Nombre de la Materia:
Fundamentos de Telecomunicaciones Aula

Nombre de la Licenciatura:
Ing. Sistemas Computacionales.

Nombre del Alumno(a):

Pool Ramírez Miguel Ángel.

Nombre de la Tarea:

Gestión de información y eventos de seguridad. (SIEM)

Unidad #3

Nombre de la Unidad: Modulación

Nombre del Profesor(a):

Ing. Ismael Jiménez Sánchez

Fecha: 03/12/20

"SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran"

¿Qué es un sistema SIEM?

SIEM (información de seguridad y gestión de eventos), es una tecnología capaz de detectar rápidamente, responder y neutralizar las amenazas informáticas. Su objetivo principal es el de proporcionar una visión global de la seguridad de la tecnología de la información.

Un sistema SIEM permite tener control absoluto sobre la seguridad informática de la empresa. Al tener información y administración total sobre todos los eventos que suceden segundo a segundo, resulta más fácil detectar tendencias y centrarse en patrones fuera de lo común.

La tecnología SIEM nace de la combinación de las funciones de dos categorías de productos: SEM (gestión de eventos de seguridad) y SIM (gestión de información de seguridad).

- SEM centraliza el almacenamiento y permite un análisis casi en tiempo real de lo que está sucediendo en la gestión de la seguridad, detectando patrones anormales de accesibilidad y dando mayor visibilidad a los sistemas de seguridad.

- Mientas que SIM recopila los datos a largo plazo en un repositorio central para luego analizarlo, proporcionando informes automatizados al personal de seguridad informática.

Ambas funciones permiten que se pueda actuar más rápidamente sobre los ataques, ya que por un lado ofrecen más visibilidad y por otro permiten utilizar los datos para la supervisión y el análisis de la seguridad en tiempo real, avisando de los ataques que se están produciendo, o incluso los que se van a producir.

¿Cuál es la importancia y finalidad de un sistema SIEM?

La importancia de estas soluciones está en la prevención de amenazas no relacionadas con vulnerabilidades del software, tales como malware, o la denegación del servicio (DoS).
Pero no solo las amenazas externas están controladas con la tecnología SIEM, sino que también nos garantiza que podremos controlar las amenazas cibernéticas más difíciles de detectar: los ataques internos.

La finalidad de las herramientas SIEM es detectar y prevenir amenazas. Están diseñadas para prevenir ataques antes de que se realicen y lo hacen gracias a la información que se recopila en el sistema central.

¿Cómo funciona la tecnología SIEM?

Las herramientas SIEM proporcionan una alta velocidad a la hora de realizar la investigación de las alertas. La visibilidad y la capacidad de detectar amenazas hace que los analistas de seguridad sepan cual es el mejor modo de actuar.

Además, monitoriza las actividades que se llevan a cabo dentro de la red y recoge la información necesaria, sobre la actividad de los usuarios y los dispositivos empleados para cada interacción. Gracias a esto ayuda a identificar signos de comportamiento malicioso.

Beneficios de los sistemas SIEM que tal vez desconoces.

La tecnología SIEM tiene un mecanismo para desplegar rápidamente una infraestructura de recopilación de registros. Esto ayuda a la verificación del cumplimiento de ciertas normas de seguridad que las compañías están obligadas a cumplir ante una auditoría.

Puede incluso detectar una actividad, asociada con un ataque, al correlacionar la actividad de los procesos y las conexiones de redes de las máquinas que están protegidas por el SIEM.

- Bloquea rápidamente las amenazas a las redes, evitando filtraciones de datos y fallo de procesos y sistemas.
- Permite buscar amenazas en registros archivados. Algunos de los ataques más difíciles de detectar son los que permanecen inactivos durante largos periodos de tiempo dentro de la red interna.

¿Cuáles son los mejores fabricantes de sistemas SIEM?

QRadar La solución fabricada por IBM.

Arc Sight La solución fabricada por HP.

Referencias.

- Unknown. (2015). ¿Qué es un sistema SIEM?. 2020, de SOFECOM Sitio web: https://sofecom.com/que-es-un-siem/