ITCANCUN

ALUMNO: LÓPEZ HERNÁNDEZ JAVIER ISAC

PROFESOR: ISMAEL JIMENEZ SANCHEZ

CARRERA: INGENIERÍA EN SISTEMAS COMPUTACIONALES

CURSO: FUNDAMENTOS DE TELECOMUNICACIONES

SIEM, IDS/IPS

SIEM

El software de gestión de eventos y información de seguridad proporciona información e historial de actividades a los de seguridad empresarial. Combina la gestión de eventos de seguridad SEM con la gestion de información de seguridad SIM.
SIEM lo que hace es recopilar y agregar datos de registro generados en toda la infraestructura tecnológica de la organización, desde sistemas y aplicaciones host e incluso dispositivos de red y seguridad como Firewall y filtros antivirus. EL software SIEM tiene dos objetivos principales: El primer objetivo es proporcionar informes sobre incidentes y eventos relacionados con la seguridad, asi como inicios de sesión exitosos y fallidos, actividad de malware y otros tipos de problemas de seguridad. El segundo objetivo es enviar alertas si el análisis muestra que una actividad se ejecuta contra conjuntos de reglas predeterminados e indica un posible problema de seguridad.
Se señalo en un informe que los proveedores están introduciendo aprendizaje automático en el software, asi como análisis estadístico avanzado y otros métodos analíticos en sus productos, mientras que otros están experimentando con inteligencia artificial.

IDS

Intrusion Detection System. Su función es detectar intrusos osea accesos no permitidos en la red, este permite obtener datos, y cunado detecte el tráfico puede identificar por intermedio de anomalías o comportamientos extraños si se trata de algun ataque. El IDS reconoce ataques pasados al igual que comportamientos extraños tomando como ejemplo el escaneo de puertos. Existen dos tipos de IDS: El HIDS que busca datos que los atacantes hayan dejado en un equipo cuando intentan controlarlo. EL otro tipo es el NIDS que es IDS de red, lo que hace es detectar ataques a nivel de toda la red monitoreando a la vez todo el trafico que entra a la red.

IPS

El IPS lo que hace es controlar el acceso de usuarios ilegítimos agregando la posibilidad de bloquear los ataques. Existen varias opciones para implementarlo, Hardware, software o combinación de ambas. Los IPS se clasifican en la forma en la que detectan trafico malicioso. Un ejemplo es basarse en firmas: comparando el tráfico con firmas de ataques conocidos. Tambien basado en políticas, en anomalias asi como la detección estadística de Anormalidades analizando todo el trafico durante un tiempo concreto, Y la detección no Estadística de Anormalidades: donde el Administrador define la línea que va a ser la base para la comparación del tráfico.