Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

Tarea: Investigación SIEM (información de seguridad y gestión de eventos)

Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

SIEM (información de seguridad y gestión de eventos)

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.