INSTITUTO TECNOLÓGICO DE CANCÚN

INGENIERÍA EN
SISTEMAS COMPUTACIONALES

MATERIA:
FUNDAMENTOS DE TELECOMUNICACIONES

TAREA:

INVESTIGAR SOBRE SIEM E IDS/IPS.

NUMERO DE CONTROL Y NOMBRE DEL ALUMNO:
18530369 CRUZ GÓNGORA FERNANDO JÓSE

HORARIO:
LUNES A JUEVES
17:00 PM – 18:00 PM

MAESTRO:
ING. ISMAEL JIMÉNEZ SÁNCHEZ

SIEM

El SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management) es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas. Esto es posible mediante un análisis centralizado de datos de seguridad, obtenidos desde múltiples sistemas, que incluyen aplicaciones antivirus, firewalls y soluciones de prevención de intrusiones.

También trabaja como una inteligencia procesable para que usted pueda gestionar de forma proactiva las potenciales vulnerabilidades, protegiendo a su empresa y a sus clientes de devastadoras filtraciones de datos. Algunas de las soluciones de SIEM disponibles comparten unos puntos en común que son importantes para sus operaciones. Usted querrá contar con la capacidad de:

- Centralizar la vista de potenciales amenazas
- Determinar qué amenazas requieren resolución y cuáles son solamente ruido
- Escalar temas a los analistas de Seguridad apropiados, para que puedan tomar una acción rápida
- Incluir el contexto de los eventos de Seguridad para permitir resoluciones bien informadas
- Documentar, en un registro de auditoría, los eventos detectados y cómo fueron resueltos
- Cumplir con las regulaciones de la industria en un formato de reporte sencillo.

Los IDS corresponde a un **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 y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Ante cualquier actividad sospechosa, emiten una alerta a los administradores del sistema quienes han de tomar las medidas oportunas.

Los IPS corresponde a un Sistema de Prevención de Intrusiones 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.