UIDE

Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES:

Sandra Patricia Gómez Prado.

Nancy Aracely Sandoval Bonilla.

Juan Alejandro Ibadango Urbano.

Washington Armando Orellana Diaz.

DIRECTOR: Ing. Alejandro Cortés.Msc.

Propuesta de implementación de SIEM en un centro de capacitación, con tres casos de usos, utilizando Mitre attack.

Resumen

En este estudio, se realizó una propuesta de implementación de un SIEM como sistema de ciberdefensa para un centro de capacitación ubicado en la ciudad de Quito, Ecuador, que permita monitorear los activos de la empresa, tener una mejor visibilidad de las amenazas que puedan presentarse en su entorno. El SIEM genera alertas tempranas a través de la configuración de los casos de uso utilizando la matriz mitre attack, con lo que se puede responder de manera oportuna a los incidentes de Ciberseguridad. En nuestra propuesta de implementación del SIEM, se ha seleccionado la herramienta open source Wazuh, una de las ventajas que posee, es la versión gratuita de SIEM, su agente posee una compatibilidad con sistemas operativos tales como: Windows, Linux, Mac OS, Oracle, AIX, HPUX y sistemas de cloud como AWS. Wazuh, utiliza Elastich search como su motor de búsqueda y almacenamiento, Kibana para visualizar los gráficos y realizar la reportería y búsqueda de datos, además wazuh app que permite visualizar paneles iterativos para analizar los eventos de seguridad de manera eficiente. El análisis e implementación de los casos de uso, se debe realizar de manera continua y de acuerdo a las necesidades del negocio, estos deben ser probados y afinados para evitar el incremento de falsos positivos, enfocándose en los casos de uso que nos ayuden a prevenir el riesgo.

Palabras Clave: *siem, caso de uso, mitre attack, wazuh*

Abstract

In this study, a proposal was made for the implementation of a SIEM as a cyber defense system for a training center located in the city of Quito, Ecuador, which allows monitoring the company's assets, having better visibility of the threats that may arise in its environment. The SIEM generates early warnings through the configuration of use cases using the mitre attack matrix, which can respond in a timely manner to cybersecurity incidents. In our proposal for the implementation of the SIEM, the open-source tool Wazuh has been selected, one of the advantages it has, is the free version of SIEM, its agent has compatibility with operating systems such as: Windows, Linux, Mac OS, Oracle, AIX, HPUX and cloud systems such as AWS. Wazuh uses Elastich search as its search engine and storage. Kibana to visualize the graphs, perform the reporting and search for data. In addition, wazuh app allows you to visualize iterative dashboards to analyze security events efficiently.

Keywords: *siem, uses cases, mitre attack, wazuh*