Maestría en

Ciberseguridad

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTORES:

Arias Giraldo Juan Carlos

Manrique Cachimuel Carlos Andrés

Pichucho Bombón Jorge Aníbal

Sangucho Díaz Christian Alfonso

TUTORES:

Iván Reyes Chacón

Alejandro Cortés

TEMA:

"Desarrollo de un sistema correlacionador de eventos de bajo costo para PYMES orientado a la continuidad operativa"

Quito - Ecuador

REINVENTEMOS EL FUTURO

RESUMEN

En la presente investigación se desarrolla la idea de un sistema SIEM (Security Information and Event Management) de bajo costo para pequeñas y medianas empresas (PYMES), tomando en cuenta herramientas opensource y de hardware mínimo. Su objetivo principal es exponer que es posible fortalecer la seguridad informática y la continuidad operativa sin ser necesario de invertir soluciones comerciales costosas y de no repetir los mismos sistemas opensource aplicados en tesis anteriores. Este proyecto se construyó sobre la plataforma Elastic Stack, con una gran capacidad de centralizar, procesar y poder visualizar registros de seguridad en aplicativos Windows, en Firewall como Fortigate y en lo más actual como son las controladoras UNIFI. El proyecto fue implementado en un equipo de cómputo extremadamente sencillo, con muchos recursos limitados, demostrando que una PYME puede obtener capacidades de monitoreo, análisis y una configuración básica para poder encontrar todo tipo de información en su red, recolectando todo tipo de logs generados, logrando una visibilidad completa de los eventos que podrían comprometer la operación del negocio.

Los resultados nos muestran un SIEM basado en Elastic Stack con soluciones pequeñas pero viables, escalables y económicamente accesibles para pequeñas empresas. Su implementación en hardware limitado confirma que la seguridad informática no depende de grandes recursos, sino de un correcto entendimiento de la gestión de logs, la identificación de la infraestructura de red que estamos manejando y una voluntad por encontrar a través de las configuraciones de la herramienta que nos ayuden a fortalecer la protección de la información.

Palabras Claves: SIEM, ELASTIC STACK, Logs, Open-Source, PYMES, Seguridad Informática.

ABSTRACT

This research develops the concept of a low-cost SIEM (Security Information and Event Management) system for small and medium-sized enterprises (SMEs), utilizing open-source tools and minimal hardware. Its main objective is to demonstrate that it is possible to strengthen cybersecurity and business continuity without investing in expensive commercial solutions or replicating the same open-source systems used in previous theses. This project was built on the Elastic Stack platform, which offers a significant capacity to centralize, process, and visualize security logs in Windows applications, firewalls such as Fortigate, and more recent technologies like UniFi controllers. The project was implemented on a very basic computer with limited resources, demonstrating that an SME can obtain monitoring and analysis capabilities, along with a basic configuration, to find all types of information on its network, collect all types of generated logs, and achieve complete visibility of events that could compromise business operations.

The results show an Elastic Stack-based SIEM with small but viable, scalable, and economically accessible solutions for small businesses. Its implementation on limited hardware confirms that cybersecurity doesn't depend on vast resources, but rather on a proper understanding of log management, the identification of the network infrastructure being used, and a willingness to explore tool configurations that can help strengthen information protection.

Keywords: SIEM, Elastic Stack, Logs, Open Source, SMEs, Cybersecurity.