Maestría en

CIBERSEGURIDAD

AUTORES:

Ing. David Sebastián Chaguaro Vásconez

Ing. Juan Francisco Negrete Marroquin

Ing. Adriana Alejandra Cahuano Ilbay

Ing. Milton Fabian Vintimilla Barzallo

TUTOR:

Ing. Ronie Stalin MartínezGordon, Mtr.

IMPLEMENTACIÓN DE UN SIEM PARA LA AUDITORIA DE EVENTOS DE SEGURIDAD EN LA ENTIDAD REGISTRO DE LA PROPIEDAD DEL CANTÓN AZOGUES

Resumen

La situación actual en el Registro de la Propiedad del Cantón Azogues dio lugar al incremento de sus servicios digitales con proyectos de digitalización para reducir procesos manuales e información física de alta demanda. Al tener cada vez más información digital que proteger, para garantizar su disponibilidad, integridad y confidencialidad, se convierte en el candidato ideal para impulsar auditorías de los eventos que ocurren en su entorno mediante la implementación de un sistema SIEM, identificar vulnerabilidades y aplicar técnicas de hacking ético, para simular ataques y determinar el nivel de seguridad, y realizar las mejores recomendaciones. El presente trabajo analizó la infraestructura tecnológica actual de la Institución, para tener una visión general de su funcionamiento, y así determinar sus puntos críticos de equipamiento y el manejo de la información digital. En base al conocimiento previo y a la información de logs que Wazuh está recopilando, normalizando, correlacionando y analizando, pudimos establecer los parámetros sobre su condición actual, y por los cuales se ha realizado las auditorías en base a la ISO 27001 y 27002, en lo que corresponden a la autentificación y la adecuada aplicación de las políticas de administración de cuentas en el directorio activo de Windows Server; el adecuado seguimiento al monitoreo de las carpetas con los documentos críticos del Servidor de Archivos. También se consideró importante dentro de las recomendaciones, que luego de revisar los puntos auditados, es la implementación la automatización de notificaciones a eventos y alertas importantes que genera Wazuh, mediante utilización del correo electrónico. La integración con aplicaciones de terceros permitió implementar controles en caso de que sucedan comportamientos no deseados en los entornos de trabajo y los dispositivos de uso diario, mediante la API de VirusTotal; y la de notificaciones con Slack.

Palabras claves: SIEM, vulnerabilidades, información digital, Registro de la Propiedad, Wazuh, alertas, virus.

Abstract

The current situation in the Registro de la Propiedad of Canton Azogues led to the increase of its digital services with digitalization projects to reduce manual processes and high-demand physical information. By having more and more digital information to protect, to guarantee its availability, integrity and confidentiality, it becomes the ideal candidate to promote audits of the events that occur in its environment through the implementation of a SIEM system identifying vulnerabilities and applying security techniques. ethical hacking, to simulate attacks and determine the level of security, and make the best recommendations. This work analyzed the current technological infrastructure of the Institution, to have a general vision of its operation, and thus determine its critical points of equipment and the management of digital information. Based on prior knowledge and log information that Wazuh is collecting, normalizing, correlating and analyzing, we were able to establish the parameters regarding its current condition, and for which the audits have been carried out based on ISO 27001 and 27002, as far as that correspond to authentication and the proper application of account management policies in the Windows Server active directory; adequate follow-up to the monitoring of folders with critical documents on the File Server. It was also considered important within the recommendations, that after reviewing the audited points, is the implementation of the automation of notifications to important events and alerts generated by Wazuh, using an email. Integration with third-party applications made it possible to implement controls in case unwanted behaviors occur in work environments and devices in daily use, through the VirusTotal API; and notifications with Slack.

Keywords: SIEM, vulnerabilities, digital information, Registro de la Propiedad, Wazuh, alerts, viruses.