Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTOR/ES:

Calahorrano Simbaña Andrés Esteban

Chávez Bazaran Stefany Belén

Défaz Toaquiza Diego Fernando

Freire Conrado Anthony Bryan

TUTOR/ES:

Alejandro Cortés López

Iván Reyes Chacón

Desarrollo e implementación de un laboratorio de detección de amenazas mediante una solución SIEM Open Source.

Quito - Ecuador

Junio – 2025

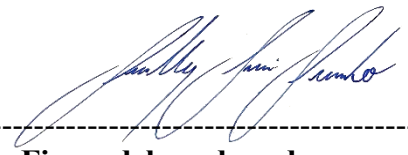
REINVENTEMOS EL FUTURO

Certificación de autoría

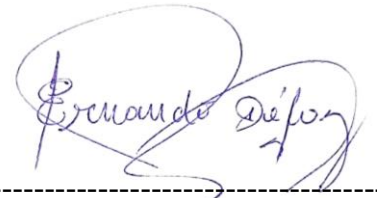
Nosotros, Chávez Bazaran Stefany Belén, Freire Conrado Anthony Bryan, Défaz Toaquiza Diego Fernando, Calahorrano Simbaña Andrés Esteban declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

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

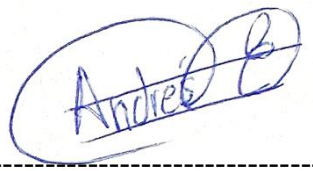
Firma del graduando
Chávez Bazaran Stefany Belén



Firma del graduando
Freire Conrado Anthony Bryan



Firma del graduando
Défaz Toaquiza Diego Fernando



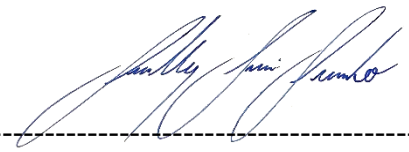
Firma del graduando
Calahorrano Simbaña Andrés Esteban

Autorización de Derechos de Propiedad Intelectual

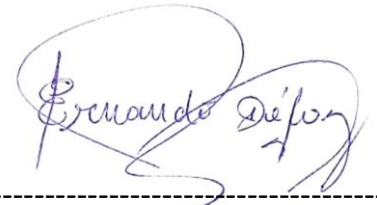
Nosotros, Chávez Bazaran Stefany Belén, Freire Conrado Anthony Bryan, Défaz Toaquiza Diego Fernando, Calahorrano Simbaña Andrés Esteban en calidad de autores del trabajo de investigación titulado Desarrollo e implementación de un laboratorio de detección de amenazas mediante una solución SIEM Open Source, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

Junio, 2025

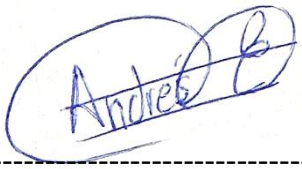
Firma del graduando
Chávez Bazaran Stefany Belén



Firma del graduando
Freire Conrado Anthony Bryan



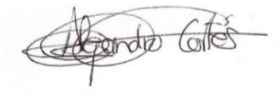
Firma del graduando
Défaz Toaquiza Diego Fernando



Firma del graduando
Calahorrano Simbaña Andrés Esteban

Aprobación de dirección y coordinación del programa

Nosotros, Alejandro Cortés e Iván Reyes, declaramos que: Chávez Bazaran Stefany Belén, Freire Conrado Anthony Bryan, Défaz Toaquiza Diego Fernando, Calahorrano Simbaña Andrés Esteban son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



_____

Alejandro Cortés L.

Maestría en Ciberseguridad

_____

Iván Reyes Ch.

Maestría en Ciberseguridad

DEDICATORIA

Dedicamos este proyecto a todas las personas que, de manera directa o indirecta, contribuyeron a su desarrollo. A nuestras familias, por su amor incondicional, su apoyo constante y por ser nuestro principal motor en los momentos de dificultad. A nuestros docentes, por guiarnos con paciencia, compartir sus conocimientos y fomentar en nosotros el compromiso académico. También agradecemos a cada persona que nos brindó una palabra de ánimo, una crítica constructiva o un gesto de apoyo. Este trabajo es reflejo del esfuerzo conjunto y de la confianza que muchos pusieron en nosotros durante cada etapa de este camino académico.

AGRADECIMIENTOS

Agradezco a mis padres que, con su esfuerzo, dedicación y trabajo, me han permitido forjarme como un profesional y como un ser humano capaz de superar las adversidades del día a día, sus palabras de aliento, su apoyo incondicional ha sido fundamental para elaborar este proyecto, agradezco también a mis compañeros por los desvelos, el esfuerzo compartido en cada reunión que me ha permitido generar un gran conocimiento y poder finalizar este trabajo. Calahorrano Simbaña Andrés Esteban

Agradezco a Dios por entregarme la oportunidad de ser mejor ser humano con la experiencia de cada día. Gracias a mis padres por ser mi constante motivación y haberme entregado con su ejemplo el valioso significado del trabajo honesto. Y mil gracias a mis hijas. Mis tres amores preciosos que han sido mi fuerza siempre para cada desafío en mi vida.

Défaz Toaquiza Diego Fernando

Agradezco sinceramente a mi familia por su amor, paciencia y apoyo incondicional durante todo este proceso. A los docentes y personas que compartieron su conocimiento con dedicación, gracias por su valiosa orientación.

Chávez Bazaran Stefany Belén

Este trabajo de fin de máster lo dedico a mis padres Edwin y Mónica, mi hermano Erick, mi abuelita Delia, a Joss y mi abuelito Gustavo que me observa desde el cielo. Este logro es gracias a todo el apoyo incondicional que me han dado durante este tiempo, sus fuerzas para seguir cada día adelante. Agradezco a mis compañeros de grupo que se han esforzado cada día y noche para poder cumplir con un objetivo en conjunto.

Freire Conrado Anthony Bryan

RESUMEN

La ciberseguridad se ha convertido en un pilar esencial para las empresas, debido a que la creciente digitalización de los servicios las ha vuelto un objetivo prioritario para grupos y actores maliciosos. En Ecuador, aunque existe un crecimiento de concientización, muchas organizaciones aún carecen de presupuesto y conocimientos necesario para adoptar soluciones de seguridad robustas. Ante esta situación, los sistemas SIEM (Security Information and Event Management) representan una herramienta clave para monitorear, correlacionar y responder ante posibles brechas de seguridad.

En respuesta a la problemática, desarrollar e implementar un sistema SIEM basado en herramientas Open Source, con el fin de brindar alternativas eficientes y de bajo costo, ayuda a mejorar la postura de seguridad ente posibles incidentes y brechas informáticas. Permitiendo la integración de múltiples fuentes de datos, herramientas de seguridad perimetral y feeds de ciberinteligencia, para proporcionar una visión global del estado de seguridad de la organización.

El proyecto se ejecuta en un entorno de laboratorio virtualizado que replica componentes esenciales de una red empresarial, basadas en código abierto y un SIEM que permite centralizar los logs, generar alertas y realizar correlaciones de eventos. Se realiza en un ambiente controlado basándose en criterio de viabilidad técnica y ética, permitiendo simular ataques, evaluar reglas de detección y ejecutar pruebas que puedan afectar y comprometer entornos productivos.

Palabras clave: Ciberseguridad, SIEM, Open Source, Ataques, Feeds, Ciberinteligencia.

ABSTRACT

Cybersecurity has become an essential pillar for businesses, as the increasing digitalization of services has made them a priority target for malicious groups and actors. In Ecuador, although awareness is growing, many organizations still lack the budget and knowledge necessary to adopt robust security solutions. Given this situation, SIEM (Security Information and Event Management) systems represent a key tool for monitoring, correlating, and responding to potential security breaches.

In response to this problem, developing and implementing an SIEM system based on open source tools, with the aim of providing efficient and low-cost alternatives, helps improve the security posture in the face of potential cyber incidents and breaches. It allows for the integration of multiple data sources, perimeter security tools, and cyber intelligence feeds to provide a comprehensive view of the organization's security status.

The project is executed in a virtualized laboratory environment that replicates essential components of an enterprise network, based on open source code and a SIEM that centralizes logs, generates alerts, and performs event correlations. It is carried out in a controlled environment based on technical and ethical feasibility criteria, allowing for the simulation of attacks, evaluation of detection rules, and execution of tests that could affect and compromise production environments.

Keywords: Cybersecurity, SIEM, Open Source, Attacks, Feeds, Cyberintelligence.

Tabla de contenido

Glosario de Términos de Redes y Ciberseguridad

Servidor DHCP (Dynamic Host Configuration Protocol)

Es un servidor que asigna automáticamente direcciones IP y otros parámetros de red (como puerta de enlace y DNS) a los dispositivos de una red, evitando la configuración manual en cada estación de trabajo.

IDS (Intrusion Detection System)

Sistema de detección de intrusos. Monitorea el tráfico de red en busca de comportamientos anómalos o actividades maliciosas, alertando a los administradores cuando detecta posibles ataques.

MISP (Malware Information Sharing Platform & Threat Sharing)

Plataforma de código abierto utilizada para el intercambio de información sobre amenazas (como malware, campañas de phishing, indicadores de compromiso).

LAN (Local Área Network)

Red de área local. Conjunto de equipos conectados entre sí como computadoras, impresoras, servidores y otros equipos dentro de un mismo espacio físico, como una oficina, edificio o campus.

WAN (Wide Area Network)

Red de área amplia. Conecta varias LANs en diferentes ubicaciones geográficas, como sucursales de una empresa. Utiliza enlaces públicos o privados (como Internet o enlaces dedicados).

DMZ (Demilitarized Zone)

Zona desmilitarizada. Área de la red donde se ubican servidores públicos (como web, correo, DNS) aislados tanto de la red interna como de Internet.

Máquina Virtual (VM – Virtual Machine)

Es un entorno de software que simula un equipo físico, permitiendo ejecutar sistemas y aplicaciones de forma aislada para pruebas, simulaciones, entornos seguros y laboratorios en ciberseguridad.

SOCAT (SOcket CAT)

Herramienta de línea de comandos que establece conexiones bidireccionales entre flujos de datos; se ejecuta para redirigir puertos, crear túneles, y depurar redes.

DoS (Denial of Service – Denegación de Servicio)

Ataque que busca saturar un servicio o servidor enviando una gran cantidad de solicitudes desde una única fuente.

DDoS (Distributed Denial of Service – Denegación de Servicio Distribuida)

Variante del ataque DoS en el que múltiples sistemas distribuidos (como una botnet) envían solicitudes simultáneamente a un objetivo.

APT (Advanced Persistent Threat – Amenaza Persistente Avanzada)

Tipo de ataque cibernético avanzado, ejecutado por individuos altamente calificados que intentan irrumpir en una red particular para sustraer datos confidenciales sin ser identificados.

Syslog

Protocolo estándar utilizado para enviar mensajes de registro (logs) de eventos del sistema a un servidor central.

SMB (Server Message Block)

Protocolo de red utilizado para compartir archivos, impresoras y otros recursos entre dispositivos dentro de una red.

Alerta Slack

Notificación automática enviada a través de la plataforma de mensajería **Slack**, para reportar eventos en tiempo real, incidencias o cambios en sistemas.

Webhook

Metodo que permite que una aplicación envíe datos automáticamente a otra en tiempo real mediante una URL receptora, que enruta peticiones HTTP.

Índice de Tablas

Índice de Figuras

Capítulo 1

Introducción

Definición del proyecto

En actualidad la ciberseguridad representa un papel primordial para las empresas, independiente de su rol de giro de negocio. Esto debido al gran volumen de datos que procesan y las constantes amenazas a las cuales se encuentran expuestas. Con el avance de la tecnología, las nuevas técnicas disruptivas, la necesidad de cumplir con las regulaciones y estándares de seguridad, es imprescindible contar con soluciones eficientes para la detección de amenazas.

Bajo este contexto, la implementación de un SIEM (Sistema de Gestión de Información y Eventos de seguridad, por sus siglas en inglés) se ha convertido en una estrategia clave para la mejora de visibilidad y respuesta ante incidentes de seguridad dentro de la infraestructura de las organizaciones. Permite la centralización, análisis y correlación de eventos provenientes de diversas fuentes integradas como sistemas de detección de intrusos (IPS/IDS), firewalls, servidores, endpoints y feeds, lo cual proporciona una visión integral del estado de seguridad de la organización.

Estas soluciones comerciales implican costos elevados que requieren de altas inversiones en presupuesto, mantenimiento y escalabilidad, lo que ha representado un desafío continuo para las organizaciones que han buscado fortalecer su postura de seguridad sin comprometer sus ingresos. Las herramientas Open Source representan una opción más viable, ofreciendo seguridad, flexibilidad, personalización y apoyo de la comunidad para el desarrollo continuo.

Con estas consideraciones, se busca proporcionar una alternativa eficiente a las soluciones SIEM convencionales y también contribuir al fortalecimiento de la seguridad en las empresas que buscan blindar su infraestructura mediante herramientas open source que proporcionen una detección cercana al tiempo real de incidentes de seguridad con costos reducidos.

Justificación e importancia del trabajo de investigación

La información es el activo digital más importante de toda compañía pues su valor es incalculable. Salvaguardar su integridad y disponibilidad es fundamental con buenas prácticas de seguridad que nos permitan establecer altos estándares de calidad y servicio que proporcionan prestigio y fortalecen la confianza de los clientes que entregan sus datos para diversas transacciones. Actualmente la tecnología está presente en todas las áreas de servicio que interactúa con la sociedad. Cualquier daño cibernético provocado por un delincuente u organización criminal hacia cualquier infraestructura podría comprometer servicios esenciales para el desempeño de las tareas como conectividad global a nivel de datos, llamadas telefónicas, SMS, pago de servicios, entre otros.

Las organizaciones con un alto porcentaje de automatización tecnológica son más vulnerables por la naturaleza de sus operaciones. Esto como consecuencia de que sus actividades encuentran en la primera línea de ataque en el ámbito de la Ciberseguridad. Mediante el desarrollo de un sistema SIEM basado en herramientas Open Source, se centralizará la gestión de eventos de seguridad, se recopilarán, analizarán y correlacionarán logs de múltiples fuentes integradas que proporcionan una visión holística del estado de seguridad de la empresa lo que permite la identificación temprana de patrones y comportamientos maliciosos.

Esta detección permitirá reducir el tiempo de respuesta a incidentes, minimizando los impactos del ataque y evitando la materialización del incidente de seguridad. De esta forma, evitamos que la reputación de la empresa se vea afectada, aseguramos que el servicio y atención a los clientes mantengan el mismo nivel de QoS (Calidad de servicio) adecuado. Adicionalmente, reducirá el costo de los sistemas ya que el desarrollo será con herramientas de Open Source, lo que eliminará la compra de licenciamiento asociado a soluciones comerciales, derivándose en un ahorro significativo en la inversión del presupuesto de seguridad sin afectar a la postura y desarrollo continuo de la protección de la empresa.

Alcance

Este proyecto busca fortalecer la capacidad de detección de amenazas y riesgos digitales que puedan corromper la información y dañar la infraestructura tecnológica. Para conseguirlo, se implementará un sistema SIEM basado en herramientas de código abierto, lo cual reducirá los costos de despliegue y paso a producción al no depender de soluciones comerciales con costo de licenciamiento por instalación, mantenimiento y almacenamiento.

El alcance del proyecto incluye:

- Implementación de un sistema SIEM utilizando herramientas de código abierto

Integración y configuración de las siguientes soluciones:

- Firewall
- Sistema de Detección de Intrusos (IDS)
- Integración de feeds de ciberinteligencia
- Recolección de registros (logs) de sistemas operativo Ubuntu
- Recolección de registros (logs) de sistemas operativo Windows
- Dashboard interactivo para el monitoreo de eventos

- Detección de vulnerabilidades
- Generación de alertas cercanas al tiempo real
- Canal de comunicaciones empresariales

Se desarrollarán casos de uso para cada integración mencionada, buscando situaciones reales que ayuden a detectar y detener los riesgos digitales. Estos ejemplos servirán para definir parámetros de control basados en variables como el tiempo y el volumen de actividad, lo que hará más fácil visualizar comportamientos sospechosos. También, se analizarán los ataques más comunes para entender las Tácticas, técnicas, Procedimientos, y se crearán modelos de ataque para mejorar la forma de prevenirlos y fortalecer la defensa activa.

El alcance no incluye:

- Integración con soluciones comerciales de seguridad.
- Mantenimiento continuo posterior a la entrega del sistema.
- Personalización avanzada del dashboard.
- Desplegar el sistema desarrollado en un entorno empresarial real.

Limitaciones:

- El proyecto se desarrollará exclusivamente con tecnologías Open Source.
- La implementación está sujeta a los recursos de hardware y red disponibles.

Objetivos

Objetivo General.

Establecer una solución SIEM basada en Open Source que permita centralizar, analizar y correlacionar eventos de seguridad con el fin de fortalecer la detección de amenazas y mejorar la respuesta ante incidentes en infraestructuras informáticas.

Objetivo Específico.

Evaluar herramientas Open Source adaptables con un SIEM que permitan integrar componente como firewall, IDS y sistemas de recolección de logs.

Configurar un sistema SIEM que centralice la información extraída de fuentes criticas como sistemas operativos, Firewall e IDS.

Integrar feeds de Threath Intelligence para optimizar la detección de amenazas, prevenir ataques mediante correlacionamiento de firmas de Indicadores de Compromiso.

Desplegar un dashboard interactivo que permita visualizar y monitorear en tiempo real los eventos de las fuentes integradas en el SIEM.

Ejecutar casos de uso para cada integración implementada en el SIEM simulando amenazas que ayuden a validar el rendimiento del sistema en la detección de incidentes.

Capítulo 2

Marco Teórico

Según el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST), define que una amenaza se entiende como cualquier situación o hecho que pueda causar un impacto negativo en las operaciones, los recursos, la reputación o las personas dentro de una organización, así como en otras entidades o incluso a nivel nacional, mediante el uso de sistemas de información. Esto puede suceder por filtración, alteración de datos o la interrupción de servicios, así como por la explotación exitosa de vulnerabilidades por parte de agentes maliciosos (National Institute of Standards and Technology, 2024).

Si bien esta definición abarca aspectos relacionados con los sistemas de información, no siempre diferencia claramente las ciberamenazas como una categoría específica. Esta noción se basa en los conceptos de amenaza establecidos por CNSSI 4009, FIPS 200 y el NIST SP 800-30, con el fin de proporcionar una visión más completa y precisa de los riesgos que comprometen la seguridad de la información (National Institute of Standards and Technology, 2024).

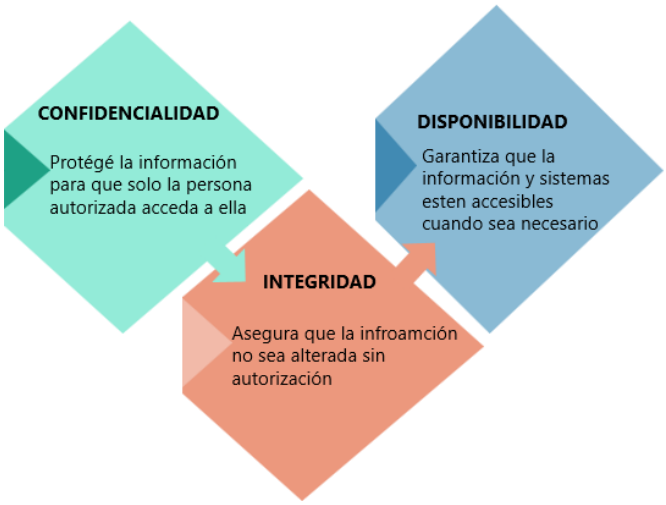
Pilares de la Seguridad Informática

Para confrontar estos desafíos cibernéticos, se debe basar en los pilares de la seguridad de la información, los cuales aseguran que la información sensible y la infraestructura de las entidades se encuentren seguras y estén resguardadas contra amenazas (Osazuwa, O. M. C., 2023).

Tener conocimiento de estos pilares es importante para cualquier empresa, ya que comprenderlos permite diseñar un proyecto de seguridad e implementar un SIEM. Esta herramienta no es una tecnológica común, sino es una pieza central para gestionar y responder riesgos en un tiempo real, basado en:

Figura 1

Pilares Seguridad de la Información



Nota: Definición de los pilares Seguridad Informática. Elaboración propia

Por este motivo, se implementan los pilares de seguridad informática:

- Confidencialidad: Se basa en resguardar la privacidad de los datos ya asegura que la información este seguro frente posibles ciberataques. Herramientas como el cifrado, la autenticación multifactorial es para asegurar la información dentro de las instituciones (Mitchell, 2023).
- Integridad: Ayuda a prevenir modificaciones no autorizadas de la información, asegurando que los datos se conserven en su estado original (Osazuwa, O. M. C., 2023).
- Disponibilidad: Permite que los sistemas y datos sean accesibles para los usuarios autorizados en todo momento, evitando perdidas o interrupciones original (Osazuwa, O. M. C., 2023).

Gestión de Información y Eventos de Seguridad

Un SIEM es una herramienta clave en la defensa cibernética moderna, ya que permite registrar, correlacionar y analizar eventos de seguridad en tiempo real desde múltiples fuentes. Esta capacidad mejora significativamente la visibilidad sobre la infraestructura de TI y facilita el cumplimiento normativo, como el Reglamento General de Protección de Datos (RGPD), al centralizar los registros y detectar accesos indebidos o posibles fugas de información. No obstante, su efectividad requiere una actualización continua de reglas, configuraciones y firmas, para adaptarse a los cambios organizacionales y al creciente nivel de sofisticación de los ciberataques actuales (Cybersecurity and Infrastructure Security Agency, s. f.).

La detección temprana y la correlación inteligente de eventos son fundamentales para mitigar amenazas cibernéticas. Un SIEM puede identificar patrones anómalos y comportamientos sospechosos mediante el análisis centralizado de logs, el monitoreo de integridad, la evaluación de vulnerabilidades y la integración con otras herramientas de seguridad. Esto permite detectar y responder rápidamente a ataques como malware, fuerza bruta, accesos no autorizados, escalamiento de privilegios o amenazas a aplicaciones web. De este modo, se refuerza la seguridad de la organización, se minimizan los riesgos operativos y se resguardan los activos antes de que se produzca un incidente significativo (Cybersecurity and Infrastructure Security Agency, s. f.).

Componentes clave de un SIEM

Una solución SIEM está compuesto de diferentes elementos que permiten a los equipos de seguridad identificar fugas de información, comportamientos maliciosos, monitorear y analizar continuamente dispositivos y eventos en la red, estos pueden identificarse de la siguiente manera (Areitio Bertolín, 2019):

Recogida centralizada de logs:

La captura de logs en un sistema SIEM es fundamental para recopilar información apropiada proveniente de varias fuentes, como servidores, routers, firewalls, entre otros. Esta captura puede llevarse a cabo de dos maneras: pasiva, cuando las fuentes envían directamente los logs al SIEM, o activa, cuando el SIEM extrae los registros directamente desde las fuentes utilizando técnicas como consultas WMI, RPC, SCP o acceso a bases de datos. Las acciones sobre logs son (Areitio Bertolín, 2019):

- **Evaluación basada en expresiones regulares:** Divide en campos los elemento que integran un log.
- **Normalización:** Asigna campos de identificación y los separa en el log mediante un parseo.
- **Categorización:** Clasifica, identifica y prioriza los eventos entrantes.
- **Agregación:** Agrupa eventos que aparecen en un periodo de tiempo definido y cuenten con campos iguales.
- **Filtrado:** Optimiza el volumen de logs que llegan a un SIEM en base a condiciones establecidas por el usuario.

Correlación en tiempo real de eventos/logs

Hace referencia al vínculo lógico que se establece entre dos o más sucesos u operaciones que ocurren dentro de un mismo sistema o entre diferentes dispositivos. Este proceso es fundamental para identificar acciones que podrían representar amenazas o comportamientos fuera de lo común dentro de una infraestructura tecnológica. La detección se realiza a partir de reglas previamente definidas, las cuales se aplican sobre registros o logs generados por los sistemas, permitiendo identificar patrones sospechosos o inconsistentes (Areitio Bertolín, 2019).

Este componente incluye la recepción y recopilación de eventos, su almacenamiento temporal en bases de datos y la creación de eventos correlacionados. Además, facilita la notificación de incidentes y proporciona herramientas para el análisis posterior mediante consultas o búsquedas (Areitio Bertolín, 2019).

Almacenamiento

El componente de almacenamiento de logs en un SIEM implica comprimir y firmar los eventos mediante una función hash al momento de escribirlos en disco, garantizando así su integridad. Se encarga de conservar estos registros y permite verificar si han sido alterados posteriormente. El almacenamiento puede ser local o externo, y clasificarse como online (acceso inmediato) u offline (requiere recuperación previa). Sus licencias suelen basarse en la cantidad de datos ingestados por día o en la tasa de número de eventos por segundo (EPS) (Areitio Bertolín, 2019).

Rol de las plataformas SIEM en la ciberseguridad.

El SIEM cumple una función crucial en la ciberseguridad al centralizar y analizar los datos de seguridad generados por diversos sistemas dentro de una red (Sreekanth, 2025).

Figura 2

Rol de soluciones SIEM

Nota: La imagen presenta las funciones clave de un sistema SIEM, resaltando su capacidad para detectar amenazas en tiempo real, responder a incidentes, cumplir con normativas y ofrecer una visión centralizada mediante la correlación y análisis de registros, Elaboración propia.

Esta centralización permite obtener una visión unificada de la actividad en la infraestructura tecnológica, facilitando la detección de comportamientos anómalos y patrones que podrían indicar intentos de intrusión, accesos no autorizados o actividades maliciosas (Sreekanth, 2025).

Tipos de Software SIEM

Tabla 1

Características de diferentes Software SIEM

Software SIEM	Características
SIEM Local	Instala y gestiona en la propia infraestructura, ofreciendo mayor control y personalización, aunque con altos costos.
SIEM basado en la Nube	Gestionada y mantenida por el proveedor, no requiere instalación ni mantenimiento de hardware ni software y ofrecen mejores funcionalidades
SIEM híbrido	Combina infraestructura local y servicios en la nube, ofreciendo un equilibrio entre control, escalabilidad y costos. Es adecuado para organizaciones que necesitan flexibilidad.

Nota: Según palo alto estas son las características para considerar en un software SIEM (Palo Alto Networks, s.f.).

Tendencias actuales y futuras del SIEM

Las empresas se centran en soluciones SIEM no solo como apoyo en la detección de amenazas y el cumplimiento de regulaciones, sino también parte de una estrategia de gestión de riesgos más amplia. Esto ha contribuido el interés por sistemas SIEM más avanzados, capaces de integrarse con otras herramientas de seguridad y ofrecer una visión completa del entorno (Maayan & Maayan, 2024).

Tabla 2

Tendencias SIEM para futuros años

Tendencia	Características
Integración con IA y aprendizaje automático	Facilita la identificación de amenazas sofisticadas y mejora la capacidad de respuesta ante incidentes. La inteligencia artificial y el aprendizaje automático posibilitan la automatización del análisis de grandes cantidades de datos de seguridad

Análisis del comportamiento del usuario (UBA)	Utiliza análisis avanzados para detectar conductas o actividades inusuales que podrían ser una amenaza para la seguridad. Esta tecnología está orientada a identificar amenazas internas y cuentas que hayan sido comprometidas.
Soluciones SIEM nativas de la nube	Ofrece escalabilidad, flexibilidad y detección de amenazas en tiempo real.
Automatización y orquestación de la respuesta a incidentes (SOAR)	Activas acciones de respuesta automatizadas permitiendo la optimización de las operaciones y reduce el tiempo de resolución

Nota: Según artículos de tendencias en crecimiento tecnológico se presentó la tabla con las características de mejora (Maayan & Maayan, 2024), (Leyden, 2025).

Controles Críticos – SIEM

Los controles se automatizan a partir de la información obtenida a través del SIEM, que proporciona una respuesta más rápida ante posibles incidentes. Se presentan los controles críticos, los cuales ofrecen una visión integral de las principales funcionalidades (Centro Nacional de Ciberseguridad, 2020):

Tabla 3

Top 5 de Controles Críticos en un SIEM

Control Crítico	Relación con herramientas SIEM
Registró de dispositivos autorizados y bloqueado	Utiliza un repositorio que registra los activos autorizados brindando mejor identificación de posibles amenazas.
Análisis de vulnerabilidades y parcheo	Capacidad de integrar las vulnerabilidades detectadas con el comportamiento del sistema para identificar si existe afectación
Configuraciones robustas para hardware y software	SIEM tiene la capacidad de reportar cuando existe mala configuración e incluso se presentan como error.
Control puertos, protocolos y servicios de una red	Puede alertar la existencia de puertos, protocolos o servicios que no están autorizados.
Monitorización de perdida de datos	Capacidad de recibir informes sobre incidentes de pérdida de datos para su análisis y correlación.

Nota: Según artículos controles críticos se presentó la tabla con las relaciones en un SIEM (Centro Nacional de Ciberseguridad, 2020).

Principales vectores de ataque detectados por un SIEM

Un vector de ataque se refiere al método o camino utilizado por un atacante para infiltrarse en un sistema informático, ya sea aprovechando vulnerabilidades técnicas, fallos de configuración o técnicas de ingeniería social.

A continuación, te presento los principales vectores de ataque que puede detectar un sistema SIEM (Katherine, 2024), (Bitso Colombia, 2023):

Ataque de fuerza bruta: Analiza el registro de aprobación para sistemas operativos y aplicaciones para identificar modelos que consisten en repetidos intentos de acceso no autorizados, como varios errores de inicio de sesión en cortos períodos de tiempo.

Accesos no autorizados: Monitorea actividades vinculadas con la autenticación y modificaciones en archivos o directorios esenciales, lo que facilita la identificación de ingresos fuera del horario normal, conexiones desde ubicaciones inusuales o usuarios que intentan acceder a recursos sin la autorización correspondiente.

Escalamiento de privilegios: Utiliza reglas específicas de análisis de logs, la plataforma detecta comandos vinculados a técnicas de ataque, como herramientas de red, escalamiento de privilegios, manipulación de procesos o intentos de obtener acceso administrador desde cuentas no autorizadas.

Modificaciones no autorizadas en archivos del sistema: Su módulo monitoreo de integridad de archivos identifica modificaciones, eliminaciones o incorporaciones en archivos clave del sistema, lo que podría señalar una intrusión en curso o una fase posterior a la explotación.

Detección de vulnerabilidades en software: Mediante el escaneo de configuraciones y versiones de software instalado en los sistemas, identifica posibles debilidades que podrían ser utilizadas como punto de entrada por un atacante.

Cómo los vectores de ataque pueden desencadenar incidentes de Ransomware

Los vectores de ataque son cruciales en la propagación y ejecución de incidentes de ransomware. En el marco de referencia MITRE ATT&CK, estos vectores están vinculados a diferentes etapas del ataque. A continuación, se describe cómo los vectores de ataque mencionados previamente pueden desencadenar un incidente de ransomware (*MITRE ATT&CK®*, s. f.), (*Kaspersky Official Blog*, 2025):

Tabla 4

Vectores de Ataque - Incidente de Ransomware

Vector de Ataque	Desencadenar un incidente de ransomware
Ataque de fuerza bruta	Según el marco MITRE ATT&CK Brute Force (T1110) es cuando un atacante puede recurrir a técnicas para acceder a sistemas mediante el Protocolo de Escritorio Remoto (RDP). Si las contraseñas en la red son poco seguras, el atacante puede intentar múltiples combinaciones hasta dar con la correcta, lo que le permitiría comprometer el sistema y desplegar el ransomware.
Accesos no autorizados	Según el marco MITRE ATT&CK, existen diversas formas de obtener accesos no autorizados, como el uso de fuerza bruta, ataques de phishing, explotación de aplicaciones expuestas públicamente, y la utilización de credenciales válidas previamente robadas. Estos métodos son esenciales en los ataques de ransomware, ya que constituyen el punto de entrada al sistema o red objetivo.
Escalamiento de privilegios	Es uno de los vectores de ataque modelado en el MITRE ATT&CK Framework. Una vez que un atacante obtiene acceso inicial, su siguiente objetivo es elevar sus privilegios para poder controlar más partes del sistema, desactivar defensas, o propagar el ataque.
Modificaciones no autorizadas en archivos del sistema	Dentro del MITRE ATT&CK Framework, este tipo de actividad se asocia principalmente con las siguientes técnicas y sub-técnicas, clasificadas según su propósito (Persistencia (T1547, T1546), Evasión de defensas

	(T1036, T1055), y Escalamiento de privilegios (T1569, T1574))
Detección de vulnerabilidades en software	En el contexto del MITRE ATT&CK Framework, esta actividad está más alineada con las tácticas de reconocimiento y descubrimiento, aunque no sea una técnica específica del atacante como tal.

Nota: Fuentes de información para detectar como puedes desencadenar un ransomware (*MITRE ATT&CK®*, s. f.), (*Kaspersky Official Blog*, 2025).

Inteligencia de Amenazas

Es un campo fundamental en el sector de la ciberseguridad, enfocada en reunir, examinar y utilizar información pertinente acerca de posibles riesgos cibernéticos. Este procedimiento abarca la obtención de datos de diferentes orígenes, como registros de vulnerabilidades, comunidades de hackers y reportes de incidentes de seguridad, con el fin de examinarlos y encontrar patrones y tendencias que pueden poner en peligro la integridad de los sistemas informáticos (Ramírez Quevedo, 2024).

Este procedimiento se alimenta de múltiples orígenes, incluyendo registros de seguridad, reportes de inteligencia sobre amenazas, investigaciones de malware y actividades de piratería. Al estudiar esta información, se pueden identificar amenazas nuevas y tomar precauciones para prevenir ciberataques (Ramírez Quevedo, 2024).

Se genera a partir del análisis de información proveniente de diversas fuentes (Ramírez Quevedo, 2024):

- Herramientas de seguridad como firewalls, sistemas para detectar intrusiones y software antivirus.
- Información de acceso público, como artículos de noticias, publicaciones en redes sociales y discusiones en foros.

- Fuentes privadas como proveedores de servicios de seguridad y organizaciones especializadas en inteligencia

Fuentes Internas de Inteligencia

Estas fuentes son esenciales, ya que proporcionan una perspectiva directa sobre los sistemas, los usuarios y las acciones que podrían ser blanco de ataques (De Pablo Bobadilla, 2024).

Las fuentes internas abarcan (De Pablo Bobadilla, 2024):

Registro de eventos de seguridad (logs): Los logs de eventos de seguridad aportan una valiosa fuente de información que puede indicar comportamientos atípicos o intentos de acceso no autorizado.

Monitoreo de Red: Las herramientas de supervisión de red facilitan a las organizaciones el seguimiento del tráfico y las comunicaciones en su sistema. Cualquier irregularidad, como un incremento repentino en el tráfico o conexiones desde lugares inusuales, puede ser un indicador de una amenaza potencial.

Alertas y notificaciones: Las soluciones de seguridad aplicadas en la institución, como firewall, sistemas de detección de intrusos (IDS) y programas antivirus, generan alertas cuando se identifica un comportamiento extraño.

Fuentes Externas de Inteligencia

Las fuentes externas de información sobre inteligencia se originan fuera de la entidad y son cruciales para captar una comprensión más amplia del escenario de riesgos (De Pablo Bobadilla, 2024).

Estas fuentes abarcan (De Pablo Bobadilla, 2024):

Threat Intelligence Feeds: Se trata de intercambio y recolección de información que brindan datos actualizados sobre amenazas reconocidas, incluyendo indicadores de compromiso, métodos de ataque y vulnerabilidades que han sido aprovechadas.

Comunidad y redes de información compartida: Contribución con otras entidades e involucrarse en comunidades de intercambio de datos.

Servicios de inteligencia comercial: Entidades ofrecen un servicio personalizado y con acceso a información que sería complicada de conseguir por otros medios.

Estado del Arte

Indicadores de ransomware y su impacto en el contexto ecuatoriano

El ransomware, un ataque cibernético en el que los atacantes encriptan los archivos de una víctima y exigen un pago para liberarlos, representa un riesgo significativo para las empresas y tiene graves implicaciones si se lleva a cabo con éxito. En Ecuador, este tipo de crimen ha crecido, impactando tanto a personas como a organizaciones gubernamentales y empresas (Lumu Technologies, 2024)

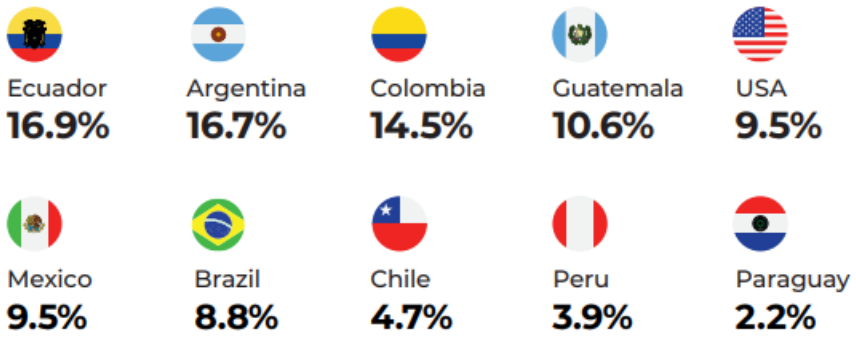
Este año, se ha observado un incremento considerable en la actividad de varias familias de ransomware, siendo el ransomware Cuba el más detectado, representando el 23,3 % de los incidentes. Le siguen el ransomware Blacksuite (Royal) y Conti, que continúan siendo amenazas persistentes. Sin embargo, se ha observado una tendencia favorable, ya que las detecciones de Lockbit han disminuido después de su desmantelamiento a principios de 2024, descendiendo a la sexta posición (Lumu Technologies, 2024).

Distribución de ataques de ransomware por país

Los ataques de ransomware han sido reportados tanto en América del Norte como del Sur. Ecuador, Argentina, Colombia, Guatemala, Estados Unidos y México fueron los seis países donde se registró el mayor número de incidentes de ransomware (Lumu Technologies, 2024).

Figura 3

Porcentaje de Ataques Ransomware por País



Nota: Según LUMU, el porcentaje de ataques por país revela que el año pasado, Ecuador experimentó una mayor exposición o vulnerabilidad ante este tipo de amenazas (Lumu Technologies, 2024).

Software y sus funcionalidades

El software es un conjunto de programas, procedimientos, reglas y datos diseñados para cumplir funciones específicas. Sus características se agrupan en componentes principales que definen su operatividad y funcionalidad. Sin embargo, existen tipos de software cuyo uso está condicionado por licenciamientos o costos obligatorios, lo que significa que una persona o entidad posee derechos exclusivos sobre él. Esto limita el libre acceso, el análisis, la modificación, la publicación de resultados y la distribución libre del software (Geeks for Geeks, 2024).

El software tiene las siguientes funcionalidades (Geeks for Geeks, 2024):

- Almacenamiento y recuperación de datos
- Procesamiento y manipulación de datos
- Interfaz de usuario y navegación
- Comunicación y redes
- Seguridad y control de acceso

Software Libre

De acuerdo con Julia Uriarte, se refiere a programas informáticos que otorgan a los usuarios la libertad de modificar, copiar, adaptar y distribuir su código fuente sin restricciones haciendo posible la creación de numerosas versiones personalizadas del software (Uriarte, J. M., 2019).

Es importante mencionar que el software libre no significa gratuito, aunque existan muchas versiones que pueden obtenerse sin costo al decir libre hace referencia de su uso y mejora del software por parte de sus usuarios (Uriarte, J. M., 2019).

El software libre está determinado por la presencia de cuatro libertades significativas basadas en los principios establecidos por Richard Stallman (Uriarte, J. M., 2019):

- Libertad de uso: Pueden ejecutar el programa para cualquier propósito que deseen.
- Libertad de estudio: Posibilidad de examinar el funcionamiento del software y modificar su código fuente según las propias necesidades o preferencias.
- Libertad de distribución: Derecho de compartir libremente copias del programa con otros.
- Libertad de mejora: Ejecutar cambios en el software, corregir errores y desarrollar

nuevas funcionalidades o soluciones.

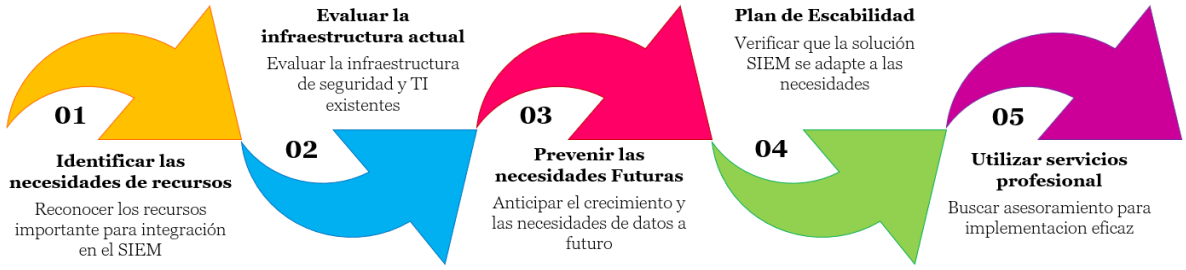
Uso de soluciones SIEM de código abierto en entornos corporativos

Un SIEM es una plataforma que unifica herramientas de seguridad para recopilar, correlacionar y analizar datos de registros provenientes de toda la infraestructura TI de una organización, permitiendo a los equipos de seguridad detectar amenazas, gestionar incidentes en tiempo real y obtener una visión centralizada y detallada del entorno de ciberseguridad (Sreekanth, 2025).

Las soluciones SIEM de Open Source son una opción ideal para las empresas que desean mejorar su ciberseguridad de manera rentable. Este tipo de software reduce los costos asociados a licencias y brinda la oportunidad de probar y analizar las funciones clave de seguridad antes de hacer una inversión definitiva (Sreekanth, 2025).

Figura 4

Implementación de SIEM Open Source



Nota: La imagen presenta los pasos esenciales para una implementación eficaz de un sistema SIEM, destacando la importancia de alinear la solución con las necesidades de la organización y considerar apoyo profesional para garantizar una integración efectiva, Elaboración propia.

Ventajas y Desventajas de un SIEM Open Source

Según Orozco Lara, Molina Miranda, Bonilla Alejandro y Ramírez Marcillo (2024) Los sistemas SIEM Open Source son capaces de manejar una cantidad ilimitada de usuarios y

datos, lo que les permite escalar fácilmente y contar con el respaldo de la comunidad tecnológica.

Tabla 5

Ventajas y Desventajas de un SIEM OpenSouce

Ventajas	Desventajas
Bajo costo de adquisición	Alta complejidad de implementación
Personalización y flexibilidad	Documentación limitada
Transparencia del código fuente	Soporte limitado
Actualizaciones frecuentes por la comunidad	Mayor tiempo de configuración inicial
Capacidad de integración con otras herramientas libres	Mayor tasa de falsos positivos si no se afina correctamente

Nota: Si bien no son ideales para todas las organizaciones debido a la necesidad de personal técnico altamente capacitado y a los posibles desafíos en el cumplimiento de normativas que exigen software certificado, no deben descartarse por completo (Orozco Lara, F. R., Molina Miranda, M. F., Bonilla Alejandro, S. B., & Ramírez Marcillo, J. L. ,2024).

Las soluciones SIEM de código abierto pueden ser viables para las empresas, siempre que se apliquen con un enfoque adecuado. Estas herramientas pueden servir como base útil para definir necesidades, evaluar funcionalidades y orientar la elección de soluciones comerciales más robustas (Orozco Lara, F. R., Molina Miranda, M. F., Bonilla Alejandro, S. B., & Ramírez Marcillo, J. L. ,2024).

Análisis comparativo de soluciones SIEM de código abierto

Impulsadas por la necesidad de soluciones rentables y personalizables, muchas empresas están adoptando plataformas SOC de Open Source como alternativas a los

productos propietarios. Estas herramientas no solo ofrecen capacidades sólidas y escalables, sino que también permiten adaptar las operaciones de seguridad a las necesidades específicas de cada organización. Sin embargo, a pesar de sus beneficios en términos de costo y flexibilidad, estas plataformas enfrentan algunos retos, especialmente en lo que se refiere a la integración de innovaciones impulsadas por inteligencia artificial (Astrid, 2024).

Tabla 6

Cuadro comparativo de OPEN SOURCE

Criterio	Peso (%)	Wazuh	Security Onion	Elastic Stack + Seguridad
Monitorización de la red	12%	4.5	5	3.5
Facilidad de despliegue y gestión	10%	4.5	3.5	3
Tecnología de IA avanzada	13%	4.5	3	5
Protección de endpoints y hosts	12%	4.5	3.5	4
Análisis y visualización	12%	4.5	4	5
Escalabilidad y flexibilidad	13%	5	4	5
Integración con otras herramientas	12%	5	4	4.5
Costo y accesibilidad	12%	5	4	3
Total	**100%**	**4.61**	**4.08**	**4.25**

Nota: La tabla compara tres soluciones SIEM según criterios técnicos y operativos esenciales, asignando puntajes ponderados para evaluar su desempeño general. Se destaca a Wazuh como la opción con mayor puntuación total en esta evaluación comparativa, Security Onion Solutions LLC (2024), (Wazuh Documentation, 2024), (Elastic N.V., 2024).

Wazuh (Puntaje total: 4.61): Es la alternativa más equilibrada, que se distingue por su facilidad de implementación, protección de endpoints e integración con otras herramientas. También proporciona una gran escalabilidad y tiene un costo accesible. Su limitación está en la tecnología de IA avanzada, donde se destaca tanto en comparación con otras opciones (Wazuh, 2024)

Security Onion (Puntaje total: 4.08): Es la opción más sobresaliente en el área de monitoreo de la red. Sin embargo, presenta fallas en cuanto a la facilidad de gestión y el uso de tecnologías avanzadas de IA, lo que puede complicar su análisis de implementación y predicción. Es una alternativa efectiva para centrarse en la seguridad de la red, pero más estructurada de manejar (Security Onion Solutions LLC, 2024)

Elastic Stack + Seguridad (Puntaje total: 4.25): Se distingue por su tecnología avanzada y visualización de IA, siendo ideal para entornos que valoran la automatización de amenazas y la visualización detallada. No obstante, presenta un elevado costo y es más complicada de implementar y administrar (Elastic N.V., 2024).

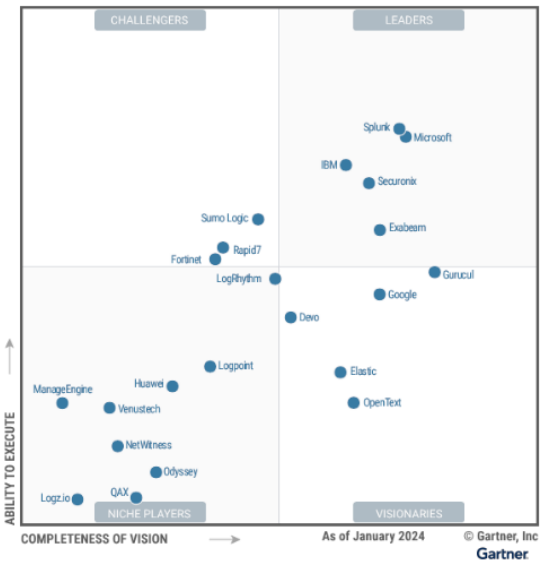
En este contexto, Wazuh se destaca por su flexibilidad, la capacidad de escalar y la capacidad de integrarse con entornos SOC, brindando una solución poderosa y económica.

Evaluación de soluciones SIEM según Gartner

De acuerdo con el informe *Magic Quadrant for Security Information and Event Management* de Gartner, publicado el 8 de mayo de 2024, Wazuh no aparece incluido en el cuadrante de evaluación. El informe clasifica a proveedores como IBM, Microsoft, Google y ManageEngine en distintas categorías, basándose en su habilidad para ejecutar y en la solidez de su visión estratégica (Fortinet, 2024).

Figura 5

Cuadrante mágico Gartner



Aunque Wazuh no fue incluido en el informe mencionado, en 2023 fue reconocida como la "Mejor Solución SIEM" por los SC Awards, gracias a su enfoque de código abierto que integra capacidades de SIEM y XDR. También cuenta con una calificación promedio de 4.5 estrellas en Gartner Peer Insights, basada en 22 opiniones de usuarios, lo que refleja una alta satisfacción (Gartner, s.f.).

Wazuh es una plataforma de seguridad adoptada a nivel mundial para salvaguardar la información en entornos locales, sistemas virtualizados, contenedores y arquitecturas en la nube. Su desarrollo es impulsado por una comunidad dinámica de código abierto que contribuye de forma continua a su desarrollo evolución (Gartner, s.f.).

Wazuh como herramienta SIEM

Después de evaluar las soluciones disponibles en el mercado y tener en cuenta la restricción de que no había costo financiero en esta etapa inicial, se decidió excluir todas las opciones comerciales. Además, era necesario un sistema que pudiera correlacionar información de varias fuentes, como firewalls, Proxy, IPS y y también pudiera recopilar datos

directamente de feeds de ciberinteligencia, Por lo tanto, tanto, Wazuh fue seleccionado como la herramienta principal para la recopilación y el análisis de registros. Esta plataforma de código abierto une la capacidad de XDR (detección y respuesta extendida) y SIEM (gestión de eventos e información de seguridad) al trabajar con Elastic Stack para brindar una defensa integral contra amenazas en entornos locales, virtuales, en contenedores y en la nube (Wazuh, 2024).

La arquitectura de Wazuh se basa en agentes de seguridad que se colocan en los sistemas que están bajo vigilancia, además de un servidor central que agrupa y estudia la información producida, lo que facilita una supervisión extensa y una respuesta rápida ante situaciones de seguridad (Wazuh, 2024).

Importancia de Wazuh en Ciberseguridad.

Wazuh como sistema de gestión de información y medidas de seguridad obtienen una serie de beneficios importantes (Manzoor et al., 2024):

Detección Anticipada: Wazuh reconoce y notifica sobre conductas sospechosas o dañinas en tiempo real, lo que posibilita que los equipos de seguridad actúen de manera rápida frente a las amenazas antes de que provoquen alguna perdida de información.

Correlación de Incidentes: Al integrar y examinar datos provenientes de diferentes fuentes, Wazuh puede vincular incidencias que parecen no estar relacionadas y generar alertas exactas, disminuyendo así los falsos positivos.

Cumplimiento Normativo: Wazuh ayuda a cumplir con normativas de seguridad y regulaciones al registrar y revisar actividades, lo que apoya en demostrar que la infraestructura se ajusta a los requerimientos.

Visualización y Generación de Informes: Kibana proporciona una visualización clara y personalizable de eventos de seguridad facilitando a los analistas tener revisiones exhaustivas y obtener comprensión más profunda del contexto de las amenazas.

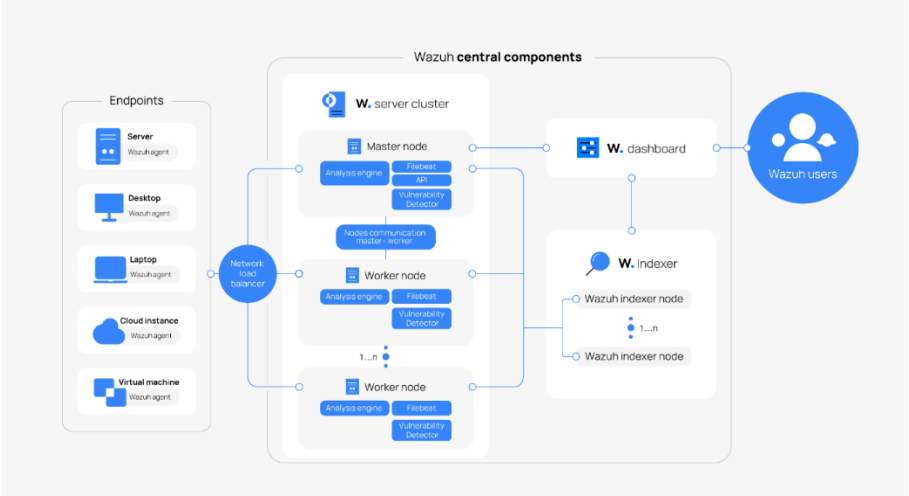
Flexibilidad y Adaptación: Wazuh ofrece una gran flexibilidad y se adapta a los requerimientos específicos de cada empresa mediante la creación de reglas y configuraciones personalizadas.

Arquitectura técnica de Wazuh como plataforma SIEM Open Source

La arquitectura de Wazuh se fundamenta en agentes que operan en los dispositivos finales que se supervisan y que envían información de seguridad a un servidor principal. También se permiten dispositivos que no tienen agentes, como firewalls, conmutadores, enrutadores y puntos de acceso, los cuales pueden transmitir información de registros de manera activa a través de Syslog, SSH o su API. El servidor principal interpreta y examina los datos que recibe y luego envía los resultados al indexador de Wazuh para su organización y almacenamiento (Wazuh, 2024), (SafeNet, 2023).

Figura 6

Arquitectura de Wazuh



Nota: Los elementos clave son el Wazuh Manager (o Wazuh Server), el Wazuh Indexer y el Wazuh Dashboard (Kibana). Todos estos elementos tienen una función significativa en la solución SIEM que ofrece Wazuh. Además, en cada uno de los dispositivos que se van a supervisar o Endpoint se instala un agente que se comunica con el servidor o clúster central (Wazuh, 2024), (SafeNet, 2023).

Wazuh Manager (Wazuh Server): Es un componente fundamental del sistema, encargado de recolectar, examinar e identificar eventos de seguridad al instante. Recibe información de los agentes que están instalados en los sistemas bajo supervisión, utiliza normas de detección para señalar amenazas y produce notificaciones (Kumar & Biju, 2023).

Wazuh Indexer (Elasticsearch): Emplea Elasticsearch y su propósito es almacenar y organizar los datos de seguridad generados por el Wazuh Manager, facilitando búsquedas instantáneas y análisis efectivos de grandes cantidades de datos en tiempo real. Es fundamental para permitir la representación gráfica de los datos en el Panel de Wazuh (Kumar & Biju, 2023).

Wazuh Dashboard (Kibana): Facilita la visualización y el análisis de la información de seguridad guardada en Elasticsearch. Proporciona instrumentos visuales y tableros personalizados para que los analistas puedan entender de manera más eficaz los incidentes y alertas. Es esencial para tener una perspectiva clara sobre la situación de la seguridad en la infraestructura que se está supervisando (Kumar & Biju, 2023).

Inteligencia de Amenazas en soluciones SIEM Open Source

Se ha transformado en un elemento fundamental dentro de los SIEM, su incorporación no solo facilita la identificación de incidentes, sino que también permite anticiparse a ellos utilizando indicadores de compromiso, reglas de correlación contextual y análisis predictivo (Alzahrani et al., 2024).

Es decir, su integración mejorará la percepción del entorno, conecta eventos con amenazas identificadas y posibilita respuestas más rápido al detectar problemas, esto se logra a través de un ciclo compuesto por las siguientes etapas (Alzahrani et al., 2024):

Investigación y planificación: Establecer un repositorio de IoC sin costo para información sobre amenazas cibernéticas.

Recopilación de datos: Crear sistemas para reunir información, aprovechando los Indicadores de Compromiso globales de OSINT. Emplear técnicas para una recolección exhaustiva y variada de datos sobre amenazas cibernéticas.

Análisis: Examinar la información obtenida utilizando métodos adecuados, como el análisis de datos. Identificar tendencias, anomalías y patrones en los datos para obtener una comprensión más clara de las ciberamenazas que se encuentran globalmente.

Clasificación: Crear un registro de los IOCs de OSINT que necesitan ser clasificados para identificar el IoC más útil para su divulgación pública.

Difusión: Da a conocer el IoC con gráficos atractivos y en un formato intuitivo para que los usuarios puedan utilizarlo de manera fácil y eficaz evitando la exposición a los riesgos de ciberataques.

Plataformas de Inteligencia de Amenazas

Hay varias plataformas y servicios que proporcionan información sobre amenazas en tiempo real.

Tabla 7

Top 5 de Plataformas de Threat Intelligence

Plataforma	Funcionalidades Principales	Integración con SIEMs

MISP	Compartir, almacenar y correlacionar IoCs; Traffic Light Protocol (TLP)	Alta (via API REST, plugins Wazuh/ELK)
OpenCTI	Modelado de amenazas, actores, campañas, relaciones contextuales	Alta (conector OpenCTI-Wazuh)
AlienVault OTX	Repositorio colaborativo de IoCs, pulsos (Pulses), reputación IP/DNS	Media (adaptadores)
Abuse.ch (ThreatFox, URLhaus)	Feed de malware, C2s, URLs maliciosas, IPs comprometidas	Alta (scripts)
TheHive (con Cortex)	Gestión de incidentes, análisis colaborativo, enriquecimiento con Cortex	Media (integración con MISP)

Nota: En base con el análisis comparativo, MISP es la más calificada para entornos SIEM de Open Source debido a su capacidad de integración, técnica y respaldo comunitario (Vandeplas et al., 2024), (Filigran, 2025), (AT&T Cybersecurity, 2024),(Abuse.ch, 2024), (TheHive Project, 2024).

La adaptación de inteligencia de amenazas en un entorno SIEM y la utilización de plataformas específicas como MISP, representan un progreso importante hacia una defensa cibernética más activa, automatizada y fundamentada en el conocimiento compartido.

Capítulo 3

Desarrollo

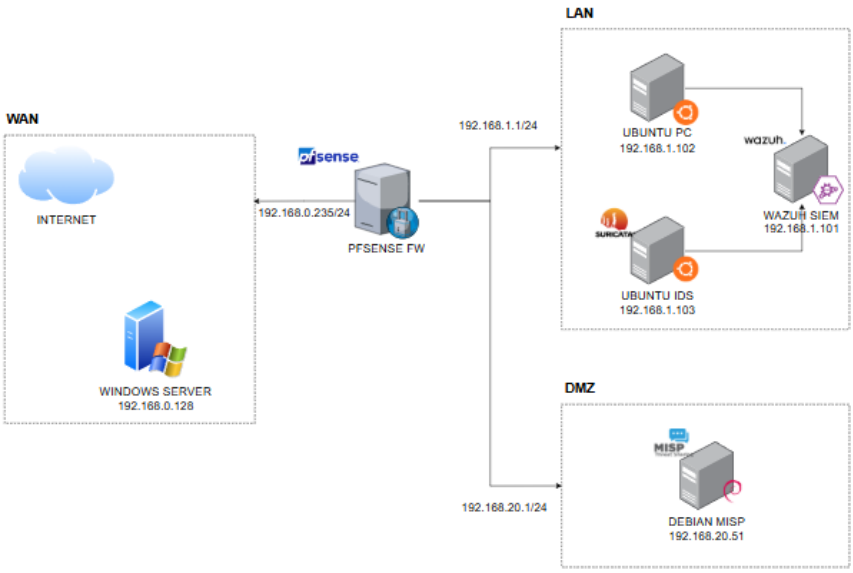
En este capítulo se detalla el proceso de desarrollo e implementación de un sistema SIEM utilizando tecnologías Open Source, como paso inicial se realiza un análisis comparativo teórico de diversas soluciones de código abierto, considerando su tecnología, protección, costo e integración con otras herramientas, adaptándose a las necesidades de cualquier entidad. Este análisis se encuentra expuesto en la sección 2.4 del Estado del arte, el cual permitió seleccionar Wazuh como la herramienta adecuada del proyecto.

Se describe el diseño de la arquitectura, así como la instalación y configuración del entorno, destacando el enfoque de Wazuh para integrarse con otras herramientas. Su uso permite construir una solución eficaz para el monitoreo de amenazas, mediante la recolección, el análisis y la gestión centralizada de eventos de seguridad.

Arquitectura de la Integración.

Figura 7

Arquitectura



Nota: La figura muestra la topología de red desplegada para el laboratorio, Elaboración Propia

Tabla 8

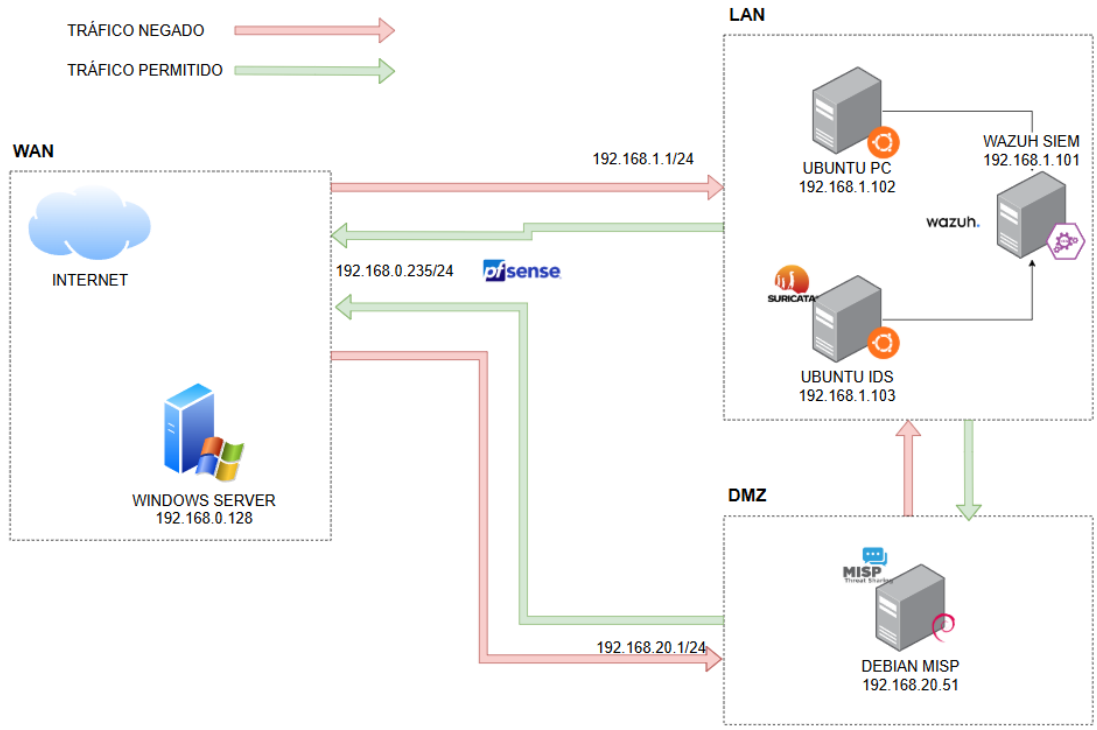
Detalle Arquitectura

S.O	HOSTNAME	DIRECCI IP	ROL
FreeBSD	PFSENSE	192.168.0.235	Firewall, servidor DHCP
Windows 11	WINDOWS	192.168.0.128	Cliente
Ubuntu 22.04 LTS	TELCO-PROD-EC-DH01	192.168.1.102	Servidor
Ubuntu 22.04 LTS	TELCO-PROD-EC-IDS	192.168.1.103	IDS
WAZUH	WAZUH-SERVER	192.168.1.101	Siem
Debian 12	TELCODEBHP	192.168.20.51	MISP

Nota: Elaboración Propia

Figura 8

Diagrama de flujo de red



Descripción e instalación de SIEM WAZUH.

Para la configuración del sistema SIEM será utiliza la ova que integra los siguientes componentes:

- Virtual Machine (OVA) - Installation alternatives
- Wazuh manager 4.12
- Wazuh indexer 4.12
- Wazuh dashboard 4.12

Para su funcionamiento se instalará sobre el hipervisor Virtual Box.

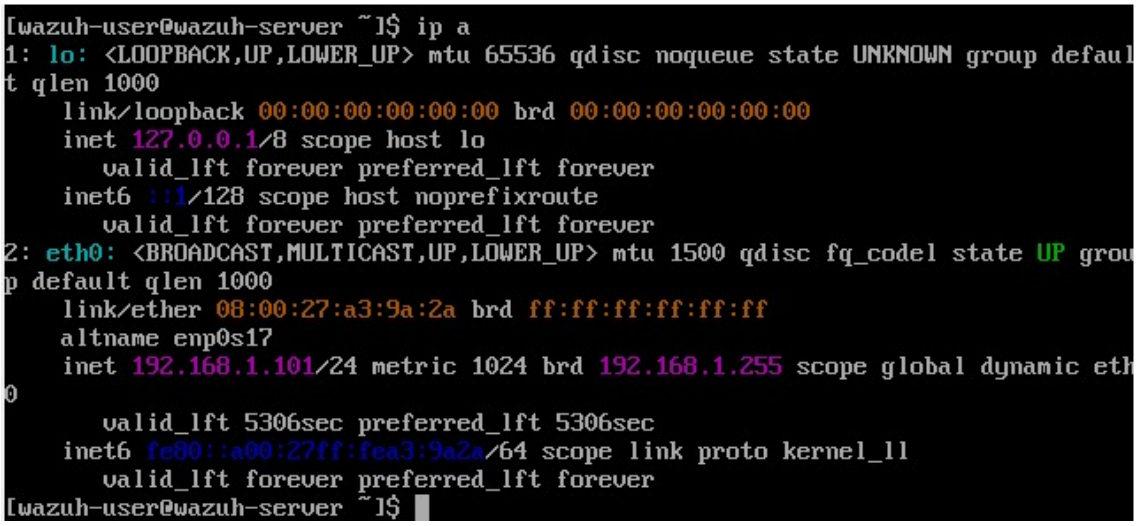
Instalación de Siem Wazuh

En el proceso de virtualización importamos el archivo.ova y se realiza la instalación y configuración de máquina.

Terminada la instalación se ejecuta la maquina y se valida la ip asignada, para este laboratorio, se configura con ip estática asignada dentro del rango DHCP generado por pfsense.

Figura 9

Validación ip WAZUH



Nota: La figura nos da un detalle de configuraciones de red Wazuh, la ip asignada para Wazuh es 192.168.1.101, Elaboración propia

Abrimos desde cualquier navegador que se encuentre en la LAN, con ip de la máquina, tenemos acceso por web a Wazuh.

Figura 10

Wazuh vía web

Nota: En la imagen muestra la primera interfaz de Wazuh, Elaboración Propia.

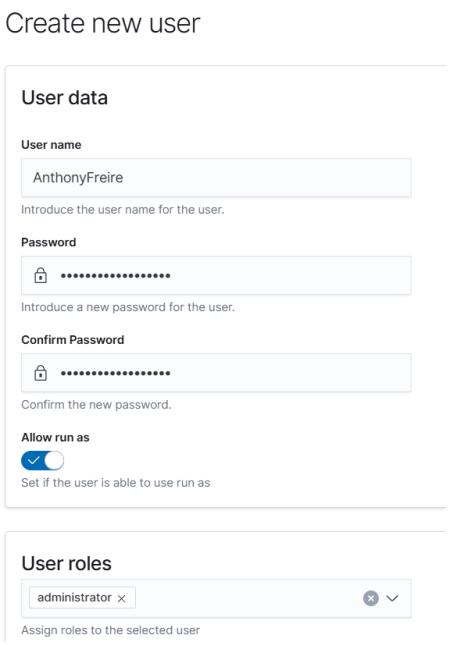
Creación de roles de usuario en SIEM

En la administración del SIEM, se crean usuarios administradores por cada integrante del equipo de trabajo.

- AnthonyFreire
- StefyChavez
- FernandoDefaz
- AndresCalahorrano

Figura 11

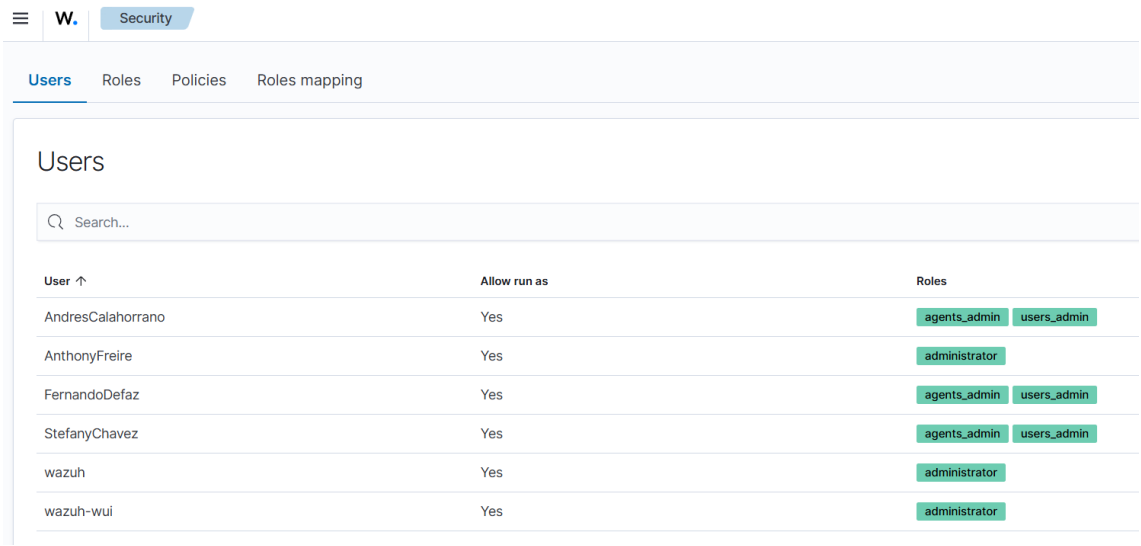
Creación de Usuario



Nota: En la figura podemos observar algunos de los campos necesarios para la creación de usuario, Elaboración propia.

Figura 12

Integrantes creados en Wazuh



Nota: La figura muestra el detalle de usuarios creados, así como roles asignados dentro del SIEM, Elaboración propia.

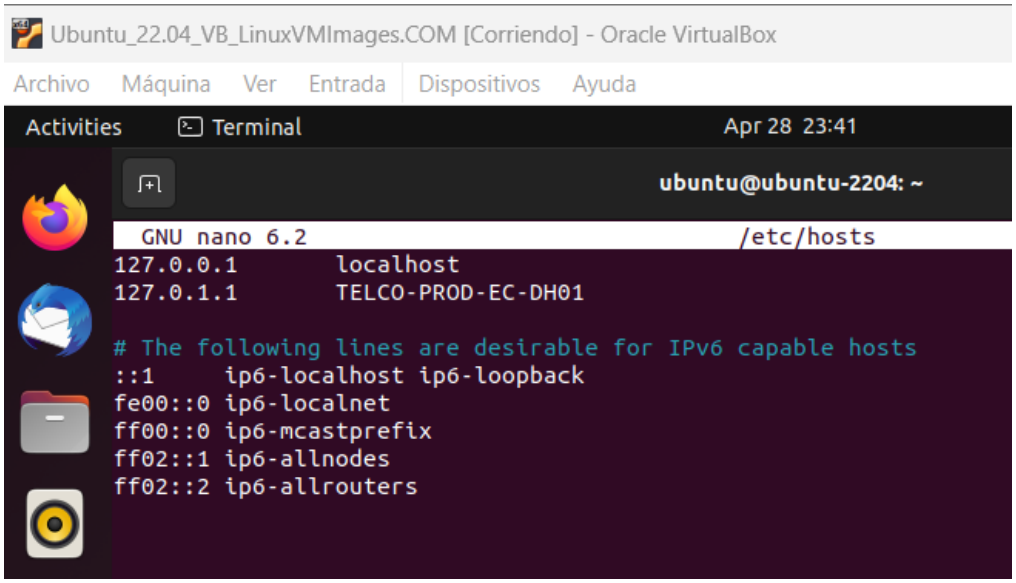
Configuración de los componentes de seguridad

Integración agente S.O Ubuntu en Wazuh

Creamos una máquina virtual a partir de una ISO Ubuntu 22.04 TLS

Figura 13

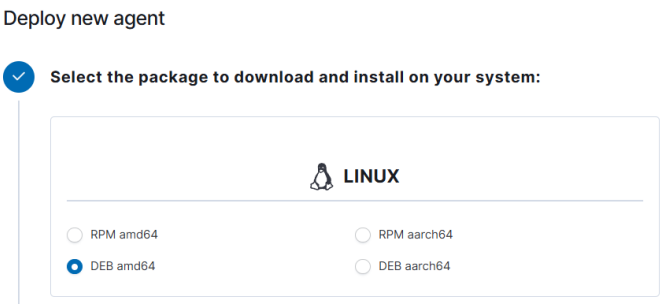
Configuración servidor Ubuntu



Ya instalado Ubuntu para la comunicación entre Wazuh “Siem” y el servidor, se configura un agente, el cual monitorizará diferentes aspectos técnicos y de seguridad.

Figura 14

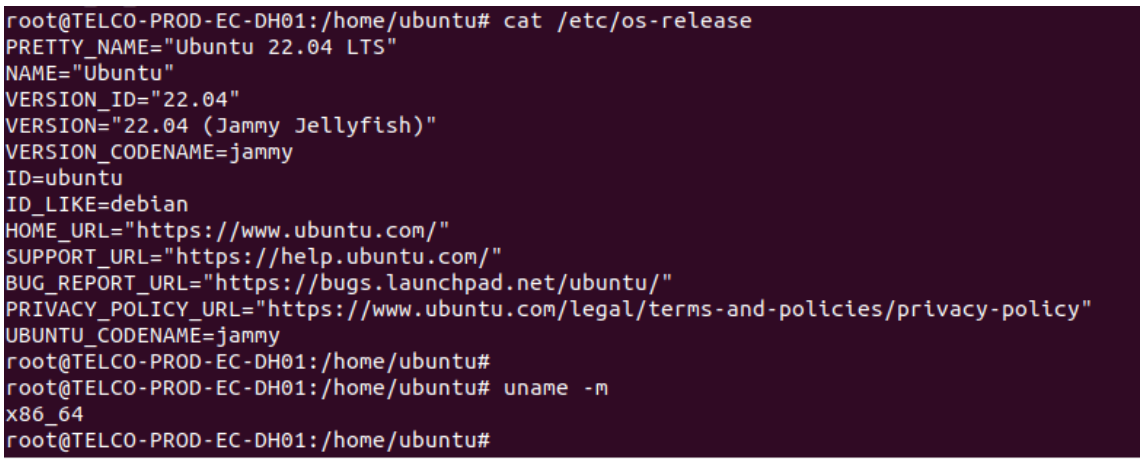
Creación de nuevo agente



Se valida la arquitectura y el S.O para poder seleccionar el paquete a instalarse, dependiendo de las características del servidor.

Figura 15

Validación de arquitectura de Ubuntu

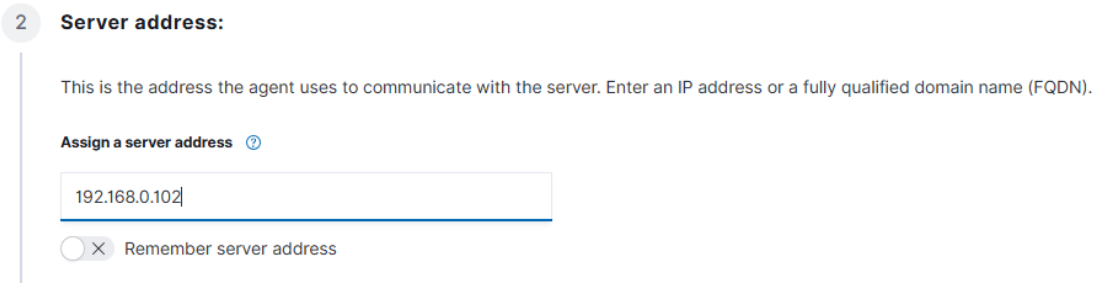


Nota: La figura muestra el detalle de arquitectura de S.O. Ubuntu mantiene una arquitectura de 64bits, Elaboración Propia.

En el proceso de configuración de agente se especifica la dirección ip para la comunicación con el servidor, este será configurado como FQDN. Como ultimo requerimiento se especifica el nombre del agente, es recomendable que tenga el nombre del host que va a monitorear para que exista coherencia y correlación en todo el entorno.

Figura 16

Asignación de IP para comunicación entre servidor y Wazuh

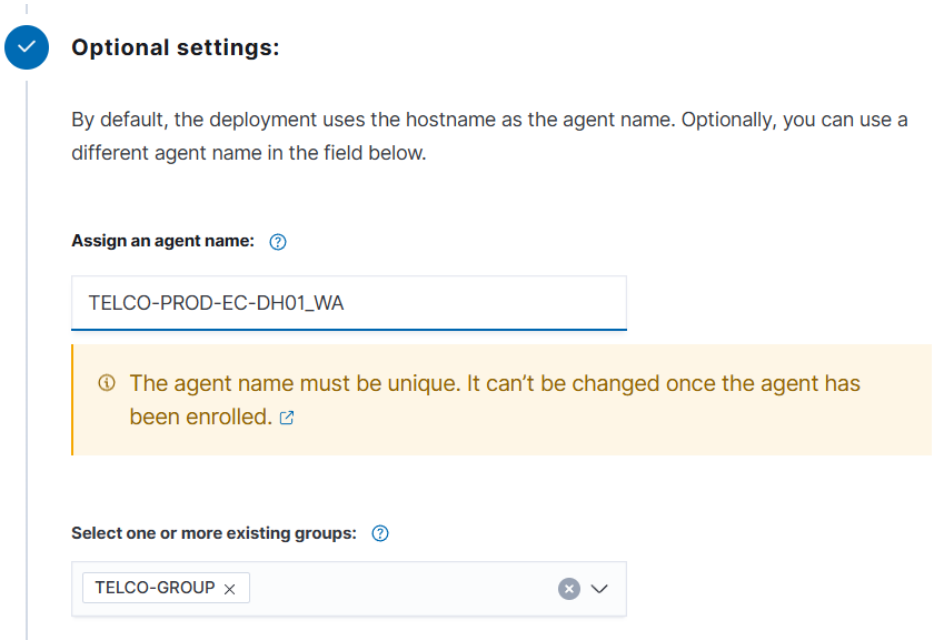


Nota: La figura muestra el campo para colocar la ip del servidor, la ip de SIEM Wazuh es 1921.168.1.101, Elaboración Propia.

El usuario creado, se agrega al grupo TELCO-GROUP. Wazuh nos proporciona comando a ejecutar para la instalación de agente desde lado de cliente.

Figura 17

Creación de agente



En Wazuh cuando se crea el agente proporciona los comandos a ejecutar, se abre un terminal desde Ubuntu y se ejecuta, pegar comandos

Figura 18

Comandos de instalación del agente

Terminada la instalación, se realiza el reinicio del demonio para que se almacene los cambios, se habilita, se reinicia y se valida el estado del agente.

Figura 19

Reinicio de agente

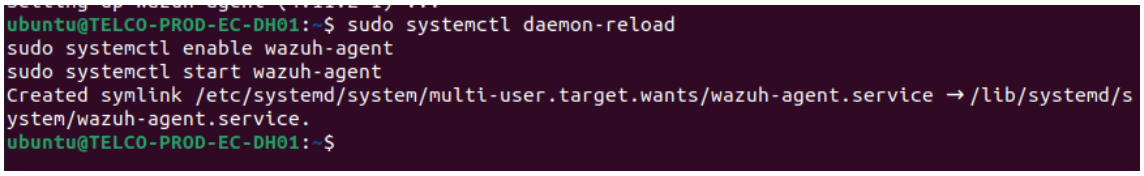
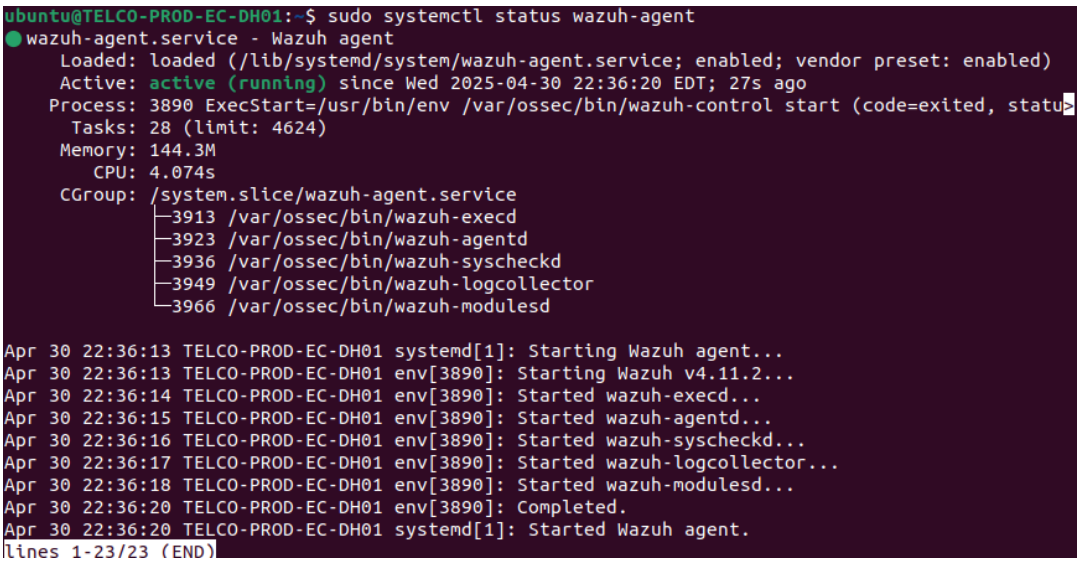


Figura 20

Estado de agente

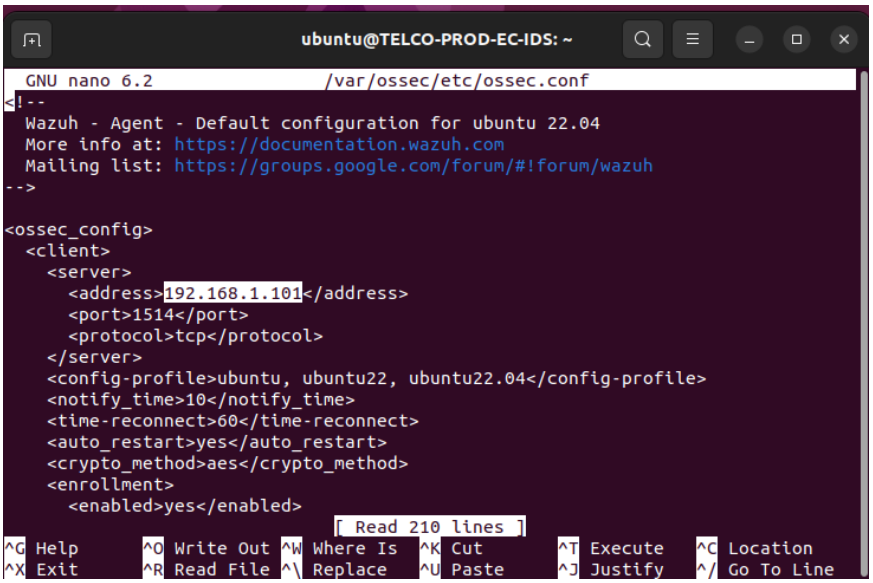


Nota: La figura muestra el servidor Ubuntu con un agente creado y ejecutándose, Elaboración Propia.

Luego en el archivo ossec.conf se configura el puerto por el cual se va a conectar al server manager de wazuh.

Figura 21

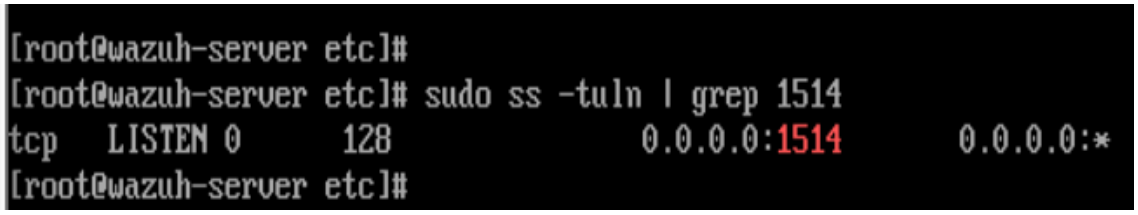
Configuración ossec



Los puertos predefinidos pueden ser el 1515 (realiza la autenticación) o 1514 (comunicación de eventos logs).

Figura 22

Validación escucha para puerto 1514 desde Wazuh



Nota: Es importante validar que en el servidor manager se encuentra aceptando las conexiones para el puerto 1514, Elaboración Propia.

Terminada la creación del agente se debe validar que exista conexión entre el servidor de Ubuntu y Wazuh por el puerto definido, en este caso el 1514.

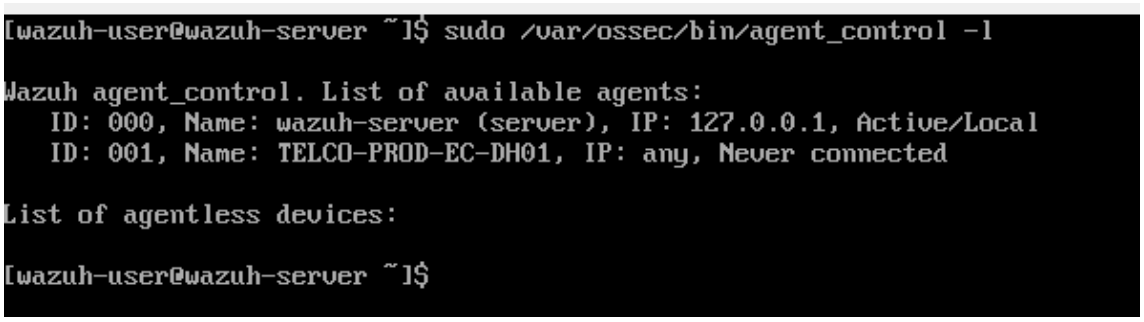
Figura 23

Validación de conexión por puerto 1514 desde Ubuntu

Se realiza el reinicio del agente de Wazuh. En el servidor mánager de Wazuh se valida que se haya establecido y registrado el agente de Ubuntu correctamente.

Figura 24

Lista de agentes disponibles desde SIEM Wazuh



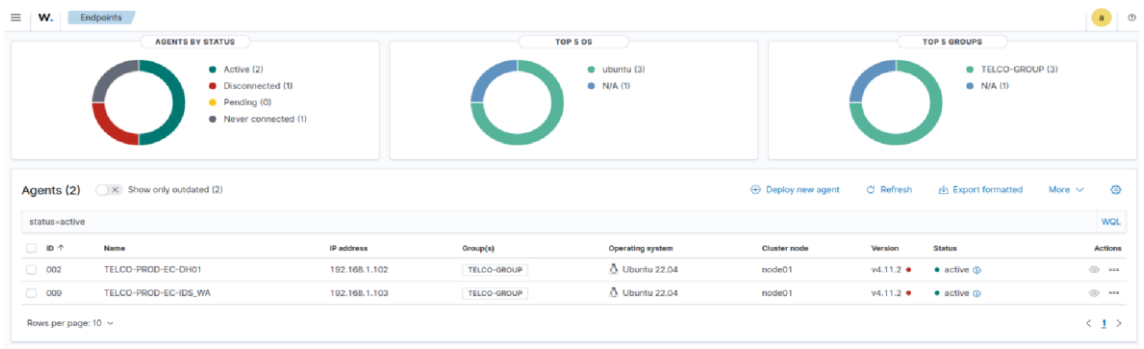
Nota: La figura lista los agentes disponibles en el servidor WAZUH, se valida agente 001 no tiene una ip asignada, Elaboración Propia

Como evidenciamos en la figura el servidor con ID 001 no tiene IP y nunca se ha conectado, por lo que se realiza la modificación del archivo clients.keys agregando los detalles faltantes, adicional es importante reiniciar el mánager y el agente.

Se procede a ingresar en la interfaz web WAZUH para validar el estado del agente, se observa que se encuentra activo y también se visualiza algunas especificaciones como sistema operativo, versión, estado.

Figura 25

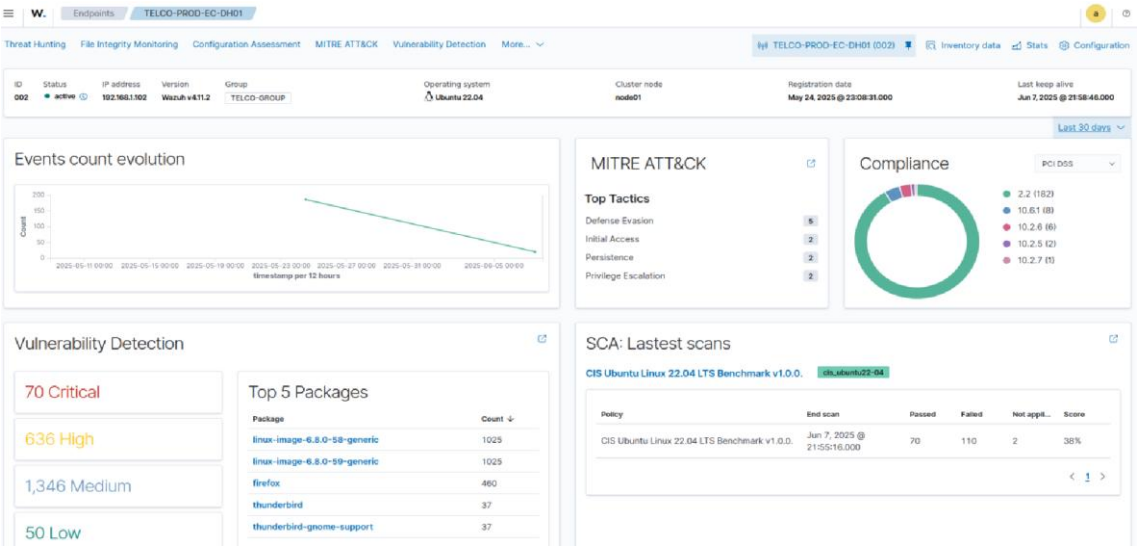
Lista de agentes disponibles desde interfaz web WAZUH



En dashboard del agente se puede tener más información sobre diferentes temas de seguridad relevantes como MITRE, vulnerabilidades, entre otros.

Figura 26

Dashboard de Agente Ubuntu

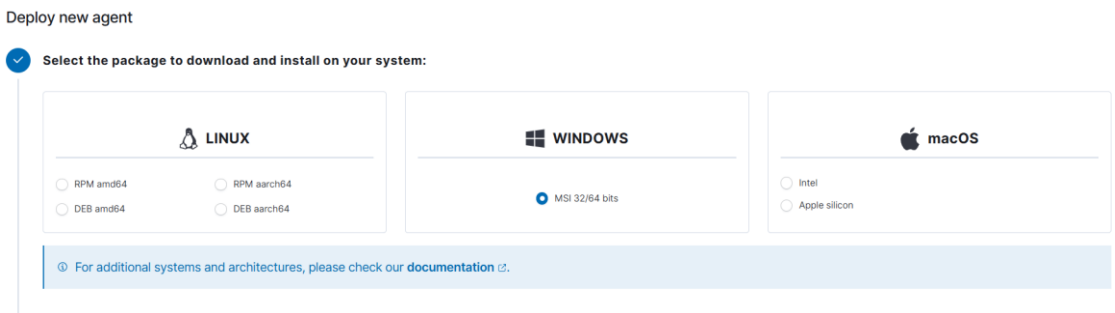


Integración de un Equipo Windows en Wazuh

Para la instalación del agente en un equipo Windows, en WAZUH vamos a la sección Endpoint/Deploy New agent/ seleccionar el sistema operativo Windows y se establece la ip de conexión:

Figura 27

Creación agente nuevo para maquina Windows

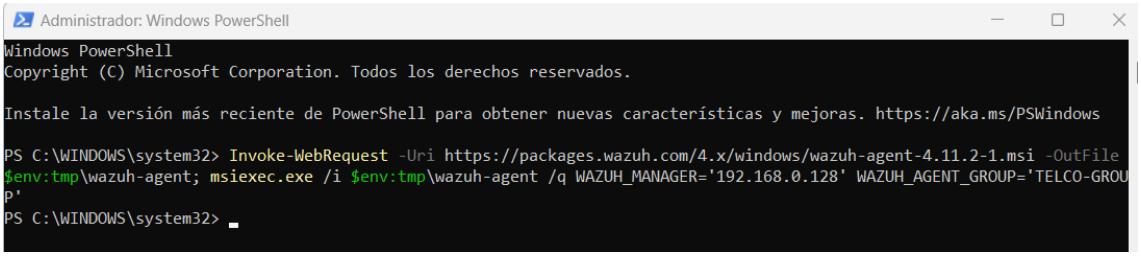


Nota: La figura muestra la configuración del agente Windows, se establece el tipo de sistema operativo y su arquitectura, Elaboración Propia.

En la maquina Windows, se abre una consola PowerShell en modo administrador y se ejecuta el código de instalación del agente que proporciona el portal web de Wazuh.

Figura 28

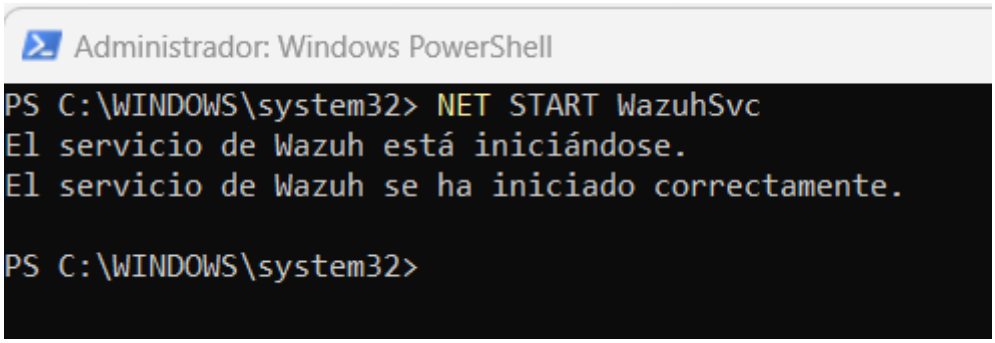
Instalación agente desde maquina Windows



Finalizada la instalación, para iniciar el agente se ejecuta el siguiente comando desde la consola de powershell.

Figura 29

Inicio de agente



En el archivo ossec.conf en la maquina de Windows, se verifica que se encuentre correctamente detallada la ip del Wazuh mánager y su puerto correspondiente.

Figura 30

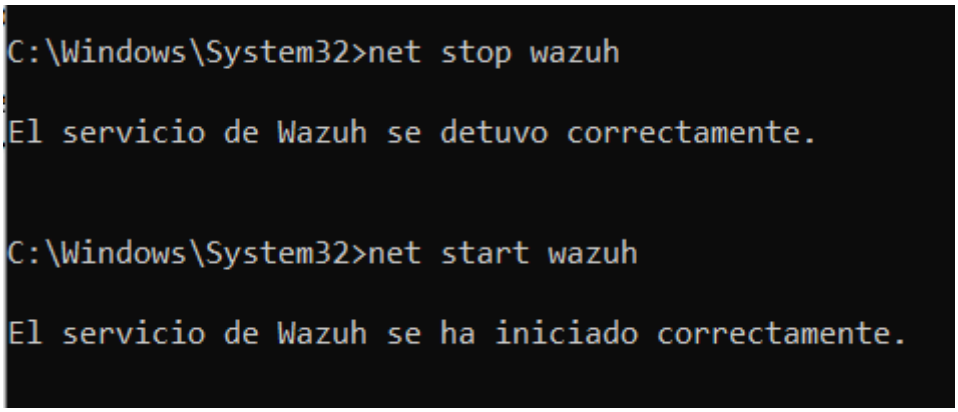
Configuración archivo ossec.conf desde maquina Windows

```
<!--
  Wazuh - Agent - Default configuration for Windows
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

  <client>
    <server>
      <address>192.168.1.101</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
    <config-profile>windows, windows10</config-profile>
    <crypto_method>aes</crypto_method>
    <notify_time>10</notify_time>
```

Para culminar el proceso de instalación, se procede a reiniciar el servicio desde PowerShell en modo administrador.

Figura 31

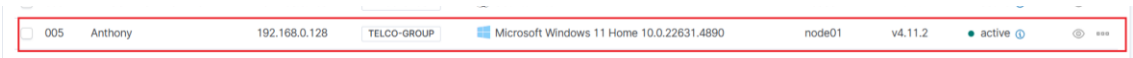
Detener/Iniciar servicio Wazuh



Desde interfaz web Wazuh se evidencia la correcta instalación del agente Windows con id 003.

Figura 32

Lista de agentes disponibles desde Wazuh



Implementación e Integración Firewall PfSense

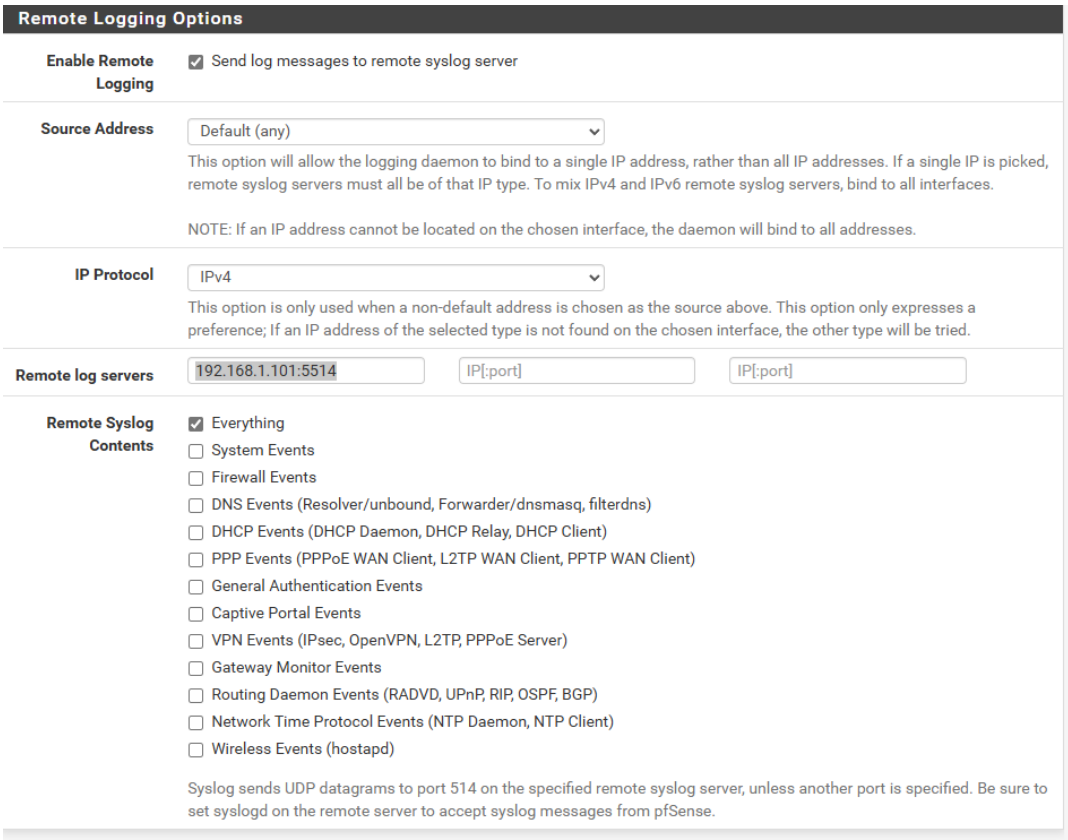
Para la instalación de Pfsense se descarga la ISO en versión 2.7.2, se utilizará el hipervisor VirtualBox, en el cual se asignarán recursos de 8gb de RAM y disco dinámico, así como 3 tarjetas de red, las cuales será utilizadas para despelegar una red LAN, WAN Y DMZ.

Integración de PfSense con Wazuh

Para generar la integración entre pfsense y Wazuh se habilita el remote logging de syslog.

Figura 33

Configuración syslog en Pfsense



Se usa socat como receptor UDP simple para escribir logs remotos mediante el puerto 5514 como alternativa a 514 debido a que muchos demonios no pueden escuchar puertos menos menores a 1024 sin permisos especiales.

Se crea un decoder personalizado, el código se aplica solo para los logs cuyo program_name sea filterlog [86161], se establece que se extraigan los primeros campos de log después del timestamp y que se encuentren separados por coma.

Figura 34

Creación decoder

```
[root@wazuh-server decoders]# cat decoder_custom_firewall.xml
<decoder name="pf">
  <program_name>filterlog[86161]:</program_name>
</decoder>

<decoder name="pf-fields">
  <parent>pf</parent>
  <regex>^\S*,\S*,\S*,(\S*),\S*,\S*,(\S*),</regex>
  <order>id,action</order>
</decoder>

<decoder name="pf-fields">
  <parent>pf</parent>
  <regex offset="after_regex">\S*,\S*,\S*,\S*,\S*,\S*,\S*,\S*,\S*,(\S*),\S*,(\S*),(\S*),</regex>
  <order>protocol,srcip,dstip</order>
</decoder>

<decoder name="pf-fields">
  <parent>pf</parent>
  <regex offset="after_regex">(\d*),(\d*),\S*</regex>
  <order>srcport,dstport</order>
</decoder>

<decoder name="pf-fields">
  <parent>pf</parent>
  <regex offset="after_regex">datalength=(\S*)|(\d*)</regex>
  <order>length</order>
</decoder>
```

Nota: La figura muestra el decoder personalizado establecido para la integración entre Pfsense y Wazuh, Elaboración Propia.

Se modifica el archivo ossec.conf, el cual especifica a wazuh la ruta donde se van a encontrar los decoders personalizados para pfsense.

Figura 35

Definición ruta decoders

```
  <!-- User-defined ruleset -->
  <decoder_dir>etc/decoders</decoder_dir>
  <rule_dir>etc/rules</rule_dir>
</ruleset>

<rule_test>
  <enabled>yes</enabled>
  <threads>1</threads>
```

Establecida la configuración se ingresa un log de prueba obtenido del archivo pfsense_wazuh.log enviado por syslog desde el firewall con el objetivo de evidenciar que el decoder se encuentre funcionando correctamente.

Figura 36

Obtención log de prueba

```
[root@wazuh-server log]# /var/ossec/bin/wazuh-logtest
Starting wazuh-logtest v4.12.0
Type one log per line

May 31 18:59:27 filterlog: 4,,,1000000103,em0,match,block,in,4,0x0,,255,12686,0,none,17,udp,328,0.0.0.0,255.25
5.255.255,68,67,308

**Phase 1: Completed pre-decoding.
       full event: 'May 31 18:59:27 filterlog: 4,,,1000000103,em0,match,block,in,4,0x0,,255,12686,0,none,17,u
dp,328,0.0.0.0,255.255.255.255,68,67,308'
       timestamp: 'May 31 18:59:27'
       hostname: 'filterlog:'
       program_name: 'filterlog'

**Phase 2: Completed decoding.
       name: 'pf'
       action: 'block'
       dstip: '255.255.255.255'
       dstport: '67'
       id: '1000000103'
       length: '308'
       protocol: 'udp'
       srcip: '0.0.0.0'
       srcport: '68'

**Phase 3: Completed filtering (rules).
       id: '87701'
       level: '5'
       description: 'pfSense firewall drop event.'
       groups: '['pfsense', 'firewall_block']'
       firedtimes: '1'
       gpg13: '['4.12']'
       hipaa: '['164.312.a.1']'
       mail: 'False'
       nist_800_53: '['SC.7']'
       pci_dss: '['1.4']'
       tsc: '['CC6.7', 'CC6.8']'
**Alert to be generated.
```

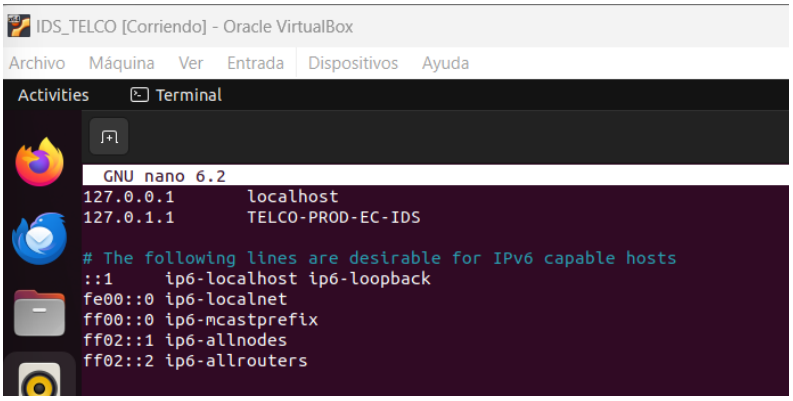
Nota: La figura muestras la asignación de los parámetros a cada uno de los valores decodificados del log, Elaboración Propia.

Integración IDS

Para obtener los logs del IDS desplegado, utilizaremos la máquina virtual de Ubuntu.

Figura 37

Máquina Virtual Ubuntu



Se realiza la instalación de Suricata.

Figura 38

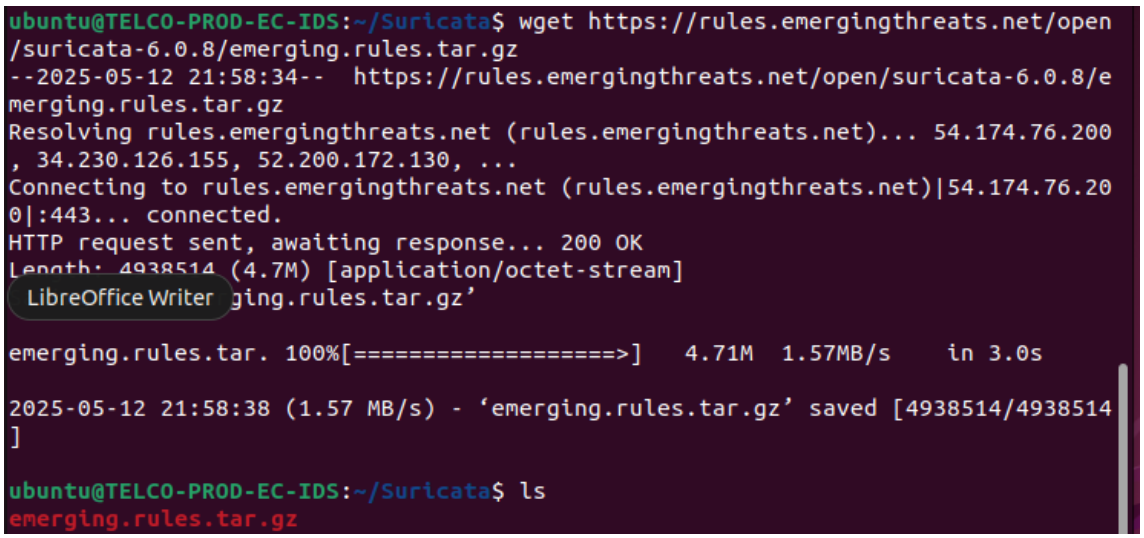
Instalación de Suricata

```
$ sudo add-apt-repository ppa:oisf/suricata-stable
$ sudo apt-get update
$ sudo apt-get install suricata -y
```

Se realiza la descarga de paquetes de Suricata.

Figura 39

Descarga Suricata



Nota: La figura muestra la instalación de paquetes necesarios para suricata extraídos.

Figura 40

Proceso Extracción e Instalación de Reglas Suricata

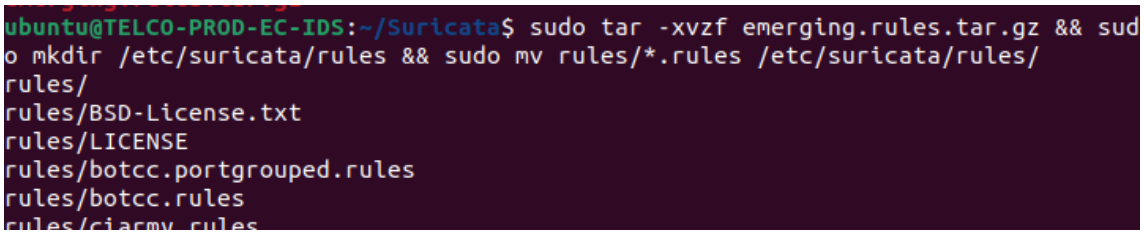
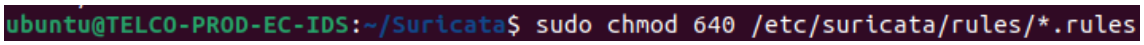


Figura 41

Asignación de permisos

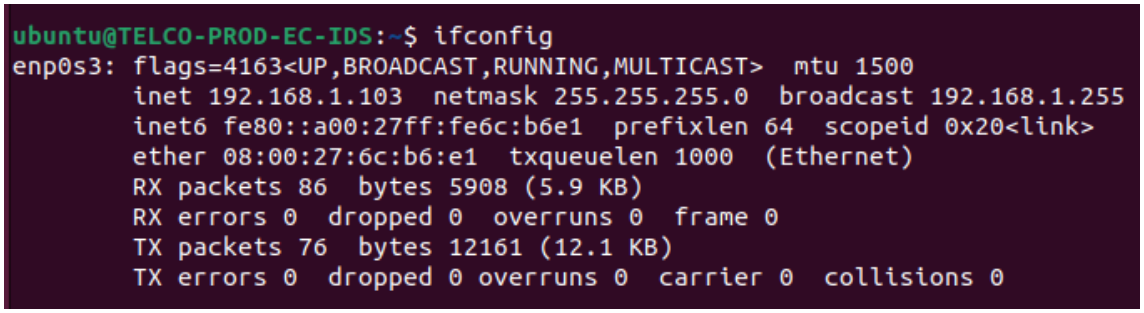


Nota: Se otorga permisos de lectura y escritura para propietario, permisos de lectura para grupo y otros usuarios ningún permiso, Elaboración propia.

Para configuración de suricata es necesario establecer la configuración de red, como su ip y tarjeta de red.

Figura 42

Configuración de Suricata



Nota: La figura muestra la configuración de red del IDS, la ip usada es 192.168.1.103, Elaboración propia.

Figura 43

Definición de ruta por defecto para reglas

```
default-rule-path: /var/suricata/rules

rule-files:
  - suricata.rules
  - emerging-icmp.rules
  - emerging-dos.rules
```

En la sección de log análisis se debe incluir los logs de suricata.

Figura 44

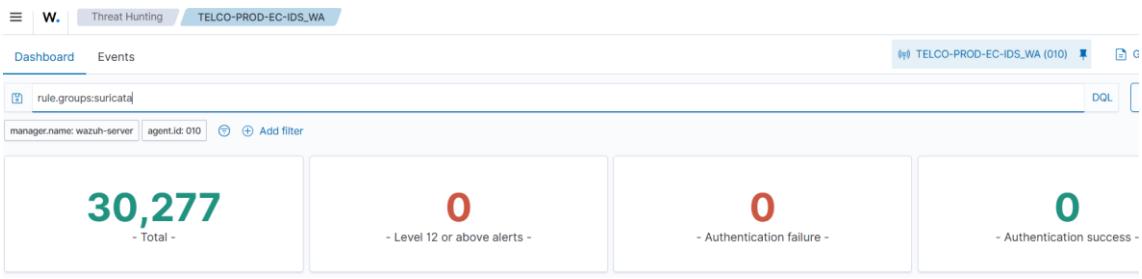
Log Suricata

```
 GNU nano 6.2                    /var/ossec/etc/ossec.conf *

  <!-- Database synchronization settings -->
  <synchronization>
    <enabled>yes</enabled>
    <interval>5m</interval>
    <max_eps>10</max_eps>
  </synchronization>
</syscheck>

<!-- Log analysis -->

<localfile>
  <log_format>json</log_format>
  <location>/var/log/suricata/eve.json</location>
</localfile>

<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
```

Finalizada la configuración del agente, se verifica en Wazuh que se están recibiendo alertas con “rule.groups:suricata”.

Figura 45

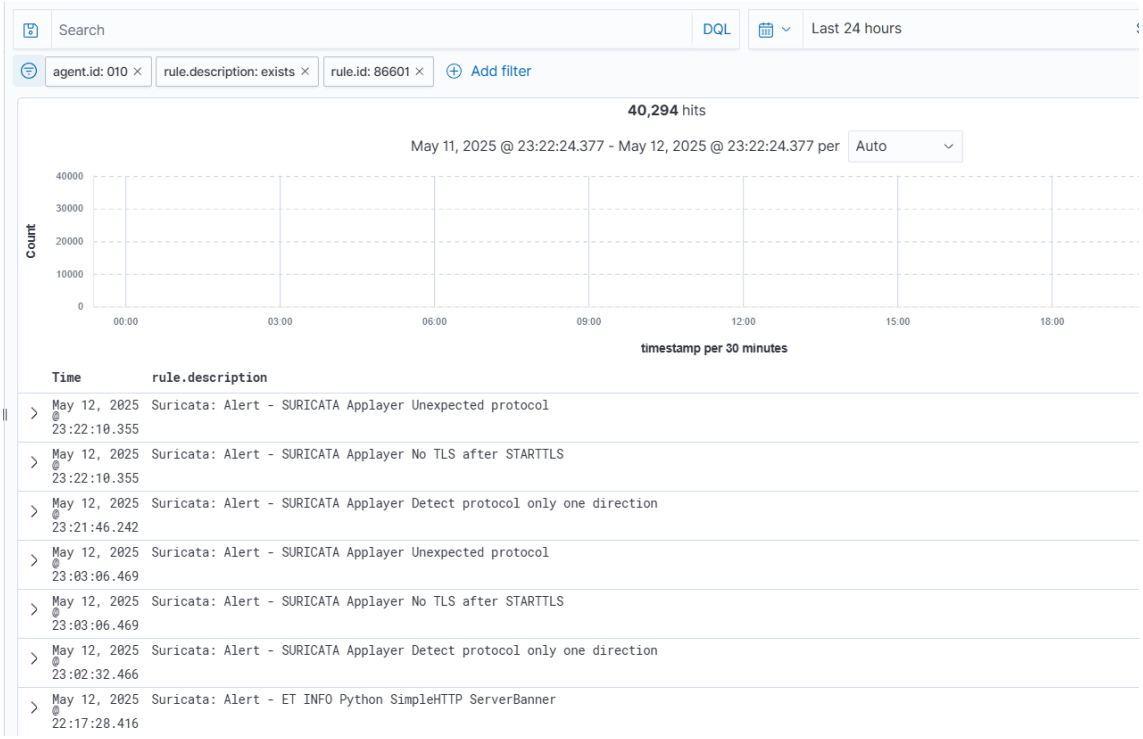
Validación desde Wazuh alertas de suricata



Se valida que exista registros de logs suricata en el apartado de Discovery

Figura 46

Logs de Suricata

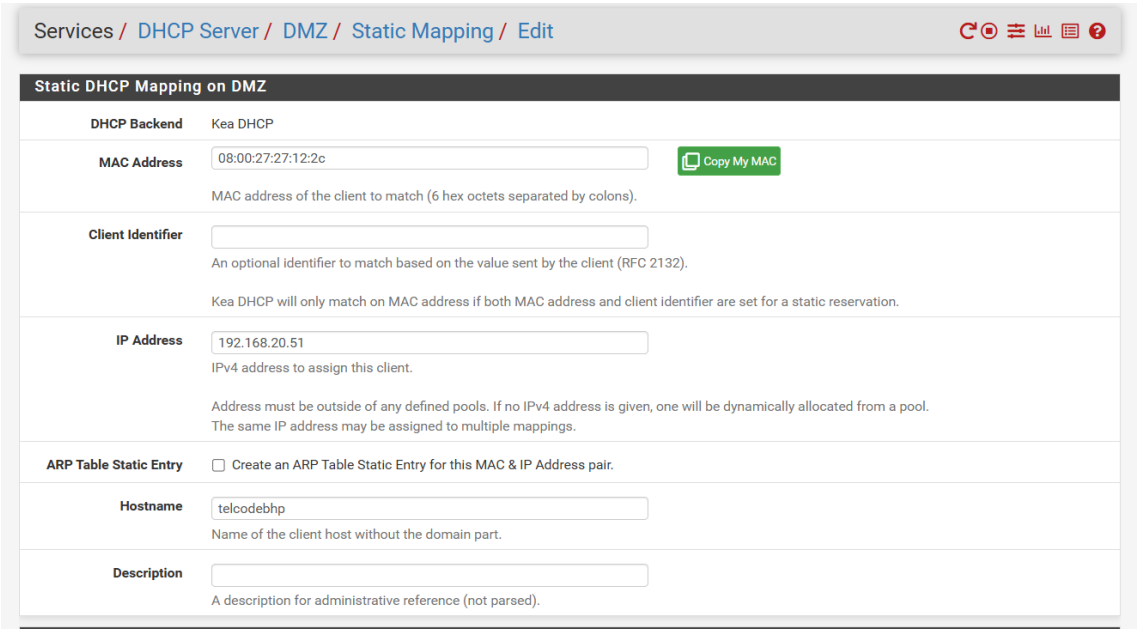


Configuración Servidor MISP

Se asigna al servidor telcodebhp una ip estática dentro de la dmz

Figura 47

Asignación ip DMZ

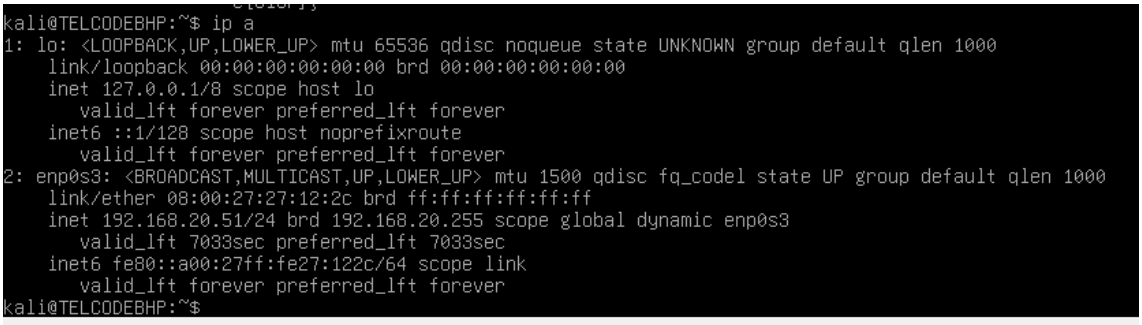


En la DMZ se instala un servidor Debian sobre el cual se configura MISP con objetivo de correlacionar amenazas con Wazuh.

Se valida que la IP obtenida por DHCP se encuentre dentro de las IPs disponibles de la DMZ

Figura 48

Validación ip asignada en DMZ



Se descarga el repositorio oficial de MISP de github “el instalador”

Figura 49

Ejecución instalación MISP

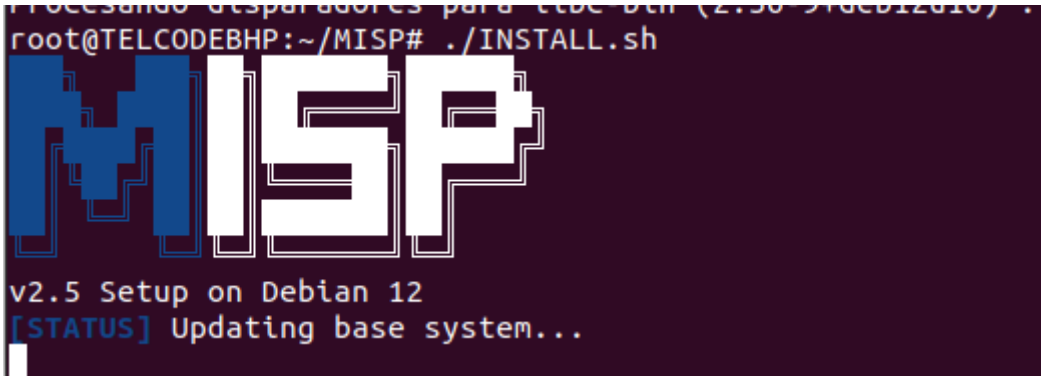
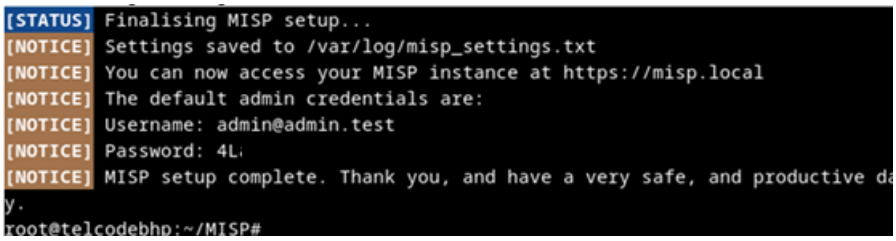


Figura 50

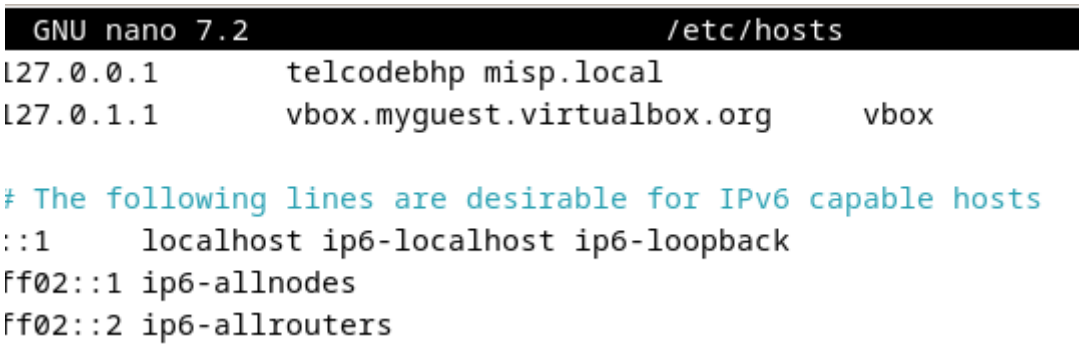
Proceso de instalacion MISP



Se modifica el archivo “hosts” agregando misp.local

Figura 51

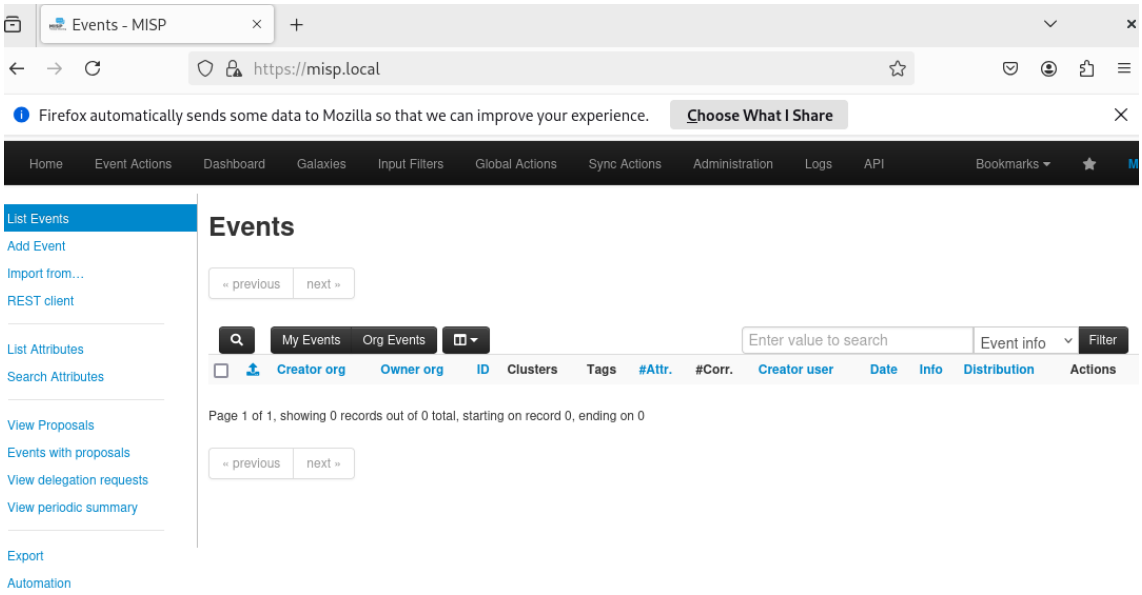
Modificación archivo hots



Se valida el correcto funcionamiento de MISP

Figura 52

MISP

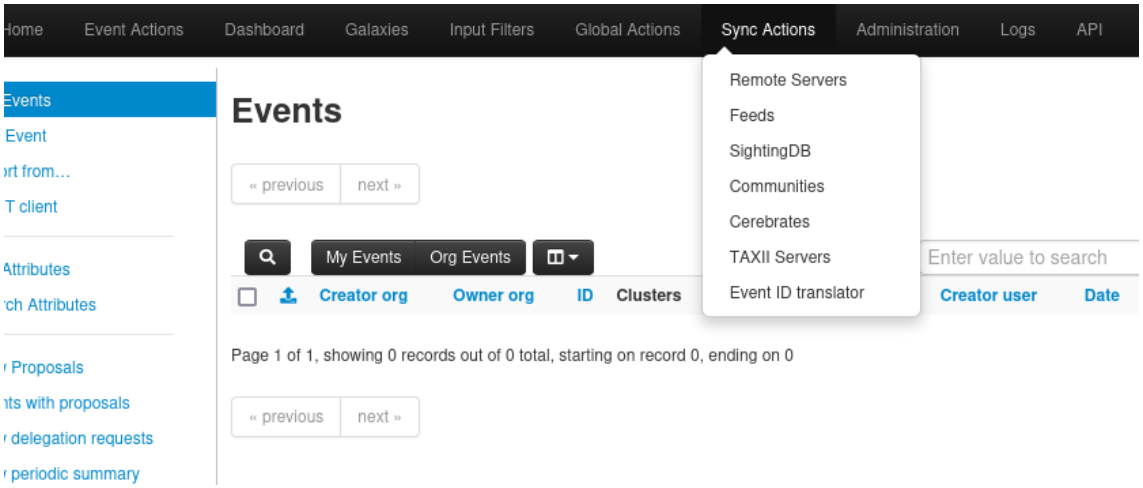


Integración feeds de ciberintelgencia

Para usar los feeds de misp se realiza la configuración como usuario administrador, se activa la sincronización de acciones.

Figura 53

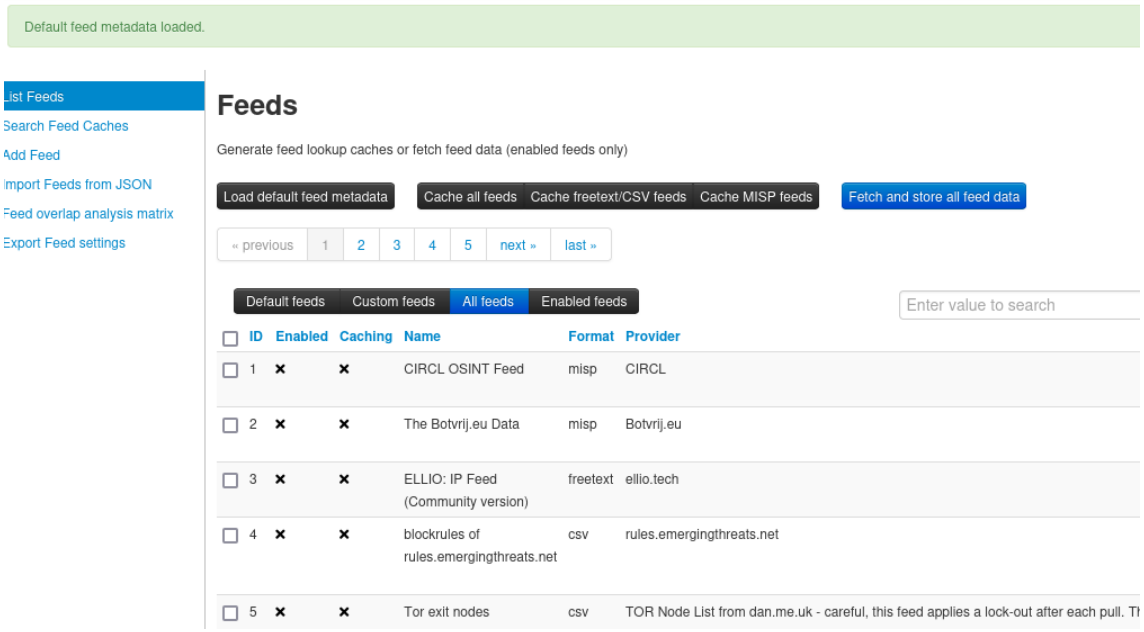
Feeds de cibertinteligencia



En el botón “Load Default feed metadata” se selecciona los feeds

Figura 54

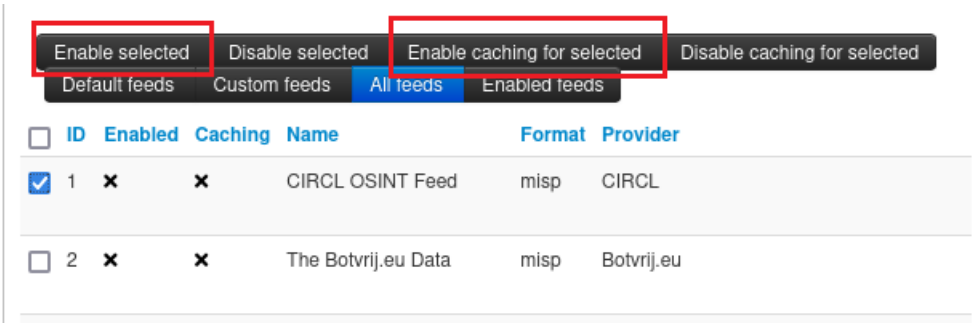
Feed en misp



Se procede a habilitar feed y se almacena en cache, la fuente descarga todos los IOCs como atributos en el servidor de la instancia de MISP.

Figura 55

Habilitación de misp



Se generar un apikey en misp esta sera consumida por wazuh

Figura 56

Generando apikey

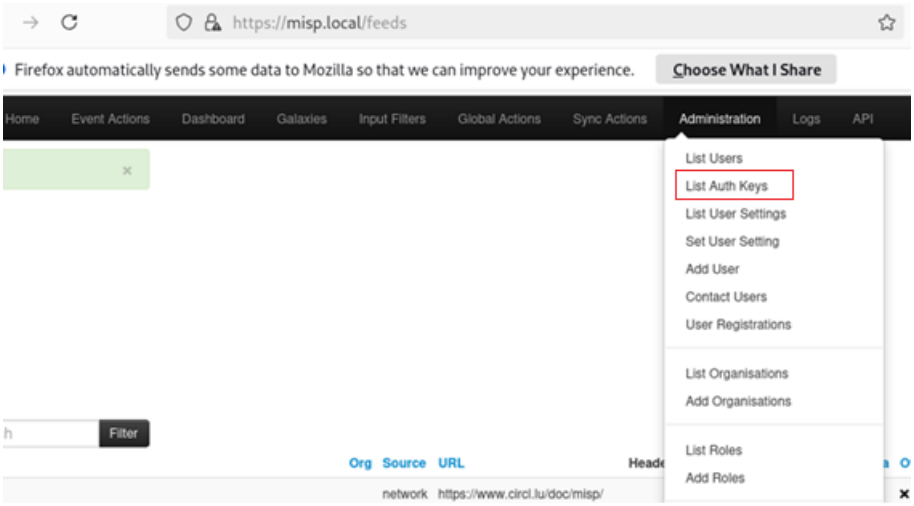
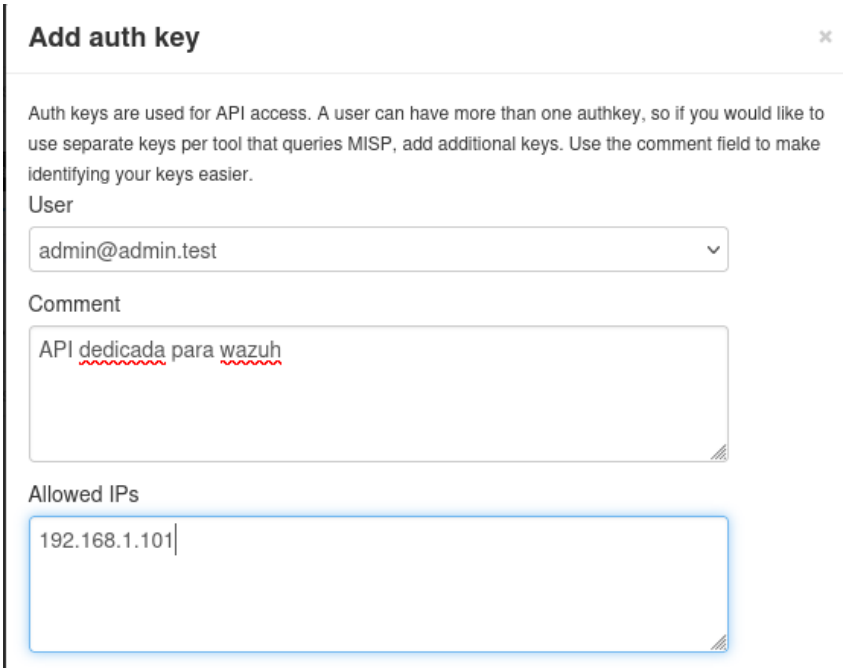


Figura 57

Apikey

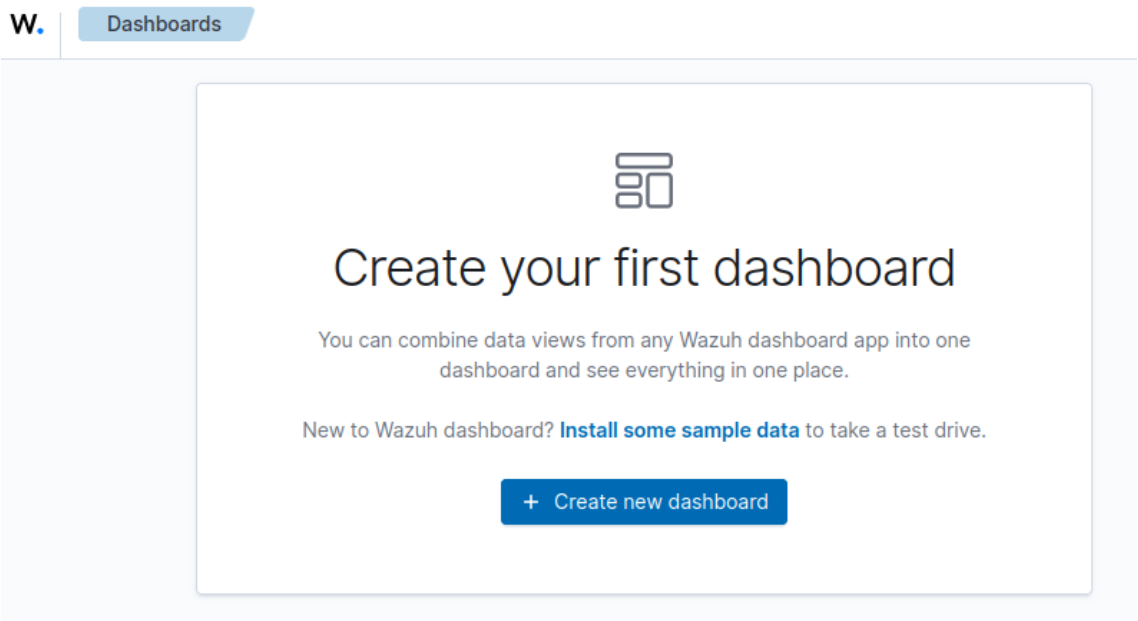


Creación de dashboard

Se genera un nuevo dashboard en la sección de panel de control, se selecciona la opción crear un nuevo dashboard “créate new dashboard”.

Figura 58

Creación de dashboard

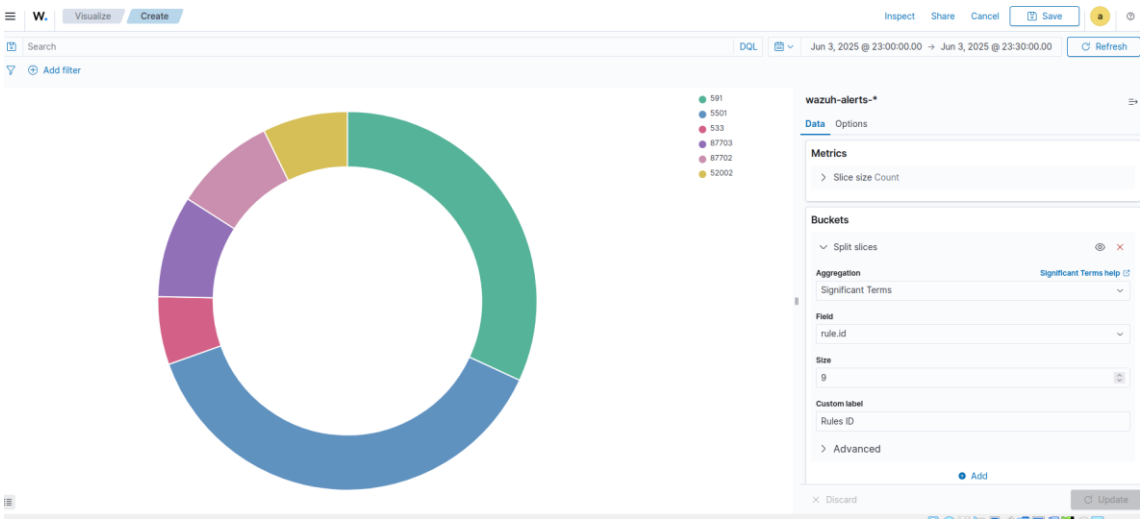


Se genera un control de todas las alertas que estamos recibiendo en wazuh. Se selecciona la fuente de la cual queremos consultar, para este laboratorio se utiliza wazuh-alerts.

Figura 59

Selección de fuente

Se selecciona el bucket que vamos a utilizar, en este caso sería Significate Terms y rule.id



Se genera el control y lo agregamos al dashboard se guarda cambios.

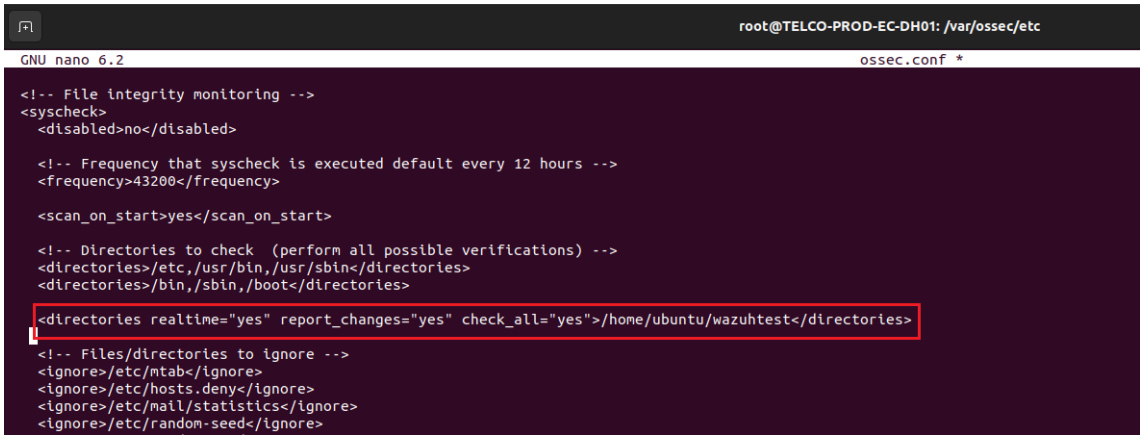
Generación de casos de uso

Monitoreo de integridad de archivos/directorios (Linux)

Para realizar un monitoreo de integridad tanto para archivos como para directorios se ingresa al archivo de configuración de wazuh agent en ossec.conf y se modifican los directorios encargados de la integridad de archivos en la sección “syscheck”.

Figura 60

Monitoreo de directorio Linux



Se agrega un nuevo monitoreo al directorio “wazuhtest” en tiempo real y se activan los reportes y el check, se guardan los cambios en el archivo y se reinicia el agente wazuh.

Monitoreo de registros Windows

Muchos actores de amenaza optan por desplegar su malware para la modificación de registros del sistema operativo, buscan controlar muchos aspectos fundamentales de los programas y aplicaciones, esto con el fin de obtener diferentes ventajas como:

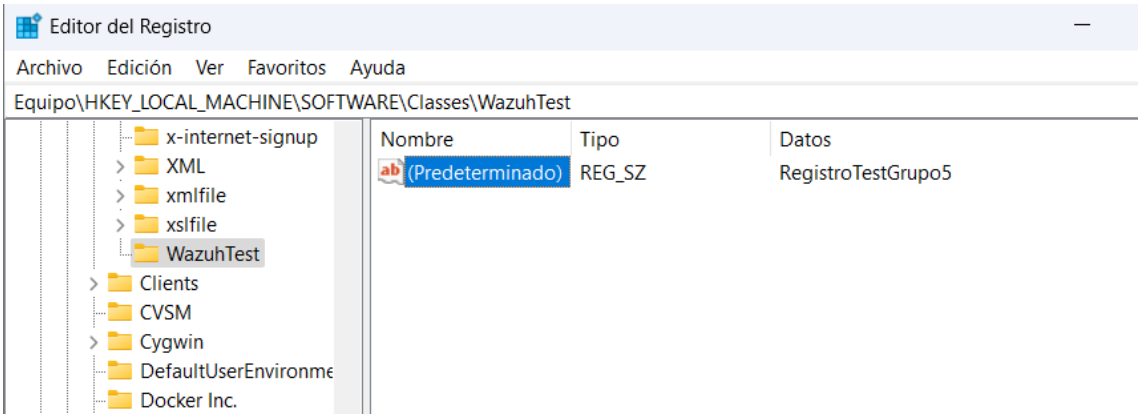
- Persistencia
- Evasión de detección de soluciones de monitoreo
- Inyección de código malicioso de forma oculta
- Desactivación de medidas de seguridad
- Movimiento lateral
- Ocultamiento de artefactos
- Generación personalizada de registros

Definidas estas posibles ventajas de los APTs, es importante generar métodos de monitoreo de integridad de los registros.

Wazuh permite monitorear los registros por default y registros únicos, para realizar esta configuración, se genera un nuevo registro de prueba en el sistema operativo Windows:

Figura 61

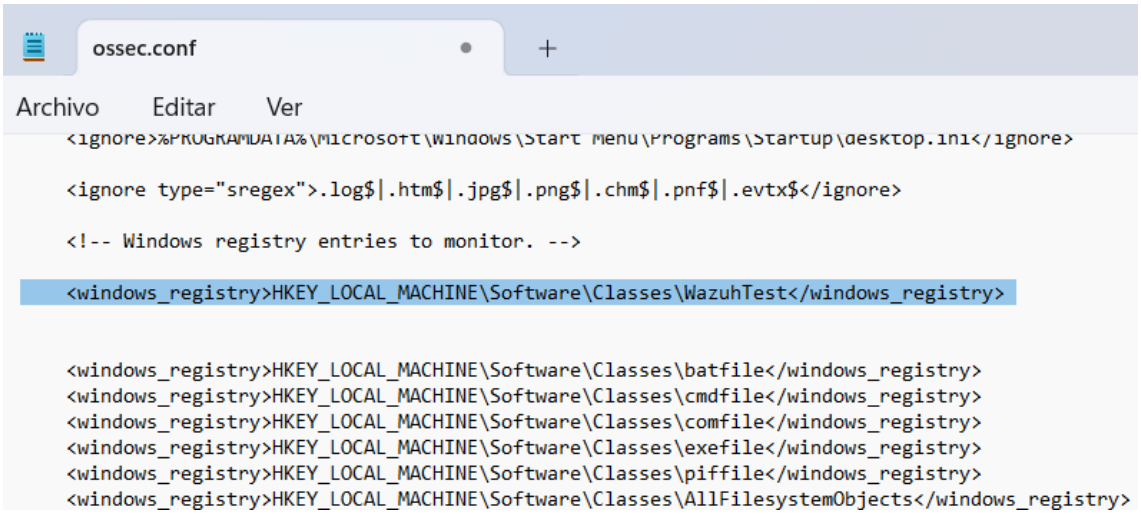
Monitoreo de directorio Windows



Se define este nuevo registro en el archivo de configuración del agente Wazuh. Para esto, se modifica, se agrega el registro al ossec.conf y se reinia el servicio del agente wazuh.

Figura 62

Modificación archivo ossec.conf

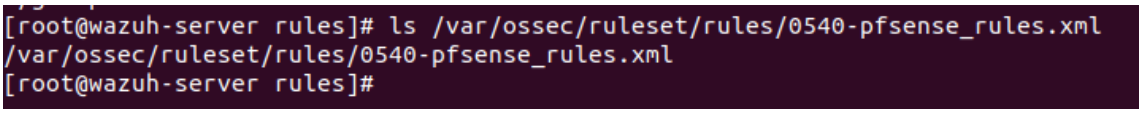


Implementación Regla Pfsense para Wazuh ip única

Se valida que se encuentre activas las reglas por defecto de pfsense para Wazuh.

Figura 63

Validación regla Pfsense en Wazuzh



Nota: En caso de no estar disponible se puede descargar el paquete de reglas de página oficial de Wazuh, REFERENCIA 2

Se valida la regla activa desde el control de pfsense en Wazuh.

Figura 64

Regla Pfsense activa

```
[root@wazuh-server rules]# cat /var/ossec/ruleset/rules/0540-pfsense_rules.xml
<!--
  -  pfSense ruleset
  -  Created by Wazuh, Inc.
  -  Copyright (C) 2015, Wazuh Inc.
  -  This program is a free software; you can redistribute it and/or modify it under the terms of GPLv2.
  ID: 87700-87799
-->

<group name="pfsense,">
  <rule id="87700" level="0">
    <decoded_as>pf</decoded_as>
    <program_name>filterlog</program_name>
    <description>pfSense firewall rules grouped.</description>
  </rule>

  <!-- We don't log firewall events, because they go
    -  to their own log file.
    -->
  <rule id="87701" level="5">
    <if_sid>87700</if_sid>
    <action>block</action>
    <options>no_log</options>
    <description>pfSense firewall drop event.</description>
    <group>firewall_block,pci_dss_1.4,gpg13_4.12,hipaa_164.312.a.1,nist_800_53_SC.7,tsc_CC6.7,tsc_CC6.8,</grou
p>
  </rule>

  <rule id="87702" level="10" frequency="18" timeframe="45" ignore="240">
    <if_matched_sid>87701</if_matched_sid>
    <same_source_ip />
    <description>Multiple pfSense firewall blocks events from same source.</description>
    <mitre>
      <id>T1110</id>
    </mitre>
    <group>multiple_blocks,pci_dss_1.4,pci_dss_10.6.1,gpg13_4.12,hipaa_164.312.a.1,hipaa_164.312.b,nist_800_53
_SC.7,nist_800_53_AU.6,tsc_CC6.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
  </rule>
</group>
[root@wazuh-server rules]# ls /var/ossec/ruleset/rules/0540-pfsense_rules.xml
```

La regla que se incluye en el control de pfsense para wazuh 87702 del archivo 0540-pfsense_rules.xml detecta múltiples eventos de bloqueo de firewall generados por pfSense desde una misma dirección IP en un intervalo de 45 segundos, elevando la alerta a nivel 10 si se supera la frecuencia de 18 eventos. Esta regla utiliza el campo same_source_ip para correlacionar los eventos, indicando un posible patrón de ataque como un escaneo agresivo o un intento de denegación de servicio (DoS). Asociada al ID MITRE ATT&CK T1110 (Brute Force), la alerta puede ayudar a detectar comportamientos maliciosos repetitivos que comprometen la disponibilidad de servicios expuestos, y permite generar respuestas automáticas o investigaciones por parte del equipo de seguridad.

Implementación Regla Pfsense para Wazuh desde varias Ips

Se genera una regla, con la finalidad de detectar intentos de conexiones bloqueados por el firewall en un periodo de tiempo similar al de la regla 87702, con la diferencia que detectará desde múltiples ips de origen, monitoreando un posible ataque de DDoS.

Figura 65

Creación regla múltiples orígenes

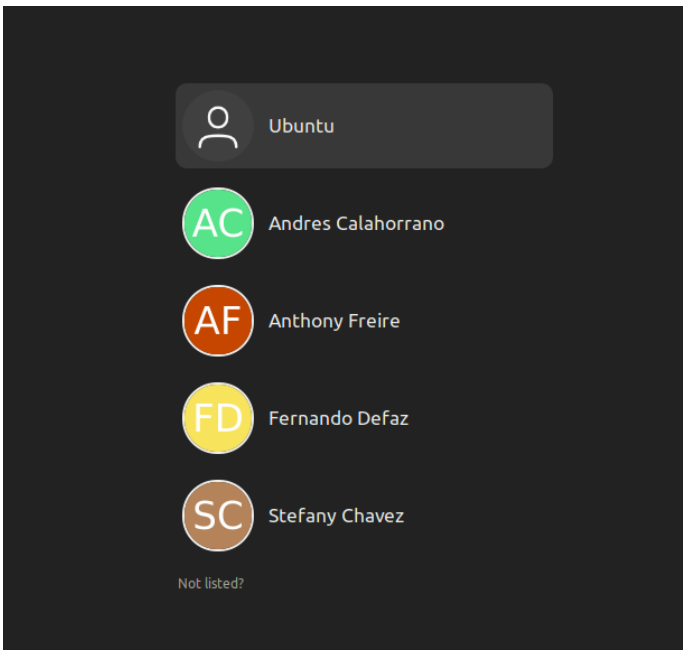
```
<rule id="87703" level="10" frequency="20" timeframe="30" ignore="240">
  <if_matched_sid>87701</if_matched_sid>
  <description>Multiple pfSense firewall bloqueo de eventos de multiples Origenes.</description>
  <mitre>
    <id>T1110</id>
  </mitre>
  <group>multiple_blocks,pci_dss_1.4,pci_dss_10.6.1,gpg13_4.12,hipaa_164.312.a.1,hipaa_164.312.b,nist_800_5
</rule>
```

Acceso no autorizado – Inicios múltiples de sesión fallidos

Para realizar esta prueba se crea los usuarios en el servidor de Ubuntu, un usuario por cada integrante de equipo.

Figura 66

Lista usuarios Ubuntu

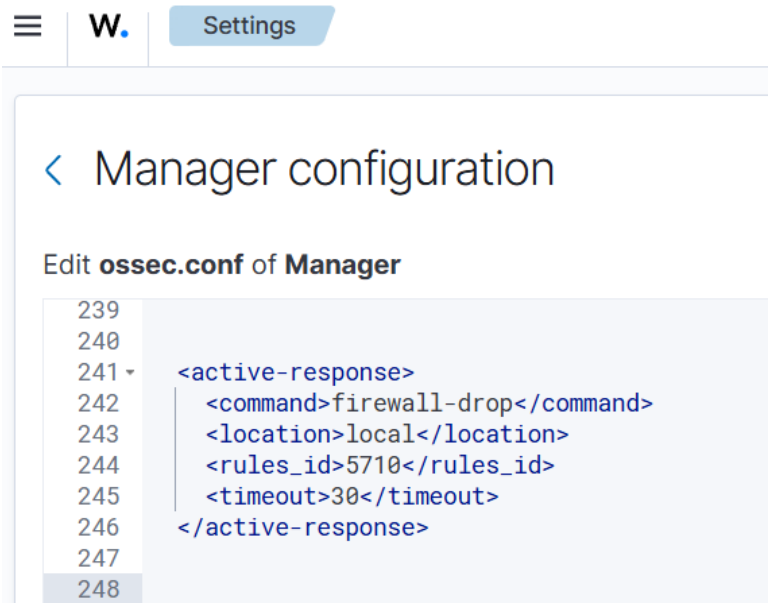


El objetivo del caso de uso es detectar inicios de sesión fallidos, con esto se podrá identificar si un usuario se encuentra probando claves de acceso de otros usuarios o intentos de intrusión en el servidor mediante fuerza bruta.

Se modifica el archivo de configuración del servidor de manager como respuesta activa con la siguiente información:

Figura 67

Configuración del servidor de manager



Donde:

- command define el comando que se va a ejecutar, para este ejemplo se realizará un drop en la regla de firewall que bloqueará al atacante.
- location: local define que solo se ejecute el comando en el agente en el que ocurrió el evento y no en los otros agentes o en el manager.
- rules_id: especifica cual es el ID de la regla de wazuh que deberá activarse para ejecutar esta respuesta.
- timeout: especifica el tiempo del bloqueo temporal, en esta configuración es de 30 segundos, posteriormente, la IP se desbloqueará automáticamente.

Detección de vulnerabilidades

Wazuh adicionalmente cuenta con un módulo de detección de vulnerabilidades que puede utilizarse para temas de bastionado y certificación de servidores. Por defecto viene

desactivado, se deberá ingresar al archivo de configuración de wazuh y modificar el siguiente apartado:

Figura 68

Activación detección de vulnerabilidades desde wazuh

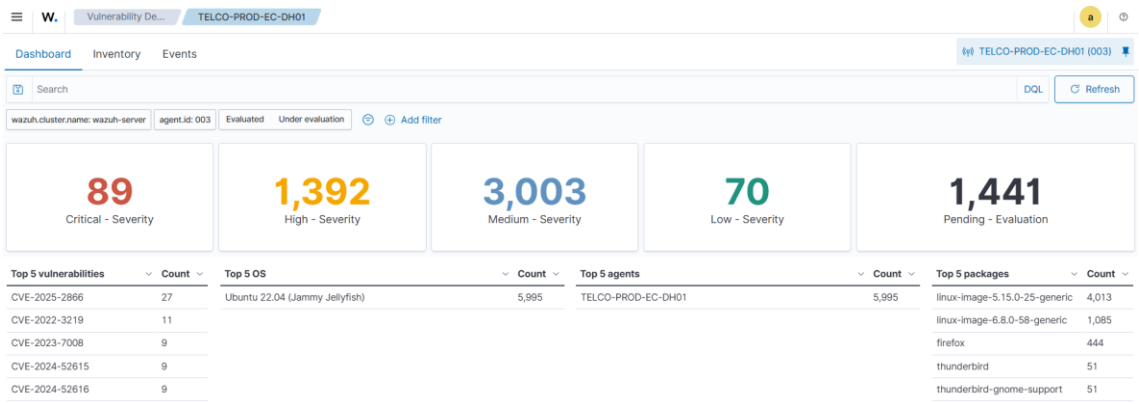
```
<vulnerability-detection>
  <enabled>yes</enabled>
  <index-status>yes</index-status>
  <feed-update-interval>60m</feed-update-interval>
</vulnerability-detection>
```

Generalmente el sistema viene con “no” en la configuración enabled, cambiar el parámetro y configurarlo en yes, reiniciar el servicio del manager.

Posterior a su activación, evidenciamos que wazuh comienza el análisis de vulnerabilidades en los agentes instalados:

Figura 69

Análisis de vulnerabilidades desde wazuh



Es importante tener en consideración que el servidor realiza un full scan cada determinado tiempo, de esta forma, se deberá coordinar con los administradores de los servidores con la finalidad de no afectar a la operatividad y disponibilidad de los servicios levantados.

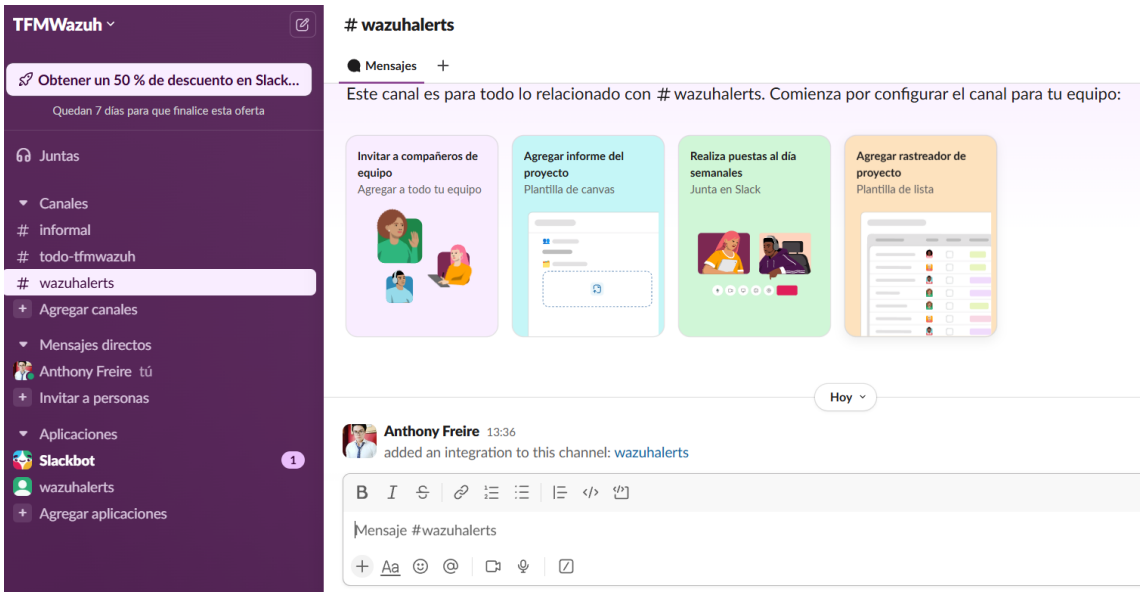
Alertas Slack

Con la finalidad de tener una asertividad y tiempo de respuesta más corto, se desarrolla un sistema de alertamiento. Wazuh permite varias integraciones, se va a desarrollar en el sistema de comunicaciones slack.

En primer lugar, es importante tener un canal de slack destinado a las alertas que se van a enviar desde Wazuh y que cuente con un webhook, una aplicación y un api para la integración.

Figura 70

Canal slack



Posterior a la configuración del canal y el webhook, se debe crear una integración con wazuh, esta integración requiere de la url del webhook que se obtiene del api de slack.

La configuración del archivo de manager de wazuh debe ser la siguiente para la integración y como punto final se debe reiniciar el manager.

Figura 71

Configuración del archivo de manager de wazuh

```
<integration>
  <name>slackAlert</name>
  <hook_url>https://hooks.slack.com/services/[redacted]/hook_url>
  <alert_format>json</alert_format>
</integration>
```

Con la finalidad de hacer más asertivo el alertamiento y no inundar el canal de slack con muchas notificaciones, se puede dar seguimiento solo a las reglas que pueden presentar un riesgo para la operación configurando el parámetro rule_id.

Figura 72

Configuración reglas para alertas slack

```
<integration>
  <name>slack</name>
  <hook_url>https://hooks.slack.com/services/T0
  <alert_format>json</alert_format>
  <rule_id>5712</rule_id>
</integration>
```

Misp

En una lista de IOC's se realiza la descarga de la lista de ips

Figura 73

Lista de IOC's

```
oot@telcodebhp:~# curl -k -H "Authorization: uNY1ZxiMzt835cFpPQAOxpSBAkjg4zI6xqCg0tRN" -H "Accept: application/json"
https://misp.local/attributes/restSearch/download/ip-src"
```

Para la integración con wazuh en los IOCs de los eventos, se descarga las IPs mediante el API y se guarda en un archivo .txt, Se genera un programa en python que realiza la descarga mediante el API y un cron que ejecutará el proceso automáticamente.

Figura 74

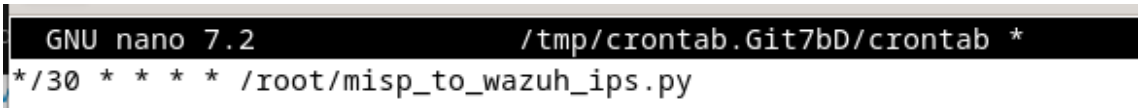
Código python

```
response = requests.post(
    f"{MISP_URL}/attributes/restSearch",
    headers=headers,
    data=json.dumps(payload),
    verify=VERIFY_SSL
)
response.raise_for_status()
data = response.json()
attributes = data.get("response", {}).get("Attribute", [])
ips = [attr["value"] for attr in attributes if "value" in attr]
os.makedirs(os.path.dirname(OUTPUT_PATH), exist_ok=True)
with open(OUTPUT_PATH, "w") as outfile:
    outfile.write("\n".join(ips) + "\n")
```

Se genera el cron que cada 30 minutos actualizará la lista de IPs de MISP.

Figura 75

Creación cron cada 30 segundos



Se evidencia que se genere el archivo con las ips descargadas de MISP y se configura la lista que consumirá wazuh en el ossec.conf.

Figura 76

Archivo con las ips descargadas de MISP

```
<ruleset>
  <!-- Default ruleset -->
  <decoder_dir>ruleset/decoders</decoder_dir>
  <rule_dir>ruleset/rules</rule_dir>
  <rule_exclude>0215-policy_rules.xml</rule_exclude>
  <list>etc/lists/audit-keys</list>
  <list>etc/lists/amazon/aws-eventnames</list>
  <list>etc/lists/security-eventchannel</list>
  <list>etc/lists/misp_ips.txt</list>
```

Se descarga los iocs sha256 de los eventos y se obtine una lista para que sea consumida por wazuh.

Figura 77

Descarga de iocs sha256

```
[root@wazuh-server bin]# cat /var/ossec/etc/lists/misp_sha256.txt
fd8db0e2c5634135b1b91e29d0909e4aaea6ac479577915f724e8fe340eb3dbd
```

Se genera un ruleset que permita ingresar los sha256 descargados de fuentes de inteligencia, esto ayuda a fortalecer la postura de seguridad y mejorar la madurez de ciberinteligencia.

Figura 78

Creacion de ruleset

```
<ruleset>
  <!-- Default ruleset -->
  <decoder_dir>ruleset/decoders</decoder_dir>
  <rule_dir>ruleset/rules</rule_dir>
  <rule_exclude>0215-policy_rules.xml</rule_exclude>
  <list>etc/lists/audit-keys</list>
  <list>etc/lists/amazon/aws-eventnames</list>
  <list>etc/lists/security-eventchannel</list>
  <list>etc/lists/misp_sha256.cdb</list>
  <!-- User-defined ruleset -->
  <decoder_dir>etc/decoders</decoder_dir>
  <rule_dir>etc/rules</rule_dir>
</ruleset>
```

Se genera una alerta que haga coincidencia en caso de encontrar el sha256 en los archivos del file integrity monitoring de wazuh.

Figura 79

Generando alerta

```
<group name="Grupo5Rules">

  <rule id="87709" level="10">
    <field name="sha256_after">cdb:/var/ossec/etc/lists/misp_sha256.cdb</field>
    <description>Wazuh: Hash SHA256 detectado en CDB list MISP</description>
    <group>malware,file_integrity,misp,</group>
  </rule>
```

Capítulo 4

Pruebas de Concepto y Análisis de Resultados

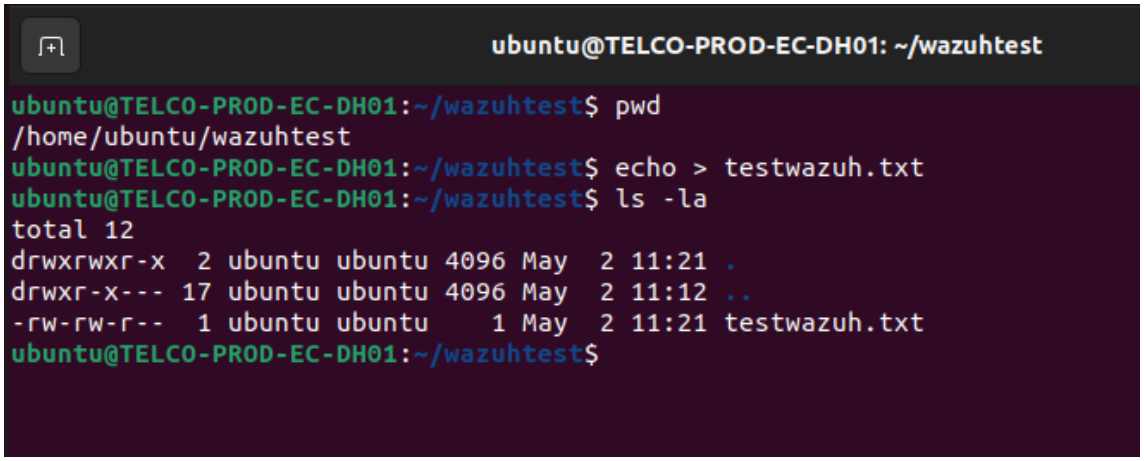
Creación de archivos maliciosos Linux.

Prueba

En el directorio de pruebas, se agrega un nuevo archivo con la finalidad de evidenciar la comunicación y monitorear la integridad de los archivos.

Figura 80

Creación de archivo para validar comunicación y monitoreo de regla

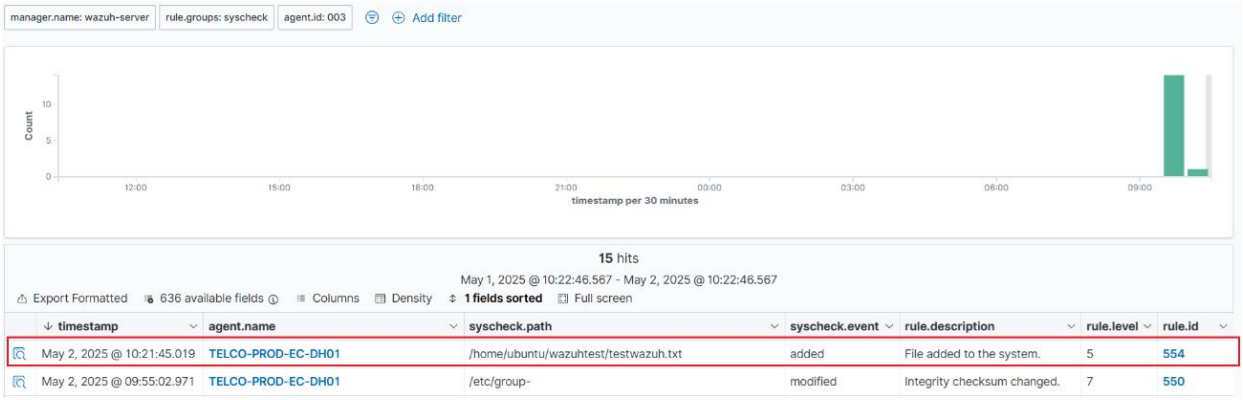


Análisis de Resultado

En Wazuh en un corto tiempo se evidencia un evento, que muestra la creación del nuevo archivo en el directorio.

Figura 81

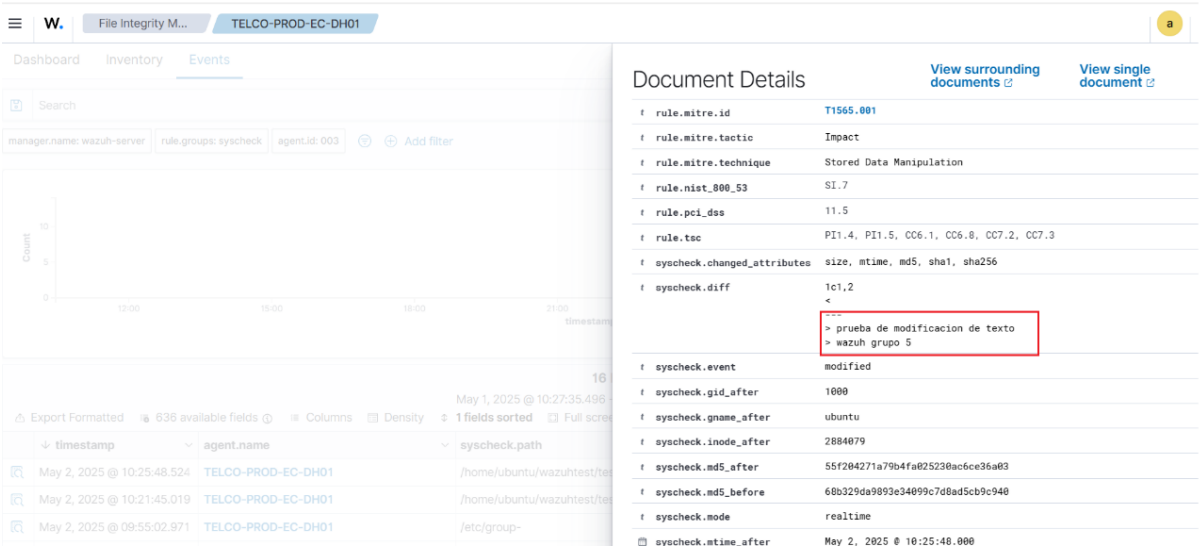
Evento de detección y modificación de archivo en SIEM



Para comprobacion, se modifica el texto del archivo, se evidencia que Wazuh tiene la capacidad de validar el cambio y de leer el texto modificado.

Figura 82

Visualización Archivo modificado desde Wazuh



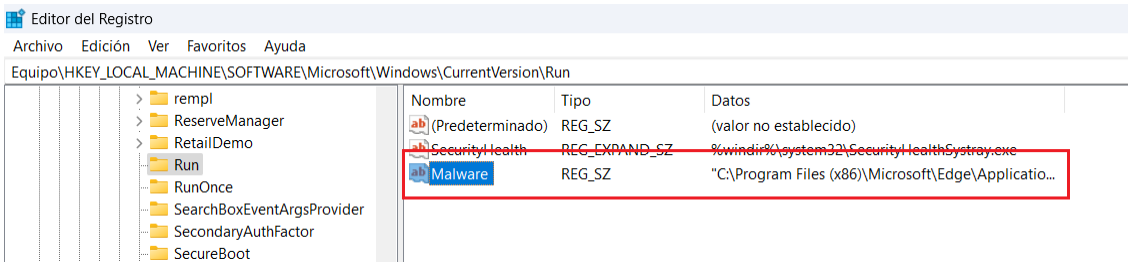
Modificación de registros del sistema en Windows

Prueba

Con el objetivo de ganar persistencia, se modifica el registro “Run” que permite inicializar una aplicación cada vez que el sistema se ponga en marcha. Para evidenciar que Wazuh pueda detectar los cambios en el registro de prueba.

Figura 83

Modificación registro de Windows



Detección

El SIEM notifica la modificación del archivo de Windows.

Figura 84

Detección de la modificación de Archivo de Windows Desde Wazuh

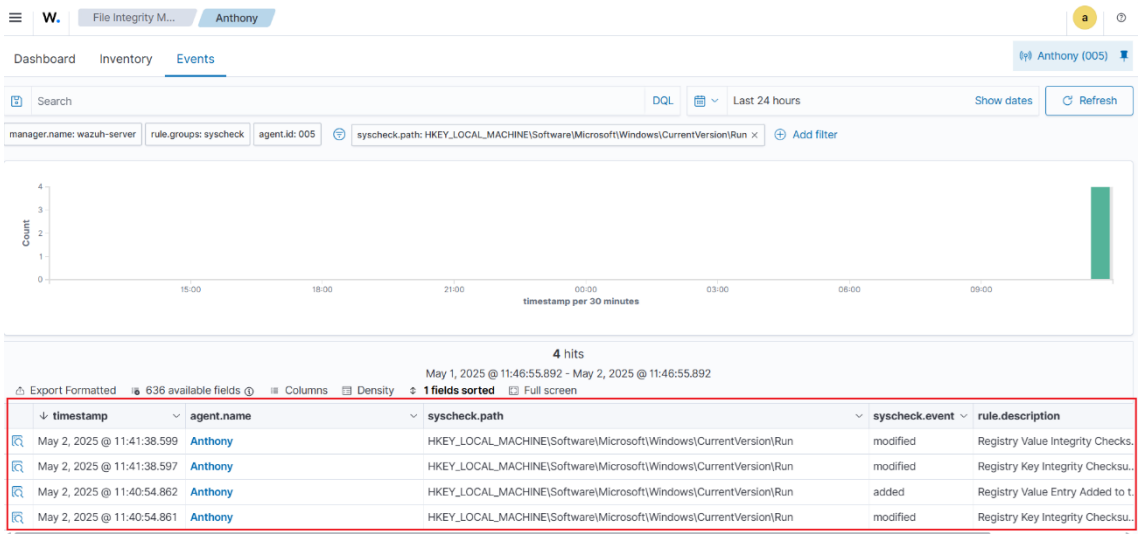
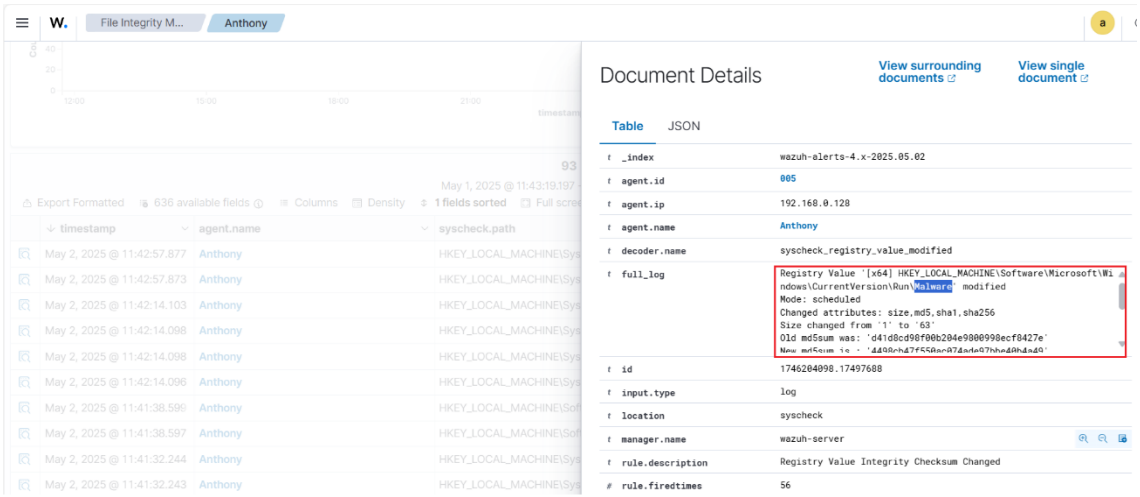


Figura 85

Visualización de Archivo Modificado de Windows desde Wazuh



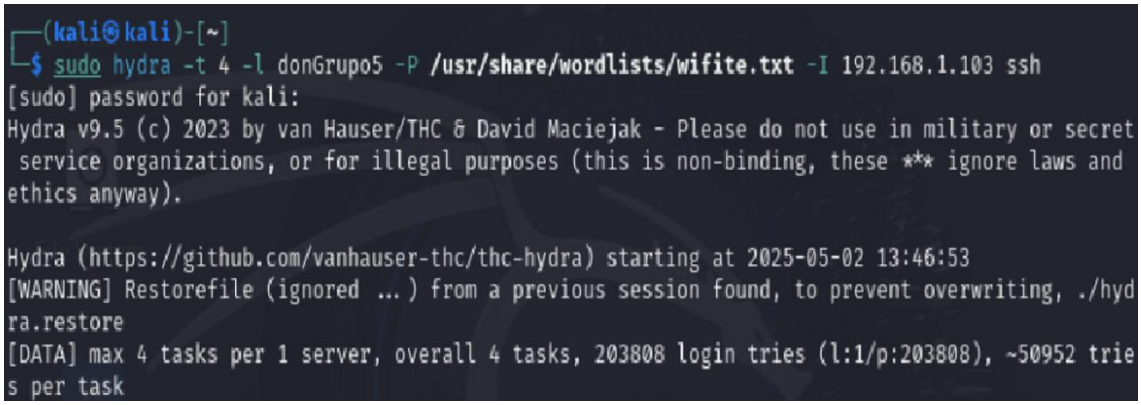
Ataque de fuerza bruta por SSH

Ejecución

Para desarrollar un ataque de fuerza bruta se ejecuta hydra con la lista wifite.txt en Kali hacia el servidor de Ubuntu.

Figura 86

Ejecución Ataque Fuerza Bruta



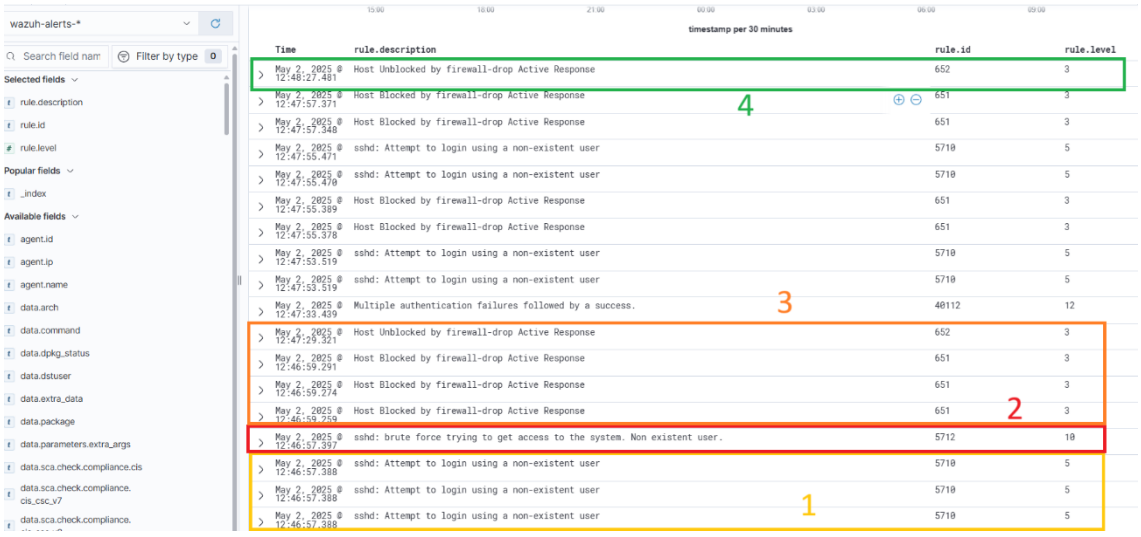
Nota: Indica la ejecución de un ataque de fuerza bruta, despliega 4 hilos simultáneos como hilos de ejecución para efectivizar el ataque. Prueba inicios de sesión con un usuario no registrado utilizando una lista de contraseñas.

Detección

En Wazuh se detecta el comportamiento de múltiples intentos fallidos de autenticación ssh y responde con un bloqueo del usuario con un tiempo de espera de 30 segundos.

Figura 87

Detección Ataque de Fuerza Bruta desde Wazuh



En el análisis de detección de Wazuh tenemos

- Detección de múltiples intentos de login SSH.
- Detección del intento de fuerza bruta.
- Bloqueo del host por la regla activa del firewall.
- Desactivación de la regla de bloqueo posterior al tiempo de timeout.

Figura 88

Detección de múltiples intentos de login SSH

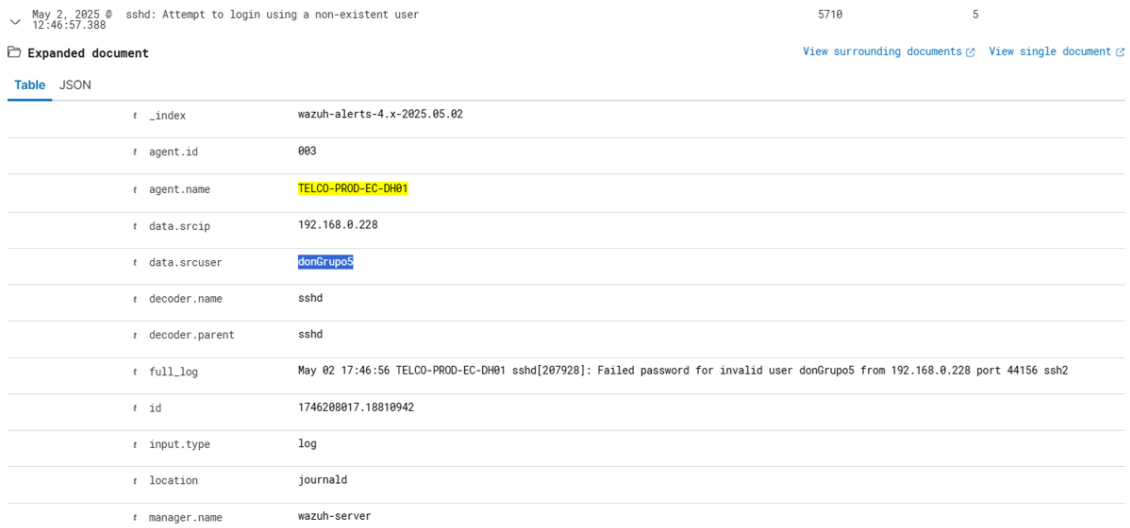
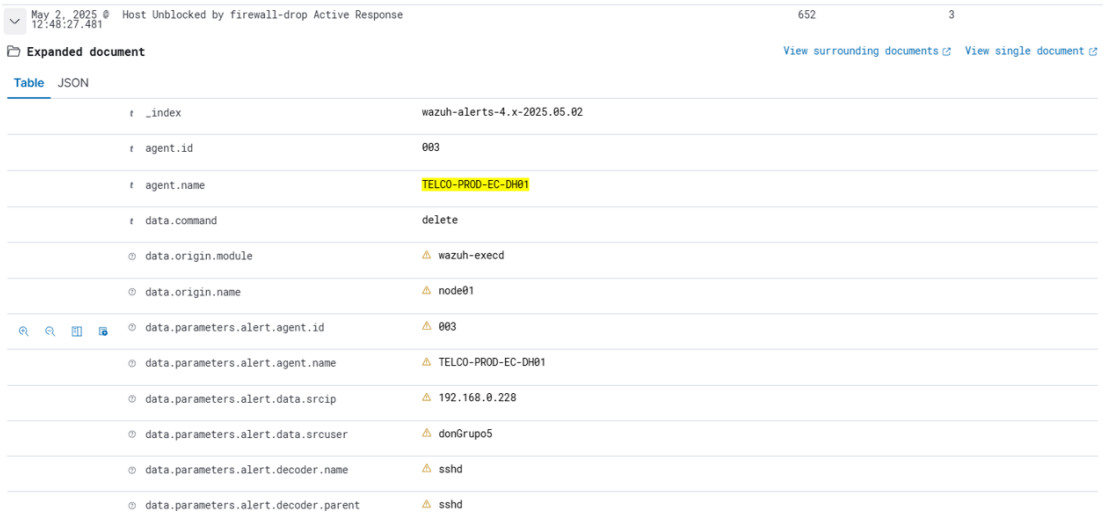


Figura 89

Bloqueo del host por la regla activa del firewall

Figura 90

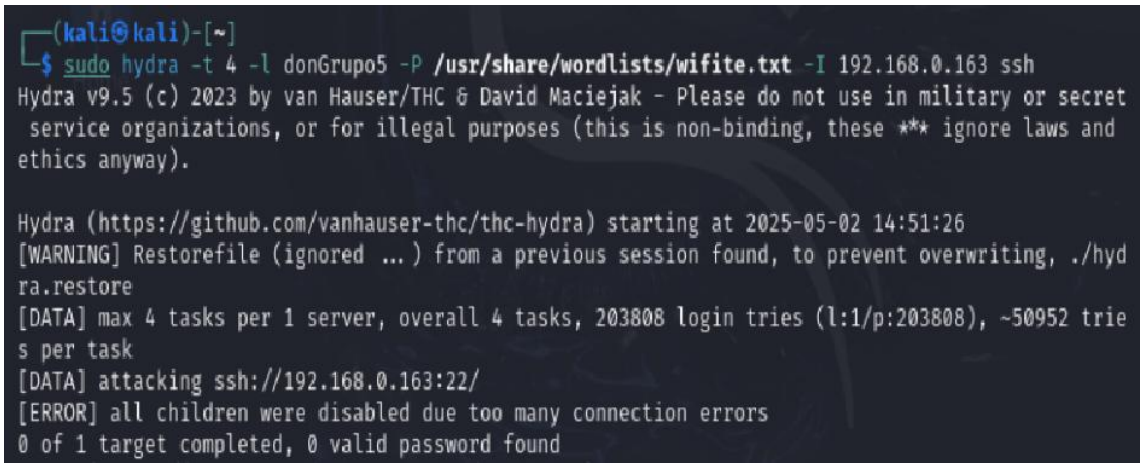
Desactivación de la regla de bloqueo posterior al tiempo de timeout



El ataque de fuerza bruta se ve afectado por el bloqueo y se detiene la ejecución de forma automática del lado del atacante.

Figura 91

Interrupción del ataque desde el lado del atacante



Notificación de eventos slack

Ejecución

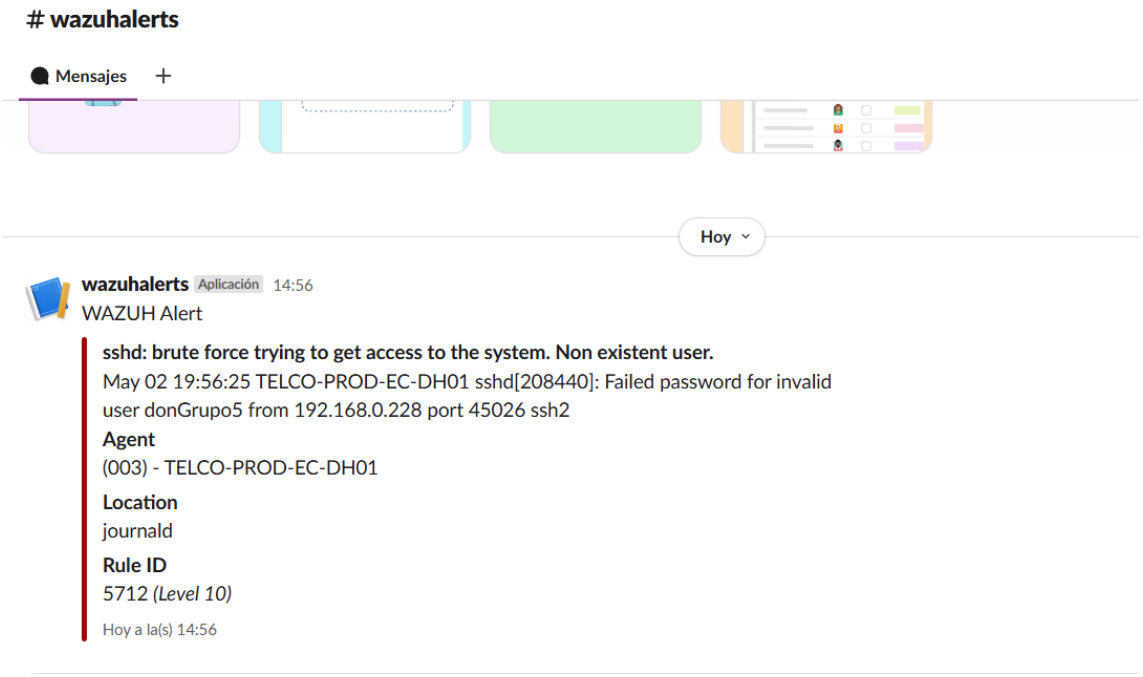
Para detectar el evento de slack, se ejecutará nuevamente el ataque de fuerza bruta desde el servidor de Kali con la siguiente configuración.

Detección

La detección fue realizada correctamente en el dashboard de wazuh y la alerta fue enviada al canal dedicado en slack

Figura 92

Alerta slack



Regla Suricata IDS

Las reglas implementadas en suricata permiten varias detecciones, mediante el caso de uso se valida que exista la regla “SURICATA Applayer No TLS after STARTTLS”.

Figura 93

Validación regla suricata

```
ubuntu@TELCO-PROD-EC-IDS:/etc/suricata/rules$ grep -R "2260004" /etc/suricata/rules/suricata.rul
es
alert tcp any any -> any any (msg:"SURICATA Applayer No TLS after STARTTLS"; flow:established; a
pp-layer-event:applayer_no_tls_after_starttls; flowint:applayer.anomaly.count,+,1; classtype:pro
tocol-command-decode; sid:2260004; rev:2;)
ubuntu@TELCO-PROD-EC-IDS:/etc/suricata/rules$
```

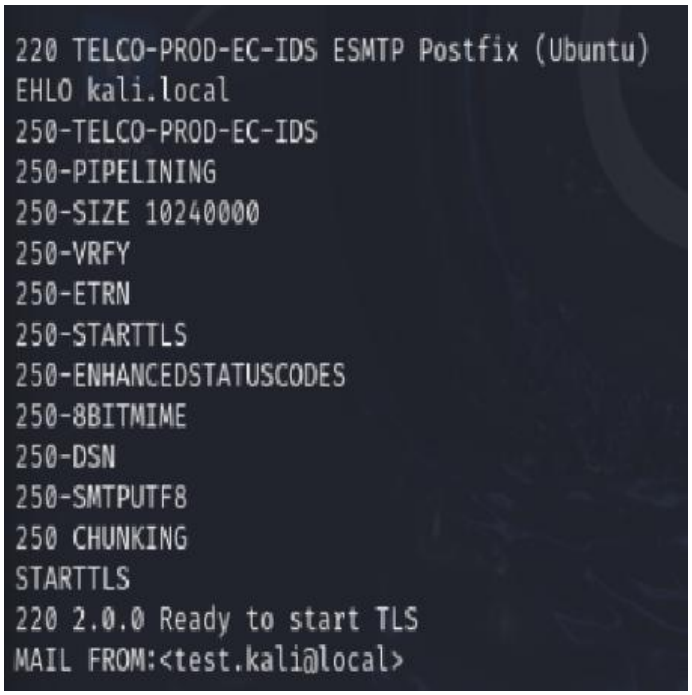
Prueba

Desde el servidor de Kali vamos a ejecutar el STARTTLS, el cual recibe un comando e inicia el handshake TLS, si la comunicación continúa con un texto en claro detectará la regla Suricata. Su importancia radica en que puede existir un intento de manipulación maliciosa del canal seguro o una configuración errónea.

Desde Kali ejecutamos el STARTTLS y enviamos un texto en claro simulando la manipulación maliciosa.

Figura 94

Simulación de un ataque



Validamos que en el log del IDS se haya registrado el evento correspondiente

Figura 95

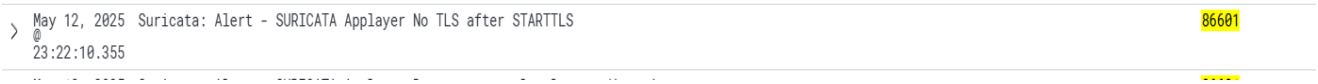
Registro del evento en IDS

```
ubuntu@TELCO-PROD-EC-IDS:/etc/suricata/rules$ sudo tail -n 20 /var/log/suricata/eve.json | grep
2260004
{"timestamp":"2025-05-13T00:03:04.529116-0400","flow_id":564384992808483,"in_iface":"enp0s3","ev
ent_type":"alert","src_ip":"192.168.1.103","src_port":25,"dest_ip":"192.168.0.228","dest_port":4
5894,"proto":"TCP","pkt_src":"wire/pcap","metadata":{"flowints":{"applayer.anomaly.count":3}},"a
lert":{"action":"allowed","gid":1,"signature_id":2260004,"rev":2,"signature":"SURICATA Applayer
No TLS after STARTTLS","category":"Generic Protocol Command Decode","severity":3},"app_proto":"f
ailed","app_proto_orig":"smtp","app_proto_expected":"tls","direction":"to_client","flow":{"pkts_
toserver":8,"pkts_toclient":6,"bytes_toserver":589,"bytes_toclient":648,"start":"2025-05-13T00:0
2:26.655694-0400","src_ip":"192.168.0.228","dest_ip":"192.168.0.164","src_port":45894,"dest_port
":25}}
```

Adicional, se valida la alerta en Wazuh.

Figura 96

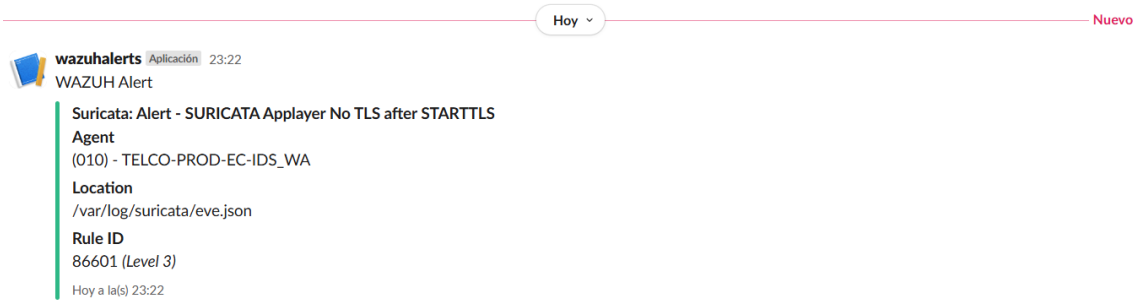
Alerta wazuh para ataque suricata



Como punto final, se genera una alerta en slack para las reglas suricata.

Figura 97

Alerta slack para suricata

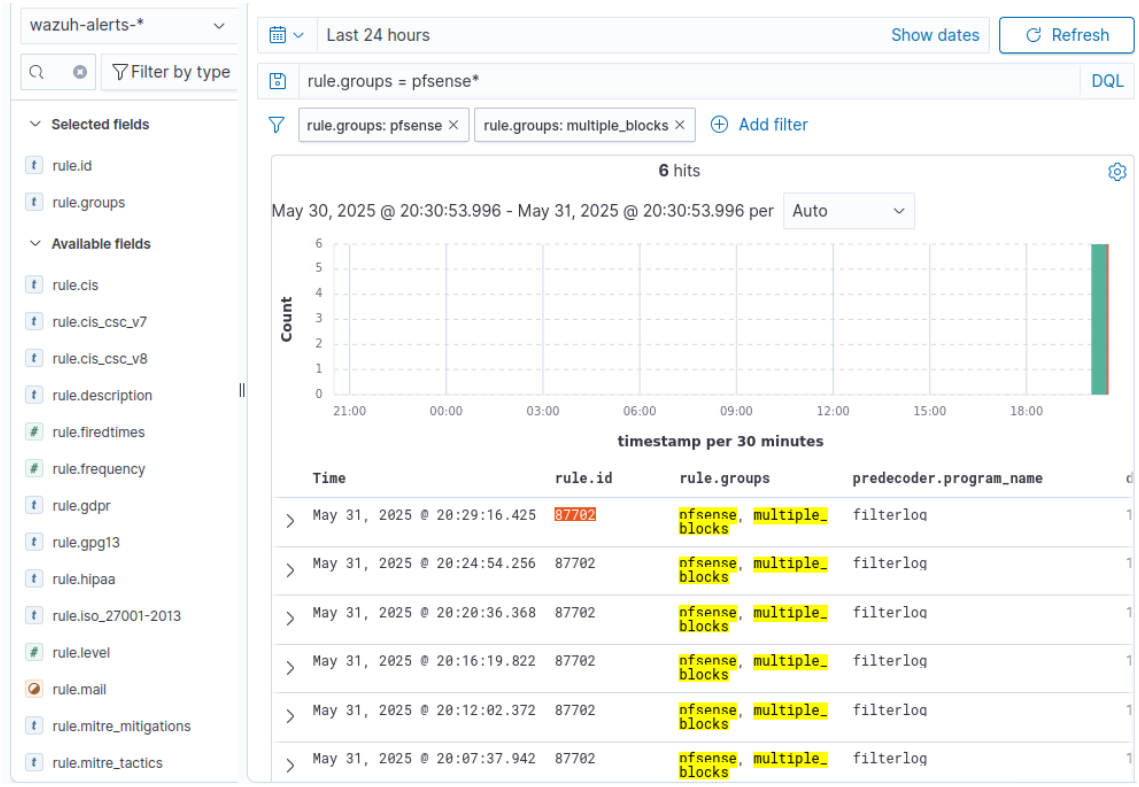


Resultado de Implementación Regla Pfsense para Wazuh ip única

Se evidencia que llegan los logs y que se están generando las alertas en el SIEM

Figura 98

Captura logs Pfsense en Wauzh



Resultado de Implementación Regla Pfsense para Wazuh desde varias Ips

Se realiza prueba de funcionamiento, se genera un comando que envía tráfico desde múltiples ips sobre el puerto 445.

Figura 99

Envió de tráfico por puerto 445

```
ubuntu@TELCO-PROD-EC-IDS:~$ sudo hping3 -S -p 445 192.168.1.1 --flood --rand-source
HPING 192.168.1.1 (enp0s3 192.168.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Desde Firewall podemos evidenciar la gran cantidad de intentos bloqueados a múltiples ips de origen.

Figura 100

Validación logs desde Firewall

✕	May 31 20:39:53	LAN	94.37.219.113:31819	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	62.206.170.129:31839	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	167.59.106.77:31841	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	171.93.58.248:31853	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	219.109.144.65:31882	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	84.163.178.254:31880	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	93.178.235.122:31890	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	167.11.103.150:31893	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	129.253.4.58:31896	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	15.64.144.135:31908	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	42.154.215.133:31916	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	212.42.111.62:31951	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	84.33.65.12:31968	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	219.119.84.41:31982	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	66.84.254.22:31976	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	114.170.145.209:32038	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	200.211.2.114:32130	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	155.116.121.122:32136	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	129.132.210.161:32162	192.168.1.1:445	TCP:S
✕	May 31 20:39:53	LAN	174.129.21.202:32164	192.168.1.1:445	TCP:S

Como respuesta preventiva para Wazuh generaremos un alertamiento en slack de la alerta

Figura 101

Configuración Alerta Slack

```
<integration>
  <name>slack</name>
  <hook_url>https://hooks.slack.com/services/T0
    </hook_url>
  <alert_format>json</alert_format>
  <rule_id>87703</rule_id>
</integration>
```

Desde Wazuh evidencia la alerta se recibe correctamente

Figura 102

Alerta Obtenida desde Wazuh

WAZUH Alert

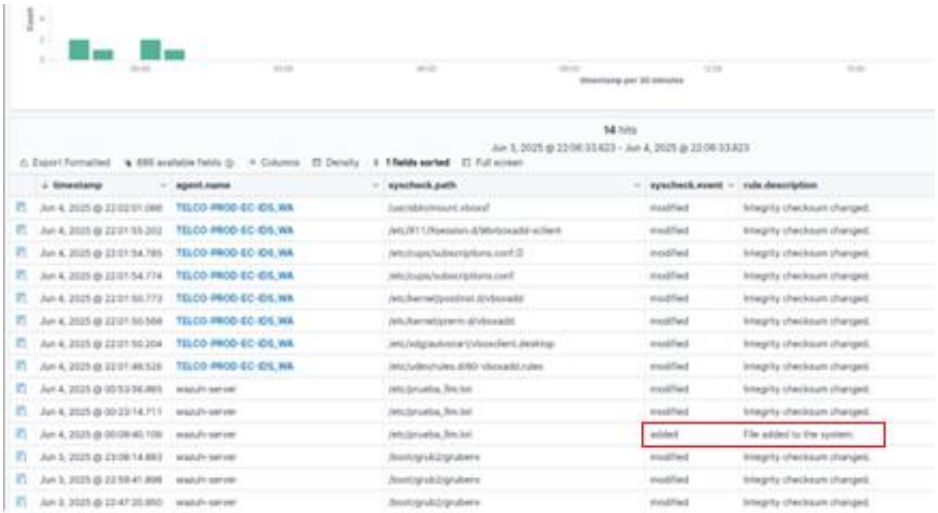
Multiple pfSense firewall bloqueo de eventos de multiples Origenes.
May 31 18:55:40 filterlog:
4,,,1000000103,em0,match,block,in,4,0x0,,64,17526,0,DF,17,udp,395,192.168.0.1,192
.168.0.255,59350,20002,375
Agent
(000) - wazuh-server
Location
/var/log/pfsense_wazuh.log
Rule ID
87703 *(Level 10)*
Hoy a la(s) 21:21

Resultado misp

En siem se tiene un alertamiento en el sistema de validación de eventos syscheck para archivos agregados maliciosos.

Figura 103

Alerta wazuh para misp



Capítulo 5

Conclusiones

De acuerdo con el análisis elaborado de las alternativas open source se determina que la herramienta Wazuh es viable como una solución de seguridad debido a su capacidad avanzada de protección, detección, respuesta ante amenazas digitales y una gran escalabilidad posicionándose como un SIEM robusto, confiable y de bajo costo.

La integración de sistemas IDS, firewalls, sistemas operativos y fuentes de ciberinteligencia demostró la capacidad del SIEM para centralizar eventos de distintas fuentes en un único entorno de análisis, permitiendo correlaciones más certeras y alertas efectivas en tiempo real.

La ejecución del proyecto fue el escenario ideal para aplicar de manera práctica los conocimientos adquiridos durante el programa de maestría, consolidando competencias en análisis de riesgos, diseño de arquitecturas seguras y gestión de incidentes de seguridad.

La integración de feeds de Threat Intelligence es una estrategia primordial que fortalece la detección y prevención de amenazas en los entornos digitales. Aprovechando fuentes actualizadas de información acerca de comportamientos maliciosos o reputación de dominios es posible tomar las medidas preventivas ante posibles ataques, optimizar el tiempo de respuesta ante incidentes reduciendo los riesgos y el impacto de los mismos.

El sistema de reporte de vulnerabilidad abiertas detectadas en los servidores desplegado en Wazuh permite gestionar el bastionado de seguridad con la finalidad de evitar posibles brechas de seguridad por explotaciones de actores maliciosos que pueden utilizarlas como backdoor.

Pfense ofrece un sistema robusto de networking con funcionalidad de equipos de alto costo, como la implementación de un firewall, servidor DHCP y creación de zonas para

diferentes propósitos de seguridad. Es importante que la comunicación entre las zonas mencionadas esté correctamente mapeada en las reglas de firewall.

El firewall se encuentra configurado con todas las conexiones bloqueadas, esto asegura un zero trust a nivel de comunicaciones entre los servidores. Las reglas se irán generando en base a las necesidades del proyecto.

Recomendaciones

Es esencial capacitar de formar continua al equipo encargado del funcionamiento de un SIEM, ya que su comprensión y gestión influirán en la efectividad del sistema frente a problemas de seguridad.

Se aconseja llevar a cabo una evaluación periódica de las reglas de correlación, umbrales y patrones definidos, para reducir los falsos positivos y mejorar la respuesta frente a amenazas reales.

Aunque se han utilizado herramientas de código abierto, es esencial que el sistema y sus elementos se encuentren con los parches de seguridad actualizados para reducir las vulnerabilidades nuevas y optimizar el funcionamiento general del entorno.

Para mejorar la automatización de respuesta ante incidentes, se recomienda contemplar la posible conexión del SIEM con sistemas SOAR (Orquestación de Seguridad, Automatización y Respuesta), que faciliten respuestas automáticas a determinadas amenazas.

Debido a la evolución continua de los ciberdelitos, se sugiere realizar un seguimiento permanente de las tendencias y amenazas, integrando nuevas fuentes de inteligencia cibernética al sistema que faciliten la previsión de los riesgos.

Es importante tomar en cuenta el versionamiento de los componentes de integración y Wazuh, esto debido a la compatibilidad de los agentes con el manager

Referencias

Osazuwa, O. M. C. (2023). Confidentiality, integrity, and availability in network systems: A review of related literature. International Journal of Innovative Science and Research Technology, 8(12), 1946–1951. https://www.researchgate.net/publication/377535526_Confidentiality_Integrity_and_Availability_in_Network_Systems_A_Review_of_Related_Literature

Mitchell, O. M. C. (2023). Confidentiality, integrity, and availability in network systems: A review of related literature (Tesis de pregrado). Escuela Politécnica Nacional. https://bibdigital.epn.edu.ec/bitstream/15000/25977/1/CD%2014683.pdf

National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/nist.cswp.29

Cybersecurity and Infrastructure Security Agency (CISA). (s. f.). Elastic SIEM | CISA. https://www.cisa.gov/resources-tools/services/elastic-siem

Areitio Bertolín, J. (2019, enero 25). Integración SIEM-SOC: Ciberseguridad, privacidad, motores clave y esencia de la accesibilidad y sostenibilidad real y creíble. Interempresas. https://www.interempresas.net/Electronica/Articulos/232650-Integracion-SIEM-SOC-Ciberseguridad-privacidad-motores-clave-esencia-accesibilidad.html

Sreekanth. (2025, mayo 16). A deep dive into open source SIEM: Features, benefits & best practices (2025). Worksent. https://worksent.com/blog/open-source-siem/

Palo Alto Networks. (s. f.). What is Security Information Event Management (SIEM) software? https://www.paloaltonetworks.com/cyberpedia/what-is-siem-software

Maayan, G. D., & Maayan, G. D. (2024, 17 enero). Security Information and Event Management (SIEM): Trends and Predictions for 2024.

GEEKrar. https://www.geekrar.com/security-information-and-event-management-siem-trends-and-predictions-for-2024/

Leyden, J. (2025, 26 febrero). 4 key trends reshaping the SIEM market. CSO Online. https://www.csoonline.com/article/3829750/4-key-trends-reshaping-the-siem-market.html

Centro Nacional de Ciberseguridad (CNCS). (2020). Guía de controles críticos de ciberseguridad: Controles CIS V7. https://cncs.gob.do/wp-content/uploads/2020/07/Guia-de-Controles-Criticos-de-Ciberseguridad-Controles-CIS-V7.pdf

Katherine, C. S. G. (2024, 1 julio). Implementación de un siem para la defensa activa ante intrusiones en la red: implementación de un siem para la defensa activa ante un ataque de fuerza bruta. http://bibdigital.epn.edu.ec/handle/15000/25977

Colombia, B. (2023, 30 octubre). 3 tipos de riesgos de ciberseguridad más comunes - Bitso Blog. Bitso. https://blog.bitso.com/es-co/seguridad-co/tipos-de-riesgos-de-ciberseguridad?utm_source=chatgpt.com

MITRE ATT&CK®. (s. f.). https://attack.mitre.org/

Kaspersky official blog. (2025, 29 mayo). Kaspersky Official Blog. https://www.kaspersky.com/blog/

Lumu Technologies. (2024). Lumu Compromise Report 2024. https://lumu.io/resources/compromise-report-2024/

Geeks for Geeks, 2024. Características del software y su clasificación. https://www.geeksforgeeks.org/caracteristicas-del-software/

Uriarte, J. M. (18 de octubre de 2019). Software libre. Enciclopedia de Humanidades. Recuperado de https://humanidades.com/software-libre/

Orozco Lara, F. R., Molina Miranda, M. F., Bonilla Alejandro, S. B., & Ramírez Marcillo, J. L. (2024). Análisis del rendimiento de soluciones SIEM de código abierto. Polo del Conocimiento. Recuperado de https://polodelconocimiento.com/ojs/index.php/es/article/view/8807/0

Astrid, W. B. L. (2024, 1 agosto). Implementación de un sistema SIEM con tecnologías Open-Source. https://repositorio.usm.cl/entities/tesis/49d9ac50-44d2-45b0-bbb5-f13654ab3da1

Wazuh Documentation. (2024). Wazuh capabilities: Network monitoring, host intrusion detection, and scalability. https://documentation.wazuh.com/current/user-manual/capabilities/

Security Onion Solutions LLC. (2024). Security Onion documentation: Network monitoring and host detection. Recuperado el 1 de junio de 2025, de https://securityonion.net/docs/

Elastic N.V. (2024). Elastic Security: Machine learning and threat detection. https://www.elastic.co/guide/en/security/current/index.html

Fortinet. (2024). Informes de analistas de Gartner, Forrester y otros. https://www.fortinet.com/lat/solutions/analyst-reports?

Gartner. (s.f.). Wazuh - The Open-Source Security Platform. Gartner Peer Insights. https://www.gartner.com/reviews/market/security-information-event-management/vendor/wazuh/product/wazuh-the-open-source-security-platform

Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Ciberseguridad con un presupuesto ajustado: evaluación de la seguridad y el rendimiento de las soluciones SIEM de

código abierto para pymes. *PLoS ONE, 19*(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

SafeNet. (2023, 18 de diciembre). Wazuh: un análisis profundo de la arquitectura y módulos con SafeNet. SafeNet Blog. https://blog.safenet.tech/wazuh-a-deep-dive-into-architecture-and-modules-with-safenet/

Kumar, P., & Biju, A. (2023). Wazuh SIEM para ciberseguridad y mitigación de amenazas en la industria de la confección. International Journal of Engineering Materials and Manufacture, 4(2), 267–274. https://doi.org/10.37622/IJEMM/4/2/279

Ramírez Quevedo, L. (2024). Tecnologías de defensa frente a inteligencia de amenazas y ciberataques. Revista Innova Research Journal, 9(1), 127–139. https://revistas.itecsur.edu.ec/index.php/inndev/article/view/94/66

De Pablo Bobadilla, V. T. L. E. (2024, 25 agosto). *Fundamentos de la inteligencia de amenazas cibernéticas: estrategias y técnicas para la protección.* Ciberprisma - Alianza Por la Ciberseguridad. https://ciberprisma.org/2024/08/25/fundamentos-de-la-inteligencia-de-amenazas-ciberneticas-estrategias-y-tecnicas-para-la-proteccion/

Alzahrani, I. Y., Lee, S., & Kim, K. (2024). Enhancing Cyber-Threat Intelligence in the Arab World: Leveraging IoC and MISP Integration. *Electronics*, *13*(13), 2526. https://doi.org/10.3390/electronics13132526

Vandeplas, C., Iklody, A., Mokaddem, S., Studer, C., Ziegler, A., Clement, S., & Dulaunoy, A. (2024). MISP: Open Source Threat Intelligence and Sharing Platform. https://misp-project.org/

Filigran. (2025). OpenCTI: Open-source cyber threat intelligence platform. https://filigran.io/solutions/open-cti/

AT&T Cybersecurity. (2024). AlienVault Open Threat Exchange (OTX). Recuperado de https://otx.alienvault.com/

Abuse.ch. (2024). Abuse.ch: Malware Information Sharing Platform. https://abuse.ch/

TheHive Project. (2024). TheHive: Scalable, Open Source and Free Security Incident Response Platform. https://thehive-project.org/

Anexo

Enlace de TFM: https://1024terabox.com/s/1j15kCz5ZLXNlQl8SZgIavg