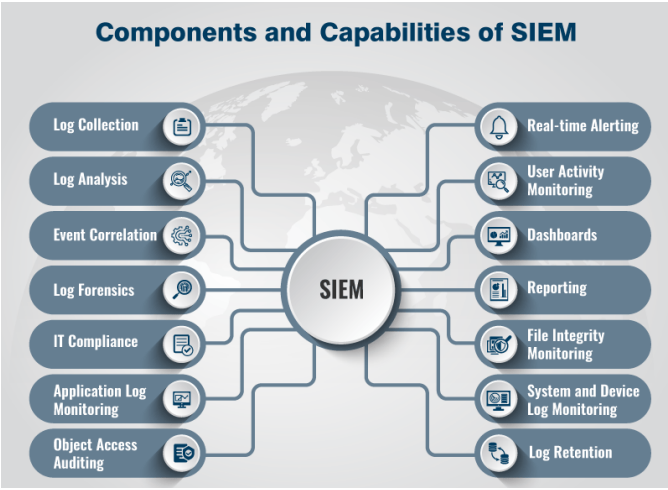
INSTITUTO TECNOLÓGICO DE CANCÚN

ESPECTRO ELECTROMAGNETICO

MIGUEL ÁNGEL OY CASTRO

DICIEMBRE 3 2020

PROFESOR: ISMAEL JIMÉNEZ SÁNCHEZ



FUNDAMENTOS DE TELECOMUNICACIONES

Gestión de información y eventos de seguridad

Un sistema de gestión de información y eventos de seguridad (en inglés, security information and event management, SIEM) es un sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad. De esta forma, permite un análisis de la situación en múltiples ubicaciones desde un punto de vista unificado que facilita la detección de tendencias y patrones no habituales. La mayoría de los sistemas SIEM funcionan desplegando múltiples agentes de recopilación que recopilan eventos relacionados con la seguridad.

Un sistema SIEM combina funciones de un sistema de gestión de información de seguridad (security information management, SIM), encargado del almacenamiento a largo plazo, el análisis y la comunicación de los datos de seguridad, y un sistema de gestión de eventos de seguridad (security event management, SEM), encargado del monitoreo en tiempo real, correlación de eventos, notificaciones y vistas de la consola de la información de seguridad

Los regímenes de seguimiento y registro de eventos normalmente pueden cubrir los siguientes aspectos de las operaciones de red:

- Escaneo de terminales y dispositivos
- Infraestructura y hardware de red
- Gestión de parches de aplicaciones y sistemas operativos
- Implementaciones antivirus para servidores, equipos de escritorio y dispositivos móviles
- Administrar firewalls de red
- Gestión de autenticación
- Sistemas de prevención de intrusiones (IPS)
- Filtros de contenido web y proxies web
- Registros anti-spam y anti-phishing para correo electrónico
- Escaneo de vulnerabilidades