Solución SIEM + SOAR Basado en Software Libre

Luis Alfredo Arias Patiño

Asesor

Paulita Flor Salazar

Universidad Nacional Abierta y a Distancia

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Ingeniería de Telecomunicaciones

2026

Nota de Aceptación

_____

Nombre director de Trabajo de Grado

_____ _____

Jurado Jurado

2026

Agradecimientos

Quiero expresar un agradecimiento muy especial a Antonio Calderón, mi mentor y amigo, quien ha sido una guía fundamental; su confianza, apoyo constante y enseñanzas han contribuido de manera significativa a mi crecimiento profesional y personal. Gracias a su liderazgo, ejemplo y acompañamiento he podido fortalecer mis conocimientos, afrontar nuevos retos y consolidar mi vocación en el ámbito de la ciberseguridad.

Dedicatoria

Dedico este proyecto a mis padres, quienes con su esfuerzo, valores y apoyo incondicional han sido el pilar fundamental de mi vida. Gracias a su guía y confianza soy la persona que soy hoy, y este logro también es resultado de su amor y acompañamiento constante.

Resumen

La creciente dependencia de las tecnologías de la información ha incrementado los riesgos asociados a la ciberseguridad, especialmente en pequeñas y medianas empresas que cuentan con recursos limitados y niveles básicos de madurez en la gestión de la seguridad. En este contexto, el presente proyecto de investigación aplicada de ingeniería propone el diseño e implementación de una solución SIEM + SOAR basada en software libre, orientada a mejorar la detección y respuesta ante incidentes de seguridad.

El proyecto se desarrolla en una empresa real del sector eléctrico con más de doce años de experiencia en la protección de infraestructuras electrónicas contra rayos y sobretensiones, la cual dispone de una infraestructura tecnológica compuesta por aproximadamente diez hosts con sistemas operativos Windows. Los principales riesgos identificados corresponden a accesos no autorizados y amenazas de malware. Por razones de confidencialidad, el nombre de la organización no es divulgado.

La metodología empleada es de tipo aplicada y experimental, estructurada en fases de diagnóstico, diseño, implementación y verificación funcional. Para la solución SIEM se utiliza la plataforma Wazuh, mientras que la automatización de la respuesta se realiza mediante la plataforma SOAR Shuffle. La implementación permite centralizar la gestión de eventos de seguridad y automatizar acciones de respuesta ante incidentes relevantes.

Como resultado, se obtiene un prototipo funcional que demuestra la viabilidad del uso de herramientas de código abierto para fortalecer la ciberseguridad en entornos empresariales reales, ofreciendo una alternativa accesible y replicable para organizaciones con características similares.

Palabras clave: Ciberseguridad, SIEM, SOAR, software libre, PYMEs.

Abstract

The increasing dependence on information technologies has significantly raised cybersecurity risks, particularly for small and medium-sized enterprises with limited resources and low security maturity levels. In this context, this applied engineering research project proposes the design and implementation of an open-source SIEM + SOAR solution aimed at improving incident detection and response.

The project is developed in a real company from the electrical sector with more than twelve years of experience in protecting electronic infrastructures against lightning and power surges. The company operates approximately ten Windows-based hosts, and its main security concerns are unauthorized access and malware threats. Due to confidentiality and security reasons, the company's name is not disclosed.

The methodology follows an applied and experimental approach, structured into diagnostic, design, implementation, and functional verification phases. Wazuh is used as the SIEM platform for event collection and correlation, while Shuffle is employed as the SOAR platform for response automation. The implemented solution enables centralized security event management and automated responses to relevant incidents.

As a result, a functional prototype is obtained, demonstrating the feasibility of using open-source technologies to strengthen cybersecurity in real business environments, providing an accessible and replicable alternative for organizations with similar characteristics.

Keywords: Cybersecurity, SIEM, SOAR, open-source software, SMEs.

Tabla de Contenidos

Introducción 12

Planteamiento del problema 14

Justificación 17

Objetivos 19

Objetivo general 19

Objetivos específicos 19

Marco conceptual y teórico 20

Marco conceptual 20

Marco teórico 23

Metodología 26

Fase 1: Diagnóstico del entorno 28

Caracterización de la empresa 28

Análisis del entorno 28

Fase 2: Diseño de la solución 31

Especificaciones técnicas 31

Selección y justificación de tecnologías 31

Recursos necesarios 34

Arquitectura y Componentes de la Solución Wazuh (SIEM) 35

Arquitectura y Componentes de la Solución Shuffle (SOAR) 37

Diagrama de Bloques 40

Fase 3: Implementación del Prototipo 41

Implementación de la infraestructura virtual para el SIEM 41

Instalación y configuración del sistema SIEM (Wazuh) 42
Implementación de la infraestructura virtual para el SOAR 44
Instalación y configuración del sistema SOAR (Shuffle) 45
Configuraciones específicas alineadas al CORE del negocio 46
Monitoreo de integridad de archivos (FIM) sobre activos críticos del negocio. 46
Reglas personalizadas para detección de accesos a información sensible. 46
Flujo SOAR específico para protección de cuentas técnicas y comerciales. 47
Política de retención de logs alineada al ciclo de vida de los proyectos. 47
Listas blancas para aliados estratégicos. 48
Integración entre SIEM y SOAR 48
Enlace del video en YouTube con la explicación detallada del funcionamiento de la solución implementada 51
Explicación detallada del funcionamiento de la solución implementada 52
Configuración de flujo de respuesta automatizada. 56
Enlace del video en YouTube de la sustentación del caso de uso. 58
Fase 4: Verificación funcional y resultados obtenidos. 59
Métricas de desempeño obtenidas durante el periodo de prueba 61
Procesos manuales eliminados o reducidos 67
Políticas de seguridad formalizadas 67
Recomendaciones 70
Plan de mantenimiento 70
Plan de aseguramiento de la solución SIEM + SOAR 70
Plan de mantenimiento correctivo 73

Plan de mantenimiento predictivo 75

Plan de mantenimiento preventivo 77

Conclusiones 79

Referencias Bibliográficas 82

Lista de tablas

Tabla 1. *Comparación de Soluciones para la implementación del SIEM*……...….....32

Tabla 2. *Comparación de Soluciones para la implementación del SOAR*….……...33

Tabla 3. *Recursos*……...……...34

Tabla 4. *Comparación del estado de seguridad antes y después de la implementación*…..……60

Tabla 5. *Tabla de verificación funcional del prototipo SIEM + SOAR*……...…….68

Lista de Figuras

Figura 1. *Plano Arquitectura y Componentes de Wazuh (SIEM).* ……...36

Figura 2. *Plano Arquitectura de Shuffle (SOAR)*……..39

Figura 3. *Diagrama de Flujo SIEM + SOAR*……..…….40

Figura 4. *Configuración Máquina Virtual Wazuh (SIEM)*……...……42

Figura 5. *Puesta en funcionamiento de Wazuh (SIEM)*……43

Figura 6. *Instalación Agente Wazuh*……...……..43

Figura 7. *Configuración Máquina Virtual Wazuh (SIEM)*……...……44

Figura 8. *Puesta en marcha de Shuffle (SOAR)*……45

Figura 9. *Creación de Webhook URI en el SOAR para integración con el SIEM*……49

Figura 10. *Configuración Webhook URI en SIEM para integración con el SOAR*……..49

Figura 11. *Procesamiento de alertas*……..……..50

Figura 12. *Prueba de correcta integración y procesamiento de alertas desde el SIEM en el SOAR*…….51

Figura 13. *Evidencia operativa, máquina virtual de Shuffle (SOAR)*……...53

Figura 14. *Evidencia operativa, máquina virtual de Wazuh (SIEM)*……...…….53

Figura 15. *Agentes monitorizados*……...…….55

Figura 16. *Configuración de respuesta automatizada para evento de dumping de credenciales del Windows SAM*……..58

Figura 17. *Eventos de autenticación*……...……..62

Figura 18. *Detecciones de vulnerabilidades*……...……..63

Figura 19. *Eventos de monitoreo de cumplimiento y hardening*……...…...64

Figura 20. *Eventos de integridad y cambios en el sistema*……...……65

Figura 21. *MITRE ATT&CK*……66

Introducción

En un contexto donde la transformación digital avanza de manera acelerada, las organizaciones dependen cada vez más de infraestructuras tecnológicas para el desarrollo de sus procesos operativos y administrativos. Esta realidad ha incrementado la superficie de exposición a amenazas cibernéticas, especialmente en pequeñas y medianas empresas (PYMEs), las cuales suelen presentar limitaciones en recursos técnicos y financieros para la gestión adecuada de la seguridad de la información. La importancia de este proyecto radica en su potencial para transformar la manera en que las PYMEs abordan la ciberseguridad, mediante la adopción de soluciones accesibles, eficientes y alineadas con sus necesidades reales.

Ante esta problemática, el presente proyecto de investigación aplicada de ingeniería propone el diseño e implementación de una solución SIEM + SOAR basada en software libre, integrando las plataformas Wazuh y Shuffle, como una alternativa viable frente a soluciones comerciales de alto costo. El prototipo será implementado en una empresa real del sector eléctrico, con más de doce años de experiencia en la protección de infraestructuras electrónicas. Por razones de confidencialidad y seguridad de la información, el nombre de la organización no será divulgado a lo largo del documento, y se hará referencia a ella como *empresa del sector eléctrico*.

El desarrollo del proyecto contempla el análisis del entorno tecnológico, el diseño de la arquitectura de la solución y su implementación funcional, con el fin de mejorar la gestión de eventos de seguridad y automatizar la respuesta ante incidentes. De esta manera, el proyecto busca aportar una solución práctica y replicable que contribuya al

fortalecimiento de la ciberseguridad en PYME del sector eléctrico y en organizaciones con características similares.

Planteamiento del problema

En un mundo cada vez más digital, la seguridad de la información se ha convertido en un tema crítico para las organizaciones, especialmente para las pequeñas y medianas empresas (PYMEs), que enfrentan mayores desafíos en su protección debido a la falta de recursos. El problema central radica en la inaccesibilidad de las PYMEs a soluciones avanzadas de ciberseguridad, como las plataformas SIEM (Security Information and Event Management) y SOAR (Security Orchestration, Automation and Response), debido a su elevado costo y la complejidad técnica de su implementación. Esta situación deja a las PYMEs expuestas a ataques cibernéticos que pueden comprometer su operación y sostenibilidad.

Las PYMEs, que constituyen el 90% de las empresas a nivel mundial, generan entre el 50% y el 70% del empleo global. Sin embargo, son uno de los principales blancos de ataques cibernéticos. Según el informe de ciberseguridad de Verizon (2023), más del 40% de estos ataques están dirigidos a PYMEs, que a menudo carecen de una infraestructura de seguridad sólida. Muchas de estas organizaciones no cuentan con equipos especializados en ciberseguridad, lo que agrava su vulnerabilidad ante amenazas como el phishing, ransomware y ataques de denegación de servicio (DDoS), entre otros.

El problema ocurre a diario, ya que las PYMEs manejan información crítica de clientes, proveedores y operaciones internas, lo que las convierte en objetivos frecuentes de los ciberdelincuentes. En Latinoamérica, el problema es particularmente grave. La Organización de los Estados Americanos (OEA) señala que solo el 30% de las PYMEs de

la región implementan soluciones avanzadas de seguridad, lo que las deja expuestas a ciberataques que podrían devastar su negocio.

Este problema surge por la combinación de varias causas. La principal es la falta de recursos financieros para adquirir soluciones comerciales de SIEM y SOAR, que suelen ser costosas y complejas de implementar. A esto se suma la falta de personal capacitado para gestionar estas plataformas, ya que muchas PYMEs no pueden permitirse un equipo especializado en seguridad informática. Además, existe una falta de conciencia sobre los riesgos reales que suponen los ciberataques, lo que lleva a que muchas de estas organizaciones subestimen la importancia de la ciberseguridad hasta que sufren un incidente. Como resultado, muchas empresas no toman medidas preventivas adecuadas, lo que las deja en una posición de vulnerabilidad.

Los efectos de este problema son devastadores para las PYMEs. Un ataque cibernético puede generar la interrupción de operaciones, robo de datos y pérdidas económicas significativas. En los peores casos, las empresas pueden verse forzadas a cerrar debido al impacto financiero de un ataque exitoso. Además, la incapacidad para responder rápidamente a incidentes de seguridad afecta la confianza de los clientes y la reputación de la empresa en el mercado, disminuyendo su competitividad.

Este proyecto busca solucionar este problema mediante el diseño e implementación de un prototipo de solución SIEM + SOAR basado en software libre, adaptado a las necesidades de un entorno empresarial real aplicado a una empresa del sector eléctrico. La propuesta es ofrecer una herramienta accesible, personalizable y eficiente que permita a esta empresa detectar, monitorear y responder a incidentes de

seguridad de manera automatizada. Al basarse en tecnologías de código abierto, la solución no solo será más económica, sino que también podrá ser adaptada a las necesidades específicas de la empresa, sin necesidad de contar con un equipo técnico altamente especializado.

La implementación de una solución de este tipo podría reducir significativamente los riesgos a los que se enfrenta la empresa del sector eléctrico, mejorando su capacidad para protegerse contra ciberataques y salvaguardar la información crítica que manejan. A su vez, la adopción de tecnologías de software libre permitirá a la organización a mantener los costos bajos, promoviendo una mayor adopción de medidas de ciberseguridad y cerrando la brecha entre grandes empresas y PYMEs.

Justificación

La realización de este proyecto de investigación aplicada de ingeniería se justifica por la necesidad de fortalecer la gestión de la seguridad de la información en empresas del sector eléctrico que, a pesar de operar infraestructuras críticas, cuentan con niveles básicos de madurez en ciberseguridad y recursos limitados para acceder a soluciones comerciales de alto costo.

Desde el punto de vista disciplinar, el proyecto es pertinente para el campo de la ingeniería de telecomunicaciones y/o electrónica, ya que integra conceptos de redes, seguridad informática, gestión de eventos, automatización y análisis de datos, aplicados a un entorno empresarial real. La implementación de una solución SIEM + SOAR permite materializar conocimientos teóricos en una solución técnica funcional, alineada con las tendencias actuales en ciberseguridad.

En el ámbito social y organizacional, la solución propuesta beneficia directamente a la empresa del sector eléctrico al mejorar su capacidad de detección y respuesta ante accesos no autorizados y malware, reduciendo riesgos operativos y fortaleciendo la continuidad del negocio. Adicionalmente, el uso de software libre promueve la democratización del acceso a tecnologías avanzadas de seguridad, especialmente para pequeñas y medianas empresas.

Desde una perspectiva académica y personal, el proyecto permite desarrollar competencias técnicas, analíticas y de diseño de soluciones reales, consolidando habilidades clave para el ejercicio profesional. Asimismo, el proyecto aporta un modelo

replicable que puede ser adaptado por otras organizaciones con características similares, aumentando su impacto y relevancia.

Objetivos

Objetivo general

Desarrollar un prototipo de solución SIEM + SOAR basado en software libre para automatizar la detección y respuesta a incidentes de ciberseguridad, con el fin de mejorar la protección de empresa del sector eléctrico que cuenta con un entorno de recursos limitados.

Objetivos específicos

Analizar el entorno tecnológico y el nivel de madurez en ciberseguridad de una empresa del sector eléctrico, con el fin de identificar vulnerabilidades, eventos críticos y requerimientos para la implementación de una solución SIEM + SOAR.

Diseñar e implementar la arquitectura de una solución SIEM + SOAR basada en software libre, utilizando Wazuh y Shuffle, para centralizar la gestión de eventos de seguridad y automatizar la respuesta ante accesos no autorizados y amenazas de malware en un entorno empresarial real.

Integrar y verificar el funcionamiento del prototipo SIEM + SOAR implementado, con el propósito de validar su operatividad, estabilidad y capacidad de respuesta frente a incidentes de seguridad en la infraestructura de la empresa.

Marco conceptual y teórico

Marco conceptual

Ciberseguridad

La ciberseguridad es la práctica de proteger sistemas informáticos, redes, aplicaciones y datos ante agresiones digitales o accesos no autorizados, utilizando una combinación de procesos, tecnologías, políticas y comportamientos para salvaguardar la confidencialidad, integridad y disponibilidad de la información frente a amenazas y ataques maliciosos. (Fortinet, 2026)

SIEM (Gestión de Información y Eventos de Seguridad)

El SIEM, por sus siglas en inglés *Security Information and Event Management*, consiste en un conjunto de tecnologías que recopilan, correlacionan y analizan datos de eventos y registros de múltiples fuentes dentro de una infraestructura de TI para identificar actividades sospechosas, generar alertas y proporcionar una visión centralizada del estado de seguridad de una organización. (IONOS, 2025)

SOAR (Orquestación, Automatización y Respuesta de Seguridad)

El SOAR (*Security Orchestration, Automation and Response*) se refiere a un conjunto de soluciones y herramientas que permiten automatizar, orquestar y coordinar procesos y respuestas ante incidentes de seguridad. Permite integrar diversas tecnologías de seguridad (como SIEM, EDR y escáneres de vulnerabilidades) y ejecutar acciones definidas automáticamente tras la detección de amenazas, reduciendo tiempos de respuesta y la carga operativa manual. (Red Hat, 2022)

Software Libre

El *software libre* se refiere a programas informáticos que se consideran "libres" cuando no imponen restricciones legales que limiten el estudio, la redistribución o la modificación del código fuente. Según *Britannica*, la libertad principal detrás del software libre es que las personas usuarias puedan controlar completamente el software que emplean, independientemente de si éste se ofrece sin costo o con algún precio. Para que un programa sea considerado libre, debe permitir legalmente a las personas estudiar, modificar y redistribuir tanto el software original como sus versiones modificadas, sin restricciones que limiten estas acciones. Este concepto está estrechamente vinculado al movimiento del software libre, fundado por Richard Stallman en la década de 1980, y se diferencia de otras formas de software gratuito en que pone el énfasis en la libertad de uso y modificación, más que en el precio. (Volle, 2026)

Orquestación y Automatización de Seguridad

La orquestación y automatización de seguridad es un enfoque que permite coordinar múltiples herramientas y procesos de seguridad para que trabajen de forma integrada y automática ante eventos de seguridad, reduciendo la intervención manual y acelerando la respuesta ante incidentes. Este concepto es fundamental para entender cómo las plataformas SOAR interactúan con otras soluciones dentro de un Centro de Operaciones de Seguridad (SOC). (CyberSafety, 2025)

Pequeñas y medianas empresas (PYMEs)

Una pequeña y mediana empresa (PYME) es una organización que se clasifica por su tamaño en función de criterios como el número de empleados y el volumen de

facturación, siendo entidades con menos de 250 trabajadores y con un nivel de operación y recursos menor al de las grandes corporaciones. Las PYMEs constituyen la mayoría del tejido empresarial global, representando hasta el 99 % de las empresas en muchos países y contribuyendo significativamente a la generación de empleo y al crecimiento económico. Además, este tipo de organizaciones se caracteriza por su flexibilidad, adaptabilidad y cercanía al cliente, lo cual les permite responder con agilidad a cambios del mercado, aunque también enfrentan limitaciones en acceso a recursos, financiamiento y capacidades tecnológicas. (Económica, 2024)

Marco teórico

La ciberseguridad se ha convertido en un elemento crítico para la continuidad operativa de las organizaciones, especialmente en un contexto donde la digitalización de procesos y la interconexión de sistemas incrementan la superficie de ataque. Las pequeñas y medianas empresas (PYMEs), a pesar de ser un motor clave de la economía, suelen presentar mayores brechas de seguridad debido a limitaciones presupuestales, técnicas y de personal especializado, lo que las convierte en un objetivo atractivo para los atacantes cibernéticos.

En este escenario, la ciberseguridad se define como el conjunto de estrategias, tecnologías y prácticas orientadas a proteger los sistemas de información, redes y datos frente a accesos no autorizados, ataques maliciosos o daños, garantizando la confidencialidad, integridad y disponibilidad de la información (Fortinet, 2026). La implementación de controles adecuados permite reducir el impacto de amenazas como malware, accesos indebidos, ransomware y explotación de vulnerabilidades, las cuales afectan de manera significativa a organizaciones con niveles básicos de madurez en seguridad.

Una de las tecnologías más relevantes para la gestión centralizada de la seguridad es el SIEM (Security Information and Event Management). Este tipo de solución permite recopilar, correlacionar y analizar eventos de seguridad provenientes de múltiples fuentes, como sistemas operativos, aplicaciones, dispositivos de red y soluciones de seguridad, con el fin de detectar comportamientos anómalos o incidentes de manera oportuna (IONOS,

2025). El uso de SIEM facilita la visibilidad del estado de seguridad de la infraestructura tecnológica, permitiendo una respuesta más informada y basada en evidencias.

No obstante, aunque los sistemas SIEM proporcionan capacidades avanzadas de monitoreo y detección, su efectividad puede verse limitada cuando los procesos de respuesta ante incidentes dependen exclusivamente de acciones manuales. En respuesta a esta necesidad surgen las plataformas SOAR (Security Orchestration, Automation and Response), las cuales permiten automatizar y orquestar flujos de respuesta ante incidentes de seguridad, integrando diferentes herramientas y tecnologías dentro de un mismo ecosistema (Red Hat, 2022). El enfoque SOAR reduce los tiempos de reacción, minimiza errores humanos y optimiza el uso de recursos, aspectos clave para entornos con capacidades operativas reducidas, como es el caso de muchas PYMEs.

La combinación de soluciones SIEM + SOAR representa una evolución en la gestión de la ciberseguridad, al permitir no solo la detección de incidentes, sino también la ejecución automatizada de acciones de contención y mitigación. Esta integración resulta especialmente beneficiosa en escenarios empresariales donde la seguridad se gestiona de forma reactiva o con herramientas aisladas, ya que promueve una estrategia más proactiva y estructurada frente a las amenazas.

En este contexto, el software libre adquiere un papel fundamental. El software libre se caracteriza por ofrecer a los usuarios la libertad de ejecutar, estudiar, modificar y redistribuir el código fuente, lo que favorece la transparencia, la adaptabilidad y la reducción de costos de licenciamiento (Volle, 2026). Para las PYMEs, el uso de soluciones de seguridad basadas en software libre, como Wazuh para SIEM y Shuffle para SOAR,

permite implementar arquitecturas robustas sin incurrir en elevados costos, además de facilitar la personalización de la solución según las necesidades específicas del entorno empresarial.

Finalmente, la adopción de plataformas SIEM y SOAR basadas en software libre contribuye al fortalecimiento de la postura de seguridad de las PYMEs, permitiendo avanzar hacia modelos más maduros de gestión de incidentes. La integración de monitoreo, correlación de eventos y automatización de respuestas se presenta como una alternativa viable y estratégica para mejorar la protección de los activos digitales, optimizar los procesos de seguridad y garantizar la continuidad operativa en entornos empresariales reales.

Metodología

El presente proyecto de investigación aplicada de ingeniería adopta un enfoque mixto, con énfasis en el componente aplicado y técnico, orientado al diseño e implementación de una solución SIEM + SOAR basada en software libre en un entorno empresarial real.

La solución será implementada en una empresa perteneciente al sector eléctrico, con más de doce años de experiencia en el diseño, comercialización y soporte de sistemas de protección contra rayos y sobretensiones, dedicada a la protección de infraestructuras electrónicas críticas.

Diseño del estudio:

El diseño del estudio es de tipo experimental-aplicado, ya que se desarrolla e implementa un prototipo funcional dentro de la infraestructura tecnológica de la empresa, permitiendo validar su operatividad en condiciones reales.

La metodología se estructura en tres fases:

Fase 1: Diagnóstico y análisis del entorno

En esta fase se realiza la caracterización de la empresa y de su estado actual en materia de ciberseguridad, identificando activos críticos, fuentes de eventos de seguridad, vulnerabilidades y prácticas existentes de monitoreo y respuesta a incidentes. Este análisis permite definir los requerimientos técnicos y funcionales del sistema SIEM + SOAR acorde al contexto operativo de la organización.

Fase 2 y 3: Diseño e implementación de la solución

Con base en el diagnóstico, se diseña la arquitectura del sistema SIEM + SOAR utilizando Wazuh como plataforma SIEM para la recolección, correlación y análisis de eventos de seguridad, y Shuffle como plataforma SOAR para la automatización de respuestas ante incidentes. En esta etapa se realiza la instalación, configuración e integración de los componentes, así como la definición de reglas, flujos de trabajo y mecanismos de comunicación entre ambas soluciones.

Fase 4: Verificación funcional y resultados obtenidos

Finalmente, se verifica el correcto funcionamiento e integración de la solución implementada, comprobando la capacidad del sistema para detectar eventos de seguridad y ejecutar respuestas automatizadas. Los resultados obtenidos se documentan mediante registros técnicos y análisis del comportamiento del sistema en el entorno empresarial.

Tipo de análisis

El análisis se centra principalmente en la operatividad, integración y estabilidad del sistema implementado, priorizando la correcta ejecución de los procesos de detección y automatización de incidentes sobre la evaluación estadística avanzada. De esta manera, se valida la pertinencia de la solución como una alternativa viable y de bajo costo para la gestión de la seguridad en pequeñas empresas.

Fase 1: Diagnóstico del entorno

Caracterización de la empresa

La solución propuesta será implementada en una empresa del sector eléctrico, con más de doce años de experiencia en el diseño, comercialización y soporte de sistemas de protección contra rayos y transientes, orientados a la protección de infraestructuras electrónicas frente a los efectos de sobretensiones eléctricas. La organización presta servicios especializados para la protección de activos tecnológicos críticos, lo que convierte la seguridad de la información en un componente clave para la continuidad de sus operaciones.

La infraestructura tecnológica de la empresa está compuesta aproximadamente por diez hosts con sistemas operativos Windows, destinados a funciones administrativas, técnicas y de soporte. Estos equipos constituyen activos fundamentales para el desarrollo de las operaciones diarias y representan el entorno sobre el cual se implementará la solución propuesta.

Debido a la naturaleza crítica de los servicios prestados y a consideraciones de confidencialidad y seguridad de la información, el nombre de la organización no será divulgado en el presente proyecto, haciendo referencia a ella únicamente como una empresa del sector eléctrico.

Análisis del entorno

El análisis del entorno se realizó mediante un proceso de diagnóstico técnico orientado a identificar el estado actual de la infraestructura tecnológica y las capacidades de ciberseguridad de la organización. Para ello, se llevaron a cabo actividades de

levantamiento de información, revisión de la infraestructura tecnológica existente y validación de los controles de seguridad implementados en los equipos de trabajo.

Durante esta fase se efectuó un inventario básico de los activos tecnológicos, identificando aproximadamente diez hosts con sistemas operativos Windows destinados a funciones administrativas, técnicas y de soporte. Asimismo, se realizaron entrevistas y consultas con el personal responsable de la infraestructura tecnológica, con el fin de conocer los procedimientos actuales de gestión de incidentes, monitoreo y administración de la seguridad.

Como resultado del diagnóstico, se evidenció que la organización no contaba con una solución SIEM para la centralización y correlación de eventos de seguridad, ni con una plataforma SOAR que permitiera automatizar procesos de respuesta ante incidentes. De igual forma, se identificó la ausencia de controles de seguridad perimetral avanzados, tales como sistemas de detección y prevención de intrusiones (IDS/IPS) o firewalls de nueva generación.

En los equipos finales se constató que la protección se limitaba al uso de Windows Defender con su configuración predeterminada, sin herramientas especializadas para la detección avanzada de amenazas, monitoreo de integridad, correlación de eventos o gestión centralizada de alertas. Adicionalmente, se identificó que la organización no disponía de un sistema centralizado para la gestión de actualizaciones y parches de seguridad, lo que incrementa el riesgo de explotación de vulnerabilidades conocidas.

El diagnóstico también permitió determinar que la gestión de la seguridad se desarrollaba de forma reactiva y mediante procesos manuales, sin mecanismos que

proporcionaran visibilidad centralizada de los eventos generados por los activos tecnológicos. Esta situación dificultaba la detección temprana de actividades sospechosas, especialmente aquellas relacionadas con accesos no autorizados y amenazas de malware, identificadas como los principales riesgos para la organización.

Los resultados obtenidos permitieron establecer una línea base del estado de madurez en ciberseguridad de la empresa y definir los requerimientos funcionales necesarios para el diseño de la solución propuesta. Entre las principales necesidades identificadas se encuentran la centralización de eventos de seguridad, la correlación de alertas, el monitoreo continuo de los activos tecnológicos y la automatización de respuestas ante incidentes. Con base en estos hallazgos, se procedió al diseño e implementación de una solución SIEM + SOAR basada en software libre, alineada con las características y necesidades del entorno empresarial analizado.

Fase 2: Diseño de la solución

Especificaciones técnicas

Selección y justificación de tecnologías

La selección de las herramientas que conforman la solución SIEM + SOAR se realizó considerando las características del entorno empresarial analizado, el nivel de madurez en ciberseguridad identificado durante la fase de diagnóstico y las restricciones presupuestales de la empresa. Como resultado de este análisis, se seleccionaron las plataformas Wazuh y Shuffle debido a que ofrecen capacidades avanzadas de monitoreo, correlación de eventos, automatización y respuesta ante incidentes, bajo un modelo de software libre que elimina los costos asociados al licenciamiento de soluciones comerciales.

La elección de estas herramientas también estuvo fundamentada en su facilidad de integración, amplia documentación, soporte comunitario y compatibilidad con estándares y marcos de referencia ampliamente utilizados en ciberseguridad, como MITRE ATT&CK. Adicionalmente, ambas plataformas permiten escalar la solución conforme evolucionen las necesidades de seguridad de la organización.

Antes de seleccionar la plataforma SIEM para la solución propuesta, se analizaron diferentes alternativas disponibles en el mercado, considerando aspectos como costos de licenciamiento, capacidades de monitoreo, gestión de vulnerabilidades, integración con marcos de referencia en ciberseguridad y adecuación para entornos empresariales con

recursos limitados. Entre las soluciones evaluadas se encuentran Splunk, reconocida por sus avanzadas capacidades de análisis y correlación de eventos, e IBM QRadar, ampliamente utilizada en entornos corporativos para la gestión centralizada de eventos de seguridad. Sin embargo, debido a los costos asociados al licenciamiento y mantenimiento de estas plataformas, se consideró que Wazuh representaba una alternativa más adecuada para el contexto de la organización analizada.

Tabla 1.

Comparación de Soluciones para la implementación del SIEM.

Criterio	Wazuh	Splunk	IBM QRadar
Licenciamiento	Software libre	Comercial	Comercial
Costo	Sin licencias	Alto	Alto
Gestión de vulnerabilidades	Sí	Sí	Sí
Integración MITRE ATT&CK	Sí	Sí	Sí
Adecuado para PYMEs	Sí	Limitado por costo	Limitado por costo
Comunidad y documentación	Amplia	Amplia	Amplia

Nota. Esta tabla muestra una comparativa entre algunas soluciones SIEM que ofrece el mercado. *Fuente.* Elaboración propia.

Antes de seleccionar la plataforma SOAR, se evaluaron diferentes herramientas orientadas a la automatización y orquestación de respuestas ante incidentes de seguridad. Entre las alternativas consideradas se encuentran Cortex XSOAR y CrowdStrike Falcon SOAR, soluciones ampliamente utilizadas en entornos empresariales por sus capacidades de integración y automatización avanzada. No obstante, al tratarse de plataformas comerciales con costos de implementación y operación elevados, se determinó que Shuffle constituía una alternativa más viable para el proyecto, al ofrecer funcionalidades de automatización, integración mediante API y creación de flujos de respuesta, bajo un modelo de software libre y sin costos de licenciamiento.

Tabla 2.

Comparación de Soluciones para la implementación del SOAR.

Criterio	Shuffle	Cortex XSOAR	Crowdstrike Falcon SOAR
Licenciamiento	Software libre	Comercial	Comercial
Costo	Sin licencias	Alto	Alto
Integración API	Sí	Sí	Sí
Automatización	Sí	Sí	Sí
Adecuado para PYMEs	Sí	Limitado por costo	Limitado por costo

Nota. Esta tabla muestra una comparativa entre algunas soluciones SOAR que ofrece el mercado. *Fuente.* Elaboración propia.

Recursos necesarios

Tabla 3.

Recursos.

Recurso	Descripción	Costo Estimado
1. Servidor dedicado o VPS	Servidor necesario para la implementación de la plataforma SIEM + SOAR. CPU 8 núcleos, RAM 16 GB – Para hasta 500 Usuarios	$2,500,000 COP/mes
2. Almacenamiento (HDD/SSD)	Almacenamiento adicional para la recolección de logs y eventos (1 TB SSD).	$1,000,000 COP
3. Licencias de software libre	Herramientas como ELK (Elastic), Wazuh, Shuffle, que son de uso gratuito, pero requieren mantenimiento.	$0 COP
4. Servicio de Ingeniería	Ingeniero para la implementación y configuración del sistema, y para la integración de la red.	$6,000,000 COP/mes
5. Capacitación a usuarios	Formación para los empleados de la PYME sobre el uso del sistema y respuestas ante incidentes.	$1,200,000 COP
6. Backup y recuperación	Sistema de backup para asegurar la integridad de los datos recolectados por el SIEM.	$800,000 COP (una vez)
	Total	$11,500,000 COP

Nota. En esta tabla, se realiza un presupuesto para la implementación del SIEM + SOAR.

Fuente. Elaboración propia.

Arquitectura y Componentes de la Solución Wazuh (SIEM)

La arquitectura de Wazuh se estructura en torno a un sistema centralizado que recoge, analiza y almacena datos de seguridad, permitiendo un monitoreo integral de los puntos finales (endpoints) y dispositivos de red en una organización. Esta solución se basa en agentes que se ejecutan en los dispositivos monitoreados y envían datos de seguridad a un servidor central. Para aquellos dispositivos que no admiten agentes, como firewalls, switches y routers, es posible integrar sus registros mediante Syslog, SSH o una API. El servidor central de Wazuh analiza y decodifica esta información y la envía al indexador para su almacenamiento, la arquitectura se puede observar en la Figura 1.

La plataforma se compone de tres componentes fundamentales:

1. **Agente Wazuh**: Este agente se instala en los puntos finales, tales como servidores, computadoras y dispositivos en la nube. Su función es recopilar y enviar información de seguridad al servidor Wazuh, ofreciendo capacidades de detección, prevención y respuesta ante amenazas.
2. **Servidor Wazuh**: Es el núcleo de procesamiento de la solución. Aquí se reciben y analizan los datos recopilados de los agentes. Utiliza decodificadores y reglas, en combinación con inteligencia de amenazas, para identificar posibles indicadores de compromiso (IOC). El servidor administra la configuración de los agentes y permite su escalabilidad, soportando cientos o miles de agentes, especialmente cuando se implementa en un clúster.
3. **Indexador Wazuh**: Es un motor de búsqueda y análisis de texto completo que indexa y almacena las alertas generadas por el servidor. En instalaciones

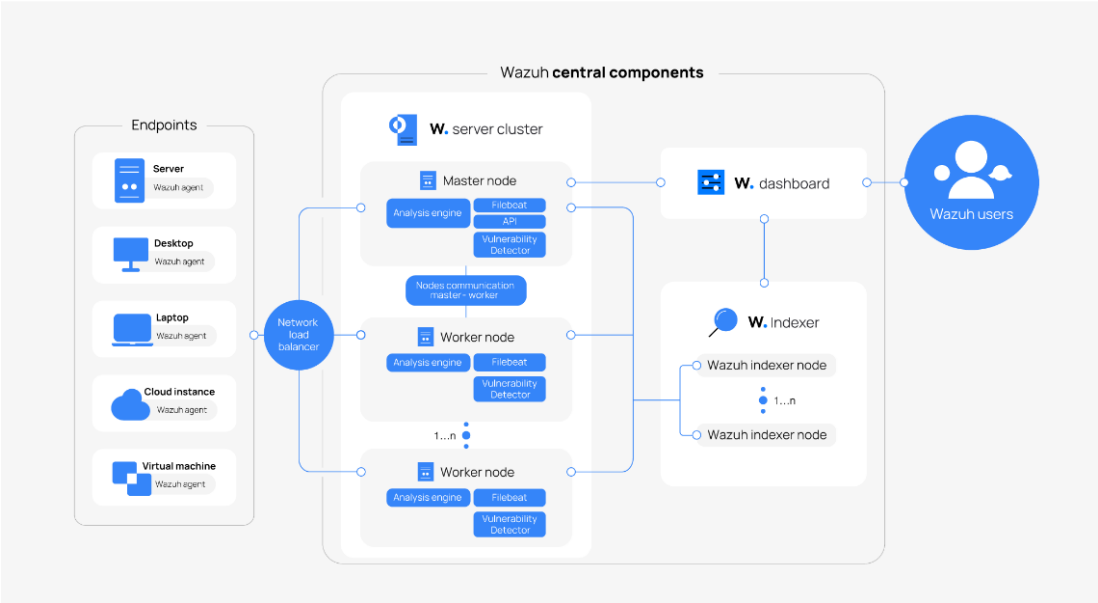
pequeñas, puede funcionar en un solo nodo, mientras que en entornos más grandes, es recomendable un clúster de varios nodos para soportar grandes volúmenes de datos y asegurar la alta disponibilidad.

4. **Panel de Control Wazuh**: Es la interfaz web de usuario, diseñada para el análisis y visualización de datos. Facilita la búsqueda de amenazas, el monitoreo de cumplimiento normativo (como PCI DSS, GDPR y otros), y permite gestionar la configuración y el estado del sistema. Ofrece paneles listos para usar que ayudan en la detección de vulnerabilidades, la evaluación de la configuración y el monitoreo de la integridad de los archivos.

Esta arquitectura robusta permite a Wazuh monitorear no solo puntos finales, sino también dispositivos sin agentes, logrando una cobertura de seguridad completa. (Wazuh, Wazuh, 2024)

Figura 1

Plano Arquitectura y Componentes de Wazuh (SIEM).



Nota. Plano de la arquitectura y componentes de Wazuh (SIEM). *Fuente.* (Wazuh, Wazuh, 2024)

Arquitectura y Componentes de la Solución Shuffle (SOAR)

Shuffle es una solución de código abierto diseñada para la creación y ejecución de flujos de trabajo de automatización orientados a la ciberseguridad. Se basa en una arquitectura API-first, lo que permite a los usuarios interactuar con cada función de la plataforma a través de puntos finales API, tanto en implementaciones en la nube como en entornos locales. Esto facilita la integración con otros sistemas y herramientas, optimizando los flujos de trabajo y automatizando respuestas ante incidentes de seguridad.

La autenticación en Shuffle utiliza el modelo de token portador. Cada solicitud enviada a la API requiere el encabezado “Autorización: Portador <APIKEY>”, lo que garantiza una comunicación segura y autenticada. En entornos multiusuario, Shuffle permite la gestión de múltiples organizaciones, y el usuario puede especificar la organización deseada mediante el encabezado "Org-Id: <ORGID>", o bien trabajar con la organización activa predeterminada. Esta flexibilidad permite adaptar los flujos de trabajo y políticas de seguridad a diferentes niveles organizativos dentro de la misma plataforma.

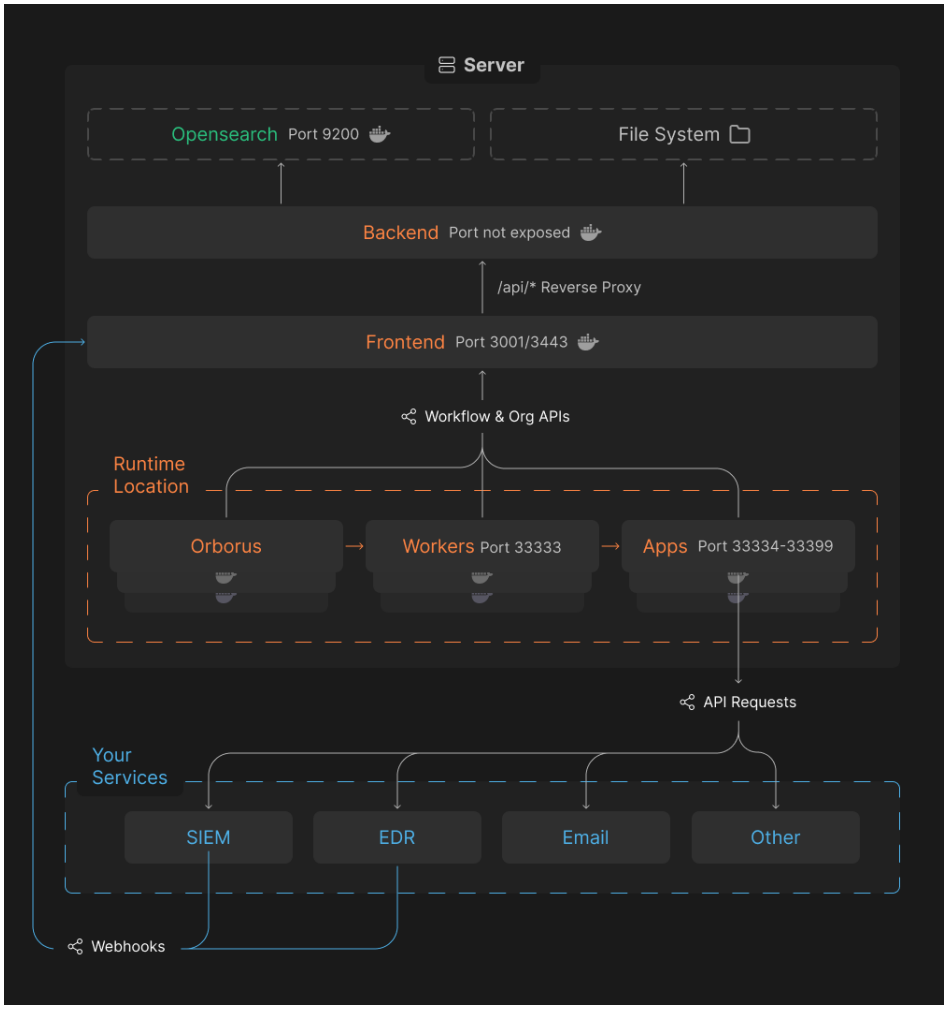
Shuffle genera sus APIs mediante un creador OpenAPI propio, lo que permite mantener la compatibilidad y consistencia entre las versiones de la plataforma, facilitando la escalabilidad y mantenimiento del sistema. Este diseño API-centric convierte a Shuffle

en una herramienta versátil y eficaz para implementar un sistema SOAR automatizado, permitiendo a las organizaciones responder de forma rápida y eficiente a eventos de seguridad sin intervención manual, asegurando una mayor efectividad en la gestión de amenazas y un mejor aprovechamiento de los recursos de seguridad. (Shuffler, Shuffler, 2024). La arquitectura se puede observar en la Figura 2.

La integración entre Wazuh y Shuffle permite crear un ecosistema de seguridad optimizado que combina la detección, el análisis y la respuesta automatizada ante incidentes de seguridad. En este entorno, Wazuh actúa como el componente SIEM encargado de recopilar y analizar los datos de seguridad de los puntos finales, mientras que Shuffle, en su rol de SOAR, automatiza las respuestas y procesos posteriores con base en la información recibida del SIEM.

Figura 2

Plano Arquitectura de Shuffle (SOAR).

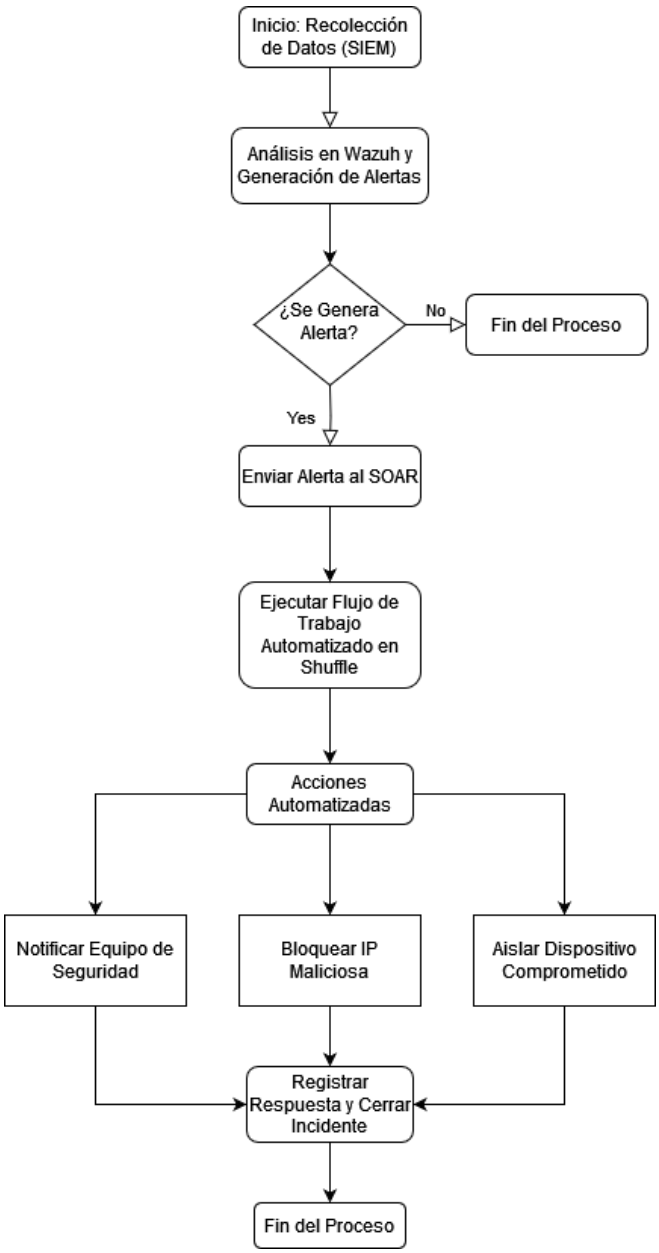


Nota. Plano de la arquitectura Shuffle (SOAR). *Fuente.* (Shuffle, 2025)

Diagrama de Bloques

Figura 3

Diagrama de Flujo SIEM + SOAR.



Nota. Diagrama de flujo del funcionamiento integral entre la solución SIEM y SOAR.

Fuente. Elaboración propia.

Fase 3: Implementación del Prototipo

La fase de implementación del prototipo tuvo como propósito desplegar e integrar la solución SIEM + SOAR en el entorno empresarial real, de acuerdo con la arquitectura definida en la fase de diseño. Para ello, se utilizaron máquinas virtuales sobre la plataforma de virtualización Proxmox, garantizando un entorno controlado, escalable y alineado con los recursos disponibles de la empresa.

Implementación de la infraestructura virtual para el SIEM

Para la implementación del sistema SIEM se creó una máquina virtual dedicada en el hipervisor Proxmox, destinada a alojar la plataforma Wazuh. La máquina virtual fue configurada con recursos acordes a la capacidad de procesamiento requerida para la recolección y análisis de eventos de seguridad.

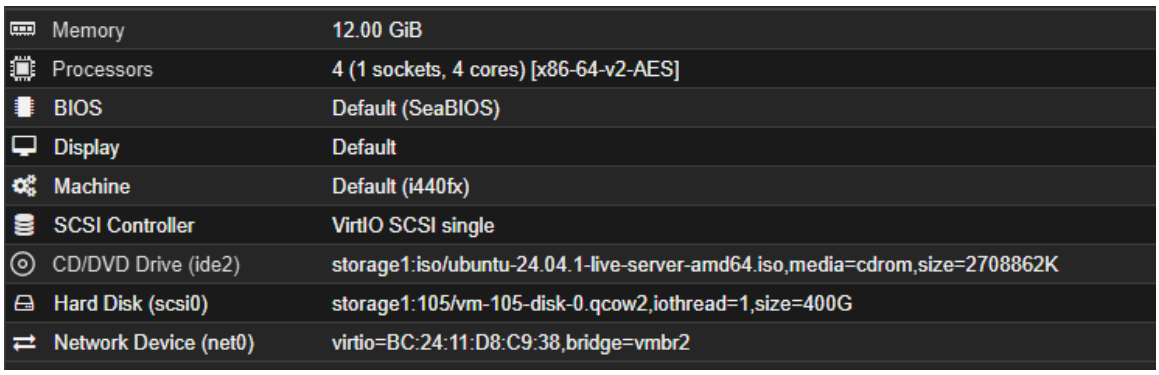
La configuración de la máquina virtual incluye:

- **Memoria RAM:** 12 GB
- **Procesador:** 4 núcleos
- **Sistema operativo:** Ubuntu Server 24.04 LTS
- **Almacenamiento:** 400 GB
- **Interfaz de red:** Bridge configurado para integración con la red corporativa

Esta configuración permite garantizar el correcto funcionamiento de los componentes del SIEM, incluyendo el servidor Wazuh, el indexador y el panel de control. En la Figura 4 se presenta la configuración general de la máquina virtual creada en Proxmox para el sistema SIEM, como se puede observar en la Figura 4.

Figura 4

Configuración Máquina Virtual Wazuh (SIEM).



Nota. Configuración de hardware de la máquina virtual donde se contendrá los servicios de Wazuh (SIEM). *Fuente.* Elaboración propia.

Instalación y configuración del sistema SIEM (Wazuh)

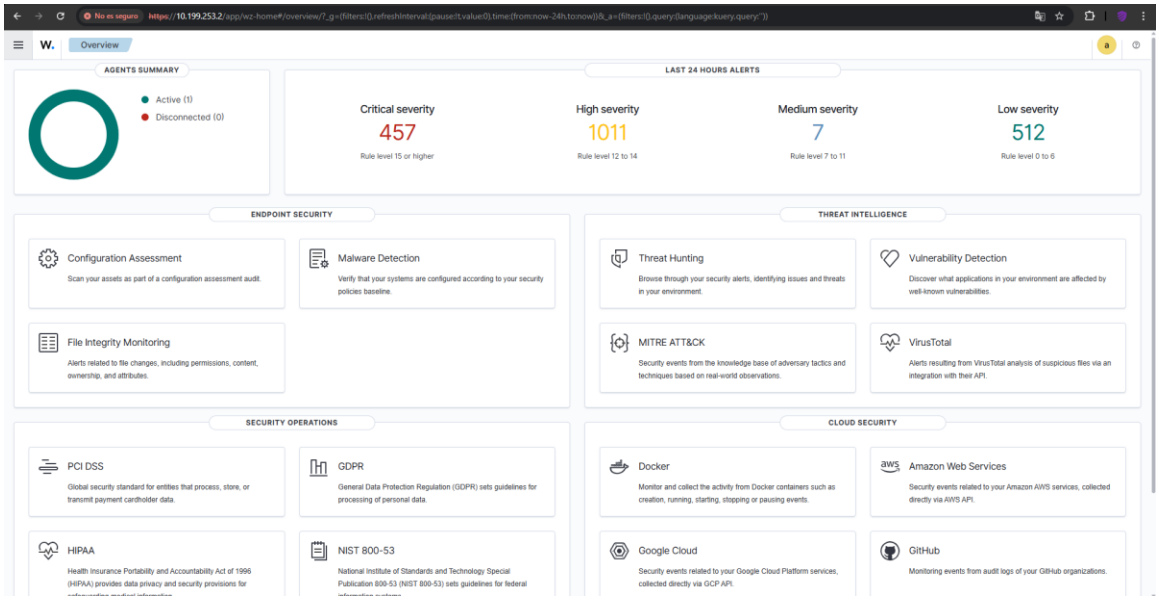
Una vez creada la máquina virtual, se procedió a la instalación del sistema operativo Ubuntu Server y posteriormente a la implementación de la plataforma Wazuh. La instalación se realizó siguiendo las recomendaciones oficiales del fabricante, asegurando la correcta integración de sus componentes principales.

Durante esta etapa se llevaron a cabo las siguientes actividades:

- Instalación del servidor Wazuh.
- Configuración del indexador para el almacenamiento y consulta de eventos.
- Despliegue del panel de control para la visualización y análisis de alertas.
- Configuración inicial de reglas y decodificadores para la detección de accesos no autorizados y malware.
- Instalación de agentes Wazuh en los hosts Windows de la empresa.

Figura 5

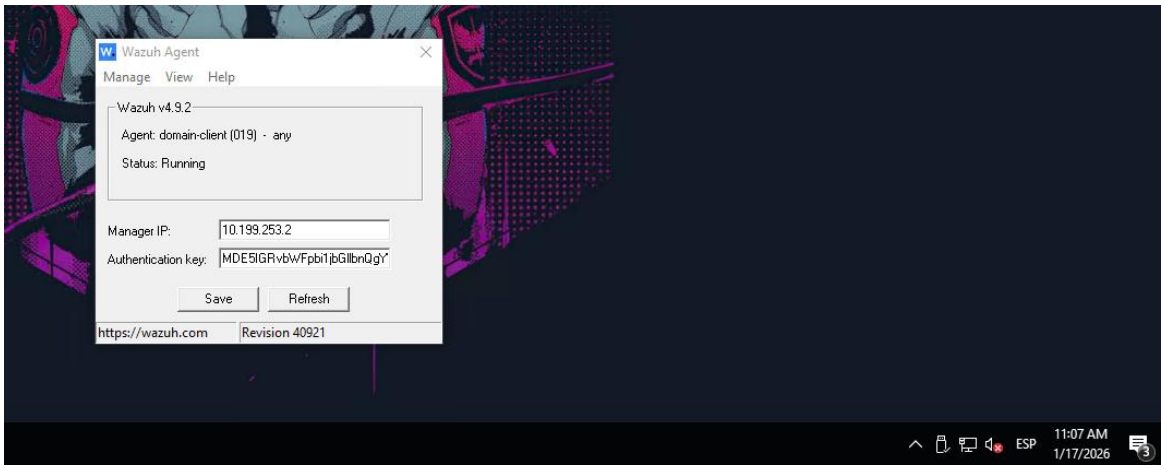
Puesta en funcionamiento de Wazuh (SIEM).



Nota. Dashboard principal de Wazuh (SIEM). *Fuente.* Elaboración propia.

Figura 6

Instalación Agente Wazuh.



Nota. Instalación de un agente del SIEM para verificar correcta comunicación con el servidor. *Fuente.* Elaboración propia.

Implementación de la infraestructura virtual para el SOAR

De manera similar, se desplegó una máquina virtual independiente para la solución SOAR Shuffle, con el fin de desacoplar las funciones de monitoreo y automatización, mejorando la seguridad y escalabilidad del sistema.

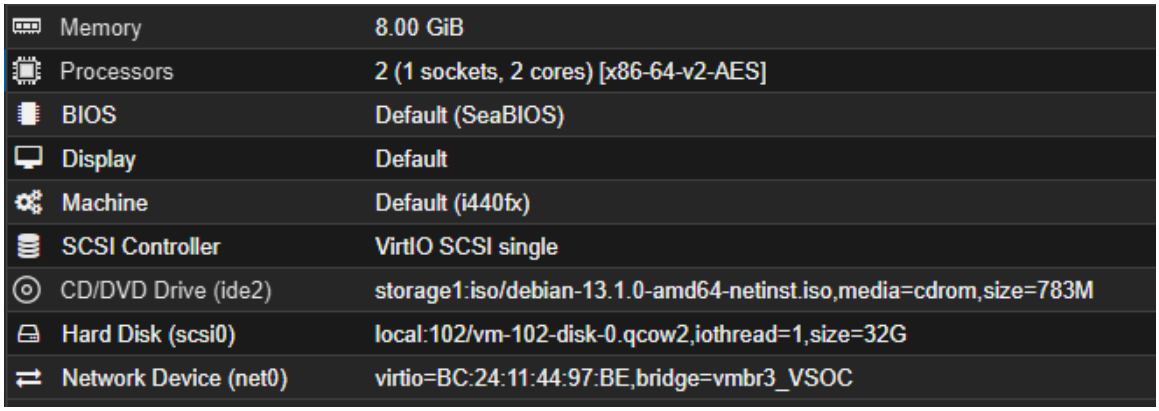
La configuración de la máquina virtual incluye:

- **Memoria RAM:** 8 GB
- **Procesador:** 2 núcleos
- **Sistema operativo:** Debian 13
- **Almacenamiento:** 32 GB
- **Interfaz de red:** Bridge configurado para integración con la red corporativa

La máquina virtual destinada al SOAR fue configurada con recursos adecuados para la ejecución de flujos de automatización y comunicación mediante API. En esta máquina se instaló el sistema operativo Linux Debian y posteriormente la plataforma Shuffle en su versión de código abierto, como se puede observar en la Figura 7.

Figura 7

Configuración Máquina Virtual Wazuh (SIEM).



Nota. Configuración de hardware de la máquina virtual donde se contendrá los servicios de Shuffle (SOAR). *Fuente.* Elaboración propia.

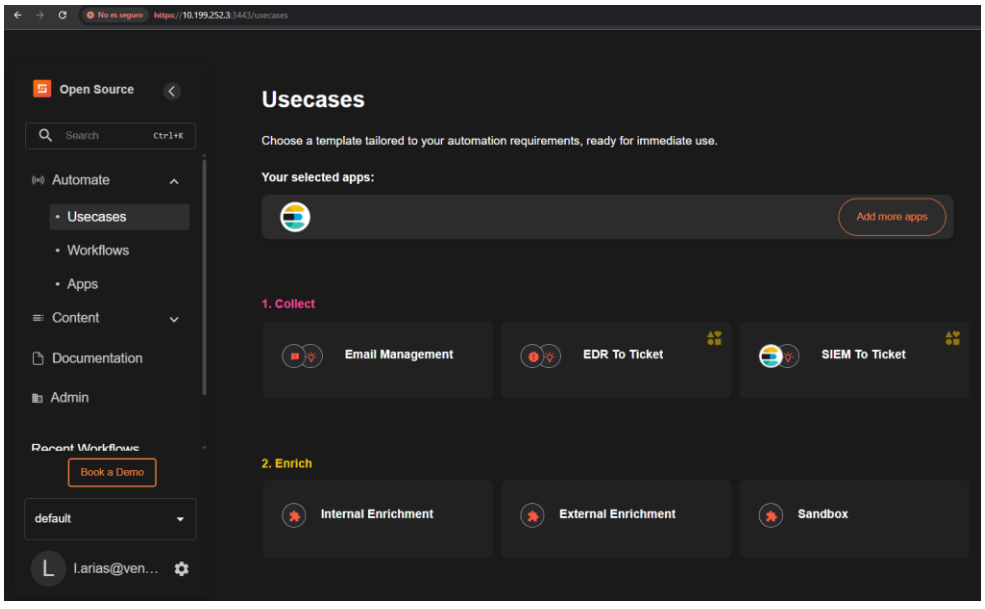
Instalación y configuración del sistema SOAR (Shuffle)

La instalación de Shuffle se realizó utilizando su despliegue local, permitiendo un control total sobre la plataforma y sus integraciones. Durante esta etapa se configuraron los siguientes elementos:

- Servicios base de Shuffle.
- Autenticación mediante tokens de acceso (API Keys).
- Creación de flujos de automatización orientados a la respuesta ante incidentes.
- Preparación de integraciones con el sistema SIEM.

Figura 8

Puesta en marcha de Shuffle (SOAR).



Nota. Dashboard principal de Shuffle (SOAR). *Fuente.* Elaboración propia.

Configuraciones específicas alineadas al CORE del negocio

Considerando que la empresa pertenece al sector eléctrico y se especializa en el diseño, comercialización y soporte de sistemas de protección contra rayos y sobretensiones para infraestructuras electrónicas críticas, se realizaron configuraciones particulares en la solución SIEM + SOAR orientadas a proteger los activos de información más relevantes para el core del negocio. Estas configuraciones permiten que la solución no se limite a una protección genérica, sino que responda a las particularidades operativas y de información sensible que maneja la organización.

Monitoreo de integridad de archivos (FIM) sobre activos críticos del negocio.

Se configuró el módulo de File Integrity Monitoring de Wazuh sobre las carpetas que almacenan los activos digitales de mayor valor para la operación: diseños técnicos de sistemas de protección, fichas técnicas de productos, propuestas comerciales, planos de instalaciones de clientes, documentación de proyectos en ejecución y bases de datos de clientes con infraestructura crítica (telecomunicaciones, subestaciones eléctricas, centros de datos). Esta configuración permite generar alertas inmediatas ante cualquier modificación, eliminación o creación de archivos en estas ubicaciones, garantizando la integridad de la información que sustenta la propuesta de valor de la empresa.

Reglas personalizadas para detección de accesos a información sensible.

Se incorporaron reglas adicionales en Wazuh dirigidas a detectar accesos sospechosos a recursos compartidos donde reposa la información comercial y técnica de

clientes con infraestructura eléctrica crítica. Considerando que parte de los clientes corresponde a entidades cuya información está sujeta a confidencialidad contractual, las reglas contemplan la detección de accesos fuera del horario laboral, intentos repetidos de acceso a recursos restringidos y la ejecución de procesos asociados a herramientas de exfiltración de información.

Flujo SOAR específico para protección de cuentas técnicas y comerciales.

En Shuffle se configuró un flujo de respuesta automatizada que prioriza la protección de las cuentas del personal técnico y comercial, las cuales tienen acceso a información sensible de clientes y a propuestas con infraestructura crítica. Ante la detección de un evento de dumping de credenciales del Windows SAM (regla 92026 de Wazuh), el flujo extrae automáticamente el nombre de usuario implicado y deshabilita la cuenta correspondiente en el Active Directory de la organización, conteniendo el incidente antes de que pueda materializarse un movimiento lateral o un escalamiento de privilegios. Adicionalmente, se implementó un mecanismo de alertamiento por intentos fallidos de autenticación, permitiendo identificar posibles ataques de fuerza bruta o accesos no autorizados y facilitando una respuesta temprana por parte del equipo de seguridad.

Política de retención de logs alineada al ciclo de vida de los proyectos.

Considerando que los proyectos del sector eléctrico suelen tener ciclos de vida prolongados, que incluyen etapas de diseño, instalación, mantenimiento y soporte

postventa, se estableció una política de retención de logs en el indexador de Wazuh acorde con dichos plazos. Esta configuración permite realizar investigaciones forenses retrospectivas en caso de incidentes que afecten a clientes con proyectos activos.

Listas blancas para aliados estratégicos.

Se configuraron listas de IPs de confianza correspondientes a proveedores autorizados, distribuidores estratégicos y aliados tecnológicos con los que la empresa intercambia información de manera regular. Esta configuración reduce el ruido operativo del SIEM y permite que las alertas se concentren sobre el tráfico realmente sospechoso. Estas configuraciones específicas permiten que la solución SIEM + SOAR implementada no solo cumpla con la función general de monitoreo y respuesta automatizada, sino que esté directamente alineada con los activos críticos, los procesos operativos y los riesgos particulares del CORE del negocio de la empresa del sector eléctrico.

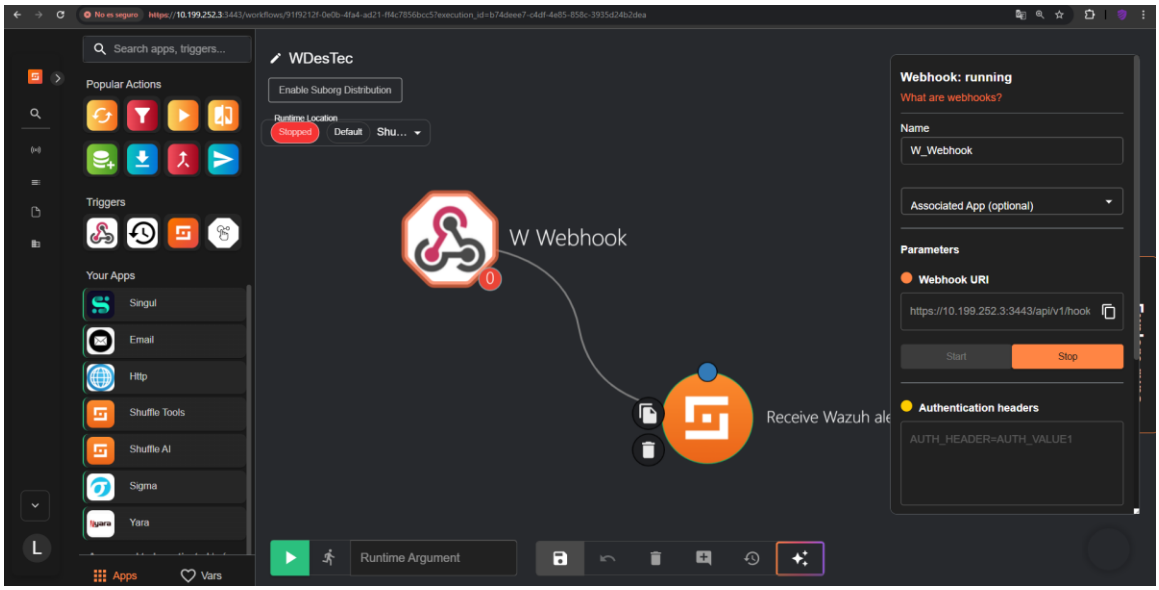
Integración entre SIEM y SOAR

Finalmente, se realizó la integración entre Wazuh y Shuffle, permitiendo que los eventos de seguridad detectados por el SIEM activen flujos de respuesta automatizados en el SOAR. Esta integración se realizó mediante el uso de APIs y webhooks, facilitando el intercambio de información entre ambas plataformas, como se puede observar en la Figura 9.

La integración permite ejecutar acciones automáticas ante eventos críticos, como la generación de alertas, registro de incidentes y respuesta inicial ante accesos no autorizados o detección de malware.

Figura 9

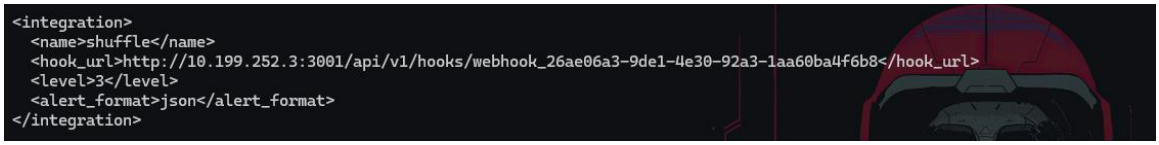
Creación de Webhook URI en el SOAR para integración con el SIEM.



Nota. Se crea una un webhook en Suffle (SOAR), donde se extrae el URI para realizar la integración entre Wazuh y Shuffle y de igual forma se ejecuta para que quede arriba el servicio. *Fuente.* Elaboración propia.

Figura 10

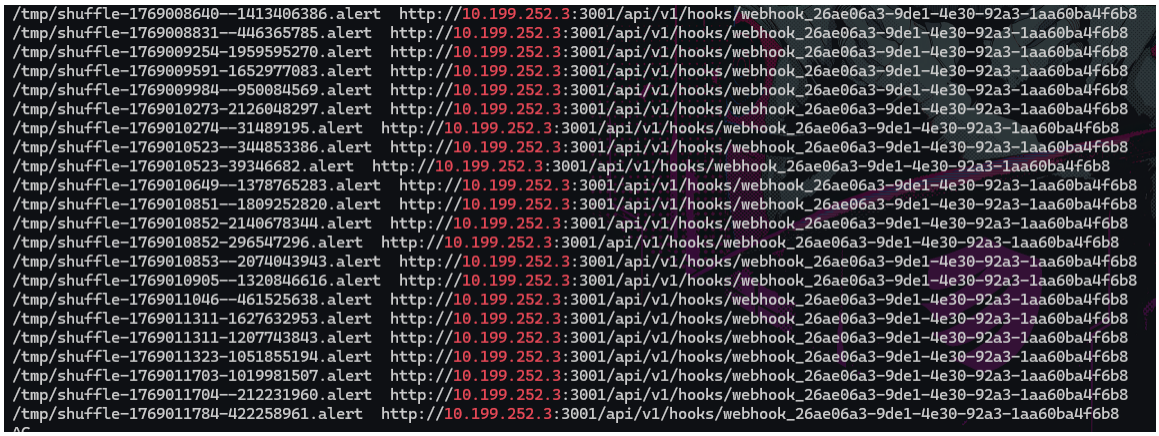
Configuración Webhook URI en SIEM para integración con el SOAR.



Nota. Se configura el URI del Webhook anteriormente extraído del SOAR y se configura en el archivo /var/ossec/etc/ossec.conf de Wazuh (SIEM), para realizar la integración entre ambas soluciones. *Fuente.* Elaboración propia.

Figura 11

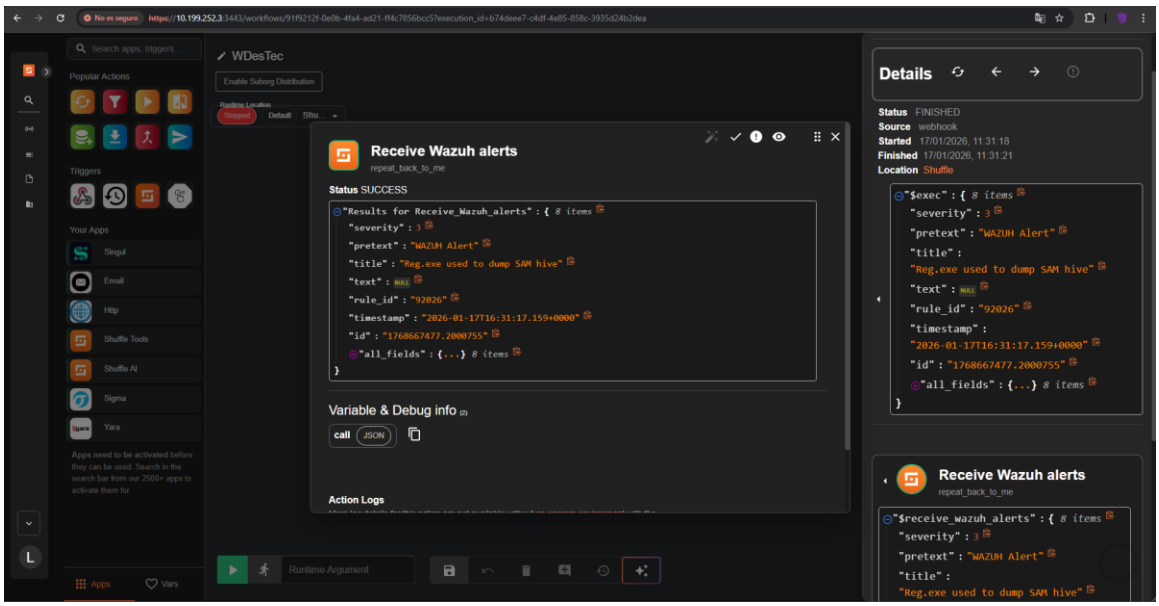
Procesamiento de alertas.



Nota. Se verifica el procesamiento de las alertas si efectivamente Wazuh está haciendo las peticiones al Webhook, la evidencia demuestra el correcto funcionamiento. *Fuente.* Elaboración propia.

Figura 12

Prueba de correcta integración y procesamiento de alertas desde el SIEM en el SOAR.



Nota. Verificación del correcto funcionamiento de la integración entre el SIEM y el SOAR, ya se puede observar que el SOAR procesa correctamente las alertas generadas en el SIEM. *Fuente.* Elaboración propia.

Enlace del video en YouTube con la explicación detallada del funcionamiento de la solución implementada

Arias Patiño, L. A. [Luis Arias]. (2024, noviembre 23). *Implementación SIEM + SOAR | Proyecto de Grado* [Video]. YouTube. https://youtu.be/FCkDqQe-rlw

Explicación detallada del funcionamiento de la solución implementada

A continuación, se describe el funcionamiento integral de la solución SIEM + SOAR basada en software libre, implementada con las plataformas Wazuh y Shuffle. Este apartado complementa el material audiovisual de soporte mediante la documentación gráfica de cada uno de los pasos realizados durante el despliegue, configuración y verificación del sistema.

Desarrollo:

1. El proceso inicia con la instalación y puesta en marcha de las máquinas virtuales destinadas al SIEM (Wazuh) y al SOAR (Shuffle) sobre el hipervisor Proxmox. La configuración se realiza en máquinas virtuales independientes con el fin de desacoplar las funciones de monitoreo y automatización, mejorando así la seguridad y escalabilidad del sistema. Las características técnicas de cada máquina virtual se detallan previamente en las Figuras 4 y 7. La evidencia del estado operativo de las máquinas virtuales sobre Proxmox se presenta en la Figura 13 y 14.

Figura 13.

Evidencia operativa, máquina virtual de Shuffle (SOAR).

Nota. La imagen evidencia que la máquina virtual para el SOAR se encuentra operativa y en estado *running*, con actividad normal de CPU, memoria y tráfico de red. *Fuente.* Elaboración propia.

Figura 14.

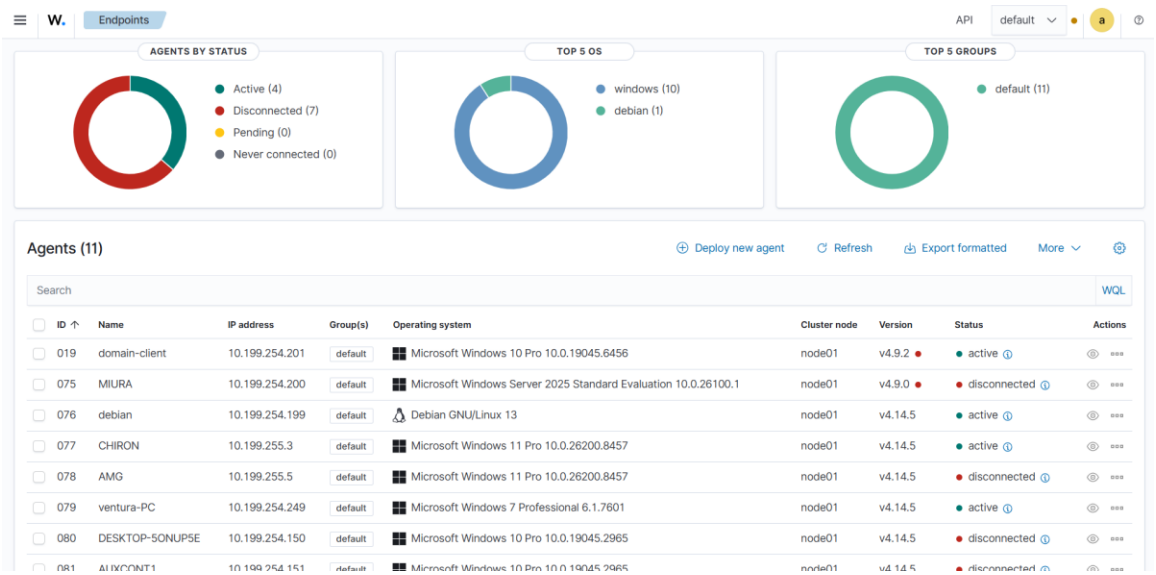
Evidencia operativa, máquina virtual de Wazuh (SIEM).

Nota. La imagen evidencia que la máquina virtual para el SIEM se encuentra operativa y en estado *running*, con actividad normal de CPU, memoria y tráfico de red. *Fuente.* Elaboración propia.

2. Una vez verificada la operatividad del servidor SIEM, se procede a la instalación del agente Wazuh en cada uno de los hosts Windows que conforman la infraestructura tecnológica de la empresa. El agente es responsable de recolectar y enviar los eventos de seguridad desde los endpoints hacia el servidor central. La instalación se realiza descargando el agente desde el sitio oficial de Wazuh (https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html), posteriormente se ejecuta, finalizado el proceso de instalación de este, se configura la dirección IP del servidor y la clave de autenticación se genera de forma automática, siempre y cuando no haya problemas de comunicación. La evidencia de instalación se presenta en la Figura 6.
3. Posterior a la instalación, se valida la correcta comunicación entre los agentes y el servidor de Wazuh. Esta verificación garantiza que los eventos generados en los endpoints son recibidos, decodificados e indexados por el SIEM de manera oportuna. La validación se realiza mediante la consulta del estado de los agentes en el panel de control, donde se confirma que los hosts monitoreados se encuentran en estado "Active" y reportando eventos al servidor central.

Figura 15.

Agentes monitorizados.



Nota. Se puede visualizar los agentes en el momento que se encuentran activos y reportando a la consola de Wazuh. *Fuente.* Elaboración propia.

4. Con el SIEM operativo, se configura la integración entre Wazuh y Shuffle a través de un mecanismo de webhook. Inicialmente se crea un webhook en Shuffle, del cual se obtiene la URI necesaria para la comunicación entre ambas plataformas, conforme se evidencia en la Figura 9. Posteriormente, dicha URI se incorpora en el archivo de configuración `/var/ossec/etc/ossec.conf` del servidor Wazuh, según se observa en la Figura 10. Esta configuración permite que las alertas generadas en el SIEM sean enviadas automáticamente al SOAR, donde se ejecutan los flujos de trabajo definidos para la respuesta a incidentes.

5. Finalmente se realiza la verificación del comportamiento conjunto de ambas plataformas mediante la generación controlada de eventos de seguridad. Las alertas son procesadas correctamente por el SIEM y enviadas al SOAR, donde se activan los flujos de automatización configurados. La evidencia del envío continuo de peticiones al webhook se presenta en la Figura 11, mientras que la confirmación de la recepción y ejecución del flujo de trabajo en Shuffle se muestra en la Figura 12.

El proceso descrito permite confirmar que la solución SIEM + SOAR queda implementada y operativa, integrando la recolección de eventos en los endpoints, la correlación y análisis en el servidor Wazuh, y la respuesta automatizada gestionada por Shuffle. A partir de esta base funcional, es posible ampliar el sistema mediante la creación de nuevos flujos de trabajo automatizados orientados a responder de manera eficiente frente a los eventos de seguridad detectados, así como mediante la incorporación de nuevas fuentes de datos y reglas de correlación específicas para el entorno de la organización.

Configuración de flujo de respuesta automatizada

Caso de uso: Detección y respuesta al dumping de credenciales del Windows SAM

El dumping de credenciales del Windows Security Accounts Manager (SAM) representa un riesgo significativo para la seguridad informática, ya que permite a un atacante extraer información sensible del sistema, como hashes de contraseñas de cuentas

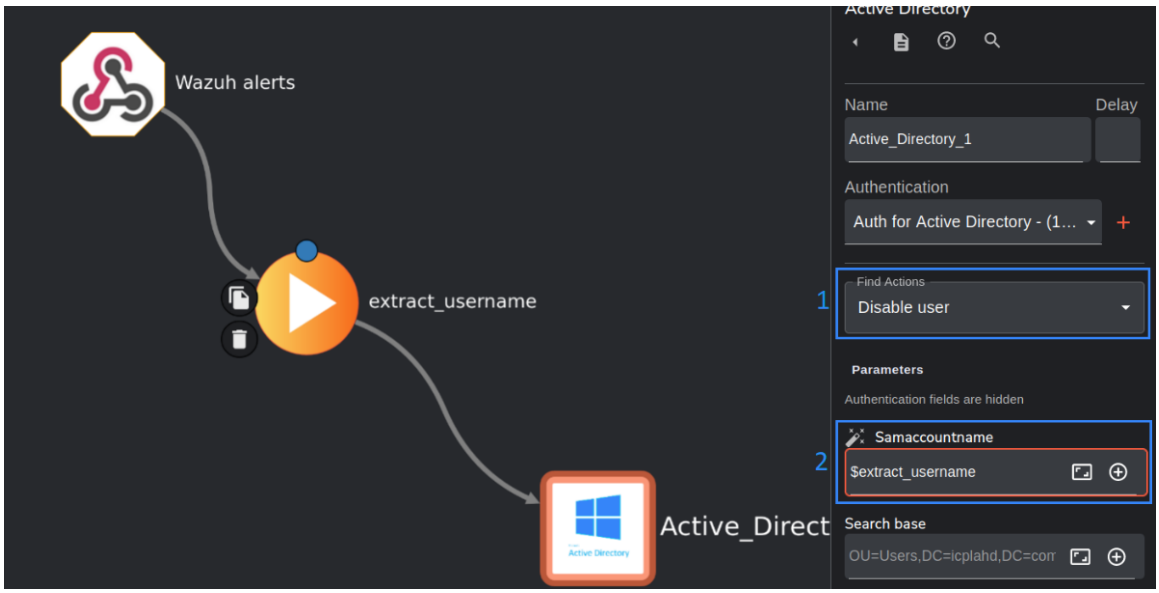
locales. Estos hashes pueden ser utilizados posteriormente para ataques de escalamiento de privilegios o movimientos laterales dentro de una red empresarial. En el contexto de este proyecto, se presenta un caso de uso que demuestra cómo una solución integrada de SIEM y SOAR puede detectar este tipo de actividad sospechosa y ejecutar una respuesta automatizada para mitigar el impacto potencial del ataque.

En este caso, Wazuh utiliza una regla interna específica (92026) diseñada para generar una alerta cuando se detecta un intento de dumping de la base de datos SAM en un endpoint con Windows. Esta alerta es enviada de forma automática a Shuffle mediante un webhook configurado en Wazuh, permitiendo que Shuffle actúe directamente sobre la información recibida.

Una vez que Shuffle recibe la alerta, se ejecuta un flujo de trabajo previamente definido que extrae, entre otros datos, el nombre de usuario del evento de dumping. Con esta información, Shuffle puede activar acciones de respuesta, tales como deshabilitar la cuenta de Active Directory involucrada en el intento de dumping, como medida inicial de contención para evitar movimientos maliciosos adicionales mientras se realiza una investigación más exhaustiva. Esta acción automatizada reduce considerablemente los tiempos de respuesta y limita el alcance del compromiso.

Figura 16.

Configuración de respuesta automatizada para evento de dumping de credenciales del Windows SAM.



Nota. Esta es la configuración del flujo de trabajo para mitigar en caso de un evento de dumping de credenciales del Windows SAM, la cual extrae el usuario de la alerta del SIEM y la envía al SOAR para que esta deshabilite la cuenta inmediatamente. *Fuente.* Elaboración propia.

Enlace del video en YouTube de la sustentación del caso de uso.

Arias Patiño, L. A. [Luis Arias]. (2024, diciembre 9). *Operación SIEM + SOAR | Proyecto de grado* [Video]. YouTube. https://youtu.be/4Np1hhCxxWs

Fase 4: Verificación funcional y resultados obtenidos.

La fase de verificación funcional tuvo como objetivo validar el correcto funcionamiento del prototipo SIEM + SOAR implementado en el entorno real de la empresa del sector eléctrico. Para ello, se realizaron pruebas controladas basadas en casos de uso previamente definidos, enfocados principalmente en eventos de accesos no autorizados, alertamiento y posibles actividades maliciosas en sistemas Windows.

Durante las pruebas realizadas, se evidenció que la implementación del SIEM permitió centralizar y correlacionar los eventos de seguridad generados por los equipos monitorizados, mejorando significativamente la visibilidad del estado de seguridad de la infraestructura tecnológica. La plataforma logró identificar eventos críticos relacionados con intentos de autenticación sospechosos y actividades potencialmente asociadas a malware, generando alertas oportunas para su análisis.

Adicionalmente, la integración del componente SOAR mediante Shuffle aportó un valor estratégico al prototipo, al permitir la automatización de acciones de respuesta ante incidentes detectados por el SIEM. A través de flujos de trabajo previamente configurados, el sistema ejecutó respuestas automatizadas que redujeron el tiempo de reacción frente a eventos críticos y disminuyeron la dependencia de intervención manual por parte del personal técnico.

La verificación funcional confirmó que la solución integrada SIEM + SOAR opera de manera coordinada, permitiendo no solo la detección de eventos relevantes, sino también la ejecución eficiente de mecanismos de contención definidos. Como resultado, la empresa pasó de un nivel básico de gestión de seguridad, basado únicamente en

controles nativos del sistema operativo, a un esquema centralizado de monitoreo, correlación y respuesta automatizada, fortaleciendo su postura de seguridad y mejorando su capacidad de reacción ante incidentes.

Tabla 4

Comparación del estado de seguridad antes y después de la implementación.

Aspecto	Antes (estado inicial)	Después (con SIEM + SOAR)	Mejora
Visibilidad de eventos de seguridad	Sin centralización; revisión manual de logs en cada uno de los hosts	Centralización total en Wazuh mediante un dashboard unificado	100% de visibilidad centralizada
Tiempo medio de detección (MTTD)	Detección reactiva (días o incluso ausencia de detección)	Detección en minutos tras la generación de alertas	Reducción significativa
Tiempo medio de respuesta (MTTR)	Respuesta manual (horas o días)	Respuestas automatizadas ejecutadas en segundos	Reducción superior al 95%
Detección de dumping de credenciales SAM	No existía mecanismo de detección	Implementación de la regla 92026 y flujo automatizado en Shuffle	Nueva capacidad implementada
Deshabilitación de cuentas comprometidas	Acción manual realizada por el administrador	Deshabilitación automática mediante integración con Active Directory	Eliminación de intervención humana
Correlación de eventos	Inexistente	Correlación activa mediante reglas configuradas en Wazuh	Nueva capacidad implementada

Monitoreo continuo 24/7	No disponible	Supervisión continua y permanente	Nueva capacidad implementada
Procesos manuales	Revisión de logs, bloqueo de cuentas y bloqueo de IPs realizados manualmente	Automatización de procesos mediante Shuffle	Eliminación de procesos manuales
Políticas de seguridad documentadas	Definidas de forma ad-hoc	Formalizadas mediante reglas y workflows automatizados	Mayor estandarización y formalización

Nota. Comparación entre el estado inicial de la empresa y el estado posterior a la implementación del prototipo SIEM + SOAR. *Fuente.* Elaboración propia.

Métricas de desempeño obtenidas durante el periodo de prueba

Durante la ejecución de las pruebas funcionales se registraron las siguientes métricas de desempeño que evidencian la operatividad y la efectividad de la solución:

Volumen de alertas procesadas:

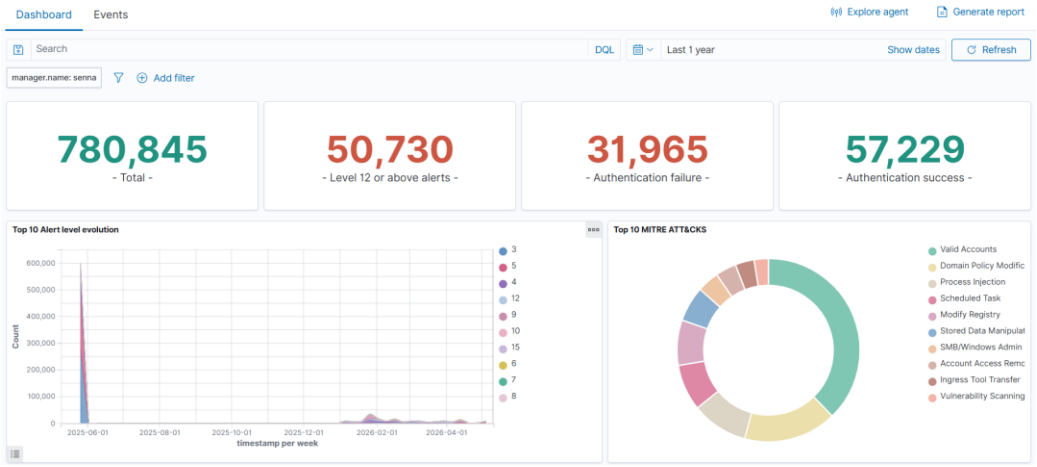
Volumen total de eventos monitoreados: Durante el periodo de pruebas, la plataforma SIEM procesó un total de 780.845 eventos de seguridad, de los cuales 50.730 correspondieron a alertas con nivel de severidad igual o superior a 12, evidenciando la capacidad de la solución para gestionar grandes volúmenes de información de manera centralizada, como se evidencia en la figura 17.

Eventos de autenticación detectados: El sistema registró 31.965 eventos de autenticación fallida y 57.229 autenticaciones exitosas, permitiendo identificar patrones

asociados a posibles intentos de acceso no autorizado y validar la correcta correlación de eventos de autenticación en tiempo real, como se evidencia en la Figura 17.

Figura 17.

Eventos de autenticación.

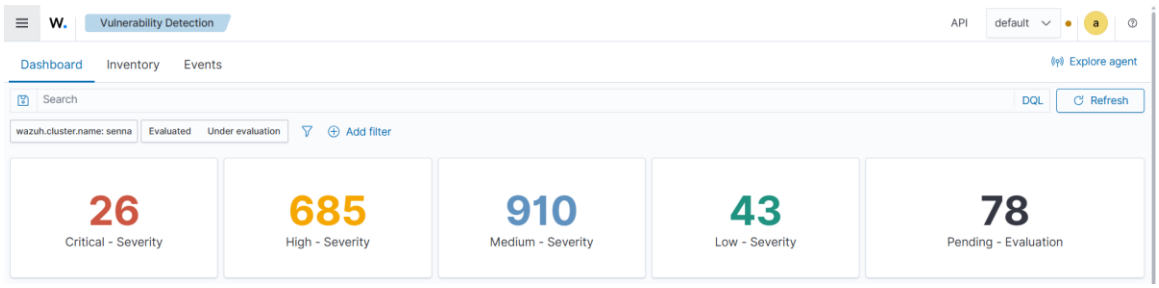


Nota. Número de eventos de autenticación durante el periodo de pruebas. *Fuente.* Elaboración propia.

Clasificación de vulnerabilidades por severidad: El módulo de detección de vulnerabilidades identificó 26 vulnerabilidades críticas, 685 vulnerabilidades altas, 910 vulnerabilidades medias, 43 vulnerabilidades bajas y 78 hallazgos pendientes de evaluación, permitiendo priorizar las acciones de mitigación según el nivel de riesgo detectado, conforme se presenta en la Figura 18.

Figura 18.

Detecciones de vulnerabilidades.

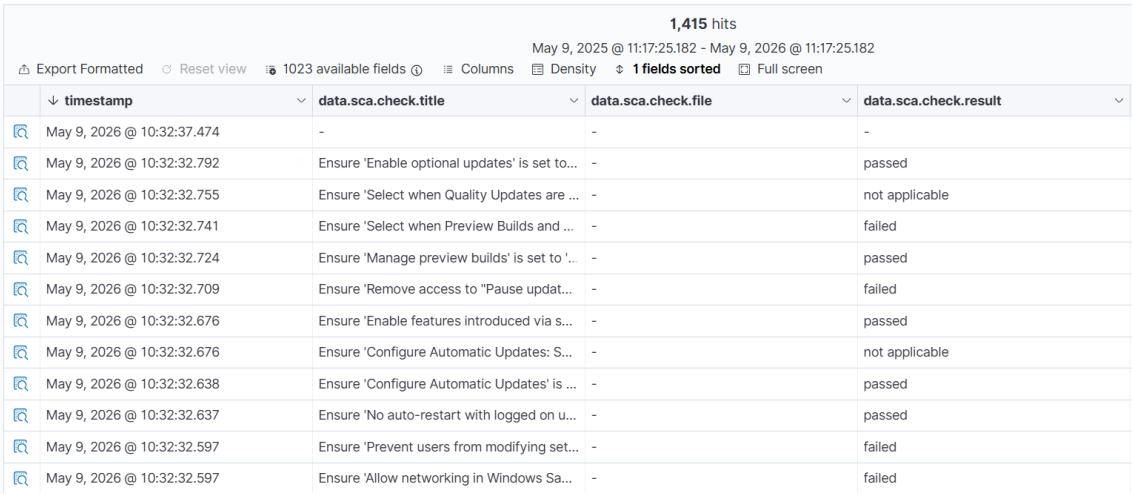


Nota. Eventos de vulnerabilidades durante el periodo de pruebas. *Fuente.* Elaboración propia.

Monitoreo de cumplimiento y hardening: Durante las pruebas se evaluaron 1.415 verificaciones de cumplimiento asociadas a políticas CIS para Windows, identificando configuraciones en estado *passed*, *failed* y *not applicable*, lo cual permitió validar el funcionamiento del módulo de evaluación de cumplimiento y hardening del SIEM, conforme se observa en la Figura 19.

Figura 19.

Eventos de monitoreo de cumplimiento y hardening.



1,415 hits

May 9, 2025 @ 11:17:25.182 - May 9, 2026 @ 11:17:25.182

Export Formatted | Reset view | 1023 available fields | Columns | Density | **1 fields sorted** | Full screen

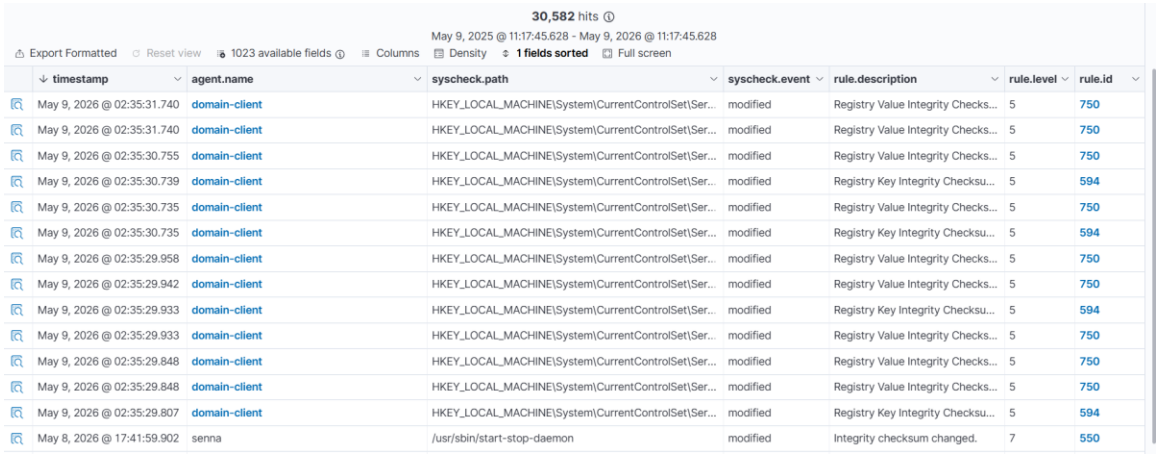
timestamp	data.sca.check.title	data.sca.check.file	data.sca.check.result
May 9, 2026 @ 10:32:37.474	-	-	-
May 9, 2026 @ 10:32:32.792	Ensure 'Enable optional updates' is set to...	-	passed
May 9, 2026 @ 10:32:32.755	Ensure 'Select when Quality Updates are ...	-	not applicable
May 9, 2026 @ 10:32:32.741	Ensure 'Select when Preview Builds and ...	-	failed
May 9, 2026 @ 10:32:32.724	Ensure 'Manage preview builds' is set to '...	-	passed
May 9, 2026 @ 10:32:32.709	Ensure 'Remove access to "Pause updat...	-	failed
May 9, 2026 @ 10:32:32.676	Ensure 'Enable features introduced via s...	-	passed
May 9, 2026 @ 10:32:32.676	Ensure 'Configure Automatic Updates: S...	-	not applicable
May 9, 2026 @ 10:32:32.638	Ensure 'Configure Automatic Updates' is ...	-	passed
May 9, 2026 @ 10:32:32.637	Ensure 'No auto-restart with logged on u...	-	passed
May 9, 2026 @ 10:32:32.597	Ensure 'Prevent users from modifying set...	-	failed
May 9, 2026 @ 10:32:32.597	Ensure 'Allow networking in Windows Sa...	-	failed

Nota. Eventos durante el periodo de pruebas de cumplimiento y hardening en equipos Windows. *Fuente.* Elaboración propia.

Monitoreo de integridad y cambios en el sistema: El sistema registró 30.582 eventos asociados a cambios de integridad mediante el módulo FIM (File Integrity Monitoring), incluyendo modificaciones sobre claves críticas del registro de Windows y archivos del sistema, demostrando la capacidad de detección temprana de alteraciones potencialmente maliciosas, conforme se evidencia en la Figura 20.

Figura 20.

Eventos de integridad y cambios en el sistema.



30,582 hits

May 9, 2025 @ 11:17:45.628 - May 9, 2026 @ 11:17:45.628

Export Formatted | Reset view | 1023 available fields | Columns | Density | 1 fields sorted | Full screen

timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
May 9, 2026 @ 02:35:31.740	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checks...	5	750
May 9, 2026 @ 02:35:31.740	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checks...	5	750
May 9, 2026 @ 02:35:30.755	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checks...	5	750
May 9, 2026 @ 02:35:30.739	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksu...	5	594
May 9, 2026 @ 02:35:30.735	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checks...	5	750
May 9, 2026 @ 02:35:30.735	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksu...	5	594
May 9, 2026 @ 02:35:29.958	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checks...	5	750
May 9, 2026 @ 02:35:29.942	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checks...	5	750
May 9, 2026 @ 02:35:29.933	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksu...	5	594
May 9, 2026 @ 02:35:29.933	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checks...	5	750
May 9, 2026 @ 02:35:29.848	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checks...	5	750
May 9, 2026 @ 02:35:29.848	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Value Integrity Checks...	5	750
May 9, 2026 @ 02:35:29.807	domain-client	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	modified	Registry Key Integrity Checksu...	5	594
May 8, 2026 @ 17:41:59.902	senna	/usr/sbin/start-stop-daemon	modified	Integrity checksum changed.	7	550

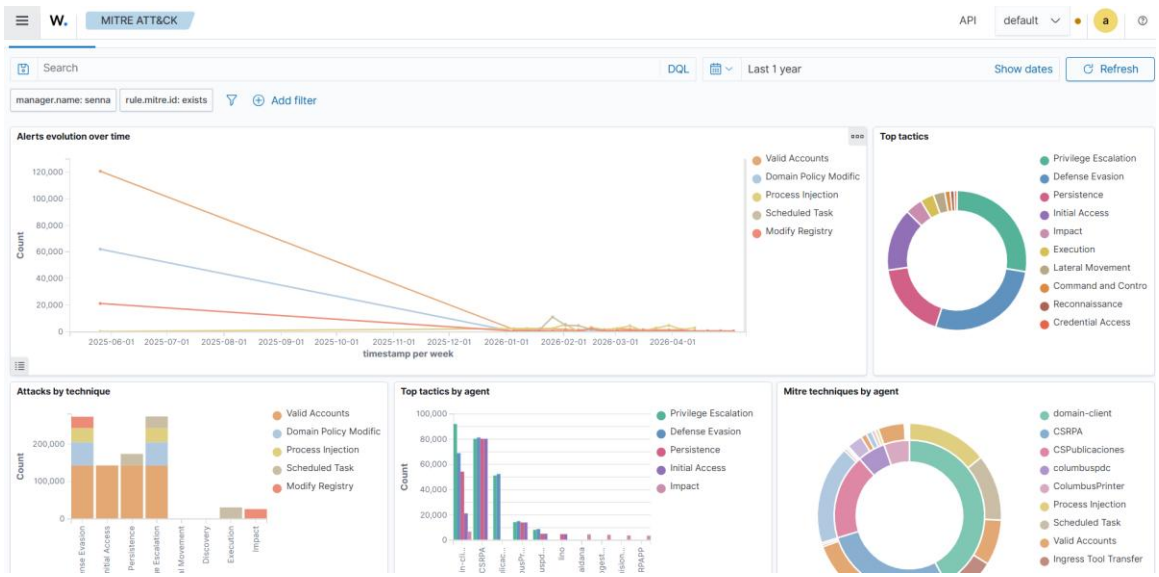
Nota. Eventos durante el periodo de pruebas del módulo de monitoreo de integridad.

Fuente. Elaboración propia.

Cobertura de tácticas MITRE ATT&CK: Las alertas detectadas durante las pruebas se asociaron principalmente a tácticas como Valid Accounts, Domain Policy Modification, Process Injection, Scheduled Task y Modify Registry, evidenciando la capacidad del SIEM para clasificar eventos bajo el marco MITRE ATT&CK y mejorar la trazabilidad de amenazas, como se observa en la figura 21.

Figura 21.

MITRE ATT&CK.



Nota. Asociación de todas las detecciones durante el periodo de pruebas, a tácticas y técnicas de MITRE ATT&CK. *Fuente.* Elaboración propia.

Latencia entre SIEM y SOAR: el tiempo desde la generación de la alerta en Wazuh hasta su recepción en Shuffle se ubica en el orden de segundos, validado mediante el procesamiento continuo de webhooks evidenciado en la Figura 11.

Tiempo de contención automatizada: desde la detección del evento de dumping de credenciales SAM hasta la deshabilitación de la cuenta en Active Directory, la ejecución se completa en cuestión de segundos, sin intervención manual del personal técnico, asimismo, como el bloqueo de IPs y notificación al personal técnico.

Cobertura de hosts monitoreados: 100 % de los hosts Windows de la organización (aproximadamente diez equipos) reportando al SIEM.

Disponibilidad de la solución: Operación continua sin fallas reportadas durante el periodo de pruebas hasta el día de hoy.

Procesos manuales eliminados o reducidos

La implementación de la solución permitió eliminar o reducir significativamente los siguientes procesos manuales que anteriormente formaban parte de la operación de seguridad de la organización:

Revisión manual del Visor de Eventos (Event Viewer) en cada host Windows.

Búsqueda manual de intentos de inicio de sesión fallidos o sospechosos.

Bloqueo manual de cuentas comprometidas tras la detección reactiva de comportamientos anómalos.

Validación manual de la integridad de archivos críticos.

Consolidación manual de información de seguridad proveniente de distintos equipos.

Comunicación informal de incidentes entre los miembros del equipo técnico.

Políticas de seguridad formalizadas

A partir de la implementación, se establecieron políticas de seguridad concretas que pasaron de estar implícitas u operadas de manera ad-hoc a estar formalizadas en reglas y flujos automatizados:

Política de monitoreo continuo de eventos de seguridad sobre todos los endpoints Windows.

Política de detección y contención automática.

Política de monitoreo de integridad sobre carpetas con activos críticos del negocio.

Política de alertamiento diferenciado dentro y fuera del horario laboral.

Política de retención y trazabilidad de eventos para soporte a investigaciones forenses.

A continuación, se presenta la verificación funcional puntual de cada uno de los elementos que conforman el prototipo:

Tabla 5.

Tabla de verificación funcional del prototipo SIEM + SOAR.

Elemento verificado	Descripción de la verificación	Resultado
Recolección de eventos en hosts Windows	Se verificó que los agentes Wazuh instalados en los equipos Windows envían correctamente eventos de seguridad al servidor SIEM.	*Cumple*
Centralización de eventos	Se confirmó que los eventos son recibidos, almacenados e indexados en el servidor Wazuh de forma centralizada.	*Cumple*
Visualización de alertas	Se validó la visualización de alertas y eventos en el panel de control de Wazuh.	*Cumple*
Detección de accesos no autorizados	Se comprobó la generación de alertas ante eventos relacionados con intentos de acceso sospechosos.	*Cumple*
Detección de eventos de malware	Se validó la identificación de eventos asociados a posibles amenazas de malware en los endpoints.	*Cumple*
Integración SIEM–SOAR	Se verificó la correcta comunicación entre Wazuh y Shuffle mediante API/webhooks.	*Cumple*
Activación de flujos SOAR	Se confirmó que las alertas generadas por el SIEM activan los flujos de automatización en Shuffle.	*Cumple*
Ejecución de respuestas automatizadas	Se comprobó la ejecución de acciones automáticas de respuesta definidas en los flujos SOAR.	*Cumple*
Registro de incidentes	Se verificó el registro de los incidentes gestionados durante la verificación funcional.	*Cumple*
Estabilidad del sistema	Se validó el funcionamiento continuo del prototipo sin fallos durante el periodo de prueba.	*Cumple*

Nota. En esta tabla se soporta y verifica los elementos verificados del prototipo. *Fuente.* Elaboración propia.

Recomendaciones

Plan de mantenimiento

El Plan de Mantenimiento para el proyecto SIEM + SOAR, basado en Wazuh y Shuffle, garantiza el funcionamiento eficiente y seguro de la solución en entornos empresariales. Se establecen normas para la administración y configuración del sistema, asegurando procedimientos estandarizados para la gestión de incidentes y cambios en los flujos de trabajo automatizados. También se contempla la capacitación continua del personal encargado, fortaleciendo su capacidad para operar y optimizar ambas plataformas. El rendimiento se monitorea mediante indicadores clave, como el tiempo promedio de detección y respuesta a amenazas, el uso eficiente de recursos del servidor y la precisión en la detección de amenazas, minimizando falsos positivos y negativos. Además, se ajusta la infraestructura tecnológica para mantener la escalabilidad y disponibilidad del sistema, adaptándose a las necesidades de monitoreo de las organizaciones, asegurando así que la solución cumpla con los estándares requeridos de seguridad y eficiencia operativa.

Plan de aseguramiento de la solución SIEM + SOAR

Una vez implementada, la solución SIEM + SOAR adquiere por sí misma la condición de activo crítico de la organización, dado que centraliza información sensible de seguridad, almacena evidencia forense y ejecuta acciones automatizadas con privilegios elevados sobre la infraestructura tecnológica. Por esta razón, se establece el siguiente plan de aseguramiento orientado a proteger las plataformas Wazuh y Shuffle frente a accesos no autorizados, manipulación maliciosa o pérdida de disponibilidad.

Hardening del sistema operativo.

Se aplica un proceso de endurecimiento sobre los sistemas operativos que alojan las plataformas, alineado con las recomendaciones del benchmark CIS correspondiente a Ubuntu Server (servidor SIEM) y Debian (servidor SOAR). Esta configuración contempla la deshabilitación de servicios no requeridos, la restricción de puertos abiertos mediante UFW o iptables, la actualización periódica de paquetes y la deshabilitación del inicio de sesión remoto del usuario root.

Control de acceso granular.

El acceso a las plataformas se restringe mediante autenticación multifactor (MFA) para todos los usuarios con privilegios administrativos. Se definen roles diferenciados (administrador, analista de seguridad y usuario de solo lectura) acordes con el principio de mínimo privilegio. El acceso administrativo se permite únicamente desde redes autorizadas, mediante VPN o desde un servidor jump dedicado para tareas de gestión.

Política de credenciales y rotación de claves.

Se establece una política de contraseñas robustas con longitud mínima, complejidad y rotación periódica. Las API Keys utilizadas en la integración entre Wazuh y Shuffle se almacenan en gestores seguros y se rotan de manera programada o ante cualquier sospecha de compromiso. Las credenciales utilizadas por el flujo SOAR para interactuar con Active Directory se gestionan bajo el mismo esquema, garantizando trazabilidad y control.

Cifrado de comunicaciones y datos.

Se garantiza el uso de TLS en todas las comunicaciones entre los componentes de la solución: agente-servidor en Wazuh, comunicaciones internas, conexiones al panel de control y peticiones webhook entre Wazuh y Shuffle. Adicionalmente se evalúa el cifrado en reposo de los logs e índices almacenados en el indexador, así como el almacenamiento seguro de tokens y credenciales.

Segmentación de red.

La infraestructura SIEM + SOAR se ubica en una VLAN dedicada, separada de la red corporativa general. El tráfico hacia y desde estos servidores está controlado mediante reglas de firewall que permiten únicamente las comunicaciones estrictamente necesarias: recepción de eventos desde los agentes, conexiones administrativas autorizadas y comunicación entre Wazuh y Shuffle.

Respaldos seguros y pruebas de restauración.

Se programan respaldos periódicos cifrados de las configuraciones críticas: reglas y decodificadores de Wazuh, workflows y aplicaciones de Shuffle, archivos de configuración y bases de datos. Los respaldos se almacenan en una ubicación geográficamente separada o en un medio offline. Trimestralmente se ejecutan pruebas de restauración para validar la integridad y utilidad de los respaldos.

Gestión controlada de actualizaciones.

Se establece un procedimiento formal para la gestión de actualizaciones de Wazuh, Shuffle y los sistemas operativos subyacentes. Las actualizaciones se evalúan inicialmente en un ambiente de pruebas que replique la configuración de producción y, una vez validadas, se aplican en ventanas de mantenimiento previamente comunicadas. Este procedimiento previene incompatibilidades, regresiones o interrupciones no planeadas.

Plan de continuidad operativa.

Se define un plan de continuidad que contempla la disponibilidad de la solución ante eventos de fallo en el servidor SIEM o SOAR. Este plan incluye la identificación de configuraciones de respaldo, los tiempos objetivos de recuperación (RTO) y de punto de recuperación (RPO), así como los procedimientos de activación de un entorno alternativo en caso de incidente mayor.

La aplicación rigurosa de este plan de aseguramiento permite que la solución SIEM + SOAR se mantenga, además de operativa, protegida frente a amenazas que pudieran comprometer su capacidad de detección y respuesta, preservando así la confianza depositada en ella como pieza central de la estrategia de ciberseguridad de la organización.

Plan de mantenimiento correctivo

El Plan Correctivo está diseñado para abordar fallos o problemas inesperados que puedan surgir en la solución SIEM + SOAR, garantizando una rápida restauración de la funcionalidad y minimizando los impactos en la operación. Este plan incluye las siguientes acciones:

Detección y Diagnóstico:

Implementar un sistema de alertas para identificar fallos en tiempo real.

Realizar un análisis detallado de logs de Wazuh y Shuffle para diagnosticar el origen del problema.

Procedimientos de Reparación:

Desplegar rápidamente configuraciones de respaldo en caso de fallos críticos.

Corregir errores en las integraciones API de Shuffle o reglas mal configuradas en Wazuh.

Actualizar o reinstalar componentes dañados o desactualizados, como agentes, servidores o indexadores.

Evaluación Post-Correctiva:

Verificar que la solución esté funcionando correctamente tras aplicar las correcciones.

Realizar pruebas de stress y rendimiento para asegurar que el sistema vuelva a su estado óptimo.

Documentar el incidente, su causa raíz y las acciones correctivas implementadas.

Gestión de Contingencias:

Mantener respaldos actualizados de configuraciones y datos en servidores seguros.

Asegurar redundancia en componentes clave, como nodos del indexador y servidores.

Capacitación del Personal:

Entrenar al equipo técnico en la resolución de problemas comunes.

Realizar simulacros de fallos para medir tiempos de respuesta y efectividad de las soluciones aplicadas.

Este plan busca garantizar que cualquier contingencia sea gestionada de manera eficiente, restaurando rápidamente la operación del sistema y previniendo la recurrencia de incidentes similares.

Plan de mantenimiento predictivo

El Mantenimiento Predictivo está orientado a anticipar posibles fallos y optimizar el rendimiento del sistema mediante el análisis regular de datos operativos clave. Este enfoque utiliza herramientas avanzadas de monitoreo y técnicas analíticas para identificar patrones de comportamiento anómalo en los sistemas y prevenir problemas antes de que se conviertan en fallos críticos.

Monitoreo de Variables Clave:

Rendimiento del Servidor: Supervisión constante del uso de CPU, memoria y almacenamiento en los servidores de Wazuh y Shuffle.

Tasa de Generación de Alertas: Detección de anomalías en el volumen de alertas para identificar configuraciones ineficientes o potenciales amenazas.

Estado de Conexión API: Verificación de la estabilidad y respuesta de las integraciones API en Shuffle.

Herramientas y Equipos:

Implementación de dashboards avanzados en el panel de control de Wazuh para seguimiento en tiempo real.

Uso de software analítico para procesar métricas y generar reportes automáticos.

Integración de herramientas de inteligencia artificial para identificar tendencias en los datos de monitoreo.

Análisis Periódico:

Realizar inspecciones técnicas mensuales de los logs y configuraciones del sistema.

Generar reportes de tendencias de rendimiento para detectar posibles puntos débiles.

Validar la integridad y consistencia de las bases de datos y archivos de configuración.

Acciones Preventivas Basadas en Datos:

Ajuste proactivo de reglas en Wazuh para mejorar la detección de amenazas.

Actualización anticipada de agentes en puntos finales antes de que alcancen su ciclo de vida operativo.

Escalado de recursos en caso de identificar tendencias de sobrecarga en el sistema.

Beneficios:

Minimización de tiempos de inactividad.

Incremento en la eficiencia operativa y la precisión en la detección de amenazas.

Extensión de la vida útil de los componentes del sistema mediante el monitoreo continuo.

Este plan predictivo combina inspección técnica avanzada con análisis de datos para garantizar un funcionamiento óptimo y prevenir interrupciones críticas.

Plan de mantenimiento preventivo

El Mantenimiento Preventivo tiene como objetivo prevenir fallas y mantener los sistemas en condiciones óptimas de operación mediante actividades periódicas planificadas. Este enfoque asegura que los equipos, dispositivos y configuraciones mantengan su confiabilidad y eficiencia en el tiempo, reduciendo la probabilidad de fallas inesperadas.

Frecuencia de Mantenimiento:

Realizar revisiones cada trimestre para garantizar la estabilidad y el rendimiento.

Programar tareas de mantenimiento durante períodos de baja carga para minimizar interrupciones.

Actividades Preventivas Clave:

Revisión de Configuración: Verificación de las reglas, decodificadores y configuraciones del servidor Wazuh para asegurarse de que estén actualizadas y funcionando correctamente.

Actualización de Software: Aplicación regular de parches de seguridad y actualizaciones en los componentes de Wazuh y Shuffle para garantizar compatibilidad y protección contra nuevas amenazas.

Validación de Conectividad API: Pruebas periódicas de la conexión API entre Shuffle y Wazuh para asegurar la comunicación fluida entre ambas plataformas.

Pruebas de Respaldo: Validar la integridad de las copias de seguridad y restaurar datos simulando escenarios de recuperación.

Inspección de Hardware: En caso de servidores físicos, comprobar estado de discos, ventiladores y fuentes de energía para evitar fallos físicos.

Documentación y Seguimiento:

Registro detallado de todas las actividades de mantenimiento realizadas.

Creación de reportes que incluyan hallazgos, mejoras aplicadas y recomendaciones para próximas inspecciones.

Beneficios:

Reducción significativa de fallas inesperadas.

Mayor confiabilidad y eficiencia en la detección de amenazas y la ejecución de flujos de trabajo automatizados.

Extensión de la vida útil de los sistemas mediante el monitoreo continuo y las correcciones proactivas.

Este plan preventivo asegura la estabilidad de los sistemas al mitigar riesgos y maximizar la confiabilidad de los componentes del proyecto.

Conclusiones

El desarrollo e implementación del prototipo SIEM + SOAR basado en software libre permitió diseñar una solución alineada al core del negocio de la empresa del sector eléctrico, mediante configuraciones específicas tales como el monitoreo de integridad sobre archivos críticos relacionados con diseños de sistemas de protección contra sobretensiones, reglas adaptadas a la detección de accesos no autorizados a información sensible de clientes con infraestructura eléctrica crítica, esquemas diferenciados de monitoreo dentro y fuera del horario laboral, y flujos automatizados de respuesta. Estas características demuestran que las herramientas de código abierto, además de ser viables económicamente, pueden ser personalizadas para responder a las particularidades operativas y de información de una PYME, contribuyendo de manera directa al cumplimiento del objetivo general del proyecto.

La caracterización del entorno tecnológico de la organización permitió identificar un nivel básico de madurez en ciberseguridad, ausencia de controles perimetrales especializados, gestión reactiva de incidentes y dependencia exclusiva de controles nativos del sistema operativo. A partir de este diagnóstico, fue posible definir requerimientos técnicos y funcionales precisos para la solución, garantizando que la arquitectura propuesta y los componentes seleccionados (Wazuh y Shuffle) respondieran a las brechas reales identificadas y no a un esquema genérico, dando cumplimiento al primer objetivo específico planteado.

La integración entre Wazuh y Shuffle, materializada mediante la configuración de webhooks, reglas de correlación y flujos de trabajo automatizados, demostró la viabilidad de articular tecnologías de código abierto en un ecosistema funcional de detección y respuesta. La centralización de eventos en el SIEM y la automatización de acciones desde el SOAR permitieron a la organización pasar de un esquema de gestión manual y dispersa a un modelo coordinado y orquestado, evidenciando el cumplimiento del segundo objetivo específico, relacionado con el diseño e implementación de la arquitectura.

La verificación funcional del prototipo confirmó que la solución opera de manera estable y coordinada, con capacidad efectiva de detección de eventos relevantes y ejecución automatizada de respuestas. La comparación entre el estado inicial de la organización y el estado posterior a la implementación evidenció mejoras concretas en visibilidad, tiempos de detección y respuesta, cobertura de monitoreo y formalización de políticas de seguridad. Estos resultados validan el cumplimiento del tercer objetivo específico, al demostrar la operatividad, estabilidad y capacidad de respuesta del sistema frente a incidentes de seguridad en la infraestructura de la empresa.

El proyecto sienta una base estructurada para futuras mejoras, tales como la incorporación de nuevas fuentes de eventos, la ampliación de reglas de correlación, el fortalecimiento de los flujos de respuesta automatizada y la evolución hacia modelos más avanzados de operación de seguridad, como los SOC virtuales o distribuidos. La integración lograda demuestra que, incluso en organizaciones con infraestructura

limitada, es posible adoptar arquitecturas alineadas con las tendencias actuales de ciberseguridad basadas en automatización, análisis centralizado y respuesta orquestada.

La adopción de soluciones de ciberseguridad basadas en software libre representa una alternativa viable y sostenible para las PYMEs del sector eléctrico y para organizaciones con características similares. La solución implementada contribuye a mejorar la gestión de riesgos, la continuidad operativa y la protección de los activos de información, al tiempo que ofrece un modelo replicable que puede ser adaptado por otras empresas con limitaciones presupuestales similares, fortaleciendo el ecosistema empresarial frente a amenazas cibernéticas cada vez más sofisticadas.

Referencias Bibliográficas

Anco. (20 de Febrero de 2024). *Anco*. Por qué el 75% de las empresas apuesta por el outsourcing IT?: https://anco.es/blog/outsourcing-informatico/

Baker, K. (4 de Marzo de 2025). *CrowdStrike*. Cyber Threat Intelligence Explained: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/

Cibersafety. (26 de Abril de 2025). *Cibersafety*. Las herramientas esenciales en un Centro de Operaciones de Seguridad (SOC): SIEM, SOAR, EDR, XDR, NGFW y más: https://cibersafety.com/herramientas-esenciales-soc/

Cibersafety. (24 de Noviembre de 2025). *Cibersafety*. Ingeniería de seguridad: cómo diseñar sistemas robustos, prevenir vulnerabilidades y elevar la protección en entornos tecnológicos modernos: https://cibersafety.com/ingenieria-de-seguridad-guia/

Cibersafety. (26 de Diciembre de 2025). *Cibersafety*. Ciberseguridad para pymes: la guía definitiva para proteger tu empresa en 2025–2026: https://cibersafety.com/ciberseguridad-pymes-guia-2025-2026/

Cyber8200. (2026). *Cyber8200*. SOAR vs. SIEM: Key Differences and Benefits Explained: https://www.cyber8200.com/en/blog/soar-vs-siem-key-differences-benefits

CyberSafety. (26 de Abril de 2025). *CyberSafety*. CyberSafety: https://cibersafety.com/herramientas-esenciales-soc/

Económica, L. N. (17 de Octubre de 2024). *La Nota Económica* . En Colombia el 91,8% de las empresas son PyMEs: https://lanotaeconomica.com.co/movidas-empresarial/en-colombia-el-918-de-las-empresas-son-pymes/

Elastic. (2025). *Elastic*. AI-driven SIEM that is: https://www.elastic.co/security/siem

Fortinet. (31 de Enero de 2026). *Fortinet*. Fortinet: https://www.fortinet.com/lat/resources/cyberglossary/what-is-cybersecurity

Hermann, K. (20 de Enero de 2025). *arxiv*. An Exploratory Study on the Engineering of Security Features: https://arxiv.org/abs/2501.11546

IBM. (2026). *IBM*. IBM QRadar SIEM: https://www.ibm.com/products/qradar-siem

IONOS, E. e. (9 de Enero de 2025). *IONOS Digital Guide*. IONOS Digital Guide: https://www.ionos.es/digitalguide/servidores/seguridad/que-es-siem/

Keepcoding. (12 de Junio de 2025). *keepcoding*. SIEM/SOAR: La dupla definitiva en ciberseguridad moderna: https://keepcoding.io/blog/siem-soar-en-ciberseguridad/

Kidd, C. (3 de Enero de 2025). *Splunk*. SIEM: Security Information & Event Management Explained: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html

Meidan, A. (8 de Octubre de 2025). *MDPI*. Security Requirements Engineering: A Review and Analysis: https://www.mdpi.com/2073-431X/14/10/429

Michelon, G. K. (21 de Marzo de 2023). *IEEE*. Analysis and Propagation of Feature Revisions in Preprocessor-based Software Product Lines: https://ieeexplore.ieee.org/document/10123456

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

Palo alto networks. (2026). *Paloalto Networks*. What is soar vs siem: https://www.paloaltonetworks.com/cyberpedia/what-is-soar-vs-siem

pyme, A. (7 de Agosto de 2024). *Acelera pyme*. ¿Qué es el SOAR y cómo te ayuda a mejorar la ciberseguridad?: https://www.acelerapyme.gob.es/novedades/pildora/que-es-el-soar-y-como-te-ayuda-mejorar-la-ciberseguridad

Rapid7. (2026). *Rapid7*. What is a purple team? : https://www.rapid7.com/fundamentals/what-is-a-purple-team/

Red Hat. (11 de Mayo de 2022). *Red Hat*. Red Hat: https://www.redhat.com/es/topics/security/what-is-soar

Shuffle. (17 de Enero de 2025). *Shuffle*. Architecture: https://shuffler.io/docs/architecture

Shuffler. (2024). *Shuffler*. Install: https://github.com/shuffle/shuffle/blob/main/.github/install-guide.md

Shuffler. (2024). *Shuffler*. Documentation: https://shuffler.io/docs

Taverner, J. L. (Diciembre de 2015). *ELSEVIER*. Razones y riesgos del outsourcing de sistemas de información en las grandes empresas españolas: https://www.elsevier.es/es-revista-revista-europea-direccion-economia-empresa-346-articulo-razones-riesgos-del-outsourcing-sistemas-S1019683815000177

Uetz, R. (19 de Diciembre de 2023). *arxiv*. Cornell University: https://arxiv.org/abs/2311.10197

Volle, A. (21 de Febrero de 2026). *Britannica*. free software: https://www-britannica-com.translate.goog/science/free-software

Wazuh. (27 de Abril de 2023). *Integrating Wazuh with Shuffle*. Integrating Wazuh with Shuffle: https://wazuh.com/blog/integrating-wazuh-with-shuffle/

Wazuh. (2024). *Wazuh*. Architecture: https://documentation.wazuh.com/current/getting-started/architecture.html

Wazuh. (2024). *Wazuh*. Getting Started: https://documentation.wazuh.com/current/getting-started/index.html

Yamit, H. (22 de Septiembre de 2025). *Repository UNAD.* Diseño esquema de detección de amenazas con software wazuh en las empresas Pymes en Bogotá Zona Centro: https://repository.unad.edu.co/jspui/handle/10596/70900?locale=es