Instituto Tecnológico de Cancún.

SIEM e IDS/IPS.

Daniel Pérez Vélez.

Fundamentos de telecomunicaciones.

Ismael Jiménez Sánchez.

Diciembre 2020.

SIEM.

Sus siglas significan “Security Information and Event Management”. Es un sistema que permite visualizar y obtener información de los ataques recibidos y evaluar la seguridad de la red. Mas que nada sirve para detectar amenazas, sin embargo, se necesitan definir los procesos importantes para la seguridad para que funcione de forma autónoma.

Lo que es relevante resaltar es que un SIEM permite actuar antes y después de la amenaza en tiempo real.

IDS.

“Intrusion Detections System”. Es una herramienta que sólo se centra a la detección de instrusos en nuestra red, en contraste, es imposible detener un ataque usando esta herramienta.

Existen 2 tipos de IDS:

HIDS (Host Intrusion Detections System).

Se centraliza en el host de una computadora, ignorando a los demás equipos de la red.

NIDS (Network Instrusion Detection System).

A diferencia del HIDS, NIDS da cobertura a toda una red para detectar actividad malintencionada mediante un análisis del tráfico de red.

IPS.

“Intrusion Prevention System”. Previene de ataques teniendo un acceso controlado a la red en la que usemos el IPS. Se llega a considerar una extensión que complemente el IDS.

Al igual que la herramienta anterior tiene diferentes clases:

NIPS.

Análisis para red.

WIPS.

Análisis para una red inalámbrica.

NBA.

Analiza comportamientos inusuales en la red, como malwares y denegación de servicios.

HIPS.

Análisis de red para un host específico.