captura de pantalla representa un feed de Decoder. Si hace clic en el ícono Tipo de recurso, se abre una nueva pestaña del navegador con la vista detallada del recurso en la vista Recurso de Live.
Nombre del recurso	El nombre del recurso, por ejemplo, **Rangos de IP de la lista EDROP de Spamhaus**. Si hace clic en Nombre del recurso, se muestra la vista detallada del recurso en la vista Recurso de Live. La vista se abre en la pestaña actual del navegador.
Fecha de creación	La fecha en que se creó el recurso.
Fecha de la última actualización	La fecha en que el recurso se actualizó por última vez.

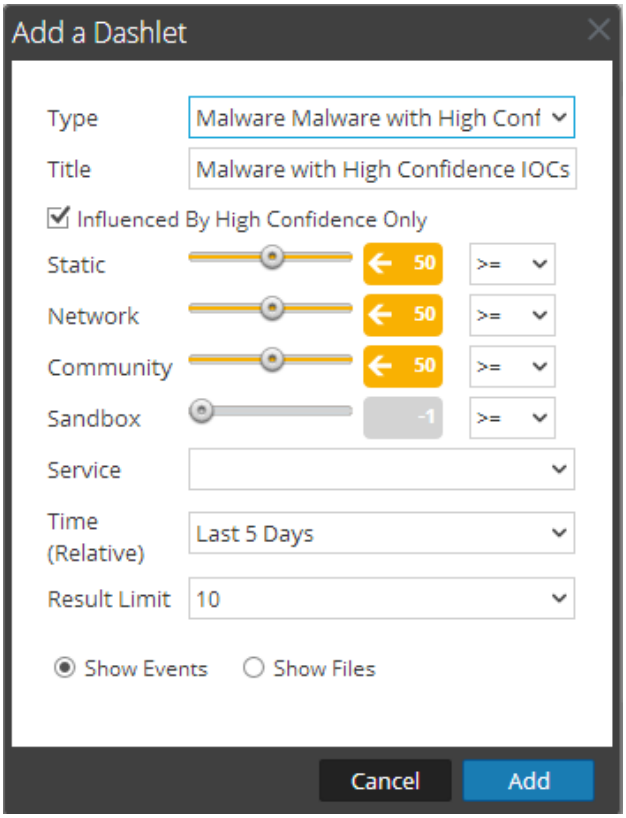
Dashlet Malware con IOC de alta confianza y altos puntajes de la vista Malware

El dashlet Malware con IOC de alta confianza y altos puntajes de la vista Malware presenta los eventos que Malware Analysis detectó con indicadores de riesgo, alta probabilidad de albergar malware y altos puntajes en los módulos de puntaje. Este dashlet está disponible en el tablero Unified y en la vista Malware. Cuando un analista de malware inicia sesión por primera vez en Security Analytics, de forma predeterminada, el único dashlet visible en la vista Unified es el dashlet Novedades. El analista debe crear otros dashlets de Malware.

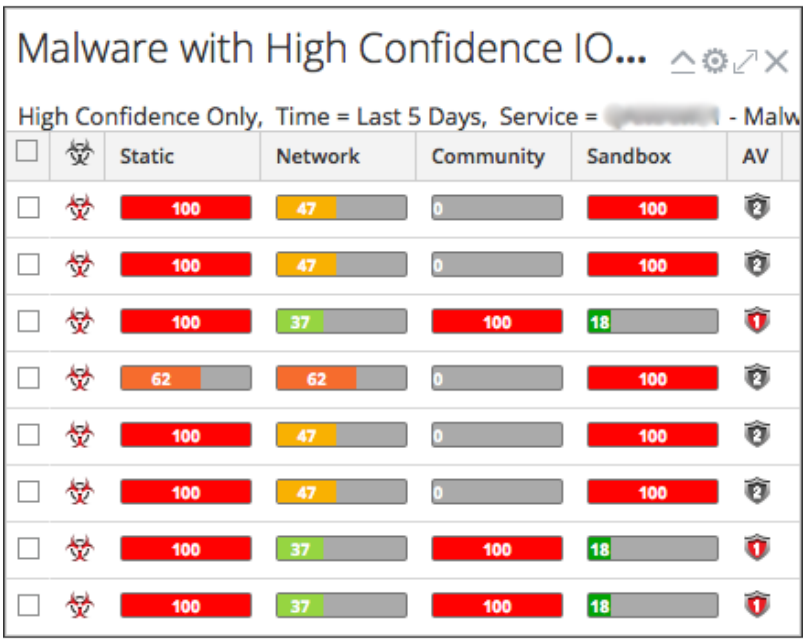
El dashlet Malware con IOC de alta confianza y altos puntajes de la vista Malware se puede configurar. Puede crear varias copias del dashlet, filtrar resultados y configurar la visualización de estos como una lista de eventos o una lista de archivos.

Para mostrar este dashlet en el **tablero de Security Analytics** o como parte de un tablero personalizado, haga clic en  > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Malware con IOC de alta confianza y altos puntajes de la vista Malware** en el menú desplegable **Tipo**.

Este es un ejemplo de la configuración del dashlet Malware con IOC de alta confianza y altos puntajes de la vista Malware.



Este es un ejemplo del dashlet Malware con IOC de alta confianza y altos puntajes de la vista Malware.



Características

En la siguiente tabla se indican los valores configurables de este dashlet.

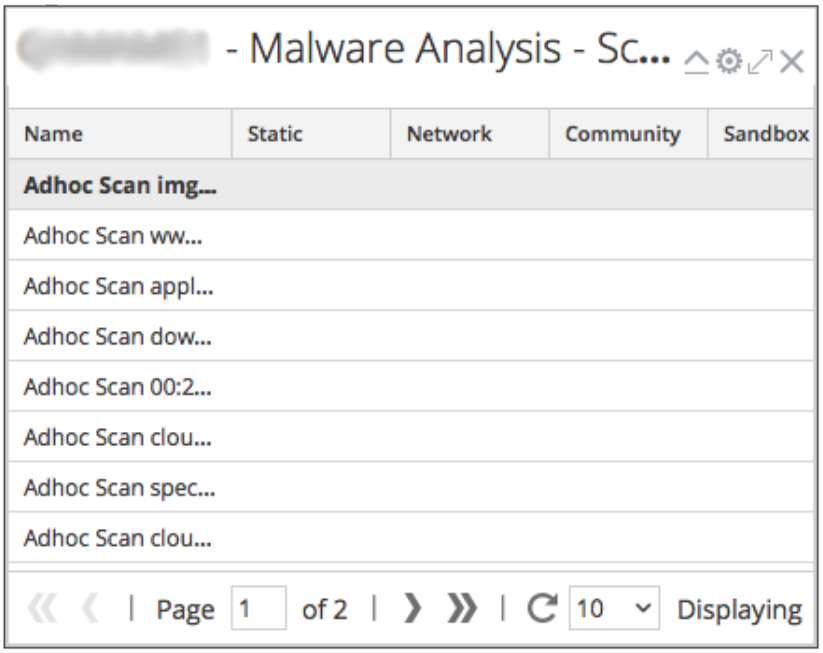
Variable	Descripción
Título	Identifica el nombre del dashlet. Cada dashlet necesita un nombre único, en especial si tiene más de una instancia del mismo dashlet. El nombre aparece en la barra de título del dashlet.
Solo con influencia de alta confianza	Cuando se selecciona, solo se muestran en el dashlet los eventos y los archivos que se marcaron como de alta confianza (o probabilidad) por contener indicadores de riesgo.
Estático, Red, Comunidad y Sandbox	Filtra los resultados en función de los puntajes para cada módulo de puntaje. Puede configurar el valor como =, <= o >=.
Límite de resultado	Establece la cantidad de resultados que se mostrarán. Los posibles valores en la lista desplegable son 5, 10, 20, 30 o 40.

Variable	Descripción
Servicio	Selecciona el servicio que se monitoreará.
Tiempo (relativo)	Limita el rango de tiempo de los resultados mostrados.
Mostrar eventos o Mostrar archivos	Especifica el formato de los resultados, ya sea Lista de eventos o Lista de archivos.

Dashlet Lista de trabajos de escaneo de malware

El dashlet Lista de trabajos de escaneo de malware muestra la misma lista de trabajos de escaneo que se presenta en el cuadro de diálogo Seleccionar un servicio de malware. Puede abrir escaneos completados directamente desde este dashlet.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Lista de trabajos de escaneo de malware**.



Características

Las columnas de esta lista de trabajos de escaneo son las mismas que las que aparecen en la lista de trabajos de escaneo del cuadro de diálogo Seleccionar un servicio de malware.

Si hace doble clic en un trabajo, puede verlo en la vista Investigation > Malware Analysis. Se abre el Resumen de eventos para el escaneo seleccionado que muestra los dashlets predeterminados en una nueva pestaña del navegador.

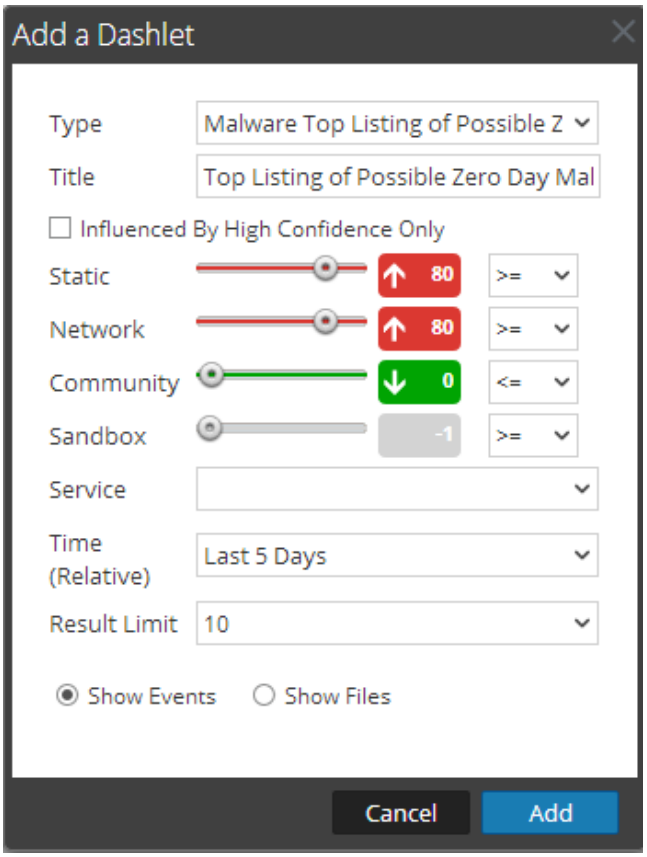
Dashlet Lista del posible malware de día cero principal de la vista Malware

El dashlet Lista del posible malware de día cero principal presenta los 10 eventos principales que indican un posible ataque de día cero en la Lista de eventos o en la Lista de archivos de Malware Analysis. Este dashlet está disponible en el tablero y en la vista Malware. Cuando un analista de malware inicia sesión por primera vez en Security Analytics, de forma predeterminada, el único dashlet visible en la vista es el dashlet Novedades. El analista debe crear otros dashlets de Malware.

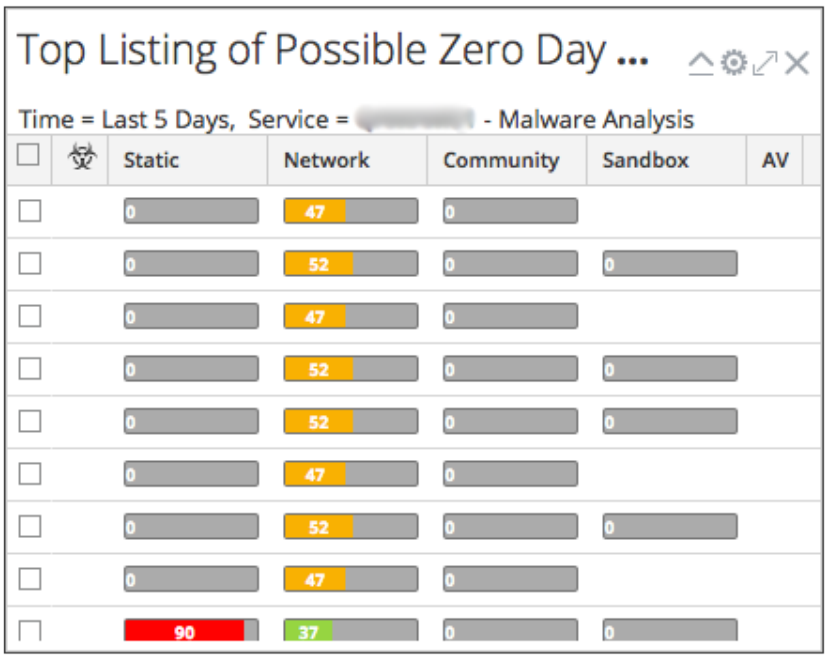
El dashlet Lista del posible malware de día cero principal de la vista Malware es configurable. Puede crear varias copias del dashlet, filtrar resultados y configurar la visualización de estos como una Lista de eventos o una Lista de archivos. Desde este dashlet, puede iniciar una investigación de Malware Analysis de un evento directamente si hace doble clic en el evento; no es necesario que vaya a Investigation > vista Malware para comenzar.

Para mostrar este dashlet en el tablero de **Security Analytics** o como parte de un tablero personalizado, haga clic en  **> Agregar dashlet** en la barra de herramientas del tablero y seleccione **Lista del posible malware de día cero principal** de la vista **Malware** en el menú desplegable **Tipo**.

Este es un ejemplo del dashlet configurado para mostrar la Lista de eventos.



Este es un ejemplo del dashlet. Las funciones del dashlet son las mismas que las de la Lista de eventos o la Lista de archivos de Malware Analysis.



Características

En la siguiente tabla se indican los valores configurables de este dashlet.

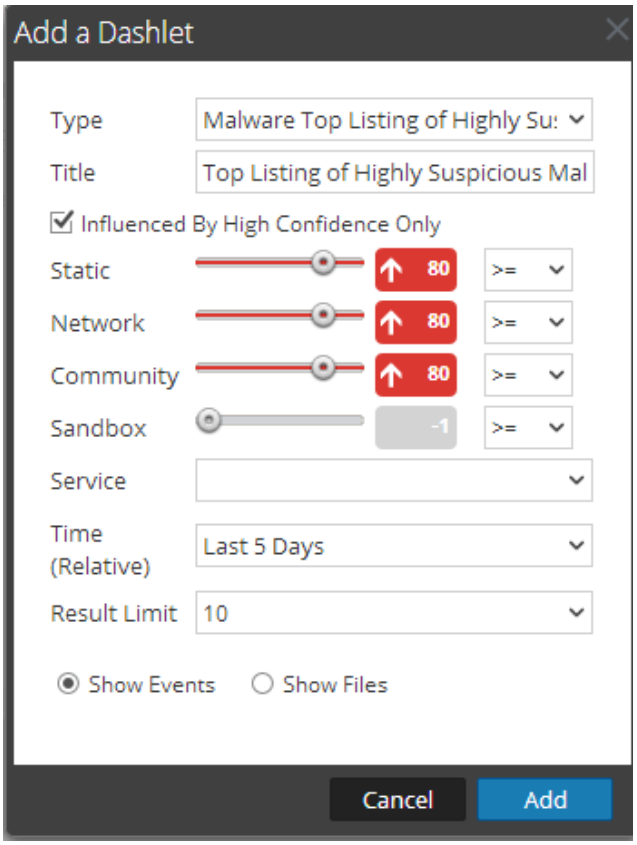
Variable	Descripción
Título	Identifica el nombre del dashlet. Cada dashlet necesita un nombre único, en especial si tiene más de una instancia del mismo dashlet. El nombre aparece en la barra de título del dashlet.
Solo con influencia de alta confianza	Cuando se selecciona, solo se muestran en el dashlet los eventos y los archivos que se marcaron como de alta confianza (o probabilidad) por contener indicadores de riesgo.
Estático, Red, Comunidad y Sandbox	Filtra los resultados en función de los puntajes para cada módulo de puntaje. Puede configurar el valor como =, <= o >=. El operador del filtro de la comunidad es menor o igual al valor del control deslizante aplicado de manera predeterminada. El operador de los otros filtros es mayor o igual que el valor predeterminado.
Servicio	Selecciona el servicio que se monitoreará.
Tiempo (relativo)	Limita el rango de tiempo de los resultados mostrados.
Límite de resultado	Establece la cantidad de resultados que se mostrarán. Los posibles valores en la lista desplegable son 5, 10, 20, 30 o 40.
Mostrar eventos o Mostrar archivos	Especifica el formato de los resultados, ya sea Lista de eventos o Lista de archivos.

Dashlet Lista del malware altamente sospechoso principal de la vista Malware

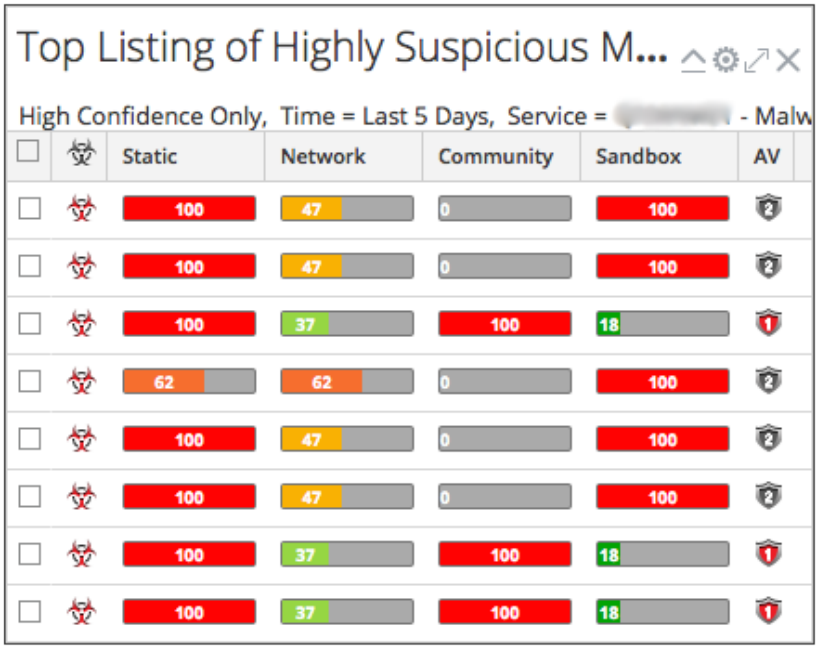
El dashlet Lista del malware altamente sospechoso principal de la vista Malware presenta los 10 eventos principales más sospechosos en la Lista de eventos o en la Lista de archivos de Malware Analysis. Este dashlet está disponible en el tablero y en la vista Malware Analysis. Cuando un analista de malware inicia sesión por primera vez en Security Analytics, de forma predeterminada, el único tablero de dashlet visible es el dashlet Novedades. El analista debe crear otros dashlets de Malware Analysis.

El dashlet Lista del malware altamente sospechoso principal se puede configurar. Puede crear varias copias del dashlet, filtrar resultados y configurar la visualización de estos como una lista de eventos o una lista de archivos.

Para mostrar este dashlet en el **tablero de Security Analytics** o como parte de un tablero personalizado, haga clic en  > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Lista del malware altamente sospechoso principal** de **Malware** en el menú desplegable **Tipo**.



Este es un ejemplo del dashlet.



Características

Las funciones son las mismas que las de la **Lista de eventos y la Lista de archivos de Malware Analysis** (consulte la *Guía de Investigation y Malware Analysis* para obtener detalles). Para iniciar una investigación de Malware Analysis de un elemento del dashlet, haga doble clic en un evento o nombre de archivo en la cuadrícula.

En la siguiente tabla se indican los valores configurables de este dashlet.

Variable	Descripción
Título	Identifica el nombre del dashlet. Cada dashlet necesita un nombre único, en especial si tiene más de una instancia del mismo dashlet. El nombre aparece en la barra de título del dashlet.
Solo con influencia de alta confianza	Cuando se selecciona, solo se muestran en el dashlet los eventos y los archivos que se marcaron como de alta confianza (o probabilidad) por contener indicadores de riesgo.
Estático, Red, Comunidad y Sandbox	Filtra los resultados en función de los puntajes para cada módulo de puntaje. Puede configurar el valor como =, <= o >=.
Servicio	Selecciona el servicio que se monitoreará.

Variable	Descripción
Tiempo (relativo)	Limita el rango de tiempo de los resultados mostrados.
Límite de resultado	Establece la cantidad de resultados que se mostrarán. Los posibles valores en la lista desplegable son 5, 10, 20, 30 o 40.
Mostrar eventos o Mostrar archivos	Especifica el formato de los resultados, ya sea Lista de eventos o Lista de archivos.

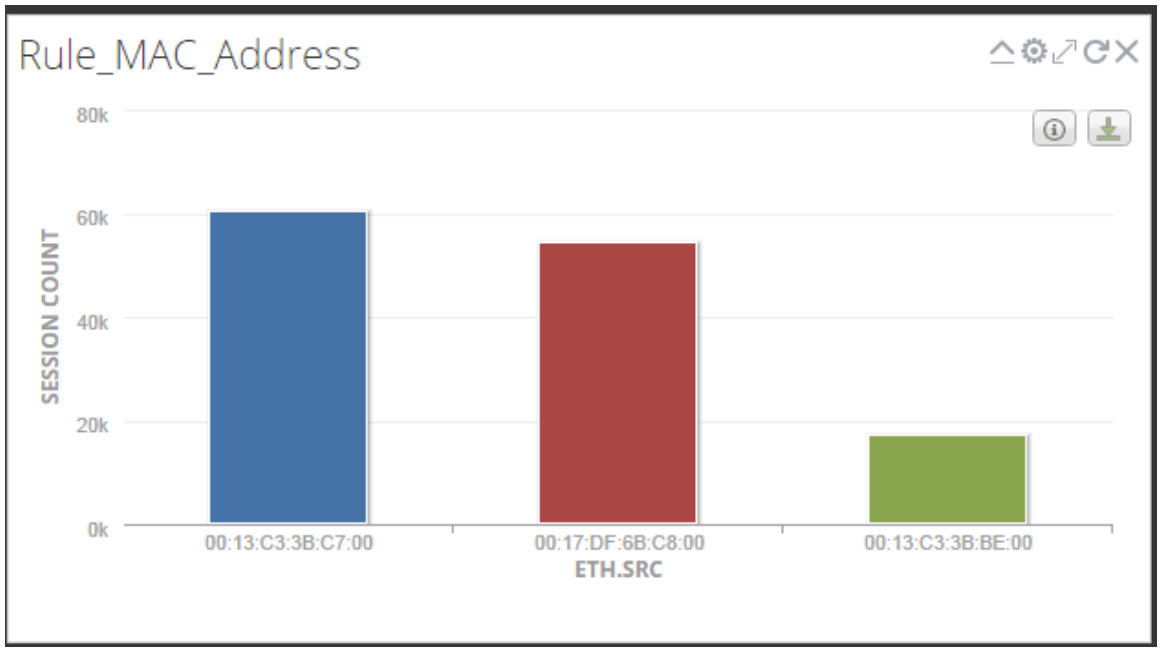
Dashlet Gráfica en tiempo real de Reports

El dashlet Gráfica en tiempo real de Reports muestra uno de los gráficos de la lista de gráficos que definió. El resultado del gráfico proviene de los datos de Live y se actualiza según el intervalo de actualización que configure. Cada gráfico se define según el Tipo de gráfico y el valor Horas pasadas que se selecciona.

Puede seleccionar la opción Valores del gráfico en el tiempo o Gráfico con totales. El gráfico muestra los datos actuales y no muestra los puntos de datos para datos históricos.

Se genera el gráfico para los datos según el intervalo de tiempo que definió en la definición del gráfico. Los datos se encuentran disponibles a partir de los últimos 20 intervalos de tiempo como máximo. Por ejemplo, si en la definición del gráfico seleccionó un intervalo de actualización de cinco minutos y la hora pasada como una hora, entonces el gráfico muestra los datos de los últimos 60 minutos. El gráfico en el dashlet se actualiza según el intervalo de actualización de dashlet que definió.

Para mostrar este dashlet en el tablero de **Security Analytics** o como parte de un tablero personalizado, haga clic en  > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Gráfica en tiempo real de Reports** en el menú desplegable **Tipo**.



Características

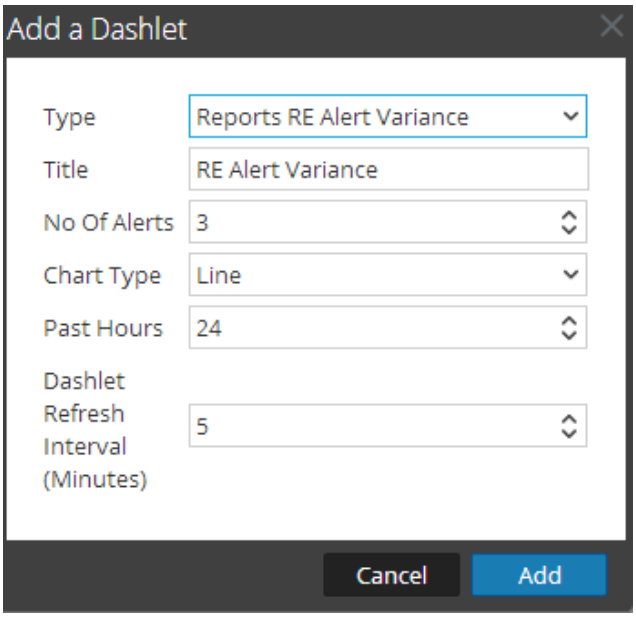
Las opciones del gráfico aparecen en la siguiente tabla.

Variable	Descripción
Gráfico	Seleccione un gráfico de los gráficos ya definidos. Puede seleccionar solo un gráfico por dashlet.
Título	Escriba un nombre para el dashlet Gráfica en tiempo real de Reporting. El nombre aparece en la barra de título del dashlet.
Serie	**Valores del gráfico en el tiempo:** El gráfico muestra el cambio en los valores para la hora seleccionada.
	Gráfico con totales: El gráfico muestra un total para cada valor agregado para la hora seleccionada.
Tipo de gráfico	Seleccione el tipo de gráfico que desea en el dashlet. Los valores proporcionados en la lista desplegable son: barra, columna y línea.
Horas pasadas	Seleccione el intervalo de tiempo pasado.
Intervalo de actualización del dashlet (minutos)	Configure el intervalo de tiempo en minutos en el cual se actualiza el dashlet. El valor del intervalo oscila entre 1 y 180 minutos.

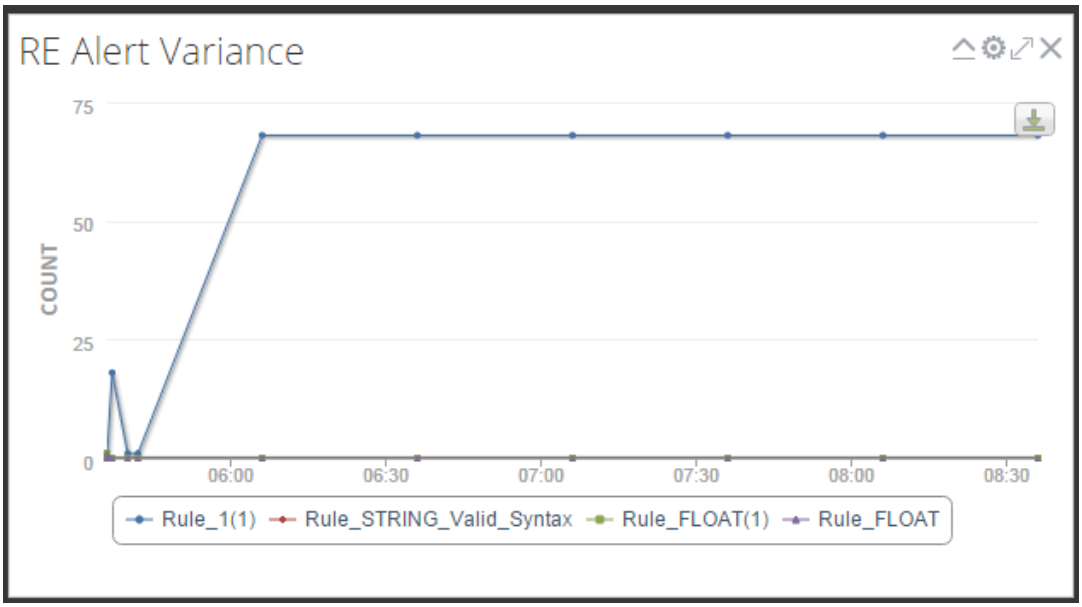
Dashlet Diferencia de alertas de RE de Reports

El dashlet Variación de alertas de RE de Reports es un dashlet configurable en el cual se representan las principales alertas en cuatro tipos de gráficos de serie de tiempo distintos. Puede configurar los resultados que desea incluir en el gráfico (desde las 2 alertas principales hasta las 15 alertas principales en el rango de tiempo especificado).

Para mostrar este dashlet en el tablero de **Security Analytics** o como parte de un tablero personalizado, seleccione  > **Agregar dashlet** en la barra de herramientas del tablero y elija **Variación de alertas de RE de Reports** en el menú desplegable **Tipo**.



La siguiente figura es un ejemplo:



Características

Este dashlet es una representación visual de las alertas más frecuentes activadas por el Reporting Engine asociado. Cada tipo de gráfico se puede definir según la cantidad de alertas, las horas transcurridas desde el momento en que se deben obtener las alertas y el intervalo de actualización del dashlet para el gráfico que se actualizará.

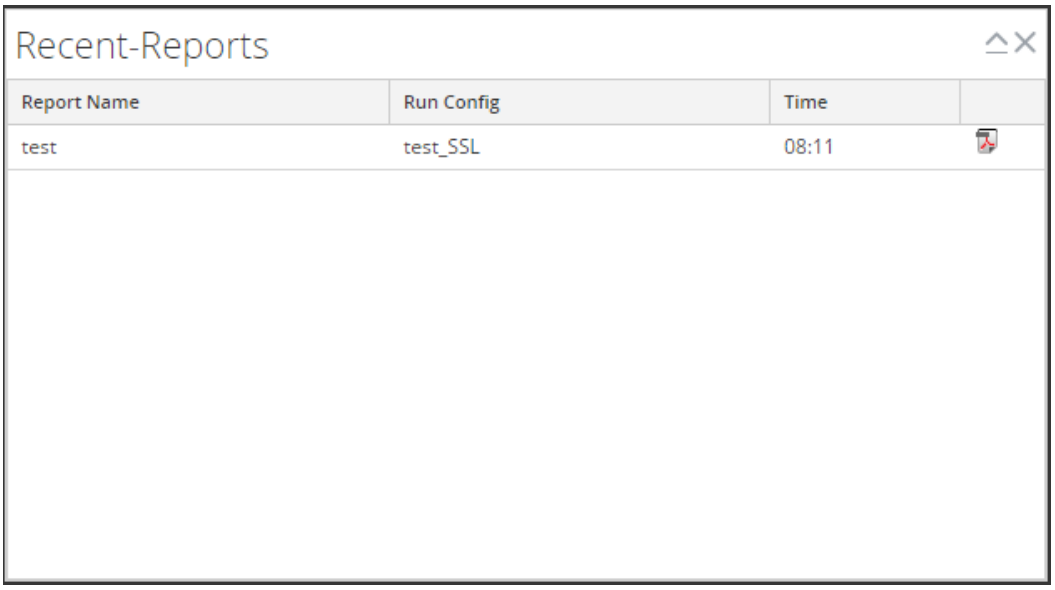
Variable	Descripción
Tipo	Seleccione el tipo de gráfico que desea en el dashlet: • Barra (eje X = conteo y eje Y = nombre de la alerta) • Columnas (eje X = Conteo y eje Y = Nombre de alerta) • Líneas (eje X = Conteo y eje Y = Nombre de alerta)
Título	Proporcione un nombre para el dashlet Gráfica en tiempo real de Reporter. El nombre aparece en la barra de título del dashlet.
N.º de alertas	Seleccione la cantidad de alertas que se considerarán mientras se configura el dashlet. El valor varía entre 2 y 15.
Horas pasadas	Seleccione la hora desde el momento en que se deben obtener las alertas.

Variable	Descripción
Intervalo de actualización del dashlet (minutos)	Configure el intervalo de tiempo en minutos en el cual se actualiza el dashlet. El valor del intervalo varía entre 1 y 180 minutos.

Dashlet Informe de ejecuciones recientes de Reports

El dashlet Informe de ejecución reciente de Reports consta de una lista de los informes que se acaban de ejecutar en Security Analytics. Los informes recientes que se muestran corresponden a las últimas 24 horas.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Informe de ejecución reciente de Reports** en el menú desplegable **Tipo**.



Características

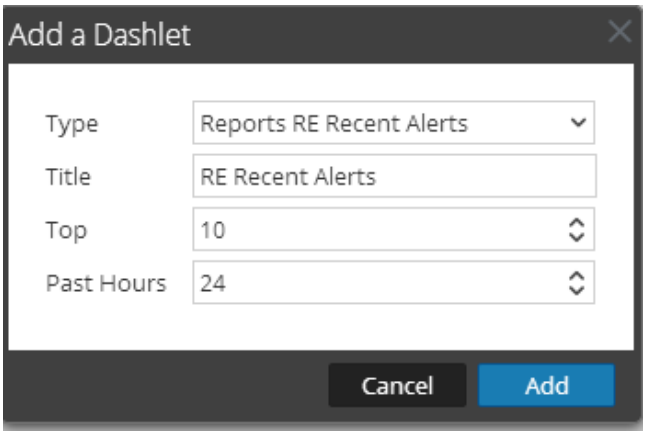
En la siguiente tabla se describen las columnas presentes en el dashlet de manera predeterminada.

Columna	Descripción
Nombre de informe	El nombre del informe ejecutado recientemente.
Configuración de ejecución	La configuración de ejecución del informe ejecutado recientemente.
Hora	La hora que se calendarizó el informe.
Exportación	Haga clic en el ícono de exportación ( ) para exportar el archivo.

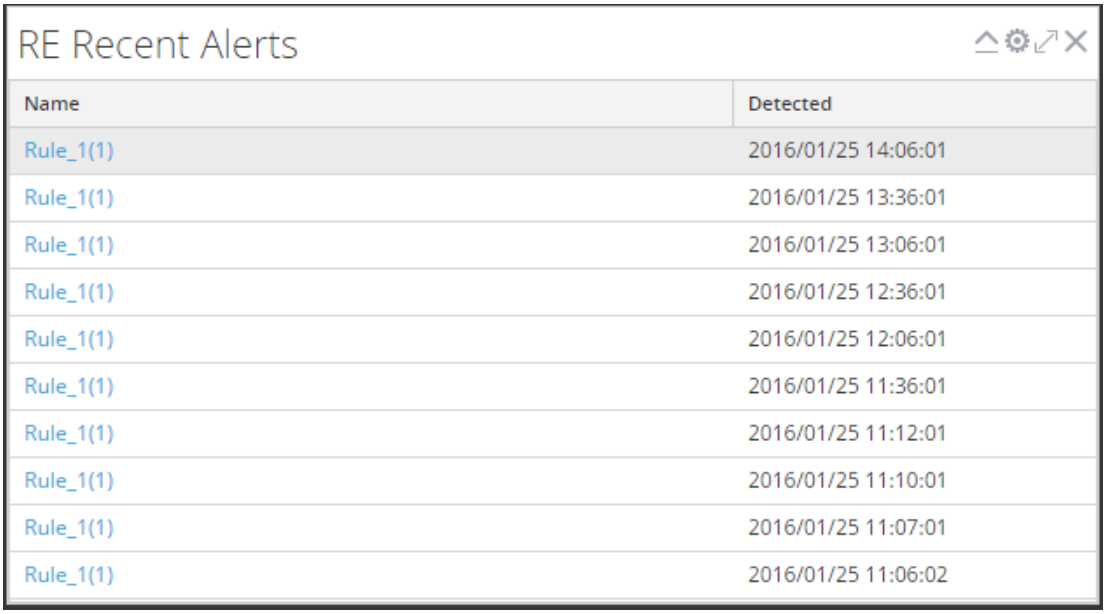
Dashlet Alertas recientes de RE de Reports

El dashlet Alertas recientes de RE de Reports muestra las alertas más recientes en el tablero. Puede configurar la cantidad de alertas más recientes que se mostrarán y también especificar el rango de tiempo en que se deben recuperar las alertas.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en  > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Alertas recientes de RE de Reports** en el menú desplegable **Tipo**.



La siguiente figura es un ejemplo:



Características

En la siguiente tabla se describen las columnas del dashlet Alertas recientes de RE de Reports.

Columna	Descripción
Nombre	El nombre de la alerta como se definió.
Detected	La fecha y la hora en que se activó la alerta. Esta hora de detección es cuando Security Analytics detectó las condiciones para disparar esta alerta.

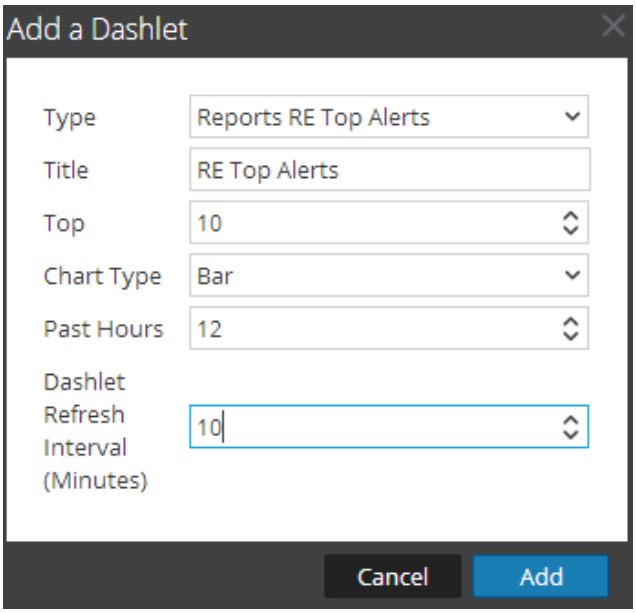
Dashlet Alertas principales de RE de Reporting

El dashlet Alertas principales de RE de Reports es un dashlet configurable en el cual se representan las principales alertas en cuatro tipos de gráficos. Puede configurar los resultados que desea incluir en el gráfico (desde las 2 alertas principales hasta las 15 alertas principales en el rango de tiempo especificado).

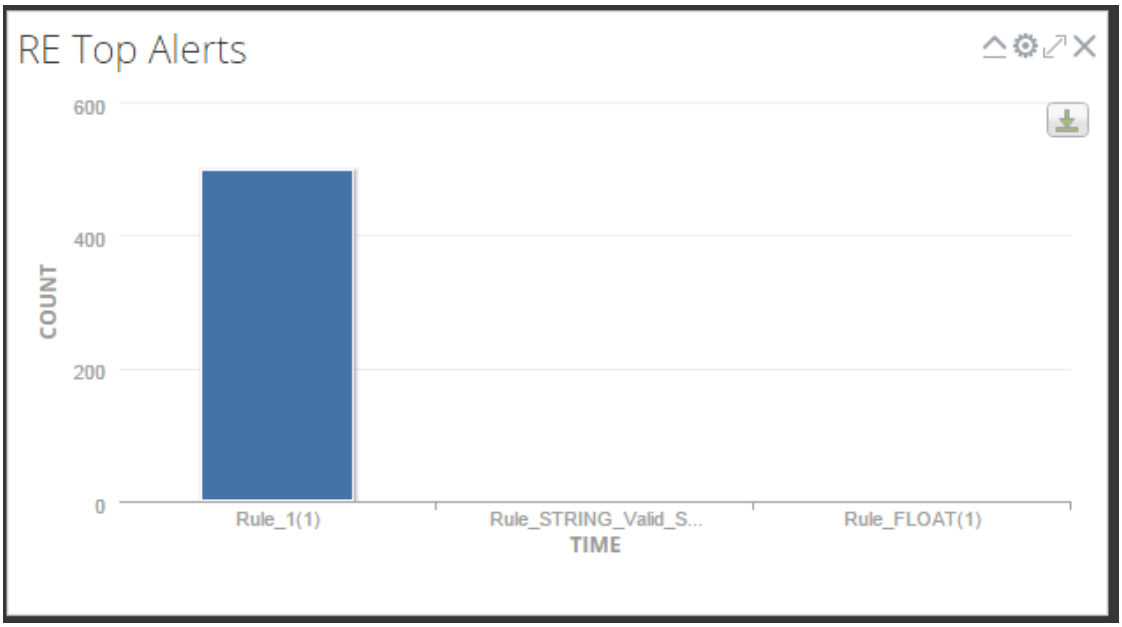
El gráfico se resume para cada alerta principal con la cantidad de eventos que activó la alerta para los intervalos de tiempo y de actualización definidos. El primer punto de datos en el gráfico define la cantidad de eventos (conteo de alertas) activados por la alerta para el tiempo definido. Los puntos de datos subsiguientes se muestran al agregar el conteo de alertas en el primer punto de datos y el conteo de alertas en los intervalos de actualización definidos.

Por ejemplo, si para el rango de tiempo definido, la cantidad de eventos (conteo de alertas) activados por la alerta es 10, entonces el primer punto de datos en el gráfico se muestra como 10. El punto de datos subsiguiente = 10 + cantidad de eventos (conteo de alertas) activados por la alerta en el intervalo de actualización de dashlet definido.

Para mostrar este dashlet en el tablero de Security Analytics o como parte de un tablero personalizado, haga clic en > **Agregar dashlet** en la barra de herramientas del tablero y seleccione **Alertas principales de RE de Reports** en el menú desplegable **Tipo**.



La siguiente figura es un ejemplo:



Características

Este dashlet es una representación visual de las alertas más frecuentes activadas por el Reporting Engine asociado. Se puede definir cada tipo de gráfico por el número de alertas principales, la fecha y hora cuando se deben recuperar las alertas, y el intervalo de actualización del dashlet para el gráfico que se actualizará.

Variable	Descripción
Tipo de gráfico	Seleccione el tipo de gráfico que desea en el dashlet: • Barra (eje X = conteo y eje Y = nombre de la alerta) • Columnas (eje X = Conteo y eje Y = Nombre de alerta) • Circular • Líneas (eje X = Conteo y eje Y = Nombre de alerta) • Tabular(eje X = conteo y eje Y = nombre de la alerta)
Título	Escriba un nombre para el dashlet Gráfica en tiempo real de Reporting. El nombre aparece en la barra de título del dashlet.
Principales	Seleccione la cantidad de alertas principales que se considerarán mientras se configura el dashlet. El valor varía entre 2 y 15.

Variable	Descripción
Horas pasadas	Seleccione la hora desde el momento en que se deben obtener las alertas.
Intervalo de actualización del dashlet (minutos)	Configure el intervalo de tiempo en minutos en el cual se actualiza el dashlet. El valor del intervalo varía entre 1 y 180 minutos.