FORTINET
NSE Training Institute

NSE 2 SIEM Scripts—Spanish Version

¡Hola! En esta clase, explicaremos qué es la administración de eventos e información de seguridad o SIEM, y cómo ha evolucionado con el paso del tiempo.

Los sistemas SIEM se empezaron a usar en 2005 y analizan las alertas de seguridad en tiempo real. Llevan a cabo tres funciones principales:

En primer lugar, recopilan y normalizan las alertas y los eventos de registro de la red de una organización y de sus dispositivos de seguridad, servidores, bases de datos, aplicaciones y dispositivos terminales, y los almacenan en una ubicación central y segura. Los sistemas SIEM recopilan información de dispositivos no solo físicos, sino también virtuales, tanto locales como en la nube. Las investigaciones demuestran que conectarse a cada sistema para identificar eventos de registro relevantes era cada vez más difícil. Además, si los registros no eran seguros, no había garantías de que un atacante no hubiera borrado las entradas para ocultar su actividad.

En segundo lugar, llevan a cabo análisis avanzados de los datos, tanto históricos como en tiempo real, para identificar posibles incidentes de seguridad que deban ser examinados por personas. Los incidentes potenciales se clasifican según su riesgo, gravedad e impacto. Con el tiempo, estos análisis de seguridad han pasado de emplear reglas simples de correlación cruzada a monitorear anomalías en el comportamiento del usuario, detectar identificadores de compromiso o IoC, y aplicar modelos complejos de aprendizaje automático.

En tercer lugar, verifican que todos los controles de seguridad dentro de su alcance estén en orden y sean efectivos. Si bien la protección en sí misma debería fijar requerimientos de seguridad y fomentar una inversión adecuada, la realidad es que muchas empresas adquieren un sistema SIEM principalmente para cumplir con las normativas.

Durante las primeras dos décadas del siglo XXI, ha habido un aluvión de nuevos requerimientos, ya sean leyes o estándares de la industria. Algunos ejemplos son:

- el estándar de la industria de tarjetas de pago o PCI

- la Ley Sarbanes-Oxley, de 2002
- la Ley de Portabilidad y Responsabilidad de Seguros Médicos o HIPAA
- el Reglamento General de Protección de Datos <pause> o RGPD, de 2018

Las empresas, los hospitales y otras organizaciones hacen caso omiso de la normativa a su propio riesgo, y su violación puede acarrear sanciones punitivas.

A medida que los ciberataques se volvieron más complejos y subrepticios, fue cada vez más imperiosa la necesidad de información sobre ellos, es decir, sobre sus características y propósitos, y el alcance de la penetración en la red. Otro hecho preocupante era que los equipos de seguridad no detectaban las vulneraciones hasta meses después de ocurridas, y normalmente no lo hacía la seguridad interna, sino agentes externos. La seguridad de TI requería una imagen holística de la actividad de red, y los datos en tiempo real de los sistemas SIEM fueron la solución. En una segunda etapa de su desarrollo, los proveedores de SIEM incorporaron capacidades de detección de amenazas mediante la información integrada sobre amenazas, los análisis históricos y en tiempo real, y el análisis del comportamiento de usuarios y entidades o UEBA. Asimismo, hace poco, el aprendizaje automático pasó a formar parte del conjunto de herramientas SIEM y es especialmente necesario a la hora de analizar *big data*.

Otro obstáculo para que los sistemas SIEM tuvieran una mayor aceptación entre las organizaciones fue el esfuerzo que implicaba su configuración, integración y uso. La tecnología era compleja y difícil de ajustar, no resultaba sencillo identificar ataques y los usuarios requerían conocimientos avanzados para saber qué buscar. Por todas sus capacidades, los sistemas SIEM no eran una tecnología que podía adoptarse sin supervisión posterior. Hubo otros dos hechos que empeoraron aún más la situación. Por un lado, la seguridad de TI no disponía de un número suficiente de profesionales calificados. Por el otro, el enfoque de silos utilizado en los típicos centros de operaciones de red, o NOC, y en los centros de operaciones de seguridad, o SOC, aumentó la complejidad y generó una falta de visibilidad de red. Un entorno compuesto por soluciones puntuales de varios proveedores y con diferentes sistemas operativos, ciclos de aplicación de parches, protocolos y lógicas iba en contra de la

interoperabilidad y la simplicidad. Como resultado, hubo una demanda mayor de recursos de TI, de por sí escasos, una mayor probabilidad de error humano y una menor visibilidad de la seguridad de red. Así, si bien el paso de una plataforma de información a un centro de información sobre amenazas fue un avance importante, los sistemas SIEM tenían limitaciones tanto internas como externas.

La escasez general de personal capacitado constituyó un impulso hacia la automatización y el aprendizaje automático en los dispositivos SIEM posteriores. La inteligencia artificial detecta tendencias y patrones en cargas de datos de gran volumen más rápido que la persona más brillante. Además, se gana tiempo y precisión al configurar el sistema SIEM para responder y remediar de manera automática. Lo últimos avances han integrado los NOC y los SOC, por lo que los sistemas SIEM se han consolidado como el centro neurálgico de todas las operaciones de red y de seguridad. En consecuencia, desde un único panel, la seguridad de TI obtiene una visibilidad de toda la red. Los sistemas SIEM simplifican la implementación y la integración mediante un motor de descubrimiento de recursos y configuración de dispositivos con autoaprendizaje en tiempo real. Esta herramienta establece un inventario de dispositivos de red, aplicaciones, usuarios y servicios empresariales. Luego construye una topología que muestra cómo se interconecta cada objeto y establece así una referencia para el comportamiento normal de la red. De esta manera, y gracias al aprendizaje automático, el comportamiento anormal puede alertar a los analistas sobre un ciberataque, que puede detenerse antes de que se produzca una vulneración.

En un par de décadas, los sistemas SIEM han pasado de ser una plataforma de información a conformar un centro de información sobre amenazas y a convertirse en un centro completamente integrado y automatizado para operaciones de red y de seguridad.

El producto SIEM de Fortinet se llama FortiSIEM™ e incluye todas estas características y otras.

Gracias por su tiempo, y no olvide responder las preguntas a continuación.