Materia:

Fundamentos de telecomunicaciones

SIEM

(Security Information and Events Management)

Profesor:

Ismael Jiménez Sánchez

Alumno:

Ángel Eduardo Hernández Pimentel

03 De diciembre del 2020

La información de seguridad y la gestión de eventos (SIEM) es un enfoque de gestión de seguridad que combina las funciones SIM (gestión de información de seguridad) y SEM (gestión de eventos de seguridad) en un solo sistema de gestión de seguridad. El acrónimo SIEM se pronuncia "sim" con una *s*ilenciosa.

Los principios subyacentes de cada sistema SIEM son agregar datos relevantes de múltiples fuentes, identificar desviaciones de la norma y tomar las medidas apropiadas. Por ejemplo, cuando se detecta un posible problema, un sistema SIEM puede registrar información adicional, generar una alerta e indicar a otros controles de seguridad que detengan el progreso de una actividad.

En el nivel más básico, un sistema SIEM puede estar basado en reglas o emplear un motor de correlación estadística para establecer relaciones entre las entradas del registro de eventos. Los sistemas SIEM avanzados han evolucionado para incluir análisis de comportamiento de usuarios y entidades (UEBA) y orquestación de seguridad, automatización y respuesta (SOAR).

Los sistemas SIEM funcionan mediante la implementación de varios agentes de recopilación de forma jerárquica para recopilar eventos relacionados con la seguridad desde dispositivos, servidores y equipos de red del usuario final, así como equipos de seguridad especializados, como firewalls, antivirus o sistemas de prevención de intrusiones (IPS). Los recopiladores reenvían eventos a una consola de administración centralizada, donde los analistas de seguridad examinan el ruido, conectan los puntos y priorizan los incidentes de seguridad.

Las herramientas SIEM funcionan recopilando datos de eventos y registros creados por sistemas host, aplicaciones y dispositivos de seguridad, como filtros antivirus y firewalls, en toda la infraestructura de una empresa y reuniendo esos datos en una plataforma centralizada. Las herramientas SIEM identifican y ordenan los datos en categorías tales como inicios de sesión exitosos y fallidos, actividad de malware y otras actividades maliciosas probables.