Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en ciberseguridad

AUTOR/ES:

ALCÍVAR SOLORZANO RONALD MAURICIO

ERAZO PÉREZ MARCOS ESTEBAN

LARA BEDÓN LUIS ALEXANDER

PLÚAS RUGEL ERWIN FABIÁN

ZURITA RODRIGUEZ VICENTE DAVID

TUTOR/ES:

Ivan Reyes Chacón

Alejandro Cortés López

TEMA

INTEGRACIÓN DE INTELIGENCIA DE AMENAZAS EN SPLUNK SIEM PARA LA DETECCIÓN PROACTIVA DE INCIDENTES DE SEGURIDAD

REINVENTEMOS EL FUTURO

RESUMEN

Esta investigación aborda la integración de inteligencia de amenazas en la plataforma SIEM de Splunk con el fin de mejorar la detección proactiva de incidentes de seguridad en entornos corporativos. Analiza cómo la integración de fuentes externas de indicadores de riesgo (IoC), como direcciones IP maliciosas, dominios sospechosos y hashes de malware, ayuda a mejorar la correlación de eventos y reduce los falsos positivos. El proyecto propuesto se implementa en un entorno de laboratorio controlado: se instala Splunk como SIEM central, se integran las fuentes de inteligencia de amenazas (en combinación con MISP, AlienVault OTX, Abuse.ch y STIX/TAXII) y se desarrollan reglas de correlación para validar la eficacia de la solución. Los resultados demuestran que la integración de inteligencia de amenazas mejora la anticipación, la priorización y la respuesta a los riesgos emergentes, aportando valor al posicionamiento estratégico de la seguridad de la información.

Palabras Claves: Splunk SIEM, Inteligencia de Amenazas (Threat Intelligence), Indicadores de Compromiso (IoCs), STIX/TAXII, MISP, AlienVault OTX, Abuse.ch, Correlación de Eventos, Detección Proactiva de Incidentes, Centro de Operaciones de Seguridad (SOC), ISO/IEC 27001, ISO/IEC 27035, EGSI v3, Dashboards y Alertas, Automatización y SOAR.

ABSTRACT

This research concerns threat intelligence integration into the Splunk SIEM platform in an effort to enhance proactive detection of security incidents in corporate environments. It discusses how integrating external sources of IoCs, such as malicious IP addresses, suspicious domains, and malware hashes, helps improve event correlation and reduces false positives. The proposed project is then implemented in a controlled laboratory environment: Splunk is installed as the central SIEM, the threat intelligence feeds are integrated-coupled with MISP, AlienVault OTX, Abuse.ch, and STIX/TAXII-and correlation rules are developed to validate the efficacy of the solution. The results prove that threat intelligence integration enhances anticipation, prioritization, and response to emerging risks by providing adequate value for information security's strategic positioning.

Keywords: Splunk SIEM, Threat Intelligence, Indicators of Compromise (IoCs), STIX/TAXII, MISP, AlienVault OTX, Abuse.ch, Event Correlation, Proactive Incident Detection, Security Operations Center (SOC), ISO/IEC 27001, ISO/IEC 27035, EGSI v3, Dashboards and Alerts, SOAR Automation