Nombre de la materia:
Fundamento de telecomunicaciones

Nombre de la licenciatura:
SISTEMAS COMPUTACIONALES

Nombre del alumno(a):
ALAN GERARDO GIJON AGOSTO

Número de control:
18530390

Nombre de la tarea: Investigación (SIEM)

Unidad #: nombre de la unidad:

Nombre del profesor(a):
ING. ISMAEL JIMENEZ SANCHEZ

Fecha:

¿QUÉ ES EL SIEM?

SIEM

SIEM (Security Information and Event Management) o sistema de gestión de eventos e información de seguridad: es una solución híbrida centralizada que engloba la gestión de información de seguridad (Security Information Management) y la gestión de eventos (Security Event Manager). La tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por los distintos dispositivos hardware y software de la red.

Recoge los registros de actividad (logs) de los distintos sistemas, los relaciona y detecta eventos de seguridad, es decir, actividades sospechosas o inesperadas que pueden suponer el inicio de un incidente, descartando los resultados anómalos, también conocidos como falsos positivos y generando respuestas acordes en base a los informes y evaluaciones que registra, es decir, es una herramienta en la que se centraliza la información y se integra con otras herramientas de detección de amenazas.

Ventajas y desventajas de cada herramienta

Entre las ventajas de contar con un SIEM destacan la centralización de la información y eventos, es decir, se proporciona un punto de referencia común. La centralización permite automatizar tareas, con su consiguiente ahorro de tiempo y costes, el seguimiento de los eventos para detectar anomalías de seguridad o la visualización de datos históricos a lo largo del tiempo. Además, los sistemas SIEM muestran al administrador la existencia de vulnerabilidades, así como si están siendo aprovechadas en los ataques.

Entre sus desventajas en el caso de que se encargue de su mantenimiento un departamento de la empresa destacan sus altos costes de implantación, una curva de aprendizaje larga al tener que formar personal propio para esta tarea y una integración limitada con el resto del sistema. En el caso de que se externalice esta tarea se experimenta una pérdida de control de la información generada o un acceso limitado a

determinada información y una fatiga por la alta recepción de notificaciones. Estos aspectos pueden gestionarse con el proveedor del servicio a través de los acuerdos de nivel de servicios o ANS.

Bibliografía:

https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips