UIDE

Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Trabajo Final de Maestría previa a la obtención del título de Magíster en Ciberseguridad

Fortalecer la infraestructura de detección de amenazas y vulnerabilidades en una industria atunera ecuatoriana mediante la implementación de un SIEM

AUTORES: Ab. Verónica Estefanía Cabezas Cabrera
Ing. Jorge Gabriel Sampedro Ocaña
Ing. José Rubén Mendoza Muñoz
Ing. Juan Fernando Villalba Gallardo

TUTOR: Ing. Alejandro Cortés López

QUITO - ECUADOR | 2023

Resumen

El presente proyecto de titulación está enfocado a fortalecer la infraestructura de detección de amenazas y vulnerabilidades en una industria atunera ecuatoriana, mediante la implementación de un SIEM (Security Information and Event Management), con el objetivo de lograr obtener una solución mediante la cual se fortalezca el marco de ciberseguridad existente en la industria en mención.

De esta manera, por ser una industria que maneja información considerable e importante, puede volverse vulnerable y convertirse en víctima de ataques propuestos por los ciberdelincuentes, para lo cual a través del desarrollo del presente proyecto de titulación se va a implementar la solución SIEM y el despliegue de sus agentes en los equipos que se encuentran dentro de la infraestructura de TI, para garantizar la funcionalidad y eficacia.

A través de lo cual, se va a buscar garantizar su funcionalidad y eficacia, mediante pruebas que garanticen la correcta funcionalidad de la SIEM a implementarse.

Finalmente se va a establecer una propuesta a futuro para el desarrollo de un plan de gestión y monitoreo de la solución SIEM implementada, la cual va a incluir aquellas definiciones de roles, responsabilidades, establecimiento de aquellos procesos a seguir cuando se produzca la detección y de qué manera se va a actuar en respuesta a los indicadores de compromiso que se identifiquen en los equipos.

Abstract

The present graduation project aims to enhance the threat detection and vulnerability infrastructure within the Ecuadorian tuna industry by implementing a Security Information and Event Management (SIEM) system. The objective is to achieve a solution that strengthens the existing cybersecurity framework in the industry under consideration.

Given that the industry handles significant and important information, it can become vulnerable and fall victim to cyber attacks proposed by cybercriminals. Therefore, through the development of this graduation project, the SIEM solution will be implemented, along with the deployment of its agents on the equipment within the IT infrastructure, in order to ensure functionality and effectiveness.

Throughout this process, efforts will be made to guarantee the functionality and effectiveness of the SIEM by conducting tests that ensure its proper operation upon implementation.

Lastly, a future proposal will be established for the development of a management and monitoring plan for the implemented SIEM solution. This plan will include defining roles and responsibilities, establishing processes to follow when detection occurs, and determining the appropriate response to identified compromise indicators on the equipment.