Guía de descripción general

Sentinel 7.0.1

March 2012

Información legal

Para obtener más información, póngase en contacto con NetIQ en:

1233 West Loop South, Houston, Texas 77027
EE. UU.
www.netiq.com

Tabla de contenido

Acerca de esta guía

Esta guía le introduce a Sentinel, un producto WorkloadIQ.

Usuarios a los que va dirigida

Esta guía está dirigida a los profesionales de seguridad de la información.

Comentarios

Nos gustaría recibir sus comentarios y sugerencias acerca de este manual y del resto de la documentación incluida con este producto. Utilice la función de comentarios del usuario situada en la parte inferior de las páginas de la documentación en línea.

Actualizaciones de la documentación

Para ver la versión más reciente de la *Guía de descripción general de Sentinel 7.0.1*, visite el sitio Web de documentación de Sentinel (http://www.novell.com/documentation/sentinel70).

Documentación adicional

La documentación técnica de Sentinel se divide en varios volúmenes distintos. Son los siguientes:

- Sentinel Quick Start Guide (Guía de inicio rápido de Sentinel) (http://www.novell.com/documentation/sentinel70/s70_quickstart/data/s70_quickstart.html)
- Sentinel Installation Guide (Guía de instalación de Sentinel) (http://www.novell.com/documentation/sentinel70/s70_install/data/bookinfo.html)
- Sentinel Administration Guide (Guía de administración de Sentinel) (http://www.novell.com/documentation/sentinel70/s70_admin/data/bookinfo.html)
- Sentinel User Guide (Guía del usuario de Sentinel) (http://www.novell.com/documentation/sentinel70/s70_user/data/bookinfo.html)
- Sentinel Link Overview Guide (Guía de descripción general de Sentinel Link) (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html)
- Eventos de auditoría interna de Sentinel (http://www.novell.com/documentation/sentinel70/s70_auditevents/data/bookinfo.html)
- SDK de Sentinel (http://www.novell.com/developer/develop_to_sentinel.html)

  El sitio de SDK de Sentinel proporciona información sobre cómo crear sus propios módulos auxiliares (plug-ins).

Contacto con Novell y NetIQ

Sentinel es ahora un producto de NetIQ, si bien Novell sigue manejando muchas funciones de asistencia.

- Sitio Web de Novell (http://www.novell.com)

- Sitio Web de NetIQ (http://www.netiq.com)
- Asistencia técnica (http://support.novell.com/contact/getsupport.html?sourceidint=suplnav4_phonesup)
- Autoasistencia (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- Sitio de descarga de revisión (http://download.novell.com/index.jsp)
- Foros de asistencia de la comunidad de Sentinel (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Sentinel TIDs (http://support.novell.com/products/sentinel)
- Sitio Web del módulo auxiliar (plug-in) de Sentinel (http://support.novell.com/products/sentinel/secure/sentinel61.html)
- **Lista de notificación por correo electrónico:** Inscríbase a través del sitio Web de módulos auxiliares de Sentinel

Cómo contactar con asistencia para ventas

Para cualquier pregunta sobre nuestros productos, precios y capacidades, póngase en contacto con su representante local. Si no puede contactar con su representante local, comuníquese con nuestro equipo de Asistencia para ventas.

Oficinas mundiales: Ubicaciones de las oficinas de NetIQ (http://www.netiq.com/about_netiq/officelocations.asp)

Estados Unidos y Canadá: 888-323-6768

Correo electrónico: info@netiq.com

Sitio Web: www.netiq.com

1 Descripción general del producto de Sentinel

Sentinel es una solución de gestión de información de seguridad y eventos (SIEM) y de supervisión del cumplimiento. Sentinel supervisa automáticamente los entornos TI más complejos y ofrece la seguridad requerida para protegerlos.

1.1 Por qué la seguridad es importante.

La seguridad debe convertirse en una preocupación principal para las compañías en el mundo actual para reducir costes y asegurar la fidelidad del cliente. Cada fuga de información registrada cuesta una media de 200 dólares. Una vulneración de seguridad que ocasione la pérdida de unos 200.000 registros tendrá un efecto importante en una empresa.

Si su compañía sufre un ataque, podría incurrir en los siguientes gastos:

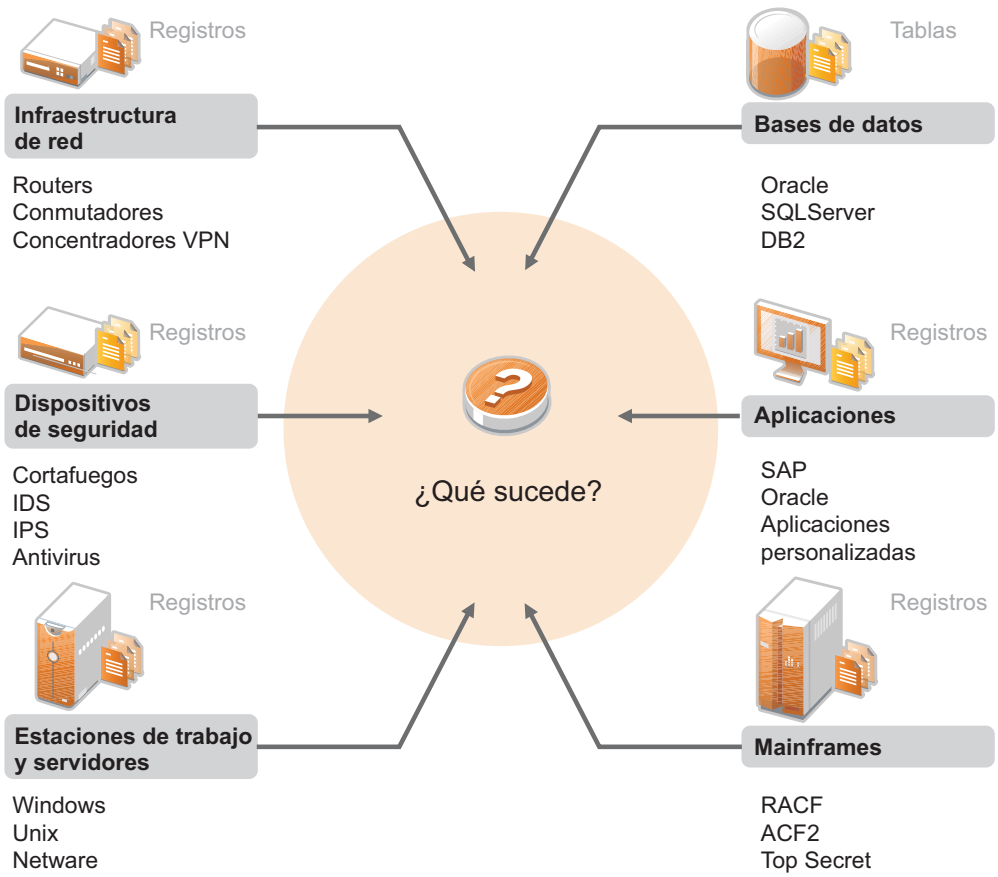
- Costes legales
- Costes de investigación y forenses
- Más auditorías
- Multas y penalizaciones
- Coste oculto de pérdida de credibilidad con los clientes
- Clientes perdidos por la falta de credibilidad

Esto demuestra la importancia de asegurar su entorno TI. En el mundo actual la línea entre las personas internas y externas es poco nítida debido al uso de Internet y el creciente uso de la tecnología de nube.

1.2 Retos de asegurar el entorno TI

Asegurar su entorno TI es un reto debido a su complejidad. Existen muchas aplicaciones diferentes, bases de datos, unidades centrales, estaciones de trabajo y servidores que realizan registros de eventos. Además, cuenta con los dispositivos de seguridad y los dispositivos de infraestructura de red que contienen registros de lo que ocurre en su entorno TI..

Figura 1-1 *Qué ocurre en su entorno.*



Los retos surgen porque:

- Hay muchos dispositivos en su entorno TI.
- Los registros tienen diferentes formatos.
- Los registros se almacenan en silos.
- La cantidad de información generada en los registros.
- No puede determinar quién hizo qué manualmente analizando todos los registros.

Para hacer que la información sea útil, usted debe poder:

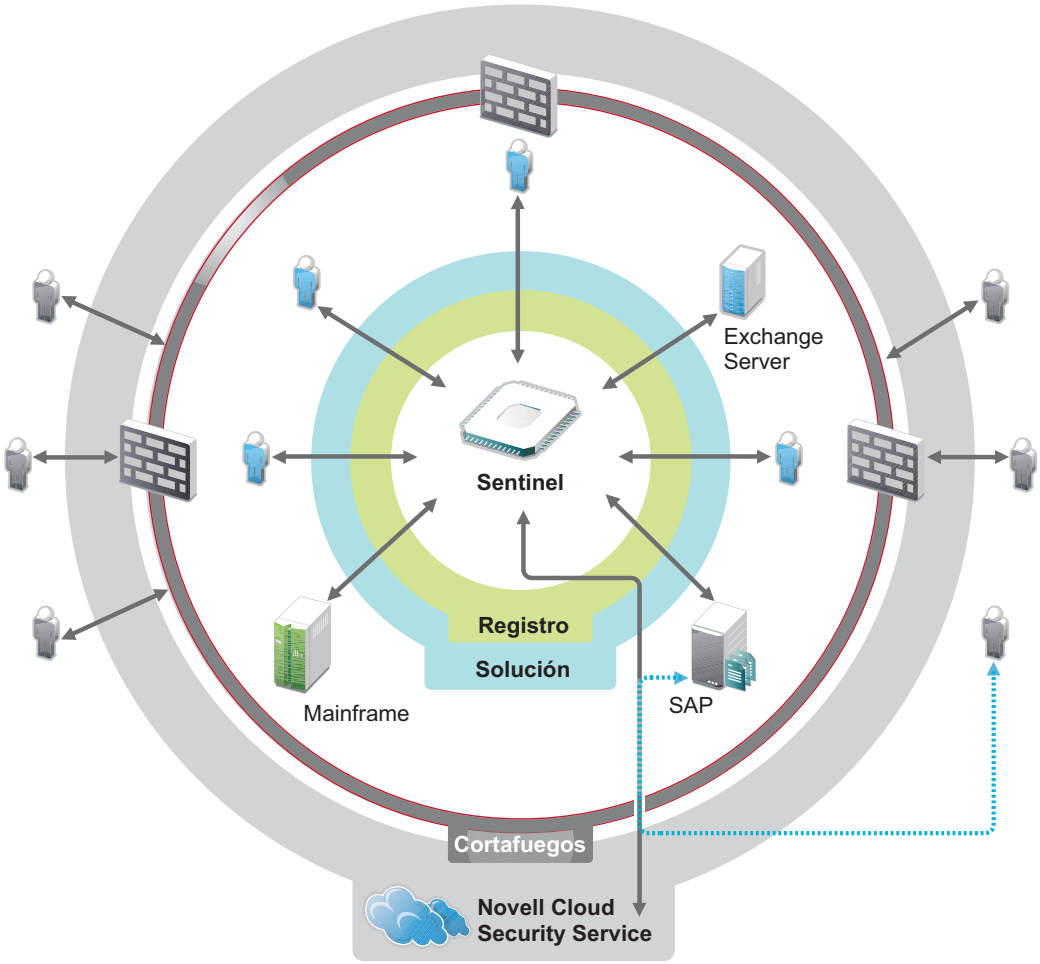
- Recoger los datos.
- Consolidar los datos.
- Normalizar datos dispares en eventos que se puedan comparar fácilmente.
- Asignar eventos a regulaciones estándar.
- Analizar los datos.
- Comparar los eventos en múltiples sistemas para determinar si existen problemas de seguridad.
- Enviar notificaciones cuando los datos estén fuera de las normas.
- Tomar medidas en las notificaciones para cumplir las políticas de empresa.
- Generar informes para demostrar el cumplimiento.

Si conoce los retos de asegurar su entorno TI, necesita determinar cómo asegurar la empresa para y de los usuarios sin tratarles como delincuentes, o cargarles hasta el punto que sea imposible ser productivo. Sentinel ofrece la solución.

1.3 La solución Sentinel ofrece:

Sentinel actúa como el sistema nervioso central para la seguridad de la empresa. Recoge datos de toda la infraestructura: aplicaciones, bases de datos, servidores, almacenamiento y dispositivos de seguridad. Analiza y establece correlaciones entre datos, y los convierte en datos procesables, ya sea de forma manual o automática.

Figura 1-2 *La solución Sentinel ofrece:*



El resultado es que usted conoce las cosas importantes que se producen en su entorno TI en un punto dado, y tiene la capacidad de enlazar las acciones tomadas sobre los recursos con las personas que realizan esas acciones. Esto le permite determinar la conducta del usuario y supervisar el control efectivamente. Independientemente de si la persona es interna o no, puede enlazar todas las acciones juntas de modo que las actividades que verdaderamente son un riesgo estén claras antes de que supongan un daño.

Sentinel realiza esto de un modo rentable del siguiente modo:

- Ofreciendo una solución única para tratar los controles TI en múltiples regulaciones.

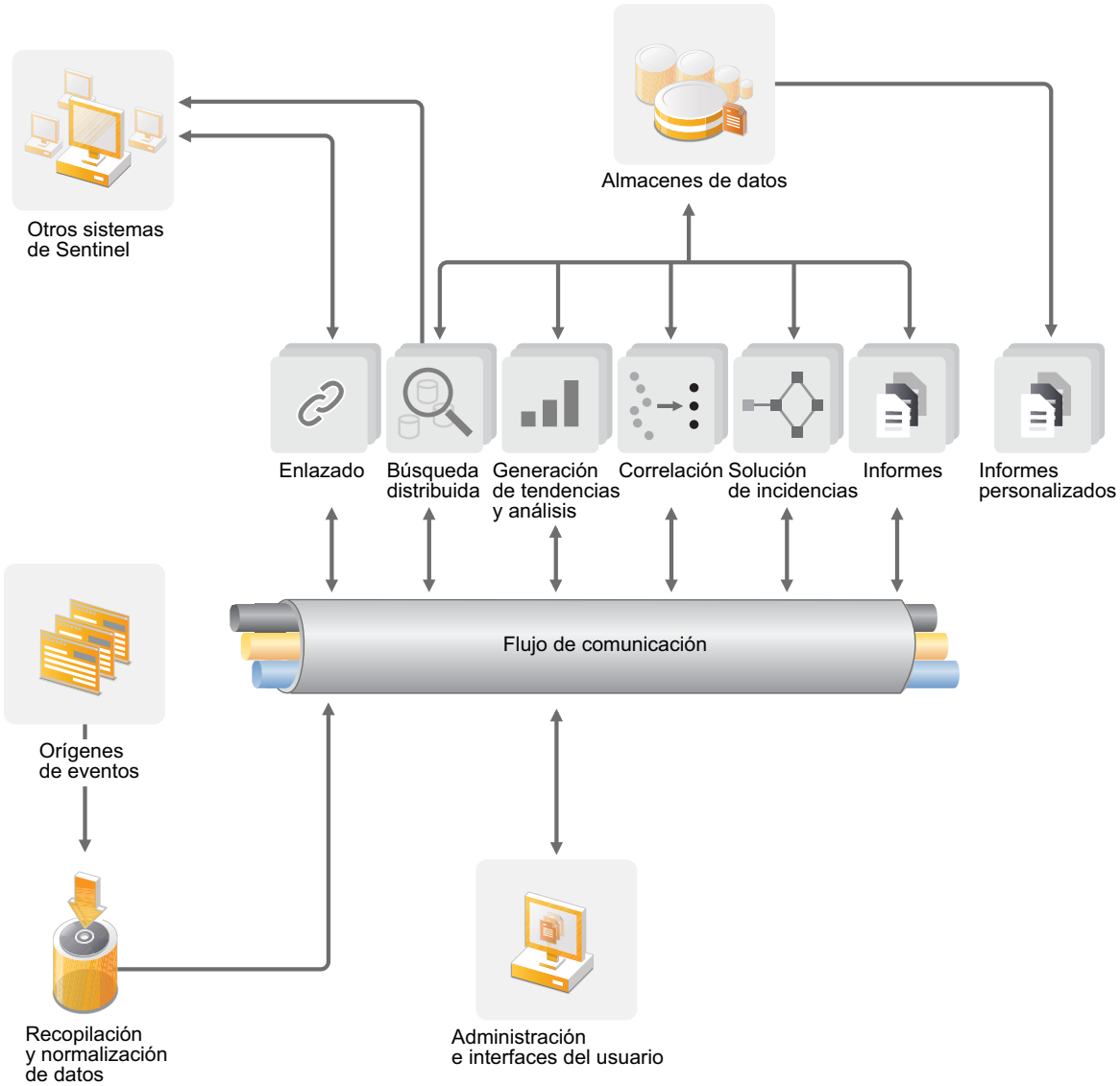
- Llenando el vacío de conocimiento entre lo que debería ocurrir y lo que está ocurriendo realmente en su entorno conectado.
- Demostrando a los auditores y reguladores que su organización documente, supervise e informe sobre los controles de seguridad.
- Ofreciendo programas de supervisión e informe de cumplimiento genéricos.
- Obteniendo la visibilidad y control requeridos para evaluar continuamente el éxito de los programas de cumplimiento y seguridad de su organización.

Sentinel automatiza la recogida de registros, análisis y los procesos de generación de informes para asegurar que los controles TI son efectivos para apoyar los requisitos de detección de amenazas y auditoría. Sentinel proporciona funciones de supervisión automática de los eventos de seguridad, los eventos de conformidad y de los controles de TI, permitiendo tomar medidas inmediatas si se produce una vulneración de la seguridad o un evento no conforme. Sentinel también le permite reunir con facilidad información resumida sobre su entorno para que pueda comunicar su postura general en materia de seguridad a los principales interesados.

2 Cómo funciona Sentinel

Sentinel gestiona de forma continua la información de seguridad y los eventos en todo el entorno de TI para ofrecer una solución de supervisión completa. La siguiente figura muestra cómo funciona Sentinel.

Figura 2-1 *Cómo funciona Sentinel*



Sentinel trabaja del siguiente modo:

- Reuniendo registros, eventos e información de seguridad de todas las fuentes de eventos diferentes en su entorno TI.
- Normalizando los registros recogidos, eventos e información de seguridad en un formato común.
- Añadiendo la información normalizada en un bus de mensaje que pueda mover miles de paquetes de mensajes por segundo.
- Comunicando todos los componentes de Sentinel mediante el bus de mensaje para su escalabilidad.

En este momento, los diferentes componentes de Sentinel acceden al bus de mensajes y Sentinel hace lo siguiente:

- Almacena eventos en un almacén de datos basado en archivos con directivas de retención de datos personalizables.
- Ofrece la capacidad de vincular jerárquicamente múltiples sistemas Sentinel, incluyendo Sentinel Log Manager, Sentinel y Sentinel Rapid Deployment.
- Le permite buscar eventos no solo en su servidor local de Sentinel, sino también en otros servidores de Sentinel distribuidos en el mundo.
- Realiza un análisis estático que le permite definir una línea de base y luego lo compara con lo que está ocurriendo para determinar si hay problemas no detectados.
- Correlaciona un conjunto de eventos similares o comparables en un período dado para determinar un patrón.
- Organiza eventos de incidentes para una gestión de la respuesta y seguimiento eficiente.
- Informa de las capacidades basadas en eventos en tiempo real e históricos.

Las siguientes secciones describen los componentes de Sentinel en detalle.

2.1 Orígenes de eventos

Sentinel reúne información de seguridad y eventos de muchos orígenes diferentes en su entorno TI. Estos orígenes se llaman orígenes de eventos. Los orígenes de eventos pueden ser diferentes elementos en su red.

Los siguientes gráficos muestran algunos de los orígenes de eventos diferentes de los que Sentinel puede obtener información:

Perímetro de seguridad: Dispositivos y software utilizados para crear un parámetro de seguridad para su entorno.

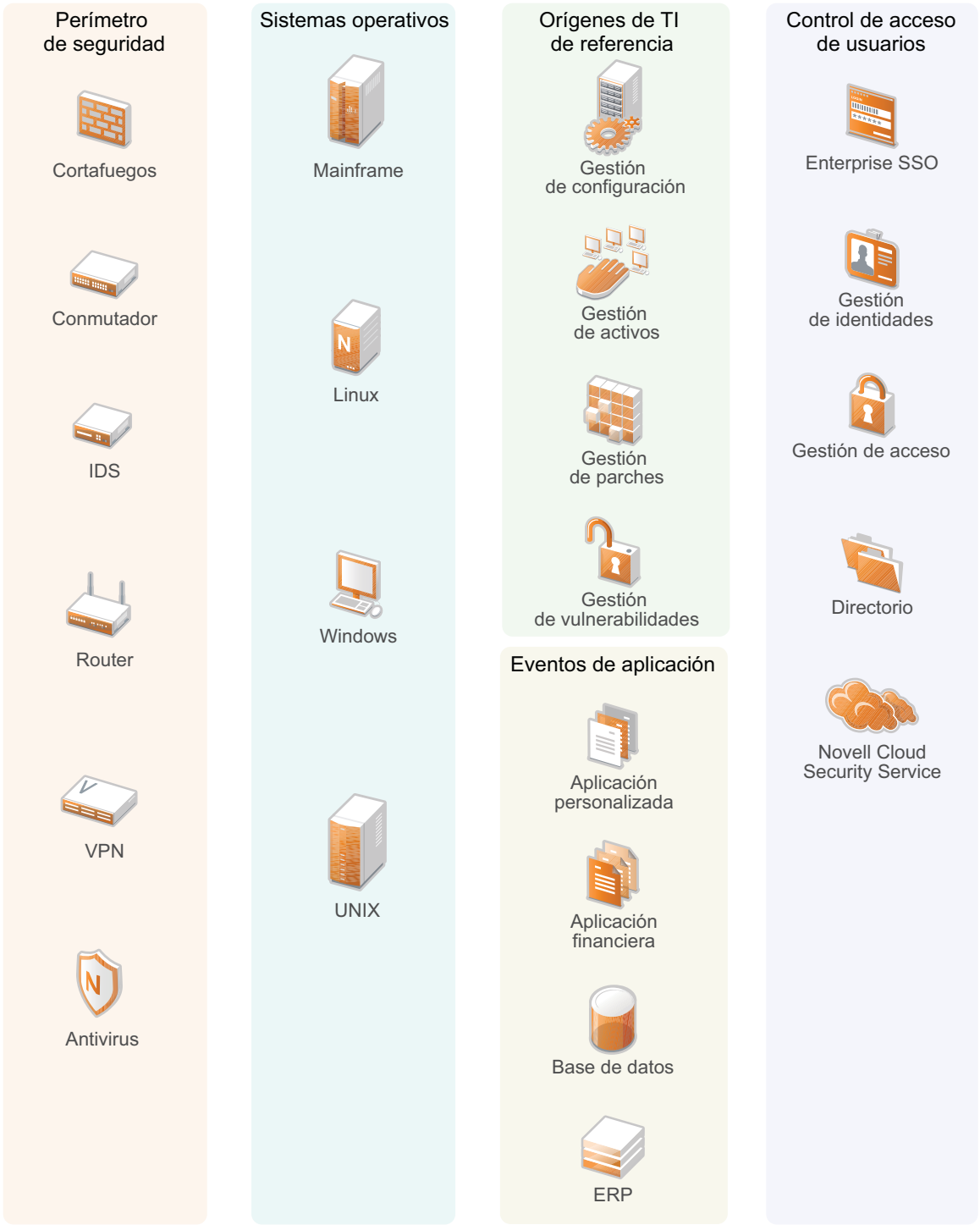
Sistemas operativos: Eventos de los diferentes sistemas operativos que operan en la red.

Orígenes de TI referenciales: El software utilizado para mantener y seguir activos, revisiones, configuración y vulnerabilidad.

Eventos de la aplicación: Los eventos generados de las aplicaciones instaladas en la red.

Control de acceso de usuarios: Los eventos generados de las aplicaciones o dispositivos que permiten a los usuarios acceder a los recursos de la compañía.

Figura 2-2 *Orígenes de eventos*



2.2 Evento de Sentinel

Sentinel recibe información de los dispositivos, normaliza esta información en una estructura denominada evento, clasifica el evento y lo envía para ser procesado. Al añadir la información de categoría (taxonomía) a los eventos, estos pueden compararse más fácilmente entre los sistemas que

notifican los eventos de manera diferente. Por ejemplo, fallos de autenticación. Los eventos se procesan mediante la visualización en tiempo real, motor de correlación, consolas y servidor backend.

Un evento está formado por más de 200 campos. Los campos de evento son de diferentes tipos y sirven para diferentes fines. Existen algunos campos predefinidos como gravedad, importancia, IP de destino y puerto de destino. Existen dos conjuntos de campos configurables: campos reservados para el uso interno de Sentinel para permitir la expansión futura y campos del cliente para extensiones de clientes.

Los campos pueden determinarse de nuevo renombrándolos. El origen de un campo puede ser externo, lo que significa que es definido explícitamente por el dispositivo o el recopilador correspondiente, o referencial. El valor de un campo referencial se calcula como una función de uno o más campos utilizando el servicio de asignación. Por ejemplo, puede definirse un campo para que sea el código de generación para la asignación que contiene el activo mencionado como la IP de destino de un evento. Por ejemplo, el servicio de asignación puede calcular un campo utilizando una asignación definida por el cliente mediante una IP de destino desde el evento.

- Sección 2.2.1, “Servicio de asignación”, en la página 15
- Sección 2.2.2, “Asignaciones de emisión continua”, en la página 16
- Sección 2.2.3, “Detección de explotaciones (Servicio de asignación)”, en la página 16

2.2.1 Servicio de asignación

El servicio de asignación permite un mecanismo sofisticado para propagar los datos de relevancia empresarial en el sistema. Estos datos pueden enriquecer los eventos con información de referencia que proporcionará el contexto que permita a los analistas tomar mejores decisiones, redactar informes más útiles y crear reglas de correlación bien fundadas.

Puede enriquecer los datos de eventos utilizando asignaciones para añadir información adicional como el host y los datos de identidad a los eventos entrantes de los dispositivos de origen. Esta información adicional puede utilizarse para fines de correlación y generación de informes avanzados. El sistema admite varias asignaciones incorporadas además de asignaciones definidas por el usuario personalizadas.

Las asignaciones definidas en Sentinel se almacenan de dos formas diferentes:

- Las asignaciones incorporadas se almacenan en la base de datos, se actualizan utilizando APIs en código del recopilador y se exportan automáticamente al servicio de asignación.
- Las asignaciones personalizadas se almacenan en archivos CSV y se pueden actualizar en el sistema de archivos o a través de la interfaz del usuario de Configuración de los datos de la asignación, y luego los carga el Servicio de asignación.

En ambos casos, los archivos CSV se guardan en el servidor Sentinel central, pero los cambios en las asignaciones se distribuyen a cada gestor de recopiladores y se aplican a nivel local. Este procesamiento distribuido garantiza que la actividad de asignación no sobrecargue el servidor principal.

2.2.2 Asignaciones de emisión continua

El servicio de asignación emplea un modelo de actualización dinámico y reproduce las asignaciones de un punto a otro, evitando la creación de grandes asignaciones estáticas en la memoria dinámica. El valor de esta función de emisión es particularmente importante en un sistema en tiempo real esencial como Sentinel donde debe haber un movimiento seguro, predictivo y ágil de independencia de datos de alguna carga transitoria en el sistema.

2.2.3 Detección de explotaciones (Servicio de asignación)

Sentinel ofrece la capacidad de contrastar las firmas de datos de eventos con los datos del escáner de vulnerabilidad. Los usuarios son notificados automática e inmediatamente cuando un ataque intenta explotar un sistema vulnerable. Esto se realiza mediante:

- Datos del asesor
- Detección de intrusiones
- Exploración de vulnerabilidades
- Cortafuegos

El asesor proporciona una referencia cruzada entre firmas de datos de eventos y datos del escáner de vulnerabilidad. Los datos del asesor contienen información sobre vulnerabilidades y amenazas así como una normalización de las firmas de eventos y los módulos auxiliares (plug-in) de vulnerabilidad. Para más información sobre el asesor, visite "Cómo configurar el asesor" en la *Guía de administración de NetIQ Sentinel 7.0.1* .

2.3 Conectores

Los conectores ofrecen conexiones desde los orígenes de eventos al sistema Sentinel. Utilizando protocolos estándar de la industria para obtener los eventos, como por ejemplo syslog, JDBC para leer tablas de la base de datos, WMI para leer los registros de eventos de Windows, etc., los conectores proporcionan:

- Transporte de datos de eventos en bruto desde los orígenes de eventos al recopilador.
- Filtrado específico de conexión.
- Gestión de errores de conexión.

2.4 Recopiladores

Los recopiladores normalizan y recogen la información de los conectores. Los recopiladores están escritos en Javascript y definen la lógica para:

- Recibir datos en bruto de los conectores.
- Analizar y normalizar los datos.
- Aplicar la lógica repetible a los datos.
- Traducir los datos específicos de dispositivos a los datos específicos de Sentinel.
- Dar formato a los eventos.
- Pasar los datos normalizados, analizados y formateados al gestor de recopiladores.

2.5 Gestor de recopiladores

El gestor de recopiladores gestiona la recopilación de datos, supervisa los mensajes de estado del sistema y realiza un filtrado de eventos según sea necesario. Las principales funciones del gestor de recopiladores son:

- Transformar eventos..
- Añadir relevancia empresarial a los eventos a través del servicio de asignación.
- Realizar el filtrado global de los eventos.
- Enrutar eventos.
- Determinar los datos de tiempo real, vulnerabilidad, activos o de tiempo no real.
- Enviar mensajes de estado al servidor de Sentinel.

2.6 Bus de comunicación

La arquitectura del bus de comunicación se crea utilizando la arquitectura orientada al servicio (SOA) basada en estándares que combina las ventajas del procesamiento en la memoria y la computación distribuida. El bus de comunicación se llama iSCALE y es un bus de mensajes especializado capaz de gestionar grandes volúmenes de datos.

- Sección 2.6.1, “Bus de mensajes”, en la página 17
- Sección 2.6.2, “Canales”, en la página 18

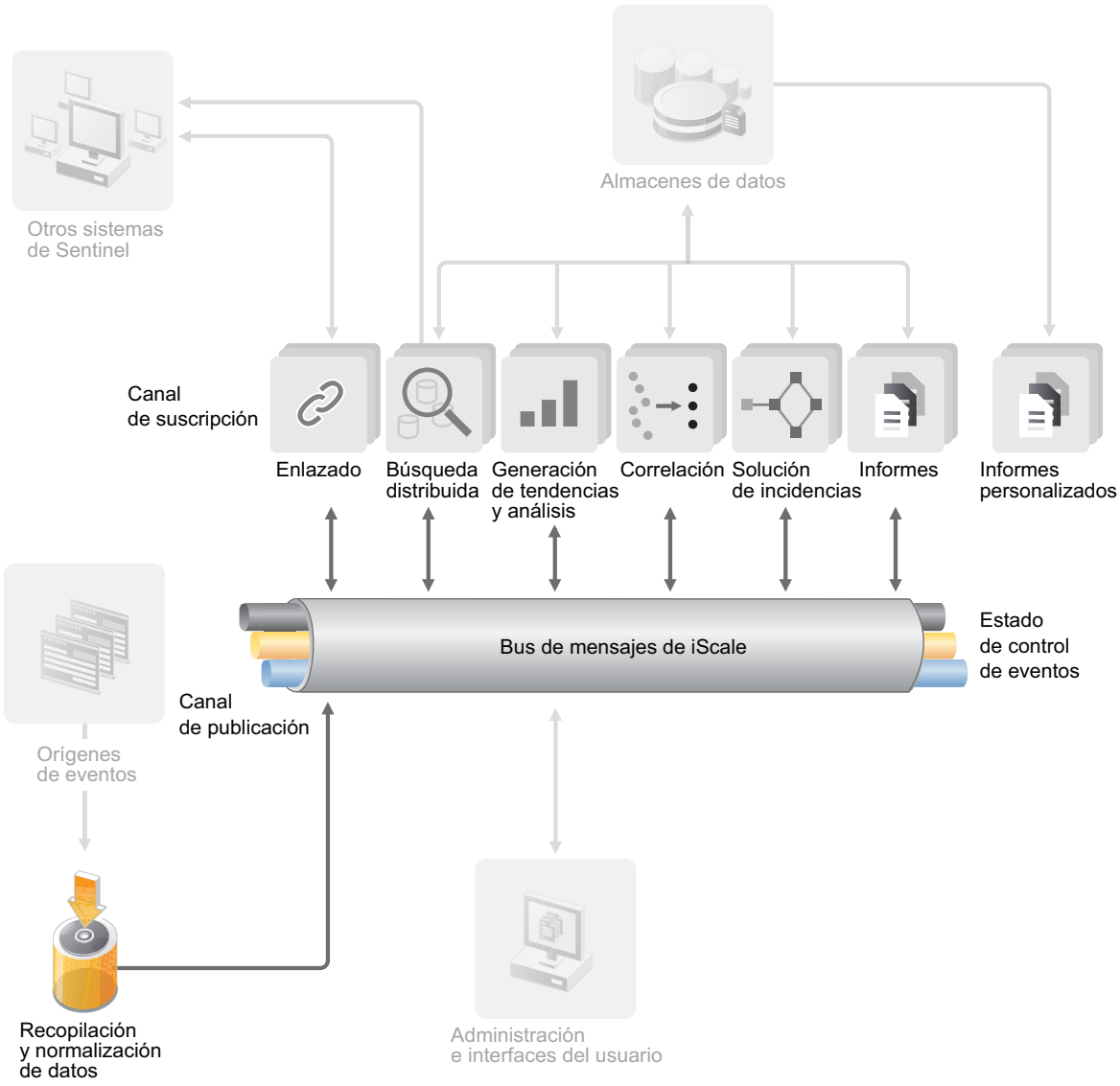
2.6.1 Bus de mensajes

El bus de mensajes de iSCALE permite la ampliación independiente de componentes individuales, además de una integración basada en estándares con aplicaciones externas. El factor clave para la capacidad de ampliación es que, a diferencia de otro software distribuido, no se comunican dos componentes de pares entre ellos directamente. Todos los componentes se comunican mediante el bus de mensajes, que es capaz de mover miles de paquetes de mensajes por segundo.

Mediante el potenciamiento de las funciones únicas del bus de mensajes, el canal de comunicación de alto rendimiento puede maximizar y sostener una alta velocidad de rendimiento de datos mediante los componentes independientes del sistema. Los eventos se comprimen y se cifran por cable para una entrega segura y eficiente desde el borde de la red o puntos de recopilación al eje del sistema, donde se realiza el análisis en tiempo real.

El bus de mensajes iSCALE utiliza una gran variedad de servicios en cola que mejoran la fiabilidad de la comunicación por encima de los aspectos de seguridad y rendimiento de la plataforma. Mediante el uso de una gran variedad de colas transitorias y duraderas, el sistema ofrece una excelente fiabilidad y tolerancia a fallos. Por ejemplo, los mensajes importantes en tránsito se guardan (en colas) en caso de que se produzca un fallo en la vía de comunicación. El mensaje en cola se entrega al destino después de que el sistema se recupere del estado de fallo.

Figura 2-3 *Bus de mensajes iSCALE*



2.6.2 Canales

La plataforma iSCALE utiliza un modelo basado en datos o eventos que permite la ampliación independiente de componentes en todo el sistema en función de la cantidad de trabajo. Esto ofrece un modelo de despliegue flexible porque el entorno de cada cliente varía: un sitio puede tener un gran número de dispositivos con bajos volúmenes de eventos, otro sitio puede tener menos dispositivos con volúmenes de eventos muy altos. Las densidades del evento (es decir, la agregación de eventos y el patrón de multiplexado de eventos por cable desde los puntos de recopilación) son diferentes en estos casos y el bus de mensajes permite la escalada consistente de cargas de trabajo dispares.

iSCALE se aprovecha de un entorno independiente y con múltiples canales, que elimina virtualmente la disputa y fomenta el procesamiento paralelo de eventos. Estos canales y subcanales no sólo funcionan para el transporte de datos de eventos sino que también ofrecen un control del proceso de granulado fino para poder realizar una ampliación y un balance de la carga del sistema

bajo condiciones de carga variable. Mediante el uso de canales de servicio independiente, como canales de control y canales de estado, además del canal de eventos principales, se permite una ampliación sofisticada y rentable de la arquitectura basada en eventos.

2.7 Almacenamiento de datos de Sentinel

Sentinel ofrece múltiples opciones para almacenar los datos recopilados. Por defecto, Sentinel recibe dos cadenas de datos independientes pero similares desde los gestores de recopiladores: los datos del evento y los datos en bruto. Estos datos se almacenan en el sistema de archivos local del servidor de Sentinel.

Puede configurar Sentinel para almacenar los datos en una localización de almacenamiento conectada. También puede configurar Sentinel para almacenar los datos de eventos en una base de datos externa utilizando políticas de sincronización de datos. Para obtener más información, consulte "Configuring Data Storage" (Configuración de almacenamiento de datos) en la *NetIQ Sentinel 7.0.1 Administration Guide* (Guía de administración de NetIQ Sentinel 7.0.1).

2.8 Filtros

Los filtros en Sentinel le permiten personalizar la búsqueda de eventos y prevenir la sobrecarga de datos. Esta característica ofrece un compilador de filtros que ayuda a crear consultas de búsqueda que van de fáciles a complejas. Puede guardar una consulta de búsqueda como filtro y reutilizarla como se requiera, de modo que pueda realizar una búsqueda seleccionando el filtro, en lugar de especificar la consulta manualmente cada vez.

Puede reutilizar filtros mientras utiliza o configura características de Sentinel, como:

- Creación de consolas de Inteligencia de seguridad.

  Para más información, consulte "Creating a Dashboard" (Cómo crear consolas) en la *NetIQ Sentinel 7.0.1 User Guide (Guía del usuario de NetIQ Sentinel 7.0.1)*.

- Ver eventos en tiempo real en Active Views.

  Para más información, consulte "Viewing Events" (Cómo visualizar eventos) en la *NetIQ Sentinel 7.0.1 User Guide (Guía del usuario de NetIQ Sentinel 7.0.1)*.

- Configurar una directiva de retención de datos.

  Para más información, consulte "Configuring Data Retention Policies" (Cómo configurar directivas de retención de datos) en la *NetIQ Sentinel 7.0.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.0.1)*.

- Configurar la sincronización de datos.

  Para más información, consulte "Configuring Data Synchronization" (Cómo configurar la sincronización de datos) en la *NetIQ Sentinel 7.0.1 Administration Guide (Guía de administración de NetIQ Sentinel 7.0.1*.

- Probar una regla de correlación.

  Para más información, consulte "Correlating Event Data" (Datos de eventos de correlación) en la *NetIQ Sentinel 7.0.1 User Guide (Guía del usuario de NetIQ Sentinel 7.0.1)*.

Sentinel ofrece una lista de filtros por defecto. También puede crear sus propios filtros. Para más información, consulte "Configuring Filters" (Cómo configurar filtros) en la *NetIQ Sentinel 7.0.1 User Guide (Guía del usuario de NetIQ Sentinel 7.0.1)*.

2.9 Correlación

Un solo evento puede parecer insignificante, pero en combinación con otros eventos, puede advertir sobre un problema potencial. Sentinel le ayuda a establecer correlaciones entre estos eventos al usar las reglas que crea e implementa en el motor de correlación, y al tomar las medidas adecuadas para paliar los problemas.

La correlación añade inteligencia a la gestión de eventos de seguridad mediante la automatización del análisis de los flujos de eventos entrantes para buscar patrones de interés. Además, la correlación permite definir reglas que identifican las amenazas importantes y los patrones complejos de ataque con el fin de asignar una prioridad a los eventos e iniciar tareas eficientes de gestión y respuesta para las incidencias. Para más información, consulte "Correlating Event Data" (Datos de eventos de correlación) en la *NetIQ Sentinel 7.0.1 User Guide (Guía del usuario de NetIQ Sentinel 7.0.1)*.

2.10 Inteligencia de seguridad

La función de correlación de Sentinel proporciona la capacidad de conocer patrones de actividad, ya sea por motivos de seguridad, conformidad o de otro tipo. La función de Inteligencia de seguridad busca actividad fuera de lo normal, que puede ser de tipo malicioso, pero que no coincide con ningún patrón conocido.

La característica de Inteligencia de seguridad en Sentinel se centra en el análisis estadístico de los datos de series temporales para permitir a los analistas identificar y analizar las desviaciones (anomalías) mediante un motor estadístico automatizado o mediante la representación visual de los datos estadísticos para la interpretación manual. Para más información, consulte "Analyzing Trends in Data" (Cómo analizar tendencias en datos) en la *NetIQ Sentinel 7.0.1 User Guide (Guía del usuario de NetIQ Sentinel 7.0.1)*.

2.11 iTrac

Los flujos de trabajo de iTrac están diseñados para ofrecer una solución sencilla y flexible para automatizar y seguir los procesos de respuesta a incidentes de una empresa. iTrac aprovecha el sistema de incidentes interno de Sentinel para seguir la seguridad o problemas de sistemas de la identificación (mediante las reglas de correlación o identificación manual) a la resolución.

Los flujos de trabajo pueden crearse utilizando pasos manuales o automatizados. Las características avanzadas como ramificación, escalada basada en el tiempo y variables locales son compatibles. La integración con guiones externos y plug-ins permite la interacción flexible con sistemas de terceros. La generación de informes completa permite a los administradores entender y afinar los procesos de respuesta a incidentes. Para más información, consulte "Configuring iTRAC Workflows" (Cómo configurar los flujos de trabajo iTRAC) en la *NetIQ Sentinel 7.0.1 User Guide (Guía del usuario de NetIQ Sentinel 7.0.1)*.

2.12 Informes

Sentinel ofrece la capacidad para ejecutar informes sobre los datos reunidos. Sentinel está pre-empaquetado con una variedad de informes personalizables, alguno de los cuales son generales y otros específicos de dispositivos (por ejemplo, SUSE Linux). Algunos de informes son flexibles para permitir a los usuarios especificar las columnas para mostrarse en los resultados.

Los usuarios pueden ejecutar, programar o enviar por correo electrónico informes en PDF. También pueden ejecutar informes como búsquedas y luego interactuar con los resultados como si fueran una búsqueda, como refinar la búsqueda o realizar una acción basada en los resultados. También puede ejecutar informes en los servidores Sentinel que se distribuyen en diferentes localizaciones geográficas. Para más información, consulte "Reporting" (Informe) en la *NetIQ Sentinel 7.0.1 User Guide (Guía de usuario de NetIQ Sentinel 7.0.1)*.

2.13 Análisis de eventos

Sentinel proporciona un potente conjunto de herramientas que le ayudan a buscar y analizar con facilidad datos de eventos fundamentales. El sistema se ajusta y optimiza para obtener una máxima eficiencia en cualquier tipo de análisis en particular, y se proporcionan métodos para hacer fácilmente la transición de un tipo de análisis a otro de una forma transparente.

La investigación de eventos en Sentinel a menudo comienza con las Vistas activas casi en tiempo real. Si bien se dispone de herramientas más avanzadas, Vistas activas muestra los flujos de eventos filtrados junto con diagramas de resumen que pueden servir para un análisis sencillo y somero de las tendencias de los eventos, los datos de eventos y para la identificación de eventos específicos. Con el tiempo, se construyen filtros mejorados para clases de datos específicos, como por ejemplo resultados de correlación. Puede usar Vistas activas como consola para mostrar una posición operativa y de seguridad general.

Luego puede usar la búsqueda interactiva para realizar un análisis más detallado de los eventos. Esto le permite buscar fácil y rápidamente datos relacionados con una consulta específica, como la actividad de un usuario en particular o en un sistema específico. Al hacer clic en los datos del evento o usar el panel de mejora de la izquierda, podrá enfocarse en eventos de interés específico.

Al analizar cientos de eventos, las funciones de generación de eventos de Sentinel proporcionan un control personalizado de la disposición de los eventos y pueden mostrar un mayor volumen de datos. Sentinel facilita esta transición aún más al permitirle transferir búsquedas interactivas incorporadas a la interfaz de búsqueda a una plantilla de generación de informe, que permite crear de manera inmediata un informe que muestra los mismos datos pero en un formato más adecuado para un mayor número de eventos.

Sentinel incluye muchas plantillas para este fin. Algunas plantillas están mejoradas para mostrar un tipo particular de información, como datos de autenticación o creación de usuarios, y otras plantillas son de uso general y permiten personalizar grupos y columnas en el informe de manera interactiva.

Con el tiempo, desarrollará filtros de uso común e informes que facilitan el flujo de trabajo. Sentinel admite plenamente el almacenamiento de esta información y su distribución a personas de su organización. Para obtener más información, consulte la *Guía del usuario de NetIQ Sentinel 7.0.1*.