UIDE
Powered by
Arizona State University

eig Business School

Maestría en

Ciberseguridad

Trabajo de investigación previo a la obtención del título de Magíster en Ciberseguridad

AUTORES:

Cristopher Alexander Gualoto Palacios
Anthony Fernando Jiménez Perugachi
Klever Fernando Villa Yungan
Roberto William Rodriguez Benalcazar

TUTOR:
Alejandro Cortés

TEMA:

Implementación y configuración de un SIEM Open Source en una pequeña o mediana Empresa

Quito, Octubre 2024

RESUMEN

El presente proyecto de titulación se centra en la implementación de un Sistema de Gestión de la Seguridad de la Información, también conocido por sus siglas SIEM, utilizando tecnologías de código abierto. Se considera su aplicación en un entorno real, donde los activos críticos son dispositivos de un proveedor de servicios de internet. El objetivo principal es fortalecer la seguridad digital de la organización, asegurando que la respuesta ante un incidente sea oportuna.

La importancia del estudio radica en la creciente necesidad de soluciones accesibles y efectivas que permitan a las pequeñas y medianas empresas obtener una forma de protección sin incurrir en los altos costos de las soluciones comerciales. Este proyecto explora la viabilidad, configuración y optimización de un SIEM en un entorno donde los recursos económicos y tecnológicos son limitados, aprovechando herramientas de código abierto.

Palabras Claves: Código abierto, SIEM, ISP, Incidente.

ABSTRACT

This degree project focuses on the implementation of an Information Security Management System, also known by its acronym SIEM, using open source technologies. Its application is considered in a real environment, where the critical assets are devices of an internet service provider. The main objective is to strengthen the organization's digital security, ensuring that the response to an incident is timely.

The importance of the study lies in the growing need for affordable and effective solutions that allow small and medium enterprises to obtain a form of protection without incurring the high costs of commercial solutions. This project explores the feasibility, configuration and optimization of a SIEM in an environment where economic and technological resources are limited, taking advantage of open source tools.

Keywords: Open source, SIEM, ISP, Incident.