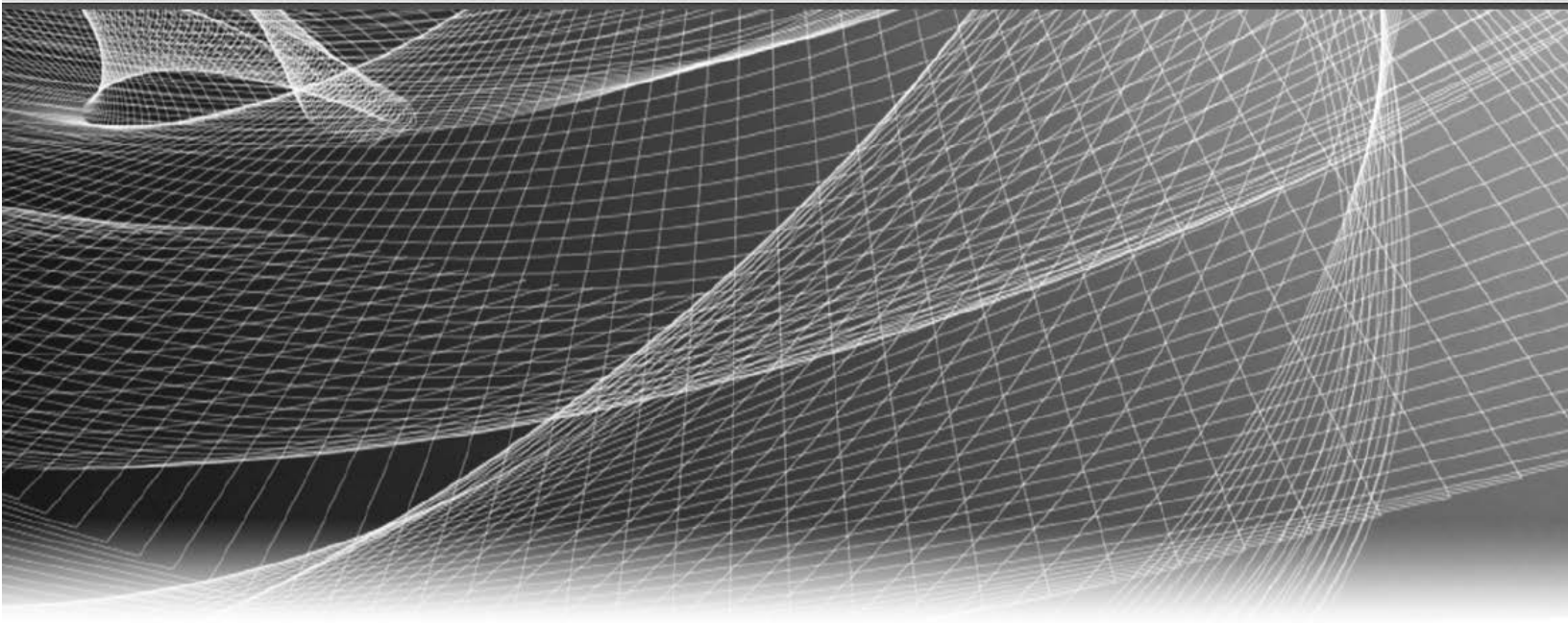


RSA Security Analytics

Guía de Incident Management

para la versión 10.6

RSA EMC²

Marcas comerciales

Acuerdo de licencia

Licencias de otros fabricantes

Nota sobre tecnologías de cifrado

Distribución

Contenido

Incident Management

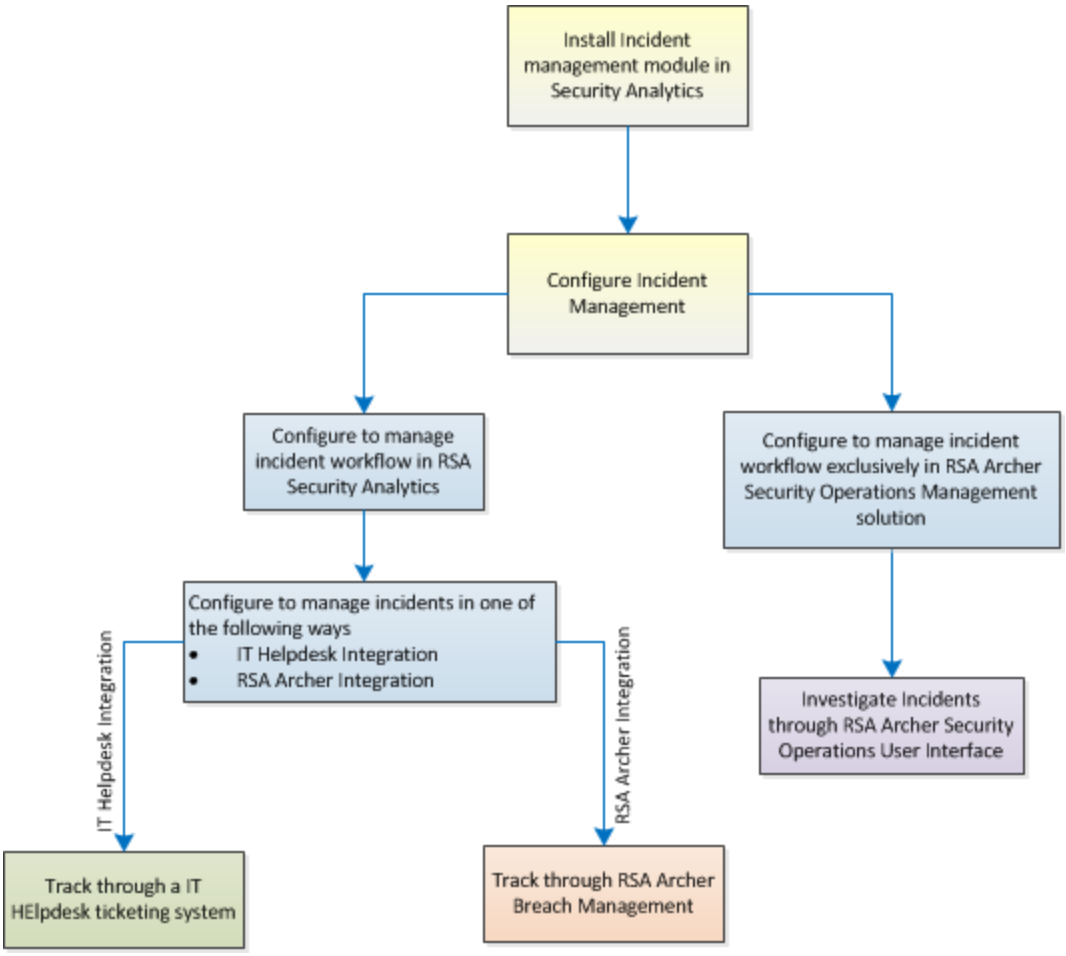
El módulo Incidentes de Security Analytics ofrece una manera sencilla de rastrear el proceso de respuesta ante incidentes. La solución de administración de incidentes proporciona lo siguiente:

- 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.

La mayor parte de las investigaciones se lleva a cabo dentro de la interfaz de Security Analytics, la cual permite crear y rastrear tareas de corrección, pero Security Analytics también tiene las siguientes opciones:

- Integración con un sistema de vales de otros fabricantes que permite elevar las tareas de corrección para la línea de espera de destino de operaciones como vales.
- Integración con RSA Archer que permite elevar las tareas de corrección para la línea de espera objetivo de **GRC** como observaciones o informar vulneraciones de datos y activar el proceso de respuesta ante vulneración en la solución RSA Archer Security Operations Management.

En la siguiente figura se representan los diversos métodos disponibles para rastrear las alertas entrantes y llevar a cabo el proceso de administración de incidentes.



Temas

Proceso de administración de incidentes

Flujo de trabajo de administración de incidentes

El módulo Security Analytics Incidents recopila alertas de varios orígenes y ofrece la posibilidad de agruparlas de manera lógica e iniciar un flujo de trabajo de respuesta a incidentes para investigar y corregir los problemas de seguridad que se presenten. El módulo Security Analytics Incidents permite configurar reglas para automatizar la agregación de alertas en incidentes. Las alertas se normalizan en el sistema a un formato común para ofrecer a los usuarios una vista coherente de los criterios de las reglas, independientemente del origen de datos. Puede generar criterios de consulta en función de los datos de la alerta con la posibilidad de consultar en los campos que son comunes, así como específicos de los orígenes de datos.

El motor de reglas permite agrupar alertas similares juntas en un incidente de manera que el flujo de trabajo de investigación y corrección se pueda compartir en un conjunto de alertas similares. Puede crear reglas que puedan agrupar alertas en incidentes en función de un valor común que comparten para uno o dos atributos (por ejemplo, nombre de host de origen) o si se informan dentro de una ventana de tiempo limitado (por ejemplo, alertas que tienen una diferencia de 4 horas entre ellas).

Si una alerta coincide con una regla, se crea un incidente mediante el uso de los criterios. A medida que se recopilan nuevas alertas, si ya se creó un incidente que coincide con estos criterios, y ese incidente aún no está “en curso”, las nuevas alertas se agregan al mismo incidente. Si no hay ningún incidente para el valor agrupado (por ejemplo, el nombre de host específico) o la ventana de tiempo, se crea un nuevo incidente, al cual se agregará la alerta.

Puede tener varias reglas de agregación. Las reglas pueden agrupar alertas en incidentes o impedir que una regla coincida con las alertas; por lo tanto, las reglas se clasifican de arriba abajo y solo la primera regla que coincida con una alerta entrante se usará para incluir esa alerta en un incidente. Los incidentes proporcionan un contexto para las alertas, brindan herramientas para registrar el estado de la investigación y rastrean el avance de la corrección.

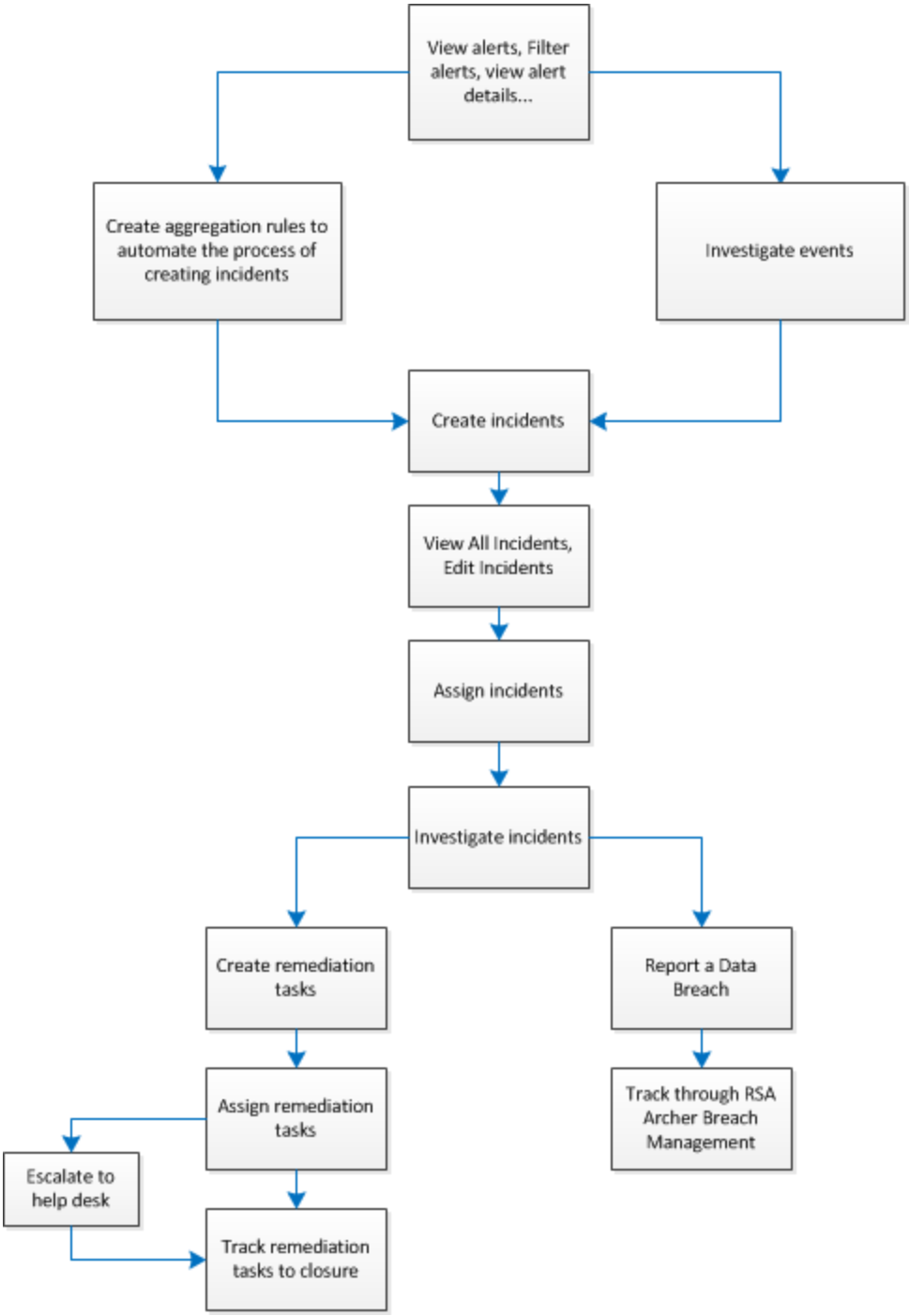
Las diversas etapas en el proceso de administración de incidentes son:

- Revisar alertas
- Administrar incidentes
- Automatizar el proceso de administración de incidentes
- Rastrear la respuesta de los incidentes a través de
  - Interfaz del usuario de Security Analytics
  - un sistema de help desk de terceros

- administración de vulneraciones de RSA Archer

Diagrama de flujo de trabajo de administración de incidentes

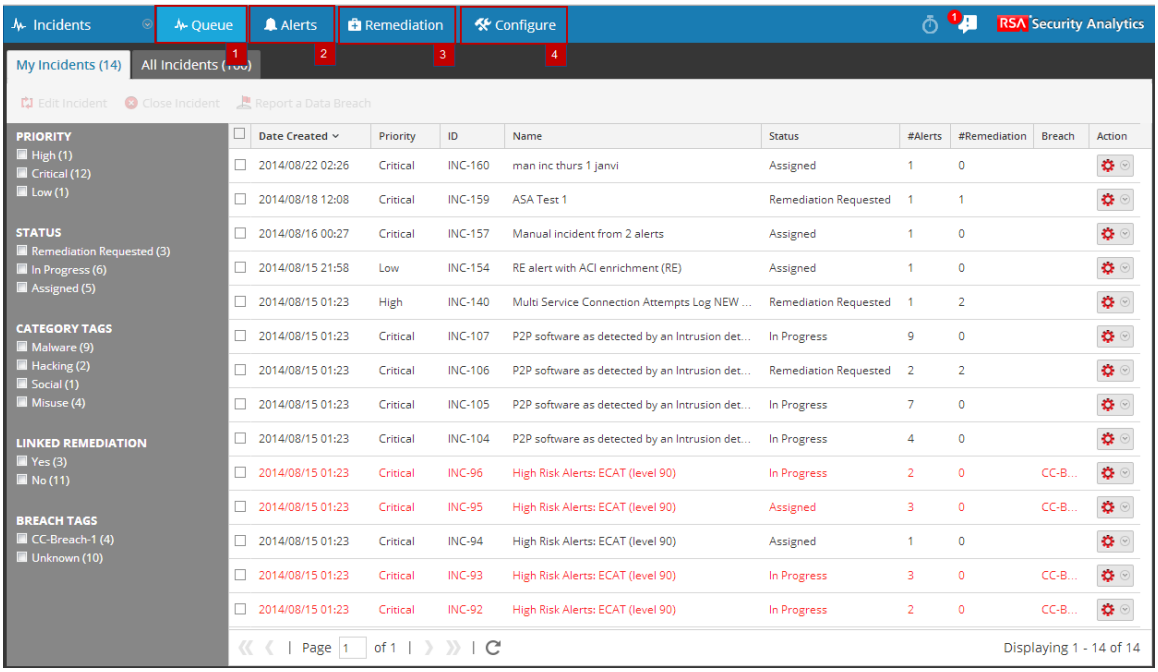
En la siguiente figura se muestra el proceso de flujo de trabajo de administración de incidentes.



La vista Incident Management

En el menú de **Security Analytics**, seleccione **Dashboard > Incidentes**. Se muestran las diversas secciones del módulo Incidents.

En la siguiente figura se ilustra el módulo Incidentes que se muestra en la interfaz del usuario de Security Analytics.



1. **Línea de espera**: En la línea de espera de incidentes, puede ver una lista de todos los incidentes asignados y no asignados. Puede filtrar incidentes, ver detalles de incidentes, investigar incidentes y rastrearlos hasta su cierre.
2. **Alertas**: en la vista Alertas puede ver una lista de alertas recopiladas desde diversos orígenes. Puede navegar hasta las diversas alertas, filtrarlas y agruparlas para crear incidentes.
3. **Corrección**: En la vista Corrección, puede ver una lista de todas las tareas de corrección creadas para diversos incidentes. Puede administrar y rastrar las tareas de corrección, y enviarlas a help desk si así se requiere, además de rastrear el incidente para su cierre.
4. **Configurar**: En la vista Configuración, puede establecer la configuración de notificaciones, la integración con sistemas de otros fabricantes para la administración de incidentes y configurar reglas de agregación para automatizar el flujo de trabajo de administración de incidentes con el fin de crear incidentes automáticamente.

Revisar alertas

Las siguientes tareas se realizan como parte de la revisión de las alertas:

- Nociones básicas sobre la Vista Alertas.
- Filtrar alertas según se requiera en función del tipo de origen, la gravedad, etc.
- Crear un incidente manualmente.
- Agregar alertas a un incidente existente.
- Eliminar alertas según sea necesario.

Filtrar alertas

Este procedimiento es útil cuando desea ver las alertas con un criterio específico, por ejemplo, alertas de un origen específico, alertas de una gravedad específica, alertas de un origen que no forman parte de un incidente, etc. Además, puede desglosar a detalles específicos de una alerta para analizarla e investigar más a fondo una alerta si es necesario.

Requisitos previos

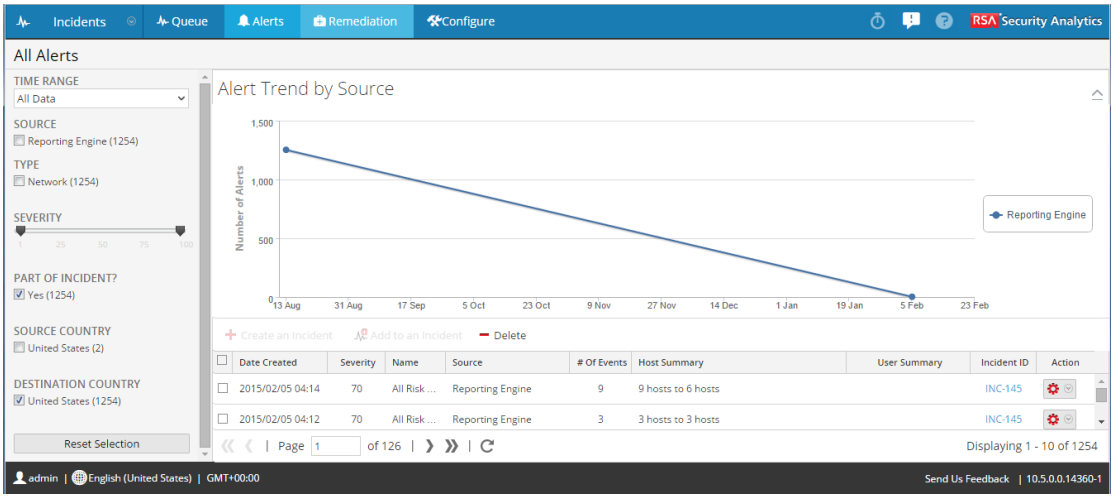
Asegúrese de que comprende los parámetros de la vista Alerta antes de proceder a filtrarla. Para obtener más información, consulte Vista Alertas.

Procedimiento

En el siguiente ejemplo se describe cómo puede personalizar la vista para mostrar todas las alertas de ESA con un nivel de gravedad 5.

1. En el menú de **Security Analytics**, seleccione **Incidentes > Alertas**.

   Se muestra la vista **Todas las alertas**.

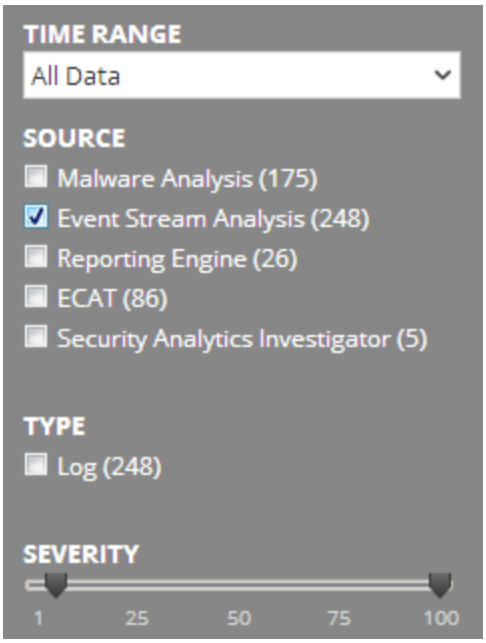


2. En el panel de opciones, seleccione **Todos los datos** para **RANGO DE TIEMPO**.

   Nota: de forma predeterminada, se muestran las alertas de los últimos cinco días. Para ver las alertas de otro periodo, cambie el rango de tiempo.

3. Seleccione **Event Stream Analysis** como **SOURCE**.

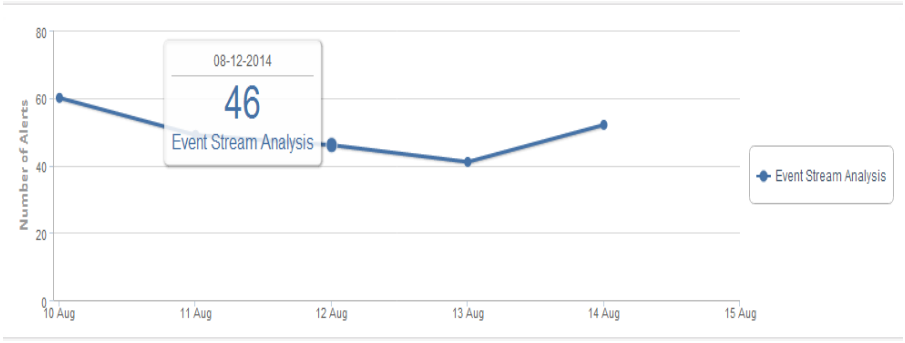
4. Establezca el nivel de **SEVERIDAD** en **5**.



El panel derecho muestra una representación gráfica de todas las alertas de ESA con gravedad 5.

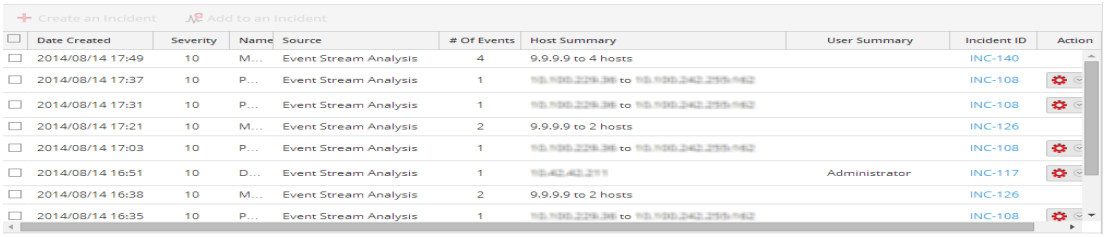
Nota: cuando no hay datos para un filtro seleccionado, el filtro se inhabilita. Haga clic en **Restablecer selección** para mostrar los criterios de selección predeterminados. Esto se aplica a alertas, incidentes y correcciones. Por ejemplo, en el gráfico anterior, si cambia el Rango de tiempo a Última hora y no hay alertas para ESA en la última hora, el origen Event Stream Analysis (0) aparecerá en gris. En tal caso, haga clic en Restablecer selección. Se muestran los criterios predeterminados para todas las opciones.

5. Mantenga el mouse sobre el gráfico para ver detalles de la cantidad de alertas activadas en un día específico.



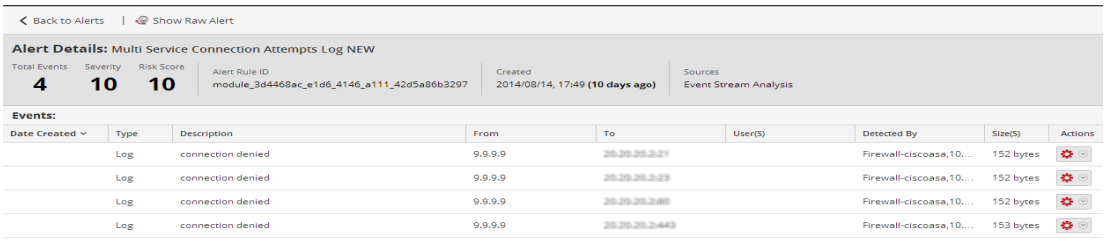
Los detalles de las alertas se muestran en la vista de detalles en la mitad inferior de la página.

Nota: Puede seleccionar una alerta para crear incidentes, agregar una alerta a un incidente existente o investigar una alerta desde esta vista. Para obtener más información, consulte Agregar alertas a un incidente existente.



6. Haga doble clic en una alerta.

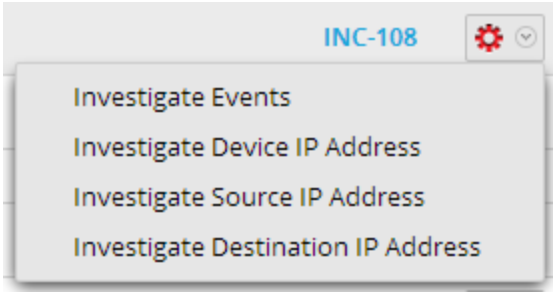
   Se muestra la vista Detalles de la alerta.



   Los detalles que se muestran son la fecha de creación, el tipo de alerta, la descripción de la alerta, la cantidad de eventos, la información de usuario y de archivo y el tamaño de la alerta. Puede investigar la alerta más a fondo si es necesario.

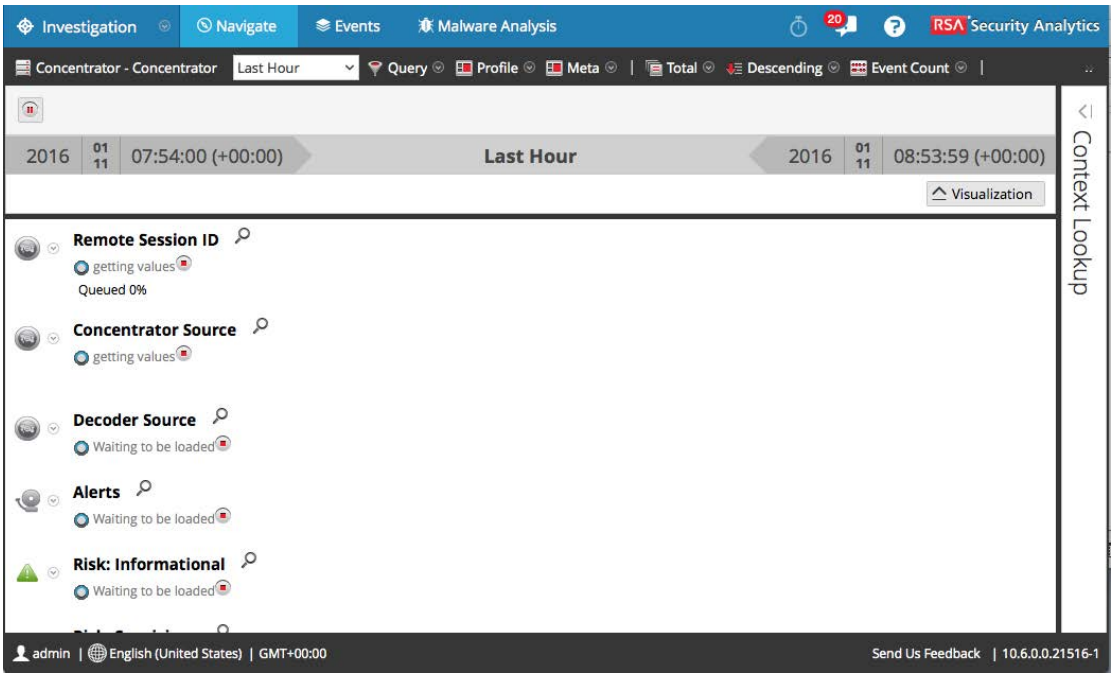
Nota: Puede hacer clic en Mostrar alerta cruda para ver la información de la alerta en formato crudo.

7. En la columna **Acciones**, seleccione **Investigar eventos**.



Nota: Las opciones disponibles en el menú Acciones difieren según los distintos tipos de alertas. Para obtener información detallada, consulte Vista Alertas.

Se muestra la vista **Investigar > Navegar** del servicio. Puede seleccionar las opciones disponibles para investigar más a fondo.



8. Haga clic en **Volver a Alertas** para navegar a la vista **Todas las alertas**.
9. Si desea restaurar los valores predeterminados, haga clic en **Restablecer selección**.

Para obtener detalles sobre los diversos parámetros y una descripción en la vista **Incidentes > Todas las alertas**, consulte Vista Alertas.

Crear un incidente manualmente

Este procedimiento es útil cuando un analista desea navegar a través de varias alertas, seleccionar las alertas necesarias para agruparlas y crear un incidente para incluir las alertas seleccionadas.

Nota: Los incidentes se pueden crear manual o automáticamente. Una alerta solo se puede asociar con un incidente. Para la creación automática de incidentes, debe crear reglas de agregación que analizarán las alertas recopiladas y las agruparán automáticamente en incidentes en función de las reglas con las cuales coinciden. Para obtener información detallada, consulte Crear una regla de agregación.

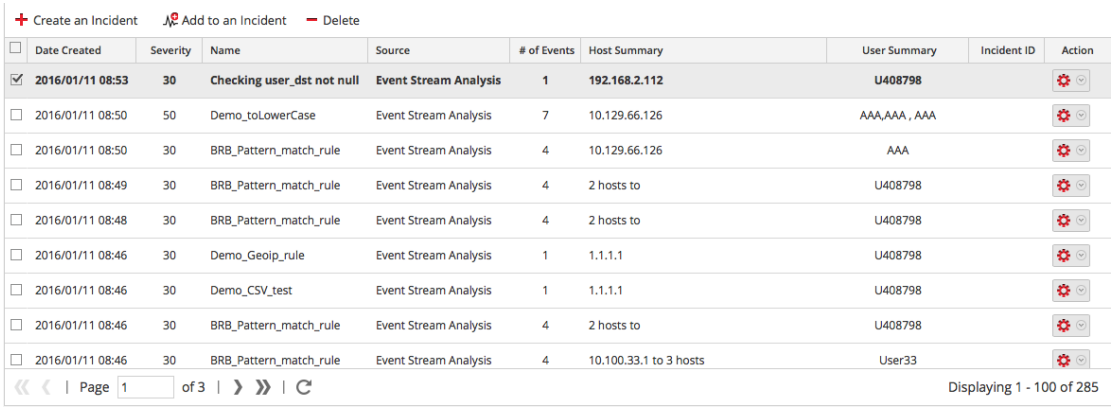
Para crear un incidente manualmente:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Alertas**.

   Se muestra la vista **Todas las alertas**.

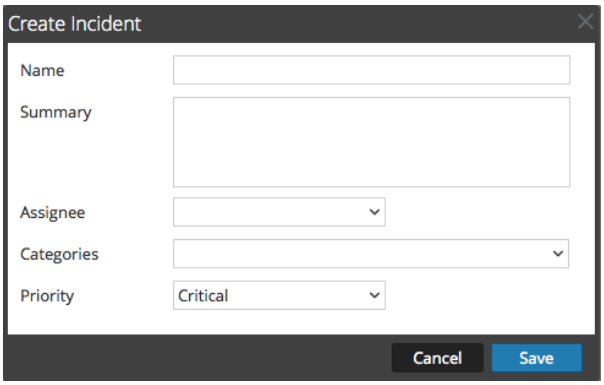
2. Seleccione una o más alertas en la vista de detalles de la alerta ven en la mitad derecha inferior de la página

   Nota: Solo cuando selecciona alertas que no tienen un ID de incidente mencionado, se activa la opción **Crear un incidente**, de lo contrario se desactiva si la alerta ya es parte de un incidente. Puede filtrar alertas que no forman parte de un incidente con la opción **Parte de un incidente** configurada como **No** en el panel de opciones.



3. Haga clic en **Crear un incidente**.

   Se muestra el cuadro de diálogo **Crear incidente**.



4. Proporcione la siguiente información:

   Nombre: escriba un nombre para identificar el incidente.

   Resumen: (opcional) escriba una descripción del incidente.

   Usuario asignado: (opcional) seleccione un usuario asignado a quien se asigna el incidente.

   Categorías: (Opcional) Seleccione una o más categorías a las cuales pertenece el incidente.

   Prioridad : seleccione una prioridad para el incidente en las opciones Crítica, Alta, Media o Baja que se muestran en la lista desplegable.

5. Haga clic en **Guardar**.

   El incidente se guarda y muestra en la vista **Incidentes > Línea de espera > Todos los incidentes**.

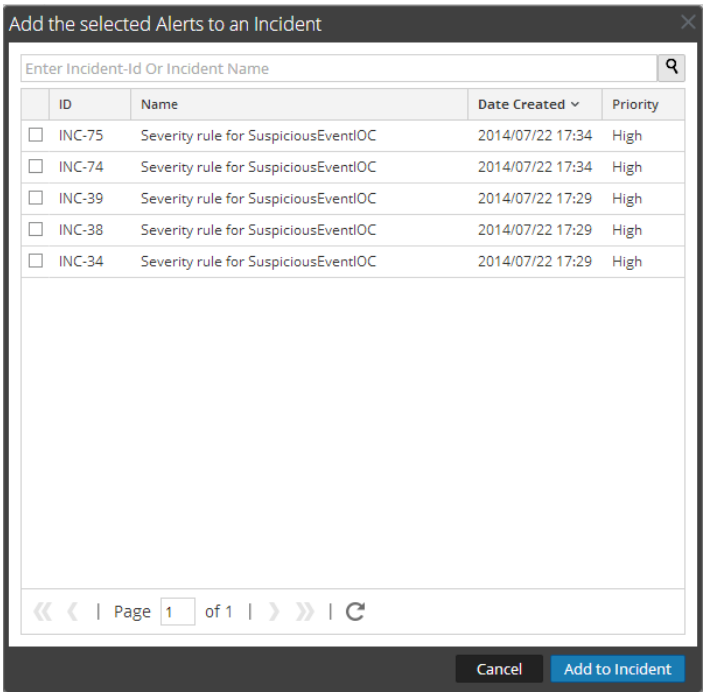
   Nota: Si se asigna el incidente a sí mismo, el incidente se guarda y muestra en la vista **Incidentes > Línea de espera > Mis incidentes**.

Agregar alertas a un incidente existente

Este procedimiento es necesario cuando tiene una alerta con un criterio particular que se ajusta a un incidente existente y no tiene que crear un nuevo incidente.

Para agregar alertas a un incidente existente:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Alertas**.
   Se muestra la vista **Todas las alertas**.
2. En la vista de detalles de las alertas de la mitad inferior derecha de la página, seleccione una o más alertas que sea necesario agregar a un incidente.
3. Haga clic en Add to an Incident.
   Se muestra el cuadro de diálogo **Agregar las alertas seleccionadas a un incidente**.
   Se muestran todos los incidentes que se le han asignado que permanecen abiertos. Puede buscar dentro del cuadro de diálogo para limitar la lista.



Nota: Solo cuando tiene una alerta sin un ID de incidente asignado, se habilita la opción **Agregar a un incidente**; de lo contrario, se deshabilita si la alerta ya es parte de un incidente.

4. En la lista que se muestra, seleccione un incidente al cual sea necesario agregar la alerta.

5. Haga clic en **Agregar a incidente**.
   Una o más alertas seleccionadas son ahora parte del incidente elegido y tendrán un ID de incidente.

Eliminar alertas

Este procedimiento es útil cuando hay alertas no deseadas o irrelevantes. La eliminación de estas alertas libera espacio en disco.

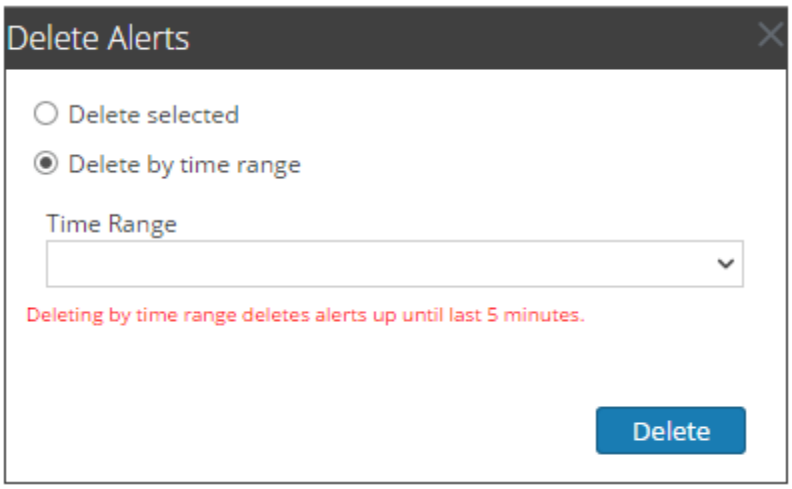
Requisitos previos

Se le debe asignar la función de administrador.

Procedimiento

Para eliminar alertas:

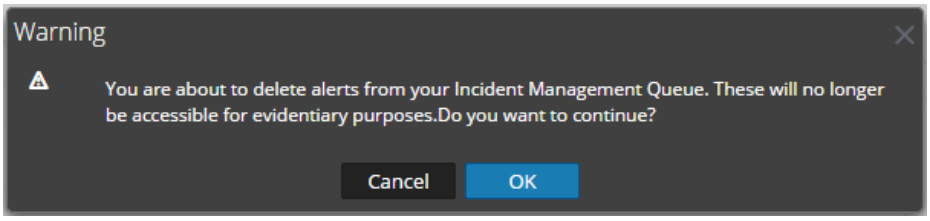
1. En el menú de **Security Analytics**, seleccione **Incidentes > Alertas**.
   Se muestra la vista Todas las alertas.
2. Si desea eliminar ciertas alertas, seleccione cada una de ellas.
3. Haga clic en Delete.



4. Ejecute una de las siguientes acciones:
   - Haga clic en **Eliminar seleccionada** para eliminar las alertas seleccionadas con anterioridad.
   - Seleccione **Eliminar por rango de tiempo**, elija el rango de tiempo y, a continuación, haga clic en **Eliminar**.

Nota: Cuando realiza una eliminación por rango de tiempo, elimina alertas hasta la última hora.

5. Haga clic en **Aceptar**.
   Se muestra un cuadro de diálogo de confirmación.



6. Haga clic en **Aceptar** para eliminar las alertas.

Resultado

Se elimina cada alerta seleccionada. Se aplican las siguientes condiciones:

- Si una alerta eliminada es la única alerta en un incidente, el incidente también se elimina.
- Si la alerta eliminada no es la única alerta en un incidente, el incidente se actualiza para reflejar la eliminación.
- Puede agregar manualmente una alerta que formaba parte de un incidente eliminado a un incidente nuevo o existente.
- El motor de reglas no selecciona automáticamente ninguna alerta que formaba parte de un incidente eliminado.

Flujo del proceso de administración de incidentes

Como parte del flujo del proceso de Incident Management, puede editar incidentes para modificar sus parámetros según sea necesario, eliminar incidentes, asignarlos a distintos usuarios y rastrearlos y monitorearlos hasta su cierre.

En la siguiente lista se presentan varias tareas que se realizan como parte del proceso de administración de incidentes:

- Ver la línea de espera de incidentes
- Ver detalles de incidentes
- Editar incidentes
- Investigar un incidente
    - Agregar una entrada del registro
    - Crear una tarea de corrección
    - Enviar una tarea de corrección como un vale de help desk
    - Enviar una tarea de corrección a RSA Archer
    - Cerrar un incidente
- Eliminar incidentes

Ver la línea de espera de incidentes

Los administradores y los analistas pueden ver incidentes en la línea de espera de incidentes. Puede ver los incidentes asignados o todos los incidentes, también puede ver la línea de espera mediante distintos filtros.

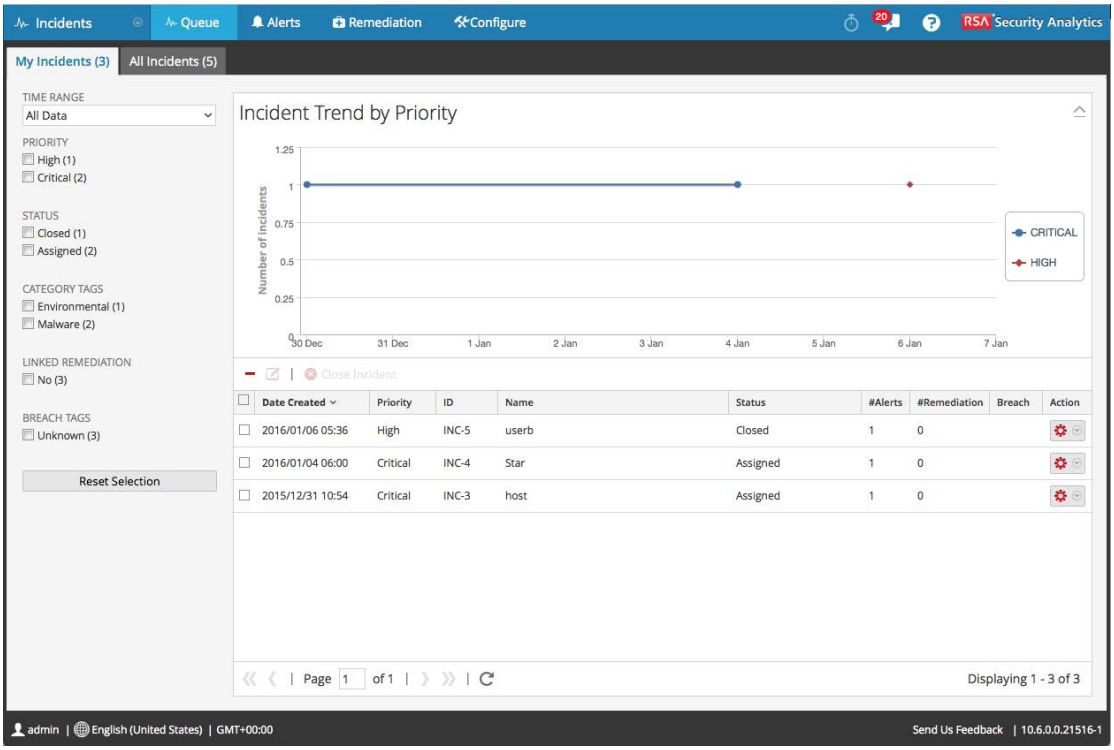
Para ver la línea de espera de incidentes:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Línea de espera**.

   De forma predeterminada se muestra la vista **Mis incidentes**. Aquí se muestra una lista de incidentes asignados a usted.

   El panel de la derecha muestra la representación gráfica de los incidentes que se le asignaron. El gráfico muestra la tendencia de los incidentes por prioridad y presenta una línea por prioridad.

   Para obtener detalles sobre los diversos parámetros que se muestran y su descripción, consulte Vista Línea de espera de incidentes.

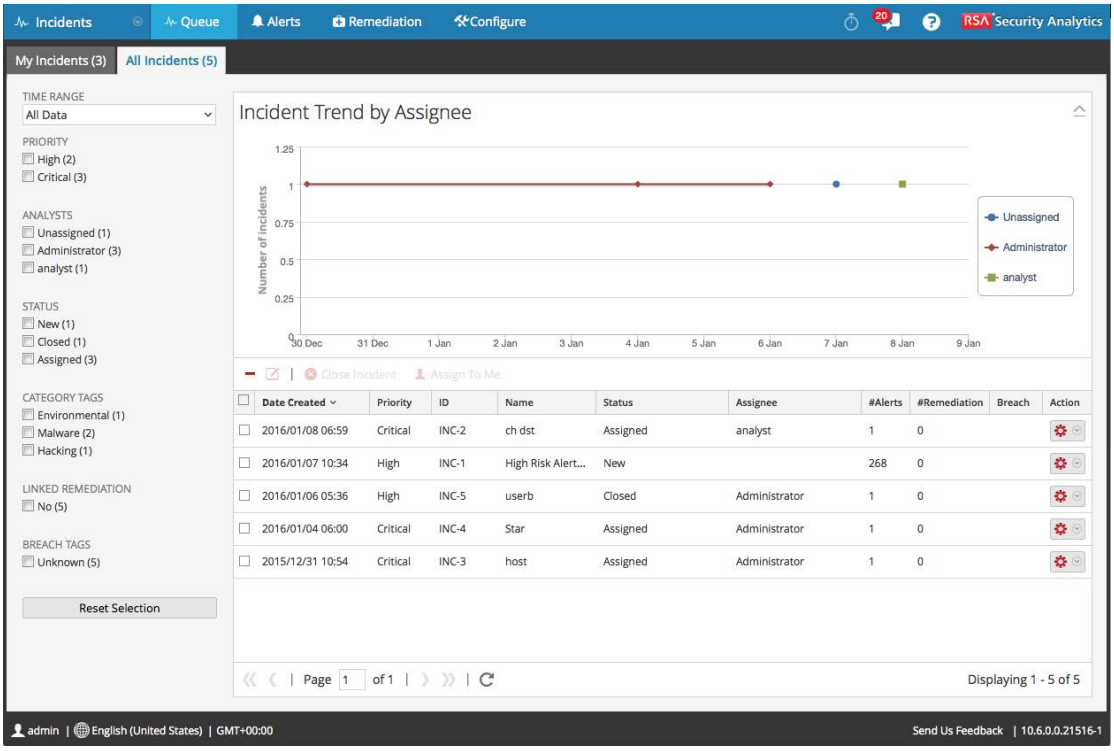


2. Seleccione **Todos los incidentes**.

   La vista Todos los incidentes se muestra con una lista de todos los incidentes.

   El panel de la derecha muestra la representación gráfica de la tendencia de los incidentes por usuario asignado y presenta una línea por usuario asignado.

Para obtener detalles sobre los diversos parámetros que se muestran y su descripción, consulte Vista Línea de espera de incidentes.



Ver detalles de incidentes

Este procedimiento es necesario cuando se debe investigar más un incidente y decidir cómo proceder con su corrección, además de hacerle un seguimiento para cerrarlo.

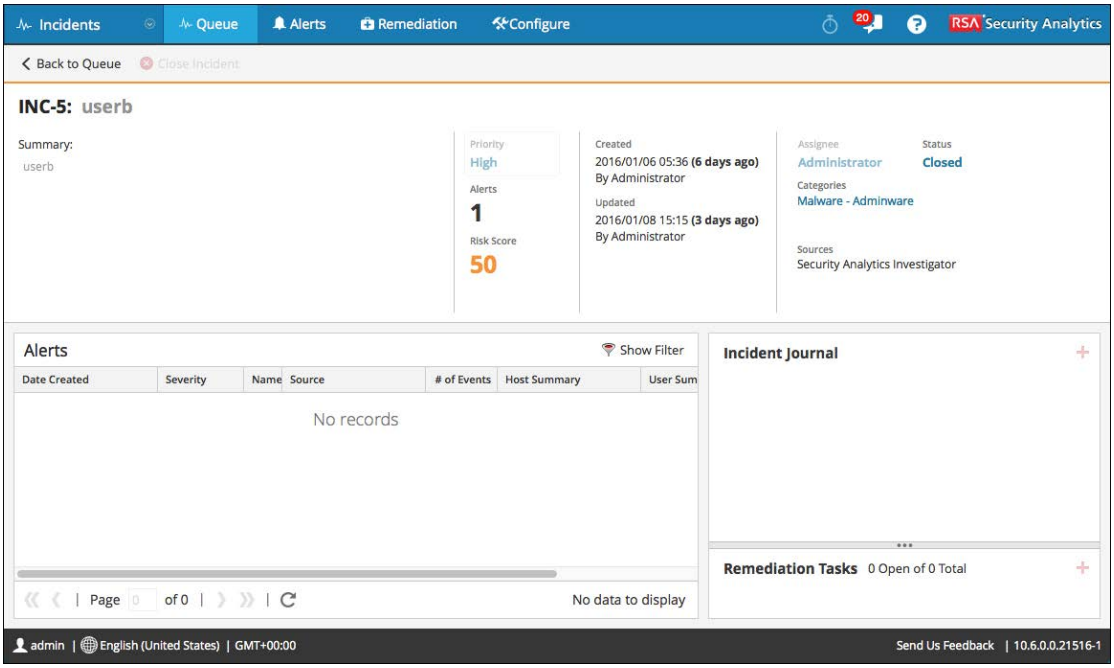
Para acceder y ver detalles de incidentes:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Línea de espera**.

   Se muestra la vista **Mis incidentes**. Enumera todos los incidentes asignados a usted. La vista **Todos los incidentes** enumera todos los incidentes en Security Analytics.

2. En la vista **Mis incidentes**, haga doble clic en un incidente.

   Se muestra la página Detalles de incidente.



La página Detalles de incidente muestra todos los detalles relacionados con el incidente. Puede analizar los datos y realizar las siguientes operaciones desde esta vista:

- Descubra el contexto y el riesgo del incidente mediante la visualización de alertas y/o sus eventos, o mediante el uso del menú de acciones para investigar los eventos relacionados.
- Rastree el progreso del flujo de trabajo en el incidente mediante su asignación al analista adecuado, la configuración de la prioridad, el registro del estado de la investigación o la categorización del incidente.
- Documente los resultados de la investigación con el Diario de incidentes o haga un seguimiento del proceso de corrección con Tareas de corrección.

Ver detalles de incidentes

Este procedimiento es necesario cuando se debe investigar más un incidente y decidir cómo proceder con su corrección, además de hacerle un seguimiento para cerrarlo.

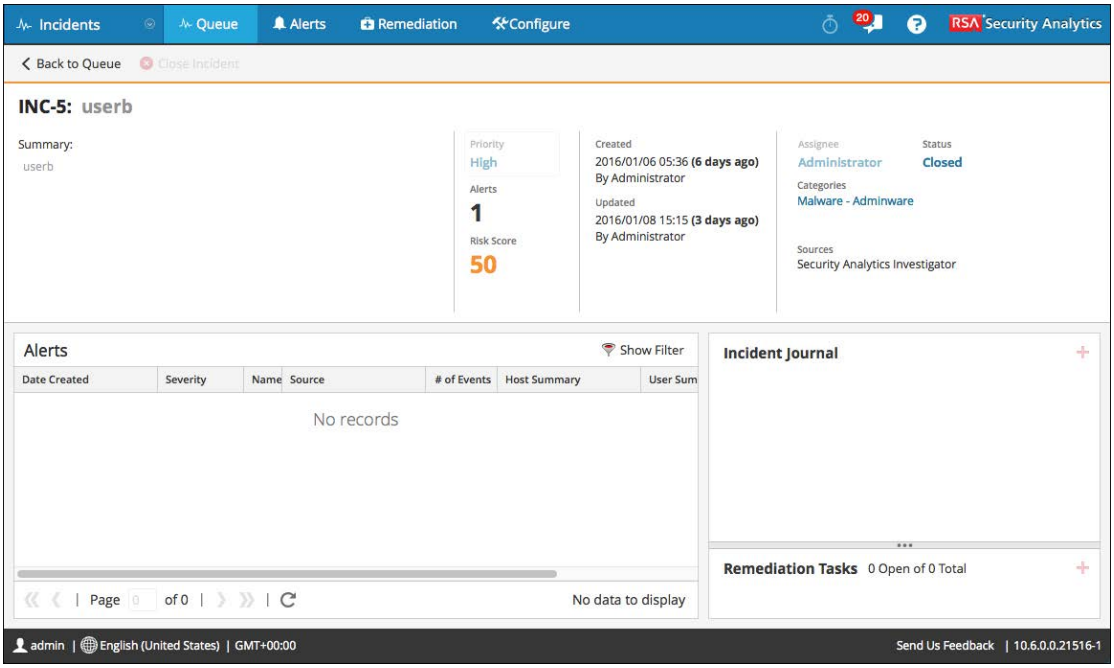
Para acceder y ver detalles de incidentes:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Línea de espera**.

   Se muestra la vista **Mis incidentes**. Enumera todos los incidentes asignados a usted. La vista **Todos los incidentes** enumera todos los incidentes en Security Analytics.

2. En la vista **Mis incidentes**, haga doble clic en un incidente.

   Se muestra la página Detalles de incidente.



La página Detalles de incidente muestra todos los detalles relacionados con el incidente. Puede analizar los datos y realizar las siguientes operaciones desde esta vista:

- Descubra el contexto y el riesgo del incidente mediante la visualización de alertas y/o sus eventos, o mediante el uso del menú de acciones para investigar los eventos relacionados.
- Rastree el progreso del flujo de trabajo en el incidente mediante su asignación al analista adecuado, la configuración de la prioridad, el registro del estado de la investigación o la categorización del incidente.
- Documente los resultados de la investigación con el Diario de incidentes o haga un seguimiento del proceso de corrección con Tareas de corrección.

- En casos donde existen pruebas de una vulneración de datos, infórmelo al equipo de cumplimiento de las normas.
- Cierre el incidente una vez que finalice la investigación.

3. Haga clic en **Volver a línea de espera** para volver a la vista Incidentes.

Editar incidentes

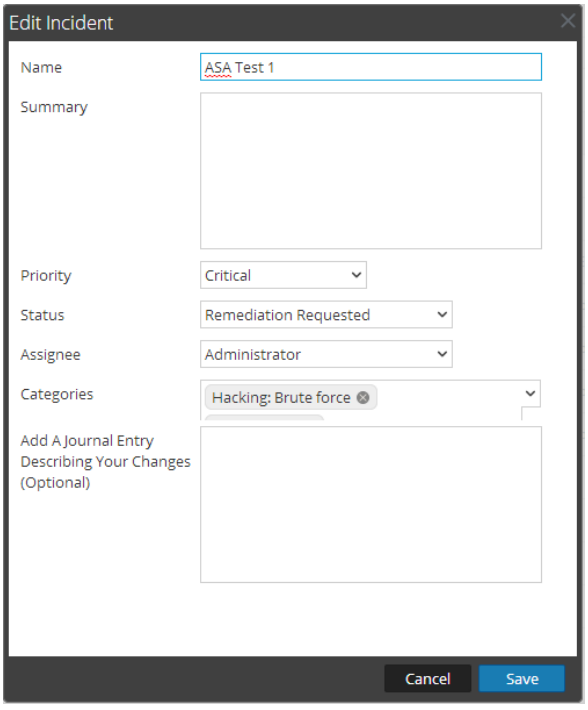
Puede editar incidentes en una de las siguientes maneras:

- **Editar un incidente**: use este método cuando necesite modificar detalles de un único incidente.
- **Editar incidentes en masa**: use este método cuando necesite modificar un criterio específico de varios incidentes.

Editar un incidente

1. En el menú de **Security Analytics**, seleccione **Incidentes > Línea de espera**.
2. En la vista **Todos los incidentes**, seleccione un incidente.
3. Haga clic en .

   Se muestra el cuadro de diálogo **Editar incidente**.



Nota: como alternativa, puede seleccionar Editar incidente en la columna de acciones del incidente seleccionado.

4. Modifique los valores necesarios.
5. Haga clic en **Guardar**.

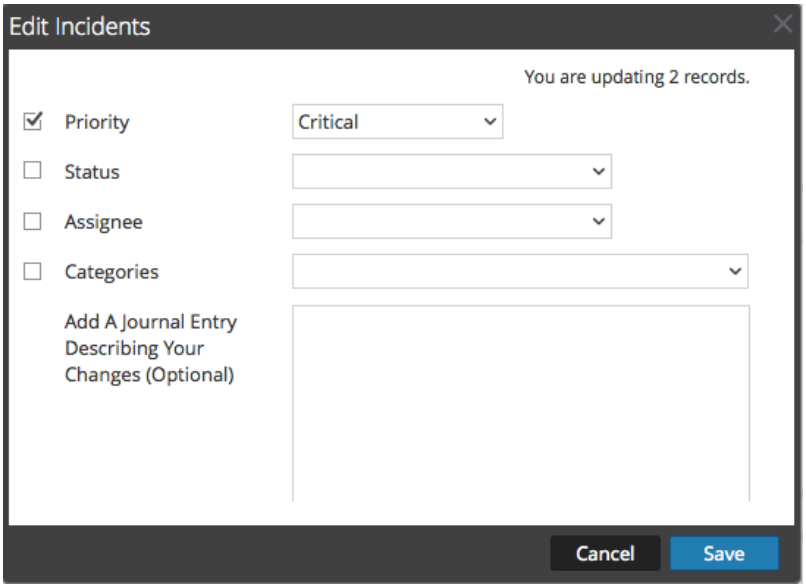
   El incidente editado se muestra en la vista **Todos los incidentes**.

Nota: este procedimiento también se puede realizar de manera similar en la vista Mi incidente.

Editar incidentes en masa

1. En el menú de **Security Analytics**, seleccione **Incidentes > Línea de espera**.
2. En la vista **Todos los incidentes**, seleccione 2 o más incidentes.
3. Haga clic en  .

   Se muestra el cuadro de diálogo **Editar incidentes**.



4. Modifique los valores necesarios.

   Los valores que se pueden modificar en masa son Prioridad, Estado, Usuario asignado y Categorías. Si selecciona una casilla de verificación, cualquier modificación en los valores de ese campo (incluida la desactivación del valor) se aplica a ese campo para todos los incidentes seleccionados. Si la casilla de verificación no se selecciona, ese campo permanece sin cambios para los incidentes seleccionados.

5. Haga clic en **Guardar**.

   Los incidentes editados se muestran en la vista **Todos los incidentes**.

Nota: este procedimiento también se puede realizar de manera similar en la vista **Mis incidentes**.

Investigar un incidente

Una vez creado un incidente de forma manual o mediante el uso de un proceso automatizado, el siguiente paso es investigar el incidente, crear una tarea de corrección, agregar entradas de registro para incluir detalles e información adicional del incidente, hacer un seguimiento de las tareas de corrección para cierre, enviar las tareas como vale de help desk para resolverlas y finalmente desactivar el incidente.

Las diferentes etapas de la investigación de un incidente y las acciones que realiza un administrador se resumen en la siguiente tabla.

Tareas	Referencia
1. Acceder y ver detalles de incidentes.	Consulte Ver detalles de incidentes.
2. Agregar una entrada del registro.	Consulte Agregar una entrada del registro.
3. Crear y hacer un seguimiento de una tarea de corrección.	Consulte Crear una tarea de corrección.
4. Enviar una tarea de corrección como un vale de help desk	Consulte Enviar una tarea de corrección como un vale de help desk.
5. Cerrar un incidente.	Consulte Cerrar un incidente.

Temas

- Agregar una entrada del registro
- Crear una tarea de corrección
- Enviar una tarea de corrección como un vale de help desk
- Enviar una tarea de corrección a RSA Archer
- Cerrar un incidente

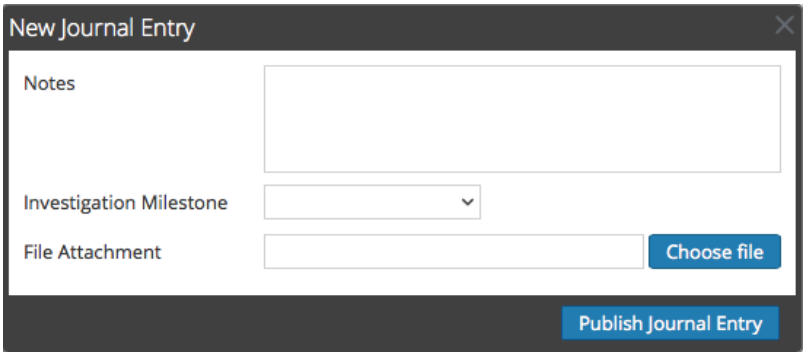
Agregar una entrada del registro

Se crea una entrada de registro para un incidente con el fin de capturar información adicional con respecto al incidente que ayude al usuario asignado a comprenderlo y rastrearlo de mejor manera.

Procedimiento

Para crear una entrada de diario para un incidente:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Línea de espera**.
   Se muestra la vista Mis incidentes.
2. En la vista **Mis incidentes**, haga doble clic en un incidente.
   Se muestra la vista Detalles de incidente.
3. En **Diario de incidentes**, haga clic en 
   Se muestra el cuadro de diálogo Nueva entrada de diario.



4. Proporcione la información requerida. Se requiere el campo Notas. Escriba la información útil pertinente en el campo Notas para describir la investigación. El modelo de investigación y los archivos adjuntos son opcionales y se pueden incluir cuando sea útil para una investigación más a fondo. Las opciones del modelo de investigación son: Reconocimiento, distribución, explotación, instalación, comando y control, acción en objetivo, contención, erradicación y cierre.
5. Haga clic en **Publicar entrada de diario**.
   La entrada de diario se crea y se muestra en **Diario de incidentes**.

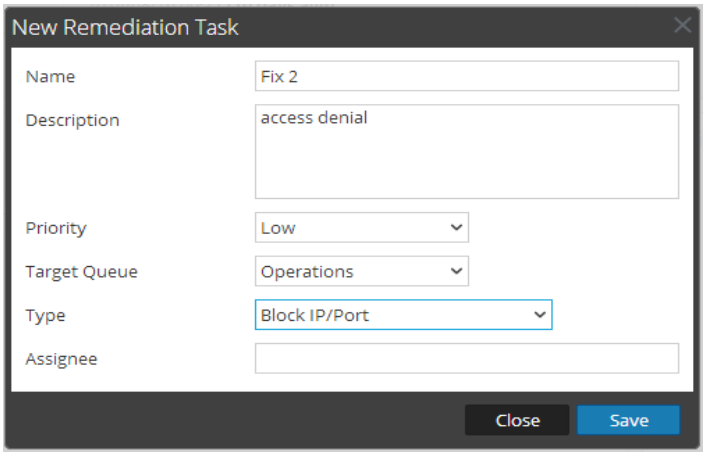
Crear una tarea de corrección

Cuando ha investigado un incidente y ha identificado la causa, puede crear una tarea de corrección, asignarla a un grupo específico y rastrearla hasta el cierre.

Procedimientos

Crear una tarea de corrección

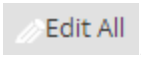
1. En el menú de Security Analytics, seleccione **Incidentes > Línea de espera**.
   Se muestra la pestaña Mis incidentes.
2. En la pestaña **Mis incidentes**, haga doble clic en un incidente.
   Se muestra la vista Detalles de incidente.
3. En **Tareas de corrección**, haga clic en 
   Se muestra el cuadro de diálogo Nueva tarea de corrección.



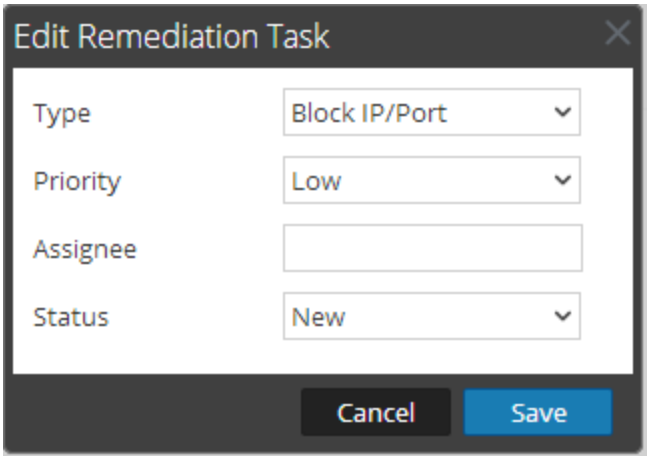
4. Proporcione la siguiente información:
   Nombre: nombre de la tarea de corrección.
   Descripción: (opcional) ingrese información que describa la tarea de corrección.
   Prioridad: seleccione la prioridad de la tarea: Baja, Media, Alta o Crítico.
   Línea de espera de destino: seleccione la línea de espera objetivo según el tipo de tarea: Operaciones, GRC o mejora del contenido.
   Tipo: seleccione un tipo de tarea: Host en cuarentena, dispositivo de red en cuarentena, bloquear IP/puerto, bloquear acceso externo a DMZ, bloquear acceso a VPN, volver a crear la imagen del host, actualizar política de firewall, actualizar política de IDS/IPS, actualizar política de proxy web, actualizar política de acceso, actualizar política de VPN o personalizado.
   Usuario asignado: (opcional) escriba el nombre del usuario a quien se va a asignar la tarea.

5. Haga clic en **Guardar**.
   La tarea de corrección se indica bajo Tareas de corrección.

Modificar una tarea de corrección

1. En el menú de Security Analytics, seleccione **Incidentes > Línea de espera**.
   Se muestra la vista Mis incidentes.
2. En la vista **Mis incidentes**, haga doble clic en un incidente.
   Se muestra la vista Detalles de incidente.
3. En **Tareas de corrección**, haga doble clic en una tarea de corrección.
   Se muestra la vista Detalles de tarea de corrección.
4. Haga clic en 

.
   Se muestra el cuadro de diálogo Editar tarea de corrección.



5. Modifique los campos obligatorios.
6. Haga clic en **Guardar**.

Nota: Como alternativa, puede hacer clic en el parámetro que desea modificar en el panel superior y modificar el valor cuando se requiera.

Enviar una tarea de corrección como un vale de help desk

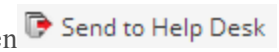
Puede enviar una tarea de corrección como vale de help desk, donde se puede administrar en un sistema de help desk de otros fabricantes y se puede rastrear para su cierre.

Requisitos previos

Asegúrese de haber activado la integración con el sistema de vales del help desk de otros fabricantes. Consulte Configurar ajustes de integración para administrar incidentes en Security Analytics para obtener más información.

Procedimiento

Para enviar una tarea de corrección como un vale de help desk:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Línea de espera**.
   Se muestra la vista Mis incidentes.
2. En la vista **Mis incidentes**, haga doble clic en un incidente.
   Se muestra la vista Detalles de incidente.
3. En **Tareas de corrección**, haga doble clic en una tarea de corrección.
   Se muestra la vista Detalles de tarea de corrección.
4. Haga clic en 

   La tarea de corrección se envía al sistema de vales de help desk.
5. Haga clic en 

para ver el vale en el sistema de help desk.

Enviar una tarea de corrección a RSA Archer

Puede enviar las tareas de corrección a la línea de espera de destino de Archer e informar vulneraciones de datos y rastrearlas a través del proceso de respuesta a vulneraciones en la solución RSA Security Operations Management.

Requisitos previos

Asegúrese de haber activado la integración con RSA Archer. Consulte Configurar ajustes de integración para administrar incidentes en RSA Archer Security Operations para obtener detalles.

Procedimiento

Para enviar una tarea de corrección a RSA Archer:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Línea de espera**.
   Se muestra la vista Mis incidentes.
2. En la vista **Mis incidentes**, haga doble clic en un incidente.
   Se muestra la vista Detalles de incidente.
3. En **Tareas de corrección**, haga doble clic en una tarea de corrección.
   Se muestra la vista Detalles de tarea de corrección.
4. Haga clic en 

.
   La tarea de corrección se envía a RSA Archer.
5. Navegue a la interfaz del usuario de RSA Archer UI para ver y rastrear la tarea de corrección hasta el cierre.

Cerrar un incidente

Una vez que encuentra una solución después de investigar un incidente y lo corrige, el incidente se cierra.

Procedimiento

Para cerrar un incidente:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Línea de espera**.
   Se muestra la vista Mis incidentes.
2. En la vista **Mis incidentes**, seleccione un incidente.
3. Haga clic en 

   El incidente se cierra y su estado se muestra como **Cerrado** en la vista Incidentes.

Nota: como alternativa, puede cerrar el incidente si selecciona **Cerrar incidente** en la columna **Acciones** del incidente o si elige **Cerrar incidente** en la vista Detalles de incidente de un incidente.

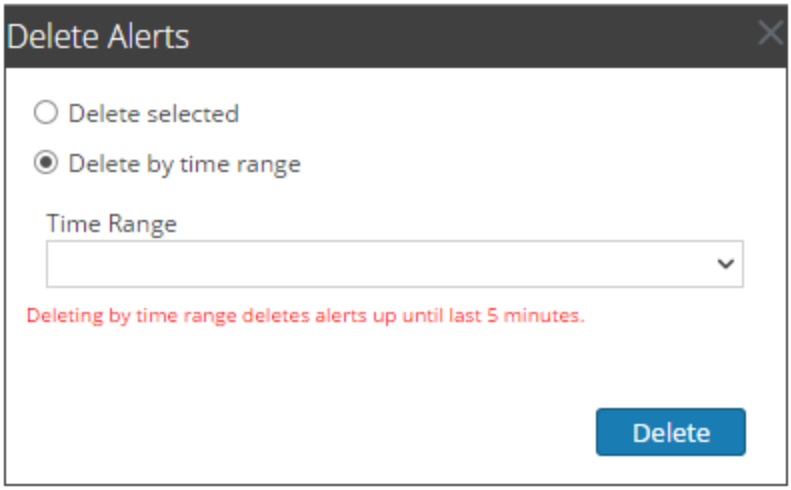
Eliminar incidentes

Este procedimiento es útil para liberar espacio en disco mediante la eliminación de incidentes que no se necesitan.

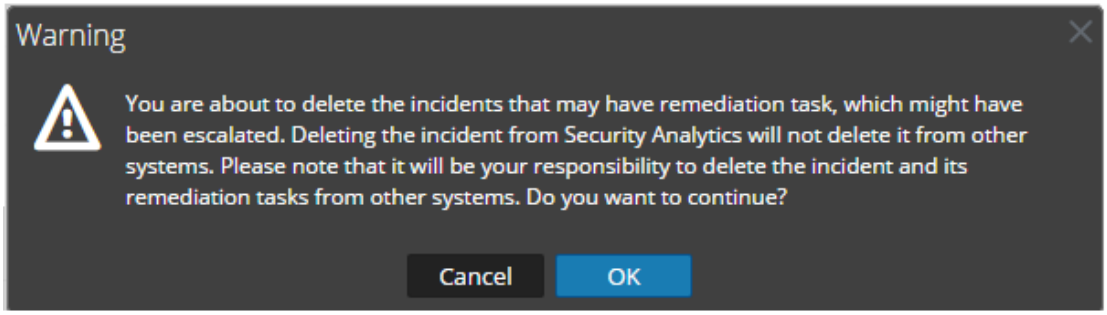
Procedimiento

1. En el menú de **Security Analytics**, seleccione **Incidentes > Línea de espera**.
   Se muestra la pestaña Mis incidentes.
2. Seleccione la pestaña **Todos los incidentes** para ver todos los incidentes para todos los analistas.
3. Ejecute una de las siguientes acciones:
   - Seleccione cada incidente que desee eliminar y haga clic en Delete .
   - Haga clic en Delete , elija **Eliminar por rango de tiempo** y seleccione el periodo cuyas alertas se eliminarán.

3. Haga clic en **Aceptar**.



4. Se muestra un cuadro de diálogo de confirmación.



5. Haga clic en **Aceptar** para eliminar los incidentes.

Resultado

Los incidentes eliminados, incluidas entradas del registro y tareas de corrección, se eliminan. Estos dejarán de estar accesibles con fines probatorios.

Las alertas que estaban asociadas a un incidente eliminado continúan apareciendo en la pestaña Alertas y puede agregarlas manualmente a otro incidente. Sin embargo, el motor de reglas ya no las seleccionará ni las agrupará automáticamente en incidentes.

Un registro de auditoría registra la cantidad de incidentes que se eliminaron.

Automatizar el proceso de administración de incidentes

Puede automatizar el flujo de trabajo para evitar la intervención manual siempre que sea necesario para facilitar su uso. Puede crear y administrar usuarios y permisos de usuarios que se requieren para investigar los incidentes, y crear reglas de agregación para agrupar alertas según los criterios especificados y crear incidentes automáticamente. Estos incidentes creados se investigan más detalladamente, como se describe en Proceso de administración de incidentes.

En la siguiente lista se indican los procedimientos para automatizar el proceso de administración de incidentes:

- Agregar usuario con permiso requerido para investigar los incidentes asignados. Para obtener más información, consulte **Administrar usuarios con funciones y permisos** en la guía *Administración de usuarios y de la seguridad del sistema*.
- Establecer la configuración de notificaciones para enviar notificaciones por correo electrónico una vez que los incidentes se crean y pasan por varias etapas del flujo de trabajo de administración de incidentes.
- Crear una regla de agregación para agrupar alertas en incidentes en función del conjunto de criterios.
- Configurar un periodo de retención para alertas e incidentes
- Ocultar datos privados: Valores de hash para claves de metadatos que contienen datos confidenciales, como nombres de host, nombres de usuario y direcciones IP.

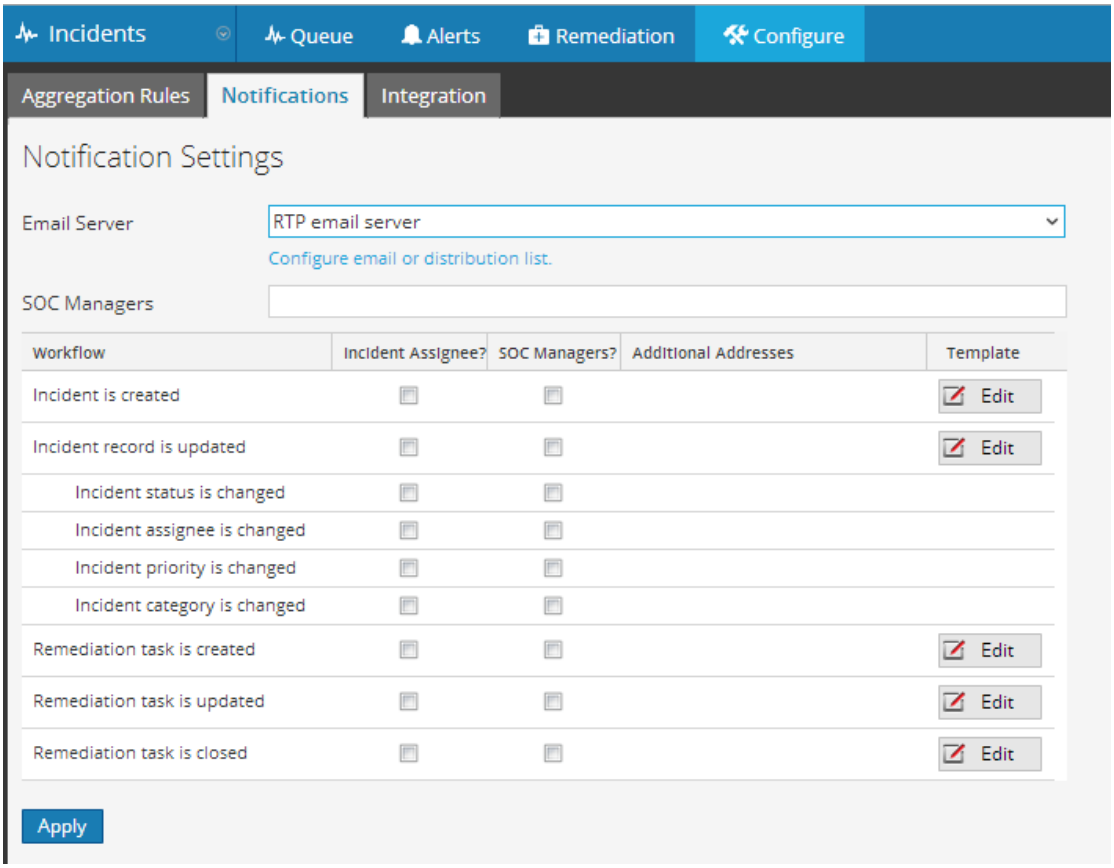
Establecer la configuración de notificaciones

El establecimiento de la configuración de notificaciones permite un mecanismo de notificación para diversas operaciones realizadas durante el flujo de trabajo de Administración de incidentes.

Para establecer la configuración de notificaciones:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Configurar**.
2. Haga clic en **Notificaciones**.

   Se muestra la vista Configuración de notificaciones.



3. Proporcione la siguiente información para establecer diversas configuraciones de notificaciones.

Parámetro	Descripción
Servidor de correo electrónico	En la lista desplegable, seleccione la dirección del servidor de correo electrónico que se va a configurar para enviar notificaciones por correo cuando la configuración de notificaciones está activada. Si no hay una dirección de servidor de correo electrónico configurada, no verá un servidor de correo electrónico en la lista desplegable. Tiene que configurar un servidor de correo electrónico antes de continuar con este procedimiento. Para configurar el servidor de correo electrónico, haga clic en **Configurar correo electrónico o lista de distribución** y proporcione los detalles requeridos. Consulte **Configurar el servidor de correo electrónico y la cuenta de notificaciones** en la *Guía de configuración del sistema* para saber cómo configurar un servidor de correo electrónico.
Administradores del SOC	Escriba las direcciones de correo electrónico del Administrador del SOC a las cuales se envía un correo de notificación de las operaciones seleccionadas.
¿Usuario asignado al incidente?	Seleccione si desea que se envíe una notificación por correo electrónico, a quien se le asigna el incidente, por el flujo de trabajo correspondiente cada vez que se asigna un incidente.
¿Administrador del SOC?	Seleccione si desea que se envíe una notificación por correo electrónico al grupo de administradores del SOC para el flujo de trabajo correspondiente. Esto corresponde a las direcciones de correo electrónico del administrador que se proporcionan en **Administradores del SOC**.
Direcciones adicionales	Escriba las direcciones adicionales a las que desea que se envíen las notificaciones por correo electrónico para el flujo de trabajo correspondiente.

4. (Opcional) En la columna **Plantilla**, haga clic en Edit para modificar la plantilla para cualquier flujo de trabajo.
5. Haga clic en **Aplicar** para guardar la configuración de notificaciones.

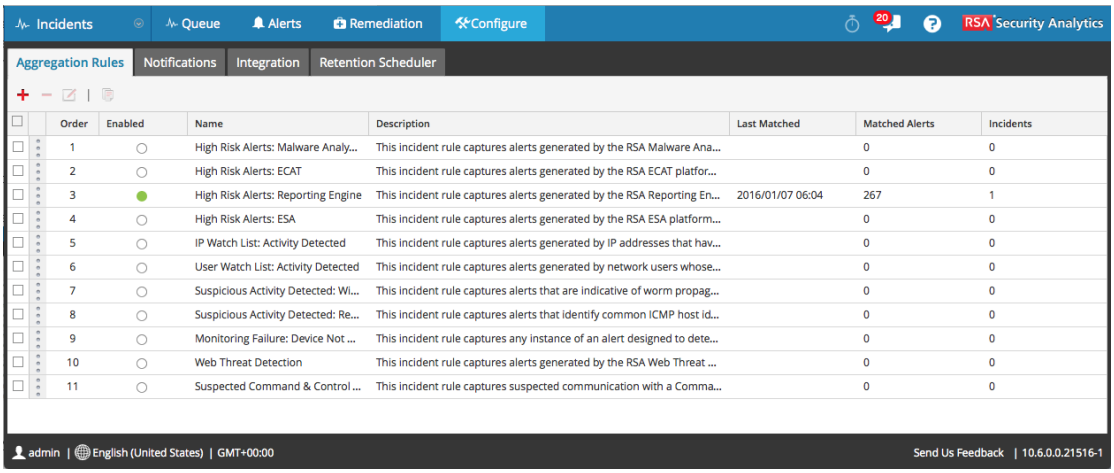
Crear una regla de agregación

Puede crear reglas de agregación con diversos criterios para automatizar el proceso de creación de incidentes. Las alertas que cumplen con los criterios de la regla se agrupan para formar un incidente. Esto es útil cuando se sabe que un conjunto específico de alertas se puede agrupar en un incidente y se puede configurar una regla de agregación que se encargue de agrupar las alertas en lugar de desperdiciar tiempo en crear manualmente un incidente y agregar en él las alertas de manera individual. Para crear incidentes automáticamente, debe crear una regla de agregación.

Para crear una regla de agregación:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Configurar**.
2. Seleccione **Reglas de agregación**.

   Se muestra la vista **Reglas de agregación**.



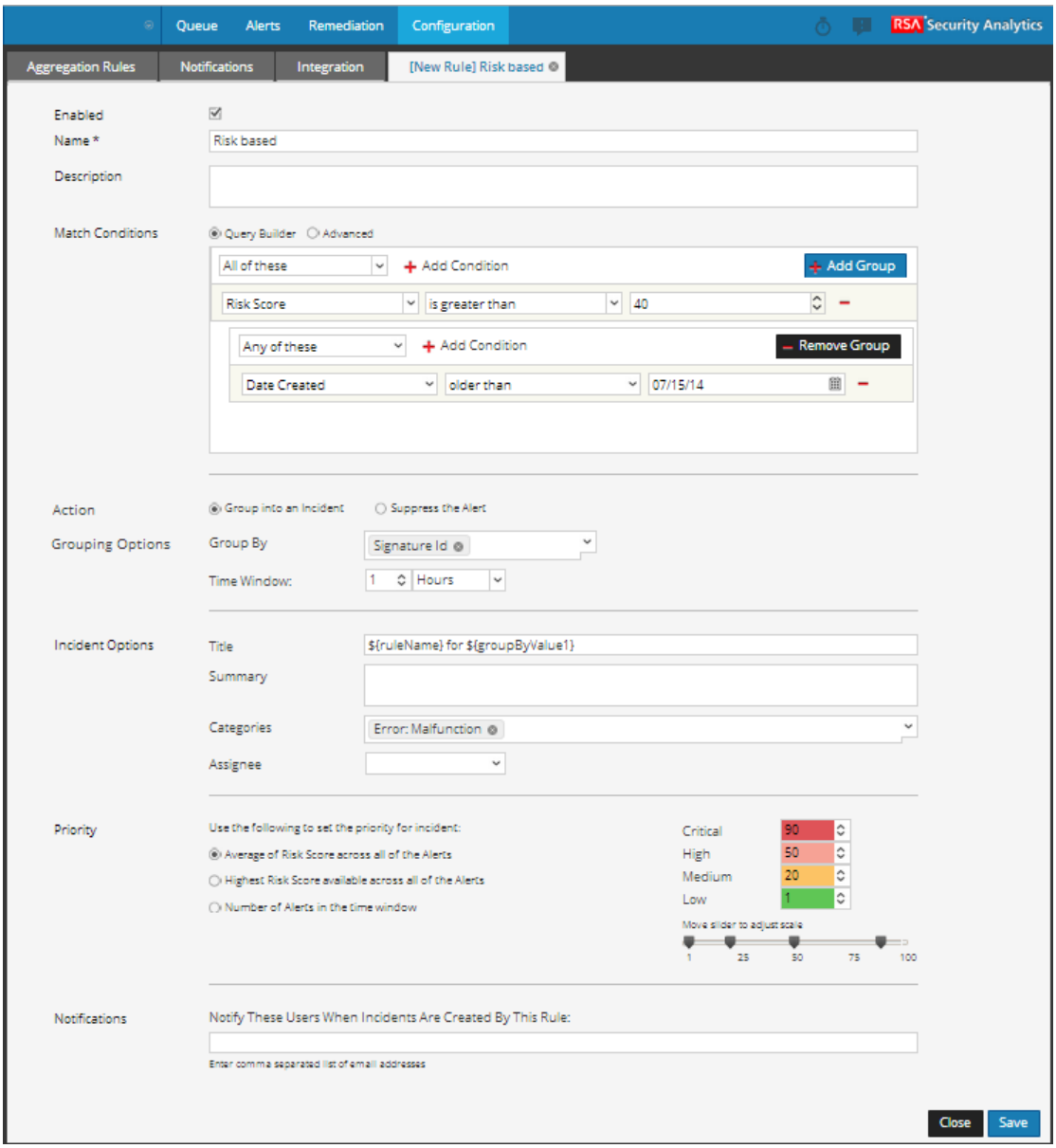
   Se muestra una lista de nueve reglas predefinidas. Puede realizar una de las siguientes acciones:

   - agregar una nueva regla
   - editar una regla existente
   - clonar una regla

3. Para agregar una nueva regla, seleccione  .

   Se muestra la pestaña **Nueva regla**.

   En el siguiente ejemplo se muestra la agrupación de alertas en un incidente en función del puntaje de riesgo.



4. Haga clic en **Guardar**.

   La regla se muestra en la vista **Reglas de agregación**. La regla se activa y comienza a crear incidentes de acuerdo con las alertas entrantes que coinciden con los criterios seleccionados.

Consulte también:

- Para obtener detalles sobre los diversos parámetros que se pueden configurar como criterios para una regla de agregación, consulte Pestaña Nueva regla.
- Para obtener detalles sobre la descripción de los parámetros y los campos de la vista Reglas de agregación, consulte Pestaña Reglas de agregación.

Configurar un periodo de retención para alertas e incidentes

En ocasiones, los encargados de la privacidad de datos desean conservar datos durante cierto periodo y después eliminarlos. Un periodo de retención más breve libera espacio en disco antes. En algunos casos, el periodo de retención debe ser breve. Por ejemplo, las leyes de Europa establecen que los datos confidenciales no se pueden conservar durante más de 30 días. Después de 30 días, los datos se deben ocultar o eliminar.

La configuración de un periodo de retención para los datos es un procedimiento opcional. El momento en que Incident Management recibe alertas y crea un incidente determina cuándo comienza la retención. Los períodos de retención varían entre 30 y 365 días. Si configura un periodo de retención, los datos se eliminan de manera definitiva un día después de la finalización del periodo.

La retención se basa en el momento en que IM recibe las alertas y en la hora de creación del incidente.

Precaución: Los datos que se eliminan después del periodo de retención no se pueden recuperar.

Cuando vence el periodo de retención, los siguientes datos se **eliminan de manera definitiva**:

- Alertas
- Incidentes
- Tareas de corrección
- Entradas del registro
- Archivos adjuntos para los anteriores

Los registros rastrean la retención y la eliminación manual, de modo que puede ver lo que se eliminó. Para ver im.log, haga clic en **Administration > Servicios**. Seleccione un servicio de Incident Management y haga clic en **Ver > Registros**. Para ver registros de auditoría, vaya a /opt/rsa/im/logs en el servidor de Security Analytics.

La función no se aplica a Archer ni a otras herramientas de SOC de otros fabricantes. Las alertas y los incidentes de otros sistemas se deben eliminar por separado.

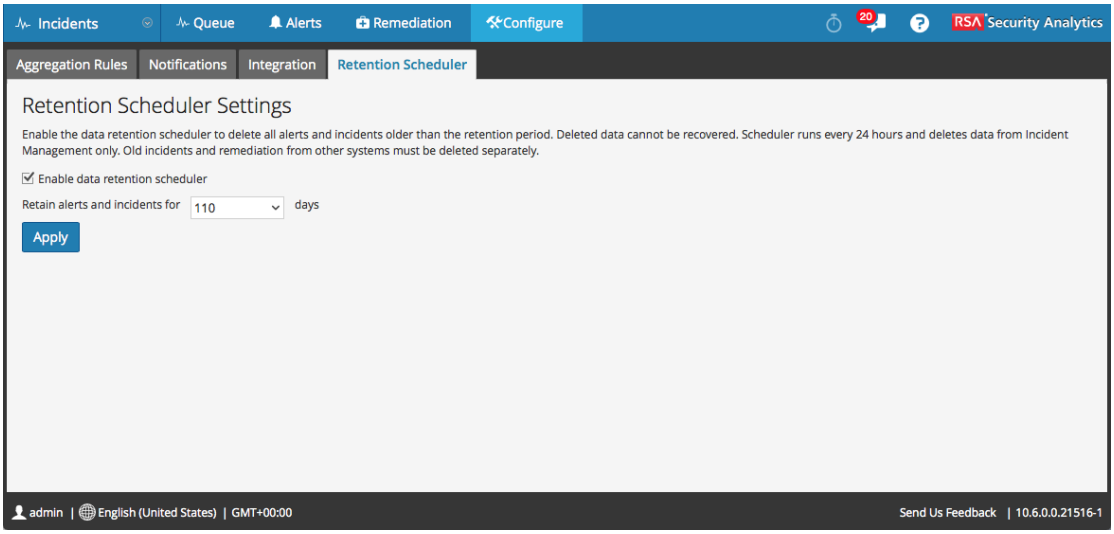
Requisitos previos

Se le debe asignar la función de administrador.

Procedimiento

1. En el menú de **Security Analytics**, seleccione **Incidentes > Configurar**.
   El panel Configurar se muestra con la pestaña Reglas de agregación abierta.

2. Seleccione la pestaña **Calendarizador de retención**.



3. Seleccione **Habilitar el calendarizador de retención de datos** para eliminar las alertas y los incidentes más antiguos que el periodo de retención.
   El programador se ejecuta cada 24 horas a las 23:00 h.
4. En el campo **Conservar alertas e incidentes durante**, seleccione 30, 60, 90, 120 o 365 días o escriba cualquier número.
5. Haga clic en **Aplicar**.

Resultado

24 horas después del fin del periodo de retención, el programador elimina de manera definitiva del módulo Incident Management todas las alertas y los incidentes más antiguos que el periodo especificado. Las entradas del registro y las tareas de corrección asociados a los incidentes eliminados también se eliminan.

Ocultar datos privados

La función Encargado de la privacidad de datos (DPO) puede identificar claves de metadatos que contienen datos confidenciales y que deben mostrar datos ocultos. En este tema se explica la forma en que el administrador mapea esas claves de metadatos para mostrar un valor al que se aplicó hash en lugar del valor real.

Para los valores de metadatos a los cuales se aplicó hash se aplican las siguientes advertencias:

- Security Analytics es compatible con dos métodos de almacenamiento para valores de metadatos a los cuales se aplicó hash, hexadecimal (predeterminado) y cadena.
- Cuando una clave de metadatos está configurada para mostrar un valor al cual se aplicó hash, todas las funciones de seguridad ven únicamente el valor con hash en el módulo Incidentes.
- Los valores a los cuales se aplicó hash se usan de la misma manera en que se usan los valores reales. Por ejemplo, cuando usa un valor al cual se aplicó hash en criterios de regla, los resultados son los mismos que si usa el valor real.

En este tema se explica cómo ocultar datos privados en Incident Management. Consulte el tema **Descripción general de la administración de la privacidad de datos** en la guía *Administración de la privacidad de datos* para obtener información adicional acerca de la privacidad de datos.

Archivo de mapeo para ocultar claves de metadatos

En el módulo Incidentes, el archivo de mapeo para el ocultamiento de datos es data_privacy_map.js. En él, se escribe un nombre de clave de metadatos oculta y se mapea al nombre de clave de metadatos real.

En el siguiente ejemplo se muestran los mapeos para ocultar datos de dos claves de metadatos, ip.src y user.dst:

```
'ip.src.hash' : 'ip.src',
 'user.dst.hash' : 'user.dst'
```

Usted determina la convención de asignación de nombres para los nombres de claves de metadatos ocultas. Por ejemplo, ip.src.hash podría ser ip.src.private o ip.src.bin. Debe elegir una convención de asignación de nombres y usarla coherentemente en todos los hosts.

Requisitos previos

- La función DPO debe especificar qué claves de metadatos requieren ocultamiento de datos.
- La función de administrador debe mapear las claves de metadatos para el ocultamiento de datos.

Procedimiento

1. Abra el archivo de mapeo de la privacidad de datos:
   /opt/rsa/im/scripts/normalize/data_privacy_map.js
2. En la variable `obfuscated_attribute_map`, escriba el nombre de una clave de metadatos que tendrá datos ocultos. A continuación, mapéela a la clave de metadatos que no contiene datos ocultos de acuerdo con este formato:
   `'ip.src.hash' : 'ip.src'`
3. Repita el paso 2 para cada clave de metadatos que deba mostrar un valor al cual se aplicó hash.
4. Use la misma convención de asignación de nombres que en el paso 2 y aplíquela coherentemente en todos los hosts.
5. Guarde el archivo.
   Todas las claves de metadatos mapeadas mostrarán valores a los cuales se aplicó hash en lugar de valores reales.
   En el siguiente gráfico se muestran valores a los cuales se aplicó hash para la dirección IP y el usuario:

   Las nuevas alertas mostrarán datos ocultos.

Nota: Las alertas existentes continuarán mostrando datos confidenciales. Este procedimiento no es retroactivo.

Integración de sistemas

Puede configurar los ajustes de integración para que pueda administrar incidentes en RSA Security Analytics o en RSA Archer Security Operations.

Temas

Configurar ajustes de integración para administrar incidentes en Security Analytics

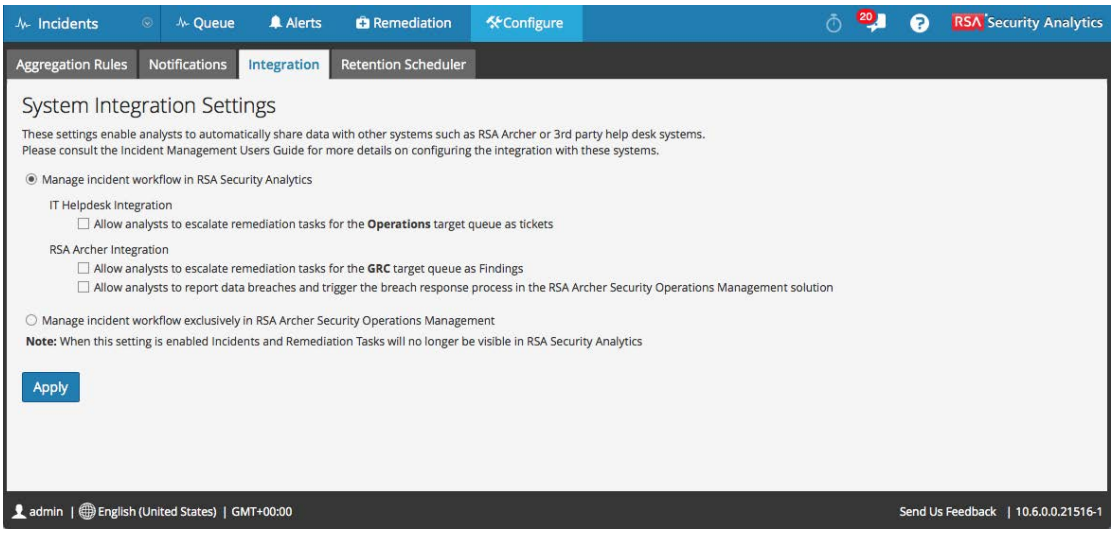
Debe configurar los ajustes de integración del sistema para administrar incidentes en Security Analytics. Puede habilitar la integración con:

- El sistema de vales de help desk de TI, que le ayuda a enviar tareas de corrección como vales de help desk.
- RSA Archer, que le ayuda a enviar tareas de corrección a la línea de espera de destino de Archer y a informar y rastrear vulneraciones de datos mediante el proceso de respuesta de vulneración en la solución RSA Security Operations Management.

Para configurar ajustes de integración con el fin de administrar incidentes en Security Analytics:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Configurar**.
2. Seleccione **Integración**.

   Se muestra la vista Configuración de integración de sistemas.



3. Seleccione **Administrar el flujo de trabajo de incidentes en RSA Security Analytics**.
4. Seleccione una o más de las siguientes opciones:
   - **Permita que los analistas eleven tareas de corrección para la línea de espera de destino de Operaciones como vales**: esto le permite enviar tareas de corrección como vales de help desk y rastrearlas para su cierre.

- **Permita que los analistas eleven tareas de corrección para la línea de espera de destino de GRC como observaciones**: esto le permite elevar y enviar tareas de corrección a la línea de espera de destino de Archer con información adicional que ayuda a rastrearlas para su cierre.
- **Permita a los analistas informar vulneraciones de datos y activar el proceso de respuesta ante vulneración en la solución RSA Archer Security Operations Management**: esto permite informar una vulneración de datos y rastrearla mediante el proceso de respuesta de vulneración en la solución RSA Security Operations Management

5. Seleccione **Aplicar** para guardar los ajustes de configuración.

Configurar ajustes de integración para administrar incidentes en RSA Archer Security Operations

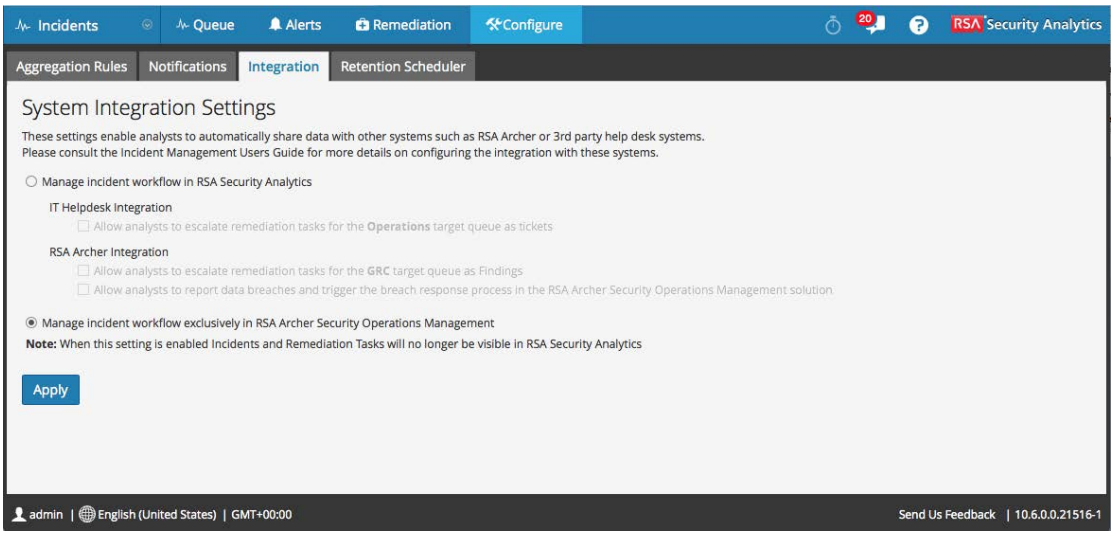
Debe configurar los ajustes de integración del sistema para administrar el flujo de trabajo de incidentes en RSA Archer Security Operations. Cuando se habilita esta configuración, los incidentes y las tareas de corrección dejan de estar visibles en RSA Security Analytics.

Para conocer las versiones de Archer SecOps que son compatibles con Security Analytics, consulte la *Guía de integración de RSA Archer*.

Para configurar ajustes de integración con el fin de administrar el flujo de trabajo de incidentes en RSA Archer Security Operations:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Configurar**.
2. Haga clic en la pestaña **Integración**.

   Se muestra la vista Configuración de integración de sistemas.



3. Seleccione **Administrar el flujo de trabajo de incidentes exclusivamente en RSA Archer Security Operations Management.**
4. Seleccione **Aplicar** para guardar los ajustes de configuración.

Información de referencia de Incident Management

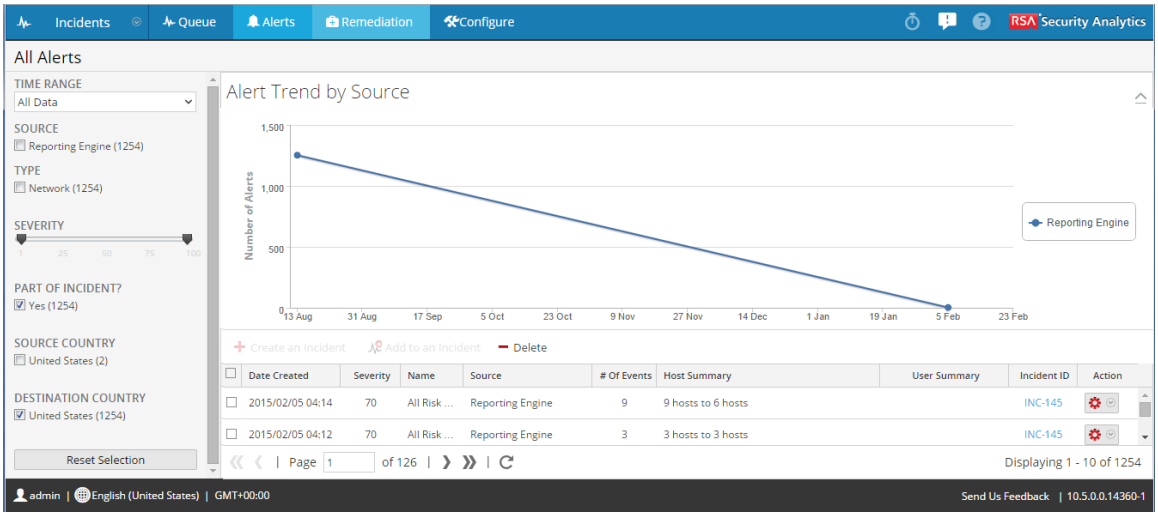
La interfaz del usuario del módulo Incident Management proporciona acceso a las funciones de administración de incidentes de Security Analytics. Este tema contiene descripciones de la interfaz del usuario, así como otra información de referencia para ayudar a los usuarios a entender las funciones de Incident Management.

Temas

Vista Alertas

En este tema se describe cómo acceder a la vista Alertas, se proporciona información detallada acerca de la vista Alertas y sobre diversos aspectos de las alertas. En la vista Alertas, puede navegar por diversas alertas, filtrarlas y agruparlas para crear incidentes.

Para acceder a la vista Alertas, en el menú de **Security Analytics**, seleccione **Incidentes** > **Alertas**. Se muestra la vista Todas las alertas. Puede personalizar la vista Alertas para ver las alertas según sus necesidades.



Características

La vista Alertas ofrece varios detalles y comandos que ayudan a personalizar la vista y a mostrar las alertas.

Detalles de la vista Alertas

El panel de opciones de la vista Todas las alertas muestra varios parámetros que se pueden usar para personalizar la presentación de las alertas.

En la siguiente tabla se describen los distintos parámetros que puede seleccionar para filtrar las alertas y personalizar la vista. Los parámetros de filtro que elige para filtrar las alertas persisten y se conservan cuando abandona la vista actual con el fin de cambiar entre pestañas o sesiones, o cuando navega a la pantalla de detalles. La opción Restablecer selección permite restablecer las opciones de filtro al valor predeterminado.

Parámetro	Descripción
RANGO DE TIEMPO	Seleccione un rango de tiempo para ver alertas dentro de ese rango. Por ejemplo: • Seleccione **Últimas 24 horas** para ver las alertas activadas en las últimas 24 horas. • Seleccione **Todos los datos** para ver las alertas activadas desde el momento en que se agregó el servicio. • Seleccione **Personalizado** y proporcione un rango de fechas para ver las alertas activadas en ese intervalo de tiempo.
ORIGEN	Indica la cantidad de alertas categorizadas según sus orígenes. Por ejemplo, RSA ECAT(86) indica que hay 86 alertas que activó RSA ECAT. Seleccione uno o varios orígenes para ver las alertas que activaron los orígenes seleccionados. Por ejemplo, para ver solo alertas de ECAT, seleccione RSA ECAT como el origen.
TYPE	Indica el tipo de eventos en la alerta, por ejemplo, registros, sesiones de red, etc.
GRAVEDAD	Indica la gravedad de las alertas. Seleccione un valor para ver las alertas de la gravedad requerida. Por ejemplo, para ver alertas de gravedad 75, seleccione 75 como el nivel de gravedad.
¿PARTE DE INCIDENTE?	Indica la cantidad de alertas categorizadas en función de si pertenecen a un incidente. Por ejemplo, Sí(180) indica que hay 180 alertas que son parte de un incidente. Seleccione **Sí** para ver las alertas que son parte de un incidente. Seleccione **No** para ver las alertas que no son parte de ningún incidente.

Parámetro	Descripción
PAÍS DE ORIGEN	Si geo-ip está activado en el Decoder, se filtra por el país etiquetado en el dispositivo de origen en un evento dentro de la alerta.
PAÍS DE DESTINO	Si geo-ip está activado en el Decoder, se filtra por el país etiquetado en el dispositivo de destino en un evento dentro de la alerta.
Reset Selection	Restablece las opciones de filtro a los valores pre-determinados.

En la mitad superior del panel Alerta se muestra la representación gráfica de la tendencia de las alertas en el transcurso del tiempo (agrupadas por cada origen) que coinciden con los criterios de filtro según los parámetros elegidos.

Detalles de la alerta

En la mitad inferior del panel Alerta se muestran los detalles de las alertas. En la siguiente tabla se describen los diversos detalles de las alertas.

Campo	Descripción
Fecha de creación	Muestra la fecha en que se creó la alerta.
Gravedad	Muestra la gravedad de la alerta. Los valores varían entre 1 y 100.
Nombre	Muestra el nombre de la alerta.
Source	Muestra el origen de la alerta. El origen de las alertas puede ser ECAT, Malware Analytics, ESA, el servicio Investigator o Reporting Engine.
N.º de eventos	Indica la cantidad de eventos que se incluyen dentro de una alerta. **Nota:** esto varía según el origen de la alerta. Por ejemplo, las alertas de ECAT y MA siempre tienen un evento. Para ciertos tipos de alertas, una alta cantidad de eventos puede significar que la alerta es más riesgosa.

Campo	Descripción
Resumen de host	Muestra detalles del host, como el nombre del host donde se activó la alerta. Los detalles pueden incluir información sobre los dispositivos de origen y/o de destino en una alerta. Algunas alertas pueden describir eventos en más de un dispositivo.
Resumen de usuario	Muestra el resumen del o los usuarios asociados a los eventos en la alerta.
ID del incidente	Muestra el ID del incidente al cual pertenece la alerta. Si no hay un ID del incidente, esto implica que la alerta no pertenece a ningún incidente y se puede crear uno para incluirla o se puede agregar a un incidente existente.
Acción	Permite realizar una investigación adicional de la alerta. Las opciones disponibles para realizar una investigación adicional difieren según los distintos tipos de alertas. Por ejemplo: En el caso de una alerta de ECAT, la opción disponible es **Ver análisis de ECAT**. Esto permite ver el análisis del host en el cliente de ECAT, si lo instaló en la máquina cliente. En el caso de ESA o Reporting Engine, las opciones disponibles son **Investigar eventos**, **Investigar dirección IP de dispositivo**, **Investigar dirección IP de origen** e **Investigar dirección IP de destino**. Esto permite ver los eventos en la vista Investigator o ver eventos similares (por ejemplo, por la misma dirección IP de origen o destino). En el caso de Malware Analytics, la opción disponible es **Ver Malware Analysis**. Esto permite ver los detalles del evento desde el análisis de malware.

Opciones

En la mitad inferior del panel Alerta se proporcionan las opciones para ejecutar varias operaciones. En la tabla se describen varios comandos disponibles.

Comando	Acción
Create an Incident	Seleccione esta opción para crear un incidente. Consulte Crear un incidente manualmente.
Add to an Incident	Seleccione esta opción para agregar la alerta elegida a un incidente existente. Consulte Agregar alertas a un incidente existente.

Comando	Acción
	Seleccione esta opción para eliminar alertas. Consulte Eliminar alertas.

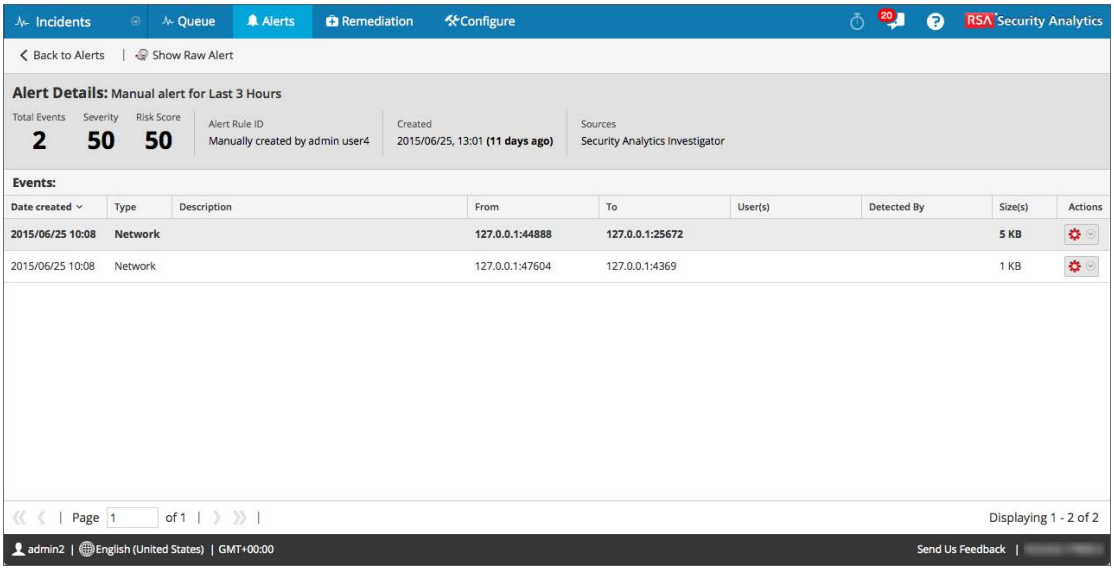
Vista Detalles de alertas

La vista Detalles de alertas permite ver los detalles de una alerta.

Para acceder a la vista Detalles de alertas:

1. 1. En el menú de **Security Analytics**, seleccione **Incidentes > Alertas**.
2. Haga doble clic en una alerta.

   Se muestra la vista Detalles de la alerta.



Los procedimientos relacionados están disponibles en Filtrar alertas.

Características

En la siguiente tabla se enumeran los parámetros que se muestran en la vista Detalles de alertas.

Parámetro	Descripción
Total de eventos	Muestra la cantidad total de eventos.
Gravedad	Muestra el nivel de severidad.
Puntaje de riesgo	Muestra el nivel de riesgo.
ID de regla de alerta	Muestra cómo y quién creó la alerta.
Created	Muestra detalles sobre la fecha y la hora en que se creó la tarea.
Orígenes	Muestra el origen original.

Barra de herramientas

En la siguiente tabla se indican las operaciones que se pueden realizar en la vista Detalles de alertas.

Parámetro	Descripción
Volver a Alertas	Permite volver a la vista Alertas.
Mostrar alerta cruda	Muestra detalles de datos de la alerta cruda.
Ver detalles de evento	Muestra detalles del evento, incluidos vínculos relacionados, datos, destino y origen.
Ver evento original	Muestra la reconstrucción del evento y detalles sobre el servicio, el ID, el tipo, el origen y el destino.

Vista Configurar

La vista Configurar permite configurar la funcionalidad Administración de incidentes del sistema. Puede configurar ajustes de notificaciones, la integración de sistemas de otros fabricantes para la administración de incidentes y reglas de agregación para automatizar el flujo de trabajo de administración de incidentes con el fin de crear incidentes de forma automática.

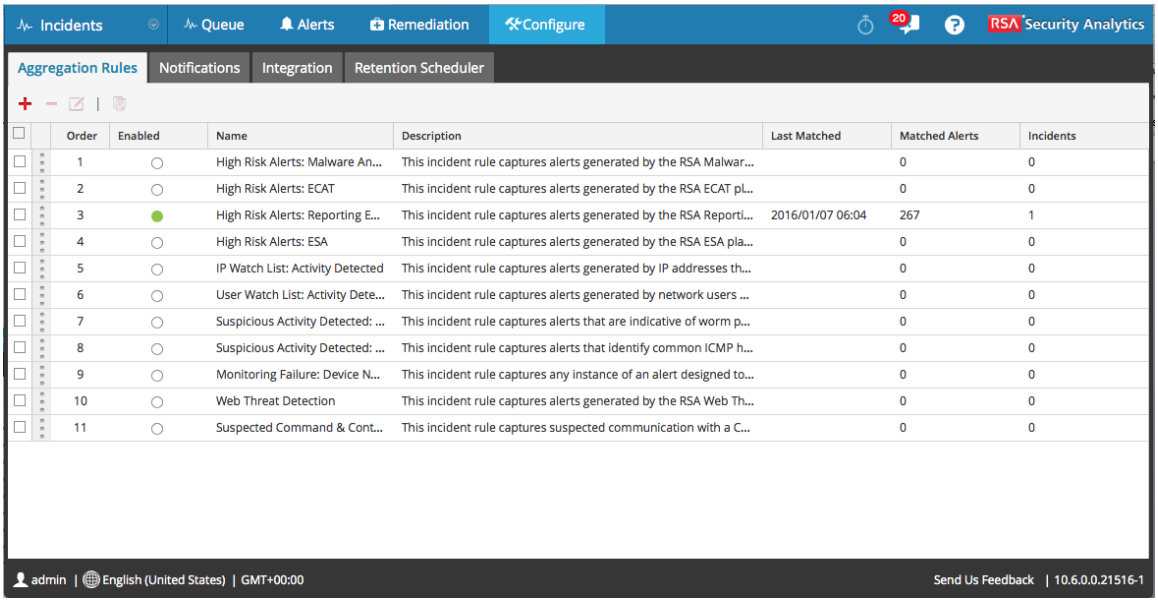
La vista Configurar tiene tres vistas secundarias para las diversas funciones.

Temas

Pestaña Reglas de agregación

En este tema se aborda la información de los parámetros necesarios en la creación y administración de reglas de agregación para automatizar el proceso de creación de incidentes como parte del flujo de trabajo de administración de incidentes.

Para acceder a la vista Reglas de agregación, en el menú de **Security Analytics**, seleccione **Incidentes > Configurar > Reglas de agregación**. Se muestra la vista Reglas de agregación.



Características

La pestaña Reglas de agregación consta de una cuadrícula y una barra de herramientas.

Cuadrícula Reglas de agregación

En la siguiente tabla se detallan los parámetros que se deben proporcionar para crear nuevas reglas de agregación.

Parámetro	Descripción
Pedido	Indica el orden en que se coloca la regla. El orden de la regla determina cuál regla se aplica si los criterios de varias reglas coinciden con la misma alerta.
Nombre	Muestra el nombre de la regla.
Activado	Indica si la regla está activada o desactivada. especifica que la regla está activada.

Parámetro	Descripción
Descripción	Muestra la descripción de la regla.
Última ejecución	Muestra la hora de última ejecución de la regla. Este valor se reinicia una vez por semana.
Alertas con coincidencia	Muestra la cantidad de alertas con coincidencia. Este valor se restablece una vez por semana. Para cambiar la configuración, consulte el tema **Configurar el contador para alertas e incidentes con coincidencia** de la *Guía de configuración de Incident Management*.
Incidentes	Muestra la cantidad de incidentes que creó la regla. Este valor se restablece una vez por semana. Para cambiar la configuración, consulte el tema **Configurar el contador para alertas e incidentes con coincidencia** de la *Guía de configuración de Incident Management*.

Barra de herramientas

La tabla siguiente muestra las operaciones que se pueden realizar en la vista Reglas de agregación.

Parámetro	Descripción
	Le permite agregar una regla nueva.
	Le permite editar una regla.
	Le permite eliminar una regla.
	Permite duplicar una regla.

Pestaña Nueva regla

En este tema se proporciona información sobre los parámetros necesarios para crear una nueva regla.

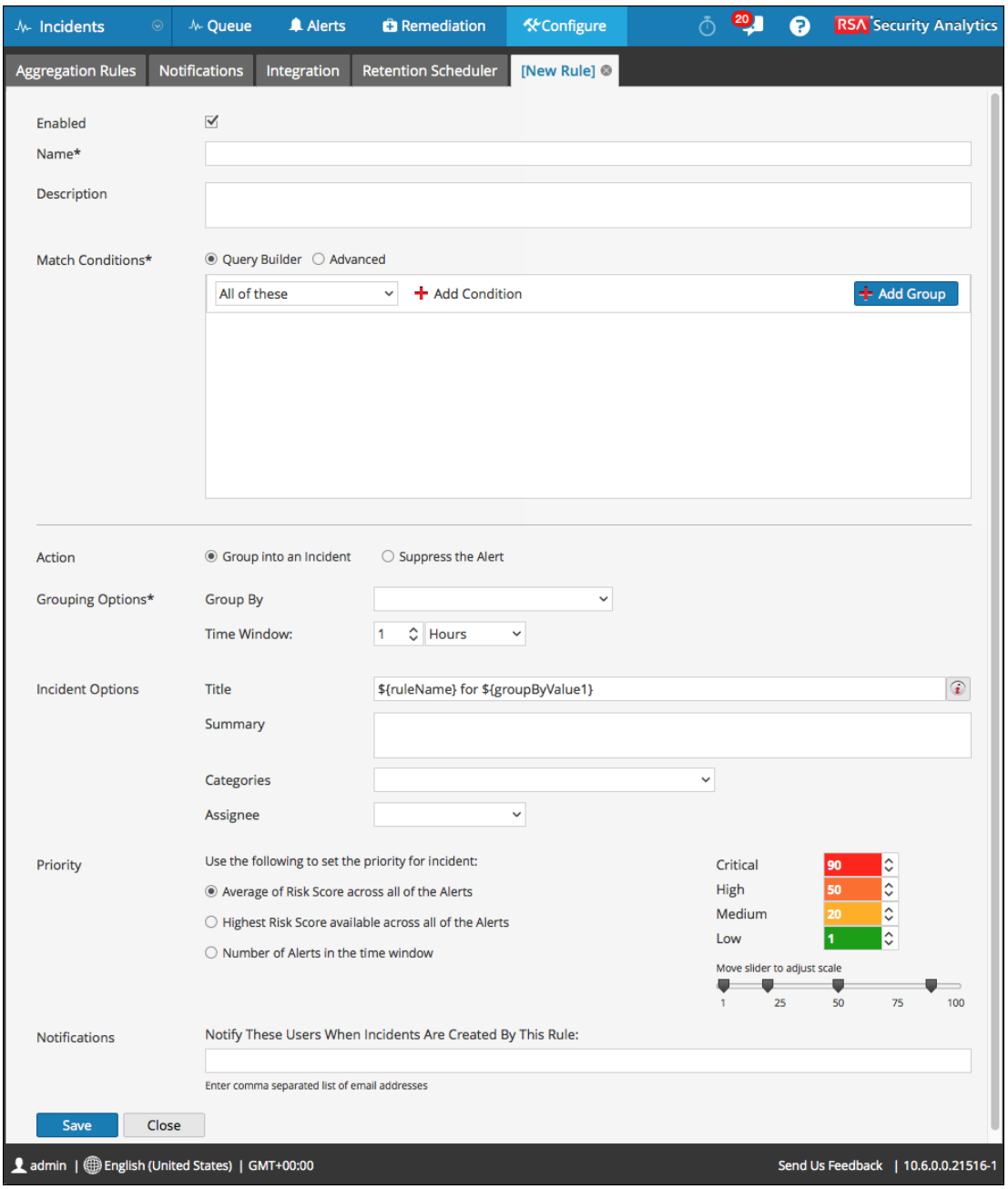
Para acceder a la vista de la pestaña Nueva regla:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Configurar > Reglas de agregación**.

   Se muestra la vista Reglas de agregación.

2. Haga clic en  .

Se muestra la pestaña **Nueva regla**.



La vista Nueva regla ofrece varios campos en los cuales puede personalizar una nueva regla.

En la siguiente tabla se detallan los parámetros que se deben proporcionar para crear nuevas reglas de agregación.

Parámetro	Descripción
Activado	Seleccione esta opción para activar la regla.

Parámetro	Descripción
Nombre*	Nombre de la regla. Este campo es obligatorio.
Descripción	Descripción de la regla que permite formarse una idea de las alertas que se agregan.
Condiciones de coin-cidencia*	**Generador de consultas**: seleccione si desea crear una consulta con diversas condiciones que se pueden agrupar. También puede tener grupos de condiciones anidados. Condiciones de coincidencia: puede configurar el valor en **Todas estas**, **Cualquiera de estas** o **Ninguna de estas**. De acuerdo con la selección, se buscan coincidencias con los tipos de criterios especificados en las condiciones y el grupo de condiciones para agrupar las alertas. **Por ejemplo**, si configura la condición de coincidencia en Todas estas, las alertas que coinciden con los criterios mencionados en las condiciones y el grupo de condiciones se agrupan en un incidente. Haga clic en <> para agregar una condición para la cual se buscarán coincidencias Haga clic en <> para agregar un grupo de condiciones y haga clic en <> para agregar condiciones Puede incluir múltiples condiciones y grupos de condiciones para los cuales se pueden buscar coincidencias conforme a los criterios establecidos con el fin de agrupar las alertas entrantes en incidentes.
	Avanzado: seleccione si desea agregar un generador de consultas avanzado. Puede agregar una condición específica que se deba hacer coincidir de acuerdo con la opción de coincidencia seleccionada. **Por ejemplo:** puede ingresar el formato del generador de criterios **{"$and": [{"alert.severity" : {"$gt":4}}]}** para agrupar alertas que tienen una gravedad mayor que 4. Para conocer la sintaxis avanzada, consulte http://docs.mongodb.org/manual/reference/operator/query/ o http://docs.mongodb.org/manual/reference/method/db.collection.find/
Acción	**Agrupar en un incidente**: si esta opción está activada, las alertas que coinciden con los criterios establecidos se agrupan en una alerta. **Suprimir la alerta**: si esta opción está activada, las alertas que coinciden con los criterios se suprimen.

Parámetro	Descripción
Opciones de agrupación*	**Agrupar por:** Los criterios para agrupar las alertas según la categoría especificada. Puede agrupar las alertas sin atributos (todas las alertas coincidentes se agrupan juntas), 1 atributo o 2 atributos. Agrupar en un atributo significa que todas las alertas coincidentes que contienen el mismo valor para ese atributo se agrupan en el mismo incidente. **Ventana de tiempo:** El rango de tiempo especificado para agrupar alertas. Por ejemplo, si la ventana de tiempo se configura en una hora, todas las alertas que coinciden con los criterios establecidos en el campo Agrupar por y que llegan con una hora de diferencia unas de otras se agrupan en un incidente.
Opciones de incidente	**Título:** (Opcional) Título del incidente. Puede proporcionar marcadores de posición basados en los atributos que agrupó. Los marcadores de posición son opcionales. Si no usa marcadores de posición, todos los incidentes que crea la regla tendrán el mismo título. Por ejemplo, si los agrupó según el origen, el incidente resultante se puede llamar Alertas para **${groupByValue1}**, y el incidente para todas las alertas de ECAT tendría el nombre **Alertas para ECAT**.
	Resumen: (opcional) resumen del incidente.
	Categoría: (opcional) categoría del incidente creado. Un incidente se puede clasificar por más de una categoría.
	Usuario asignado: (opcional) nombre del usuario asignado a quien se asigna el incidente.
Prioridad	**Promedio de puntaje de riesgo en todas las alertas**: toma el promedio de los puntajes de riesgo en todas las alertas para establecer la prioridad del incidente creado. **Puntaje de riesgo más alto disponible en todas las alertas**: toma el puntaje más alto disponible en todas las alertas para establecer la prioridad del incidente creado. **Cantidad de alertas en la ventana de tiempo**: toma el conteo de la cantidad de alertas en la ventana de tiempo seleccionada para establecer la prioridad del incidente creado. Mueva el control deslizante para ajustar la escala que establece el nivel de prioridad del incidente.

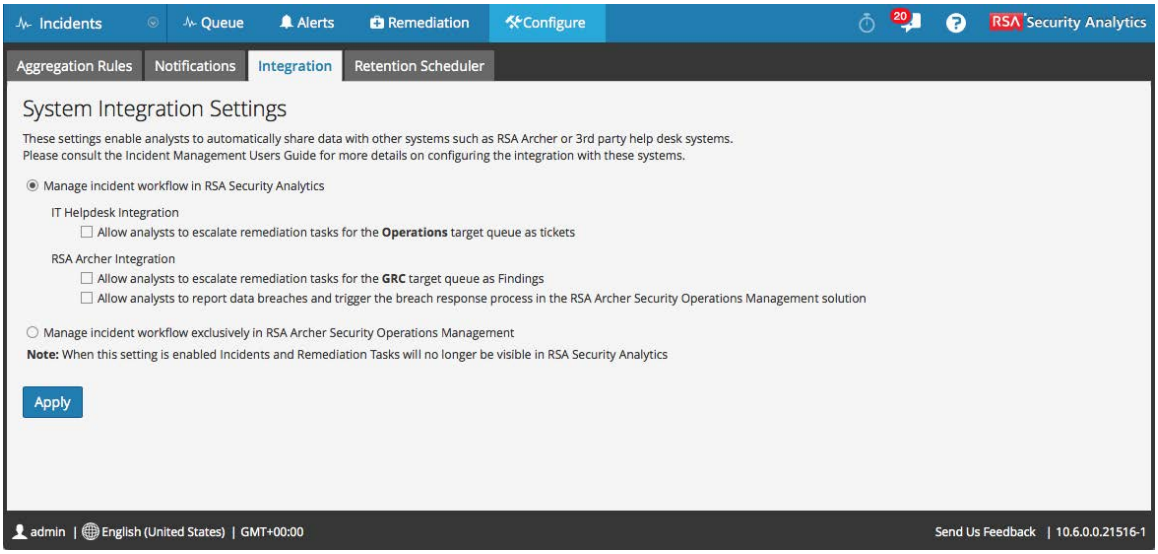
Parámetro	Descripción
Notificaciones	Conjunto de direcciones de correo electrónico de los usuarios que recibirán notificación cuando esta regla cree incidentes.

Pestaña Integración

La pestaña Integración permite ajustar la configuración de integración de sistemas, lo cual permite que los analistas compartan datos automáticamente con otros sistemas, como RSA Archer o sistemas de help desk de otros fabricantes.

Para acceder a esta pestaña, seleccione **Incidentes > Configurar** en el menú de **Security Analytics** y, a continuación, seleccione la pestaña **Integración**.

La pestaña Integración consta del panel Configuración de integración de sistemas, el cual permite elegir dónde se administra el flujo de trabajo de incidentes y configurar permisos de integración para los analistas. En la siguiente figura se muestra la pestaña Integración.



En la siguiente tabla se describen los parámetros de configuración.

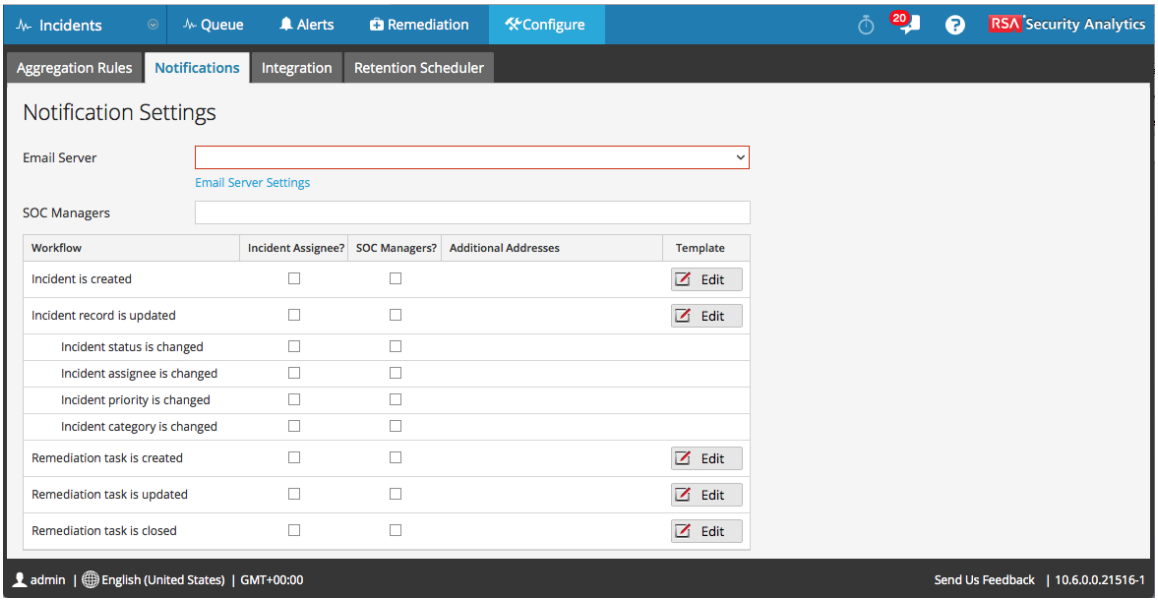
Parámetro	Descripción
Administrar el flujo de trabajo de incidentes en Security Analytics	Permite la administración del flujo de trabajo de incidentes en Security Analytics. La selección de esta opción inhabilita la opción **Administrar el flujo de trabajo de incidentes exclusivamente en RSA Archer Security Operations Management.**
Permita que los analistas eleven tareas de corrección para la línea de espera de destino de **Operaciones** como vales	Permite enviar tareas de corrección como vales de help desk y rastrearlas hasta su cierre.

Parámetro	Descripción
Permita que los analistas eleven tareas de corrección para la línea de espera de destino de **GRC** como observaciones	Permite elevar y enviar tareas de corrección a la línea de espera objetivo de Archer con información adicional que ayuda a rastrearlas hasta su cierre.
Permita a los analistas informar vulneraciones de datos y activar el proceso de respuesta ante vulneración en la solución RSA Archer Security Operations Management	Permite informar una vulneración de datos y rastrearla a través del proceso de respuesta ante vulneración en la solución RSA Archer Security Operations Management.
Administrar el flujo de trabajo de incidentes exclusivamente en RSA Archer Security Operations Management	Deshabilita la administración del flujo de trabajo de incidentes fuera de RSA Archer Security Operations Management. Los incidentes y las tareas de corrección ya no están visibles en RSA Security Analytics y las opciones **Administrar el flujo de trabajo de incidentes en Security Analytics** no están disponibles.

Pestaña Notificaciones

En esta vista puede establecer notificaciones para diversas operaciones que se realizan a lo largo del flujo de trabajo de administración de incidentes.

Para acceder a la vista Configuración de notificaciones, en el menú de **Security Analytics**, seleccione **Incidentes > Configurar > Notificaciones**. Se muestra la vista Configuración de notificaciones.



La pestaña Notificaciones consta del panel Configuración de notificaciones.

La siguiente tabla indica los parámetros que deben estar activados para la configuración de notificaciones.

Parámetro	Descripción
Servidor de correo electrónico	La dirección del servidor de correo electrónico que se debe configurar para enviar notificaciones de correo electrónico para la configuración de notificaciones activada.
Configurar correo electrónico o lista de distribución	Haga clic aquí para configurar un servidor de correo electrónico si este servidor no aparece en la lista desplegable Servidor de correo electrónico.

Parámetro	Descripción
Administradores del SOC	Direcciones de correo electrónico del Administrador del SOC a las cuales se envía el correo de notificación de las operaciones seleccionadas.
Flujo de trabajo	El flujo de trabajo en el cual se envía una notificación, si está habilitado.
¿Usuario asignado al incidente?	Seleccione si desea que se envíe una notificación de correo para el flujo de trabajo correspondiente cuando se asigne un incidente.
¿Administradores del SOC?	Seleccione si desea que se envíe una notificación de correo a los administradores del SOC para el flujo de trabajo correspondiente.
Direcciones adicionales	Direcciones adicionales a las que desea que se envíen las notificaciones por correo electrónico para el flujo de trabajo correspondiente.
Plantilla	Haga clic en **Editar** para modificar la plantilla para el flujo de trabajo seleccionado.
Aplicar	Haga clic en **Aplicar** para guardar la configuración.

Pestaña Calendarizador de retención

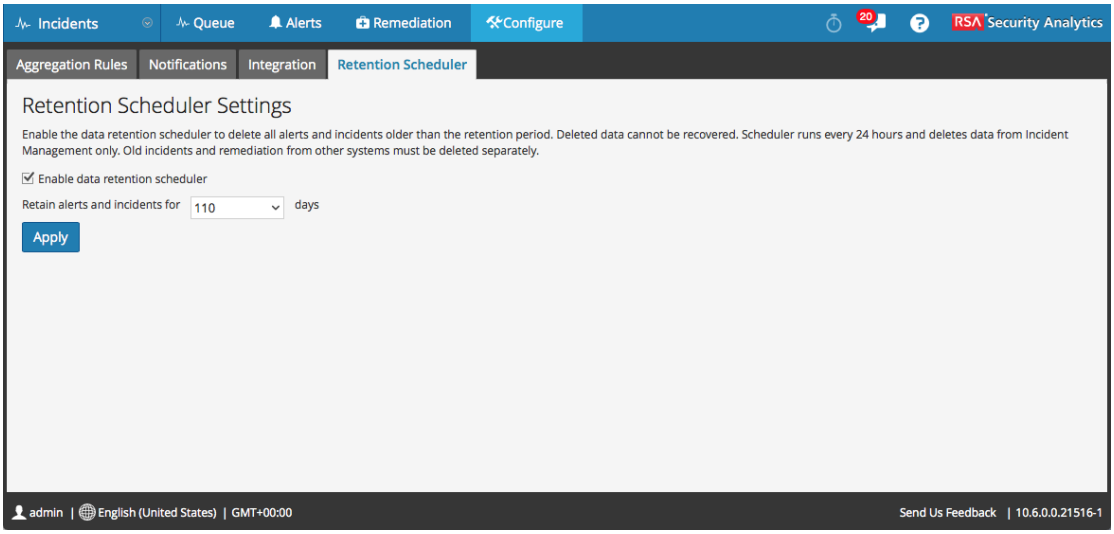
La configuración en la pestaña Calendarizador de retención permite especificar un periodo de retención para alertas e incidentes.

Para acceder a la pestaña Calendarizador de retención:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Configurar**.

   El panel Configurar se abre de manera predeterminada en la pestaña Reglas de agregación.

2. Seleccione la pestaña **Calendarizador de retención**.



En la pestaña Calendarizador de retención se incluyen las siguientes funciones:

Característica	Descripción
Cantidad de días	Especifica por cuánto tiempo se conservarán las alertas y los incidentes antes de que se eliminen.
Habilitar	Elimina las alertas y los incidentes cuando termina el periodo de retención.
Aplicar	Aplica la configuración de inmediato.

Vista Línea de espera de incidentes

La vista Línea de espera de Incidente permite ver una lista de todos los incidentes asignados y no asignados. Puede administrar y rastrear estos incidentes hasta el cierre.

Para acceder a la pestaña Línea de espera de incidentes, en el menú de **Security Analytics**, seleccione **Incidentes > Línea de espera.** Se muestra una línea de espera de todos los incidentes.

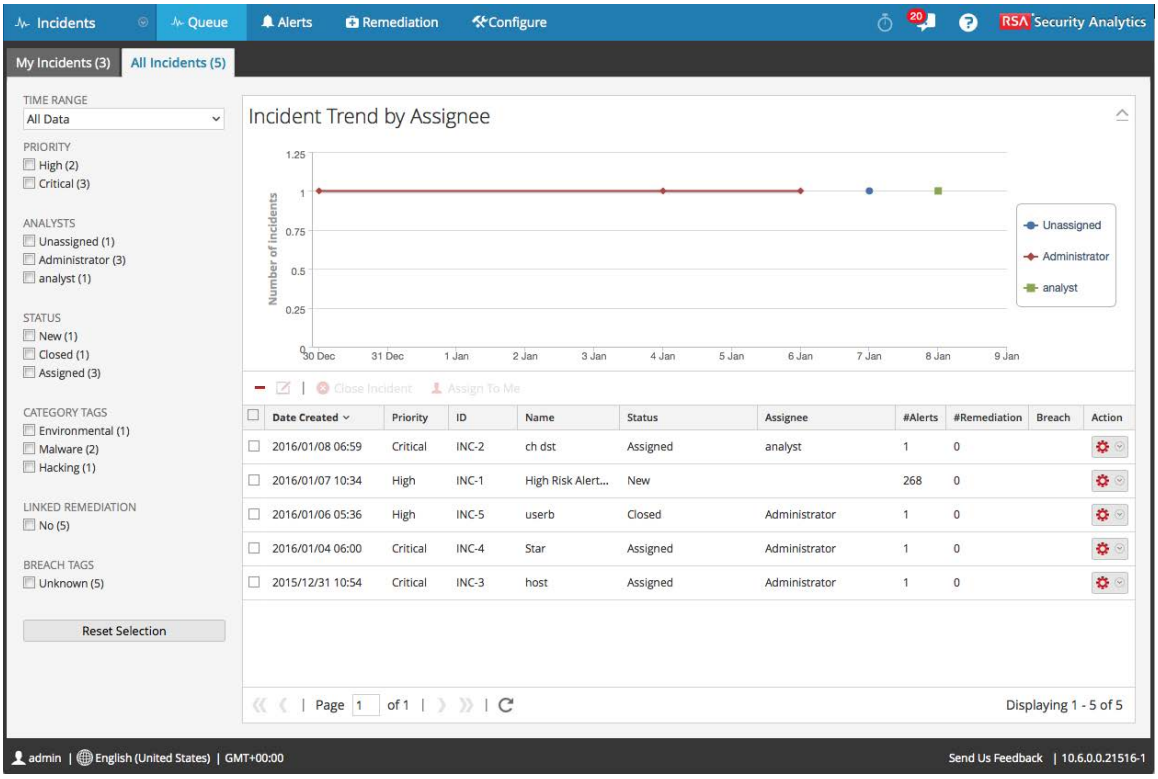
Características

Esta vista incluye las siguientes pestañas:

- Todos los incidentes: muestra todos los incidentes.
- Mis incidentes: muestra todos los incidentes que se le asignaron.

Pestaña Todos los incidentes

Este es un ejemplo de la pestaña Todos los incidentes.



El panel de opciones tiene parámetros que se pueden usar para filtrar incidentes. Los parámetros de filtro que elige para filtrar la línea de espera de incidentes persisten y se conservan cuando abandona la vista actual para cambiar entre pestañas o sesiones, o cuando navega a la pantalla de detalles de incidentes. La opción **Restablecer selección** permite restablecer las opciones de filtro al valor predeterminado.

Parámetro	Descripción
RANGO DE TIEMPO	Seleccione un rango de tiempo para ver incidentes dentro de ese rango. Por ejemplo: • Seleccione Últimas 24 horas para ver incidentes creados en las últimas 24 horas. • Seleccione Todos los datos para ver todos los incidentes creados. • Seleccione Personalizado y proporcione un rango de fechas para ver los incidentes creados en ese intervalo de tiempo.
PRIORIDAD	Indica la cantidad de incidentes según sus prioridades. Por ejemplo: Crítico (18) indica que hay 18 incidentes cuya prioridad está configurada en Crítico. La selección de una de las opciones mostradas filtra los incidentes y solo muestra la prioridad de incidentes seleccionada. Por ejemplo: si selecciona Crítico (18), el panel Incidente muestra solo los 18 incidentes cuya prioridad está configurada en Crítico.
ANALISTAS	Esto indica los incidentes categorizados según el usuario al cual se asignaron.

Parámetro	Descripción
STATUS	Indica los incidentes categorizados según su estado. Por ejemplo: Asignado (7) indica que hay siete incidentes que están en el estado Asignado. La selección de una de las opciones mostradas filtra los incidentes y solo muestra los que pertenecen a la categoría seleccionada. Por ejemplo: Si selecciona Asignado (7), el panel Incidente muestra solo los 7 incidentes que se encuentran en el estado Asignado.
ETIQUETAS DE CATEGORÍA	Indica la cantidad de incidentes que pertenecen a una categoría específica. Dado que las categorías son jerárquicas, las etiquetas de categoría solo cuentan la categoría principal. Por ejemplo: Malware (5) indica que hay cinco incidentes que pertenecen a la categoría Malware. La selección de una de las opciones mostradas filtra los incidentes y solo muestra los que pertenecen a la categoría seleccionada. Por ejemplo: Si selecciona Malware (5), el panel Incidente muestra solo los cinco incidentes que pertenecen a la categoría Malware.

Parámetro	Descripción
CORRECCIÓN VINCULADA	Indica los incidentes categorizados en función de si tienen o no tareas de corrección. Por ejemplo: Sí (5) indica que hay cinco incidentes que tienen tareas de corrección. No (3) indica que hay tres incidentes que no tienen tareas de corrección. La selección de una de las opciones mostradas filtra los incidentes y solo los muestra según la opción que se elige. Por ejemplo: Si selecciona Sí (5), el panel Incidente muestra solo los 5 incidentes que tienen tareas de corrección.
ETIQUETAS DE VULNERACIÓN	Muestra la etiqueta de vulneración asociada con el incidente.
Reset Selection	Restablece las opciones de filtro a los valores predeterminados.

El panel Incidente muestra la siguiente información:

En la parte superior hay una representación gráfica de la tendencia de incidentes por usuario asignado, con una línea por usuario asignado. La representación gráfica se basa en el filtro elegido. Puede resaltar la línea por usuario asignado requerida mediante la inhabilitación de las otras dos en la casilla que se encuentra en el lado del Incidente en el gráfico.

En la parte inferior se muestra una lista de incidentes y sus detalles de acuerdo con el filtro elegido.

Parámetro	Descripción
Fecha de creación	Muestra la fecha de creación del incidente.

Parámetro	Descripción
Prioridad	Muestra la prioridad del incidente. La prioridad puede ser cualquiera de las siguientes: Crítica, Alta, Media o Baja.
ID	Muestra el ID del incidente.
Nombre	Muestra el nombre del incidente.
Status	Muestra el estado del flujo de trabajo del incidente.
Usuario asignado	Muestra el usuario a quien se asignó el incidente. Esto solo se puede ver en la vista de detalles de TODOS los incidentes.
N.º de alertas	Muestra la cantidad de alertas que componen el incidente.
N.º de corrección	Muestra la cantidad de tareas de corrección creadas para el incidente.
Vulneración	Muestra si el incidente tiene una vulneración de datos y, si es así, muestra la etiqueta de vulneración.
Acciones	Muestra las acciones que se pueden realizar en el incidente. Las acciones posibles son: Asignar a mí, Editar incidente y Cerrar incidente.

Operaciones

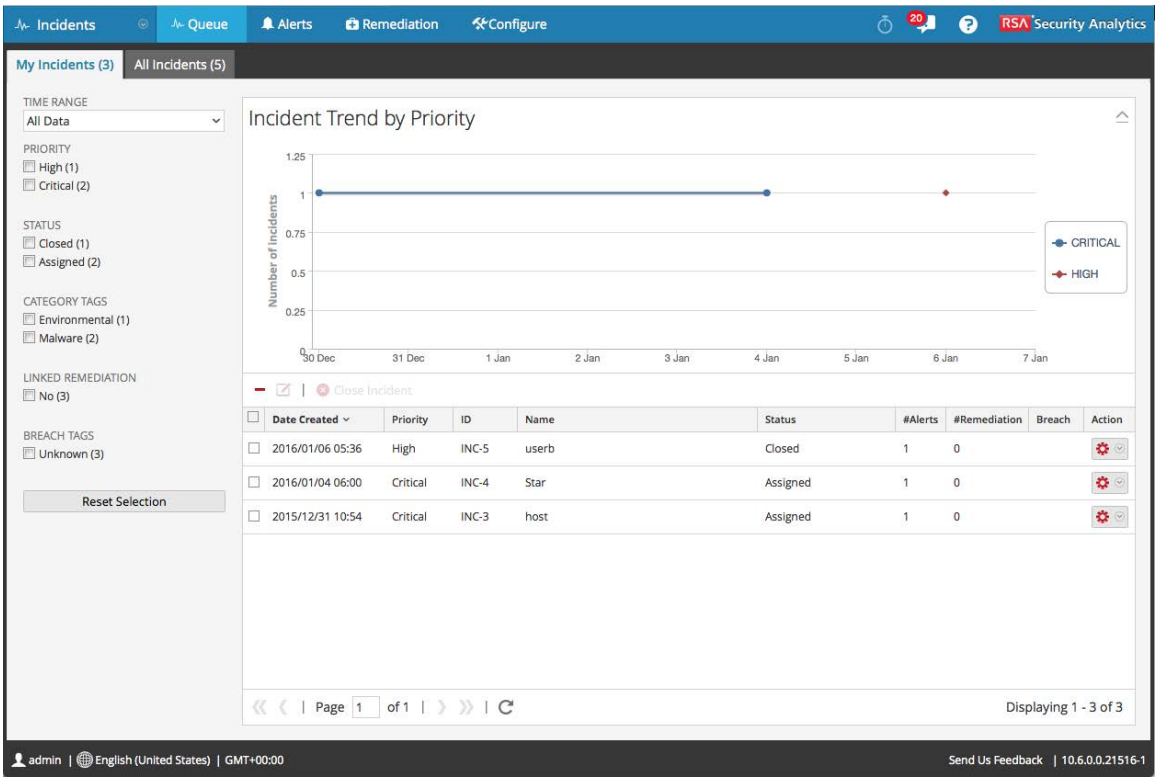
Esta tabla muestra las operaciones que se pueden realizar en la vista Resumen.

Parámetro	Descripción
Asignar a mí	Permite que usted se asigne el incidente a usted mismo. Esta opción está disponible en la vista Todos los incidentes.
Editar incidente	Le permite modificar un incidente.

Parámetro	Descripción
Cerrar incidente	Permite cerrar un incidente.
Delete	Permite eliminar un incidente.
Informar una vulneración de datos	Permite informar si hay una vulneración de datos. Esto solo está visible si configuró la compatibilidad con la vulneración de datos en los ajustes de la integración.

Pestaña Mis incidentes

Esta pestaña está visible solo cuando se le han asignado incidentes. Esta figura es un ejemplo de la pestaña Mis incidentes.



El panel de opciones tiene parámetros que se pueden usar para filtrar incidentes. Los parámetros de filtro que elige para filtrar la línea de espera de incidentes persisten y se conservan cuando abandona la vista actual para cambiar entre pestañas o sesiones, o cuando navega a la pantalla de detalles de incidentes. La opción **Restablecer selección** permite restablecer las opciones de filtro al valor predeterminado.

Parámetro	Descripción
RANGO DE TIEMPO	Seleccione un rango de tiempo para ver incidentes dentro de ese rango. Por ejemplo: • Seleccione Últimas 24 horas para ver incidentes creados en las últimas 24 horas. • Seleccione Todos los datos para ver todos los incidentes creados. • Seleccione Personalizado y proporcione un rango de fechas para ver los incidentes creados en ese intervalo de tiempo.
PRIORIDAD	Indica la cantidad de incidentes según sus prioridades. Por ejemplo: Crítico (18) indica que hay 18 incidentes cuya prioridad está configurada en Crítico. La selección de una de las opciones mostradas filtra los incidentes y solo muestra la prioridad de incidentes seleccionada. Por ejemplo: Si selecciona Crítico (18), el panel Incidente muestra solo los 18 incidentes cuya prioridad está configurada en Crítico.
STATUS	Indica los incidentes categorizados según su estado. Por ejemplo: Asignado (2) indica que hay 2 incidentes que están en el estado Asignado. La selección de una de las opciones mostradas filtra los incidentes y solo muestra los que pertenecen a la categoría seleccionada. Por ejemplo: Si selecciona Asignado (2), el panel Incidente muestra solo los 2 incidentes que se encuentran en el estado Asignado.

Parámetro	Descripción
ETIQUETAS DE CATEGORÍA	Indica la cantidad de incidentes que pertenecen a una categoría específica. Por ejemplo: Malware (5) indica que hay 5 incidentes que pertenecen a la categoría Malware. La selección de una de las opciones mostradas filtra los incidentes y solo muestra los que pertenecen a la categoría seleccionada. Por ejemplo: Si selecciona Malware (5), el panel Incidente muestra solo los 5 incidentes que pertenecen a la categoría Malware.
CORRECCIÓN VINCULADA	Indica los incidentes categorizados en función de si tienen o no tareas de corrección. Por ejemplo: Sí (5) indica que hay cinco incidentes que tienen tareas de corrección. No (3) indica que hay tres incidentes que no tienen tareas de corrección. La selección de una de las opciones mostradas filtra los incidentes y solo los muestra según la opción que se elige. Por ejemplo: Si selecciona Sí (5), el panel Incidente muestra solo los 5 incidentes que tienen tareas de corrección.
ETIQUETAS DE VULNERACIÓN	Muestra la etiqueta de vulneración asociada con el incidente.
	Seleccione esta opción para restablecer las opciones de filtro al valor predeterminado.

La parte superior del panel Incidente incluye una representación gráfica de los incidentes que se le asignaron. El gráfico muestra una tendencia por prioridad y presenta una línea por prioridad. La representación gráfica se basa en el filtro elegido. Puede resaltar la línea por prioridad requerida mediante la inhabilitación de las otras opciones de prioridad en la casilla del lado derecho del gráfico.

En la parte inferior se muestra una lista de incidentes que se le asignaron y sus detalles de acuerdo con el filtro elegido.

La vista Mis incidentes permite realizar las siguientes operaciones:

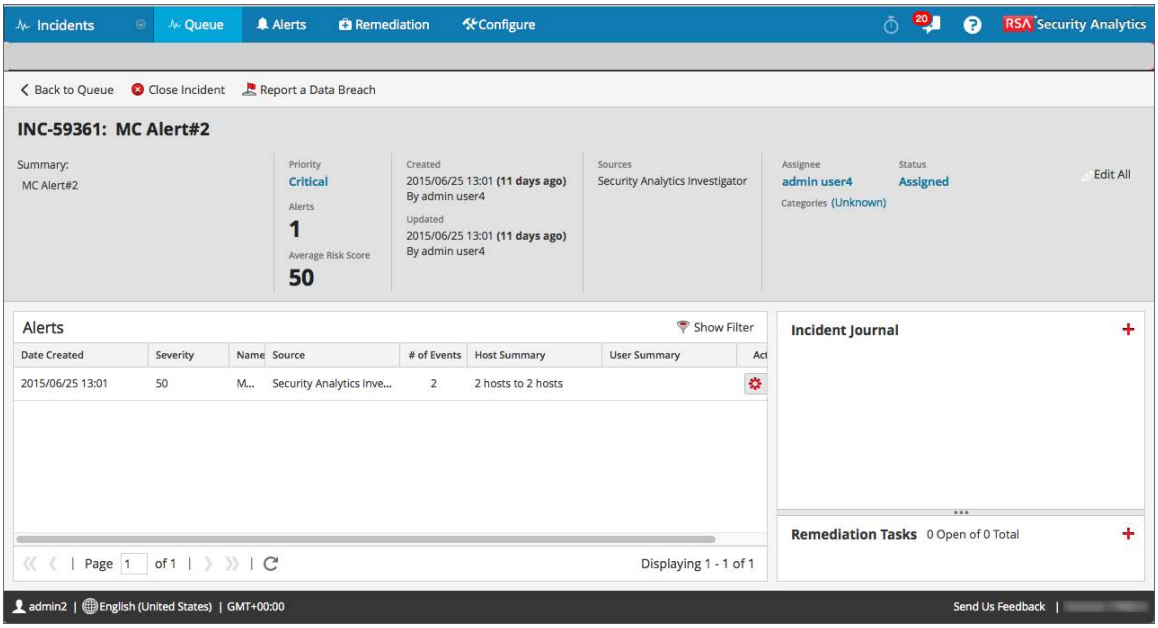
- Editar un incidente
- Cerrar un incidente
- Eliminar un incidente
- Informar una vulneración de datos

Vista Detalles de línea de espera de incidentes

La vista Detalles de línea de espera de incidentes permite ver detalles de un incidente o editar un incidente.

Para acceder a la vista Detalles de línea de espera de incidentes:

1. En el menú de **Security Analytics**, seleccione **Incidentes** > **Línea de espera**.
   Se muestra la vista Incidentes.
2. Haga doble clic en uno de los incidentes.
   Se muestra la vista Detalles de línea de espera de incidentes.



Los procedimientos relacionados están disponibles en Ver detalles de incidentes.

Características

En la siguiente tabla se enumeran los parámetros que se muestran en la vista Detalles de línea de espera de incidentes.

Parámetro	Descripción
Resumen	Proporciona detalles generales sobre la alerta de riesgo.
Prioridad	Muestra la prioridad de la tarea. Este es un campo editable.
Alertas	Muestra la cantidad de alertas.

Parámetro	Descripción
Average Risk Score	Muestra el riesgo promedio.
Created	Muestra detalles sobre la fecha y la hora en que se creó la tarea y quién la creó.
Fragmento C	Muestra la fecha y hora de la última actualización de la tarea.
Orígenes	Muestra de dónde provino el incidente.
Usuario asignado	Muestra el usuario a quien se asignó el incidente. Este es un campo editable.
Categorías	Enumera las categorías asignadas.
Status	Muestra el estado del incidente. Este es un campo editable.

Barra de herramientas

En la siguiente tabla se indican las operaciones que se pueden realizar en la vista Detalles de línea de espera de incidentes.

Parámetro	Acción
Volver a línea de espera	Permite volver a la vista Línea de espera de incidentes.
Cerrar incidente	Permite cerrar el incidente actual que está viendo.
Informar una vulneración de datos	Envía un informe sobre una vulneración de datos.
Editar todo	Permite modificar el incidente si es necesario.
Investigar eventos	Permite investigar un evento de manera más detallada.
Investigar dirección IP de origen	Permite investigar la dirección IP del origen de manera más detallada.

Parámetro	Acción
Investigar dirección IP de destino	Permite investigar la dirección IP del destino de manera más detallada.
Nueva entrada de diario	Permite crear y publicar una nueva entrada del registro.
Nueva tarea de corrección	Permite crear una nueva tarea de corrección.

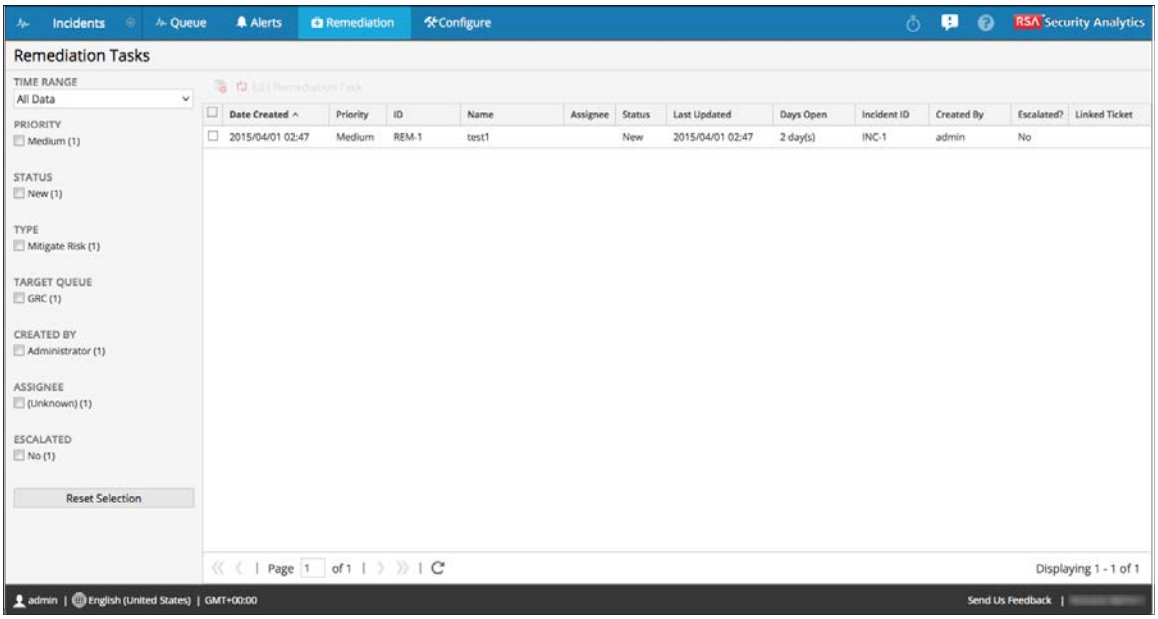
Vista Corrección

En la vista Remediación, puede administrar y rastrear las tareas de corrección y hacer lo siguiente:

- Envíe una tarea de corrección como un vale de help desk, donde se puede administrar en un sistema de help desk de terceros y rastrear hasta su cierre.
- Envíe una tarea de corrección a RSA Archer para que la solución RSA Security Operations Management la rastree.

Estas dos opciones están disponibles si están configurados los ajustes de Configuración de integración.

Para acceder a la vista Tareas de corrección, en el menú de **Security Analytics**, seleccione **Incidentes > Corrección**. Se muestra la vista Tareas de corrección. Es una lista de todas las tareas de corrección.



Características

La vista Tareas de corrección consta de dos paneles y una barra de herramientas.

El panel de opciones, a la izquierda, tiene parámetros que se pueden usar para filtrar las tareas de corrección.

Parámetro	Descripción
RANGO DE TIEMPO	Seleccione un rango de tiempo para ver tareas de corrección creadas en el rango de tiempo seleccionado. Por ejemplo: • Seleccione **Últimas 24 horas** para ver tareas de corrección creadas en las últimas 24 horas. • Seleccione **Todos los datos** para ver tareas de corrección creadas desde el momento en que se instaló el host. • Seleccione **Personalizado** y proporcione un rango de fechas para ver las tareas de corrección creadas en ese intervalo de tiempo.
PRIORIDAD	Indica la cantidad de tareas de corrección según sus prioridades. Por ejemplo: Crítico (2) indica que hay 2 tareas de corrección cuya prioridad está configurada en Crítico. Si selecciona una de las opciones mostradas, las tareas de corrección se filtran y se muestran solo las que corresponden a la prioridad seleccionada. Por ejemplo: Si se selecciona Crítico (2), el panel Tareas de corrección muestra solo las 2 tareas de corrección cuya prioridad está configurada en Crítico.

Parámetro	Descripción
STATUS	Indica la cantidad de tareas de corrección que pertenecen a un estado específico. Por ejemplo: Asignados (5) indica que hay cinco tareas de corrección que están en el estado Asignados. La selección de una de las opciones mostradas filtra las tareas de corrección y solo muestra las tareas que pertenecen al estado seleccionado. Por ejemplo: si selecciona Asignados (5), el panel Tareas de corrección muestra solo las cinco tareas que pertenecen al estado Asignados.
TYPE	Indica la cantidad de tareas de corrección categorizadas en su tipo. Por ejemplo: Poner host en cuarentena (2) indica que hay 2 tareas del tipo Poner host en cuarentena. La selección de una de las opciones mostradas filtra las tareas y solo muestra las tareas del tipo seleccionado. Por ejemplo: Si selecciona Poner host en cuarentena (2), el panel Tareas de corrección muestra solo los 2 incidentes que son del tipo Poner host en cuarentena.

Parámetro	Descripción
LÍNEA DE ESPERA DE DESTINO	Indica las tareas de corrección categorizadas según la línea de espera de asignación. Por ejemplo: Operaciones (5) indica que hay cinco incidentes que tienen tareas de corrección con la línea de espera de asignación para Operaciones. La selección de una de las opciones mostradas filtra las tareas y solo las muestra según la opción que se elige. Por ejemplo: Si selecciona Operaciones (5), el panel Tareas de corrección muestra solo las 5 tareas que están en la línea de espera de asignación para Operaciones.
CREADO POR	Indica las tareas de corrección categorizadas según la persona que creó las tareas. Por ejemplo: Administrador (3) indica que hay tres tareas de corrección creadas por el administrador. La selección de una de las opciones mostradas filtra las tareas y solo las muestra según la opción que se elige. Por ejemplo: Si selecciona Administrador (3), el panel Tareas de corrección muestra solo las 3 tareas que creó el administrador.
USUARIO ASIGNADO	Indica las tareas de corrección categorizadas según el usuario a quién están asignadas. Por ejemplo: <user1> (3) indica que hay 3 tareas de corrección asignadas a user1. La selección de una de las opciones mostradas filtra las tareas y solo las muestra según la opción que se elige. Por ejemplo: si selecciona <user1> (3), el panel Tareas de corrección muestra solo las 3 tareas asignadas a user1.

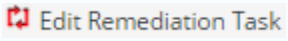
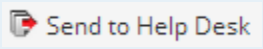
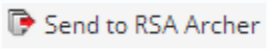
Parámetro	Descripción
ELEVADO	Indica las tareas de corrección que se elevaron.
Reset Selection	Restablece las opciones de filtro a los valores predeterminados

En el panel Tareas de corrección se incluye una lista de tareas de corrección y sus detalles.

Parámetro	Descripción
Fecha de creación	Muestra la fecha en que se creó la tarea de corrección.
Prioridad	Muestra la prioridad asignada a la tarea de corrección. La prioridad puede ser cualquiera de las siguientes: Crítica, Alta, Media o Baja.
ID	Muestra el ID de tarea de corrección.
Nombre	Muestra el nombre de la tarea de corrección.
Usuario asignado	Muestra el nombre del usuario a quien se asigna la tarea de corrección.
Status	Muestra el estado de la tarea de corrección. Por ejemplo, Nuevo, En curso, Corregido.
Última actualización	Muestra la fecha y hora de la última actualización de la tarea de corrección.
Días abierta	Muestra la cantidad de días en que estuvo abierta la tarea de corrección.
ID del incidente	Muestra el ID del incidente para el que se creó la tarea de corrección.
Creado por	Muestra el usuario que creó la tarea de corrección.
¿Elevado?	Muestra si la tarea de corrección se elevó.
Vale vinculado	Muestra si la tarea de corrección se envió como vale de help desk o a cualquier solución de otros fabricantes.

Barra de herramientas

En esta tabla se indican las operaciones que se pueden realizar en la vista Tareas de corrección.

Parámetro	Descripción
	Permite eliminar tareas de corrección.
	Permite modificar la tarea de corrección.
	Permite enviar la tarea de corrección a help desk.
	Permite enviar la tarea de corrección a RSA Archer.

Vista Detalles de tareas de corrección

En la vista de detalles Tarea de corrección, puede ver los detalles de la tarea de corrección, modificarla y ver los detalles del incidente para el cual se creó.

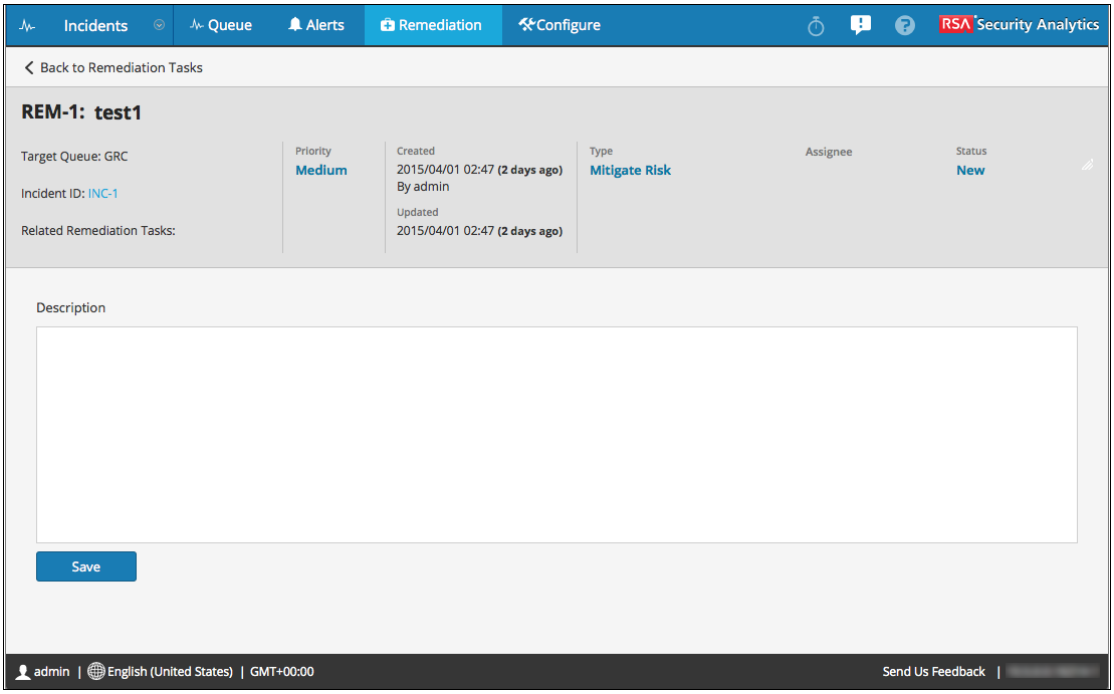
Para acceder a la vista de detalles Tarea de corrección:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Corrección**.

   Se muestra la vista Tareas de corrección.

2. Haga doble clic en una de las tareas de corrección.

   Se muestra la vista Detalles de tarea de corrección.



Características

En la siguiente tabla se enumeran los parámetros que se muestran en la vista de detalles Tarea de corrección.

Parámetro	Descripción
Línea de espera de destino	Muestra la línea de espera de destino a la cual se asignó la tarea.
ID del incidente	Muestra el ID del incidente para el cual se creó la tarea. Haga clic en el ID para mostrar los detalles del incidente.

Parámetro	Descripción
Tareas de corrección relacionadas	Muestra las tareas de corrección relacionadas. Haga clic en la tarea relacionada para navegar a la vista de tareas relacionadas.
Prioridad	Muestra la prioridad de la tarea. Este es un campo editable.
Created	Muestra detalles sobre la fecha y hora en que se creó la tarea y quién la creó.
Fragmento C	Muestra la fecha y hora de la última actualización de la tarea.
Tipo	Muestra el tipo según el cual se categoriza la tarea de corrección. Este es un campo editable.
Usuario asignado	Muestra el usuario a quien se asigna la tarea de corrección. Este es un campo editable.
Status	Muestra el estado de la tarea de corrección. Este es un campo editable.

Barra de herramientas

En esta tabla se muestran las operaciones que se pueden ejecutar en la vista de detalles Tarea de corrección.

Parámetro	Acción
Volver a Tareas de corrección	Permite volver a la vista Tareas de corrección.
Enviar a help desk	Permite enviar la tarea a help desk. Esta opción solo está visible cuando se configura en los ajustes de la integración.
Enviar a RSA Archer	Le permite enviar la tarea a la solución RSA Archer. Esta opción solo está visible cuando se configura en los ajustes de integración.

Parámetro	Acción
Editar	Permite modificar la tareas si es necesario. Puede modificar los siguientes parámetros: Tipo, Prioridad, Usuario asignado y Estado.

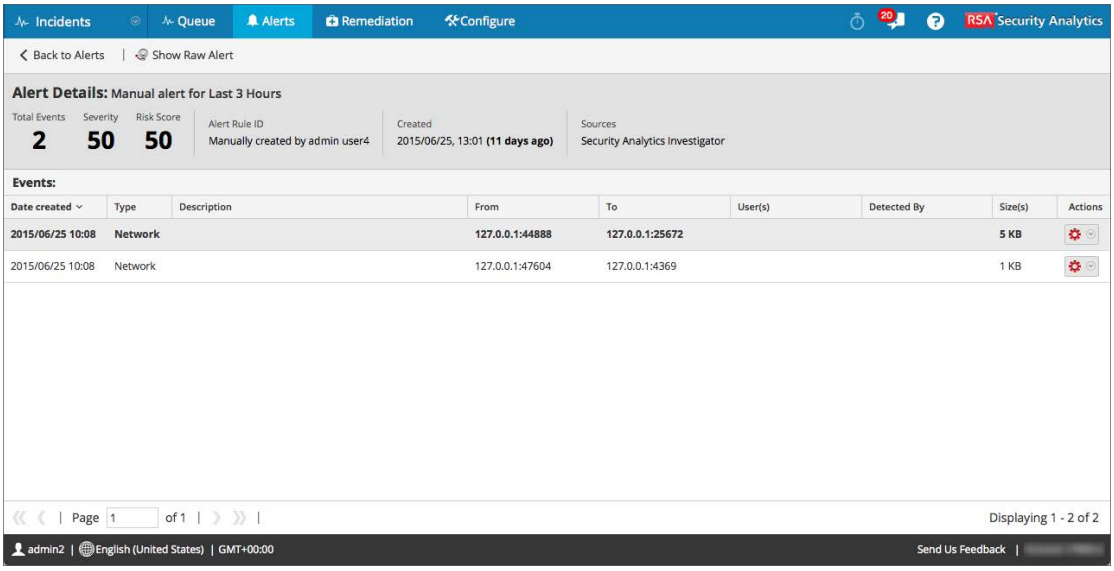
Vista Detalles de alertas

La vista Detalles de alertas permite ver los detalles de una alerta.

Para acceder a la vista Detalles de alertas:

1. 1. En el menú de **Security Analytics**, seleccione **Incidentes > Alertas**.
2. Haga doble clic en una alerta.

   Se muestra la vista Detalles de la alerta.



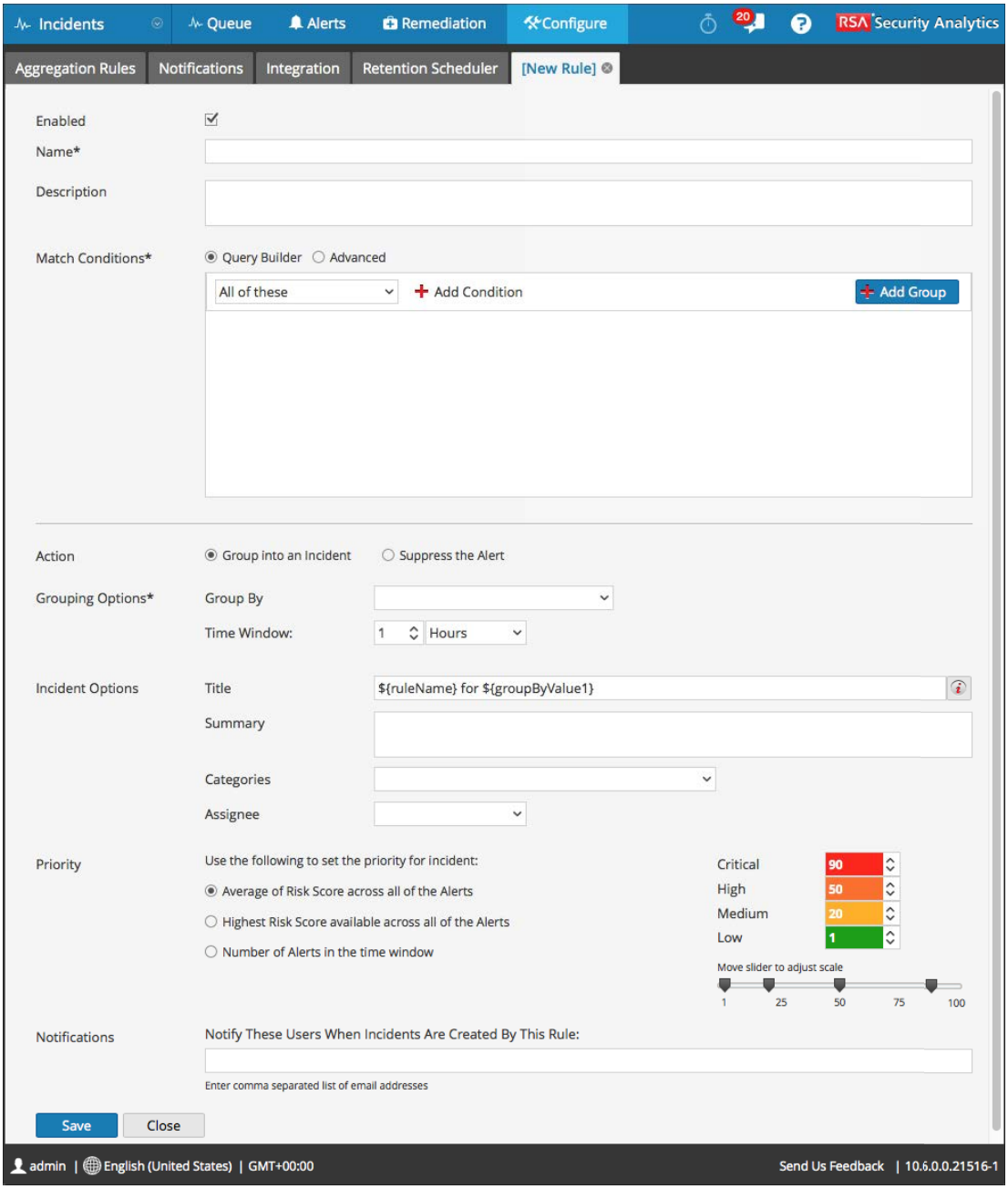
Los procedimientos relacionados están disponibles en Filtrar alertas.

Características

En la siguiente tabla se enumeran los parámetros que se muestran en la vista Detalles de alertas.

Parámetro	Descripción
Total de eventos	Muestra la cantidad total de eventos.
Gravedad	Muestra el nivel de severidad.
Puntaje de riesgo	Muestra el nivel de riesgo.
ID de regla de alerta	Muestra cómo y quién creó la alerta.
Created	Muestra detalles sobre la fecha y la hora en que se creó la tarea.
Orígenes	Muestra el origen original.

Se muestra la pestaña **Nueva regla**.



La vista Nueva regla ofrece varios campos en los cuales puede personalizar una nueva regla.

En la siguiente tabla se detallan los parámetros que se deben proporcionar para crear nuevas reglas de agregación.

Parámetro	Descripción
Activado	Seleccione esta opción para activar la regla.

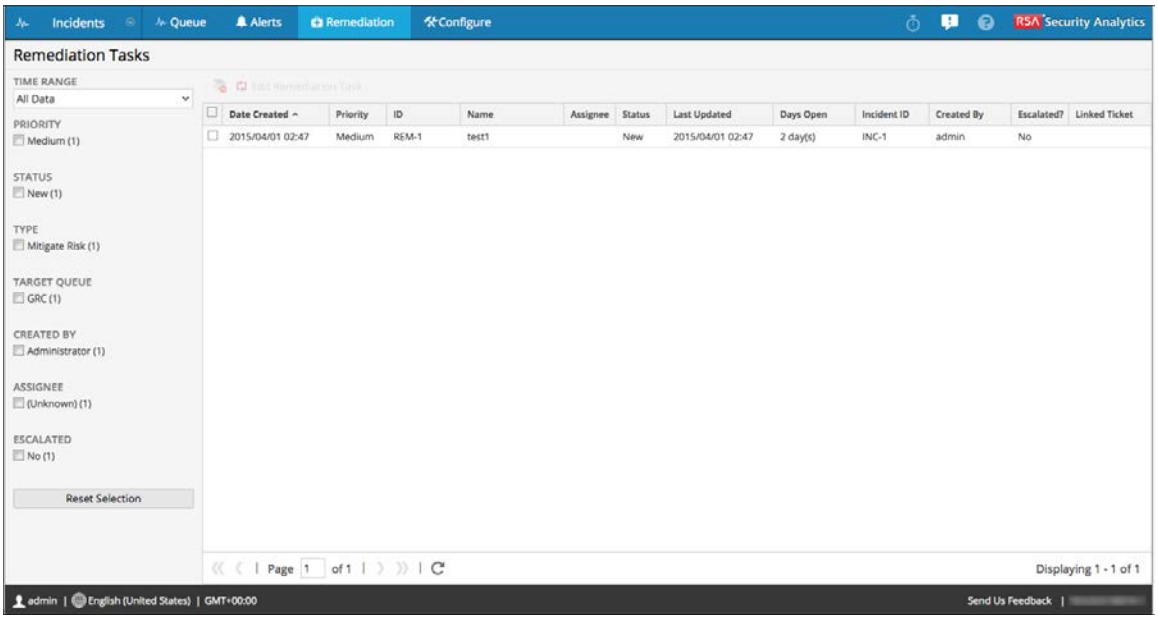
Vista Corrección

En la vista Remediación, puede administrar y rastrear las tareas de corrección y hacer lo siguiente:

- Envíe una tarea de corrección como un vale de help desk, donde se puede administrar en un sistema de help desk de terceros y rastrear hasta su cierre.
- Envíe una tarea de corrección a RSA Archer para que la solución RSA Security Operations Management la rastree.

Estas dos opciones están disponibles si están configurados los ajustes de Configuración de integración.

Para acceder a la vista Tareas de corrección, en el menú de **Security Analytics**, seleccione **Incidentes > Corrección**. Se muestra la vista Tareas de corrección. Es una lista de todas las tareas de corrección.



Características

La vista Tareas de corrección consta de dos paneles y una barra de herramientas.

El panel de opciones, a la izquierda, tiene parámetros que se pueden usar para filtrar las tareas de corrección.

Vista Detalles de tareas de corrección

En la vista de detalles Tarea de corrección, puede ver los detalles de la tarea de corrección, modificarla y ver los detalles del incidente para el cual se creó.

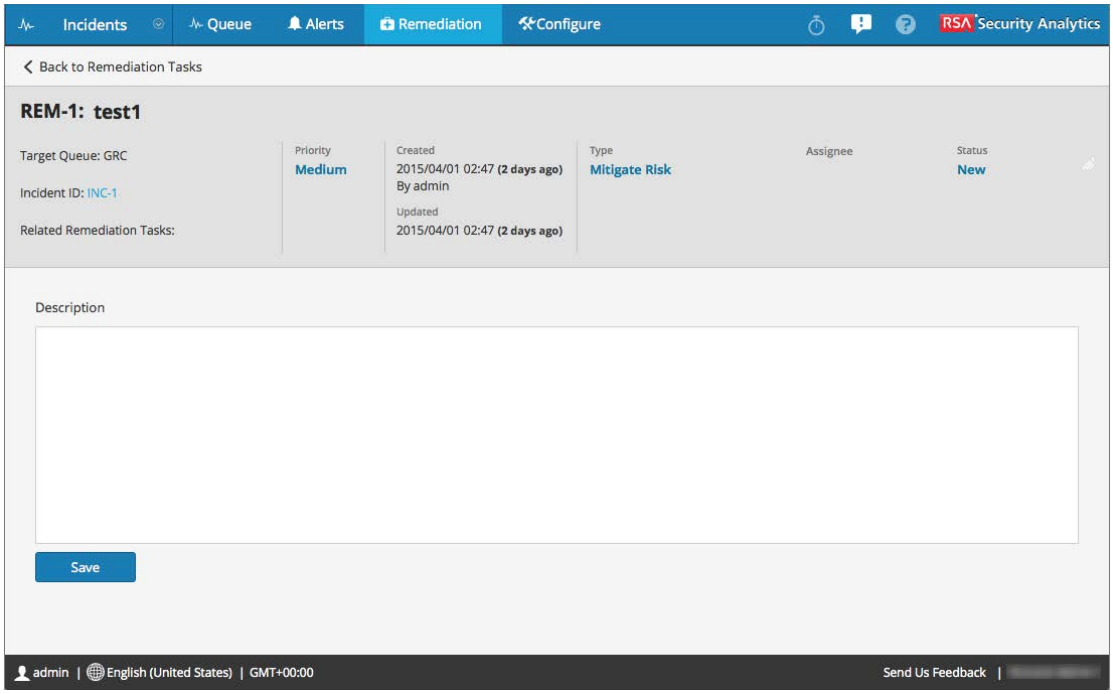
Para acceder a la vista de detalles Tarea de corrección:

1. En el menú de **Security Analytics**, seleccione **Incidentes > Corrección**.

   Se muestra la vista Tareas de corrección.

2. Haga doble clic en una de las tareas de corrección.

   Se muestra la vista Detalles de tarea de corrección.



Características

En la siguiente tabla se enumeran los parámetros que se muestran en la vista de detalles Tarea de corrección.

Parámetro	Descripción
Línea de espera de destino	Muestra la línea de espera de destino a la cual se asignó la tarea.
ID del incidente	Muestra el ID del incidente para el cual se creó la tarea. Haga clic en el ID para mostrar los detalles del incidente.