ManageEngine
Log360

Top 5 Alertas Críticas

que necesitas para seguridad IT

Introducción

Analizar los datos de registro e identificar qué eventos de seguridad son motivo de preocupación entre miles de eventos de rutina puede ser un desafío, especialmente si no está seguro de qué eventos seguir.

Mientras los requisitos de seguridad de TI varían para las diferentes empresas, hay algunos eventos clave de seguridad que plantean preocupaciones importantes de seguridad y cumplimiento para todos. Para ayudarte a estar al tanto de seguridad, hemos compilado una lista de cinco eventos críticos que su organización debería tener cuidado.

1. Modificaciones hechas a datos confidenciales

La seguridad de los datos confidenciales es la principal preocupación para los administradores de TI. Esta información incluye datos confidenciales de empleados, clientes y negocios almacenados en archivos y bases de datos. Configurar el proceso de auditoría para alertarlo sobre los accesos y modificaciones hechas a datos en archivos, carpetas y bases de datos garantiza que solo las personas autorizadas estén realizando operaciones. También debe hacer un seguimiento de los cambios realizados en los derechos de acceso a datos, como cambios realizados en las listas de control de acceso (ACL).

Esto certifica que no solo revise periódicamente actividades importantes en sus archivos, carpetas, y bases de datos mediante la programación de informes de auditoría, pero que también recibirá alertas cuando haya un evento que requiere su atención.

2. Apagados y reinicios repetidos del servidor

Los servidores críticos siempre deben estar en funcionamiento para garantizar la continuidad del negocio (COB).

Los hackers a menudo se dirigen a estos servidores en un intento de afectar la productividad de una organización, lo que hace que el seguimiento de los registros de seguridad generados por su servidor sea vital.

Por sí solo, el cierre de un servidor no significa necesariamente que esté siendo atacado. Pero una actividad anómala tal como un servidor que se reinicia cinco veces en media hora es inquietante. Asigne automáticamente un ticket a este tipo de actividad y envíela a un designado administrador del servidor para que puedan analizar rápidamente el evento y resolver el incidente.

3. Fallas de inicio de sesión y bloqueos de cuenta

Usted ya sabe que la actividad de inicio de sesión debe ser rastreada para asegurarse de que se está reuniendo regulaciones de cumplimiento. La auditoría de la actividad de inicio de sesión en tiempo real puede ayudarlo a detectar repeticiones.
Fallas de inicio de sesión que podrían asociarse con un ataque. También puede obtener detalles sobre las cuentas a las que se les niega el acceso al servidor e identifican la causa del bloqueo. Los inicios de sesión con cuenta privilegiada son especialmente importantes para rastreo, ya que estas cuentas son específicamente dirigidas por piratas informáticos.
Es esencial configurar la auditoría tanto para el éxito y los inicios de sesión fallidos para estas cuentas para que pueda analizar los datos de registro con informes y alertas.

4. Cambios en la membresía del grupo de seguridad en Active Directory

Los grupos de seguridad en Active Directory proporcionan a los usuarios acceso a los recursos. Los cambios realizados para grupos de seguridad, ya sea intencional o no, pueden crear una laguna de seguridad potencial. Para asegurar el acceso privilegiado, necesita alertas en tiempo real sobre cambios críticos realizado en su Active Directory, como cambios a grupos privilegiados elevados.
La auditoría de cambio de Active Directory es vital para alinearse con diferentes regulaciones de seguridad de datos y mantener las amenazas internas bajo control.
Las alertas en tiempo real ayudan a evitar amenazas de seguridad, pero debido a las deficiencias de Event Viewer, necesita aprovechar una auditoría especializada solución para lograr esto.

5. Cambios de las reglas de Firewall

Cambios en la regla del firewall

Los Firewalls son una fuente crítica de registro para SIEM, porque tienen el poder de permitir o denegar acceso al tráfico de la red. Al analizar los datos syslog de los firewalls, puede detectar el aumento amenazas en el nivel del perímetro de la red. Mientras puede estar viendo el tráfico que pasa a través de sus firewalls, los cambios en las configuraciones de red a menudo pasan por alto. Su importancia para rastrear las reglas de firewall que se agregan, elimina o modifican, ya que podrían inadvertidamente otorgar permiso a un actor malicioso.

Registro de Auditoría con la solución SIEM

Esto solo es una parte de todas las alertas comunes de eventos que necesita ver para estar en el top de la seguridad de la organización. Usted además necesita alertas para solicitudes de servidores web maliciosos, bloqueo de aplicaciones, y más. Una herramienta de auditoría especializada, como la solución de información de seguridad y administración de eventos (SIEM), puede ayudarlo a hacer todo esto al centralizar los datos de registro de su infraestructura de red. Luego puede alertarlo sobre eventos de seguridad importantes que requieren su atención. Esto garantiza que podrá detectar rápidamente amenazas de seguridad y responderlas rápidamente.

Explore Log360

La completa solución SIEM de ManageEngine, Log360, integra dos herramientas de auditoría de seguridad en una sola consola:

1. **EventLog Analyzer:** Una herramienta de gestión de registros para SIEM.
2. **ADAudit Plus:** Una herramienta de auditoría de cambios de Active Directory en tiempo real.

Ademas de generar reportes de auditoria de seguridad y alertarte sobre eventos de seguridad o interes, Log360 puede puede agilizar el proceso de resolución de incidentes creando automaticamente tickets alertando al administrador asignado.

Aprenda más sobre Log360