SIEM e IDS/IPS

Morales Aguilar Miguel Ángel

Docente: Jiménez Sánchez Ismael

Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

SIEM

Un sistema SIEM es un entorno basado en software el cual nos permite analizar, prevenir y localizar posibles amenazas en nuestra red, para que esto sea posible es necesario que todos los datos dentro de nuestro sistema estén estandarizados, es decir, que todos tengan un mismo formato. Para que esto sea posible y un sistema SIEM trabaje con eficiencia debe tener claro todas las necesidades de la empresa y cada una debe ser individual. Estas necesidades deben ser enfocadas en la seguridad. Con esto me refiero a que debe saber que procesos son importantes para la seguridad del sistema y llevarlos acabo de forma jerarquica es decir, que tenga un orden sobre que proceso tiene prioridad sobre otro.

Los resultados pueden ser presentados en una tabla en la que es posible ver y analizar uno a uno los resultados, para que así, si el sistema detecta alguna potencial amenaza este notifique al usuario inmediatamente.

Algunas de las ventajas de este sistema es que tiene respuestas en tiempo real, optimiza los recursos humanos, etc.

Así mismo uno de los usos mas comunes para este sistema es para empresas que manejan datos importantes sobre sus clientes. A continuación se presentan dos casos practicos donde el uso de este sistema es realemnte efectivo.

Ataque de fuerza bruta.

Cuando un usuario intenta registrarse en vano, en varias aplicaciones de su red de trabajo o bien un atacante trata de entrar a la red y tiene varios intentos fallidos, el sistema SIEM es recomendable ya que permite la detección de este tipo de acceso y permite la creación de oportunidades para evitar que se produzcan nuevos intentos de ingreso.

Intento de acceso a VPN.

Ya que los accesos remotos por VPN son comunes en redes empresariales, siempre existe la posibilidad de que existan atacantes que traten de aprovecharse de esta oportunidad, para este tipo de situaciones que igual se trata de un intento de acceso el sistema SIEM permite la identificación y clasificación de actividad como sospechosa de un intento de inicio de sesión desde distintos lugares.

Con todo lo presentado hasta ahora se puede mencionar que para que el sistema tenga un mejor desempeño es sumamente importante estandarizar los datos del entorno donde se trabaja. Todo esto para que el SIEM pueda ejecutar de una mejor manera el análisis y la correlación. Lo cual como se mencionó anteriormente en las ventajas, reduce la carga de trabajo del equipo y permite tener una vista más optimizada de la actividad y de los potenciales riesgos.

Funcionalidades claves de un SIEM.

- 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.

IDS/IPS

IDS (Intrusion Detection System)

El IDS es un sistema que permite la detección de intrusos a una red, este posee sensores que permiten obtener datos. Con lo cual el sistema IDS puede detectar anomalías en el tráfico de red.

La forma en la que funciona este sistema es analizando a detalle el tráfico de red, para que el IDS tenga un buen funcionamiento se debe usar junto a un Firewall ya que, por si solo un IDS no tiene la capacidad de detener un ataque.

IPS (Intrusion Prevention System)

Se encarga de controlar el acceso a usuarios no registrados, con la posibilidad de poder bloquearlos. Para hacerlo puede usar distintas herramientas ya sea Hardware, Software o una combinación de ambas.

Según la forma de detectar ataques se categorizan en:

Basado en firmas: compara el tráfico con firmas de ataques conocidos.

Basado en políticas: como lo indica su nombre, se definen políticas estrictas.

Basado en anomalías: método menos fiable ya que da muchos falsos positivos, para este método se encuentran dos opciones.

Detección estadística de anormalidades: analiza el tráfico en un lapso de tiempo, después crea una lista de lo “normal”, posteriormente si el comportamiento varía mucho se considera la posibilidad de un ataque.

Detección no estadística de anormalidades: para esta opción, el encargado de definir lo “normal” es el administrador del sistema.