INSTITUTO TECNOLOGICO DE CANCÚN

INGENIERIA EN SISTEMAS COMPUTACIONALES

FUNDAMENTOS DE TELECOMUNICACIONES

INVESTIGAR QUÉ ES SIEM y IDS/IPS

Peraza Soberanis Gabriel Alfredo

¿Qué es SIEM?

SIEM, por sus siglas en inglés, Security Information and Event Management, que en español significa, Información de seguridad y gestión de eventos.

Son plataformas completas dedicadas al escaneo activo y pasivo de tus redes para detectar eventos, actividades sospechosas, y predecir los ataques antes de que tengan lugar. Así, evitas ataques informáticos y potencias tu seguridad digital.

Objetivo

Tienen como objetivo detectar preventivamente amenazas potenciales a la empresa y resolverlas lo más rápido y de lo forma más eficaz posible. Para lograrlo, procesan y monitorizan una cantidad enorme de datos tanto de hardware, software como fuentes de seguridad,

El objetivo del Security Information and Event Management es poder responder con rapidez y precisión ante las amenazas.

Sistemas de detección y prevención IDS e IPS: ¿Para qué sirven?

Sirven como herramientas que se usan para monitorizar y detectar intrusiones en los equipos o en la red de la empresa son diferentes entre sí.

IDS

IDS *(Intrusion Detection System)* o Sistema de Detección de Intrusiones: es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante. Es un **sistema IDS** es que permite **ver lo que está sucediendo en la red en tiempo real** en base a la información recopilada, reconocer modificaciones en los documentos y automatizar los patrones de búsqueda en los paquetes de datos enviados a través de la red.

IPS

IPS *(Intrusion Prevention System)* o Sistema de Prevención de Intrusiones: es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva. es un software que se utiliza para **proteger a los sistemas de ataques** e intrusiones. Su actuación es preventiva. Estos sistemas llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red, implementando políticas que **se basan en el contenido del tráfico monitorizado**, es decir, el IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones.