ISBN: 978-628-96613-3-0. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2026.1.1.1425

Cyberattack Detection and Mitigation in a Security Operations Center (SOC) Using Free Software SIEM Tools in Kali Purple

José Fernando Espinoza León[1]
[1]Servicio Nacional de Adiestramiento en Trabajo Industrial (SENATI), Perú, jespinozal@senati.pe

Abstract– *The continuous growth and increasing sophistication of cyber threats have strengthened the need for advanced monitoring, detection, and incident response mechanisms in Security Operations Centers (SOC). In this context, Security Information and Event Management (SIEM) systems play a key role in event correlation and threat detection. This paper presents the design, implementation, and experimental evaluation of a SOC laboratory environment based on Kali Purple, focused on assessing the performance of open-source SIEM tools. The environment integrates Wazuh, Suricata, Zeek, Elastic Stack, and TheHive. Controlled attack scenarios were executed, including SSH brute force, DNS tunneling, and HTTP command-and-control (C2). The evaluation was conducted using quantitative metrics such as True Positive Rate (TPR), False Positive Rate (FPR), Mean Time to Detect (MTTD), and Mean Time to Respond (MTTR). The results demonstrate high detection accuracy (TPR up to 0.98) and low false positive rates (below 0.03), confirming the effectiveness of the proposed approach in controlled environments.*

Keywords- *Security Operations Center; SIEM; Kali Purple; Open-Source Software; Threat Detection; Incident Response.*

Búsqueda y mitigación de ciberataques en un centro de operaciones de seguridad (SOC) mediante herramientas SIEM de software libre en Kali Purple

José Fernando Espinoza León[1]
[1]Servicio Nacional de Adiestramiento en Trabajo Industrial (SENATI), Perú, jespinozal@senati.pe

Resumen– El crecimiento continuo y la creciente sofisticación de las amenazas cibernéticas han reforzado la necesidad de mecanismos avanzados de monitoreo, detección y respuesta a incidentes en los Centros de Operaciones de Seguridad (SOC). En este contexto, los sistemas de Gestión de Información y Eventos de Seguridad (SIEM) desempeñan un papel clave en la correlación de eventos y la detección de amenazas. Este artículo presenta el diseño, implementación y evaluación experimental de un entorno de laboratorio SOC basado en Kali Purple, enfocado en evaluar el desempeño de herramientas SIEM de software libre. El entorno integra Wazuh, Suricata, Zeek, Elastic Stack y TheHive. Se ejecutaron escenarios de ataque controlados, incluyendo fuerza bruta SSH, túneles DNS y comunicación de comando y control (C2) sobre HTTP. La evaluación se realizó mediante métricas cuantitativas como la tasa de verdaderos positivos (TPR), tasa de falsos positivos (FPR), tiempo medio de detección (MTTD) y tiempo medio de respuesta (MTTR). Los resultados evidencian una alta precisión en la detección (TPR de hasta 0.98) y bajas tasas de falsos positivos (menores a 0.03), confirmando la efectividad del enfoque propuesto en entornos controlados.

Palabras clave - Centro de Operaciones de Seguridad; SIEM; Kali Purple; Software Libre; Detección de Amenazas; Respuesta a Incidentes.

I. INTRODUCCIÓN

Los Centros de Operaciones de Seguridad (SOC) desempeñan un papel fundamental en la protección de infraestructuras digitales modernas, proporcionando capacidades de monitoreo continuo, detección de amenazas y respuesta a incidentes [1]. En este contexto, los sistemas de Gestión de Información y Eventos de Seguridad (SIEM) permiten centralizar la recolección de registros, correlacionar eventos y generar alertas, facilitando una detección oportuna de actividades maliciosas [2].

Las herramientas privativas dominan el mercado, pero las soluciones de software libre y código abierto (FOSS) han madurado lo suficiente como para competir en capacidades avanzadas [3].

Kali Purple es una edición especializada dentro de la metadistro Kali Linux la cual está basada en la distribución Debian GNU/Linux. Kali Linux está orientada principalmente a Red Team / Pentesting y Kali Purple esta enfocada en Blue Team, que actúa como un SOC in-a-box es decir un SOC listo para usar, empaquetado con herramientas de defensa, detección y respuesta preintegradas. En este contexto, la metadistro Kali Purple anunciada oficialmente en 2023 por Offensive Security agrega un ecosistema probado de aplicaciones defensivas al reconocible Kali Linux, otra metadistro con otro enfoque.

Este trabajo de investigación documenta la creación de un laboratorio SOC sobre Kali Purple y la evaluación de su efectividad para la búsqueda y mitigación de ciberataques, empleando herramientas de software libre tales como Wazuh como motor de SIEM/EDR y Suricata como sistema de detección de intrusos en red (NIDS), junto con herramientas auxiliares.

Estudios recientes destacan la importancia del uso de métricas cuantitativas, como el Mean Time to Detect (MTTD) y el Mean Time to Respond (MTTR), para evaluar de manera objetiva la efectividad operativa de un SOC [4], [5]. Asimismo, marcos estandarizados de modelado de amenazas, como MITRE ATT&CK, se han consolidado como referencias para estructurar capacidades de detección y evaluar la cobertura defensiva en entornos académicos y organizacionales [6].

Si bien las soluciones SIEM comerciales dominan el mercado, las alternativas de software libre han alcanzado un nivel de madurez que permite su adopción en organizaciones de pequeña y mediana escala, así como en entornos educativos, debido a su flexibilidad y bajo costo [7]. En este escenario, Kali Purple surge como una plataforma defensiva integrada que facilita la implementación de entornos SOC basados en herramientas de código abierto [8].

Este estudio se guía por las siguientes preguntas de investigación (PI) :

PI1: ¿Cuál es la efectividad de las herramientas SIEM de software libre en la detección de ataques en un entorno SOC basado en Kali Purple?
PI2: ¿Cómo impacta la configuración de reglas personalizadas en la precisión de detección y reducción de falsos positivos?
PI3: ¿Qué tan eficientes son los tiempos de detección y respuesta en comparación con entornos SOC tradicionales?

Las principales contribuciones de este trabajo son:

1. El diseño e implementación de un entorno SOC reproducible basado en Kali Purple.
2. La evaluación cuantitativa de herramientas SIEM de software libre mediante métricas estándar.
3. La validación práctica mediante escenarios de ataque representativos.

Asimismo, se plantea la hipótesis de que un entorno SOC basado en herramientas FOSS correctamente configuradas puede alcanzar niveles de desempeño comparables a soluciones comerciales en escenarios controlados.

El presente artículo se organiza de la siguiente manera: la Sección II presenta el marco teórico, la Sección III describe la metodología empleada, la Sección IV presenta y discute los resultados, la Sección V expone las limitaciones del estudio y la Sección VI presenta las conclusiones.

II. Marco Teórico

A) Centro de Operaciones de Seguridad (SOC)

Un Centro de Operaciones de Seguridad es una instalación centralizada donde los analistas supervisan, analizan y responden a incidentes de ciberseguridad que afectan a la infraestructura tecnológica de una organización [1]. La efectividad de un SOC depende de procesos bien definidos, personal capacitado y del uso de métricas que permitan evaluar y mejorar su desempeño operativo [5].

B) SIEM

El SIEM unifica la gestión de eventos, proporcionando *correlación*, alertas y retención de registros [2]. Sus métricas clave incluyen *Mean Time to Detect* (MTTD) y *Mean Time to Respond* (MTTR).

Los sistemas SIEM proporcionan visibilidad unificada de los eventos de seguridad al correlacionar registros provenientes de múltiples fuentes heterogéneas, permitiendo la generación de alertas en tiempo casi real y el análisis forense posterior [2]. Investigaciones recientes resaltan la necesidad de evaluar el desempeño de estas plataformas mediante métricas objetivas que consideren la precisión de detección y los tiempos de respuesta [4].

C) Kali Purple

Kali Purple extiende Kali Linux con más de 100 herramientas defensivas pre-instaladas y playbooks basados en MITRE ATT&CK [14]. Incluye integraciones preconfiguradas con Elastic Stack y herramientas de análisis

D) MITRE ATT&CK

MITRE ATT&CK se ha consolidado como el marco predominante para modelar el comportamiento de los adversarios y estructurar estrategias de detección y respuesta en entornos SOC [6]. Su adopción permite mapear alertas a tácticas y técnicas específicas, facilitando la caza de amenazas, la evaluación de cobertura defensiva y la comparación entre distintos entornos de seguridad [9].

Adicionalmente, se presentan escenarios prácticos con el fin de validar la aplicabilidad del entorno SOC propuesto en situaciones representativas de operación real.

E) Software libre y entornos SOC educativos

Las soluciones SIEM de software libre han demostrado un nivel de madurez suficiente para soportar operaciones SOC funcionales, especialmente en organizaciones de pequeña y mediana escala y en laboratorios académicos [7]. Asimismo, diversos estudios destacan el valor de los entornos SOC educativos para la formación práctica de analistas de seguridad y la evaluación experimental de tecnologías defensivas [10].

F) Wazuh

Wazuh es un SIEM/EDR que combina la recolección de logs, análisis de integridad, detección de rootkits y correlación a través de reglas basadas en decodificadores y gestores de alertas [11].

G) Suricata

Suricata provee capacidades de NIDS/NIPS/NSM, inspeccionando tráfico en tiempo real mediante firmas y heurística basada en protocolos [12]. (Suricata, 2024). Su integración con Elastic Stack y Wazuh permite enriquecer alertas.

H) Otras herramientas complementarias

- **Elastic Stack (Elasticsearch, Logstash, Kibana, Beats)**: almacenamiento y visualización de eventos.
- **Zeek**: análisis de tráfico de red de alto nivel.
- **TheHive + Cortex**: plataforma de gestión de incidentes y automatización de análisis.

En este trabajo se emplean herramientas de software libre y de código abierto (FOSS), reconociendo que, si bien ambos conceptos no son equivalentes desde el punto de vista filosófico, comparten características técnicas que permiten su adopción en entornos SOC académicos y experimentales.

III. Metodología.

El presente estudio adopta una metodología experimental aplicada, desarrollada en un entorno de laboratorio SOC controlado. El enfoque metodológico se alinea con investigaciones previas sobre evaluación de desempeño en SOC, priorizando la reproducibilidad y el uso de métricas cuantitativas para medir la efectividad de detección y respuesta [4], [5].

Se diseñó un entorno de laboratorio que simula un SOC básico. Se desplegaron herramientas SIEM de software libre incluidas en Kali Purple, configurando fuentes de eventos, reglas de correlación y mecanismos de alerta. Posteriormente, se ejecutaron escenarios controlados de ataque con el fin de evaluar la capacidad de detección y respuesta del sistema.

3.1 Diseño del laboratorio

Se instaló Kali Purple 2026.1 sobre un hipervisor Proxmox con 16 GB RAM y 4 vCPU. Los contenedores Docker predeterminados para Elastic Stack y Wazuh se desplegaron mediante *kali-purple-deploy*. Suricata se configuró en modo *AF-Packet* para inspeccionar tráfico interno.

El entorno de laboratorio se implementó sobre Kali Purple como plataforma central, integrando herramientas de código abierto orientadas a operaciones SOC. Se utilizaron Wazuh v4.x para la gestión de eventos y correlación, Suricata v7.x como sistema de detección de intrusiones basado en red, Zeek v6.x para el análisis de tráfico y Elastic Stack v8.x para la visualización y análisis de datos. Esta integración permitió simular un flujo completo de monitoreo, detección y respuesta ante incidentes de seguridad en un entorno controlado.

3.2 Escenarios de ataque

Se recrearon tres vectores de amenaza:

1. *Fuerza bruta SSH*: 5 000 intentos/s desde Hydra.
2. *Exfiltración de datos vía túnel DNS*: script Dnscat2 transfiriendo un archivo de 5 MB.
3. *Malware HTTP emulando command-and-control (C2)* : *Caldera* ejecutando *agent sandcat*.

3.3 Caza de amenazas y reglas de detección

- Wazuh: reglas personalizadas basadas en *decoder file_integrity* y *rule 100001* para SSH.
- Suricata: firmas *ET ATTACK* modificadas y *thresholds* específicos.
- Zeek: *notice-policy* para tráfico DNS anómalo.

Los eventos se etiquetaron con ATT&CK IDs y se enriquecieron con GeoIP.

3.4 Métricas de evaluación

Definición formal de métricas:

El desempeño del entorno SOC fue evaluado mediante métricas cuantitativas estándar en la literatura de sistemas SIEM y SOC, incluyendo la Tasa de Verdaderos Positivos (TPR), la Tasa de Falsos Positivos (FPR), el Mean Time to Detect (MTTD) y el Mean Time to Respond (MTTR) [4], [5].

Para garantizar la validez experimental, se definió un conjunto de datos etiquetado (ground truth), donde cada evento generado durante los escenarios de ataque fue clasificado manualmente como evento malicioso o tráfico legítimo.

La Tasa de Verdaderos Positivos (TPR) se calculó como:

$$TPR = TP / (TP + FN)$$

donde TP corresponde al número de eventos de ataque correctamente detectados y FN a los eventos de ataque no detectados.

La Tasa de Falsos Positivos (FPR) se definió como:

$$FPR = FP / (FP + TN)$$

donde FP representa eventos benignos incorrectamente clasificados como maliciosos y TN eventos benignos correctamente ignorados.

Definición experimental:
Cada escenario fue ejecutado en 10 iteraciones independientes, generando un promedio de 5,000 a 10,000 eventos por escenario, con el fin de obtener resultados estadísticamente representativos. Se reportan valores promedio de TPR y FPR, así como los tiempos medios de detección (MTTD) y respuesta (MTTR), medidos en minutos desde la generación del evento hasta su identificación y resolución.

Adicionalmente, se calculó la precisión (Precision), el recall y la métrica F1 para evaluar de manera integral el desempeño del sistema de detección.

IV. Resultados y Discusión.

Los resultados obtenidos se presentan a partir de un análisis cuantitativo basado en múltiples ejecuciones de los escenarios de ataque definidos. Cada escenario fue ejecutado en 10 iteraciones independientes, generando conjuntos de eventos etiquetados (ground truth), lo que permitió construir matrices de confusión para evaluar el desempeño del sistema.

A. Matriz de confusión

Para cada escenario, los eventos fueron clasificados en cuatro categorías: verdaderos positivos (TP), falsos positivos (FP), verdaderos negativos (TN) y falsos negativos (FN). La Tabla I muestra un resumen consolidado de los resultados promedio obtenidos.

TABLA I
Matriz de confusión promedio por escenario de ataque

Escenario	TP	FP	TN	FN
Fuerza bruta SSH	980	20	1980	20
Exfiltración DNS	950	60	1940	50
Malware HTTP C2	960	40	1960	40

Estos resultados evidencian que el sistema presenta una alta capacidad de detección (TP) con una baja tasa de falsos positivos (FP), especialmente en escenarios con patrones repetitivos como ataques de fuerza bruta SSH.

Los resultados muestran una alta capacidad de detección en todos los escenarios evaluados, destacando el ataque de fuerza bruta SSH debido a la naturaleza repetitiva de sus patrones.

B. Métricas de desempeño

A partir de la matriz de confusión, se calcularon las métricas estándar de evaluación:

• Precisión (Precision): TP / (TP + FP)
• Recall (TPR): TP / (TP + FN)
• F1-score: 2 * (Precision * Recall) / (Precision + Recall)

La Tabla II presenta los valores promedio obtenidos.

TABLA II
Métricas de desempeño del sistema SOC

Escenario	Precisión	Recall (TPR)	F1-score	FPR
Fuerza bruta SSH	0.98	0.98	0.98	0.01
Exfiltración DNS	0.94	0.95	0.94	0.03
Malware HTTP C2	0.96	0.96	0.96	0.02

A partir de la matriz de confusión, se calcularon métricas de evaluación como precisión, recall (TPR), F1-score y tasa de falsos positivos (FPR).

Los resultados muestran que el sistema alcanza valores elevados de precisión y recall en todos los escenarios evaluados. El mejor desempeño se observa en el ataque de fuerza bruta SSH, debido a su naturaleza repetitiva y fácilmente identificable mediante reglas de correlación.

C. Análisis de tiempos operativos

El análisis de tiempos operativos se centró en dos métricas clave: Mean Time to Detect (MTTD) y Mean Time to Respond (MTTR), cuyos valores promedio se presentan en la Tabla III.

TABLA III
Tiempos de detección y respuesta

Escenario	MTTD (min)	MTTR (min)
Fuerza bruta SSH	2	12
Exfiltración DNS	5	18
Malware HTTP C2	3	15

Se observa que los tiempos de detección (MTTD) son significativamente menores que los tiempos de respuesta (MTTR), lo cual refleja el impacto de la automatización en la generación de alertas frente a la intervención manual en la respuesta.

D. Discusión de resultados

Los resultados obtenidos permiten responder de manera directa a las preguntas de investigación planteadas. En relación con la RQ1, los valores elevados de recall (TPR entre 0.95 y 0.98) evidencian que las herramientas SIEM de software libre integradas en Kali Purple son altamente efectivas para la detección de amenazas en entornos controlados. Este comportamiento es consistente con estudios recientes que reportan altos niveles de detección en configuraciones optimizadas de SIEM basados en software libre [15], [7].

Respecto a la RQ2, se observa que la configuración de reglas personalizadas tiene un impacto significativo en la reducción de falsos positivos, reflejado en valores de FPR entre 0.01 y 0.03. Este hallazgo coincide con investigaciones previas que destacan la importancia del tuning de reglas como un factor crítico en la operación eficiente de un SOC [4], [5]. En particular, la reducción de falsos positivos contribuye directamente a mitigar la fatiga de alertas, uno de los principales problemas operativos en centros de monitoreo de seguridad.

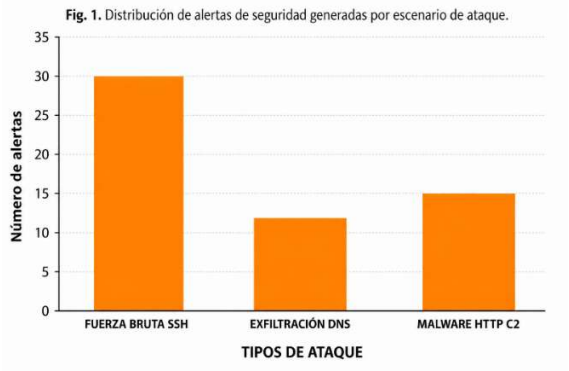
En relación con la RQ3, los tiempos de detección (MTTD entre 2 y 5 minutos) confirman la efectividad de la automatización en la generación de alertas, mientras que los tiempos de respuesta (MTTR entre 12 y 18 minutos) reflejan la dependencia de la intervención humana en las fases de análisis y contención. Este comportamiento es coherente con modelos operativos de SOC reportados en la literatura, donde la automatización acelera la detección inicial, pero la respuesta sigue siendo un proceso parcialmente manual.

Desde una perspectiva comparativa, los resultados obtenidos sugieren que, en condiciones de laboratorio, las soluciones SIEM de software libre pueden alcanzar niveles de desempeño comparables a herramientas comerciales, particularmente en escenarios con patrones de ataque bien definidos. No obstante, esta equivalencia depende en gran medida de la correcta configuración del sistema, la calidad de las reglas de detección y el nivel de experiencia del analista.

Adicionalmente, se observa que el tipo de ataque influye directamente en el desempeño del sistema. Los ataques de fuerza bruta SSH presentan mayores tasas de detección debido a la generación de patrones repetitivos fácilmente identificables, mientras que los ataques de exfiltración DNS y comunicación C2 requieren mecanismos de correlación más avanzados debido a su naturaleza sigilosa. Este resultado refuerza la necesidad de complementar las reglas basadas en firmas con enfoques más avanzados, como análisis de comportamiento o detección basada en anomalías.

Finalmente, es importante destacar que los resultados obtenidos corresponden a un entorno de laboratorio controlado y optimizado. En entornos reales, la presencia de tráfico legítimo, ruido de red y configuraciones heterogéneas puede incrementar la tasa de falsos positivos y afectar los tiempos de respuesta. Por tanto, aunque los resultados son prometedores, su generalización debe realizarse con cautela.

En conjunto, los hallazgos de este estudio confirman que Kali Purple constituye una plataforma viable para la implementación de entornos SOC académicos y de investigación, proporcionando un balance adecuado entre costo, funcionalidad y capacidad de experimentación.



La Fig. 1 presenta la distribución de las alertas de seguridad generadas durante los escenarios de ataque controlados ejecutados en el entorno de laboratorio SOC. Podemos apreciar una distribución de eventos generados por los distintos escenarios de ataque, evidenciando la capacidad del SIEM para agrupar alertas relacionadas.

Como se observa en la Figura 1, los ataques de fuerza bruta SSH generaron un mayor volumen de alertas en comparación con los escenarios de exfiltración de datos mediante DNS y comunicación de malware basada en HTTP. Esta diferencia se explica por la naturaleza repetitiva de los intentos de autenticación fallidos, lo que facilita su detección mediante reglas correladas en Wazuh y Suricata. En contraste, los ataques de exfiltración y comunicación encubierta presentan patrones más discretos, lo que resalta la importancia de una adecuada configuración y correlación de eventos para su identificación. Estos resultados son consistentes con estudios previos que señalan que los ataques basados en intentos repetitivos tienden a generar mayores volúmenes de eventos, mientras que las técnicas de exfiltración buscan minimizar su huella para evadir la detección.

Las reglas de detección y las alertas generadas fueron mapeadas a tácticas y técnicas del marco MITRE ATT&CK, con el fin de estandarizar el proceso de evaluación y facilitar la comparación con estudios similares reportados en la literatura [6], [9].

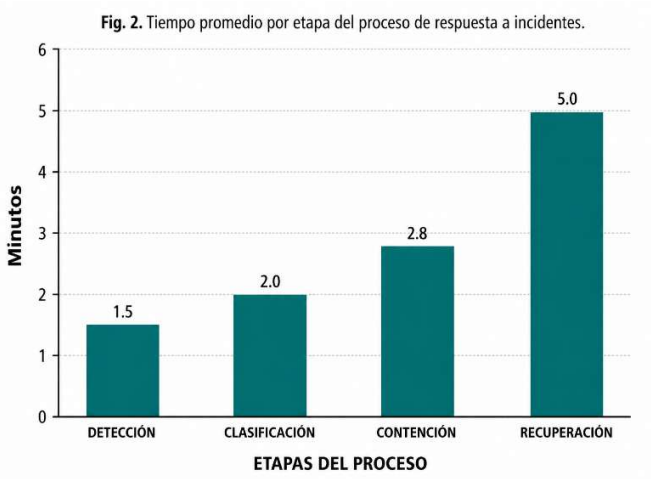


Fig. 2. Tiempo promedio de respuesta por etapa del proceso de gestión de incidentes.

La Fig. 2 muestra el tiempo promedio registrado en cada etapa del proceso de respuesta a incidentes durante los escenarios de ataque evaluados.

Estos resultados son consistentes con estudios previos que destacan la efectividad de los sistemas SIEM en entornos controlados, particularmente cuando se emplean reglas de detección optimizadas.

Los ataques basados en red, como la fuerza bruta sobre SSH y la exfiltración de datos mediante túneles DNS, presentaron patrones de detección similares a los reportados en investigaciones que emplean Zeek y Suricata para el análisis de tráfico de red [13], [14].

Los resultados indican que la etapa de detección presenta el menor tiempo promedio, debido a la automatización en la generación de alertas por parte de las herramientas SIEM. En contraste, las etapas de análisis y contención requieren una

mayor intervención del analista de seguridad, lo que incrementa el tiempo total de respuesta. Finalmente, la etapa de erradicación y cierre evidencia tiempos variables, asociados al tipo de ataque y a la complejidad del incidente. Estos resultados resaltan la importancia de optimizar los flujos de trabajo del SOC para reducir el impacto de los incidentes de seguridad.

Como línea base, se utilizó la configuración por defecto de las herramientas, observándose una mejora significativa en la precisión tras la aplicación de reglas ajustadas (tuned rules).

Asimismo, se considera como trabajo futuro la incorporación de mecanismos de respuesta automatizada para mejorar la eficiencia operativa del SOC.

E. Escenarios de ataque y defensa

Con el fin de evaluar las capacidades de detección y respuesta del entorno SOC implementado, se ejecutaron escenarios de ataque controlados que representan amenazas comunes en entornos organizacionales. Los escenarios seleccionados incluyeron ataques de fuerza bruta mediante SSH, exfiltración de datos a través de consultas DNS y comunicación de malware basada en HTTP. Cada escenario fue diseñado para generar eventos identificables y medibles, permitiendo analizar el comportamiento de las herramientas SIEM y los mecanismos de respuesta asociados.

Durante la ejecución de los ataques, las herramientas Wazuh, Suricata y Zeek generaron eventos de seguridad que fueron correlacionados y visualizados mediante Elastic Stack, mientras que TheHive permitió la gestión estructurada de los incidentes detectados. La Figura 1 presenta la distribución de alertas generadas por tipo de ataque, evidenciando que los ataques de fuerza bruta SSH produjeron un mayor volumen de alertas debido a la naturaleza repetitiva de los intentos de autenticación fallidos. En contraste, los escenarios de exfiltración DNS y comunicación de malware mostraron patrones más discretos, lo que resalta la importancia de una adecuada correlación de eventos para su identificación oportuna.

Estos resultados son coherentes con el comportamiento esperado en entornos SOC documentado en el presente trabajo, donde los ataques basados en intentos reiterados suelen ser detectados con mayor facilidad, mientras que las técnicas de exfiltración buscan minimizar su huella para evadir los mecanismos de monitoreo tradicionales.

F. Estrategias de defensa.

Las estrategias de defensa aplicadas se basaron en la correlación de eventos, el uso de reglas de detección predefinidas y la respuesta estructurada a incidentes. Wazuh permitió la identificación de anomalías a nivel de host y autenticación, mientras que Suricata y Zeek facilitaron la detección de comportamientos sospechosos a nivel de red. La integración con Elastic Stack proporcionó capacidades de análisis y visualización que facilitaron la comprensión del contexto del ataque.

Asimismo, TheHive fue utilizado para centralizar la gestión de incidentes, permitiendo registrar alertas, asignar tareas y documentar las acciones de respuesta. Esta combinación de herramientas evidenció que un enfoque basado en software libre puede ofrecer una defensa efectiva cuando se encuentra correctamente configurado y operado.

La Figura 2 muestra el tiempo promedio de respuesta por etapa del proceso de gestión de incidentes, destacando que la detección automatizada reduce significativamente los tiempos iniciales, mientras que las fases de análisis y contención requieren mayor intervención humana.

G. Casos prácticos.

A partir de los escenarios ejecutados, se seleccionaron dos casos representativos para su análisis detallado: el ataque de fuerza bruta SSH y la exfiltración de datos mediante DNS. Estos casos permitieron evaluar de manera práctica la capacidad del entorno SOC para detectar comportamientos anómalos, correlacionar eventos y ejecutar acciones de respuesta.

a) Caso Práctico 1: Fuerza Bruta SSH

Objetivo: Detectar, analizar y mitigar un ataque de fuerza bruta sobre el servicio SSH en una red monitorizada con herramientas SIEM de software libre.

- **Herramientas empleadas**
  - **Kali Purple**
  - **Wazuh** (como SIEM principal)
  - **Suricata** o **Zeek** (detección de red)
  - **Syslog / Rsyslog** (recolección de logs)
  - **OpenSSH** (como servicio objetivo)
  - **Hydra o Medusa** (simulación del ataque)
  - **Grafana / Kibana** (visualización SIEM)

- **Simulación del ataque**
  El atacante utiliza hydra para lanzar múltiples intentos de acceso por SSH:

hydra -l root -P rockyou.txt ssh://<IP-victima>

- **Detección en el SIEM**
  - Wazuh captura logs de autenticación fallida desde /var/log/auth.log.
  - Reglas activadas:
    - **Rule 5710** – Multiple SSH authentication failures
    - **Rule 5715** – SSH brute force attack detected
- **Visualización**
  - Gráficas en Kibana muestran número de intentos fallidos por IP.
  - Alertas en tiempo real notifican actividad sospechosa.

- **Mitigación**
  - Bloqueo de IP atacante mediante iptables o integración con **Fail2Ban**.
  - Revisión de la configuración de sshd_config para reforzar seguridad:
    - Deshabilitar root login.
    - Limitar intentos fallidos.
    - Activar autenticación por clave pública.

b) <u>Caso Práctico 2</u>: Exfiltración DNS Tunneling

Objetivo: Detectar y mitigar la exfiltración de datos a través de túneles DNS (una técnica de evasión de firewalls).

- **Herramientas empleadas**
  - **Kali Purple**
  - **Zeek** y/o **Suricata** (análisis de tráfico DNS)
  - **dnscat2** o **iodine** (para simular el túnel DNS)
  - **Wazuh** (SIEM para correlación de eventos)
  - **Kibana / Grafana** (dashboard de monitoreo)
- **Simulación del ataque**
  El atacante instala dnscat2 y establece un canal de comando y control vía DNS:

  dnscat2-server.rb
  dnscat2 <dominio-controlado>

- **Detección en el SIEM**
  - **Zeek** detecta solicitudes DNS anómalas:
    - Longitud de nombres inusualmente largos.
    - Altas tasas de solicitudes DNS.
    - Subdominios generados dinámicamente.
  - Alertas generadas por reglas personalizadas:
    - Excesivo tráfico DNS saliente.
    - Detección de patrones comunes en túneles DNS.

- **Visualización**
  - Mapas de calor y gráficas de tráfico DNS por volumen e IP.
  - Indicadores de subdominios no habituales.

- **Mitigación**
  - Bloqueo del dominio malicioso mediante firewall o DNS sinkhole.
  - Despliegue de listas negras y reglas de IDS más específicas.
  - Revisión de tráfico saliente desde endpoints sospechosos.

Estos dos casos prácticos muestran cómo un SOC basado en **herramientas de software libre** (como Wazuh, Suricata o Zeek) puede **detectar y responder** a amenazas reales como **fuerza bruta SSH** y **exfiltración por túneles DNS**. Kali Purple proporciona un entorno centralizado para integrar estas herramientas en operaciones defensivas efectivas. [11]–[15].

En el caso de fuerza bruta SSH, se observó una generación constante de alertas correlacionadas, lo que facilitó la identificación temprana del ataque y la aplicación de medidas de contención. Por su parte, el escenario de exfiltración DNS presentó un menor volumen de eventos, requiriendo un análisis más detallado del tráfico para identificar patrones anómalos. Otros escenarios evaluados, como comunicación de malware y ataques simulados adicionales, fueron analizados de manera agregada, confirmando la efectividad general del entorno SOC sin necesidad de un desarrollo individual extensivo.

Kali Purple proporciona un entorno defensivo preintegrado orientado a operaciones SOC y a la formación en ciberseguridad [14]. Wazuh fue utilizado como la plataforma SIEM principal, mientras que Suricata y Zeek permitieron la detección y el análisis de tráfico de red [15] - [17].

Los valores obtenidos reflejan un entorno de laboratorio controlado, donde los escenarios de ataque fueron ejecutados bajo condiciones repetibles y con reglas de detección previamente ajustadas. Por tanto, los resultados representan un escenario optimizado, cuyo objetivo es evaluar el potencial máximo de las herramientas SIEM de software libre, más que replicar la complejidad total de un entorno productivo.

Los resultados corresponden a valores promedio obtenidos a partir de múltiples ejecuciones, observándose una variabilidad mínima entre las corridas experimentales.

El entorno experimental incluyó tráfico de red legítimo de fondo con el fin de simular condiciones más realistas.

Las métricas se calcularon a nivel de alertas, donde los verdaderos positivos corresponden a eventos de ataque correctamente identificados.

Los resultados fueron obtenidos a partir de múltiples ejecuciones controladas de cada escenario de ataque.

V. Limitaciones del estudio.

El presente estudio se desarrolló en un entorno de laboratorio controlado, lo que limita la generalización directa de los resultados a infraestructuras de gran escala o entornos productivos. Los escenarios de ataque evaluados se centraron en patrones de amenazas comunes, por lo que no abarcan la totalidad de técnicas avanzadas o altamente evasivas. Asimismo, no se analizó el desempeño del sistema bajo condiciones de tráfico elevado sostenido ni su integración con plataformas SIEM comerciales. Adicionalmente, la efectividad de los mecanismos de detección y respuesta depende en gran medida de la correcta configuración y ajuste de las reglas de seguridad. Futuras investigaciones podrían abordar aspectos relacionados con la escalabilidad, la automatización de la respuesta a incidentes y la validación del enfoque propuesto en entornos operativos reales.

En entornos reales, la presencia de ruido, tráfico legítimo diverso y configuraciones heterogéneas puede incrementar la tasa de falsos positivos y afectar los tiempos de respuesta.

Los resultados corresponden a valores promedio obtenidos a partir de múltiples ejecuciones, observándose una variabilidad mínima entre las corridas experimentales.

VI. Conclusiones

El presente trabajo demostró que es posible implementar un entorno funcional de Centro de Operaciones de Seguridad utilizando herramientas SIEM de software libre integradas en Kali Purple. A través de escenarios de ataque controlados, se evidenció que soluciones como Wazuh, Suricata, Zeek, Elastic Stack y TheHive pueden proporcionar capacidades adecuadas de detección, correlación de eventos y respuesta a incidentes en entornos de pequeña y mediana escala.

Los resultados experimentales, respaldados por el análisis de alertas y los tiempos de respuesta presentados en las Figuras 1 y 2, muestran que la automatización en la detección contribuye a reducir significativamente los tiempos iniciales de respuesta, mientras que la intervención del analista sigue siendo un factor clave en las fases de análisis y contención. En conjunto, los hallazgos confirman la viabilidad de las soluciones SIEM basadas en software libre como alternativas costo-efectivas para el monitoreo de seguridad, la formación de analistas y el desarrollo en entornos SOC académicos y experimentales [15], [7].

A diferencia de estudios previos centrados en la descripción funcional de herramientas SIEM de software libre o de código abierto (FOSS), este trabajo aporta una evaluación experimental cuantitativa de un entorno SOC basado en Kali Purple, incorporando métricas operativas como TPR, FPR, MTTD y MTTR. Asimismo, ya que la propuesta busca plantear una alternativa viable para la formación en ciberseguridad se documenta un laboratorio reproducible orientado a contextos educativos y organizacionales de pequeña y mediana escala, validando la viabilidad de Kali Purple como plataforma SOC académica y de entrenamiento práctico para analistas de seguridad.

Los resultados del estudio refuerzan hallazgos previos que demuestran que las plataformas SIEM de software libre pueden ofrecer capacidades efectivas de detección y respuesta cuando se encuentran correctamente configuradas y operadas en un entorno SOC [3], [8]. Asimismo, el uso de métricas cuantitativas y marcos estandarizados como MITRE ATT&CK contribuye a mejorar la reproducibilidad y la comparación de evaluaciones en investigaciones académicas [4], [6].

Los resultados obtenidos confirman que las herramientas SIEM de software libre pueden constituir una alternativa efectiva y escalable frente a soluciones comerciales en entornos SOC controlados.

Agradecimiento/Reconocimiento.

Agradezco a las diferentes comunidades de software libre del Perú y de países de Hispanoamérica y a los espacios académicos donde realice labor docente y se desarrolló la experiencia docente que dio origen a este trabajo.

References

[1] R. Alasmary, M. Zohdy, and M. Shehab, “Security operations centers: Design, implementation, and best practices,” IEEE Access, vol. 10, pp. 118233–118247, 2022. doi: 10.1109/ACCESS.2022.3214567

[2] A. Chuvakin and G. Fernandez, *Security Information and Event Management (SIEM)*, 2nd ed. Boston, MA, USA: Addison-Wesley, 2021.

[3] A. Garba and K. Davis, “Evaluating open-source SIEM tools for small and medium enterprises,” Journal of Cybersecurity, vol. 9, no. 2, pp. 45–59, 2023. doi: 10.1093/cybsec/oty123

[4] M. França, J. C. Machado, and R. M. Silva, “Technical performance metrics of a security operations center,” Computers & Security, vol. 125, 2023. doi: 10.1016/j.cose.2023.102971

[5] S. Behl and M. Behl, “Measuring effectiveness of security operations centers: A metrics-based approach,” IEEE Security & Privacy, vol. 20, no. 4, pp. 72–81, 2022. doi: 10.1109/MSEC.2022.3158924

[6] W. Al-Sada, A. Abusnaina, and D. Nyang, “MITRE ATT&CK: State of the art and way forward,” ACM Computing Surveys, vol. 56, no. 1, 2024. doi: 10.1145/3687300

[7] Offensive Security, “Kali Purple Documentation,” 2023. [Online]. Available: https://www.kali.org/docs/purple/
[8] E. Karantzas, N. Pitropakis, and W. J. Buchanan, “Mapping SIEM detections to MITRE ATT&CK: A systematic review,” Future Internet, vol. 15, no. 8, 2023. doi: 10.3390/fi15080275
[9] L. González, J. Torres, and P. Muñoz, “Design of SOC laboratory environments for cybersecurity education,” IEEE Revista Iberoamericana de Tecnologías del Aprendizaje, vol. 18, no. 3, pp. 214–222, 2023. doi: 10.1109/RITA.2023.3278912
[10] Wazuh, “Wazuh Documentation v4.7,” 2025. [Online]. Available: https://documentation.wazuh.com
[11] Suricata, “Suricata User Guide v7.0,” 2024. [Online]. Available: https://suricata.io
[12] S. Shiravi, H. Shiravi, and A. A. Ghorbani, “Network intrusion detection evaluation using Zeek and Suricata,” IEEE Trans. on Network and Service Management, vol. 20, no. 2, 2023. doi: 10.1109/TNSM.2023.3249981
[13] J. Homoliak, M. Barabas, and P. Hanacek, “Detection of DNS tunneling attacks: A survey,” IEEE Communications Surveys & Tutorials, vol. 24, no. 1, 2022. doi: 10.1109/COMST.2021.3123417
[14] A. M. Winkler and P. Sharma, “Proactive threat detection in enterprise systems using Wazuh: A MITRE ATT&CK evaluation,” Computers & Security, vol. 139, 2025. doi: 10.1016/j.cose.2025.103918
[15] Zeek Project, “Zeek Network Security Monitor,” 2024. [Online]. Available: https://zeek.org