Polo del Conocimiento

Pol. Con. (Edición núm. 102) Vol. 10, No 1
Enero 2025, pp. 2233-2250
ISSN: 2550 - 682X
DOI: https://doi.org/10.23857/pc.v10i1.8807

Análisis del rendimiento de soluciones SIEM de código abierto

Open Source SIEM Solutions Performance Analysis

Análise de desempenho de soluções SIEM de código aberto

Fausto Raúl Orozco-Lara [I]
fausto.orozcol@ug.edu.ec
https://orcid.org/0000-0003-4872-3702

María Fernanda Molina-Miranda [II]
maria.molinam@ug.edu.ec
https://orcid.org/0000-0002-4237-4364

Sergia Beatriz Bonilla-Alejando [III]
sergia.bonillaa@ug.edu.ec
https://orcid.org/0009-0007-9241-4807

Jamilette Lisbeth Ramírez-Marcillo [IV]
jamilette.ramirezm@ug.edu.ec
https://orcid.org/0009-0001-8167-6285

Correspondencia: fausto.orozcol@ug.edu.ec

Ciencias Técnicas y Aplicadas
Artículo de Investigación

*** Recibido:** 27 de noviembre de 2024 ***Aceptado:** 20 de diciembre de 2024 *** Publicado:** 23 de enero de 2025

I. Universidad de Guayaquil, Guayaquil, Ecuador.
II. Universidad de Guayaquil, Guayaquil, Ecuador.
III. Universidad de Guayaquil, Guayaquil, Ecuador.
IV. Universidad de Guayaquil, Guayaquil, Ecuador.

Resumen

Este articulo surge como producto final del trabajo de titulación que tiene como tema Análisis del rendimiento de soluciones SIEM de código abierto para la detección y respuesta automatizada a amenazas cibernéticas el objetivo de la investigación es de evaluar el rendimiento de diversas soluciones SIEM de código abierto, dichas herramientas están diseñadas para detectar y responder de manera automatizada ante ataques cibernéticos. El estudio se llevó a cabo mediante ambientes controlados simulando los ataques cibernéticos más comunes con la finalidad de evaluar y analizar métricas clave como, tasa de detección, tiempo de respuesta, tasa de falsos positivos y tasa de respuestas automatizadas. Mediante dichas simulaciones controladas se logró reconocer las capacidades de estas soluciones para centralizar la seguridad, vincular eventos y automatizar respuestas de forma eficaz.

Los hallazgos no solo corroboraron la efectividad de las soluciones SIEM de código abierto, sino que también evidenciaron su capacidad para cambiar el modo en que las entidades abordan las amenazas cibernéticas. Estas herramientas se muestran como una solución eficiente, accesible y potente frente a los retos de la era digital actual, proporcionando una protección robusta y flexible ante escenarios de riesgos cada vez más complicados. Este trabajo no solo propone un estudio técnico, sino que también aspira a motivar la implementación de tecnologías que fortalezcan a las organizaciones en su batalla contra los ciberataques y los ciberdelincuentes.

Palabras clave: SIEM; detección; respuesta automatizada; ciberseguridad.

Abstract

This article arises as a final product of the thesis work on the topic of Analysis of the performance of open source SIEM solutions for the detection and automated response to cyber threats. The objective of the research is to evaluate the performance of various open source SIEM solutions, these tools are designed to detect and respond automatically to cyber attacks. The study was carried out through controlled environments simulating the most common cyber attacks in order to evaluate and analyze key metrics such as detection rate, response time, false positive rate and automated response rate. Through these controlled simulations, it was possible to recognize the capabilities of these solutions to centralize security, link events and automate responses effectively.

The findings not only corroborated the effectiveness of open source SIEM solutions, but also demonstrated their ability to change the way entities address cyber threats. These tools are presented as an efficient, accessible and powerful solution to the challenges of the current digital era, providing robust and flexible protection against increasingly complicated risk scenarios. This work not only proposes a technical study, but also aims to motivate the implementation of technologies that strengthen organizations in their battle against cyberattacks and cybercriminals.
Keywords: SIEM; detection; automated response; cybersecurity.

Resumo

Este artigo surge como produto final do trabalho de tese que tem como tema Análise do desempenho de soluções SIEM de código aberto para deteção e resposta automatizada a ciberameaças O objetivo da investigação é avaliar o desempenho de várias soluções SIEM de código aberto, Estas ferramentas são concebidas para detetar e responder automaticamente a ataques cibernéticos. O estudo foi realizado utilizando ambientes controlados simulando os ciberataques mais comuns para avaliar e analisar métricas importantes, como a taxa de deteção, o tempo de resposta, a taxa de falsos positivos e a taxa de resposta automatizada. Através destas simulações controladas, foi possível reconhecer as capacidades destas soluções para centralizar a segurança, ligar eventos e automatizar respostas de forma eficaz.

As descobertas não só corroboraram a eficácia das soluções SIEM de código aberto, como também demonstraram a sua capacidade de mudar a forma como as organizações lidam com as ciberameaças. Estas ferramentas apresentam-se como uma solução eficiente, acessível e poderosa para os desafios da atual era digital, proporcionando uma proteção robusta e flexível contra cenários de risco cada vez mais complicados. Este trabalho não propõe apenas um estudo técnico, mas também visa motivar a implementação de tecnologias que fortaleçam as organizações no combate aos ciberataques e aos cibercriminosos.
Palavras-chave: SIEM; detecção; resposta automatizada; cibersegurança.

Introducción

Una amenaza cibernética representa un riesgo crítico que compromete sistemas y datos, afectando directamente a personas y organizaciones. Se ha registrado un aumento alarmante en los informes sobre incidentes cibernéticos, evidenciando un creciente número de cuentas comprometidas y los

devastadores impactos en la reputación de las organizaciones, comprometiendo uno de los activos digitales más valiosos: la información.

Según IBM (2024) en su informe anual sobre el costo de las brechas en la seguridad de la información, la vulneración de datos aumento su costo en un 10% con respecto al año anterior alcanzando los 4,88 millones de dólares en pérdidas, debido a este panorama las organizaciones se enfrentan a la necesidad de buscar soluciones efectivas a mediano y largo plazo con respecto a la protección de su información.

Según Check Point Software (s. f.) entre los principales tipos de amenazas de ciberseguridad a las que se enfrentan las organizaciones se destacan el malware, la ingeniera social, los exploits de aplicaciones web, los ataques a la cadena de suministro, los ataques DoS (denegación de servicios) y los ataques de intermediario (men in the middle).

Merello Cruz y Hidalgo Ramírez (2019) indican que “una amenaza se la puede considerar como un incidente de alto peligro y que se vale de una vulnerabilidad del sistema o activo de información para ocasionar daños graves a la organización” (pág. 96), por lo tanto, se puede afirmar que las amenazas representan un factor crítico en la gestión de la seguridad de la información dentro de las organizaciones. Este escenario ha llevado a las organizaciones a buscar soluciones robustas, confiables y eficaces que les permitan mitigar y responder oportunamente a estas amenazas.

Ante estos desafíos, las organizaciones han comenzado a adoptar herramientas avanzadas de seguridad como las soluciones SIEM (Gestión de Información y Eventos de Seguridad, por sus siglas en inglés) para mitigar los riesgos asociados a las brechas de seguridad. Un SIEM permite recopilar, analizar y gestionar los datos de seguridad generados por sistemas y aplicaciones en tiempo real. Estas herramientas no solo ayudan a detectar y responder de manera eficaz a los incidentes de seguridad, sino que también proporcionan un control centralizado y una correlación automatizada de eventos, posicionándose como una solución integral frente a las amenazas cibernéticas.

Pino Medina (2021) especifica que cualquier proceso llevado a cabo por una máquina puede considerarse automatización, esto incluye también el uso de máquinas para operar herramientas de seguridad y sistemas de TI como parte de la "respuesta a incidentes". En este sentido, los SIEM no solo automatizan la recolección y análisis de eventos, sino que también facilitan la respuesta a incidentes, lo que mejora la eficiencia y reduce los tiempos de reacción ante posibles amenazas.

Como menciona Nacimba Loachamín (2023) existen diversas recomendaciones y mejores prácticas, como firewalls y sistemas de prevención, para mitigar amenazas cibernéticas, sin embargo, presentan desafíos importantes, como la gestión de múltiples interfaces, la acumulación masiva de registros de eventos que a menudo no son analizados de manera eficiente y la falta de personal capacitado para gestionar estos sistemas. Es por ello que las soluciones SIEM han surgido como herramientas esenciales para superar estos desafíos al centralizar y correlacionar eventos de seguridad en una plataforma única.

Quintero Martínez y Tovar Balderas (2019) describen a los SIEM como sistemas que recopilan datos de eventos de diversos dispositivos y, al correlacionar esta información, emiten alertas y generan informes que ayudan a las organizaciones a tomar decisiones informadas para proteger la confidencialidad, integridad y disponibilidad de sus datos.

Este trabajo se centrará en la evaluación de soluciones SIEM de código abierto, específicamente enfocándose en el análisis de rendimiento para la detección y respuesta automatizada ante amenazas cibernéticas. Se analizarán herramientas SIEM de código abierto, las cuales serán evaluadas en entornos simulados de ataques cibernéticos para medir su efectividad en la detección de amenazas y la automatización de las respuestas. Se incluirán simulaciones de diversos tipos de ataques, como fuerza bruta, malware y ataques de DoS. Además, se configurará un entorno de prueba controlado en una máquina virtual para llevar a cabo estas simulaciones.

Metodología

Dentro de lo que es la ciberseguridad el análisis de las soluciones SIEM requiere un enfoque detallado y bien estructurado. El presente estudio se centra en la evaluación práctica de soluciones SIEM de código abierto, con el propósito de analizar su efectividad en la detección y respuesta automatizada a amenazas cibernéticas en entornos simulados. El objetivo es no solo generar y contribuir al conocimiento teórico, sino también aplicarlo en situaciones prácticas simuladas, realizando pruebas de ataques y situaciones de amenazas similares a las que las organizaciones enfrentan en condiciones cotidianas. Dado que el objetivo principal es analizar el rendimiento de estas soluciones, se ha adoptado un enfoque cuantitativo. En esta fase cuantitativa, se medirán y compararán la eficiencia de distintas herramientas de código abierto mediante indicadores como la tasa de detección, el tiempo de respuesta, la tasa de falsos positivos y la tasa de respuestas automatizadas, como se visualiza en la Tabla 1.

Tabla 1. *Métricas para evaluar el rendimiento de un SIEM*

Métrica	**Fórmula**	**Unidad de medida**	**Descripción**
Tasa de detección	Tasa de detección $= \left(\frac{\text{Incidentes detectadas}}{\text{Incidentes Totales}}\right) \text{x } 100$	porcentaje (%)	Es el porcentaje de incidentes de seguridad reales que el sistema identifica correctamente.
Tiempo de respuesta	Tiempo de respuesta $= \frac{\text{Tiempo total a responder incidentes}}{\text{Número de incidentes respondidos}}$	segundos (s)	Es el período que sucede desde que se detecta una amenaza hasta que se toma una acción efectiva para mitigarla
Tasa de falsos positivos	Tasa de falsos positivos $= \left(\frac{\text{Alertas falsas}}{\text{Alertas totales}}\right) * 100$	porcentaje (%)	Es el porcentaje de alertas generadas que, tras su análisis.
Tasa de Respuestas Automatizadas	Tasa de Respuestas Automatizadas $= \left(\frac{\text{Número de respuestas automatizadas}}{\text{Número total de respuestas}}\right) * 100$	porcentaje (%)	Es el porcentaje de incidentes de seguridad que el sistema resuelve de manera automática sin intervención humana.

A continuación, se presenta el procedimiento de la investigación que consistió en crear un entorno simulado que permitiera evaluar el rendimiento de las soluciones SIEM.

Fase 1: Implementación de ambiente controlado

Para llevar a cabo este análisis se diseñó un entorno controlado utilizando VirtualBox donde se instalaron varias máquinas virtuales, este entorno simula una infraestructura empresarial que incluye servidores de correo, archivos, bases de datos, y la máquina destinada a funcionar como el servidor SIEM. Además, se incorporaron dos estaciones de trabajo, una telefonía IP y una máquina que tiene como sistema operativo Kali Linux el cual va a simular los ataques cibernéticos. Para simular y gestionar de manera efectiva esta red interna se utilizó GNS3, lo que permitió enlazar todas las máquinas virtuales en una red segura y estable, como se visualiza en figura 1.

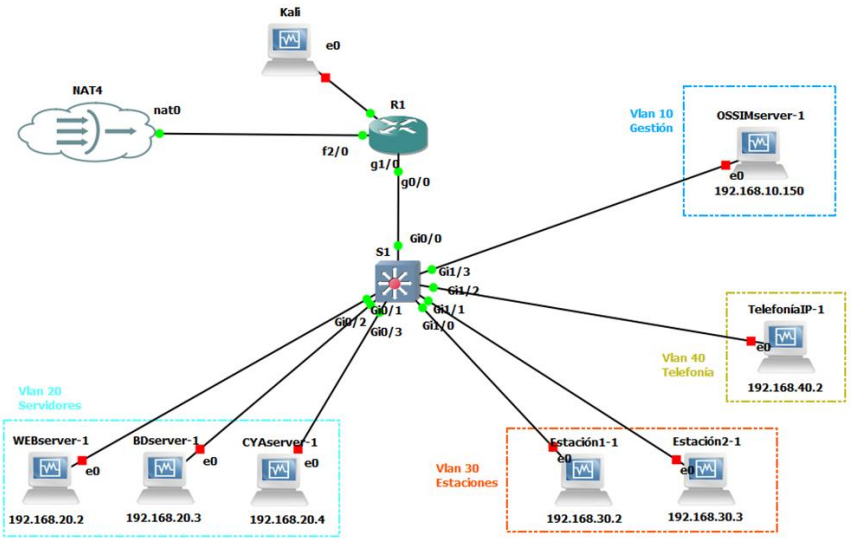

Figura 1. *Desarrollo GNS3*

Fase 2: Configuración de dispositivos virtuales en GNS3 para enrutamiento entre VLANs y acceso a internet

Se configuran subinterfaces en el router con encapsulación dot1Q para el enrutamiento entre VLANs, cada subinterfaz representa una VLAN específica y se le ha asignado una dirección IP: VLAN 10 (SIEM) con 192.168.10.1, VLAN 20 (Servidores) con 192.168.20.1, VLAN 30 (Estaciones de trabajo) con 192.168.30.1, y VLAN 40 (Telefonía) con 192.168.40.1. En el switch, se crean las VLANs correspondientes y se asignan a los puertos en modo acceso. Se configura un puerto trunk con el protocolo dot1Q para permitir la comunicación entre VLANs y se habilita Rapid PVST para garantizar una convergencia rápida y evitar bucles, manteniendo una topología estable. Para la configuración de NAT, se ajusta la interfaz externa del router para que obtenga una dirección IP automáticamente mediante DHCP. El NAT dinámico se configura con una lista de acceso que permite el tráfico de las subredes de las VLANs y la opción overload para compartir una IP pública entre varios dispositivos internos. Las subinterfaces correspondientes a las VLANs se marcan como "inside", mientras que la interfaz externa se marca como "outside". Finalmente, se añade una ruta por defecto para dirigir el tráfico desconocido a Internet, tal como se visualiza en la figura 2.

Figura 2. *Configuración de NAT en el router*

Fase 3: Instalación y Configuración de Servicios de Infraestructura en el Proyecto de Simulación

El proceso de instalación y configuración de servicios en la simulación comenzó con la implementación de un servidor web Apache sobre Ubuntu, donde se comprobó su correcto funcionamiento creando una página web de prueba. Luego, se instaló y configuró MySQL para gestionar bases de datos, con acceso seguro mediante usuario y contraseña, y se utilizó phpMyAdmin para facilitar su administración, tal como se visualiza en la figura 3.

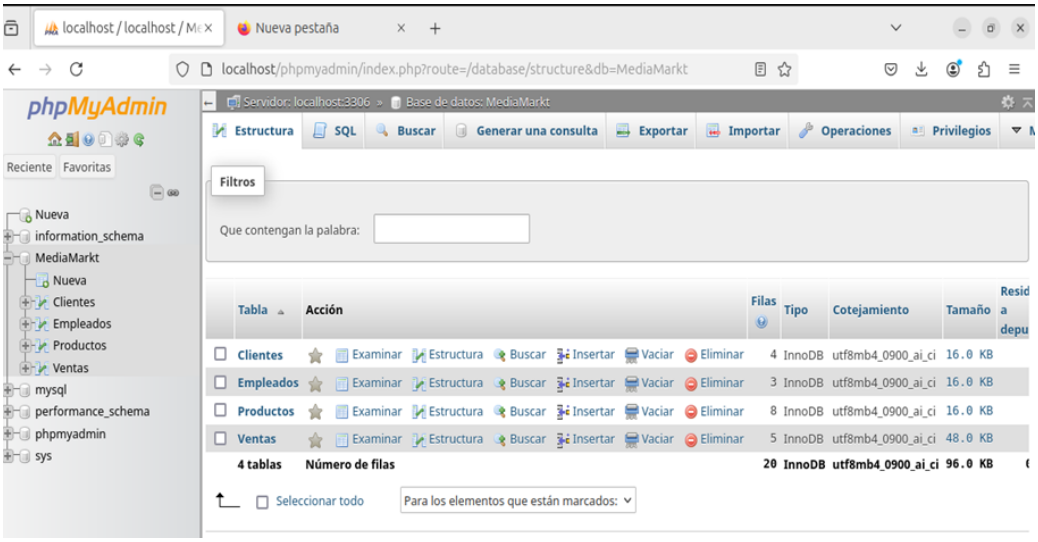

Figura 3. *Vista de la base de datos en phpMyAdmin*

Pol. Con. (Edición núm. 102) Vol. 10, No 1, Enero 2025, pp. 2233-2250, ISSN: 2550 - 682X

En el servidor de archivos, se configuró Samba para compartir carpetas por departamento, implementando control de acceso mediante permisos específicos. También se configuró un servidor de correo utilizando Postfix, Dovecot y SquirrelMail, creando cuentas de usuario para gestionar el envío y recepción de correos electrónicos. Luego, se instaló y configuró el sistema de telefonía IP Issabel PBX, donde se gestionaron extensiones y se habilitó la grabación de llamadas para asegurar el registro de comunicaciones dentro de la red telefónica, tal como se visualiza en la figura 4.

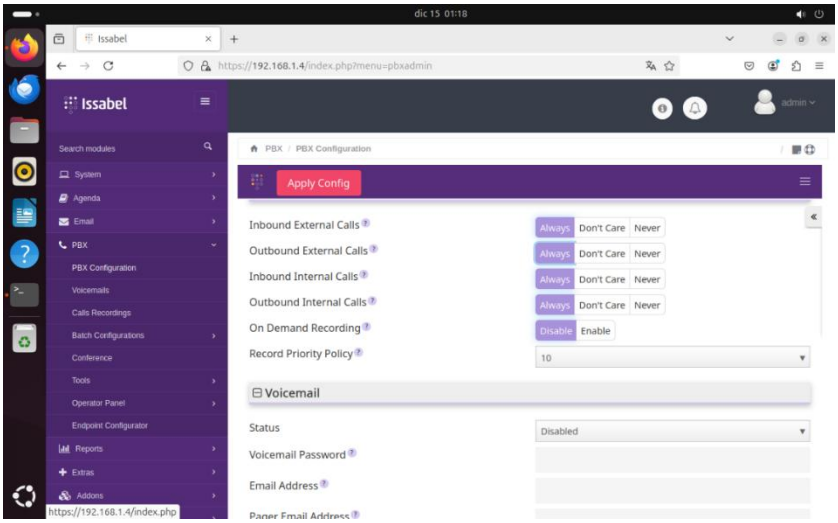

Figura 4. *Opciones para habilitar o deshabilitar la grabación de llamadas en Issabel*

Por último, se instaló Kali Linux en una máquina virtual para simular ataques cibernéticos, dada su eficacia en pruebas de penetración. La instalación fue sencilla, configurando solo opciones básicas como idioma y zona horaria. Con Kali Linux listo, se prepararon las herramientas necesarias para ejecutar un ataque, simulando así los intentos de un atacante por vulnerar la red, tal como se visualiza en la figura 5.

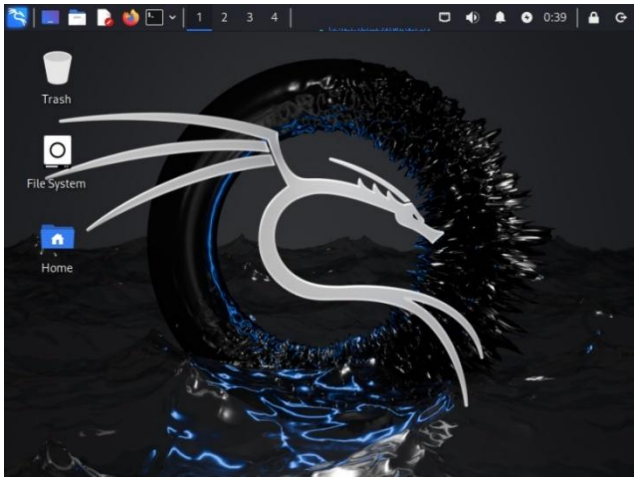

Figura 5. *Pantalla de inicio de Kali Linux*

Fase 4: Instalación y configuración de SIEM

Opción 1: AlienVault OSSIM

Se instaló el SIEM AlienVault OSSIM versión 5.8.11 en VirtualBox con Debian x64. Durante la instalación, se configuró la subred (192.168.10.150/24), el reloj y el usuario root. Posteriormente, se reinició la máquina. Para gestionar los logs de dispositivos finales, se configuró un sensor con OSSIM en la dirección IP 192.168.10.151. En la interfaz web de OSSIM, se crearon cuentas para agregar dispositivos mediante escaneo, permitiendo visualizar detalles como hostname, IP, tipo de dispositivo, sistema operativo y estado de los sistemas de detección de intrusiones, tal como se visualiza en la figura 6.

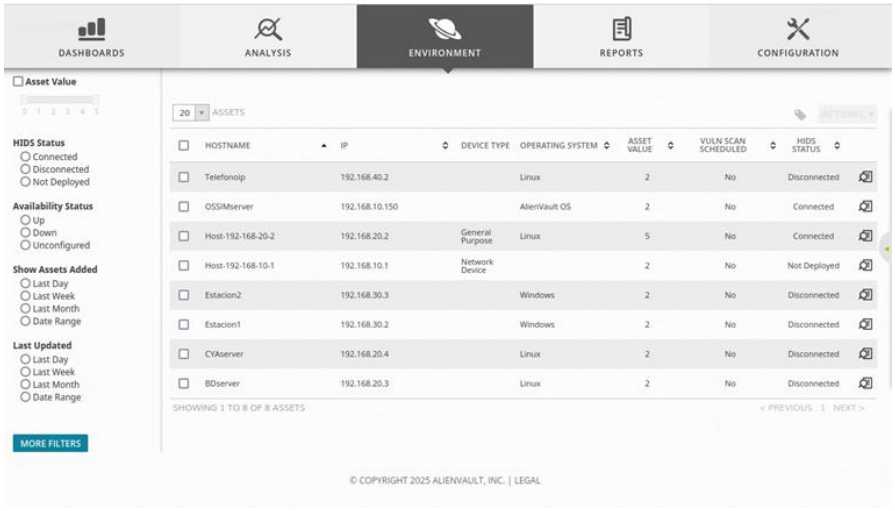

Figura 6. *Dashboard de OSSIM con los agentes disponibles para monitoreo*

Pol. Con. (Edición núm. 102) Vol. 10, No 1, Enero 2025, pp. 2233-2250, ISSN: 2550 - 682X

Simulación de Ataques y Respuestas Automatizadas en OSSIM

Se simularon varios tipos de ataques utilizando Kali Linux, comenzando con un escaneo de puertos con Nmap, que fue reconocido por OSSIM al detectar intentos de escanear puertos SSH. Posteriormente, se realizó un ataque de fuerza bruta con Hydra, lo que generó alertas en OSSIM detallando los intentos de acceso no autorizado. Para evaluar vulnerabilidades, se utilizó Nikto, revelando configuraciones inseguras en el servidor y activando alertas de explotación. Se simuló también un ataque DoS con Slowloris y explotación de directorios con Gobuster, ambos detectados por OSSIM, tal como se visualiza en la figura 7.

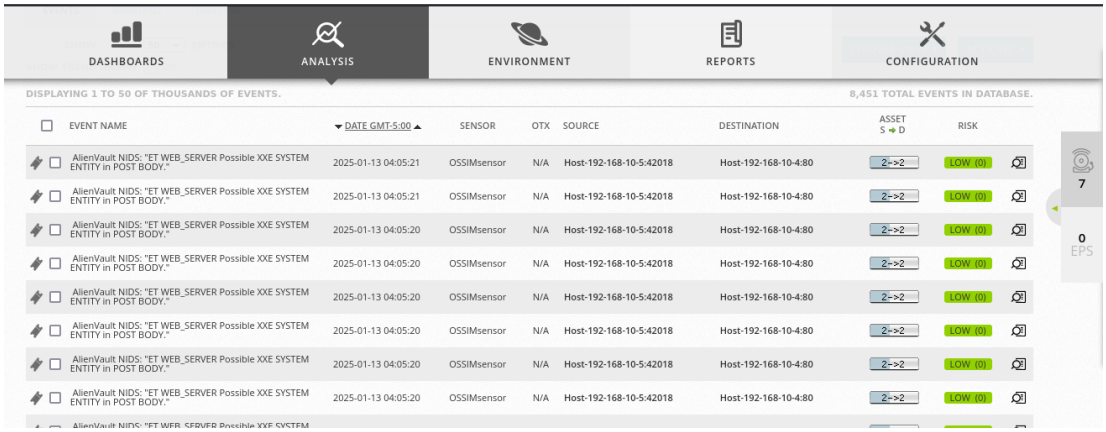

Figura 7. *Eventos generados en OSSIM*

Además, se implementaron respuestas automatizadas para mejorar la eficiencia en la gestión de incidentes, como la creación automática de tickets y un script para bloquear IPs comprometidas, lo cual fue confirmado mediante la interfaz de OSSIM. Esto optimizó la respuesta ante eventos de seguridad y mejoró la administración de incidentes, tal como se visualiza en la figura 8.

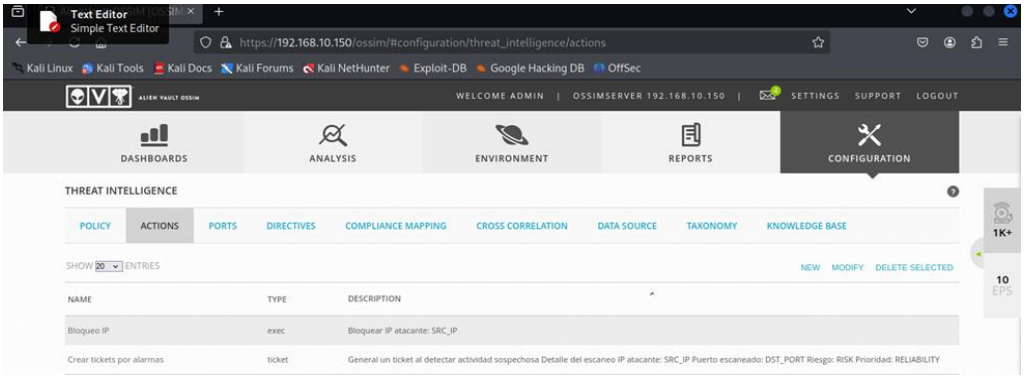

Figura 8. *Comprobación de las acciones creadas*

Opción 2: Wazuh SIEM

La instalación del SIEM Wazuh versión 4.9.2 fue directa y eficiente, siguiendo la documentación oficial y comandos en Red Hat Enterprise Linux 8.8. Después de completar la instalación inicial, se procedió a agregar agentes a través de la interfaz de Wazuh, seleccionando el sistema operativo correspondiente. Los comandos generados para instalar los agentes fueron ejecutados en las máquinas objetivo y al finalizar se verificó que los agentes estuvieran registrados correctamente en la plataforma, confirmando su funcionamiento adecuado en el sistema de monitoreo, tal como se visualiza en la figura 9.

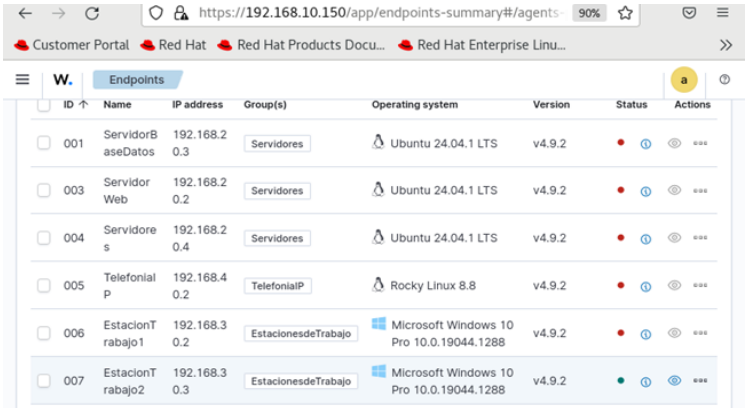

Figura 9. *Panel de control con los agentes instalados*

Simulación de Ataques y Análisis de Eventos Detectados en Wazuh

Para evaluar la capacidad de detección de Wazuh, se simularon varios ataques y acciones no autorizadas. Primero, se intentó detener y reiniciar el servicio del agente Wazuh, lo que generó alertas críticas. Luego, se realizó un intento de explotación de vulnerabilidades utilizando SSH y un ataque de fuerza bruta con Hydra, ambos detectados por Wazuh, quien generó alertas en tiempo real. También se llevó a cabo un escaneo de vulnerabilidades con Nikto, lo cual fue registrado por Wazuh asociándolo con la técnica MITRE ATT&CK. Además, se simuló un ataque con malware usando msfvenom, y Wazuh detectó la ejecución de un archivo malicioso, generando alertas correspondientes. Finalmente, se configuró un firewall para bloquear accesos no autorizados, lo que activó alertas de respuesta automática en Wazuh. Todos los eventos fueron registrados en tiempo real, lo que permitió monitorear la efectividad de Wazuh en la detección y respuesta ante diversas amenazas, tal como se visualiza en la figura 10.

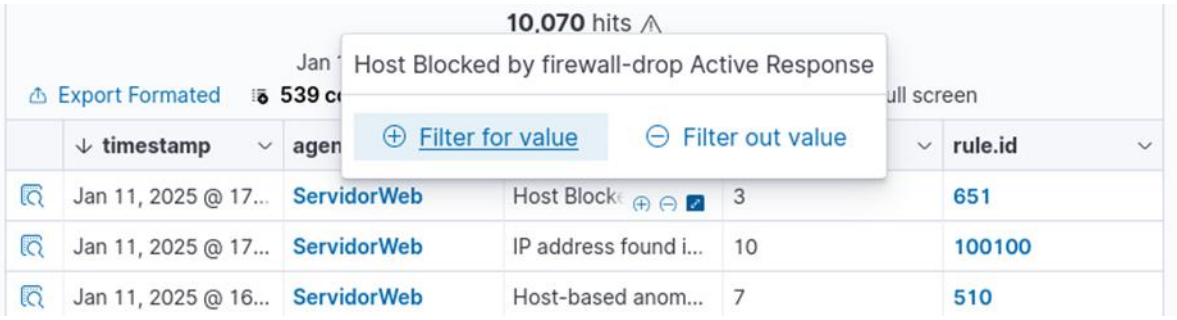

Figura 10. *Detección de IP maliciosa, bloqueo de host y anomalía en ServidorWeb*

Opción 3: SIEM Splunk

Se instaló Splunk en un entorno de prueba utilizando el comando oficial para descargar la versión 9.4.0 de Splunk para Linux. Aunque Splunk no ofrece el código fuente completo, se utilizó el componente de código abierto Splunk Universal Forwarder para la recopilación y envío de datos desde diversas fuentes hacia la instancia central de Splunk. La interfaz web de Splunk proporciona herramientas avanzadas para visualizar los datos de manera eficiente, incluyendo gráficos y alertas en tiempo real. Además, se configuró el Splunk Universal Forwarder para enviar logs y eventos a la instancia centralizada de Splunk, permitiendo realizar búsquedas detalladas y obtener información valiosa para el análisis de seguridad y gestión de incidentes, tal como se visualiza en la figura 11.

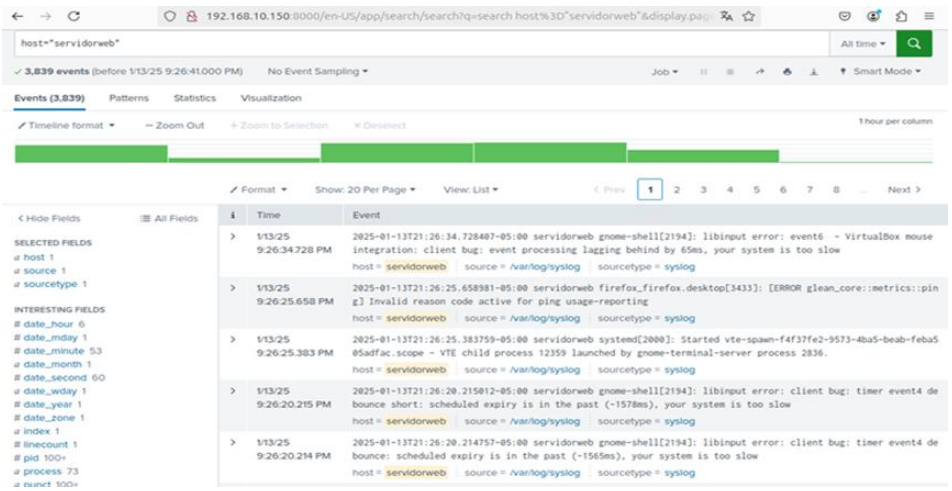

Figura 11. *Visualización de datos recolectados por el Splunk Forwarder*

Pol. Con. (Edición núm. 102) Vol. 10, No 1, Enero 2025, pp. 2233-2250, ISSN: 2550 - 682X

Simulación de Ataques y Detección de Eventos en Splunk

Se simularon varios ataques para evaluar la capacidad de detección de Splunk. El primer ataque consistió en detener el servicio del Splunk Universal Forwarder, lo que generó alertas sobre la pérdida de conexión y fallos en la recopilación de datos. Posteriormente, se realizó un ataque SSH mediante intentos de acceso no autorizado, lo que fue detectado en tiempo real a través de intentos fallidos de autenticación en los logs del servidor. También se ejecutó un escaneo de vulnerabilidades con Nikto, lo que generó registros detallados sobre las solicitudes y respuestas del servidor web. Finalmente, se simuló un ataque de malware que implicó la creación de un usuario no autorizado y la modificación de configuraciones del sistema, detectado por Splunk gracias a su monitoreo de actividades sospechosas, tal como se visualiza en la figura 12.

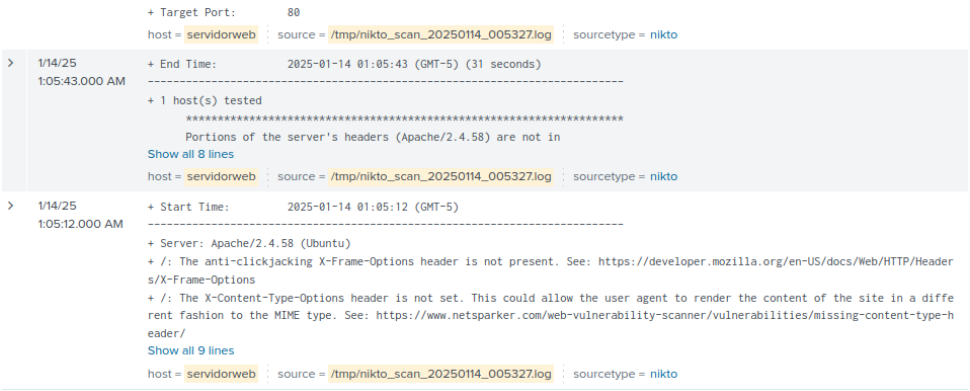

Figura 12. *Visualización de los resultados del escaneo Nikto en Splunk*

Resultados y discusión

Para evaluar el rendimiento de las soluciones SIEM analizadas, se utilizaron métricas clave que permiten medir la eficiencia en la tasa de detección, tiempo de respuesta, tasa de falso positivos y tasa de respuestas automatizadas. Estas métricas calculadas a partir de los datos recopilados durante las simulaciones en un entorno controlado, proporcionan un análisis cuantitativo que respalda las conclusiones del estudio, tal como se visualiza en tabla 2.

Tabla 2. *Comparativa del Rendimiento de Soluciones SIEM*

SIEM	Tasa de detección (%)	Tiempo de respuesta (seg)	Tasa de falsos positivos (%)	Tasa de respuestas automatizadas (%)
OSSIM	100.0	18.0	10.0	100.0
Wazuh	100.0	6.0	10.0	100.0
Splunk	90.0	12	20.0	0.0

Basándose en los resultados obtenidos, podemos deducir que Wazuh es el mejor SIEM en términos de rapidez de detección y respuesta, destacándose también por su alta tasa de automatización y su baja tasa de falsos positivos. Por otro lado, AlienVault OSSIM es una opción igualmente válida, aunque su tiempo de respuesta es ligeramente más lento en comparación con Wazuh. En cuanto a Splunk, aunque presenta un buen rendimiento en algunos aspectos, queda rezagado debido a su menor tasa de detección, una mayor tasa de falsos positivos y la falta de automatización en las respuestas.

Investigaciones anteriores

Los resultados obtenidos en esta investigación han sido respaldados por diversos estudios previos, lo que refuerza la validez de nuestros hallazgos. Esto respalda las conclusiones obtenidas en investigaciones previas como el trabajo de Gálvez Soriano (2024), que también subraya la importancia de Wazuh en la mejora de la visibilidad y el control en tiempo real de la infraestructura tecnológica.

En cuanto al trabajo de Herrera (2024), su estudio resalta la importancia de personalizar las configuraciones de los SIEMs de acuerdo con las amenazas específicas a las que se enfrenta cada organización. Su estudio se centra en la implementación de un SIEM para la defensa activa frente a intrusiones en la red, un enfoque que resulta también clave para nuestra investigación. Este enfoque resalta la necesidad de que las organizaciones adapten tanto las reglas como las herramientas de seguridad a sus circunstancias particulares, con el fin de mejorar la efectividad del monitoreo y la respuesta ante incidentes.

Por otro lado, el trabajo de Morales Morera y Sanabria Echeverría (2020) enfatiza la falta de guías estandarizadas y la capacitación adecuada, lo que limita la capacidad de respuesta ante incidentes de seguridad, un desafío que también hemos identificado en nuestra investigación. En nuestro estudio, hemos implementado un proceso estructurado para optimizar las reglas de correlación y

mejorar la capacidad de detección de amenazas, siguiendo un enfoque similar al propuesto por estos autores.

Asimismo, el modelo utilizado por Agudelo Castro et al. (2022) para la creación de los casos de uso proporciona una base sólida para definir métricas de evaluación de las soluciones SIEM. Este modelo detalla los parámetros esenciales para cada caso de uso como el objetivo, alcance, fuentes de eventos, flujo lógico, notificación y severidad, lo que contribuye a la formulación de métricas específicas para evaluar el rendimiento de las herramientas SIEM en nuestro estudio. Este trabajo refuerza la importancia de personalizar las soluciones SIEM de acuerdo a las necesidades particulares de cada entorno, y cómo las mejores prácticas y modelos utilizados en investigaciones previas pueden servir como guía para optimizar la implementación de estas herramientas en la detección y respuesta ante amenazas cibernéticas.

Conclusiones

- El resultado del estudio nos permitió identificar las fortalezas y debilidades específicas de cada herramienta con lo que respecta a las métricas definidas y mencionadas con anterioridad. En la tasa de detección, OSSIM y Wazuh demostraron una efectividad del 100% en comparación con Splunk que demostró una efectividad del 90%, aunque con una ligera diferencia en relación con las otras herramientas, aún demostró un excelente desempeño.
- En la evaluación del tiempo de respuesta, Wazuh se destaca con un promedio de respuesta notablemente inferior a 6 segundos, posicionándose como la herramienta más rápida para manejar incidentes. OSSIM, con un tiempo de 18 segundos, y Splunk, con 13. 33 segundos, tienen tiempos de respuesta más prolongados en comparación con la anterior. Recordando que un tiempo de respuesta más corto es crucial al momento de mitigar los impactos de una brecha de seguridad.
- OSSIM y Wazuh alcanzaron una tasa de falsos positivos del 10%, demostrando una capacidad adecuada para reducir alertas innecesarias y mejorar el análisis de amenazas.
- Se puede afirmar que Wazuh se posiciona como la solución más equilibrada, sobresaliendo en la rapidez de respuesta y manteniendo altos índices de detección, con una baja tasa de falsos positivos y una completa automatización.

Referencias

1. IBM. (2024). Cost of a Data Breach Report 2024. No. 19a edición. https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec
2. Check Point Software. (s. f.). Las 6 principales amenazas a la ciberseguridad. Check Point Software. Recuperado 26 de octubre de 2024, de https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-cybersecurity/top-6-cybersecurity-threats/
3. Merello Cruz, C., & Hidalgo Ramírez, D. (2019). Análisis de riesgos tecnológicos para la plataforma informática de un hospital del sector público de la ciudad de Guayaquil [Universidad de Guayaquil]. https://repositorio.ug.edu.ec/server/api/core/bitstreams/9da986cd-991a-4b59-9b64-a03908880b9a/content
4. Pino Medina, A. (2021). Plataformas SOAR. Respuesta orquestada y automatizada de la seguridad [Tesis de maestría, Universitat Oberta de Catalunya].: http://hdl.handle.net/10609/132128
5. Nacimba Loachamín, P. F. (2023). Análisis comparativo de plataformas de SIEM y las soluciones de detección y respuesta extendida [Tesis de maestría, Universidad de Israel]. http://repositorio.uisrael.edu.ec/handle/47000/3558
6. Quintero Martínez, M. I., & Tovar Balderas, S. A. (2019). Sistema de Gestión de Información y Eventos de Seguridad (SIEM). TIES, Revista de Tecnología e Innovación en Educación Superior, 2, 9. https://doi.org/10.22201/dgtic.26832968e.2019.2.3
7. Gálvez Soriano, P. (2024). Despliegue e implantación de un SIEM con Wazuh [Universidad Politécnica de Catalunya]. http://hdl.handle.net/2117/418178
8. Herrera, D. (2024). Implementación de un SIEM para la defensa activa ante un ataque de denegación de servicio. http://bibdigital.epn.edu.ec/handle/15000/25842
9. Morales Morera, R., & Sanabria Echeverría, E. (2020). Casos de uso resilientes SIEM. Universidad Cenfotec.
10. Agudelo Castro, B. A., Álvarez Yépez, D. J., Andrade Valdez, J. A., & Escobar Tucta, J. M. (2022). Elaboración de 5 Casos de Uso para Plataforma SIEM Institucional en el Sector Financiero a ser implementado por la empresa de Seguridad Informática Secure Soft [Tesis

de maestría, Universidad Internacional del Ecuador]. https://repositorio.uide.edu.ec/handle/37000/5610