Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTOR/ES:

CORDOVA CABRERA EMILIO JOSE

DELGADO MURILLO JORGE LUIS

LARREA RODRIGUEZ OMAR ANDRES

MOLINA SARCO JEAN CARLOS

TUTORES:

Iván Reyes Chacón

Juan Fernando López

TEMA

Diseño e implementación de un SIEM All-in-One basado en OpenSearch para la detección y correlación de eventos de seguridad en una infraestructura corporativa de laboratorio alineada al framework MITRE ATT&CK®.

Quito - Ecuador

Junio – 20206

REINVENTEMOS EL FUTURO

Diseño y despliegue de SIEM con OpenSearch

CERTIFICACIÓN DE AUTORÍA

Nosotros, **Jorge Luís Delgado Murillo, Omar Andrés Larrea Rodríguez, Jean Carlos Molina Sarco y Emilio José Córdova Cabrera,** declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Jorge Luís Delgado Murillo

Omar Andrés Larrea Rodríguez

Jean Carlos Molina Sarco

Emilio José Córdova Cabrera

Diseño y despliegue de SIEM con OpenSearch

AUTORIZACIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL

Nosotros, Jorge Luís Delgado Murillo, Omar Andrés Larrea Rodríguez, Jean Carlos Molina Sarco y Emilio José Córdova Cabrera, en calidad de autores del trabajo de investigación titulado Diseño y despliegue de un SIEM All-in-One basado en OpenSearch para la detección y correlación de eventos de seguridad en una infraestructura corporativa de laboratorio alineada al framework MITRE ATT&CK®., autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, (mayo 2026)

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JORGE LUIS DELGADO MURILLO

Jorge Luís Delgado Murillo

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
OMAR ANDRES LARREA RODRIGUEZ

Omar Andrés Larrea Rodríguez

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JEAN CARLOS MOLINA SARCO

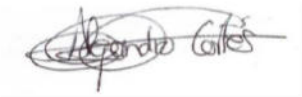
Jean Carlos Molina Sarco

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
EMILIO JOSE CORDOVA CABRERA

Emilio José Córdova Cabrera

APROBACIÓN DE DIRECCIÓN Y COORDINACIÓN DEL PROGRAMA

Nosotros, **Alejandro Cortes López EIG y Iván Galo Reyes Chacón UIDE,** declaramos que: **(Jorge Luís Delgado Murillo, Omar Andrés Larrea Rodríguez, Jean Carlos Molina Sarco y Emilio José Córdova Cabrera**, son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



Alejandro Cortés
Director/a de la
Maestría en Ciberseguridad

Iván Reyes
Coordinador/a de la
Maestría en Ciberseguridad

DEDICATORIA

Dedicamos este trabajo a nuestras familias, quienes han sido el principal soporte durante este proceso académico. Su confianza, comprensión y apoyo constante nos permitieron superar los desafíos que se presentaron a lo largo de esta etapa de formación profesional.

A nuestros padres, por los valores inculcados, el esfuerzo ejemplar y el acompañamiento permanente que han contribuido a nuestro crecimiento personal y académico.

A nuestros seres queridos, por su paciencia, motivación y palabras de aliento en los momentos de mayor exigencia, impulsándonos a continuar hasta alcanzar esta meta.

Finalmente, dedicamos este proyecto a todas las personas que creen en el conocimiento, la innovación y el aprendizaje continuo como herramientas para construir un futuro más seguro y tecnológicamente responsable.

AGRADECIMIENTOS

Expresamos nuestro más sincero agradecimiento a la Universidad Internacional del Ecuador (UIDE) y a la Escuela de Innovación y Gobierno (EIG) por brindarnos los conocimientos, recursos y espacios académicos necesarios para el desarrollo de esta investigación.

A nuestro tutor, Juan Fernando López Tito, por su orientación, acompañamiento y valiosos aportes durante cada etapa del proyecto. Su experiencia y recomendaciones fueron fundamentales para fortalecer el enfoque técnico y metodológico de este trabajo.

A los docentes de la Maestría en Ciberseguridad, quienes compartieron sus conocimientos y experiencias profesionales, contribuyendo significativamente a nuestra formación académica y al desarrollo de competencias especializadas en el área.

A nuestras familias y seres queridos, por su comprensión, paciencia y apoyo incondicional durante el tiempo dedicado a la elaboración de este proyecto, especialmente en los momentos de mayor exigencia académica.

Finalmente, agradecemos a todas las personas que, de manera directa o indirecta, aportaron con ideas, sugerencias y motivación para culminar satisfactoriamente esta investigación.

Diseño y despliegue de SIEM con OpenSearch

RESUMEN

El incremento de los eventos de seguridad y la creciente complejidad de las infraestructuras tecnológicas han generado la necesidad de implementar mecanismos que permitan centralizar, monitorear y correlacionar información proveniente de múltiples fuentes. En este contexto, los sistemas Security Information and Event Management (SIEM) se han consolidado como herramientas fundamentales para mejorar la visibilidad de los eventos de seguridad y fortalecer las capacidades de detección dentro de las organizaciones. Sin embargo, las soluciones SIEM comerciales suelen requerir costos de licenciamiento, infraestructura y administración especializada que pueden dificultar su adopción en entornos con recursos limitados.

El objetivo de esta investigación fue diseñar, implementar y evaluar una solución SIEM All-in-One basada en OpenSearch para la centralización, correlación y detección de eventos de seguridad dentro de una infraestructura corporativa de laboratorio. La investigación se desarrolló mediante un enfoque aplicado y experimental, integrando estaciones de trabajo, servidores, dispositivos de red, puntos de acceso inalámbricos y firewalls como fuentes de generación de eventos.

La solución implementada utilizó OpenSearch como plataforma principal de almacenamiento y análisis de información, OpenSearch Dashboards para la visualización y monitoreo de eventos, Fluent Bit y Fluentd para la recolección y procesamiento de logs, así como Syslog para la integración de dispositivos de infraestructura. Adicionalmente, se implementaron reglas de detección y correlación alineadas al framework MITRE ATT&CK® con el propósito de relacionar eventos observados con técnicas de ataque reconocidas en el ámbito de la ciberseguridad.

Diseño y despliegue de SIEM con OpenSearch

La validación de la solución se realizó mediante escenarios controlados que incluyeron actividades de fuerza bruta sobre servicios de autenticación, reconocimiento de red, creación de cuentas de usuario y cambios administrativos en dispositivos de seguridad. Los resultados obtenidos evidenciaron la capacidad de la plataforma para centralizar eventos provenientes de múltiples fuentes, generar alertas oportunas, correlacionar actividades relacionadas y proporcionar visibilidad sobre eventos relevantes de seguridad. Finalmente, se concluye que una solución SIEM basada en tecnologías de código abierto (open source) constituye una alternativa técnicamente viable para implementar capacidades de monitoreo y detección de eventos de seguridad dentro de entornos corporativos de laboratorio.

Palabras clave: Ciberseguridad, SIEM, OpenSearch, correlación de eventos, monitoreo de seguridad, MITRE ATT&CK®, detección de amenazas.

Diseño y despliegue de SIEM con OpenSearch

ABSTRACT

The increasing volume of security events and the growing complexity of technological infrastructures have created the need for mechanisms capable of centralizing, monitoring, and correlating information from multiple sources. In this context, Security Information and Event Management (SIEM) systems have become essential tools for improving security event visibility and strengthening threat detection capabilities within organizations. However, commercial SIEM solutions often require licensing costs, infrastructure resources, and specialized administration that may limit their adoption in environments with restricted resources.

The objective of this research was to design, implement, and evaluate an All-in-One SIEM solution based on OpenSearch for the centralization, correlation, and detection of security events within a corporate laboratory infrastructure. The study followed an applied and experimental approach, integrating workstations, servers, network devices, wireless access points, and firewalls as event sources.

The implemented solution employed OpenSearch as the primary platform for data storage and analysis, OpenSearch Dashboards for event visualization and monitoring, Fluent Bit and Fluentd for log collection and processing, and Syslog for the integration of infrastructure devices. In addition, detection and correlation rules aligned with the MITRE ATT&CK® framework were implemented to associate observed events with recognized attack techniques in the cybersecurity domain.

The solution was validated through controlled scenarios that included brute-force activities against authentication services, network reconnaissance, user account creation, and administrative changes on security devices. The results demonstrated the platform's ability to centralize events from multiple sources, generate timely alerts, correlate related activities, and

provide visibility into relevant security events. Finally, the study concludes that an open-source SIEM solution represents a technically feasible alternative for implementing security monitoring and event detection capabilities within corporate laboratory environments.

Keywords: Cybersecurity, SIEM, OpenSearch, Event Correlation, Security Monitoring, MITRE ATT&CK®, Threat Detection.

ÍNDICE GENERAL

Diseño y despliegue de SIEM con OpenSearch

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Diseño y despliegue de SIEM con OpenSearch

Introducción

El crecimiento de dispositivos conectados, servicios digitalizados y entornos empresariales interconectados ha incrementado significativamente la superficie de ataque de las organizaciones, generando nuevos desafíos para el monitoreo y la protección de los activos de información (Lella, 2024). Asimismo, el informe *Verizon Data Breach Investigations Report* (Verizon, 2026) señala que la dificultad para monitorear múltiples fuentes de eventos y correlacionar actividades sospechosas incrementa el tiempo medio de detección de incidentes dentro de las organizaciones. En este escenario, la implementación de soluciones de monitoreo y correlación de eventos se vuelve fundamental para garantizar la protección de los activos de información.

Los sistemas Security Information and Event Management (SIEM) se han consolidado como herramientas fundamentales para centralizar, almacenar, analizar y correlacionar eventos de seguridad provenientes de múltiples fuentes, permitiendo mejorar la visibilidad de la infraestructura tecnológica y facilitar la detección temprana de amenazas (Canadian Centre for Cyber Security, 2025; Kent & Souppaya, 2006). Sin embargo, muchas organizaciones medianas enfrentan limitaciones económicas, técnicas y de infraestructura para implementar plataformas SIEM comerciales, lo que reduce sus capacidades de monitoreo, detección y respuesta ante incidentes de ciberseguridad (Elastic, 2024; Hase, 2024).

Las organizaciones que no disponen de soluciones centralizadas para el monitoreo de seguridad enfrentan mayores dificultades para identificar oportunamente eventos sospechosos y correlacionar actividades maliciosas provenientes de múltiples dispositivos y sistemas (Canadian Centre for Cyber Security, 2025). Esta situación incrementa el tiempo medio de detección y respuesta ante incidentes de seguridad, reduciendo la capacidad de las organizaciones para

responder de manera oportuna a las amenazas cibernéticas (Verizon, 2026). En este contexto, el presente trabajo propone el diseño e implementación de una solución SIEM basada en tecnologías de código abierto, utilizando OpenSearch como plataforma principal para centralizar, analizar y correlacionar eventos de seguridad generados por dispositivos de red, firewalls, estaciones de trabajo y servidores dentro de un entorno corporativo de laboratorio (OpenSearch Project, 2026). La solución busca mejorar la visibilidad de las amenazas y facilitar la detección temprana de comportamientos anómalos mediante reglas de correlación alineadas con el framework MITRE ATT&CK® (MITRE ATT&CK, 2026).

Definición del Proyecto

El proyecto consiste en el diseño e implementación de una solución SIEM basada en OpenSearch para la centralización, procesamiento y correlación de eventos de seguridad dentro de un entorno corporativo de laboratorio.

La infraestructura utilizada estará compuesta por dispositivos físicos de red y seguridad, incluyendo firewall FortiGate, switches y puntos de acceso Aruba, así como estaciones de trabajo Windows y servidores Linux y Windows. Estos dispositivos generarán eventos relacionados con autenticación, tráfico de red, actividad del sistema y eventos de seguridad.

La solución SIEM será desplegada sobre Ubuntu Server virtualizado en un entorno Proxmox VE (Proxmox Server Solutions, 2026). Para la recolección y procesamiento de logs se utilizarán Fluentd como colector central y Fluent Bit como agente de envío instalado en estaciones de trabajo y servidores (Fluent Bit Project, 2025; Fluentd Project, 2025). Asimismo, los dispositivos de red y seguridad enviarán eventos mediante el protocolo Syslog (Gerhards & Gerhards, 2009).

Diseño y despliegue de SIEM con OpenSearch

Los eventos recolectados serán clasificados y almacenados en índices específicos dentro de OpenSearch, permitiendo centralizar el análisis y correlación de información proveniente de múltiples fuentes. Finalmente, la solución implementará reglas de correlación alineadas al framework MITRE ATT&CK® con el objetivo de detectar comportamientos anómalos y generar alertas tempranas ante posibles incidentes de ciberseguridad.

Justificación e Importancia del Trabajo de Investigación

Las organizaciones medianas suelen enfrentar limitaciones para implementar soluciones avanzadas de monitoreo de seguridad debido al alto costo de licenciamiento, requerimientos de infraestructura y complejidad administrativa de plataformas SIEM comerciales. De acuerdo con Elastic (2024), muchas soluciones empresariales requieren inversiones elevadas en almacenamiento, procesamiento y personal especializado para su operación y mantenimiento. Esta situación incrementa significativamente el tiempo de detección y respuesta ante incidentes, permitiendo que amenazas, como accesos no autorizados, movimientos laterales o exfiltración de datos permanezcan sin ser detectadas durante largos períodos.

El desarrollo de una solución SIEM basada en herramientas open source representa una alternativa viable, económica y escalable para mejorar la postura de ciberseguridad en organizaciones medianas (Manzoor et al., 2024). La viabilidad de la solución se fundamenta en el uso de tecnologías de código abierto como OpenSearch, Fluentd y Fluent Bit, las cuales reducen costos de licenciamiento y permiten flexibilidad de implementación sobre infraestructura existente (OpenSearch Project, 2026). Asimismo, la solución será evaluada considerando criterios como capacidad de correlación de eventos, generación de alertas, centralización de logs y consumo de recursos tecnológicos.

La importancia de este trabajo radica en:

Diseño y despliegue de SIEM con OpenSearch

Implementar una arquitectura SIEM funcional basada en tecnologías open source sin dependencia de soluciones comerciales.

Centralizar y correlacionar eventos de seguridad provenientes de firewalls, dispositivos de red, estaciones de trabajo y servidores.

Implementar mecanismos de detección y correlación basados en reglas alineadas al framework ATT&CK.

Reducir el tiempo medio de detección de incidentes (MTTD) mediante la correlación automatizada de eventos de seguridad.

Mejorar la visibilidad centralizada de eventos de seguridad dentro de un entorno corporativo de laboratorio.

Validar la integración de herramientas como OpenSearch, Fluentd, Fluent Bit y Syslog para el monitoreo continuo de eventos de seguridad.

La efectividad de la solución será evaluada mediante métricas como tiempo medio de detección (MTTD), generación de alertas y capacidad de correlación de eventos frente a escenarios controlados de ataque.

Además, el proyecto tiene un valor académico significativo, ya que propone una metodología reproducible para el despliegue de un SIEM basado en OpenSearch, incluyendo configuraciones de recolección de logs, integración de dispositivos de red y seguridad, reglas de correlación y escenarios de validación. Esto permitirá que la solución pueda ser replicada en otros entornos corporativos de laboratorio o académicos con requerimientos similares.

Diseño y despliegue de SIEM con OpenSearch

Alcance

El proyecto se enfocará en el diseño, implementación y validación de una solución SIEM All-in-One basada en OpenSearch dentro de un entorno corporativo de laboratorio compuesto por dispositivos físicos de red y seguridad, estaciones de trabajo y servidores.

En esta arquitectura, todos los componentes funcionales del SIEM (recolección, procesamiento, almacenamiento, correlación y visualización de eventos) se ejecutan sobre una única máquina virtual, sin contemplar una infraestructura distribuida ni mecanismos de alta disponibilidad.

La arquitectura del SIEM incluirá componentes como OpenSearch para almacenamiento y análisis de eventos, OpenSearch Dashboards para visualización y monitoreo, Fluentd como colector central de logs y Fluent Bit como agente de recolección instalado en estaciones de trabajo y servidores. Asimismo, se utilizará el protocolo Syslog para la integración de eventos provenientes de dispositivos de red y seguridad.

Las fuentes de eventos que se integrarán al SIEM comprenderán firewall FortiGate, switches y puntos de acceso Aruba, estaciones de trabajo Windows y servidores Linux y Windows. Los eventos recolectados estarán relacionados con autenticación, tráfico de red, actividad del sistema, conexiones, accesos administrativos y eventos de seguridad.

El proyecto comprenderá las siguientes fases y actividades:

- Implementación y configuración de OpenSearch como núcleo del SIEM.
- Recolección y centralización de logs mediante Fluentd, Fluent Bit y Syslog.
- Normalización y clasificación de eventos provenientes de múltiples fuentes.
- Diseño de reglas de correlación basadas en eventos sospechosos y comportamientos alineados al framework MITRE ATT&CK®.

Diseño y despliegue de SIEM con OpenSearch

- Construcción de dashboards para la visualización de eventos, alertas, autenticaciones, tráfico de red y actividades sospechosas.
- Ejecución de escenarios controlados relacionados con intentos de acceso no autorizado, descubrimiento de servicios de red, creación de cuentas y cambios administrativos en dispositivos de seguridad, representando técnicas ATT&CK como Brute Force (T1110), Network Service Discovery (T1046), Create Account (T1136), Account Manipulation (T1098) e Impair Defenses (T1562).
- Evaluación de métricas como tiempo medio de detección (MTTD), generación de alertas y capacidad de correlación de eventos.

Exclusiones y Límites del Alcance

El alcance del proyecto no contempla la implementación de capacidades SOAR (Security Orchestration, Automation and Response), respuesta automática ante incidentes, integración con servicios en la nube ni alta disponibilidad distribuida del SIEM basada en redundancia de hardware a nivel de infraestructura física. El sistema se limitará a funciones de monitoreo, centralización y correlación de eventos de seguridad dentro del entorno corporativo de laboratorio bajo un enfoque estructural All-in-One.

Para optimizar la gestión interna de índices y el balanceo lógico de carga de trabajo (workload balancing), el motor de OpenSearch se planteará mediante dos nodos lógicos independientes dentro del mismo host virtual, excluyendo explícitamente del alcance cualquier esquema de tolerancia a fallos por replicación de servidores físicos.

Asimismo, los mecanismos de alertamiento contemplados se limitarán exclusivamente al envío de notificaciones pasivas (como alertas por correo electrónico) orientadas a informar al administrador sobre los hallazgos o correlaciones detectadas. Se excluye explícitamente del

alcance la ejecución de acciones automáticas de contención, mitigación, bloqueo o recuperación sobre los dispositivos, usuarios o servicios monitoreados. Por lo tanto, el sistema no constituirá una solución SOAR ni ejecutará respuestas automatizadas ante incidentes, actuando únicamente como una plataforma de apoyo para el posterior análisis manual de los eventos de seguridad.

Objetivos

Objetivo General

Diseñar, implementar y evaluar una solución SIEM basada en OpenSearch para la centralización, correlación y detección de eventos de seguridad dentro de un entorno corporativo de laboratorio, utilizando reglas alineadas al framework MITRE ATT&CK®.

Objetivos Específicos

- Analizar los requerimientos técnicos y de seguridad del entorno corporativo de laboratorio considerando dispositivos de red, firewalls, estaciones de trabajo y servidores que serán integrados al SIEM.
- Diseñar la arquitectura del SIEM definiendo sus componentes principales.
- Implementar la recolección, centralización y normalización de logs mediante Fluentd, Fluent Bit y Syslog.
- Desarrollar reglas de correlación multi-evento para la detección de amenazas alineadas al framework ATT&CK.
- Diseñar paneles de monitoreo (dashboards) de monitoreo para la visualización centralizada de eventos de seguridad, alertas y actividades sospechosas.
- Simular escenarios de ataque dentro del entorno corporativo de laboratorio.
- Evaluar la efectividad del sistema mediante métricas como tiempo medio de detección (MTTD), generación de alertas y capacidad de correlación de eventos.

Diseño y despliegue de SIEM con OpenSearch

- Analizar la viabilidad de implementación de la solución en organizaciones medianas considerando costos de licenciamiento, requerimientos de infraestructura y capacidades de monitoreo de seguridad.

Revisión de Literatura

El crecimiento exponencial de las amenazas cibernéticas ha impulsado la evolución de los sistemas de monitoreo de seguridad, especialmente los sistemas SIEM (Security Information and Event Management), los cuales han pasado de ser herramientas de recolección de logs a plataformas avanzadas de análisis y detección de amenazas. En este contexto, el presente capítulo aborda el estado del arte y los fundamentos teóricos que sustentan el desarrollo de un SIEM basado en OpenSearch, alineado al framework MITRE ATT&CK®.

Estado del Arte

Los sistemas Security Information and Event Management (SIEM) han evolucionado significativamente durante la última década, pasando de plataformas orientadas principalmente a la recolección y almacenamiento de registros hacia soluciones capaces de realizar correlación avanzada de eventos, analítica en tiempo real y detección basada en el comportamiento (Manzoor et al., 2024). Esta evolución ha sido impulsada por el incremento de las amenazas cibernéticas y la necesidad de reducir los tiempos de detección y respuesta ante incidentes de seguridad (Verizon, 2026).

La literatura reciente evidencia que la evolución de los sistemas SIEM ha estado orientada hacia la incorporación de capacidades avanzadas de análisis, automatización e integración con fuentes de inteligencia de amenazas. Según López Velásquez et al. (2023), los SIEM modernos han dejado de ser plataformas enfocadas exclusivamente en la recopilación de registros para convertirse en soluciones capaces de correlacionar eventos, integrar inteligencia

contextual y apoyar procesos de respuesta ante incidentes. Los autores destacan que la tendencia actual se orienta hacia arquitecturas flexibles capaces de adaptarse a entornos híbridos y distribuidos, donde la cantidad de eventos generados crece de forma constante (López Velásquez et al., 2023; Microsoft, 2025).

Investigaciones recientes destacan que los sistemas SIEM modernos integran capacidades de correlación avanzada, inteligencia de amenazas y análisis contextual para mejorar la detección de ataques complejos y reducir falsos positivos. Asimismo, estudios relacionados con ATT&CK señalan que la incorporación de automatización y análisis en tiempo real permite fortalecer la capacidad de detección y respuesta frente a incidentes de ciberseguridad (Bader et al., 2023).

Diversas investigaciones han demostrado que la integración de frameworks de inteligencia de amenazas como ATT&CK permite fortalecer las capacidades de detección dentro de arquitecturas SIEM (Van Pelt, 2021). Sin embargo, los resultados obtenidos dependen del contexto, las reglas de correlación implementadas y las fuentes de eventos utilizadas. Estudios recientes reportan mejoras en la correlación de eventos y reducción del tiempo medio de detección (MTTD) en implementaciones alineadas al framework ATT&CK dentro de los escenarios analizados (Mgbemele, 2026).

Por otro lado, las soluciones SIEM comerciales como Splunk, IBM QRadar SIEM y ArcSight continúan dominando gran parte del mercado debido a sus capacidades avanzadas de análisis, automatización y escalabilidad. No obstante, estas plataformas suelen requerir altos costos de licenciamiento, infraestructura dedicada y personal especializado para su administración, lo que limita su adopción en organizaciones medianas con restricciones presupuestarias y técnicas (Elastic, 2024).

Diseño y despliegue de SIEM con OpenSearch

En respuesta a estas limitaciones, han surgido alternativas open source como OpenSearch, las cuales permiten desarrollar arquitecturas SIEM flexibles y escalables con menores costos de implementación. OpenSearch destaca por sus capacidades de indexación distribuida, análisis de grandes volúmenes de datos y compatibilidad con herramientas de visualización y monitoreo en tiempo real. Asimismo, soluciones basadas en OpenSearch permiten personalizar Pipelines de ingestión, correlación y clasificación de eventos provenientes de múltiples fuentes (Instaclustr, 2022).

Experiencias previas sobre implementaciones SIEM basadas en OpenSearch reportan ventajas relacionadas con flexibilidad, reducción de costos y capacidad de integración con herramientas open source. Sin embargo, también se identifican limitaciones asociadas a la complejidad de configuración, necesidad de conocimientos técnicos avanzados y ausencia de ciertas funcionalidades automatizadas presentes en plataformas comerciales (Instaclustr, 2022).

De igual manera, investigaciones recientes destacan la importancia de correlacionar eventos provenientes de múltiples dispositivos y sistemas para detectar amenazas avanzadas, debido a que los ataques modernos suelen ejecutarse en múltiples etapas y vectores. En este contexto, el uso de correlación multi-evento basada en reglas permite relacionar eventos dentro de ventanas temporales definidas, facilitando la identificación de comportamientos asociados a técnicas como fuerza bruta, escaneo de servicios y movimientos laterales (Zhang, 2023).

Las investigaciones más recientes muestran que la evolución de los sistemas SIEM se orienta hacia la incorporación de capacidades de análisis avanzado, inteligencia de amenazas y automatización de procesos de detección. De acuerdo con el Canadian Centre for Cyber Security (2025), los SIEM de nueva generación han evolucionado desde plataformas enfocadas principalmente en la recopilación de logs hacia soluciones capaces de agregar, correlacionar y

analizar grandes volúmenes de eventos provenientes de múltiples fuentes para enfrentar amenazas cada vez más sofisticadas.

Por otra parte, estudios recientes destacan que las arquitecturas SIEM actuales buscan complementar la correlación tradicional basada en reglas con enfoques apoyados en analítica avanzada y monitoreo contextual, permitiendo identificar comportamientos anómalos que podrían pasar desapercibidos mediante mecanismos de detección convencionales (Bader et al., 2023).

Por otra parte, la creciente adopción de infraestructuras distribuidas y entornos híbridos ha incrementado la necesidad de soluciones capaces de centralizar eventos provenientes de múltiples fuentes tecnológicas. En este contexto, los sistemas SIEM continúan desempeñando un papel fundamental como plataforma de consolidación, correlación y visualización de eventos de seguridad, especialmente en organizaciones que requieren mejorar sus capacidades de monitoreo sin incurrir en elevados costos de licenciamiento (Elastic, 2024).

Marco Teórico

SIEM (Security Information and Event Management)

Un sistema SIEM (Security Information and Event Management) es una plataforma orientada a la recopilación, almacenamiento, análisis y correlación de eventos de seguridad provenientes de múltiples dispositivos y sistemas dentro de una infraestructura tecnológica. Su principal objetivo es proporcionar visibilidad centralizada de eventos, facilitar la detección temprana de amenazas y mejorar la capacidad de monitoreo de seguridad (CrowdStrike, 2023; Kent & Souppaya, 2006).

De acuerdo con CrowdStrike (2023), los SIEM modernos integran capacidades de centralización de logs, correlación de eventos, generación de alertas y análisis contextual para

detectar comportamientos anómalos dentro de entornos empresariales. Estas plataformas permiten relacionar eventos provenientes de diferentes fuentes con el fin de identificar patrones asociados a posibles incidentes de seguridad.

Las funcionalidades más relevantes de un SIEM incluyen centralización de logs, correlación multi-evento, generación de alertas y visualización de información mediante dashboards de monitoreo. Estas funcionalidades constituyen la base operativa de los sistemas SIEM modernos y permiten mejorar significativamente la capacidad de monitoreo y respuesta frente a incidentes de seguridad.

OpenSearch como Plataforma SIEM

OpenSearch es una plataforma open source orientada al almacenamiento, búsqueda, análisis y visualización de grandes volúmenes de datos en tiempo real. En el contexto de ciberseguridad, puede ser utilizada como núcleo de un sistema SIEM debido a sus capacidades de indexación distribuida, procesamiento de eventos y generación de dashboards de monitoreo.

De acuerdo con OpenSearch Project (2026), la plataforma incorpora funcionalidades como Security Analytics, Alerting y Dashboards, las cuales permiten implementar mecanismos de correlación de eventos, generación de alertas y análisis de actividades sospechosas dentro de infraestructuras empresariales.

OpenSearch ha sido adoptado como alternativa open source para arquitecturas SIEM debido a su flexibilidad de integración y compatibilidad con herramientas como Fluentd, Fluent Bit y Syslog. A diferencia de diversas soluciones comerciales, permite implementar capacidades de monitoreo y correlación de eventos sin requerir costos elevados de licenciamiento, convirtiéndose en una opción adecuada para entornos académicos y organizaciones medianas.

Diseño y despliegue de SIEM con OpenSearch

Adicionalmente, experiencias previas sobre implementaciones SIEM basadas en OpenSearch reportan ventajas relacionadas con escalabilidad, flexibilidad y reducción de costos. Sin embargo, también se identifican limitaciones asociadas a la complejidad de configuración y necesidad de conocimientos técnicos avanzados para la administración de Pipelines, correlación y análisis de eventos (Instaclustr, 2022).

Con el fin de identificar las principales características de las plataformas SIEM disponibles en el mercado, la Tabla 1 presenta una comparación general entre soluciones comerciales y open source, considerando aspectos relacionados con ventajas operativas y limitaciones de implementación.

Tabla 1

Comparación general entre soluciones SIEM

Solución	Tipo	Ventajas	Limitaciones
Splunk	Comercial	Alta escalabilidad y analítica avanzada	Alto costo de licenciamiento
IBM QRadar SIEM	Comercial	Correlación avanzada y soporte empresarial	Requiere infraestructura dedicada
Wazuh	Open source	Integración con Elastic/OpenSearch	Configuración compleja
OpenSearch	Open source	Flexibilidad, escalabilidad y bajo costo	Requiere conocimientos técnicos avanzados

Diversos estudios señalan que las plataformas SIEM basadas en software de código abierto representan una alternativa viable frente a soluciones comerciales debido a la reducción de costos de licenciamiento y a su flexibilidad de integración. Hase (2024) indica que organizaciones medianas y académicas suelen optar por soluciones de código abierto debido a la

posibilidad de adaptar la arquitectura a necesidades específicas sin depender de modelos comerciales basados en volumen de datos o número de eventos procesados.

Correlación de Eventos

La correlación de eventos es el proceso mediante el cual se identifican relaciones entre múltiples eventos de seguridad provenientes de diferentes dispositivos, aplicaciones y sistemas con el objetivo de detectar patrones asociados a actividades potencialmente maliciosas. Este mecanismo permite analizar los eventos de forma contextual, en lugar de evaluarlos de manera aislada, mejorando la capacidad para identificar amenazas complejas y reducir los falsos positivos (Sheeraz et al., 2024; Zhang, 2023).

Las investigaciones más recientes destacan que la efectividad de los sistemas SIEM depende en gran medida de la calidad de sus mecanismos de correlación. Sheeraz et al. (2024), señalan que los motores de correlación avanzados permiten relacionar eventos procedentes de diferentes dispositivos, protocolos y sistemas mediante reglas temporales y contextuales, incrementando significativamente la capacidad para identificar amenazas complejas que podrían pasar desapercibidas cuando los eventos son analizados de forma individual.

Según Zhang (2023), la correlación de eventos es fundamental para detectar amenazas avanzadas debido a que los ataques modernos suelen ejecutarse en múltiples etapas y vectores dentro de la infraestructura tecnológica.

Existen diferentes Tipos de correlación utilizados en plataformas SIEM:

Correlación basada en tiempo: relaciona eventos ocurridos dentro de una ventana temporal determinada. Es utilizada para detectar comportamientos como múltiples intentos fallidos de autenticación o escaneos rápidos de red (Zhang, 2023).

Correlación secuencial: relaciona eventos que ocurren en un orden específico para identificar patrones asociados a accesos no autorizados o escalamiento de privilegios (Sheeraz et al., 2024).

Correlación por agregación: agrupa eventos similares con el objetivo de identificar actividades anómalas repetitivas provenientes de uno o varios dispositivos (OpenSearch Project, 2026).

Correlación multi-fuente: relaciona eventos provenientes de diferentes sistemas y dispositivos, permitiendo detectar amenazas complejas mediante el análisis contextual de múltiples fuentes de información (Canadian Centre for Cyber Security, 2025).

La correlación de eventos constituye uno de los componentes principales dentro de las arquitecturas SIEM modernas debido a su capacidad para mejorar la detección temprana de amenazas y reducir falsos positivos mediante el análisis conjunto de múltiples eventos de seguridad (Sheeraz et al., 2024). La Tabla 2 resume los principales Tipos de correlación utilizados en plataformas SIEM y algunos ejemplos de aplicación en escenarios de seguridad.

Tabla 2

Tipos de correlación de eventos en SIEM

Tipo de correlación	Descripción	Aplicación
Basada en tiempo	Relaciona eventos dentro de una ventana temporal	Detección de fuerza bruta
Basada en secuencia	Analiza eventos en orden específico	Escalamiento de privilegios
Basada en agregación	Agrupa eventos similares	Identificación de anomalías
Basada en múltiples fuentes	Relaciona eventos de distintos dispositivos	Correlación entre firewall, servidores y endpoints

Diseño y despliegue de SIEM con OpenSearch

Arquitectura General de un SIEM

Una arquitectura SIEM está compuesta por diversos componentes encargados de recopilar, procesar, almacenar, correlacionar y visualizar eventos de seguridad provenientes de múltiples fuentes dentro de una infraestructura tecnológica. La integración de estos componentes permite transformar grandes volúmenes de registros en información útil para los procesos de monitoreo, detección y respuesta ante incidentes (Canadian Centre for Cyber Security, 2025; González-Granadillo et al., 2021).

De acuerdo con Canadian Centre for Cyber Security (2025), una arquitectura SIEM moderna debe ser capaz de centralizar eventos generados por dispositivos de red, sistemas operativos, aplicaciones y herramientas de seguridad, proporcionando capacidades de análisis, correlación y generación de alertas dentro de una plataforma unificada.

Según González-Granadillo et al. (2021), una arquitectura SIEM está compuesta por diferentes bloques funcionales que incluyen fuentes de datos, recolección de registros, normalización, correlación de eventos, almacenamiento y monitoreo de seguridad. Estos componentes trabajan de forma integrada para proporcionar visibilidad centralizada de la infraestructura tecnológica y facilitar la identificación de comportamientos anómalos.

De forma general, una arquitectura SIEM incorpora elementos encargados de la adquisición, procesamiento, almacenamiento y análisis de eventos de seguridad. La Tabla 3 describe los principales componentes funcionales que integran este tipo de plataformas.

Tabla 3

Componentes principales de una arquitectura SIEM

Componente	Función principal
Fuentes de eventos	Generación de logs y eventos de seguridad
Colectores de eventos	Recepción y transporte de registros
Normalización	Estandarización de formatos de eventos
Motor de correlación	Relación entre eventos para identificar patrones
Almacenamiento	Conservación e indexación de registros
Dashboards	Visualización y monitoreo de eventos
Sistema de alertas	Notificación de actividades sospechosas

De manera similar, la arquitectura de un SIEM se fundamenta en la recopilación de eventos generados por estaciones de trabajo, servidores, dispositivos de red, aplicaciones y soluciones de seguridad. Posteriormente, dichos eventos son procesados mediante mecanismos de normalización y correlación que permiten transformar grandes volúmenes de registros en información útil para la detección de amenazas, generación de alertas y respuesta a incidentes.

De igual manera, los sistemas SIEM permiten centralizar los registros de seguridad en una base de datos especializada, desde donde se ejecutan procesos de análisis, generación de reportes, monitoreo en tiempo real y cumplimiento normativo. Esta capacidad proporciona una visión integral del estado de seguridad de la organización y mejora significativamente los procesos de auditoría e investigación forense.

Diseño y despliegue de SIEM con OpenSearch

Figura 1

Diagrama de flujo de solución SIEM

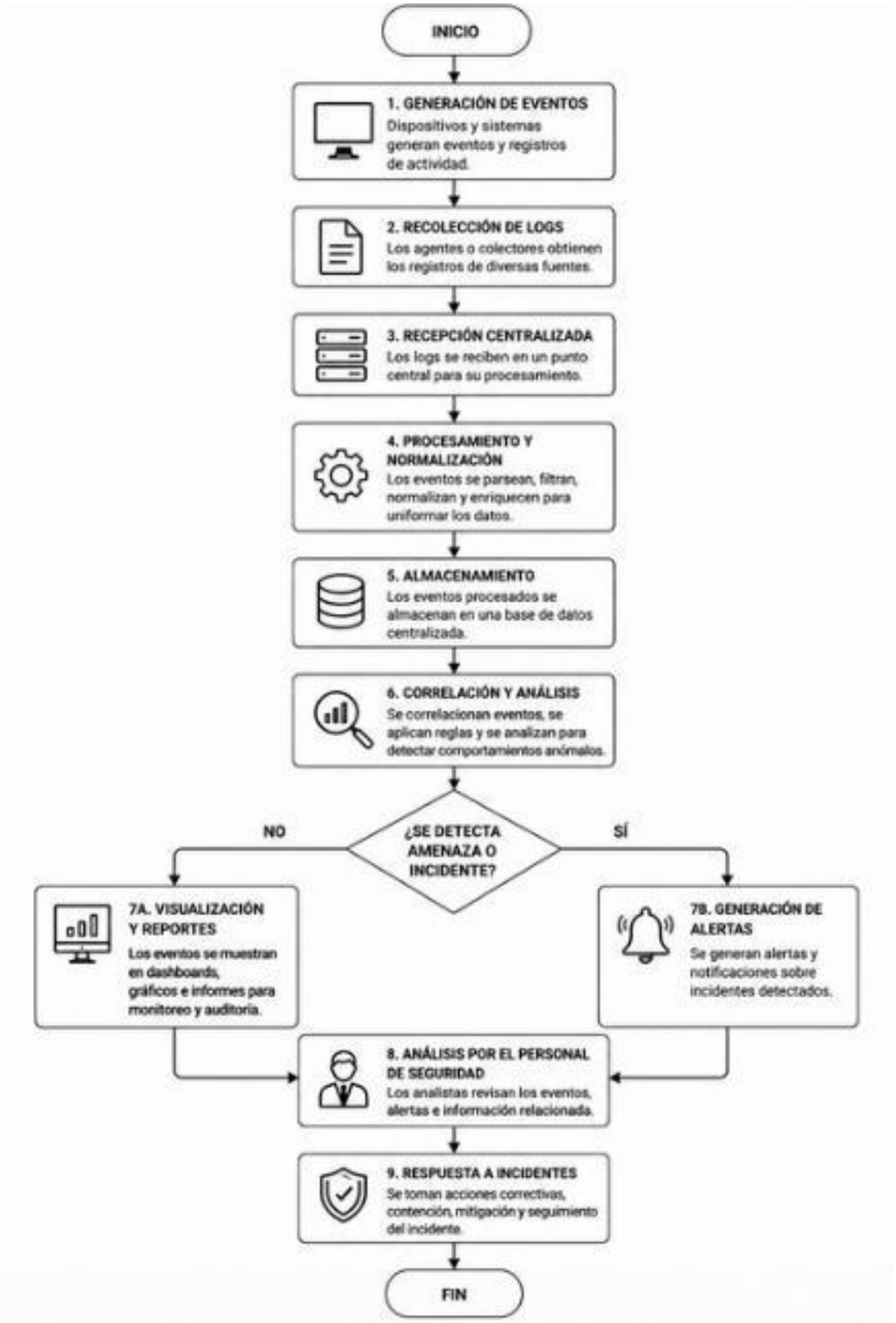
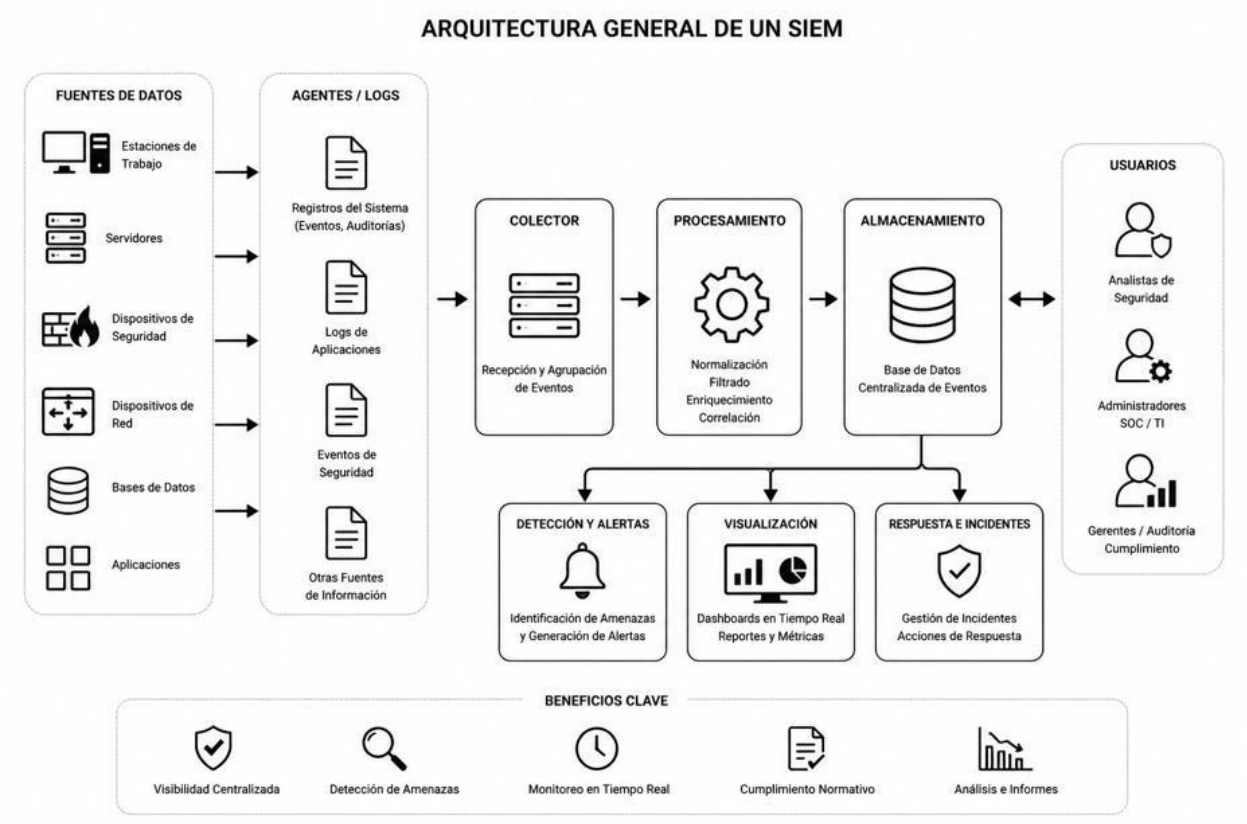


Figura 2

Arquitectura de recolección y procesamiento de eventos del SIEM



Nota. La figura presenta una representación general de la arquitectura funcional de un sistema SIEM, identificando sus principales componentes y el flujo de procesamiento de la información desde la generación de eventos hasta la detección y gestión de incidentes de seguridad.

MITRE ATT&CK®

MITRE ATT&CK® es un marco de conocimiento ampliamente utilizado en ciberseguridad para clasificar las tácticas, técnicas y procedimientos (TTPs) empleados por los adversarios durante las diferentes fases de un ciberataque. Este framework proporciona una estructura estandarizada para analizar comportamientos maliciosos y diseñar mecanismos de detección basados en patrones de ataque observados en escenarios reales (MITRE ATT&CK, 2026; Strom et al., 2020).

Diseño y despliegue de SIEM con OpenSearch

De acuerdo con Strom et al. (2020), ATT&CK permite modelar tácticas, técnicas y procedimientos (TTPs) utilizados por actores maliciosos, facilitando la construcción de estrategias de monitoreo y detección más efectivas dentro de plataformas SIEM.

Por otra parte, investigaciones recientes destacan que ATT&CK se ha consolidado como uno de los frameworks más utilizados para el análisis de amenazas y validación de capacidades de detección dentro de arquitecturas SOC y SIEM modernas (Bader et al., 2023).

Estructura del Framework MITRE ATT&CK®

El framework ATT&CK organiza el conocimiento sobre el comportamiento de los atacantes mediante una estructura jerárquica compuesta por tácticas, técnicas y subtécnicas. Esta clasificación permite describir las diferentes etapas de un ataque y los métodos utilizados para alcanzar objetivos específicos dentro de una infraestructura tecnológica.

Las tácticas representan el objetivo que persigue un atacante durante una fase determinada del ataque, mientras que las técnicas describen los métodos empleados para lograr dicho objetivo. Por su parte, las subtécnicas proporcionan un nivel adicional de detalle sobre la forma específica en que una técnica puede ser ejecutada.

Según MITRE ATT&CK (2026), esta estructura facilita la estandarización de mecanismos de detección, el análisis de amenazas y la evaluación de capacidades defensivas dentro de organizaciones públicas y privadas. Asimismo, permite mapear eventos de seguridad y reglas de correlación hacia comportamientos reales observados en campañas de ataque.

La utilización de tácticas, técnicas y subtécnicas proporciona una base común para el diseño de mecanismos de monitoreo y detección, facilitando la identificación de brechas de cobertura y el fortalecimiento de las funcionalidades de seguridad dentro de los sistemas SIEM.

Diseño y despliegue de SIEM con OpenSearch

El framework ATT&CK organiza el conocimiento sobre el comportamiento de los atacantes mediante diferentes niveles de clasificación. La Tabla 4 presenta los componentes principales que conforman la estructura del framework.

Tabla 4

Componentes principales del framework MITRE ATT&CK®

Componente	Descripción
Táctica	Objetivo que persigue el atacante durante una fase del ataque
Técnica	Método utilizado para alcanzar una táctica específica
Subtécnica	Variante detallada de una técnica
Procedimiento	Implementación real observada de una técnica durante un ataque

Diseño y despliegue de SIEM con OpenSearch

Figura 3

Matriz Enterprise del framework MITRE ATT&CK®

Nota. Reproducido de "MITRE ATT&CK®," por The MITRE Corporation, 2026 (https://attack.mitre.org/). Todos los derechos reservados [2026] por The MITRE Corporation. Reproducido con permiso del autor.

Diseño y despliegue de SIEM con OpenSearch

Integración SIEM con MITRE ATT&CK®

La integración entre plataformas SIEM y el framework ATT&CK permite desarrollar mecanismos de detección basados en tácticas y técnicas utilizadas por atacantes reales. Este enfoque facilita la construcción de reglas de correlación alineadas a comportamientos observados en incidentes de ciberseguridad, mejorando la capacidad de detección dentro de la infraestructura monitoreada.

De acuerdo con Bader et al. (2023), ATT&CK se ha consolidado como uno de los frameworks más utilizados para modelar tácticas, técnicas y procedimientos (TTPs) dentro de arquitecturas SOC y plataformas SIEM modernas, debido a su capacidad para estandarizar procesos de monitoreo y detección.

Dentro de los sistemas SIEM, las reglas de correlación pueden asociarse con técnicas ATT&CK para identificar patrones relacionados con fuerza bruta, escaneo de servicios, autenticación sospechosa y cambios administrativos en dispositivos de seguridad. Este enfoque facilita la detección contextual de amenazas y permite evaluar la cobertura de monitoreo implementada.

Por otra parte, el mapeo entre reglas SIEM y técnicas ATT&CK permite validar qué tácticas y técnicas quedan cubiertas dentro del entorno monitoreado. Esto facilita la identificación de brechas de detección y fortalece las características de monitoreo y análisis de seguridad.

La utilización de ATT&CK dentro de entornos de laboratorio permite ejecutar escenarios controlados de ataque orientados a validar la efectividad de las reglas de correlación implementadas en el SIEM, facilitando el análisis de capacidades de detección frente a técnicas reales de ciberataque.

Diseño y despliegue de SIEM con OpenSearch

La adopción del framework ATT&CK dentro de plataformas SIEM se ha consolidado como una práctica ampliamente utilizada para mejorar la visibilidad de amenazas y evaluar capacidades de detección. Farouk et al. (2024) destacan que la utilización de ATT&CK permite relacionar eventos observados con comportamientos reales de adversarios, proporcionando un mecanismo estandarizado para analizar coberturas defensivas y validar reglas de detección dentro de entornos corporativos.

Mapeo de Detecciones SIEM con MITRE ATT&CK®

Uno de los principales beneficios de la integración entre plataformas SIEM y el framework ATT&CK consiste en la posibilidad de asociar reglas de detección con tácticas y técnicas específicas utilizadas por los atacantes. Este enfoque permite relacionar eventos observados dentro de la infraestructura con comportamientos descritos en escenarios reales de ciberataque.

De acuerdo con Bader et al. (2023), el mapeo de mecanismos de detección hacia tácticas y técnicas facilita la evaluación de cobertura defensiva y la identificación de brechas dentro de las capacidades de monitoreo desplegadas. Asimismo, proporciona un lenguaje común para la clasificación y análisis de amenazas dentro de los centros de operaciones de seguridad.

Las plataformas SIEM modernas utilizan este enfoque para diseñar reglas de correlación orientadas a identificar actividades asociadas con diferentes fases de un ataque. La relación entre eventos observados y técnicas ATT&CK permite mejorar el contexto de las alertas generadas y facilitar el análisis de incidentes de seguridad.

El uso de mecanismos de mapeo también permite medir el nivel de cobertura alcanzado por las reglas implementadas, identificando qué tácticas y técnicas son monitoreadas dentro de la infraestructura y cuáles requieren mecanismos adicionales de detección.

Diseño y despliegue de SIEM con OpenSearch

Con el propósito de ilustrar la relación entre escenarios de detección y técnicas ATT&CK, la Tabla 5 presenta algunos ejemplos de mapeo utilizados comúnmente en plataformas SIEM para el diseño de reglas de correlación y mecanismos de detección.

Tabla 5

Ejemplos de mapeo entre escenarios de detección y técnicas MITRE ATT&CK®

Escenario de detección	Técnica ATT&CK	Descripción	Táctica
Fuerza bruta	T1110	Intentos repetidos de autenticación para obtener acceso	Credential Access
Escaneo de servicios	T1046	Descubrimiento de servicios disponibles en sistemas remotos	Discovery
Creación de usuario local en FortiGate	T1136.001	Creación de una cuenta local en un dispositivo de seguridad	Persistence
Creación de usuario administrador en FortiGate	T1098	Asignación o modificación de privilegios administrativos	Persistence
Cambios en políticas u objetos de firewall	T1562	Modificación de controles de seguridad perimetral	Defense Evasion
Enumeración de cuentas	T1087	Obtención de información sobre usuarios y cuentas	Discovery
Descubrimiento de red	T1016	Identificación de configuraciones y recursos de red	Discovery

Diseño y despliegue de SIEM con OpenSearch

Recolección y Centralización de Logs

La recolección y centralización de logs constituye uno de los procesos fundamentales dentro de las arquitecturas SIEM, debido a que permite consolidar eventos provenientes de múltiples dispositivos y sistemas en una plataforma centralizada de monitoreo y análisis.

Los logs representan registros de eventos generados por dispositivos de red, sistemas operativos, aplicaciones y herramientas de seguridad, los cuales contienen información relacionada con autenticación, conexiones, actividad del sistema, tráfico de red y eventos de seguridad.

Según Kent & Souppaya (2006), la centralización de logs facilita la correlación de eventos, mejora la visibilidad de amenazas y optimiza los procesos de monitoreo y análisis dentro de infraestructuras empresariales.

Dentro de las arquitecturas SIEM modernas, la recolección de eventos puede realizarse mediante diferentes mecanismos y protocolos, entre los cuales destacan Syslog, agentes de recolección y pipelines de procesamiento de eventos.

La centralización de logs permite consolidar eventos provenientes de diferentes fuentes dentro de una única plataforma de monitoreo, facilitando la correlación multi-fuente y la detección temprana de actividades sospechosas.

Herramientas de Recolección y Procesamiento de Eventos

Las arquitecturas SIEM modernas requieren mecanismos capaces de recopilar, transportar, procesar y enriquecer eventos provenientes de múltiples fuentes. Para cumplir este objetivo, existen diversas herramientas especializadas que permiten implementar Pipelines de ingestión de datos orientados al monitoreo y análisis de seguridad. Por otra parte, el procesamiento y la normalización de los registros constituyen etapas fundamentales para facilitar

el análisis automatizado y la detección de anomalías dentro de plataformas SIEM (Zhu et al., 2018)

De acuerdo con Fluent Bit Project (2025), Fluent Bit es un procesador y reenviador ligero de datos diseñado para recopilar y transmitir eventos desde estaciones de trabajo, servidores, dispositivos de red y contenedores hacia plataformas centralizadas de análisis. Su bajo consumo de recursos y capacidad de integración con múltiples tecnologías lo convierten en una solución ampliamente utilizada para la recolección distribuida de logs dentro de arquitecturas SIEM.

Por su parte, Fluentd constituye una plataforma open source orientada a la agregación, transformación y enrutamiento de eventos provenientes de múltiples fuentes. Según Fluentd Project (2025), su arquitectura basada en plugins permite implementar procesos de filtrado, normalización y envío de información hacia motores de almacenamiento y análisis, facilitando la integración de diferentes sistemas dentro de una infraestructura de monitoreo de seguridad.

La correcta identificación de plantillas y estructuras dentro de los registros constituye un paso fundamental para facilitar tareas posteriores de correlación, detección y análisis de incidentes, ya que permite transformar eventos heterogéneos en información estructurada apta para su procesamiento automatizado (Vaarandi & Bah¸sibah¸si, 2024).

Adicionalmente, Osquery es una herramienta de monitoreo de endpoints que permite consultar información del sistema operativo mediante sentencias SQL. De acuerdo con Osquery Project (2025), esta capacidad facilita la obtención de información relacionada con procesos, usuarios, servicios, conexiones activas, dispositivos y actividad del sistema, proporcionando datos relevantes para los procesos de detección y análisis de amenazas. La integración de información proveniente de los endpoints con eventos de red mejora significativamente la

correlación de actividades sospechosas y proporciona un mayor contexto para la detección de intrusiones (Haas et al., 2020)

Por otra parte, Syslog constituye uno de los protocolos más utilizados para la transmisión de eventos y registros dentro de infraestructuras tecnológicas. Según Gerhards (2009), Syslog proporciona un mecanismo estandarizado para el envío de logs desde dispositivos de red, sistemas operativos y aplicaciones hacia servidores centralizados de monitoreo. Su amplia compatibilidad con firewalls, switches, routers y puntos de acceso facilita la integración de eventos provenientes de diferentes fabricantes dentro de plataformas SIEM.

La combinación de herramientas como Fluent Bit, Fluentd, Osquery y Syslog permite implementar mecanismos eficientes de adquisición, transporte y procesamiento de eventos, proporcionando la información necesaria para las tareas de correlación, detección y monitoreo dentro de los sistemas SIEM modernos.

Análisis de Impacto en Endpoints

La implementación de agentes de telemetría en estaciones de trabajo requiere un equilibrio entre la exhaustividad de la visibilidad y el mantenimiento del rendimiento operativo. En este entorno, se desplegaron los agentes Osquery y Fluent Bit para la recolección de eventos y logs. Para validar su viabilidad, se realizó una medición del consumo de recursos en una estación de trabajo con sistema operativo Windows 11 Pro, equipada con 12GB de RAM y procesador Intel Core i5.

Resultados de Rendimiento

Durante la ejecución de las consultas de Osquery programadas (snapshot queries) y el envío continuo de logs mediante Fluent Bit, se obtuvieron las siguientes métricas promedio de consumo:

Tabla 6

Métricas de consumo

Agente	Uso de CPU (%)	Uso de RAM (MB)
Osquery	0.2% - 0.6%	1,7 - 11 MB
Fluent Bit	0.2% - 2.3%	9,5 – 11,5 MB
Total, Combinado	**0.4% - 2.9%**	**11,2 – 22,5 MB**

Los picos de CPU registrados en Osquery y Fluent Bit ocurren únicamente durante la ejecución programada de la consulta (cada 60 segundos), retornando a niveles de reposo inferiores al 0.2% inmediatamente después.

Figura 4

Consumo de recurso de Osquery

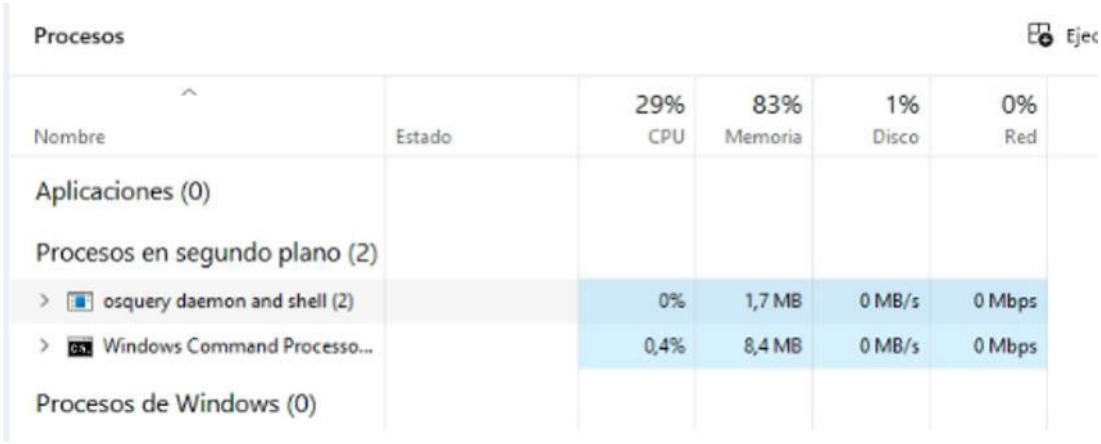
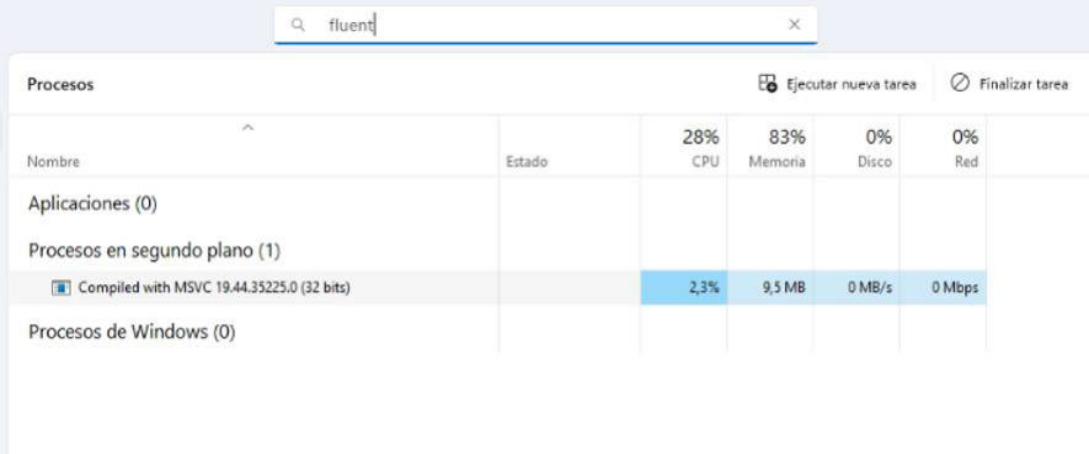


Figura 5

Consumo de recurso de Fluent Bit



Justificación del Intervalo de Monitoreo

Se ha establecido un intervalo de ejecución de 60 segundos como configuración estándar para el despliegue. Esta elección se justifica bajo los siguientes criterios técnicos:

- Equilibrio entre latencia y carga: Un intervalo inferior a 60 segundos aumentaría la frecuencia de despertar (*wake-up*) de los procesos del agente, elevando la carga del procesador sin ofrecer una ventaja significativa en la detección de incidentes.
- Visibilidad operativa: La ventana de un minuto permite capturar la mayoría de los intentos de persistencia, ejecución de procesos maliciosos y cambios en la configuración del endpoint en un tiempo adecuado para una respuesta ante incidentes (IR).
- Mitigación de "jitter": Al programar consultas cada 60 segundos, se minimiza la probabilidad de que múltiples endpoints saturen la red simultáneamente con el envío de telemetría hacia el servidor del SIEM, garantizando una ingesta de datos fluida.

Diseño y despliegue de SIEM con OpenSearch

Reglas de Detección y Alertamiento

Las reglas de detección constituyen mecanismos utilizados por los sistemas SIEM para identificar eventos o comportamientos que puedan representar una amenaza para la seguridad de la información. Estas reglas permiten analizar eventos individuales o correlacionados mediante condiciones previamente definidas, generando alertas cuando se cumplen determinados criterios de detección.

De acuerdo con OpenSearch Project (2026), las plataformas SIEM modernas incorporan motores de detección capaces de evaluar eventos en tiempo real mediante reglas basadas en umbrales, patrones de comportamiento y correlación de múltiples eventos provenientes de diferentes fuentes.

Las reglas de detección pueden clasificarse en reglas basadas en firmas, reglas basadas en comportamiento y reglas de correlación. Las reglas basadas en firmas permiten identificar eventos previamente conocidos, mientras que las reglas basadas en comportamiento buscan detectar actividades anómalas respecto al comportamiento esperado de usuarios, sistemas o dispositivos. Por su parte, las reglas de correlación permiten relacionar múltiples eventos dentro de una ventana temporal determinada para identificar patrones asociados a posibles incidentes de seguridad.

La generación de alertas constituye una de las funciones principales de los sistemas SIEM. Una alerta representa una notificación generada cuando una regla de detección identifica un evento o conjunto de eventos que requieren atención por parte del personal de seguridad. Estas alertas permiten priorizar incidentes, facilitar el monitoreo continuo y mejorar la capacidad de respuesta frente a amenazas potenciales.

Diseño y despliegue de SIEM con OpenSearch

La combinación de mecanismos de detección y alertamiento permite transformar grandes volúmenes de eventos en información útil para los procesos de monitoreo, análisis y respuesta dentro de los centros de operaciones de seguridad (SOC).

Dashboards y Visualización de Seguridad

Los dashboards de seguridad constituyen herramientas de visualización utilizadas en los sistemas SIEM para presentar de forma gráfica y centralizada la información obtenida a partir de los eventos de seguridad recolectados desde múltiples fuentes. Su principal objetivo es facilitar el monitoreo continuo, la identificación de anomalías y el análisis oportuno de incidentes dentro de una infraestructura tecnológica.

De acuerdo con OpenSearch Project (2026), los dashboards permiten representar información mediante gráficos, tablas, indicadores y métricas que facilitan la interpretación de grandes volúmenes de datos generados por dispositivos de red, sistemas operativos, aplicaciones y herramientas de seguridad.

Dentro de las arquitecturas SIEM modernas, los dashboards son utilizados para visualizar eventos de seguridad en tiempo real, tendencias históricas, alertas generadas por reglas de detección, actividades de usuarios y comportamientos potencialmente sospechosos. Estas capacidades permiten mejorar la visibilidad operacional y apoyar la toma de decisiones durante los procesos de monitoreo y análisis de seguridad.

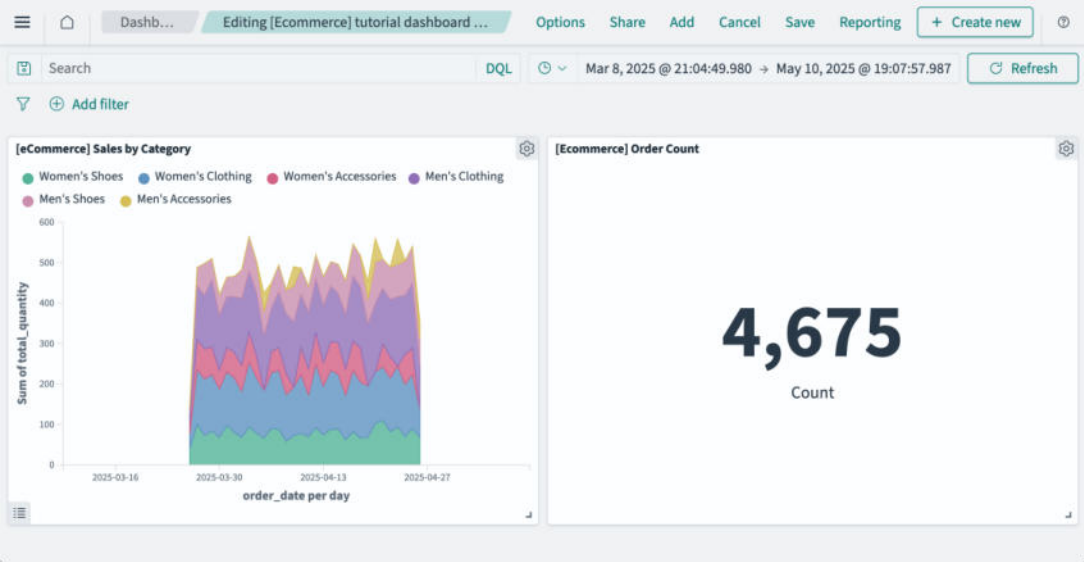
Según Kent & Souppaya (2006), la visualización adecuada de eventos facilita la identificación de patrones de comportamiento, la correlación de actividades relacionadas y la detección temprana de incidentes que podrían pasar desapercibidos al analizar registros individuales.

Los dashboards pueden incorporar indicadores relacionados con autenticaciones exitosas y fallidas, eventos de red, generación de alertas, actividad de dispositivos, consumo de recursos y distribución temporal de eventos. La representación visual de esta información permite reducir el tiempo requerido para identificar comportamientos anómalos y mejorar la eficiencia de los procesos de monitoreo de seguridad.

En el contexto de los sistemas SIEM basados en OpenSearch, los dashboards constituyen uno de los principales mecanismos para la visualización centralizada de eventos y resultados de correlación, permitiendo consolidar información proveniente de múltiples fuentes dentro de una única interfaz de monitoreo.

Figura 6

Ejemplo de dashboard para visualización de eventos y métricas en OpenSearch Dashboards



Nota. Reproducido de (OpenSearch Project, 2026)

Como podemos ver en la Figura 6

Ejemplo de dashboard para visualización de eventos y métricas en OpenSearch Dashboards, se muestra un ejemplo de dashboard utilizado para la representación gráfica de métricas y

eventos dentro de plataformas basadas en OpenSearch. Este Tipo de visualizaciones permite consolidar grandes volúmenes de información en una interfaz centralizada, facilitando el monitoreo continuo y el análisis de eventos de seguridad

Simulación de Escenarios de Ataque

La simulación de escenarios de ataque constituye una práctica ampliamente utilizada para validar la efectividad de los mecanismos de monitoreo y detección implementados dentro de plataformas SIEM. Mediante la ejecución controlada de actividades que representan comportamientos reales de adversarios, es posible verificar la capacidad de las reglas de correlación para identificar eventos sospechosos y generar alertas oportunas.

De acuerdo con (MITRE ATT&CK, 2026), la utilización de tácticas y técnicas documentadas dentro del framework permite reproducir comportamientos observados en incidentes reales de ciberseguridad, facilitando la evaluación de capacidades defensivas y la validación de mecanismos de detección. Este enfoque es ampliamente utilizado por equipos SOC y analistas de seguridad para medir la cobertura de monitoreo frente a diferentes escenarios de amenaza.

Los entornos de laboratorio representan una alternativa adecuada para la ejecución de pruebas controladas, debido a que permiten generar eventos de seguridad sin afectar infraestructuras productivas. Asimismo, facilitan la observación del comportamiento del sistema SIEM ante diferentes patrones de ataque y la validación de reglas de correlación alineadas al framework ATT&CK.

Entre los escenarios de ataque comúnmente utilizados para evaluar sistemas SIEM se encuentran los intentos de fuerza bruta sobre servicios de autenticación, el descubrimiento y escaneo de servicios de red, la enumeración de cuentas y cambios administrativos en dispositivos

de seguridad. Estas actividades generan eventos que pueden ser correlacionados por el SIEM para identificar comportamientos asociados a técnicas específicas descritas dentro del framework ATT&CK.

La ejecución de escenarios controlados de ataque permite analizar métricas como tiempo medio de detección (MTTD), tasa de detección, generación de alertas y cobertura de técnicas ATT&CK. Estas métricas proporcionan evidencia objetiva sobre el desempeño del sistema y permiten determinar el nivel de efectividad alcanzado por los mecanismos de monitoreo implementados.

Métricas de Evaluación en Sistemas SIEM

La evaluación del desempeño de un sistema SIEM requiere el uso de métricas que permitan medir objetivamente su capacidad para detectar, correlacionar y presentar eventos de seguridad relevantes. Estas métricas facilitan el análisis de la efectividad de los mecanismos de monitoreo implementados y permiten comparar el rendimiento de diferentes arquitecturas de detección.

De acuerdo con Kent & Souppaya (2006), las métricas de monitoreo de seguridad constituyen un mecanismo fundamental para determinar la capacidad de una organización para identificar y responder oportunamente ante incidentes de seguridad.

Una de las métricas más utilizadas en entornos SIEM es el Tiempo Medio de Detección (Mean Time To Detect, MTTD), el cual representa el tiempo transcurrido entre la ocurrencia de un evento o incidente y su detección por parte de los mecanismos de monitoreo. Un valor reducido de MTTD indica una mayor capacidad para identificar amenazas de forma temprana.

Otra métrica relevante corresponde a la tasa de detección, la cual mide la proporción de eventos o escenarios de ataque que son identificados correctamente por las reglas de detección

implementadas. Esta métrica permite evaluar la efectividad de los mecanismos de correlación y alertamiento configurados dentro del sistema.

Asimismo, la tasa de falsos positivos representa la cantidad de alertas generadas incorrectamente ante actividades legítimas. La reducción de falsos positivos constituye uno de los principales objetivos de las plataformas SIEM modernas, debido a que permite optimizar el trabajo de análisis y reducir la fatiga operativa de los equipos de seguridad.

En entornos alineados al framework ATT&CK también resulta relevante evaluar la cobertura de detección. Esta métrica permite determinar qué tácticas y técnicas del framework se encuentran cubiertas por las reglas implementadas dentro del sistema SIEM, proporcionando una visión del nivel de protección alcanzado frente a diferentes escenarios de ataque.

La evaluación del desempeño de un sistema SIEM requiere indicadores que permitan medir objetivamente su capacidad de detección y monitoreo. La Tabla 7 resume algunas de las métricas más utilizadas para analizar la efectividad de estas plataformas.

Tabla 7

Principales métricas utilizadas para evaluar sistemas SIEM

Métrica	Descripción	Objetivo
MTTD	Tiempo medio requerido para detectar un incidente	Reducir el tiempo de identificación de amenazas
Tasa de detección	Porcentaje de eventos detectados correctamente	Medir efectividad de las reglas
Tasa de falsos positivos	Alertas incorrectas generadas por el sistema	Evaluar precisión de detección
Cobertura ATT&CK	Técnicas y tácticas cubiertas por las reglas implementadas	Medir alcance de monitoreo

Las métricas de evaluación permiten medir objetivamente el desempeño de un sistema SIEM y determinar su capacidad para detectar, correlacionar y presentar eventos de seguridad relevantes. Estas métricas proporcionan criterios cuantificables para evaluar la efectividad de los mecanismos de monitoreo implementados y validar el cumplimiento de los objetivos de detección establecidos.

Además de identificar las métricas relevantes, es necesario establecer mecanismos que permitan cuantificar su comportamiento. La Tabla 8 presenta los métodos de cálculo utilizados para evaluar el desempeño de los sistemas SIEM dentro de escenarios de prueba controlados.

Tabla 8

Cálculo de métricas de evaluación

Métrica	Método de cálculo
MTTD	Tiempo de detección − tiempo de ocurrencia
Tasa de detección	Eventos detectados / eventos simulados × 100
Falsos positivos	Alertas incorrectas / alertas totales × 100
Cobertura ATT&CK	Técnicas cubiertas / técnicas evaluadas × 100

Estas métricas permiten evaluar cuantitativamente el desempeño del sistema SIEM. El MTTD mide la rapidez de detección de incidentes, la tasa de detección evalúa la efectividad de las reglas implementadas, la tasa de falsos positivos permite medir la precisión de las alertas generadas y la cobertura ATT&CK determina el nivel de protección alcanzado frente a las técnicas evaluadas dentro de los escenarios de prueba.

Diseño y despliegue de SIEM con OpenSearch

Tendencias Actuales en Sistemas SIEM

Los sistemas SIEM continúan evolucionando para responder al incremento de amenazas avanzadas y al crecimiento exponencial del volumen de datos generado por infraestructuras modernas. Una de las principales tendencias identificadas en investigaciones recientes es la incorporación de algoritmos de aprendizaje automático para complementar los mecanismos tradicionales de correlación basados en reglas.

De acuerdo con Nurusheva et al. (2024), los algoritmos de machine learning permiten identificar patrones anómalos dentro de grandes volúmenes de eventos, mejorando la capacidad de detección frente a amenazas desconocidas y reduciendo la dependencia de firmas previamente definidas. Asimismo, estas capacidades permiten complementar las funciones tradicionales de monitoreo y correlación implementadas por las plataformas SIEM.

Paralelamente, la integración de inteligencia de amenazas (Threat Intelligence) se ha convertido en un componente fundamental para fortalecer los procesos de detección y análisis de seguridad. Según Falasi & Zhang (2025), la incorporación de fuentes externas de inteligencia permite enriquecer los eventos observados dentro de la infraestructura y mejorar la capacidad para identificar indicadores de compromiso asociados con campañas maliciosas activas.

Estas tendencias reflejan la evolución de los SIEM hacia plataformas más inteligentes, capaces de combinar correlación de eventos, análisis contextual e inteligencia de amenazas para fortalecer las capacidades de monitoreo y detección dentro de las organizaciones.

Desarrollo Del Trabajo

El desarrollo del presente proyecto consistió en el diseño, implementación y validación de una solución SIEM basada en OpenSearch para la centralización, procesamiento, correlación y visualización de eventos de seguridad dentro de un entorno corporativo de laboratorio. Este proceso siguió un enfoque estructurado de análisis, diseño, implementación y validación, acorde con metodologías propuestas para la adopción de plataformas SIEM en entornos empresariales (Rosenberg et al., 2023).

Para la implementación se utilizó una infraestructura compuesta por dispositivos físicos de red y seguridad, estaciones de trabajo, servidores y plataformas de virtualización, con el propósito de simular un entorno similar al encontrado en organizaciones medianas. La arquitectura desarrollada permitió integrar eventos provenientes de diferentes fuentes mediante tecnologías open source orientadas al monitoreo continuo de seguridad.

La solución implementada estuvo conformada por OpenSearch como plataforma central de almacenamiento y análisis de eventos, OpenSearch Dashboards para visualización y monitoreo, Fluentd para agregación y procesamiento de logs, Fluent Bit para recolección de eventos desde estaciones de trabajo Windows, Data Prepper para la ingestión de información proveniente de endpoints mediante Pipelines HTTP y Syslog para la integración de dispositivos de red y seguridad.

Como fuentes de eventos se integraron un firewall FortiGate 80F, un punto de acceso Aruba AP-505, un switch core Aruba CX 8360, un switch de acceso Aruba 2930, estaciones de trabajo Windows 11, un servidor Windows Server 2025 con servicios Active Directory y DNS, servidores Ubuntu Linux y un equipo Kali Linux utilizado para la simulación de escenarios de ataque.

Diseño y despliegue de SIEM con OpenSearch

Durante el desarrollo se implementaron mecanismos de centralización de logs, normalización de eventos, construcción de dashboards de monitoreo y preparación de escenarios de validación orientados a medir la capacidad de detección y correlación de la solución SIEM propuesta.

Para validar la solución implementada se ejecutaron escenarios controlados asociados a fuerza bruta SSH, descubrimiento de red, creación de cuentas en Active Directory y cambios administrativos sobre FortiGate. Estos escenarios permitieron validar técnicas ATT&CK como T1110, T1046, T1136, T1136.001, T1098 y T1562, verificando la generación de eventos, la activación de reglas de detección, la generación de hallazgos y el envío de alertas mediante OpenSearch Security Analytics y OpenSearch Alerting.. La evidencia de validación se presenta en las secciones 3.6.1 y 3.6.2.

Análisis De Requerimientos Técnicos Y De Seguridad

Previo a la implementación de la solución SIEM, se realizó un análisis de los requerimientos técnicos y de seguridad necesarios para soportar las funciones de recolección, procesamiento, almacenamiento y visualización de eventos provenientes de múltiples fuentes dentro del entorno corporativo de laboratorio.

El análisis permitió identificar los recursos de hardware, software y conectividad requeridos para garantizar la correcta operación de OpenSearch, Fluentd, Fluent Bit, Data Prepper y OpenSearch Dashboards, así como la integración de dispositivos de red, seguridad, servidores y estaciones de trabajo.

Diseño y despliegue de SIEM con OpenSearch

Requerimientos De Hardware

La infraestructura utilizada para el despliegue de la solución SIEM fue implementada sobre una plataforma de virtualización Proxmox VE 9.0.3 instalada en un servidor físico con procesador Intel Xeon E-2224 de cuatro núcleos y 64 GB de memoria RAM.

La máquina virtual destinada al servidor SIEM fue configurada con 2 vCPU, 8 GB de memoria RAM y un disco virtual de 60 GB, ejecutando Ubuntu Server 24.04 LTS como sistema operativo base. Adicionalmente, se dispuso de almacenamiento externo de 500 GB para respaldo y conservación de información generada durante las pruebas del laboratorio.

Tabla 9

Requerimientos de hardware del servidor SIEM

Componente	Especificación
Plataforma de virtualización	Proxmox VE 9.0.3
Procesador del host	Intel Xeon E-2224 (4 núcleos)
Memoria RAM del host	64 GB
Sistema operativo SIEM	Ubuntu Server 24.04 LTS
CPU asignada al SIEM	2 vCPU
Memoria RAM asignada	8 GB
Disco virtual	60 GB
Almacenamiento adicional	500 GB

*Nota***.** Recursos de hardware utilizados durante la implementación de la solución SIEM en el entorno de laboratorio.

Los recursos descritos corresponden a la implementación realizada durante el proyecto y no representan los requerimientos mínimos para replicar la solución.

Diseño y despliegue de SIEM con OpenSearch

Requerimientos de Software

La plataforma SIEM fue construida principalmente utilizando herramientas open source, incluyendo OpenSearch, OpenSearch Dashboards, Fluentd, Fluent Bit, Data Prepper, Osquery y Docker Compose. Sin embargo, algunas fuentes de eventos utilizadas durante la validación corresponden a soluciones comerciales, específicamente FortiGate 80F y equipos Aruba, mientras que el servicio SMTP utilizado para las notificaciones fue Gmail.

Tabla 10

Componentes de software implementados

Componente	Función principal
Ubuntu Server 24.04 LTS	Sistema operativo del SIEM
OpenSearch	Almacenamiento e indexación de eventos
OpenSearch Dashboards	Visualización y monitoreo
Fluentd	Procesamiento y agregación de logs
Fluent Bit	Recolección de eventos de endpoints
Data Prepper	Ingestión de datos mediante Pipelines
Docker Compose	Orquestación de contenedores
Syslog	Recepción de eventos de red y seguridad
Osquery	Inventario y monitoreo de endpoints

Requerimientos de Seguridad

La implementación de la solución SIEM requirió definir una serie de requerimientos de seguridad orientados a garantizar la visibilidad centralizada de los eventos generados dentro de la infraestructura tecnológica del laboratorio. Estos requerimientos permitieron establecer las

capacidades mínimas necesarias para la detección, monitoreo y análisis de actividades potencialmente sospechosas.

Uno de los principales requerimientos consistió en la capacidad de recopilar eventos provenientes de múltiples fuentes, incluyendo dispositivos de seguridad, infraestructura de red, servidores y estaciones de trabajo. Esto permitió disponer de una visión unificada de la actividad generada dentro del entorno monitoreado.

Asimismo, se estableció la necesidad de centralizar los registros de eventos en una única plataforma, facilitando las tareas de búsqueda, análisis forense y correlación de información. La centralización de eventos constituye uno de los princIPios fundamentales de los sistemas SIEM, debido a que permite reducir la dispersión de información y mejorar la capacidad de detección de incidentes.

Otro requerimiento importante fue la capacidad de correlacionar eventos provenientes de diferentes dispositivos y sistemas con el propósito de identificar patrones de comportamiento asociados a posibles amenazas de seguridad. Para ello, la solución debía permitir la implementación de reglas de detección alineadas con técnicas y tácticas descritas en el framework ATT&CK.

Adicionalmente, se definió como requisito la generación de alertas ante eventos considerados relevantes para la seguridad, permitiendo notificar oportunamente actividades que requieran análisis o intervención por parte del administrador del sistema.

Finalmente, la solución debía proporcionar mecanismos de visualización y monitoreo mediante dashboards interactivos que facilitaran el análisis de eventos, la identificación de tendencias y el seguimiento de indicadores relacionados con la seguridad de la infraestructura.

Tabla 11

Requerimientos de seguridad de la solución SIEM

ID	Requerimiento	Evidencia de cumplimiento
RS-01	Centralizar eventos de seguridad provenientes de múltiples fuentes	Integración exitosa de FortiGate, Aruba, Windows y Linux en OpenSearch
RS-02	Almacenar eventos de manera organizada para análisis posterior	Creación de índices especializados FortiGate-*, Aruba-*, security-* y metrics-*
RS-03	Correlacionar eventos de diferentes dispositivos y sistemas	Implementación de reglas de correlación en Security Analytics
RS-04	Generar alertas ante actividades sospechosas	Alertas generadas automáticamente y visualizadas en OpenSearch Alerting
RS-05	Facilitar el monitoreo mediante dashboards	Dashboards implementados para infraestructura, endpoints y seguridad
RS-06	Permitir detección alineada con ATT&CK	Reglas asociadas a T1110 Brute Force, T1046 Network Service Discovery, T1136.001-002 Create Account

Diseño de la Arquitectura del SIEM

La arquitectura de la solución SIEM fue diseñada siguiendo un modelo de recolección, procesamiento, almacenamiento y visualización centralizada de eventos de seguridad. El objetivo principal consistió en integrar información proveniente de diferentes dispositivos de red, seguridad, servidores y estaciones de trabajo dentro de una única plataforma de monitoreo.

La arquitectura implementada se compone de cuatro capas principales: adquisición de eventos, procesamiento y normalización, almacenamiento y correlación, y visualización. Cada una de estas capas cumple una función específica dentro del flujo de procesamiento de información de seguridad.

Diseño y despliegue de SIEM con OpenSearch

La capa de adquisición está conformada por las fuentes generadoras de eventos, incluyendo el firewall FortiGate 80F, el punto de acceso Aruba AP-505, los switches Aruba CX 8360 y Aruba 2930F, estaciones de trabajo Windows 11, un servidor Windows Server 2025 y servidores Ubuntu Linux. Los eventos son recolectados mediante Syslog, Fluent Bit y Osquery dependiendo del Tipo de dispositivo.

La capa de procesamiento está integrada por Fluentd y Data Prepper. Fluentd recibe eventos mediante Syslog y Fluent Pipelines, realizando tareas de clasificación y enrutamiento hacia índices específicos de OpenSearch. Por su parte, Data Prepper procesa eventos provenientes de endpoints mediante Pipelines HTTP especializados para métricas, procesos, programas instalados y puertos de red.

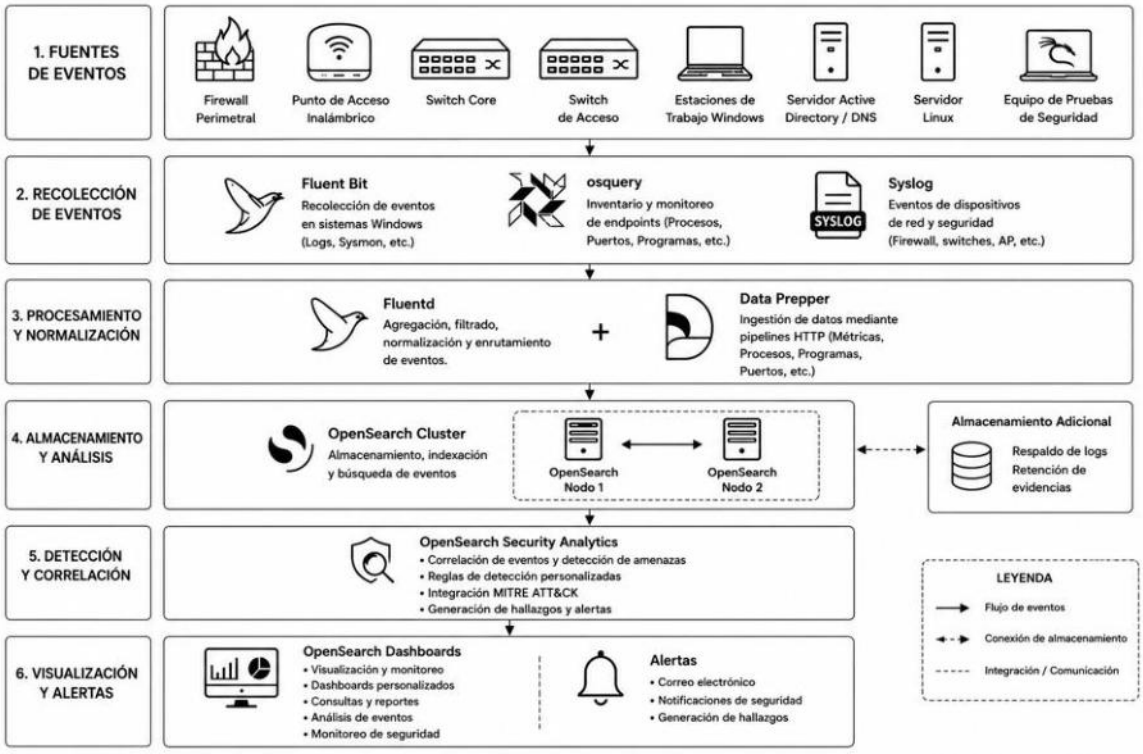
La capa de almacenamiento y análisis está conformada por OpenSearch, desplegado mediante contenedores Docker y configurado como repositorio central para la indexación y consulta de eventos. Finalmente, OpenSearch Dashboards proporciona la capa de visualización mediante dashboards interactivos utilizados para monitoreo, análisis y detección de eventos de seguridad.

La comunicación entre componentes se realiza mediante Syslog UDP 514 para dispositivos Fortinet y Aruba, HTTP puerto 2021 para la recepción de eventos provenientes de Fluent Bit y Osquery hacia Data Prepper, y HTTPS puerto 9200 para la indexación y consulta de información dentro de OpenSearch.

Diseño y despliegue de SIEM con OpenSearch

Figura 7

Arquitectura implementada de la solución SIEM



Cada componente cumple una función específica dentro del flujo de procesamiento de eventos. Las fuentes generan registros de seguridad, Fluent Bit y Fluentd realizan la recolección y procesamiento, Data Prepper ejecuta la ingestión y clasificación de datos provenientes de endpoints, OpenSearch almacena y correlaciona la información, mientras que OpenSearch Dashboards proporciona capacidades de visualización, monitoreo y alertamiento.

Tabla 12

Componentes principales de la arquitectura SIEM

Componente	Función
FortiGate	Generación de eventos de seguridad perimetral
Aruba AP-505	Generación de eventos inalámbricos
Aruba CX 8360	Eventos de red del núcleo
Aruba 2930F	Eventos de acceso
Windows 11	Eventos de endpoint
Windows Server 2025	Eventos de Active Directory y DNS
Ubuntu Server	Server Linux
Fluent Bit	Recolección de eventos Windows
Osquery	Inventario y monitoreo de endpoints
Fluentd	Procesamiento y agregación de eventos
Data Prepper	Ingestión mediante Pipelines HTTP
OpenSearch	Almacenamiento y análisis
OpenSearch Dashboards	Visualización y monitoreo

Implementación del Entorno de Laboratorio

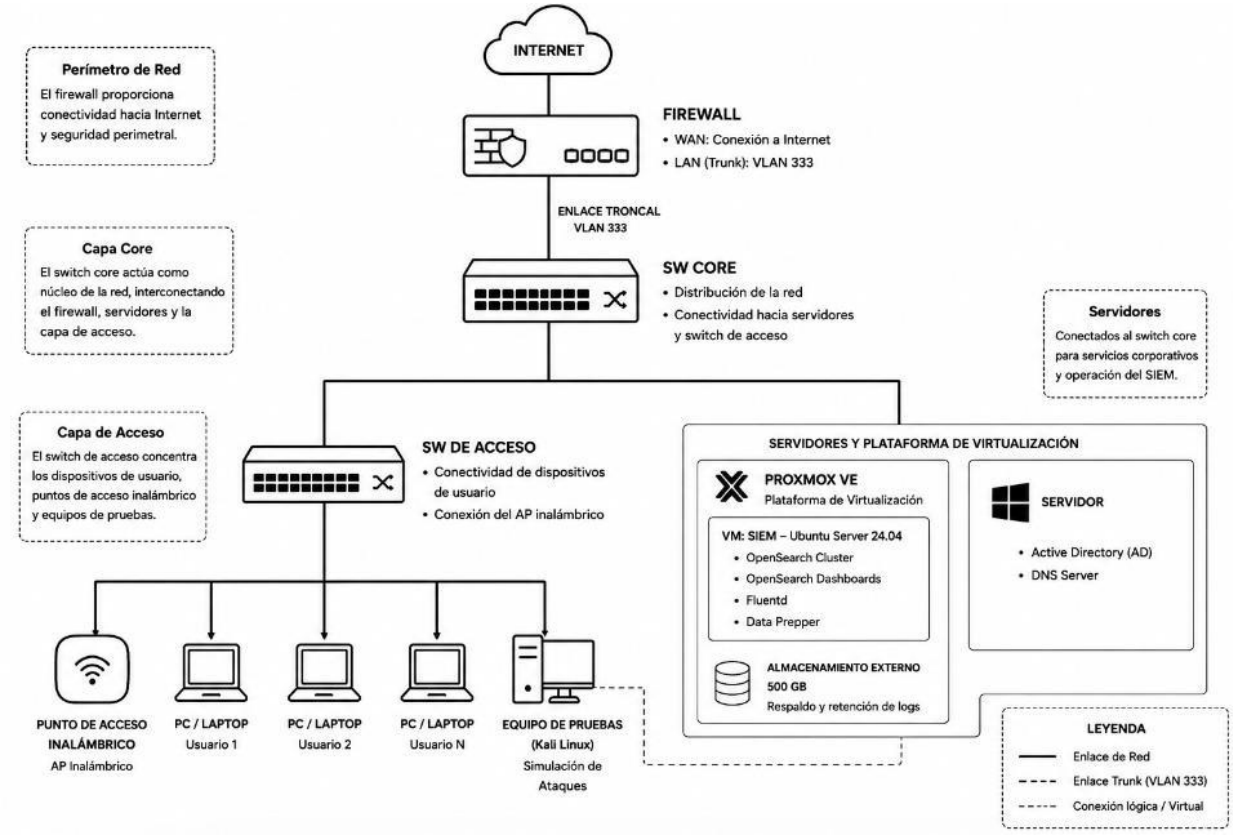
Con el propósito de validar la solución SIEM propuesta, se implementó un entorno corporativo de laboratorio que permitió simular la operación de una infraestructura tecnológica compuesta por dispositivos de red, seguridad, servidores y estaciones de trabajo. La finalidad de este entorno fue generar eventos reales de seguridad para evaluar los procesos de recolección, procesamiento, almacenamiento, correlación y visualización implementados dentro de la plataforma SIEM basada en OpenSearch.

Diseño y despliegue de SIEM con OpenSearch

La infraestructura fue diseñada siguiendo una arquitectura jerárquica compuesta por una capa perimetral, una capa de núcleo y una capa de acceso. Adicionalmente, se incorporaron servidores físicos y virtuales encargados de proporcionar servicios de directorio, monitoreo y análisis de eventos. La Figura 6 presenta la arquitectura física implementada dentro del entorno de laboratorio.

Figura 8

Arquitectura física implementada dentro del entorno de laboratorio



*Nota***.** Elaboración propia basada en el SIEM instalado.

La Figura 6 presenta la arquitectura física implementada dentro del entorno de laboratorio. La infraestructura fue diseñada para simular una red corporativa compuesta por dispositivos de seguridad, infraestructura de acceso, servicios de directorio y estaciones de trabajo.

Diseño y despliegue de SIEM con OpenSearch

La conectividad perimetral fue proporcionada por un firewall FortiGate conectado a Internet mediante su interfaz WAN. Desde el firewall se estableció un enlace troncal utilizando la VLAN 333 hacia el switch core Aruba CX 8360, encargado de distribuir la conectividad hacia los diferentes segmentos de la red.

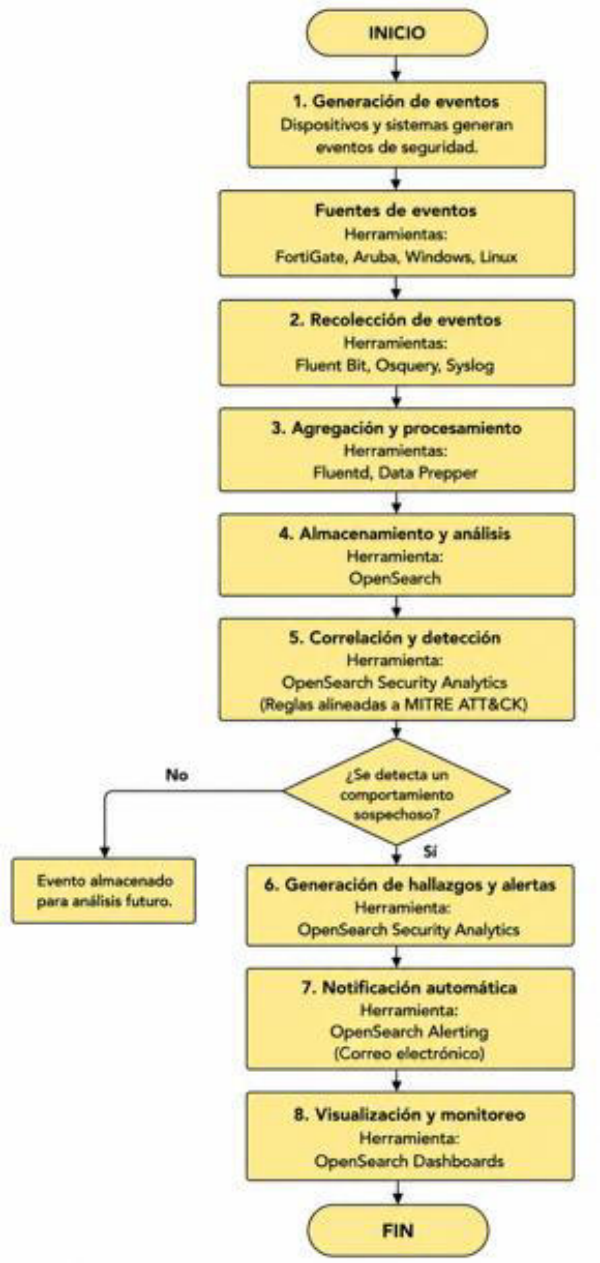
Sobre el switch core se conectaron los servidores utilizados para el laboratorio, incluyendo la plataforma Proxmox VE, donde fueron desplegadas las máquinas virtuales correspondientes al servidor SIEM basado en OpenSearch y al servidor Windows Server 2025 encargado de los servicios de Active Directory y DNS.

La capa de acceso fue implementada mediante un switch Aruba 2930F, al cual se conectaron las estaciones de trabajo Windows 11, el punto de acceso Aruba AP-505 y el equipo destinado a pruebas de seguridad. Sobre este último se ejecutó Kali Linux para la simulación de escenarios de ataque utilizados durante la validación de la solución SIEM.

Diseño y despliegue de SIEM con OpenSearch

Figura 9

Diagrama de flujo de eventos de seguridad



Toda la infraestructura operó sobre la VLAN 333 utilizada para los servicios de laboratorio. Las rutas principales de comunicación corresponden al envío Syslog hacia el

servidor SIEM (10.33.33.101), consultas DNS hacia Windows Server 2025 y tráfico de administración desde las estaciones de trabajo hacia los dispositivos de red y seguridad.

Tabla 13

Direccionamiento implementado

Equipo	IP
FortiGate	10.33.33.254
Aruba Core	10.33.33.113
Aruba Access	10.33.33.103
Aruba AP	10.33.33.106
SIEM	10.33.33.101
AD/DNS	10.33.33.105
Kali Linux	10.33.33.112
PC-01	10.33.33.100

*Nota***.** Detalle del direccionamiento de cada uno de los equipos del laboratorio.

Despliegue de la Plataforma SIEM

La plataforma SIEM fue desplegada sobre una máquina virtual Ubuntu Server 24.04 LTS alojada en el entorno de virtualización Proxmox VE. Para facilitar la administración, escalabilidad y mantenimiento de los componentes, se utilizó Docker Compose como mecanismo de orquestación de contenedores.

Aunque OpenSearch fue desplegado utilizando dos nodos lógicos (opensearch-node1 y opensearch-node2), ambos forman parte del mismo clúster de OpenSearch y se ejecutan como

contenedores Docker dentro de una única máquina virtual Ubuntu Server, compartiendo el mismo kernel del sistema operativo, el almacenamiento y los recursos físicos asignados al sistema anfitrión.

La justificación técnica para implementar dos nodos lógicos, en lugar de uno solo, se fundamenta en la optimización de la arquitectura interna de OpenSearch:

- **Optimización del procesamiento de índices:** La configuración con dos nodos permite una mejor organización lógica de los índices y de las tareas internas del motor OpenSearch, favoreciendo el procesamiento concurrente de consultas y operaciones de indexación durante la ingestión de eventos.
- **Distribución interna de la carga de trabajo:** La existencia de dos nodos permite que OpenSearch distribuya internamente determinadas tareas del motor de búsqueda, el procesamiento de reglas de Security Analytics y las consultas generadas desde OpenSearch Dashboards, mejorando la eficiencia operativa sin requerir múltiples servidores físicos.

En consecuencia, la solución implementada mantiene una arquitectura completamente centralizada tipo All-in-One. La utilización de dos nodos lógicos responde exclusivamente a requerimientos internos de funcionamiento del motor OpenSearch y no proporciona tolerancia a fallos, redundancia física, replicación entre servidores ni mecanismos de alta disponibilidad, ya que toda la plataforma depende de una única máquina virtual desplegada sobre el entorno Proxmox VE.

Figura 10

Contenedores Docker desplegados para la solución SIEM

```
siem01@siem01-Standard:~$ docker ps
CONTAINER ID   IMAGE                                          COMMAND                  CREATED      STATUS
    PORTS                                       NAMES
4853a24e00bf   nginx:1.27.4-alpine                            "/docker-entrypoint.…"   2 days ago   Up 2 day
s   0.0.0.0:8080->80/tcp, [::]:8080->80/tcp   nginx
5712bd8e8a8f   alpine:3.21.3                                  "/bin/sh -c 'apk add…"   2 days ago   Up 2 day
s   0.0.0.0:514->514/udp, [::]:514->514/udp, 0.0.0.0:5044-5045->5044-5045/tcp, [::]:5044-5045->5044-5045/tcp,
0.0.0.0:8022->2022/tcp, [::]:8022->2022/tcp   fluentd
adf681914c96   opensearchproject/opensearch-dashboards:latest   "./opensearch-dashbo…"   2 days ago   Up 2 day
s   0.0.0.0:5601->5601/tcp, [::]:5601->5601/tcp   opensearch-dashboards
75a61abfce2c   opensearchproject/opensearch:latest             "./opensearch-docker…"   2 days ago   Up 2 day
s   0.0.0.0:9200->9200/tcp, [::]:9200->9200/tcp, 9300/tcp, 0.0.0.0:9600->9600/tcp, [::]:9600->9600/tcp, 9650/t
cp                                          opensearch-node1
937c0e817907   opensearchproject/opensearch:latest             "./opensearch-docker…"   2 days ago   Up 2 day
s   9200/tcp, 9300/tcp, 9600/tcp, 9650/tcp   opensearch-node2
8ee2656d5cea   opensearchproject/data-prepper:latest           "bin/data-prepper"       3 days ago   Up 3 day
s                                           data-prepper
```

Los dos nodos OpenSearch fueron desplegados como contenedores Docker dentro de una misma máquina virtual Ubuntu Server 24.04. Aunque existen dos nodos lógicos para distribución de índices y servicios internos, ambos residen en un único host, manteniendo el enfoque All-in-One.

Integración de Fuentes de Eventos

Una vez desplegada la infraestructura del laboratorio y configurados los componentes principales del SIEM, se procedió a integrar las diferentes fuentes de eventos con el objetivo de centralizar la información de seguridad dentro de OpenSearch.

La integración fue realizada utilizando distintos mecanismos de recolección según las características de cada dispositivo o sistema operativo. Los dispositivos de red y seguridad fueron configurados para enviar eventos mediante Syslog, mientras que las estaciones de trabajo Windows utilizaron Fluent Bit y Osquery para la recolección de información relacionada con eventos del sistema operativo, procesos, programas instalados, métricas del sistema y conexiones de red.

Diseño y despliegue de SIEM con OpenSearch

Los eventos recibidos fueron procesados mediante Fluentd y Data Prepper antes de ser almacenados dentro de índices específicos de OpenSearch. Esta segmentación permitió organizar la información según su origen y facilitar posteriormente las tareas de búsqueda, análisis y correlación de eventos.

La Toda la infraestructura operó sobre la VLAN 333 utilizada para los servicios de laboratorio. Las rutas principales de comunicación corresponden al envío Syslog hacia el servidor SIEM (10.33.33.101), consultas DNS hacia Windows Server 2025 y tráfico de administración desde las estaciones de trabajo hacia los dispositivos de red y seguridad.

Tabla 13 presenta las fuentes de eventos integradas dentro de la solución SIEM y los mecanismos utilizados para su recolección.

Tabla 14

Integración de fuentes de eventos

Fuente de eventos	Método de recolección	Tipo de eventos aportados	Procesamiento	Destino
FortiGate	Syslog UDP 514	Eventos de tráfico permitido y bloqueado, políticas de seguridad, autenticaciones administrativas, creación de usuarios locales, asignación de privilegios administrativos, creación de objetos de dirección, cambios de configuración y eventos del sistema	Fluentd	OpenSearch
Aruba AP	Syslog UDP 514	Eventos de autenticación inalámbrica, asociación y desasociación de clientes, detección de Rogue AP, cambios de configuración y eventos WLAN	Fluentd	OpenSearch
Aruba Acceso	Syslog UDP 514	Eventos de acceso de usuarios, autenticación SSH, cambios de configuración, estado de interfaces y eventos VLAN	Fluentd	OpenSearch
Aruba CX Core	Syslog UDP 514	Eventos del núcleo de red, accesos administrativos SSH, cambios de configuración, enlaces físicos y eventos de conectividad	Fluentd	OpenSearch
Windows 11	Fluent Bit	Eventos Security, System, Sysmon, PowerShell, autenticaciones, procesos y actividad del sistema operativo	Fluentd	OpenSearch
Windows Server 2025	Fluent Bit	Eventos Active Directory, DNS, autenticaciones, privilegios, PowerShell y actividad del sistema	Fluentd	OpenSearch
Windows 11	Osquery	Inventario del sistema, procesos activos, programas instalados, puertos abiertos e información de red	Data Prepper	OpenSearch
Ubuntu Server	Syslog	Eventos SSH, autenticaciones, procesos, servicios y registros del sistema operativo Linux	Fluentd	OpenSearch

*Nota***.** La correcta recepción de los eventos fue validada mediante consultas en OpenSearch Discover y la verificación de documentos almacenados dentro de los índices FortiGate*-*,* Aruba-cor*-*, *Aruba-acc**- y siem-win*,

Diseño y despliegue de SIEM con OpenSearch

Integración de Dispositivos Fortinet y Aruba

La integración de los dispositivos de red y seguridad fue realizada mediante el protocolo Syslog, permitiendo centralizar los eventos generados por el firewall FortiGate, el punto de acceso Aruba AP-505, el switch Aruba CX 8360 y el switch Aruba 2930F dentro de la plataforma SIEM.

Para la recepción de eventos se configuró un servidor Syslog central ubicado en la dirección IP 10.33.33.101, correspondiente al servidor SIEM implementado sobre Ubuntu Server. Todos los dispositivos fueron configurados para enviar eventos utilizando el puerto UDP 514 y diferentes facilities Syslog, permitiendo posteriormente clasificar y enrutar los registros mediante Fluentd hacia índices específicos dentro de OpenSearch.

En el caso del firewall FortiGate, se configuró el envío de registros hacia el servidor SIEM utilizando la facility local4 y un nivel de severidad debug, permitiendo capturar eventos relacionados con tráfico de red, políticas de seguridad, autenticaciones y actividades administrativas.

Por otra parte, los dispositivos Aruba fueron configurados para enviar eventos al mismo servidor Syslog utilizando facilities diferenciadas. El punto de acceso Aruba AP-505 fue asociado a la facility local1, mientras que los switches Aruba 2930F y Aruba CX 8360 utilizaron la facility local 2 y 3 para el envío de eventos relacionados con conectividad, cambios de configuración, enlaces físicos y actividad de red.

La utilización de facilities independientes permitió implementar mecanismos de clasificación automática dentro de Fluentd, facilitando el almacenamiento de los eventos en índices específicos de OpenSearch y simplificando las tareas de análisis y monitoreo posteriores.

Figura 11

Configuración Syslog implementada en el firewall FortiGate

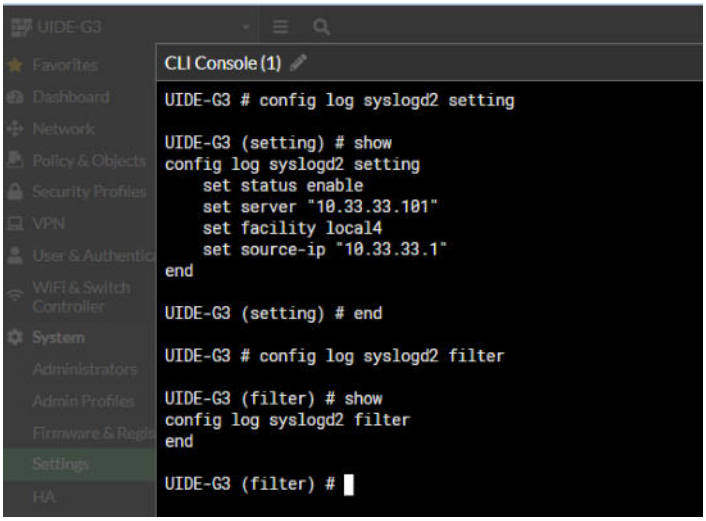


Figura 12

Configuración de exportación Syslog implementada en Aruba AP-505

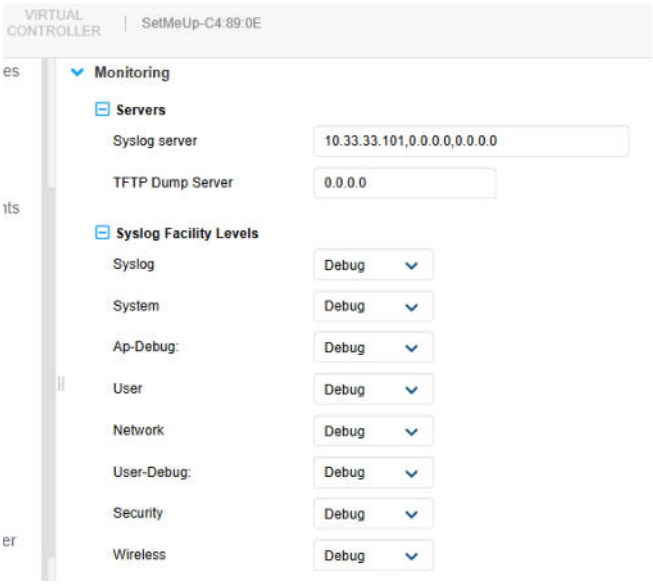


Figura 13

Configuración Syslog implementada en switches Aruba

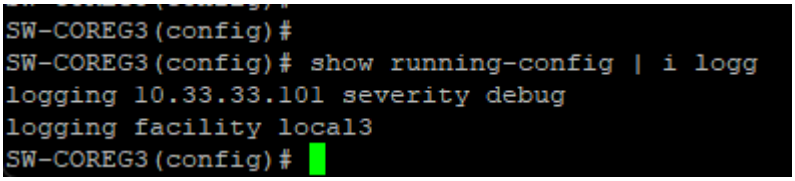


Figura 14

Configuración de Syslog implementada en switch Aruba

Tabla 15

Parámetros de integración Syslog implementados

Dispositivo	Servidor Syslog	Facility	Severidad
FortiGate 80F	10.33.33.101	local4	debug
Aruba AP-505	10.33.33.101	local1	debug
Aruba 2930F	10.33.33.101	local2	debug
Aruba CX 8360	10.33.33.101	Local3	debug

Diseño y despliegue de SIEM con OpenSearch

Clasificación y Almacenamiento de Eventos Mediante Fluentd

Una vez recibidos los eventos Syslog provenientes de los dispositivos Fortinet y Aruba, Fluentd fue utilizado como componente encargado de procesar, clasificar y enrutar la información hacia OpenSearch. Para ello se implementó una estrategia de segmentación basada en facilities Syslog, permitiendo identificar automáticamente el origen de los eventos y almacenarlos en índices independientes.

La clasificación fue configurada utilizando diferentes facilities para cada Tipo de dispositivo. Los eventos provenientes del punto de acceso Aruba AP-505 fueron asociados a la facility local1, mientras que los switches Aruba utilizaron facilities específicas para diferenciar eventos de acceso y núcleo de red. Por su parte, el firewall FortiGate fue configurado utilizando la facility local4.

Fluentd recibió los eventos mediante el puerto Syslog UDP 514 y aplicó reglas de enrutamiento que permitieron almacenar la información en índices específicos dentro de OpenSearch. Esta segmentación facilitó posteriormente la construcción de dashboards especializados y la implementación de reglas de detección orientadas a cada fuente de eventos.

La Figura 15 presenta los patrones de índices configurados dentro de OpenSearch para el almacenamiento de los eventos recibidos desde las diferentes fuentes integradas al SIEM.

Figura 15

Patrones de índices configurados en OpenSearch para la clasificación de eventos

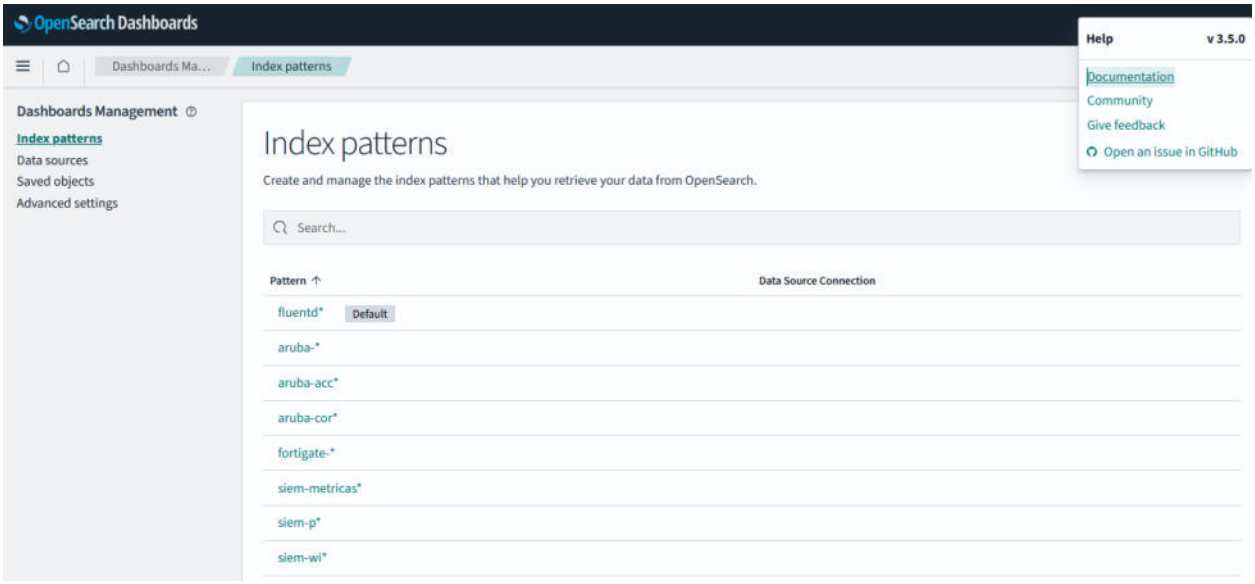


Tabla 16

Clasificación de eventos implementada mediante Fluentd

Facility Syslog	Fuente de eventos	Índice OpenSearch
local1	Aruba AP-505	Aruba-*
local2	Aruba 2930F	Aruba-acc-*
local3	Aruba CX 8360	Aruba-cor-*
local4	FortiGate	FortiGate-*

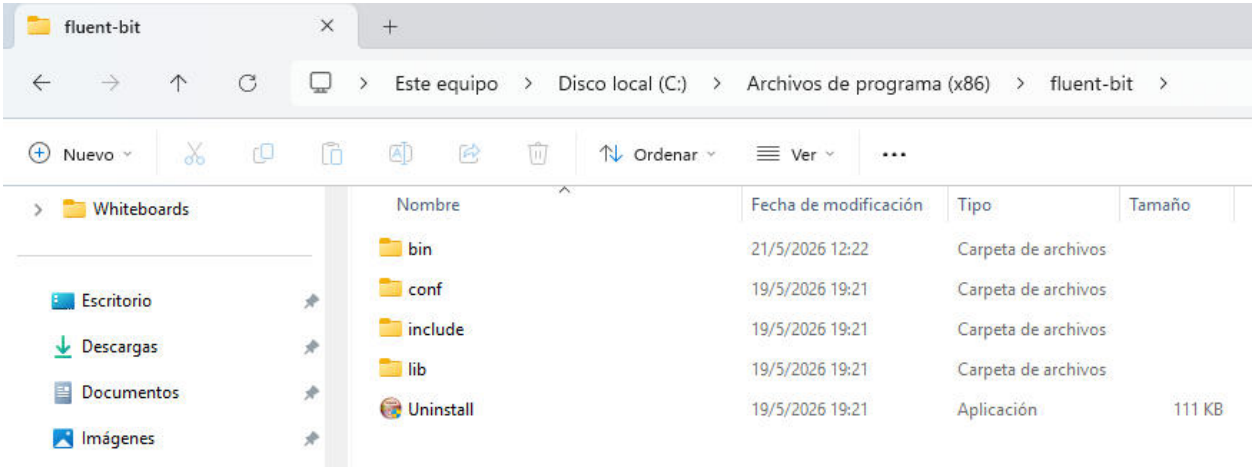
Integración de Eventos Windows Mediante Fluent Bit y Osquery

Con el objetivo de incorporar información proveniente de estaciones de trabajo Windows al sistema SIEM, se implementó Fluent Bit como agente de recolección de eventos. Esta herramienta fue instalada en los equipos cliente y configurada para capturar registros del sistema

operativo, eventos de seguridad, actividad de PowerShell, eventos Sysmon y métricas del sistema.

Figura 16

Herramienta instalada en sistemas Windows Fluent Bit

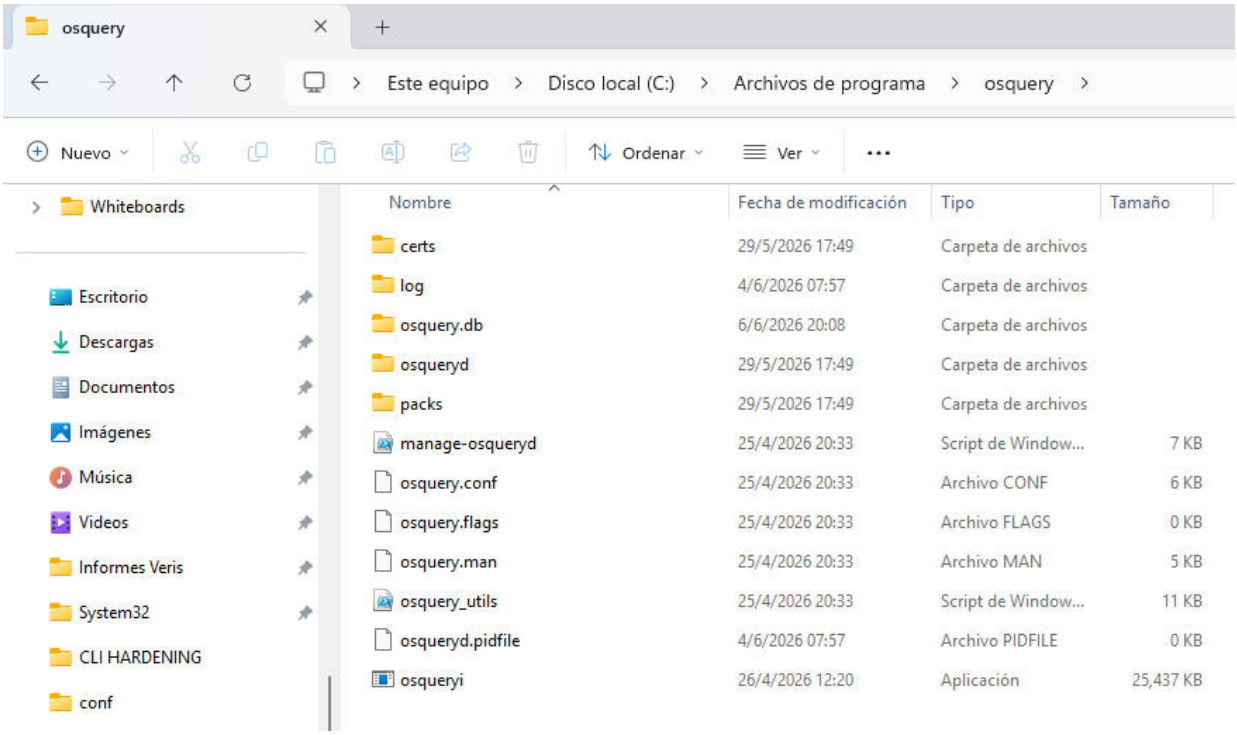


La configuración implementada permitió recopilar eventos provenientes de los canales Security, System, Microsoft-Windows-Sysmon/Operational y Microsoft-Windows-PowerShell/Operational. Adicionalmente, Fluent Bit fue utilizado para ejecutar consultas periódicas mediante Osquery, permitiendo obtener información relacionada con inventario de equipos, procesos críticos, programas instalados, interfaces de red y puertos abiertos.

Osquery ejecuta consultas programadas cada 60 segundos para recopilar información de inventario, procesos, programas instalados y puertos abiertos. Fluent Bit recibe estos resultados y los envía mediante peticiones HTTP al puerto 2021 de Data Prepper utilizando endpoints específicos para cada Tipo de información. Posteriormente, Data Prepper procesa los eventos recibidos y los almacena dentro de índices especializados en OpenSearch.

Figura 17

Herramienta instalada en sistemas Windows Osquery



Esta arquitectura permitió centralizar información de seguridad proveniente de los endpoints Windows y generar dashboards orientados al monitoreo de equipos, procesos, recursos del sistema y eventos de seguridad.

Figura 18

Eventos Windows almacenados en OpenSearch mediante Fluent Bit

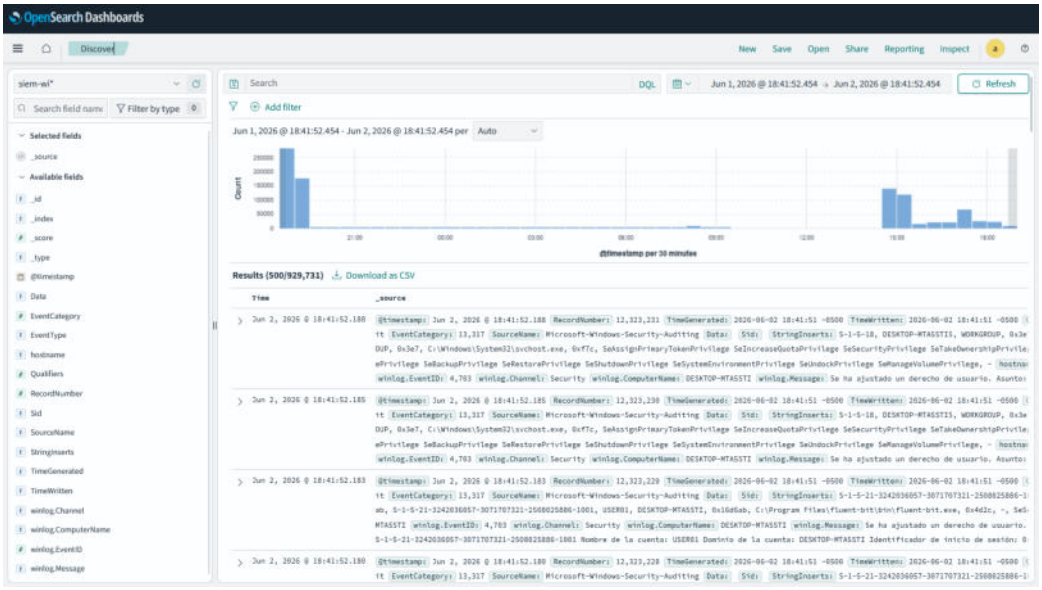
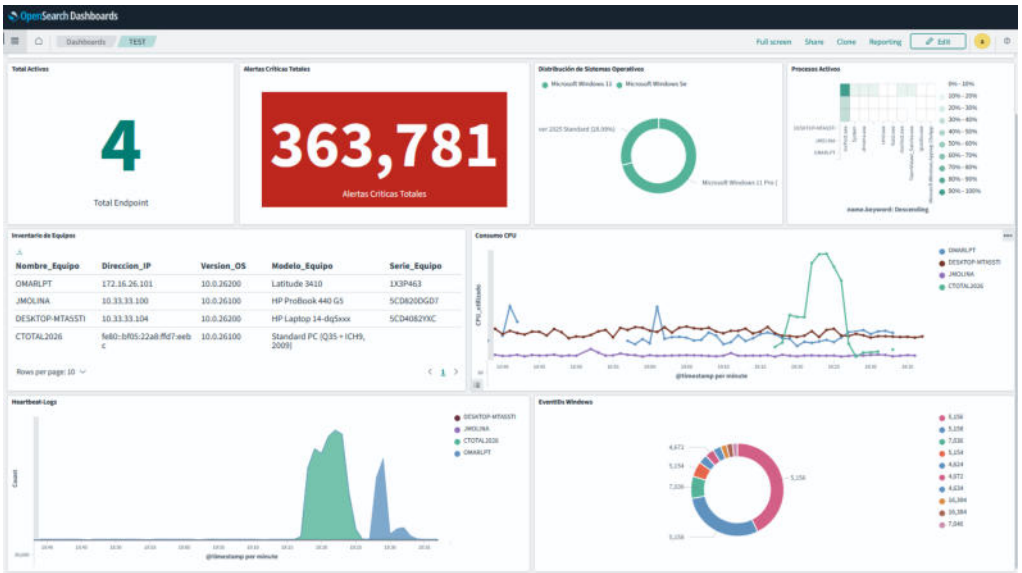


Figura 19

Dashboard de monitoreo de endpoints implementado en OpenSearch



El dashboard permite visualizar información consolidada de los endpoints monitoreados, incluyendo inventario de equipos, sistema operativo, procesos activos, consumo de CPU, eventos Windows y métricas recolectadas mediante Fluent Bit y Osquery.

Diseño y despliegue de SIEM con OpenSearch

La Figura 19 muestra el dashboard implementado para el monitoreo de endpoints dentro de OpenSearch Dashboards. Esta visualización permitió centralizar información operativa y de seguridad de los equipos Windows integrados al SIEM, facilitando el seguimiento de activos, recursos del sistema, eventos recolectados y posibles comportamientos anómalos.

Tabla 17

Canales Windows monitoreados mediante Fluent Bit

Canal	Información recopilada
Security	Eventos de autenticación y seguridad
System	Eventos del sistema operativo
Sysmon	Actividad avanzada de procesos y conexiones
PowerShell	Ejecución de comandos y scrIPts
Winstat	Métricas de rendimiento del equipo

Integración de Endpoints Mediante Osquery y Data Prepper

Con el propósito de ampliar las capacidades de monitoreo de endpoints, se integró Osquery como herramienta de consulta y recopilación de información del sistema operativo. La solución permitió ejecutar consultas periódicas sobre los equipos Windows utilizando sentencias SQL orientadas a obtener información relevante para procesos de monitoreo y análisis de seguridad.

Entre los datos recopilados se incluyeron versiones del sistema operativo, configuraciones de red, características de hardware, programas instalados, procesos considerados críticos y puertos abiertos. Esta información fue enviada por Fluent Bit hacia Data Prepper utilizando diferentes Pipelines especializados.

Diseño y despliegue de SIEM con OpenSearch

Para la recepción de los eventos se implementaron Pipelines independientes dentro de Data Prepper, permitiendo clasificar la información según su naturaleza y almacenarla posteriormente en índices específicos dentro de OpenSearch. Esta estrategia facilitó la organización de los datos y permitió construir dashboards orientados al monitoreo de activos y la detección de comportamientos potencialmente sospechosos.

La integración entre Osquery, Fluent Bit y Data Prepper proporcionó una capa adicional de visibilidad sobre los equipos monitoreados, complementando la información obtenida desde los registros tradicionales del sistema operativo.

Tabla 18

Pipelines implementados en Data Prepper

Pipeline	Información procesada	Endpoint de recepción	Índice OpenSearch
Metrics pipeline	Métricas del sistema operativo, CPU, memoria, disco y red	/metrics	metrics-*
Security pipeline	Eventos de seguridad de Windows, Sysmon y PowerShell	/security	security-*
prog-pipeline	Programas instalados y software inventariado	/programs	programs-*
proceso-pipeline	Procesos activos y servicios monitoreados	/process	process-*
puertos-pipeline	Puertos abiertos y conexiones activas	/ports	ports-*

Diseño y despliegue de SIEM con OpenSearch

Implementación de Dashboards de Monitoreo

La visualización de información constituye uno de los componentes fundamentales dentro de una plataforma SIEM, debido a que permite transformar grandes volúmenes de eventos en información comprensible para los analistas de seguridad. Para este propósito se utilizaron las capacidades de visualización proporcionadas por OpenSearch Dashboards, permitiendo construir paneles de monitoreo orientados al seguimiento de la infraestructura, los endpoints y los eventos de seguridad generados dentro del entorno de laboratorio.

Los dashboards implementados fueron diseñados para proporcionar una visión centralizada del estado de los equipos monitoreados, los eventos de seguridad recopilados y las alertas generadas por los mecanismos de detección. Asimismo, se incorporaron métricas relacionadas con inventario de activos, utilización de recursos, procesos críticos y eventos asociados a técnicas potencialmente maliciosas.

Tabla 19

Dashboards implementados en OpenSearch

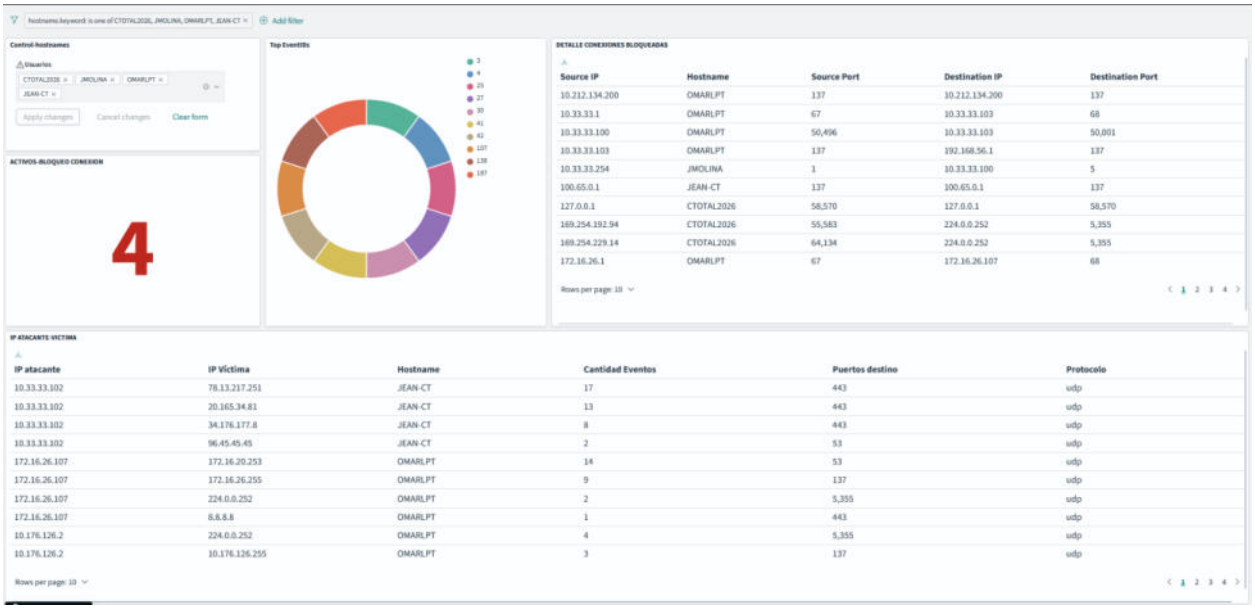
Dashboard	Objetivo	Fuente de datos	Visualizaciones principales	Indicadores monitoreados
Infraestructura Aruba	Monitorear dispositivos de red Aruba	Aruba AP, Aruba 2930F, Aruba CX 8360	Gráficos temporales, tablas de eventos, métricas de autenticación	Logins exitosos, logins fallidos, cambios de configuración, conexiones SSH
Endpoints	Supervisar estaciones de trabajo y servidores Windows	Fluent Bit y Osquery	Inventario, procesos, puertos, recursos del sistema	Procesos activos, programas instalados, puertos abiertos y métricas del sistema
Ataques	Analizar actividades sospechosas y tráfico bloqueado	FortiGate y Windows	Tablas, gráficos de eventos y distribución de ataques	Conexiones bloqueadas, IP origen, puertos destino y eventos críticos

Nota. Clasificación de dashboard realizados.

La utilización de dashboards especializados facilitó las tareas de supervisión continua, permitiendo identificar comportamientos anómalos y analizar la información generada por las diferentes fuentes integradas al SIEM.

Figura 20

Dashboard de monitoreo de infraestructura Aruba y eventos de seguridad

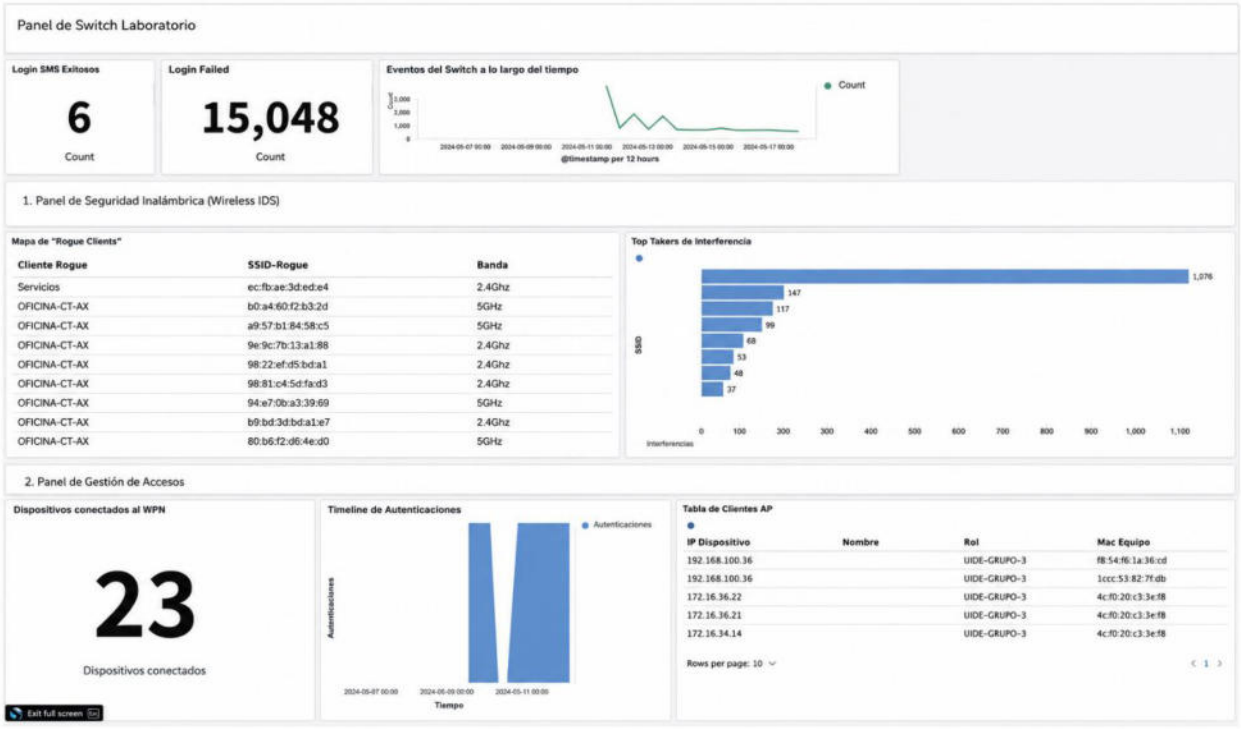


Nota. Captura obtenida del entorno de laboratorio. El dashboard permite visualizar eventos provenientes de switches Aruba y Aruba AP, incluyendo autenticaciones SSH, eventos de red, clientes inalámbricos, posibles clientes no autorizados y métricas relacionadas con la infraestructura de acceso.

La Figura 17 evidencia el dashboard construido para el monitoreo de la infraestructura Aruba integrada al SIEM. Esta visualización permitió centralizar eventos de red, autenticaciones, actividad inalámbrica y registros generados por los dispositivos de acceso, fortaleciendo la visibilidad operativa de la infraestructura corporativa de laboratorio.

Figura 21

Dashboard de monitoreo de infraestructura Aruba y actividad inalámbrica



Nota. Captura obtenida del entorno de laboratorio. El dashboard permite visualizar sesiones de acceso, dispositivos conectados a la red inalámbrica, eventos asociados al punto de acceso Aruba AP y autenticaciones SSH exitosas y fallidas hacia los switches Aruba integrados al SIEM.

La Figura 21 complementa la visualización de infraestructura Aruba mediante paneles orientados al análisis de actividad inalámbrica, sesiones de acceso y eventos de autenticación sobre dispositivos de red. Esta información permitió fortalecer la visibilidad operativa de la infraestructura de acceso dentro del entorno corporativo de laboratorio.

Diseño y despliegue de SIEM con OpenSearch

Implementación de Reglas de Detección y Correlación

La capacidad de detección constituye uno de los componentes más importantes dentro de una plataforma SIEM, debido a que permite identificar comportamientos potencialmente sospechosos a partir de los eventos recolectados desde las diferentes fuentes integradas. Con este propósito, se implementaron reglas de detección utilizando el módulo Security Analytics de OpenSearch.

Las reglas fueron configuradas considerando los escenarios efectivamente ejecutados dentro del entorno de laboratorio. Estos escenarios incluyeron intentos de fuerza bruta SSH contra dispositivos Aruba, actividades de reconocimiento de red mediante Nmap y eventos administrativos generados en Active Directory, específicamente la creación de una cuenta de dominio registrada mediante el Event ID 4720.

Para la construcción de las reglas se utilizaron como referencia las tácticas y técnicas definidas por el framework ATT&CK, permitiendo relacionar los eventos observados con comportamientos documentados dentro de escenarios reales de ataque. En este sentido, las reglas implementadas fueron asociadas principalmente con las técnicas T1110 Brute Force, T1046 Network Service Discovery y T1136.002 Domain Account.

Adicionalmente, se implementó una regla de correlación denominada “Fuerza bruta SSH y creación de cuenta en Active Directory”, cuyo propósito consistió en relacionar eventos de autenticación fallida mediante SSH con eventos administrativos posteriores en Active Directory. La lógica de correlación permite asociar intentos repetidos de acceso no autorizado con la creación de una cuenta de dominio dentro de una ventana temporal definida. Cuando ambas condiciones son detectadas, el sistema genera una alerta de criticidad alta y, según la

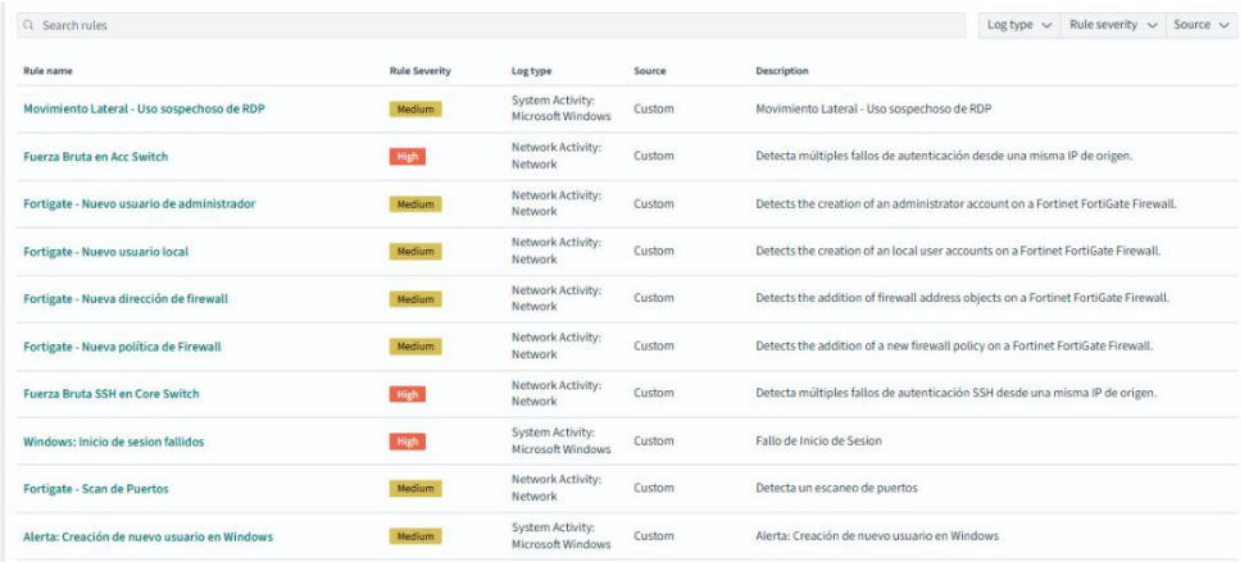
configuración de alertamiento, envía una notificación por correo electrónico al administrador del SIEM.

La implementación de estas capacidades permitió validar el funcionamiento del proceso de detección, correlación y alertamiento dentro de la solución SIEM desarrollada, utilizando únicamente eventos generados y evidenciados durante las pruebas realizadas en el entorno corporativo de laboratorio.

Adicionalmente, se implementaron reglas de detección para eventos administrativos generados por el firewall FortiGate 80F. Estas reglas permitieron identificar la creación de usuarios locales, la creación de usuarios con privilegios administrativos, la creación de políticas de firewall y la creación de objetos de dirección. Los hallazgos generados por OpenSearch Security Analytics permitieron validar eventos relacionados con persistencia, manipulación de cuentas y alteración de controles de seguridad perimetral.

Figura 22

Reglas de detección configuradas dentro de OpenSearch Security Analytics



Rule name	Rule Severity	Log type	Source	Description
Movimiento Lateral - Uso sospechoso de RDP	Medium	System Activity: Microsoft Windows	Custom	Movimiento Lateral - Uso sospechoso de RDP
Fuerza Bruta en Acc Switch	High	Network Activity: Network	Custom	Detecta múltiples fallos de autenticación desde una misma IP de origen.
Fortigate - Nuevo usuario de administrador	Medium	Network Activity: Network	Custom	Detects the creation of an administrator account on a Fortinet FortiGate Firewall.
Fortigate - Nuevo usuario local	Medium	Network Activity: Network	Custom	Detects the creation of an local user accounts on a Fortinet FortiGate Firewall.
Fortigate - Nueva dirección de firewall	Medium	Network Activity: Network	Custom	Detects the addition of firewall address objects on a Fortinet FortiGate Firewall.
Fortigate - Nueva política de Firewall	Medium	Network Activity: Network	Custom	Detects the addition of a new firewall policy on a Fortinet FortiGate Firewall.
Fuerza Bruta SSH en Core Switch	High	Network Activity: Network	Custom	Detecta múltiples fallos de autenticación SSH desde una misma IP de origen.
Windows: Inicio de sesion fallidos	High	System Activity: Microsoft Windows	Custom	Fallo de Inicio de Sesion
Fortigate - Scan de Puertos	Medium	Network Activity: Network	Custom	Detecta un escaneo de puertos
Alerta: Creación de nuevo usuario en Windows	Medium	System Activity: Microsoft Windows	Custom	Alerta: Creación de nuevo usuario en Windows

Figura 23

Regla de correlación Acceso Inicial y Creación de Cuenta

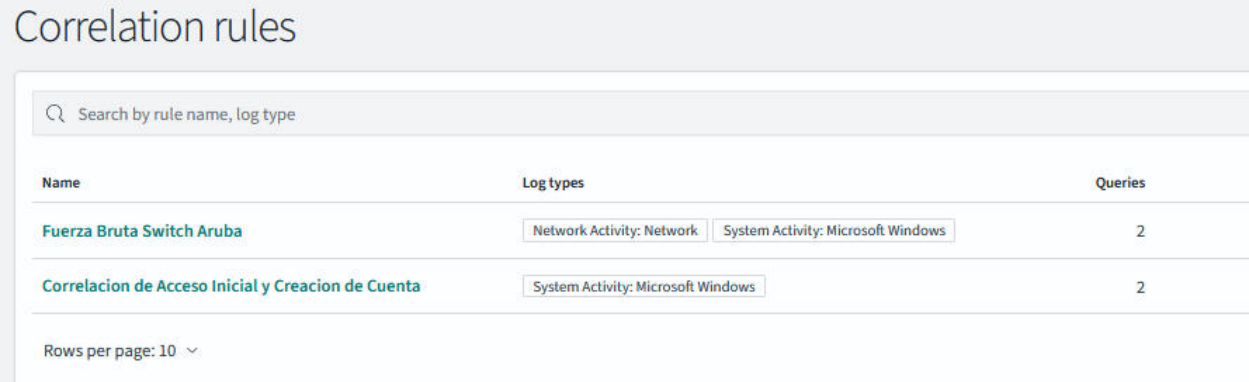
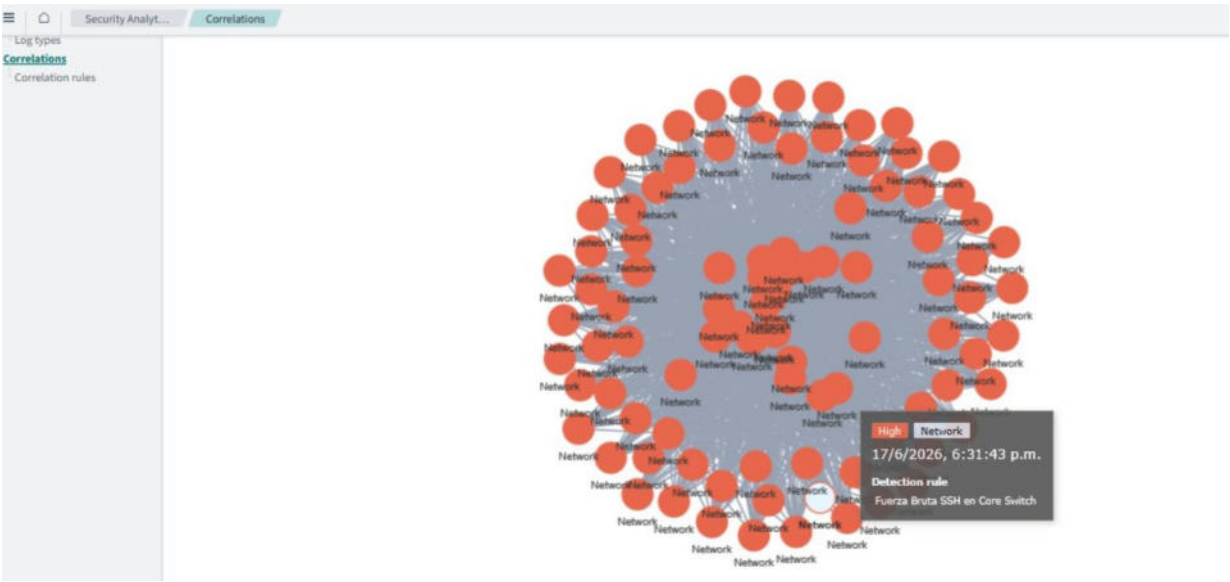


Figura 24

Visualización gráfica de eventos correlacionados en OpenSearch Security Analytics



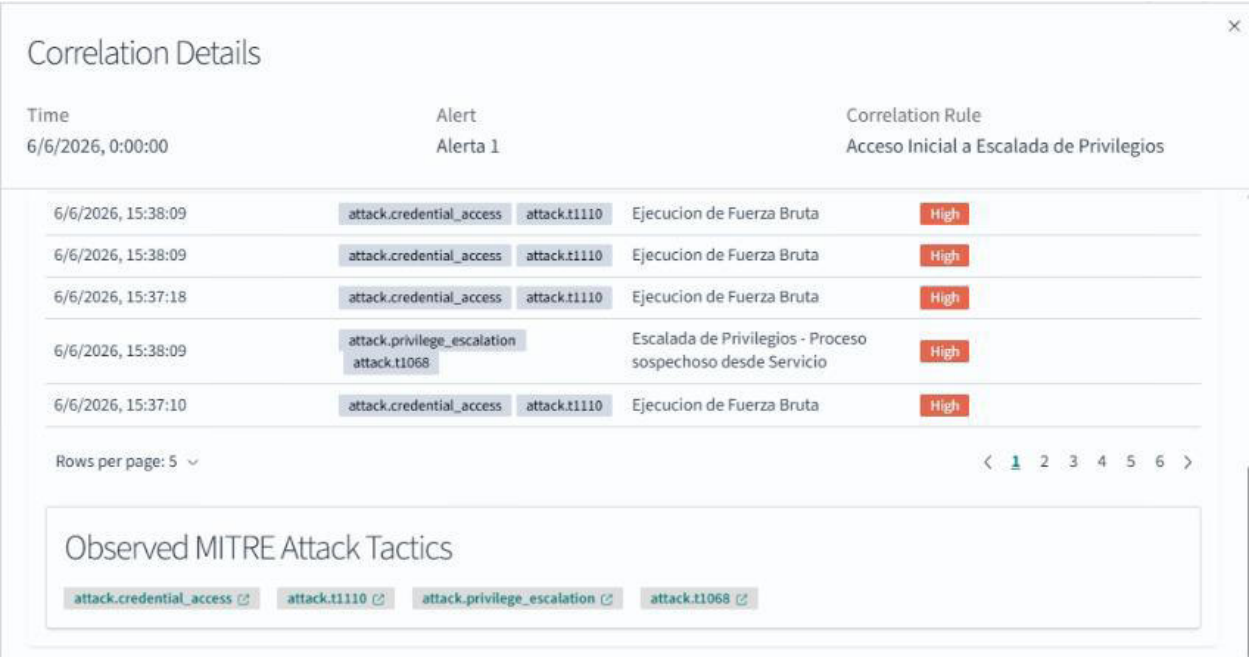
Nota. Captura obtenida del entorno de laboratorio. La figura muestra la visualización gráfica de eventos correlacionados dentro de OpenSearch Security Analytics, permitiendo identificar relaciones entre hallazgos generados por reglas de detección asociadas a eventos de seguridad.

La Figura 24 evidencia la capacidad de OpenSearch Security Analytics para representar gráficamente relaciones entre eventos detectados por las reglas configuradas. Esta visualización permitió analizar de forma contextual los hallazgos generados, facilitando la identificación de

patrones asociados a comportamientos sospechosos dentro del entorno corporativo de laboratorio.

Figura 25

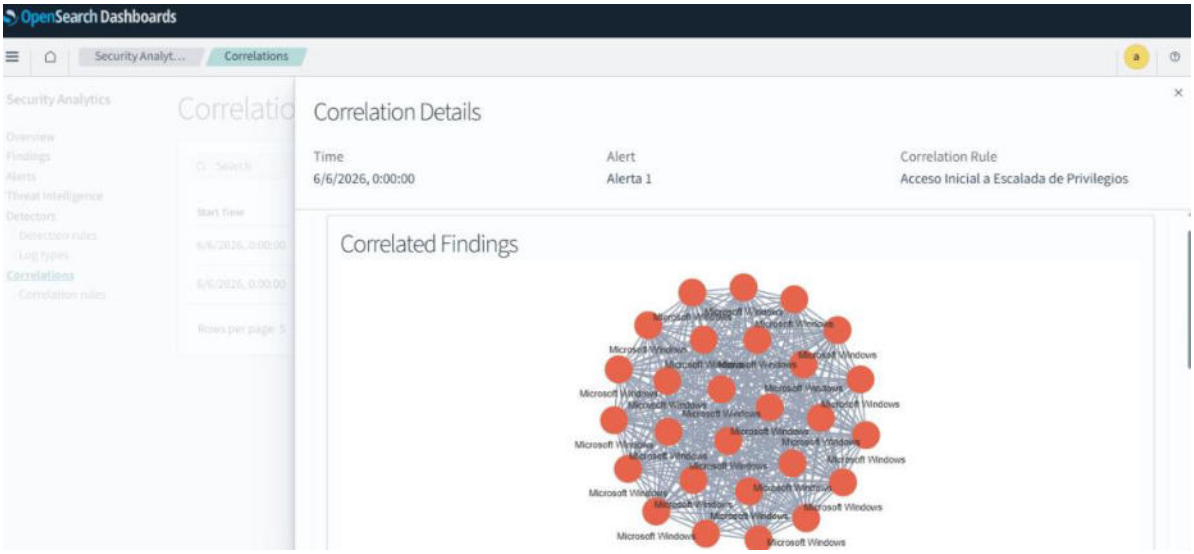
Resultados generados por la correlación de eventos



Nota. Visualización a detalle de correlación de eventos.

Figura 26

Resultados generados por la correlación de eventos



*Nota***.** Visualización de comportamiento de correlación.

Para demostrar la relación entre las reglas implementadas y las técnicas ATT&CK seleccionadas, se elaboró una matriz de trazabilidad que permite vincular cada regla de detección con el comportamiento observado, la fuente de eventos utilizada, la condición lógica aplicada y la evidencia generada por el SIEM.

Esta matriz permite comprobar que la asociación con ATT&CK no se realizó únicamente de forma conceptual, sino a partir de eventos reales generados dentro del laboratorio, recolectados por las fuentes de logs integradas y procesados por OpenSearch Security Analytics. De esta manera, cada regla queda relacionada con una técnica específica mediante criterios observables y verificables.

Tabla 20

Reglas de detección y correlación implementadas

Escenario ejecutado	Regla activada	Condición	Resultado	Notificación enviada
Fuerza bruta SSH contra Aruba CX 8360	Fuerza Bruta SSH en Core Switch	Más de 15 intentos fallidos SSH desde una misma IP en 5 minutos	Alerta generada	Correo electrónico de alta severidad
Escaneo de red mediante Nmap	Reconocimiento de Red	Múltiples conexiones a puertos y servicios de red	Alerta generada	Registro en dashboard y Security Analytics
Creación de cuenta en Active Directory	Creación de Cuenta en Active Directory	Event ID 4720 detectado por Windows Security	Alerta generada	Correo electrónico de alta severidad
Fuerza bruta SSH seguida de creación de cuenta AD	Acceso Inicial y Creación de Cuenta	Correlación entre T1110 y T1136 dentro de 15 minutos	Alerta crítica	Correo electrónico de severidad crítica

Nota. Matriz basada en las reglas implementadas y los escenarios ejecutados en el laboratorio.

Como se observa en la Tabla 20, cada regla implementada se relaciona con una técnica ATT&CK a partir del comportamiento observado durante las pruebas realizadas en el entorno de laboratorio. Los intentos repetidos de autenticación fallida mediante SSH contra dispositivos Aruba se asociaron con la técnica T1110, correspondiente a fuerza bruta. Por otra parte, el escaneo de red ejecutado mediante Nmap se relacionó con la técnica T1046, correspondiente al descubrimiento de servicios de red. Adicionalmente, la creación de una cuenta de dominio en Active Directory, evidenciada mediante el Event ID 4720 en los registros de seguridad de Windows, se asoció con la técnica T1136.002, correspondiente a la creación de cuentas de dominio.

Asimismo, la regla de correlación denominada “Fuerza bruta SSH y creación de cuenta en Active Directory” permite relacionar eventos de autenticación fallida con una actividad administrativa posterior dentro del dominio. Esta correlación no representa una respuesta automatizada ni una explotación real de escalada de privilegios, sino una secuencia de eventos potencialmente sospechosa observada dentro del laboratorio y utilizada para validar la capacidad de correlación del SIEM.

Es importante precisar que la cobertura de ATT&CK demostrada en este proyecto corresponde únicamente a los escenarios evaluados dentro del entorno corporativo de laboratorio. Por lo tanto, las reglas implementadas no pretenden cubrir la totalidad de variantes posibles de cada técnica, sino validar comportamientos específicos observables mediante las fuentes de logs integradas al SIEM.

Diseño y despliegue de SIEM con OpenSearch

Configuración de Notificaciones y Alertas

Con el propósito de garantizar una respuesta oportuna ante eventos de seguridad detectados por la plataforma SIEM, se implementó un mecanismo de notificación automática mediante correo electrónico utilizando las capacidades nativas de OpenSearch Alerting.

Para ello se configuró un servidor SMTP basado en Gmail, el cual permitió el envío de mensajes automáticos hacia los responsables de la administración y monitoreo de seguridad. Esta funcionalidad fue integrada con los canales de notificación utilizados por las reglas de detección y correlación implementadas dentro del SIEM.

Adicionalmente, se definieron grupos de destinatarios que permiten centralizar la gestión de alertas y facilitar la distribución de notificaciones según los diferentes escenarios de seguridad monitoreados.

La validación del mecanismo fue realizada mediante pruebas de envío de correos electrónicos generados automáticamente por las reglas configuradas, verificando la correcta recepción de las alertas por parte de los usuarios designados.

El envío de notificaciones por correo electrónico fue configurado como parte del proceso de alertamiento del SIEM. Su función consiste en informar al administrador cuando una regla de detección o correlación genera una alerta dentro de OpenSearch. No obstante, este mecanismo no ejecuta acciones automáticas sobre los dispositivos, usuarios, servicios o endpoints afectados; por tanto, no representa una funcionalidad SOAR ni una respuesta automatizada ante incidentes.

En este proyecto, las notificaciones por correo permiten apoyar el análisis manual del evento detectado, proporcionando información oportuna sobre la alerta generada, la severidad asociada y la regla que activó el mecanismo de notificación

Tabla 21

Relación entre reglas, escenarios ejecutados y notificaciones generadas

Escenario ejecutado	Regla activada	Condición	Resultado	Notificación / hallazgo
Fuerza bruta SSH contra Aruba CX 8360	Fuerza Bruta SSH en Core Switch	Más de 15 intentos fallidos SSH	Alerta generada	Correo electrónico de alta severidad
Fuerza bruta SSH contra Aruba AP-505	Fuerza Bruta SSH Aruba AP	Intentos fallidos SSH repetidos	Alerta generada	Hallazgo en Security Analytics
Escaneo de red mediante Nmap	Reconocimiento de Red	Múltiples conexiones a servicios	Alerta generada	Hallazgo en Security Analytics y notificación por correo electrónico
Creación de cuenta en Active Directory	Creación de Cuenta AD	Event ID 4720	Alerta generada	Hallazgo en OpenSearch y notificación por correo con IP de origen, IP de destino y datos de la cuenta creada
Creación de usuario local en FortiGate	FortiGate - Nuevo usuario local	Creación de usuario local	Hallazgo generado	Hallazgo en Security Analytics y notificación por correo con los detalles del usuario creado
Creación de usuario administrador en FortiGate	FortiGate - Nuevo usuario de administrador	Usuario con privilegios administrativos	Hallazgo generado	Hallazgo y notificación por correo con IP de origen, IP de destino, usuario y perfil administrativo

Creación de política de firewall	FortiGate - Nueva política de Firewall	Nueva política agregada	Hallazgo generado	Hallazgo y notificación por correo con los detalles de la política creada
Creación de objeto de dirección en FortiGate	FortiGate - Nueva dirección de firewall	Nuevo objeto de dirección	Hallazgo generado	Hallazgo y notificación por correo con los detalles del objeto creado

Nota. En la matriz basada en las reglas implementadas y los escenarios ejecutados en el laboratorio.

La Tabla 21 permite evidenciar la relación entre los escenarios ejecutados, las reglas activadas y los hallazgos generados por OpenSearch Security Analytics. En el caso de FortiGate, los eventos corresponden a cambios administrativos sobre el firewall, tales como creación de usuarios, asignación de privilegios, creación de políticas y modificación de objetos de dirección. Estos hallazgos no representan una respuesta automática, sino evidencia del mecanismo de detección y alertamiento implementado dentro del SIEM.

Los resultados obtenidos demuestran que los eventos generados por dispositivos Aruba, sistemas Windows y herramientas de monitoreo fueron correctamente almacenados, procesados y correlacionados por OpenSearch Security Analytics, generando alertas y notificaciones consistentes con las condiciones definidas en cada regla.

Figura 27

Configuración del servidor SMTP utilizado para el envío de alertas

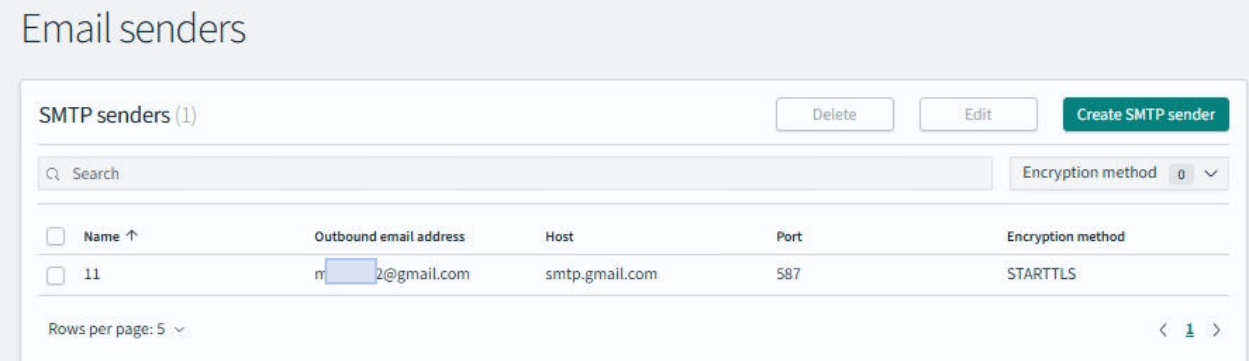


Figura 28

Canal de notificación configurado en OpenSearch Alerting

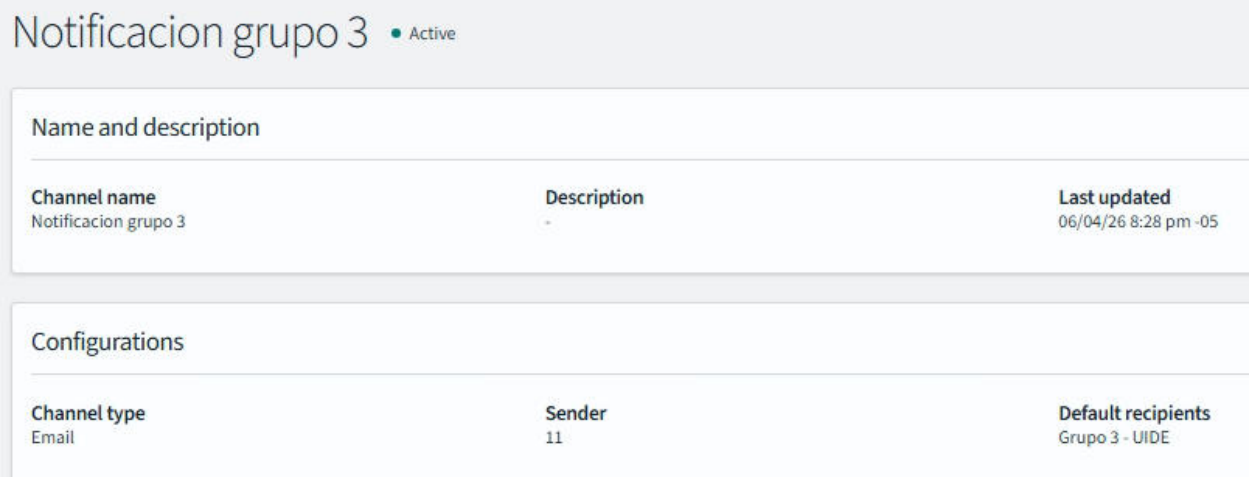
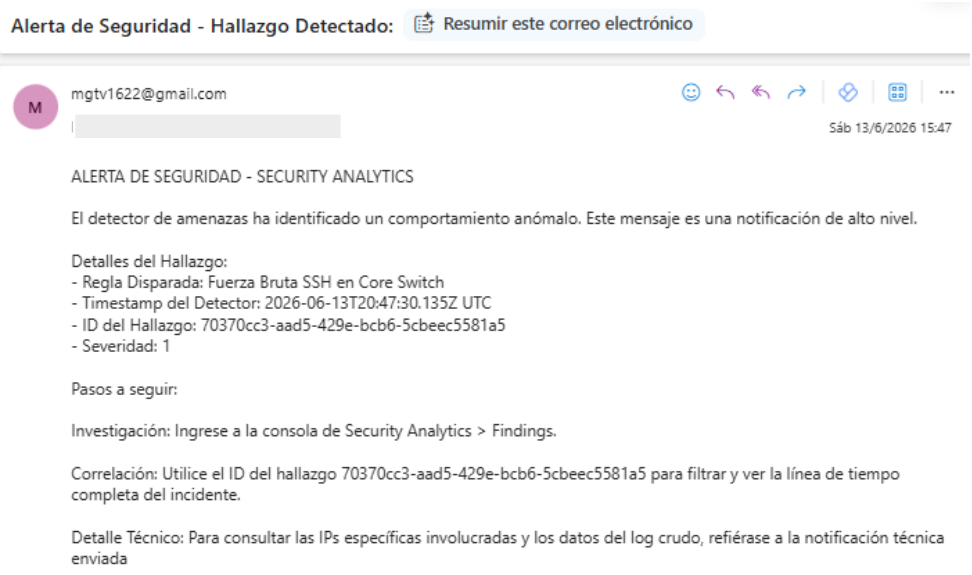


Figura 29

Correo electrónico generado por OpenSearch tras la detección de eventos de seguridad



Nota. Correo de correlación.

Tabla 22

Parámetros de configuración de notificaciones

Parámetro	Valor
Servidor SMTP	smtp.gmail.com
Puerto	587
Método de cifrado	STARTTLS
Tipo de canal	Correo electrónico
Grupo de destinatarios	Grupo 3 - UIDE
Método de autenticación	Usuario y contraseña de Aplicación en Gmail

Nota. Cada uno de los valores que configuramos como servidor smtp.

Validación de la Solución SIEM

Con el propósito de verificar el funcionamiento de la solución SIEM implementada, se ejecutaron escenarios controlados de seguridad dentro del entorno corporativo de laboratorio. Estos escenarios permitieron comprobar la capacidad de la plataforma para recolectar eventos, almacenarlos en OpenSearch, activar reglas de detección, generar hallazgos en Security Analytics y emitir notificaciones de alerta.

La validación se realizó mediante pruebas controladas ejecutadas desde el equipo Kali Linux con dirección IP 10.33.33.112, utilizado como origen de las actividades simuladas. Los escenarios fueron seleccionados considerando técnicas del framework ATT&CK relacionadas con fuerza bruta, descubrimiento de servicios de red, creación de cuentas en Active Directory y cambios administrativos en FortiGate.

Diseño y despliegue de SIEM con OpenSearch

La Tabla 23 presenta los escenarios ejecutados, la herramienta utilizada, la técnica ATT&CK asociada y la evidencia empleada para comprobar su detección dentro del SIEM.

Tabla 23

Escenarios de validación ejecutados

Escenario	Herramienta utilizada	Origen	Objetivo	Técnica ATT&CK	Evidencia de detección
Fuerza bruta SSH contra switch Aruba	Hydra	Kali Linux 10.33.33.112	Switch Aruba 10.33.33.113	T1110 - Brute Force	Logs Syslog, regla de detección y alerta en OpenSearch
Fuerza bruta SSH contra switch Aruba	Hydra	Kali Linux 10.33.33.112	Switch Aruba 10.33.33.3	T1110 - Brute Force	Logs Syslog, regla de detección y alerta en OpenSearch
Fuerza bruta SSH contra AP Aruba	Hydra	Kali Linux 10.33.33.112	Aruba AP 10.33.33.106	T1110 - Brute Force	Eventos SSH fallidos y hallazgos en Security Analytics
Escaneo de red	Nmap	Kali Linux 10.33.33.112	Red 10.33.33.0/24	T1046 - Network Service Discovery	Resultado del escaneo, eventos recolectados y visualización en dashboard
Creación de cuenta Active Directory	PowerShell	Windows Server 2025	Active Directory 10.33.33.105	T1136.002	Evento 4720 + OpenSearch
Creación de usuario local en FortiGate	GUI FortiGate	FortiGate 80F	FortiGate 80F	T1136.001	Logs Syslog, regla de detección

Creación de usuario administrador en FortiGate	GUI FortiGate	FortiGate 80F	FortiGate 80F	T1098 / T1136.001	Logs Syslog y regla de detección
Creación de política en el firewall	GUI FortiGate	FortiGate 80F	FortiGate 80F	T1562	Logs Syslog y regla de detección
Creación de objeto de dirección en FortiGate	GUI FortiGate	FortiGate 80F	FortiGate 80F	T1562	Logs Syslog y regla de detección

Diseño y despliegue de SIEM con OpenSearch

Durante el escenario de fuerza bruta SSH contra dispositivos Aruba, se utilizó la herramienta Hydra para generar múltiples intentos fallidos de autenticación hacia servicios SSH expuestos en el laboratorio. Los eventos fueron registrados por los dispositivos Aruba y enviados mediante Syslog hacia Fluentd, donde posteriormente fueron almacenados en OpenSearch. La detección se verificó mediante la generación de alertas asociadas a intentos repetidos de autenticación fallida.

En el escenario de escaneo de red, se ejecutó la herramienta Nmap desde Kali Linux sobre el segmento 10.33.33.0/24. Esta prueba permitió identificar servicios activos, puertos abiertos y hosts disponibles dentro del entorno monitoreado. La evidencia de este escenario se obtuvo mediante la salida del comando ejecutado, los eventos registrados en el SIEM y las visualizaciones configuradas en OpenSearch Dashboards.

Escenarios de Validación Ejecutados

Tabla 24

Técnica MITRE ATT&CK® por escenario

Escenario	Herramienta / medio utilizado	Objetivo	Técnica ATT&CK
Fuerza bruta SSH Aruba CX 8360	Hydra	10.33.33.113	T1110
Fuerza bruta SSH switch Aruba acceso	Hydra	10.33.33.3	T1110
Fuerza bruta SSH Aruba AP	Hydra	10.33.33.106	T1110
Escaneo de red	Nmap	10.33.33.0/24	T1046
Creación de cuenta en Active Directory	PowerShell / Windows Server	Active Directory	T1136.002

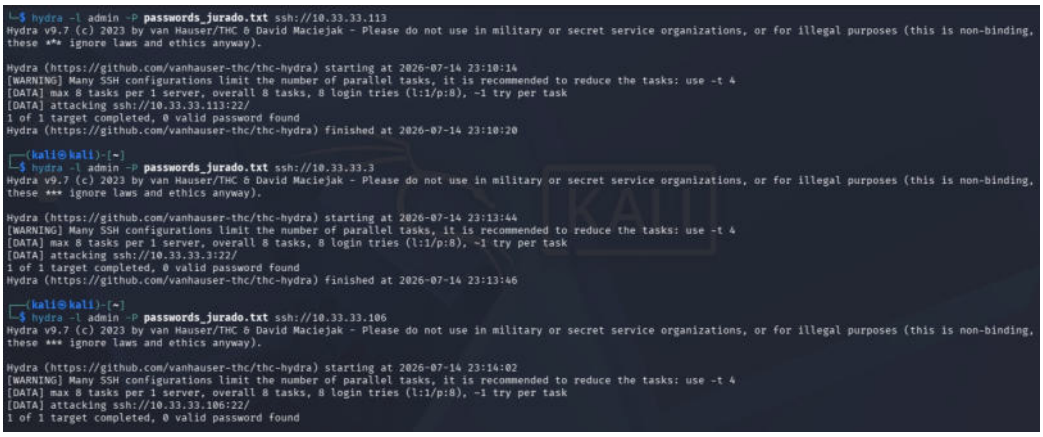
Creación de usuario local en FortiGate	GUI FortiGate	FortiGate 80F	T1136.001
Creación de usuario administrador en FortiGate	GUI FortiGate	FortiGate 80F	T1136.001 / T1098
Creación de política de firewall	GUI FortiGate	FortiGate 80F	T1562
Creación de objeto de dirección	GUI FortiGate	FortiGate 80F	T1562

Nota. Herramientas y medios utilizados para ejecutar los escenarios de validación dentro del entorno corporativo de laboratorio

Evidencias de Detección

Figura 30

Ejecución de prueba de fuerza bruta SSH mediante Hydra



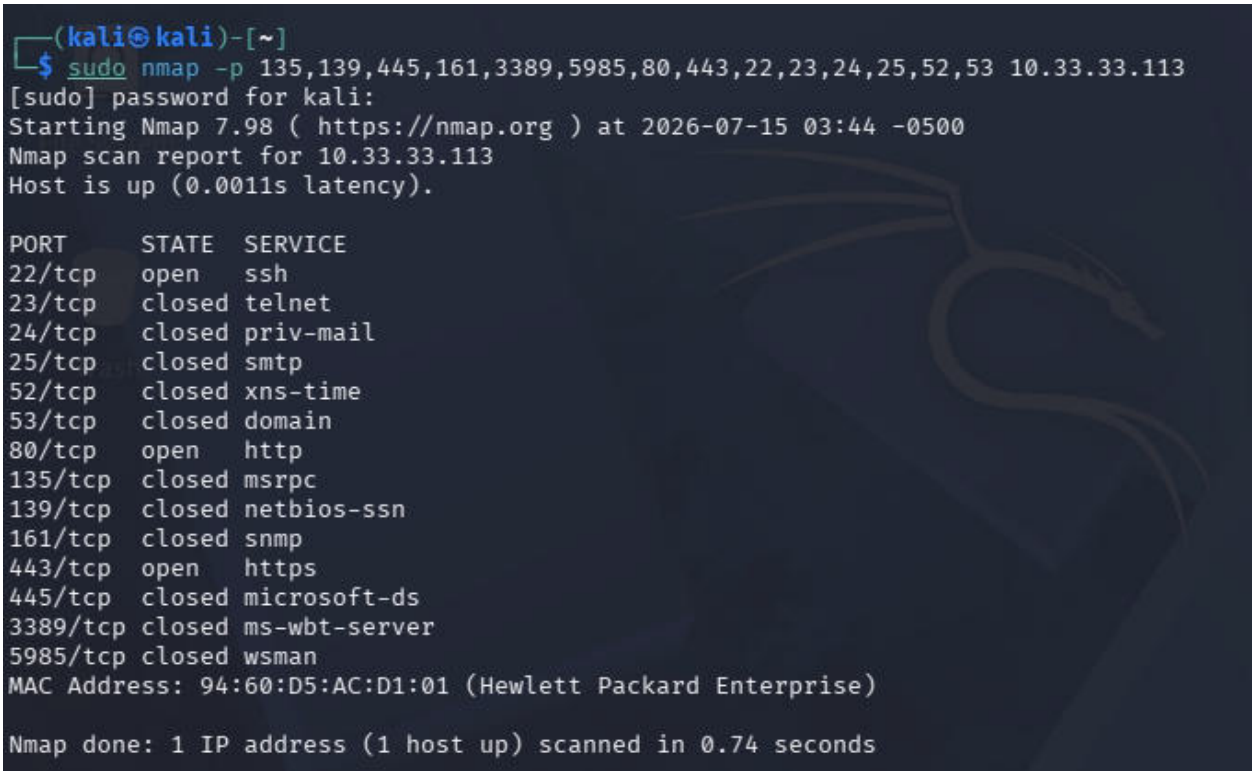
Nota. La herramienta Hydra fue utilizada para generar múltiples intentos fallidos de autenticación SSH contra dispositivos Aruba del entorno de laboratorio, permitiendo validar la capacidad de detección del SIEM frente a eventos asociados a ataques de fuerza bruta.

Para validar el escenario de descubrimiento de servicios de red, se ejecutaron escaneos dirigidos mediante Nmap sobre los dispositivos principales de infraestructura Aruba. En lugar de presentar la salida completa del escaneo sobre toda la red, se documentaron los resultados

individuales correspondientes al switch core Aruba CX 8360, el switch de acceso Aruba y el punto de acceso Aruba AP-505. Esta estrategia permitió evidenciar de forma más clara los servicios expuestos en cada dispositivo y relacionar la actividad con la técnica T1046 Network Service Discovery de ATT&CK.

Figura 31

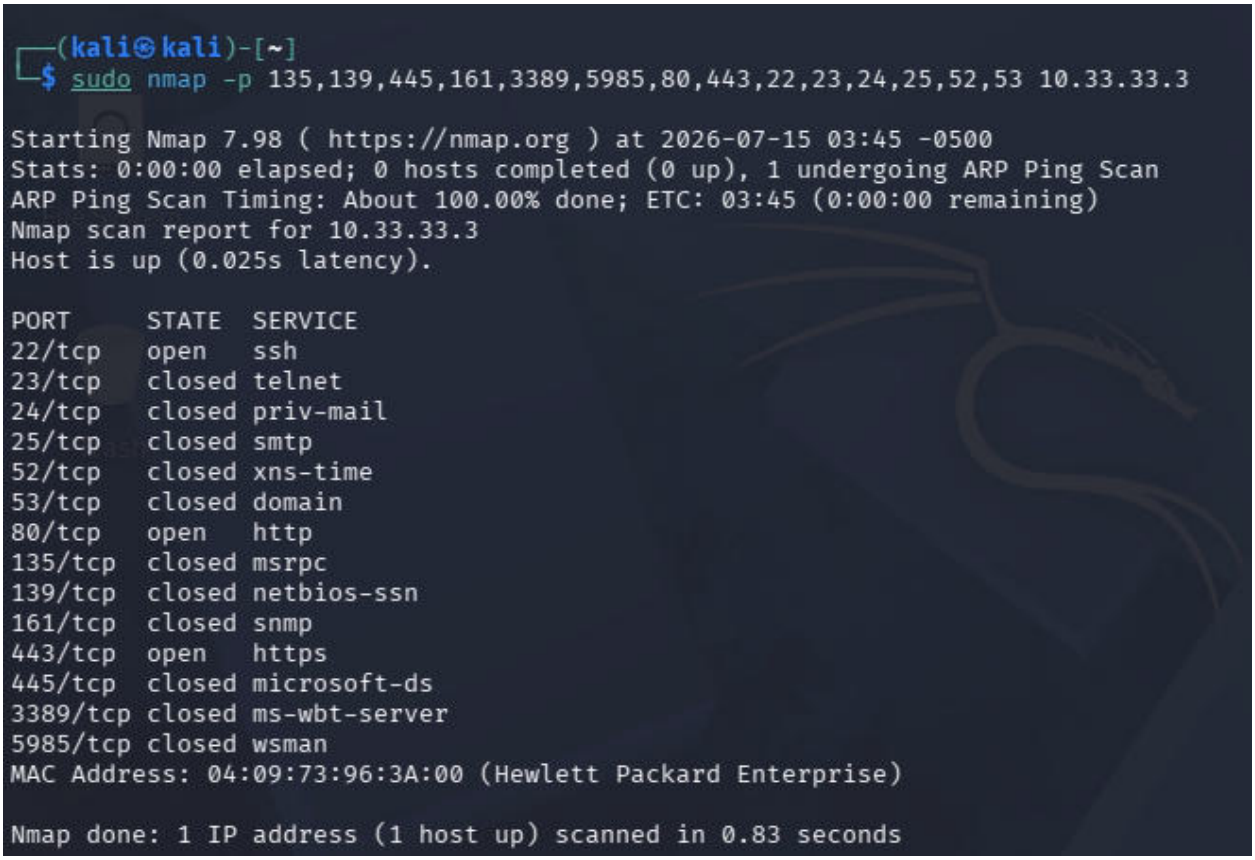
Escaneo de servicios sobre el switch core Aruba de IP 10.33.33.113



Nota. La prueba permitió identificar servicios expuestos de switch core Aruba del entorno de laboratorio, validando el escenario de descubrimiento de servicios de red asociado a la técnica T1046 de ATT&CK.

Figura 32

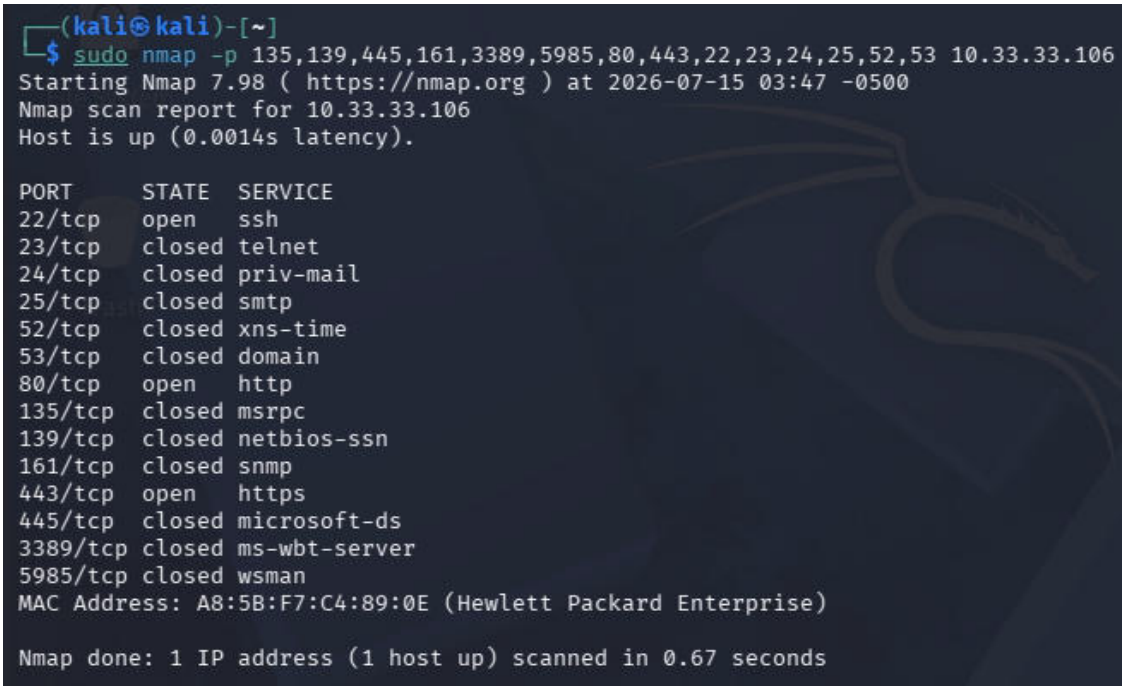
Escaneo de servicios sobre el switch core acceso de IP 10.33.33.3



Nota. La prueba permitió identificar servicios expuestos de switch de acceso Aruba del entorno de laboratorio, validando el escenario de descubrimiento de servicios de red asociado a la técnica T1046 de ATT&CK.

Figura 33

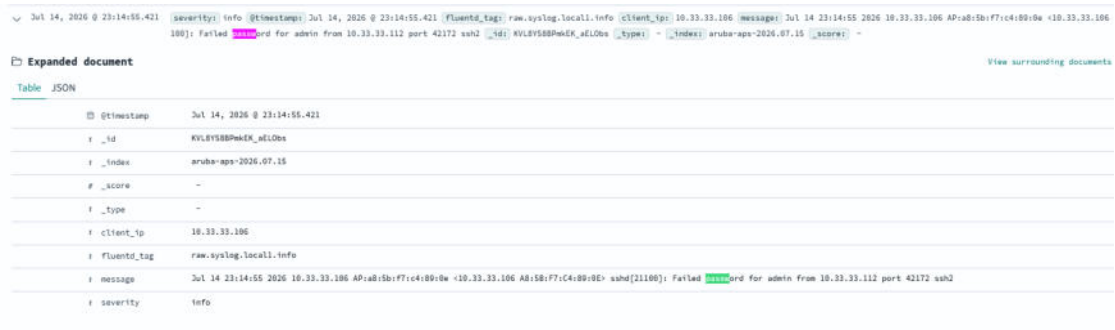
Escaneo de servicios sobre el AP Aruba de IP 10.33.33.106



Nota. La prueba permitió identificar servicios expuestos del Access Point Aruba del entorno de laboratorio, validando el escenario de descubrimiento de servicios de red asociado a la técnica T1046 de ATT&CK.

Figura 34

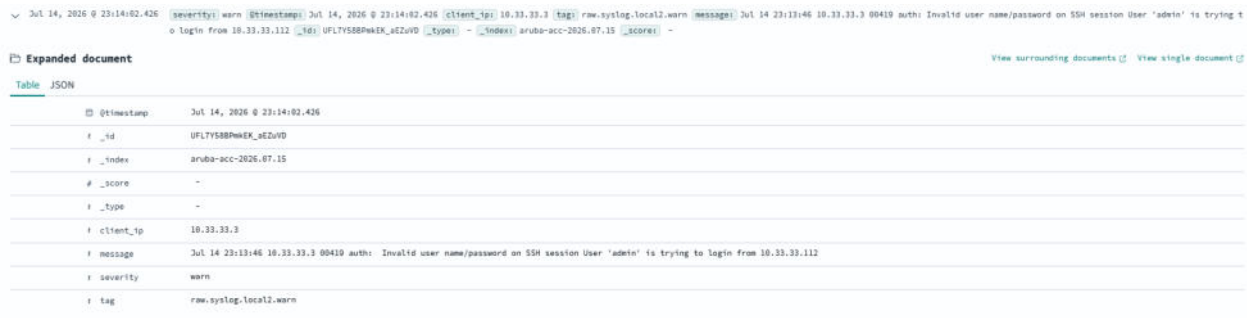
Evento Syslog generado por Aruba AP durante prueba de fuerza bruta SSH



Nota. En discover se visualiza los logs recibidos del ap luego de realizar un ataque de fuerza bruta.

Figura 35

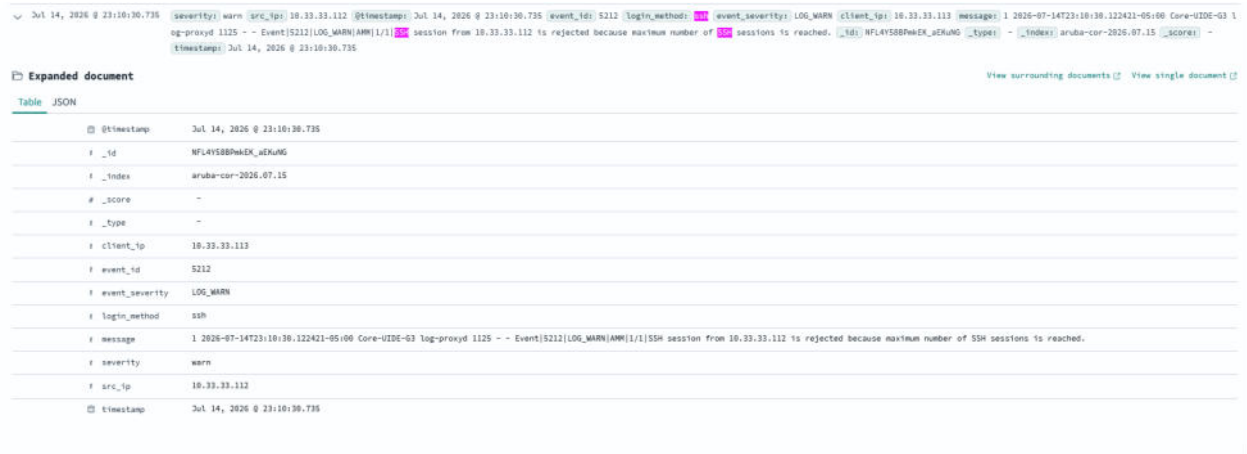
Registro generado por el switch de acceso durante el ataque de fuerza bruta



Nota. En discover se visualiza los logs recibidos del switch de acceso luego de realizar un ataque de fuerza bruta.

Figura 36

Registro de eventos generado por ataque de fuerza bruta SSH sobre switch Aruba CX 8360



Nota. La figura muestra la recepción y visualización de eventos provenientes del switch Aruba CX 8360 dentro de OpenSearch Dashboards. Esta evidencia confirma la correcta ingestión y almacenamiento de los registros enviados mediante Syslog hacia la plataforma SIEM.

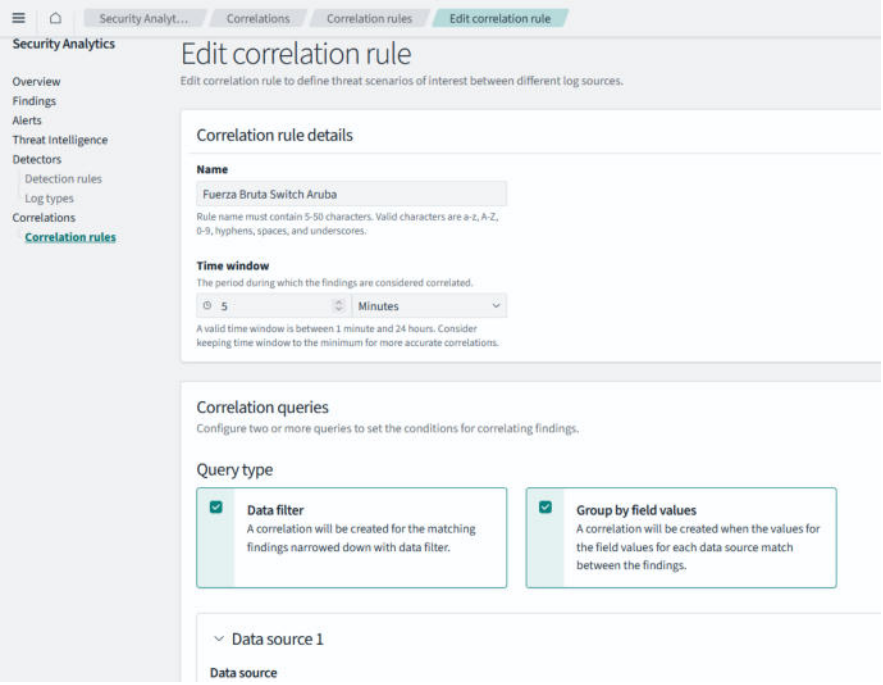
Figura 37

Visualización de intentos fallidos de autenticación SSH

Nota. La figura evidencia la consolidación y visualización de múltiples intentos fallidos de autenticación SSH detectados por la plataforma SIEM.

Figura 38

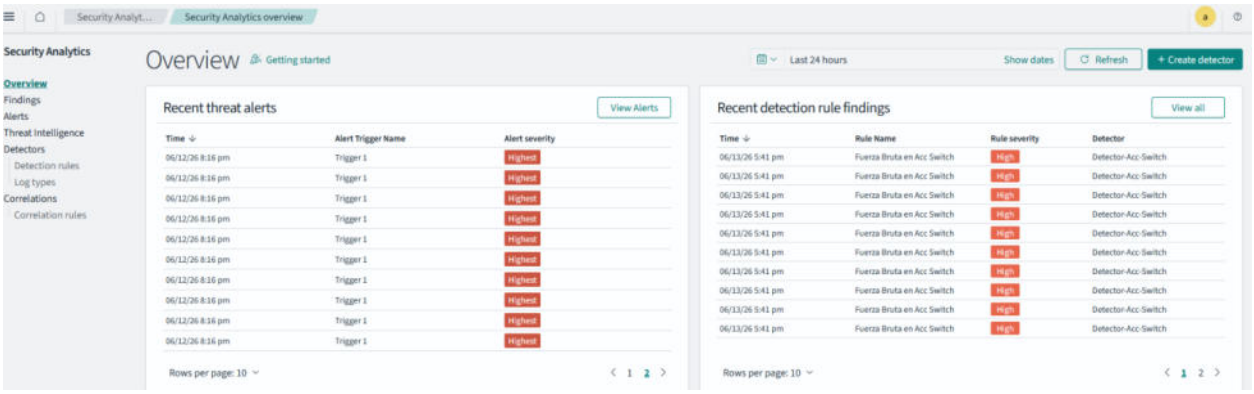
Regla de detección de fuerza bruta SSH implementada en OpenSearch Security Analytics



Nota. La regla de detección fue configurada para identificar múltiples intentos fallidos de autenticación SSH provenientes de una misma dirección IP dentro de una ventana temporal determinada.

Figura 39

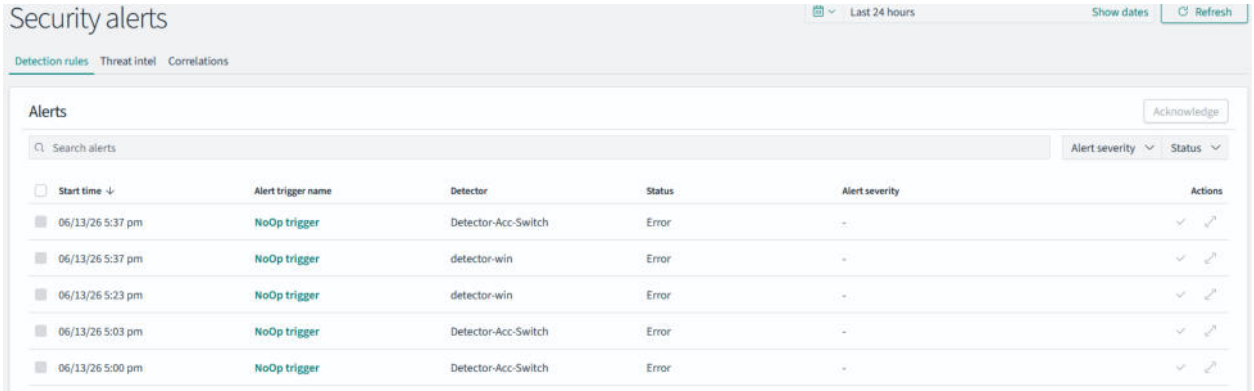
Hallazgo de seguridad generado por la detección de fuerza bruta SSH



Nota. La figura evidencia el hallazgo de seguridad generado automáticamente por la regla de detección de fuerza bruta SSH configurada en OpenSearch Security Analytics.

Figura 40

Detalle de alerta asociado a intento de fuerza bruta SSH



Nota. La figura confirma la generación de una alerta de seguridad asociada a eventos de autenticación fallida que superaron el umbral definido por la regla de detección.

Figura 41

Notificación por correo electrónico generada ante la detección de fuerza bruta SSH

Nota. La figura valida el funcionamiento del mecanismo de notificación automática implementado, mediante el envío de alertas por correo electrónico cuando se detectan eventos de seguridad críticos.

Figura 42

Evento de creación de cuenta en Windows Server

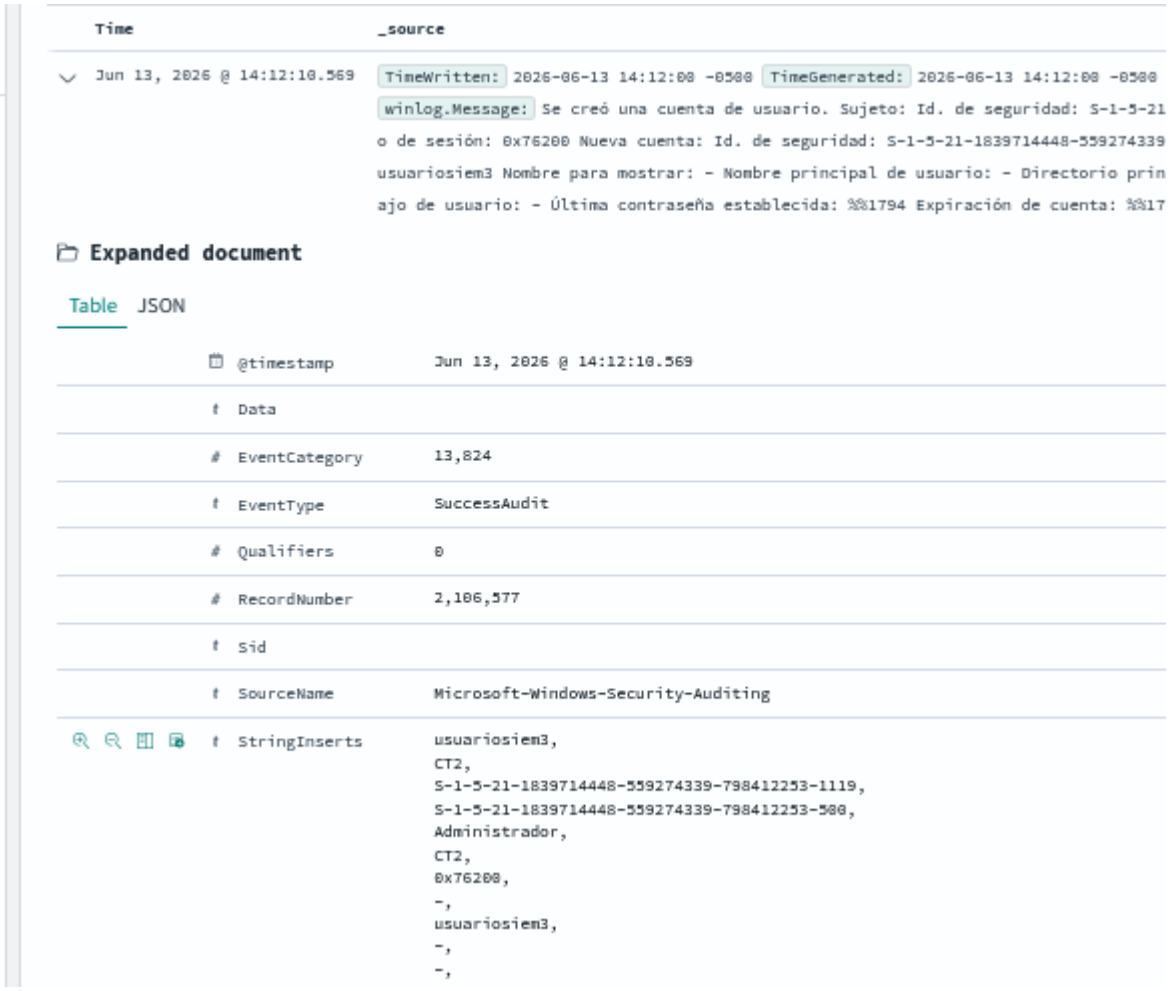
```
PS C:\Users\Administrador> New-ADUser `
>> -Name "UsuarioSIEM3" `
>> -SamAccountName "usuariosiem3" `
>> -AccountPassword (ConvertTo-SecureString "Lab123456!" -AsPlainText -Force) `
>> -Enabled $true
PS C:\Users\Administrador> Get-WinEvent -FilterHashtable @{LogName='Security';ID=4720} -MaxEvents 5


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
13/06/2026 14:12:00           4720 Información      Se creó una cuenta de usuario....
```

Nota. La figura muestra la creación controlada de una cuenta de dominio mediante PowerShell utilizando el cmdlet New-ADUser.

Esta acción generó el evento de auditoría 4720 en el registro de seguridad de Windows Server, el cual fue recolectado mediante Fluent Bit y enviado hacia OpenSearch para su análisis. La actividad fue utilizada para validar la capacidad de la plataforma para detectar eventos asociados a la técnica T1136.002 (Create Domain Account) del framework ATT&CK

Figura 43

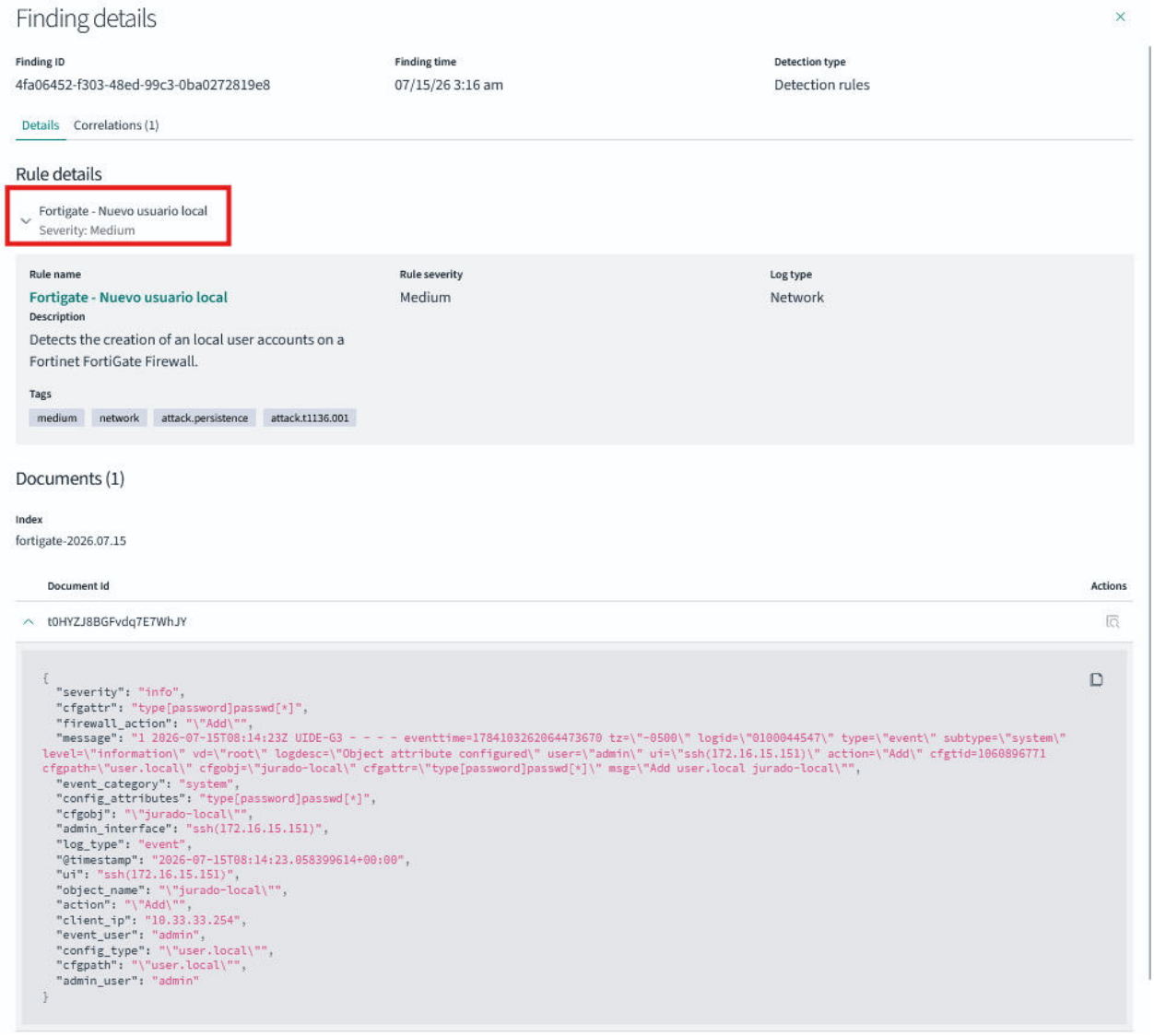
Evento de creación de cuenta en Active Directory detectado por OpenSearch



La Figura 43 evidencia la correcta recepción y almacenamiento del evento 4720 dentro de OpenSearch. El evento corresponde a la creación de una cuenta de dominio en Active Directory y permitió validar la detección de la técnica T1136.002 (Create Domain Account) del framework ATT&CK.

Figura 44

Hallazgo generado por creación de usuario local en FortiGate

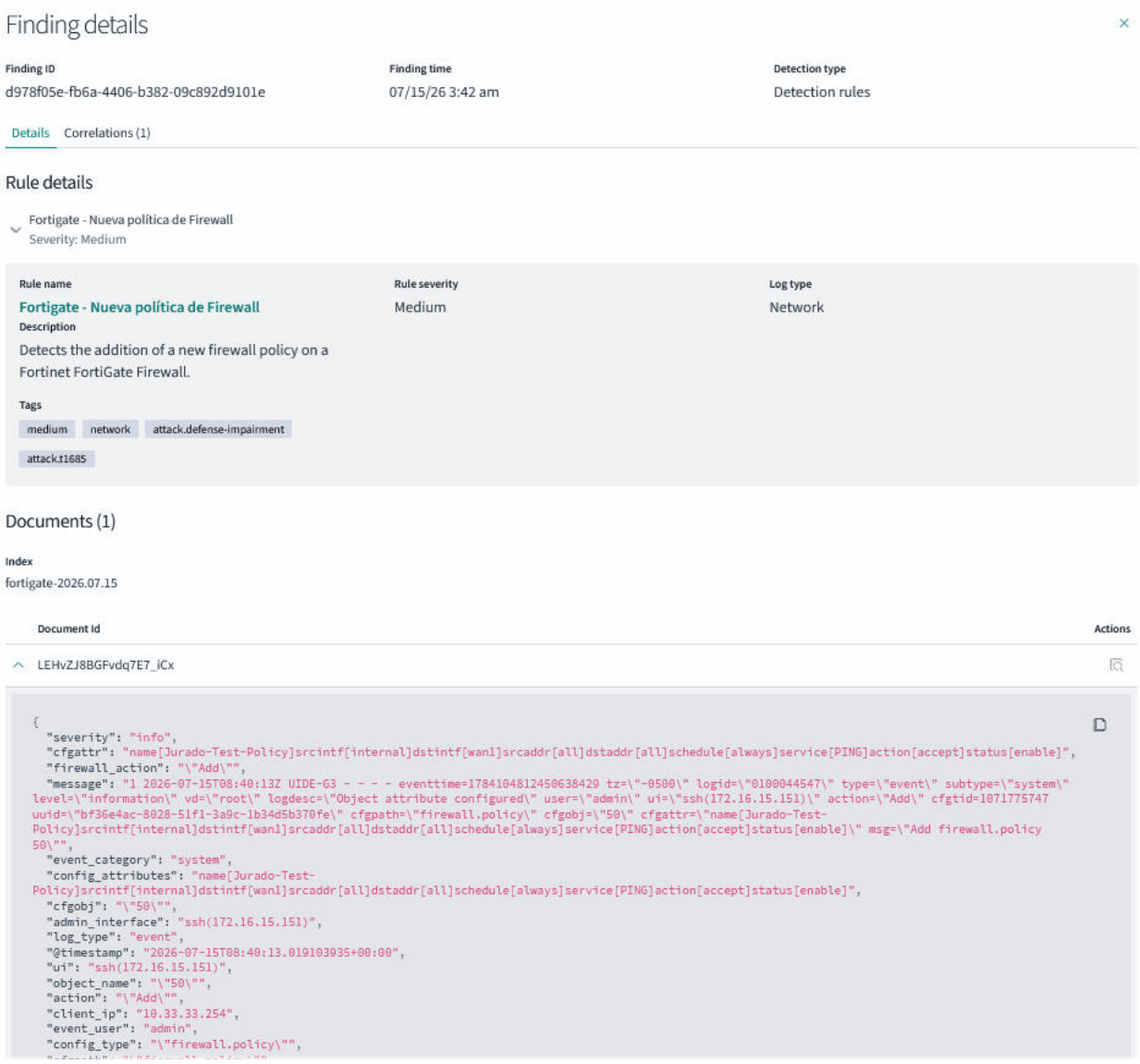


Nota. OpenSearch Security Analytics generó un hallazgo asociado a la creación de un usuario local en FortiGate 80F, evento relacionado con la técnica T1136.001 Create Account: Local Account

Diseño y despliegue de SIEM con OpenSearch

Figura 45

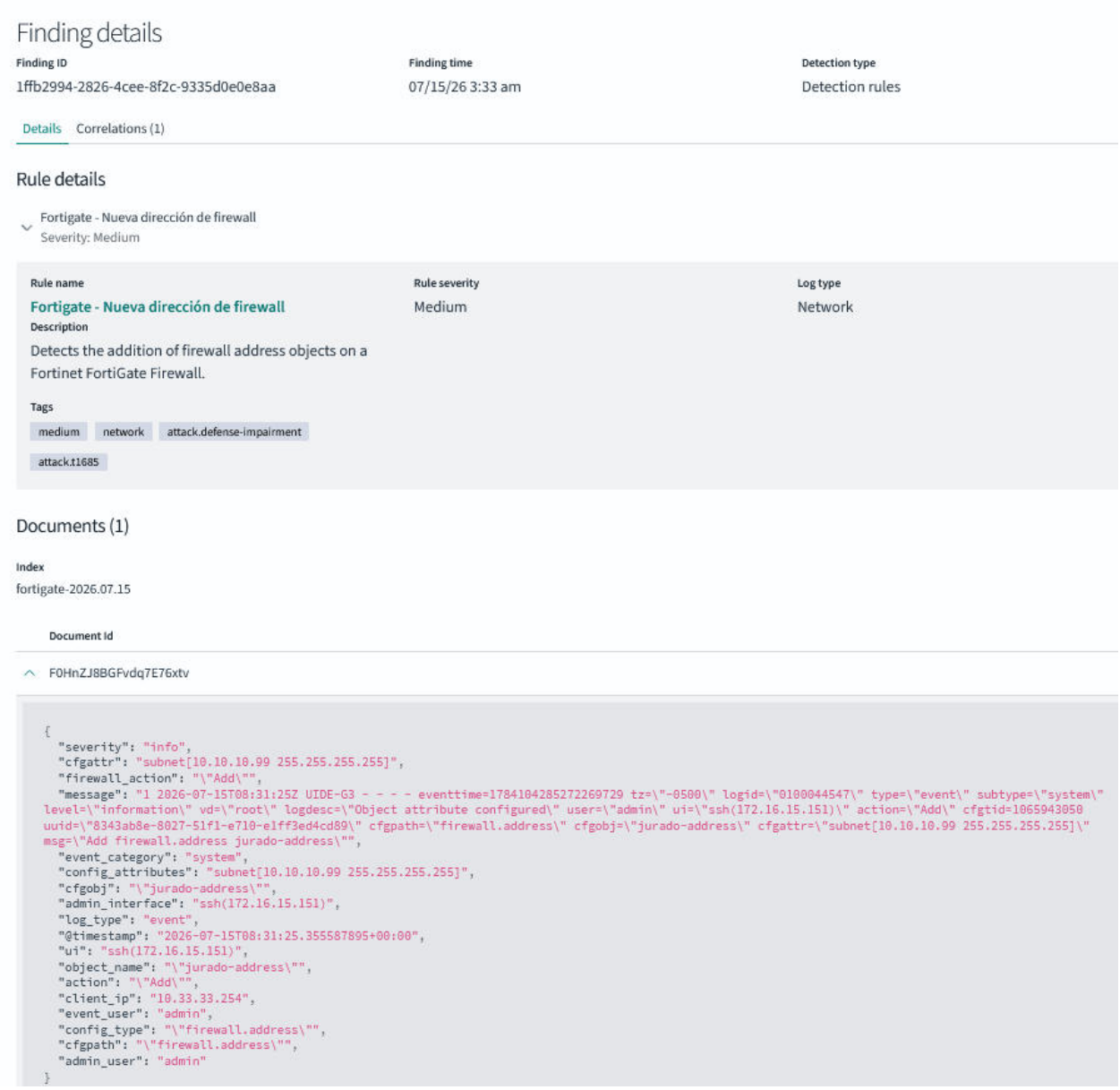
Hallazgo generado por creación de política de firewall en FortiGate



Nota. El SIEM registró la creación de una nueva política de firewall en FortiGate 80F, evento asociado a la técnica T1562 Impair Defenses, debido a que representa una modificación en controles de seguridad perimetral.

Figura 46

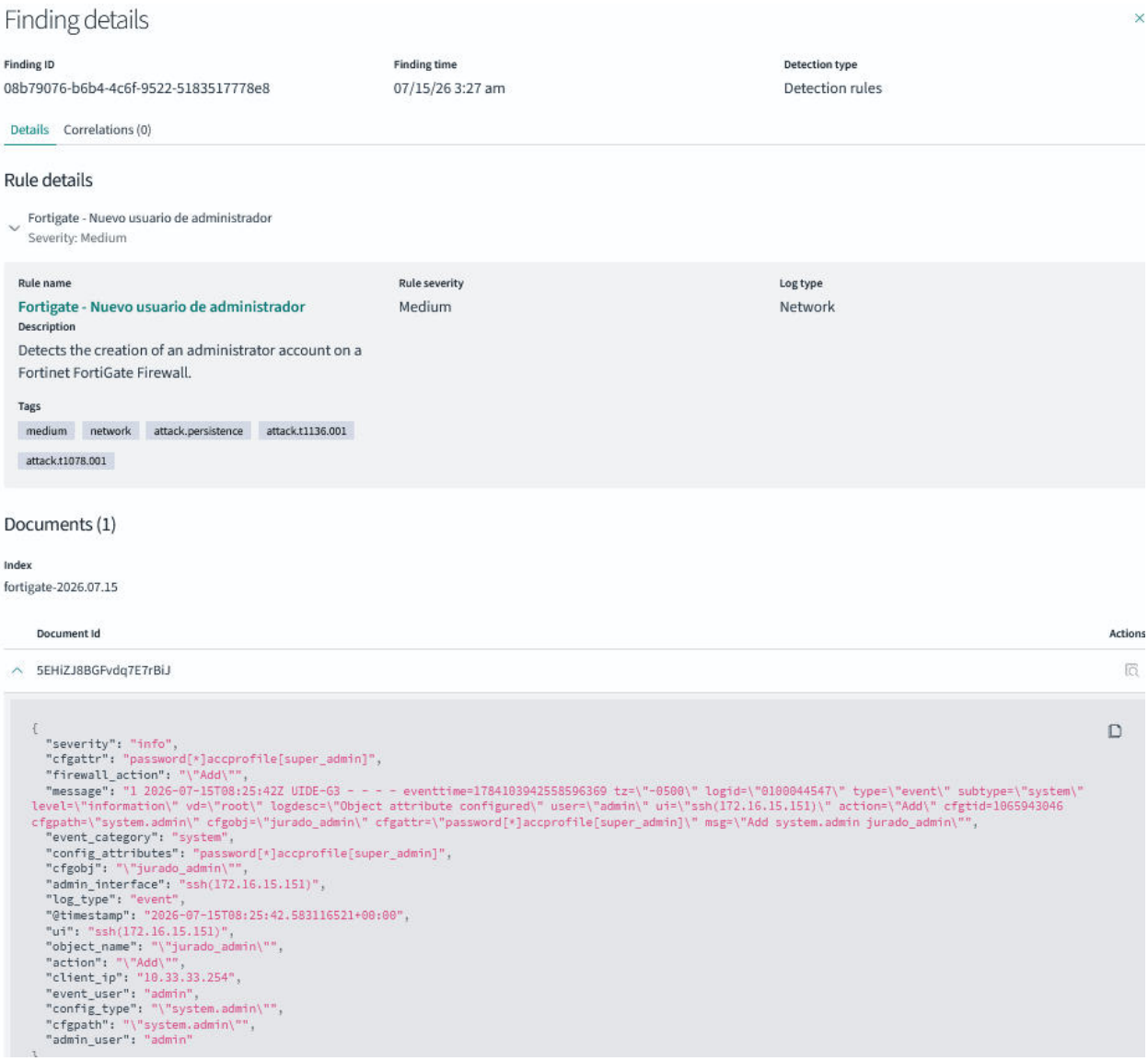
Hallazgo generado por creación de objeto de dirección en FortiGate



Nota. OpenSearch Security Analytics detectó la creación de un objeto de dirección en FortiGate 80F, evento asociado a la técnica T1562 Impair Defenses dentro del contexto de cambios administrativos en la configuración del firewall.

Figura 47

Hallazgo generado por creación de usuario administrador en FortiGate



Nota. El hallazgo corresponde a la creación de un usuario administrador en FortiGate 80F, evento asociado a la técnica T1136.001 Create Account: Local Account y a T1098 Account Manipulation debido a la asignación de privilegios administrativos.

Resultados de Validación

Tabla 25

Resultados obtenidos durante las pruebas

Escenario	Evento Detectado	Alerta Generada	Resultado
Fuerza bruta SSH Aruba CX 8360	Sí	Sí	Exitoso
Fuerza bruta SSH Aruba AP-505	Sí	Sí	Exitoso
Fuerza bruta SSH en switch de acceso	Sí	Sí	Exitoso
Escaneo Nmap	Sí	Sí	Exitoso
Creación de cuenta AD	Sí	Sí	Exitoso
Creación de usuario local FortiGate	Sí	Sí	Exitoso
Creación de usuario administrador FortiGate	Sí	Sí	Exitoso
Creación de política firewall FortiGate	Sí	Sí	Exitoso
Creación de objeto de dirección FortiGate	Sí	Sí	Exitoso

Los resultados obtenidos demuestran que la plataforma fue capaz de recolectar, almacenar y correlacionar los eventos generados durante las pruebas realizadas. Adicionalmente, todos los escenarios ejecutados fueron detectados correctamente por los mecanismos de monitoreo implementados, generando alertas y hallazgos de seguridad de forma consistente. Esto evidencia la capacidad de la solución para proporcionar visibilidad centralizada y apoyo a las actividades de detección temprana de incidentes.

Limitaciones del alcance de validación

A pesar del éxito analítico registrado en la matriz anterior, es metodológicamente indispensable establecer que los resultados expuestos corresponden a simulaciones controladas dentro de una infraestructura de laboratorio acotada y predecible. En un entorno de red corporativa real, la efectividad neta de la solución SIEM estaría condicionada por factores operativos complejos que no se replican en ambientes de prueba.

El volumen masivo de tráfico legítimo concurrente y el "ruido de fondo" generado por las actividades cotidianas de los usuarios empresariales elevan significativamente la probabilidad de encubrir comportamientos maliciosos sutiles o de saturar los hilos de procesamiento del colector central. Asimismo, la presencia de herramientas administrativas legítimas y actualizaciones de software suele mimetizarse con patrones de ataque reales, lo que genera falsos positivos y exige un proceso continuo de afinamiento (tuning) de las reglas de detección para evitar la fatiga de alertas. Finalmente, un adversario real empleará técnicas dinámicas de evasión de defensas u ofuscación de código diseñadas para sortear umbrales rígidos. Por consiguiente, la tasa de detección del 100% obtenida en esta fase valida la correcta integración lógica de la arquitectura, reconociendo explícitamente que dicha efectividad neta solo es directamente aplicable a las técnicas y escenarios específicos evaluados en este proyecto de investigación.

Diseño y despliegue de SIEM con OpenSearch

Cobertura MITRE ATT&CK® Obtenida

Tabla 26

Técnicas MITRE ATT&CK® validadas

Técnica	Nombre	Evidencia
T1110	Brute Force	Hydra + Security Analytics
T1046	Network Service Discovery	Nmap + OpenSearch
T1136.002	Create Account	Event ID 4720
T1136.001	Create Account: Local Account	GUI FortiGate + OpenSearch
T1098	Account Manipulation	GUI FortiGate + OpenSearch
T1562	Impair Defenses	GUI FortiGate + OpenSearch

La validación permitió comprobar la cobertura de técnicas pertenecientes a las tácticas de acceso inicial, descubrimiento y persistencia definidas en ATT&CK. La detección exitosa de estas técnicas demuestra que la solución implementada puede identificar actividades asociadas a diferentes fases de un posible ciclo de ataque dentro de un entorno corporativo.

Diseño y despliegue de SIEM con OpenSearch

Métricas obtenidas

Tabla 27

Resumen de resultados de validación

Métrica	Resultado
Fuentes de eventos integradas	4
Dashboards implementados	4
Reglas de detección implementadas	12
Escenarios de validación ejecutados	9
Escenarios detectados correctamente	9
Tasa de detección	100 %
Técnicas ATT&CK validadas	6
Hallazgos de seguridad generados	Múltiples
Notificaciones automáticas por correo	Sí
Tiempo medio hasta la disponibilidad del evento en OpenSearch	23,3 segundos

Los resultados obtenidos permiten concluir que la solución implementada fue capaz de recolectar, procesar, correlacionar y visualizar eventos de seguridad provenientes de diferentes fuentes dentro del entorno corporativo de laboratorio. La plataforma generó hallazgos asociados a fuerza bruta SSH, descubrimiento de red, creación de cuentas en Active Directory y cambios administrativos en FortiGate, evidenciando la funcionalidad del SIEM basado en OpenSearch.

Los resultados obtenidos evidencian que la solución SIEM implementada fue capaz de detectar correctamente la totalidad de los escenarios ejecutados durante la validación. Asimismo,

se verificó la generación automática de alertas y notificaciones, así como la cobertura de múltiples técnicas del framework ATT&CK.

Los resultados obtenidos evidencian que la solución SIEM implementada fue capaz de detectar y visualizar correctamente los eventos correspondientes a los escenarios ejecutados durante la validación. Para los siete escenarios que contaban con marcas temporales registradas con resolución de segundos, se obtuvo un tiempo medio de detección observado en OpenSearch de 23,3 segundos. Los tiempos individuales estuvieron comprendidos entre 10 y 41 segundos, lo que demuestra que los eventos estuvieron disponibles para su consulta dentro de la plataforma en menos de un minuto bajo las condiciones controladas del laboratorio.

El menor intervalo correspondió a la creación de una cuenta en Active Directory, con 10 segundos, mientras que el mayor correspondió al reconocimiento de red mediante Nmap, con 41 segundos. Las diferencias observadas se relacionan con la naturaleza de los escenarios, la cantidad de registros generados y los procesos de recolección, procesamiento, normalización e indexación realizados por la solución.

Tabla 28

Tiempo de detección observado y recepción de notificaciones durante las pruebas de validación

Escenario ejecutado	Hora del evento	Hora de visualización en OpenSearch	Hora de recepción de la notificación	Tiempo de detección observado en OpenSearch
Fuerza bruta SSH sobre switch Aruba CX 8360	23:10:11	23:10:38	23:11:11	27 segundos
Escaneo de red mediante Nmap	04:42:00	04:42:41	04:43:41	41 segundos
Creación de cuenta en Active Directory	14:12:00	14:12:10	14:13:08	10 segundos
Creación de usuario local en FortiGate	03:14:00	03:14:23	03:16:02	23 segundos
Creación de política de firewall	03:40:00	03:40:13	03:42:04	13 segundos
Creación de objeto de dirección en FortiGate	03:31:00	03:31:25	03:32:58	25 segundos
Creación de usuario administrador en FortiGate	03:25:18	03:25:42	03:26:08	24 segundos

Nota. La hora del evento corresponde a la marca temporal registrada al ejecutar o iniciar cada escenario de validación. La hora de visualización en OpenSearch corresponde al momento en que el registro estuvo disponible para su consulta dentro de la plataforma. La

hora de recepción de la notificación corresponde al momento en que el correo electrónico generado por el mecanismo de alertamiento fue recibido por el destinatario. El tiempo de detección observado se calculó exclusivamente como la diferencia entre la hora del evento y la hora de visualización en OpenSearch; por consiguiente, el tiempo de generación, procesamiento y entrega de la notificación por correo electrónico no forma parte de esta métrica.

Diseño y despliegue de SIEM con OpenSearch

A partir de las marcas temporales registradas en los siete escenarios de validación, se obtuvo un tiempo medio de detección observado de 23,3 segundos. Este valor se calculó como la diferencia entre la hora registrada de ejecución o inicio del escenario y la hora en que el evento estuvo disponible para consulta en OpenSearch Discover. Los tiempos individuales se situaron entre 10 y 41 segundos; el menor intervalo correspondió a la creación de una cuenta en Active Directory, mientras que el mayor se presentó durante el escaneo de red mediante Nmap.

En los escenarios de fuerza bruta SSH y reconocimiento mediante Nmap, la medición comenzó desde el inicio de la actividad que generó la secuencia de registros procesados por la plataforma. Por su parte, en los escenarios de Active Directory y cambios administrativos sobre FortiGate, la hora inicial correspondió a la marca temporal registrada al ejecutar la acción evaluada. Las diferencias observadas se relacionan con la naturaleza de cada escenario, la cantidad de eventos generados y los procesos de recolección, normalización e indexación realizados por el SIEM.

La hora de recepción de la notificación por correo electrónico se incorporó como evidencia complementaria para verificar el funcionamiento integral del mecanismo de alertamiento. Sin embargo, esta marca temporal no fue utilizada en el cálculo del tiempo medio de detección, debido a que incluye tiempos adicionales asociados con la evaluación del monitor, la generación del mensaje, el procesamiento mediante el servidor SMTP y la entrega del correo al destinatario. En consecuencia, los 23,3 segundos representan el tiempo medio transcurrido hasta la disponibilidad del evento en OpenSearch y no la latencia total hasta la recepción de la notificación.

Diseño y despliegue de SIEM con OpenSearch

Discusión de resultados

Los resultados obtenidos evidencian que la solución implementada fue capaz de identificar comportamientos asociados a las técnicas T1110 (Brute Force), T1046 (Network Service Discovery), T1136.002 (Create Domain Account), T1136.001 (Create Account: Local Account), T1098 (Account Manipulation) y T1562 (Impair Defenses) del framework ATT&CK. Estas técnicas fueron validadas mediante escenarios controlados de fuerza bruta SSH sobre dispositivos Aruba, escaneo de red con Nmap, creación de cuentas en Active Directory y cambios administrativos realizados sobre el firewall FortiGate.

Asimismo, la generación de hallazgos en OpenSearch Security Analytics permitió comprobar que la plataforma no se limitó a una única fuente de eventos, sino que logró procesar información proveniente de dispositivos de red, sistemas Windows y firewall perimetral. Esto incrementó la visibilidad del entorno monitoreado y permitió relacionar eventos con comportamientos asociados a acceso no autorizado, descubrimiento de red, persistencia, manipulación de cuentas y modificación de controles de seguridad.

Análisis de Resultados

Resultados de las Pruebas de Concepto

Con el propósito de validar el funcionamiento de la solución SIEM implementada, se ejecutaron diferentes pruebas de concepto orientadas a verificar la capacidad de recolección, procesamiento, correlación y alertamiento de eventos de seguridad. Los escenarios seleccionados fueron diseñados con base en técnicas comúnmente asociadas a actividades de reconocimiento, acceso inicial y persistencia, permitiendo evaluar la efectividad de las reglas de detección implementadas y su alineación con el framework ATT&CK.

Las pruebas incluyeron escenarios de fuerza bruta sobre servicios SSH, reconocimiento de red mediante escaneo de servicios, creación de cuentas en Active Directory, correlación de eventos provenientes de distintas fuentes de logs y cambios administrativos sobre FortiGate. Para cada escenario se verificó la generación de hallazgos, alertas y notificaciones, así como la correcta visualización de la información dentro de OpenSearch Dashboards.

Los resultados obtenidos permitieron validar el correcto funcionamiento de la arquitectura propuesta y evidenciar la capacidad de la plataforma para detectar comportamientos relevantes de seguridad dentro del entorno corporativo de laboratorio.

Escenario de Fuerza Bruta SSH

El primer escenario de validación consistió en la simulación de un ataque de fuerza bruta contra el servicio SSH de un switch Aruba CX 8360. Para la ejecución de la prueba se utilizó la herramienta Hydra desde un equipo Kali Linux, generando múltiples intentos fallidos de autenticación sobre el dispositivo de red.

Los eventos producidos por el switch fueron enviados mediante Syslog hacia la plataforma OpenSearch, donde fueron procesados y almacenados para su posterior análisis. Sobre esta fuente de datos se implementó una regla de detección orientada a identificar múltiples intentos fallidos de autenticación SSH provenientes de una misma dirección IP dentro de una ventana temporal definida.

Durante la ejecución de la prueba, la regla de detección fue activada correctamente al alcanzarse el umbral configurado, generando un hallazgo dentro del módulo Security Analytics. Posteriormente, el sistema emitió una notificación por correo electrónico como mecanismo de alertamiento para el administrador de seguridad.

La validación de este escenario permitió comprobar la capacidad de la solución para detectar intentos de acceso no autorizados sobre dispositivos de infraestructura de red, así como verificar el correcto funcionamiento de los procesos de recolección, correlación y alertamiento implementados.

De acuerdo con el framework ATT&CK, este escenario se encuentra asociado a la técnica T1110 (Brute Force), correspondiente a intentos repetitivos de autenticación utilizados para obtener acceso a sistemas mediante la validación masiva de credenciales.

Figura 48

Ejecución de ataque de fuerza bruta SSH mediante Hydra

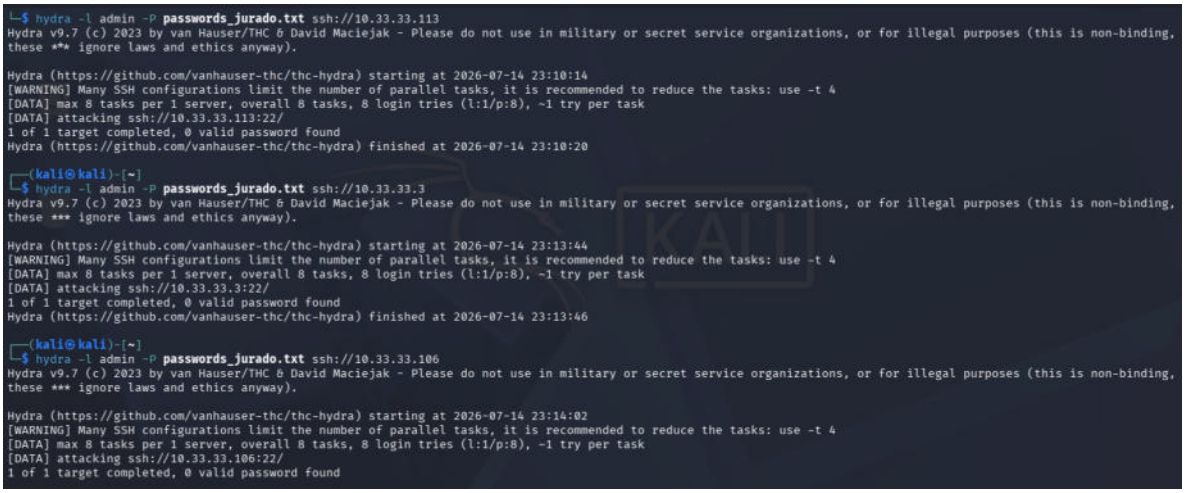


Figura 49

Hallazgo generado por la regla de detección de fuerza bruta SSH

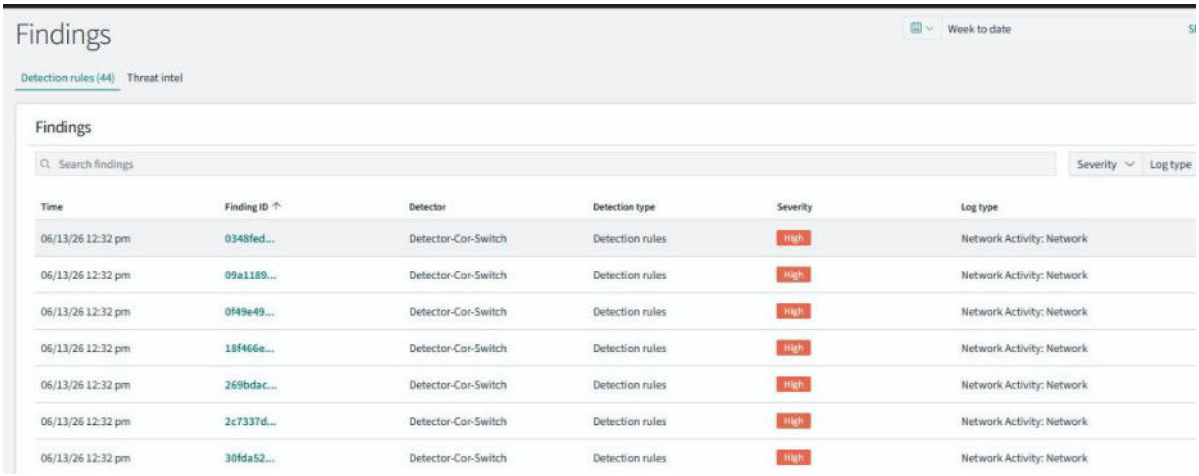


Figura 50

Notificación por correo electrónico generada por la alerta de fuerza bruta SSH

La figura evidencia la generación automática de una notificación por correo electrónico como mecanismo de alertamiento del SIEM tras la detección de múltiples intentos fallidos de autenticación SSH. Esta funcionalidad corresponde al proceso de alertamiento de la plataforma y no constituye una capacidad SOAR o de respuesta automatizada ante incidentes.

Escenario de Reconocimiento de Red

El segundo escenario de validación consistió en la ejecución de actividades de reconocimiento de red mediante la herramienta Nmap desde un equipo Kali Linux. El objetivo de esta prueba fue verificar la capacidad del SIEM para detectar comportamientos asociados a la identificación de servicios y dispositivos presentes en la infraestructura monitoreada.

Durante la ejecución de la prueba se realizaron escaneos dirigidos hacia los dispositivos del entorno corporativo de laboratorio, generando eventos relacionados con conexiones y consultas de red. Dichos eventos fueron recolectados por las fuentes de monitoreo configuradas y posteriormente procesados por la plataforma OpenSearch.

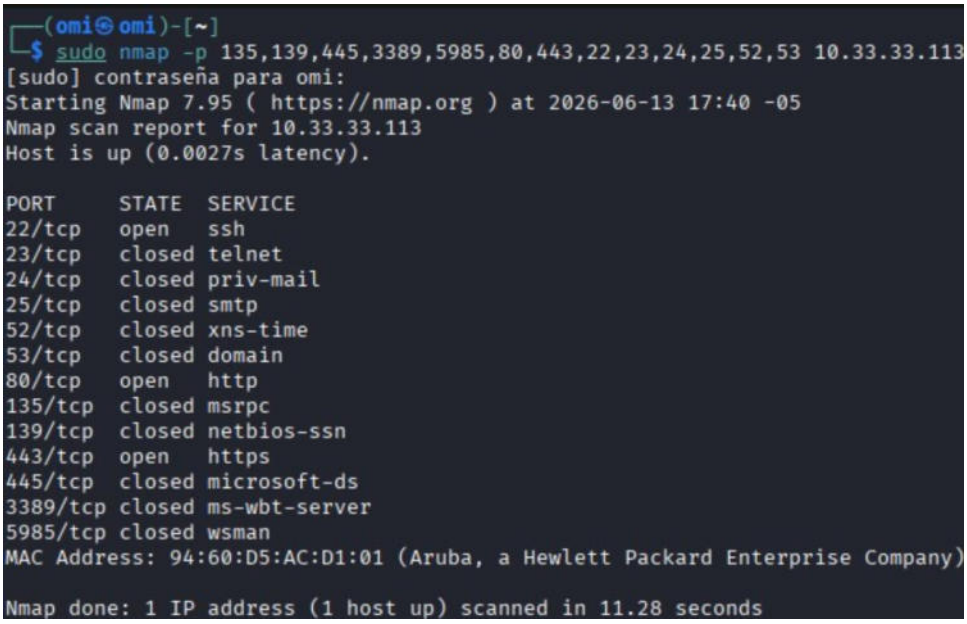
La regla de detección implementada para este escenario permitió identificar patrones compatibles con actividades de reconocimiento de red, generando un hallazgo dentro del módulo Security Analytics y activando los mecanismos de alertamiento definidos para la solución.

Los resultados obtenidos evidenciaron la capacidad de la plataforma para detectar actividades preliminares de reconocimiento utilizadas comúnmente por un atacante antes de intentar comprometer sistemas o servicios. Asimismo, se verificó la correcta visualización de la información en los dashboards implementados y la generación de alertas asociadas al evento detectado.

De acuerdo con el framework ATT&CK, este escenario se encuentra alineado con la técnica T1046 (Network Service Discovery), correspondiente a actividades orientadas a identificar servicios de red disponibles dentro de una infraestructura tecnológica.

Figura 51

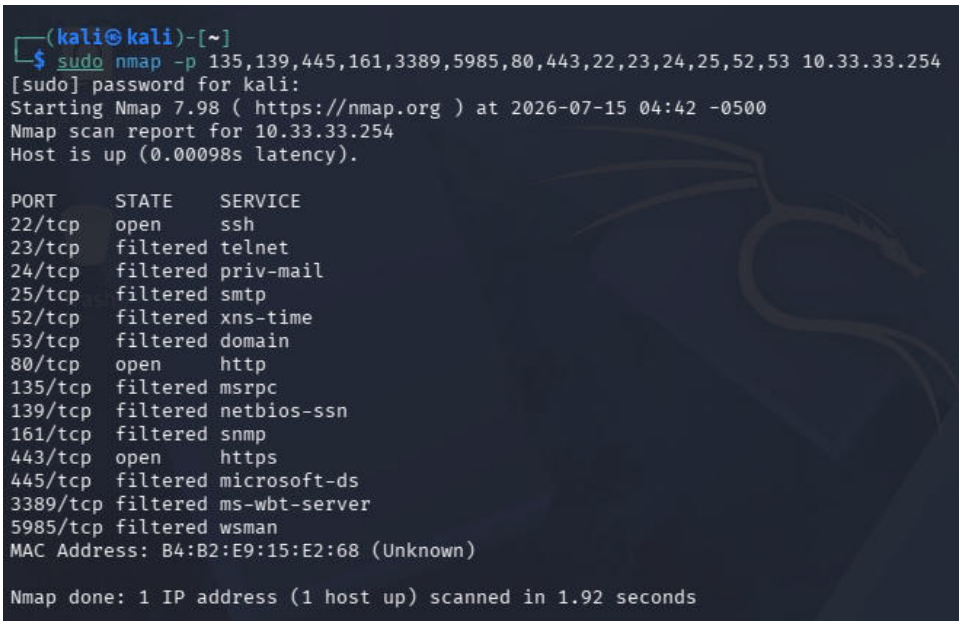
Ejecución de reconocimiento de red mediante Nmap



Nota. Ejecución de Nmap al switch core Aruba para verificar puertos abiertos.

Figura 52

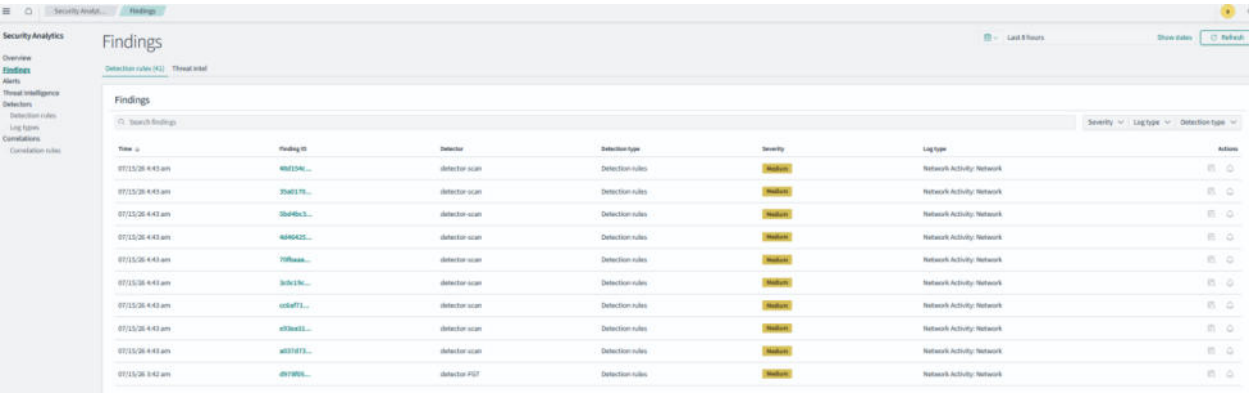
Ejecución de reconocimiento de red hacia FortiGate mediante Nmap



La figura 52 evidencia la ejecución de un escaneo de reconocimiento de red mediante Nmap hacia el firewall FortiGate, con el propósito de identificar servicios expuestos y validar la detección de actividad asociada a la técnica T1046 Network Service Discovery.

Figura 53

Hallazgo generado por la regla de detección de reconocimiento de red



Nota. OpenSearch Security Analytics generó un hallazgo asociado al escenario de reconocimiento ejecutado mediante Nmap, permitiendo validar la detección de actividad relacionada con la técnica T1046 Network Service Discovery.

Escenario de Creación de Cuenta en Active Directory

El tercer escenario de validación consistió en la creación controlada de una cuenta de usuario dentro del servicio Active Directory del entorno de laboratorio. La prueba fue ejecutada desde Windows Server mediante PowerShell utilizando comandos administrativos autorizados, con el objetivo de verificar la capacidad del SIEM para detectar eventos relacionados con la administración de cuentas.

Durante la ejecución se generó el evento de seguridad 4720 de Microsoft Windows, correspondiente a la creación de una nueva cuenta de usuario. Dicho evento fue recolectado por los mecanismos de monitoreo implementados y posteriormente enviado hacia OpenSearch para su procesamiento y almacenamiento.

La regla de detección configurada para este escenario permitió identificar correctamente el evento generado, registrando un hallazgo dentro de OpenSearch Security Analytics y validando la correcta recepción de los logs provenientes de Active Directory. Adicionalmente, la información fue visualizada en los dashboards de monitoreo diseñados para el análisis de eventos de seguridad sobre sistemas Windows.

Los resultados obtenidos demostraron la capacidad de la solución para detectar actividades relacionadas con la administración de cuentas dentro de un dominio corporativo, proporcionando visibilidad sobre cambios que podrían representar riesgos de seguridad cuando son realizados sin autorización o fuera de los procedimientos establecidos.

De acuerdo con ATT&CK, este escenario se relaciona con la técnica T1136.002 (Create Domain Account), asociada a la creación de cuentas dentro de entornos de dominio como mecanismo de persistencia o establecimiento de acceso dentro de una infraestructura corporativa.

La figura evidencia la correcta recepción y almacenamiento del evento 4720 dentro de OpenSearch. El evento corresponde a la creación de una cuenta de usuario en Active Directory y permitió validar la detección de la técnica T1136.002 (Create Domain Account) del framework ATT&CK.

Figura 54

Creación de cuenta de usuario mediante PowerShell en Active Directory

```
PS C:\Users\Administrador> New-ADUser `
>> -Name "UsuarioSIEM3" `
>> -SamAccountName "usuariosiem3" `
>> -AccountPassword (ConvertTo-SecureString "Lab123456!" -AsPlainText -Force) `
>> -Enabled $true
```

Figura 55

Evento 4720 generado por la creación de una cuenta de usuario

```
PS C:\Users\Administrador> Get-WinEvent -FilterHashtable @{LogName='Security';ID=4720} -MaxEvents 5


   ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated                     Id LevelDisplayName Message
-----------                     -- ---------------- -------
13/06/2026 14:12:00           4720 Información      Se creó una cuenta de usuario....
```

Figura 56

Evento de creación de cuenta almacenado en OpenSearch

Figura 57

Detalle de evento de creación de cuenta almacenado en OpenSearch

Escenario de Correlación de Eventos

Además de la detección individual de eventos, se evaluó la capacidad de correlación de la plataforma mediante la implementación de reglas orientadas a relacionar actividades potencialmente sospechosas dentro de una misma ventana temporal. El objetivo de esta prueba fue verificar que OpenSearch Security Analytics pudiera asociar múltiples eventos provenientes de distintas fuentes para proporcionar un contexto de análisis más amplio.

Para esta validación se configuró una regla de correlación que relaciona eventos de autenticación fallida y actividades posteriores registradas dentro de una ventana temporal definida. La lógica implementada permite identificar secuencias de eventos que, analizados de forma individual, podrían no representar una amenaza relevante, pero que en conjunto pueden indicar comportamientos asociados a intentos de compromiso de sistemas.

Durante las pruebas realizadas, la plataforma generó hallazgos correlacionados cuando se cumplieron las condiciones establecidas en la regla. Estos hallazgos fueron registrados dentro del

módulo Security Analytics y visualizados en los dashboards de monitoreo, permitiendo identificar la relación existente entre los eventos detectados.

Los resultados obtenidos demostraron la capacidad de OpenSearch para correlacionar información proveniente de diferentes fuentes de logs, facilitando el análisis de eventos de seguridad y reduciendo la necesidad de realizar revisiones manuales sobre grandes volúmenes de registros. Esta capacidad constituye uno de los elementos fundamentales de una plataforma SIEM, al proporcionar contexto adicional para la identificación de actividades potencialmente maliciosas.

Figura 58

Regla de correlación implementada en OpenSearch Security Analytics

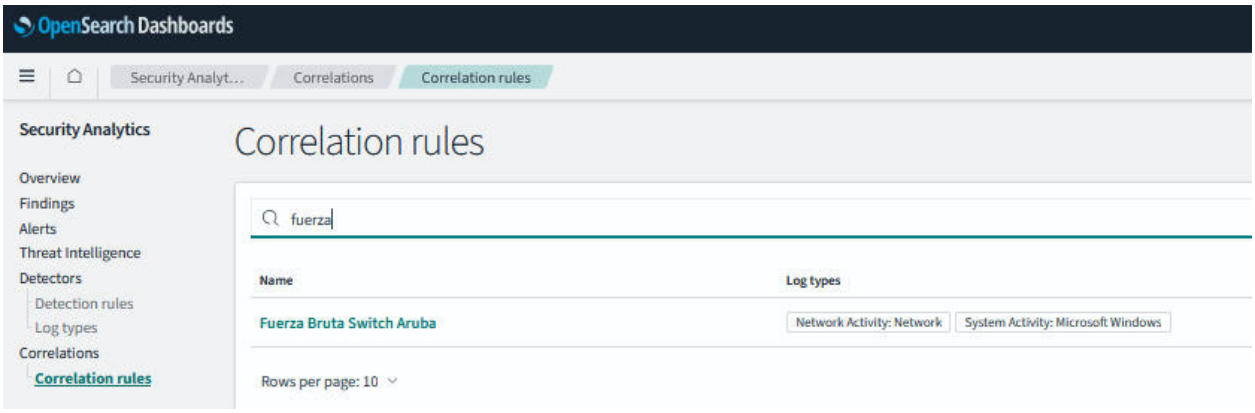


Figura 59

Detalle de correlación generado por OpenSearch Security Analytics

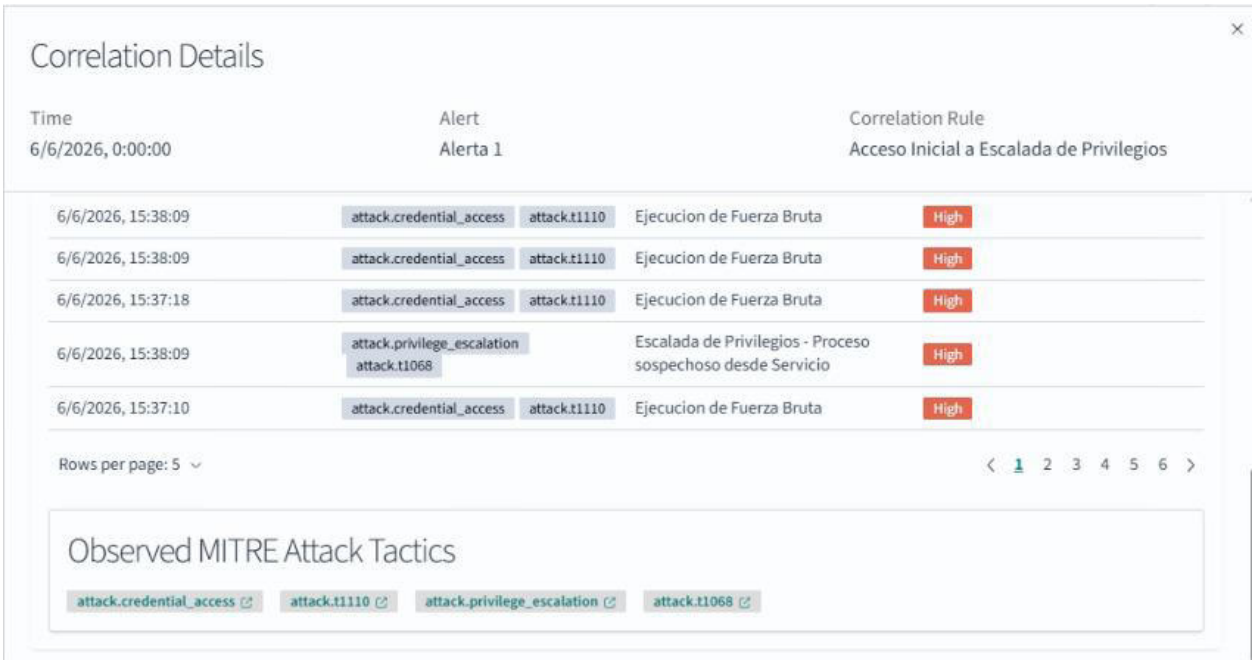
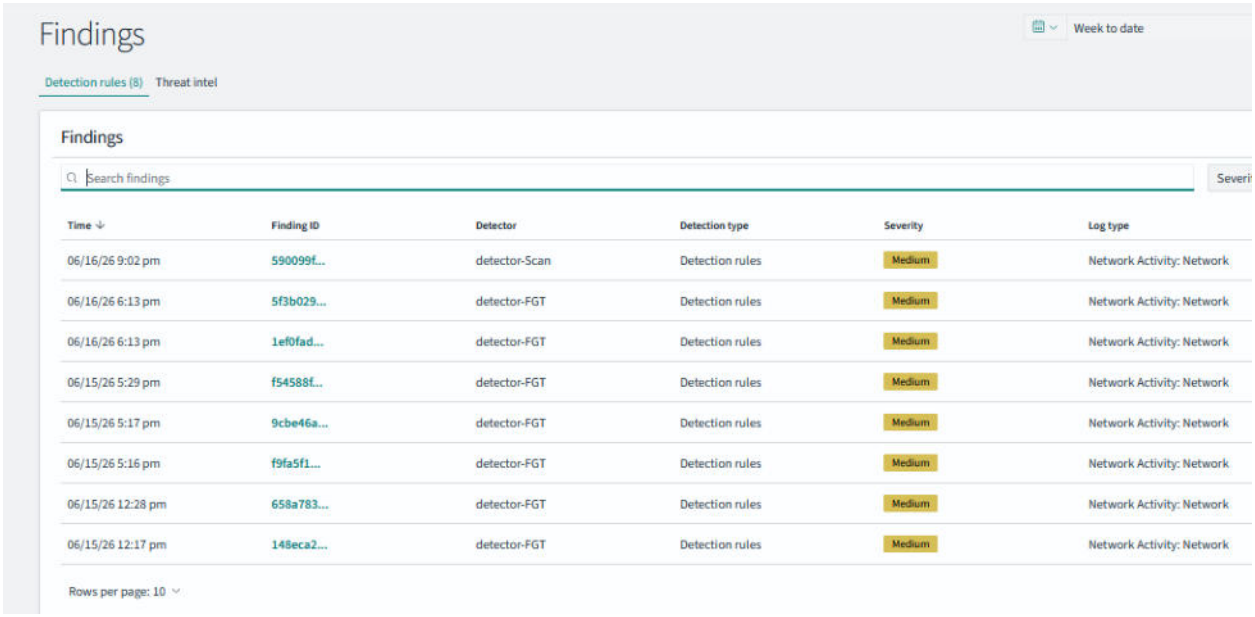


Figura 60

Hallazgo correlacionado generado durante las pruebas de validación



Nota. La figura evidencia la generación de un hallazgo correlacionado por OpenSearch Security Analytics a partir de la relación temporal entre múltiples eventos de seguridad. Esta

funcionalidad permitió validar la capacidad de correlación de la plataforma dentro del entorno corporativo de laboratorio.

Escenarios de Cambios Sobre FortiGate

Los escenarios administrativos ejecutados sobre FortiGate fueron incluidos en la evaluación temporal de la solución. Para cada escenario se registró la marca temporal correspondiente a la ejecución de la acción administrativa y la hora en que el registro estuvo disponible para consulta en OpenSearch Discover.

El tiempo de detección observado se calculó mediante la diferencia entre ambas marcas temporales. Adicionalmente, se registró la hora de recepción de la notificación por correo electrónico como evidencia complementaria del funcionamiento del mecanismo de alertamiento; sin embargo, dicha marca no fue utilizada para calcular el tiempo medio de detección.

Tabla 29

Escenarios administrativos validados sobre FortiGate

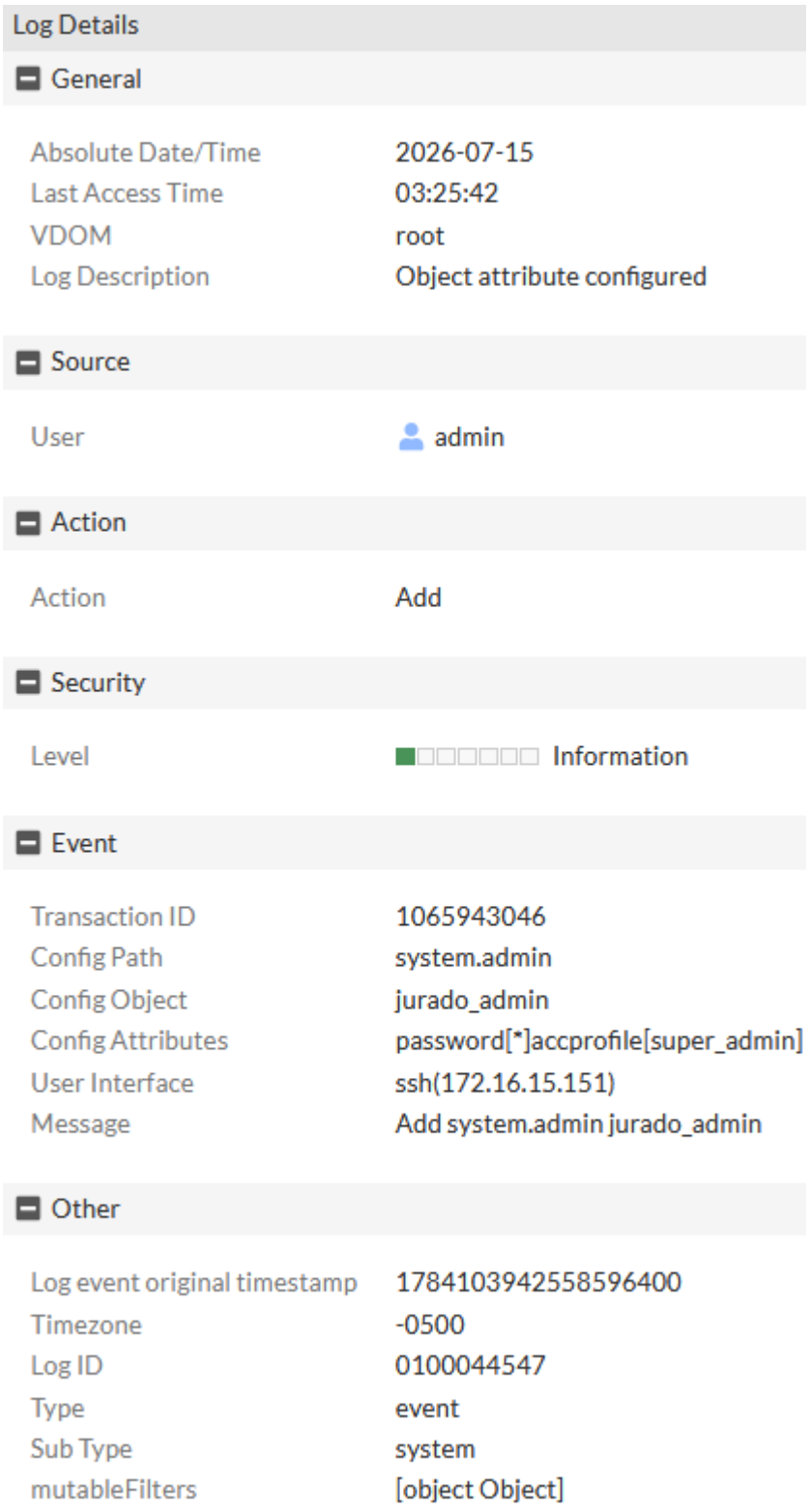
Actividad ejecutada	Fuente de eventos	Técnica ATT&CK asociada	Evidencia obtenida
Creación de usuario local	FortiGate 80F	T1136.001 Create Account: Local Account	Hallazgo generado en Security Analytics
Creación de usuario administrador	FortiGate 80F	T1136.001 Create Account: Local Account / T1098 Account Manipulation	Hallazgo generado en Security Analytics
Creación de política de firewall	FortiGate 80F	T1562 Impair Defenses	Hallazgo generado en Security Analytics
Creación de objeto de dirección	FortiGate 80F	T1562 Impair Defenses	Hallazgo generado en Security Analytics

La creación de un usuario local permitió validar la detección de eventos relacionados con la técnica T1136.001 Create Account: Local Account. En el caso de la creación de un usuario administrador, el evento fue asociado con T1136.001 debido a la creación de una nueva cuenta local, y con T1098 Account Manipulation debido a la asignación de privilegios administrativos mediante el perfil correspondiente.

Por otra parte, la creación de políticas de firewall y objetos de dirección fue asociada con la técnica T1562 Impair Defenses, considerando que este tipo de cambios administrativos puede modificar el comportamiento de los controles de seguridad perimetral. Esta asociación fue utilizada dentro del contexto de las reglas implementadas para identificar modificaciones relevantes en la configuración del firewall y generar los hallazgos correspondientes en la solución SIEM.

Figura 61

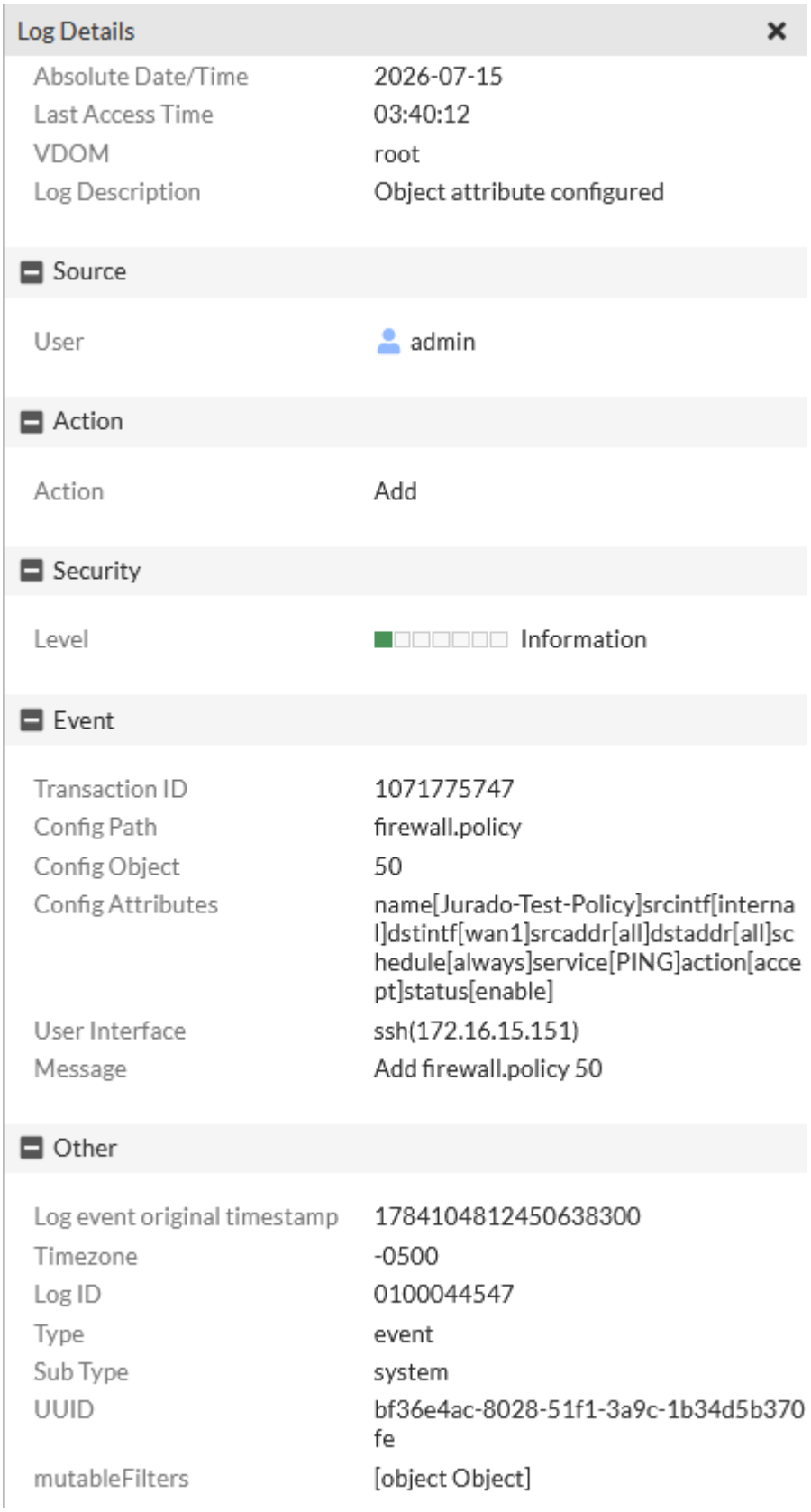
Hallazgo generado por creación de usuario local en FortiGate



Nota. OpenSearch Security Analytics detectó la creación de un usuario local en FortiGate, evento asociado a la técnica T1136.001 Create Account: Local Account dentro del framework ATT&CK.

Figura 62

Hallazgo generado por creación de política de firewall en FortiGate



Log Details

Absolute Date/Time	2026-07-15
Last Access Time	03:40:12
VDOM	root
Log Description	Object attribute configured

Source

User	admin

Action

Action	Add

Security

Level	Information

Event

Transaction ID	1071775747
Config Path	firewall.policy
Config Object	50
Config Attributes	name[Jurado-Test-Policy]srcintf[internal]dstintf[wan1]srcaddr[all]dstaddr[all]schedule[always]service[PING]action[accept]status[enable]
User Interface	ssh(172.16.15.151)
Message	Add firewall.policy 50

Other

Log event original timestamp	1784104812450638300
Timezone	-0500
Log ID	0100044547
Type	event
Sub Type	system
UUID	bf36e4ac-8028-51f1-3a9c-1b34d5b370fe
mutableFilters	[object Object]

Nota. OpenSearch Security Analytics detectó la creación de una nueva política de firewall en FortiGate, evento asociado a la técnica T1562 Impair Defenses, debido a que representa una modificación en controles de seguridad perimetral.

Figura 63

Hallazgo generado por cambio de privilegios de usuario en FortiGate

General

Absolute Date/Time	2026-07-15
Last Access Time	03:25:42
VDOM	root
Log Description	Object attribute configured

Source

User	admin

Action

Action	Add

Security

Level	Information

Event

Transaction ID	1065943046
Config Path	system.admin
Config Object	jurado_admin
Config Attributes	password[*]accprofile[super_admin]
User Interface	ssh(172.16.15.151)
Message	Add system.admin jurado_admin

Other

Log event original timestamp	1784103942558596400
Timezone	-0500
Log ID	0100044547
Type	event
Sub Type	system
mutableFilters	[object Object]

Nota. El hallazgo corresponde a la modificación de privilegios de una cuenta en FortiGate, evento asociado a la técnica T1098 Account Manipulation debido al cambio de atributos o permisos administrativos de una cuenta existente.

Figura 64

Hallazgo generado por la detección de escaneo de puertos hacia FortiGate

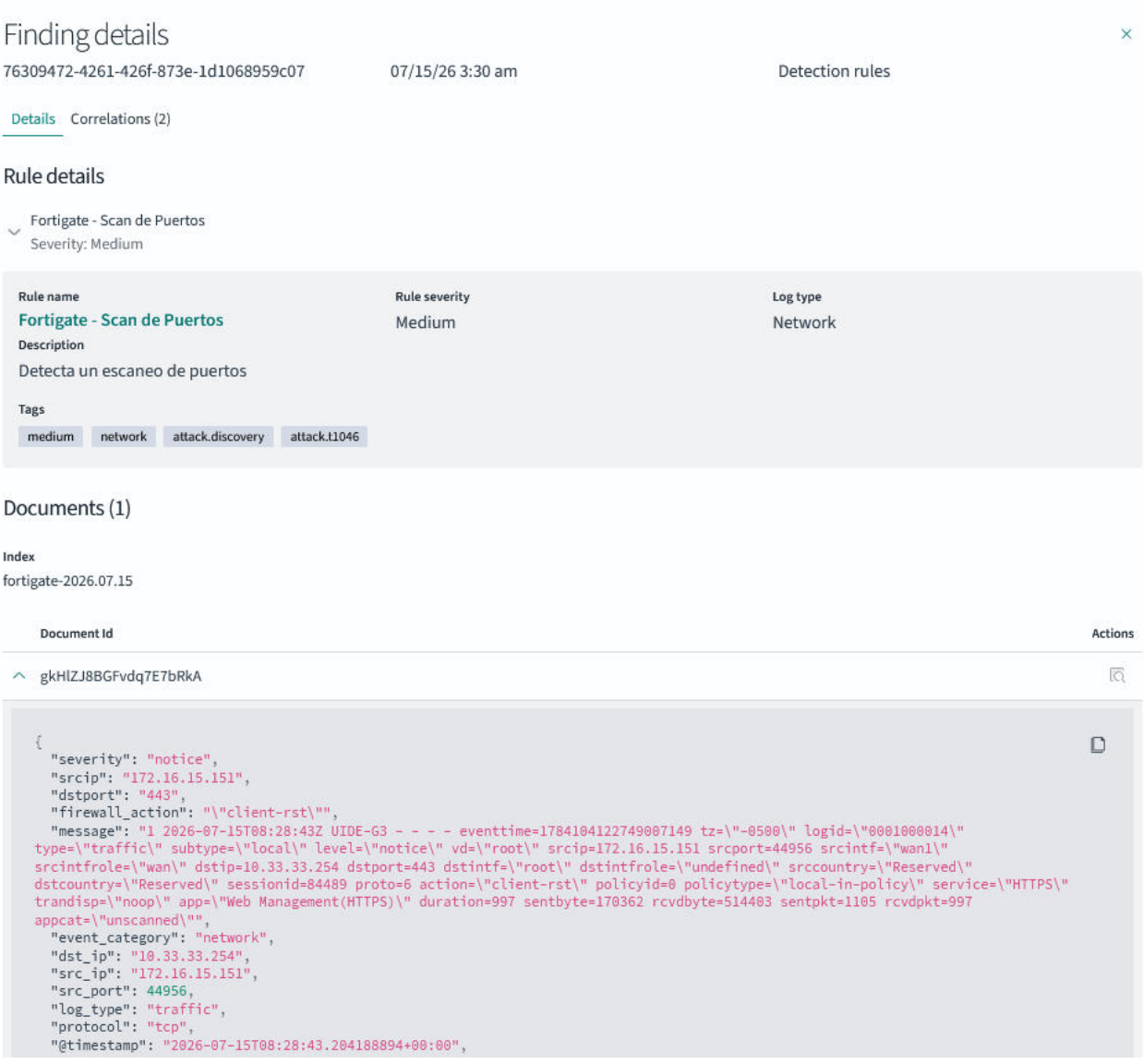


Figura 65

Notificación por correo electrónico generada ante escaneo de puertos hacia FortiGate

Nota. OpenSearch Security Analytics generó un hallazgo asociado al escaneo de puertos hacia FortiGate, permitiendo validar la detección de actividad relacionada con la técnica T1046 Network Service Discovery.

Evaluación de los Objetivos Específicos

Con el fin de determinar el grado de cumplimiento de los objetivos planteados en la investigación, se realizó una evaluación basada en los resultados obtenidos durante la implementación y validación de la solución SIEM. Los resultados permitieron verificar el cumplimiento de cada uno de los objetivos específicos definidos en el Capítulo 1, evidenciando la capacidad de la plataforma para centralizar eventos, correlacionar información de seguridad y generar alertas oportunas dentro del entorno corporativo de laboratorio.

Tabla 30

Evaluación de cumplimiento de los objetivos específicos

Objetivo específico	Resultado obtenido	Estado
Analizar los requerimientos funcionales y de seguridad para la implementación de una solución SIEM	Se identificaron las necesidades de recolección, almacenamiento, correlación y alertamiento para el entorno corporativo de laboratorio.	Cumplido
Diseñar una arquitectura SIEM basada en OpenSearch	Se diseñó una arquitectura All-in-One incorporando OpenSearch, Data Prepper, Fluent Bit, Osquery y Security Analytics.	Cumplido
Implementar mecanismos de centralización de eventos de seguridad	Se integraron múltiples fuentes de logs provenientes de Windows Server, dispositivos Aruba, FortiGate y sistemas Linux.	Cumplido
Implementar reglas de detección y correlación de eventos	Se desarrollaron reglas alineadas con ATT&CK y mecanismos de correlación dentro de OpenSearch Security Analytics.	Cumplido
Diseñar dashboards para el monitoreo de eventos de seguridad	Se implementaron dashboards orientados a monitoreo de autenticación, eventos de red y actividades de seguridad.	Cumplido
Validar la solución mediante escenarios controlados de seguridad	Se ejecutaron escenarios de fuerza bruta SSH, reconocimiento de red, creación de cuentas en Active Directory y cambios administrativos en FortiGate, todos evidenciados mediante eventos, alertas o hallazgos en OpenSearch Security Analytics.	Cumplido
Evaluar la efectividad de la solución mediante métricas de desempeño	Se calcularon métricas de detección, cobertura ATT&CK, correlación y tiempo medio de detección (MTTD).	Cumplido

Diseño y despliegue de SIEM con OpenSearch

Los resultados obtenidos evidencian que todos los objetivos específicos definidos para la investigación fueron alcanzados satisfactoriamente. La arquitectura implementada permitió centralizar eventos provenientes de diferentes fuentes, aplicar mecanismos de detección y correlación, generar alertas automáticas y proporcionar capacidades de monitoreo alineadas con las necesidades del entorno evaluado.

Análisis de Cobertura MITRE ATT&CK®

Uno de los objetivos de la investigación fue implementar mecanismos de detección alineados con el framework ATT&CK, permitiendo relacionar los eventos observados con técnicas ampliamente utilizadas para describir comportamientos asociados a amenazas de ciberseguridad. Durante la fase de validación se ejecutaron diferentes escenarios controlados que permitieron verificar la capacidad de la plataforma para identificar actividades correspondientes a distintas tácticas y técnicas definidas por dicho framework.

La cobertura obtenida se evaluó considerando las técnicas efectivamente validadas mediante la generación de eventos reales, detección por parte del SIEM y evidencia documentada dentro del entorno corporativo de laboratorio.

Tabla 31

Cobertura MITRE ATT&CK® validada durante las pruebas

Técnica ATT&CK	Nombre de la técnica	Escenario ejecutado	Evidencia obtenida
T1110	Brute Force	Ataque de fuerza bruta SSH mediante Hydra	Hallazgo, alerta y notificación generada
T1046	Network Service Discovery	Escaneo de red mediante Nmap	Hallazgo generado por Security Analytics
T1136.002	Create Domain Account	Creación de cuenta en Active Directory	Evento 4720 detectado y almacenado en OpenSearch
T1136.001	Create Account: Local Account	Creación de usuario local en FortiGate	Hallazgo “FortiGate - Nuevo usuario local” generado en OpenSearch Security Analytics
T1098	Account Manipulation	Creación o asignación de privilegios administrativos a un usuario en FortiGate	Hallazgo “FortiGate - Nuevo usuario de administrador” generado en OpenSearch Security Analytics
T1562	Impair Defenses	Creación de política de firewall y objeto de dirección en FortiGate	Hallazgos “FortiGate - Nueva política de Firewall” y “FortiGate - Nueva dirección de firewall”

Diseño y despliegue de SIEM con OpenSearch

Los resultados obtenidos permitieron validar la detección de técnicas pertenecientes a diferentes etapas del ciclo de ataque descrito por ATT&CK. La técnica T1110 se asocia con intentos repetitivos de autenticación, los cuales fueron evaluados mediante pruebas de fuerza bruta SSH contra dispositivos Aruba. La técnica T1046 corresponde a actividades de descubrimiento orientadas a identificar servicios de red disponibles, validada mediante el escaneo ejecutado con Nmap dentro del segmento de laboratorio. Por su parte, la técnica T1136.002 se relaciona con la creación de cuentas en entornos de dominio, evidenciada mediante el evento 4720 generado en Active Directory.

Adicionalmente, los eventos administrativos generados en el firewall FortiGate permitieron ampliar la cobertura ATT&CK validada. La técnica T1136.001 fue asociada con la creación de usuarios locales en el dispositivo de seguridad, mientras que la técnica T1098 se relacionó con la creación o modificación de cuentas con privilegios administrativos. Asimismo, la técnica T1562 fue vinculada con cambios en controles de seguridad perimetral, como la creación de políticas de firewall y objetos de dirección.

La detección exitosa de estas técnicas evidencia que la solución SIEM implementada fue capaz de proporcionar visibilidad sobre eventos relevantes provenientes de diferentes fuentes, incluyendo dispositivos Aruba, Windows Server con Active Directory y FortiGate. Esto demuestra que las reglas configuradas no se limitaron a una única fuente de eventos, sino que permitieron validar escenarios relacionados con acceso no autorizado, descubrimiento de red, persistencia, manipulación de cuentas y modificación de configuraciones de seguridad.

Es importante precisar que la cobertura obtenida corresponde únicamente a las técnicas evaluadas dentro del entorno corporativo de laboratorio. Por lo tanto, los resultados no representan una cobertura total del framework ATT&CK, sino una validación específica de las

técnicas incluidas en los escenarios ejecutados y evidenciados mediante OpenSearch, OpenSearch Security Analytics y los registros generados por las fuentes integradas.

Para los escenarios administrativos de FortiGate, las marcas temporales utilizadas fueron obtenidas con resolución de segundos a partir de los registros disponibles en OpenSearch Discover. No se utilizó como fuente del cálculo la hora redondeada a nivel de minuto presentada en la consola visual de hallazgos. Tampoco se infirieron valores de milisegundos que no estuvieran disponibles en las evidencias originales.

Evaluación de Métricas de Desempeño

Con el propósito de evaluar la efectividad de la solución implementada, se analizaron diferentes métricas asociadas a la capacidad de detección, correlación y alertamiento de la plataforma SIEM. Estas métricas permitieron medir el comportamiento de la solución durante la ejecución de los escenarios de validación descritos en el capítulo anterior y determinar su desempeño dentro del entorno corporativo de laboratorio.

Desarrollo de sincronización horaria y precisión de las métricas

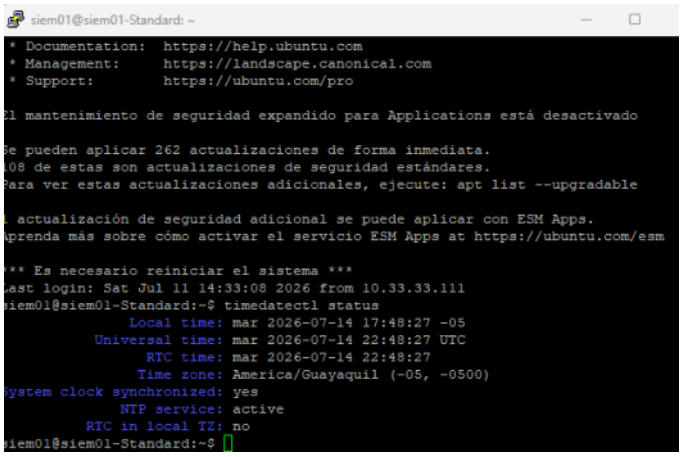
La medición de los intervalos temporales requiere revisar la configuración horaria de los componentes que intervienen en la generación, recepción, procesamiento y visualización de los eventos. Una diferencia entre los relojes de los dispositivos puede afectar la comparación directa de las marcas temporales utilizadas durante las pruebas.

Como parte de la revisión metodológica, se documentaron la zona horaria, la fuente temporal y el estado de sincronización disponible en los principales componentes del laboratorio, incluyendo el servidor Ubuntu donde se desplegó OpenSearch, el servidor Windows con Active Directory, el firewall FortiGate, los dispositivos Aruba y el equipo utilizado para ejecutar los escenarios de validación.

Las evidencias obtenidas mostraron que la configuración horaria no era homogénea en todos los componentes. Algunos equipos presentaban el servicio NTP habilitado y una fuente temporal identificable, mientras que en otros casos se observó el uso del reloj local, la ausencia de un servidor configurado o un estado de sincronización no confirmado. Por esta razón, no se asumió que todos los dispositivos utilizaran una única fuente NTP ni que existiera una sincronización estricta entre la totalidad de los nodos participantes.

Figura 66

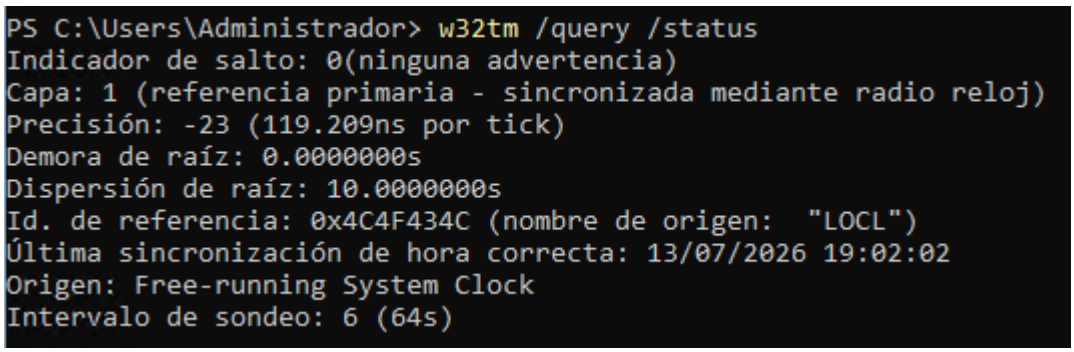
Configuración horaria del servidor Ubuntu que aloja la solución SIEM



*Nota***.** Estado de la zona horaria y sincronización temporal del servidor Ubuntu que aloja la solución OpenSearch.

Figura 67

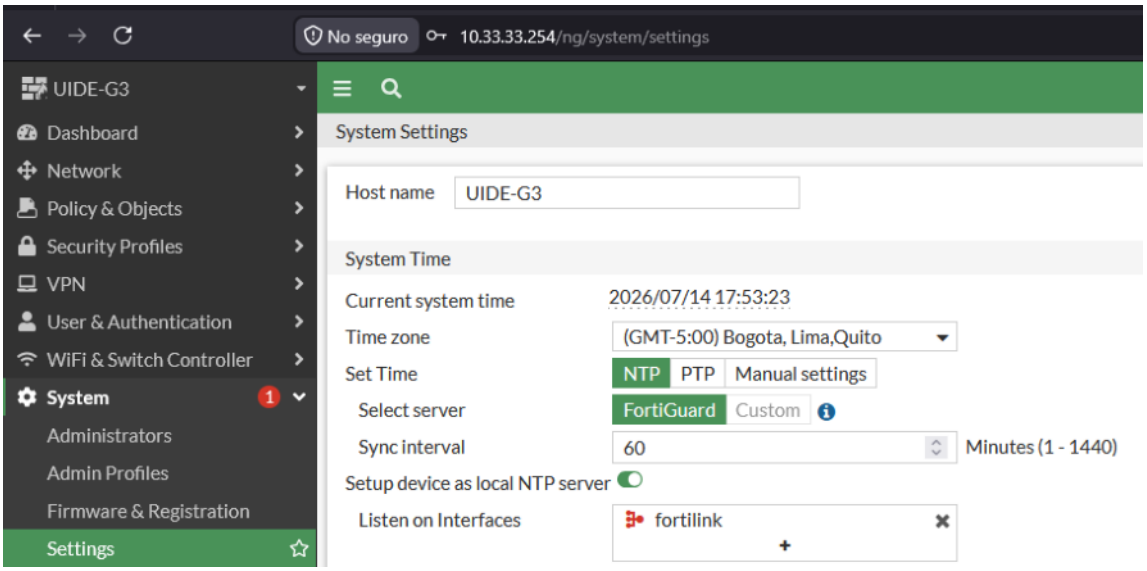
Configuración horaria del servidor Windows con Active Directory



*Nota***.** El servidor Active Directory utiliza el reloj local del sistema (referencia LOCL), establecido mediante configuración horaria manual

Figura 68

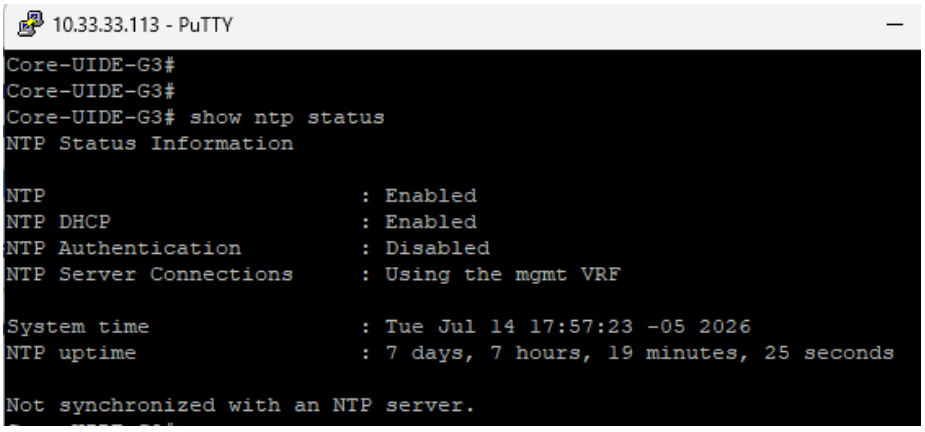
Configuración de sincronización NTP del firewall FortiGate



*Nota***.** La captura muestra que el firewall FortiGate utiliza el servicio NTP de FortiGuard, opera con la zona horaria GMT−05:00 correspondiente a Bogotá, Lima y Quito, y tiene configurado un intervalo de sincronización de 60 minutos.

Figura 69

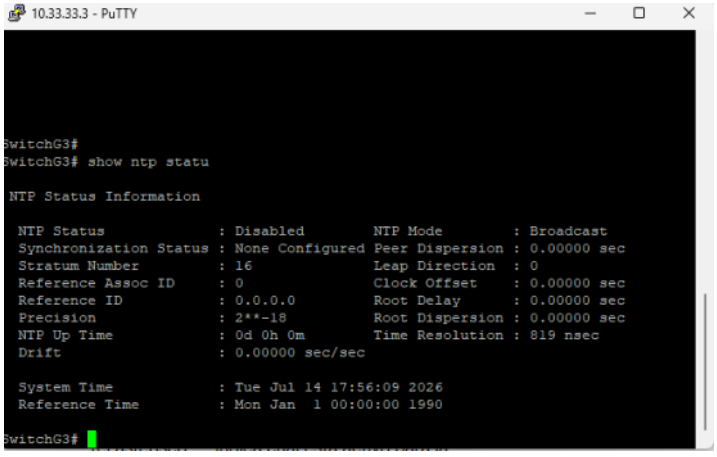
Configuración horaria del switch Aruba CX 8360



Nota. El switch Aruba CX 8360 operaba con la hora del sistema establecida de forma manual para el registro de eventos Syslog.

Figura 70

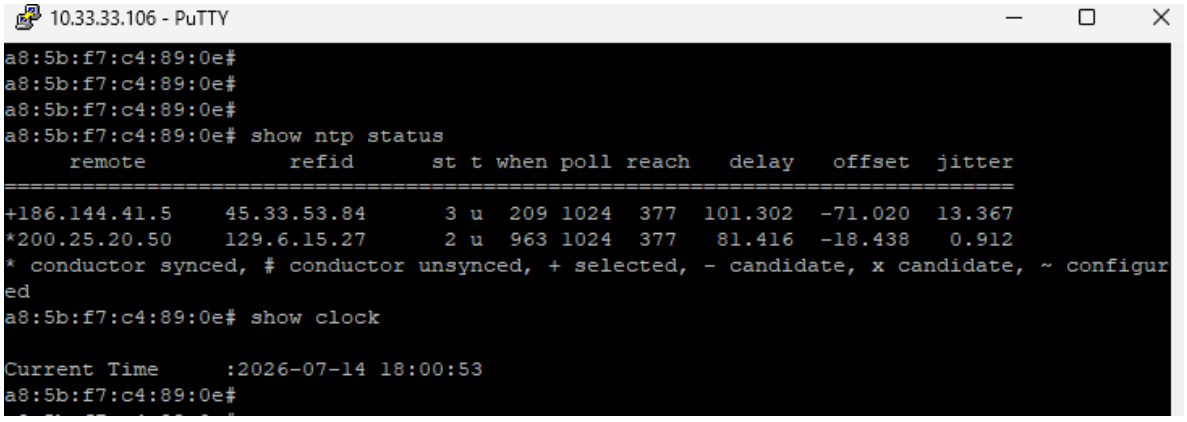
Configuración horaria del switch Aruba



Nota. Configuración horaria del switch Aruba administrada y ajustada de manera manual en el dispositivo.

Figura 71

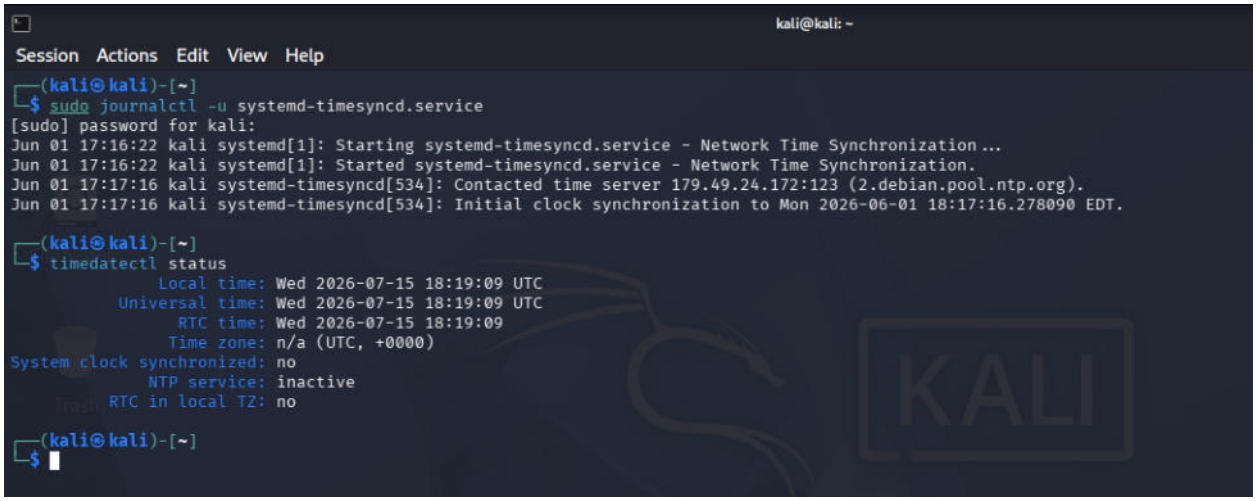
Configuración horaria del AP Aruba



Nota. Servidores NTP del punto de acceso Aruba; el asterisco indica la fuente activa seleccionada para la sincronización.

Figura 72

Estado de sincronización horaria del equipo Kali Linux utilizado en las pruebas



Nota. Configuración horaria de la estación Kali Linux establecida manualmente para el desarrollo de las pruebas de seguridad.

Las evidencias presentadas permiten identificar la configuración y el estado de sincronización horaria observado en los componentes participantes. Debido a que algunos dispositivos no demostraron una sincronización NTP efectiva, los intervalos calculados se interpretaron como tiempos de detección observados dentro del entorno controlado de laboratorio y no como mediciones exactas de latencia extremo a extremo. Esta limitación fue considerada durante el análisis de los resultados presentados en la Tabla 28, Tabla 32 y Tabla 33.

Para realizar los cálculos, las marcas temporales fueron expresadas bajo la zona horaria UTC−05:00 y se utilizaron valores con resolución de segundos. No obstante, debido a que las evidencias disponibles no confirman una sincronización NTP efectiva y uniforme en todos los equipos, los resultados se presentan como tiempos de detección observados dentro del entorno de laboratorio y no como mediciones exactas de latencia extremo a extremo.

Las evidencias de configuración y estado horario de los componentes participantes se presentan en el Anexo A. Estas evidencias permiten identificar las fuentes temporales utilizadas y las limitaciones metodológicas que deben considerarse al interpretar los resultados de las Tabla 28, Tabla 32 y

Tabla 33.

Resolución de marcas temporales y metodología de medición

Para mejorar la consistencia de las métricas temporales, se utilizaron marcas de tiempo con resolución de segundos obtenidas de las evidencias de ejecución de cada escenario y de los registros disponibles en OpenSearch Discover. La hora inicial corresponde a la marca temporal registrada al ejecutar o comenzar la actividad evaluada, mientras que la hora final utilizada para calcular el tiempo de detección observado corresponde al momento en que el registro estuvo disponible para su consulta en OpenSearch.

En los escenarios de creación de cuenta en Active Directory y cambios administrativos sobre FortiGate, la hora del evento corresponde a la marca temporal registrada al momento de realizar la acción evaluada. En los escenarios de fuerza bruta SSH y reconocimiento de red mediante Nmap, la hora inicial corresponde al comienzo de la actividad que generó la secuencia de registros procesados por la plataforma.

El tiempo de detección observado para cada escenario se calculó mediante la diferencia entre la hora de visualización del registro en OpenSearch y la hora de ejecución del evento:

$$TD_i = t_{OpenSearch,i} - t_{evento,i}$$

donde TD_i es el tiempo de detección observado para el escenario i, $t_{OpenSearch,i}$ es la hora de visualización del registro en OpenSearch para el escenario i, y $t_{evento,i}$ es la hora de ejecución del evento para el escenario i.

Posteriormente, el tiempo medio de detección observado se obtuvo mediante la fórmula:

$$MTTD_{observado} = \frac{\sum_{i=1}^{n} TD_i}{n}$$

donde $MTTD_{observado}$ es el tiempo medio de detección observado, n es el número total de escenarios o eventos evaluados, y i representa cada escenario individual.

La hora de recepción de la notificación por correo electrónico se registró como evidencia complementaria para verificar el funcionamiento integral del mecanismo de alertamiento. Sin embargo, esta marca temporal no fue utilizada para calcular el tiempo de detección observado, debido a que incluye tiempos adicionales relacionados con la evaluación del monitor, la generación del mensaje, el procesamiento del servidor SMTP y la entrega de la notificación al destinatario.

Los resultados obtenidos mediante esta metodología se presentan en las Tabla 28, Tabla 32 y

Tabla 33. En los siete escenarios evaluados se obtuvo un tiempo medio de detección observado de 23,3 segundos, con valores individuales comprendidos entre 10 y 41 segundos.

Tabla 32

Tiempo de detección observado en los escenarios generales de validación

Escenario	Hora del evento	Hora de disponibilidad en OpenSearch Discover	Hora de recepción de la notificación	Tiempo de detección observado en OpenSearch
Fuerza bruta SSH	23:10:11	23:10:38	23:11:11	27 segundos
Reconocimiento de red mediante Nmap	04:42:00	04:42:41	04:43:41	41 segundos

Creación de cuenta en Active Directory	14:12:00	14:12:10	14:13:08	10 segundos

Tabla 33

Tiempo de detección observado en escenarios administrativos de FortiGate

Escenario evaluado	Hora del evento	Hora de disponibilidad en OpenSearch Discover	Hora de recepción de la notificación	Tiempo de detección observado en OpenSearch
Creación de usuario local en FortiGate	03:14:00	03:14:23	03:16:02	23 segundos
Creación de política de firewall	03:40:00	03:40:13	03:42:04	13 segundos
Creación de objeto de dirección en FortiGate	03:31:00	03:31:25	03:32:58	25 segundos
Creación de usuario administrador en FortiGate	03:25:18	03:25:42	03:26:08	24 segundos

A partir de los tiempos registrados en los siete escenarios evaluados, se obtuvo un tiempo medio de detección observado en OpenSearch de 23,3 segundos. Este resultado se calculó mediante el promedio de los tiempos transcurridos entre la ejecución o inicio de cada escenario y la disponibilidad del registro correspondiente en OpenSearch Discover. Los valores individuales estuvieron comprendidos entre 10 y 41 segundos.

El menor tiempo observado correspondió a la creación de una cuenta en Active Directory, con 10 segundos, mientras que el mayor correspondió al reconocimiento de red mediante Nmap, con 41 segundos. En los escenarios administrativos sobre FortiGate, los tiempos estuvieron comprendidos entre 13 y 25 segundos.

Diseño y despliegue de SIEM con OpenSearch

Los resultados evidencian que la solución SIEM permitió recolectar, procesar, normalizar e indexar los eventos en intervalos inferiores a un minuto dentro de las condiciones controladas del laboratorio. La medición se realizó utilizando la marca temporal registrada durante la ejecución del escenario y la hora en que el registro estuvo disponible para su consulta en OpenSearch Discover.

La hora de recepción de la notificación por correo electrónico se registró como evidencia complementaria del funcionamiento del mecanismo de alertamiento. Sin embargo, esta marca temporal no fue utilizada en el cálculo del tiempo medio de detección, debido a que incluye tiempos adicionales asociados con la evaluación del monitor, la generación del mensaje, el procesamiento SMTP y la entrega del correo al destinatario.

El cálculo del tiempo medio se realizó sobre siete escenarios representativos: fuerza bruta SSH, reconocimiento de red mediante Nmap, creación de cuenta en Active Directory, creación de usuario local en FortiGate, creación de política de firewall, creación de objeto de dirección y creación de usuario administrador en FortiGate. Durante estas pruebas se validaron seis técnicas MITRE ATT&CK®: T1110, T1046, T1136.002, T1136.001, T1098 y T1562.

Tabla 34

Resultados de las métricas de desempeño evaluadas

Métrica	Resultado obtenido
Tasa de detección	100 %
Técnicas ATT&CK validadas	6
Hallazgos generados	100 % de los escenarios ejecutados
Correlaciones exitosas	Sí
Tiempo medio de detección observado en OpenSearch	23,3 segundos

Falsos positivos observados	0%

Los resultados muestran que la plataforma detectó correctamente los escenarios ejecutados durante la fase de validación, generando los hallazgos y alertas esperadas. En total, se validaron seis técnicas ATT&CK: T1110, T1046, T1136.002, T1136.001, T1098 y T1562, de acuerdo con los escenarios documentados en la Tabla 31. Asimismo, la capacidad de correlación implementada permitió relacionar eventos provenientes de diferentes fuentes de información, proporcionando contexto adicional para el análisis de seguridad.

Durante las pruebas realizadas no se observaron alertas incorrectas asociadas a los escenarios ejecutados, por lo que la tasa de falsos positivos observada fue del 0 % dentro del entorno corporativo de laboratorio. No obstante, este resultado debe interpretarse considerando que las pruebas fueron realizadas en un entorno controlado y con un conjunto limitado de escenarios de validación.

Tabla 35

Matriz de trazabilidad entre escenarios, reglas, técnicas MITRE ATT&CK® y evidencias

Escenario	Fuente de logs	Regla activada	Técnica MITRE	Evidencia	Resultado
Fuerza bruta SSH	Aruba CX 8360	Fuerza Bruta SSH en Core Switch	T1110	Hallazgo y correo	Detectado
Escaneo de red	FortiGate / OpenSearch	Reconocimiento de Red	T1046	Hallazgo y correo	Detectado
Creación de cuenta AD	Windows Server	Creación de Cuenta AD	T1136.002	Evento 4720	Detectado
Usuario local FortiGate	FortiGate	Nuevo usuario local	T1136.001	Hallazgo y correo	Detectado
Usuario administrador FortiGate	FortiGate	Nuevo usuario administrador	T1098	Hallazgo y correo	Detectado
Política de firewall	FortiGate	Nueva política firewall	T1562	Hallazgo y correo	Detectado
Objeto de dirección	FortiGate	Nueva dirección firewall	T1562	Hallazgo y correo	Detectado

Diseño y despliegue de SIEM con OpenSearch

Viabilidad de Implementación en Organizaciones Medianas

La viabilidad de la solución propuesta para organizaciones medianas fue evaluada considerando aspectos técnicos, económicos y operativos. Los resultados obtenidos durante la implementación y validación permitieron evidenciar que una plataforma SIEM basada en OpenSearch puede proporcionar capacidades de monitoreo, detección y correlación de eventos sin requerir inversiones significativas en licenciamiento de software.

A diferencia de diversas soluciones comerciales disponibles en el mercado, la arquitectura implementada utiliza herramientas open source como OpenSearch, Data Prepper, Fluent Bit y Osquery, lo que reduce considerablemente los costos asociados a la adquisición y operación de una plataforma SIEM. Esta característica resulta especialmente relevante para organizaciones medianas que requieren fortalecer sus capacidades de monitoreo de seguridad manteniendo un control adecuado de los recursos financieros destinados a tecnologías de información.

Adicionalmente, la arquitectura propuesta fue desplegada sobre infraestructura virtualizada de recursos moderados, demostrando que es posible implementar capacidades SIEM utilizando equIPamiento comúnmente disponible en entornos corporativos. La solución también permite incorporar nuevas fuentes de eventos mediante protocolos estándar como Syslog, HTTP y APIs, facilitando su adaptación a diferentes escenarios operativos.

Tabla 36

Componentes principales de la solución y costos de licenciamiento

Componente	Tipo de licencia	Costo de licenciamiento
OpenSearch	Open Source	Sin costo
Data Prepper	Open Source	Sin costo

Fluent Bit	Open Source	Sin costo
Osquery	Open Source	Sin costo
OpenSearch Dashboards	Open Source	Sin costo
Security Analytics	Open Source	Sin costo

Nota. Elaboración propia a partir de los componentes utilizados en la implementación de la solución.

Análisis del Costo Total de Propiedad (TCO)

Si bien el costo por adquisición de licencias de software es equivalente a cero (USD 0.00), un análisis de viabilidad financiera riguroso para el sector corporativo exige la determinación del Costo Total de Propiedad (TCO - Total Cost of Ownership). El TCO integra no solo la inversión inicial de despliegue, sino también los costos operativos indirectos derivados del mantenimiento, administración técnica y soporte de la plataforma a mediano y largo plazo.

Para la estimación del costo operativo mensual se consideró una tarifa referencial promedio por hora de profesionales especializados en administración de sistemas y ciberseguridad dentro del contexto ecuatoriano. Estos valores tienen un carácter estimativo y fueron utilizados únicamente para realizar el análisis financiero del TCO de la solución propuesta.

Para que una organización mediana mantenga esta arquitectura SIEM en un estado óptimo, seguro y eficiente, se estima un esfuerzo operativo mensual recurrente desglosado en la siguiente matriz de ingeniería.

Tabla 37

Estimación del esfuerzo operativo mensual para el mantenimiento de la solución SIEM

Actividad Operativa / Mantenimiento Técnico	Horas / Mes	Perfil Técnico Requerido	Costo Estimado (USD)
Administración y *tuning* del clúster: gestión de índices en OpenSearch, optimización de *shards*, purga y archivado de registros (*logs*), y monitoreo de recursos del servidor (CPU, memoria RAM y almacenamiento).	10 hrs	Administrador de Sistemas / SysOps	$150,00
Mantenimiento y actualización de reglas: ajuste de reglas de correlación basadas en ATT&CK, reducción de falsos positivos y creación de nuevos casos de uso para la detección de amenazas.	16 hrs	Analista de Seguridad (SOC Tier 2)	$320,00
Gestión de agentes y *pipelines*: actualización, monitoreo y aplicación de parches de seguridad a los agentes (Osquery y Fluent Bit), además del ajuste de filtros en Fluentd y Data Prepper.	8 hrs	Ingeniero de Seguridad / NetOps	$140,00
Actualización del sistema operativo y del software: aplicación de parches de Ubuntu Server, actualización de imágenes Docker y remediación de vulnerabilidades detectadas.	6 hrs	Administrador de Sistemas / Ingeniero de Seguridad	$100,00
Total operativo mensual estimado	**40 hrs**	**Soporte interno dedicado**	**$710,00**

El análisis cuantitativo del TCO demuestra que la plataforma demanda aproximadamente 40 horas mensuales de atención técnica especializada. Esto evidencia que el software libre no elimina los costos, sino que desplaza la inversión desde el pago de licenciamiento comercial (que en soluciones privativas equivaldría a miles de dólares anuales según el volumen de datos o cantidad de *endpoints*) hacia el desarrollo y sostenimiento del capital humano interno.

Otro aspecto relevante identificado durante el desarrollo de la investigación corresponde a la capacidad de personalización ofrecida por la plataforma. La naturaleza open source de los componentes utilizados permite adaptar reglas de detección, dashboards, pipelines de procesamiento y mecanismos de correlación según las necesidades específicas de cada organización.

Asimismo, la solución no se limita a los dispositivos utilizados durante la validación. Debido al uso de protocolos y mecanismos estándar de integración, es posible incorporar nuevas fuentes de eventos provenientes de servidores, dispositivos de red, sistemas de seguridad, plataformas de virtualización, equipos industriales (OT) y otros activos tecnológicos compatibles con mecanismos de generación de registros y telemetría.

Considerando los resultados obtenidos, la ausencia de costos de licenciamiento comercial, el costo operativo estimado mediante el análisis del TCO, la flexibilidad de integración y los requerimientos de infraestructura observados durante la implementación, se concluye que la solución propuesta resulta altamente viable desde una perspectiva técnica y financiera para organizaciones medianas que buscan fortalecer sus capacidades de monitoreo y detección de eventos de seguridad mediante tecnologías open source, siempre que se asuma el compromiso de inversión en la capacitación continua de su personal técnico.

Además del costo operativo asociado al mantenimiento de la plataforma, una organización debe considerar el tiempo requerido para la planificación, implementación e integración inicial de la solución SIEM. Estas actividades representan el esfuerzo necesario para poner en funcionamiento la plataforma antes de iniciar su operación continua. La Tabla 38 presenta una estimación referencial del tiempo requerido para ejecutar las principales fases de implementación en una organización mediana.

Tabla 38

Cronograma referencial para la implementación de la solución SIEM

Actividad	Tiempo estimado
Levantamiento de requerimientos	1 semana
Diseño de arquitectura	1 semana
Implementación de la plataforma	1 semana
Integración de fuentes de eventos	1 semana
Configuración de reglas y dashboards	1 semana
Validación y ajustes operativos	1 semana

Nota. Los tiempos corresponden a una estimación referencial basada en la experiencia obtenida durante el desarrollo del proyecto.

Discusión de Resultados

Diseño y despliegue de SIEM con OpenSearch

Los resultados obtenidos durante la implementación y validación de la solución SIEM permitieron evidenciar que una arquitectura basada en OpenSearch puede proporcionar capacidades efectivas de centralización, procesamiento, correlación y visualización de eventos de seguridad dentro de un entorno corporativo de laboratorio. La detección exitosa de los escenarios ejecutados demostró la capacidad de la plataforma para identificar actividades relevantes de seguridad provenientes de diferentes fuentes de información.

Uno de los hallazgos más relevantes corresponde a la capacidad de integración alcanzada mediante el uso de tecnologías open source. La arquitectura implementada permitió consolidar eventos generados por dispositivos de red, sistemas operativos Windows y Linux, herramientas de monitoreo y mecanismos de detección de amenazas, proporcionando una visión centralizada de la información de seguridad. Este resultado coincide con los planteamientos identificados en la literatura revisada, donde los sistemas SIEM son descritos como plataformas orientadas a mejorar la visibilidad y el análisis de eventos dentro de las organizaciones.

La validación de técnicas asociadas al framework ATT&CK permitió verificar la capacidad de la solución para detectar actividades relacionadas con acceso no autorizado, descubrimiento de red, persistencia, manipulación de cuentas y modificación de controles de seguridad. La detección de las técnicas T1110 (Brute Force), T1046 (Network Service Discovery), T1136.002 (Create Domain Account), T1136.001 (Create Account: Local Account), T1098 (Account Manipulation) y T1562 (Impair Defenses) evidenció que las reglas implementadas fueron capaces de identificar comportamientos relevantes de seguridad mediante eventos reales generados durante las pruebas de validación.

Estos resultados demuestran que la cobertura ATT&CK validada no se limitó a eventos generados por una única fuente, sino que integró información proveniente de dispositivos Aruba,

Windows Server con Active Directory y FortiGate. De esta forma, la solución SIEM permitió relacionar eventos de autenticación, reconocimiento de red, creación de cuentas y cambios administrativos sobre dispositivos de seguridad dentro del entorno corporativo de laboratorio.

Desde una perspectiva operativa, los resultados obtenidos muestran que la plataforma permitió que los eventos generados durante los escenarios de validación estuvieran disponibles para su consulta en OpenSearch en intervalos adecuados para las actividades de monitoreo continuo. El tiempo medio de detección observado fue de 23,3 segundos, considerando los siete escenarios incluidos en la evaluación temporal, con valores individuales comprendidos entre 10 y 41 segundos.

El menor intervalo correspondió a la creación de una cuenta en Active Directory, con 10 segundos, mientras que el mayor se presentó durante el reconocimiento de red mediante Nmap, con 41 segundos. En los escenarios administrativos ejecutados sobre FortiGate, los tiempos observados estuvieron comprendidos entre 13 y 25 segundos.

La medición se realizó calculando la diferencia entre la marca temporal registrada durante la ejecución o inicio de cada escenario y la hora en que el registro estuvo disponible para su visualización en OpenSearch Discover. Por tanto, este resultado representa el tiempo operacional de generación, transmisión, procesamiento, normalización e indexación de los eventos dentro de la plataforma.

La hora de recepción de las notificaciones por correo electrónico fue registrada como evidencia complementaria para verificar el funcionamiento integral del mecanismo de alertamiento. Sin embargo, dicha marca temporal no fue incorporada en el cálculo del tiempo medio de detección, debido a que incluye latencias adicionales asociadas con la evaluación del monitor, la generación del mensaje, el procesamiento SMTP y la entrega de la notificación al destinatario.

No obstante, es importante considerar que las pruebas fueron realizadas dentro de un entorno controlado de laboratorio. Si bien los resultados obtenidos permiten validar el funcionamiento de la solución propuesta, escenarios de producción podrían incorporar un mayor volumen de eventos, fuentes de información adicionales y requerimientos operativos más complejos. En consecuencia, futuras implementaciones deberían contemplar pruebas de rendimiento, escalabilidad y disponibilidad en entornos con cargas superiores a las utilizadas durante esta investigación.

A pesar de estas limitaciones, los resultados obtenidos respaldan la utilización de OpenSearch como alternativa viable para la construcción de plataformas SIEM basadas en tecnologías open source, especialmente en organizaciones que requieren fortalecer sus capacidades de monitoreo de seguridad manteniendo un adecuado equilibrio entre funcionalidad, flexibilidad y costos de implementación.

Conclusiones y Recomendaciones

Conclusiones

La presente investigación permitió diseñar, implementar y validar una solución SIEM All-in-One basada en OpenSearch para la detección y correlación de eventos de seguridad dentro de un entorno corporativo de laboratorio. Los resultados obtenidos evidenciaron que la arquitectura propuesta fue capaz de centralizar información proveniente de múltiples fuentes de eventos, procesarla de forma eficiente y generar mecanismos de monitoreo orientados a la identificación de actividades relevantes de seguridad.

Respecto al primer objetivo específico, se logró identificar y analizar los requerimientos funcionales y de seguridad necesarios para la implementación de una plataforma SIEM,

definiendo los componentes, fuentes de información y mecanismos de integración requeridos para el entorno evaluado.

En relación con el diseño de la arquitectura, se implementó exitosamente una solución basada en OpenSearch, Data Prepper, Fluent Bit, Osquery y Security Analytics, permitiendo la recolección, procesamiento, almacenamiento y visualización centralizada de eventos de seguridad provenientes de diferentes dispositivos y sistemas.

Asimismo, se integraron múltiples fuentes de logs, incluyendo sistemas Windows, dispositivos de red Aruba, infraestructura FortiGate y equipos Linux, validando la capacidad de la plataforma para consolidar información heterogénea dentro de un único entorno de monitoreo.

La implementación de reglas de detección y mecanismos de correlación permitió identificar actividades asociadas a técnicas del framework ATT&CK, validándose específicamente las técnicas T1110 (Brute Force), T1046 (Network Service Discovery), T1136.002 (Create Domain Account), T1136.001 (Create Account: Local Account), T1098 (Account Manipulation) y T1562 (Impair Defenses). Estas técnicas fueron evidenciadas mediante escenarios controlados de fuerza bruta SSH, escaneo de red, creación de cuentas en Active Directory y cambios administrativos sobre el firewall FortiGate. Los resultados obtenidos demostraron que la plataforma fue capaz de generar hallazgos, alertas y notificaciones de forma consistente durante los escenarios ejecutados.

Los resultados de validación permitieron comprobar que los nueve escenarios ejecutados fueron identificados correctamente por la solución SIEM, alcanzando una tasa de detección del 100 % dentro del entorno corporativo de laboratorio. De estos escenarios, siete contaron con marcas temporales registradas con resolución de segundos, las cuales permitieron evaluar el

tiempo transcurrido entre la ejecución o inicio de la actividad y la disponibilidad del registro en OpenSearch Discover.

El tiempo medio de detección observado en OpenSearch fue de 23,3 segundos, con valores individuales comprendidos entre 10 y 41 segundos. El menor intervalo correspondió a la creación de una cuenta en Active Directory, mientras que el mayor se presentó durante el reconocimiento de red mediante Nmap. Estos resultados evidencian que la arquitectura implementada permitió recolectar, procesar, normalizar e indexar los eventos en intervalos inferiores a un minuto bajo las condiciones controladas del laboratorio.

La hora de recepción de las notificaciones por correo electrónico fue registrada como evidencia complementaria para validar el funcionamiento integral del mecanismo de alertamiento. Sin embargo, esta marca temporal no fue incluida en el cálculo del tiempo medio de detección, debido a que incorpora latencias adicionales asociadas con la evaluación del monitor, la generación del mensaje, el procesamiento SMTP y la entrega de la notificación.

La solución implementada demuestra viabilidad técnica para entornos académicos y organizaciones medianas que requieran capacidades básicas de monitoreo, detección y correlación de eventos de seguridad sin depender de licenciamiento comercial especializado. No obstante, su adopción en ambientes productivos requeriría considerar aspectos adicionales como alta disponibilidad, crecimiento del almacenamiento, endurecimiento de la plataforma, gestión de respaldos y pruebas de rendimiento bajo cargas superiores.

Recomendaciones

Se recomienda realizar futuras evaluaciones de rendimiento y escalabilidad de la plataforma en entornos con un mayor volumen de eventos y fuentes de información, con el fin de

analizar el comportamiento de OpenSearch frente a escenarios operativos más cercanos a ambientes productivos.

Se recomienda ampliar el conjunto de reglas de detección implementadas mediante la incorporación de nuevas técnicas y tácticas del framework ATT&CK, permitiendo incrementar la cobertura de amenazas y fortalecer las capacidades de monitoreo de la solución.

Se recomienda incorporar nuevas fuentes de eventos compatibles con mecanismos de integración estándar, tales como plataformas de virtualización, soluciones EDR, dispositivos de seguridad adicionales y sistemas industriales (OT), con el propósito de enriquecer los procesos de correlación y análisis de seguridad.

Para implementaciones en entornos productivos se recomienda evaluar arquitecturas con mecanismos de alta disponibilidad y redundancia, permitiendo mejorar la continuidad operativa y la resiliencia de la plataforma frente a fallos de infraestructura.

Se recomienda desarrollar estudios comparativos entre soluciones SIEM basadas en tecnologías open source y plataformas comerciales, considerando aspectos como costos de implementación, capacidades de detección, requerimientos de infraestructura y facilidad de administración, con el objetivo de apoyar procesos de toma de decisiones en organizaciones medianas.

Referencias

Bader, A.-S., Sadighian, A., & Oligeri, G. (2023). MITRE ATT&CK: State of the Art and Way Forward. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, *37*.

Canadian Centre for Cyber Security. (2025, marzo 31). *Using security information and event management tools to manage cyber security risks (ITSM.80.024) - Canadian Centre for Cyber Security*. https://www.cyber.gc.ca/en/guidance/using-security-information-event-management-tools-manage-cyber-security-risks-itsm80024

CrowdStrike. (2023). *The Complete Guide to Next-Gen SIEM*.

Elastic. (2024). *SIEM Buyer's Guide for the Modern SOC Key considerations when selecting your SIEM solution*.

Falasi, Dr. M. A.-, & Zhang, Dr. T. (2025). AUGMENTING SIEM WITH THREAT INTELLIGENCE FOR PREDICTIVE CYBER DEFENSE: A PROACTIVE THREAT HUNTING APPROACH. *International Journal of Cyber Threat Intelligence and Secure Networking*, *2*(03), 1-5. https://doi.org/10.55640/IJCTISN-V02I03-01

Farouk, M., Rob, A. El, & Islam, M. A. (2024). *Issues in Information Systems The application of MITRE ATT&CK framework in mitigating cybersecurity threats in the public sector*. *25*(3), 62-80. https://doi.org/10.48009/3_iis_2024_106

Fluent Bit Project. (2025). *What's Fluent Bit? | Fluent Bit: Official Manual*. https://docs.fluentbit.io/manual/about/what-is-fluent-bit

Fluentd Project. (2025). *What is Fluentd? | Fluentd*. https://www.fluentd.org/architecture/

Gerhards, R. (2009). *RFC 5424 - The Syslog Protocol*. https://datatracker.ietf.org/doc/html/rfc5424

Gerhards, R., & Gerhards, R. (2009). *The Syslog Protocol*. https://doi.org/10.17487/RFC5424

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). *Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures Security Information and Event*. https://doi.org/10.3390/s21144759

Haas, S., Sommer, R., & Fischer, M. (2020). *zeek-osquery: Host-Network Correlation for Advanced Monitoring and Intrusion Detection*. https://github.com/zeek/zeek-osquery

Hase, L. F. W. W. G. (2024). *The Path to Choosing a SIEM System-A Systematic Literature Review*.

Instaclustr. (2022). *Opensearch for SIEM: The Basics and a Quick Tutorial*. https://www.instaclustr.com/education/opensearch/opensearch-for-siem-the-basics-and-a-quick-tutorial/

Kent, K., & Souppaya, M. (2006). *Guide to Computer Security Log Management*. https://doi.org/10.6028/NIST.SP.800-92

Lella, I. (2024). *ENISA THREAT LANDSCAPE 2024*. https://doi.org/10.2824/0710888

López Velásquez, J. M., Martínez Monterrubio, S. M., Sánchez Crespo, L. E., & Garcia Rosado, D. (2023). Systematic review of SIEM technology: SIEM-SC birth. *International Journal of Information Security 2022 22:3*, *22*(3), 691-711. https://doi.org/10.1007/S10207-022-00657-9

Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLOS ONE*, *19*(3), e0301183. https://doi.org/10.1371/JOURNAL.PONE.0301183

MGBEMELE, A. F. (2026). Advancing Cyber Threat Detection through SIEM-Based Automation and MITRE ATT&CK Aligned Analytics: A Systematic Review. *Asian Journal of Research in Computer Science*, *19*(1), 233-254. https://doi.org/10.9734/AJRCOS/2026/V19I1816

Microsoft. (2025). *What is Microsoft Sentinel SIEM? | Microsoft Learn*. https://learn.microsoft.com/en-us/azure/sentinel/overview?tabs=defender-portal

MITRE ATT&CK. (2026). *MITRE ATT&CK*. https://attack.mitre.org/

Nurusheva, A., Abdiraman, A., Satybaldina, D., Goranin, N., & Gumilyov, L. N. (2024). Machine learning algorithms in SIEM systems for enhanced detection and management of security events. *Bulletin of L.N. Gumilyov Eurasian National University. Mathematics, computer science, mechanics series*, *148*(3), 6-17. https://doi.org/10.32523/BULMATHENU.2024/3.1

OpenSearch Project. (2026). *About Security Analytics - OpenSearch Documentation*. https://docs.opensearch.org/latest/security-analytics/

Osquery Project. (2025). *Welcome to osquery - osquery*. https://osquery.readthedocs.io/en/stable/

Proxmox Server Solutions. (2026). *Proxmox Virtual Environment - Open-Source Server Virtualization Platform*. https://www.proxmox.com/en/products/proxmox-virtual-environment/overview

Rosenberg, M., Schneider, B., Scherb, C., & Asprion, P. M. (2023). *AN ADAPTABLE APPROACH FOR SUCCESSFUL SIEM ADOPTION IN COMPANIES*.

Sheeraz, M., Durad, M. H., Paracha, M. A., Mohsin, S. M., Kazmi, S. N., & Maple, C. (2024). Revolutionizing SIEM Security: An Innovative Correlation Engine Design for

Multi-Layered Attack Detection. *Sensors (Basel, Switzerland)*, *24*(15), 4901. https://doi.org/10.3390/S24154901

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). *MITRE ATT&CKÒ: Design and Philosophy*. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

Vaarandi, R., & Bah¸sibah¸si, H. (2024). *Using Large Language Models for Template Detection from Security Event Logs*. https://doi.org/10.1007/s10207-025-01018-y

Van Pelt, A. (2021). *MITRE ATT&CK Framework as a Standard for Developing SIEM Use Cases | by Iman Akbari | Medium*. https://medium.com/@imanvanpersien/mitre-att-ck-framework-as-a-standard-for-developing-siem-use-cases-d7dc7db4e1ba

Verizon. (2026). *2026 Verizon DBIR: Breakthroughs in vulnerabilities, AI-assisted cyber attacks and social engineering*. https://www.verizon.com/business/resources/T27e/reports/2026-dbir-data-breach-investigations-report.pdf

Zhang, Y. , C. X. , & L. Z. (2023). *View of Unveiling Anomalies: Leveraging Machine Learning for Internal User Behaviour Analysis – Top 10 Use Cases*. https://journals.tultech.eu/index.php/ijitis/article/view/254/244

Zhu, J., He, S., Liu, J., He, P., Xie, Q., Zheng, Z., & Lyu, M. R. (2018). *Tools and Benchmarks for Automated Log Parsing*. https://github.com/logpai/logparser

Diseño y despliegue de SIEM con OpenSearch

ANEXOS

MANUAL DE ATAQUE

MANUAL DE VALIDACIÓN CONTROLADA DEL SIEM OPENSEARCH.pdf

MANUAL DE ACCESO AL LABORATORIO

MANUAL DE ACCESO AXIS - INGRESO A LABORATORIO.pdf