Maestría en

Ciberseguridad

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTORES:

Felipe Alfonso Castro Vélez

Jherman Fernando Canacuán Segovia

Luis Alexander Espinosa Gallardo

Jonathan Xavier Zurita Flores

TUTORES:

Iván Reyes Chacón

Alejandro Cortés

TEMA

Fortalecimiento de la detección de amenazas mediante la integración de inteligencia de amenazas en un SIEM

REINVENTEMOS EL FUTURO

RESUMEN

El aumento de ciberataques ha obligado a las empresas a mejorar sus capacidades de detección, e especial a través del uso de un SIEM integrados con fuentes de inteligencia de amenazas. Este proyecto tiene como propósito integrar fuentes de inteligencia en un entorno de SIEM de Elasticsearch on premise, con el fin de robustecer el enriquecimiento de datos ingestados y la detección de indicadores de compromiso. Para lograr este objetivo se levantó un ambiente de laboratorio controlado en onde se incorporó las fuentes de Abuse.ch y AlienVault OTX, el despliegue de un agente en un equipo Windows para la reelección de logs.

La metodología incluyo la selección y evaluación de herramientas de inteligencia de amenazas, configuración de ingesta y la ejecución de pruebas en un ambiente controlado. A si mismo se identificó la necesidad de migrar hacia un ambiente en nube para garantizar la escalabilidad y robustez en un entorno productivo. Este proyecto evidencia que la integración adecuada de inteligencia de amenazas fortalece la detección de indicadores de compromiso y optimiza la operación de un SIEM moderno

Palabras Claves: Inteligencia de amenazas, SIEM, Elasticsearch, indicadores de compromiso, integración

ABSTRACT

The increase in cyberattacks has forced companies to improve their detection capabilities, particularly through the use of SIEM integrated with threat intelligence sources. The purpose of this project is to integrate intelligence sources into an on-premise Elasticsearch SIEM environment in order to strengthen the enrichment of ingested data and the detection of indicators of compromise. To achieve this goal, a controlled laboratory environment was set up incorporating Abuse.ch and AlienVault OTX sources, and an agent was deployed on a Windows computer for log collection. The methodology included the selection and evaluation of threat intelligence tools, ingestion configuration, and testing in a controlled environment. The need to migrate to a cloud environment was also identified to ensure scalability and robustness in a production environment. This project demonstrates that the proper integration of threat intelligence strengthens the detection of indicators of compromise and optimizes the operation of a modern SIEM.

Keywords: Threat intelligence, SIEM, Elasticsearch, indicators of compromise, integration