RSA NETWITNESS® SUITE

Guía del usuario de NetWitness Respond

para la versión 11.1

Información de contacto

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

Marcas comerciales

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

Acuerdo de licencia

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

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

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

Licencias de otros fabricantes

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

Nota sobre tecnologías de cifrado

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

Distribución

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

julio 2018

Contenido

Proceso de NetWitness Respond **7**

Flujo de trabajo de NetWitness Respond 9

Respuesta ante incidentes **10**

Flujo de trabajo de respuesta ante incidentes 12

Revisar la lista de incidentes ordenados por prioridad 12

Ver la Lista de incidentes 12

Filtrar la Lista de incidentes 14

Quitar los filtros de la vista Lista de incidentes 17

Ver mis incidentes 17

Buscar un incidente 17

Ordenar la Lista de incidentes 18

Ver los incidentes sin asignar 19

Asignar los incidentes a uno mismo 19

Cancelar asignación de un incidente 21

Ermitteln, welche Incidents eine Aktion erfordern **23**

Ver detalles de incidentes 23

Ver información de resumen básica acerca del incidente 26

Ver los indicadores y los enriquecimientos 28

Ver y estudiar los eventos 30

Ver y estudiar las entidades involucradas en los eventos 33

Filtrar los datos en la vista Detalles de incidente 36

Ver las tareas asociadas a un incidente 39

Ver notas sobre los incidentes 39

Buscar indicadores relacionados 40

Agregar indicadores relacionados al incidente 42

Investigar el incidente **44**

Ver información contextual 44

Agregar una entidad a una lista blanca 47

Crear una lista 48

Cambiar a NetWitness Endpoint 49

Cambiar a Investigate 49
Documentar los pasos realizados fuera de NetWitness 50
Ver las entradas del registro para un incidente 51
Agregar una nota 52
Eliminar una nota 53

Elevar o corregir el incidente 54

Actualizar un incidente 54
Cambiar el estado de un incidente 54
Cambiar la prioridad del incidente 57
Asignar incidentes a otros analistas 60
Cambiar el nombre de un incidente 62
Ver todas las tareas de incidentes 64
Filtrar la Lista de tareas 65
Quitar los filtros de la Lista de tareas 67
Crear una tarea 68
Buscar una tarea 72
Modificar una tarea 72
Eliminar una tarea 76
Cerrar un incidente 78

Revisión de alertas 80

Ver alertas 80
Filtrar la Lista de alertas 82
Quitar los filtros de la Lista de alertas 85
Ver información de resumen de las alertas 85
Ver detalles de los eventos de una alerta 86
Investigar eventos 90
Ver información contextual 90
Agregar una entidad a una lista blanca 93
Crear una lista blanca 94
Cambiar a NetWitness Endpoint 94
Cambiar a Investigation 94
Crear un incidente manualmente 94
Agregar alertas a un incidente 96
Eliminar alertas 99

Información de referencia de NetWitness Respond 100

Vista Lista de incidentes 101
Flujo de trabajo 101
¿Qué desea hacer? 102
Temas relacionados 103
Vista rápida 104
Vista Lista de incidentes 104
Lista de incidentes 106
Panel Filtros 108
Panel Descripción general 110
Acciones de la barra de herramientas 112
Vista Detalles de incidente 113
Flujo de trabajo 113
¿Qué desea hacer? 114
Temas relacionados 115
Vista rápida 116
Panel Descripción general 117
Panel Indicadores 117
Gráfico de nodos 118
Hoja de datos Eventos 120
Panel Registro 123
Panel Tareas 124
Panel Indicadores relacionados 125
Acciones de la barra de herramientas 127
Vista Lista de alertas 129
Flujo de trabajo 129
¿Qué desea hacer? 129
Temas relacionados 131
Vista Lista de alertas 131
Lista de alertas 132
Panel Filtros 134
Panel Descripción general 136
Acciones de la barra de herramientas 139
Vista Detalles de la alerta 140
Flujo de trabajo 140
¿Qué desea hacer? 140

Temas relacionados 142
Vista Detalles de la alerta 142
Panel Descripción general 142
Panel Eventos 143
Lista de eventos 143
Detalles de eventos 144
Metadatos de eventos 144
Atributos de dispositivos de origen o destino de eventos 146
Atributos de usuarios de origen o destino de eventos 147
Acciones de la barra de herramientas 148
Vista Lista de tareas 149
¿Qué desea hacer? 149
Temas relacionados 149
Lista de tareas 150
Panel Descripción general de tareas 154
Acciones de la barra de herramientas 156
Cuadro de diálogo Agregar/eliminar de la lista 157
¿Qué desea hacer? 157
Agregar/eliminar de la lista 159
Panel Búsqueda de contexto: Vista Respond 161
¿Qué desea hacer? 161
Temas relacionados 162
Información contextual que se muestra en el panel Búsqueda de contexto 162

Proceso de NetWitness Respond

NetWitness Suite Respond recopila alertas de varios orígenes y ofrece la capacidad de agruparlas de manera lógica e iniciar un flujo de trabajo de respuesta ante incidentes para investigar y corregir los problemas de seguridad que se presenten. NetWitness Suite Respond permite configurar reglas que agregan alertas en incidentes. El sistema normalizará las alertas en 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 agrupen las 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 cuatro 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 alertas nuevas, si ya se creó un incidente que coincide con estos criterios y ese incidente aún no está “en curso”, las alertas nuevas 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 incidentes. 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 usa 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 las tareas asociadas.

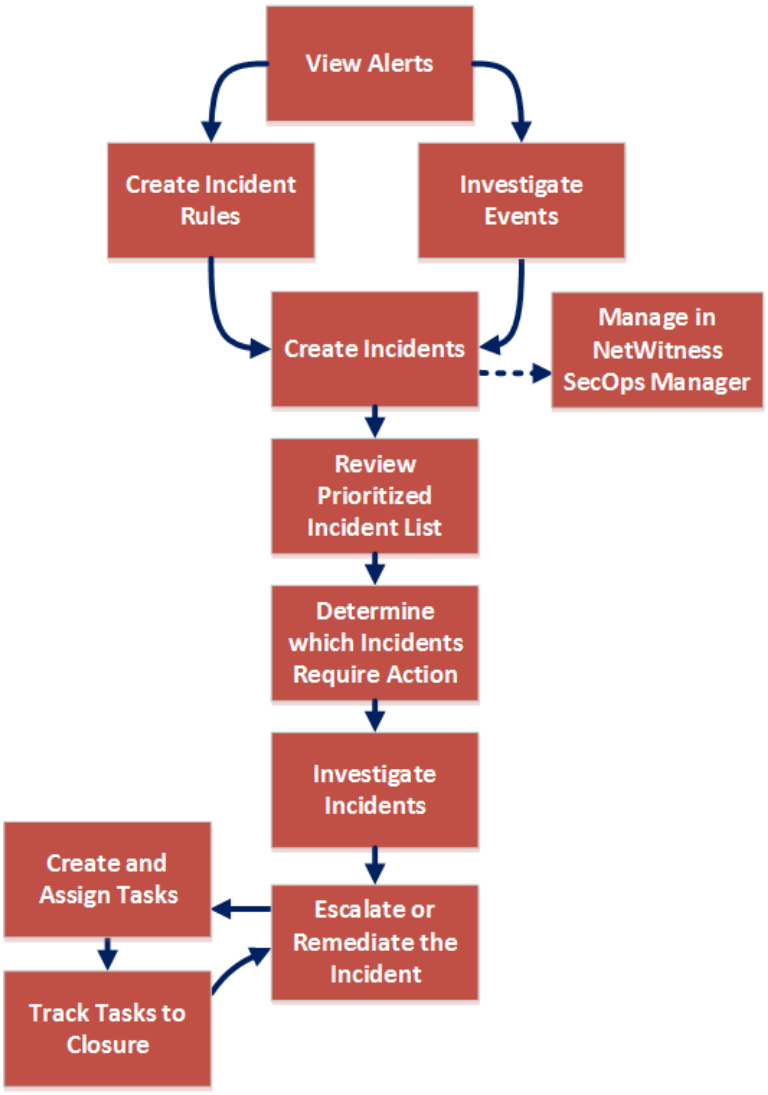
Las etapas del proceso de NetWitness Respond son las siguientes:

- Revisar alertas
- Crear incidentes
- Responder ante incidentes:
  - Revisar la lista de incidentes ordenados por prioridad
  - Determinar los incidentes que requieren acción
  - Investigar incidentes
  - Elevar o corregir el incidente (esto incluye la creación y la asignación de tareas, así como su rastreo hasta el cierre).

También tiene la opción de administrar incidentes en RSA NetWitness® SecOps Manager en lugar de NetWitness Respond.

Flujo de trabajo de NetWitness Respond

En la siguiente figura se muestra el proceso general del flujo de trabajo de NetWitness Respond.



Respuesta ante incidentes

Un *incidente* es un conjunto de alertas agrupado de manera lógica que el motor de agregación de incidentes crea automáticamente y que se agrupa según un criterio específico. Un incidente, disponible en la vista Responder, permite a un analista realizar triage, investigar y corregir estos grupos de alertas. Los incidentes se pueden transferir entre usuarios, se les pueden agregar notas y se pueden explorar mediante un gráfico de nodos. Los incidentes permiten que los usuarios se aseguren de comprender el alcance completo de un ataque o un evento en su sistema NetWitness Suite y, a continuación, que tomen medidas.

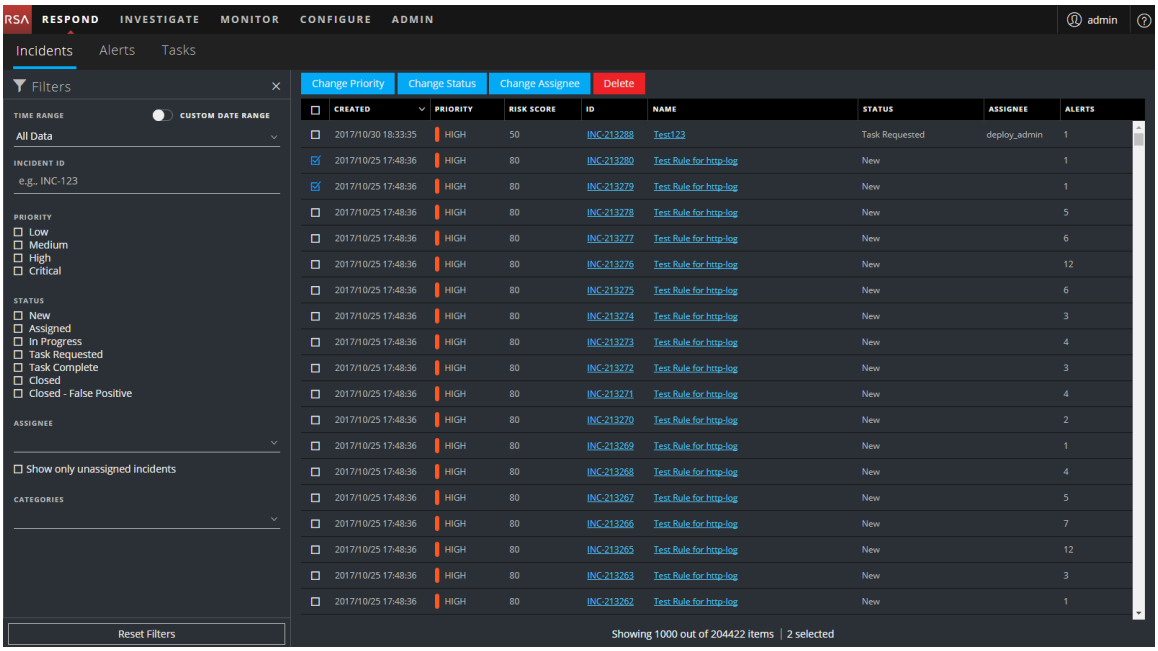
La vista **Respond** está diseñada para ayudarlo a identificar ágilmente los problemas existentes en la red y a trabajar con otros analistas para resolverlos con rapidez.

La vista Respond presenta a los encargados de respuesta ante incidentes una línea de espera de incidentes en orden de gravedad. Cuando selecciona un incidente en la línea de espera, usted recibe los datos de soporte pertinentes que lo ayudarán a investigarlo. Esto le permite determinar el alcance del incidente y elevarlo o corregirlo según corresponda.

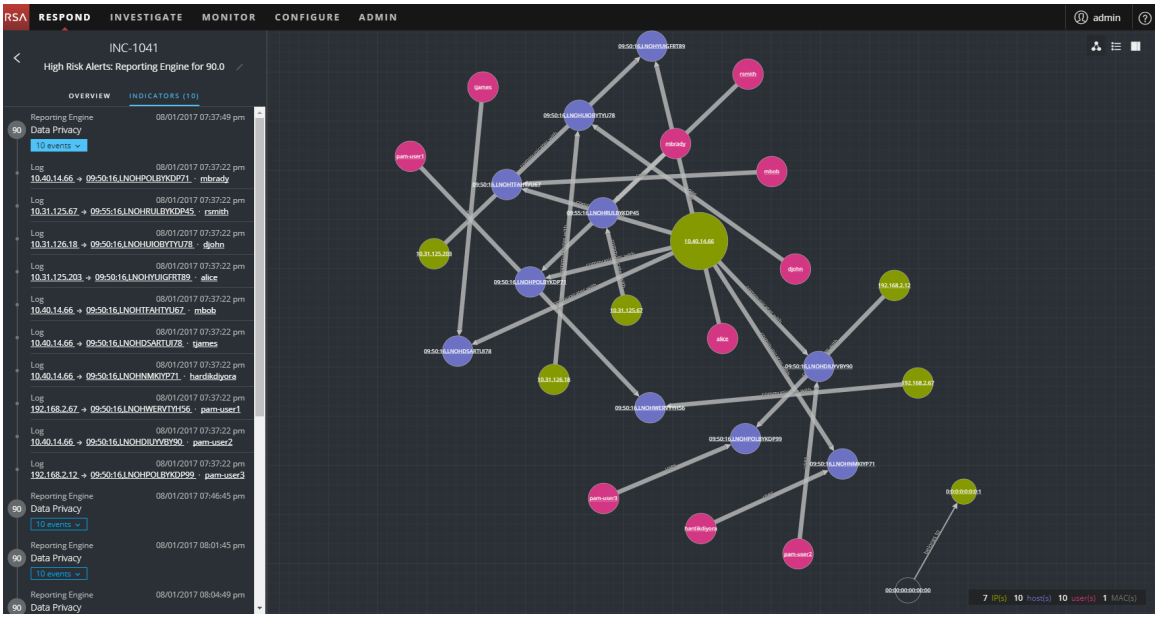
En la vista Respond, puede incidentes, alertas y tareas:

- **Incidentes**: Permite responder ante incidentes y administrarlos de principio a fin.
- **Alertas**: Permite administrar las alertas de todos los orígenes que recibe NetWitness Suite y crear incidentes a partir de alertas seleccionadas.
- **Tareas**: Permite ver y administrar la lista completa de tareas creadas para todos los incidentes.

Si navega a RESPOND > Incidentes, puede acceder a la vista Lista de incidentes y, desde ahí, acceder a la vista Detalles de incidente correspondiente a un incidente seleccionado. Estas son las vistas principales que utiliza para responder ante incidentes. En la siguiente figura se muestra la lista de incidentes ordenados por prioridad en la vista **Lista de incidentes**.



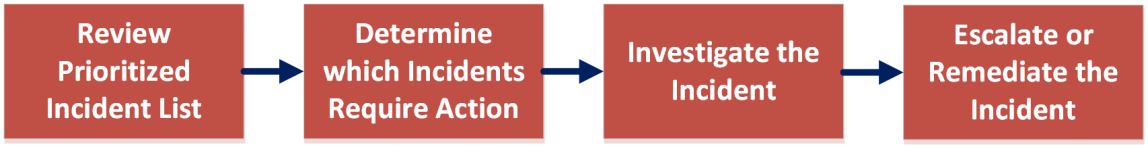
En la siguiente figura se muestra un ejemplo de los detalles disponibles en la vista **Detalles de incidente**.



La vista Respond está diseñada para facilitar la evaluación de los incidentes, contextualizar esos datos, colaborar con otros analistas y pasar a una investigación detallada según sea necesario.

Flujo de trabajo de respuesta ante incidentes

En este flujo de trabajo se muestra el proceso general que usan los encargados de respuesta ante incidentes para responder ante incidentes en NetWitness Suite.



En primer lugar, debe revisar la lista de incidentes ordenados por prioridad, la que muestra información básica acerca de cada incidente, y determinar cuáles de ellos requieren una acción. Puede hacer clic en un vínculo en un incidente para obtener un panorama más claro de este y detalles de soporte en la vista Detalles de incidente. Desde ahí, puede investigarlo más a fondo. A continuación, puede determinar cómo responder ante el incidente, ya sea con su escalación o su corrección.

Estos son los pasos básicos para responder ante un incidente:

1. Revisar la lista de incidentes ordenados por prioridad
2. Ermitteln, welche Incidents eine Aktion erfordern
3. Investigar el incidente
4. Elevar o corregir el incidente

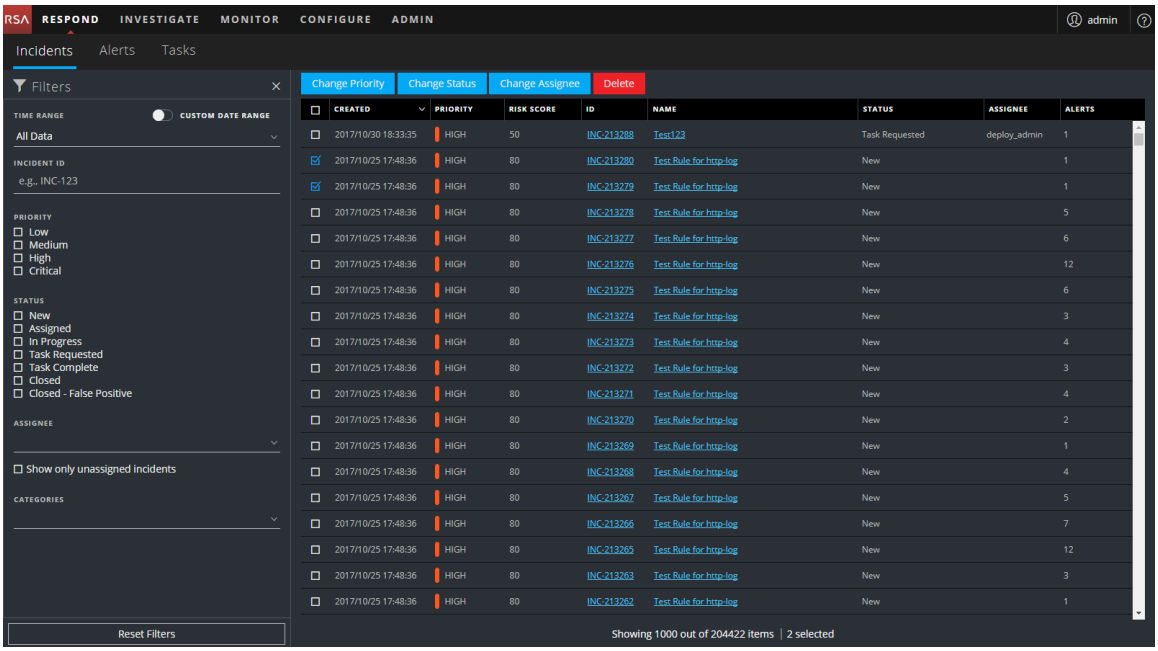
Revisar la lista de incidentes ordenados por prioridad

En la vista Respond, puede ver la lista de incidentes ordenados por prioridad. La Lista de incidentes muestra los incidentes activos y cerrados.

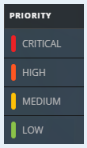
Ver la Lista de incidentes

Después de iniciar sesión en NetWitness Suite, para la mayoría de los encargados de respuesta ante incidentes se abre la vista Respond, la que está configurada como la vista predeterminada. Si su vista inicial es otra, puede navegar a la vista Respond.

1. Inicie sesión en NetWitness Suite.
   La vista Respond muestra la lista de incidentes, a la cual también se denomina la vista Lista de incidentes.



2. Si no ve la lista de incidentes en la vista Responder, vaya a **RESPONDER > Incidentes**.
3. Desplácese por la lista de incidentes, la que muestra información básica acerca de cada incidente, como se describe en la siguiente tabla.

Columna	Descripción
CREADO	Muestra la fecha de creación del incidente.
PRIORIDAD	Muestra la prioridad del incidente. La prioridad puede ser Crítica, Alta, Media o Baja. La prioridad está codificada en colores. El rojo indica un incidente con prioridad **Crítica**, el naranja, uno con riesgo de prioridad **Alta**, el amarillo, **Media** y el verde, **Baja**. Por ejemplo: 
PUNTAJE DE RIESGO	Muestra el puntaje de riesgo del incidente. El puntaje de riesgo indica el riesgo del incidente que se calcula por medio de un algoritmo y que está entre 0 y 100. 100 es el puntaje de riesgo más alto.
ID	Muestra el número de incidente creado automáticamente. A cada incidente se le asigna un número único que puede utilizar para rastrearlo.

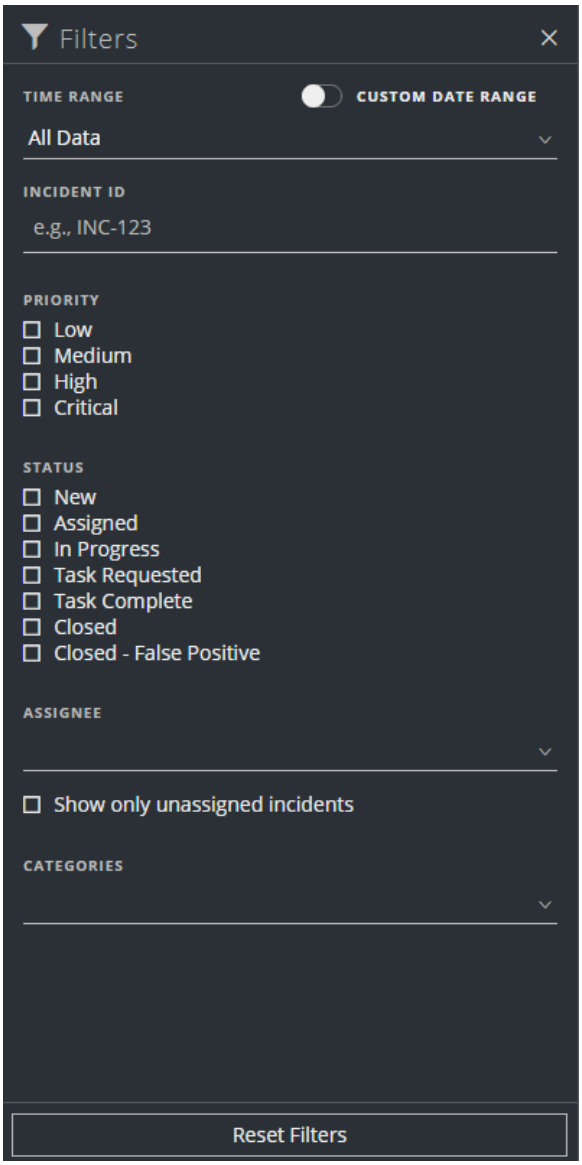
Columna	Descripción
NAME	Muestra el nombre del incidente. El nombre del incidente proviene de la regla que se usa para activar el incidente. Haga clic en el vínculo para ir a la vista Detalles de incidente del incidente seleccionado.
ESTADO	Muestra el estado del incidente. El estado puede ser: **Nuevo**, **Asignado**, **En curso**, **Tarea solicitada**, **Tarea completa**, **Cerrado** y **Cerrado: falso positivo**.
USUARIO ASIGNADO	Muestra el miembro del equipo que está asignado al incidente.
ALERTAS	Muestra la cantidad de alertas asociadas con el incidente. Un incidente puede incluir muchas alertas. Una gran cantidad de alertas puede significar que se experimenta un ataque a gran escala.

En la parte inferior de la lista, puede ver la cantidad de incidentes que se muestran en la página actual, la cantidad total de incidentes y la cantidad de incidentes seleccionados. Por ejemplo: **Mostrando 1,000 de 1,115 elementos | 3 seleccionado(s)**. La cantidad máxima de incidentes que se pueden ver al mismo tiempo es 1,000.

Filtrar la Lista de incidentes

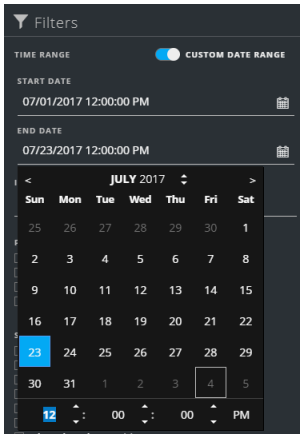
La cantidad de incidentes en la vista Lista de incidentes puede ser muy alta, lo que dificulta la localización de determinados incidentes. El Filtro permite especificar los incidentes que desea ver. También puede elegir el intervalo de tiempo en que ocurrieron esos incidentes. Por ejemplo, tal vez desee ver todos los incidentes críticos nuevos que se crearon en la última hora.

1. Verifique que el panel Filtros aparezca a la izquierda de la lista de incidentes. Si no ve el panel Filtros, en la barra de herramientas de la vista Lista de incidentes, haga clic en ▼ para abrirlo.



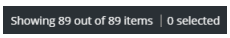
2. En el panel Filtros, seleccione una o más opciones para filtrar la lista de incidentes:
   - **RANGO DE TIEMPO**: Puede seleccionar un período específico en la lista desplegable Rango de tiempo. El rango de tiempo se basa en la fecha de creación de los incidentes. Por ejemplo, si selecciona Última hora, verá los incidentes que se crearon en los últimos 60 minutos.
   - **RANGO DE FECHAS PERSONALIZADO**: Puede especificar un rango de fechas determinado en lugar de seleccionar una opción de Rango de tiempo. Para ello, haga clic en el círculo blanco frente a Rango de fechas personalizado para ver los campos Fecha de

inicio y Fecha de finalización. Seleccione las fechas y las horas en el calendario.



- **ID DEL INCIDENTE**: Escriba el ID de un incidente que desee localizar, por ejemplo, INC-1050.
- **PRIORIDAD**: Seleccione las prioridades que desea ver.
- **ESTADO**: Seleccione uno o más estados de incidentes. Por ejemplo, seleccione Cerrado: falso positivo para ver solo los incidentes que son falsos positivos, los cuales se identificaron inicialmente como sospechosos, pero después se determinó que eran seguros.
- **USUARIO ASIGNADO**: Seleccione el usuario o los usuarios asignados de los incidentes que desea ver. Por ejemplo, si solo desea ver los incidentes asignados a Cale o Stanley, seleccione Cale y Stanley en la lista desplegable Usuario asignado. Si desea ver los incidentes sin tener en cuenta el usuario asignado, no realice ninguna selección en Usuario asignado.
  (Disponible en la versión 11.1 y superior) Para ver solamente los incidentes sin asignar, seleccione **Mostrar solo los incidentes sin asignar**.
- **CATEGORÍAS**: Seleccione una o más categorías en la lista desplegable. Por ejemplo, si solo desea ver incidentes clasificados con las categorías de abuso Backdoor o Privilegio, seleccione abuso de Backdoor y Privilegio.

La Lista de incidentes muestra los incidentes que cumplen con los criterios de selección. Puede ver la cantidad de incidentes de la lista filtrada en la parte inferior de la lista de incidentes.



3. Haga clic en ✕ para cerrar el panel Filtros y volver a la vista Lista de incidentes, que ahora muestra los incidentes filtrados.

Quitar los filtros de la vista Lista de incidentes

NetWitness Suite recuerda las selecciones de filtros en la vista Lista de incidentes. Puede quitar las selecciones de filtros cuando ya no las necesite. Por ejemplo, si no ve la cantidad de incidentes que espera o que desea ver, o desea ver todos los incidentes en la lista de incidentes, puede restablecer los filtros.

1. En la barra de herramientas de la vista Lista de incidentes, haga clic en .
   El panel Filtros aparece a la izquierda de la lista de incidentes.
2. En la parte inferior del panel Filtros, haga clic en **Restablecer filtros**.

Ver mis incidentes

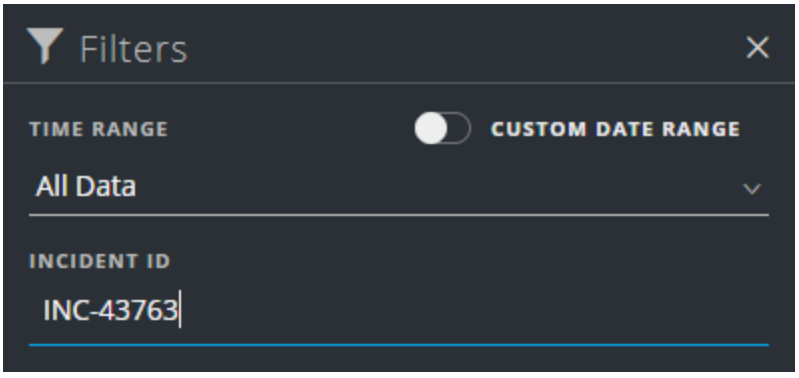
Puede ver sus incidentes si los filtra por su nombre de usuario.

1. Si no puede ver el panel Filtro, en la barra de herramientas de la vista Lista de incidentes, haga clic en .
2. En el panel Filtro, bajo USUARIO ASIGNADO, seleccione su nombre de usuario en la lista desplegable.
   La Lista de incidentes muestra los incidentes que se le asignaron.

Buscar un incidente

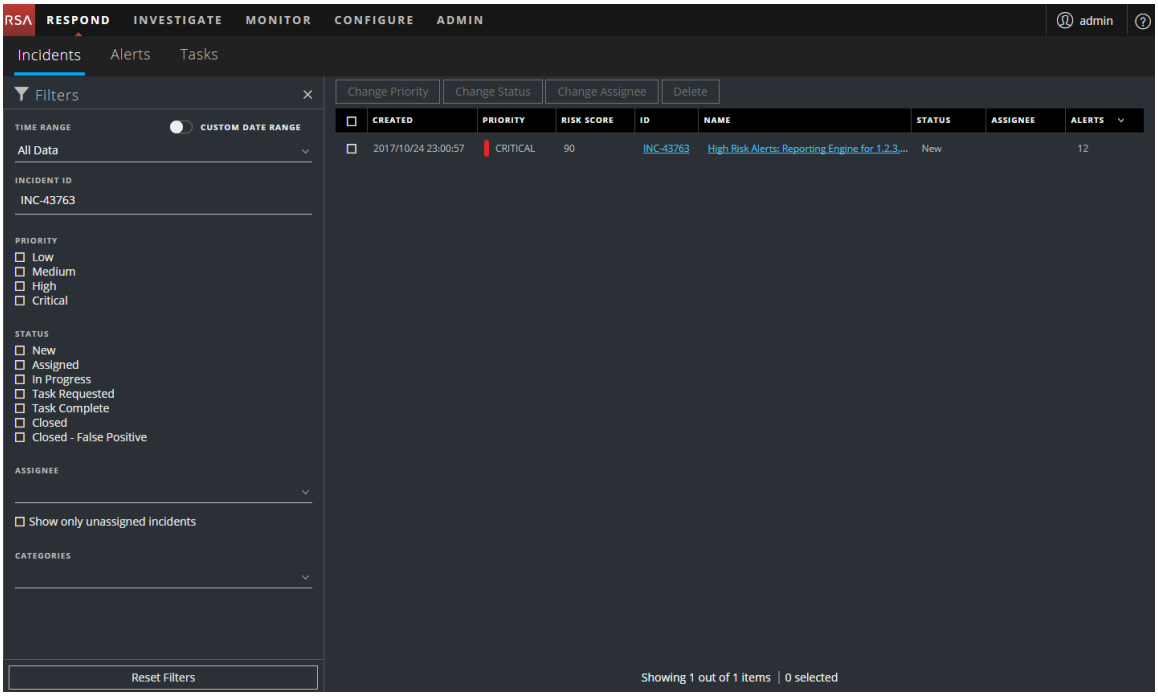
Si conoce el ID de incidente, puede buscar rápidamente un incidente mediante el filtro. Por ejemplo, tal vez desee buscar un incidente específico entre miles de incidentes.

1. Vaya a **RESPONDER > Incidentes**.
   El panel Filtros aparece a la izquierda de la lista de incidentes. Si no ve el panel Filtros, en la barra de herramientas de la vista Lista de incidentes, haga clic en para abrirlo.



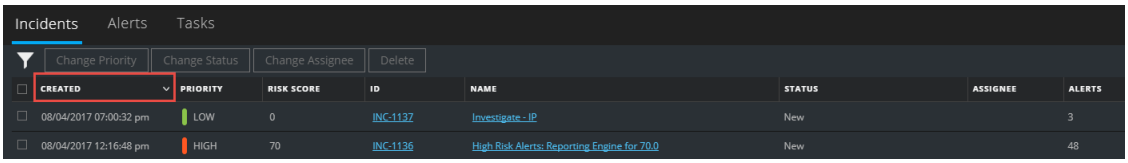
2. En el campo ID DEL INCIDENTE, escriba el ID de un incidente que desee localizar; por ejemplo, INC-43763.

El incidente especificado aparece en la lista de incidentes. Si no ve ningún resultado, intente restablecer los filtros.



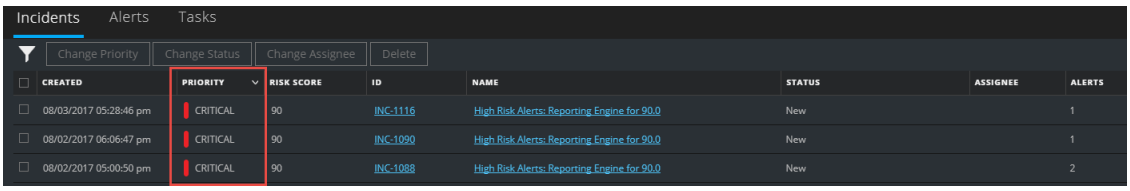
Ordenar la Lista de incidentes

El orden predeterminado de la Lista de incidentes es por Fecha de creación en orden descendente (los más recientes en la parte superior).

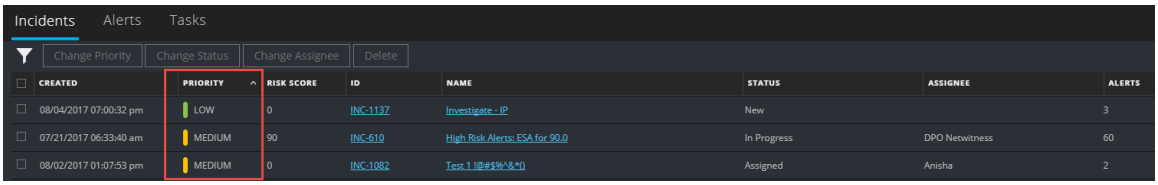


Para cambiar el orden de la Lista de incidentes, haga clic en una columna de la lista.

Por ejemplo, para clasificar los incidentes por prioridad, puede ordenar la vista por la columna Prioridad. Para esto, coloque el cursor sobre la columna Prioridad y haga clic en la flecha hacia abajo ⌄. La Lista de incidentes se ordena por Prioridad en orden descendente (la prioridad más alta en la parte superior), como se muestra en la siguiente figura.



Para ordenarla por Prioridad en orden ascendente (la prioridad más baja en la parte superior), haga clic en la flecha hacia arriba ⌃, como se muestra en la siguiente figura.

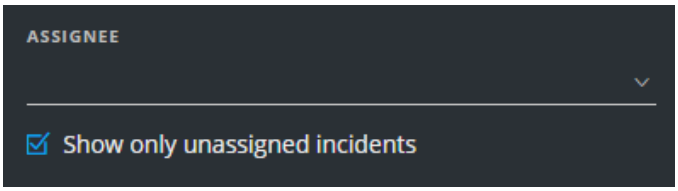


Ver los incidentes sin asignar

Esta opción está disponible en la versión 11.1 y superior.

Puede ver los incidentes sin asignar mediante el filtro.

1. Si no puede ver el panel Filtro, en la barra de herramientas de la vista Lista de incidentes, haga clic en ▼.
2. En el panel Filtros, bajo USUARIO ASIGNADO, seleccione **Mostrar solo los incidentes sin asignar**.

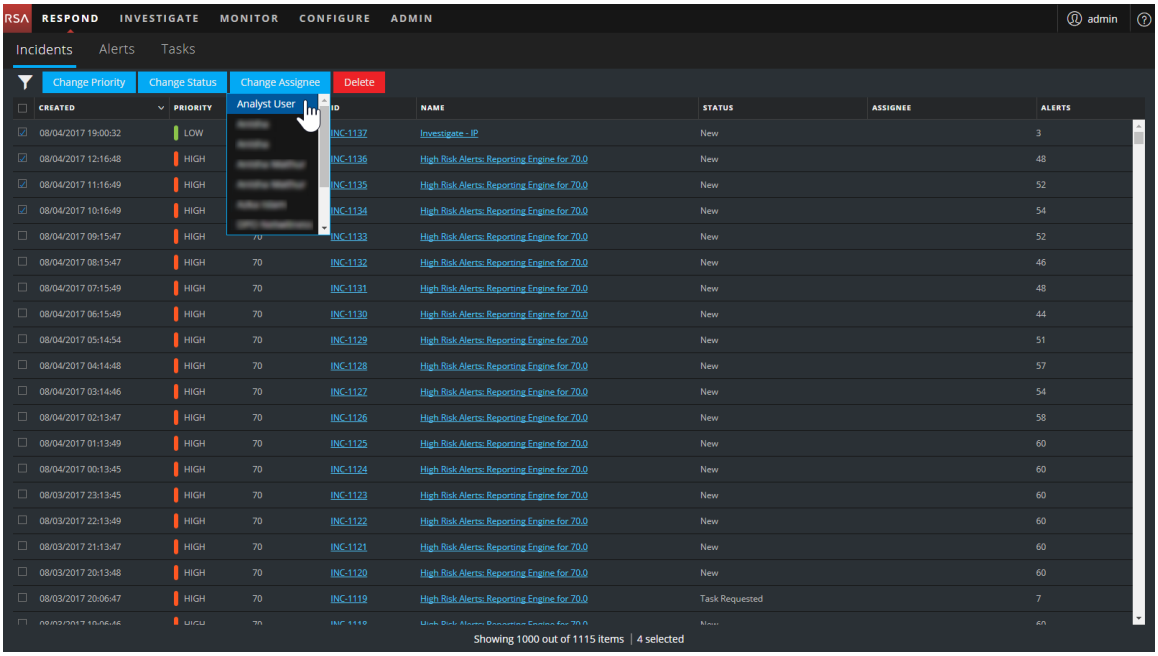
   

   La lista de incidentes se filtrará para mostrar los incidentes sin asignar.

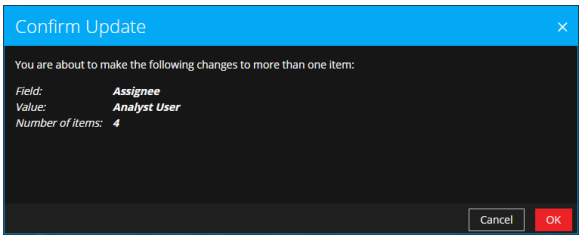
Asignar los incidentes a uno mismo

1. En la vista Lista de incidentes, seleccione uno o más incidentes que desee asignar a usted mismo.

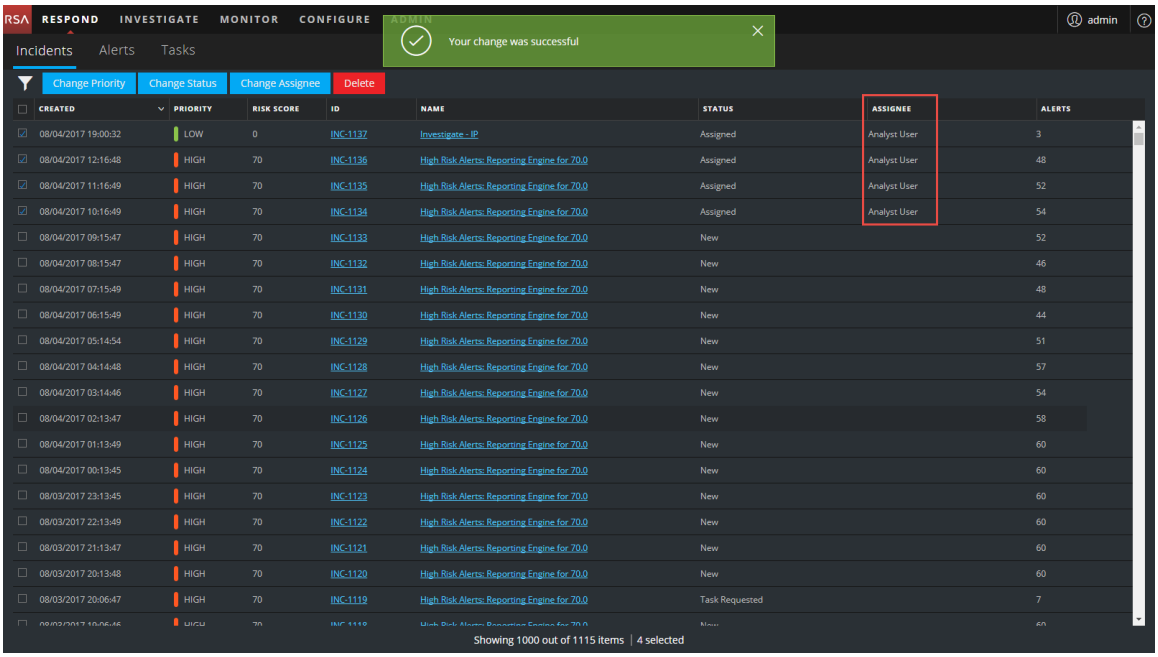
2. Haga clic en **Cambiar usuario asignado** y seleccione un nombre de usuario en la lista desplegable.



3. Si seleccionó más de un incidente, en el cuadro de diálogo Confirmar actualización, haga clic en **Aceptar**.

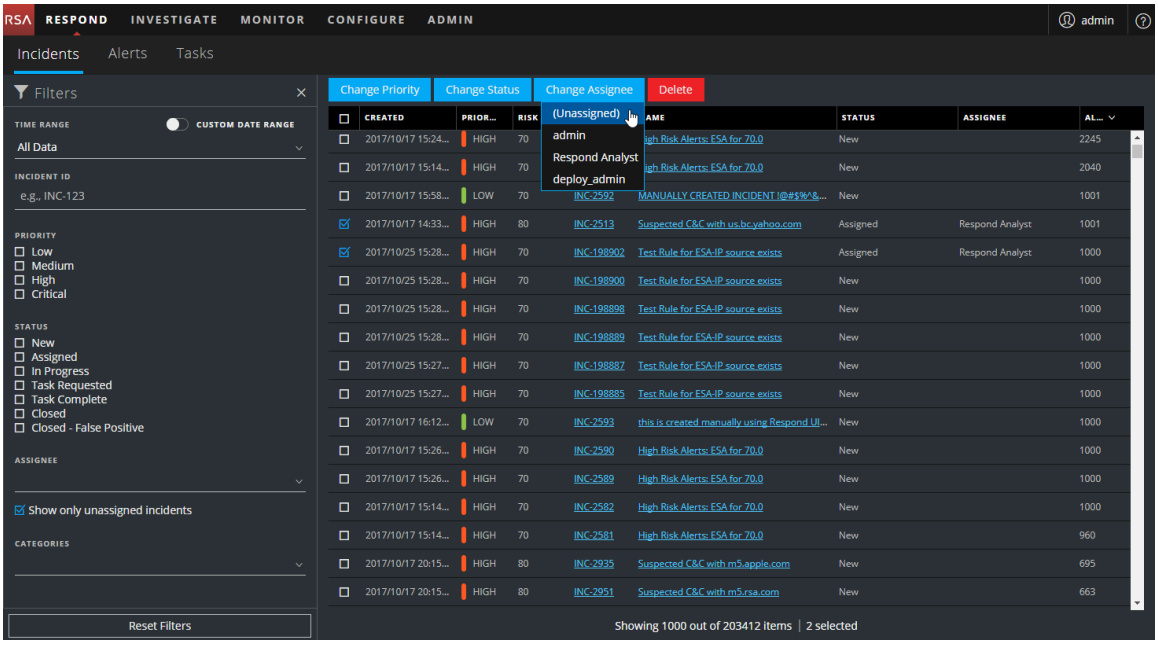


Verá una notificación de cambio correcto.

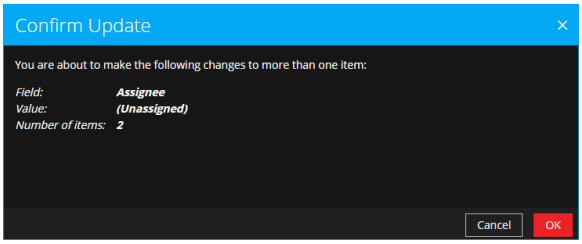


Cancelar asignación de un incidente

1. En la vista Lista de incidentes, seleccione uno o más incidentes cuya asignación desee cancelar.
2. Haga clic en **Cambiar usuario asignado** y seleccione **(Sin asignar)** en la lista desplegable.



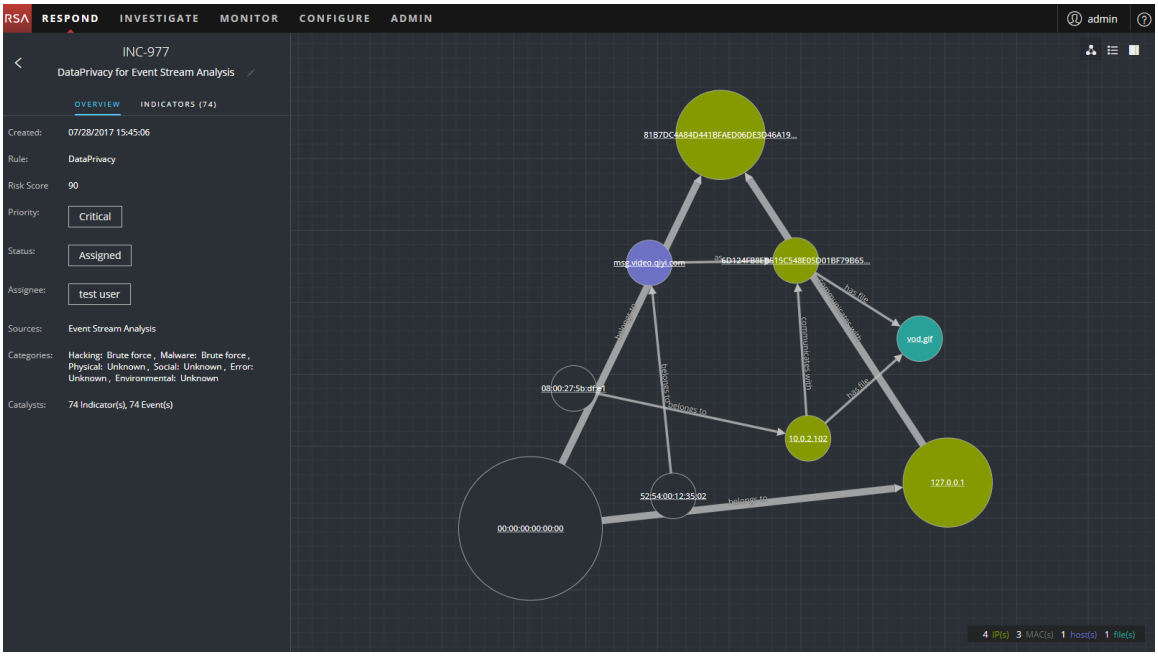
3. Si seleccionó más de un incidente, en el cuadro de diálogo Confirmar actualización, haga clic en **Aceptar**.



4. Verifique que el Estado aún esté correcto y realice cambios según sea necesario. Para cambiar el estado, seleccione uno o más incidentes, haga clic en **Cambiar estado** y seleccione un estado nuevo.
   Por ejemplo, si asignó un incidente a usted mismo por error, puede cancelar la asignación del incidente y, a continuación, cambiar el Estado de Asignado a Nuevo.

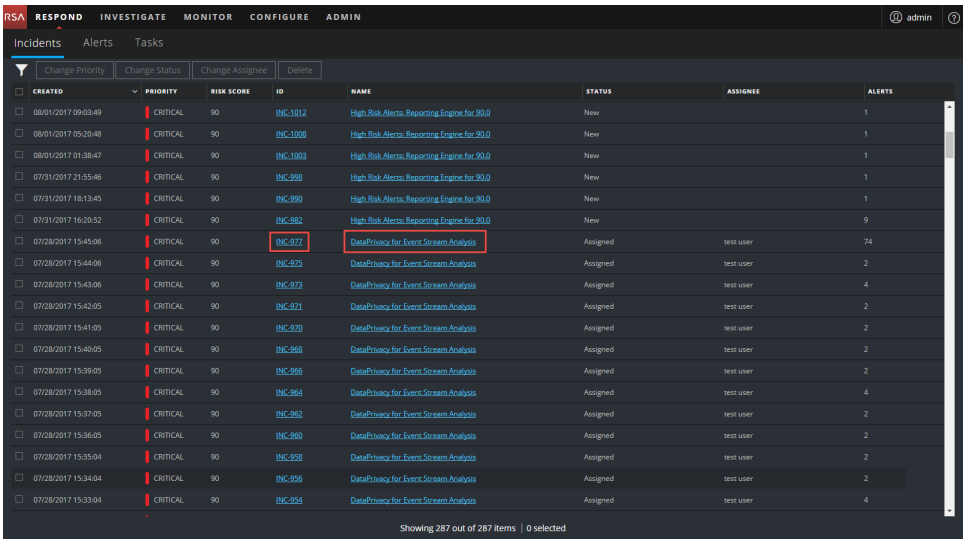
Ermitteln, welche Incidents eine Aktion erfordern

Una vez que obtiene la información general acerca del incidente en la vista Lista de incidentes, puede ir a la vista Detalles de incidente para obtener más información con el fin de determinar la acción requerida.

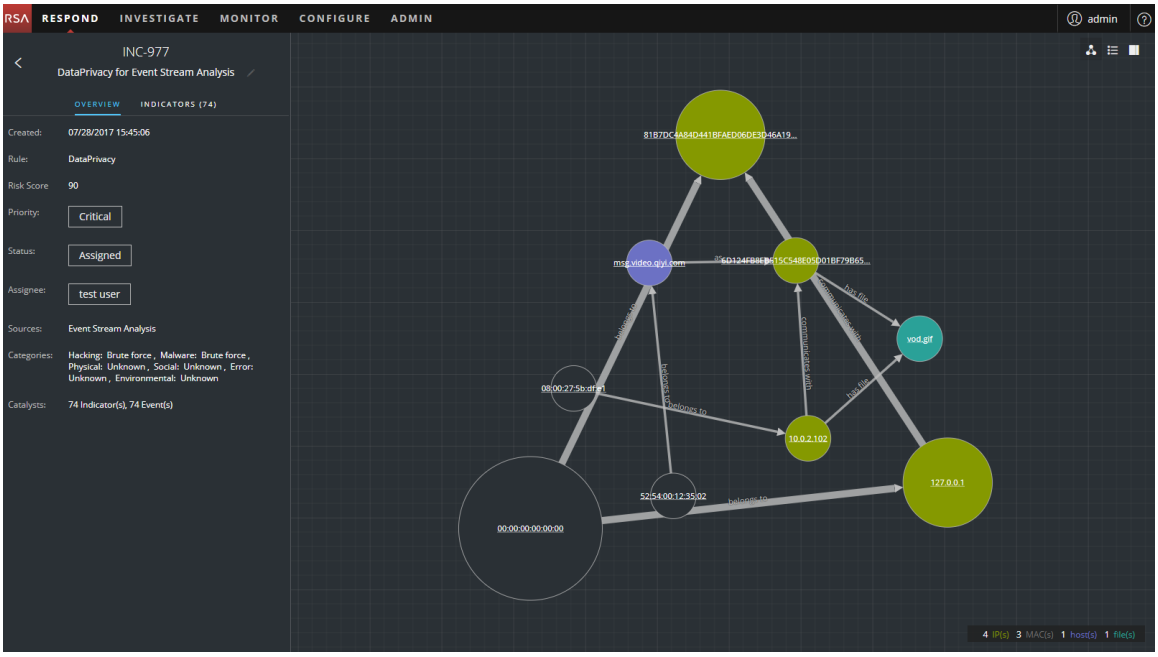


Ver detalles de incidentes

Para ver los detalles de un incidente, en la vista Lista de incidentes, elija un incidente que desee ver y, a continuación, haga clic en el vínculo de la columna ID o NOMBRE correspondiente a ese incidente.



La vista Detalles de incidente del incidente seleccionado aparece con el panel Descripción general y un gráfico de nodos.

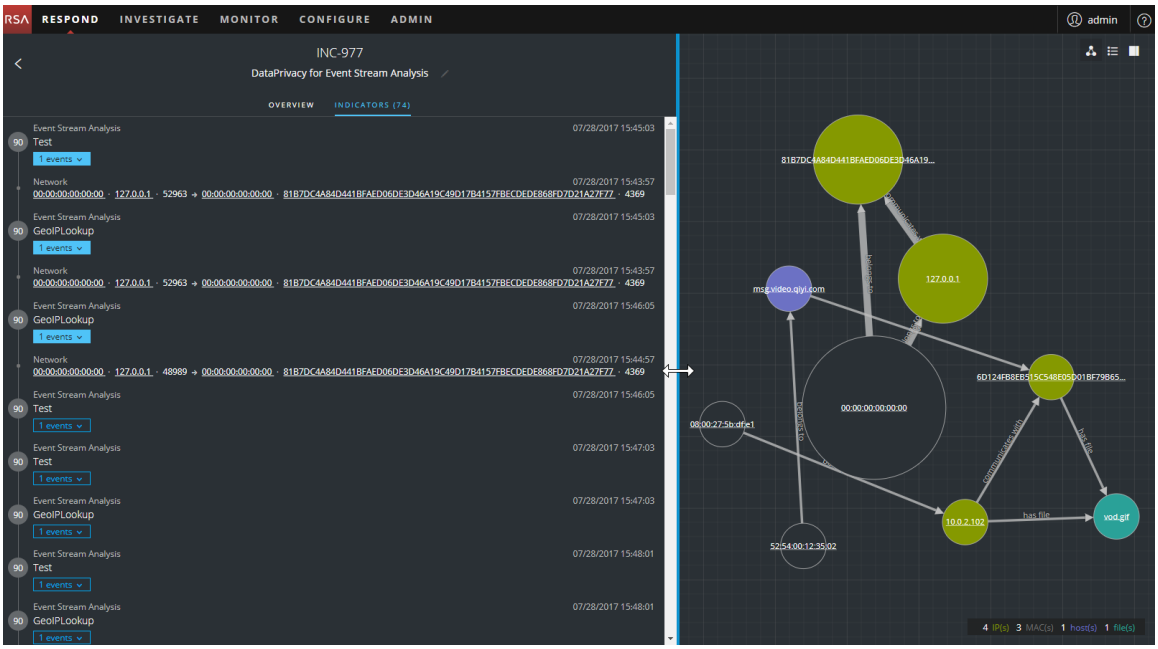


La vista Detalles de incidente incluye los siguientes paneles:

- **DESCRIPCIÓN GENERAL**: El panel de descripción general de incidentes contiene información de resumen general sobre el incidente; por ejemplo, el puntaje, la prioridad, las alertas y el estado. Tiene la opción de cambiar la prioridad, el estado y el usuario asignado del incidente.

- **INDICADORES**: El panel Indicadores contiene una lista cronológica de indicadores. Los ***indicadores*** son alertas, como una alerta de ESA o una alerta de NetWitness Endpoint. Esta lista permite conectar indicadores con datos relevantes. Por ejemplo, una dirección IP conectada a una alerta de ESA de comando y comunicación también podría haber activado una alerta de NetWitness Endpoint u otras actividades sospechosas.
- **Gráfico de nodos**: El gráfico de nodos es un gráfico interactivo que muestra la relación entre las entidades involucradas en el incidente. Una *entidad* es un elemento de metadatos especificado, como una dirección IP, una dirección MAC, un usuario, un host, un dominio, un nombre de archivo o un hash de archivo.
- **Eventos**: El panel Eventos, también conocido como la tabla Eventos, enumera los eventos asociados con el incidente. También muestra información acerca del origen y el destino del evento, junto con información adicional que depende del tipo de evento. Puede hacer clic en un evento de la lista para ver los datos detallados de ese evento.
- **REGISTRO**: En el panel Registro, puede acceder al registro del incidente seleccionado, lo cual le permite comunicarse y colaborar con otros analistas. Puede publicar notas en un registro, agregar etiquetas del Modelo de investigación (Reconocimiento, Distribución, Explotación, Instalación y Comando y control) y ver el historial de actividad en el incidente.
- **TAREAS**: El panel Tareas muestra todas las tareas que se han creado para el incidente. Desde aquí también puede crear tareas adicionales.
- **RELACIONADO**: El panel Indicadores relacionados permite buscar alertas que están relacionadas con este incidente en la base de datos de alertas de NetWitness Suite. También puede agregar al incidente las alertas relacionadas que encuentra.

Para ver más información en el panel lateral izquierdo, sin desplazarse, puede colocar el cursor sobre el borde derecho y arrastrar la línea para cambiar el tamaño del panel, como se muestra en la siguiente figura:

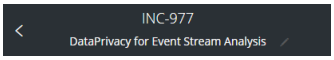


Ver información de resumen básica acerca del incidente

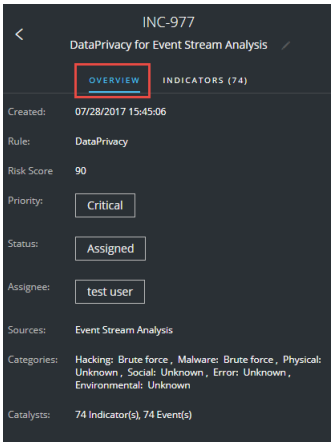
Puede ver información de resumen básica acerca de un incidente en el panel Descripción general.

Sobre el panel Descripción general, puede ver la siguiente información:

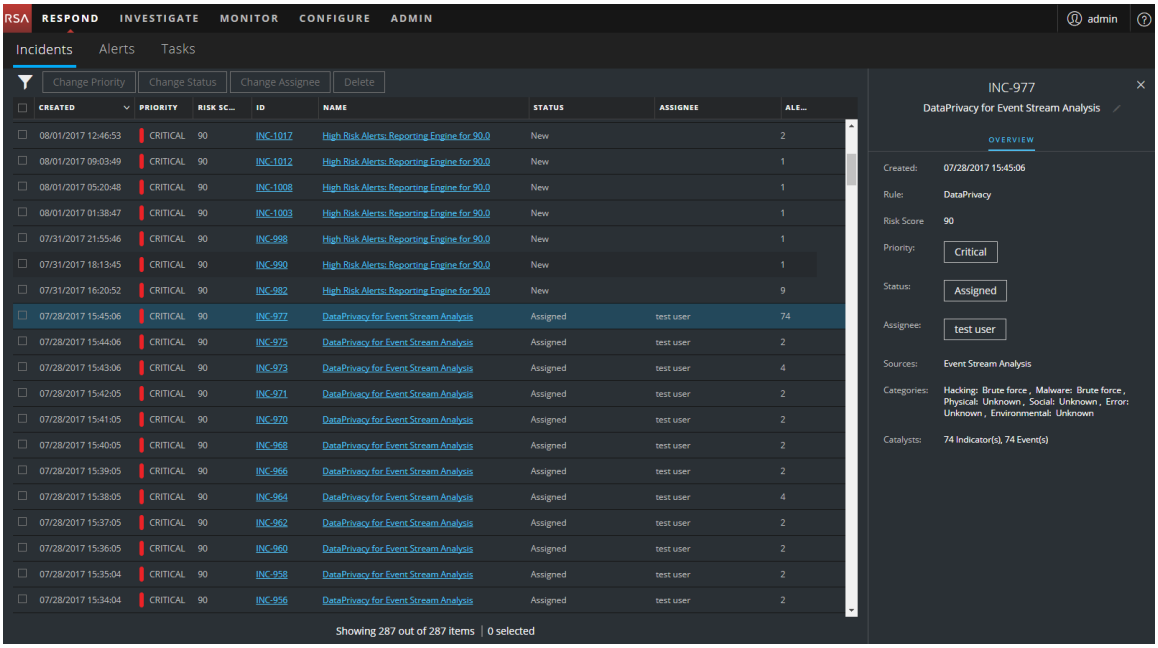
- **ID del incidente**: Se trata de un ID único creado automáticamente que se asigna al incidente.
- **Nombre**: El nombre del incidente proviene de la regla que se usa para activar el incidente.



Para ver el panel Descripción general desde la vista Detalles de incidente, seleccione **DESCRIPCIÓN GENERAL** en el panel izquierdo.



Para ver el panel Descripción general desde la vista Lista de incidentes, haga clic en un incidente de la lista. El panel Descripción general aparece a la derecha.



El panel Descripción general contiene información de resumen básica acerca del incidente seleccionado:

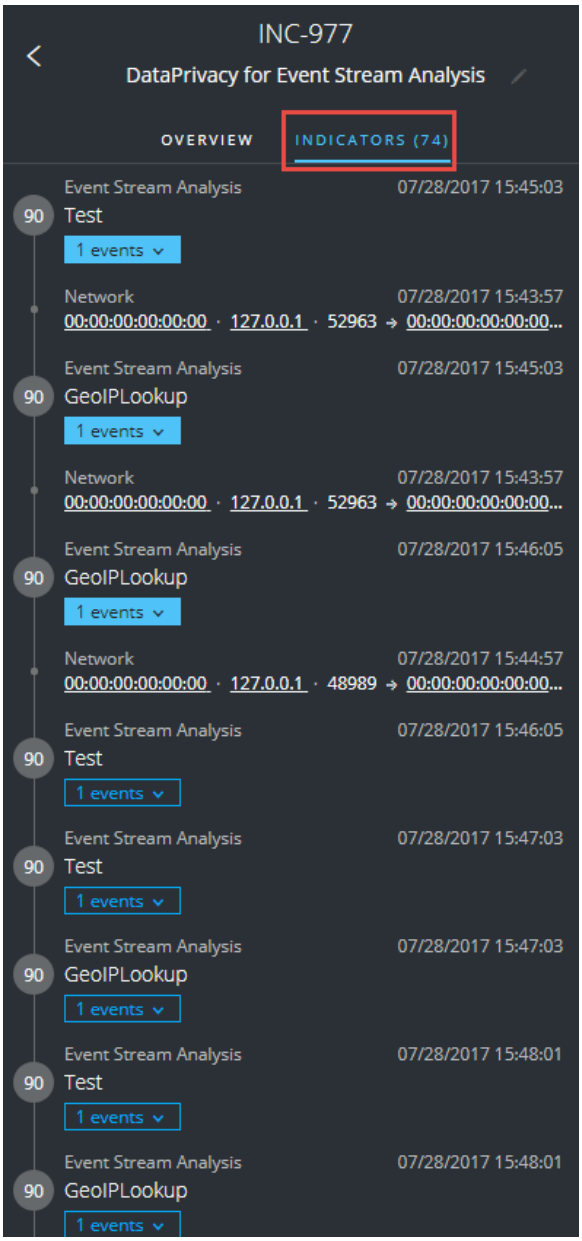
- **Creado**: Muestra la fecha y la hora de creación del incidente.
- **Regla/Por**: Muestra el nombre de la regla o de la persona que creó el incidente.
- **Puntaje de riesgo**: Indica el riesgo del incidente que se calcula por medio de un algoritmo y que está entre 0 y 100. 100 es el puntaje de riesgo más alto.
- **Prioridad**: Muestra la prioridad del incidente. La prioridad puede ser Crítica, Alta, Media o Baja.
- **Estado**: Muestra el estado del incidente. El estado puede ser Nuevo, Asignado, En curso, Tarea solicitada, Tarea completa, Cerrado y Cerrado: falso positivo. Después de que se crea una tarea, el estado cambia a Tarea solicitada.
- **Usuario asignado**: Muestra el miembro del equipo que está asignado al incidente.
- **Orígenes**: Indica los orígenes de datos que se utilizan para ubicar la actividad sospechosa.
- **Categorías**: Muestra las categorías de los eventos del incidente.
- **Catalizadores**: Muestra el conteo de indicadores que dieron lugar al incidente.

Ver los indicadores y los enriquecimientos

Nota: Los *indicadores* son alertas, como una alerta de ESA o una alerta de NetWitness Endpoint.

Puede encontrar indicadores, eventos y enriquecimientos en el panel Indicadores. El panel Indicadores es una lista cronológica de indicadores que permite buscar enriquecimientos y eventos relacionados con el indicador desencadenante. Por ejemplo, un indicador podría ser una alerta de Command and Control, una alerta de NetWitness Endpoint, una alerta de Suspicious Domain (C2) o una alerta de una regla de Event Stream Analysis (ESA). El panel Indicadores permite agregar y ordenar estos indicadores (alertas) de distintos sistemas, de modo que pueda ver cómo se relacionan y también desarrollar un cronograma de un ataque determinado.

Para ver el panel Indicadores, en el panel izquierdo de la vista Detalles de incidente, seleccione **INDICADORES**.



Los *indicadores* son alertas, como una alerta de ESA o una alerta de NetWitness Endpoint. Esta lista permite conectar indicadores con datos relevantes. Por ejemplo, los indicadores pueden mostrar los datos que encuentran las reglas. En el panel Indicadores, el puntaje de riesgo de un indicador se muestra dentro de un círculo de color sólido.

La información del origen de datos se muestra debajo de los nombres de los indicadores. También puede ver la fecha y la hora de creación del indicador y la cantidad de eventos que incluye. Cuando hay datos disponibles, puede ver la cantidad de enriquecimientos. Puede hacer clic en los botones de eventos y enriquecimientos para ver los detalles.

Ver y estudiar los eventos

Puede ver y estudiar los eventos asociados con el incidente desde el panel Eventos. Muestra información acerca de los eventos, como la hora del evento, la dirección IP de origen, la dirección IP de destino, la dirección IP del detector, el usuario de origen, el usuario de destino e información de los archivos acerca de los eventos. La cantidad de información que se muestra depende del tipo de evento.

Hay dos tipos de eventos:

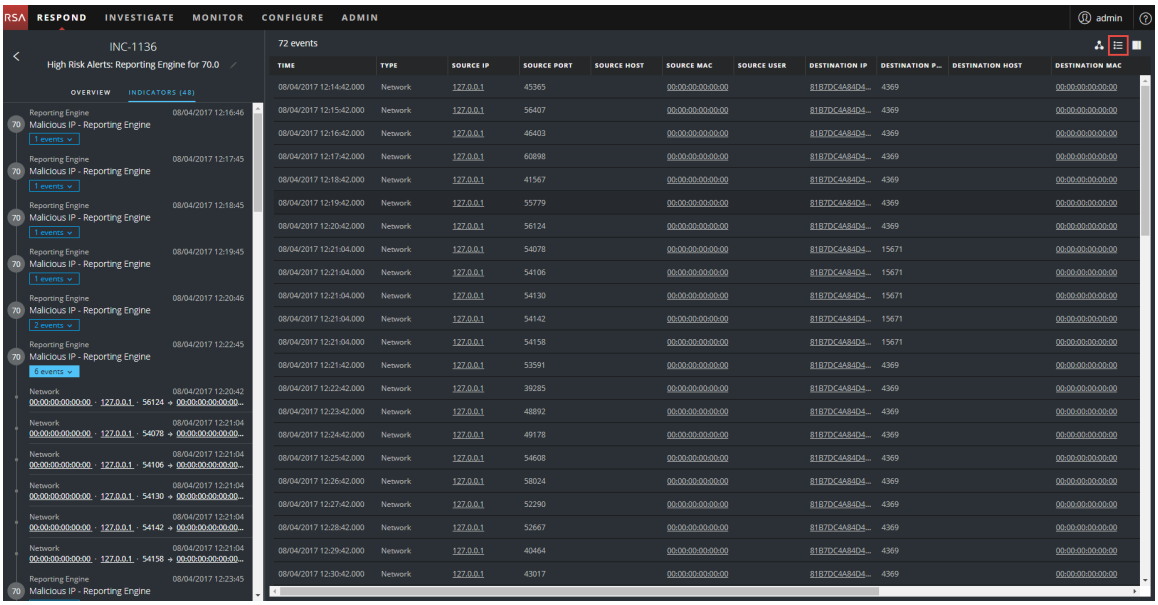
- Una transacción entre dos máquinas (un origen y un destino)
- Una anomalía detectada en una máquina (un detector)

Algunos eventos solo tendrán un detector. Por ejemplo, NetWitness Endpoint busca malware en una máquina. Otros eventos tendrán un origen y un destino. Por ejemplo, los datos de paquetes muestran la comunicación entre una máquina y un dominio de comando y control (C2).

Puede desglosar aún más a un evento para obtener datos detallados acerca de este.

Para ver y estudiar los eventos:

1. Para ver el panel Eventos, en la barra de herramientas de la vista Detalles de incidente, haga clic en .



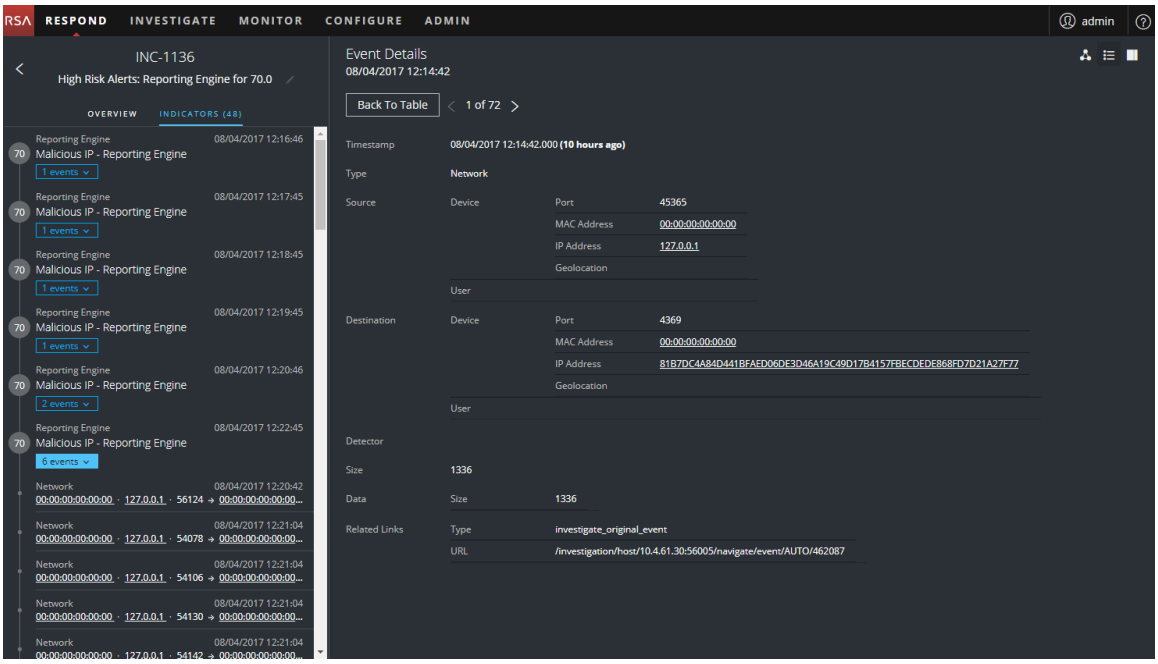
   El panel Eventos presenta una lista de información acerca de cada evento, como se muestra en la siguiente tabla.

Columna	Descripción
TIEMPO	Muestra la hora en que se produjo el evento.
TIPO	Muestra el tipo de alerta, como Registro y Red.
DIRECCIÓN IP DE ORIGEN	Muestra la dirección IP de origen si hubo una transacción entre dos máquinas.
PUERTO DE ORIGEN	Muestra el puerto de origen de la transacción. Los puertos de origen y destino pueden estar en la misma dirección IP.
HOST DE ORIGEN	Muestra el host de origen donde se produjo el evento.
MAC DE ORIGEN	Muestra la dirección MAC de la máquina de origen.
USUARIO DE ORIGEN	Muestra el usuario de la máquina de origen.
DIRECCIÓN IP DE DESTINO	Muestra la dirección IP de destino si hubo una transacción entre dos máquinas.
PUERTO DE DESTINO	Muestra el puerto de destino de la transacción. Los puertos de origen y destino pueden estar en la misma dirección IP.
HOST DE DESTINO	Muestra el host de destino donde se produjo el evento.
MAC DE DESTINO	Muestra la dirección MAC de la máquina de destino.
USUARIO DE DESTINO	Muestra el usuario de la máquina de destino.
IP DE DETECTOR	Muestra la dirección IP de la máquina en la que se detectó una anomalía.
NOMBRE DE ARCHIVO	Muestra el nombre del archivo, si hubo uno implicado en el evento.

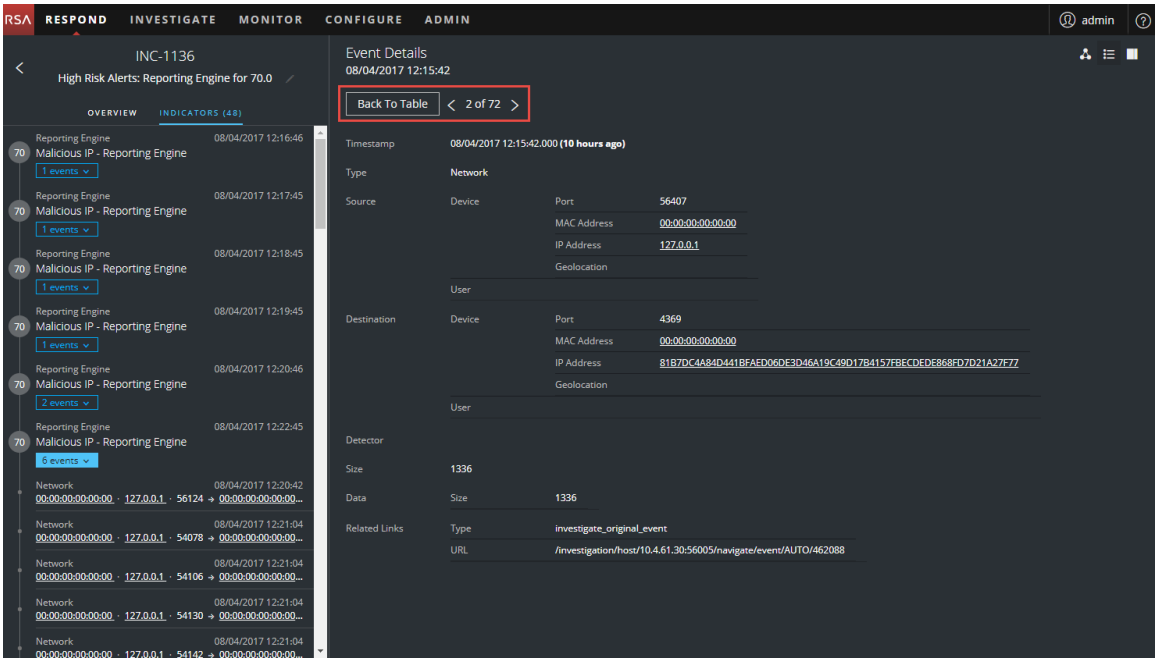
Columna	Descripción
HASH DE ARCHIVO	Muestra un hash del contenido del archivo.

Si solo hay un evento en la lista, verá los detalles de ese evento en lugar de una lista.

2. Haga clic en un evento de la Lista de eventos para ver sus detalles.
   En este ejemplo se muestran los detalles del primer evento de la lista.



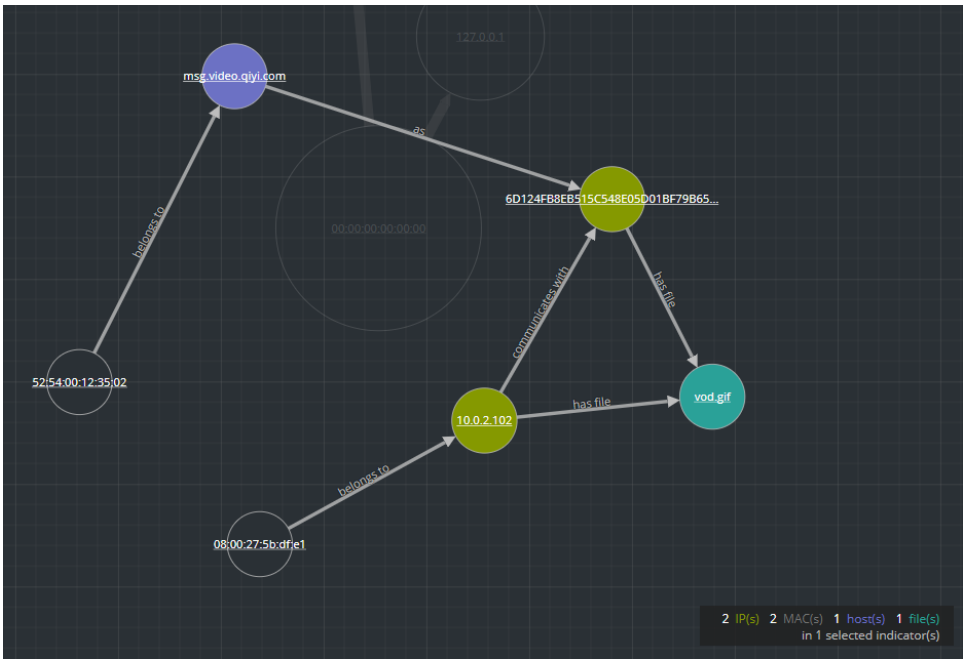
3. Use la navegación de Detalles de eventos para ver detalles de eventos adicionales.
   En este ejemplo se muestra el segundo evento de la lista.



Ver y estudiar las entidades involucradas en los eventos

Una *entidad* es una dirección IP, una dirección MAC, un usuario, un host, un dominio, un nombre de archivo o un hash de archivo. El gráfico de nodos es un gráfico interactivo que se puede reposicionar para obtener una mejor comprensión de la manera en que se relacionan las entidades involucradas en los eventos. Los gráficos de nodos tienen distintos aspectos según el tipo de evento, la cantidad de máquinas involucradas, si las máquinas están asociadas a usuarios y si hay archivos asociados al evento.

En la siguiente figura se muestra un ejemplo de gráfico de nodos con seis nodos.



Si observa el gráfico de nodos con detención, puede ver círculos que representan nodos. Un gráfico de nodos puede contener uno o más de los siguientes tipos de nodos:

- **Dirección IP**. Si el evento es una anomalía detectada, puede ver una dirección IP de detector. Si el evento es una transacción, puede ver una dirección IP de destino y una de origen.
- **Dirección MAC**. Puede ver una dirección MAC para cada tipo de dirección IP.
- **Usuario**. Si la máquina está asociada a un usuario, puede ver un nodo de usuario.
- **Host**
- **Dominio**
- **Nombre de archivo**. Si el evento implica archivos, puede ver un nombre de archivo.
- **Hash de archivo**. Si el evento implica archivos, puede ver un hash de archivo.

La leyenda en la parte inferior del gráfico de nodos muestra la cantidad de nodos de cada tipo y la codificación en colores de los nodos.

Puede hacer clic en cualquier nodo y arrastrarlo para cambiar su ubicación.

Las flechas entre los nodos ofrecen información adicional acerca de las relaciones entre las entidades:

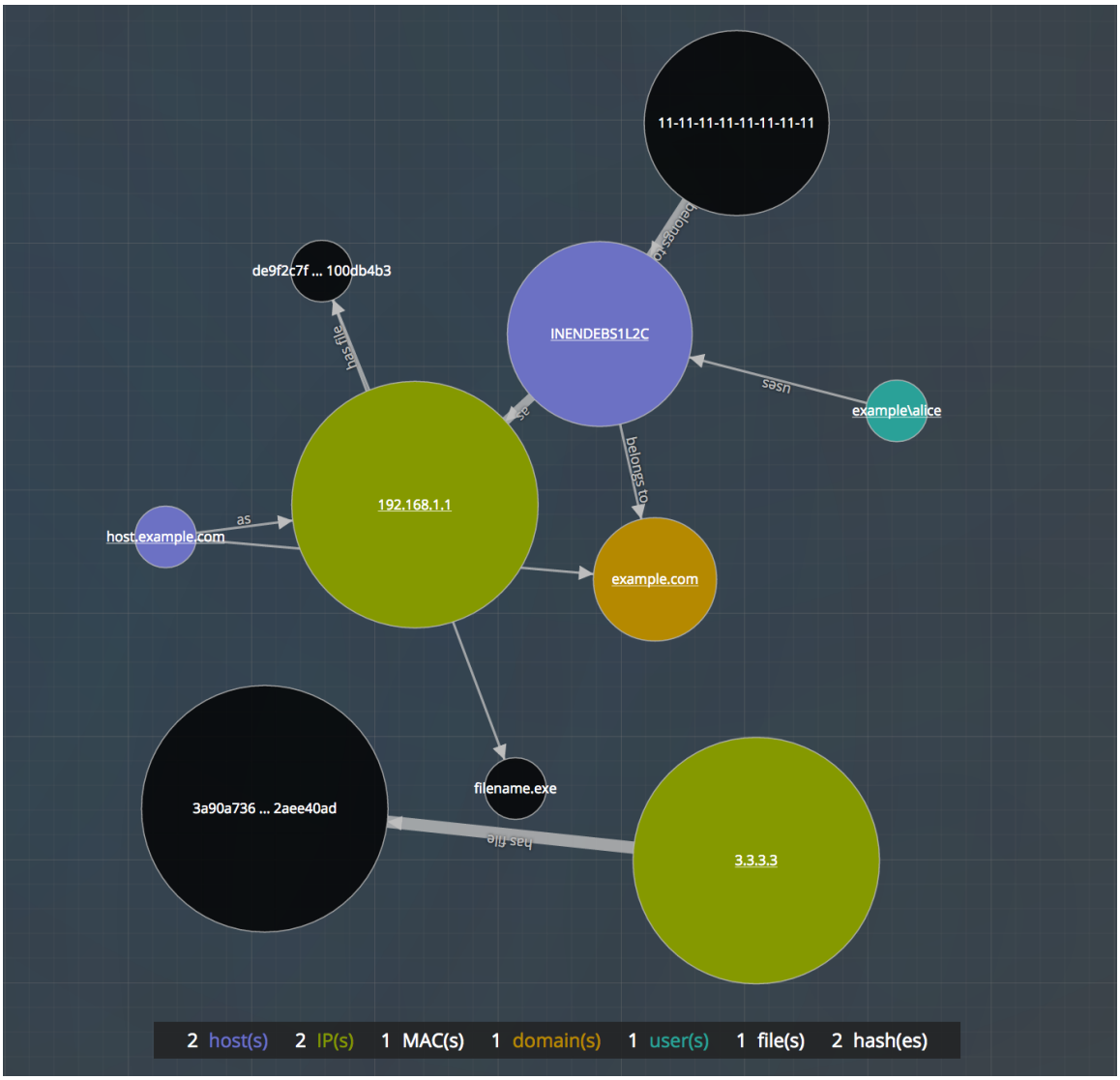
- **Se comunica con**: Una flecha entre un nodo de máquina de origen (dirección IP o dirección MAC) y un nodo de máquina de destino etiquetada con “Se comunica con” muestra la

dirección de la comunicación.

- **Como**: Una flecha entre los nodos etiquetada con “Como” proporciona información adicional sobre la dirección IP que señala la flecha. En el ejemplo anterior, hay una flecha desde el círculo del nodo de host que señala a un nodo de dirección IP con hash, la cual está etiquetada con “Como”. Esto indica que el nombre en el círculo del nodo de host es el nombre de host de esa dirección IP y no una entidad distinta.
- **Tiene archivo**: Una flecha entre un nodo de máquina (dirección IP, dirección MAC o host) y un nodo de hash de archivo etiquetada con “Tiene” indica que la dirección IP tiene ese archivo.
- **Usos**: Una flecha entre un nodo de usuario y un nodo de máquina (dirección IP, dirección MAC o host) etiquetada con “Usos” muestra la máquina que utilizó el usuario durante el evento.
- **Se denomina**: Una flecha desde un nodo de hash de archivo a un nodo de nombre de archivo etiquetada con “Se denomina” indica que el hash de archivo corresponde a un archivo con ese nombre.
- **Pertenece a**: Una flecha entre dos nodos etiquetada con “Pertenece a” indica que se relaciona con el mismo nodo. Por ejemplo, una flecha entre una dirección MAC y un host etiquetada “Pertenece a” indica que es la dirección MAC del host.

Las flechas con mayores tamaños de línea indican que hay más comunicación entre los nodos. Los nodos (círculos) más grandes indican mayor actividad en comparación con los nodos más pequeños. Los nodos de mayor tamaño son las entidades más comunes que se mencionan en los eventos.

El siguiente ejemplo de gráfico de nodos tiene 10 nodos.

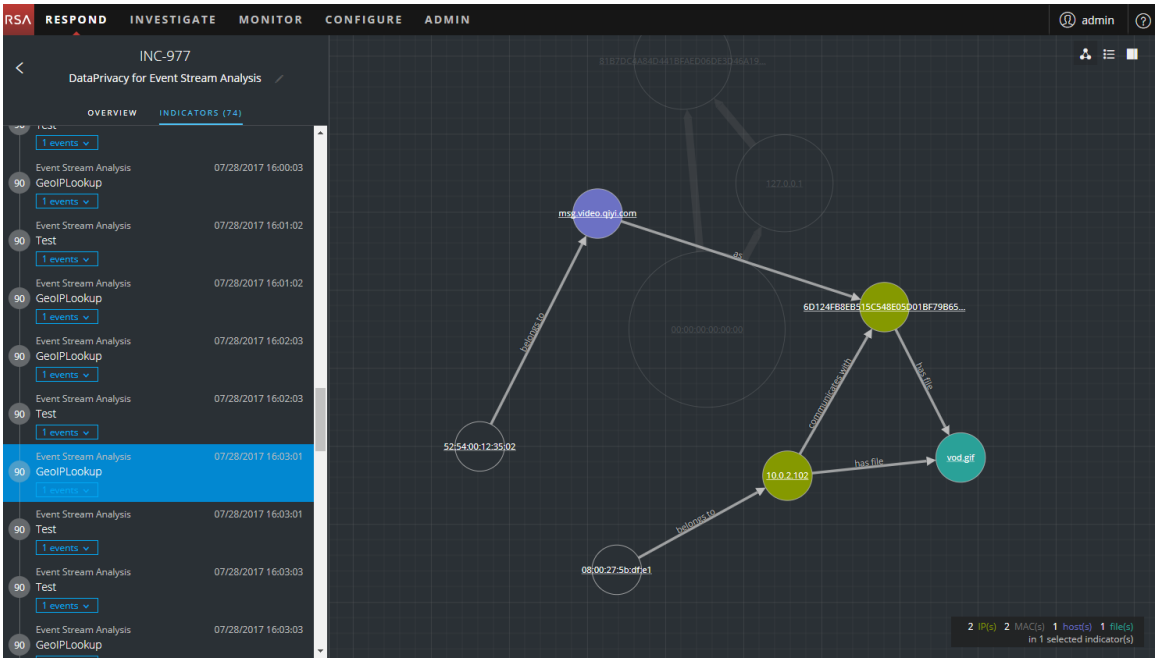


En este ejemplo, observe que hay dos nodos de IP que tienen mucha actividad. Ambos tienen archivos, pero no se comunican entre sí. La dirección IP en la parte superior (192.168.1.1) representa una máquina con dos nombres de host (host.example.com e INENDEBS1L2C) en el dominio example.com. La dirección MAC de la máquina es 11-11-11-11-11-11-11-11-11-11 y la utiliza Alice.

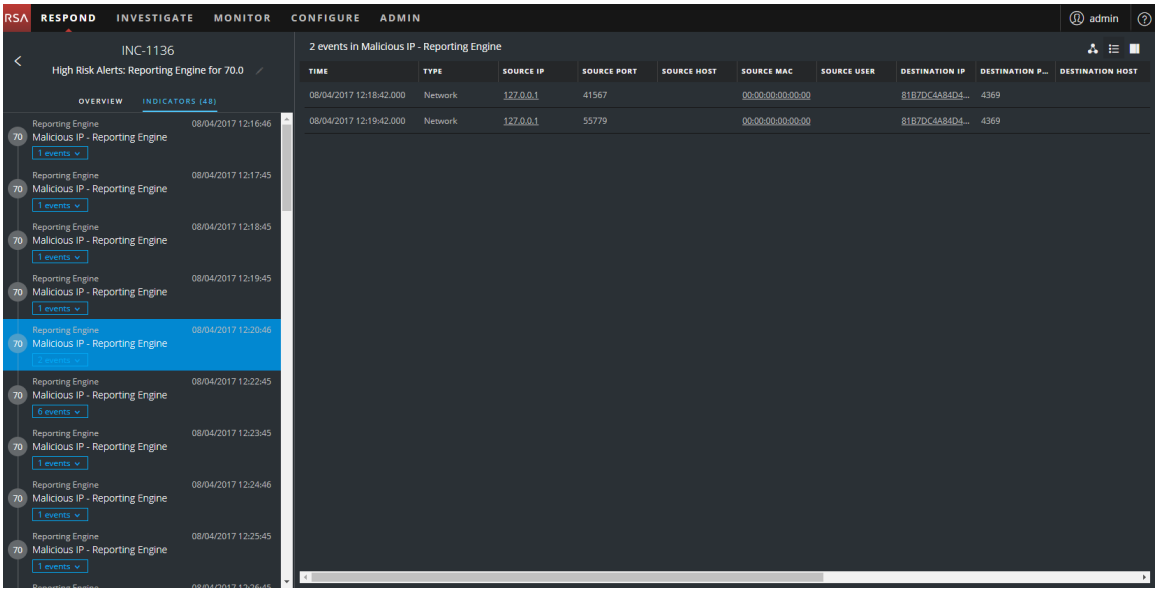
Filtrar los datos en la vista Detalles de incidente

Puede hacer clic en los indicadores del panel Indicadores para filtrar lo que puede ver en el gráfico de nodos y en la Lista de eventos.

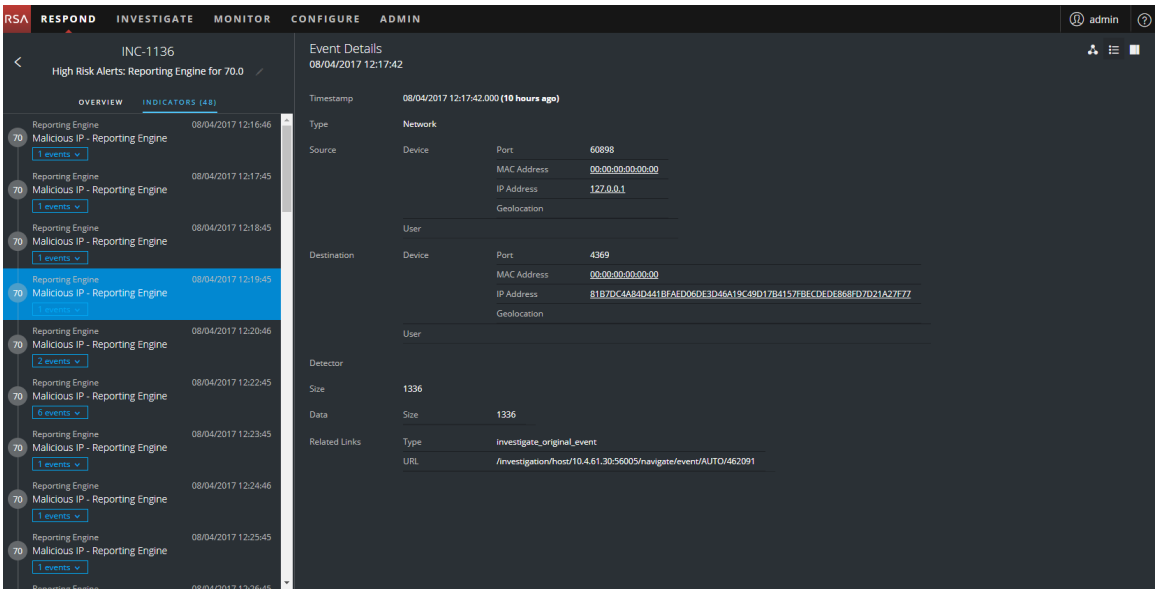
Si selecciona un indicador para filtrar el gráfico de nodos, los datos que no son parte de su selección se atenúan, pero continúan en la vista, como se muestra en la siguiente figura.



Si selecciona un indicador para filtrar la lista de eventos, solo se muestran en la lista los eventos de ese indicador. En la siguiente figura se muestra un indicador seleccionado que contiene dos eventos. La Lista de eventos filtrada muestra estos dos eventos.



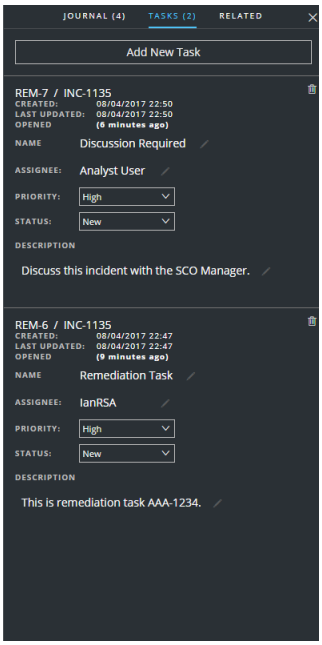
Si selecciona un indicador para filtrar la lista de eventos y hay solo un evento para ese indicador, puede ver los detalles de ese evento, como se muestra en la siguiente figura.


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
INC-1136
High Risk Alerts: Reporting Engine for 70.0
OVERVIEW
INDICATORS (48)
Reporting Engine
Malicious IP - Reporting Engine
08/04/2017 12:16:46
1 events
08/04/2017 12:17:45
08/04/2017 12:18:45
08/04/2017 12:19:45
08/04/2017 12:20:46
2 events
08/04/2017 12:22:45
6 events
08/04/2017 12:23:45
08/04/2017 12:24:46
08/04/2017 12:25:45
Event Details
08/04/2017 12:17:42
Timestamp
08/04/2017 12:17:42.000 (10 hours ago)
Type
Network
Source
Device
Port
60898
MAC Address
00:00:00:00:00:00
IP Address
127.0.0.1
Geolocation
User
Destination
Device
Port
4369
MAC Address
00:00:00:00:00:00
IP Address
81B7DC4A84D441BFAED06DE3D46A19C49D17B4157FBECDEDE868FD7D21A27F77
Geolocation
User
Detector
Size
1336
Data
Size
1336
Related Links
Type
investigate_original_event
URL
/investigation/host/10.4.61.30:56005/navigate/event/AUTO/462091

Ver las tareas asociadas a un incidente

Los encargados de responder ante amenazas y otros analistas pueden crear tareas para un incidente y rastrear esas tareas hasta su finalización. Esto puede ser muy útil, por ejemplo, cuando se requieren acciones relativas a los incidentes de equipos fuera de sus operaciones de seguridad. Puede ver las tareas asociadas a un incidente en la vista Detalles de incidente.

1. Vaya a **RESPONDER > Incidentes** y busque el incidente que desea ver en la Lista de incidentes.
2. Haga clic en el vínculo del campo **ID** o **NOMBRE** del incidente para ir a la vista Detalles de incidente.
3. En la barra de herramientas de la vista Detalles de incidente, haga clic en ▣.
   Se abre el panel Registro.
4. Haga clic en la pestaña **TAREAS**.
   El panel Tareas muestra todas las tareas que se han creado para el incidente.

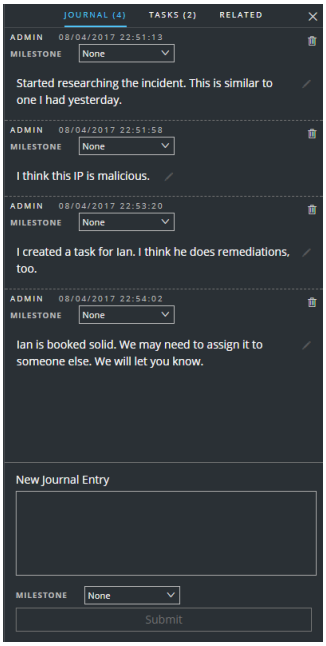


Para obtener más información acerca de las tareas, consulte Vista Lista de tareas, Ver todas las tareas de incidentes y Crear una tarea.

Ver notas sobre los incidentes

El registro de incidentes permite ver el historial de actividad del incidente. Puede ver las entradas del registro de otros analistas y también comunicarse y colaborar con ellos.

1. Vaya a **RESPONDER > Incidentes** y busque el incidente que desea ver en la Lista de incidentes.
2. Haga clic en el vínculo del campo **ID** o **NOMBRE** del incidente para ir a la vista Detalles de incidente.
3. En la barra de herramientas de la vista Detalles de incidente, haga clic en .
   El panel Registro muestra todas las entradas del registro para el incidente.



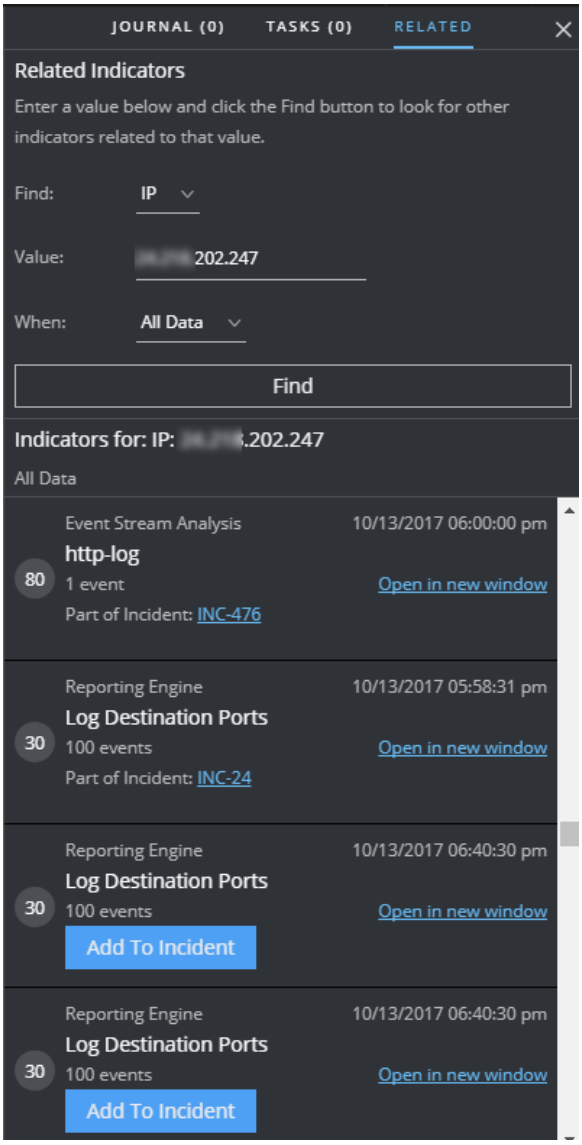
Buscar indicadores relacionados

Los *indicadores relacionados* son alertas que no formaban parte originalmente del incidente seleccionado, pero que se relacionan de alguna manera con este. La relación puede o no ser obvia. Por ejemplo, los indicadores relacionados pueden implicar una o más entidades del incidente, pero también se pueden relacionar debido a inteligencia externa a NetWitness Suite.

En el panel Relacionado de la vista Detalles de incidente, puede buscar una entidad (por ejemplo, IP, MAC, host, dominio, usuario, nombre de archivo o hash) en otras alertas fuera del incidente actual.

1. Vaya a **RESPONDER > Incidentes** y busque el incidente que desea ver en la Lista de incidentes.
2. Haga clic en el vínculo del campo **ID** o **NOMBRE** del incidente para ir a la vista Detalles de incidente.
3. En la barra de herramientas de la vista Detalles de incidente, haga clic en .
   El panel Registro se abre en el lado derecho.

4. Haga clic en la pestaña **Relacionado**.

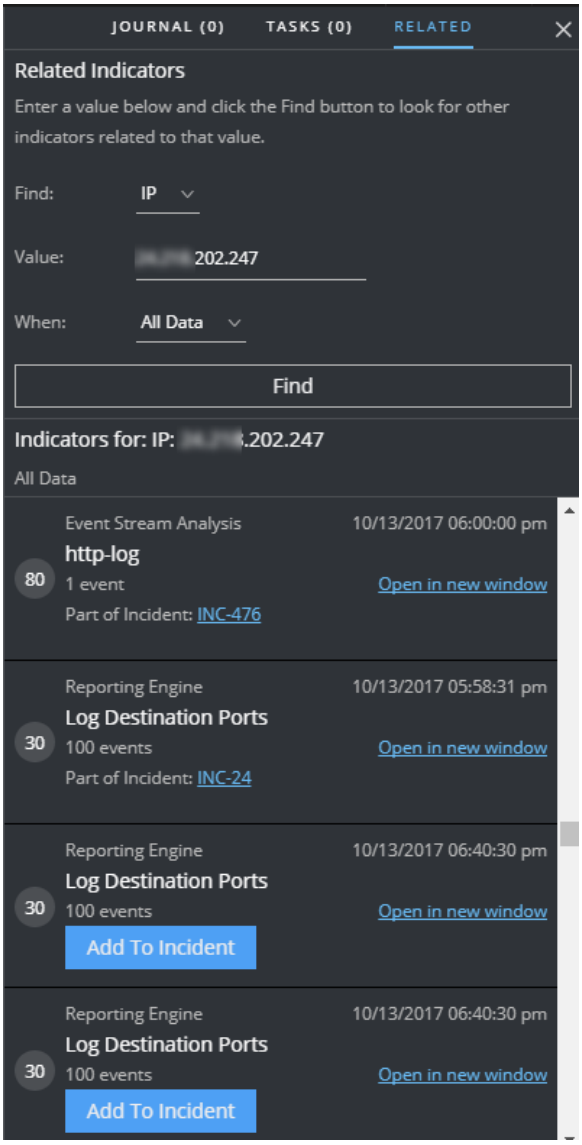


5. Haga clic en **Buscar**.
   Aparece una lista de indicadores relacionados (alertas) debajo del botón **Buscar** en la sección **Indicadores para**. Si una alerta no forma parte de otro incidente, puede hacer clic en el botón **Agregar a incidente** para agregar el indicador relacionado (alerta) al incidente actual. Consulte Agregar indicadores relacionados al incidente a continuación.

Agregar indicadores relacionados al incidente

Puede agregar indicadores relacionados (alertas) al incidente actual desde el panel Indicadores relacionados. Un indicador que ya forma parte de un incidente no puede formar parte de otro. En los resultados de búsqueda, si una alerta aún no forma parte de un incidente, aparece con un botón **Agregar a incidente**.

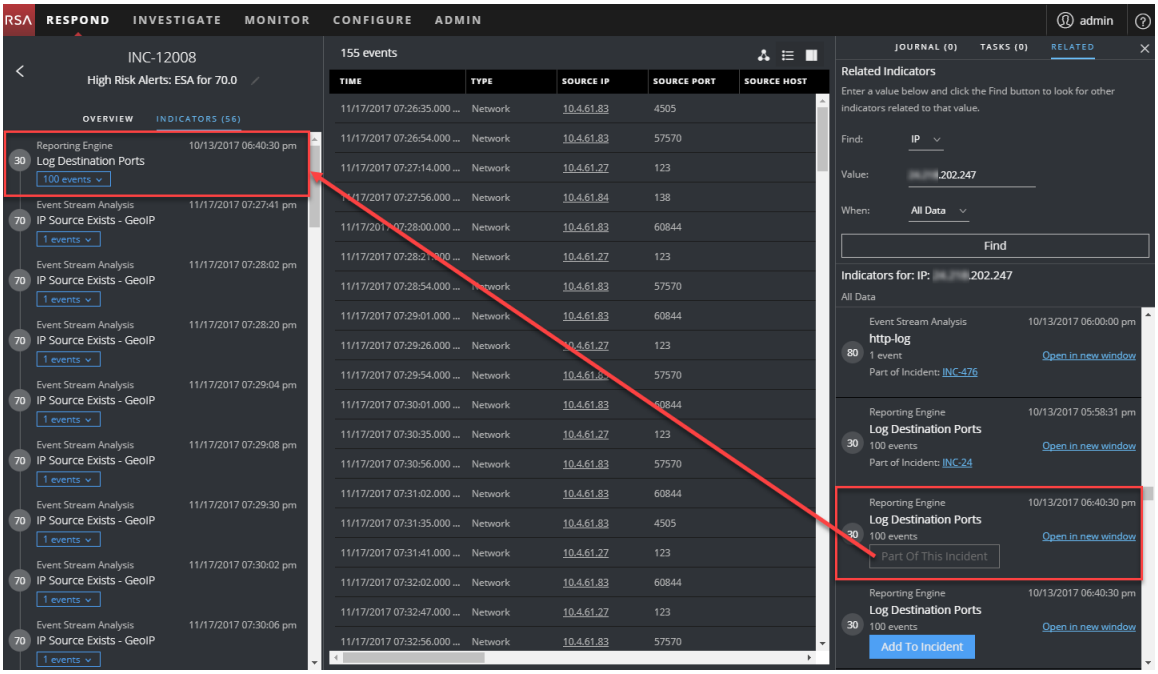
1. En el panel **RELACIONADO** (Indicadores relacionados), realice una búsqueda para encontrar indicadores relacionados. Consulte Buscar indicadores relacionados anteriormente.



2. Revise las alertas en los resultados de búsqueda. La sección **Indicadores para** (debajo del botón Buscar) muestra los indicadores relacionados (alertas).

3. Para examinar los detalles de una alerta antes de agregarla como un indicador relacionado con el incidente, puede hacer clic en el vínculo **Abrir en una nueva ventana** para ver los detalles de la alerta para ese indicador.

4. Para cada alerta que desee agregar al incidente actual como un indicador relacionado, haga clic en el botón **Agregar a incidente**.
   El indicador relacionado seleccionado se agrega al panel Indicadores en el lado izquierdo. Ahora, el botón del panel Indicadores relacionados del lado derecho muestra **Parte de este incidente**.



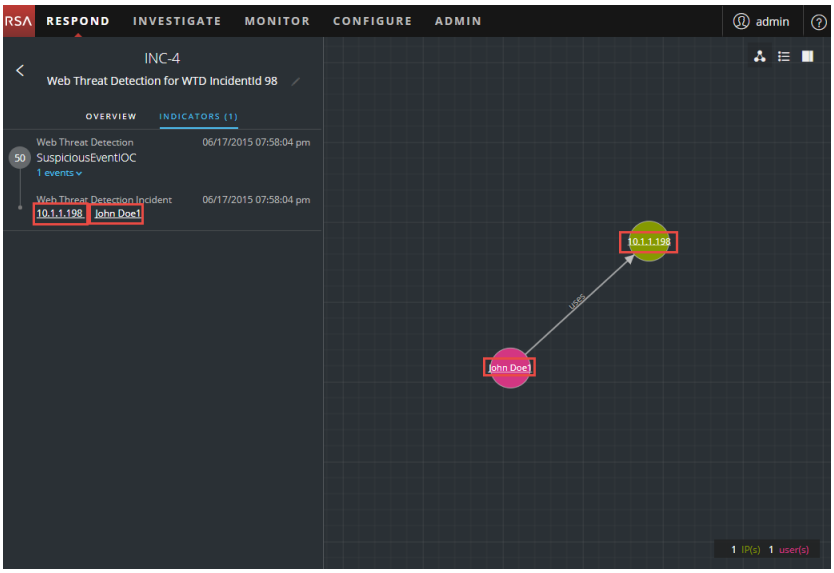
Investigar el incidente

Para investigar más a fondo un incidente en la vista Detalles de incidente, puede encontrar vínculos que lo dirigen a información contextual adicional sobre el incidente cuando está disponible. Este contexto adicional puede ayudarlo a comprender el contexto técnico adicional y el contexto de negocios acerca de una entidad específica en el incidente. También puede proporcionar información adicional que tal vez desee investigar para asegurarse de comprender el alcance completo del incidente.

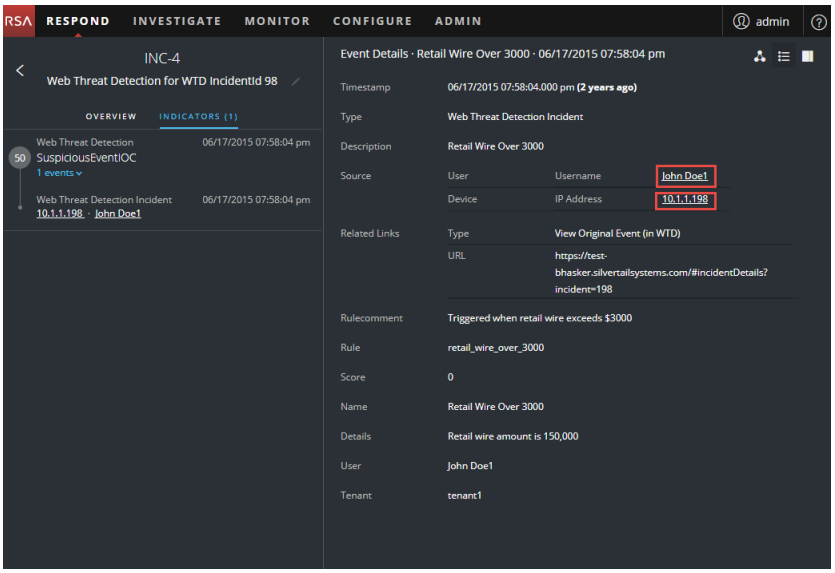
Ver información contextual

En los paneles Indicadores, Lista de eventos, Detalles de eventos o en el gráfico de nodos, puede ver entidades subrayadas. Si una entidad está subrayada, NetWitness Suite está completando información acerca de ese tipo de entidad en Context Hub. Puede estar disponible información adicional sobre esa entidad en Context Hub.

En la siguiente figura se muestran entidades subrayadas en el panel Indicadores y en el gráfico de nodos.



En la siguiente figura se muestran entidades subrayadas en el panel Detalles de eventos.



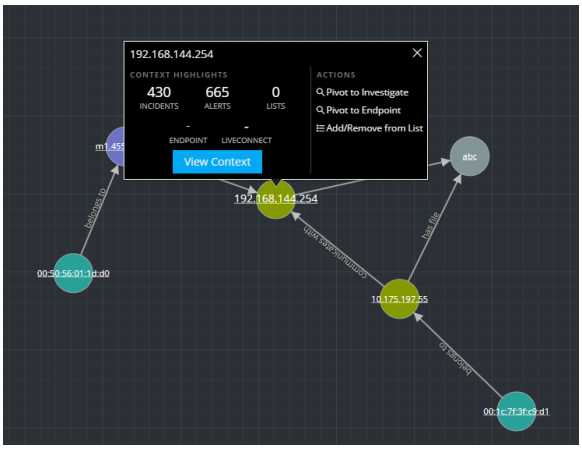
Context Hub está preconfigurado con campos de metadatos mapeados a las entidades. NetWitness Respond e Investigate usan estos mapeos predeterminados para la búsqueda de contexto. Para obtener información acerca de cómo agregar claves de metadatos, consulte "Configurar ajustes para un origen de datos" en la *Guía de configuración de Context Hub*.

Precaución: Para que la búsqueda de contexto funcione de manera correcta en las vistas Respond e Investigate, al mapear claves de metadatos en la pestaña **ADMINISTRAR > SISTEMA > Investigaciones > Búsqueda de contexto**, RSA recomienda agregar únicamente claves de metadatos a los mapeos de claves de metadatos, no campos de MongoDB. Por ejemplo, ip.address es una clave de metadatos e ip_address no lo es (es un campo de MongoDB).

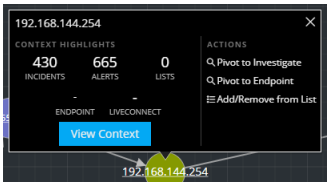
Para ver información contextual:

1. En los paneles Indicadores, Lista de eventos, Detalles de eventos o en el gráfico de nodos, coloque el cursor sobre una entidad subrayada.

   Aparece un mensaje de globo de contexto con un resumen rápido del tipo de datos de contexto que está disponible para la entidad seleccionada.



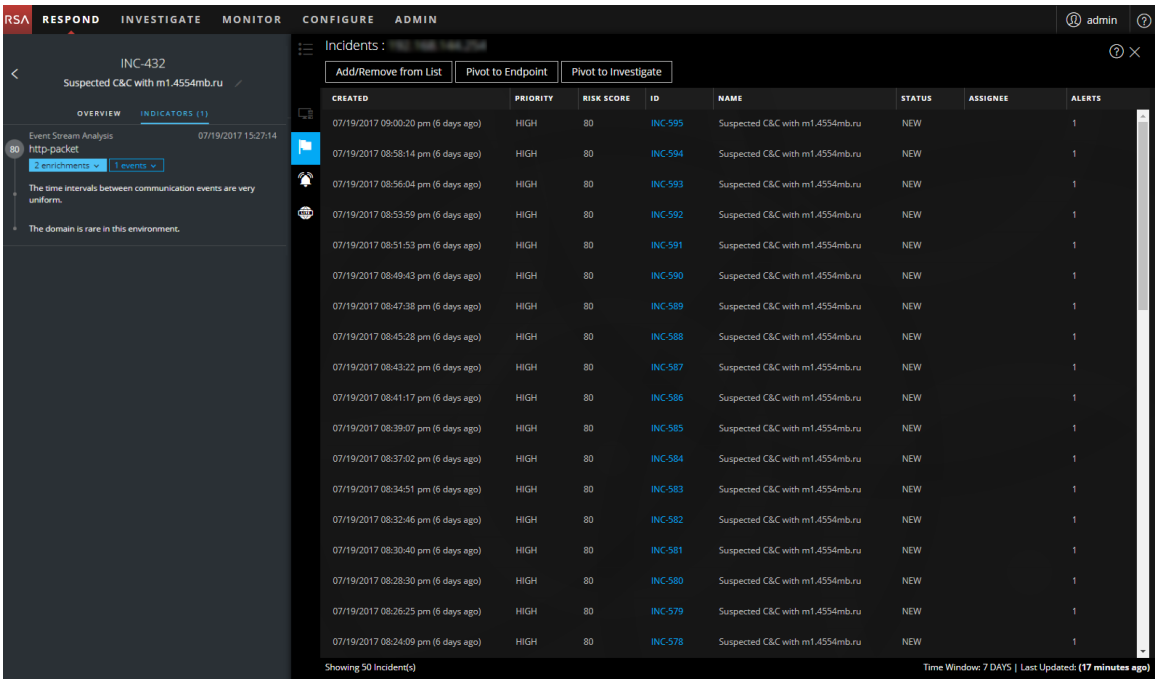
El mensaje de globo de contexto tiene dos secciones: Puntos destacados de contexto y Acciones.



La información de la sección **Puntos destacados de contexto** lo ayuda a determinar las acciones que desea realizar. Puede mostrar datos relacionados de incidentes, alertas, listas, Endpoint y Live Connect. Según los datos, tal vez pueda hacer clic en estos elementos para obtener más información. En el ejemplo anterior se muestran 430 incidentes relacionados, 665 alertas, 0 listas y no se muestra información en NetWitness Endpoint o Live Connect que mencione la entidad de dirección IP, 192.168.144.254.

En la sección **Acciones** se enumeran las acciones disponibles. En el ejemplo anterior, están disponibles las opciones Cambiar a Investigate, Cambiar a Endpoint y Agregar/eliminar de la lista. Para obtener más información, consulte Cambiar a Investigate, Cambiar a NetWitness Endpoint y Agregar una entidad a una lista blanca.

2. Para ver más detalles acerca de la entidad seleccionada, haga clic en el botón **Ver contexto**. Se abre el panel Búsqueda de contexto, el cual muestra toda la información relacionada con la entidad.
   En el siguiente ejemplo se muestra información contextual para una dirección IP de origen seleccionada. Enumera todos los incidentes que mencionan la dirección IP.

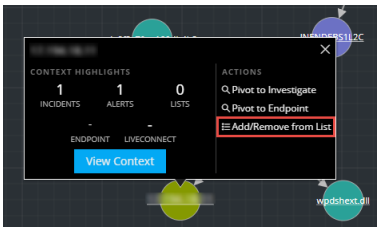


Para comprender las distintas vistas dentro del panel Búsqueda de Context Hub, consulte Panel Búsqueda de contexto: Vista Respond .

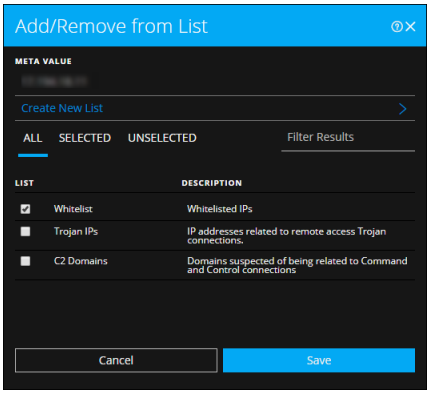
Agregar una entidad a una lista blanca

Puede agregar cualquier entidad subrayada a una lista, como una lista blanca o una lista negra, desde un mensaje de globo de contexto. Por ejemplo, para reducir los falsos positivos, tal vez desee incluir en la lista blanca un dominio subrayado con el fin de excluirlo de las entidades relacionadas.

1. En los paneles Indicadores, Lista de eventos, Detalles de eventos o en el gráfico de nodos, coloque el cursor sobre una entidad subrayada que desee agregar a una lista de Context Hub. Aparece un mensaje de globo de contexto que muestra las acciones disponibles.



2. En la sección **ACCIONES** del mensaje de globo, haga clic en **Agregar/eliminar de la lista**.
   El cuadro de diálogo Agregar/eliminar de la lista muestra las listas disponibles.



3. Seleccione una o más listas y haga clic en **Guardar**.
   La entidad aparece en las listas seleccionadas.
   El Cuadro de diálogo Agregar/eliminar de la lista proporciona información adicional.

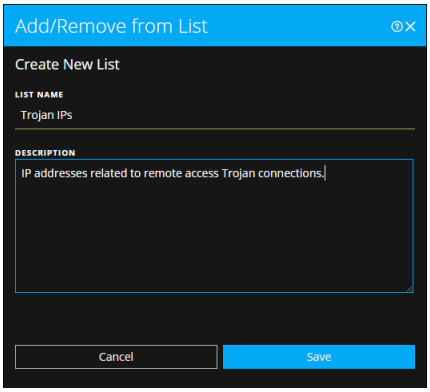
Crear una lista

Puede crear listas en Context Hub desde la vista Respond. Además de usar listas para ingresar entidades en listas blancas y negras, puede usarlas para monitorear el comportamiento anormal en las entidades. Por ejemplo, para mejorar la visibilidad de una dirección IP y un dominio sospechosos que se están investigando, tal vez desee incluirlos en dos listas por separado. Una lista podría incluir dominios que posiblemente tengan relación con conexiones de comando y control, y la otra, direcciones IP relacionadas con conexiones de troyanos de acceso remoto. A continuación, puede identificar indicadores de riesgo mediante estas listas.

Para crear una lista en Context Hub:

1. En los paneles Indicadores, Lista de eventos, Detalles de eventos o en el gráfico de nodos, coloque el cursor sobre una entidad subrayada que desee agregar a una lista de Context Hub.
   Aparece un mensaje de globo de contexto que muestra las acciones disponibles.
2. En la sección **ACCIONES** del mensaje de globo, haga clic en **Agregar/eliminar de la lista**.

3. En el cuadro de diálogo Agregar/eliminar de la lista, haga clic en **Crear lista nueva**.



4. Escriba un **Nombre de lista** único para la lista. El nombre de lista no distingue mayúsculas de minúsculas.
5. (Opcional) Escriba una **DESCRIPCIÓN** para la lista.
   Los analistas con los permisos adecuados también pueden exportar listas en formato CSV para enviarlas a otros analistas, quienes pueden realizar tareas adicionales de rastreo y análisis. En la *Guía de configuración de Context Hub* se proporciona información adicional.

Cambiar a NetWitness Endpoint

Si la aplicación del cliente grueso de NetWitness Endpoint está instalada, puede iniciarla mediante el mensaje de globo de contexto. Desde allí, puede investigar más a fondo una dirección IP, una dirección MAC o un host sospechosos.

1. En los paneles Indicadores, Lista de eventos, Detalles de eventos o en el gráfico de nodos, coloque el cursor sobre una entidad subrayada para acceder a un mensaje de globo de contexto.
2. En la sección **ACCIONES** del mensaje de globo, seleccione **Cambiar a Endpoint**.
   La aplicación del cliente grueso de NetWitness Endpoint se abre fuera del navegador web.

Para obtener más información sobre el cliente grueso, consulte la *Guía del usuario de NetWitness Endpoint*.

Cambiar a Investigate

Si desea realizar una investigación más completa del incidente, puede acceder a la vista Investigate.

1. En los paneles Indicadores, Lista de eventos, Detalles de eventos o en el gráfico de nodos, coloque el cursor sobre una entidad subrayada para acceder a un mensaje de globo de

contexto.

2. En la sección **ACCIONES** del mensaje de globo, seleccione **Cambiar a Investigate**.
   Se abre la vista Navegar de Investigate, la que permite realizar una investigación más detallada.

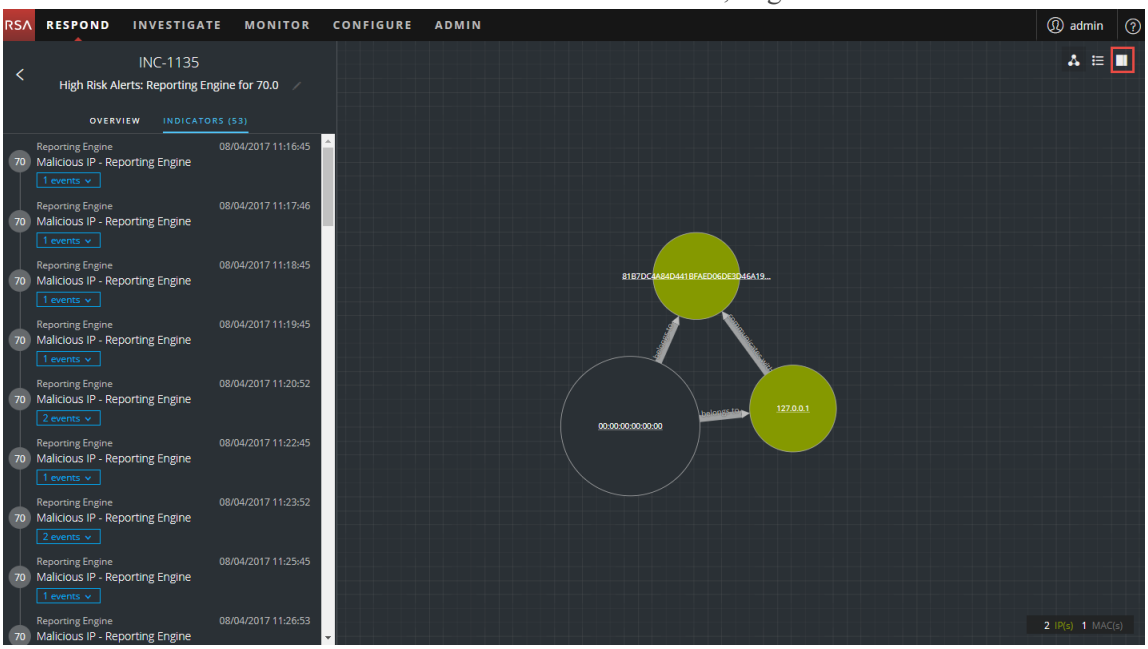
Para obtener más información, consulte la *Guía del usuario de NetWitness Investigate*.

Documentar los pasos realizados fuera de NetWitness

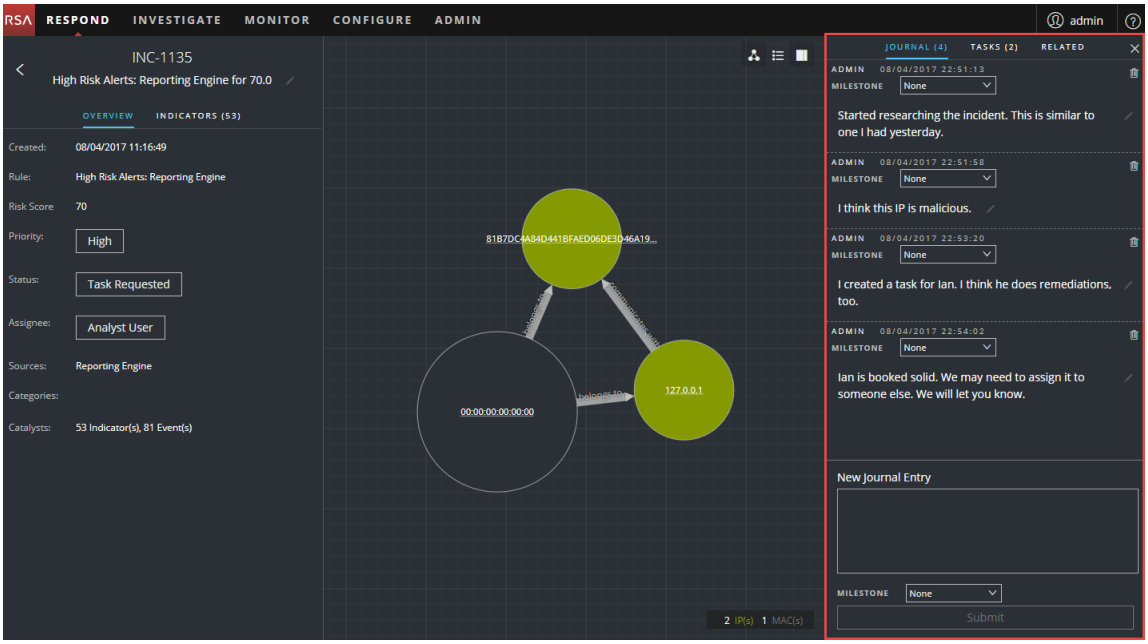
El registro muestra notas que agregan los analistas y permite colaborar con los pares. Puede publicar notas en un registro, agregar etiquetas del Modelo de investigación (Reconocimiento, Distribución, Explotación, Instalación y Comando y control) y ver el historial de actividad en el incidente.

Ver las entradas del registro para un incidente

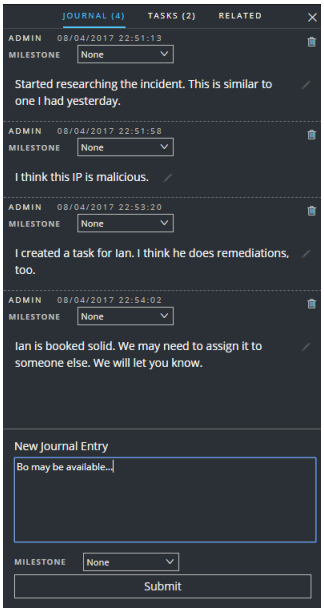
En la barra de herramientas de la vista Detalles de incidente, haga clic en ■.



El diario aparece en el lado derecho de la vista Detalles de incidente.



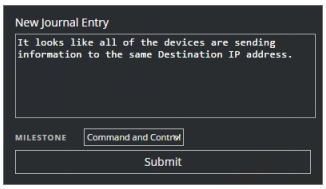
El registro muestra el historial de actividad en un incidente. Para cada entrada del registro, puede ver el autor y la hora de la entrada.



Agregar una nota

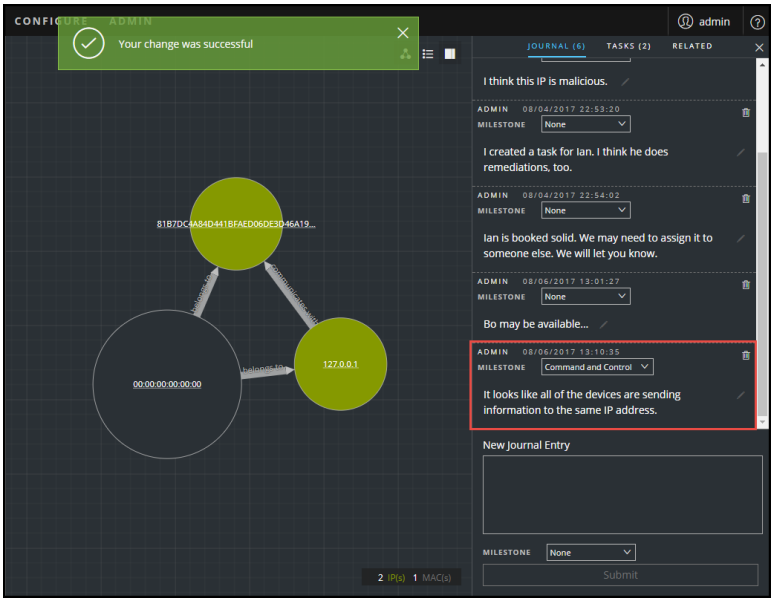
Por lo general, deberá agregar una nota para permitir que otro analista comprenda el incidente o para la posteridad con el fin de documentar los pasos de la investigación.

1. En la parte inferior del panel Registro, escriba la nota en el cuadro **Nueva entrada de diario**.



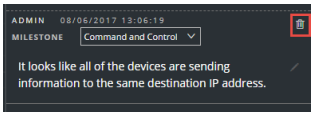
2. (Opcional) Seleccione un Modelo de investigación en la lista desplegable (Reconocimiento, Distribución, Explotación, Instalación, Comando y control, Acción en objetivo, Contención, Erradicación y Cierre).

3. Después de terminar la nota, haga clic en **Enviar**.
   La entrada nueva del registro aparece en el registro.



Eliminar una nota

1. En el panel Registro, busque la entrada del registro que desea eliminar.
2. Haga clic en el ícono Papelera (eliminar) junto a la entrada del registro.



3. En el cuadro de diálogo de confirmación que aparece, haga clic en **Aceptar** para confirmar que desea eliminar la entrada del registro. No se puede revertir esta acción.

Elevar o corregir el incidente

Es posible que deba asignar incidentes a otro analista o cambiar el estado y la prioridad de un incidente a medida que recopila más información sobre el mismo. Esto es útil, por ejemplo, si usted actualiza la prioridad de un incidente de **media** a **alta** después de determinar que el incidente es una vulneración grave.

Actualizar un incidente

Puede actualizar un incidente desde varias ubicaciones. Puede cambiar la prioridad, el estado o el usuario asignado en las vistas Lista de incidentes y Detalles de incidente. Por ejemplo, si es un analista, tal vez desee asignarse un caso desde la vista Lista de incidentes si ve que está relacionado con otro en el que está trabajando. Si es un administrador del SOC o un administrador, puede que desee ver los incidentes no asignados en la vista Lista de incidentes y asignar los incidentes a medida que llegan. Los administradores del SOC y los administradores pueden realizar actualizaciones masivas de la prioridad, el estado o el usuario asignado en lugar de actualizarlos un incidente por vez.

En la vista Detalles, tal vez desee cambiar el estado a En curso una vez que comience a trabajar en un incidente y, a continuación, actualizarlo a Cerrado o Cerrado: falso positivo después de resolver el problema. O bien, puede cambiar la prioridad del incidente a Media o Alta mientras determina los detalles del caso.

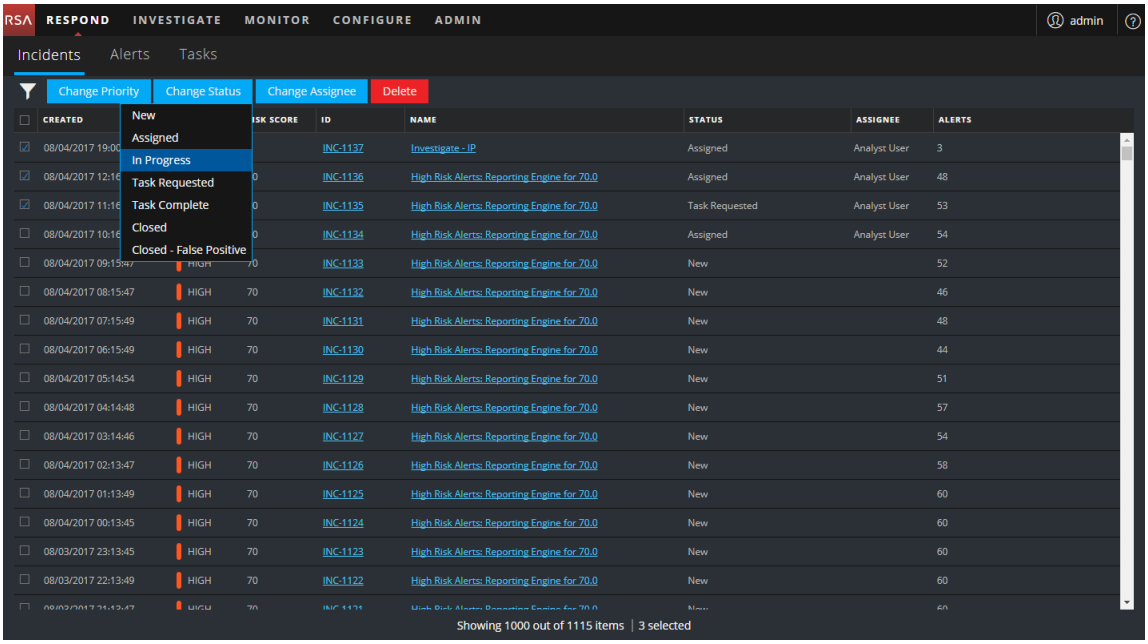
Cambiar el estado de un incidente

Cuando un incidente aparece por primera vez en la lista de incidentes, tiene un estado inicial de Nuevo. Puede actualizar el estado a medida que trabaja en el incidente. Los siguientes estados están disponibles:

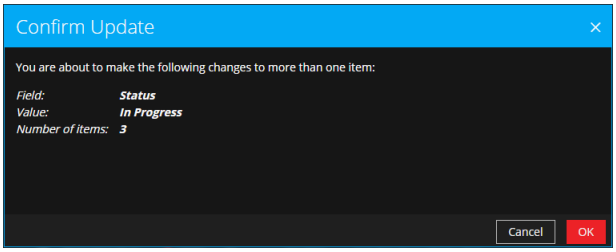
- Nuevo
- Asignado
- En curso
- Tarea solicitada
- Tarea completa
- Cerrado
- Cerrado: falso positivo

Para actualizar el estado de varios incidentes:

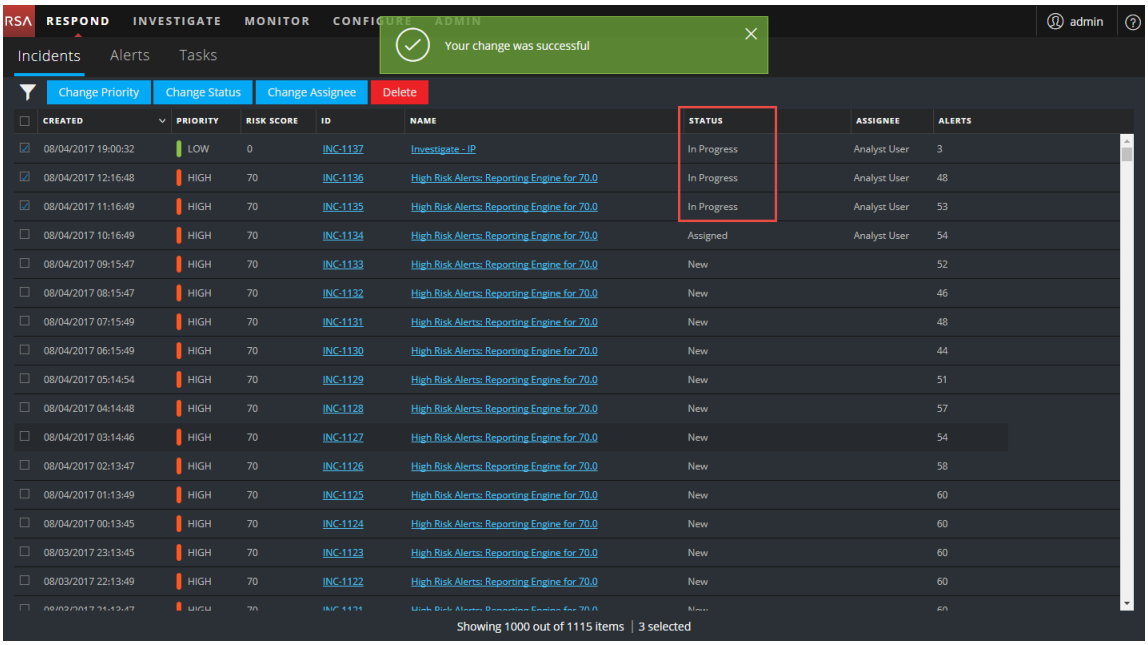
1. En la vista Lista de incidentes, seleccione uno o más incidentes que desee cambiar. Para seleccionar todos los incidentes que aparecen en la página, seleccione la casilla de la fila del encabezado de la lista de incidentes. La cantidad de incidentes seleccionados aparece en el pie de página de la lista de incidentes.
2. Haga clic en **Cambiar estado** y seleccione un estado en la lista desplegable. En este ejemplo, el estado actual es Asignado, pero el analista desea cambiarlo a En curso para los incidentes seleccionados.



3. Si selecciona más de un incidente, en el cuadro de diálogo **Confirmar actualización**, haga clic en **Aceptar**.



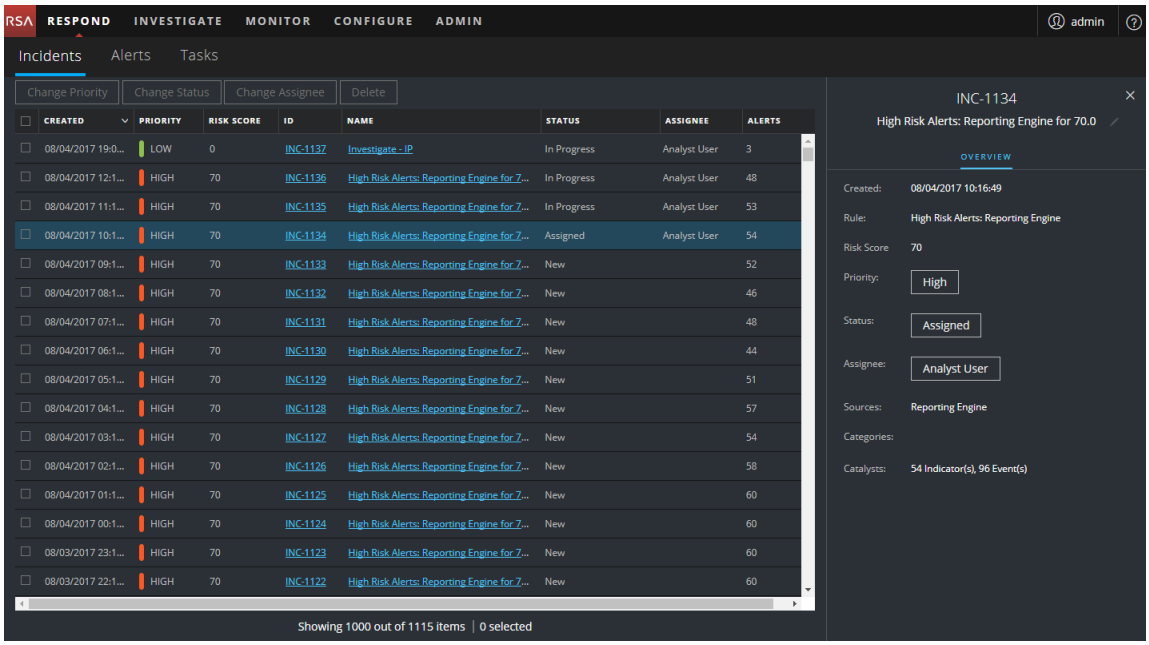
Verá una notificación de cambio correcto. En este ejemplo, el estado de los incidentes actualizados muestra ahora el estado En curso.



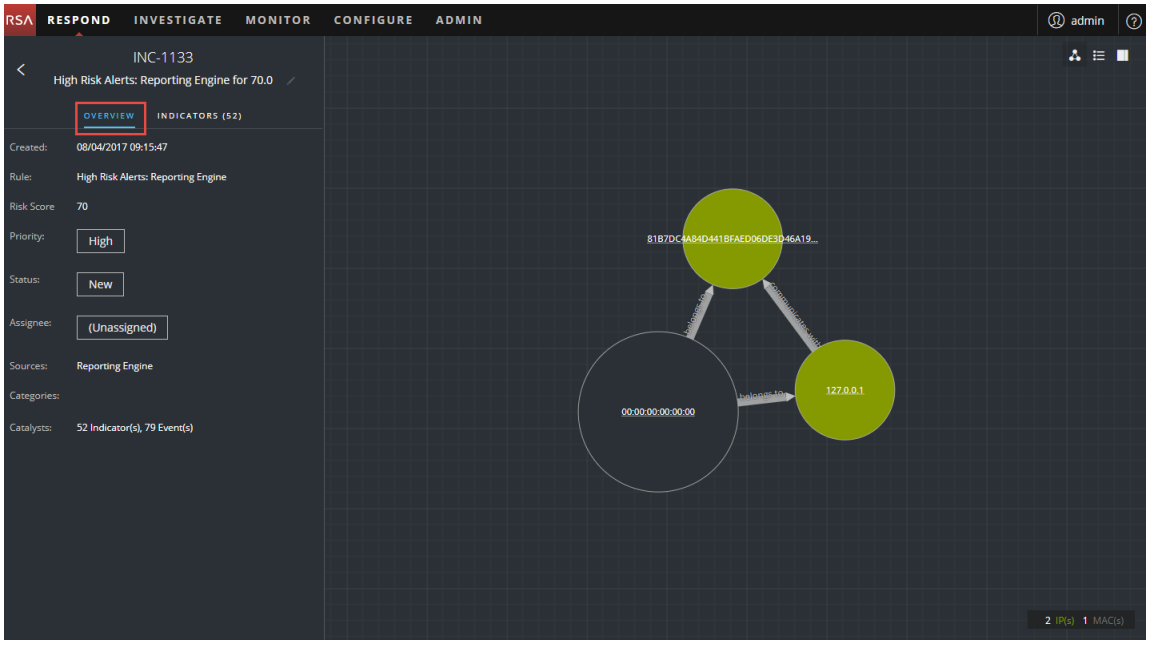
Para cambiar el estado de un único incidente desde el panel Descripción general:

1. Para abrir el panel Descripción general, realice una de las siguientes acciones:

   - En la vista Lista de incidentes, haga clic en un incidente cuyo estado desee actualizar.

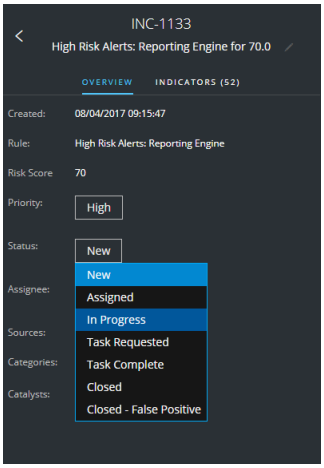


- En la vista Detalles de incidente, haga clic en la pestaña **DESCRIPCIÓN GENERAL**.



En el panel Descripción general, el botón Estado muestra el estado actual del incidente.

2. Haga clic en el botón **Estado** y seleccione un estado en la lista desplegable.



Verá una notificación de cambio correcto.

Cambiar la prioridad del incidente

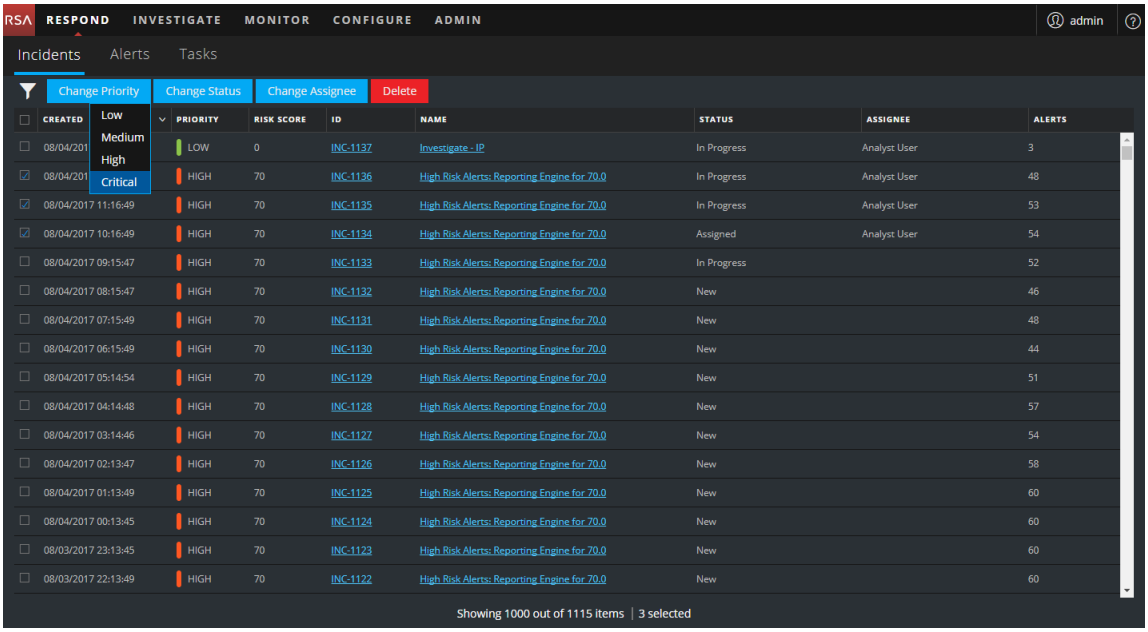
De manera predeterminada, la lista de incidentes se ordena por prioridad. Puede actualizar la prioridad a medida que estudia los detalles del caso. Las siguientes prioridades están disponibles:

- Crítica
- Alta
- Media
- Baja

Nota: No puede cambiar la prioridad de un incidente cerrado.

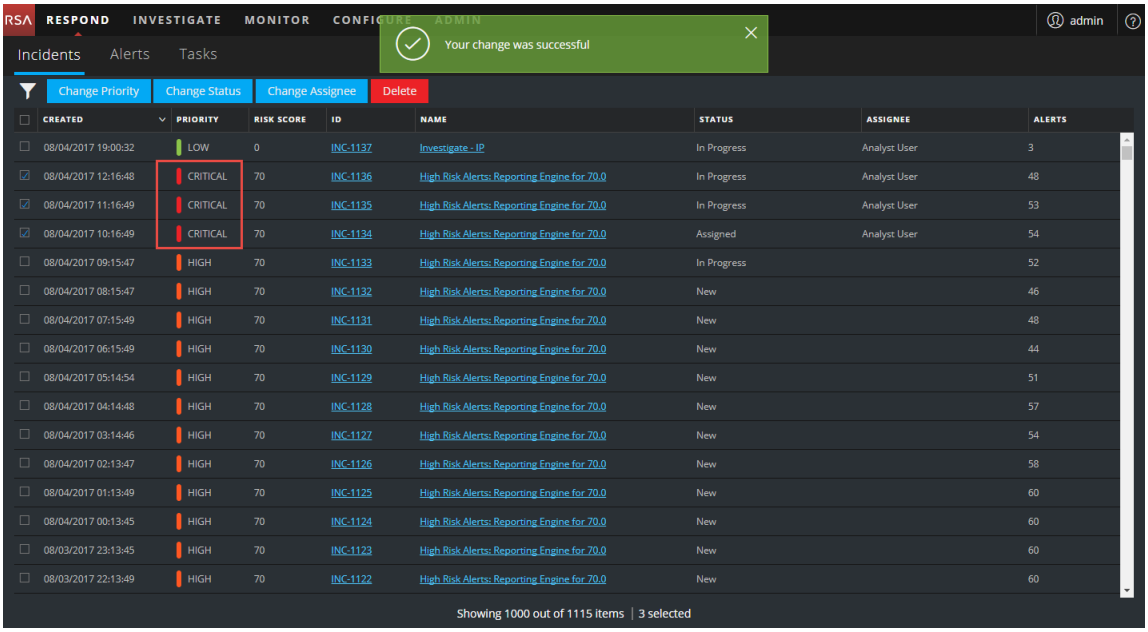
Para actualizar la prioridad de varios incidentes:

1. En la vista Lista de incidentes, seleccione uno o más incidentes que desee cambiar. Para seleccionar todos los incidentes que aparecen en la página, seleccione la casilla de la fila del encabezado de la lista de incidentes. La cantidad de incidentes seleccionados aparece en el pie de página de la lista de incidentes.
2. Haga clic en **Cambiar prioridad** y seleccione una prioridad en la lista desplegable. En este ejemplo, la prioridad actual es Alta, pero el analista desea cambiarla a Crítica para los incidentes seleccionados.



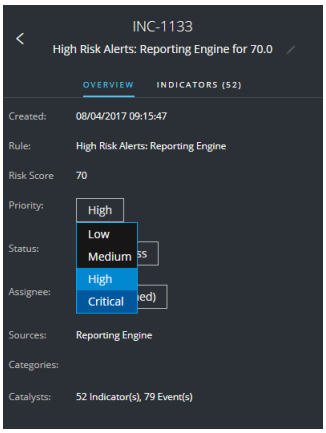
3. Si selecciona más de un incidente, en el cuadro de diálogo **Confirmar actualización**, haga clic en **Aceptar**.
   Verá una notificación de cambio correcto. En este ejemplo, el estado de los incidentes

actualizados muestra ahora la prioridad Crítica.



Para cambiar la prioridad de un único incidente desde el panel Descripción general

1. Para abrir el panel Descripción general, realice una de las siguientes acciones:
   - En la vista Lista de incidentes, haga clic en un incidente cuya prioridad desee actualizar.
   - En la vista Detalles de incidente, haga clic en la pestaña **DESCRIPCIÓN GENERAL**. En el panel Descripción general, el botón Prioridad muestra la prioridad actual del incidente.
2. Haga clic en el botón **Prioridad** y seleccione un estado en la lista desplegable.



Verá una notificación de cambio correcto. El botón Prioridad cambia para mostrar la nueva prioridad del incidente.

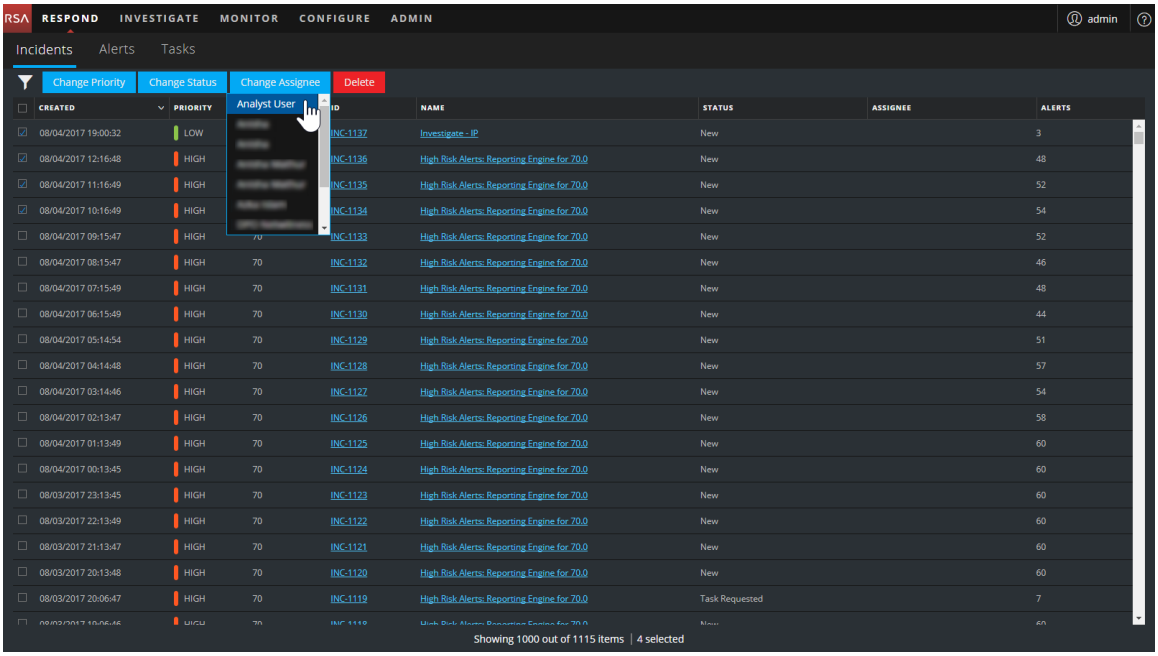
Asignar incidentes a otros analistas

Puede asignar incidentes a otros analistas de la misma manera en que se asigna incidentes a usted mismo. Los administradores del SOC y los administradores pueden asignar varios incidentes a un usuario de forma simultánea.

Nota: No puede cambiar el usuario asignado de un incidente cerrado.

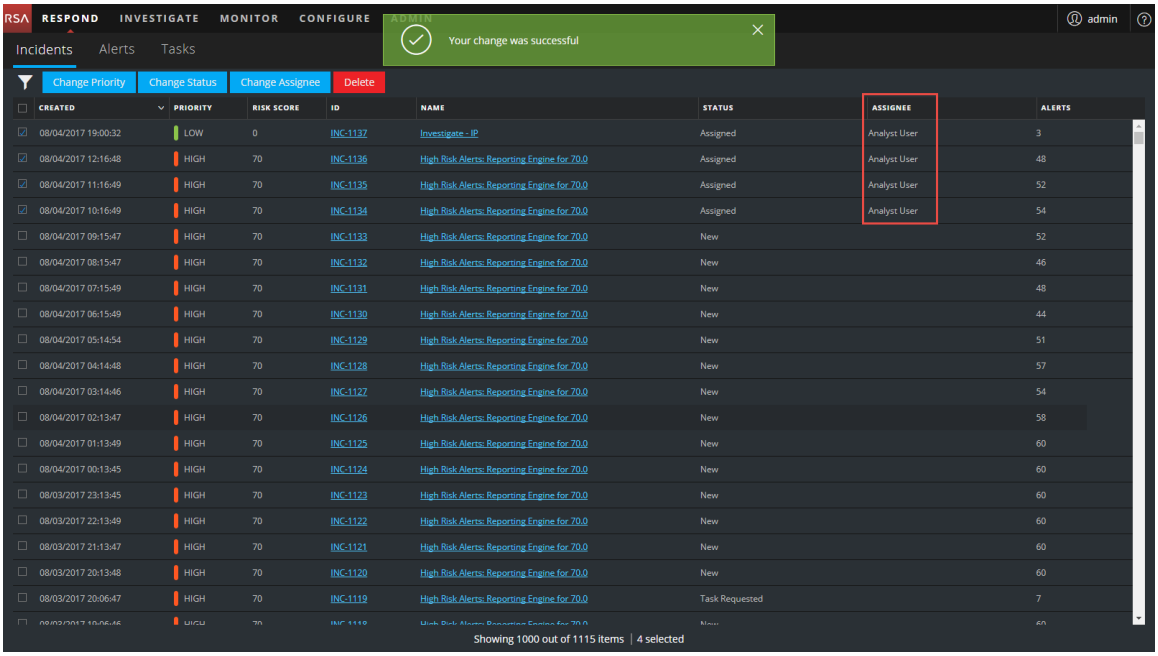
Para asignar varios incidentes a un usuario:

1. En la vista Lista de incidentes, seleccione los incidentes que desea asignar a un usuario. Para seleccionar todos los incidentes que aparecen en la página, seleccione la casilla de la fila del encabezado de la lista de incidentes. La cantidad de incidentes seleccionados aparece en el pie de página de la lista de incidentes.
2. Haga clic en **Cambiar usuario asignado** y seleccione un usuario en la lista desplegable. En este ejemplo, los incidentes no están asignados, pero se deben asignar a un analista.



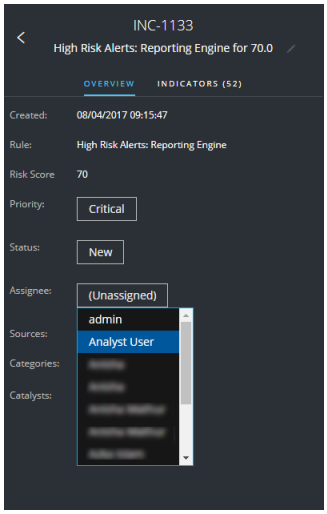
3. Si selecciona más de un incidente, en el cuadro de diálogo **Confirmar actualización**, haga clic en **Aceptar**.
   Verá una notificación de cambio correcto. El usuario asignado cambia al usuario

seleccionado.



Para asignar un usuario a un incidente en el panel Descripción general:

1. Para abrir el panel Descripción general, realice una de las siguientes acciones:
   - En la vista Lista de incidentes, haga clic en un incidente cuya prioridad desee actualizar.
   - En la vista Detalles de incidente, haga clic en la pestaña **DESCRIPCIÓN GENERAL**. En el panel Descripción general, el botón Prioridad muestra la prioridad actual del incidente. En el siguiente ejemplo, el botón Usuario asignado tiene el estado actual Sin asignar.



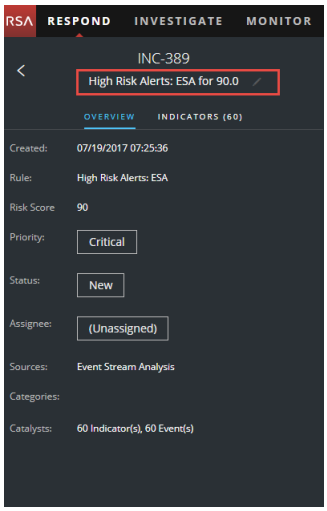
2. Haga clic en el botón **Usuario asignado** y seleccione un usuario en la lista desplegable. Verá una notificación de cambio correcto. El botón Usuario asignado cambia para mostrar el usuario asignado.

Cambiar el nombre de un incidente

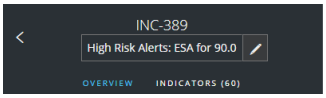
Puede cambiar el nombre de un incidente desde el panel Descripción general en las vistas Lista de incidentes y Detalles de incidente. Por ejemplo, tal vez desee cambiar el nombre de un incidente para proporcionar una aclaración sobre el problema, especialmente si varios incidentes tienen el mismo nombre.

1. Vaya a **RESPONDER > Incidentes**.
2. Para abrir el panel Descripción general, realice una de las siguientes acciones:
   - En la vista Lista de incidentes, haga clic en un incidente cuyo nombre desee cambiar. Se abre el panel Descripción general.

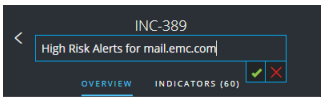
- En la vista Detalles de incidente, vaya al panel **DESCRIPCIÓN GENERAL**.
  En el encabezado sobre el panel Descripción general, puede ver el ID y el nombre del incidente.



3. Haga clic en el nombre del incidente en el encabezado para abrir un editor de texto.

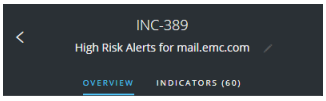


4. Escriba un nuevo nombre para el incidente en el editor de texto y haga clic en la marca de verificación para confirmar el cambio.



   Por ejemplo, puede cambiar “High Risk Alerts: ESA for 90.0” a “Alerts for mail.emc.com” a modo de aclaración.
   Verá una notificación de cambio correcto.

   El campo nombre del incidente muestra el nuevo nombre.

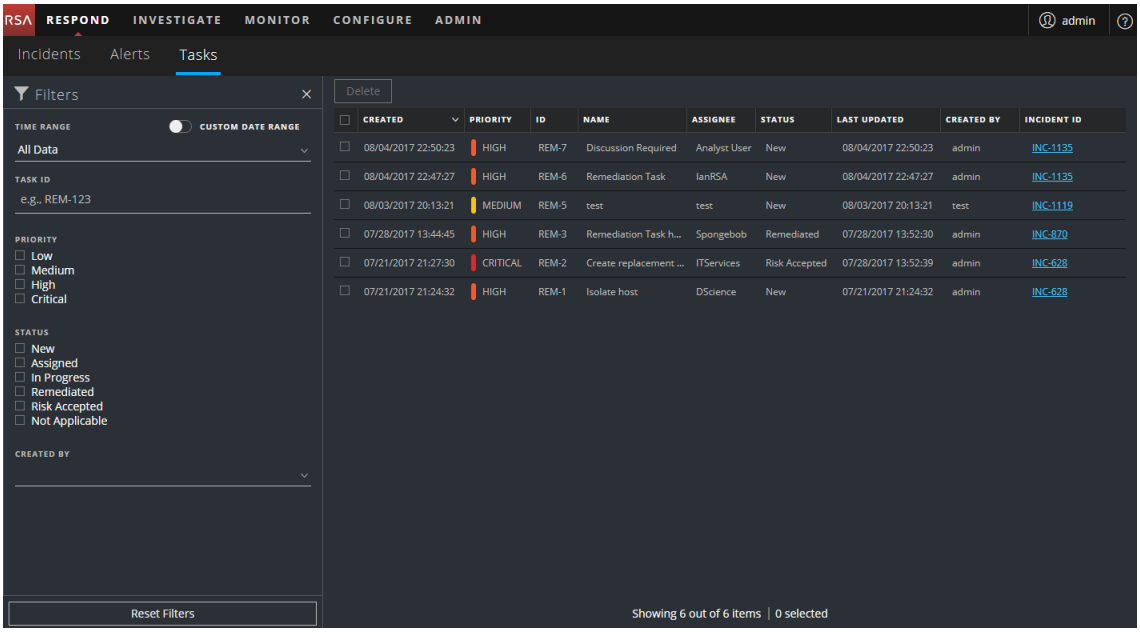


Ver todas las tareas de incidentes

Cuando se requiere trabajo adicional para un incidente, puede crear tareas para este y rastrear el progreso de esas tareas. Esto es útil, por ejemplo, cuando el trabajo que se realiza es externo a las operaciones de seguridad o se hace una solicitud de creación de una nueva imagen de una computadora. En la vista Lista de tareas, puede administrar y rastrear las tareas hasta su cierre.

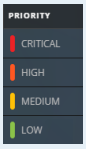
1. Vaya a **RESPONDER > Tareas**.

   La vista Lista de tareas muestra una lista de todas las tareas de incidentes.



2. Desplácese por la Lista de tareas, la que muestra información básica acerca de cada tarea, como se describe en la siguiente tabla.

Columna	Descripción
CREADO	Muestra la fecha en que se creó la tarea.

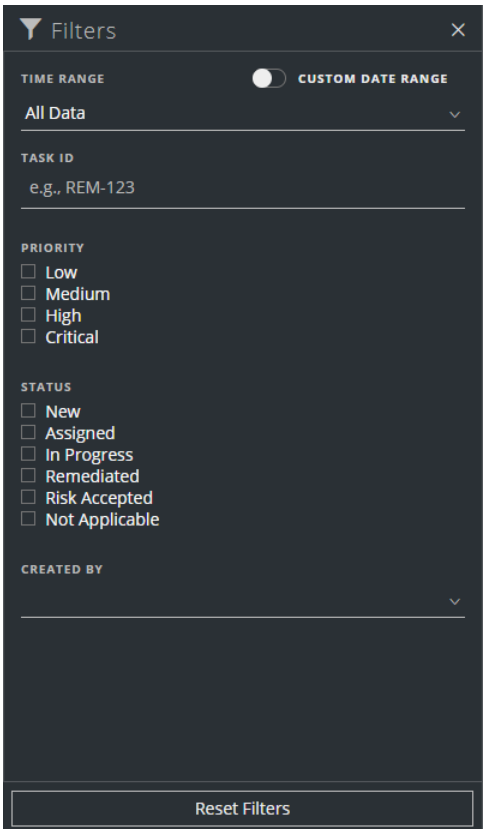
Columna	Descripción
PRIORIDAD	Muestra la prioridad asignada a la tarea. La prioridad puede ser cualquiera de las siguientes: Crítica, Alta, Media o Baja. La prioridad también está codificada en colores. El rojo indica un riesgo de prioridad **Crítica**, el naranja, **Alta**, el amarillo, **Media** y el verde, **Baja**, como se muestra en la siguiente figura: 
ID	Muestra el ID de la tarea.
NAME	Muestra el nombre de la tarea.
USUARIO ASIGNADO	Muestra el nombre del usuario asignado a la tarea.
ESTADO	Muestra el estado de la tarea: Nuevo, Asignado, En Curso, Corregido, Riesgo aceptado y No aplicable.
ÚLTIMA ACTUALIZACIÓN	Muestra la fecha y hora de la última actualización de la tarea.
CREADO POR	Muestra el usuario que creó 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.

En la parte inferior de la lista, puede ver la cantidad de tareas que se muestran en la página actual, la cantidad total de tareas y la cantidad de tareas seleccionadas. Por ejemplo: **Mostrando 6 de 6 elementos | 2 seleccionado(s)**.

Filtrar la Lista de tareas

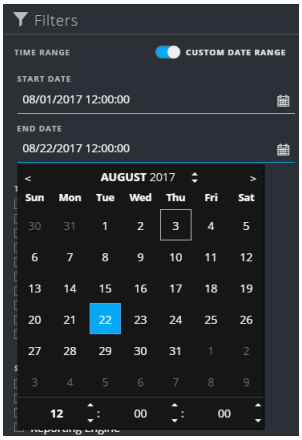
La cantidad de tareas en la Lista de tareas puede ser muy alta, lo que dificulta la localización de determinadas tareas. El filtro le permite especificar las tareas que desea ver, como las tareas que se crearon en los últimos 7 días. También puede buscar una tarea específica.

1. Vaya a **RESPONDER > Tareas**.
   El panel Filtros aparece a la izquierda de la Lista de tareas. Si no ve el panel Filtros, en la barra de herramientas de la vista Lista de tareas, haga clic en para abrirlo.



2. En el panel Filtros, seleccione una o más opciones para filtrar la lista de incidentes:
   - **RANGO DE TIEMPO**: Puede seleccionar un período específico en la lista desplegable Rango de tiempo. El rango de tiempo se basa en la fecha de creación de las tareas. Por ejemplo, si selecciona Última hora, verá las tareas que se crearon en los últimos 60 minutos.
   - **RANGO DE FECHAS PERSONALIZADO**: Puede especificar un rango de fechas determinado en lugar de seleccionar una opción de Rango de tiempo. Para ello, haga clic en el círculo blanco frente a RANGO DE FECHAS PERSONALIZADO para ver los campos Fecha de inicio y Fecha de finalización. Seleccione las fechas y las horas en el

calendario.



- **ID DE TAREA**: Escriba el ID de tarea que desea buscar, por ejemplo, REM-123.
- **PRIORIDAD**: Seleccione las prioridades que desea ver.
- **ESTADO**: Seleccione uno o más estados de incidentes. Por ejemplo, seleccione Corregido para ver las tareas de corrección completas.
- **CREADO POR**: Seleccione el usuario que creó las tareas que desea ver. Por ejemplo, si solo desea ver las tareas que creó Edwardo, seleccione Edwardo en la lista desplegable CREADO POR. Si desea ver las tareas independientemente de la persona que las creó, no realice una selección en CREADO POR.

La Lista de tareas muestra las tareas que cumplen con los criterios de selección. Puede ver la cantidad de elementos de la lista filtrada en la parte inferior de la lista de tareas.
Por ejemplo: **Mostrando 6 de 6 elementos**

3. Si desea cerrar el panel Filtros, haga clic en **X**. Los filtros permanecen en su lugar hasta que los quita.

Quitar los filtros de la Lista de tareas

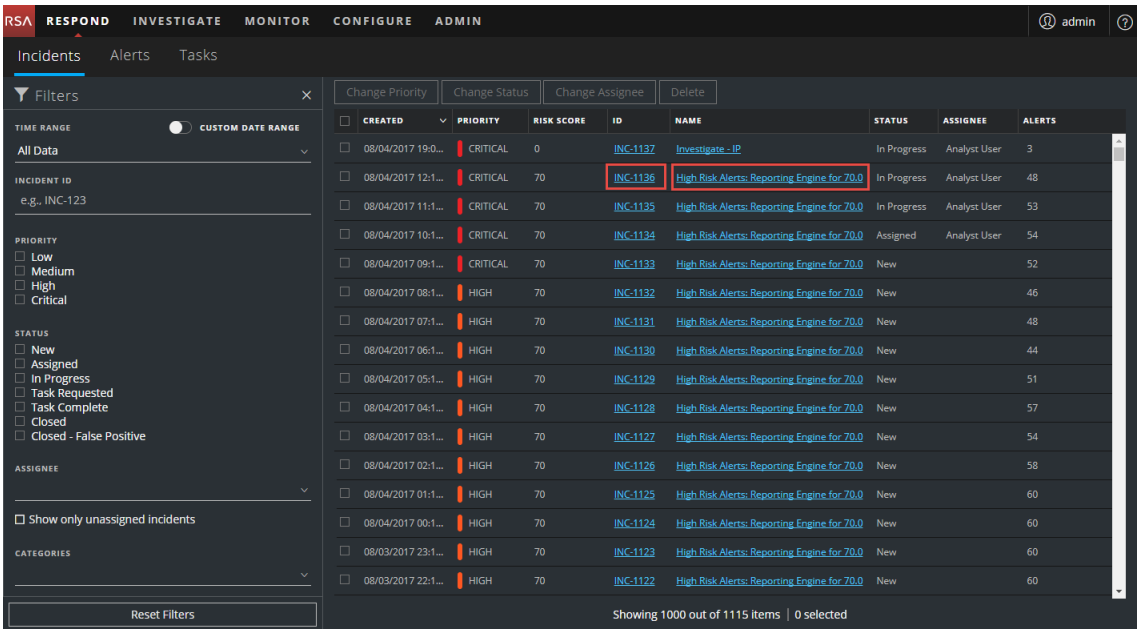
NetWitness Suite recuerda las selecciones de filtros en la vista Lista de tareas. Puede quitar las selecciones de filtros cuando ya no las necesite. Por ejemplo, si no ve la cantidad de tareas que espera o que desea ver, o desea ver todas las tareas en la lista de tareas, puede restablecer los filtros.

1. Vaya a **RESPONDER > Tareas**.
   El panel Filtros aparece a la izquierda de la Lista de tareas. Si no ve el panel Filtros, en la barra de herramientas de la vista Lista de tareas, haga clic en para abrirlo.
2. En la parte inferior del panel Filtros, haga clic en **Restablecer filtros**.

Crear una tarea

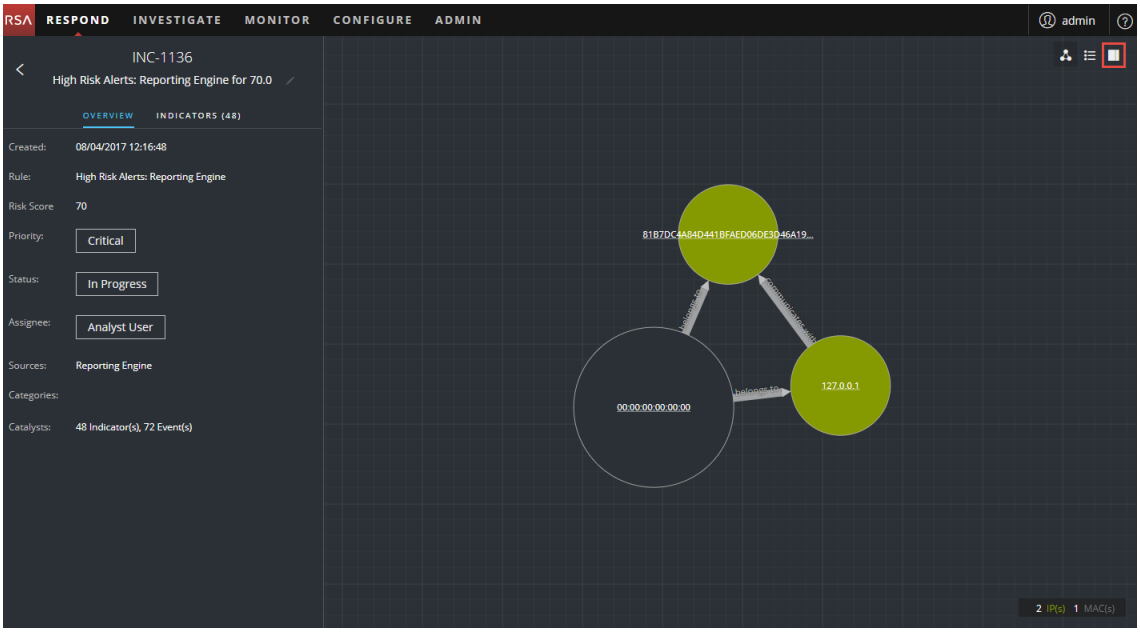
Después de investigar un incidente y obtener más información sobre este, puede crear una tarea, asignarla a un usuario y rastrearla hasta su cierre. Las tareas se crean en la vista Detalles de incidente.

1. Vaya a **RESPONDER > Incidentes**.
   La vista Lista de incidentes muestra una lista de todos los incidentes.



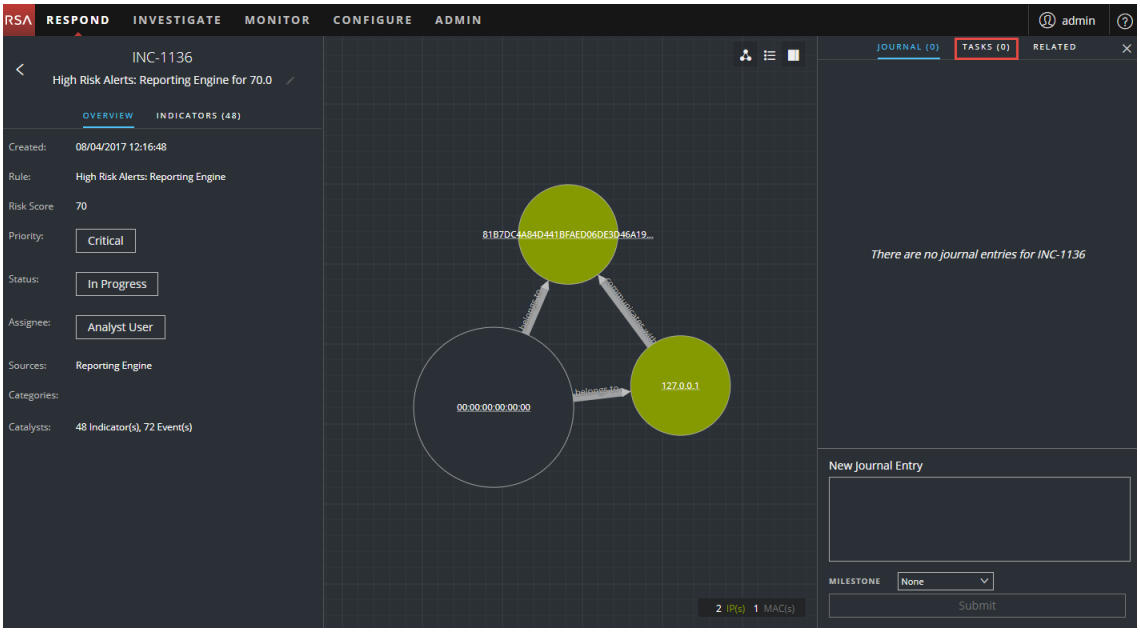
2. Busque el incidente que necesita una tarea y haga clic en el vínculo del campo **ID** o **Nombre**.

Se abre la vista Detalles de incidente.

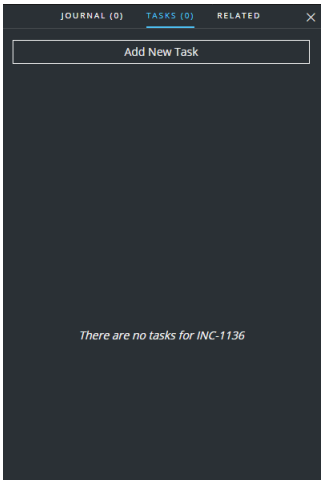


3. En la barra de herramientas de la parte superior derecha de la vista Detalles de incidente, seleccione ▣.

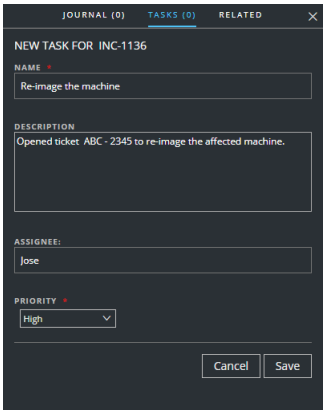
   Se abre el panel Registro.



4. Seleccione la pestaña **TAREAS**.



5. En el panel Tareas, haga clic en **Agregar tarea nueva.**
   Verá los campos de la tarea nueva.

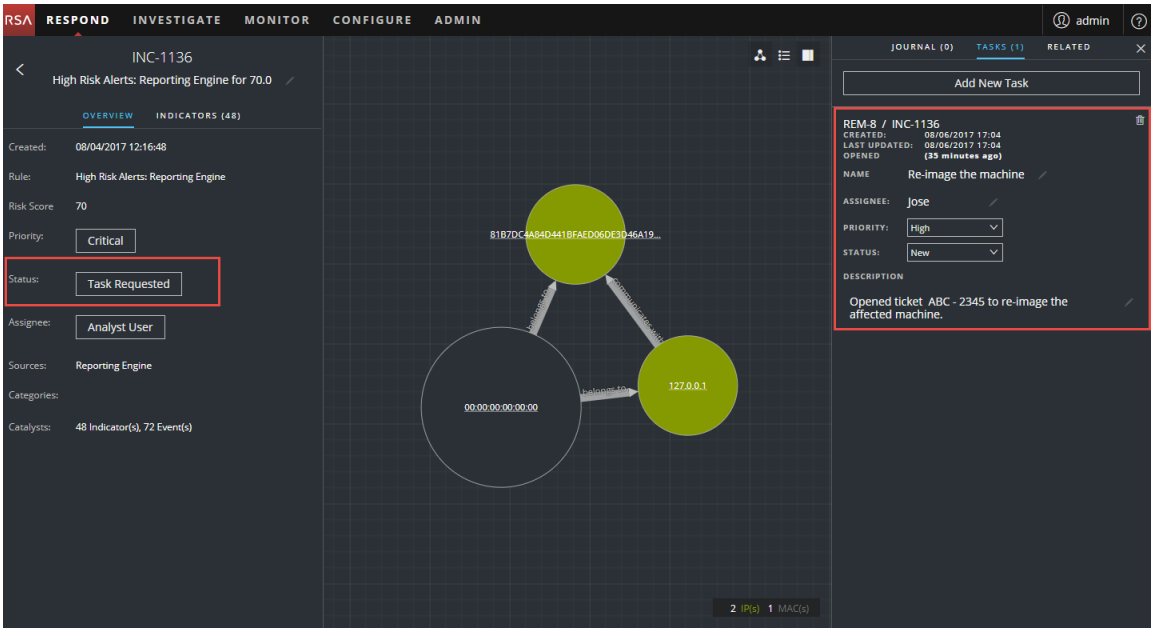


   Si el incidente se encuentra en un estado cerrado (Cerrado o Cerrado: falso positivo), el botón Agregar tarea nueva se deshabilita.

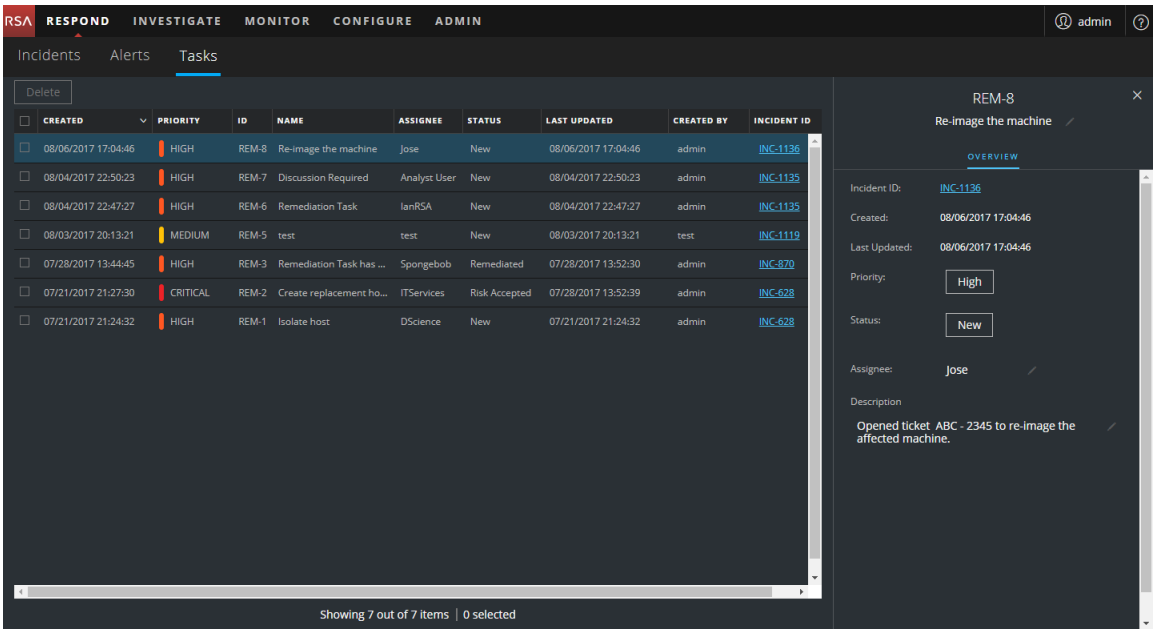
6. Proporcione la siguiente información:
   - **Nombre**: Nombre de la tarea. Por ejemplo: Re-image the machine.
   - **Descripción** (opcional): Ingrese información que describa la tarea. Tal vez desee incluir números de referencia correspondientes.
   - **Usuario asignado** (opcional): Escriba el nombre del usuario a quien se asignará la tarea.
   - **Prioridad**: Haga clic en el botón Prioridad y seleccione una prioridad para las tareas en la lista desplegable: Baja, Media, Alta o Crítica.

7. Haga clic en **Guardar**.
   Verá una confirmación que indica que el cambio se realizó correctamente. El estado del incidente cambia a **Tarea solicitada**. La tarea aparece en el panel Tareas para este

incidente.



También aparece en la Lista de tareas (RESPONDER > Tareas), la que muestra una lista de todas las tareas de incidentes.

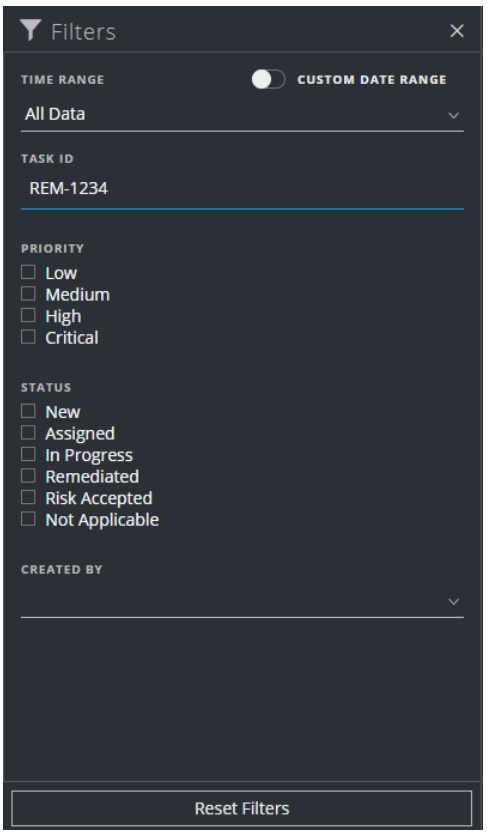


Nota: Si no ve el cambio de estado, puede ser necesario actualizar el navegador de Internet.

Buscar una tarea

Si conoce el ID de tarea, puede buscar rápidamente una tarea mediante el filtro. Por ejemplo, tal vez desee buscar una tarea específica entre miles de tareas.

1. Vaya a **RESPONDER > Tareas**.
   El panel Filtros aparece a la izquierda de la Lista de tareas. Si no ve el panel Filtros, en la barra de herramientas de la vista Lista de tareas, haga clic en para abrirlo.



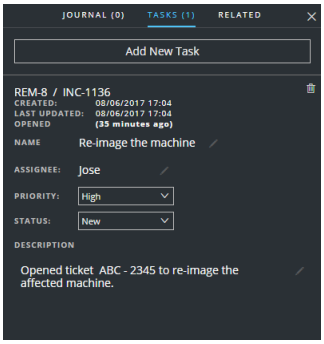
2. En el campo ID de tarea, escriba el ID de tarea que desea buscar, por ejemplo, REM-1234.
   La tarea especificada aparece en la lista de tareas. Si no ve ningún resultado, intente restablecer los filtros.

Modificar una tarea

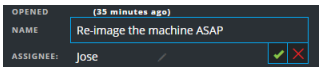
Puede modificar una tarea desde dentro de un incidente y en la Lista de tareas. Por ejemplo, tal vez desee mostrar el estado de la tarea como En curso y agregar información adicional a la tarea. Si la tarea está en estado Cerrado (No aplicable, Riesgo aceptado o Corregido), no puede modificar la Prioridad ni el Usuario asignado.

Para modificar una tarea desde dentro de un incidente:

1. Vaya a **RESPONDER > Incidentes**.
   La vista Lista de incidentes muestra una lista de todos los incidentes.
2. Busque el incidente para el cual se actualizará una tarea y haga clic en el vínculo del campo **ID** o **Nombre**.
   Se abre la vista Detalles de incidente.
3. En la barra de herramientas de la parte superior derecha de la vista, seleccione ◻.
   Se abre el panel Registro.
4. Seleccione la pestaña **TAREAS**.
5. En el panel Tareas, un ícono de lápiz indica un campo de texto que puede modificar. Un botón indica que hay una lista desplegable para realizar una selección.

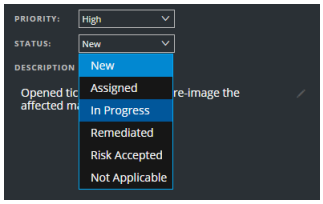


6. Puede modificar cualquiera de los siguientes campos:
   - **NOMBRE**: Haga clic en el nombre de la tarea actual para abrir un editor de texto.

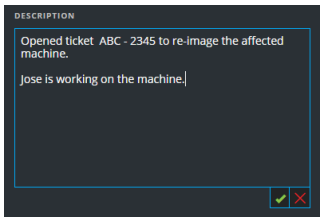


     Haga clic en la marca de verificación para confirmar el cambio. Por ejemplo, puede cambiar “Re-image the machine” a “Re-image the machine ASAP”.
   - **USUARIO ASIGNADO**: Haga clic en (Sin asignar) o en el nombre del usuario asignado anterior para abrir un editor de texto. Escriba el nombre del usuario a quien se asignará la tarea.
     Haga clic en la marca de verificación para confirmar el cambio.
   - **PRIORIDAD**: Haga clic en el botón Prioridad y seleccione una prioridad para la tarea en la lista desplegable: Baja, Media, Alta o Crítica.
   - **ESTADO**: Haga clic en el botón Estado y seleccione un estado para la tarea en la lista desplegable: Nuevo, Asignado, En Curso, Corregido, Riesgo aceptado y No aplicable. Por

ejemplo, puede cambiar el estado a En curso.



- **DESCRIPCIÓN**: Haga clic en el texto debajo de la descripción para abrir un editor de texto.

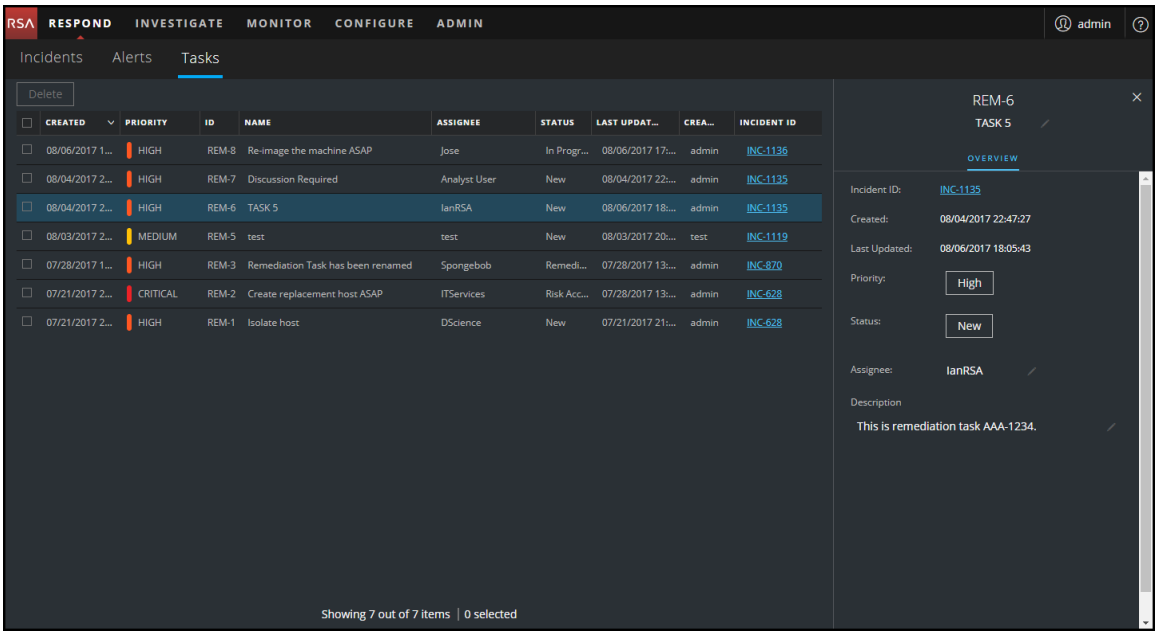


Modifique el texto y haga clic en la marca de verificación para confirmar el cambio.

Por cada cambio que realiza, verá una confirmación que indica que el cambio se realizó correctamente.

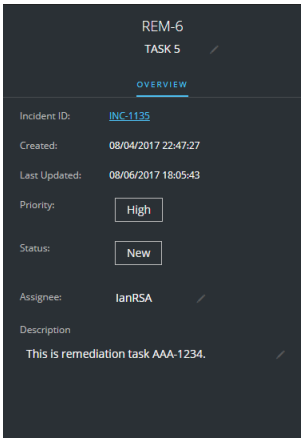
Para modificar una tarea en la Lista de tareas:

1. Vaya a **RESPONDER > Tareas**.
   La vista Lista de tareas muestra una lista de todas las tareas de incidentes.
2. En la Lista de tareas, haga clic en la tarea que desea actualizar.
   El panel Descripción general de tareas aparece a la derecha de la lista de tareas.



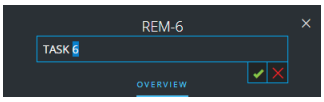
En el panel Descripción general de la tarea, un ícono de lápiz indica un campo de texto que

puede modificar. Un botón indica que hay una lista desplegable para realizar una selección.



3. Puede modificar cualquiera de los siguientes campos:

   - **<Nombre de la tarea>**: En la parte superior del panel Descripción general de la tarea, bajo el ID de tarea, haga clic en el nombre actual de la tarea para abrir un editor de texto.

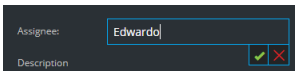
     

     Haga clic en la marca de verificación para confirmar el cambio. Por ejemplo, puede cambiar TASK 5 a TASK 6.

   - **Prioridad**: Haga clic en el botón Prioridad y seleccione una prioridad para la tarea en la lista desplegable: Baja, Media, Alta o Crítica.

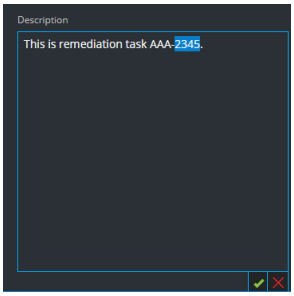
   - **Estado**: Haga clic en el botón Estado y seleccione un estado para la tarea en la lista desplegable: Nuevo, Asignado, En Curso, Corregido, Riesgo aceptado y No aplicable.

   - **Usuario asignado**: Haga clic en (Sin asignar) o en el nombre del usuario asignado anterior para abrir un editor de texto. Escriba el nombre del usuario a quien se asignará la tarea.

     Haga clic en la marca de verificación para confirmar el cambio.

- **Descripción**: Haga clic en el texto debajo de la descripción para abrir un editor de texto.



  Modifique el texto y haga clic en la marca de verificación para confirmar el cambio.

Por cada cambio que realiza, verá una confirmación que indica que el cambio se realizó correctamente.

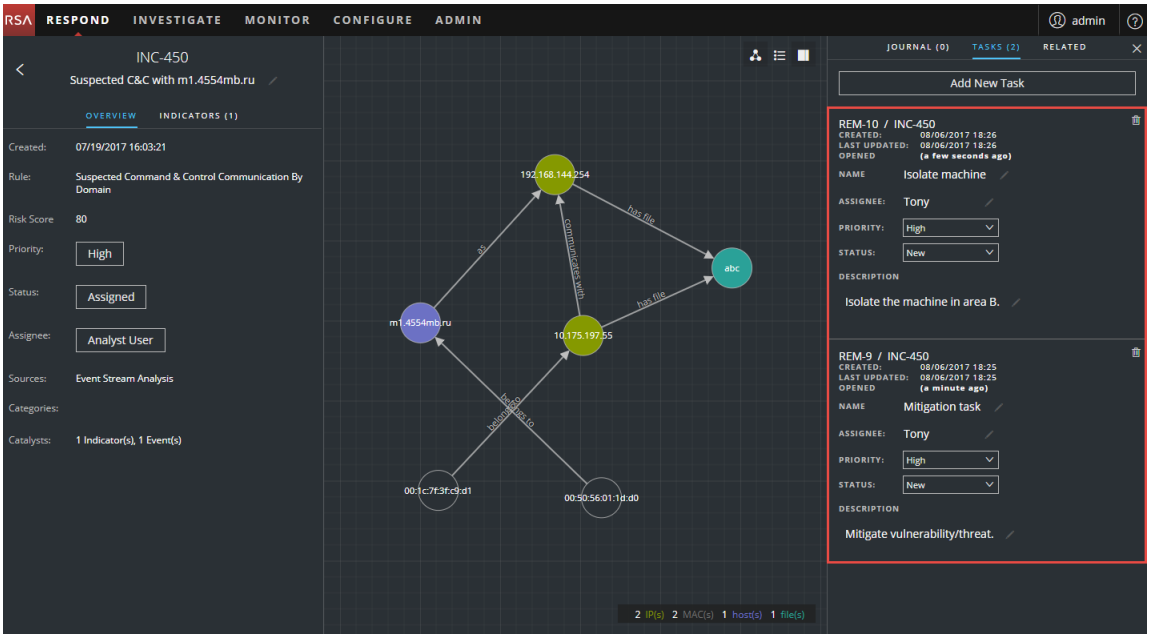
Eliminar una tarea

Puede eliminar una tarea, si, por ejemplo, la creó por error o descubre que no se necesita. Puede eliminar una tarea desde dentro de un incidente y también en la vista Lista de tareas. En la vista Lista de tareas, puede eliminar varias tareas al mismo tiempo.

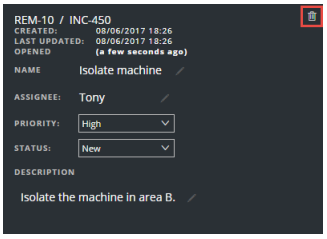
Para eliminar una tarea desde dentro de un incidente:

1. Vaya a **RESPONDER > Incidentes**.
   La vista Lista de incidentes muestra una lista de todos los incidentes.
2. Busque el incidente para el cual se actualizará una tarea y haga clic en el vínculo del campo **ID** o **Nombre**.
   Se abre la vista Detalles de incidente.
3. En la barra de herramientas de la parte superior derecha de la vista, seleccione ▣.
   Se abre el panel Registro.
4. Seleccione la pestaña TAREAS.

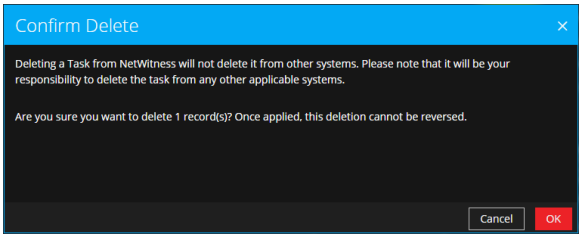
5. En el panel Tareas, puede ver las tareas creadas para el incidente.



6. Haga clic en 🗑 a la derecha de la tarea que desea eliminar.



7. Confirme su intención de eliminar la tarea y haga clic en **Aceptar**.

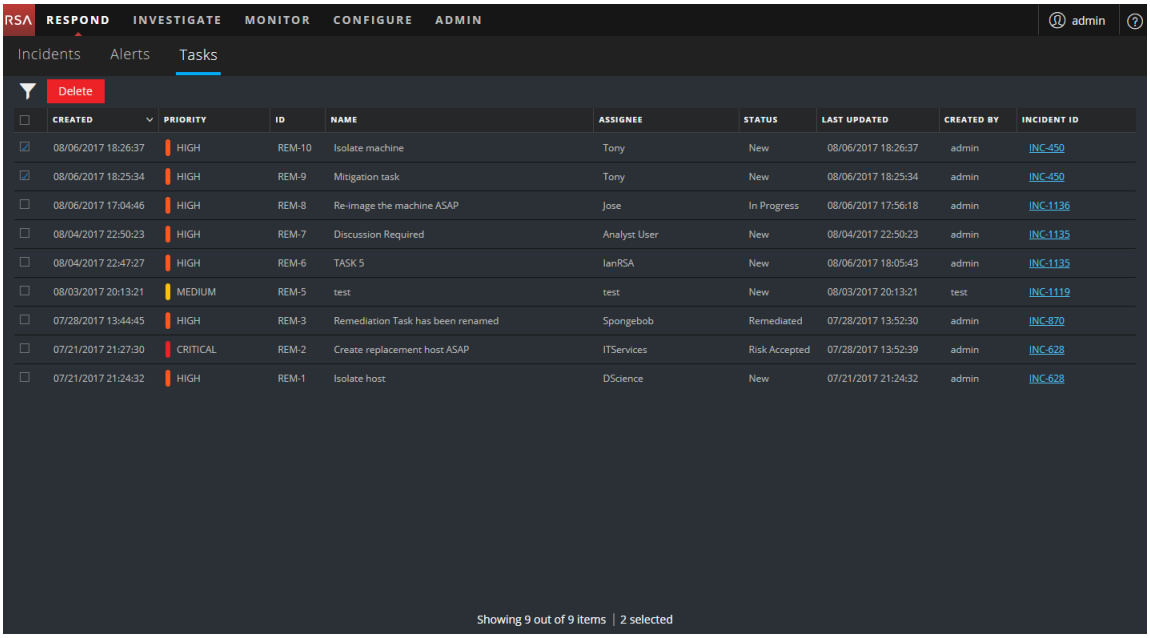


La tarea se elimina de NetWitness Suite. La eliminación de tareas de NetWitness Suite no las elimina de otros sistemas.

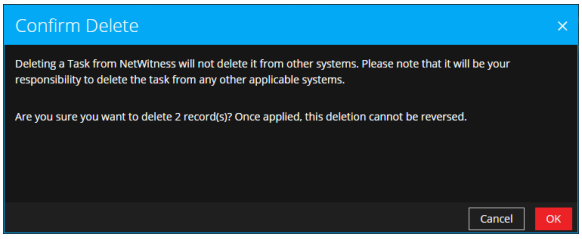
Para eliminar tareas desde la Lista de tareas:

1. Vaya a **RESPONDER > Tareas**.
   La vista Lista de tareas muestra una lista de todas las tareas de incidentes.

2. En la Lista de tareas, seleccione las tareas que desea eliminar y haga clic en **Eliminar**.



3. Confirme su intención de eliminar las tareas y haga clic en **Aceptar**.



Las tareas se eliminan de NetWitness Suite. La eliminación de tareas de NetWitness Suite no las elimina de otros sistemas.

Cerrar un incidente

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

1. Vaya a **RESPONDER > Incidentes**.
2. En la vista Lista de incidentes, seleccione el incidente que desea cerrar y haga clic en **Cambiar estado**.
3. Seleccione **Cerrado** en la lista desplegable.
   Verá una notificación de cambio correcto. Ahora, el incidente se cierra. No puede cambiar la prioridad ni el usuario asignado de un incidente cerrado.

Nota: También puede cerrar un incidente en el panel Descripción general. Puede cerrar varios incidentes al mismo tiempo en la vista Lista de incidentes. En Cambiar el estado de un incidente se proporcionan detalles adicionales.

Revisión de alertas

NetWitness Suite permite ver una lista consolidada de alertas de amenazas generadas a partir de varios orígenes en una ubicación. Puede encontrar estas alertas en la vista RESPOND > Alertas. El origen de las alertas puede ser ESA Correlation Rules, ESA Analytics, NetWitness Endpoint, Malware Analysis, Reporting Engine y muchos otros. Puede ver el origen original de las alertas, su gravedad y detalles adicionales acerca de estas.

Nota: Las alertas de reglas de correlación de ESA SOLO se pueden encontrar en la vista RESPOND > Alertas.

Para administrar mejor una gran cantidad de alertas, tiene la capacidad de filtrar la lista de alertas en función de criterios que usted especifica, como la gravedad, el rango de tiempo y el origen de las alertas. Por ejemplo, tal vez desee filtrar las alertas para mostrar solo aquellas cuya gravedad está entre 90 y 100, y que aún no forman parte de un incidente. A continuación, puede seleccionar un grupo de alertas para crear un incidente o para agregarlo a un incidente existente.

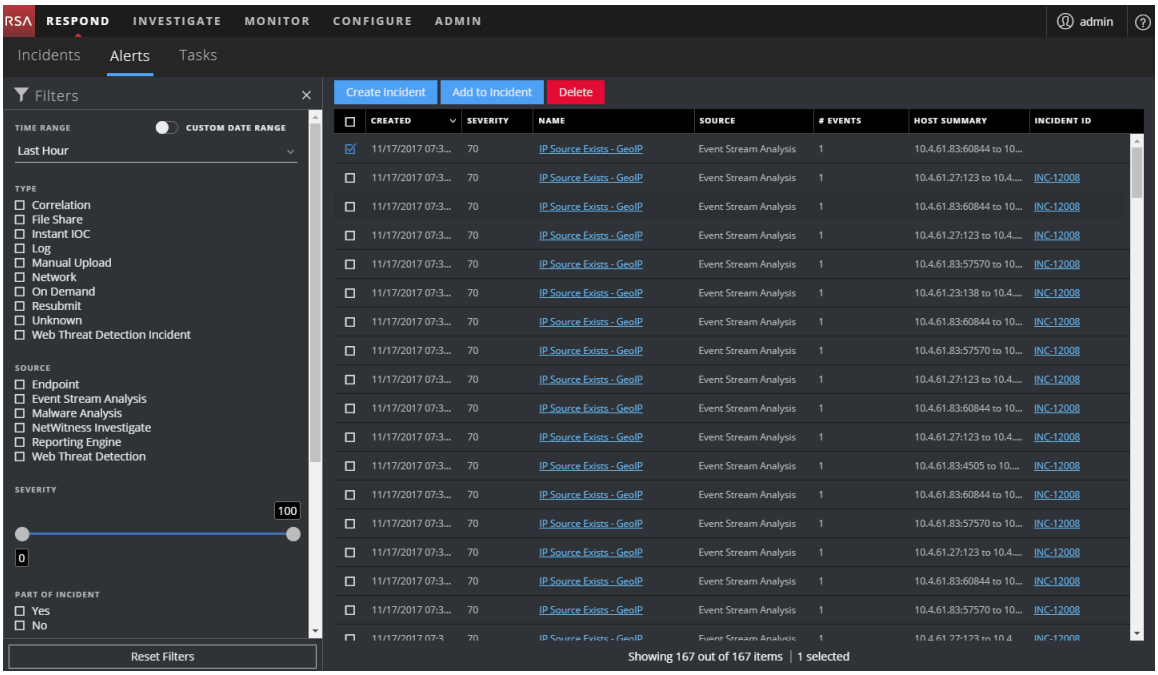
Puede realizar los siguientes procedimientos para revisar y administrar las alertas:

- Ver alertas
- Filtrar la Lista de alertas
- Quitar los filtros de la Lista de alertas
- Ver información de resumen de las alertas
- Ver detalles de los eventos de una alerta
- Investigar eventos
- Crear un incidente manualmente
- Agregar alertas a un incidente
- Eliminar alertas

Ver alertas

En la vista Lista de alertas, puede navegar para explorar las diversas alertas de múltiples orígenes, filtrarlas y agruparlas para crear incidentes. En este procedimiento se muestra cómo acceder a la lista de alertas.

1. Vaya a **RESPONDER > Alertas**.
   La vista Lista de alertas muestra una lista de todas las aletas de NetWitness Suite.



2. Desplácese por la lista de alertas, la que muestra información básica acerca de cada alerta, como se describe en la siguiente tabla.

Columna	Descripción
CREADO	Muestra la fecha y la hora en que se registró la alerta en el sistema de origen.
GRAVEDAD	Muestra el nivel de gravedad de la alerta. Los valores varían entre 1 y 100.
NAME	Muestra una descripción básica de la alerta.
ORIGEN	Muestra el origen original de la alerta. El origen de las alertas puede ser NetWitness Endpoint, Malware Analysis, Event Stream Analysis (ESA Correlation Rules), ESA Analytics, Reporting Engine, Web Threat Detection y muchos otros.
CANTIDAD DE EVENTOS	Indica la cantidad de eventos que se incluyen dentro de una alerta. esto varía según el origen de la alerta. Por ejemplo, las alertas de NetWitness Endpoint y Malware Analysis siempre tienen un evento. Para ciertos tipos de alertas, una alta cantidad de eventos puede significar que la alerta es más riesgosa.

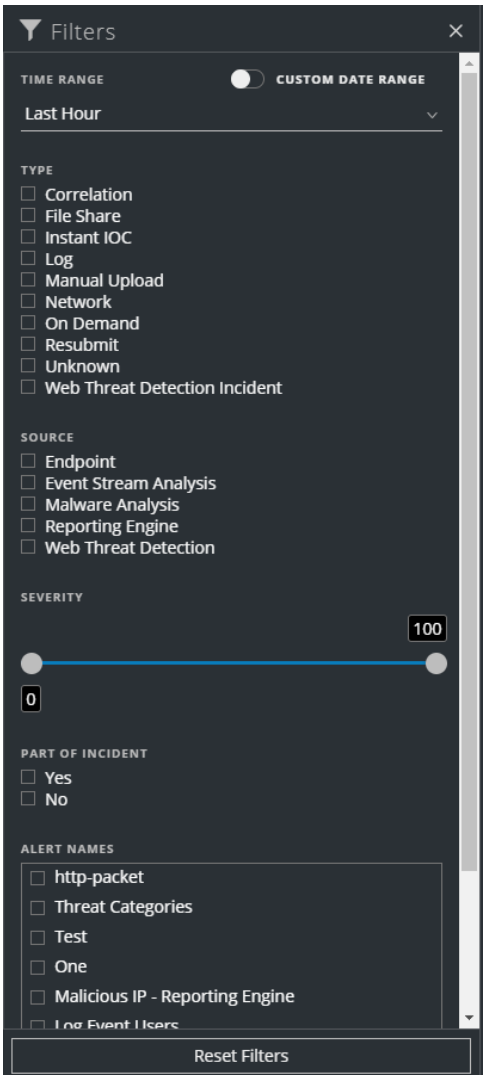
Columna	Descripción
RESUMEN DE HOST	Muestra detalles del host, como el nombre del host donde se activó la alerta. Los detalles pueden incluir información acerca de los hosts de origen y destino en una alerta. Algunas alertas pueden describir eventos en más de un host.
ID del incidente	Muestra el ID del incidente de la alerta. Si no hay un ID del incidente, la alerta no pertenece a ningún incidente y se puede crear uno para incluirla o se puede agregar a un incidente existente.

En la parte inferior de la lista, puede ver la cantidad de alertas que se muestran en la página actual y la cantidad total de alertas. Por ejemplo: **Mostrando 377 de 377 elementos**

Filtrar la Lista de alertas

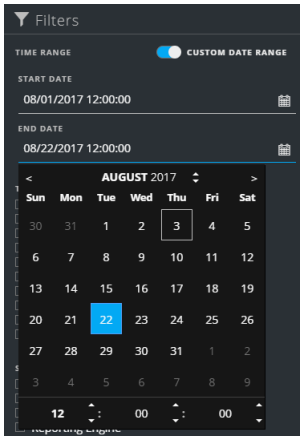
La cantidad de alertas en la Lista de alertas puede ser muy alta, lo que dificulta la localización de determinadas alertas. El filtro permite ver las alertas que desea ver, por ejemplo, las alertas de un origen específico, las alertas con una gravedad específica, las alertas que no forman parte de un incidente, etc.

1. Vaya a **RESPONDER > Alertas**.
   El panel Filtros aparece a la izquierda de la Lista de alertas. Si no ve el panel Filtros, en la barra de herramientas de la vista Lista de alertas, haga clic en para abrirlo.



2. En el panel Filtros, seleccione una o más opciones para filtrar la lista de alertas:
   - **RANGO DE TIEMPO**: Puede seleccionar un período específico en la lista desplegable Rango de tiempo. El rango de tiempo se basa en la fecha en que se recibieron las alertas. Por ejemplo, si selecciona Última hora, verá las alertas que se recibieron en los últimos 60 minutos.
   - **RANGO DE FECHAS PERSONALIZADO**: Puede especificar un rango de fechas determinado en lugar de seleccionar una opción de Rango de tiempo. Para ello, haga clic en el círculo blanco frente a RANGO DE FECHAS PERSONALIZADO para ver los campos Fecha de inicio y Fecha de finalización. Seleccione las fechas y las horas en el

calendario.



- **TIPO**: Seleccione el tipo de eventos en la alerta que desea ver, por ejemplo, registros, sesiones de red, etc.
- **ORIGEN**: Seleccione uno o más orígenes para ver las alertas que activaron los orígenes seleccionados. Por ejemplo, para ver solo las alertas de NetWitness Endpoint, seleccione Endpoint como el origen.
- **GRAVEDAD**: Seleccione el nivel de gravedad de las alertas que desea ver. Los valores son del 1 al 100. Por ejemplo, para concentrarse en las alertas con gravedad más alta en primer lugar, tal vez desee ver solo las alertas con una gravedad entre 90 y 100.
- **PARTE DE INCIDENTE**: Para ver solo las alertas que no forman parte de un incidente, seleccione **No**. Para ver solo las alertas que forman parte de un incidente, seleccione **Sí**. Por ejemplo, cuando esté listo para crear un incidente a partir de un grupo de alertas, puede seleccionar No con el fin de ver solo las alertas que no forman parte de ningún incidente en ese momento.
- **NOMBRES DE ALERTA**: Seleccione el nombre de la alerta que desea ver. Puede utilizar este filtro para buscar todas las alertas que genera una regla o un origen específicos, por ejemplo, IP maliciosa: Reporting Engine.

La Lista de alertas muestra las alertas que cumplen con los criterios de selección. Puede ver la cantidad de elementos de la lista filtrada en la parte inferior de la lista de alertas.
Por ejemplo: **Mostrando 30 de 30 elementos**

3. Si desea cerrar el panel Filtros, haga clic en **X**. Los filtros permanecen en su lugar hasta que los quita.

Quitar los filtros de la Lista de alertas

NetWitness Suite recuerda las selecciones de filtros en la vista Lista de alertas. Puede quitar las selecciones de filtros cuando ya no las necesite. Por ejemplo, si no ve la cantidad de alertas que espera o que desea ver, o desea ver todas las alertas en la lista de alertas, puede restablecer los filtros.

1. Vaya a **RESPONDER > Alertas**.

   El panel Filtros aparece a la izquierda de la lista de alertas. Si no ve el panel Filtros, en la barra de herramientas de la vista Lista de alertas, haga clic en ▼ para abrirlo.

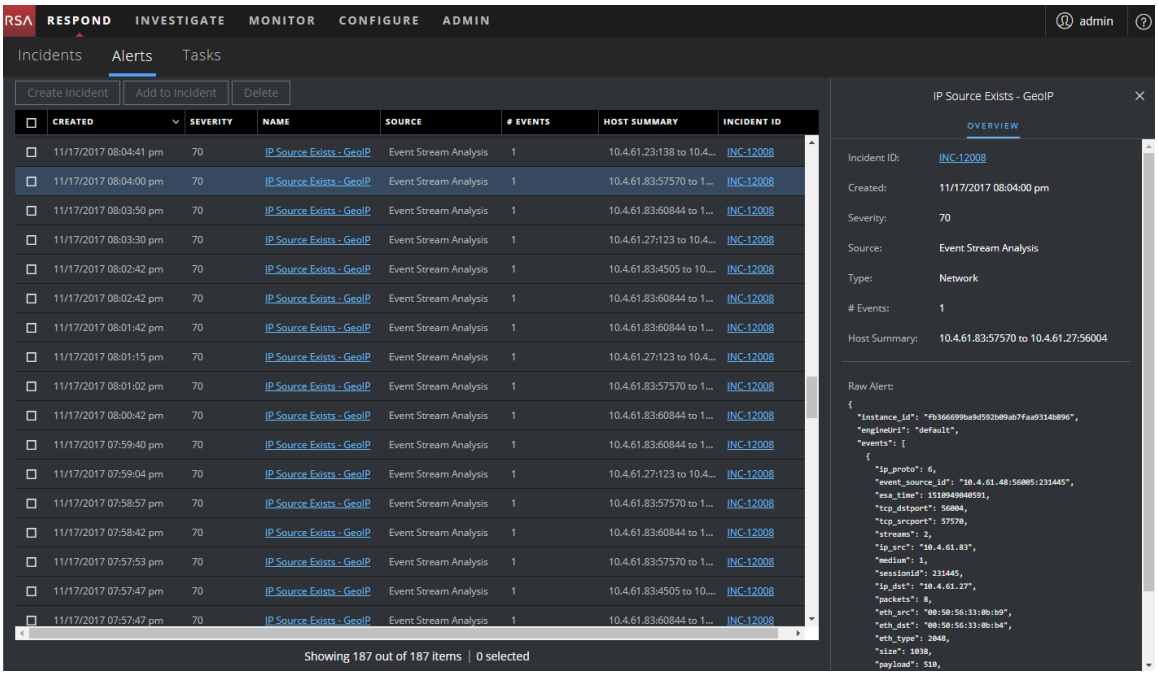
2. En la parte inferior del panel Filtros, haga clic en **Restablecer filtros**.

Ver información de resumen de las alertas

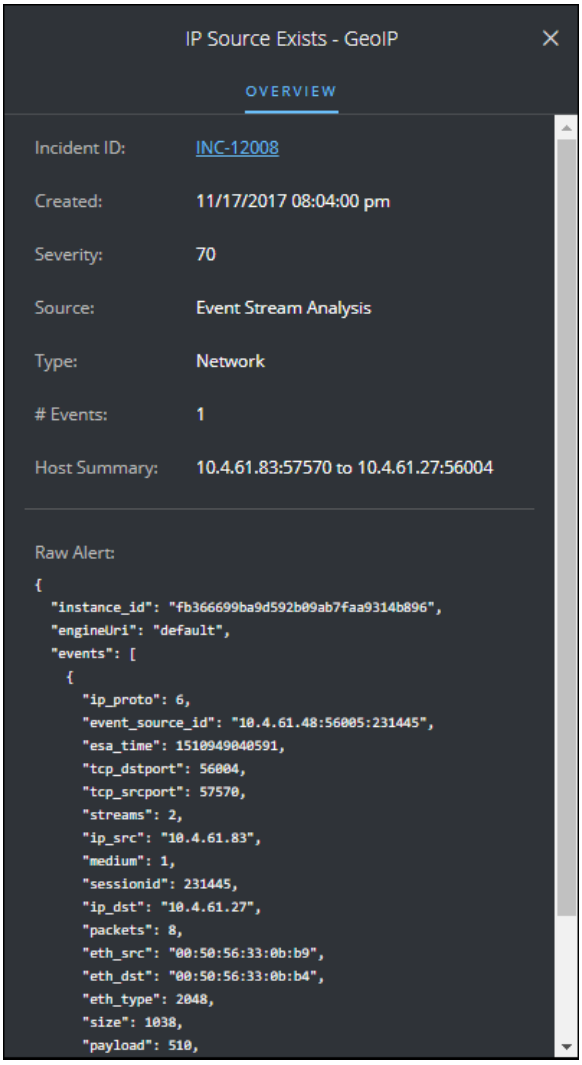
Además de ver la información básica acerca de una alerta, también puede ver los metadatos de la alerta cruda en el panel Descripción general.

1. En la Lista de alertas, haga clic en la alerta que desea ver.

   El panel Descripción general de la alerta aparece a la derecha de la Lista de alertas.

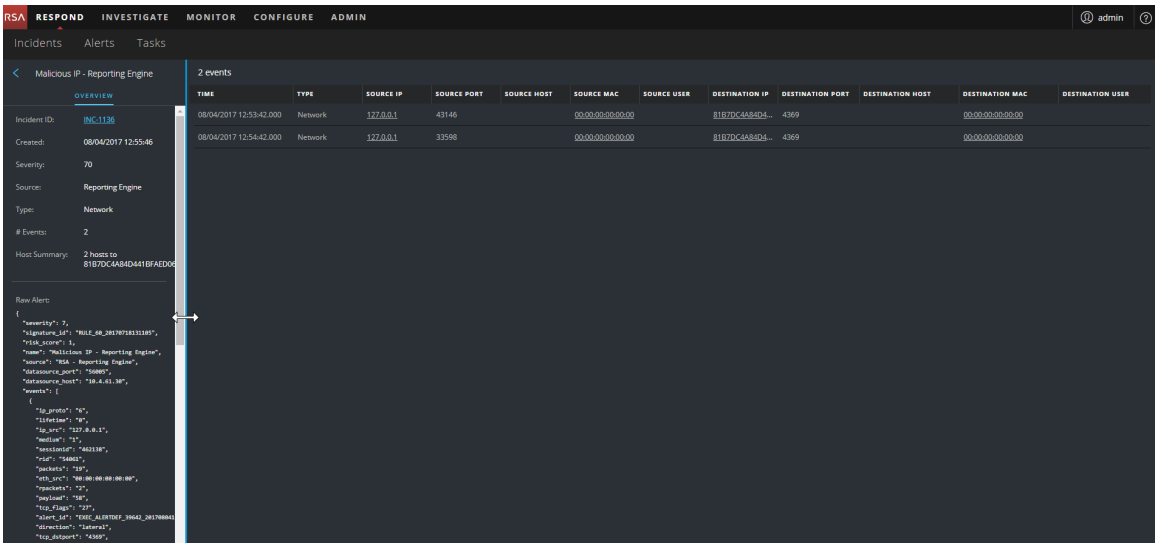


2. En la sección Alerta cruda, puede desplazarse para ver los metadatos de la alerta cruda.



Ver detalles de los eventos de una alerta

Una vez que revisa la información general acerca de la alerta en la vista Lista de alertas, puede ir a la vista Detalles de la alerta para obtener información más detallada con el fin de determinar la acción requerida. Una alerta contiene uno o más eventos. En la vista Detalles de la alerta, puede desglosar a una alerta para obtener detalles adicionales sobre el evento e investigar la alerta más a fondo. En la siguiente figura se muestra un ejemplo de la vista Detalles de la alerta.



El panel Descripción general de la izquierda tiene la misma información para una alerta que el panel Descripción general de la vista Lista de alertas.

El panel Eventos de la derecha muestra información acerca de los eventos, como la hora del evento, la dirección IP de origen, la dirección IP de destino, la dirección IP del detector, el usuario de origen, el usuario de destino e información de los archivos acerca de los eventos. La cantidad de información que se muestra depende del tipo de evento.

Hay dos tipos de eventos:

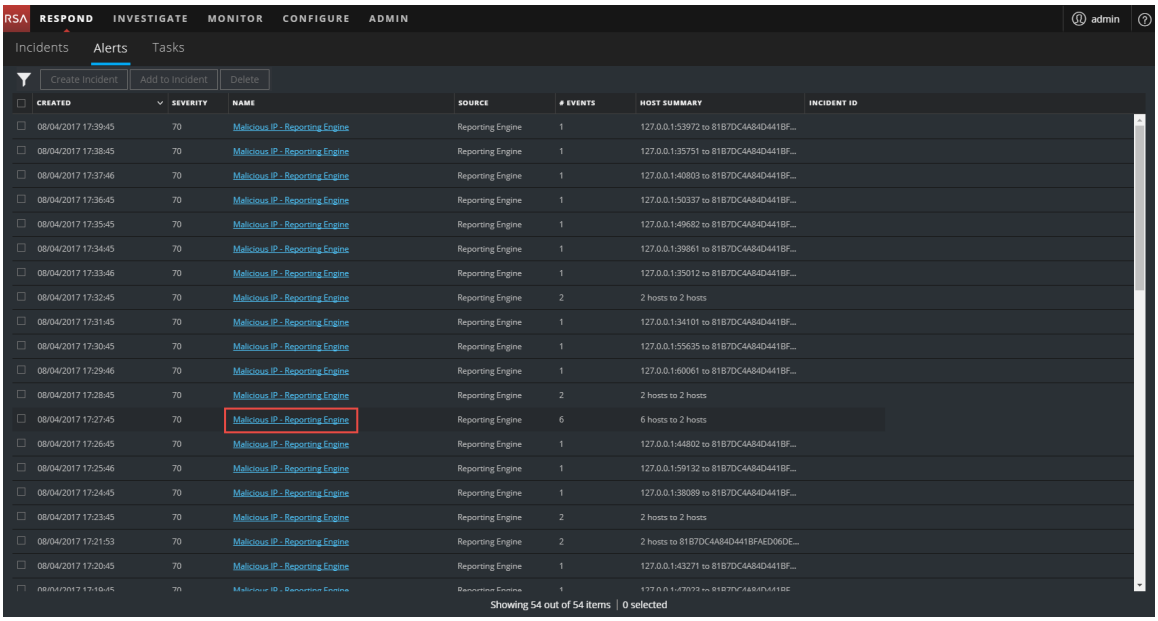
- Una transacción entre dos máquinas (un origen y un destino)
- Una anomalía detectada en una máquina (un detector)

Algunos eventos solo tendrán un detector. Por ejemplo, NetWitness Endpoint busca malware en una máquina. Otros eventos tendrán un origen y un destino. Por ejemplo, los datos de paquetes muestran la comunicación entre una máquina y un dominio de comando y control (C2).

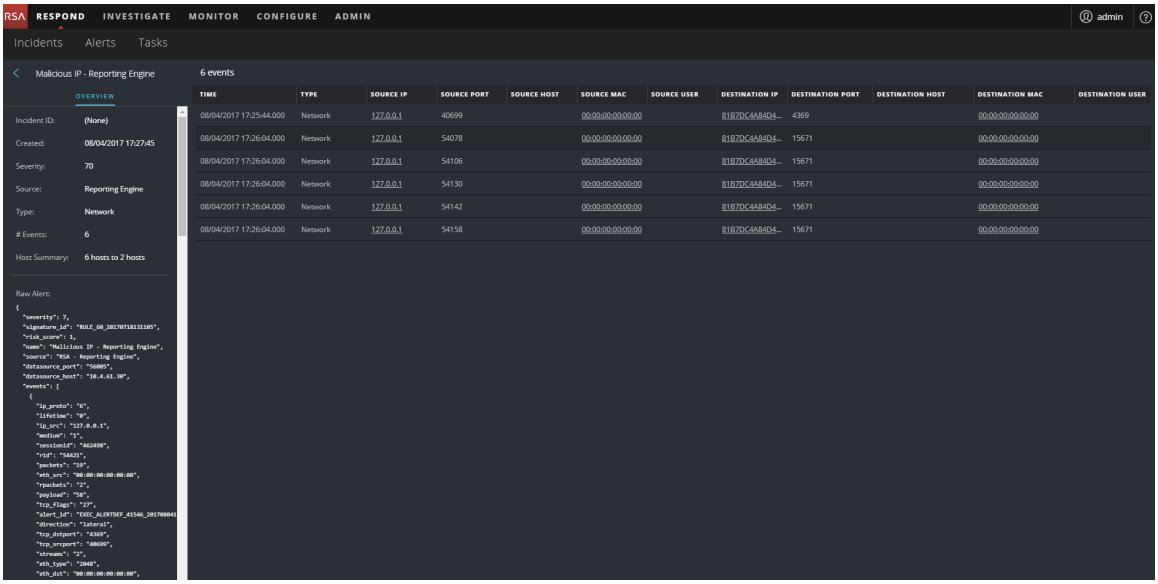
Puede desglosar aún más a un evento para obtener datos detallados acerca de este.

Para ver detalles de los eventos de una alerta:

1. Para ver los detalles de los eventos de una alerta, en la vista Lista de alertas, elija una alerta que desee ver y, a continuación, haga clic en el vínculo de la columna NOMBRE correspondiente a esa alerta.



La vista Detalles de la alerta muestra el panel Descripción general en el lado izquierdo y el panel Eventos en el lado derecho.



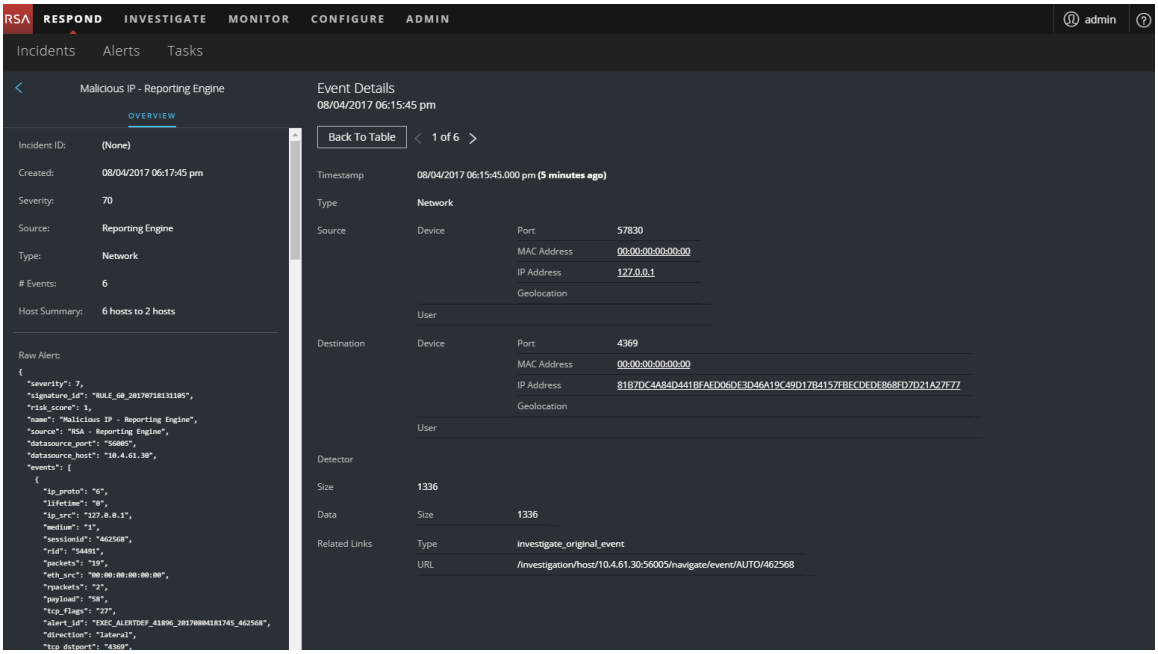
El panel Eventos muestra una lista de eventos con información acerca de cada uno de ellos. En la siguiente tabla se muestran algunas de las columnas que pueden aparecer en la Lista de eventos (tabla Eventos).

Columna	Descripción
TIEMPO	Muestra la hora en que se produjo el evento.
TIPO	Muestra el tipo de alerta, como Registro y Red.

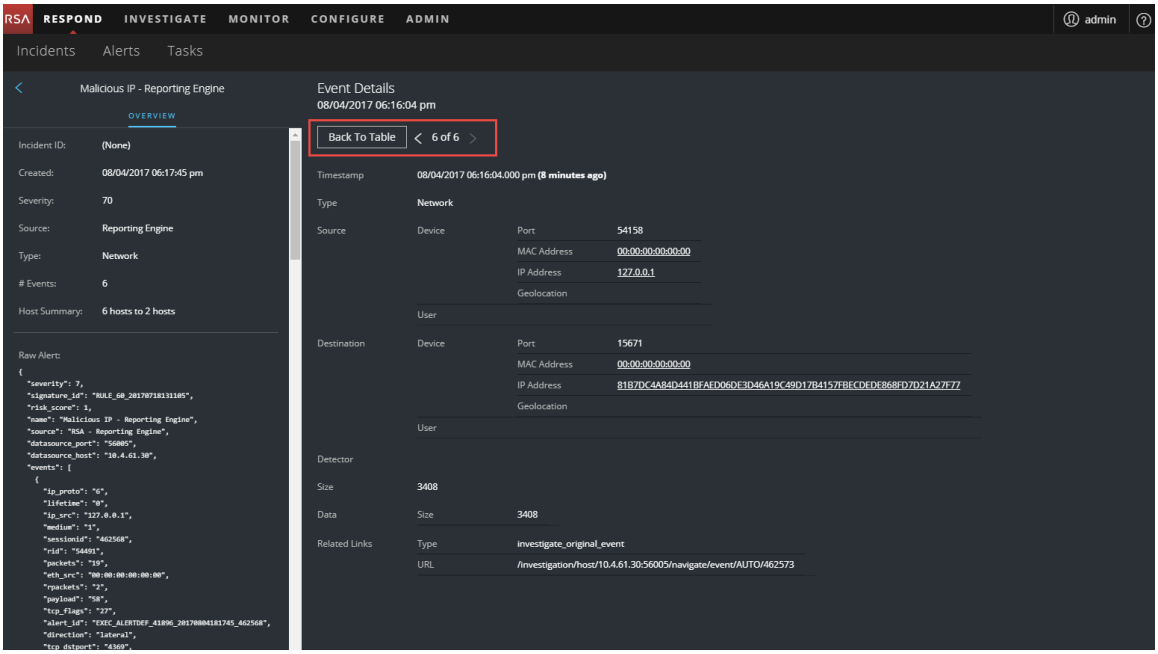
Columna	Descripción
DIRECCIÓN IP DE ORIGEN	Muestra la dirección IP de origen si hubo una transacción entre dos máquinas.
DIRECCIÓN IP DE DESTINO	Muestra la dirección IP de destino si hubo una transacción entre dos máquinas.
IP DE DETECTOR	Muestra la dirección IP de la máquina en la que se detectó una anomalía.
USUARIO DE ORIGEN	Muestra el usuario de la máquina de origen.
USUARIO DE DESTINO	Muestra el usuario de la máquina de destino.
NOMBRE DE ARCHIVO	Muestra el nombre del archivo, si hubo uno implicado en el evento.
HASH DE ARCHIVO	Muestra un hash del contenido del archivo.

Si solo hay un evento en la lista, verá los detalles de ese evento en lugar de una lista.

2. Haga clic en un evento de la Lista de eventos para ver sus detalles.
   En este ejemplo se muestran los detalles del primer evento de la lista.



3. Utilice la navegación de la página a la derecha del botón Volver a tabla para ver otros eventos. En este ejemplo se muestran los detalles del último evento de la lista.



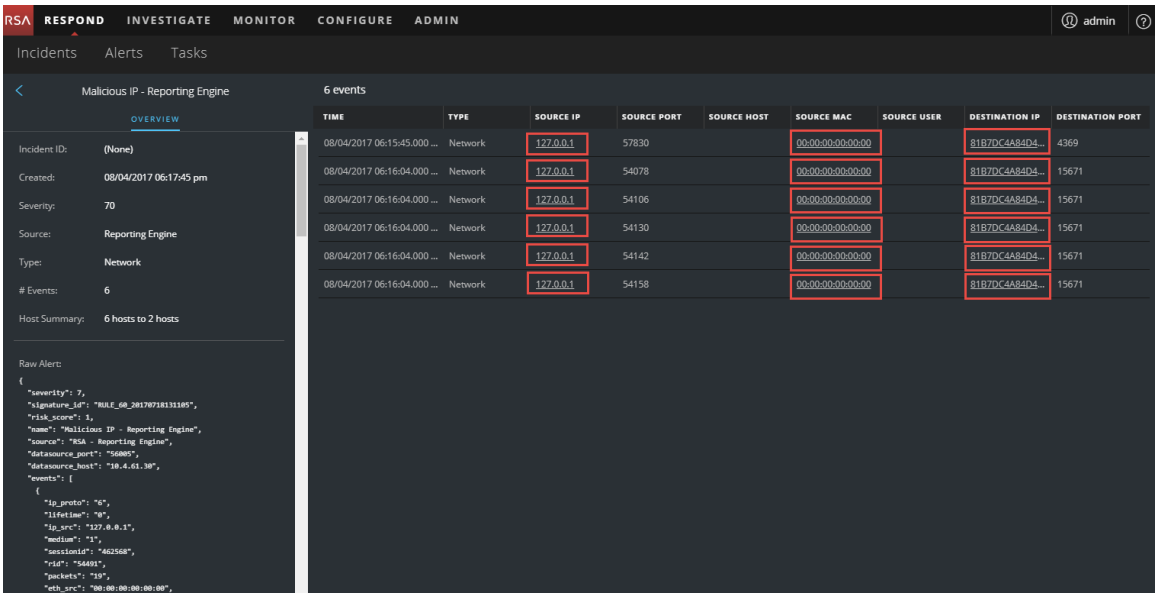
Consulte Vista Detalles de la alerta para obtener información detallada acerca de los datos de eventos que se enumeran en el panel Detalles de la alerta.

Investigar eventos

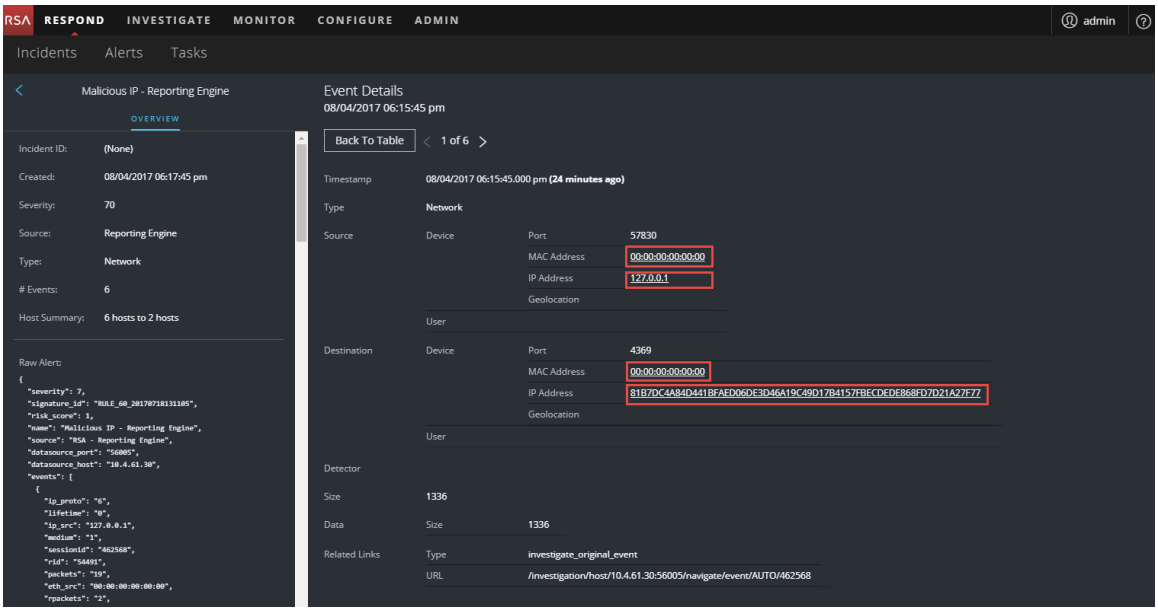
Para investigar más a fondo los eventos, puede encontrar vínculos que lo llevan a información contextual adicional. Desde allí, hay opciones disponibles según su selección.

Ver información contextual

En la vista Detalles de la alerta, puede ver entidades subrayadas en el panel Eventos. Una entidad subrayada se considera una entidad en Context Hub y tiene información contextual adicional disponible. En la siguiente figura se muestran entidades subrayadas en la Lista de eventos.



En la siguiente figura se muestran entidades subrayadas en Detalles de eventos.

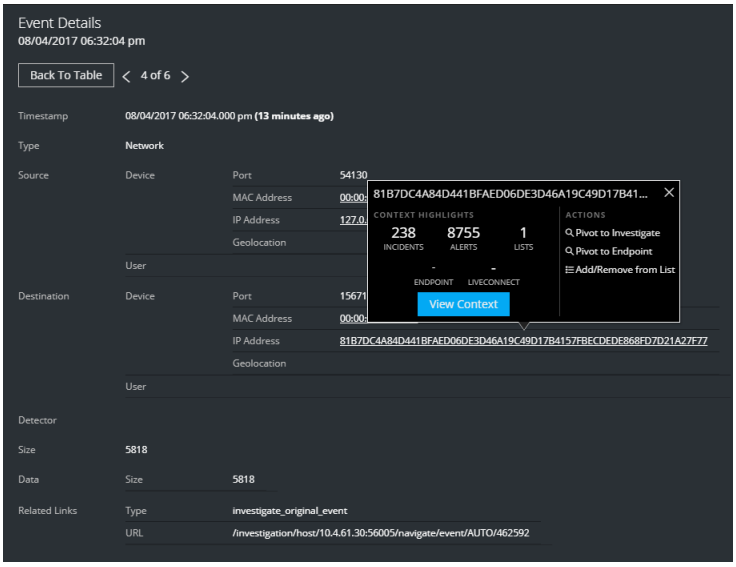


Context Hub está preconfigurado con campos de metadatos mapeados a las entidades. NetWitness Respond e Investigation usan estos mapeos predeterminados para la búsqueda de contexto. Para obtener información acerca de cómo agregar claves de metadatos, consulte "Configurar ajustes para un origen de datos" en la *Guía de configuración de Context Hub*.

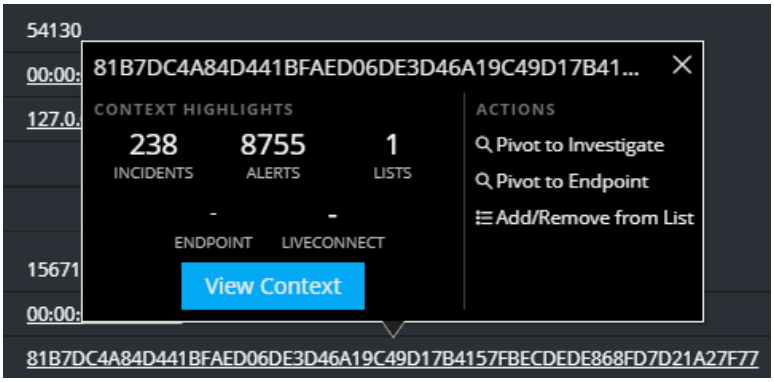
Precaución: Para que la búsqueda de contexto funcione de manera correcta en las vistas Respond e Investigate, al mapear claves de metadatos en la pestaña **ADMINISTRAR > SISTEMA > Investigaciones > Búsqueda de contexto**, RSA recomienda agregar únicamente claves de metadatos a los mapeos de claves de metadatos, no campos de MongoDB. Por ejemplo, ip.address es una clave de metadatos e ip_address no lo es (es un campo de MongoDB).

Para ver información contextual:

1. En Detalles de eventos o en la Lista de eventos de la vista Detalles de la alerta, coloque el cursor sobre una entidad subrayada.
   Aparece un mensaje de globo de contexto con un resumen rápido del tipo de datos de contexto que está disponible para la entidad seleccionada.



   El mensaje de globo de contexto tiene dos secciones: Puntos destacados de contexto y Acciones.



   La información de la sección **Puntos destacados de contexto** lo ayuda a determinar las acciones que desea realizar. Muestra la cantidad de alertas e incidentes relacionados. Según los datos, tal vez pueda hacer clic en estos elementos numerados para obtener más información. En el ejemplo anterior se muestran 238 incidentes relacionados, 8,755 alertas relacionadas y una lista relacionada de Context Hub.

   En la sección **Acciones** se enumeran las acciones disponibles. En el ejemplo anterior, están disponibles las opciones Cambiar a Investigate, Cambiar a Endpoint y Agregar/eliminar de la

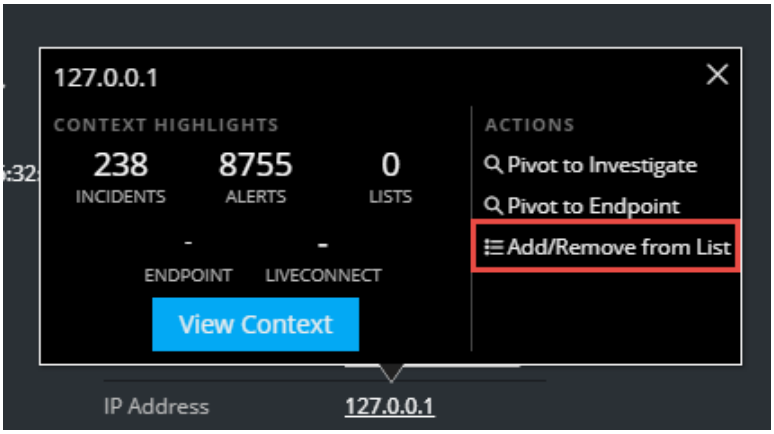
lista.

2. Para ver más detalles acerca de la entidad seleccionada, haga clic en el botón **Ver contexto**.
   Se abre el panel de contexto, el cual muestra toda la información relacionada con la entidad.
   El Panel Búsqueda de contexto: Vista Respond proporciona información adicional.

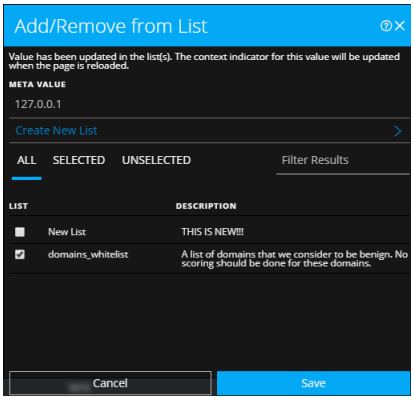
Agregar una entidad a una lista blanca

Puede agregar cualquier entidad subrayada a una lista, como una lista blanca o una lista negra, desde un mensaje de globo de contexto. Por ejemplo, para reducir los falsos positivos, tal vez desee incluir en la lista blanca un dominio subrayado con el fin de excluirlo de las entidades relacionadas.

1. En Detalles de eventos o en la Lista de eventos de la vista Detalles de la alerta, coloque el cursor sobre la entidad subrayada que desea agregar a una lista de Context Hub.
   Aparece un mensaje de globo de contexto que muestra las acciones disponibles.



2. En la sección **Acciones** del mensaje de globo, haga clic en **Agregar/eliminar de la lista**.
   El cuadro de diálogo Agregar/eliminar de la lista muestra las listas disponibles.



3. Seleccione una o más listas y haga clic en **Guardar**.
   La entidad aparece en las listas seleccionadas.
   El Cuadro de diálogo Agregar/eliminar de la lista proporciona información adicional.

Crear una lista blanca

Puede crear una lista blanca en Context Hub de la misma manera en que lo haría en la vista Detalles de incidente. Consulte Crear una lista.

Cambiar a NetWitness Endpoint

Si la aplicación del cliente grueso de NetWitness Endpoint está instalada, puede iniciarla mediante el mensaje de globo de contexto. Desde allí, puede investigar más a fondo una dirección IP, una dirección MAC o un host sospechosos.

1. En Detalles de eventos o en la Lista de eventos de la vista Detalles de la alerta, coloque el cursor sobre cualquier entidad subrayada para acceder al mensaje de globo de contexto.
2. En la sección **ACCIONES** del mensaje de globo, seleccione **Cambiar a Endpoint**.
   La aplicación del cliente grueso de NetWitness Endpoint se abre fuera del navegador web.

Para obtener más información sobre el cliente grueso, consulte la *Guía del usuario de NetWitness Endpoint*.

Cambiar a Investigation

Si desea realizar una investigación más completa del incidente, puede acceder a la vista Investigate.

1. En Detalles de eventos o en la Lista de eventos de la vista Detalles de la alerta, coloque el cursor sobre cualquier entidad subrayada para acceder al mensaje de globo de contexto.
2. En la sección **ACCIONES** del mensaje de globo, seleccione **Cambiar a Investigate**.
   Se abre la vista Navegar de Investigate, la que permite realizar una investigación más detallada.

Para obtener más información, consulte la *Guía del usuario de NetWitness Investigate*.

Crear un incidente manualmente

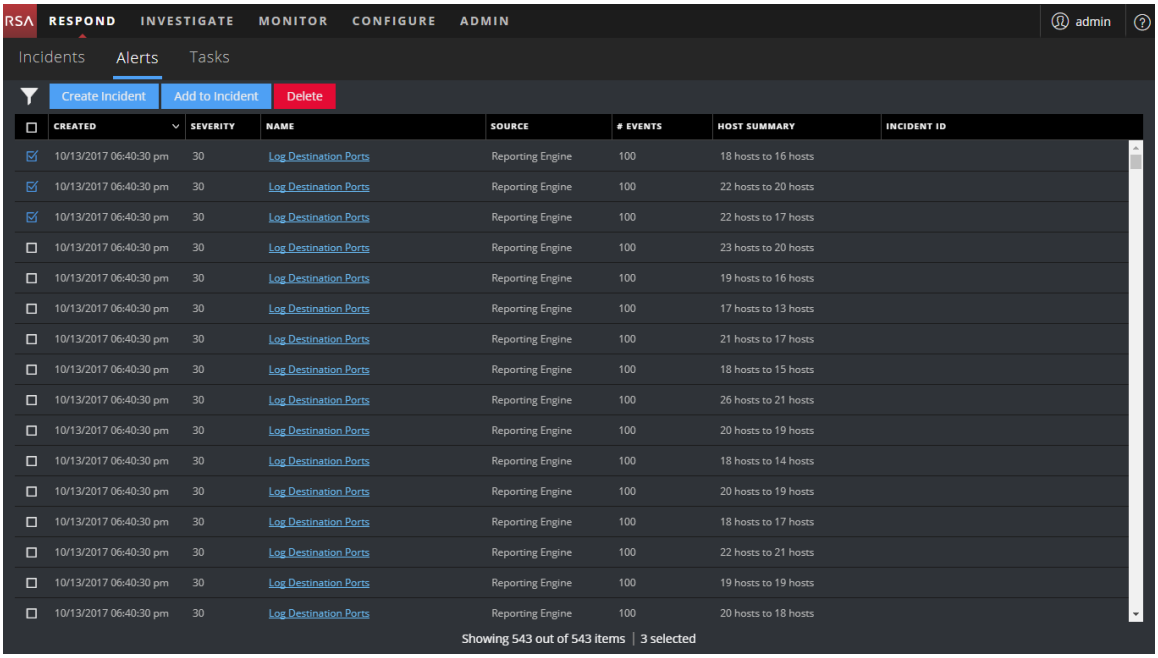
Puede crear incidentes manualmente a partir de alertas en la vista Lista de alertas. Las alertas que selecciona no pueden formar parte de otro incidente. Los incidentes que se crean manualmente a partir de alertas se configuran de manera predeterminada con prioridad Baja, pero puede cambiar la prioridad después de crearlos. No puede agregar categorías a los incidentes creados manualmente.

Nota: Los incidentes se pueden crear manual o automáticamente. Una alerta solo se puede asociar a un incidente. Puede crear reglas de incidentes para analizar las alertas recopiladas y agruparlas en incidentes en función de las reglas con las cuales coinciden. Para obtener detalles, consulte el tema "Crear una regla de incidentes para alertas" en la *Guía de configuración de NetWitness Respond.*

Para crear un incidente manualmente:

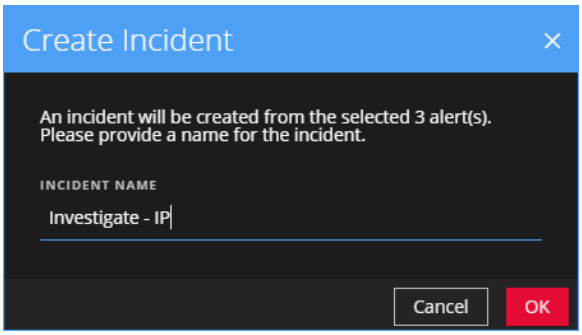
1. Vaya a **RESPONDER > Alertas**.
2. Seleccione una o más alertas en la Lista de alertas.

   Nota: La selección de alertas que no tienen ID de incidente habilita el botón **Crear incidente**. Si la alerta ya forma parte de un incidente, el botón está deshabilitado. Puede filtrar alertas que no forman parte de un incidente mediante la opción **PARTE DE INCIDENTE** configurada en **No** en el panel Filtros.

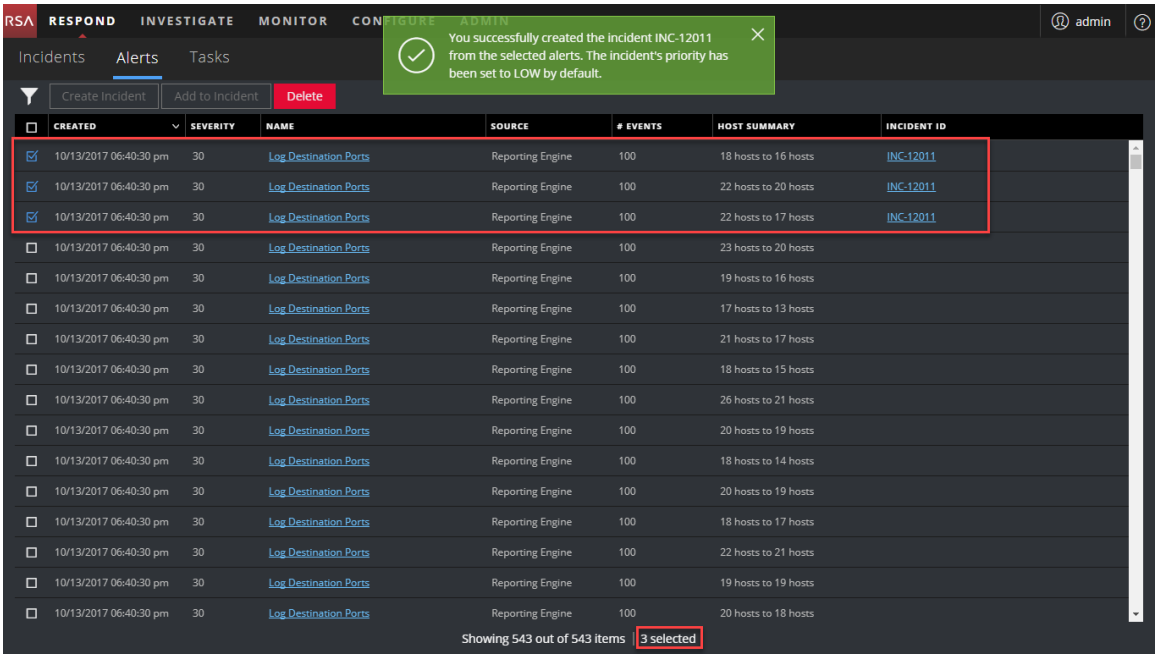


3. Haga clic en **Crear incidente**.

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



4. En el campo **NOMBRE DEL INCIDENTE**, escriba un nombre para identificar el incidente. Por ejemplo, Investigate - IP.
5. Haga clic en **Aceptar**.



.

Verá un mensaje de confirmación que indica que se creó un incidente a partir de las alertas seleccionadas. El nuevo ID de incidente aparece como un vínculo en la columna ID de incidente de las alertas seleccionadas. Si hace clic en el vínculo, se dirigirá a la vista Detalles de incidente correspondiente a este incidente, donde puede actualizar la información, como cambiar la prioridad de baja a alta.

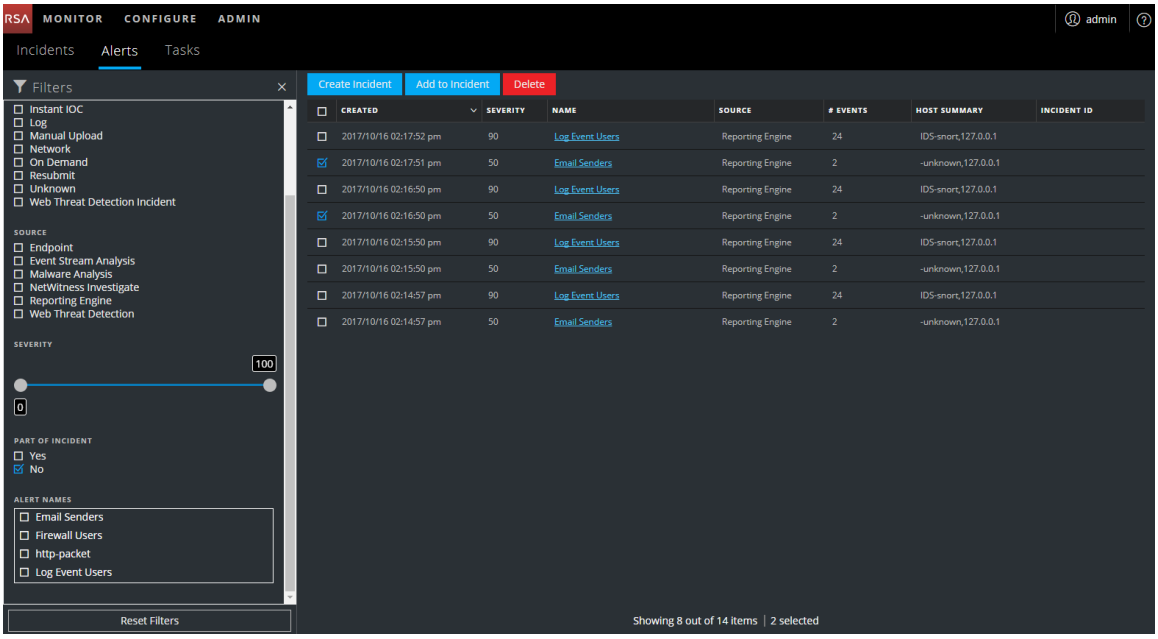
Agregar alertas a un incidente

Nota: Esta opción está disponible en la versión 11.1 y superior.

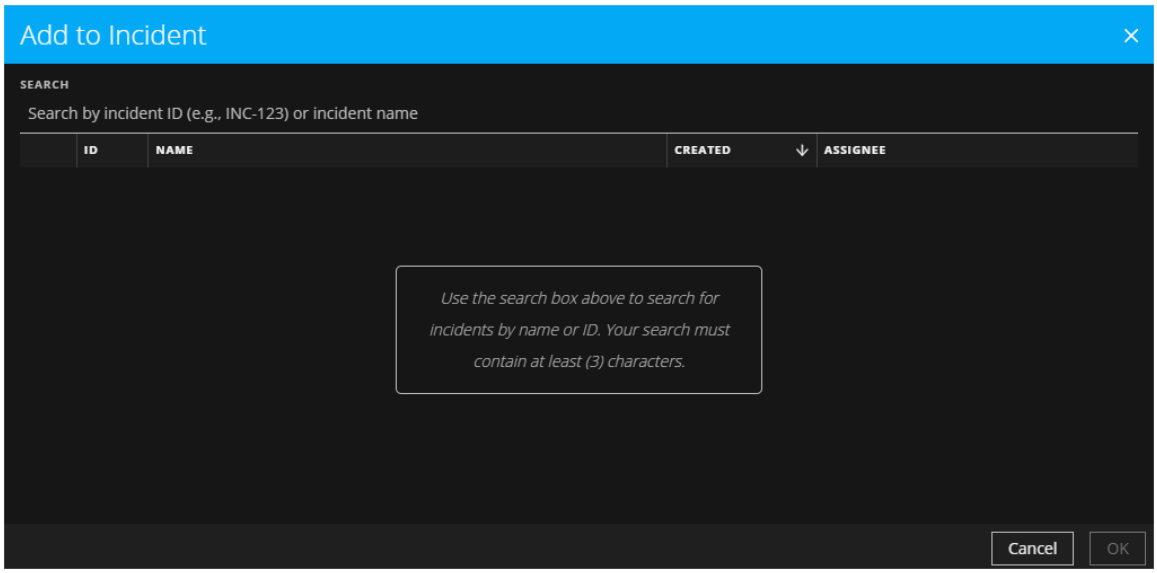
Si tiene alertas que se ajustan a un incidente existente específico, no necesita crear un incidente nuevo. En su lugar, puede agregar alertas a ese incidente desde la vista Lista de alertas. Las alertas que selecciona no pueden formar parte de otro incidente.

1. Vaya a **RESPONDER > Alertas**.
2. En la Lista de alertas, seleccione una o más alertas que desee agregar a un incidente y haga clic en **Agregar a incidente**.

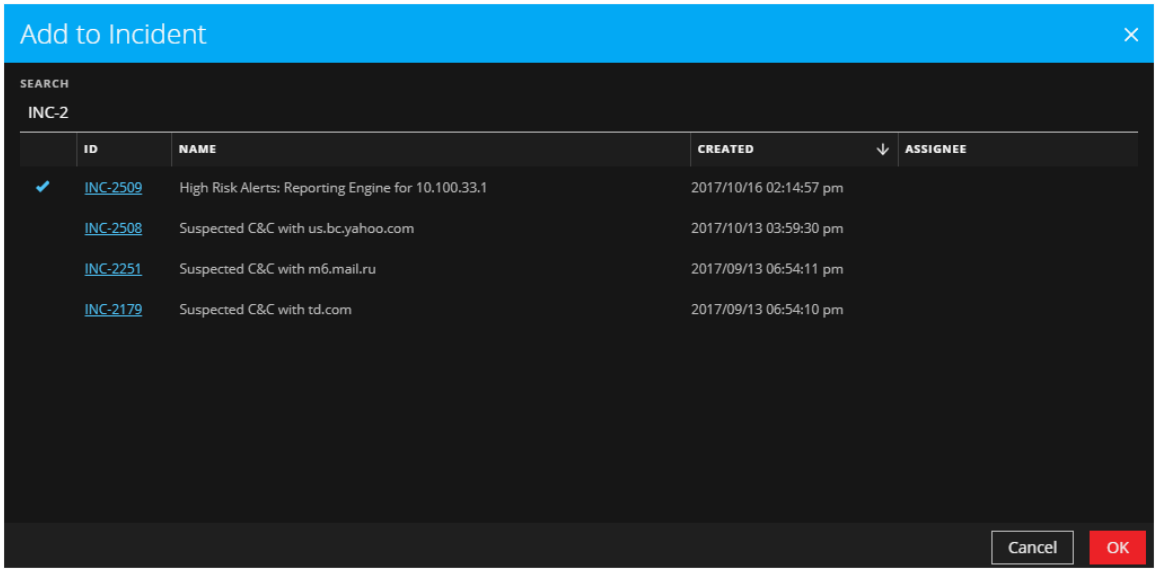
Nota: La selección de alertas que no tienen ID de incidente habilita el botón **Agregar a incidente**. Si la alerta ya forma parte de un incidente, el botón está deshabilitado. Puede filtrar alertas que no forman parte de un incidente mediante la opción **PARTE DE INCIDENTE** configurada en **No** en el panel Filtros.



3. En el cuadro de diálogo **Agregar a incidente**, escriba al menos tres caracteres en el campo **Buscar** para buscar el incidente por **Nombre** o **ID de incidente**.



4. En la lista de resultados, seleccione el incidente que recibirá las alertas seleccionadas y haga clic en **Aceptar**.

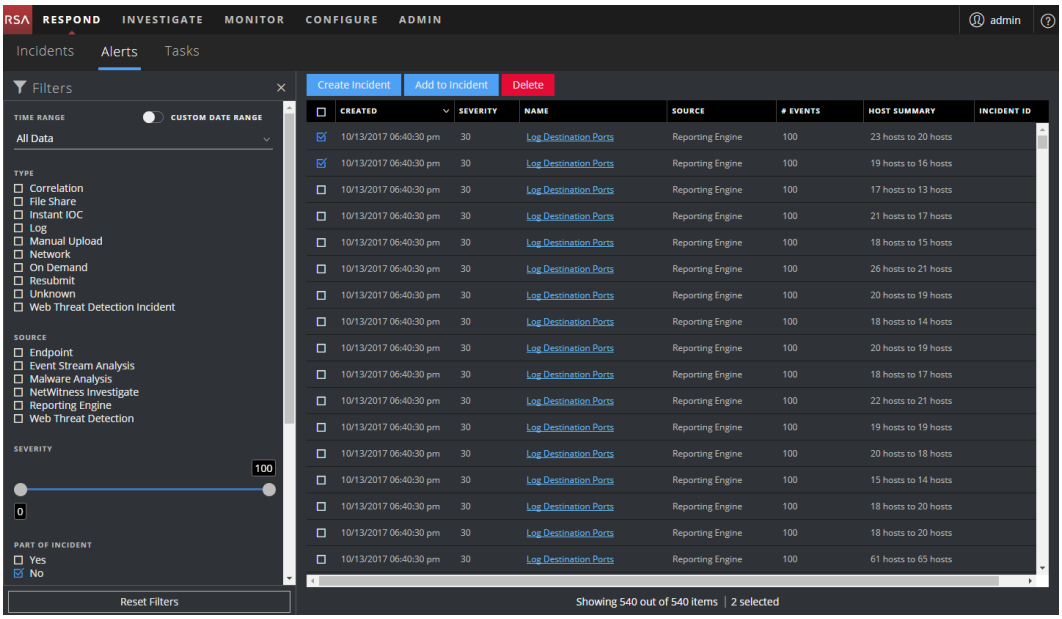


Una o más alertas seleccionadas son ahora parte del incidente elegido y tendrán un ID de incidente.

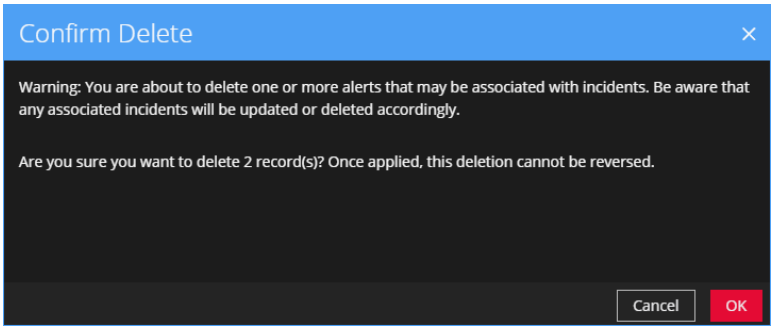
Eliminar alertas

Los usuarios con los permisos adecuados, como los administradores y los encargados de la privacidad de datos, pueden eliminar las alertas. Este procedimiento es útil cuando desea quitar alertas innecesarias o irrelevantes. La eliminación de estas alertas libera espacio en disco.

1. Vaya a **RESPONDER > Alertas**.
   La vista Lista de alertas muestra una lista de todas las aletas de NetWitness Suite.
2. En la Lista de alertas, seleccione las alertas que desea eliminar y haga clic en **Eliminar**.



   Si no tiene permiso para eliminar las alertas, no verá el botón Eliminar.
3. Confirme su intención de eliminar las alertas y haga clic en **Aceptar**.



   Las alertas se eliminan de NetWitness Suite. 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.

Información de referencia de NetWitness Respond

La interfaz del usuario de la vista Respond proporciona acceso a las funciones de NetWitness Respond. Este tema contiene descripciones de las interfaces del usuario, así como otra información de referencia para ayudar a los usuarios a comprender las funciones de NetWitness Respond.

Temas

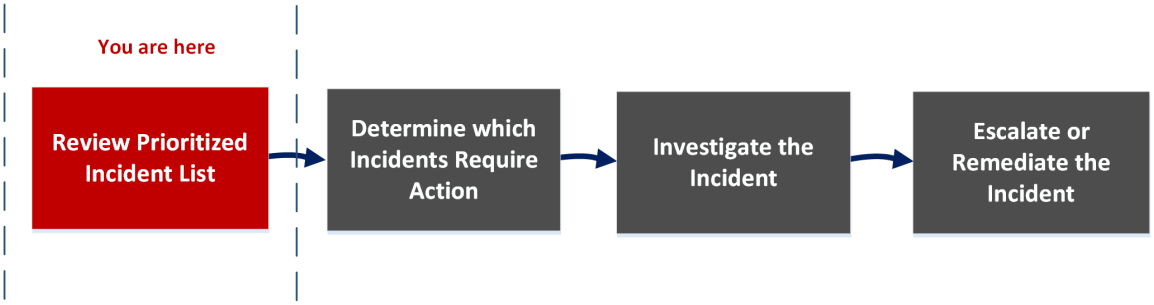
- Vista Lista de incidentes
- Vista Detalles de incidente
- Vista Lista de alertas
- Vista Detalles de la alerta
- Vista Lista de tareas
- Cuadro de diálogo Agregar/eliminar de la lista
- Panel Búsqueda de contexto: Vista Respond

Vista Lista de incidentes

La vista Lista de incidentes (RESPOND > Incidentes) muestra a los encargados de respuesta ante incidentes y a otros analistas una lista de resultados de incidentes creados a partir de diversos orígenes, la cual está ordenada según la prioridad. Por ejemplo, la lista de resultados podría mostrar incidentes creados a partir de reglas de ESA, NetWitness Endpoint o módulos de ESA Analytics para la Detección de amenazas automatizadas, como C2 para paquetes o registros. La vista Lista de incidentes ofrece un acceso sencillo a la información que necesita para realizar rápidamente tareas de triage y administración de los incidentes hasta su finalización.

Flujo de trabajo

En este flujo de trabajo se muestra el proceso general que usan los encargados de respuesta ante incidentes para responder ante incidentes en NetWitness Suite.



En la vista Lista de incidentes, puede revisar la lista de incidentes ordenados por prioridad, la que muestra información básica acerca de cada incidente. También puede cambiar el usuario asignado, la prioridad y el estado de los incidentes. Debido a la gran cantidad de resultados que puede haber en la lista de incidentes, tiene la opción de filtrar esos incidentes por rango de tiempo, ID de incidente, rango de fechas personalizado, prioridad, estado, usuario asignado y categorías.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Encargados de respuesta ante incidentes, analistas y administrador del SOC	Ver incidentes ordenados por prioridad*	Revisar la lista de incidentes ordenados por prioridad
Encargados de respuesta ante incidentes, analistas y administrador del SOC	Filtrar y ordenar la lista de incidentes*	Filtrar la Lista de incidentes
Encargados de respuesta ante incidentes, analistas	Ver mis incidentes*	Ver mis incidentes
Encargados de respuesta ante incidentes, analistas	Asignar los incidentes a uno mismo*	Asignar los incidentes a uno mismo
Encargados de respuesta ante incidentes, analistas y administrador del SOC	Buscar incidentes*	Buscar un incidente
Encargados de respuesta ante incidentes, analistas y administrador del SOC	Actualizar un incidente.*	Elevar o corregir el incidente
Encargados de respuesta ante incidentes, analistas	Ver detalles de incidentes.	Ermitteln, welche Incidents eine Aktion erfordern
Encargados de respuesta ante incidentes, analistas	Investigar un incidente más a fondo.	Investigar el incidente
Encargados de respuesta ante incidentes, analistas y administrador del SOC	Crear una tarea.	Elevar o corregir el incidente

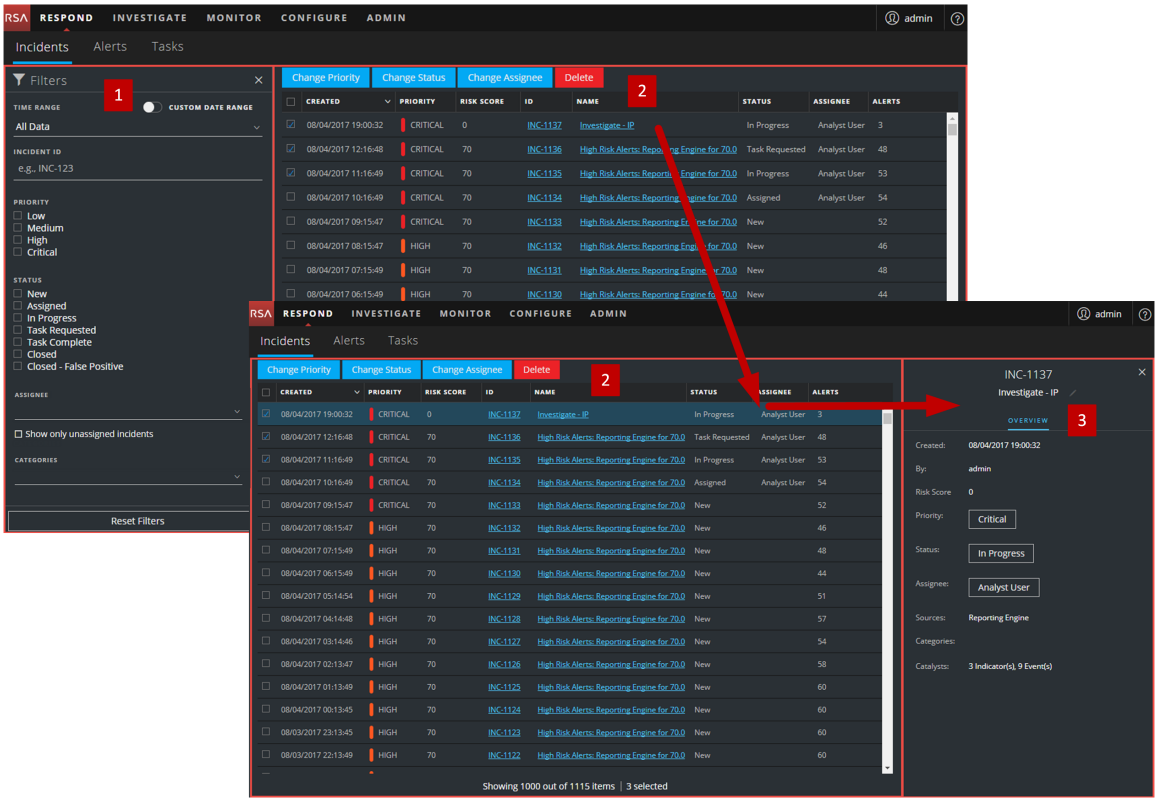
*Puede realizar estas tareas aquí (es decir, en la vista Lista de incidentes).

Temas relacionados

- Vista Detalles de incidente
- Respuesta ante incidentes

Vista rápida

En el siguiente ejemplo se muestra la vista Lista de incidentes inicial con el panel Filtro. Puede abrir el panel Descripción general para un incidente si hace clic en un incidente en la Lista de incidentes.



1 Panel Filtros

2 Lista de incidentes

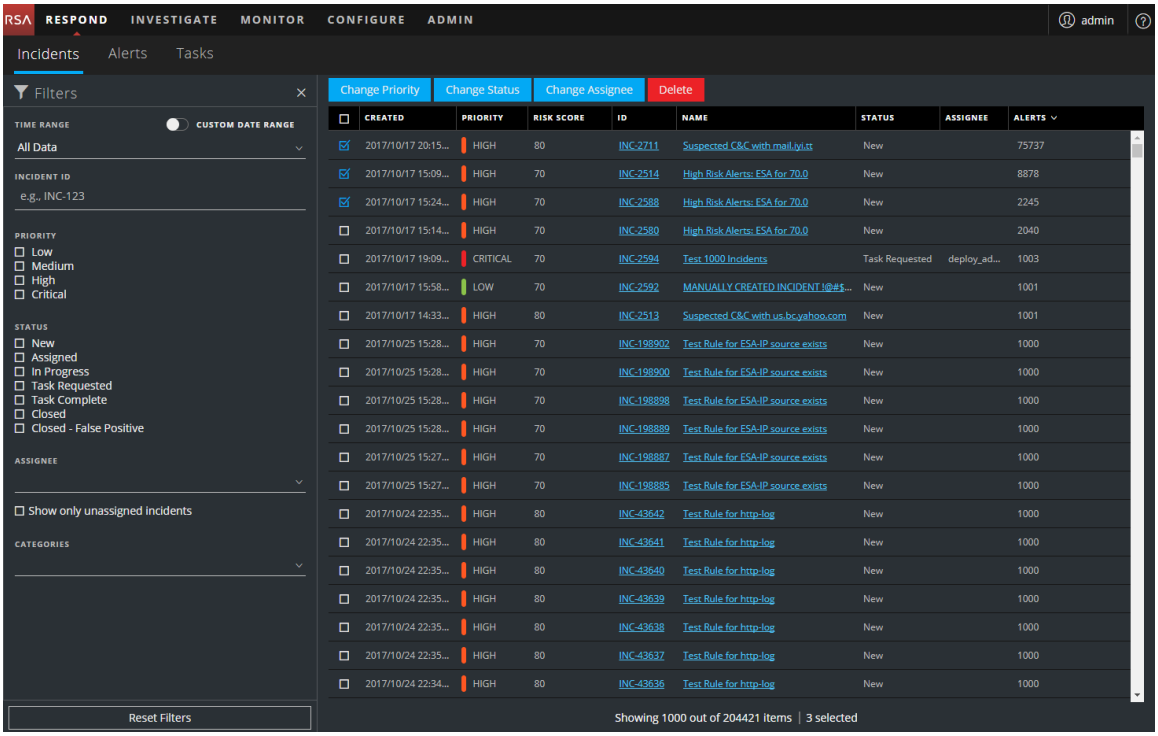
3 Panel Descripción general

Puede ir directamente a la vista Detalles de incidente desde la Lista de incidentes si hace clic en el ID o el NOMBRE con hipervínculo. El panel Descripción general también está disponible en la vista Detalles de incidente. Para obtener más información acerca de la vista Detalles de incidente, consulte Vista Detalles de incidente.

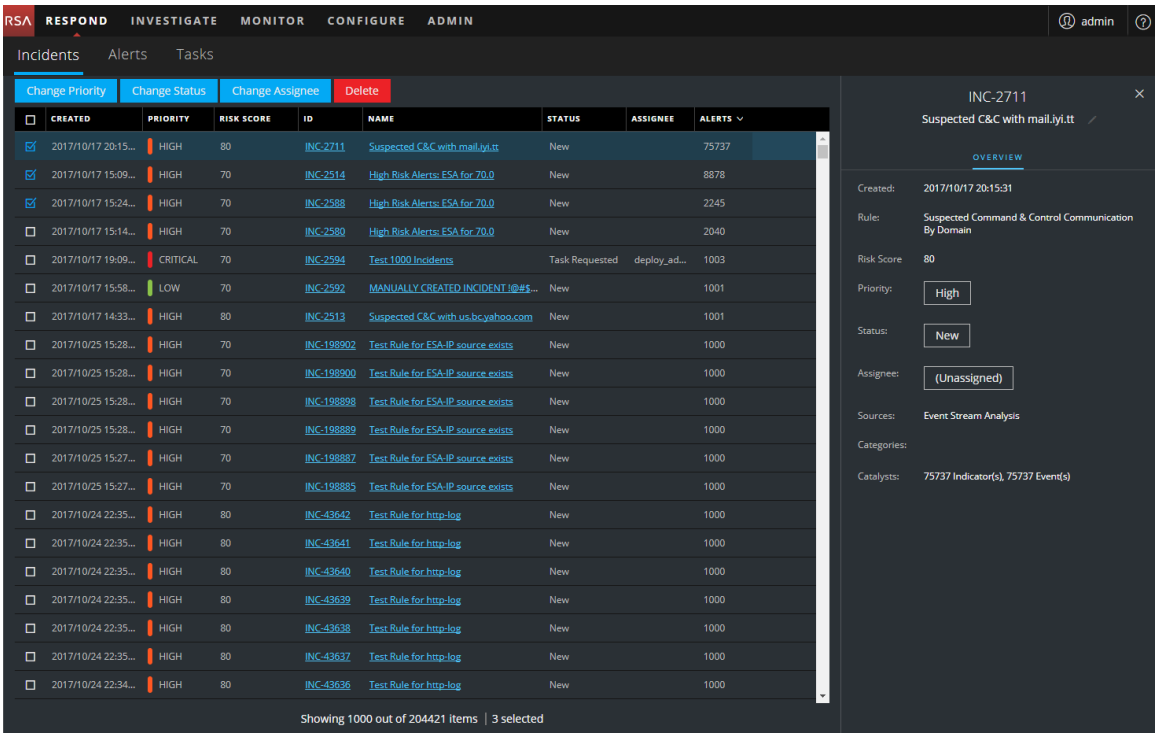
Vista Lista de incidentes

Para acceder a la vista Lista de incidentes, vaya a **RESPONDER > Incidentes**. La vista Lista de incidentes muestra una lista de todos los incidentes. La vista Lista de incidentes consta de un panel Filtros, una Lista de incidentes y un panel Descripción general de incidentes.

En la siguiente figura se muestra el panel Filtro a la izquierda y la Lista de incidentes a la derecha.

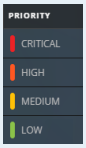


En la siguiente figura se muestra la Lista de incidentes a la izquierda y el panel Descripción general de incidentes a la derecha.



Lista de incidentes

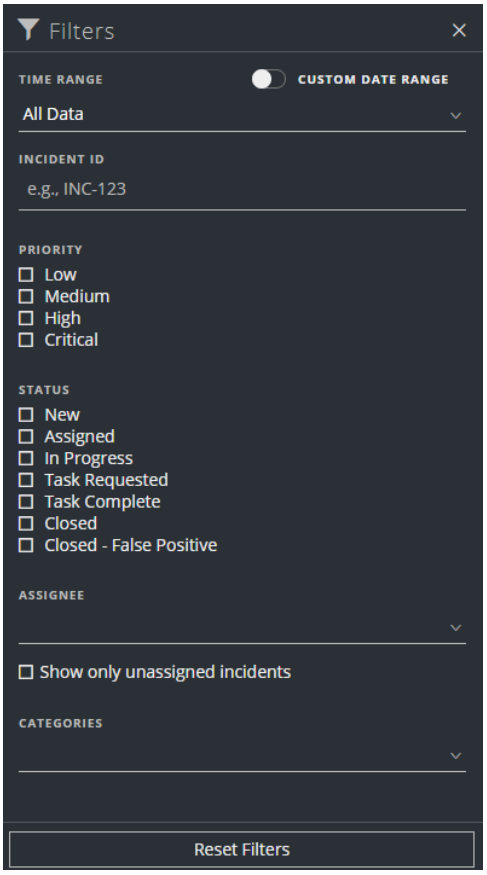
La Lista de incidentes muestra una lista de todos los incidentes ordenados por prioridad. Puede filtrar esta lista para mostrar solo los incidentes de interés.

Columna	Descripción
CREADO	Muestra la fecha de creación del incidente.
PRIORIDAD	Muestra la prioridad del incidente. La prioridad puede ser Crítica, Alta, Media o Baja. La prioridad está codificada en colores. El rojo indica un incidente con prioridad **Crítica**, el naranja, uno con riesgo de prioridad **Alta**, el amarillo, **Media** y el verde, **Baja**. Por ejemplo: 
PUNTAJE DE RIESGO	Muestra el puntaje de riesgo del incidente. El puntaje de riesgo indica el riesgo del incidente que se calcula por medio de un algoritmo y que está entre 0 y 100. 100 es el puntaje de riesgo más alto.
ID	Muestra el número de incidente creado automáticamente. A cada incidente se le asigna un número único que puede utilizar para rastrearlo.
NAME	Muestra el nombre del incidente. El nombre del incidente proviene de la regla que se usa para activar el incidente. Haga clic en el vínculo para ir a la vista Detalles de incidente del incidente seleccionado.
ESTADO	Muestra el estado del incidente. El estado puede ser: Nuevo, Asignado, En curso, Tarea solicitada, Tarea completa, Cerrado y Cerrado: falso positivo.
USUARIO ASIGNADO	Muestra el miembro del equipo que está asignado al incidente.
ALERTAS	Muestra la cantidad de alertas asociadas con el incidente. Un incidente puede incluir muchas alertas. Una gran cantidad de alertas puede significar que se experimenta un ataque a gran escala.

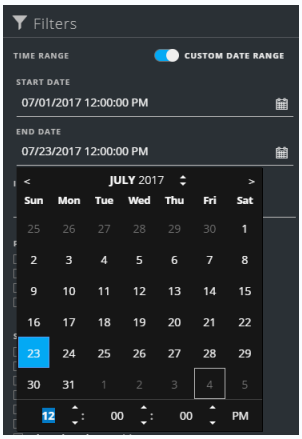
En la parte inferior de la lista, puede ver la cantidad de incidentes que se muestran en la página actual, la cantidad total de incidentes y la cantidad de incidentes seleccionados. Por ejemplo: **Mostrando 1,000 de 2,517 elementos | 2 seleccionado(s)**. La cantidad máxima de incidentes que se pueden ver al mismo tiempo es 1,000.

Panel Filtros

En la siguiente figura se muestran los filtros disponibles en el panel Filtros.



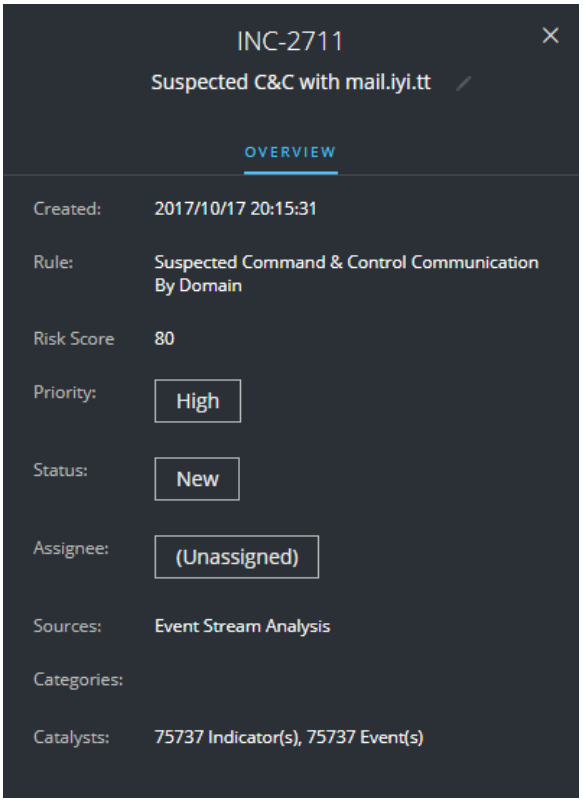
El panel Filtros, a la izquierda de la vista Lista de incidentes, tiene opciones que puede usar para filtrar la lista de incidentes. Cuando sale del panel Filtros, la vista Lista de incidentes conserva sus selecciones de filtros.

Opción	Descripción
RANGO DE TIEMPO	Puede seleccionar un período específico en la lista desplegable Rango de tiempo. El rango de tiempo se basa en la fecha de recepción de las alertas. Por ejemplo, si selecciona Última hora, verá las alertas que se recibieron en los últimos 60 minutos.
RANGO DE FECHAS PERSONALIZADO	Puede especificar un rango de fechas determinado en lugar de seleccionar una opción de Rango de tiempo. Para ello, haga clic en el círculo blanco frente a Rango de fechas personalizado para ver los campos Fecha de inicio y Fecha de finalización. Seleccione las fechas y las horas en el calendario. 
ID del incidente	Puede escribir el ID de un incidente que desea localizar, por ejemplo, INC-1050.
PRIORIDAD	Seleccione las prioridades que desea ver.
ESTADO	Seleccione uno o más estados de incidentes. Por ejemplo, seleccione Cerrado: falso positivo para ver solo los incidentes que son falsos positivos, los cuales se identificaron inicialmente como sospechosos, pero después se determinó que eran seguros.

Opción	Descripción
USUARIO ASIGNADO	Seleccione el usuario o los usuarios asignados de los incidentes que desea ver. Por ejemplo, si solo desea ver los incidentes asignados a Cale o Stanley, seleccione Cale y Stanley en la lista desplegable Usuario asignado. Si desea ver los incidentes sin tener en cuenta el usuario asignado, no realice ninguna selección en Usuario asignado. (Disponible en la versión 11.1 y superior) Para ver solamente los incidentes sin asignar, seleccione **Mostrar solo los incidentes sin asignar**.
CATEGORÍAS	Seleccione una o más categorías en la lista desplegable. Por ejemplo, si solo desea ver incidentes clasificados con las categorías de abuso Backdoor o Privilegio, seleccione abuso de Backdoor y Privilegio.
Restablecer filtros	Quita las selecciones de filtros.

Panel Descripción general

El panel Descripción general muestra información de resumen básica acerca de un incidente seleccionado. En la Lista de incidentes, puede hacer clic en un incidente para acceder al panel Descripción general. El panel Descripción general de la vista Detalles de incidente contiene la misma información.



En la siguiente tabla se indican los campos que se muestran en el panel Descripción general de incidentes.

Campo	Descripción
<ID del incidente>	Muestra el ID del incidente.
<Nombre del incidente>	Muestra el nombre del incidente. Puede hacer clic en el nombre del incidente para cambiarlo. Por ejemplo, las reglas pueden crear muchos incidentes con el mismo nombre. Puede cambiar los nombres de los incidentes de modo que sean más específicos.
Creado	Muestra la fecha y la hora de creación del incidente.
Regla/Por	Muestra el nombre de la regla o de la persona que creó el incidente.
Puntaje de riesgo	Indica el riesgo del incidente que se calcula por medio de un algoritmo y que está entre 0 y 100. 100 es el puntaje de riesgo más alto.
Prioridad	Muestra la prioridad del incidente. La prioridad puede ser Crítica, Alta, Media o Baja. Para cambiar la prioridad, puede hacer clic en el botón Prioridad y seleccionar una prioridad nueva en la lista desplegable.
Estado	Muestra el estado del incidente. El estado puede ser Nuevo, Asignado, En curso, Tarea solicitada, Tarea completa, Cerrado y Cerrado: falso positivo. Para cambiar el estado, puede hacer clic en el botón Estado y seleccionar un estado nuevo en la lista desplegable.
Usuario asignado	Muestra el miembro del equipo que está asignado al incidente. Para cambiar el usuario asignado, puede hacer clic en el botón Usuario asignado y seleccionar un usuario asignado nuevo en la lista desplegable.

Campo	Descripción
Orígenes	Muestra los orígenes de datos que se utilizan para localizar la actividad sospechosa.
Categorías	Muestra las categorías de los eventos del incidente.
Catalizadores	Muestra el conteo de indicadores que dieron lugar al incidente.

Acciones de la barra de herramientas

En esta tabla se enumeran las acciones de la barra de herramientas disponibles en la vista Lista de incidentes.

Opción	Descripción
	Permite abrir el panel Filtros, de modo que pueda especificar las alertas que desearía ver en la Lista de alertas.
	Cierra el panel.
Botón **Cambiar prioridad**	Permite cambiar la prioridad de uno o más incidentes seleccionados en la Lista de incidentes.
Botón **Cambiar estado**	Permite cambiar el estado de uno o más incidentes seleccionados.
Botón **Cambiar usuario asignado**	Permite cambiar el usuario asignado de uno o más incidentes seleccionados.
Botón **Eliminar**	Permite eliminar los incidentes seleccionados si tiene los permisos adecuados, por ejemplo, un administrador o un encargado de la privacidad de datos.

Vista Detalles de incidente

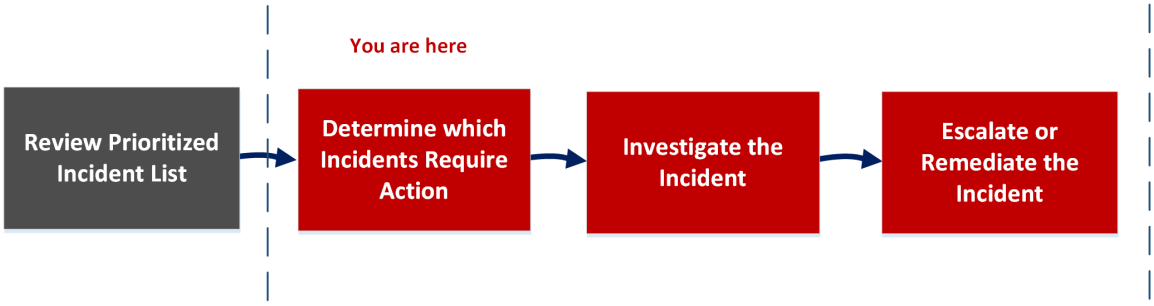
La vista Detalles de incidente (RESPOND > Incidentes > haga clic en un hipervínculo de ID o NOMBRE en la Lista de incidentes) permite ver y acceder a amplios detalles de los incidentes. La vista Detalles de incidente contiene varios paneles que proporcionan los siguientes beneficios:

- **Descripción general**: Vea un resumen del incidente y actualícelo.
- **Indicadores**: Vea los indicadores (alertas) involucrados en el incidente, los eventos dentro de esas alertas e información de enriquecimiento disponible.
- **Gráfico de nodos**: Visualice el tamaño y las interacciones entre las entidades (dirección IP, dirección MAC, usuario, host, dominio, nombre de archivo o hash de archivo).
- **Hoja de datos Eventos**: Estudie los eventos asociados con el incidente.
- **Registro**: Agregue notas y colabore con otros analistas.
- **Tareas**: Cree tareas de incidentes y rastréelas hasta su cierre.
- **Indicadores relacionados**: Vea los indicadores (alertas) que se relacionan con el incidente y agréguelos al incidente sin no están asociadas con uno.

También puede filtrar los datos en la vista Detalles de incidente para estudiar indicadores y entidades de interés.

Flujo de trabajo

En este flujo de trabajo se muestra el proceso general que usan los encargados de respuesta ante incidentes para responder ante incidentes en NetWitness Suite.



En la vista Detalles de incidente, puede usar la amplia información que se proporciona acerca de los incidentes para determinar los incidentes que requieren una acción. También dispone de herramientas e información para investigar el incidente y, a continuación, elevarlo o corregirlo.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Encargados de respuesta ante incidentes, analistas y administrador del SOC	Ver los incidentes a los cuales se les dio prioridad, filtrar y ordenar la lista de incidentes, buscar incidentes, ver mis incidentes y asignar incidentes a uno mismo.	Revisar la lista de incidentes ordenados por prioridad
Encargados de respuesta ante incidentes, analistas	Ver detalles de incidentes.*	Ver detalles de incidentes
Encargados de respuesta ante incidentes, analistas	Ver alertas y enriquecimientos.*	Ver los indicadores y los enriquecimientos
Encargados de respuesta ante incidentes, analistas	Ver eventos.*	Ver y estudiar los eventos
Encargados de respuesta ante incidentes, analistas	Ver un gráfico de las entidades involucradas en los eventos.*	Ver y estudiar las entidades involucradas en los eventos
Encargados de respuesta ante incidentes, analistas	Filtrar los datos de los incidentes.*	Filtrar los datos en la vista Detalles de incidente
Encargados de respuesta ante incidentes, analistas	Ver y agregar notas sobre los incidentes.*	Ver notas sobre los incidentes y Documentar los pasos realizados fuera de NetWitness
Encargados de respuesta ante incidentes, analistas	Ver y crear tareas.*	Ver las tareas asociadas a un incidente y Crear una tarea
Encargados de respuesta ante incidentes, analistas	Agregar alertas relacionadas y agregarlas al incidente.*	Buscar indicadores relacionados y Agregar indicadores relacionados al incidente

Función	Deseo…	Mostrarme cómo
Encargados de respuesta ante incidentes, analistas	Ver información contextual acerca de un incidente desde Context Hub.*	Ver información contextual
Encargados de respuesta ante incidentes, analistas	Reducir los falsos positivos mediante la adición de una entidad a la lista blanca.*	Agregar una entidad a una lista blanca
Encargados de respuesta ante incidentes, analistas	Cambiar a Investigation.*	Cambiar a Investigate
Encargados de respuesta ante incidentes, analistas	Cambiar a NetWitness Endpoint.*	Cambiar a NetWitness Endpoint
Encargados de respuesta ante incidentes, analistas	Actualizar o cerrar un incidente.*	Actualizar un incidente y Cerrar un incidente
Encargados de respuesta ante incidentes, analistas y administrador del SOC	Ver todas las tareas.	Elevar o corregir el incidente
Encargados de respuesta ante incidentes, analistas y administrador del SOC	Actualizar incidentes y tareas de manera masiva.	Elevar o corregir el incidente

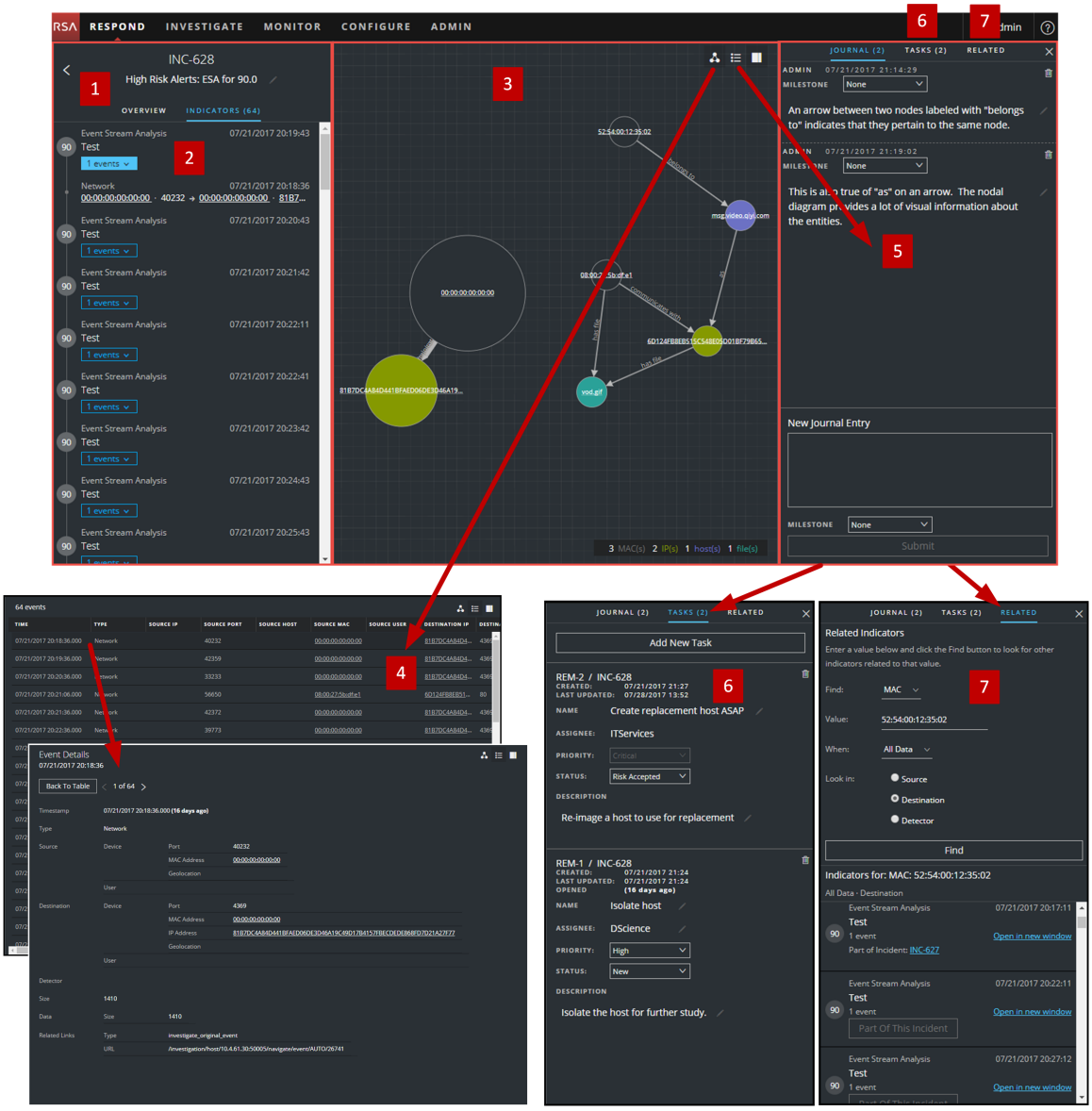
*Puede realizar estas tareas aquí (es decir, en la vista Detalles de incidente).

Temas relacionados

- Vista Lista de incidentes
- Ermitteln, welche Incidents eine Aktion erfordern
- Investigar el incidente
- Elevar o corregir el incidente

Vista rápida

En el siguiente ejemplo se muestran las ubicaciones de los paneles de la vista Detalles de incidente.

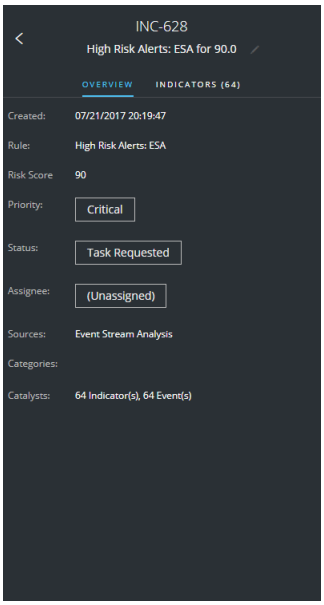


1	Panel Descripción general (haga clic en la pestaña DESCRIPCIÓN GENERAL para verlo).
2	Panel Indicadores
3	Gráfico de nodos
4	Hoja de datos Eventos (haga clic en un evento de la Lista de eventos para ver Detalles de

	eventos).
5	Panel Registro
6	Panel Tareas (haga clic en la pestaña TAREAS para verla).
7	Panel Indicadores relacionados (haga clic en la pestaña RELACIONADO para verla).

Panel Descripción general

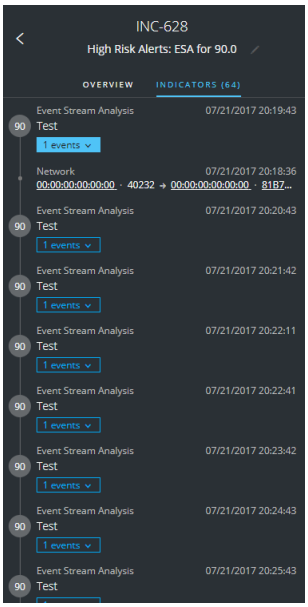
El panel Descripción general muestra información de resumen básica acerca de un incidente seleccionado. También permite cambiar el nombre del incidente y actualizar la prioridad, el estado y el usuario asignado del incidente. El panel Descripción general de la vista Lista de incidentes contiene la misma información. En el tema Panel Descripción general de la vista Lista de incidentes se proporcionan detalles.



Panel Indicadores

El panel Indicadores contiene una lista cronológica de indicadores. Los *indicadores* son alertas, como una alerta de ESA o una alerta de NetWitness Endpoint. (Esto difiere de un cronograma, el cual proporciona una representación visual de los tiempos de los eventos en el incidente). Esta lista permite conectar indicadores con datos relevantes. Por ejemplo, una dirección IP conectada a una alerta de ESA de comando y comunicación también podría haber activado una alerta de NetWitness Endpoint u otras actividades sospechosas.

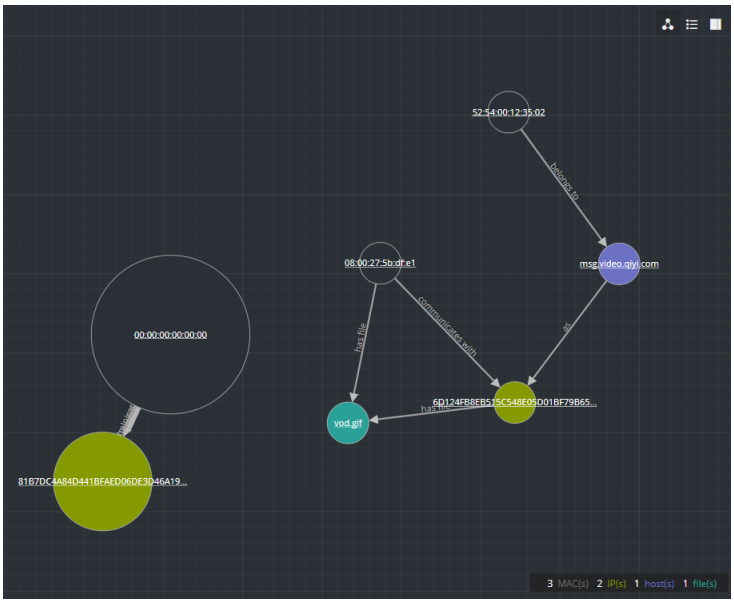
Para ver el panel Indicadores, en el panel izquierdo de la vista Detalles de incidente, seleccione **INDICADORES**.



La información del origen de datos se muestra debajo de los nombres de los indicadores. También puede ver la fecha y la hora de creación del indicador y la cantidad de eventos que incluye.

Gráfico de nodos

El gráfico de nodos es un gráfico interactivo que muestra las entidades involucradas en el incidente. Una *entidad* es un elemento de metadatos especificado, como una dirección IP, una dirección MAC, un usuario, un host, un dominio, un nombre de archivo o un hash de archivo.



Nodos

En el gráfico de nodos, los círculos representan nodos. En la siguiente tabla se describen los tipos de nodo del gráfico de nodos.

Nodo	Descripción
Dirección IP	Si el evento es una anomalía detectada, puede ver una dirección IP del detector. Si el evento es una transacción, puede ver una dirección IP de destino y una dirección IP de origen.
Dirección MAC	Puede ver una dirección MAC para cada tipo de dirección IP.
Usuario	Si la máquina está asociada a un usuario, puede ver un nodo de usuario.
Host	Un host puede ser un equipo físico o una máquina virtual, designados con un nombre de dominio calificado o una dirección IP, en los cuales están instalados los servicios.
Dominio	
Nombre del archivo	Si el evento implica archivos, puede ver un nombre de archivo.
Hash de archivo	Si el evento implica archivos, puede ver un hash de archivo.

La leyenda en la parte inferior del gráfico de nodos muestra la cantidad de nodos de cada tipo y la codificación en colores de los nodos. También ayuda a localizar las entidades cuando se aplica hash a los valores, como las direcciones IP.

Puede hacer clic en cualquier nodo y arrastrarlo para cambiar su ubicación.

Flechas

Las flechas entre los nodos ofrecen información adicional acerca de las relaciones entre las entidades. En la siguiente tabla se describen los tipos de flecha del gráfico de nodos.

Flecha	Descripción
Se comunica con	Una flecha entre un nodo de máquina de origen (dirección IP o dirección MAC) y un nodo de máquina de destino etiquetada con “Se comunica con” muestra la dirección de la comunicación.

Flecha	Descripción
Como	Una flecha entre los nodos etiquetada con “Como” proporciona información adicional sobre la dirección IP que señala la flecha. Por ejemplo, si hay una flecha desde el círculo del nodo de host que señala a un nodo de dirección IP, la cual está etiquetada con “Como”, esta indica que el nombre en el círculo del nodo de host es el nombre de host de esa dirección IP y no una entidad distinta.
Tiene archivo	Una flecha entre un nodo de máquina (dirección IP, dirección MAC o host) y un nodo de hash de archivo etiquetada con “Tiene” indica que la dirección IP tiene ese archivo.
Usa	Una flecha entre un nodo de usuario y un nodo de máquina (dirección IP, dirección MAC o host) etiquetada con “Usos” muestra la máquina que utilizó el usuario durante el evento.
Se denomina	Una flecha desde un nodo de hash de archivo a un nodo de nombre de archivo etiquetada con “Se denomina” indica que el hash de archivo corresponde a un archivo con ese nombre.
Pertenece a	Una flecha entre dos nodos etiquetada con “Pertenece a” indica que se relaciona con el mismo nodo. Por ejemplo, una flecha entre una dirección MAC y un host etiquetada “Pertenece a” indica que es la dirección MAC del host.

Las flechas con mayores tamaños de línea indican que hay más comunicación entre los nodos. Los nodos (círculos) más grandes indican mayor actividad en comparación con los nodos más pequeños. Los nodos de mayor tamaño son las entidades más comunes que se mencionan en los eventos.

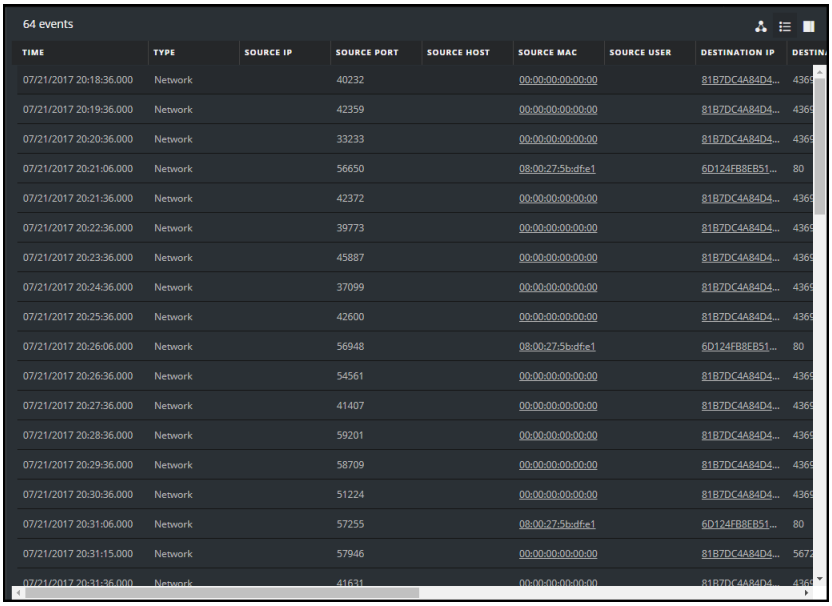
Hoja de datos Eventos

La hoja de datos Eventos muestra los eventos asociados con el incidente. Muestra información acerca de los eventos, como la hora del evento, la dirección IP de origen, la dirección IP de destino, la dirección IP del detector, el usuario de origen, el usuario de destino e información de los archivos acerca de los eventos. La cantidad de información que se muestra depende del tipo de evento.

La hoja de datos Eventos muestra una Lista de eventos para varios eventos o Detalles de eventos para un único evento.

Lista de eventos

En la siguiente figura se muestra la Lista de eventos.



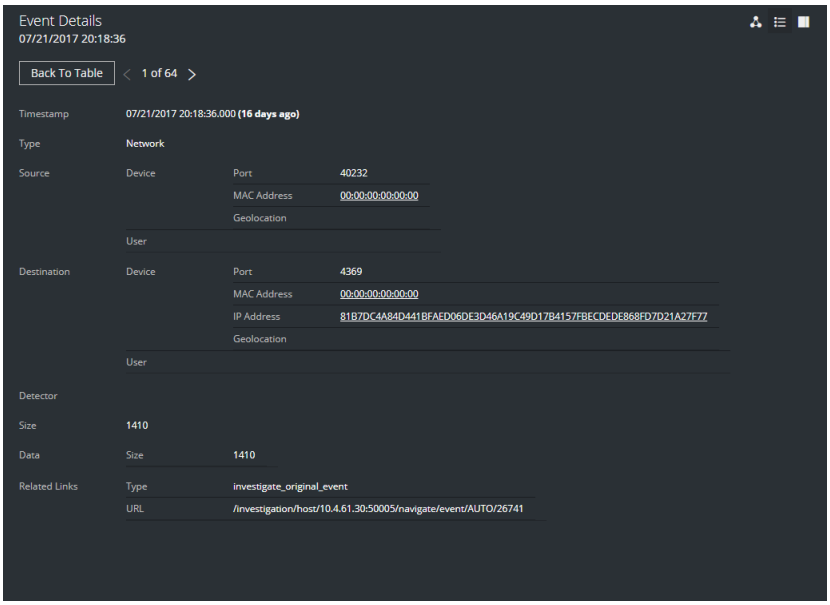
En la siguiente tabla se describen las columnas de la Lista de eventos.

Columna	Descripción
TIEMPO	Muestra la hora en que se produjo el evento.
TIPO	Muestra el tipo de alerta, como Registro y Red.
DIRECCIÓN IP DE ORIGEN	Muestra la dirección IP de origen si hubo una transacción entre dos máquinas.
PUERTO DE ORIGEN	Muestra el puerto de origen de la transacción. Los puertos de origen y destino pueden estar en la misma dirección IP.
HOST DE ORIGEN	Muestra el host de destino donde se produjo el evento.
MAC DE ORIGEN	Muestra la dirección MAC de la máquina de origen.
USUARIO DE ORIGEN	Muestra el usuario de la máquina de origen.

Columna	Descripción
DIRECCIÓN IP DE DESTINO	Muestra la dirección IP de destino si hubo una transacción entre dos máquinas.
PUERTO DE DESTINO	Muestra el puerto de destino de la transacción. Los puertos de origen y destino pueden estar en la misma dirección IP.
HOST DE DESTINO	Muestra el nombre del HOST de la máquina de destino.
MAC DE DESTINO	Muestra la dirección MAC de la máquina de destino.
USUARIO DE DESTINO	Muestra el usuario de la máquina de destino.
IP DE DETECTOR	Muestra la dirección IP de la máquina en la que se detectó una anomalía.
NOMBRE DE ARCHIVO	Muestra el nombre del archivo, si hubo uno implicado en el evento.
HASH DE ARCHIVO	Muestra un hash del contenido del archivo.

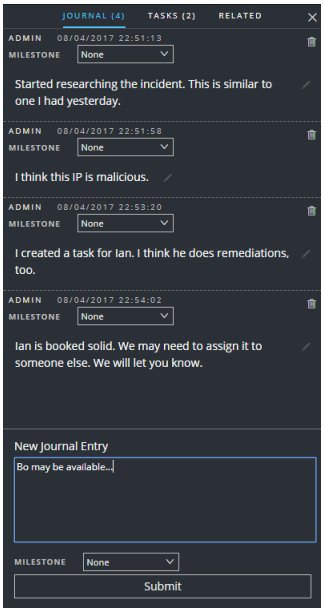
Detalles de eventos

Para ver los detalles del evento, haga clic en un evento en la lista de eventos. Si solo hay un evento en la lista, verá los detalles de ese evento en lugar de una lista.



Panel Registro

El registro del incidente muestra el historial de actividad en un incidente.



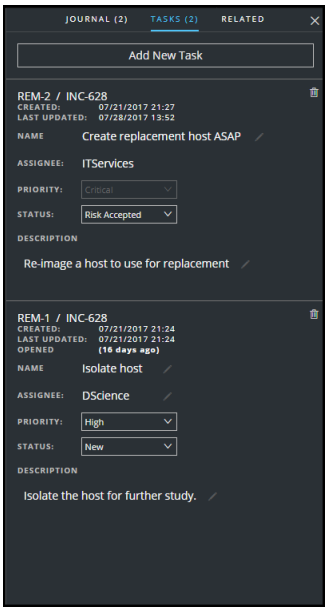
En la siguiente tabla se describen las opciones de Nueva entrada de diario.

Campo	Descripción
Nueva entrada de diario	Escriba una nota en el campo.

Campo	Descripción
Punto de control	(Opcional) Seleccione un punto de control, si corresponde. Este campo se utiliza para rastrear los eventos significativos para el incidente.
Botón **Enviar**	Haga clic en Enviar para agregar una entrada al registro. Cualquier persona que vea el incidente podrá ver la entrada del registro.

Panel Tareas

En el panel Tareas, puede administrar y rastrear las tareas del incidente hasta su cierre.



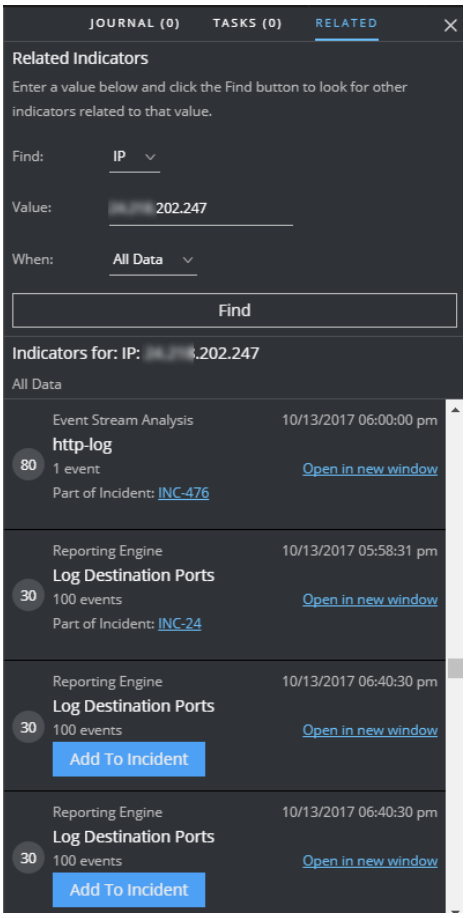
En la siguiente tabla se describen los campos de Tarea.

Campo	Descripción
<ID de tarea>/<ID de incidente>	El ID de tarea/ID de incidente generado automáticamente que está asociado con la tarea.
CREADO	La fecha de creación de la tarea.
ÚLTIMA ACTUALIZACIÓN	La fecha en que la tarea se modificó por última vez.
ABIERTA	El tiempo que ha transcurrido desde que se abrió la tarea. Por ejemplo, hace 3 minutos o hace 2 días.

Campo	Descripción
NAME	El nombre de la tarea. Por ejemplo: Re-image the machine. Puede hacer clic en este campo para editarlo.
USUARIO ASIGNADO	El nombre del usuario a quien se asignó la tarea. Puede hacer clic en este campo para editarlo.
PRIORIDAD	La prioridad de la tarea: Baja, Media, Alta o Crítica. Puede hacer clic en el botón Prioridad y seleccionar una prioridad nueva para la tarea en la lista desplegable.
ESTADO	El estado de la tarea: Nuevo, Asignado, En Curso, Corregido, Riesgo aceptado y No aplicable. Puede hacer clic en el botón Estado y seleccionar un estado nuevo para la tarea en la lista desplegable.
DESCRIPCIÓN	Escriba información que describa la tarea. Tal vez desee incluir números de referencia correspondientes. Puede hacer clic en este campo para editarlo.

Panel Indicadores relacionados

El panel Indicadores relacionados permite buscar alertas que están relacionadas con este incidente en la base de datos de alertas de NetWitness Suite. Puede agregar las alertas que encuentra al incidente si aún no están asociadas a un incidente.



En la siguiente tabla se describen los campos de la sección de búsqueda de la parte superior del panel.

Campo	Descripción
Buscar	Seleccione la entidad que desea buscar en las alertas. Por ejemplo, IP.
Valor	Escriba el valor de la entidad. Por ejemplo, escriba la dirección IP real de la entidad.
Cuándo	Seleccione un rango de tiempo para buscar las alertas. Por ejemplo, Últimas 24 horas.
Botón **Buscar**	Inicia la búsqueda. Aparece una lista de indicadores relacionados debajo del botón **Buscar** en la sección **Indicadores para**.

En la siguiente tabla se describen las opciones de la sección **Indicadores para** (resultados) en la parte inferior del panel.

Opción	Descripción
Indicadores para:	Muestra los resultados de la búsqueda.
Vínculo **Abrir en una nueva ventana**	Muestra detalles de la alerta para el indicador.
Botón **Agregar a incidente**	Agregar el indicador relacionado al incidente. El indicador relacionado se agrega al panel Indicadores.
Botón **Parte de este incidente**	Muestra que el indicador ya forma parte del incidente.

Acciones de la barra de herramientas

Opción	Descripción
	(Volver a los incidentes) Permite volver a la vista Lista de incidentes.
	Cierra el panel.
	Elimina la entrada, como una tarea o una entrada del registro.
Botón **Prioridad**	(En el panel Descripción general) Permite cambiar la prioridad de uno o más incidentes seleccionados en la Lista de incidentes.
Botón **Estado**	(En el panel Descripción general) Permite cambiar el estado de uno o más incidentes seleccionados.
Botón **Usuario asignado**	(En el panel Descripción general) Permite cambiar el usuario asignado de uno o más incidentes seleccionados.
 (Ver: Gráfico)	Permite ver el gráfico de nodos.

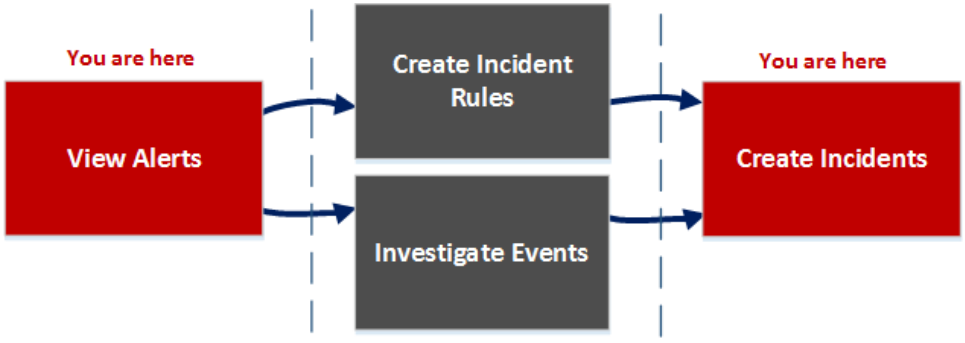
Opción	Descripción
 (Ver: Hoja de datos)	Permite ver la hoja de datos Eventos, la que puede aparecer como una Lista de eventos para varios eventos o como Detalles de eventos para un único evento.
 (Registro, tareas y relacionados)	Permite ver los paneles Registro, Tareas e Indicadores relacionados.

Vista Lista de alertas

La vista Lista de alertas (RESPOND > Alertas) permite ver todas las alertas y los indicadores de amenazas que recibió NetWitness Suite en una sola ubicación. Esto puede incluir alertas recibidas desde ESA Correlation Rules, ESA Analytics, NetWitness Endpoint, Malware Analysis, Reporting Engine y muchos otros. La vista Lista de alertas permite navegar por diversas alertas, filtrarlas y agruparlas para crear incidentes.

Flujo de trabajo

En este flujo de trabajo se muestra el proceso general que usan los analistas para revisar alertas y crear incidentes.



En la vista Lista de alertas, puede revisar una lista de alertas de todos los orígenes que recibió NetWitness Suite. Después de eso, puede investigar esas alertas más a fondo y crear incidentes a partir de ellas, o puede crear reglas de incidentes para crear incidentes.

Nota: Puede usar Detección de amenazas automatizadas de NetWitness Suite para crear incidentes sin crear reglas manualmente.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Encargados de respuesta ante incidentes, analistas	Ver todas las alertas en NetWitness Suite.*	Ver alertas

Función	Deseo…	Mostrarme cómo
Encargados de respuesta ante incidentes, analistas	Filtrar alertas.*	Filtrar la Lista de alertas
Encargados de respuesta ante incidentes, analistas	Ver información de descripción general de alertas y metadatos de alertas crudas.*	Ver información de resumen de las alertas
Encargados de respuesta ante incidentes, analistas	Crear incidentes a partir de alertas.*	Crear un incidente manualmente
Encargados de respuesta ante incidentes, analistas	(Disponible en la versión 11.1 y superior) Agregar alertas a un incidente existente.*	Agregar alertas a un incidente
Administradores, encargados de la privacidad de datos	Eliminar alertas.*	Eliminar alertas
Administradores del SOC, administradores	Crear reglas de incidentes.	Consulte “Crear una regla de incidentes para alertas” en la *Guía de configuración de NetWitness Respond.*
Encargados de respuesta ante incidentes, analistas	Investigar los eventos en una alerta.	Ver detalles de los eventos de una alerta e Investigar eventos
Encargados de respuesta ante incidentes, analistas	Agregar alertas relacionadas a un incidente existente.	Agregar indicadores relacionados al incidente

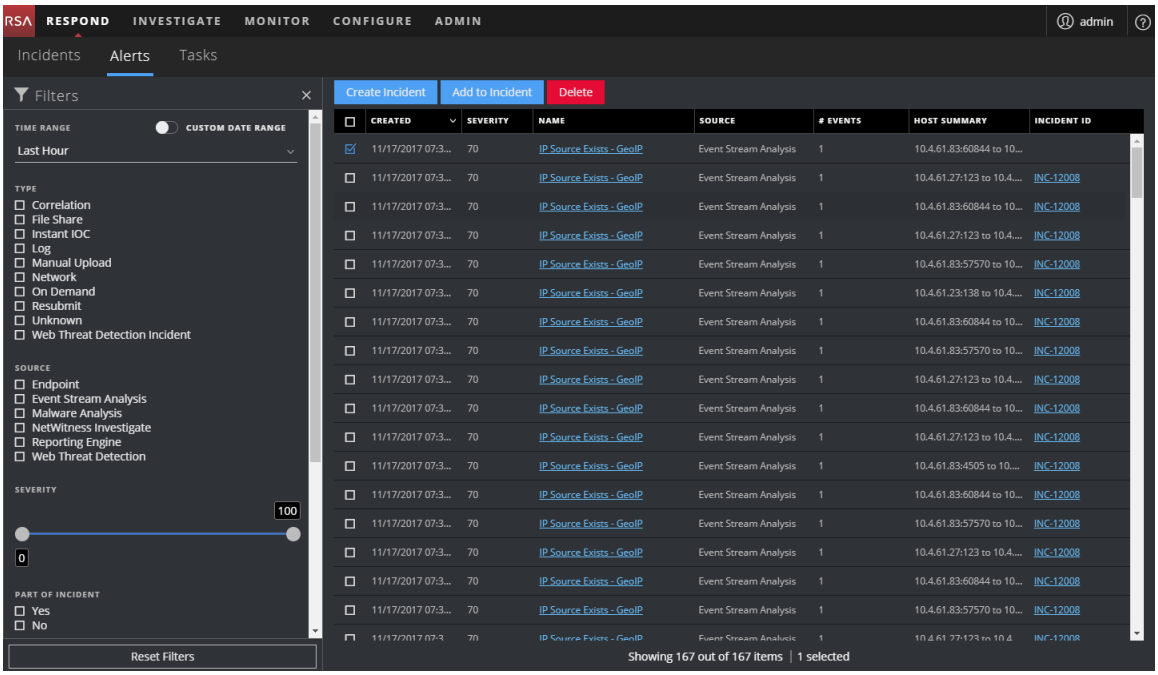
*Puede realizar estas tareas aquí (es decir, en la vista Lista de alertas).

Temas relacionados

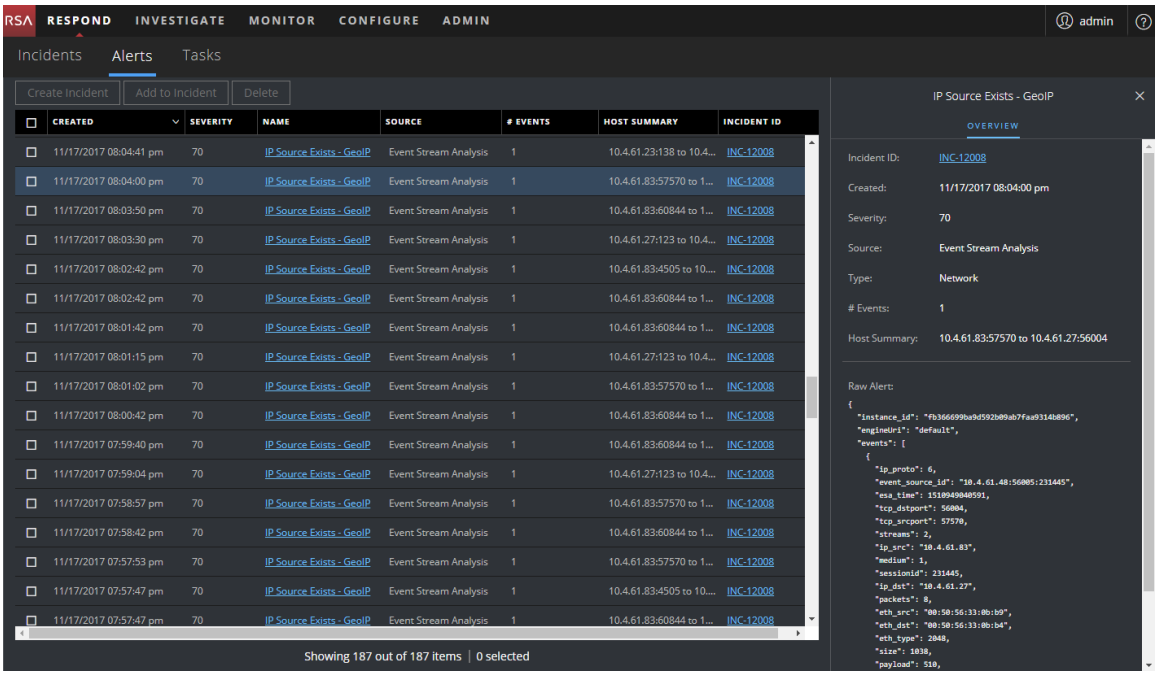
- Vista Detalles de la alerta
- Revisión de alertas

Vista Lista de alertas

Para acceder a la vista Lista de alertas, vaya a **RESPONDER > Alertas**. La vista Lista de alertas muestra una lista de todas las alertas y los indicadores que recibió la base de datos de Servidor de Respond en NetWitness Suite. En la siguiente figura se muestra el panel Filtros a la izquierda.

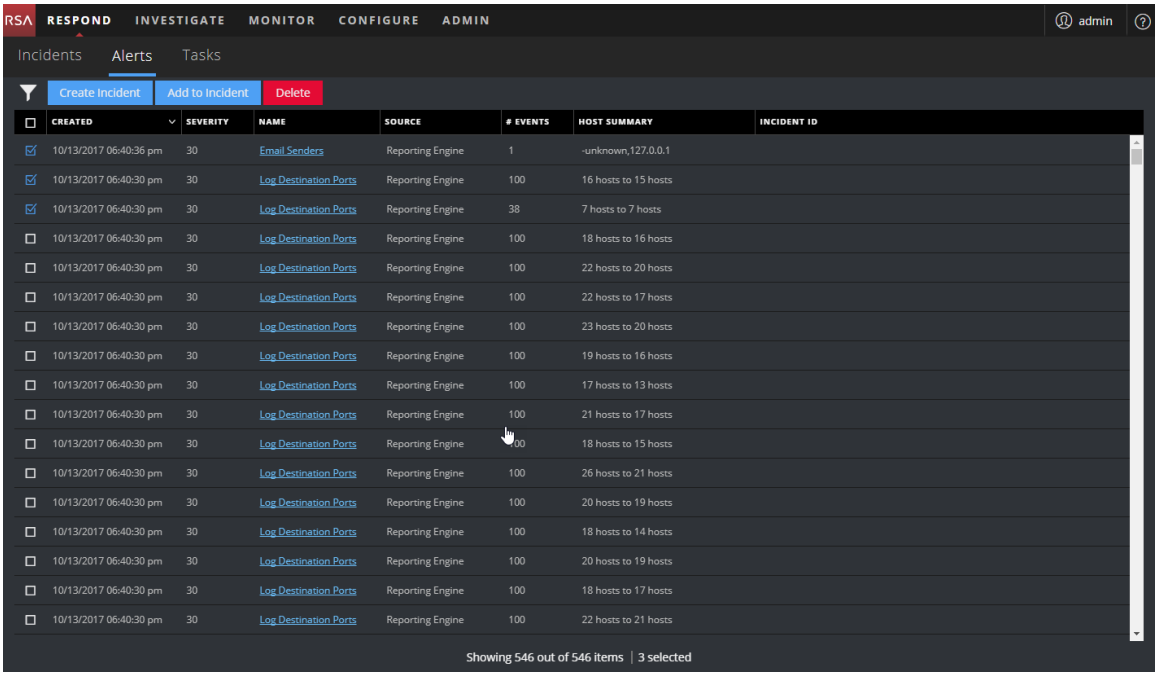


La vista Lista de alertas consta de un panel Filtros, una Lista de alertas y un panel Descripción general de alertas. Puede hacer clic en una alerta de la Lista de alertas para ver el panel Descripción general de alertas a la derecha.



Lista de alertas

En la Lista de alertas se muestran todas las alertas de NetWitness Suite. Puede filtrar esta lista para mostrar solo las alertas de interés.

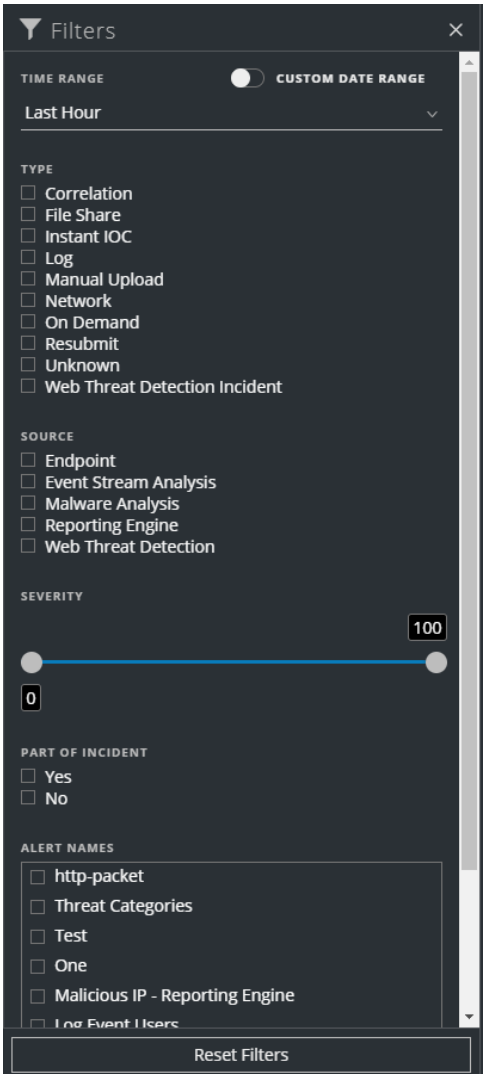


Columna	Descripción
	Permite seleccionar una o más alertas que se eliminarán. Los usuarios con los permisos adecuados, como los administradores y los encargados de la privacidad de datos, pueden eliminar las alertas.
CREADO	Muestra la fecha y la hora en que se registró la alerta en el sistema de origen.
GRAVEDAD	Muestra el nivel de gravedad de la alerta. Los valores varían entre 1 y 100.
NAME	Muestra una descripción básica de la alerta.
ORIGEN	Muestra el origen original de la alerta. El origen de las alertas puede ser NetWitness Endpoint, Malware Analysis, ESA Correlation Rules, ESA Analytics, Reporting Engine y muchos otros.
CANTIDAD DE EVENTOS	Indica la cantidad de eventos que se incluyen dentro de una alerta. esto varía según el origen de la alerta. Por ejemplo, las alertas de NetWitness Endpoint y Malware Analysis siempre tienen un evento. Para ciertos tipos de alertas, una alta cantidad de eventos puede significar que la alerta es más riesgosa.
RESUMEN DE HOST	Muestra detalles del host, como el nombre del host donde se activó la alerta. Los detalles pueden incluir información acerca de los hosts de origen y destino en una alerta. Algunas alertas pueden describir eventos en más de un host.
ID del incidente	Muestra el ID del incidente de la alerta. Si no hay un ID del incidente, la alerta no pertenece a ningún incidente y se puede crear uno para incluirla o se puede agregar a un incidente existente.

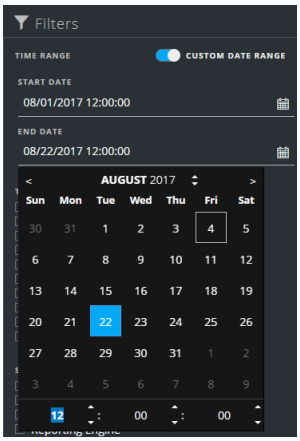
En la parte inferior de la lista, puede ver la cantidad de alertas que se muestran en la página actual, la cantidad total de alertas y la cantidad de alertas seleccionadas. Por ejemplo:
Mostrando 377 de 377 elementos | 3 seleccionado(s)

Panel Filtros

En la siguiente figura se muestran los filtros disponibles en el panel Filtros.



El panel Filtros, a la izquierda de la vista Lista de alertas, tiene opciones que puede usar para filtrar la lista de alertas. Cuando sale del panel Filtros, la vista Lista de alertas conserva sus selecciones de filtros.

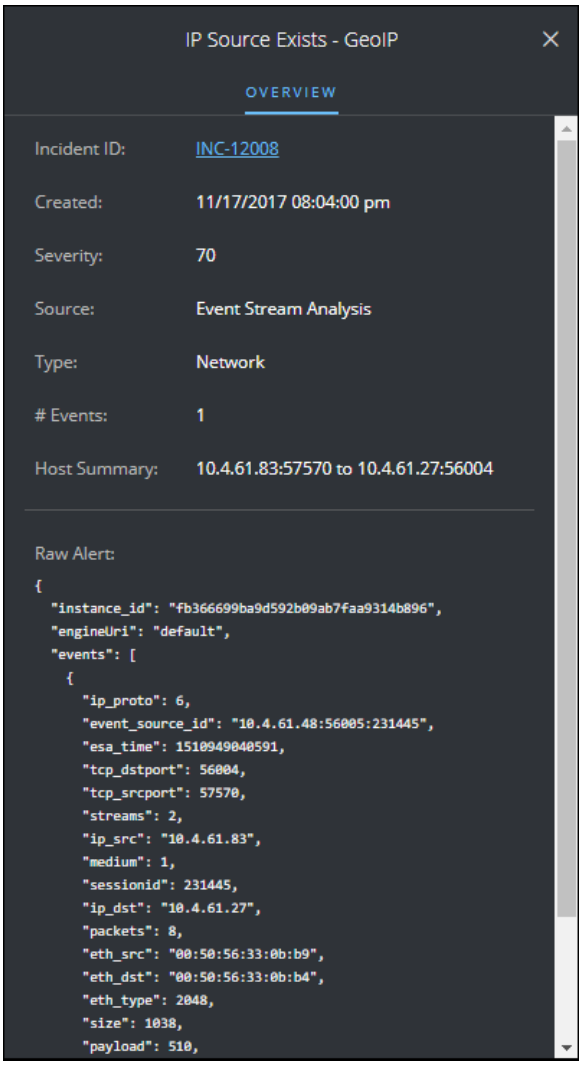
Opción	Descripción
RANGO DE TIEMPO	Puede seleccionar un período específico en la lista desplegable Rango de tiempo. El rango de tiempo se basa en la fecha de recepción de las alertas. Por ejemplo, si selecciona Última hora, verá las alertas que se recibieron en los últimos 60 minutos.
RANGO DE FECHAS PERSONALIZADO	Puede especificar un rango de fechas determinado en lugar de seleccionar una opción de Rango de tiempo. Para ello, haga clic en el círculo blanco frente a Rango de fechas personalizado para ver los campos Fecha de inicio y Fecha de finalización. Seleccione las fechas y las horas en el calendario. 
TIPO	Indica el tipo de eventos en la alerta; por ejemplo, registros, sesiones de red, etc.
ORIGEN	Muestra el origen original de la alerta. El origen de las alertas puede ser NetWitness Endpoint, Malware Analysis, Event Stream Analysis (ESA Correlation Rules), ESA Analytics, Reporting Engine, Web Threat Detection y muchos otros.
GRAVEDAD	Muestra el nivel de gravedad de la alerta. Los valores varían entre 1 y 100.

Opción	Descripción
PARTE DE INCIDENTE	Categoriza las alertas en función de si están o no asociadas con 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. Por ejemplo, antes de crear incidentes a partir de alertas, tal vez desee seleccionar No con el fin de ver solo las alertas que no forman parte de un incidente.
NOMBRES DE ALERTA	Muestra el nombre de la alerta. Puede utilizar este filtro para buscar todas las alertas que genera una regla o un origen específicos, por ejemplo, IP maliciosa: Reporting Engine.
Restablecer filtros	Quita las selecciones de filtros.

La Lista de alertas muestra las alertas que cumplen con los criterios de selección. Puede ver la cantidad de elementos de la lista filtrada en la parte inferior de la lista de alertas. Por ejemplo: **Mostrando 30 de 30 elementos**

Panel Descripción general

El panel Descripción general muestra información de resumen básica acerca de una alerta seleccionada y de metadatos de alertas crudas. El panel Descripción general de la vista Detalles de la alerta contiene la misma información, pero en la vista Detalles de la alerta, puede expandir el panel para ver más información.



En la siguiente tabla se indican los campos que se muestran en el panel Descripción general de alertas.

Campo	Descripción
<Nombre de la alerta>	Muestra el nombre de la alerta.

Campo	Descripción
ID del incidente	Muestra el ID del incidente asociado con la alerta. Puede hacer clic en el vínculo de ID de incidente para ir a la vista Detalles de incidente del incidente asociado. Si no hay ningún ID de incidente, la alerta no pertenece a un incidente. Puede crear un incidente para esta alerta o puede agregarla a un incidente.
Creado	Muestra la fecha y la hora en que se creó la alerta.
Gravedad	Muestra el nivel de gravedad de la alerta. Los valores varían entre 1 y 100.
Origen	Muestra el origen original de la alerta. El origen de las alertas puede ser NetWitness Endpoint, Malware Analysis, ESA Correlation Rules, ESA Analytics, Reporting Engine y muchos otros.
Tipo	Indica el tipo de eventos en la alerta; por ejemplo, registros, sesiones de red, etc.
Cantidad de eventos	Indica la cantidad de eventos que se incluyen dentro de una alerta. esto varía según el origen de la alerta. Por ejemplo, las alertas de NetWitness Endpoint y Malware Analysis siempre tienen un evento. Para ciertos tipos de alertas, una alta cantidad de eventos puede significar que la alerta es más riesgosa.
Alerta cruda	Muestra los metadatos de alertas crudas.

Acciones de la barra de herramientas

En esta tabla se enumeran las acciones de la barra de herramientas disponibles en la vista Lista de alertas.

Opción	Descripción
	Permite abrir el panel Filtros, de modo que pueda especificar las alertas que desearía ver en la Lista de alertas.
	Cierra el panel.
Botón **Crear incidente**	Permite crear incidentes a partir de alertas. Las alertas no pueden formar parte de un incidente. Para obtener una lista de alertas sin incidentes, puede filtrar la Lista de alertas. En la sección PARTE DE INCIDENTE, seleccione No.
Botón **Agregar a incidente**	(Esta opción está disponible en la versión 11.1 y superior). Permite agregar las alertas seleccionadas a un incidente. Las alertas no pueden formar parte de un incidente. Para obtener una lista de alertas sin incidentes, puede filtrar la Lista de alertas. En la sección PARTE DE INCIDENTE, seleccione No.
Botón **Eliminar**	Permite eliminar alertas.

Vista Detalles de la alerta

En la vista Detalles de la alerta (RESPOND > Alertas > haga clic en un hipervínculo de NOMBRE en la Lista de alertas), puede ver información resumida sobre una alerta, como el origen de la alerta, la cantidad de eventos dentro de la alerta y si es parte de un incidente. También puede ver información detallada acerca de los eventos dentro de la alerta, así como los metadatos de los eventos.

Flujo de trabajo

En este flujo de trabajo se muestra el proceso general que usan los analistas para revisar alertas y crear incidentes.

Después de revisar la lista de alertas, en la vista Detalles de la alerta, puede investigar aún más esas alertas y crear incidentes a partir de ellas. En CONFIGURAR > vista Reglas de incidentes, puede crear reglas de incidentes para crear incidentes.

Nota: También puede usar Detección de amenazas automatizadas de NetWitness Suite para crear incidentes sin crear reglas manualmente.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Encargados de respuesta ante incidentes, analistas	Ver todas las alertas en NetWitness Suite.	Ver alertas

Función	Deseo…	Mostrarme cómo
Administradores del SOC, administradores	Crear reglas de incidentes.	Consulte “Crear una regla de incidentes para alertas” en la *Guía de configuración de NetWitness Respond*.
Encargados de respuesta ante incidentes, analistas	Ver una lista de eventos en la alerta.*	Ver detalles de los eventos de una alerta
Encargados de respuesta ante incidentes, analistas	Ver los metadatos de cada evento en la alerta.*	Ver detalles de los eventos de una alerta
Encargados de respuesta ante incidentes, analistas	Investigar más a fondo los eventos en la alerta.*	Investigar eventos
Encargados de respuesta ante incidentes, analistas	Agregar alertas a un incidente existente.	Agregar alertas a un incidente Agregar indicadores relacionados al incidente
Encargados de respuesta ante incidentes, analistas	Crear incidentes a partir de alertas.	Crear un incidente manualmente
Encargados de la privacidad de datos, administradores	Eliminar alertas.	Eliminar alertas

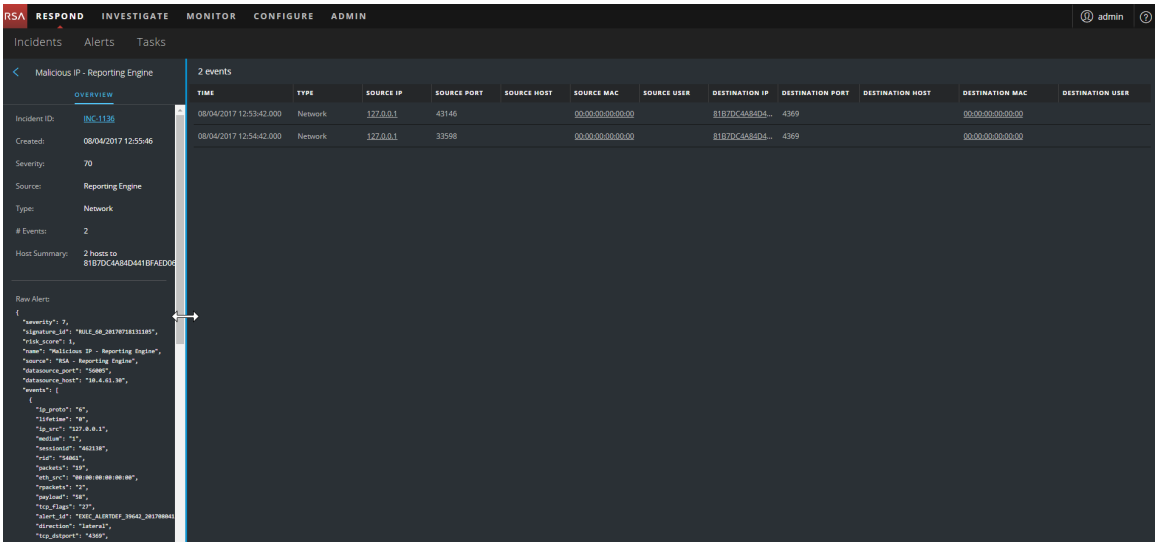
*Puede realizar estas tareas aquí (es decir, en la vista Detalles de la alerta).

Temas relacionados

- Vista Lista de alertas
- Revisión de alertas

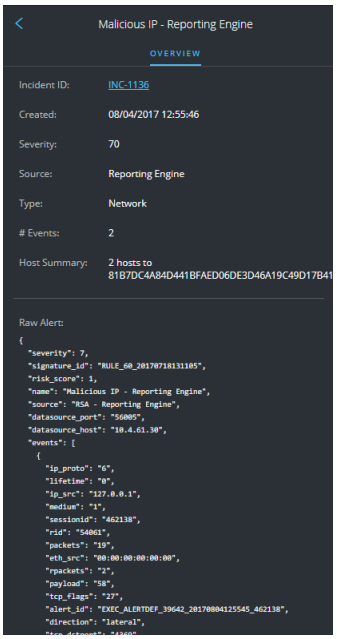
Vista Detalles de la alerta

1. Para acceder a la vista Detalles de la alerta, vaya a **RESPONDER > Alertas**.
2. En la Lista de alertas, elija una alerta que desee ver y, a continuación, haga clic en el vínculo de la columna NOMBRE correspondiente a esa alerta.
   La vista Detalles de la alerta tiene un panel Descripción general en el lado izquierdo y un panel Eventos en el lado derecho. Puede cambiar el tamaño de los paneles para visualizar más información, como se muestra en la siguiente figura.



Panel Descripción general

El panel Descripción general muestra información de resumen básica acerca de una alerta seleccionada. El panel Descripción general de la vista Lista de alertas contiene la misma información. En el tema Panel Descripción general de la vista Lista de alertas se proporcionan detalles.

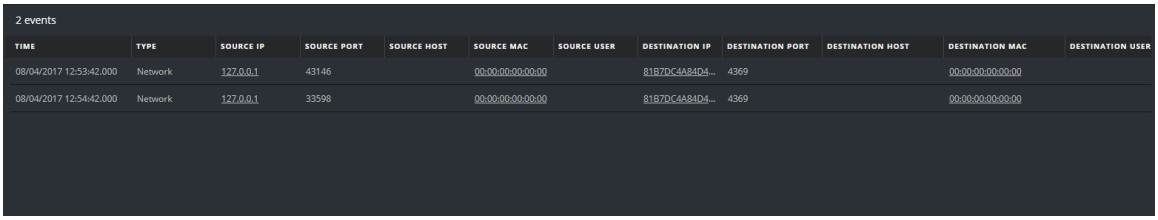


Panel Eventos

El panel Eventos puede mostrar una Lista de eventos si la alerta tiene más de un evento. Si la alerta tiene un solo evento o si usted hace clic en un evento de la Lista de eventos, puede ver Detalles de eventos en el panel Eventos.

Lista de eventos

La Lista de eventos de una alerta seleccionada muestra todos los eventos incluidos en esa alerta.



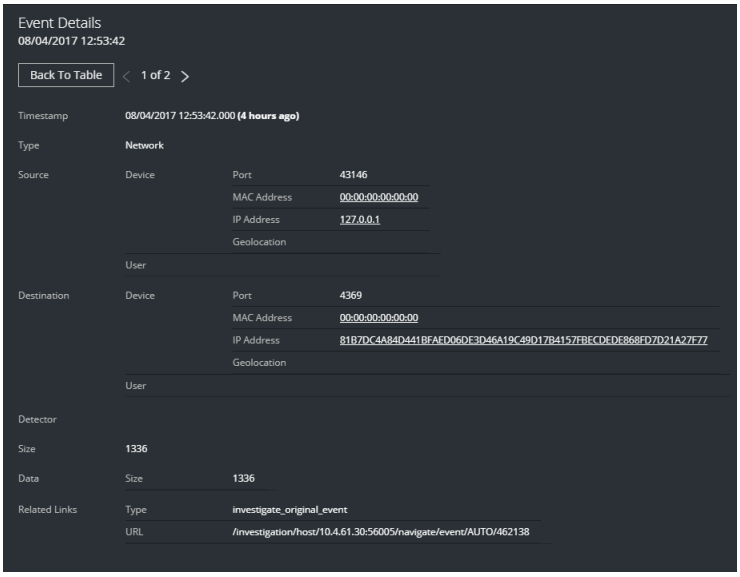
En la siguiente tabla se indican algunas de las columnas que se muestran en la Lista de eventos, las cuales proporcionan un resumen de los eventos enumerados.

Columna	Descripción
TIEMPO	Muestra la hora en que se produjo el evento.
TIPO	Muestra el tipo de alerta, como Registro y Red.
DIRECCIÓN IP DE ORIGEN	Muestra la dirección IP de origen si hubo una transacción entre dos máquinas.

Columna	Descripción
DIRECCIÓN IP DE DESTINO	Muestra la dirección IP de destino si hubo una transacción entre dos máquinas.
IP DE DETECTOR	Muestra la dirección IP de la máquina en la que se detectó una anomalía.
USUARIO DE ORIGEN	Muestra el usuario de la máquina de origen.
USUARIO DE DESTINO	Muestra el usuario de la máquina de destino.
NOMBRE DE ARCHIVO	Muestra el nombre del archivo, si hubo uno implicado en el evento.
HASH DE ARCHIVO	Muestra un hash del contenido del archivo.

Detalles de eventos

En Detalles de eventos en el panel Eventos se muestran los metadatos de cada evento en la alerta.



Metadatos de eventos

En la siguiente tabla se indican algunas secciones y subsecciones de metadatos de eventos que se muestran en las primeras dos columnas de Detalles de eventos. Esta lista no es extensa.

Sección	Subsección	Descripción
Datos		Muestra información acerca de los datos relacionados con el evento, por ejemplo, los archivos involucrados. Puede haber 0 o más por evento.
	Nombre del archivo	Muestra el nombre del archivo, si hubo uno implicado en el evento.
	Hash	Muestra un hash del contenido del archivo, por ejemplo, MD5 o SHA1.
	Tamaño	Muestra el tamaño de la transmisión o del archivo involucrados en el evento.
Descripción		Muestra una descripción general del evento.
Destino		Muestra el dispositivo y el usuario de destino.
	Dispositivo	Muestra información acerca del dispositivo de destino. Consulte Atributos de dispositivos de origen o destino de eventos, a continuación.
	Usuario	Muestra información acerca del usuario o los usuarios del destino. Consulte Atributos de usuarios de origen o destino de eventos, a continuación.
Detector		Muestra el producto de software o el host que detectaron el problema. Esto tiene mayor relación con los escáneres de malware y los registros.
	Clase de dispositivo	Muestra la clase de dispositivo del producto que detectó la alerta.
	Dirección IP	Muestra la dirección IP del producto que detectó la alerta.
	Nombre del producto	Muestra el nombre del producto que detectó la alerta.
Dominio		Muestra el dominio asociado con el evento.

Sección	Subsección	Descripción
Enriquecimiento		Muestra información de enriquecimiento disponible.
Vínculos relacionados		Si está disponible, muestra un vínculo a la interfaz del usuario del producto de origen.
	Tipo	Muestra el tipo de evento, como investigate_original_event.
	URL	Muestra el vínculo de URL a la interfaz del usuario del producto de origen.
Tamaño		Muestra el tamaño de la transmisión o el archivo involucrados.
Origen		Muestra el dispositivo y el usuario de origen.
	Dispositivo	Muestra información acerca de la máquina de origen. Consulte Atributos de dispositivos de origen o destino de eventos, a continuación.
	Usuario	Muestra información acerca del usuario o los usuarios de la máquina de origen. Consulte Atributos de usuarios de origen o destino de eventos, a continuación.
Registro de fecha y hora		Muestra la hora en que se produjo el evento.
Tipo		Muestra el tipo de la alerta, como registro, red, correlación, Volver a enviar, Carga manual, Según demanda, Recurso compartido de archivos o IOC instantáneo.

Atributos de dispositivos de origen o destino de eventos

En la siguiente tabla se indican los atributos de un dispositivo de origen o destino de eventos que se pueden mostrar en Detalles de eventos.

Nombre	Descripción
Tipo de recurso	Muestra el tipo de dispositivo, por ejemplo, escritorio, laptop, servidor, equipo de red, tableta, etc.
Unidad de negocios	Muestra la unidad de negocios asociada.

Nombre	Descripción
Clasificación de cumplimiento de normas	Muestra la clasificación de cumplimiento de normas del dispositivo. Puede ser Baja, Media o Alta.
Criticidad	Muestra lo importante que es el dispositivo para el negocio (importancia para el negocio).
Funcionalidad	Muestra la ubicación del dispositivo.
Ubicación geográfica	Muestra la ubicación geográfica para el host. Puede contener los siguientes atributos: ciudad, país, latitud, longitud, organización y dominio.
Dirección IP	Muestra la dirección IP del dispositivo.
Dirección MAC	Muestra la dirección MAC del dispositivo.
Nombre NetBIOS	Muestra el nombre de NetBIOS del dispositivo.
Puerto	Muestra el puerto TCP, el puerto UDP o el puerto IP Src (el primero disponible) que se utilizan para la conexión al host y desde este.

Atributos de usuarios de origen o destino de eventos

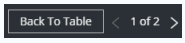
En la siguiente tabla se indican los atributos de un usuario de origen o destino de eventos que se pueden mostrar en Detalles de eventos.

Nombre de atributo	Descripción
Dominio AD	Muestra el dominio de Active Directory.
Nombre de usuario de AD	Muestra el nombre de usuario de Active Directory.
Dirección de correo electrónico	Muestra la dirección de correo electrónico del usuario.

Nombre de atributo	Descripción
Nombre de usuario	Muestra un nombre general si no conoce el origen del nombre de usuario, por ejemplo, UNIX o un nombre de usuario en un sistema específico.

Acciones de la barra de herramientas

En esta tabla se enumeran las acciones de la barra de herramientas disponibles en la vista Detalles de la alerta.

Opción	Descripción
	(Volver a alertas) Permite volver a la vista Lista de alertas.
	Haga clic en las flechas para navegar entre los detalles de los metadatos de cada evento en la alerta. Los números, como “1 de 2”, muestran el número del evento que se observa. Haga clic en **Volver a tabla** para volver a la vista Lista de eventos, que también se conoce como Tabla de eventos.

Vista Lista de tareas

Después de investigar incidentes, la vista Lista de tareas (RESPOND > Tareas) permite crear y rastrear tareas de incidentes. Por ejemplo, puede crear tareas de corrección cuando se requieren acciones relativas a los incidentes de equipos fuera de sus operaciones de seguridad. Puede hacer referencia a números de vale externos dentro de las tareas y, a continuación, rastrear esas tareas hasta su finalización. También puede modificar y eliminar las tareas según sea necesario, según los permisos de usuario.

¿Qué desea hacer?

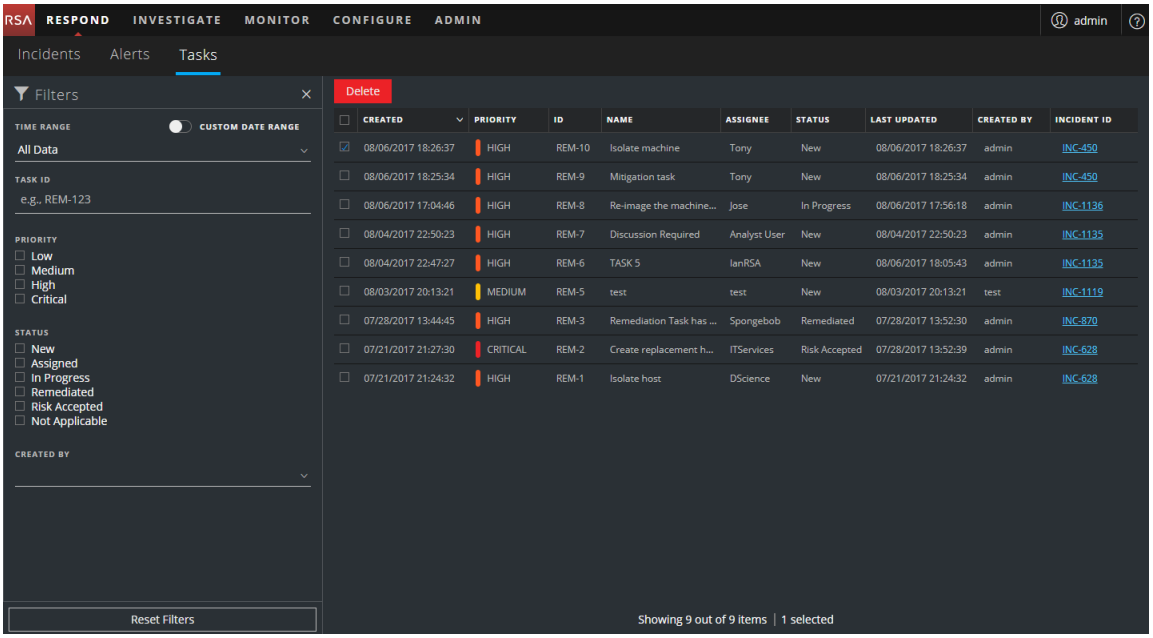
Función	Deseo…	Mostrarme cómo
Encargados de respuesta ante incidentes, analistas	Ver tareas.	Ver todas las tareas de incidentes y Ver las tareas asociadas a un incidente
Encargados de respuesta ante incidentes, analistas	Filtrar las tareas.	Filtrar la Lista de tareas
Encargados de respuesta ante incidentes, analistas	Crear una tarea.	Crear una tarea
Encargados de respuesta ante incidentes, analistas	Buscar y modificar tareas.	Buscar una tarea y Modificar una tarea
Encargados de respuesta ante incidentes, analistas	Cerrar una tarea (cambiar el estado a Corregido, Riesgo aceptado o No aplicable).	Modificar una tarea
Encargados de respuesta ante incidentes, analistas, administradores del SOC	Eliminar una tarea.	Eliminar una tarea

Temas relacionados

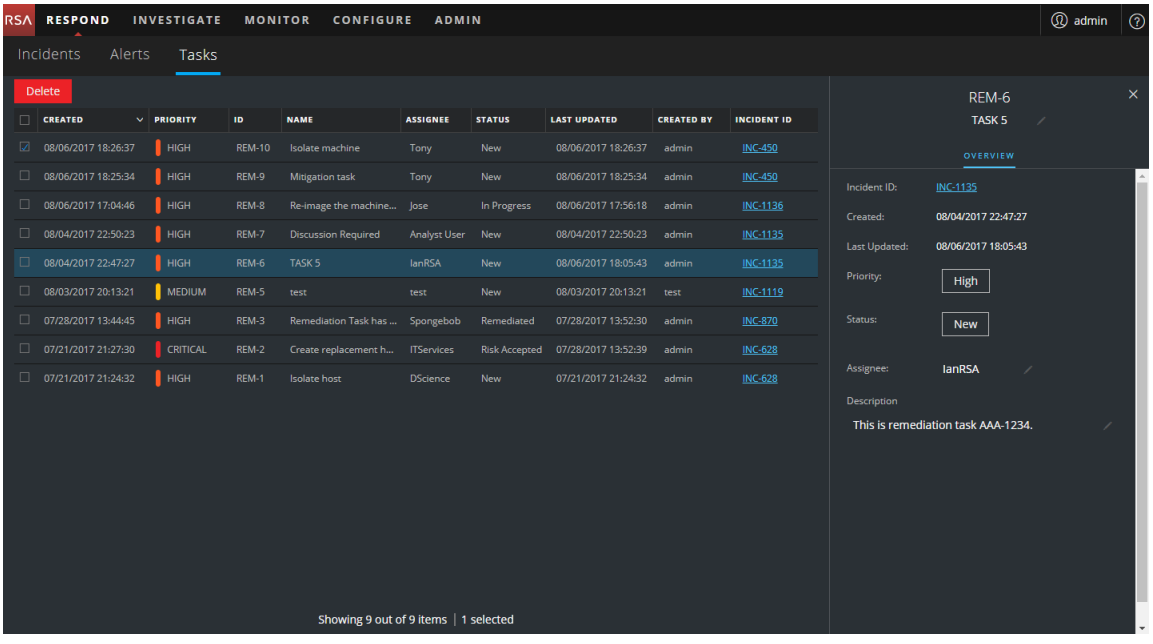
- Vista Detalles de incidente
- Elevar o corregir el incidente

Lista de tareas

Para acceder a la vista Lista de tareas, vaya a **RESPONDER > Tareas**. La vista Lista de tareas muestra una lista de todas las tareas de incidentes.

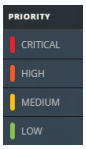


La vista Lista de tareas consta de un panel Filtros, una Lista de tareas y un panel Descripción general de tareas. En la siguiente figura se muestra la Lista de tareas y el panel Descripción general.



Lista de tareas

La Lista de tareas muestra todas las tareas de incidentes. Puede filtrar esta lista para mostrar solo las tareas de interés.

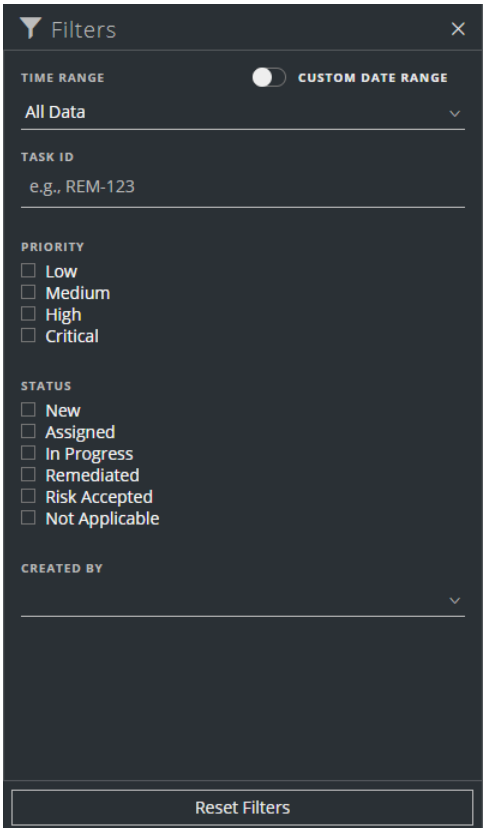
Columna	Descripción
	Permite seleccionar una o más tareas que se modificarán o eliminarán. Los usuarios con los permisos adecuados, como los administradores del SOC, pueden realizar actualizaciones y eliminaciones masivas de tareas. Por ejemplo, puede que un administrador del SOC desee asignar varias tareas a un usuario al mismo tiempo.
CREADO	Muestra la fecha en que se creó la tarea.
PRIORIDAD	Muestra la prioridad asignada a la tarea. La prioridad puede ser cualquiera de las siguientes: Crítica, Alta, Media o Baja. La prioridad también está codificada en colores. El rojo indica un riesgo de prioridad **Crítica**, el naranja, **Alta**, el amarillo, **Media** y el verde, **Baja**, como se muestra en la siguiente figura: 
ID	Muestra el ID de la tarea.
NAME	Muestra el nombre de la tarea.
USUARIO ASIGNADO	Muestra el nombre del usuario asignado a la tarea.
ESTADO	Muestra el estado de la tarea: Nuevo, Asignado, En Curso, Corregido, Riesgo aceptado y No aplicable.
ÚLTIMA ACTUALIZACIÓN	Muestra la fecha y hora de la última actualización de la tarea.
CREADO POR	Muestra el usuario que creó la tarea.

Columna	Descripción
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.

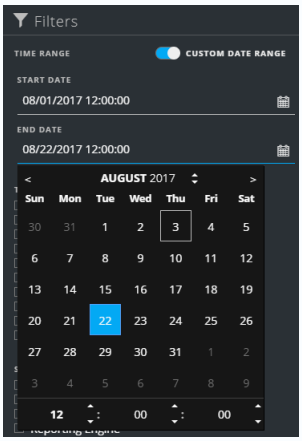
En la parte inferior de la lista, puede ver la cantidad de tareas que se muestran en la página actual y la cantidad total de tareas. Por ejemplo: **Mostrando 23 de 23 elementos**

Panel Filtros

En la siguiente figura se muestran los filtros disponibles en el panel Filtros.



El panel Filtros, a la izquierda de la vista Lista de tareas, tiene opciones que puede usar para filtrar las tareas de incidentes.

Opción	Descripción
RANGO DE TIEMPO	Puede seleccionar un período específico en la lista desplegable Rango de tiempo. El rango de tiempo se basa en la fecha de creación de las tareas. Por ejemplo, si selecciona Última hora, verá las tareas que se crearon en los últimos 60 minutos.
RANGO DE FECHAS PERSONALIZADO	Puede especificar un rango de fechas determinado en lugar de seleccionar una opción de Rango de tiempo. Para ello, haga clic en el círculo blanco frente a Rango de fechas personalizado para ver los campos Fecha de inicio y Fecha de finalización. Seleccione las fechas y las horas en el calendario. 
ID DE TAREA	Puede escribir el ID de tarea que desea buscar, por ejemplo, REM-123.
PRIORIDAD	Puede seleccionar las prioridades que desea ver. Si realiza una o más selecciones, la Lista de tareas muestra solo las tareas con las prioridades seleccionadas. Por ejemplo: Si se selecciona Crítica, la Lista de tareas muestra solo las tareas cuya prioridad está configurada en Crítica.

Opción	Descripción
ESTADO	Puede seleccionar los estados que desea ver. Si realiza una o más selecciones, la Lista de tareas muestra solo las tareas con los estados seleccionados. Por ejemplo: Si selecciona Asignada, el panel Tareas muestra solo las tareas que están asignadas a los usuarios.
CREADO POR	Puede seleccionar el usuario que creó las tareas que desea ver. Por ejemplo, si solo desea ver las tareas que creó Edwardo, seleccione Edwardo en la lista desplegable CREADO POR. Si desea ver las tareas independientemente de la persona que las creó, no realice una selección en CREADO POR.
Restablecer filtros	Quita las selecciones de filtros.

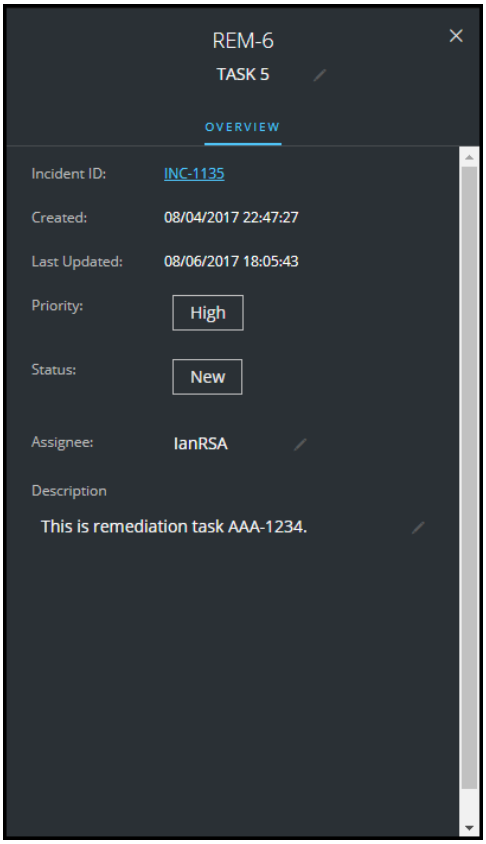
La Lista de tareas muestra las tareas que cumplen con los criterios de selección. Puede ver la cantidad de elementos de la lista filtrada en la parte inferior de la lista de tareas. Por ejemplo: **Mostrando 18 de 18 elementos**

Panel Descripción general de tareas

Para acceder al panel Descripción general de tareas:

1. Vaya a **RESPONDER > Tareas**.

2. En la Lista de tareas, haga clic en la tarea que desea ver.
   El panel Descripción general de tareas aparece a la derecha de la Lista de tareas.



En la siguiente tabla se indican los campos que se muestran en el panel Descripción general de tareas.

Campo	Descripción
<ID de tarea>	Muestra el ID de la tarea asignado automáticamente.
<Nombre de la tarea>	Muestra el nombre de la tarea. Este es un campo editable. Para cambiar el nombre de la tarea, puede hacer clic en el nombre actual para abrir un editor de texto. Por ejemplo, puede cambiar un nombre de tarea de “Volver a crear la imagen de una laptop” a “Volver a crear la imagen de un servidor”.
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.

Campo	Descripción
Creado	Muestra detalles sobre la fecha y la hora en que se creó la tarea.
Última actualización	Muestra la fecha y hora de la última actualización de la tarea.
Prioridad	Muestra la prioridad de la tarea: Baja, Media, Alta o Crítica. Para cambiar la prioridad, puede hacer clic en el botón Prioridad y seleccionar una prioridad para la tarea en la lista desplegable.
Estado	Muestra el estado de la tarea: Nuevo, Asignado, En Curso, Corregido, Riesgo aceptado y No aplicable. Para cambiar el estado, puede hacer clic en el botón Estado y seleccionar un estado para la tarea en la lista desplegable.
Usuario asignado	Muestra el usuario asignado a la tarea. Para cambiar el usuario a quien se asignó la tarea, puede hacer clic en (Sin asignar) o en el nombre de usuario asignado anterior para abrir un editor de texto.
Descripción	Muestra detalles de la tarea. Para modificar la descripción, puede hacer clic en el texto que aparece debajo de esta para abrir un editor de texto.

Acciones de la barra de herramientas

En esta tabla se enumeran las acciones de la barra de herramientas disponibles en la vista Lista de tareas.

Opción	Descripción
	Permite abrir el panel Filtros, de modo que pueda especificar las tareas que desearía ver en la Lista de tareas.
	Cierra el panel.
Botón **Eliminar**	Permite eliminar las tareas seleccionadas.

Cuadro de diálogo Agregar/eliminar de la lista

El cuadro de diálogo Agregar/eliminar de la lista permite agregar una entidad o un valor de metadatos a una lista existente o quitarlos de esta, o crear una lista nueva. Por ejemplo, cuando observa una dirección IP y la encuentra sospechosa o interesante, puede agregarla a una lista pertinente a la cual se agregó un origen de datos. Esto mejora la visibilidad de las direcciones IP sospechosas. También puede agregar entidades o valores de metadatos a distintas listas. Por ejemplo, puede agregarlos a una lista de dominios sospechosos relacionados con conexiones de comando y control y a otra lista de direcciones IP de conexiones de troyanos relacionadas con el acceso remoto. Si no hay una lista disponible, puede crearla. También puede quitar la entidad o el valor de metadatos de una lista.

Nota: En el cuadro de diálogo Agregar/eliminar de la lista, solo puede agregar o quitar entidades o valores de metadatos como un origen de datos desde listas de una única columna, no desde listas de varias columnas. Y, cuando edite una lista o un valor de una lista desde la vista de nodos o la vista de búsqueda de contexto, asegúrese de actualizar la página web para ver los datos actualizados.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Encargados de respuesta ante incidentes, analistas	Agregar una entidad a una lista.	En la vista Detalles de incidente, consulte Agregar una entidad a una lista blanca. En la vista Detalles de la alerta, consulte Agregar una entidad a una lista blanca.
Encargados de respuesta ante incidentes, analistas	Crear una lista blanca, una lista negra u otra lista.	Crear una lista
Administradores	Agregar una lista de Context Hub como un origen de datos.	Consulte “Configurar listas como un origen de datos” en la *Guía de configuración de Context Hub*.
Administradores	Importar o exportar una lista para Context Hub.	Consulte “Importar o exportar listas para Context Hub” en la *Guía de configuración de Context Hub*.

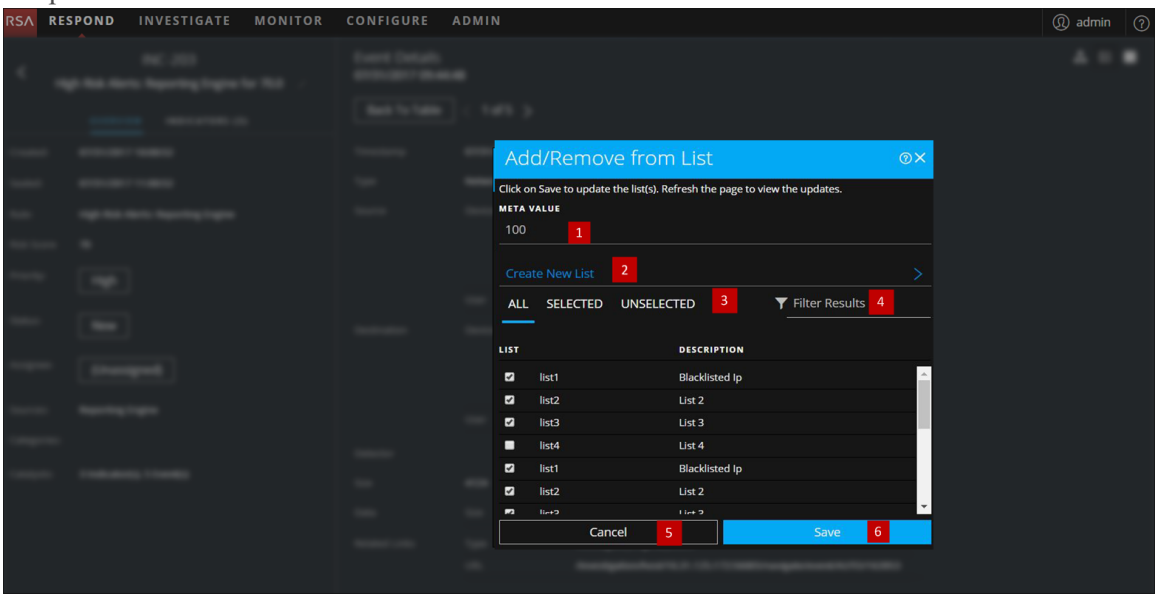
Temas relacionados

- Investigar el incidente
- Revisión de alertas
- Ver información contextual (vista Detalles de incidente)
- Ver información contextual (vista Detalles de la alerta)

Nota: No puede eliminar una lista, pero puede eliminar sus valores.

Vista rápida

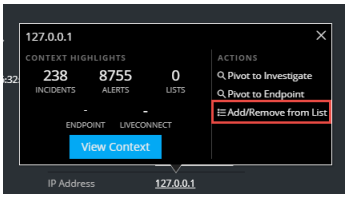
El siguiente es un ejemplo del cuadro de diálogo **Agregar/eliminar de la lista** en la vista Respond.



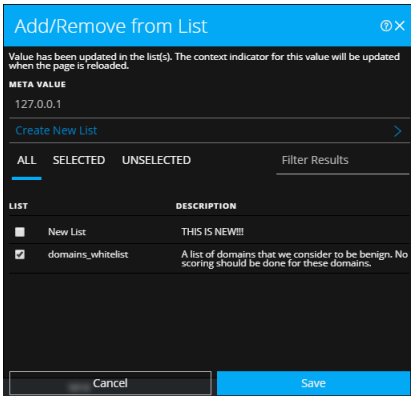
1. Entidades o valores de metadatos que se agregarán o se quitarán.
2. Cree una lista nueva mediante los metadatos seleccionados.
3. Seleccione cualquiera de las pestañas: Todo, Seleccionado o No seleccionado.
4. Busque mediante el nombre de la lista o la descripción.
5. Cancele la acción.
6. Guarde para actualizar las listas o crear una lista nueva.

Agregar/eliminar de la lista

Para acceder al cuadro de diálogo Agregar/eliminar de la lista, en la vista Detalles de incidente o en la vista Detalles de la alerta, coloque el cursor sobre la entidad subrayada que desea agregar a una lista de Context Hub o quitar de esta. Aparece un mensaje de globo de contexto que muestra las acciones disponibles.



En la sección Acciones del mensaje de globo, haga clic en Agregar/eliminar de la lista. El cuadro de diálogo Agregar/eliminar de la lista muestra las listas disponibles.



En la siguiente tabla se muestran las opciones del cuadro de diálogo Agregar/eliminar de la lista.

Opción	Descripción
VALOR DE METADATOS	Muestra la entidad o el valor de metadatos seleccionados que se deben agregar a una o más listas o eliminar de estas. También puede crear una lista nueva mediante el valor seleccionado.
Crear lista nueva	Cuando hace clic en esta opción, muestra un cuadro de diálogo que permite crear una lista nueva mediante el valor de metadatos seleccionado.

Opción	Descripción
TODO	Muestra todas las listas de Context Hub disponibles. Se seleccionan las listas que contienen la entidad o el valor de metadatos seleccionados. Seleccione una casilla de verificación para agregar una entidad o un valor de metadatos a una lista. Deseleccione una casilla de verificación para quitarlos de la lista.
SELECCIONADO	Muestra solo las listas que contienen la entidad o el valor de metadatos seleccionados. (Se seleccionan todas las listas).
NO SELECCIONADO	Muestra solo las listas que no contienen la entidad o el valor de metadatos seleccionados. (Se deseleccionan todas las listas).
Filtrar resultados	Ingrese el nombre o la descripción de una lista específica para buscar en varias listas.
LISTA	Muestra el nombre de todas las listas.
DESCRIPCIÓN	Muestra información acerca de la lista seleccionada. En este cuadro de diálogo aparece la descripción que proporciona cuando crea una lista. Por ejemplo: Esta lista contiene todas las direcciones IP incluidas en la lista negra.
Cancelar	Cancela la operación.
Guardar	Guarda los cambios.

Panel Búsqueda de contexto: Vista Respond

El servicio Context Hub reúne información contextual de varios orígenes de datos en la vista Respond, lo cual permite a los analistas tomar mejores decisiones durante sus análisis y llevar a cabo las acciones correspondientes. La visualización de las entidades, los valores de metadatos y la información contextual en una única interfaz ayuda a los analistas a dar prioridad e identificar las áreas de interés. Por ejemplo, las alertas y los incidentes creados recientemente desde la vista Respond que implican una entidad o un valor de metadatos determinados se mostrarán cuando el analista realice consultas para obtener información adicional acerca de esa entidad o valor de metadatos. El panel Búsqueda de contexto muestra la información contextual de las entidades o los valores de metadatos seleccionados, como una dirección IP, un usuario, un host, un dominio, un nombre de archivo o un hash de archivo. Los datos disponibles dependen de los orígenes configurados en Context Hub.

El panel Búsqueda de contexto muestra la información contextual en función de los datos disponibles en los orígenes configurados en Context Hub.

¿Qué desea hacer?

Función	Deseo…	Mostrarme cómo
Encargados de respuesta ante incidentes, analistas, buscadores de amenazas	Navegar al panel Búsqueda de contexto.	Desde la vista Detalles de incidente, consulte Ver información contextual . Desde la vista Detalles de la alerta, consulte Ver información contextual .
Encargados de respuesta ante incidentes, analistas, buscadores de amenazas	Comprender la información del panel Búsqueda de contexto para una entidad seleccionada.	Consulte la información en este tema.
Administrador	Configurar orígenes de datos para Context Hub.	Consulte “Configurar orígenes de datos para Context Hub” en la *Guía de configuración de Context Hub*.

Función	Deseo…	Mostrarme cómo
Administrador	Configurar los ajustes de Context Hub.	Consulte “Configurar ajustes de orígenes de datos de Context Hub” en la *Guía de configuración de Context Hub*.

Temas relacionados

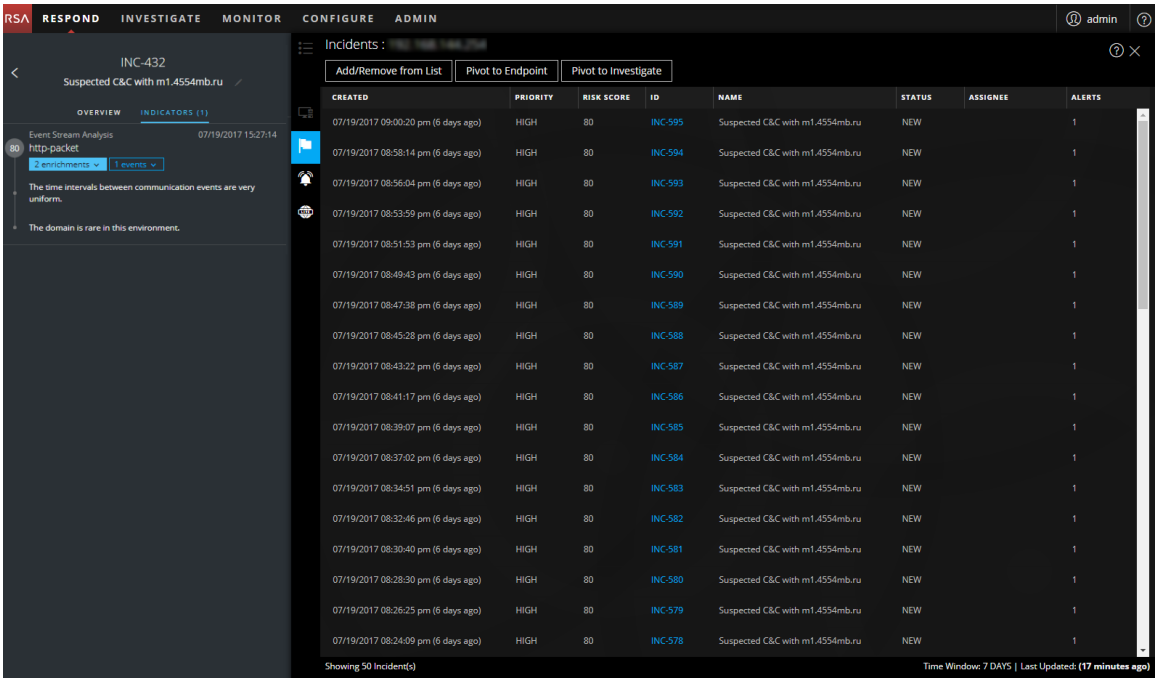
- Investigar el incidente
- Revisión de alertas

Información contextual que se muestra en el panel Búsqueda de contexto

La información contextual o los resultados de consulta que se muestran en el panel Búsqueda de contexto dependen de la entidad seleccionada y de los orígenes de datos asociados.

El panel Búsqueda de contexto tiene pestañas por separado para cada uno de los orígenes de datos. La pestaña del origen de datos Lista es la primera en el panel de contexto, seguida de Archer, Endpoint, Incidentes, Alertas y Live Connect.

En la siguiente figura se muestra el panel Búsqueda de contexto para una entidad seleccionada en la vista Detalles de incidente. La vista muestra la pestaña Incidentes del panel Búsqueda de contexto.



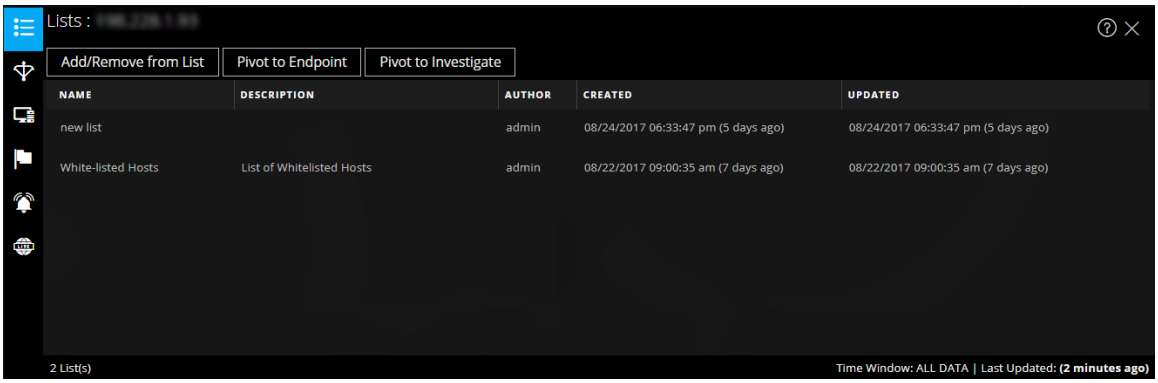
En la siguiente tabla se describen los datos disponibles en cada pestaña y las entidades compatibles.

Pestaña	Descripción	Entidades compatibles
(Listas)	Muestra todos los datos de lista asociados con la entidad o el valor de metadatos seleccionados. El resultado se ordena por la lista que se actualizó por última vez.	Todas las entidades
(Archer)	Muestra información sobre los recursos, junto con clasificaciones de criticidad que usan el origen de datos Archer.	IP y host
(Active Directory)	Muestra toda la información del usuario seleccionado.	Usuario

Pestaña	Descripción	Entidades compatibles
 (NetWitness Endpoint)	Muestra la información del origen de datos NetWitness Endpoint para la entidad o el valor de metadatos seleccionados, la cual incluye las máquinas, los módulos y los niveles de IIOC. Los módulos se muestran del puntaje de IOC más alto al puntaje de IIOC más bajo y los niveles de IIOC, de los más altos a los más bajos.	IP, dirección de MAC y host
 (Incidentes)	Muestra la lista de incidentes asociados con la entidad o el valor de metadatos seleccionados. El resultado se ordena de los incidentes más recientes a los más antiguos.	Todas las entidades
 (Alertas)	Muestra la lista de alertas asociadas con la entidad o el valor de metadatos seleccionados. El resultado se ordena de las alertas más recientes a las más antiguas.	Todas las entidades
 (Live Connect)	Muestra información relacionada con Live Connect.	IP, dominio y hash de archivo

Listas

El panel Búsqueda de contexto para Listas muestra una o más listas asociadas con la entidad o el valor de metadatos seleccionados. La siguiente figura es un ejemplo del panel de contexto para Listas.

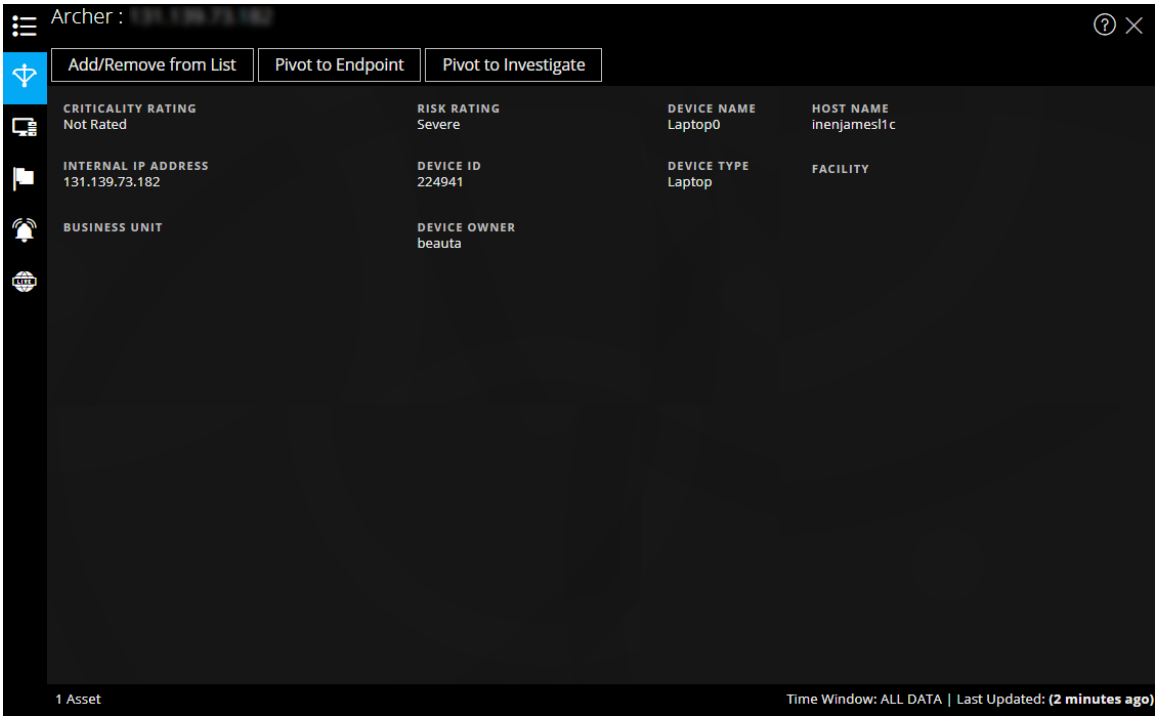


La siguiente información se muestra para Listas.

Campo	Descripción
Nombre	El nombre de la lista (definido durante la creación de la lista).
Descripción	La descripción de la lista (definida durante la creación de la lista).
Autor	El propietario que creó la lista.
Creado	La fecha en que se creó la lista.
Actualizado	La fecha en que la lista se actualizó o se modificó por última vez.
Conteo	La cantidad de listas en las cuales está disponible la entidad o el valor de metadatos seleccionados.
Ventana de tiempo	Se basa en el valor que se configura para el campo “Consultar últimos” del cuadro de diálogo Configurar respuestas. De forma predeterminada, se obtienen todos los datos de Listas.
Última actualización	La hora en que Context Hub obtuvo y almacenó los datos de búsqueda en la caché.

Archer

El panel Búsqueda de contexto para Archer muestra información sobre los recursos, junto con calificaciones de criticidad que usan el origen de datos Archer para las entidades y los valores de metadatos de IP y host. La siguiente figura es un ejemplo del panel de contexto para Archer.



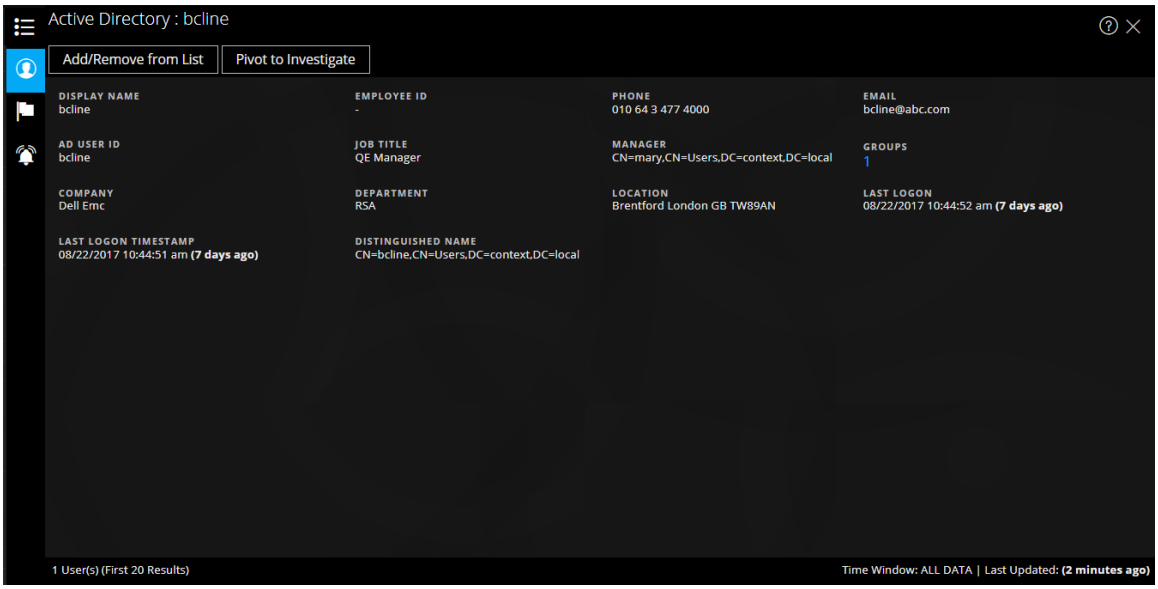
La siguiente información se muestra para Archer.

Campo	Descripción
Clasificación de criticidad	Muestra la criticidad operacional del dispositivo en función de las aplicaciones que apoya. Las clasificaciones de criticidad se pueden configurar en No clasificado, Baja, Media-baja, Media, Media-alta o Alta.
ID de dispositivo	Muestra el valor completado de forma automática que identifica de manera exclusiva el registro en todas las aplicaciones del sistema.
Nombre del dispositivo	Muestra el nombre único del dispositivo.
Propietario de dispositivos	Muestra los propietarios del dispositivo que son responsables de este y reciben derechos de lectura y actualización para el registro.

Campo	Descripción
Nombre del host	Muestra el nombre de host del dispositivo.
Instalaciones	Proporciona vínculos a los registros de la aplicación Instalaciones que se relacionan con este dispositivo.
Unidad de negocios	Proporciona vínculos a los registros de la aplicación Unidad de negocios que se relacionan con este dispositivo.
Clasificación de riesgo	Calcula la clasificación de riesgo del dispositivo según la evaluación más reciente y la clasificación de riesgo promedio de las instalaciones que utilizan el dispositivo. La clasificación de riesgo se puede configurar en Grave, Alta, Mediana, Baja o Mínima.
Tipo	Muestra el tipo de dispositivo, como servidor, laptop, escritorio, etc.
Dirección IP	Muestra la dirección IP interna primaria del dispositivo.
Conteo	Muestra la cantidad de recursos disponibles.
Ventana de tiempo	Se basa en el valor que se configura para el campo “Consultar últimos” del cuadro de diálogo Configurar respuestas. De forma predeterminada, se obtienen todos los datos para Archer.
Última actualización	La hora en que Context Hub obtuvo y almacenó los datos de búsqueda en la caché.

Active Directory

La siguiente figura es un ejemplo del panel de contexto para Active Directory.



El panel Búsqueda de contexto para Active Directory muestra toda la información, las alertas y los incidentes relacionados para un usuario. Puede realizar una búsqueda mediante los siguientes formatos:

- userPrincipalName
- Domain\UserName
- sAMAccountName

Si el usuario existe en dominios múltiples o bosques múltiples, se muestra toda la información contextual relacionada para el usuario específico.

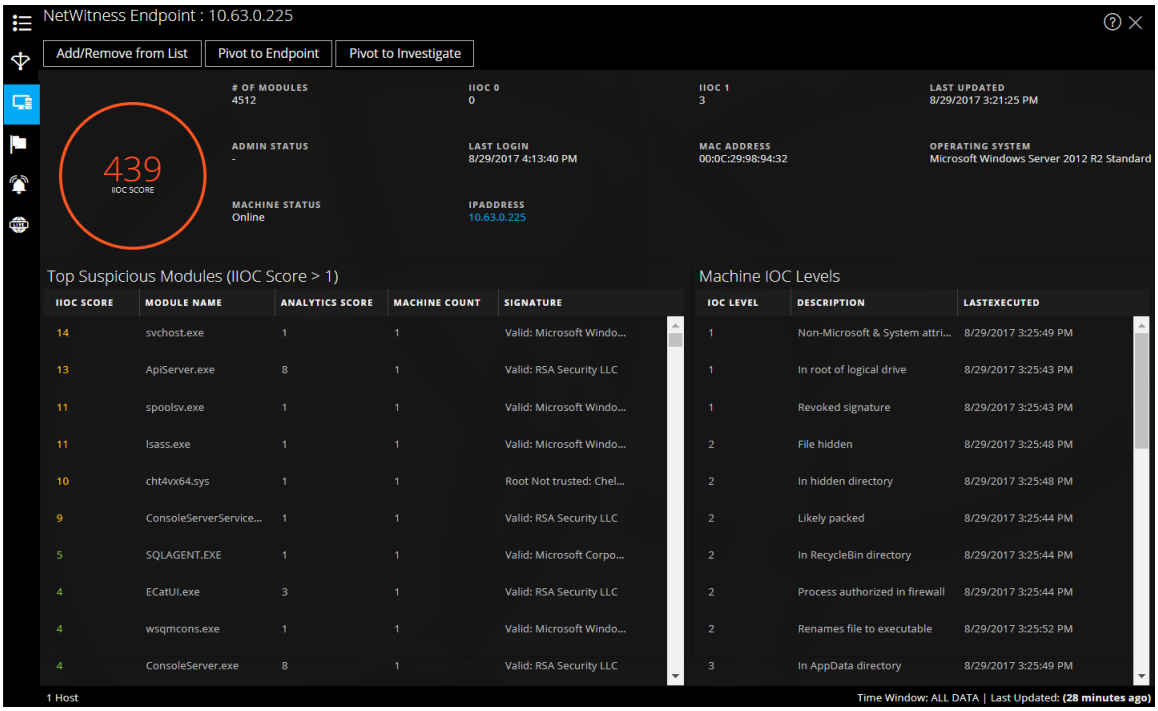
La siguiente información se muestra para Active Directory.

Campo	Descripción
Nombre para mostrar	Muestra el nombre del usuario específico.
ID de empleado	Muestra el ID de empleado del usuario específico.
Teléfono	Muestra el número de teléfono del usuario específico.
Correo electrónico	Muestra el ID de correo electrónico del usuario específico.
ID de usuario de AD	Muestra la identificación única del usuario específico dentro de una organización.
Cargo	Muestra la designación del usuario específico.
Administrador	Muestra el nombre del administrador de

Campo	Descripción
Grupos	Muestra la lista de grupos de los cuales el usuario específico es miembro.
Empresa	Muestra el nombre de la empresa a la cual pertenece el usuario específico.
Departamento	Muestra el nombre del departamento dentro de la organización a la cual pertenece el usuario específico.
Ubicación	Muestra la ubicación del usuario específico.
Último inicio de sesión	Muestra la hora en que el usuario específico inició sesión en el sistema solo si el Catálogo global está definido.
Último registro de fecha y hora de inicio de sesión	Muestra la hora en que el usuario específico inició sesión en el sistema.
Nombre distinguido	Muestra el nombre único asignado al usuario.
Conteo	Muestra la cantidad de usuarios.
Ventana de tiempo	Se basa en el valor que se configura para el campo “Consultar últimos” del cuadro de diálogo Configurar ajustes de orígenes de datos. De forma predeterminada, se obtienen todos los datos de Active Directory.
Última actualización	La hora en que Context Hub obtuvo y almacenó los datos de búsqueda en la caché.

NetWitness Endpoint

En el panel Búsqueda de contexto para NetWitness Endpoint se muestra la siguiente información.



La siguiente información se muestra para IIOC.

Campo	Descripción
Cantidad de módulos	Muestra la cantidad de módulos que se buscan.
Estado administrativo	Muestra el estado administrativo (si corresponde).
Última actualización	Muestra la hora en que los datos se actualizaron por última vez.
Último inicio de sesión	Muestra la hora en que el usuario inició sesión por última vez.
Dirección MAC	Dirección MAC de la máquina.
Sistema operativo	Versión del sistema operativo que usa la máquina de NetWitness Endpoint.
Estado de la máquina	Muestra si el módulo que se busca está En línea, Offline, Activo o Inactivo.
Dirección IP	Muestra la dirección IP del módulo específico.

La siguiente información se muestra para Módulos.

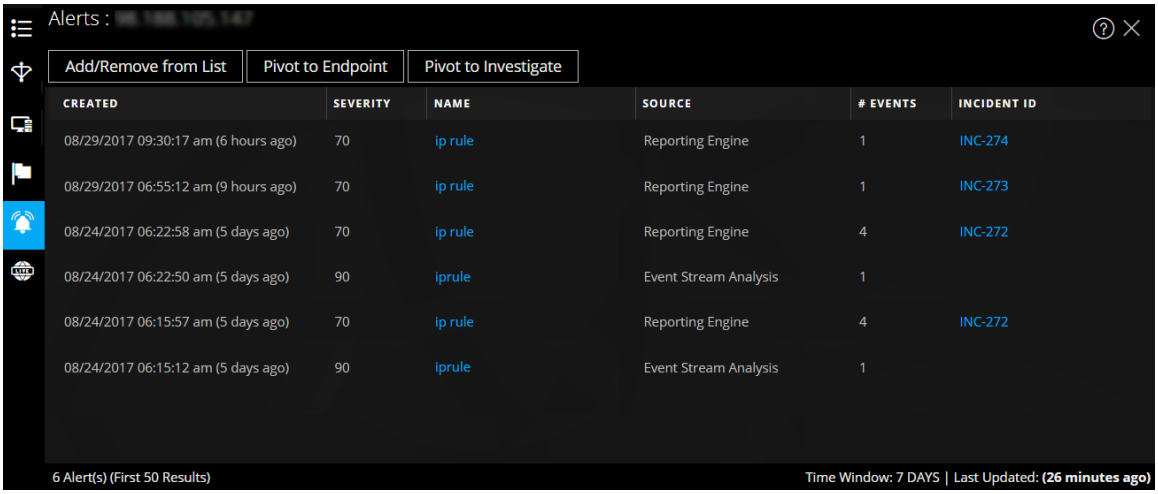
Campo	Descripción
Puntaje de IIOC	Un puntaje de IIOC de la máquina es un puntaje agregado que se basa en los puntajes del módulo. Esto se basa en el valor configurado para el campo “Puntaje de IIOC mínimo” en los ajustes de orígenes de datos de Context Hub. El valor predeterminado para “Puntaje de IIOC mínimo” es 500. Consulte el tema “Configurar ajustes de orígenes de datos de Context Hub” en la *Guía de configuración de Context Hub*.
Nombre de módulo	Nombre del módulo que se busca.
Puntaje de análisis	Cantidad de archivos activos para la máquina seleccionada.
Conteo de máquinas	Indica cuándo se actualizaron por última vez los resultados del escaneo en la base de datos de NetWitness Endpoint.
Firma	Indica si el archivo está o no firmado y si es o no válido, y proporciona información acerca del signatario. Por ejemplo, Google, Apple, etc.

La siguiente información se muestra para Máquinas.

Campo	Descripción
Niveles de IIOC	Muestra los niveles de IOC.
Descripción	Muestra la descripción para el nivel de IOC, si está disponible.
Última ejecución	Muestra la hora en que se ejecutó la acción.
Conteo	Muestra la cantidad de hosts que se buscan.
Ventana de tiempo	Se basa en el valor que se configura para el campo “Consultar últimos” del cuadro de diálogo Configurar ajustes de orígenes de datos. De forma predeterminada, se obtienen todos los datos de NetWitness Endpoint.
Última actualización	Indica cuándo se actualizaron por última vez los resultados del escaneo en la base de datos de NetWitness Endpoint.

Alertas

La siguiente figura es un ejemplo del panel de contexto para Alerts que se muestra, en primer lugar, en función del tiempo (más recientes a más antiguas) y, a continuación, la gravedad.



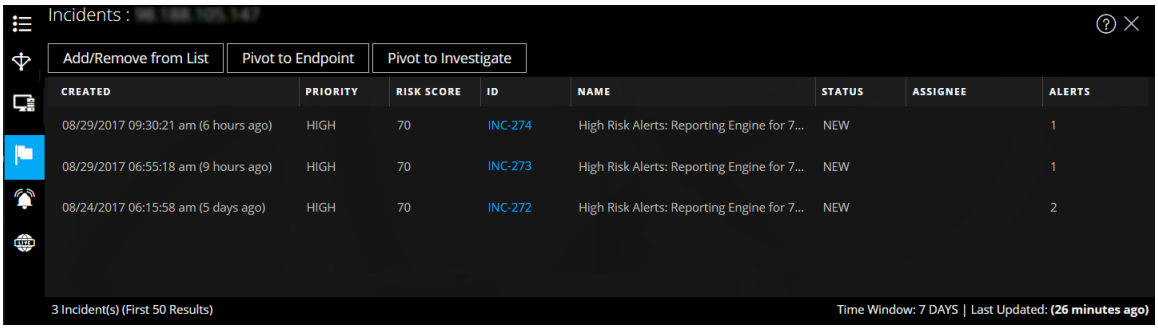
En el panel Búsqueda de contexto para Alertas se muestra la siguiente información.

Campo	Descripción
Creado	Fecha y hora en que se creó la alerta.
Gravedad	Valor de gravedad de las alertas
Nombre	Nombre de la alerta. Haga clic en el nombre para ver los detalles de una alerta específica.
Origen	Nombre del origen de alerta desde donde se activó la alerta.
Cantidad de eventos	Número de eventos asociados con la alerta.
ID del incidente	Este es el ID del incidente con el cual está asociada la alerta (si corresponde). Haga clic en el ID para ver los detalles de una alerta específica.
Conteo	Muestra la cantidad de alertas. De forma predeterminada, solo se muestran las primeras 100 alertas. Para obtener más información acerca de cómo configurar los ajustes, consulte el tema “Configurar ajustes de orígenes de datos de Context Hub” en la *Guía de configuración de Context Hub*.

Campo	Descripción
Ventana de tiempo	Se basa en el valor que se configura para el campo “Consultar últimos” del cuadro de diálogo Configurar ajustes de orígenes de datos. De forma predeterminada, se recupera los datos de alertas de los últimos 7 días.
Última actualización	Indica la última vez en que se recuperaron datos contextuales desde el origen de datos.

Incidentes

La siguiente figura es un ejemplo del panel de contexto para Incidentes que se basa, en primer lugar, en el tiempo (más recientes a más antiguos) y, a continuación, en el estado de prioridad.



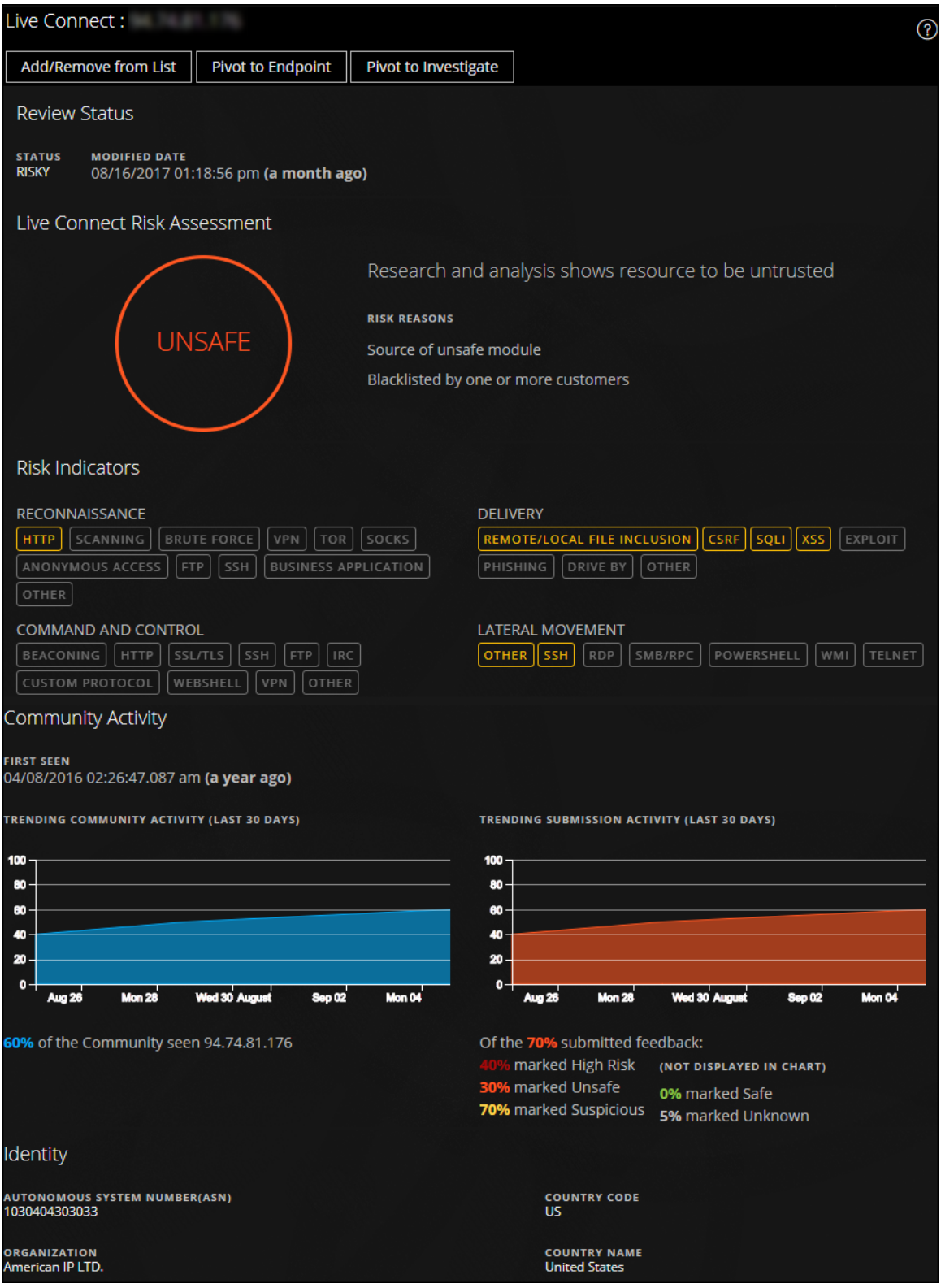
En el panel Búsqueda de contexto para Incidentes se muestra la siguiente información.

Campo	Descripción
Creado	La fecha de creación del incidente.
Prioridad	Estado de prioridad de los incidentes.
Puntaje de riesgo	Puntaje de riesgo de los incidentes.
ID	ID del incidente. Cuando se hace clic, se muestran más detalles acerca del incidente.
Nombre	Nombre del incidente.
Estado	Estado del incidente.
Usuario asignado	Propietario actual del incidente.
Alertas	Cantidad de alertas asociadas con el incidente.

Campo	Descripción
Conteo	Muestra la cantidad de incidentes. De forma predeterminada, solo se muestran las primeras 100 alertas. Para obtener más información acerca de cómo configurar los ajustes, consulte el tema “Configurar ajustes de orígenes de datos de Context Hub” en la *Guía de configuración de Context Hub*.
Ventana de tiempo	Se basa en el valor que se configura para el campo “Consultar últimos” del cuadro de diálogo Configurar ajustes de orígenes de datos. De forma predeterminada, se recupera los datos de alertas de los últimos 7 días.
Última actualización	Indica la última vez en que se recuperaron datos contextuales desde el origen de datos.

Live Connect

La siguiente figura es un ejemplo del panel de contexto para Live Connect.


Live Connect :
Add/Remove from List
Pivot to Endpoint
Pivot to Investigate
Review Status
STATUS
RISKY
MODIFIED DATE
08/16/2017 01:18:56 pm (a month ago)
Live Connect Risk Assessment
UNSAFE
Research and analysis shows resource to be untrusted
RISK REASONS
Source of unsafe module
Blacklisted by one or more customers
Risk Indicators
RECONNAISSANCE
HTTP
SCANNING
BRUTE FORCE
VPN
TOR
SOCKS
ANONYMOUS ACCESS
FTP
SSH
BUSINESS APPLICATION
OTHER
DELIVERY
REMOTE/LOCAL FILE INCLUSION
CSRF
SQLI
XSS
EXPLOIT
PHISHING
DRIVE BY
OTHER
COMMAND AND CONTROL
BEACONING
HTTP
SSL/TLS
SSH
FTP
IRC
CUSTOM PROTOCOL
WEBSHELL
VPN
OTHER
LATERAL MOVEMENT
OTHER
SSH
RDP
SMB/RPC
POWERSHELL
WMI
TELNET
Community Activity
FIRST SEEN
04/08/2016 02:26:47.087 am (a year ago)
TRENDING COMMUNITY ACTIVITY (LAST 30 DAYS)
100
80
60
40
20
0
Aug 26
Mon 28
Wed 30 August
Sep 02
Mon 04
TRENDING SUBMISSION ACTIVITY (LAST 30 DAYS)
100
80
60
40
20
0
Aug 26
Mon 28
Wed 30 August
Sep 02
Mon 04
60% of the Community seen 94.74.81.176
Of the 70% submitted feedback:
40% marked High Risk
(NOT DISPLAYED IN CHART)
30% marked Unsafe
0% marked Safe
70% marked Suspicious
5% marked Unknown
Identity
AUTONOMOUS SYSTEM NUMBER(ASN)
1030404303033
COUNTRY CODE
US
ORGANIZATION
American IP LTD.
COUNTRY NAME
United States

El panel Live Connect muestra la siguiente información:

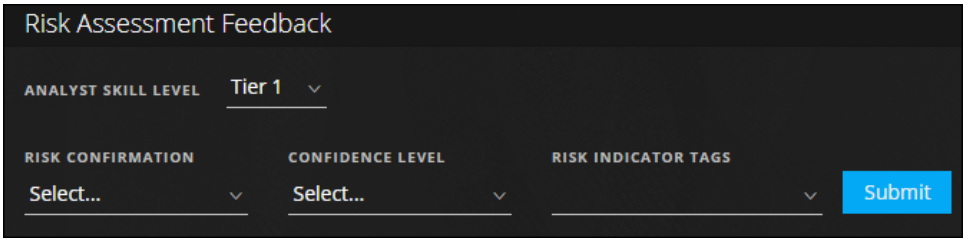
- Estado de revisión
- Evaluación del riesgo de Live Connect
- Indicadores de riesgo
- Actividad de la comunidad
- WHOIS
- Archivos relacionados, dominios y direcciones IP
- Identidad
- Información del certificado

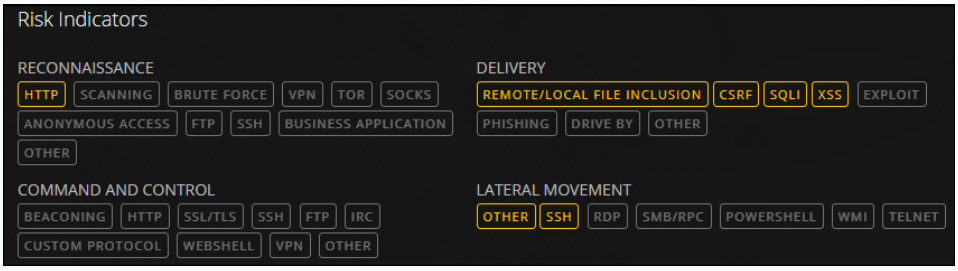
En el panel Búsqueda de contexto para Live Connect se muestra la siguiente información.

Campo	Descripción
Estado de revisión	Muestra el estado de revisión de la entidad de Live Connect seleccionada (IP, archivo o dominio) en función de la actividad de los analistas. Esto proporciona visibilidad de la actividad de los analistas dentro de una organización. **Estado** Los siguientes son los tipos de estado: • **Nuevo:** Si los resultados de búsqueda de una dirección IP se ven por primera vez dentro de la organización. • **Vistos:** Si un analista dentro de la organización ya vio los resultados de búsqueda de una dirección IP. • **Marcada como segura:** Si un analista dentro de la organización ya vio los resultados de búsqueda y marcó la dirección IP como segura. • **Marcada como riesgosa:** Si un analista dentro de la organización ya vio los resultados de búsqueda y marcó la dirección IP como riesgosa.

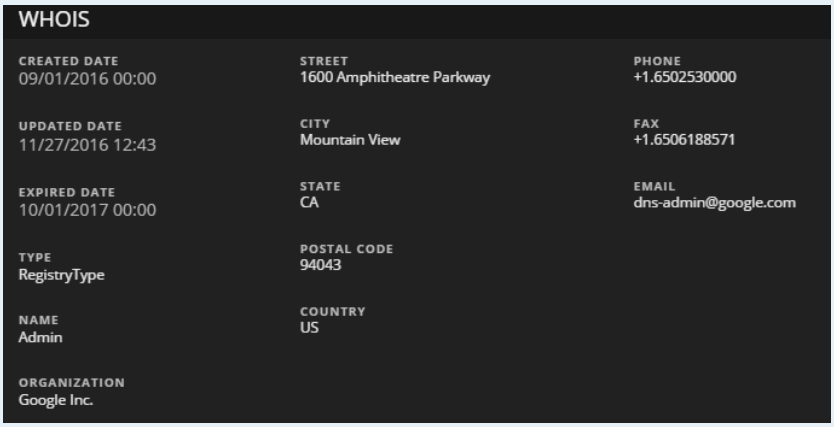
Campo	Descripción
Evaluación del riesgo	Muestra la evaluación del riesgo para la entidad de Live Connect seleccionada (IP, archivo o dominio) de acuerdo con el análisis y los comentarios de los analistas de Live Connect. Las categorías de evaluación del riesgo son: • **Segura:** La entidad de Live Connect se considera segura. • **Desconocido:** Live Connect no tiene suficiente información acerca de esta entidad para calcular el riesgo. • **Alto riesgo**: Se marca como de "Alto riesgo" en función del análisis y los motivos de riesgo que proporciona la comunidad. Las entidades marcadas como de "Alto riesgo" requieren atención inmediata. • **Sospechoso**: Se marca como "Sospechoso" en función del análisis y los motivos de riesgo que proporciona la comunidad. El análisis indica actividad potencialmente amenazante que requiere una acción. • **Inseguro:** Se marca como "Sospechoso" en función del análisis y los motivos de riesgo que proporciona la comunidad. La entidad se clasifica como Alto riesgo, Sospechoso o Inseguro y muestra los motivos de riesgo asociados según corresponde.

Campo	Descripción
Comentarios sobre la evaluación del riesgo	Comentarios sobre la evaluación del riesgo permite que el analista envíe comentarios de inteligencia de amenazas acerca de una entidad al servidor de Live Connect. • **Nivel de habilidad del analista** Las siguientes son las opciones para el nivel de habilidad del analista: ◦ **Nivel 1**: Los analistas de este nivel suelen definir procedimientos para las correcciones y decidir si un incidente se debe elevar a otras áreas de un SOC (centro de operaciones de seguridad). Este es el valor predeterminado. ◦ **Nivel 2**: Los analistas investigan incidentes y capturan inteligencia en una investigación para enviarla a los diversos flujos de trabajo en un SOC. ◦ **Nivel 3**: Los analistas comparten los resultados de la investigación con la organización del SOC. Por lo general, administran incidentes y disponen de amplitud y profundidad en las habilidades y las herramientas necesarias para la respuesta ante incidentes. **Nota:** Mientras se crea un nuevo usuario para NetWitness Suite (analista), un administrador debe poder identificar al usuario como un analista de nivel 1, nivel 2 o nivel 3. • **Confirmación de riesgo**: La confirmación de riesgo de la entidad de Live Connect seleccionada (IP, archivo o dominio). Las categorías de confirmación de riesgo son: ◦ **Segura**: La entidad de Live Connect se considera segura. ◦ **Desconocido**: El analista no tiene información suficiente para proporcionar una confirmación de riesgo. ◦ **Alto riesgo**: Se marca como de “Alto riesgo” en función del análisis y los motivos de riesgo que proporciona la comunidad. Las entidades marcadas como de “Alto riesgo” requieren atención inmediata. ◦ **Sospechoso**: Se marca como “Sospechoso” en función del análisis y los motivos de riesgo que proporciona la comunidad. El análisis indica actividad potencialmente amenazante que requiere una acción. ◦ **Inseguro**: Se marca como “Inseguro” en función del análisis y los motivos de riesgo que proporciona la comunidad.

Campo	Descripción
	• **Nivel de confianza**: El nivel de confianza de un analista en la entrega de comentarios para la entidad de Live Connect. Las categorías de nivel de confianza son las siguientes: ◦ Alta ◦ Media ◦ Baja • **Etiquetas de indicador de riesgo**: Permite seleccionar una categoría de etiqueta en función del análisis. 
Actividad de la comunidad	Actividades de la comunidad, como las siguientes: • Fecha en que se vio por primera vez en la comunidad. • Tiempo desde que la dirección IP, el archivo o el dominio se vieron por primera vez (Hora actual: hora en que se vio por primera vez). **Actividad de la comunidad de tendencias:** Si la dirección IP se conoce dentro de la comunidad de RSA, se muestra una representación gráfica de la tendencia de actividad de la comunidad para lo siguiente: • Usuarios (en %) que vieron la dirección IP en la comunidad de Live Connect con el tiempo. • Usuarios (en %) que enviaron comentarios para la dirección IP. • Usuarios (en %) que marcaron la dirección IP como insegura con el tiempo.

Campo	Descripción
Indicadores de riesgo	Los indicadores de riesgo se resaltan en función de las etiquetas que asigna la comunidad a las entidades (direcciones IP, archivos o dominios).  Las etiquetas se categorizan como se indica a continuación: • Reconocimiento • Distribución • Comando y control • Movimiento lateral • Escalación de privilegio • Creación de paquetes y exfiltración Estas etiquetas son ejemplos y varían en función de las entradas recibidas de la comunidad en el servidor de Live Connect. El analista puede elegir las etiquetas de indicadores de riesgo apropiadas y proporcionar los comentarios de revisión. Una etiqueta resaltada indica que la entidad seleccionada está asociada a esa categoría y etiqueta específicas. Cuando se hace clic en una etiqueta resaltada, se muestra su descripción.

Campo	Descripción
Identidad	Proporciona la siguiente información de identidad para la entidad o el valor de metadatos seleccionados: Para la dirección IP: • Número de sistema autónomo (ASN) • Prefijo • Código del país y Nombre de país • Inscrito (organización) • Fecha Para hash de archivo: • Nombre de archivo • Tamaño del archivo • MD5 • SH1 • SH256 • Hora de compilación • Tipo MIME Para un dominio: • Nombre del dominio • Dirección IP asociada
Información del certificado	Proporciona la siguiente información del certificado para el hash de archivo seleccionado: • Emisor del certificado • Validez del certificado • Algoritmo de firma • Número de serie del certificado

Campo	Descripción
Información WHO IS	La información **WHO IS** proporciona los detalles de propiedad de un dominio determinado.  Se muestra la siguiente información del propietario del dominio: • Fecha de creación • Fecha de actualización • Fecha de vencimiento • Tipo (tipo de registro) • Nombre • Organización • Dirección con código postal • País • Teléfono • Fax • Correo electrónico

Campo	Descripción
Archivos relacionados	Se muestran los archivos relacionados para la dirección IP y el dominio de los tipos de entidad. Se muestra una lista de archivos asociados conocidos, junto con la siguiente información: • Clasificación de riesgo de Live Connect (Seguro, Riesgoso o Desconocido) • Nombre de archivo • MD5 • Fecha y hora de compilación • Hash de importación de función de API • Tipo MIME
Dominios relacionados	Se muestran los dominios relacionados para la dirección IP y los archivos de los tipos de entidad. Se muestra una lista de dominios asociados conocidos, junto con la siguiente información: • Clasificación de riesgo de Live Connect (Seguro, Riesgoso o Desconocido) • Nombre del dominio • Nombre de país • Fecha de registro • Fecha de vencimiento • Dirección de correo electrónico del inscrito

Campo	Descripción
IP relacionadas	Se muestran las direcciones IP relacionadas para el dominio y los archivos de los tipos de entidad. Se muestra una lista de direcciones IP asociadas conocidas, junto con la siguiente información: • Clasificación de riesgo de Live Connect (Seguro, Riesgoso o Desconocido) • Dirección IP • Nombre del dominio • Código del país y Nombre de país • Nombre de país • Fecha de registro • Fecha de vencimiento • Dirección de correo electrónico del inscrito