TECNOLOGICO NACIONAL DE MEXICO

INSTITUTO TECNOLÓGICO DE CANCÚN

FUNDAMENTOS DE TELECOMUNICACIONES

Ingeniería en Sistemas Computacionales

ALUMNO: OSWALDO ENRIQUE TUYUB JIMENEZ

DOCENTE: ING. ISMAEL JIMENEZ SANCHEZ

ACTIVIDAD

“INVESTIGACION SIEM”

UNIDAD 3

¿Qué ES LA SIEM?

Su finalidad se orientaba a administrar infraestructuras de seguridad como Firewalls, VPN, IDS y Proxy para apoyar a los clientes en la administración y operación de su arquitectura de seguridad. la implementación de un SOC más orientado al monitoreo, gestión de incidentes y el análisis de diferentes fuentes de eventos de seguridad, mediante herramientas de correlación para reducir los falsos positivos. Al final, esa herramienta llamada SIEM se volvió el centro neurálgico de la operación de ciberseguridad.

las organizaciones están enfocadas en cuáles son las características que deberían tener en cuenta para seleccionar el mejor SIEM de acuerdo a sus necesidades. Para ello, el Grupo A3Sec ha desarrollado un análisis basado en el cuadrante mágico de Garner, para establecer cuáles son las características mínimas de un SIEM, las funcionalidades claves y sus diferenciales.

los requerimientos mínimos, funcionalidades obligatorias que deben tener los sistemas SIEM, su ausencia deja por fuera de competencia en el entorno actual; funcionalidades clave, que hacen referencia a cómo están constituidos los SIEM para cumplir con su propósito en la actualidad; y los diferenciales, que son las características únicas y novedosas que tienen los líderes del mercado.

Los requerimientos mínimos que debe tener una solución SIEM para que cumpla con el objetivo trazado:

- **SaaS:** es una solución Cloud Native con capacidades de escalabilidad y de fácil despliegue.
- **Onpremise**: es una solución para implementación local en equipos virtuales o máquinas físicas.
- Cifrado de Datos (Integridad y Confidencialidad): es una solución que protege la integridad de los datos desde el origen, en su procesamiento y en resguardo. Incluye capacidades de ofuscación.
- Term License: hace referencia a los términos establecidos en la licencia. Todas las herramientas tecnológicas han migrado sus modelos de un licencias de forma anual, con base en su orientación financiera.
- Licencia basada en Volumen de Datos: en la actualidad es el modelo de licenciamiento más utilizado en soluciones SIEM. La forma de dimensionar se soporta mediante eventos por segundo (EPS) o cantidad de datos indexados por día.
- Network: integración y explotación de eventos de red.
- EndPoint: integración y explotación de eventos de host.