UIDE
Powered by
Arizona State University

Maestría en
CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES: Ing. María Geovanna Ayala Labanda

Ing. Esthela Maribel Cabezas Molina

Ing. Carlos Alberto Fernández Sangucho

TUTORES: Mgs. Alejandro Cortés

Mgs. Iván Reyes

Análisis de logs para la detección de incidentes de seguridad en un IBM QRadar SIEM para una entidad del sector financiero

QUITO – ECUADOR | 2024

RESUMEN

El presente trabajo analiza los logs de eventos de seguridad en una entidad financiera utilizando el SIEM IBM QRadar, con el objetivo de mejorar la detección y respuesta a incidentes de seguridad. La investigación combina una metodología exploratoria y descriptiva.

El análisis destaca la importancia de centralizar y correlacionar los eventos generados por activos críticos como Active Directory, lo que permite identificar patrones sospechosos y generar alertas oportunas en tiempo real. Las conclusiones muestran que QRadar es capaz de reducir significativamente los tiempos de respuesta ante incidentes y mejorar la postura de seguridad de la organización.

Además, se proponen recomendaciones clave, como la optimización de reglas de clasificación, la capacitación continua del personal y el establecimiento de métricas para evaluar el desempeño del SIEM. Este estudio contribuye a fortalecer los procesos de seguridad en el sector financiero ecuatoriano, alineándose con las normativas locales y los estándares internacionales.

Palabras Claves: IBM QRadar, SIEM, Análisis de logs, Detección de incidentes, Seguridad informática

ABSTRACT

This study analyzes security event logs in a financial entity using the IBM QRadar SIEM to enhance incident detection and response. The research employs an exploratory and descriptive methodology.

The analysis highlights the importance of centralizing and correlating events from critical assets such as Active Directory, enabling the identification of suspicious patterns and real-time alert generation. Findings demonstrate that QRadar significantly reduces incident response times and enhances the organization's security posture.

Key recommendations include optimizing classification rules, continuous staff training, and establishing metrics to evaluate SIEM performance. This study contributes to strengthening security processes in the Ecuadorian financial sector, aligning with local regulations and international standards.

Keywords: IBM QRadar, SIEM, Log analysis, Incident detection, Information security