ManageEngine
ADAudit Plus

Los 8 IDs de eventos de seguridad de Windows más críticos

Tabla de contenidos

El log de seguridad de Windows

El log de seguridad de Windows, que se encuentra en el Event Viewer (Visor de Eventos), registra acciones críticas de los usuarios, como inicios y cierres de sesión, gestión de cuentas, acceso a objetos, etc.

Microsoft describe al log de seguridad de Windows como "su mejor y última defensa", y con razón. El log de seguridad ayuda a detectar posibles problemas de seguridad, garantiza la responsabilidad de los usuarios y sirve como evidencia en caso de fallos de seguridad.

¿Qué hace que un evento de seguridad de Windows sea crítico?

Entre la multitud de eventos de seguridad de Windows, los pocos que pueden considerarse críticos pueden clasificarse a grandes rasgos en dos grupos:

1. Eventos cuya sola ocurrencia indica actividad maliciosa. Por ejemplo, que una cuenta normal de usuario final se añada inesperadamente a un grupo de seguridad sensible.

2. Eventos cuya aparición sucesiva por encima de una línea de base aceptada indica actividad maliciosa. Por ejemplo, un número anormalmente elevado de inicios de sesión fallidos.

Los ocho IDs de eventos de seguridad de Windows más críticos

Número de serie	Categoría	ID del evento y descripción	Razones para monitorear (no exhaustivas)
(1) & (2)	**Inicio y cierre de sesión**	**4624** (Inicio de sesión exitoso)	• Para detectar actividades internas anormales y posiblemente no autorizadas, como el inicio de sesión desde una cuenta inactiva o restringida, usuarios que inician sesión fuera del horario laboral normal, inicios de sesión simultáneos en muchos recursos, etc. • Para obtener información sobre el comportamiento de los usuarios, como su asistencia, sus horas de trabajo, etc.
		4625 (Inicio de sesión fallido)	• Para detectar posibles ataques de fuerza bruta, diccionario y otros ataques de intento de adivinar la contraseña, que se caracterizan por un pico repentino de inicios de sesión fallidos. • Para llegar a un punto de referencia para la configuración de la política de umbral de bloqueo de cuentas.
(3), (4) y (5)	**Gestión de cuentas**	**4728** (Miembro añadido al grupo global habilitado para seguridad)	• Para garantizar que la pertenencia a los grupos de los usuarios privilegiados, que tienen las "llaves del reino", sea examinada con regularidad. Esto es especialmente cierto para las adiciones de miembros de grupos de seguridad. • Para detectar el abuso de privilegios por parte de usuarios responsables de hacer adiciones no autorizadas. • Para detectar adiciones accidentales.
		4732 (Miembro añadido al grupo local habilitado para seguridad)	
		4756 (Miembro añadido al grupo universal habilitado para seguridad)	

(6)	**Log de eventos**	**1102** (Log borrado) (Alternativamente, el servicio de log de eventos también puede ser desactivado, lo que resulta en que los logs no se registren. Esto lo hace la política de auditoría del sistema, en cuyo caso se registra el evento 4719).	• Para detectar usuarios con intenciones maliciosas, como los responsables de manipular los logs de eventos.
(7)	**Gestión de cuentas**	**4740** (Cuenta de usuario bloqueada)	• Para detectar posibles ataques de fuerza bruta, diccionario y otros ataques de intento de adivinar la contraseña, que se caracterizan por un pico repentino de inicios de sesión fallidos. • Para mitigar el impacto de que los usuarios legítimos se queden bloqueados y no puedan realizar su trabajo.
(8)	**Acceso a objetos**	**4663** (Se ha intentado acceder a un objeto)	• Para detectar intentos no autorizados de acceso a archivos y carpetas.

Protección de Active Directory

En primer lugar, usted debe configurar su política de auditoría para que Windows pueda registrar los eventos relevantes en el log de seguridad. A continuación, usted tiene que agregar y analizar los logs recopilados y, después, convertir los resultados en información práctica, como informes y alertas. El uso de herramientas nativas y scripts PowerShell para completar estas tareas exige experiencia y mucho tiempo. Para hacer el trabajo con rapidez y eficiencia, una herramienta de terceros es realmente indispensable.

Con informes detallados, alertas en tiempo real y visualizaciones gráficas, ADAudit Plus simplifica el monitoreo continuo de inicios y cierres de sesión, cambios en la pertenencia a grupos, autorización de logs de eventos, bloqueos de cuentas, servidores de archivos y mucho más en todo su Active Directory, servidores miembros y estaciones de trabajo.

Nota

Aunque se ha puesto mucho cuidado en la preparación de este documento, no ofrecemos garantía alguna con respecto al mismo, incluida, entre otras, la exactitud de la información que contiene.