UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTOR: Ing. Wilson Steven Patiño Rosero
Ing. Víctor Hugo Pulig Yanez
Ing. Henry Geovanny Quishpe Rochina
Ing. Pablo Mauricio Solorzano Cañizares

TUTOR: Msc. Alejandro Cortés

Implementación de un SIEM en el área de TI para identificar y centralizar posibles eventos en la infraestructura critica de la industria gráfica.

Resumen

El trabajo de titulación de Maestría titulado "Implementación de un SIEM en el área de TI para la Identificación y Centralización de Eventos en la Infraestructura Crítica de la Industria Gráfica" tiene como objetivo proporcionar a la industria gráfica una solución de SIEM de código abierto que pueda gestionar eventos de seguridad y proteger los activos de información de la organización. En este contexto, el estudio comenzó con una evaluación de la infraestructura de la industria gráfica para identificar los riesgos asociados a los equipos críticos que requieren monitoreo, con el propósito de actuar de manera oportuna ante posibles intentos de intrusión no autorizada en la red interna de la organización. Después de evaluar diversas opciones de herramientas de código abierto, se eligió SIEM Wazuh debido a su capacidad para recopilar información en un nodo central sin afectar el rendimiento de otros servicios en la infraestructura. Como resultado de la implementación de SIEM, se pudo constatar que esta solución permite la detección automática de eventos que pueden afectar la infraestructura de red, lo que a su vez posibilita la gestión, control, resolución y mitigación de posibles riesgos, vulnerabilidades y amenazas. Esta investigación contribuye significativamente a fortalecer la seguridad de la industria gráfica y proteger sus activos de información crítica.

Palabras clave: *eventos, seguridad, instrucción, mitigación, vulnerabilidad, proteger, datos, monitoreo, servicios, SIEM.*

ABSTRACT

The Master's degree work entitled "Implementation of a SIEM in the IT area for the Identification and Centralization of Events in the Critical Infrastructure of the Printing Industry" aims to provide the printing industry with an open source SIEM solution that can manage security events and protect the organization's information assets. In this context, the study began with an evaluation of the infrastructure of the printing industry to identify the risks associated with critical equipment that requires monitoring, with the purpose of acting in a timely manner against possible unauthorized intrusion attempts on the internal network of the organization. After evaluating several open-source tool options, Wazuh SIEM was chosen due to its ability to collect information on a central node without impacting the performance of other services in the infrastructure. As a result of the implementation of SIEM, it was found that this solution allows the automatic detection of events that may affect the network infrastructure, which in turn enables the management, control, resolution and mitigation of possible risks, vulnerabilities and threats. This research contributes significantly to strengthening the security of the printing industry and protecting its critical information assets.