Monitoreo centralizado de eventos de seguridad en redes ISP con syslog y SIEM para la detección temprana de amenazas

Resumen del trabajo técnico

En el ámbito de los proveedores de servicios de internet (ISP), la detección temprana de incidentes de seguridad sigue siendo un reto, en particular por la falta de visibilidad centralizada y herramientas automatizadas que permitan anticipar amenazas. Este proyecto plantea un modelo de monitoreo centralizado de eventos de seguridad, utilizando registros syslog y una plataforma SIEM de código abierto. La solución integra equipos críticos de red, desarrolla decodificadores personalizados y aplica reglas de correlación alineadas a MITRE ATT&CK, lo que permite identificar intentos de fuerza bruta y generar alertas en tiempo real.

El modelo fue validado en la infraestructura de Alfanet Ecuador, donde las alertas automáticas mejoraron la capacidad de reacción del equipo de seguridad y reforzaron los controles existentes en la red. En conjunto, este trabajo se presenta como un modelo replicable para otros operadores regionales interesados en fortalecer sus capacidades de detección y respuesta mediante herramientas de código abierto.

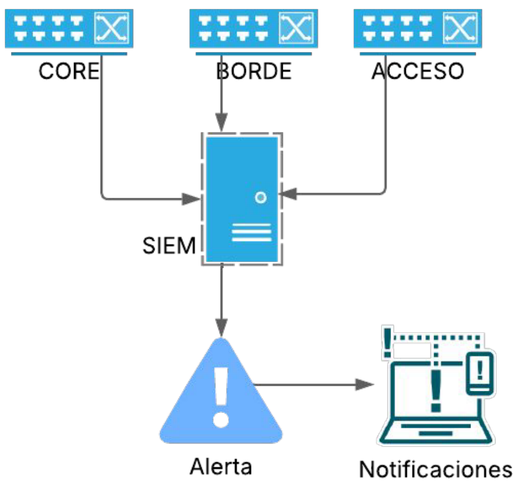
Introducción: antecedentes, descripción y resultados

El incremento sostenido de amenazas cibernéticas, como los ataques de fuerza bruta contra routers, firewalls y dispositivos de acceso, ha puesto a prueba la seguridad de las infraestructuras críticas de los ISPs. Aunque estos equipos generan numerosos registros mediante syslog, en muchos casos se almacenan localmente hasta ser sobrescritos, lo que ocasiona pérdida de evidencia y limita el análisis oportuno de incidentes. La falta de centralización y correlación reduce la capacidad de anticiparse a riesgos y responder con eficacia.

Ante este escenario, el proyecto propone centralizar los registros syslog en una plataforma SIEM de código abierto, a modo de mejorar la visibilidad de la red, detectar patrones anómalos y generar alertas en tiempo real. Su implementación en Alfanet permitió comprobar que el modelo aporta resultados inmediatos, fortaleciendo los controles de seguridad, reduciendo los tiempos de respuesta y sentando las bases para un esquema de monitoreo más robusto y escalable.

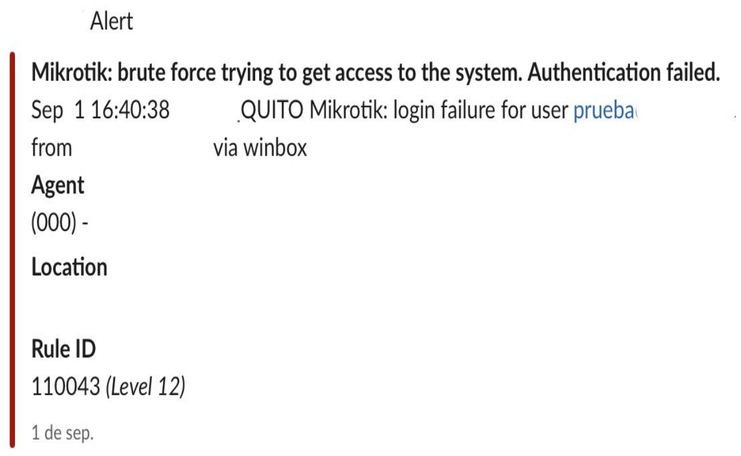
Metodología

El proyecto se estructuró en cinco fases para diseñar y validar el modelo de monitoreo centralizado. Primero, se diagnosticó la red para identificar dispositivos críticos y evaluar sus capacidades de generación y envío de logs. Luego, se implementó un SIEM de código abierto, validando comunicación y recepción de eventos en tiempo real. En la tercera fase, se configuró syslog en equipos Cisco, MikroTik y Huawei con parámetros estandarizados. Posteriormente, se desarrollaron decodificadores y reglas de correlación para detectar intentos de fuerza bruta. Finalmente, se implementaron alertas automáticas integradas con Slack para notificar incidentes críticos en tiempo real.



Gráficos, datos y principales resultados

Los principales resultados del proyecto se evidencian en la validación práctica del modelo en un entorno real. La integración de los dispositivos críticos de red al SIEM permitió centralizar y preservar grandes volúmenes de registros que antes se perdían por limitaciones locales de almacenamiento. El desarrollo de decodificadores y reglas de correlación posibilitó la detección oportuna de intentos de autenticación sospechosos, minimizando falsos positivos y fortaleciendo la capacidad de análisis. Asimismo, el sistema de alertas en tiempo real implementado en Slack facilitó la reacción inmediata del equipo de seguridad, reduciendo significativamente los tiempos de respuesta.



Relevancia del trabajo técnico

Al abordar un desafío crítico, el presente trabajo es relevante para la ciberseguridad en Proveedores de Servicios de Internet (ISP), la detección temprana de amenazas en infraestructuras de gran escala y alta criticidad. La propuesta demuestra que es posible implementar un modelo de monitoreo centralizado, basado en syslog y una plataforma SIEM de código abierto, capaz de complementar soluciones comerciales y reforzar la postura de seguridad de los operadores.

Desde el punto de vista técnico, el proyecto valida la eficacia de centralizar y normalizar registros en entornos multi fabricante, integra la detección de ataques de fuerza bruta con marcos de referencia internacionales como MITRE ATT&CK y asegura la alineación con estándares globales de ciberseguridad (NIST, PCI-DSS, HIPAA, GDPR). Asimismo, documenta una metodología práctica y replicable, aplicada en Alfanet, que evidenció mejoras en visibilidad, correlación de eventos y capacidad de respuesta, consolidándose como una propuesta abierta, escalable y de valor estratégico regional.

Conclusiones, desafíos y oportunidades

El trabajo demostró la viabilidad de diseñar e implementar un modelo de monitoreo centralizado en redes ISP, basado en registros syslog y un SIEM de código abierto. Entre los logros destacan la integración de dispositivos multifabricante, la creación de decodificadores personalizados, la aplicación de reglas de correlación alineadas a MITRE ATT&CK y la configuración de alertas en tiempo real. También se identificaron desafíos como la heterogeneidad en la configuración de syslog, la necesidad de ajustar reglas para reducir falsos positivos, la capacitación en plataformas open source y la gestión de grandes volúmenes de registros, que se transformaron en oportunidades de mejora.

Finalmente, se plantean oportunidades como la incorporación de *machine learning* para anticipar patrones complejos, la ampliación del monitoreo a servicios y aplicaciones críticas, así como la integración con herramientas SOAR. En conjunto, este proyecto constituye un modelo técnico escalable y replicable que fortalece la ciber resiliencia de los ISPs en la región.

Referencias

[1] MITRE ATT&CK, "Enterprise Matrix: Brute Force (T1110)" 2025. [En línea]. Disponible en: https://attack.mitre.org/techniques/T1110. [Consultado: 12 de junio de 2025]

[2] Splunk Threat Research Team, "Massive Infostealer Campaign Targeting ISPs," *Splunk Security Blog*, 5-mar-2025. [En línea]. Disponible en: https://www.splunk.com/en_us/blog/security/infostealer-campaign-against-isps.html. [Consultado: 3 de julio de 2025]

[3] NIST, *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*, Gaithersburg, EE.UU., 2020. [En línea]. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. [Consultado: 21 de julio de 2025]

Autora

Mag. Jenny Zambrano

Mentora

Ing. Erika Vega

Contactos

jzambranop@alfanet.net.ec.

jenny.zambrano.palacio@gmail.com

evega100309@gmail.com

Reseña profesional

Ingeniera en Telecomunicaciones y Redes por la ESPOCH, con maestría en Seguridad de la Información y diplomados en Gobierno, Riesgo y Cumplimiento y en Gerencia de Proyectos. Responsable de Seguridad de la Información en Alfanet Ecuador, lidera proyectos enfocados en automatización, mejora continua y fortalecimiento de la ciber resiliencia organizacional.

Reconocimientos

Agradezco al **Programa de Mentoreo IT Women de LACNIC** por la oportunidad de desarrollar este proyecto y a mi mentora, Erika Vega, por su guía y apoyo constante.

Extiendo también mi reconocimiento a Alfanet Ecuador, por facilitar la validación en su infraestructura y respaldar esta iniciativa de ciberseguridad.

Citación de esta publicación

J. Zambrano. “Monitoreo centralizado de eventos de seguridad en redes ISP con syslog y SIEM para la detección temprana de amenazas” [Presentación de póster]. Presentado en: LACNIC 44-LACNOG 2025, 6-10 de octubre de 2025, San Salvador, El Salvador.