**Profesor Guia David Ruete/Profesor Cliente :Oliver Tessini**

**Problemática:**

Actualmente existe diversas herramientas para la implementación de un SIEM (Security Information and Event Management), el problema es que la mayoría de ellas son pagadas a un alto valor, el objetivo es desarrollar un SIEM con herramientas OpenSource

**Título:**

Desarrollo de SIEM con herramientas OpenSource.

**Descripción:**

Se desea desarrollar un SIEM con herramientas OpenSource. Los eventos deben ser capturados por herramientas tales como Snort, Suricta, OSSIM, OSSEC, Bro y visualizados con herramientas como Snorby, Prelude, Kibana.

Se deben comparar las herramientas entre ellas y con el Sistema Operativo "Security Onion".

También se debe considerar la implementación de un "Honeypot", el cual es un sistema vulnerable que actúa como "Pote de Miel" para atraer a los atacantes y generar alertas.

Adicionalmente, se debe determinar los requisitos mínimos de infraestructura (CPU, Memoria RAM, Capacidad de Disco Duro) para gestionar y almacenar eventos con una antigüedad de un (1) año. Esto permite tener visibilidad para efectos de auditoria y va relacionado con la ISO27001:2013.

**Resultado:**

Obtener un SIEM funcionando, habiendo hecho la comparativa de cuál es la mejor opción, por ejemplo, si Snort con Snorby, si Suricata con Kibana, etc. De igual forma, se deben establecer el requerimiento de sistemas mínimos para que el SIEM gestione y almacene los eventos por un año.

**Valor Agregado y Recomendación:**

Para establecer los requisitos mínimos se debe medir el peso promedio en bytes de cada evento generado, la cantidad de eventos por unidad de tiempo (segundo, día, etc.) esto permite saber la velocidad de crecimiento de la Base de Datos. Se recomienda probar el SIEM funcionando en una red real la cual puede ser parte de la red de la Universidad. El valor agregado, es que la Universidad puede quedar con un SIEM funcionando en sus redes que le ayudará al CIRT para gestionar los incidentes de seguridad.

Como segunda recomendación se deben usar sentencias de MySQL para optimizar su tamaño.

**Conocimientos Necesarios o que se adquirirán:**

El estudiante deberá tener conocimientos en sistemas Operativos Linux y Base de Datos MySQL

Criterios de Selección de herramientas

1. Disponibilidad de documentación en línea
2. Cual es el sw mas actual