UIDE

Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Proyecto previo a la obtención del título de Magíster en Ciberseguridad

AUTOR:

Acuña Paredes Yesenia de las Mercedes
Aquino Sanchez Elvia Marina
Esteves Mariño Mario Enrique
Guachamin Tonato Juan Fernando
Verdesoto Aviles Pablo Alejandro

TUTOR:

Ing. Alejandro Cortés López

Implementación de un SIEM para la identificación de posibles ciberataques en la empresa Torres & Torres

QUITO – ECUADOR | 2022

Resumen

El progreso tecnológico ha dado lugar a que las empresas demanden la protección de los activos de información enfocándose en implementar plataformas que garanticen su funcionamiento a mediano plazo.

El presente proyecto se basa en un enfoque práctico mediante la implementación de un Sistema de Gestión de Eventos e Información de Seguridad (*SIEM*) con la herramienta de código abierto, *Wazuh*[1], el cual proporciona monitoreo, detección y alertas de eventos e incidentes.

Sus componentes principales son: agente, servidor y *Elastic Stack* que comprende a *Elasticsearch, Kibana* y *Filebeats*. Además, se integra con herramientas como: *VirusTotal, YARA, AlienVault, Amazon Macie, Slack, OwlH, Fortigate Firewall* quienes permiten fortalecer la seguridad de las redes que son blanco fácil para los piratas informáticos.

La configuración del sistema de seguridad consiste en la implementación de un servidor SQL, firewall, servidor web (*zabbix*), controlador de dominio y equipos ePO. Todos ellos han sido han sido conectados al SIEM para su monitoreo.

En el firewall se utilizó *syslog* para el análisis de logs generados y se configuró un sistema de alertas tanto por e-mail como por *MS Teams* y *Telegram*.

Por lo mencionado, utilizar *Wazuh* así como sus componentes antes mencionados, ha permitido gestionar la seguridad en la compañía Grupo Torres & Torres.

Palabras Clave: Seguridad, SIEM, Wazuh, VirusTotal, YARA, AlienVault, Amazon Macie, Slack, OwlH, Fortigate Firewall.

[1] wazuh.com

Abstract

Due to technological advance, companies demand the protection of information assets, focusing on implementing platforms that guarantee their operation in the medium term.

The present project is based on a practical approach through the implementation of a Security Information and Event Management System (SIEM) with the open-source tool, "Wazuh", which provides monitoring, detection and alerts of events and incidents.

Its main components are agent, server and Elastic Stack that includes Elastic search, Kibana and Filebeats. In addition, it integrates with tools such as: VirusTotal, YARA, AlienVault, Amazon Macie, Slack, OwlH, Fortigate Firewall, which allow strengthening the security of networks that are easy targets for hackers.

The configuration of the security system consists of the implementation of a SQL server, firewall, web server (zabbix), domain controller and ePO equipment. All of them have been connected to the SIEM for monitoring.

In the firewall, syslog was used to analyze the generated logs and an alert system was configured both by e-mail and by MS Teams and Telegram.

Due to the, using Wazuh as well as its components mentioned before, has made it possible to manage security in the Grupo Torres & Torres Company.

Keywords: Security, SIEM, Wazuh, VirusTotal, YARA, AlienVault, Amazon Macie, Slack, OwlH, Fortigate Firewall.