RSA NETWITNESS® PLATFORM

RSA NetWitness UEBA Guía del usuario

para la versión 11.2

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.

February 2019

Contenido

Introducción

RSA NetWitness UEBA (User and Entity Behavior Analytics) es una solución de analítica avanzada para descubrir, investigar y monitorear comportamientos riesgosos en todos los usuarios y todas las entidades del ambiente de red. NetWitness UEBA se utiliza para lo siguiente:

- Detección de usuarios maliciosos y deshonestos
- Detección de comportamientos de alto riesgo
- Descubrimiento de ataques
- Investigación de amenazas de seguridad emergentes

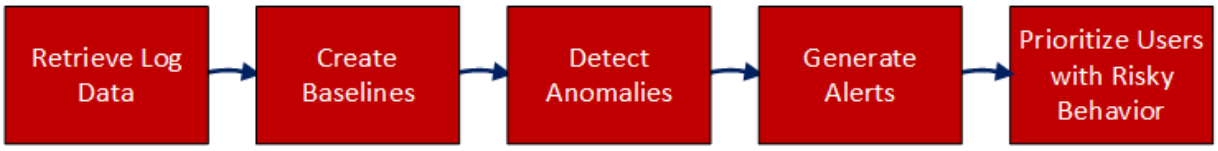
Nota: De manera inmediata, solamente los registros de Windows son compatibles. Puede agregar orígenes de registro adicionales para alimentar los modelos existentes. Para obtener más información, consulte Orígenes de registro compatibles.

NetWitness UEBA aprovecha los datos existentes en registros de NetWitness Platform y faculta al SOC empresarial y a los analistas con información valiosa y funcionalidades investigativas que permiten moderar las amenazas cibernéticas.

Esta guía está diseñada para analistas y administradores del SOC, y proporciona información e instrucciones para usar todas las funciones y las funcionalidades de NetWitness UEBA. Describe las metodologías de investigación clave, las principales funcionalidades del sistema, los casos de uso comunes y las instrucciones paso a paso para las estrategias de flujo de trabajo recomendadas.

Cómo funciona NetWitness UEBA

NetWitness UEBA utiliza analítica para detectar anomalías en datos de registro y obtiene resultados de comportamiento a partir de ellos. En este proceso hay cinco pasos básicos, los que se muestran en el siguiente diagrama:



En la siguiente tabla se proporciona una descripción breve de cada uno de estos pasos.

Paso	Descripción	Más información
1. Recuperar datos de registro	NetWitness UEBA recupera datos de registro de la base de datos de NetWitness Platform (NWDB) y los utiliza para crear resultados analíticos.	Consulte Recuperar datos de registro

Paso	Descripción	Más información
2. Crear bases	Las bases se obtienen del análisis detallado del comportamiento normal de los usuarios y se utilizan como punto de partida para la comparación con el comportamiento de los usuarios conforme avanza el tiempo.	Consulte Crear bases
3. Detectar anomalías	Una anomalía es una desviación del comportamiento de base normal de un usuario. NetWitness UEBA realiza un análisis estadístico para comparar cada actividad nueva con la base. Las actividades del usuario que se desvían de los valores de base esperados reciben un puntaje correspondiente que refleja la gravedad de la desviación.	Consulte Detectar anomalías
4. Generar alertas	Todas las anomalías encontradas en el paso 3 se agrupan en lotes por hora. Cada lote recibe un puntaje en función de la singularidad de sus indicadores. Si la composición del indicador es única en comparación con las composiciones en lotes por hora históricas de un usuario, es probable que este lote se transforme en una alerta.	Consulte Generar alertas
5. Asignar prioridad a los usuarios con comportamiento riesgoso	NetWitness UEBA da prioridad al riesgo potencial de un usuario mediante una fórmula de puntaje aditivo simplificada. A cada alerta se le asigna una gravedad que aumenta el puntaje de un usuario en una cantidad predefinida de puntos. Los usuarios con puntajes altos están asociados a varias alertas o están asociados a alertas de niveles altos de gravedad.	Consulte Asignar prioridad a los usuarios con comportamiento riesgoso

Recuperar datos de registro

El servidor de NetWitness UEBA se conecta al servicio Broker o Concentrator para recuperar datos de registro de Concentrators. Puede utilizar el servicio Broker que está disponible en el servidor de NetWitness Platform Admin si la implementación no cuenta con un Broker exclusivo. Durante la instalación de NetWitness UEBA, el administrador especifica la dirección IP del servicio Broker.

Para obtener más información, consulte el tema “(Opcional) Tarea 2: Instalar NetWitness UEBA” en la *Guía de instalación de hosts físicos de NetWitness Platform 11.2*.

Crear bases

NetWitness UEBA utiliza aprendizaje automático para analizar varios aspectos de las acciones de un usuario dentro de un flujo de datos de registro y crea gradualmente una base multidimensional de comportamiento típico de cada usuario. Por ejemplo, la base puede incluir información sobre las horas en las que un usuario suele iniciar sesión.

Las bases de comportamiento también se crean en un nivel global para describir las actividades comunes observadas en toda la red. Si un horario de trabajo fue anormal para un usuario, pero no lo es para la organización, los algoritmos de reducción de falsos positivos disminuyen el impacto en el puntaje de la alerta.

Los modelos se actualizan con frecuencia y mejoran constantemente a medida que avanza el tiempo.

Nota: NetWitness UEBA requiere 28 días de datos de registro históricos para crear una base adecuada para todos los usuarios de la red. Sin embargo, RSA recomienda configurar NetWitness UEBA de modo que comience a crear la base a partir de sus datos dos meses antes de la fecha de implementación `<today-60days>`. Los primeros 28 días se utilizarán para la capacitación del modelo y no recibirán un puntaje. Los 32 días restantes se aprovechan para mejorar y actualizar el modelo, y también reciben un puntaje para proporcionar el valor inicial.

Nota: Para la versión 11.2, la compatibilidad con los ambientes con varios dominios es limitada. Los valores de nombre de usuario distintos, que se registran en diferentes dominios, se normalizan y, a continuación, se combinan en una entidad modelada. En consecuencia, a los diferentes usuarios, que comparten el mismo nombre de usuario en diferentes dominios, se les atribuirá incorrectamente una única entidad normalizada.

Detectar anomalías

Después de establecer una base de comportamiento para todos los usuarios del ambiente, cada evento entrante se compara con la base y recibe un puntaje para determinar si el nuevo comportamiento es anormal y, específicamente, si se trata de una desviación considerable de la base. Por ejemplo, si el horario de trabajo normal de un usuario es de 9:00 h a 17:00 h, una nueva actividad a las 18:00 h o a las 19:00 h no es una desviación considerable y es probable que no reciba un puntaje que la califique como una anomalía. Sin embargo, una autenticación a medianoche es una desviación considerable y recibe un puntaje que la califica como una anomalía.

Si se detectan anomalías, se convierten en indicadores de riesgo, los que se describen como Indicadores en la interfaz del usuario. NetWitness UEBA utiliza indicadores para definir actividad anómala validada, como inicios de sesión de usuario sospechosos, ataques de contraseña de fuerza bruta, cambios inusuales de los usuarios y acceso a archivos anormal. Los indicadores representan anomalías encontradas en un único evento o en varios eventos dispuestos en lotes conforme avanza el tiempo.

Generar alertas

Todas las anomalías que se encuentran se agrupan en lotes de nombre de usuario y por hora. Cada lote recibe un puntaje en función de la singularidad de la composición de sus indicadores. Si una composición es única en comparación con el historial del usuario, es probable que este lote se transforme en una alerta y las anomalías, en indicadores. Un lote de anomalías con un puntaje alto se transforma en una alerta que contiene indicadores de riesgo validados.

Por ejemplo, una actividad anormal por sí sola, incluso si ocurre cientos de veces al día en un ambiente corporativo grande, no refleja necesariamente el riesgo para una cuenta. Sin embargo, un comportamiento anormal que se produce con una gran cantidad de otros comportamientos anormales podría indicar que la cuenta se vulneró. La aparición conjunta de estos tres comportamientos puede indicar que se requiere un análisis adicional.

- Autenticación desde una computadora anormal
- Varios intentos de autenticación identificados en un intervalo de tiempo breve
- Este usuario eliminó varios archivos del recurso compartido de archivos corporativo

Nota: La interfaz del usuario de NetWitness UEBA puede aparecer inicialmente vacía porque las alertas no se generan hasta que se establecen las bases. Si no hay datos de auditoría históricos cuando se habilita NetWitness UEBA, el sistema comienza a generar las bases desde el momento en que se implementa y requiere que transcurran 28 días completos antes de comenzar a generar nuevas alertas. Si se procesan datos de auditoría históricos cuando se habilita NetWitness UEBA, las alertas aparecen una vez procesados los datos históricos, normalmente en un máximo de dos a cuatro días.

Asignar prioridad a los usuarios con comportamiento riesgoso

Los puntajes de los usuarios son una herramienta principal para la asignación de prioridad de los incidentes. El puntaje del usuario se basa en un cálculo aditivo simple de las alertas del usuario. Las alertas y los comentarios de los analistas son los únicos factores en el cálculo del puntaje del usuario, y tienen impacto en los puntajes que determinan sus niveles de gravedad.

Se utiliza un código de color unificado para los puntajes de los usuarios y de las alertas:

Gravedad	Color	Puntaje
Crítica	Rojo	+20
Alta	Naranja	+15
Media	Amarillo	+10
Baja	Verde	+1

Orígenes de registro compatibles

NetWitness UEBA es compatible de manera nativa con los siguientes orígenes de registro de Windows:

- Windows Active Directory
- Actividad de inicio de sesión y autenticación de Windows
- Servidor de archivos de Windows

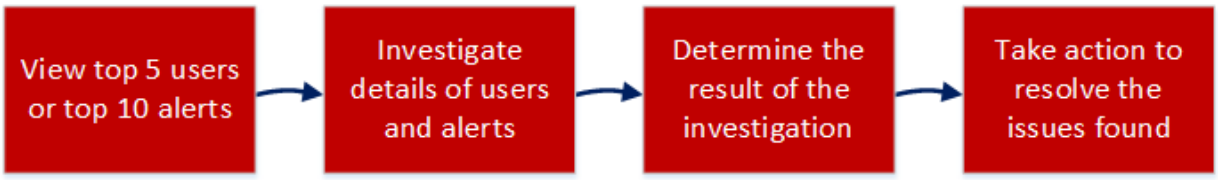
Flujos de trabajo recomendados

Para utilizar NetWitness UEBA de manera más eficaz, puede seguir dos flujos de trabajo, el flujo de trabajo de detección y el flujo de trabajo forense.

Flujo de trabajo de detección

El flujo de trabajo de detección le permite obtener una descripción general del estado del ambiente y, a continuación, centrarse en la investigación de los principales usuarios de alto riesgo y las alertas que se muestran en la pestaña Descripción general.

En el siguiente diagrama de flujo se ilustran los pasos que puede seguir para comenzar a detectar comportamiento sospechoso en el ambiente.



En la siguiente tabla se describe cada paso del flujo de trabajo.

Paso	Descripción	Instrucciones
Ver los cinco principales usuarios o las 10 principales alertas	En la pestaña Descripción general, tome nota de los usuarios con los comportamientos más riesgoso y de las alertas más críticas.	Investigar a los usuarios de alto riesgo e Investigar las alertas principales
Investigar detalles de los usuarios y las alertas	Desglose a información detallada sobre comportamientos riesgosos de los usuarios y alertas críticas para intentar determinar la causa de estas acciones y cómo resolverlas.	Investigar a los usuarios de alto riesgo e Investigar los indicadores
Determinar el resultado de la investigación	Analice la información de resumen que se proporciona en la interfaz del usuario a partir de los pasos anteriores e identifique áreas en las que debe centrarse para resolver los problemas que encontró.	Identificar a los usuarios de alto riesgo e Investigar los indicadores

Paso	Descripción	Instrucciones
Adoptar medidas para resolver los problemas encontrados	Céntrese en comportamientos de usuario y eventos específicos que debe abordar y utilice los resultados de esta investigación para mejorar y perfeccionar las investigaciones futuras.	Adoptar medidas en relación con los usuarios de alto riesgo

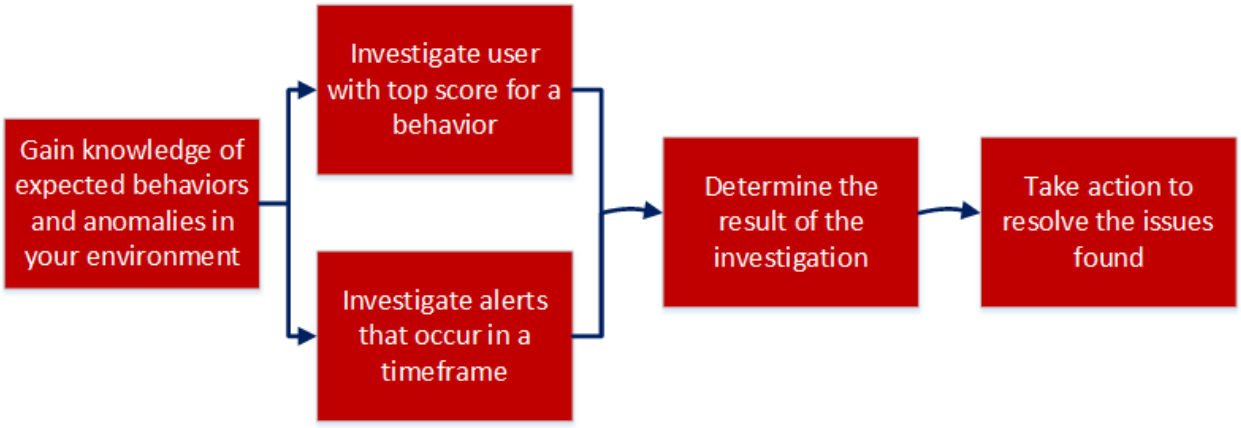
Flujo de trabajo forense

El flujo de trabajo forense se recomienda cuando se ha adquirido una comprensión de las anomalías y los comportamientos del usuario típicos del ambiente. Le permite centrarse en información forense específica que se basa en un comportamiento del usuario o en un intervalo de tiempo específico en el que se produjeron los eventos sospechosos.

Con la información forense, los analistas pueden determinar las acciones y los comportamientos que probablemente intentará el atacante mediante las siguientes preguntas:

- ¿Qué técnicas y comportamientos fundamentales son comunes a todas las intrusiones?
- ¿Qué indicios dejan estas técnicas?
- ¿Qué hacen los atacantes?
- ¿Cuáles son los comportamientos normales de mis cuentas y mis entidades?
- ¿Cuáles son mis máquinas críticas y dónde están ubicadas?

En el siguiente diagrama de flujo se ilustra cómo realizar la investigación sobre la información forense que se basa en un comportamiento de usuario específico o un intervalo de tiempo específico en el que se produjeron los eventos sospechosos.



En la siguiente tabla se describe cada paso del flujo de trabajo.

Paso	Descripción	Instrucciones
Obtener conocimiento de anomalías y comportamientos esperados en el ambiente	Establezca una base de comportamientos normales, anomalías esperadas y anomalías inesperadas, de modo que pueda centrarse en las anomalías que son significativas para el ambiente.	Recuperar datos de registro, Detectar anomalías y Generar alertas
Investigar al usuario con el puntaje más alto para un comportamiento específico	Seleccione un usuario con un puntaje alto para un comportamiento específico y recopile información detallada.	Investigar a los usuarios de alto riesgo e Investigar los indicadores

Paso	Descripción	Instrucciones
Investigar las alertas que ocurren en un intervalo de tiempo específico	Determine un intervalo de tiempo de interés y, en la pestaña Alertas, seleccione ese intervalo de tiempo para ver información detallada acerca de las alertas que ocurrieron durante ese período.	Investigar los indicadores
Determinar el resultado de la investigación	En función de su conocimiento del comportamiento del usuario esperado, céntrese en los indicadores que se muestran durante el período especificado y determine si es necesario resolver las anomalías que se descubrieron.	Investigar los indicadores e Identificar a los usuarios de alto riesgo
Adoptar medidas para resolver los problemas encontrados	Céntrese en comportamientos de usuario y eventos específicos que debe abordar y utilice los resultados de esta investigación para mejorar y perfeccionar las investigaciones futuras.	Adoptar medidas en relación con los usuarios de alto riesgo

Acceder a NetWitness UEBA

Nota: Para acceder al servicio NetWitness UEBA y a la pestaña Usuarios, debe tener asignada la función UEBA_Analyst o la función Administradores. Para obtener información sobre cómo asignar estas funciones, consulte el tema "Cómo funciona el control de acceso basado en funciones" de la *Guía de mantenimiento de usuarios y de la seguridad del sistema*. También debe asegurarse de que esté configurada la licencia correcta de NetWitness UEBA. Para obtener información acerca de la licencia de NetWitness UEBA, consulte el tema "Licencia de User and Entity Behavior Analytics" de la *Guía de administración de licencia*.

Para acceder a NetWitness UEBA, inicie sesión en NetWitness Platform y vaya a **Investigar** > **Usuarios**. Se muestra la vista Usuarios, que contiene todas las características de NetWitness UEBA.

Indicadores de NetWitness UEBA

En las siguientes tablas se enumeran los indicadores que se muestran cuando se detecta actividad potencialmente maliciosa.

Servidor de archivos de Windows

Indicador	Tipo de alerta	Descripción
Hora de acceso a archivos anormal	Horas no estándares	Un usuario accedió a un archivo a una hora anormal.
Cambio de permiso de acceso a archivos anormal	Cambios de permisos masivos	Un usuario cambió varios permisos de recursos compartidos.
Evento de acceso a archivos anormal	Acceso a archivos anormal	Un usuario accedió a un archivo de manera anormal.
Varios cambios de permisos de acceso a archivos	Cambios de permisos masivos	Un usuario cambió varios permisos de recursos compartidos de archivos.
Varios eventos de acceso a archivos	Usuario entrometido	Un usuario cambió varios permisos de recursos compartidos de archivos.
Varios eventos de acceso a archivos fallidos	Usuario entrometido	Un usuario no ha podido acceder a un archivo varias veces.
Varios eventos de archivos abiertos	Usuario entrometido	Un usuario abrió varios archivos.
Varios eventos de carpetas abiertas	Usuario entrometido	Un usuario abrió varias carpetas.
Varios eventos de eliminación de archivos	Acceso a archivos anormal	Un usuario eliminó varios archivos.

Active Directory

Indicador	Tipo de alerta	Descripción
Hora de cambio de Active Directory anormal	Horas no estándares	Un usuario realizó cambios en Active Directory a una hora anormal.
Cambio anormal en Active Directory	Cambios anormales en AD	Se realizó un cambio anormal en un atributo de Active Directory.
Varios cambios en la membresía en grupos	Cambios masivos en grupos	Un usuario realizó correctamente varios cambios en los grupos.

Indicador	Tipo de alerta	Descripción
Varios cambios en la administración de cuentas	Cambios anormales en AD	Un usuario realizó correctamente varios cambios en Active Directory.
Varios cambios en la administración de cuentas de usuarios	Cambios anormales en AD	Un usuario realizó correctamente varios cambios críticos en Active Directory.
Varios cambios fallidos en la administración de cuentas	Cambios anormales en AD	Un usuario no pudo realizar varios cambios en Active Directory.
Se cambió la contraseña de administrador	Cambio de la contraseña de administrador	Se cambió la contraseña de un administrador.
Se habilitó una cuenta de usuario	Cambios críticos en el estado de un usuario	Se habilitó la cuenta de un usuario.
Se deshabilitó una cuenta de usuario	Cambios críticos en el estado de un usuario	Se deshabilitó la cuenta de un usuario.
Se desbloqueó una cuenta de usuario	Cambios críticos en el estado de un usuario	Se desbloqueó la cuenta de un usuario.
Se cambió un tipo de cuenta de usuario	Cambios críticos en el estado de un usuario	Se cambió el tipo de un usuario.
Se bloqueó una cuenta de usuario	Cambios críticos en el estado de un usuario	Se bloqueó la cuenta de un usuario.
Se cambió la contraseña de usuario	Cambios críticos en el estado de un usuario	Se cambió la contraseña de un usuario.

Actividad de inicio de sesión

Indicador	Tipo de alerta	Descripción
Hora de inicio de sesión anormal	Horas no estándares	Un usuario inició sesión a una hora anormal.
Computadora anormal	Inicio de sesión de usuario en un host anormal	Un usuario intentó acceder a una computadora anormal.
Varias autenticaciones correctas	Varios inicios de sesión de un usuario	Un usuario inició sesión varias veces.
Varias autenticaciones fallidas	Varios inicios de sesión fallidos	Un usuario tuvo varios intentos de autenticación fallidos.
Inicio de sesión en varias computadoras	El usuario inició sesión en varios hosts	Un usuario intentó iniciar sesión desde varias computadoras.

Casos de uso de NetWitness UEBA para registros de Windows

NetWitness UEBA se centra en proporcionar funcionalidades de detección avanzadas para proteger a las empresas contra las amenazas internas. Estas podrían ser usuarios de confianza de la red vulnerados o, como alternativa, un atacante externo malicioso que aprovecha credenciales adquiridas mediante el uso de técnicas avanzadas de apropiación de cuentas.

El robo de identidad suele comenzar con el robo de credenciales, las se utilizan posteriormente para obtener acceso no autorizado a los recursos y para obtener el control de la red. Los atacantes también pueden aprovechar a los usuarios no administrativos vulnerados para obtener acceso a los recursos para los que tienen derechos administrativos y, a continuación, elevar esos privilegios.

Un atacante que usa credenciales robadas puede desencadenar eventos de red sospechosos mientras accede a los recursos. Es posible detectar el uso ilícito de credenciales, pero es necesario separar la actividad de los atacantes del alto volumen de eventos legítimos. NetWitness UEBA lo ayuda a separar la actividad posiblemente maliciosa de cualquier otro tipo de acción de usuario anormal, pero no riesgosa.

Los siguientes casos de uso definen ciertos tipos de riesgo y las funcionalidades del sistema correspondientes utilizadas para su detección. Puede revisar los casos de uso, que se representan con su tipo de alerta y descripción, para obtener una comprensión inicial del comportamiento riesgoso relacionado de cada uno. A continuación, con NetWitness UEBA, puede desglosar a los indicadores que reflejan las actividades de usuario posiblemente riesgosas para obtener más información. Para obtener más información acerca de los indicadores compatibles con NetWitness UEBA, consulte Indicadores de NetWitness UEBA.

Tipo de alerta	Descripción
Cambios masivos en grupos	Se realizó una cantidad anormal de cambios en los grupos. Investigue qué elementos cambiaron y decida si los cambios fueron legítimos o posiblemente el resultado de comportamiento riesgoso o malicioso. Esta actividad suele asociarse con el indicador **Varios cambios en la membresía en grupos**.
Se otorgaron privilegios elevados	Se delegaron privilegios de cuenta elevados a un usuario. Los atacantes suelen usar cuentas de usuario normales y otorgarles privilegios elevados para vulnerar la red. Investigue al usuario que recibió los privilegios elevados y decida si estos cambios fueron legítimos o posiblemente el resultado de comportamiento riesgoso o malicioso. Esta actividad suele asociarse con los indicadores **Se agregó un miembro anidado a un grupo empresarial crítico** y **Se agregó un miembro a un grupo empresarial crítico**.

Tipo de alerta	Descripción
Varios inicios de sesión fallidos	En los intentos de modificación ilegal de contraseñas tradicionales, el atacante intenta obtener una contraseña adivinándola o empleando otros métodos menos tecnológicos para obtener el acceso inicial. El atacante corre el riesgo de que se lo detecte o se lo bloquee al intentar autenticarse de manera explícita; pero con cierto conocimiento previo del historial de contraseñas de la víctima, tal vez pueda autenticarse correctamente. Busque indicaciones anormales adicionales de que el propietario de la cuenta no es quien intenta acceder a ella. Esta actividad suele asociarse con el indicador **Varias autenticaciones fallidas**.
Inicios de sesión de usuario en varios sitios de AD	Las controladoras de dominio almacenan los hashes de las contraseñas de las credenciales de todas las cuentas del dominio, por lo que son objetivos de alto valor para los atacantes. Las controladoras de dominio que no se actualizan y se protegen de manera estricta están expuestas a ataques y riesgos que podrían dejar vulnerable al dominio. Los privilegios de usuario en varios dominios podrían indicar que se vulneró un dominio primario. Determine si el acceso de los usuarios a varios sitios y desde estos es legítimo o es indicio de una posible vulneración. Esta actividad suele asociarse con el indicador **Inicio de sesión en varios dominios**.
Inicio de sesión de usuario en un host anormal	A menudo, los atacantes necesitan volver a adquirir credenciales y realizar otras actividades críticas, como el uso del acceso remoto. El seguimiento de la cadena de acceso hacia atrás puede permitir que se descubran otras computadoras involucradas en actividad posiblemente riesgosa. Si la presencia de un atacante se limita a un único host vulnerado o a muchos hosts vulnerados, esa actividad se puede asociar con el indicador **Computadora anormal**.
Extracción de datos	La extracción de datos es la copia, la transferencia o la recuperación no autorizadas de datos de una computadora o un servidor. La extracción de datos es una actividad maliciosa que suelen realizar los cibercriminales a través de Internet o de otra red con el uso de diversas técnicas. Esta actividad se puede asociar con los indicadores **Cantidad excesiva de eventos de cambio de nombre de archivos**, **Cantidad excesiva de archivos transferidos desde el sistema de archivos** y **Cantidad excesiva de archivos transferidos al sistema de archivos**.
Cambio de nombre de archivo masivo	Ransomware es un tipo de malware que cifra los archivos del escritorio y del sistema de modo que quedan inaccesibles. Algunos ransomware, por ejemplo, “Locky”, cifra los archivos y les cambia el nombre como parte de su ejecución inicial. Utilice esta indicación de cambio de nombre de archivo masivo para determinar si el sistema de archivos se infectó con ransomware. Esta actividad se puede asociar con el indicador **Varios eventos de cambio de nombre de archivo**.

Tipo de alerta	Descripción
Usuario entrometido	El fisgoneo es el acceso no autorizado a los datos de otra persona o de la empresa. Puede ser tan simple como observar casualmente un correo electrónico en la computadora de otra persona o ver lo que alguien más está escribiendo. El fisgoneo más sofisticado utiliza programas de software para monitorear de manera remota la actividad en una computadora o un dispositivo de red. Esta actividad se puede asociar con los indicadores **Varios eventos de acceso a archivos**, **Varios eventos de acceso a archivos fallidos**, **Varios eventos de archivos abiertos** y **Varios eventos de carpetas abiertas**.
Varios inicios de sesión de un usuario	Toda la actividad de autenticación, maliciosa o no, aparece como inicios de sesión normales. Por lo tanto, los administradores deben monitorear la actividad autorizada inesperada. La clave es que los atacantes utilizan estas credenciales robadas para el acceso no autorizado, lo que puede proporcionar una oportunidad para la detección. Cuando una cuenta se utiliza para actividades inusuales, por ejemplo, la autenticación una cantidad inusual de veces, la cuenta puede haberse vulnerado. Esta actividad se puede asociar con el indicador **Varias autenticaciones correctas**.
El usuario inició sesión en varios hosts	Normalmente, los atacantes necesitan volver a adquirir credenciales de manera periódica. Esto se debe a que su cadena de claves de credenciales robadas se degrada naturalmente con el tiempo debido a los cambios y los restablecimientos de las contraseñas. Por lo tanto, los atacantes mantienen con frecuencia un punto de apoyo en la organización vulnerada mediante la instalación de puertas traseras y el mantenimiento de credenciales de muchas computadoras del ambiente. Esta actividad se puede asociar con el indicador **Inicio de sesión en varias computadoras**.
Cambio de la contraseña de administrador	Las señas secretas a largo plazo compartidas, por ejemplo, las contraseñas de cuentas con privilegios, suelen usarse para acceder a cualquier dispositivo, desde servidores de impresión hasta controladoras de dominio. Para contener a los atacantes que intentan aprovechar estas cuentas, preste mucha atención a los cambios de contraseña de los administradores y asegúrese de que los hayan realizado personas de confianza y que no estén asociados a ningún comportamiento anormal adicional. Esta actividad se puede asociar con el indicador **Cambio de la contraseña de administrador**.

Tipo de alerta	Descripción
Cambios de permisos masivos	Algunas técnicas de robo de credenciales, por ejemplo, Pass-the-Hash, utilizan un proceso iterativo de dos etapas. En primer lugar, un atacante obtiene un permiso de lectura y escritura elevado a áreas privilegiadas de memoria volátil y sistemas de archivos, a las cuales solamente pueden acceder procesos en el nivel del sistema al menos en una computadora. En segundo lugar, el atacante intenta aumentar el acceso a otras computadoras de la red. Investigue si se han realizado cambios de permisos anormales en los sistemas de archivos para asegurarse de que un atacante no los haya vulnerado. Esta actividad se puede asociar con los indicadores **Varios cambios de permisos de acceso a archivos**, **Varios cambios de permisos de acceso a archivos fallidos** y **Cambio de permiso de acceso a archivos anormal**.
Cambios anormales en AD	Si un atacante obtiene acceso con privilegios elevados a un dominio o una controladora de dominio de Active Directory, ese acceso se puede aprovechar para acceder, controlar o, incluso, destruir todo el bosque. Si una única controladora de dominio se vulnera y un atacante modifica la base de datos de AD, esas modificaciones se replican a todas las demás controladores de dominio del dominio y, en función de la partición en la que se realizan las modificaciones, también al bosque. Investigue los cambios anormales que realizan los administradores y quienes no son administradores en AD para determinar si representan una posible vulneración real del dominio. Esta actividad se puede asociar con los indicadores **Cambio anormal en Active Directory**, **Varios cambios en la administración de cuentas**, **Varios cambios en la administración de cuentas de usuarios** y **Varios cambios fallidos en la administración de cuentas**.
Cambios críticos en el estado de un usuario	Una cuenta de administrador de dominio o empresarial tiene la capacidad predeterminada de ejercer control sobre todos los recursos de un dominio, independientemente de si funciona con malas o buenas intenciones. Este control incluye la capacidad de crear y cambiar cuentas, leer, escribir o eliminar datos, instalar o modificar aplicaciones, y borrar los sistemas operativos. Algunas de estas actividades se desencadenan orgánicamente como parte del ciclo de vida natural de la cuenta. Investigue estos cambios en cuentas de usuario críticas en cuanto a la seguridad y determine si se vulneraron. Esta actividad se puede asociar con los indicadores **Se habilitó una cuenta de usuario**, **Se deshabilitó una cuenta de usuario**, **Se desbloqueó una cuenta de usuario**, **Se cambió un tipo de cuenta de usuario**, **Se bloqueó una cuenta de usuario**, **Se cambió la opción La contraseña de usuario nunca vence**, **Alguien que no es el propietario cambió la contraseña de usuario** y **Se cambió la contraseña de usuario**.

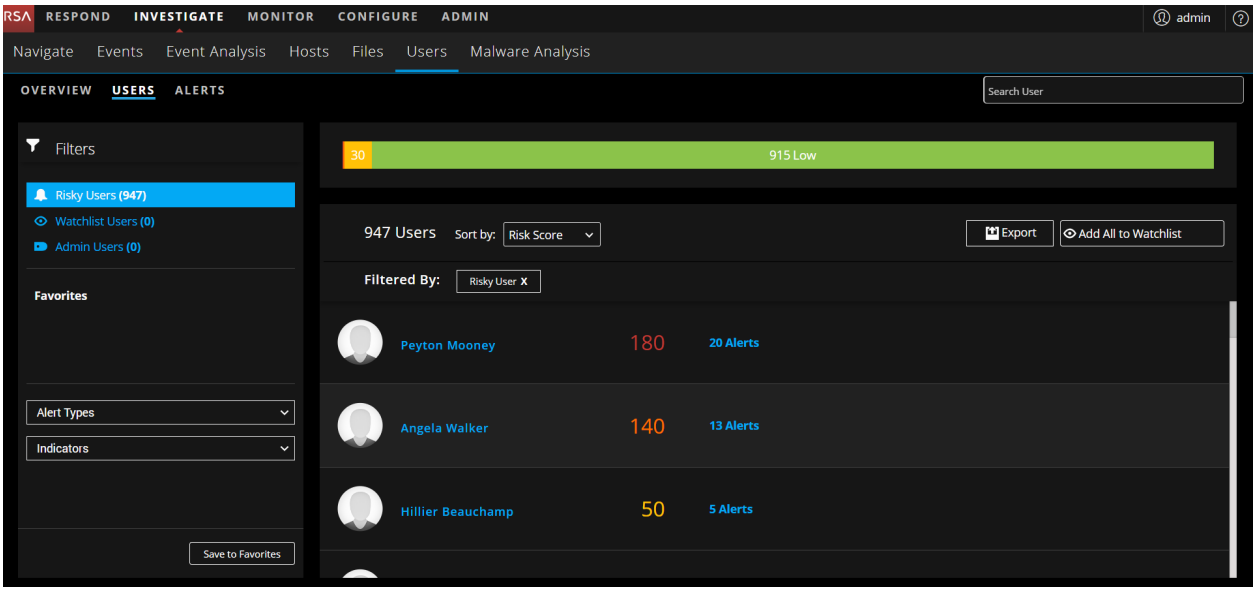
Tipo de alerta	Descripción
Acceso a archivos anormal	Monitoree el acceso a archivos anormal para evitar el acceso inadecuado a archivos confidenciales y el robo de datos confidenciales. Con el monitoreo selectivo de vistas, modificaciones y eliminaciones de archivos, puede detectar cambios posiblemente no autorizados en archivos confidenciales, tanto debido a un ataque como a un error de administración de cambios. Esta actividad se puede asociar con los indicadores **Evento de acceso a archivos anormal** y **Varios eventos de eliminación de archivos**.
Horas no estándares	Toda la actividad de autenticación, maliciosa o no, aparece como inicios de sesión normales. Por lo tanto, los administradores deben monitorear la actividad autorizada inesperada. La clave es que los atacantes utilizan estas credenciales robadas para el acceso no autorizado, lo que puede proporcionar una oportunidad para la detección. Cuando una cuenta se utiliza para actividades inusuales, por ejemplo, la autenticación una cantidad inusual de veces, la cuenta puede haberse vulnerado. Utilice el indicio de una hora de actividad anormal para determinar si un actor externo se apropió de la cuenta. Esta actividad se puede asociar con los indicadores **Hora de acceso a archivos anormal**, **Hora de cambio de Active Directory anormal** y **Hora de inicio de sesión anormal**.

Investigar a los usuarios de alto riesgo

El puntaje y la gravedad de la alerta constituyen el puntaje de un usuario. El uso del puntaje del usuario permite identificar a los usuarios que requieren atención inmediata, realizar una investigación más profunda y adoptar las medidas necesarias. Puede identificar a los usuarios de alto riesgo desde la pestaña **Descripción general** o la pestaña **Usuarios**.

La siguiente figura es un ejemplo de los cinco principales usuarios de alto riesgo en la pestaña **Descripción general**.

La siguiente figura es un ejemplo de todos los usuarios riesgosos del ambiente en la pestaña **Usuarios**.



El siguiente es un proceso general para investigar a los usuarios de alto riesgo del ambiente.

1. Identifique a los usuarios de alto riesgo. Puede identificar a los usuarios de alto riesgo de las siguientes maneras:
   - La pestaña **Descripción general** muestra los cinco principales usuarios riesgosos del ambiente. Entre los usuarios enumerados, identifique a aquellos con gravedad crítica o con un puntaje superior a 100.
   - La pestaña **Usuario** muestra a todos los usuarios riesgosos del ambiente, ordenados por puntaje de riesgo. Identifique la cantidad de usuarios con las gravedades Crítica, Alta y Media o, en función de la investigación forense, identifique el comportamiento malintencionado de los usuarios y cree listas de usuarios objetivo orientadas a casos de uso mediante filtros de comportamiento. Además, también puede usar diferentes tipos de filtros (Riesgoso, Administrador o Lista de seguimiento) para identificar un grupo objetivo de usuarios de alto riesgo.

   Nota: La investigación se debe centrar principalmente en las gravedades Crítica, Alta y Media. Comúnmente, no vale la pena investigar a los usuarios con puntaje bajo.

   Coloque el cursor sobre la cantidad de alertas asociadas con los usuarios riesgosos para ver rápidamente a qué corresponden y determinar si la combinación es adecuada.

   Nota: La cantidad de alertas no siempre se correlaciona con los puntajes más altos, ya que algunas alertas aportan únicamente puntajes pequeños al puntaje general del usuario, pero mientras más alertas existan, más fácil será demostrar una cronología de actividad que dio lugar al puntaje alto.

   Para obtener más información, consulte el tema Identificar a los usuarios de alto riesgo.
2. En la vista **Perfil de usuario**, investigue las alertas y los indicadores del usuario.
   a. Revise la lista de alertas asociadas con el usuario y el puntaje de cada alerta, ordenados por gravedad.
   b. Expanda los nombres de alerta para identificar una descripción de la amenaza. El indicador que más contribuye determina el nombre de la alerta, y esto sugiere el motivo por el que está marcada esta hora.
   c. Utilice la cronología del flujo de la alerta para comprender las actividades anormales.
   d. Revise cada indicador asociado con la alerta para ver sus detalles, incluida la cronología en la que se produjo la anomalía. Además, puede investigar adicionalmente el incidente con recursos externos, como SIEM, análisis forense de red, contacto directo con el usuario o con un director ejecutivo, etc.

   Para obtener más información, consulte el tema Iniciar una investigación de usuarios de alto riesgo.
3. Al finalizar la investigación, puede registrar su observación de la siguiente manera:
   a. Especificar si una alerta no constituye un riesgo
   b. Guardar el perfil de comportamiento para el caso de uso que se encontró en el ambiente
   c. Si desea rastrear la actividad del usuario, puede agregar usuarios a la lista de seguimiento y realizar un seguimiento a los perfiles de usuario

   Para obtener más información, consulte el tema Adoptar medidas en relación con los usuarios de alto riesgo.

Identificar a los usuarios de alto riesgo

Puede identificar a un usuario de alto riesgo en el ambiente de las siguientes maneras:

- Ver los cinco principales usuarios de alto riesgo
- Ver todos los usuarios de alto riesgo
- Ver usuarios de un grupo específico
- Ver usuarios en función de una investigación forense

Ver los cinco principales usuarios riesgosos

La pestaña **Descripción general** permite ver la lista de los cinco principales usuarios de alto riesgo del ambiente junto con su puntaje.

Para ver los cinco principales usuarios riesgosos:

Inicie sesión en **NetWitness Platform** y vaya a **Investigar** > **Usuarios**.
La pestaña Descripción general se muestra con los usuarios de alto riesgo en el panel Usuarios de alto riesgo.

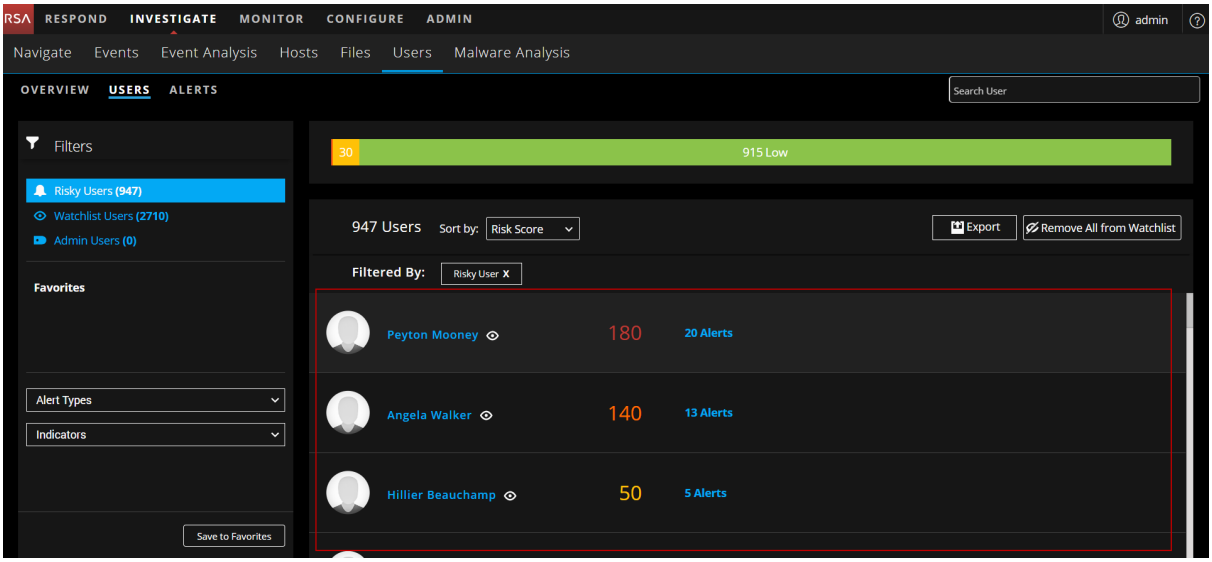
Ver todos los usuarios de alto riesgo

En la pestaña **Usuarios**, puede ver la lista de todos los usuarios de alto riesgo del ambiente junto con su puntaje y la cantidad total de alertas asociadas con ellos.

Para ver todos los usuarios de alto riesgo:

1. Inicie sesión en **NetWitness Platform** y vaya a **Investigar** > **Usuarios**.
   Se muestra la pestaña Descripción general.

2. Haga clic en la pestaña **Usuarios**.
   Se muestra la lista de todos los usuarios de alto riesgo.

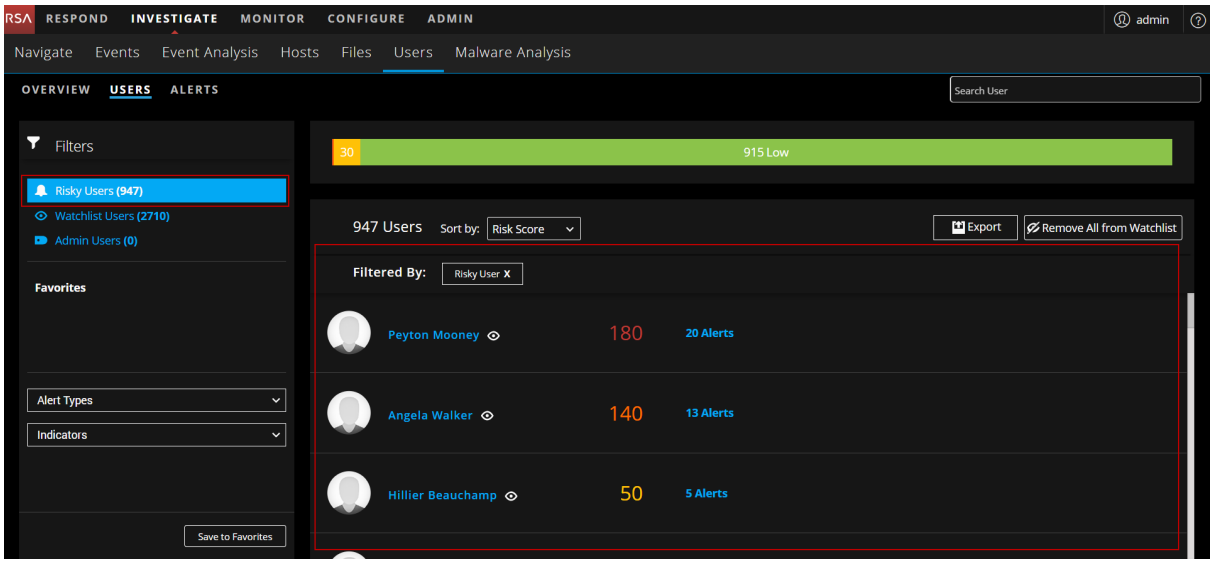


Ver usuarios de un grupo específico

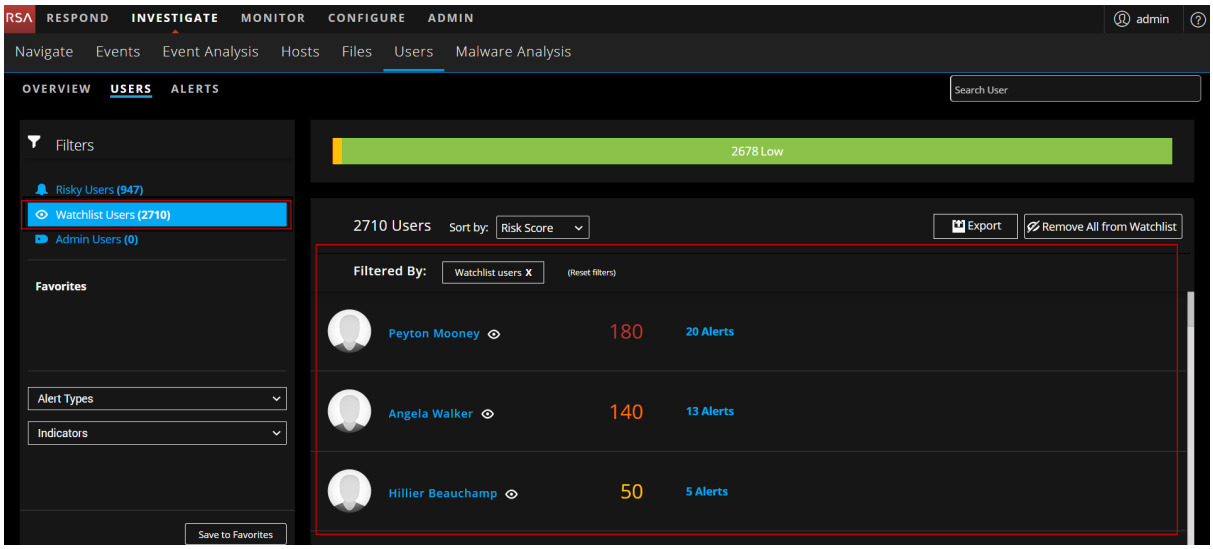
En la pestaña **Usuarios**, puede utilizar diferentes tipos de filtros para identificar el grupo objetivo de usuarios de alto riesgo.

Para ver usuarios de un grupo específico:

1. Inicie sesión en **NetWitness Platform** y vaya a **Investigar** > **Usuarios**.
   Se muestra la pestaña Descripción general.
2. Haga clic en la pestaña **Usuarios**.
3. En el panel **Filtros**, realice una de las siguientes acciones:
   - **Usuarios riesgosos**: Para ver todos los usuarios riesgosos del ambiente, seleccione **Usuarios riesgosos**. De manera predeterminada, se muestran los usuarios riesgosos junto con su puntaje.



- **Usuarios de la lista de seguimiento**: Para ver la lista de usuarios que agregó a la lista de seguimiento con el fin de monitorear cambios específicos, seleccione **Usuarios de la lista de seguimiento**.



- **Usuarios administradores**: Para ver todos los usuarios marcados como administradores en los eventos, seleccione **Usuarios administradores**.

Nota: Puede ver los usuarios de uno o más grupos seleccionando uno o más filtros. Por ejemplo, si desea ver la lista de usuarios administradores que son usuarios riesgosos, seleccione los filtros **Usuarios administradores** y **Usuarios riesgosos**.

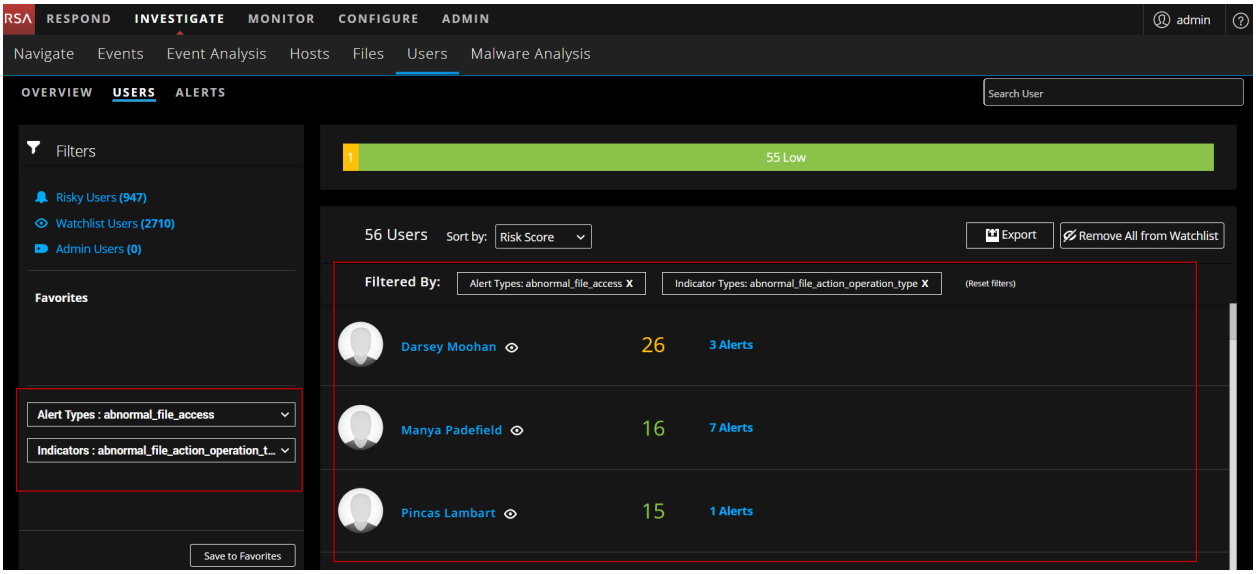
Ver usuarios en función de una investigación forense

En la pestaña **Usuarios**, puede utilizar Tipos de alerta e Indicadores, que son filtros de comportamiento que permiten ver a los usuarios de alto riesgo en función de una investigación forense. Para obtener más información sobre la investigación forense, consulte *Flujo de trabajo forense* en el tema Introducción.

Para ver usuarios en función de una investigación forense específica:

1. Inicie sesión en **NetWitness Platform** y vaya a **Investigar** > **Usuarios**.
   Se muestra la pestaña Descripción general.
2. Haga clic en la pestaña **Usuarios**.
3. Para crear un filtro de comportamiento usando tipos de alertas, seleccione una o más alertas en la lista desplegable **Tipos de alerta**.
4. Para crear un filtro de comportamiento usando indicadores, seleccione uno o más indicadores en la lista desplegable **Indicadores**.

Nota: Puede seleccionar una combinación de uno o más tipos de alertas e indicadores para crear un filtro de comportamiento basado en sus necesidades. Por ejemplo, para monitorear el acceso anormal a archivos confidenciales y el robo de datos confidenciales, puede crear un filtro de comportamiento con Tipos de alerta = **Acceso a archivos anormal** e Indicadores = **Tipo de operación de acción de archivo anormal**.



Guarde estos filtros de comportamiento como favoritos para investigaciones futuras.

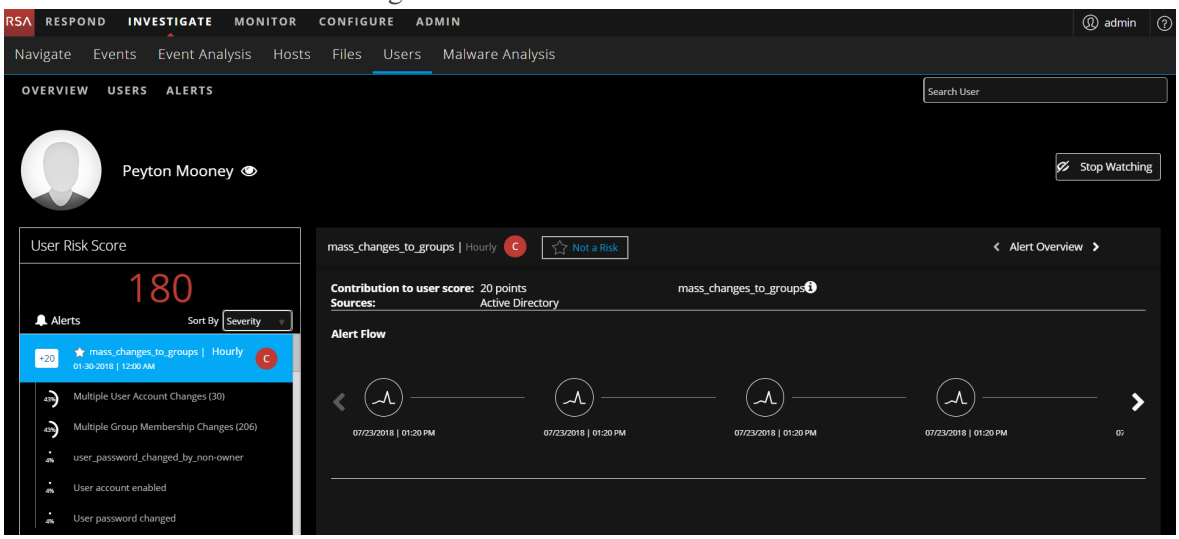
Iniciar una investigación de usuarios de alto riesgo

Después de identificar a los usuarios de alto riesgo, puede comenzar a investigarlos.

Para investigar a los usuarios de alto riesgo:

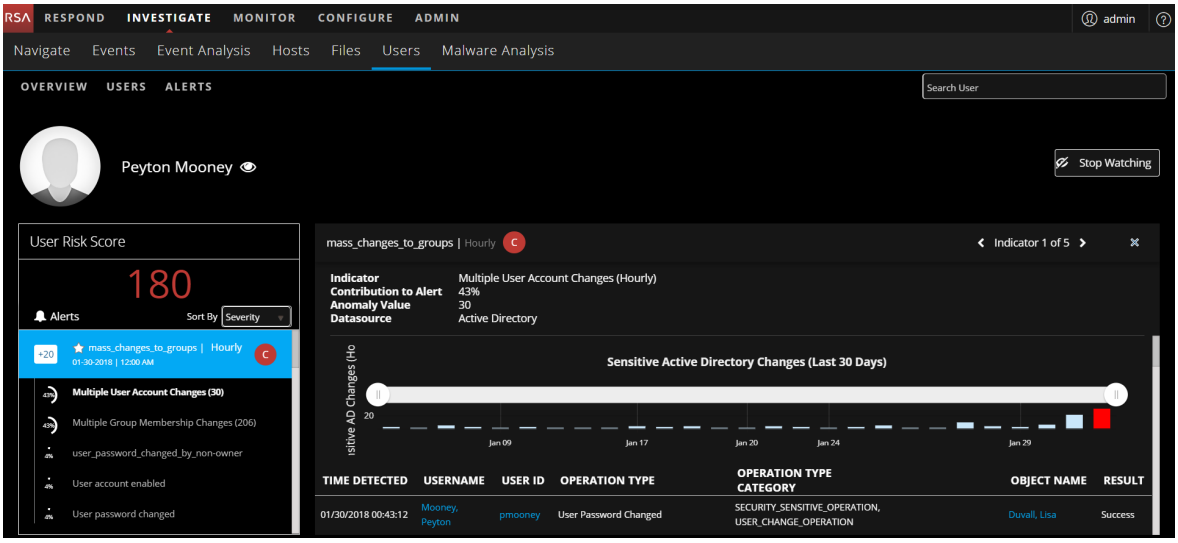
1. Inicie sesión en **NetWitness Platform** y vaya a **INVESTIGAR** > **Usuarios**. Realice cualquiera de las siguientes acciones:
   a. En la pestaña **Descripción general**, en el panel **Usuarios de alto riesgo**, seleccione un usuario que desee investigar y haga clic en el nombre de usuario o en su puntaje.
   b. En la pestaña **USUARIOS**, seleccione el usuario que desea investigar y haga clic en el nombre de usuario.
   Se muestra la vista Perfil de usuario.

2. Para investigar las alertas del usuario, haga clic en el nombre de la alerta en el panel **Puntaje de riesgo del usuario**. Se muestra la siguiente información:
   - El nombre de la alerta
   - El intervalo de tiempo de la alerta (Por hora o Diariamente)
   - El icono del nivel de gravedad
   - La contribución al valor de puntaje del usuario (por ejemplo, +20)
   - Los orígenes de datos de la alerta (por ejemplo, Inicio de sesión)
     El panel central es el panel Flujo de la alerta. En este panel se proporciona una cronología de eventos relacionados con la formación de la alerta. La cronología de eventos puede ayudar a determinar si la alerta es un riesgo real.



3. Para investigar los indicadores asociados con la alerta de un usuario, en el panel **Puntaje de riesgo del usuario**, seleccione una alerta y, a continuación, un indicador. Se muestra la siguiente información:
   - El nombre del indicador y una descripción de su tipo
   - Contribución a la alerta
   - Los valores de anomalía

- El origen de datos de los eventos encontrados en el indicador
  El panel central muestra cambios en función del indicador que se selecciona.



Adoptar medidas en relación con los usuarios de alto riesgo

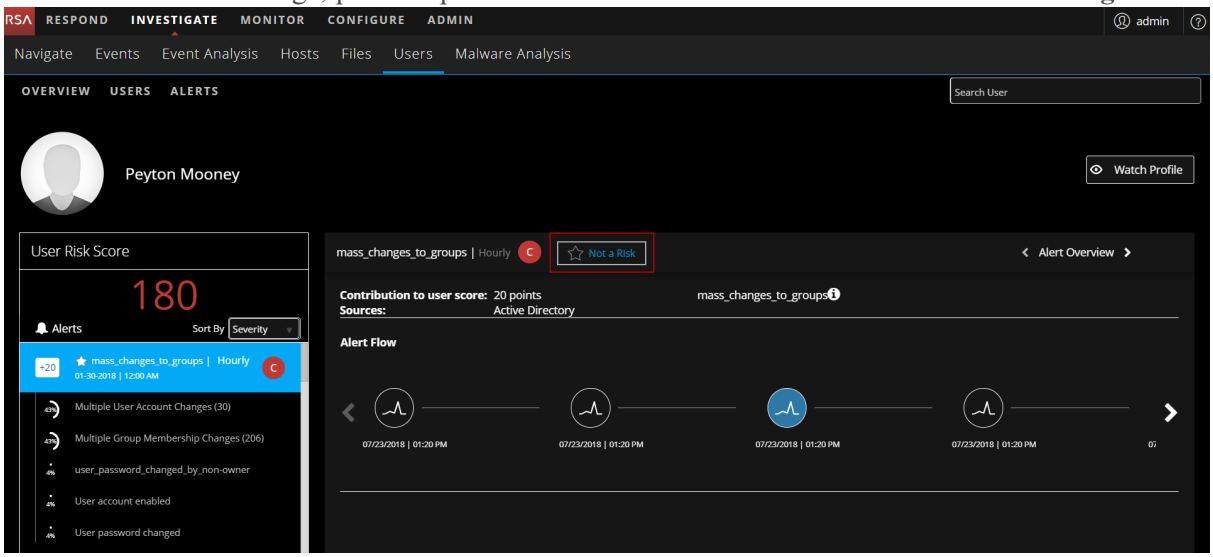
Después de la investigación, puede adoptar medidas en relación con los usuarios riesgosos para reducir los daños causados por los atacantes maliciosos en su organización o evitarlos. Puede llevar a cabo una de las siguientes acciones:

- Especificar si la alerta no es riesgosa
- Guardar el perfil de comportamiento para el caso de uso que se encontró en el ambiente
- Agregar usuarios a la lista de seguimiento y realizar un seguimiento a los perfiles de usuario si se desea rastrear la actividad del usuario

Especificar si la alerta no es riesgosa

Para especificar si la alerta no es riesgosa:

1. Inicie sesión en **NetWitness Platform** y vaya a **INVESTIGAR** > **Usuarios**.
2. Adopte medidas en relación con los usuarios desde cualquiera de las siguientes pestañas:
   a. En la pestaña **Descripción general**, en el panel **Usuarios de alto riesgo**, seleccione un usuario y haga clic en el nombre de usuario o en su puntaje.
   b. En la pestaña **Usuarios**, seleccione un usuario y haga clic en el nombre de usuario.
   Se muestra la vista Perfil de usuario.
3. Si la alerta no es un riesgo, puede especificar esta condición haciendo clic en **No es un riesgo**.



Cuando una alerta se marca como **No es un riesgo**, el puntaje del usuario se reduce automáticamente.

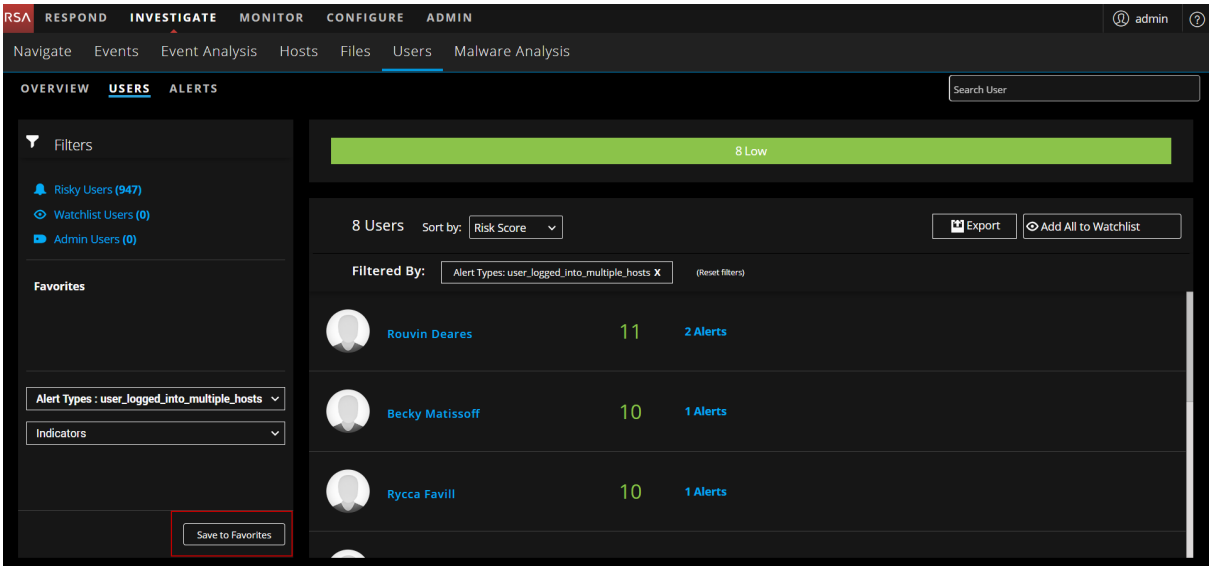
Guardar el perfil de comportamiento

La combinación de los tipos de alertas y los indicadores que selecciona durante la investigación forense es un perfil de comportamiento. Puede guardar el perfil de comportamiento de modo que pueda monitorear este caso de uso en el futuro.

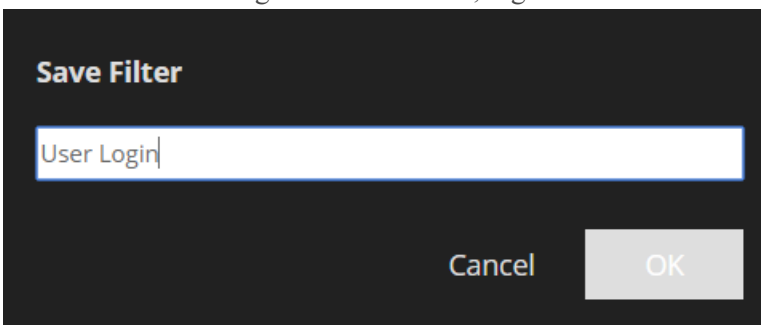
Por ejemplo, si la organización es víctima de ataque y los atacantes accedieron por fuerza bruta a las cuentas de usuario, puede seleccionar filtros utilizando el tipo de alerta de fuerza bruta. Esto se puede guardar entre los favoritos. Puede realizar un monitoreo proactivo de futuros intentos de ataques de fuerza bruta. Para ello, puede hacer clic en el perfil favorito con el objetivo de ver si los nuevos usuarios fueron víctimas de este tipo de ataque.

Para guardar el perfil de comportamiento:

1. Inicie sesión en **NetWitness Platform** y vaya a **INVESTIGAR** > **Usuarios**.
   Se muestra la pestaña Descripción general.
2. Haga clic en la pestaña **Usuarios**.
3. En el panel **Filtros**, seleccione la alerta en la lista desplegable **Tipo de alerta** e Indicadores en la lista desplegable **Indicadores**.
4. Haga clic en **Guardar en favoritos**.



5. En el cuadro de diálogo **Guardar filtro**, ingrese el nombre del filtro y haga clic en **Aceptar**.



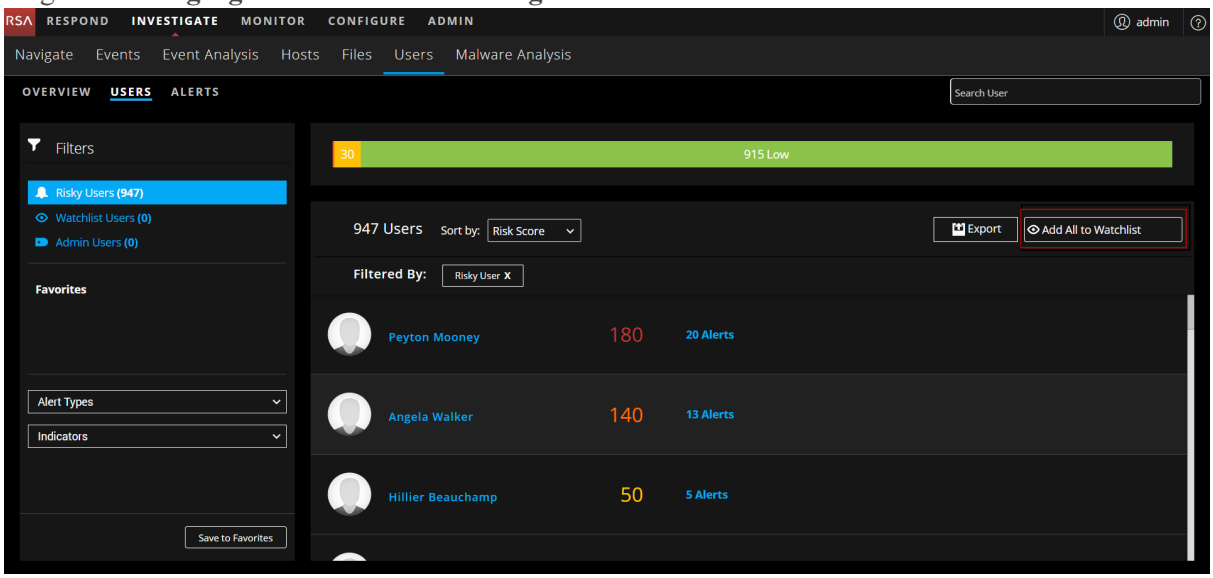
El perfil de comportamiento se guarda y se muestra en el panel Favoritos. Puede hacer clic en el perfil en los Favoritos para monitorear a los usuarios.

Agregar todos los usuarios a la lista de seguimiento

Si desea rastrear a los usuarios con actividad reciente, pero no desea realizar una investigación inmediata, puede agregar los usuarios a la lista de seguimiento y consultarla conforme avanza el tiempo para ver si el puntaje de riesgo es elevado.

Para agregar todos los usuarios a la lista de seguimiento:

1. Inicie sesión en **NetWitness Platform** y vaya a **INVESTIGAR** > **Usuarios**.
   Se muestra la pestaña Descripción general.
2. Seleccione la pestaña **Usuarios**.
3. Seleccione los usuarios de categorías específicas mediante filtros.
4. Haga clic en **Agregar todos a la lista de seguimiento**.



La lista de usuarios se agrega a la lista de seguimiento.

Seguimiento de perfiles de usuario

El seguimiento de perfiles de usuario es una lista de usuarios que se desea monitorear en busca de posibles amenazas. El seguimiento de perfiles de usuario marca usuarios de modo que se puedan consultar rápidamente en el tablero. Esto es esencialmente un marcador que permite monitorear a los usuarios sospechosos.

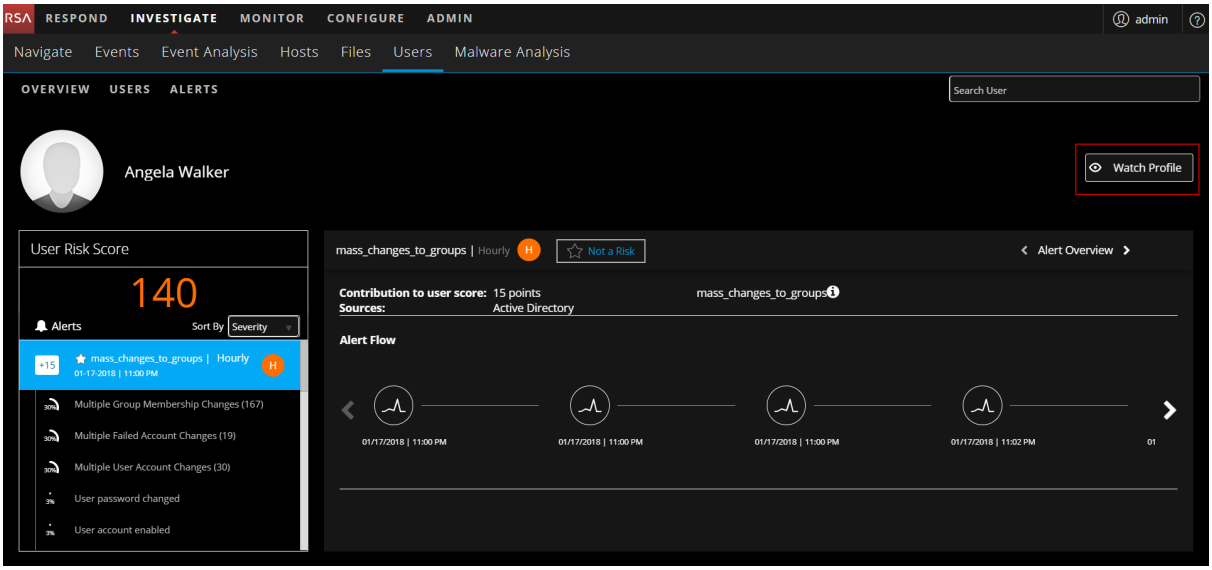
Para realizar un seguimiento a perfiles de usuario:

1. Inicie sesión en **NetWitness Platform** y vaya a **INVESTIGAR** > **Usuarios**. Realice cualquiera de las siguientes acciones:

   a. En la pestaña **Descripción general**, bajo el panel **Usuarios de alto riesgo**, seleccione un usuario y haga clic en el nombre de usuario o en su puntaje.

   b. En la pestaña **Usuarios**, seleccione un usuario y haga clic en el nombre de usuario.
   Se muestra la vista Perfil de usuario.

2. Haga clic en **Hacer un seguimiento al perfil** en la esquina superior derecha del perfil de usuario.



   El usuario se agrega a la lista de seguimiento.

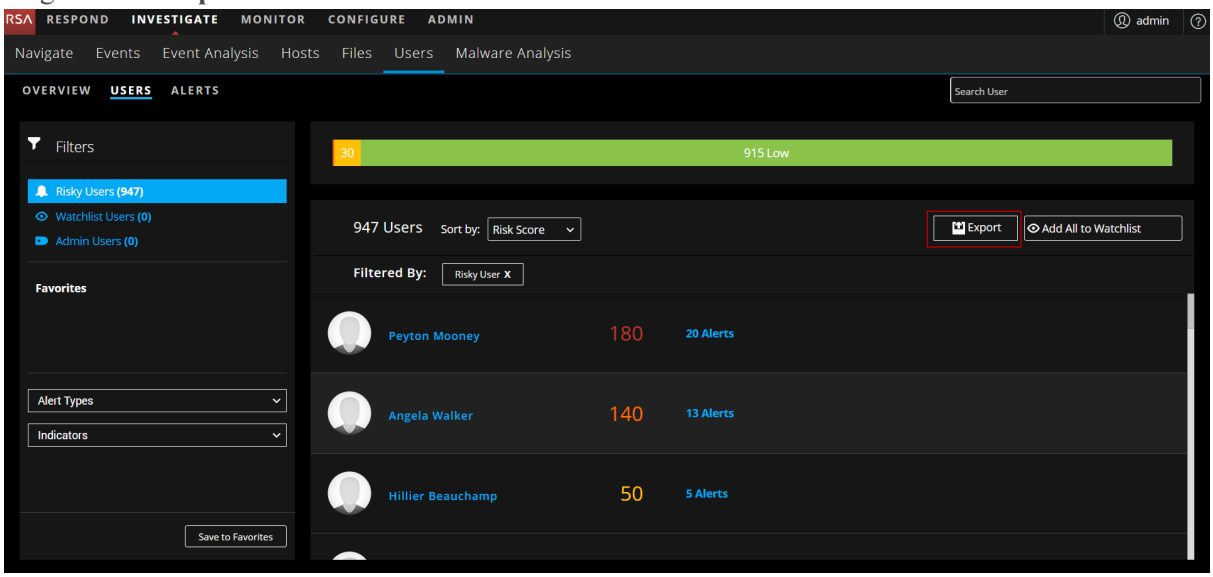
Exportar usuarios de alto riesgo

Puede exportar una lista de todos los usuarios y sus puntajes en un formato de archivo .csv. Esta información se puede usar para realizar comparaciones con otras herramientas de análisis de datos, como Tableau, Power BI y Zeppelin.

Para exportar usuarios de alto riesgo:

1. Vaya a **INVESTIGAR** > **Usuarios**.
   Se muestra la pestaña Descripción general.
2. Seleccione la pestaña **Usuarios**.

3. Haga clic en **Exportar**.



La lista de todos los usuarios y su puntaje asociado se descarga en el formato de archivo .csv.

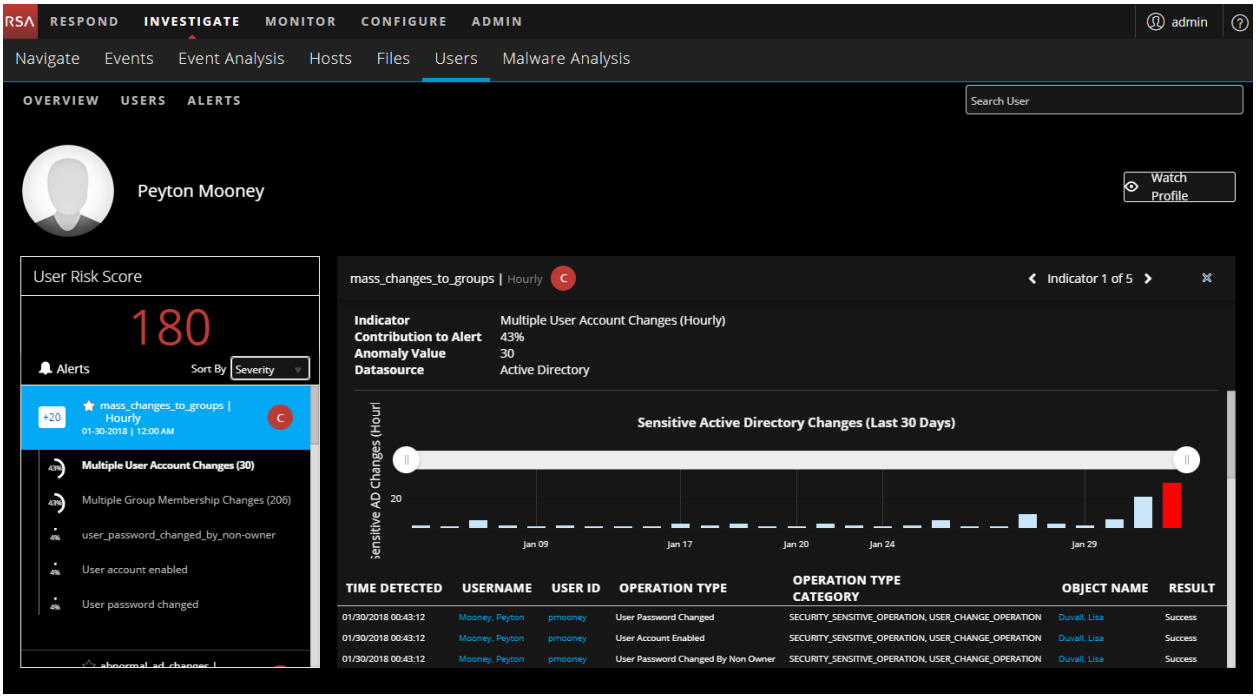
Investigar las alertas principales

Las anomalías que se encuentran como eventos entrantes se comparan con la base y se compilan en alertas por hora. Es más probable que las desviaciones de la base relativamente considerables, junto con una composición única de anomalías, reciban un puntaje de alerta más alto.

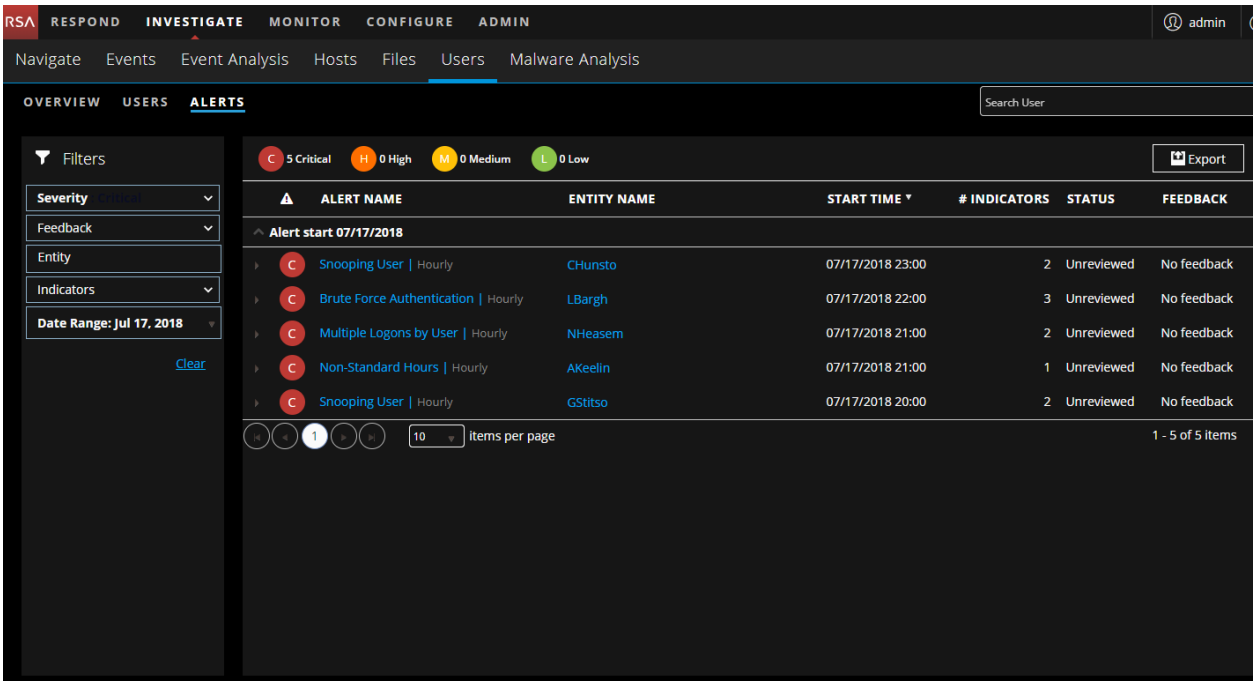
Puede ver rápidamente las alertas principales más críticas del ambiente y comenzar a investigarlas desde la pestaña DESCRIPCIÓN GENERAL o la pestaña ALERTAS. La siguiente figura es un ejemplo de alertas principales en la pestaña DESCRIPCIÓN GENERAL. Las alertas se enumeran en orden de gravedad y la cantidad de usuarios que las generan.

Para investigar una alerta en esta página, haga clic en una alerta de la sección **Alertas principales** para ver sus detalles.

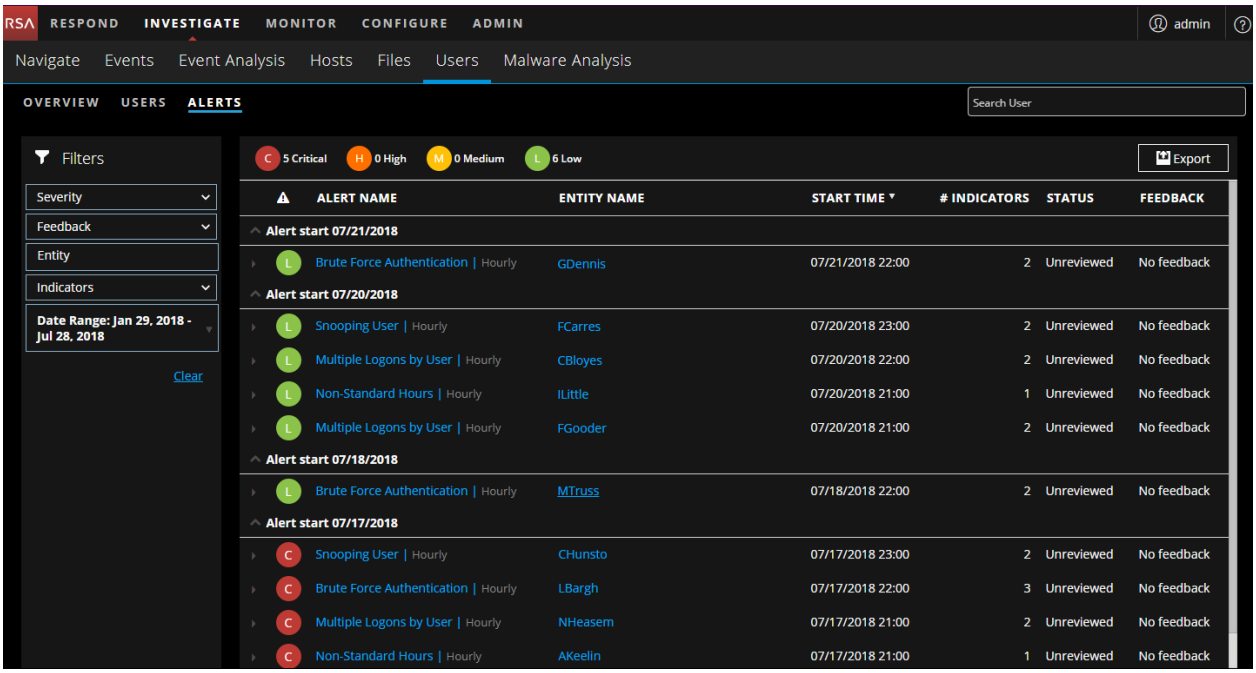
En la siguiente figura se muestran detalles sobre el evento que causó la alerta y el intervalo de tiempo en que se produjo.



En el panel Gravedad de alertas de la pestaña DESCRIPCIÓN GENERAL, puede hacer clic en una barra del gráfico para revisar las alertas principales en la pestaña ALERTAS, como se muestra en la siguiente figura.



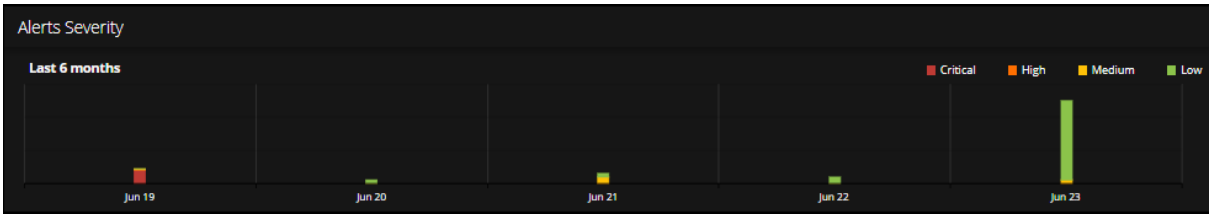
La investigación de las alertas es especialmente útil cuando es necesario centrarse en un intervalo de tiempo en el que se cree que los sistemas se vulneraron. Puede ver información forense en función de un intervalo de tiempo y recopilar información detallada sobre los eventos que ocurrieron durante ese período en la pestaña Alertas.



Iniciar una investigación de alertas críticas

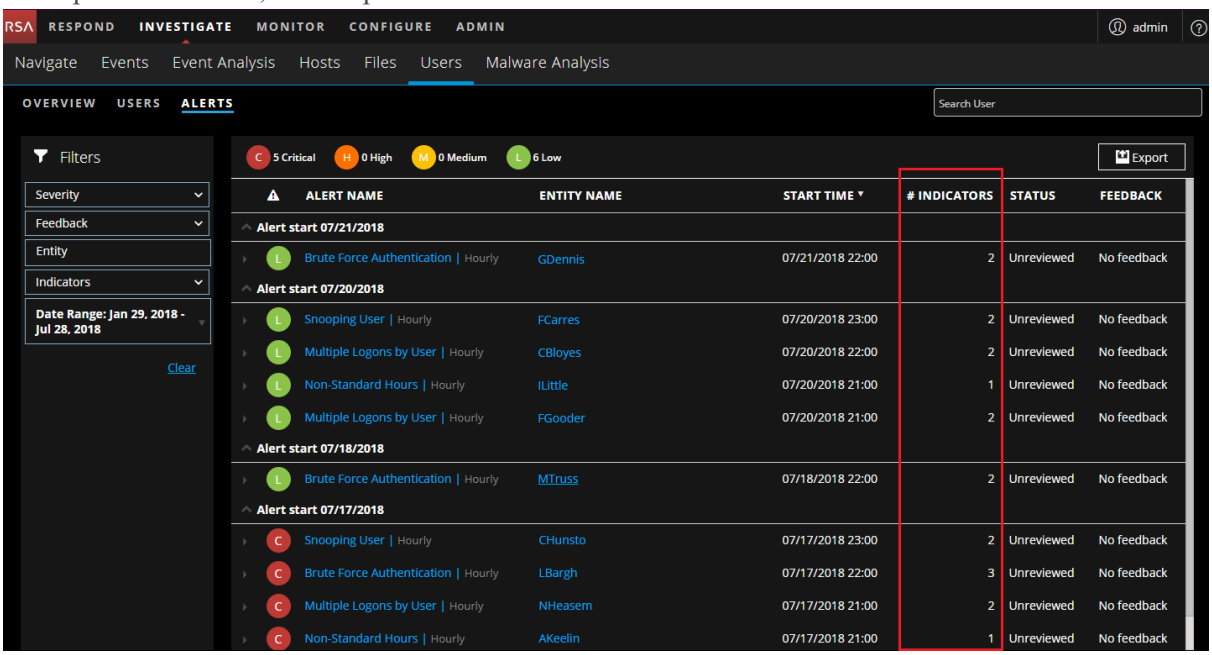
Puede comenzar a investigar alertas críticas de las siguientes maneras:

1. En la pestaña Descripción general, observe la Gravedad de las alertas.



¿Hay una distribución uniforme de alertas o hay algunos días en que hubo un incremento repentino evidente? Un incremento repentino podría indicar algo sospechoso, como malware. Tome nota de esos días para que pueda inspeccionar las alertas (la barra del gráfico establece un vínculo directo a las alertas de ese día específico).

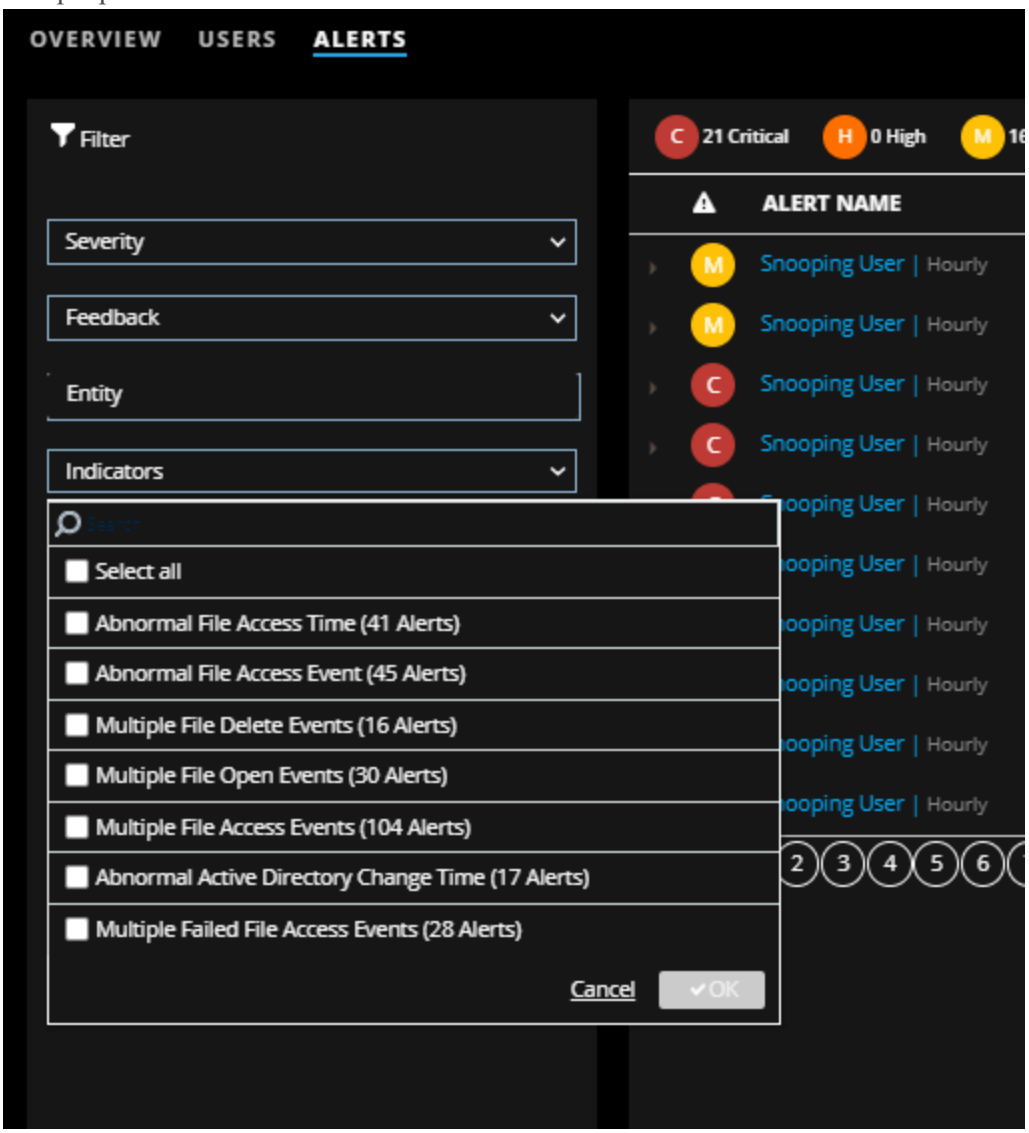
2. En la pestaña Alertas, ordene por la cantidad de indicadores:



Asegúrese de que las alertas que agregaron la mayor cantidad de indicadores aparezcan en la parte superior de la lista. De manera similar a la identificación de los usuarios con la mayor cantidad de alertas, un mayor número de indicadores ayuda a ilustrar un panorama más interesante y proporciona una cronología más sólida que puede seguir.

3. Expanda las alertas principales en la lista:
   - Busque alertas que tengan orígenes de datos variados. Estos muestran un patrón de comportamiento más amplio.
   - Busque una variedad de indicadores diferentes.
   - Busque indicadores con altos valores numéricos, específicamente altos valores que no son indicio de actividad que un humano pueda realizar manualmente (por ejemplo, un usuario accedió a 8,000 archivos).
4. Busque tipos de eventos de Windows únicos que los usuarios no suelen cambiar, ya que pueden indicar actividad administrativa sospechosa.

5. Busque por indicadores:



En la lista se muestra la cantidad de alertas emitidas que contienen cada indicador.

- Busque el mayor volumen de indicadores; filtre por uno y revise por usuario para encontrar los usuarios que experimentaron la mayor cantidad de estos indicadores.
- En general, puede descartar las alertas basadas en tiempo (por ejemplo, Hora de inicio de sesión anormal), ya que son muy comunes. Sin embargo, proporcionan un buen contexto cuando se combinan con indicadores de mayor interés.

6. Desglose a información más detallada:
   - Aproveche los nombres de alerta para comenzar a establecer una descripción de las amenazas. Utilice el hecho de que el indicador que más contribuye suele determinar el nombre de la alerta para comenzar a explicar el motivo por el que está marcado este usuario.
   - Utilice la cronología para ordenar las actividades encontradas e intente comprender qué podría explicar los comportamientos observados.

- Continúe revisando cada indicador y demostrando cómo la información de apoyo, en forma de gráficos y eventos, puede ayudar a los analistas a verificar un incidente. Sugiera posibles etapas de investigación siguientes utilizando recursos externos (por ejemplo, SIEM, análisis forense de red y contacto directo con el usuario o con un director ejecutivo).
- Concluya la investigación solicitando retroalimentación y dejando un comentario.

7. Adopte medidas para abordar las amenazas que determinó la investigación de las alertas. Para obtener más información, consulte Adoptar medidas en relación con los usuarios de alto riesgo.

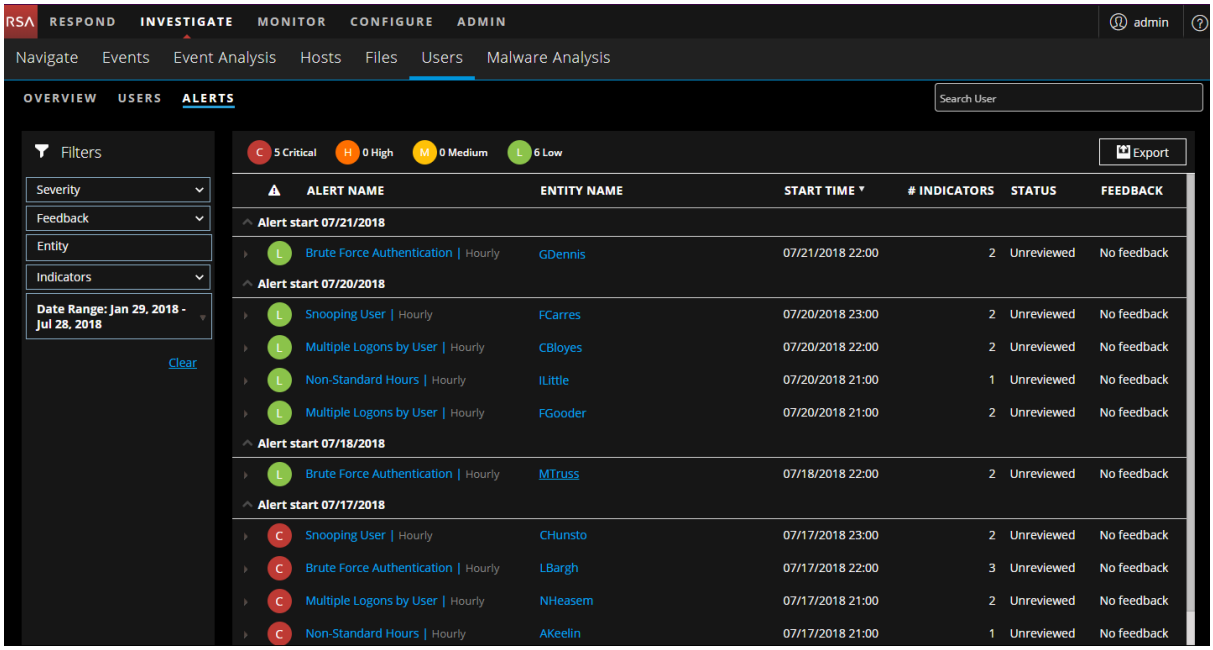
En los siguientes temas se explican varias maneras de investigar las alertas.

- Filtrar alertas
- Investigar los indicadores
- Administrar las alertas principales
- Ver métricas de NetWitness UEBA en Estado y condición

Filtrar alertas

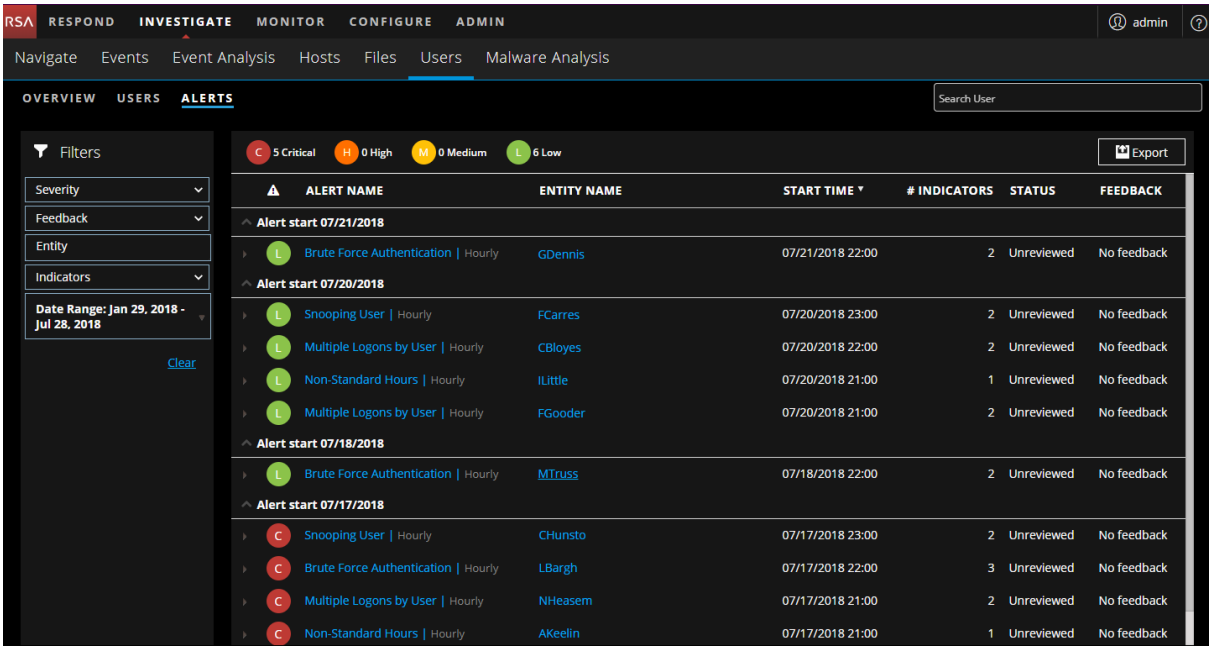
Puede filtrar las alertas mostradas en la pestaña Alertas por gravedad, comentarios, entidad, indicadores y rango de fechas.

1. Inicie sesión en NetWitness Platform y vaya a **INVESTIGAR** > **Usuarios** > **Alertas**. Se muestra la pestaña Alertas.



2. Para filtrar por gravedad, haga clic en **Gravedad** en el panel **Filtro de alertas**, seleccione una o más opciones y, a continuación, haga clic en **Aceptar**. Las opciones son Seleccionar todo, Crítica, Alta, Media y Baja.

3. Para filtrar por comentarios, haga clic en la flecha hacia abajo en **Comentarios**, seleccione una o más opciones y, a continuación, haga clic en **Aceptar**. Las opciones son Seleccionar todo, Sin comentarios y No es un riesgo.
4. Para filtrar por entidad, escriba un nombre de usuario o el nombre de una entidad en el campo **Entidad**.



5. Para filtrar por rango de fechas, haga clic en la flecha hacia abajo en **Rango de flechas**, seleccione una opción y, a continuación, haga clic en **Aceptar**. Las opciones son La semana pasada, El mes pasado y Seleccionar rango.

Las alertas se muestran en el panel derecho de acuerdo con el filtro que seleccionó. Para borrar los filtros, en el panel izquierdo, haga clic en **Borrar**.

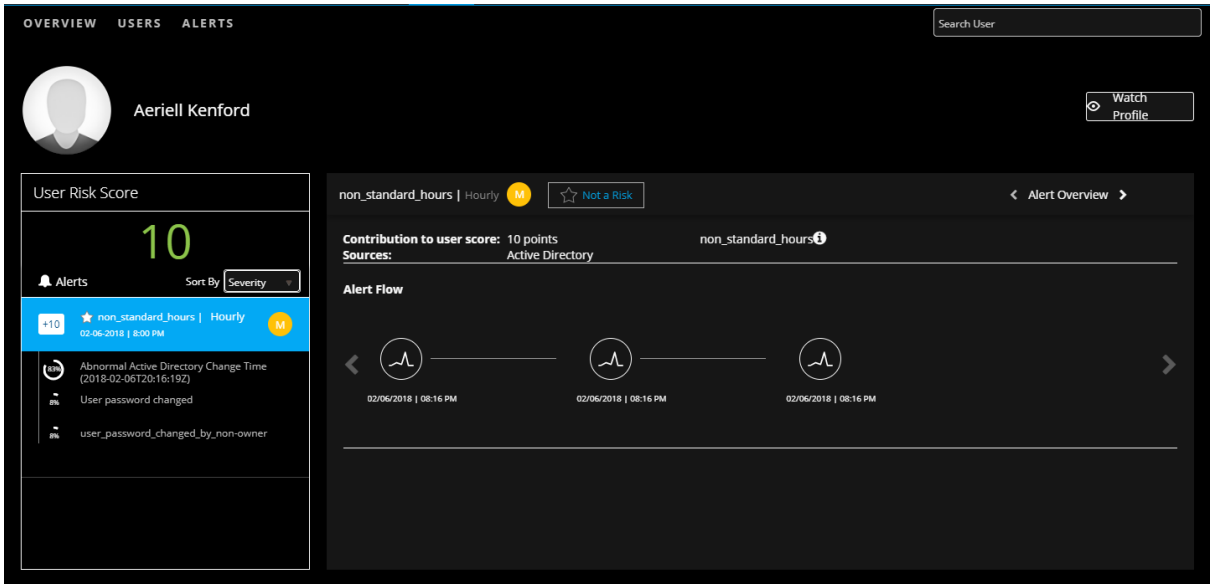
Investigar los indicadores

Puede ver todos los indicadores que forman una alerta en la pestaña ALERTAS. Cada indicador también muestra su valor de anomalía entre paréntesis. Puede encontrar el nombre del indicador y una descripción del tipo de indicador, los valores de anomalía y el origen de datos de los eventos presentes en el indicador. También puede ver un gráfico que muestra detalles sobre un indicador específico. Puede investigar un indicador para buscar actividad relacionada durante un rango de tiempo si cambia a **INVESTIGAR** > vista **Eventos**. En la vista Usuarios, los valores que habilitan el cambio se destacan en azul claro, y usted puede hacer clic en un valor para abrir la vista Evento. En la vista Evento, el valor seleccionado se configura en todas las claves de metadatos y el rango de tiempo se establece en un día. Puede cambiar el rango de tiempo.

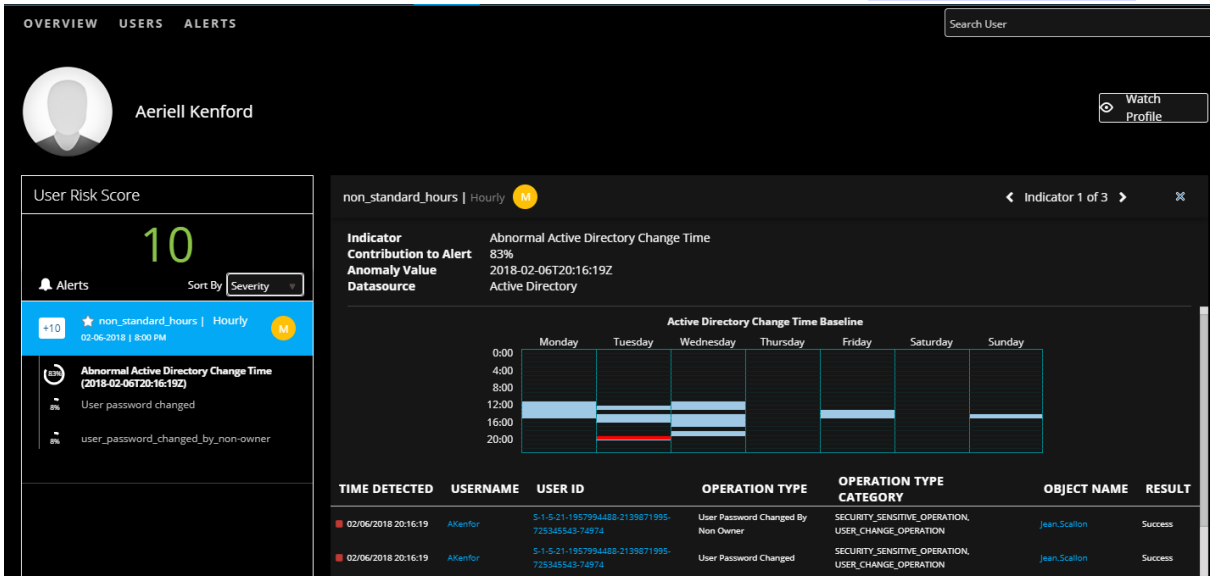
Para ver todos los indicadores de amenazas que componen una alerta:

1. Inicie sesión en NetWitness Platform y vaya a **INVESTIGAR** > **Usuarios** > **ALERTAS**.

2. En **NOMBRE DE ALERTA**, haga clic en un nombre de alerta.
   Se muestran los indicadores, junto con el valor de anomalía, el origen de datos y la hora de inicio.



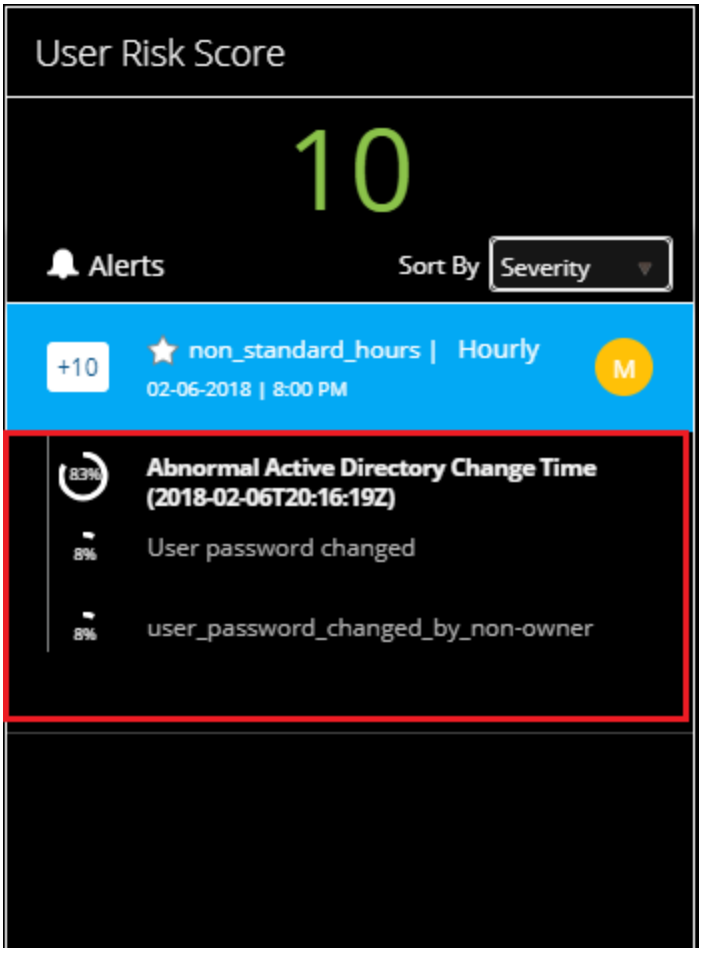
3. En **Flujo de la alerta**, haga clic en el icono de gráfico.
   Se muestra un gráfico en el que se enumeran detalles sobre un indicador específico, incluida la cronología en la que se produjo la anomalía y el usuario asociado con el indicador. En la siguiente figura se muestra un ejemplo de un gráfico. El tipo de gráfico puede variar según el tipo de análisis que realiza NetWitness UEBA. Para obtener más información, consulte Vista Perfil de usuario.



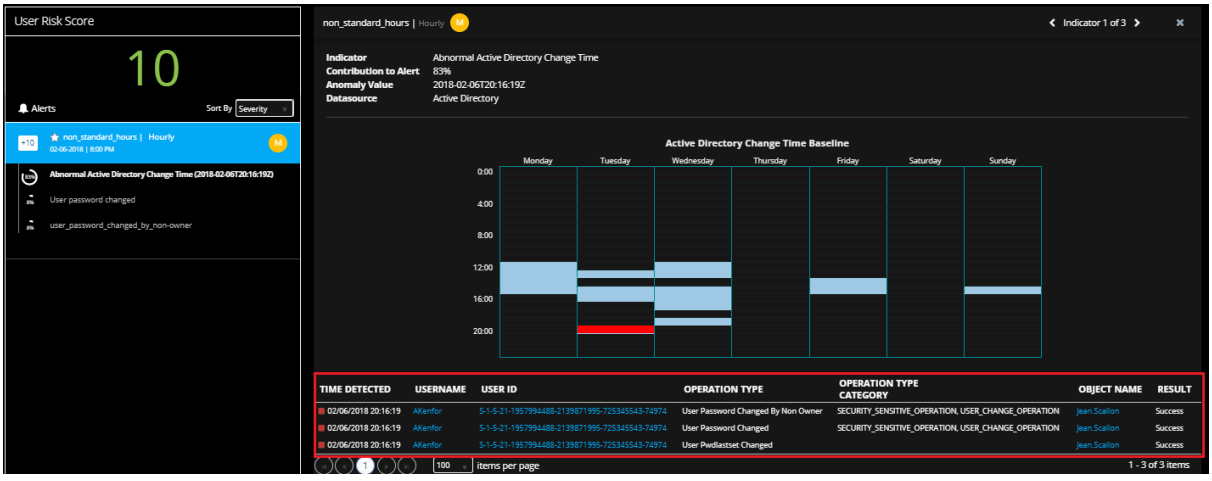
Para cambiar a la vista Eventos:

1. Vaya a **INVESTIGAR** > **Usuarios** y seleccione una alerta o un usuario.

2. En **Puntaje de riesgo del usuario**, seleccione un nombre de alerta.
   Los indicadores se muestran bajo la alerta.



3. Seleccione un indicador que sea de su interés.
   Los valores que se pueden utilizar para realizar un cambio se destacan en azul claro en la parte inferior del panel.



4. Haga clic en un elemento de indicador destacado en azul.
   Se abre la vista Eventos y se muestran detalles sobre el elemento de indicador.

La fecha en la vista Eventos es el día en que se produjo la alerta. El texto del campo de búsqueda es el valor que se seleccionó. Los eventos que se muestran son todos los eventos relacionados con el valor seleccionado.

Para obtener información sobre la investigación de elementos de interés en la vista Eventos, consulte "Investigación de eventos crudos en la vista Eventos" en la *Guía del usuario de NetWitness Investigate*.

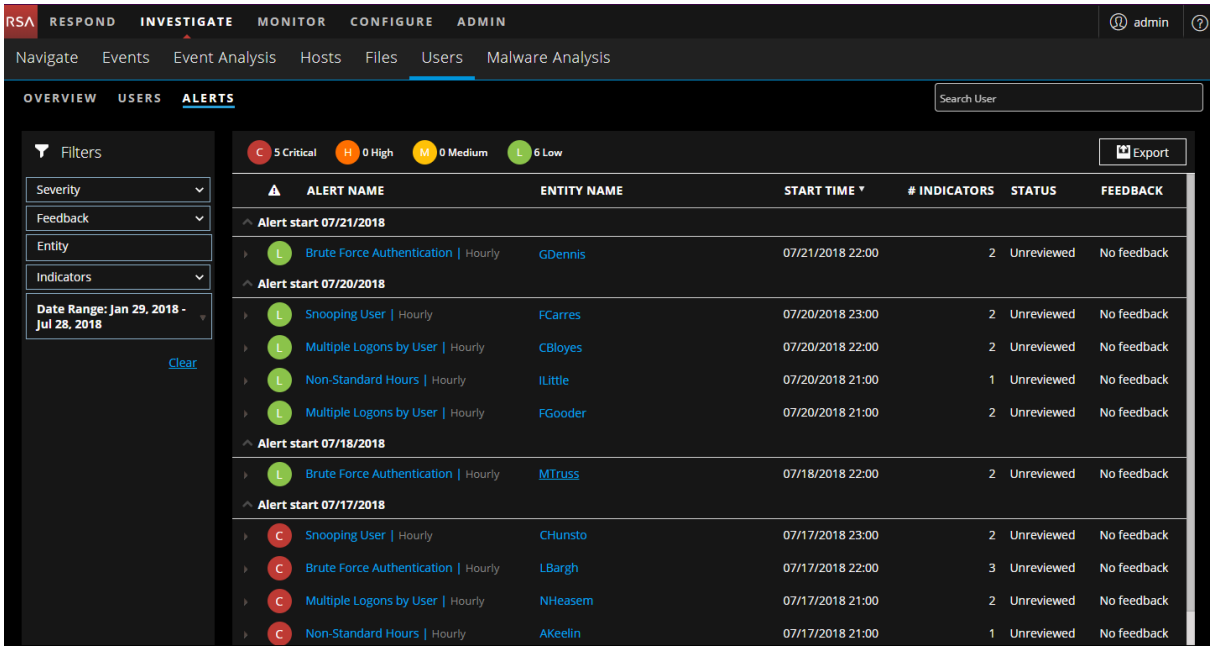
Para obtener más información sobre los indicadores de amenazas, consulte la sección Indicadores de amenazas en Introducción

Administrar las alertas principales

Puede exportar una lista de todas las alertas a un formato de archivo .csv. Un analista puede utilizar esta información para comparar los datos de otros orígenes en otras herramientas de análisis, como Tableau, Power BI y Zeppelin.

Para exportar datos de alertas a un archivo .csv:

1. Inicie sesión en NetWitness Platform y vaya a **INVESTIGAR** > **Usuarios** > **ALERTAS**.
   Se muestra la pestaña Alertas.



2. En la esquina superior derecha, haga clic en **Exportar**.
   Todos los datos de alertas se descargan en un formato de archivo .csv. A continuación se muestra un ejemplo de los datos de alertas exportados en formato .csv:

	A	B	C	D	E	F	G
1	Alert Name	Entity Name	Start Time	# of Indicators	Status	Feedback	Severity
2	Brute Force Au	presidio_4769_u	Jul 21 2018 22:0	2	Reviewed	No Feedback	Low
3	Snooping User	4769_user122	Jul 20 2018 23:0	2	Reviewed	No Feedback	Low
4	Multiple Logon	presidio_4769_u	Jul 20 2018 22:0	2	Reviewed	No Feedback	Low
5	Non-Standard I	4769_user122	Jul 20 2018 21:0	1	Reviewed	No Feedback	Low
6	Multiple Logon	PRESIDIO_USER:	Jul 20 2018 21:0	2	Reviewed	No Feedback	Low
7	Brute Force Au	presidio_4769_u	Jul 18 2018 22:0	2	Reviewed	No Feedback	Low
8	Snooping User	4769_user122	Jul 17 2018 23:0	2	Reviewed	No Feedback	Critical
9	Brute Force Au	presidio_4769_u	Jul 17 2018 22:0	3	Reviewed	No Feedback	Critical
10	Multiple Logon	PRESIDIO_USER:	Jul 17 2018 21:0	2	Reviewed	No Feedback	Critical
11	Non-Standard I	4769_user122	Jul 17 2018 21:0	1	Reviewed	No Feedback	Critical
12							

Ver métricas de NetWitness UEBA en Estado y condición

RSA NetWitness UEBA envía métricas a la pestaña Navegador de estadísticas del sistema en **ADMINISTRAR** > **Estado y condición**. Junto con información básica de uso del sistema, se proporcionan métricas que son específicas de los usuarios, las alertas y los eventos de NetWitness UEBA.

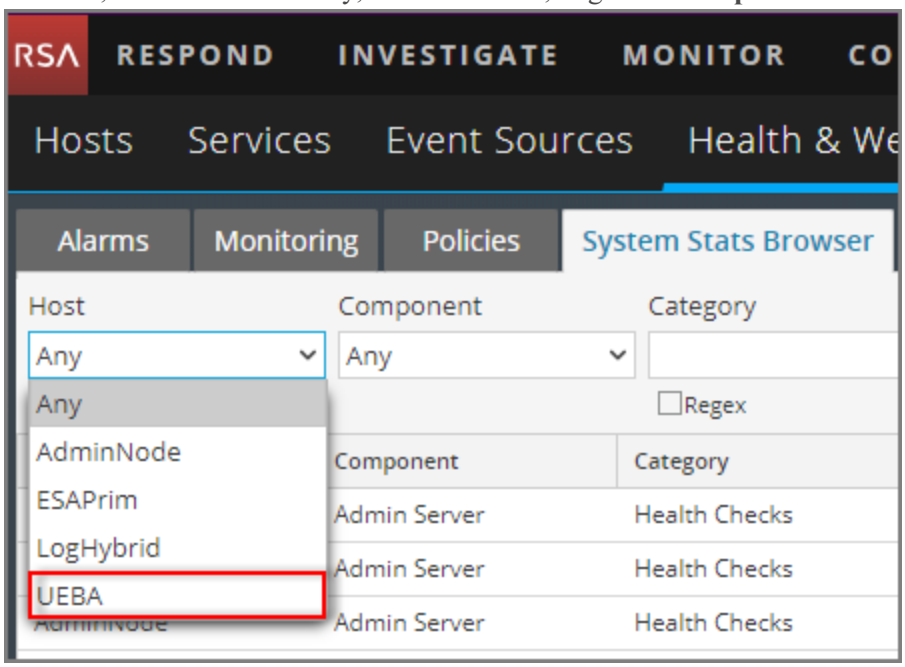
Los analistas pueden utilizar estas métricas de las siguientes maneras:

- Confirme que la licencia adquirida actualmente cumpla con sus acuerdos de licencia y por cuánto al día.
- Determine si el sistema funciona según se requiere.
- Monitoree activamente los eventos nuevos.
- Monitoree la creación de nuevos indicadores y alertas.

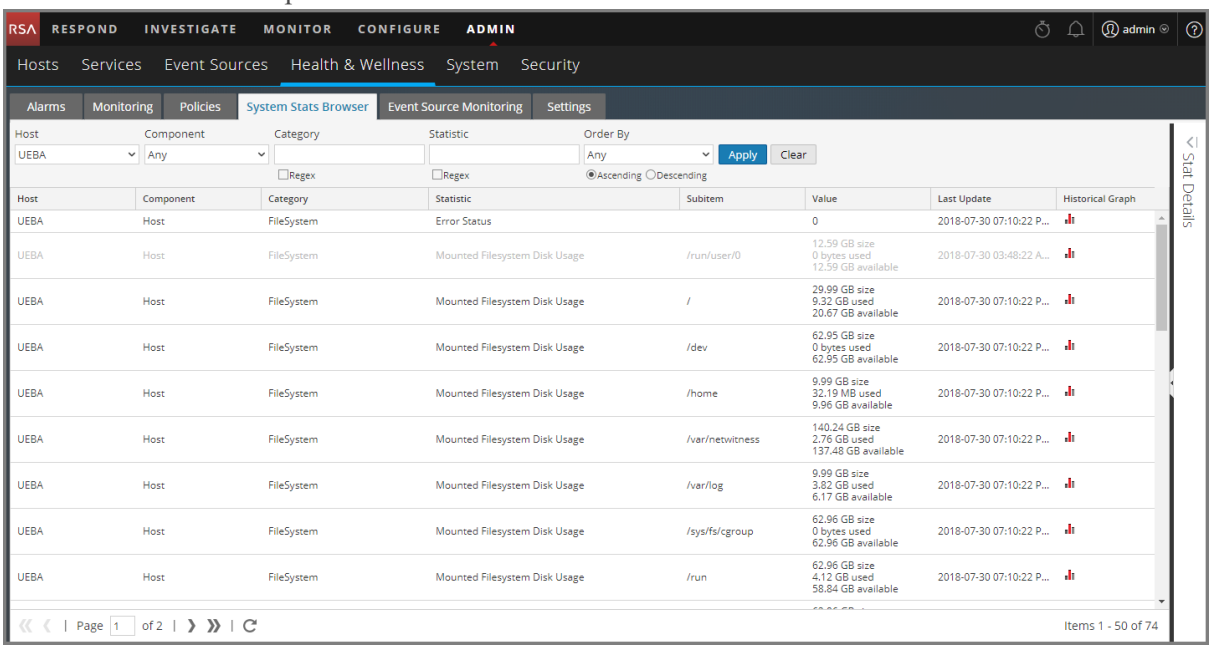
Si estas métricas críticas se informan como “0”, esto podría indicar una falla del sistema.

Para ver métricas de NetWitness UEBA en el Navegador de estadísticas del sistema en Estado y condición:

1. Inicie sesión en NetWitness Platform y vaya a **ADMINISTRAR** > **Estado y condición**.
2. Haga clic en la pestaña Navegador de estadísticas del sistema.
   Se muestra el Navegador de estadísticas del sistema.
3. En Host, seleccione **UEBA** y, a continuación, haga clic en **Aplicar**.



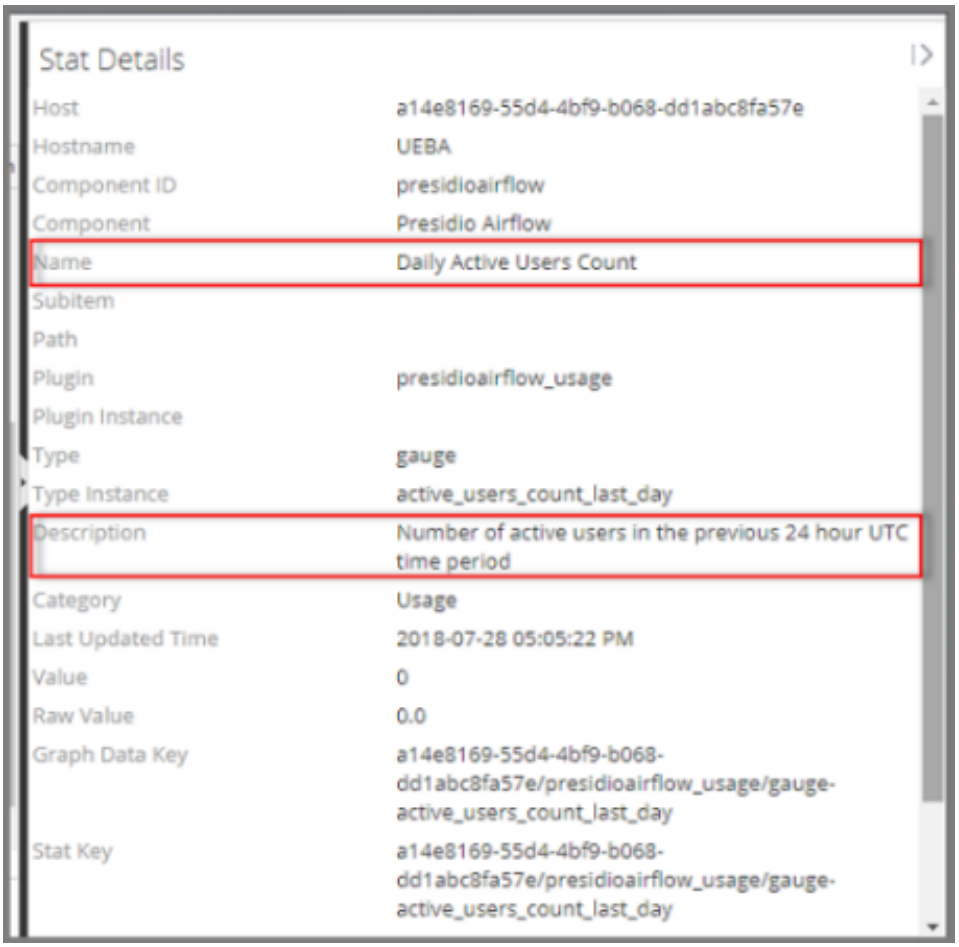
Se muestran resultados para NetWitness UEBA.



Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
UEBA	Host	FileSystem	Error Status		0	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/run/user/0	12.59 GB size 0 bytes used 12.59 GB available	2018-07-30 03:48:22 A...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/	29.99 GB size 9.32 GB used 20.67 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/dev	62.95 GB size 0 bytes used 62.95 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/home	9.99 GB size 32.19 MB used 9.96 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/var/netwitness	140.24 GB size 2.76 GB used 137.48 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/var/log	9.99 GB size 3.82 GB used 6.17 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/sys/fs/cgroup	62.96 GB size 0 bytes used 62.96 GB available	2018-07-30 07:10:22 P...	
UEBA	Host	FileSystem	Mounted Filesystem Disk Usage	/run	62.96 GB size 4.12 GB used 58.84 GB available	2018-07-30 07:10:22 P...	

4. Para ver los detalles de una estadística, haga clic en **Detalles de estadística**.

Se muestran los detalles de la estadística.



Los campos **Nombre** y **Descripción** proporcionan un resumen de las métricas que se muestran.

Para obtener más información acerca de Estado y condición y la pestaña Navegador de estadísticas del sistema, consulte “Monitorear estadísticas del sistema” en la *Guía de mantenimiento del sistema*. Vaya a la Tabla maestra de contenido para buscar todos los documentos de NetWitness Platform Logs & Network 11.x.

Referencia

En esta sección se proporciona información acerca de la interfaz del usuario de RSA NetWitness UEBA.

Pestaña Descripción general

La pestaña **Descripción general** proporciona una vista inicial de las actividades recientes y más importantes de los usuarios en el ambiente. Cada panel muestra incidentes ordenados por prioridad para su investigación o métricas consolidadas que reflejan los riesgos potenciales para la empresa.

Flujo de trabajo

¿Qué desea hacer?

Función de usuario	Deseo…	Documentación
Analista de UEBA	Ver los cinco principales usuarios de alto riesgo*.	Identificar a los usuarios de alto riesgo
Analista de UEBA	Ver usuarios riesgosos, monitorear usuarios y administrar usuarios*.	Identificar a los usuarios de alto riesgo
Analista de UEBA	Ver usuarios en función del tipo de alerta y el indicador.	Identificar a los usuarios de alto riesgo
Analista de UEBA	Investigar las alertas en mi ambiente.	Investigar las alertas principales
Analista de UEBA	Iniciar una investigación de alertas críticas.	Investigar las alertas principales
Analista de UEBA	Ordenar las alertas para centrar mi investigación.	Filtrar alertas

Función de usuario	Deseo…	Documentación
Analista de UEBA	Investigar los indicadores de amenazas.	Investigar los indicadores
Analista de UEBA	Exportar datos de gráfico	Administrar las alertas principales

* Puede realizar las tareas aquí.

Temas relacionados

- Iniciar una investigación de usuarios de alto riesgo
- Investigar las alertas principales
- Filtrar alertas
- Administrar las alertas principales

Vista rápida

En la siguiente figura se muestra la pestaña Descripción general.

Para acceder a esta vista, vaya a **INVESTIGAR** > **Usuarios**.

La pestaña Descripción general consta de los siguientes paneles:

1. Panel Usuarios de alto riesgo
2. Panel Alertas principales
3. Panel Todos los usuarios
4. Panel Gravedad de las alertas

Panel Usuarios de alto riesgo

El panel Usuarios de alto riesgo enumera los cinco principales usuarios de alto riesgo junto con su puntaje.

En la siguiente tabla se describen los elementos del panel Usuarios de alto riesgo.

Nombre	Descripción
Nombre de usuario	El nombre del usuario.
Puntaje del usuario	El puntaje del usuario con un color que indica su gravedad. El rojo indica una prioridad Crítica, el naranja, riesgo de prioridad Alta, el amarillo, Media y el verde, Baja.

Panel Alertas principales

El panel Alertas principales muestra una lista de alertas para el usuario asociado, la gravedad, la fecha de creación de las alertas y la cantidad de indicadores. La lista consta de las diez alertas principales en los últimos 7 días.

En la siguiente tabla se describen los elementos del panel Alertas principales.

Nombre	Descripción
Icono de gravedad	El icono de gravedad de la alerta. Las opciones son Crítica, Alta, Media o Baja.
Nombre de alerta	El nombre de la alerta
Fecha de creación de la alerta	La fecha en que se genera una alerta.
Cantidad de indicadores	La cantidad de indicadores asociados a la alerta.

Panel Todos los usuarios

El panel Todos los usuarios muestra la cantidad de usuarios en cada uno de los grupos predefinidos de NetWitness UEBA.

En la siguiente tabla se describen los elementos del panel Todos los usuarios.

Grupo	Descripción
Riesgosos	Todos los usuarios con un puntaje de riesgo mayor que 0.
Con seguimiento	Todos los usuarios marcados actualmente como Con seguimiento.
Administrador	Todos los usuarios que se han etiquetado anteriormente como Administrador.

Panel Gravedad de las alertas

El panel Gravedad de las alertas muestra, de manera gráfica, la cantidad de alertas generadas el año anterior por nivel de gravedad.

En la siguiente tabla se describen los elementos del panel Gravedad de las alertas.

Nombre	Descripción
El año pasado	La cantidad de alertas generadas el año anterior.
Nivel de gravedad	La gravedad está codificada en colores. El rojo indica una alerta Crítica, el naranja, riesgo de alerta Alta, el amarillo, Media y el verde, Baja. Por ejemplo: 

Pestaña Usuarios

La pestaña **Usuarios** es una consola de búsqueda de amenazas proactiva. Puede utilizar filtros de comportamiento para crear listas de objetivos orientadas a casos de uso y monitorear continuamente el ambiente en busca de patrones de comportamiento riesgoso específicos.

Flujo de trabajo

¿Qué desea hacer?

Función de usuario	Deseo…	Documentación
Analista de UEBA	Ver usuarios de alto riesgo*.	Identificar a los usuarios de alto riesgo
Analista de UEBA	Ver usuarios en función del tipo de alerta y el indicador*.	Identificar a los usuarios de alto riesgo
Analista de UEBA	Iniciar una investigación de usuarios de alto riesgo.	Iniciar una investigación de usuarios de alto riesgo
Analista de UEBA	Adoptar medidas en relación con los usuarios de alto riesgo*.	Adoptar medidas en relación con los usuarios de alto riesgo
Analista de UEBA	Exportar usuarios de alto riesgo*.	Exportar usuarios de alto riesgo
Analista de UEBA	Iniciar una investigación de alertas críticas.	Investigar las alertas principales
Analista de UEBA	Investigar los indicadores de amenazas.	Investigar los indicadores

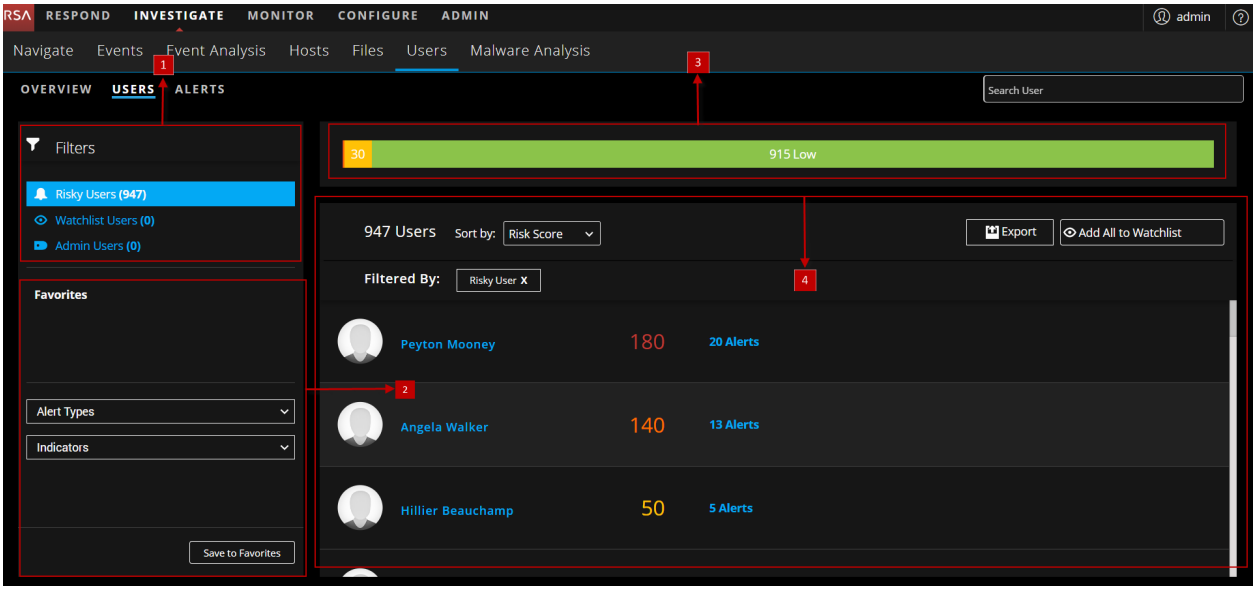
* Puede realizar las tareas aquí.

Temas relacionados

- Iniciar una investigación de usuarios de alto riesgo
- Investigar las alertas principales
- Filtrar alertas
- Investigar los indicadores
- Exportar usuarios de alto riesgo

Vista rápida

En la siguiente figura se muestra la pestaña Usuarios.



Para acceder a esta vista:

1. Vaya a **INVESTIGAR** > **Usuarios**.

   Se muestra la pestaña Descripción general.

2. Haga clic en **Usuarios**.

La pestaña Usuarios consta de los siguientes paneles:

1	Panel Filtros
2	Panel Favoritos
3	Panel Indicador de riesgo
4	Panel Lista de usuarios

Filtros del panel Filtros

El panel Filtros enumera tres filtros predefinidos y muestra la cantidad de usuarios asociados a cada uno de ellos entre paréntesis.

En la siguiente tabla se describen los tipos de filtros.

Tipo de filtro	Descripción
Usuarios riesgosos	Todos los usuarios con un puntaje de riesgo mayor que 0.
Usuarios de la lista de seguimiento	Todos los usuarios marcados actualmente como Con seguimiento.
Usuarios administradores	Todos los usuarios que se han etiquetado anteriormente como Administrador.

Panel Favoritos

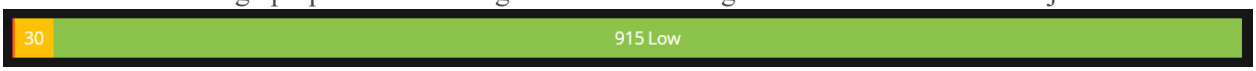
El panel Favoritos muestra la lista de perfiles de comportamiento que se guardan como favoritos.

En la siguiente tabla se describen los tipos de filtros del perfil de comportamiento.

Filtros	Descripción
Tipos de alerta	Cualquiera de los tipos de alertas existentes que describen los distintos casos de uso compatibles (p. ej., Intento de ataque de fuerza bruta, Usuario entrometido, Cambio anormal en AD y Extracción de datos).
Indicadores	Cualquiera de las características de comportamiento existentes que modela NetWitness UEBA. Este filtro también se puede usar para centrarse únicamente en alertas de una aplicación o un origen de datos específicos.

Panel Indicador de riesgo

El indicador de riesgo proporciona un desglose basado en la gravedad de los usuarios objetivo.



En la siguiente tabla se describen los elementos del panel Indicador de riesgo.

Color	Gravedad
Rojo	Crítica
Naranja	Alta
Amarillo	Media
Verde	Baja

Panel Lista de usuarios

El panel Lista de usuarios muestra la lista de todos los usuarios del ambiente junto con su puntaje y la cantidad de alertas asociadas con ellos.

En la siguiente tabla se describen los elementos del panel Lista de usuarios.

Datos del usuario	Descripción
Nombre de usuario	El nombre del usuario.
Puntaje	El puntaje del usuario.
Cantidad de alertas	La cantidad total de alertas generadas para el usuario.
Ordenar por	El menú desplegable Ordenar por permite seleccionar el método de clasificación de la lista. Las opciones son: Puntaje de riesgo, Nombre y Alertas.
Exportar	Exporte una lista de todos los usuarios y sus puntajes en un formato de archivo .csv.
Agregar todos a la lista de seguimiento	Agrega todos los usuarios de la vista filtrada a la lista de seguimiento.
Buscar usuario	Busca un nombre de usuario que usted escribió. Puede seleccionarlo de la lista que se muestra con valores que coinciden con su entrada.

Pestaña Alertas

La pestaña Alertas muestra detalles sobre todas las alertas del ambiente. Puede ver información forense sobre actividad sospechosa en el ambiente que se basa en un intervalo de tiempo específico.

Flujo de trabajo

¿Qué desea hacer?

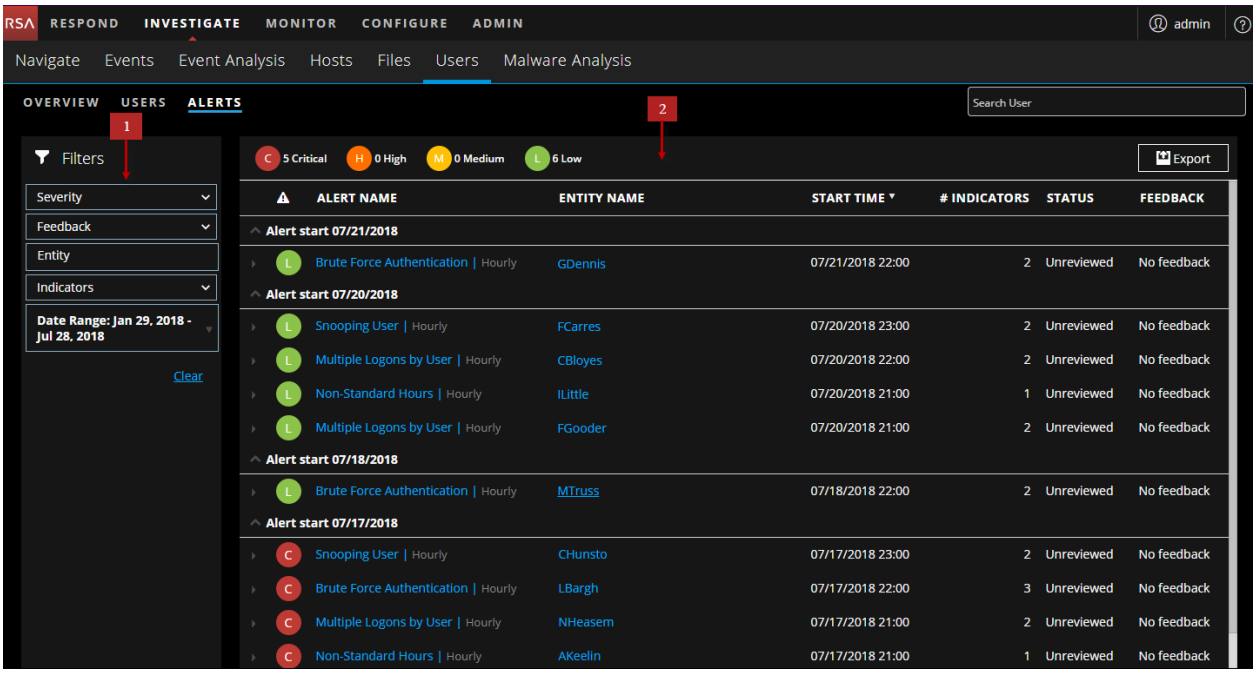
Función de usuario	Deseo…	Documentación
Analista de UEBA	Investigar las alertas en mi ambiente*.	Investigar las alertas principales
Analista de UEBA	Ordenar las alertas para centrar mi investigación*.	Filtrar alertas
Analista de UEBA	Investigar incidentes basados en indicadores de amenazas*.	Investigar los indicadores
Analista de UEBA	Compartir datos de alertas en formato de hoja de cálculo.	Administrar las alertas principales
Analista de UEBA	Ver rápidamente un resumen de alertas de usuarios.	Ver resúmenes de alertas de usuarios

* Puede realizar las tareas aquí.

Temas relacionados

- Investigar las alertas principales
- Filtrar alertas
- Investigar los indicadores
- Administrar las alertas principales

Vista rápida



Para acceder a esta vista:

1. Vaya a **INVESTIGAR** > **Usuarios**.

   Se muestra la pestaña Descripción general.

2. Haga clic en **Alertas**.

La pestaña Alertas consta de los siguientes paneles:

1 Panel Filtros
2 Panel Alerts

Panel Filtros

Utilice el panel Filtros para acotar la investigación de alertas. Los filtros se aplican automáticamente a medida que se realizan las selecciones. Puede borrar todos los filtros configurados actualmente haciendo clic en **Borrar**.

En la siguiente tabla se describen los tipos de filtros.

Nombre del filtro	Descripción	Opciones
Gravedad	Filtra la lista de alertas para incluir alertas correspondientes a uno o más niveles de gravedad.	Crítica, Alta, Media o Baja.
COMENTARIOS	Filtra la lista de alertas para incluir alertas correspondientes a uno o más tipos de comentarios.	Seleccione Todo, Sin comentarios o No es un riesgo.

Nombre del filtro	Descripción	Opciones
Entidad	Filtra la lista de alertas para incluir solamente las alertas correspondientes a un nombre de usuario específico.	N/D.
Indicadores	Filtra la lista de alertas para incluir alertas correspondientes a uno o más indicadores.	Los siguientes son ejemplos de indicadores: • Active Directory: hora de inicio de sesión anormal • Autenticación: inicio de sesión en varias computadoras • Varias fallas de acceso a archivos
Rango de fechas	Filtra la lista de alertas para incluir alertas creadas durante un rango de tiempo específico.	La semana pasada, El mes pasado o un rango especificado

Panel Alertas

El panel Alertas muestra la siguiente información para cada alerta:

- Icono de gravedad: Un icono junto al nombre de la alerta que indica el nivel de gravedad de la alerta
- Nombre de alerta: El nombre de la alerta y su intervalo de tiempo
- Nombre de entidad: El nombre de la entidad (cuenta de usuario) que generó la alerta
- Hora de inicio: Fecha y hora en que esta alerta se detectó por primera vez
- N.º de indicadores: La cantidad de anomalías de comportamiento únicas (indicadores) asociadas a la alerta
- Estado: Indica si la alerta se marcó como Sin revisar o No es un riesgo
- Comentarios: Indica si se asignó un valor de comentarios para la alerta

Al principio de cada línea de alerta hay un icono que expande la alerta para mostrar detalles adicionales. Una vez expandida, se muestran los siguientes campos:

- Nombre del indicador: El nombre de cada indicador único asociado a la alerta
- Valor de anomalía: El valor del indicador que representa la cantidad o el valor de desviación en que difiere respecto del comportamiento normal del usuario

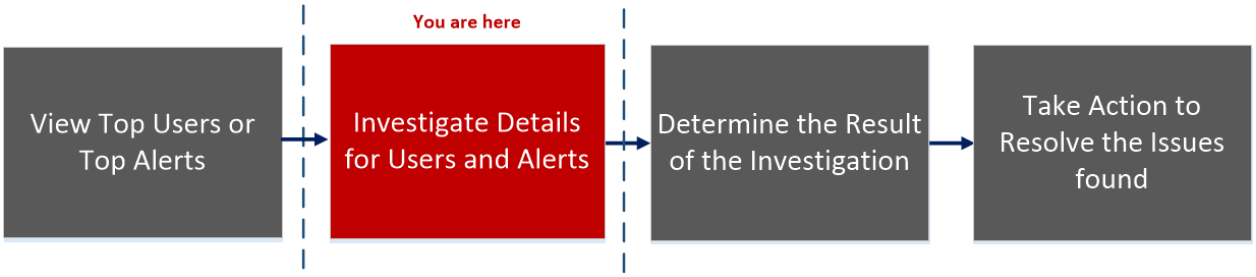
- Origen de datos: El tipo de datos donde se encontró el indicador
- Hora de Inicio: Fecha y hora en que este indicador se detectó por primera vez
- N.º de eventos: La cantidad de eventos en el indicador

Los datos que se muestran actualmente en el panel central se pueden exportar a un archivo .csv haciendo clic en Exportar en la esquina superior derecha del panel.

Vista Perfil de usuario

La vista **Perfil de usuario** proporciona información detallada sobre todas las alertas y los indicadores relacionados de un usuario.

Flujo de trabajo



¿Qué desea hacer?

Función de usuario	Deseo…	Documentación
Analista de UEBA	Ver usuarios de alto riesgo*	Identificar a los usuarios de alto riesgo
Analista de UEBA	Iniciar una investigación de usuarios de alto riesgo*	Iniciar una investigación de usuarios de alto riesgo
Analista de UEBA	Adoptar medidas en relación con los usuarios de alto riesgo.	Adoptar medidas en relación con los usuarios de alto riesgo
Analista de UEBA	Exportar usuarios de alto riesgo.	Exportar usuarios de alto riesgo
Analista de UEBA	Iniciar una investigación de alertas críticas*	Investigar las alertas principales
Analista de UEBA	Investigar los indicadores de amenazas.	Investigar los indicadores

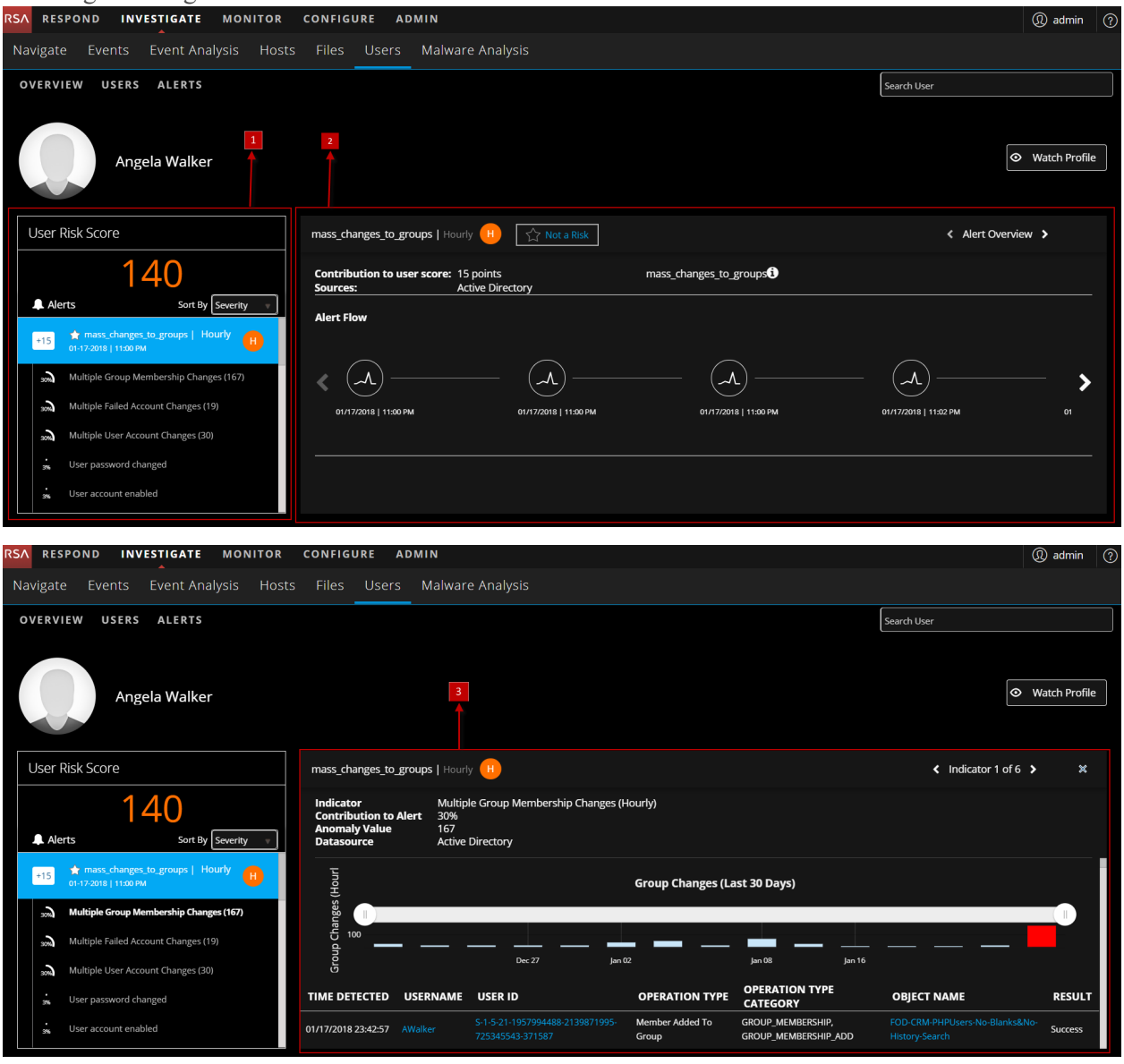
* Puede realizar las tareas aquí.

Temas relacionados

- Iniciar una investigación de usuarios de alto riesgo
- Investigar las alertas principales
- Filtrar alertas
- Investigar los indicadores
- Exportar usuarios de alto riesgo

Vista rápida

En la siguiente figura se muestra la vista Perfil de usuario.



Para acceder a esta vista:

1. Vaya a **INVESTIGAR** > **Usuarios**. Realice cualquiera de las siguientes acciones:
   a. En la pestaña **DESCRIPCIÓN GENERAL**, bajo el panel **Usuarios de alto riesgo**, seleccione un usuario y haga clic en el nombre de usuario o en su puntaje.
   b. En la pestaña **USUARIOS**, seleccione un usuario y haga clic en el nombre de usuario.
   c. En la pestaña **ALERTAS**, seleccione un nombre de alerta o un nombre de entidad.

El Perfil de usuario consta de los siguientes paneles:

1 Panel Puntaje de riesgo del usuario
2 Panel Flujo de alertas
3 Panel Indicadores

Panel Puntaje de riesgo del usuario

El panel Puntaje de riesgo del usuario contiene la siguiente información:

Nombre	Descripción
Puntaje del usuario	El puntaje del usuario destacado en función de la gravedad.
Alertas	Se muestra la siguiente información: • Los nombres de la alerta • El icono del nivel de gravedad • La fecha y la hora de inicio de la alerta • El intervalo de tiempo de la alerta (Por hora o Diariamente) • El puntaje de riesgo de la alerta (+20) • Una lista de nombres de indicadores de alerta y la cantidad de veces que ocurrieron los eventos de los indicadores.
Ordenar por	Las alertas se ordenan en función de la gravedad y la fecha. De manera predeterminada, se ordenan por gravedad.

Panel Flujo de alertas

El panel Flujo de alertas muestra la siguiente información:

Nombre	Descripción
Nombre de alerta	El nombre de la alerta

Nombre	Descripción
Plazo	El intervalo de tiempo de la alerta (Por hora o Diariamente).
Nivel de gravedad	La gravedad de la alerta.
Contribución al puntaje del usuario	La contribución al valor de puntaje del usuario (p. ej., +20).
Orígenes	Los orígenes de datos de la alerta (p. ej., Active Directory).
Gráfico de cronología	La cronología de eventos relacionados con la formación de la alerta.

Panel Indicadores

Haga clic en un icono de gráfico del panel Flujo de alertas para abrir el panel Indicador. En la siguiente tabla se describen los elementos del panel Indicadores:

Nombre	Descripción
Indicador	El nombre del indicador con el intervalo de tiempo del indicador entre paréntesis. Por ejemplo, Varios cambios en la membresía en grupos (por hora).
Contribución a la alerta	El porcentaje de contribución de la alerta.
Valor de anomalía	El valor de la anomalía.
Origen de datos	El origen de datos desde el que desencadena la alerta.
Hora de detección	La fecha y la hora en que se desencadena un indicador.
Nombre de usuario	El nombre del usuario para el que se desencadena un indicador.
ID de usuario	El ID del usuario para el que se desencadena un indicador.
Tipo de operación	La acción que realizó el usuario. Por ejemplo, Se agregó un miembro a un grupo.
Categoría de tipo de operación	El tipo de categoría de operación. Por ejemplo, GROUP_MEMBERSHIP.
Resultado	El estado de la acción que realizó el usuario.

Apéndice: Política de auditoría de Windows de NetWitness UEBA

Para sacar el máximo provecho de RSA NetWitness UEBA, RSA recomienda implementar las políticas de auditoría de Windows que se describen aquí.

Para conocer un conjunto básico de políticas de auditoría, consulte la sección “Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, and Windows Server 2008 Audit Settings Recommendations” de este artículo de Microsoft: Audit Policy Recommendations.

Las políticas señaladas en “Stronger Recommendation” son obligatorias, así como las siguientes, para asegurarse de que se auditen todos los eventos de autenticación y Active Directory requeridos:

- Auditar recurso compartido de archivos detallado
- Auditar recurso compartido de archivos
- Auditar sistema de archivos

RSA recomienda habilitar la auditoría tanto para operaciones correctas como para fallas.

Se deben auditar los siguientes eventos de Windows:

Para los modelos de autenticación:

4624	4625	4769

Para los modelos de AD:

4670	4717	4720	4722	4723	4724	4725	4726
4727	4728	4729	4730	4731	4732	4733	4734
4735	4737	4738	4739	4740	4741	4742	4743
4754	4755	4756	4757	4758	4764	4767	4794
5136	5376	5377					

Para los modelos de acceso a archivos:

4660	4663	4670	5145