# Los datos de registro de seguridad pueden ayudar a evitar un ciberataque, si se encuentran en la plataforma correcta

El humilde registro de seguridad, no tan llamativo como las herramientas de seguridad, como la administración de eventos e información de seguridad (SIEM) y la detección y respuesta extendidas (XDR), necesita ser eliminado y puesto en práctica por más equipos de seguridad. De hecho, la calidad de los datos de registro puede determinar la ciberresiliencia de una organización.

Gracias a un acceso más fácil y rápido a los datos, los registros de seguridad, los datos sin procesar que hacen que los productos digitales llamativos hagan su magia, pueden ser la clave para evitar un ciberataque, responder lo antes posible a una violación cuando los tiempos de interrupción se reducen a solo 48 minutos y comprender los detalles críticos de los incidentes de seguridad después de que ocurren.

## Cómo los registros de seguridad pueden reforzar la resistencia

Una solución de análisis de registros puede monitorear continuamente los registros de seguridad para aumentar la conciencia de los incidentes de seguridad, ya sea que se trate de acceso no autorizado, una violación de las políticas de seguridad, un cambio en los datos o las configuraciones del sistema sin los permisos adecuados, o un ataque directo. Si se marca un indicador de compromiso (IoC), las soluciones de análisis de registros pueden actuar como un sistema de advertencia temprana, lo que brinda la oportunidad de detener el avance de un atacante. Las capacidades de detección también se pueden utilizar para probar escenarios e hipótesis de seguridad y realizar una búsqueda proactiva de amenazas.

> *“Esta infiltración más rápida permite que las organizaciones tengan aún menos tiempo para responder, lo que hace que las defensas automatizadas sean cruciales para igualar, y superar, la velocidad de los adversarios”. Irene Fuentes McDonnell, investigadora de amenazas cibernéticas en ReliaQuest*

*Forbes.com*

Una vez que haya identificado y corregido un incidente de seguridad, es vital rastrear el evento hasta su inicio. Los registros de seguridad se pueden usar para identificar a la persona o el dispositivo que se infiltró en el sistema, ver cómo ingresaron, aprender exactamente qué hicieron y cuándo, y determinar si la amenaza está en curso. Esta tarea forense es una parte fundamental de la recuperación después del evento. Sin él, su equipo de TI no sabrá qué sistemas son vulnerables o cómo solucionarlos.

## ¿La ventaja de la velocidad? Visibilidad

Los registros de seguridad rápidos son importantes, mucho. Cuando los hackers obtienen acceso a una red, pueden permanecer durante días o incluso semanas antes de que las personas o la tecnología detecten su presencia. Mientras acechan sin ser detectados, los atacantes recopilan credenciales de administrador y se preparan para exfiltrar datos o activar ransomware. Tomar medidas oportunas depende de tener visibilidad casi en tiempo real, y eso requiere registros de seguridad que se activen y usen correctamente.

## 1. Elija una solución de análisis de registros avanzada.

En un solo día, los servidores, la red y los dispositivos del usuario final pueden generar cientos de miles, incluso millones, de entradas de registros. Un estudio descubrió que la empresa promedio acumulará hasta 4GB de datos de registro todos los días. Esa cantidad de datos acumulados será inútil sin las herramientas para analizarlos correctamente.

Enfóquese en poner las herramientas de análisis adecuadas sobre el inicio de sesión de seguridad en tres áreas principales: la red, los puntos finales y los usuarios finales. Después de recopilar y analizar los registros, una herramienta de organización puede enriquecer los datos que se transmiten a sus cazadores de amenazas para que tengan un conjunto de información seleccionado para comenzar su revisión.

## 2. Registre todo.

La visibilidad no se trata solo de profundidad, sino también de amplitud. No sabe dónde ocurrirá un intento de violación, por lo que tener registros en toda su infraestructura puede ahorrar tiempo en el futuro. También es esencial que su herramienta de registro agregue, correlacione y analice datos en todos estos diversos tipos de datos y fuentes, y permita la integración de datos contextuales.

## 3. Asegure los registros.

No es sorprendente que los registros de seguridad sean de gran interés para los hackers, por lo que es importante mantenerlos bien protegidos. Para proteger los registros de seguridad, puede:

- Cifre o protéjalos con contraseña.
- Haga que los archivos de registro solo se adjunten, lo que significa que un usuario puede agregarlos a los registros, pero no puede alterar ni borrar lo que ya existe, ni usar registros de auditoría inalterables para garantizar la precisión.
- Cree copias de archivos de registro y guárdelos en varios entornos.
- Almacene los archivos de registro en un sistema o servidor separado.
- Ocultar archivos de registro dentro del sistema.
- Use medios de escritura una vez para guardar archivos de registro.

## Las capacidades que necesita para multiplicar el valor de los registros

Los registros de seguridad y los sistemas utilizados para analizarlos, como Splunk y Elastic, necesitan estas capacidades:

- Procesamiento en tiempo real con rendimiento de búsqueda y consulta reproducible, sin importar el tamaño del registro. Esto requiere un alto rendimiento, una baja latencia y un rendimiento consistente ajustado a cualquier escenario o escala.
- Reducción de datos incorporada y escalabilidad según demanda para registrar y retener más datos durante más tiempo, para el análisis más rico posible.
- Escalabilidad sencilla para cargas de trabajo múltiples, consultas simultáneas y patrones de datos variables para adaptarse al análisis rápido de conjuntos de datos multipetabyte.
- Múltiples registros que correlacionan datos entre redes, puntos finales y usuarios finales.
- Simplicidad de administración que le permite crear nuevas consultas con facilidad y reducir la complejidad.

Lograr este nivel de rendimiento requiere una infraestructura backend que pueda soportarlo. Sin un potente backend de almacenamiento de datos, la realidad es

que incluso las consultas de correlación exitosas pueden ser demasiado lentas para revelar amenazas a tiempo para evitar daños.

Cuando busque esa aguja ingeniosa en el pajar del entorno de seguridad, piense en el almacenamiento de datos increíblemente eficaz como un imán para llevar esa aguja a la cima. Hace que el trabajo de detección y análisis de amenazas sea rápido. Pero si su almacenamiento es lento, su data lake es demasiado inmenso o sus consultas están mal escritas, puede tomar horas o incluso días de investigación identificar un problema o amenaza potencial.

## Cómo Pure Storage y nuestros socios pueden ayudar

FlashBlade® o FlashArray de Pure Storage®están consolidando todos sus archivos de registro e integrándolos sin problemas incluso con las plataformas de análisis de registros más avanzadas, incluidas las soluciones de nuestros socios, Elastic y Splunk. FlashBlade y FlashArray ofrecen un tiempo más rápido para obtener resultados a un costo total de propiedad más bajo.

FlashBlade y FlashArray protegen aún más sus registros de seguridad. Al ejecutar la solución en nuestra función SafeMode™ con Splunk o Elastic log analytics, se asegura de que sus registros no se puedan eliminar. De esa manera, puede recuperarse con confianza después de una violación de seguridad y tendrá la información que necesita para analizar el evento y tomar medidas para evitar que vuelva a suceder.

Independientemente de la cantidad de soluciones de seguridad que implemente, ya sea control de acceso a la red, protección contra la pérdida de datos, firewalls, sistemas de prevención de intrusiones, administración de acceso de identidad, agentes de seguridad de acceso a la nube, antimalware, detección de puntos finales o todo lo anterior, es fundamental tener un plan de acción para detectar y corregir una violación de seguridad cuando ocurra o si ocurre.

