Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTOR/ES:

LEMA SAMANIEGO LUIS ALBERTO

LUDEÑA CHALACAN FREDDY ANDRES

TRUJILLO ESTRELLA JOHN ANDRES

TUTOR/ES:

Iván Reyes Chacón

Alejandro Cortés López

Diseño e Implementación de una Solución SIEM de Código Abierto para la Empresa Synergos

Quito - Ecuador

Junio - 2025

REINVENTEMOS EL FUTURO

Resumen

La ciberseguridad se ha afianzado como un componente crítico para las organizaciones, particularmente aquellas que ejercen en el sector tecnológico, debido al incremento sostenido de amenazas cibernéticas que varían desde ataques simples hasta campañas altamente sofisticadas. Ante tal escenerio surge la necesidad de responder a la pregunta: ¿Cómo detectar, analizar y responder eficazmente a amenazas dentro de una infraestructura empresarial?

Este proyecto propone la implementación de un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) de código abierto como solución para el monitoreo continuo, análisis de eventos y respuesta en tiempo real ante incidentes de seguridad. Después de un análisis comparativo de múltiples plataformas SIEM open source, se seleccionó Wazuh por su escalabilidad, solidez, comunidad activa y soporte técnico. La solución englobó el diseño de una arquitectura de seguridad integral, la instalación de agentes en sistemas críticos, la configuración de reglas de correlación y decodificadores personalizados, así como la unificación con herramientas como FIM, Sysmon, Suricata, pfSense Plus, Gitea y Vaultwarden.

Dicho método ayudó con la evaluación de la efectividad de las soluciones SIEM de códigos abiertos, demostrando su capacidad para detectar, monitorear y mitigar amenazas en tiempo real, y contribuyendo a la protección de infraestructuras críticas en el ámbito corporativo.

Palabras clave: ciberseguridad, SIEM, Wazuh, detección de amenazas, monitoreo en tiempo real, código abierto, pfSense, Suricata.

Abstract

Cybersecurity has become established as a critical component for organizations, particularly those operating in the technology sector, due to the sustained increase in cyber threats ranging from simple attacks to highly sophisticated campaigns. Given this scenario, the question arises: How can threats be effectively detected, analyzed, and responded to within an enterprise infrastructure?

This project proposes the implementation of an open-source Security Information and Event Management (SIEM) system as a solution for continuous monitoring, event analysis, and real-time response to security incidents. After a comparative analysis of multiple open-source SIEM platforms, Wazuh was selected for its scalability, robustness, active community, and technical support. The solution included the design of a comprehensive security architecture, the installation of agents on critical systems, the configuration of correlation rules and custom decoders, and integration with tools such as FIM, Sysmon, Suricata, pfSense Plus, Gitea, and Vaultwarden.

This method helped evaluate the effectiveness of open source SIEM solutions, demonstrating their ability to detect, monitor and mitigate threats in real time, and contributing to the protection of critical infrastructures in the corporate environment.

Keywords: cybersecurity, SIEM, Wazuh, threat detection, real-time monitoring, open source, pfSense, Suricata.