Universidad Tecnológica ECOTEC

FACULTAD DE INGENIERÍAS, ARQUITECTURA Y CIENCIAS DE LA NATURALEZA

Título del trabajo:

IMPLEMENTACIÓN Y GESTIÓN DE UNA PLATAFORMA DE SEGURIDAD INTEGRAL PARA LA INFRAESTRUCTURA DE CHEVYPLAN

Línea de Investigación:

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Modalidad de titulación:

TRABAJO DE INTEGRACIÓN CURRICULAR

Carrera/programa:

SISTEMAS INTELIGENTES

Título a obtener:

INGENIERO EN SISTEMAS INTELIGENTES

Autor (a):

FRANKLIN ANDRÉ CRUZ SANDOVAL

Tutor:

ING. MARCOS ANTONIO ESPINOZA MINA, PHD.

SAMBORONDÓN - ECUADOR

2024

ANEXO No. 9

PROCESO DE TITULACIÓN
CERTIFICADO DE APROBACIÓN DEL TUTOR

Samborondón, 19 de diciembre de 2024

Magíster
Erika Ascencio
Facultad de Ingenierías, Arquitectura y Ciencias de la Naturaleza
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: IMPLEMENTACIÓN Y GESTIÓN DE UNA PLATAFORMA DE SEGURIDAD INTEGRAL PARA LA INFRAESTRUCTURA DE CHEVYPLAN, fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para su elaboración, por lo que se autoriza al estudiante: **FRANKLIN ANDRÉ CRUZ SANDOVAL,** para que proceda con la presentación oral del mismo.

ATENTAMENTE,

Firmado electrónicamente por:
MARCOS ANTONIO ESPINOZA MINA

Ing. Marcos Antonio Espinoza Mina, PhD.

Tutor

ANEXO No. 10

PROCESO DE TITULACIÓN
CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS
DEL TRABAJO DE TITULACIÓN

Habiendo sido revisado el trabajo de titulación TITULADO: IMPLEMENTACIÓN Y GESTIÓN DE UNA PLATAFORMA DE SEGURIDAD INTEGRAL PARA LA INFRAESTRUCTURA DE CHEVYPLAN elaborado por FRANKLIN ANDRÉ CRUZ SANDOVAL fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje del 10% mismo que cumple con el valor aceptado para su presentación que es inferior o igual al 10% sobre el total de hojas del documento. Adicional se adjunta print de pantalla de dicho resultado.

ATENTAMENTE,

Firmado electrónicamente por:
MARCOS ANTONIO ESPINOZA MINA

Ing. Marcos Antonio Espinoza Mina, PhD.
Tutor

Dedicatoria

Este trabajo está dedicado a cada uno de mis seres queridos el cual me han apoyado incondicionalmente en mis estudios y en las decisiones que he tomado en la vida para ser quien soy al día de hoy.

A mi madre Elita que ha sido un pilar fundamental en mi vida y es mi ejemplo a seguir de superación, a mi hermano Alfredo que siempre me ha apoyado y motivado en mi carrera universitaria y me ha cuidado siempre con el amor de hermanos, a mi hermana menor Faduah que siempre me ha motivado para perseguir mis sueños y metas, a mis abuelos, Jorge y Gladys los cuales siempre me han amado y me han brindado ese amor y apoyo incondicional para seguir adelante.

Agradecimiento

Agradezco a Dios y a cada uno de los docentes de la Facultad de Ingenierías, Arquitectura y Ciencias de la Naturaleza de la Universidad Ecotec que han impartido sus conocimientos y enseñanzas para poder llegar a alcanzar esta meta a cumplir.

Agradezco a mis familiares y amigos por el amor y apoyo incondicional que me han brindado a lo largo de este reto universitario para poder alcanzar mi sueño.

Agradezco a la empresa ChevyPlan y el equipo de IT por darme la confianza y oportunidad para poder ejercer mis conocimientos y aprender cada día más con su apoyo incondicional.

Resumen

La presente investigación aborda la implementación y gestión de una plataforma de seguridad integral, específicamente Wazuh, en la infraestructura tecnológica de ChevyPlan. El objetivo general fue optimizar la protección y gestión de los sistemas digitales de la empresa, garantizando la continuidad del negocio y la confianza de los clientes. A través de un enfoque exploratorio-descriptivo y una metodología mixta, se analizaron vulnerabilidades específicas, como configuraciones inseguras y deficiencias en la gestión de accesos, que exponían a la organización a riesgos cibernéticos significativos.

Los resultados evidencian que Wazuh contribuyó eficazmente a la mitigación de riesgos mediante capacidades como la detección de intrusiones, el monitoreo de la integridad de los archivos y la identificación de malware. Estas funcionalidades mejoraron la respuesta ante incidentes en tiempo real y facilitaron el cumplimiento normativo, incluyendo la Ley Orgánica de Protección de Datos Personales en Ecuador. La implementación de Wazuh no solo fortaleció la seguridad operativa, sino que también optimizó procesos internos al centralizar la gestión de eventos de seguridad, reduciendo costos operativos y aumentando la eficiencia. Los hallazgos respaldan que la solución implementada fue altamente efectiva, superando las expectativas iniciales y consolidando a la empresa como preparada para afrontar desafíos de seguridad informática en el entorno actual.

Palabras claves: Wazuh, Plataforma de seguridad integral, SIEM, XDR

Abstract

This research addresses the implementation and management of a comprehensive security platform, specifically Wazuh, in ChevyPlan's technological infrastructure. The overall objective was to optimize the protection and management of the company's digital systems, ensuring business continuity and customer trust. Through an exploratory-descriptive approach and a mixed methodology, specific vulnerabilities were analyzed, such as insecure configurations and deficiencies in access management, which exposed the organization to significant cyber risks.

The results show that Wazuh effectively contributed to risk mitigation through capabilities such as intrusion detection, file integrity monitoring, and malware identification. These functionalities improved real-time incident response and facilitated regulatory compliance, including the Organic Law on Personal Data Protection in Ecuador. The implementation of Wazuh not only strengthened operational security, but also optimized internal processes by centralizing security event management, reducing operating costs and increasing efficiency. The findings support that the implemented solution was highly effective, exceeding initial expectations and consolidating the company as prepared to face IT security challenges in the current environment.

Keywords: Wazuh, Comprehensive security platform, SIEM, XDR

Contenido

1. Introducción

La ciberseguridad se ha convertido en un pilar fundamental para el desarrollo empresarial en Ecuador, donde las amenazas digitales han experimentado un incremento significativo en los últimos años, lo que pone en riesgo la confidencialidad, integridad y disponibilidad de sus sistemas de información. Este desafío es relevante en el sector automotriz ecuatoriano, donde las empresas como ChevyPlan, que se especializan en la administración de planes de financiamiento vehicular deben proteger sus activos digitales para garantizar la confianza de sus clientes y cumplir con normativas internacionales como el Reglamento General de Protección de Datos (GDPR) y la Ley de Privacidad del Consumidor de California (CCPA). En Ecuador, aunque la normativa de protección de datos está en una fase de desarrollo y ajuste, cada vez más empresas buscan anticiparse para asegurar su competitividad en el mercado regional e internacional (Dirección Nacional de Registros Públicos, 2021). Además, el impacto de estos ataques ha puesto de manifiesto la necesidad de adoptar medidas preventivas y de respuesta que garanticen la integridad de los sistemas y datos empresariales. Según (Redacción Primicias, 2023), el costo promedio de una filtración de datos en un país de América Latina como lo es Ecuador podría alcanzar los USD 2,6 millones en el año 2023 que incluso podría aumentar hasta USD 10 millones según el tipo de industria.

Para ChevyPlan, una empresa líder en el sector automotriz en Ecuador, la implementación de una plataforma de seguridad integral representa no solo una inversión en tecnología, sino una herramienta estratégica para mitigar riesgos y optimizar procesos operativos. Este proyecto busca abordar de manera efectiva las vulnerabilidades identificadas y mejorar la protección de la información.

La importancia de este tema radica en su capacidad para proporcionar una solución completa y centralizada que aborde múltiples aspectos de la seguridad informática. Una plataforma de seguridad integral como Wazuh permite la detección de intrusiones, la gestión

de vulnerabilidades, el monitoreo de la integridad de archivos y el análisis de registros, entre otras funciones. Estas capacidades son esenciales para proteger la infraestructura de TI de ChevyPlan contra amenazas tanto internas como externas. Además, el momento de abordar este tema se ve reforzado por el aumento de los ataques dirigidos y las regulaciones de cumplimiento cada vez más estrictas que requieren un enfoque proactivo en la gestión de la seguridad. Según (ESET, 2022) como resultado de una encuesta realizada a personal de compañías de Latinoamérica, se tiene como segunda preocupación con un 62% el robo de información.

Es crucial considerar el impacto de una plataforma de seguridad integral en la confianza de los clientes ecuatorianos. En un mercado donde los consumidores cada vez están mas conscientes de la protección de sus datos personales, una estrategia de seguridad sólida no solo mejora la protección de sus datos personales, sino que también fortalece su reputación en el mercado. Estudios como los de (PWC, 2023) muestran que el 79% de los consumidores de la región consideran esencial la protección de sus datos personales para continuar haciendo negocios con una empresa.

La implementación de una plataforma de seguridad integral ayudará a ChevyPlan a abordar estas necesidades críticas, al proporcionar capacidades de monitoreo y respuesta en tiempo real a incidentes de seguridad. Como señala (Cisco, 2021), las organizaciones que adoptan un enfoque proactivo en la gestión de la seguridad son un 53% más efectivas en la prevención de ataques cibernéticos, en comparación con aquellas que carecen de sistemas de seguridad integrados.

El tema de la implementación y gestión de una plataforma de seguridad integral para ChevyPlan es de vital importancia para proteger los activos digitales de la empresa, cumplir con regulaciones estrictas y garantizar la confianza de los clientes. A medida que las amenazas cibernéticas continúan evolucionando, una estrategia de seguridad robusta es esencial para continuidad del negocio y el éxito a largo plazo.

1.2. Antecedentes

La acelerada digitalización de las organizaciones ha incrementado la exposición a ciber amenazas, lo que hace indispensable la adopción de soluciones de seguridad informática robustas y escalables. En el caso de Ecuador, la protección de la infraestructura tecnológica no solo es un desafío técnico, sino también estratégico, considerando el aumento de los ciberdelitos reportados en los últimos años. Esta realidad posiciona a las plataformas de seguridad integral como herramientas clave para garantizar la continuidad del negocio y la confianza del cliente. En el año 2023, el país registró más de 12 millones de ciberataques, afectando tanto a instituciones públicas como privadas, lo que posiciona la ciberseguridad como una prioridad nacional. (Teleamazonas, 2024). Estos datos reflejan la urgencia de adoptar plataformas de seguridad integral para proteger la infraestructura tecnológica, garantizar la continuidad del negocio y salvaguardar la confianza del cliente.

Uno de los desarrollos más destacados en el ámbito de la seguridad informática es el sistema de detección de intrusos (IDS) y el sistema de prevención de intrusos (IPS), que han evolucionado significativamente en los últimos años. Según (Vega Briceño, 2021) destaca que el uso de estas tecnologías permite identificar patrones anómalos y predecir posibles ataques antes de que ocurran, aumentando la eficacia de las medidas de seguridad. Junto al IPS/IDS también se obtiene como destacado en el ámbito de la seguridad informática el sistema de detección y respuesta de amenazas, mejor conocido como XDR (Extended Detection and Response). Según (Trend, 2021), XDR ofrece una visión más amplia de las amenazas al integrar datos de diversas fuentes, mejorando la capacidad de detección y respuesta en comparación con los sistemas tradicionales de detección de intrusos (IDS) y prevención de intrusos (IPS). Además, la Cámara de la Industria Automotriz Ecuatoriana ha mencionado que las empresas de la industria están comenzando a integrar plataformas de seguridad más robustas para proteger tanto sus datos como los de los clientes. Esto incluye la implementación de sistemas de detección de intrusos y prevención de intrusos en algunas empresas del sector.

La inteligencia artificial (IA) y el aprendizaje automático también han transformado el panorama de la ciberseguridad, permitiendo la identificación proactiva de patrones anómalos y predicciones más precisas sobre posibles ataques. Según (Shah, 2022) estas tecnologías permiten la identificación de patrones anómalos y la predicción de posibles ataques, lo que incrementa significativamente la eficacia de las medidas de seguridad.

Asimismo, la investigación de (Aslan, Serkant, Ozkan, & Asim, 2023) analiza el impacto de las plataformas de seguridad integral en la reducción de riesgos cibernéticos. Los resultados indican que las empresas que adoptan estas plataformas mejoran su capacidad para detectar y mitigar amenazas, lo que se traduce en una disminución en la cantidad de incidentes de seguridad. Este enfoque es particularmente relevante para ChevyPlan, ya que respalda la necesidad de revisar y configurar una plataforma que se adapte a sus necesidades específicas, tal como lo estable en sus objetivos.

La estrategia Nacional de Telecomunicaciones marca un hito importante, ya que es la primera vez que Ecuador adopta una estrategia formal que abarca desde la protección de datos hasta la infraestructura crítica. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022). Asimismo, La Ley Orgánica de protección de datos, promulgada en 2021, obliga a las empresas a implementar medidas de seguridad que aseguren la confidencialidad, integridad y disponibilidad de los datos personales. Estos avances normativos resaltan la creciente importancia de la ciberseguridad en el país y su impacto en sectores estratégicos como el automotriz.

1.3. Planteamiento del problema

ChevyPlan es una empresa que maneja planes de financiamiento automotriz es por ello por lo que enfrenta desafíos significativos en la protección de su infraestructura tecnológica contra amenazas cibernéticas. La necesidad de implementar y gestionar una plataforma de seguridad integral se debe a la creciente sofisticación de los ataques cibernéticos, que ponen en riesgo la integridad y confidencialidad de los datos sensibles de la empresa. La principal necesidad es fortalecer la postura de seguridad de la organización mediante la implementación y gestión de una solución que pueda proporcionar visibilidad y control centralizado sobre la infraestructura TI, esta va a permitir la detección, prevención y respuesta eficazmente ante incidentes de seguridad en tiempo real.

Aunque existen múltiples plataformas de seguridad en el mercado, Wazuh se destaca como una opción eficiente para la infraestructura de ChevyPlan debido a su enfoque integral y sus capacidades de monitoreo en tiempo real. Sin embargo, antes de seleccionar esta solución, se evaluaron otras alternativas como Splunk que es reconocida por su capacidad avanzada de análisis de datos y AlienVault que destaca por su enfoque en la gestión de amenazas. Wazuh fue la opción seleccionada por su capacidad de personalización y adaptación a infraestructuras, su compatibilidad con normativas internacionales y su efectividad en comparación con las soluciones alternativas.

La transformación digital y la adopción de tecnologías avanzadas han aumentado la superficie de ataques, exponiendo a la empresa a riesgos significativos. La infraestructura tecnología de ChevyPlan, que incluye tanto servidores locales como servicios en la nube, es clasificada como hibrida. Según un informe de (ManageEngine, 2023), las infraestructuras hibridas presentan mayores desafíos de seguridad debido a su distribución y a la diversidad de tecnologías involucradas, Esta complejidad requiere una solución de seguridad integral que cubra todas las áreas críticas de la infraestructura tecnológica.

En este contexto, surge la pregunta de investigación que guía este proyecto: ¿Cómo puede la implementación y gestión de la plataforma Wazuh fortalecer la postura de seguridad de la infraestructura de ChevyPlan?, esta pregunta tiene como fin delimitar el alcance del proyecto y enfocar los esfuerzos en evaluar las capacidades de Wazuh para abordar los desafíos específicos de seguridad.

En la actualidad la seguridad de la infraestructura de ChevyPlan enfrenta varios desafíos. Según (McKinsey, 2023) las plataformas de seguridad integrales son esenciales para abordar estas deficiencias, al ofrecer funcionalidades como monitoreo de actividades, cifrado de datos, análisis de riesgos, gestión de accesos, detección de intrusos y cumplimiento normativo. La capacidad de integrar y automatizar estos procesos es fundamental para mejorar la postura de seguridad y reducir el riesgo de ataques cibernéticos. Por otro lado, según (Stallings & Brown, 2023), las organizaciones que implementan plataformas de seguridad integradas logran una mejora en su capacidad para identificar y mitigar amenazas, lo que les permite actuar de manera mas proactiva frente a los ciberataques.

Como proceso a la implementación de una plataforma de seguridad integral esta divididas por varias etapas: Planificación que es donde se harán los análisis de las necesidades de seguridad de la organización y la evaluación de las soluciones disponibles, el despliegue que es la técnica de implementación de la plataforma seleccionada para asegurar que es compatible con la infraestructura existente, la configuración que es la personalización de las funcionalidades de la plataforma para satisfacer las necesidades de la organización, la gestión continua se la utiliza para monitorear constantemente la plataforma de seguridad integral para asegurar su eficacia a largo plazo y la capacitación que es la formación del personal en el uso efectivo de la plataforma y las mejores prácticas de seguridad.

Se espera que con esta implementación de una plataforma de seguridad integral proporcione a la organización una mejora significativa en la respuesta y detección ante

incidentes y que cubra una mayor visibilidad de las actividades sospechosas y reducir el riesgo de posibles ataques cibernéticos, dicha plataforma permitirá unificar y automatizar procesos de seguridad, lo que resultará en una postura de seguridad más robusta y se enfocará en abordar las necesidades específicas que requiera la infraestructura. Este proceso involucra etapas de planificación, despliegue, configuración y gestión continua, con un fuerte énfasis en la capacitación del personal y la integración de las mejores prácticas de seguridad.

1.4. Objetivos del trabajo de integración curricular

1.4.1. Objetivo General

- Implementar una plataforma de seguridad integral para optimizar la protección y gestión de la infraestructura de ChevyPlan.

1.4.2. Objetivos específicos

- Analizar las vulnerabilidades actuales de la infraestructura ChevyPlan para priorizar las áreas críticas que se requiere fortalecer.
- Desarrollar y evaluar procedimientos para el monitoreo continuo y la respuesta a incidentes de la seguridad, garantizando la efectividad constante de la plataforma de seguridad.
- Implementar la plataforma de seguridad Wazuh para adaptarla a la infraestructura de ChevyPlan asegurando la cobertura de sus servidores.

1.5. Justificación

La justificación para implementar y gestionar una plataforma de seguridad integral en ChevyPlan radica en la creciente necesidad de proteger infraestructuras contra amenazas cibernéticas. Este proyecto contribuirá significativamente al conocimiento existente al proporcionar un análisis detallado sobre la efectividad de las soluciones de seguridad integradas en entornos híbridos. Según (Kim & Solomon, 2021), las organizaciones deben fortalecer sus medidas de seguridad para proteger sus datos y operaciones críticas, además brindará beneficios inmediatos en la protección de sus activos digitales, sino que también influirá positivamente en su competitividad en el mercado ecuatoriano, la ciberseguridad es un factor clave para mantener la confianza del cliente y cumplir con regulaciones locales e internacionales, asegurando la continuidad del negocio y aumentando la resistencia frente a incidentes. A largo plazo, esta estrategia de seguridad fortalecerá el posicionamiento de ChevyPlan como una empresa confiable y segura, preparada para enfrentar los desafíos y cambios en el panorama normativo global.

Wazuh fue elegido tras una evaluación comparativa con otras plataformas, como por ejemplo Splunk o AlienVault. Splunk es reconocido por su capacidad avanzada de análisis de grandes volúmenes de datos, pero su modelo de costos lo hace menos accesible para empresas con presupuestos ajustados. AlienVault, por su parte, combina múltiples herramientas en un sistema integrado, pero carece de la flexibilidad de personalización que Wazuh ofrece. Wazuh destaca como una solución de código abierto que integra detección y respuesta a amenazas, monitorización de integridad de archivos, y gestión de vulnerabilidades sin costos adicionales. Esto lo convierte en una alternativa rentable y eficiente para ChevyPlan. (Tetra Information Services, 2024)

Desde un enfoque teórico, este proyecto contribuye significativamente al conocimiento existente al analizar la efectividad de las soluciones de seguridad integradas en entornos híbridos. Según (Stallings, 2022), las investigaciones recientes subrayan la importancia de las estrategias de seguridad en estos entornos, ya que combinan elementos locales y en la

nube, aumentando la superficie de ataque potencial. Este analisis proporcionara una comprension mas profunda de como las plataformas de seguridad integral pueden mejorar la deteccion y respuesta ante incidentes de seguridad, lo cual es cruicial en el panorama digital actual.

Metodológicamente, el proyecto desarrollará técnicas y procedimientos específicos para la implementación y gestión de plataformas de seguridad integral, Según (Moschovitis, 2021), se necesita una evaluación de vulnerabilidades, la configuración de sistemas de seguridad y la capacitación del personal para mejorar las prácticas de ciberseguridad. La documentación de estos procedimientos servirá como guía para futuras implementaciones, mejorando así el campo de la ciberseguridad.

Chevyplan enfrenta vulnerabilidades específicas, como configuraciones inseguras, deficiencias en la gestión de accesos y la ausencia de un sistema integral de monitoreo. Estas debilidades no solo exponen a la empresa a riesgos operativos, sino que también afectan a la confianza de los clientes en la seguridad de sus datos personales. Implementar una plataforma de seguridad integral no solo abordará estas deficiencias, sino que también garantizará el cumplimiento de normativas locales y fortalecerá la competitividad de la empresa en el mercado ecuatoriano.

Desde una perspectiva práctica, la implementación de una plataforma de seguridad integral abordará directamente la necesidad de proteger la infraestructura de TI de la empresa contra las amenazas cibernéticas. Según (Williams & Sawyer, 2023), esto no solo mejorará la seguridad de la organización, sino que también garantizará la continuidad del negocio y la protección de datos sensibles. Los resultados esperados incluyen una mayor eficiencia en la gestión de incidentes, la reducción de riesgos y una mejor preparación para enfrentar futuros desafíos de seguridad. Además, al mejorar la postura de seguridad, la empresa podrá cumplir más fácilmente con las regulaciones de protección de datos y demostrar su compromiso con la seguridad a sus clientes y socios comerciales.

2. Revisión de la Literatura/Marco Teórico

2.1. Plataforma de Seguridad Integral

Una plataforma de seguridad integral es un sistema o conjunto de herramientas diseñado para proporcionar una cobertura completa de seguridad a lo largo de toda la infraestructura de TI de una organización. Estas plataformas buscan integrar y coordinar diversas funciones de seguridad para proteger contra una amplia gama de amenazas y vulnerabilidades, al tiempo que facilitan la gestión y el cumplimiento de las políticas de seguridad.

Una plataforma de seguridad integral puede integrar características de SIEM y XDR, combinando el análisis centralizado y el cumplimiento normativo del SIEM con las capacidades avanzadas de detección y respuesta de XDR. Según (Blokdyk, 2021), esto permite una protección más robusta y una respuesta más rápida ante incidentes de seguridad, proporcionando a las organizaciones una solución unificada para gestionar. Como características se obtienen las siguientes:

- Supervisa constantemente la actividad en la red y los sistemas para detectar y responder a incidentes de seguridad en tiempo real.
- Asiste a las organizaciones en el cumplimiento de regulaciones y estándares de seguridad mediante la elaboración de informes, auditorías y documentación de conformidad.
- Facilita la identificación de amenazas y la respuesta efectiva a incidentes de seguridad para reducir su impacto.
- Evalúa y prioriza las vulnerabilidades en los sistemas, ofreciendo soluciones para mitigar riesgos y fortalecer la seguridad

- Combina diversas herramientas y capacidades, como la detección de intrusiones, gestión de vulnerabilidades análisis de registros (logs), cifrado de datos y prevención de pérdida de datos.
- Recopila y analiza datos de seguridad de múltiples fuentes para identificar patrones de amenazas y detectar anomalías.
- Ofrece una interfaz centralizada para gestionar todas las funciones de seguridad, facilitando el control de políticas y configuraciones de seguridad.

2.2. Sistemas de información y Gestión de seguridad

2.2.1. SIEM (Security Information and Event Management)

Una SIEM (Security Information and Event Management) es una herramienta de seguridad informática que busca proveer a las organizaciones una respuesta precisa y rápida para detectar y responder ante cualquier amenaza. Según (Añazco, 2021), las SIEM tienen un enfoque centralizado para la recopilación, correlación y análisis de eventos de seguridad y datos de registros (logs) en tiempo real y son utilizadas para detectar amenazas, asegurar el cumplimiento normativo y gestionar incidentes de seguridad.

2.2.2. Características de un SIEM

- Cumplir con las leyes y normas vigentes en materia de protección de datos y seguridad. (Ambit, 2021).
- Distinguir entre amenazas reales y falsas alarmas.
- Registrar todo el proceso de detección, acción y resolución.
- Supervisar centralizadamente todas las amenazas posibles.
- Proporcionar un conocimiento más profundo sobre los incidentes para facilitar su resolución.

- Centraliza la gestión de eventos de seguridad, reduciendo la complejidad y mejorando la eficiencia operativa.

2.2.3. Operación de un SIEM

- Recolección de datos: Las SIEM recolectan información de una variedad de fuentes como dispositivos de red (firewalls, routers, switches), servidores, sistemas operativos, bases de datos, aplicaciones y dispositivos de seguridad con el fin de normalizar los datos para asegurarse de que todos los eventos tengan un formato estándar, lo que facilita el análisis y la correlación.
- Análisis: Se utilizan reglas predefinidas y algoritmos de correlación para identificar relaciones entre eventos aparentemente aislados, detectando patrones de ataque o comportamientos anómalos, con ello se incorporan la inteligencia de amenazas para mejorar el análisis y la detección de actividades maliciosas basadas en indicadores de compromiso conocidos.
- Alertas y monitoreo: Se monitorea continuamente la infraestructura de TI en busca de eventos sospechosos o potencialmente peligrosos. Cuando se detectan amenazas o anomalías significativas, el sistema genera alertas para notificar a los equipos de seguridad.
- Gestión y respuesta a incidentes: Facilitan el seguimiento y la gestión de incidentes de seguridad desde su detección hasta su resolución, algunas SIEM pueden automatizar respuestas a ciertos eventos, como bloquear direcciones IP o cerrar sesiones de usuarios.
- Informes y cumplimiento: Producen informes detallados para auditar eventos de seguridad y evaluar el cumplimiento de normativas como GDPR, HIPAA, PCI-DSS y ayudan en la preparación de auditorías de seguridad al proporcionar registros históricos y análisis de eventos.

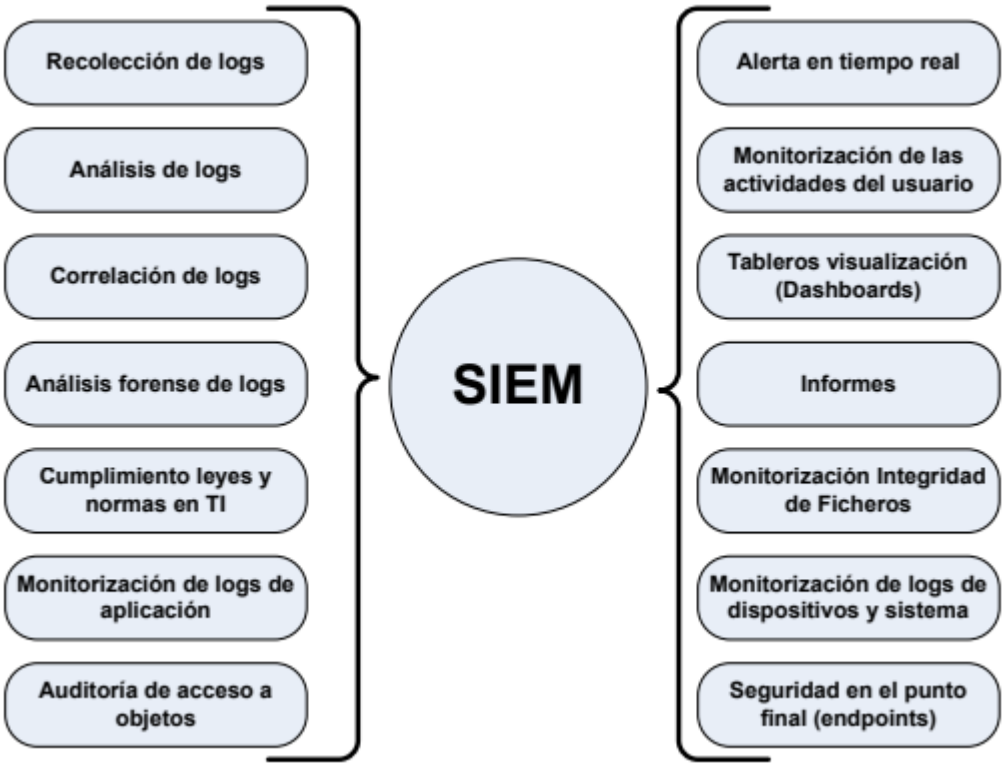


Ilustración 1 Arquitectura SIEM

2.2. XDR (Extended Detection and Response)

XDR (Extended detection and response) es una solución de seguridad que integra la detección y respuesta en diversas capas de la infraestructura de TI, como endpoints, redes, servidores y aplicaciones. Según (Sullivan, 2022), XDR unifica y automatiza la correlación de datos y la respuesta a incidentes, permitiendo a los equipos de seguridad gestionar y mitigar amenazas de manera más efectiva.

2.2.1. Características de XDR

- Cubre múltiples capas de la infraestructura de seguridad, incluyendo endpoints, redes y servidores, proporcionando una visión unificada de la seguridad y ofrece una visión de la actividad de seguridad en toda la organización. Mejorando la detección y respuesta a amenazas.
- Utiliza inteligencia artificial y aprendizaje automático para correlacionar eventos de seguridad automáticamente y detectar patrones de amenaza, con el fin de mejorar la precisión de las detecciones para reduciendo la cantidad de alertas falsas.
- Permite respuestas automáticas a incidentes, como el aislamiento de dispositivos comprometidos o la neutralización de amenazas y coordina diferentes herramientas de seguridad para proporcionar una respuesta eficiente y efectiva a las amenazas.
- Identifica amenazas avanzadas y persistentes antes de que causen daño significativo, además, permite a los equipos de seguridad buscar activamente amenazas en toda la infraestructura.
- Reduce la carga operativa al centralizar la gestión de eventos de seguridad y automatizar procesos, además, facilita la optimización continua de las estrategias de seguridad basadas en análisis de datos.

2.2.2. Componentes de una solución de XDR

Según (Sullivan, 2022), las herramientas de XDR son nuevos participantes en el espacio de seguridad y aún existen algunas diferencias en las funcionalidades que ofrecen estas soluciones. No obstante, hay ciertas características fundamentales que proporcionan las soluciones XDR:

- Vista centralizada: Las herramientas XDR destacan por proporcionar una vista centralizada de la información que recopilan. Estas soluciones analizan la mayor parte del entorno de seguridad, si no todo, y requieren de un centro de análisis para procesar toda esa información.
- Aprendizaje automático: Las plataformas XDR utilizan el aprendizaje automático para realizar análisis de datos de seguridad. Esto es particularmente útil para disminuir los tiempos de respuesta, ya que reduce la carga de trabajo del personal de seguridad al abordar un problema de seguridad.
- Integración flexible: La cantidad y el método de integración con las soluciones de seguridad existentes dependen de la solución XDR especifica, pero usualmente existe una manera de incorporar herramientas de seguridad, especialmente las de seguridad de endpoints, en una plataforma XDR.
- Automatización: Similar a las soluciones SOAR, las herramientas XDR emplean la automatización para aliviar la carga de trabajo del equipo de Operaciones de Seguridad. Aunque solo automatizan tareas sencillas.

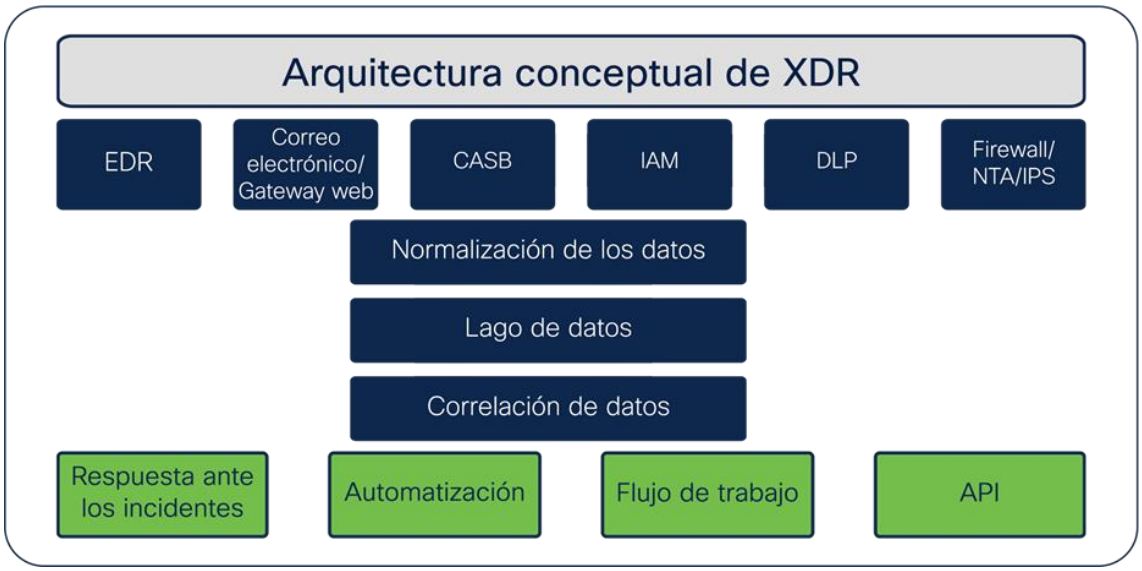


Ilustración 2 Arquitectura XDR

2.3. Wazuh

Wazuh es una plataforma de seguridad de código abierto que está diseñada para la detección de amenazas, monitorización de la integrad, respuesta a incidentes, cumplimiento normativo ofreciendo una solución integral para proteger la infraestructura de TI, incluyendo entornos locales, virtualizados, en contenedores y en la nube. (Wazuh, 2024).

Wazuh combina funcionalidades de SIEM Y XDR, ofreciendo una solución escalable y económica que satisface las necesidades de ChevyPlan como, por ejemplo:

- Monitorización de la integridad de los archivos
- Gestión de Vulnerabilidades
- Detección y respuesta a amenazas

Wazuh tiene relación con SIEM (Security Information and Event Management) y XDR (Extended Detection and Response), ya que comparte las siguientes características:

2.3.1. Relación con SIEM

Wazuh funciona como una solución SIEM al recopilar, correlacionar y analizar registros de eventos (logs) de diversas fuentes dentro de una red. Esto permite a los administradores de seguridad supervisar y reaccionar ante incidentes de seguridad en tiempo real. Además, proporciona alertas e informes que ayudan a identificar y responder a posibles amenazas, facilitando el cumplimiento de normativas y la auditoría de seguridad.

2.3.2. Relación con XDR

Aunque Wazuh no es estrictamente una solución XDR, comparte algunas funcionalidades con estas, como la detección y respuesta a amenazas de monitoreo

continuo y respuesta a incidentes, lo cuales son características claves de las soluciones XDR.

2.3.3. Ventajas de Wazuh

Según (Frayssinet Delgado, 2023), Wazuh es una plataforma de seguridad de código abierto que se destaca en proteger activamente la infraestructura de amenazas y es esencial para evitar brechas y mitigar ataques y cuenta con las siguientes ventajas:

- Detección de tiempo real y respuesta proactiva
- Integración de Múltiples Componentes de seguridad
- Capacidad de correlación de eventos
- Cumplimiento regulatorio
- Escalabilidad y flexibilidad
- Visualización y reportes detallados
- Capacidades de integración y automatización

2.3.4. Características de Wazuh

- Emplea reglas y algoritmos para analizar registros de eventos y detectar comportamientos anómalos que podrían indicar intentos de ataque o intrusión.
- Detecta modificaciones en archivos y configuraciones del sistema, permitiendo identificar posibles intrusiones o actividades no autorizadas.
- Ayuda a las organizaciones a cumplir con normativas y estándares de seguridad mediante la provisión de informes y auditorías de cumplimiento.

- Identifica y evalúa vulnerabilidades en los sistemas, proporcionando información para mitigar posibles riesgos de seguridad.
- Recopila y examina registros de diversas fuentes, ofreciendo visibilidad sobre las actividades en la infraestructura de TI.

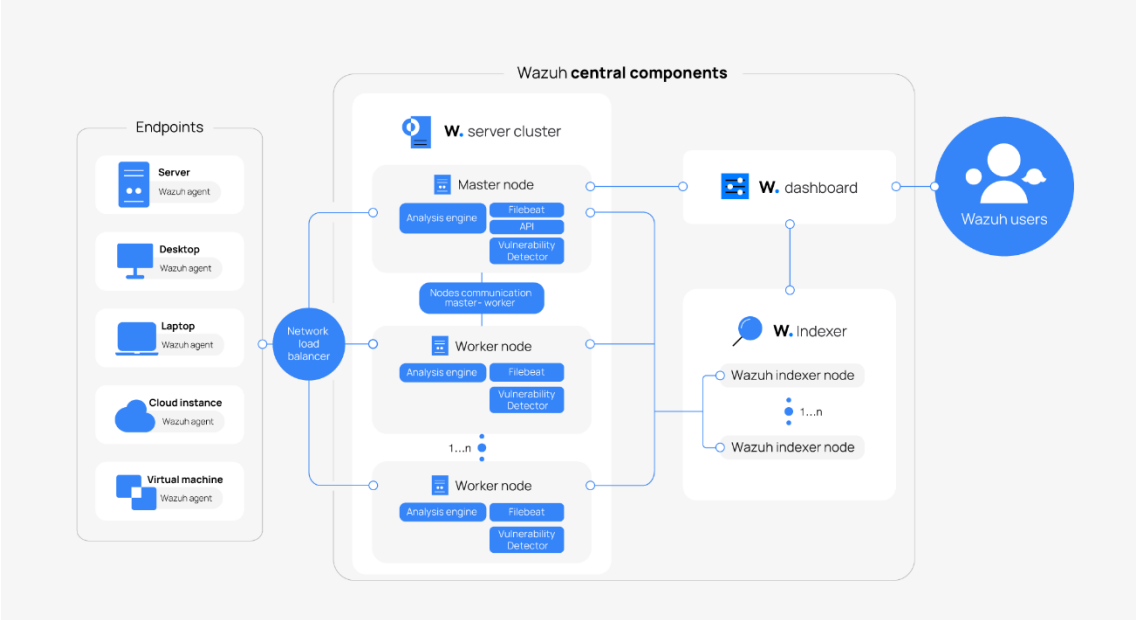


Ilustración 3 Arquitectura Wazuh

2.4. Casos de Uso Wazuh

2.4.1. Configuration assessment (Evaluación de configuración)

Las evaluaciones periódicas de la configuración son esenciales para mantener un entorno seguro y compatible, ya que ayudan a las organizaciones a identificar y parchear vulnerabilidades de forma proactiva. Esta práctica fortalece los controles de seguridad y minimiza el riesgo de incidentes de seguridad.

Wazuh ofrece un módulo de Evaluación de configuración de seguridad (SCA – Security Configuration Assessment) que ayuda a los equipos de seguridad a escanear y

detectar configuraciones incorrectas dentro de su entorno. El agente Wazuh utiliza archivos de políticas para escanear los puntos finales que monitorea. Estos archivos contienen comprobaciones predefinidas que se llevarán a cabo en cada punto final monitoreado.

Wazuh incluye políticas SCA listas para usar basadas en los puntos de referencia de seguridad del Centro para la Seguridad de Internet (CIS). Estos puntos de referencia sirven como directrices esenciales sobre las mejores prácticas para proteger los sistemas y datos de TI de los ciberataques. Proporcionan instrucciones claras para establecer una configuración básica segura y ofrecen orientación para garantizar que los usuarios implementen medidas efectivas para salvaguardar sus activos críticos y mitigar posibles vulnerabilidades. Al cumplir con estos estándares, puede mejorar su postura general de seguridad y mitigar el riesgo de amenazas cibernéticas contra su empresa. (Wazuh, 2024)

Algunos otros beneficios del módulo Evaluación de la configuración de seguridad (SCA) de Wazuh incluyen:

- Gestión de la postura de seguridad: Wazuh SCA ayuda a las organizaciones a garantizar que sus puntos finales estén configurados de forma segura. Esto minimiza las vulnerabilidades resultantes de configuraciones incorrectas y reduce el riesgo de violaciones de seguridad.
- Monitoreo de cumplimiento: permite a las organizaciones evaluar e implementar el cumplimiento de estándares regulatorios, mejores prácticas y políticas de seguridad interna.
- Monitoreo continuo: Wazuh SCA monitorea continuamente la configuración de los puntos finales y alerta cuando descubre configuraciones incorrectas.

2.4.2. Malware detection (Detección de Malware)

Malware, abreviatura de software malicioso, se refiere a cualquier software diseñado específicamente para dañar o explotar sistemas informáticos, redes o usuarios. Se crea con la intención de obtener acceso no autorizado, causar daños, robar información confidencial o realizar otras actividades maliciosas en un sistema de destino. Existen varios tipos de malware, cada uno con funciones y métodos de infección específicos. Algunos tipos comunes de malware incluyen virus, gusanos, ransomware, botnets, spyware, troyanos y rootkits.

La detección de malware es crucial para proteger los sistemas y redes informáticos de las amenazas cibernéticas. Ayuda a identificar y mitigar el software malicioso que puede provocar una filtración de datos, comprometer el sistema y pérdidas financieras.

Los métodos tradicionales, que se basan únicamente en detecciones basadas en firmas, tienen limitaciones y no logran capturar nuevas amenazas. Los enfoques basados en firmas tienen dificultades para detectar ataques de día cero, malware polimórfico y otras técnicas de evasión empleadas por los actores de amenazas. Como resultado, las organizaciones corren el riesgo de sufrir filtraciones y filtraciones de datos no detectadas. Wazuh permite a las organizaciones detectar y responder eficazmente a amenazas sofisticadas y evasivas. Wazuh abarca diferentes módulos que identifican propiedades, actividades, conexiones de red y más del malware. (Wazuh, 2024)

2.4.3. FIM (File Integrity Monitoring)

El monitoreo de integridad de archivos (FIM) implica monitorear la integridad de archivos y directorios para detectar y alertar cuando hay eventos de adición, modificación o eliminación de archivos. FIM proporciona una importante capa de protección para archivos y

datos confidenciales al escanear y verificar de forma rutinaria la integridad de esos activos. Identifica cambios en archivos que podrían ser indicativos de un ciberataque y genera alertas para una mayor investigación y reparación si es necesario.

El módulo de monitoreo de integridad de archivos de código abierto de Wazuh rastrea las actividades realizadas dentro de los directorios o archivos monitoreados para obtener información extensa sobre la creación, modificación y eliminación de archivos. Cuando se modifica un archivo, Wazuh compara su suma de verificación con una línea de base previamente calculada y activa una alerta si encuentra una discrepancia.

El módulo FIM de código abierto realiza monitoreo en tiempo real y escaneos programados según el nivel de sensibilidad de los archivos monitoreados.

2.4.4. Threat Hunting (Búsqueda de amenazas)

La búsqueda de amenazas es un enfoque proactivo que implica el análisis de numerosas fuentes de datos, como registros, tráfico de red y datos de puntos finales, para identificar y eliminar amenazas cibernéticas que han evadido las medidas de seguridad tradicionales. Su objetivo es descubrir amenazas potenciales que pueden haber pasado desapercibidas en un entorno de TI. El proceso de búsqueda de amenazas generalmente implica varios pasos: generación de hipótesis, recopilación de datos, análisis y respuesta.

Wazuh ofrece varias capacidades que ayudan a los equipos de seguridad a buscar amenazas dentro de su entorno, lo que les permite tomar medidas rápidas para contener la amenaza y evitar daños mayores.

2.4.6. Log data análisis (Análisis de datos de registro)

El análisis de datos de registro es un proceso crucial que implica examinar y extraer información valiosa de los archivos de registro creados por diferentes sistemas, aplicaciones o dispositivos. Estos registros contienen registros de eventos que brindan información útil para la resolución de problemas, el análisis y monitoreo de seguridad y la optimización del rendimiento. El análisis de datos de registro es una práctica esencial que contribuye a un ecosistema de TI seguro, eficiente y confiable.

Wazuh recopila, analiza y almacena registros de puntos finales, dispositivos de red y aplicaciones. El agente de Wazuh, que se ejecuta en un punto final monitoreado, recopila y reenvía registros del sistema y de la aplicación al servidor de Wazuh para su análisis. Además, puede enviar mensajes de registro al servidor de Wazuh a través de syslog o integraciones de API de terceros. (Wazuh, 2024)

Wazuh recopila registros de una amplia gama de fuentes, lo que permite un monitoreo integral de varios aspectos de su entorno de TI. Puede consultar nuestra documentación sobre Recopilación de datos de registro para comprender mejor cómo Wazuh recopila y analiza registros de puntos finales monitoreados. Algunas de las fuentes de registro comunes admitidas por Wazuh incluyen:

- Registros del sistema operativo: Wazuh recopila registros de varios sistemas operativos, incluidos Linux, Windows y macOS.
- Wazuh puede recopilar registros de syslog, auditd, de aplicaciones y otros desde terminales Linux.
- Wazuh recopila registros en terminales Windows mediante el canal de eventos de Windows y el formato de registro de eventos de Windows. De forma predeterminada, el agente de Wazuh monitorea los canales de eventos de Windows Sistema, Aplicación y Seguridad en

terminales Windows. El agente de Wazuh ofrece la flexibilidad de configurar y monitorear otros canales de eventos de Windows.

- Wazuh utiliza el sistema de registro unificado (ULS) para recopilar registros en terminales macOS. El ULS macOS centraliza la administración y el almacenamiento de registros en todos los niveles del sistema.

2.5. Seguridad Integral en Infraestructura TI

La seguridad integral en infraestructuras de TI se refiere a un enfoque multifacético y holístico que tiene como objetivo proteger todos los componentes tecnológicos y de información dentro de una organización. Este concepto abarca la protección de datos, redes, aplicaciones, sistemas operativos y todos los dispositivos conectados que están expuestos a ciber amenazas. La seguridad integral no solo se enfoca en la prevención de ataques, sino también en la capacidad de detección y respuesta a incidentes de seguridad en tiempo real, lo cual asegura una defensa continua y adaptativa frente a las amenazas.

Según (Streicher, 2024), la tendencia actual en la gestión de la seguridad de TI es pasar de un enfoque reactivo a un enfoque más proactivo, que permita anticipar posibles vulnerabilidades y actuar de manera preventiva. Las plataformas de seguridad integral combinan tecnologías avanzadas como la inteligencia artificial, el aprendizaje automático y la automatización para ofrecer una protección robusta y escalable.

La implementación de una plataforma de seguridad integral ayuda a reducir la superficie de ataque, identificar vulnerabilidades antes de que se conviertan en problemas críticos, y responder de forma rápida y eficaz ante ciberataques, dichas características son

esenciales para mantener la confianza de los clientes y proteger los activos digitales de las empresas.

2.6. Factores Críticos en la Implementación de Plataformas de Seguridad

La implementación de plataformas de seguridad en la infraestructura TI implica una serie de factores críticos que deben considerarse para garantizar su efectividad. Estos factores incluyen la evaluación de riesgos, la selección de tecnologías adecuadas, la capacitación del personal, la gestión de incidentes y la conformidad con normativas y estándares de la industria.

Un factor crucial es la evaluación inicial de riesgos y vulnerabilidades, ya que permite a las organizaciones identificar las áreas más vulnerables de su infraestructura y establecer prioridades para la implementación de medidas de seguridad. Según (Tariq, Ahmed, Bashir, & Shaukat, 2023), una correcta evaluación de riesgos debe incluir tanto amenazas internas como externas, así como posibles vectores de ataque que podrían comprometer la integridad de los sistemas.

La capacitación del personal y la creación de una cultura de seguridad dentro de la organización también juegan un papel fundamental, Una plataforma de seguridad, por muy avanzada que sea, no puede ser efectiva sin el soporte y la comprensión adecuada por parte del equipo que la maneja. Además, es importante garantizar que la plataforma sea escalable y adaptable a medida que evoluciones las necesidades la empresa y las amenazas de seguridad.

2.7. Ciberseguridad en Ecuador

2.7.1. Estado Actual de la Ciberseguridad en Ecuador

En Ecuador, el avance de la ciberseguridad ha crecido, pero sigue enfrentando desafíos significativos, como la falta de recursos especializados y la accesibilidad limitada de soluciones avanzadas para muchas organizaciones. La estrategia Nacional de Ciberseguridad de 2022 marca un hito importante, ya que es la primera vez que el país adopta una estrategia formal que abarca desde la protección de datos hasta la infraestructura critica. Este plan incluye medidas de protección para ciudadanos, instituciones y empresas, y busca mitigar el impacto de amenazas cibernéticas mediante el fortalecimiento de capacidades locales y la colaboración interinstitucional. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022)

A nivel regional, América Latina también enfrenta una situación de vulnerabilidad creciente, con un aumento de ataques como rasomware y phishing, además de colocar a Ecuador en el puesto 119 de 183 de países en el índice de madurez de Ciberseguridad en el año 2022. Esto se debe, en parte, a la falta de madurez en muchas empresas para implementar políticas de seguridad proactivas, sumando a la necesidad de educación en ciberseguridad para reducir riesgos a nivel empresarial y personal. Informes de expertos sugieren que, en Ecuador, aunque algunas empresas han adoptado estrategias robustas, muchas otras aun ven la seguridad informática como un aspecto secundario. (La Hora, 2024)

2.7.2. Legislación y Regulaciones en Ciberseguridad

La Ley Orgánica de Protección de Datos Personales de Ecuador fue aprobada en el año 2021 y marca un hito en la protección de datos personales en el país. Esta ley, publicada en el Registro Oficial Suplemento No. 459 el 26 de mayo de 2021, establece los derechos de los ciudadanos sobre sus datos personales y las obligaciones de las organizaciones en su tratamiento. Su aprobación ha generado un marco legal que exige que las empresas implementen medidas de seguridad que aseguren la confidencialidad, integridad y disponibilidad de los datos personales. (Asamble Nacional Republica del Ecuador, 2021)

Para un proyecto como la implementación de una plataforma de seguridad para la infraestructura, esta ley implica la necesidad de incluir mecanismos que permitan el control y la auditoria de datos personales, algo que un sistema SIEM puede facilitar mediante reportes que contribuyan al cumplimiento de auditorías y revisiones de seguridad. La ley también permite prever posibles actualizaciones y regulaciones adicionales en ciberseguridad, especialmente en sectores que manejan datos críticos, lo que refuerza la necesidad de una infraestructura de seguridad robusta y adaptable.

2.7.3. Comparativa con Normativas Internacionales

La Ley Orgánica de Protección de Datos Personales de Ecuador se inspira en el Reglamento General de Protección de Datos (GDPR) de la unión europea, aunque existen diferencias importantes en el alcance y el rigor de ambas normativas. Al igual que el GDPR, la ley ecuatoriana enfatiza los derechos de los ciudadanos sobre sus datos personales y establece obligaciones para las empresas en cuanto a la gestión de estos datos, incluyendo derechos como acceso, rectificación y portabilidad. Sin embargo, la normativa europea

impone un enfoque más detallado y proactivo en cuanto a la seguridad de la información, abarcando conceptos de gestión de riesgos, resiliencia y trazabilidad que son menos robustos en la legislación ecuatoriana.

En este contexto, la implementación de plataformas de seguridad como la de ChevyPlan está considerando que cumplan con los principios del GDPR, podría facilitar la adherencia a normas internacionales y garantizar una protección mas completa de los datos personales. El cumplimiento con el GDPR requiere que los sistemas informáticos cuenten con medidas de seguridad proactivas y registros detallados para auditorias. Adaptar estos requisitos en Ecuador fortalecería la interoperabilidad y la seguridad, alineando los estándares nacionales con las mejores prácticas globales.

2.8 Vulnerabilidades en Infraestructuras Híbridas y Estrategias de Mitigación

Las infraestructuras híbridas, que combinan recursos en la nube y locales, presentan una serie de desafíos en términos de seguridad. Algunas de las vulnerabilidades más comunes incluyen:

- Las brechas en las configuraciones de seguridad
- Falta de visibilidad y control
- Dependencia de proveedores externos

Para ChevyPlan, estas vulnerabilidades tienen una relevancia particular debido a su infraestructura híbrida, que combina servicios locales con soluciones basadas en la nube. El manejo de datos sensibles, sin una visibilidad total y control efectivo puede ser una vulnerabilidad significativa que comprometa la integridad y confidencialidad de la información. Como estrategias de mitigación de estas vulnerabilidades se pueden destacar

por ejemplo el uso de herramientas SIEM y XDR como Wazuh para proporcionar una visibilidad continua de los eventos de seguridad en ambas plataformas. Además de las auditorías y parches de seguridad para mantener una política estricta para la infraestructura y la implementación de la seguridad Zero Trust para asegurar que todos los accesos sean verificados antes de ser autorizados.

3. Metodología

3.1. Alcance de la Investigación

La investigación sobre la “Implementación y gestión de una plataforma de seguridad integral para la infraestructura Chevyplan” tiene un enfoque exploratorio-descriptivo. Este método busca analizar y describir la situación actual de la infraestructura en términos de seguridad, identificando las vulnerabilidades y áreas de mejoras.

Exploratorio: Este enfoque permite investigar las vulnerabilidades específicas y las amenazas a la infraestructura de TI, identificando problemas que no han sido suficientemente tratados en estudios previos. Esto establece las bases para las soluciones de seguridad eficaces, explorando los elementos críticos de seguridad.

Descriptivo: El enfoque descriptivo complementa el enfoque exploratorio, proporcionando una caracterización detallada de la infraestructura actual, su contexto y deficiencias en ciberseguridad. Este alcance es esencial para documentar las características del entorno y para planificar estrategias de implementación precisas.

3.2. Enfoque de la investigación

El enfoque metodológico seleccionado para esta investigación es mixto, integrando métodos cualitativos y cuantitativos, lo cual es crucial en el contexto de implementación de una plataforma de seguridad integral para abordar los aspectos técnicos como las percepciones y necesidades del personal de TI. Esto es esencial en un proyecto como este, donde se requiere evaluar el impacto cuantitativo en términos de métricas de seguridad, así como comprender los desafíos y expectativas cualitativas del equipo. La seguridad informática en una organización como ChevyPlan no solo requiere datos medibles, si no también percepciones sobre cómo las medidas implementadas son percibidas y adoptadas por el equipo de TI.

Este enfoque ha sido seleccionado ya que se considera que es adecuado para analizar tantos las percepciones cualitativas del personal de TI sobre las necesidades y desafíos de la seguridad, como para obtener datos cuantitativos que miden el impacto y desempeño de la plataforma en términos de eficiencia de seguridad. Este método permite una comprensión integral, que facilita la identificación de problemas específicos y su posible solución. Según (Hernández Sampieri, Fernández-Collado, & Baptista Lucio, 2021), los enfoques mixtos son especialmente valiosos en estudios complejos, pues combinan la profundidad descriptiva con el rigor estadístico.

3.3. Delimitación de la investigación

- Ubicación: Las investigaciones se llevará a cabo en las instalaciones de ChevyPlan y en sus sistemas de TI, incluyendo los servidores.

- Periodo: El estudio se realizará en un lapso de tres meses, cubriendo desde el diagnóstico inicial, la implementación de la plataforma y su gestión para evaluar los resultados en términos de seguridad.
- Población y Muestra: La población objeto del estudio será el personal de TI ChevyPlan, mientras que la muestra se compondrá del 50% de este equipo, seleccionando perfiles clave con experiencia en gestión y seguridad de infraestructura.

3.4. Métodos empleados

Se utilizarán métodos empíricos y estadísticos que permitan una comprensión exhaustiva de los datos, tanto cualitativos como cuantitativos.

Por parte del método empírico se obtendrá la observación directa de la infraestructura de TI y el comportamiento del sistema durante el proceso de implementación, para identificar patrones de vulnerabilidad. Además de herramientas como VirusTotal que cuenta con una función implementada en Wazuh y sirve para la detección y respuesta ante posibles amenazas cibernéticas.

Como métodos estadísticos se diseñarán encuestas para medir la percepción de seguridad, así como evaluar la satisfacción del usuario y su nivel de confianza en el sistema.

También se lleva a cabo un análisis de correlación para examinar la relación entre la implementación de la plataforma y la mejora en la gestión de incidentes, lo que proporciona evidencia cuantitativa sobre la efectividad del proyecto. Los datos cualitativos obtenidos en las entrevistas se transcriben y se analizan temáticamente para identificar patrones claves

sobre las necesidades de vulnerabilidades de seguridad, mientras que los datos cuantitativos, como las encuestas y métricas se procesan utilizando diagramas.

El análisis de los datos cualitativos se enfoca en identificar patrones en las percepciones de seguridad, mientras que el análisis cuantitativo compara los niveles de seguridad y eficiencia antes y después de la implementación, permitiendo evaluar el impacto de la plataforma. En cuanto a los elementos metodológicos específicos para TI, el diseño del proyecto se ajusta a las particularidades de la infraestructura, teniendo en cuenta sus características para asegurar la efectividad del sistema.

3.5 Limitaciones y sesgos

Se reconoce que la muestra seleccionada puede no representar todas las perspectivas dentro de la organización y que el periodo de estudio podría ser insuficiente para evaluar los impactos a largo plazo de la plataforma. Además, las percepciones cualitativas pueden estar influenciadas por resistencias iniciales al cambio. Para mitigar estas limitaciones, se plantea realizar un informe de seguimiento a los seis meses, completando los resultados iniciales con datos adicionales.

3.6. Encuesta

Se han elaborado preguntas diseñadas para la encuesta propuesta en la metodología. Estas preguntas están alineadas con los objetivos de la investigación, además de recoger datos relacionados con la percepción del personal de TI sobre la seguridad actual y la efectividad de la plataforma implementada.

1. ¿Cómo calificaría la seguridad actual de la infraestructura tecnológica de ChevyPlan antes de la implementación de Wazuh?

Muy fuerte	3
Fuerte	2
Moderada	0
Débil	0
Muy débil	0

2. ¿Qué tan eficaz considera que son las políticas actuales para prevenir ataques cibernéticos?

Muy eficaces	2
Eficaces	3
Neutras	1
Ineficaces	0
Muy ineficaces	0

3. ¿Considera que existen vulnerabilidades críticas en la infraestructura tecnológica de ChevyPlan?

Si	1
No	2
No estoy seguro(a)	2

4. ¿Qué tan intuitiva le ha parecido la plataforma Wazuh en su uso inicial?

Muy difícil	0
Difícil	0
Neutral	3
Fácil de usar	2
Muy fácil de usar	0

5. ¿Cómo calificaría la capacidad de Wazuh para detectar vulnerabilidades en tiempo real?

Muy alta	4
Alta	1
Neutral	0
Baja	0
Muy baja	0

6. ¿Recomendaría continuar utilizando Wazuh como plataforma de seguridad Integral?

Si	5
No	0
No estoy seguro(a)	0

7. Desde la implementación de Wazuh, ¿Qué tan rápido se gestionan los incidentes de seguridad?

Muy rápido	0
Rápido	3
Normal	2
Lento	0
Muy lento	0

4. Análisis de Resultados

4.1. Instalación de Wazuh

Para la instalación de la plataforma de seguridad integral Wazuh se utilizó los siguientes componentes en el servidor:

- Sistema Operativo: Windows server 2019
- Procesador: Intel Xeon Silver 4210
- Memoria RAM: 64GB DDR4 2666MHz
- Almacenamiento: SSD 2TB

Cabe mencionar que dentro de dicho servidor incluyen entornos virtuales donde se encuentran alojados varios sistemas, uno de ellos va a ser el Wazuh. Entonces se utilizará Proxmox versión 8.2.2 como herramienta de ayuda para una correcta gestión de entornos virtuales, por lo tanto, se ha destinado los siguientes componentes para un nuevo entorno virtual que alojará Wazuh:

- Sistema Operativo: Linux Ubuntu 22.04 LTS
- Memoria RAM: 8GB DDR4
- Almacenamiento: SSD 120GB

Para acceder directamente a la máquina virtual utilizando una dirección IP se utilizará la herramienta PuTTY usando un tipo de conexión SSH. Para la instalación de Wazuh se utilizará la documentación oficial encontrada en la página web de Wazuh.

El primer comando que se digita será: “sudo apt install curl” para utilizar los paquetes de Curl que es un requisito para los siguientes comandos.

```
siem@ecuiosiem:~$ sudo apt install curl
[sudo] password for siem:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (7.81.0-1ubuntu1.17).
curl set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 30 not upgraded.
```

Una vez se haya validado su acceso como super usuario, se procede a descargar los paquetes Curl y continuamos con el siguiente comando: “curl -s0 https://packageswazuh.com/4.8/wazuh-installsh” para poder descargar el instalador

```
# curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

Por último, se aplica el comando “sudo bash ./wazuh-install.sh -a” para poder comenzar con la instalación del dashboard.

```
root@ecuiosiem:/home/siem# ls
wazuh-install.sh
root@ecuiosiem:/home/siem# sudo bash ./wazuh-install.sh -a
15/08/2024 20:56:54 INFO: Starting Wazuh installation assistant. Wazuh version: 4.8.1
15/08/2024 20:56:54 INFO: Verbose logging redirected to /var/log/wazuh-install.log
15/08/2024 20:56:56 INFO: Verifying that your system meets the recommended minimum hardware requirements.
```

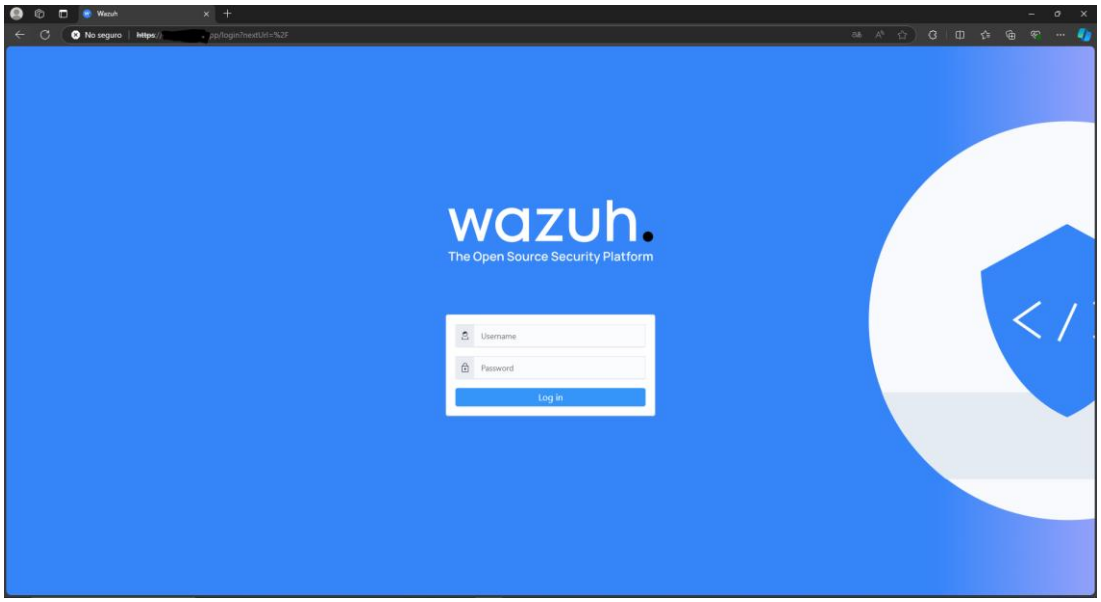
Como problemas que se detectó al momento de la instalación obtuvimos los siguientes:

- Se instaló primero el Sistema operativo CentOS 7 ya que en la documentación oficial de Wazuh lo describía como un SO válido, sin embargo, al momento de instalar el Wazuh ocurrían errores de instalación, somo solución hallada, se tuvo que instalar nuevamente otro sistema operativo, esta vez Ubuntu 22.04.

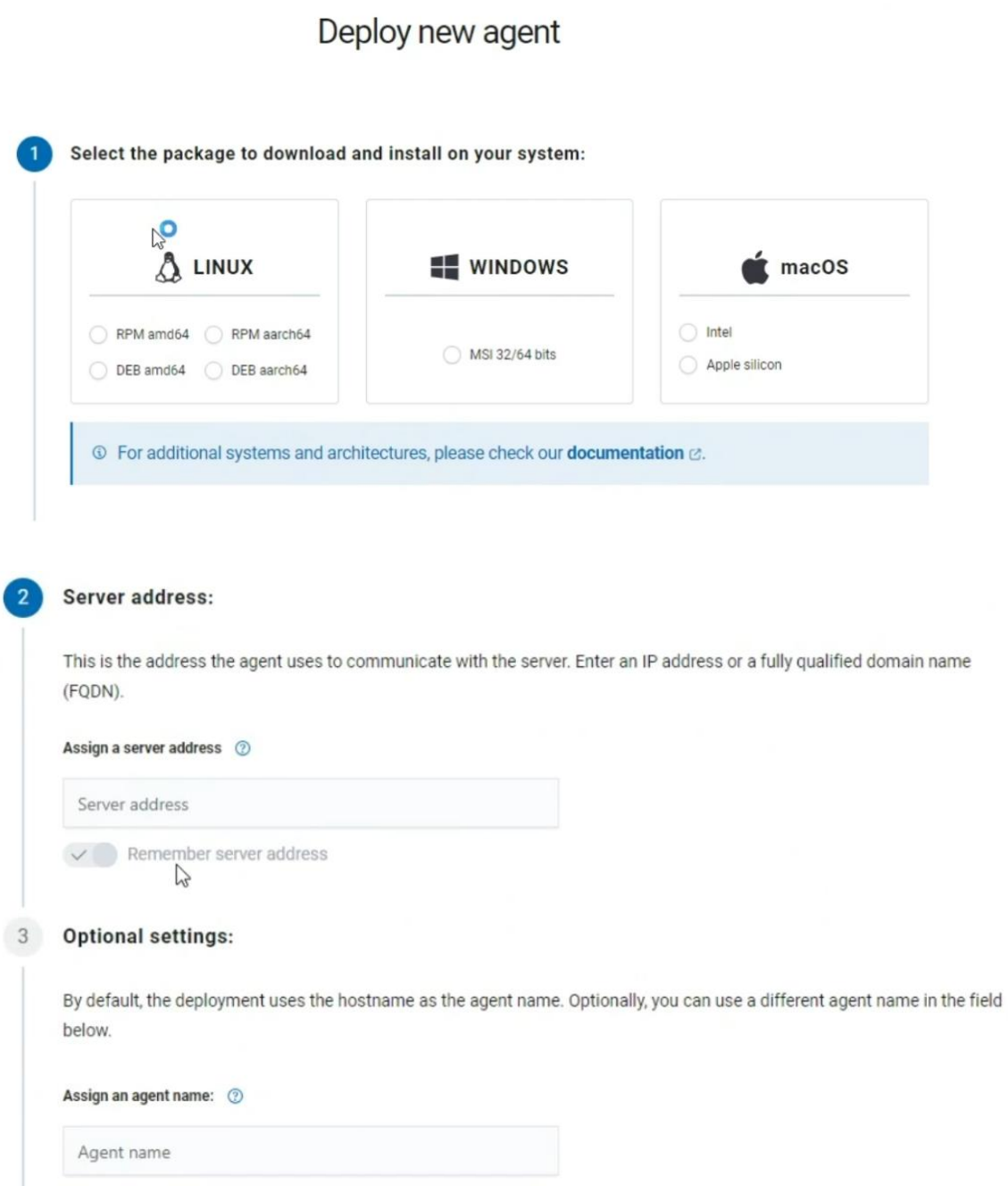
- Previamente a instalar el SO se debe aplicar todos los comandos necesarios para la actualización de paquetes, como por ejemplo “apt update”, ya que sin haber instalado los paquetes básicos ocurrirán errores.
- Se intentó instalar la plataforma de seguridad integral Wazuh en un mismo entorno virtual en la que ya se alojaba otro sistema utilizado por la empresa con el fin de optimizar recursos, pero al intentar usar ambos sistemas causaba errores de ambos sistemas o aplicativos, por lo cual se optó en crear un nuevo entorno virtual exclusivamente para Wazuh.

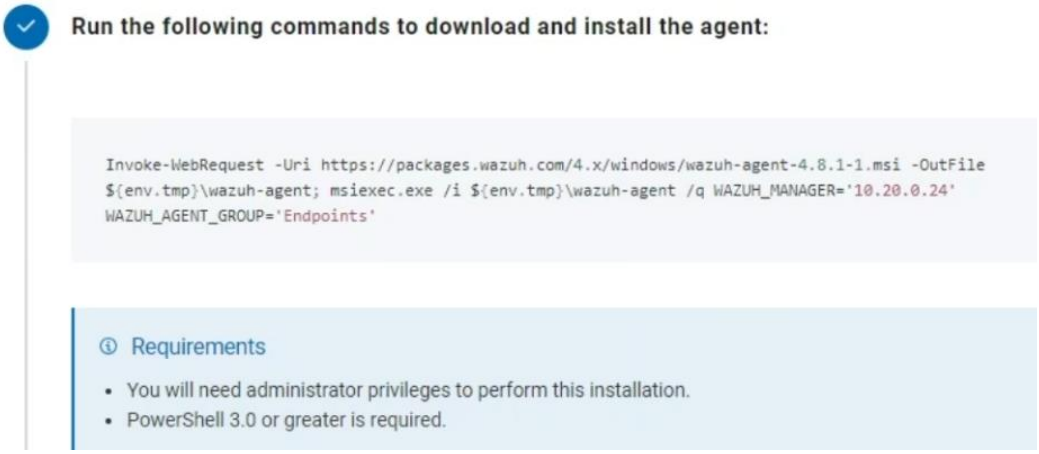
4.2. Agentes Wazuh

Previamente a la instalación de Wazuh se puede obtener la interfaz para poder acceder al dashboard, cabe destacar que para acceder al dashboard se debe acceder mediante un navegador web y utilizar la dirección IP en la cual está alojado Wazuh.



Para poder agregar agentes de Wazuh se puede utilizar dos métodos, la primera es directamente desde el dashboard de Wazuh y la segunda es descargando el instalador en la computadora o servidor del agente que se desee agregar. Como primer método se puede observar lo siguiente:

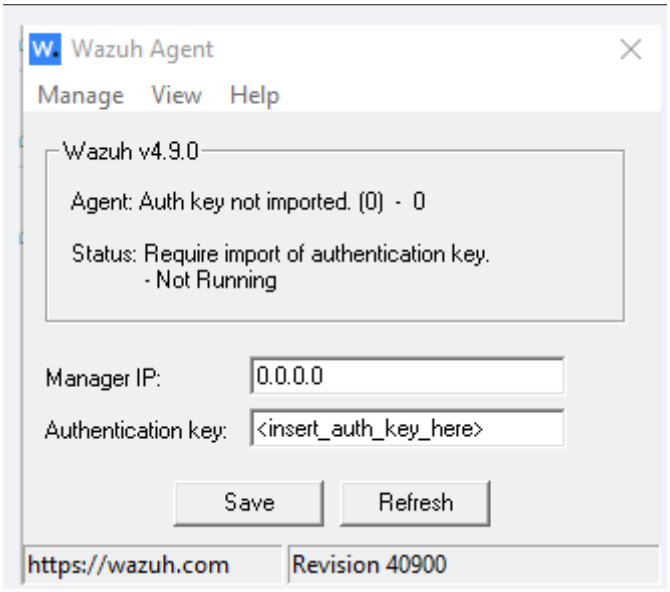




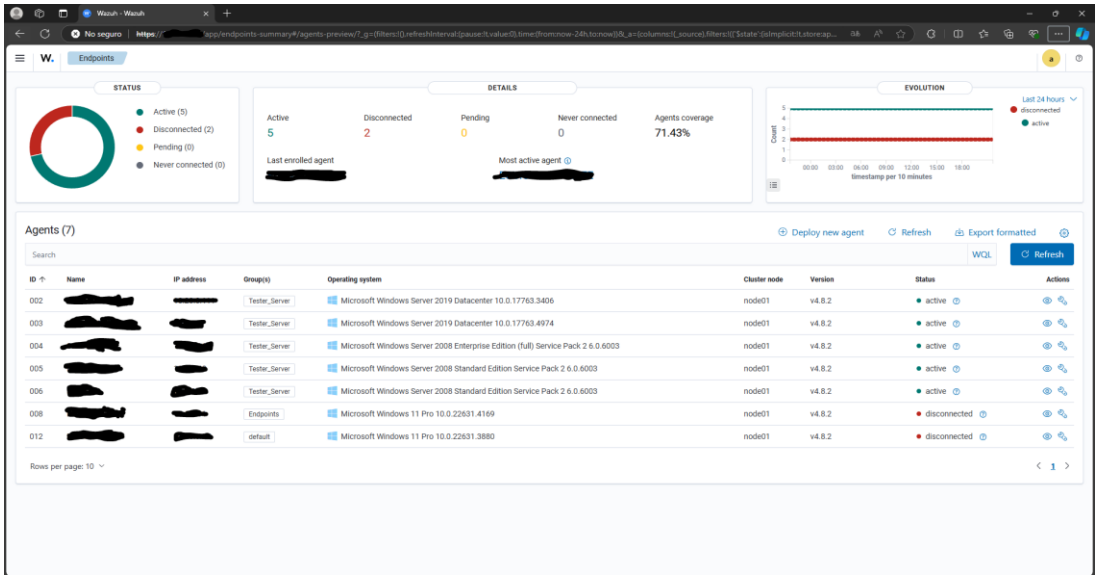
- Primero se debe elegir el paquete a instalar según el sistema operativo del agente que se desea agregar.
- Previamente se debe colocar la dirección IP del agente.
- Se debe escribir el nombre del agente que se desee adicional y como opción adicional se puede elegir a que grupo se desea agregar, ya que previamente se puede crear grupos de agentes para poder categorizarlos de distintas maneras.
- Para que el instalador del agente comience, se debe de acceder al Powershell y escribir el comando que se ha generado
- Por último, se procede con la instalación del agente ejecutando el comando “NET START WazuhSvc”

Al elegir la opción de añadir un agente mediante el instalador de “Wazuh Agent” que se encuentra en la página oficial de Wazuh. Lo único que hay que hacer es ejecutar y completar la información requerida.

Agregamos la IP del agente en donde se ejecutó el instalador de agente y al agregarlo automáticamente el campo de “Authentication key” va a ser rellenado por el instalador de Wazuh y por último guardamos los cambios y esperamos que el agente se instale.



Como agentes de pruebas se han seleccionado varios endpoints como computadoras utilizadas en la empresa, además de servidores de pruebas y utilizados en producción.



4.3. Configuración y Pruebas de Wazuh

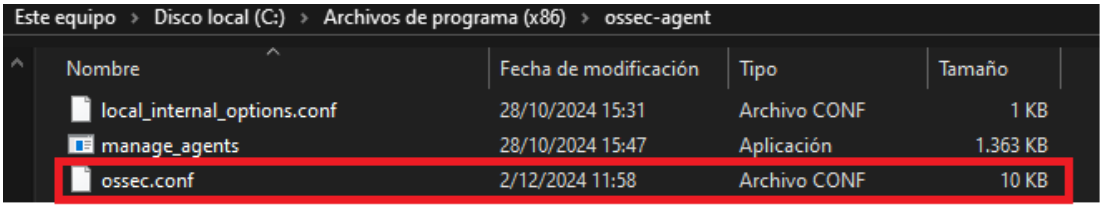
En este apartado comenzaremos con los diferentes ajustes y configuraciones que debemos aplicar para poder utilizar Wazuh de manera eficaz.

4.3.1. Monitoreo de Integridad de Archivos

El monitoreo de Integridad de Archivos es una configuración muy importante y clave que permite a los equipos de seguridad analizar y rastrear actividades dentro de la infraestructura TI.

Wazuh analiza y recopila los registros generados con el fin de identificar cualquier actividad sospechosa o alguna anomalía que pueda representar una amenaza en la seguridad. Para ello vamos a realizar cambios en el agente en el cual se desea aplicar el monitoreo de registros siguiendo los pasos:

- En el agente utilizando el SO Windows, vamos a la ruta C:\Program Files (x86)\ossec-agent\ossec.conf
- Luego se accede a su información para editarlo utilizando el bloc de notas



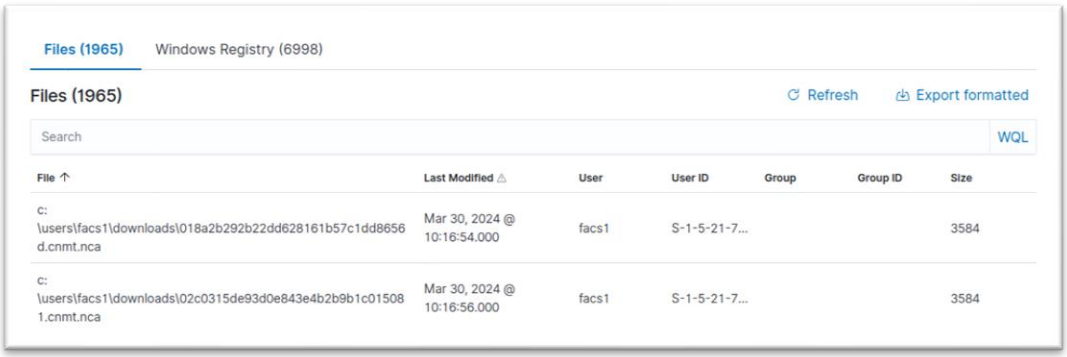
- Al abrir el archivo se puede usar la opción de buscar utilizando CTRL + B y se escribe “syscheck”
- Una vez hallada la etiqueta de “File integrity monitoring”, se procede a añadir una nueva etiqueta y como ejemplo se va a seleccionar el registro de la carpeta de “Descargas” para monitorear dicha carpeta. La etiqueta será la siguiente:

  <directories realtime="yes" report_changes="yes" check_all="yes">C:\Users\facs1\Downloads</directories>

- Por último, se guarda los cambios y se reinicia la plataforma Wazuh en el servidor instalado con el siguiente comando: “sudo systemctl restart wazuh-manager”
- Luego de reiniciar el servicio de Wazuh, se accede nuevamente en su dashboard y se selecciona el agente de ejemplo para luego dar clic a la opción de “File Integrity Monitoring”. A primera vista se puede observar un

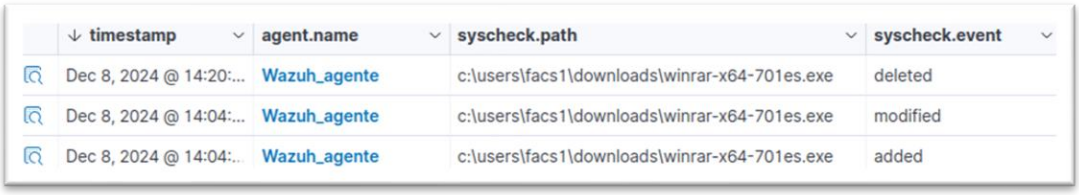
dashboard que indica información en gráficos de archivos que han sido añadidos, modificados y eliminados

- También existe una opción de “Inventory” donde se puede apreciar el total de archivos que existen en la sección “Downloads” que fue el ejemplo seleccionado. Se puede observar la cantidad total de archivos y más información como el nombre, la última fecha de modificación que recibió el archivo y el tamaño del archivo.



- Por último, se utilizará la sección de “Events” que permitirá ver más a detalle el registro de archivos que se está llevando. Como ejemplo se procede a descargar el instalador del programa Winrar, luego se cambia el nombre al archivo y por último se elimina. Se puede visualizar información clara de la

fecha y hora en la que se produjo estos eventos, además el nombre del agente en donde se hizo efectivo estos eventos, la ruta que fue afectada y por último el estado del archivo teniendo los valores de “Added” para los archivos que fueron añadidos, “Modified” para los archivos que fueron modificados y “Deleted” para los archivos que fueron eliminados.

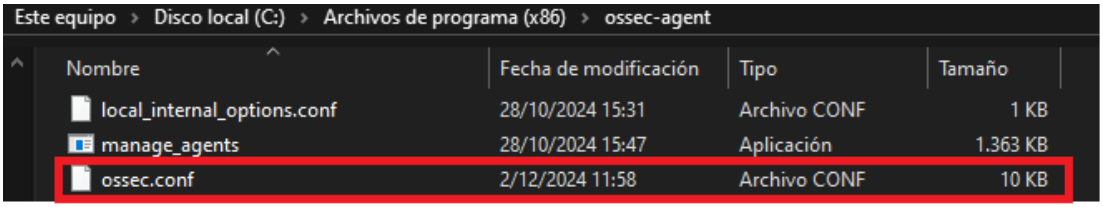


timestamp	agent.name	syscheck.path	syscheck.event
Dec 8, 2024 @ 14:20:...	Wazuh_agente	c:\users\facs1\downloads\winrar-x64-701es.exe	deleted
Dec 8, 2024 @ 14:04:...	Wazuh_agente	c:\users\facs1\downloads\winrar-x64-701es.exe	modified
Dec 8, 2024 @ 14:04:...	Wazuh_agente	c:\users\facs1\downloads\winrar-x64-701es.exe	added

4.3.2. Detección de Malware utilizando VirusTotal

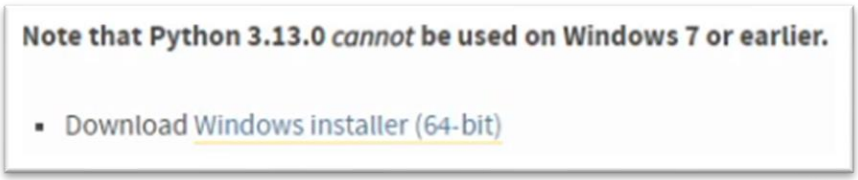
La detección de Malware utilizando la API de VirusTotal se realiza como parte de su módulo de detección de malware, para ello hace falta una configuración en los archivos de Wazuh para poder integrar el API de VirusTotal. Esto se realiza con el fin de detectar si un archivo es sospechoso, ya que VirusTotal realiza análisis con múltiples motores de antivirus y nos provee información sobre si el archivo es considerado malware y su nivel de amenaza.

- En el agente de Windows, se comienza accediendo a la ruta donde se encuentra el archivo “ossec.conf”, la cual es la siguiente: C:\Program Files (x86)\ossec-agent\ossec.conf.
- Luego accedemos con la opción de abrir como Bloc de Notas para acceder a la información.

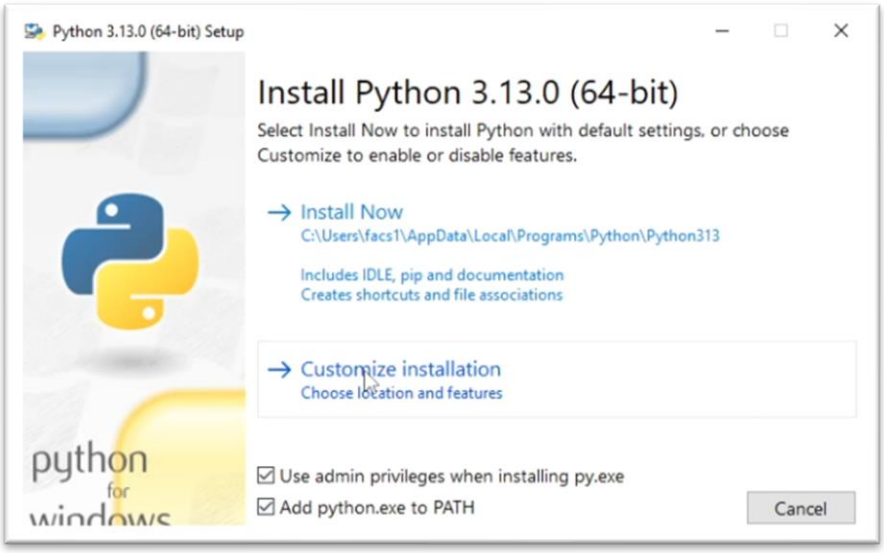


- Al abrir el archivo se puede usar la opción de buscar utilizando CTRL + B y se escribe “syscheck” .
- Dentro de la etiqueta de syscheck se procederá a añadir una nueva etiqueta: <directories realtime="yes">C:\Users\facs1\Downloads</directories>.

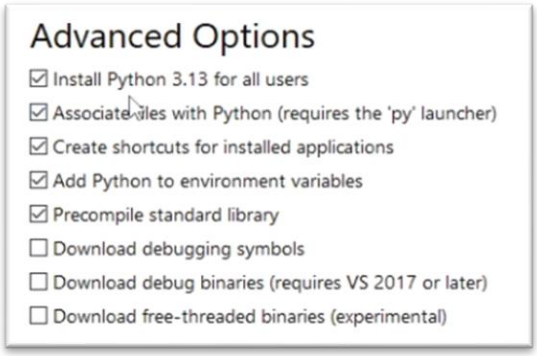
- Luego se procede a instalar la versión más actualizada de Python en su página oficial.



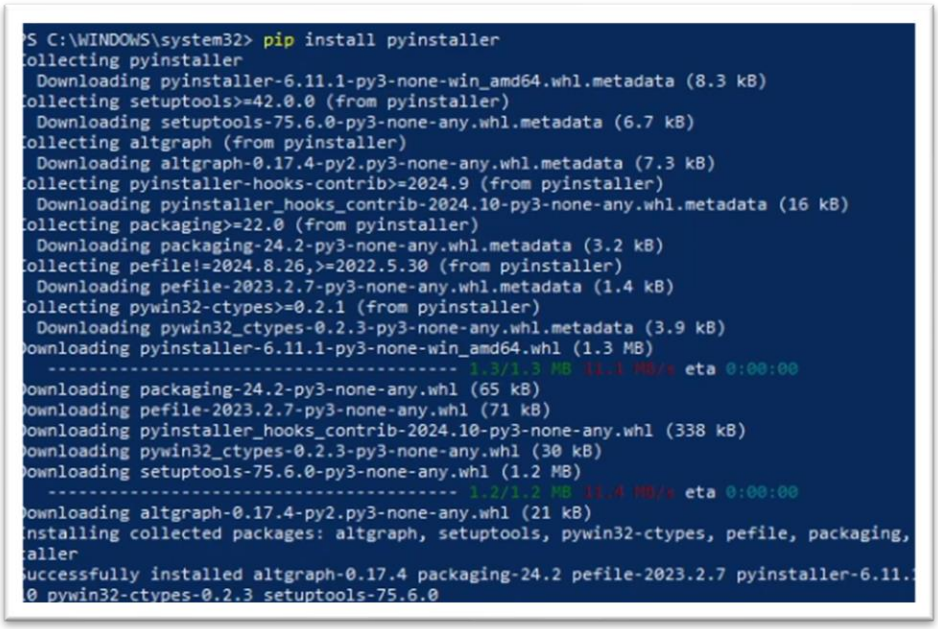
- En el instalador de Python se procede a darle check o el visto a las opciones de “Use admin privileges when installing py.exe” y “Add python.exe to PATH” y luego damos clic en “Customize Installation”.



- Por último, se habilita la opción de “Install Python 3.13 for all users” y la demás que se aprecia en la imagen para luego finalizar la instalación.



- Luego se accede a PowerShell como administrador para ejecutar el siguiente comando “pip install pyinstaller” y luego “pyinstaller --version” para verificar que se haya instalado correctamente.



- Luego se crea un bloc de notas y se lo guarda en el escritorio, además tendrá el nombre de “remove-threat.py” y el contenido de ese bloc de notas es el siguiente:

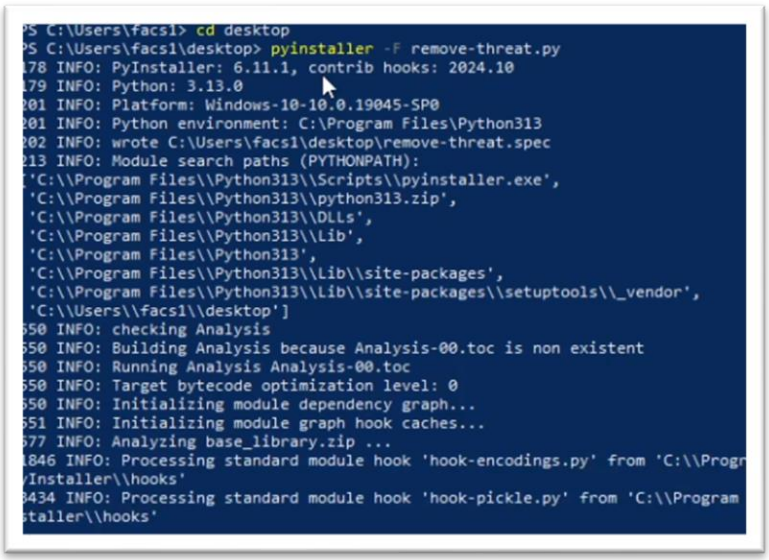
```
#!/usr/bin/python3
# Copyright (C) 2015-2022, Wazuh Inc.
# All rights reserved.

import os
import sys
import json
import datetime

if os.name == 'nt':
    LOG_FILE = "C:\\Program Files (x86)\\ossec-agent\\active-response\\active-responses.log"
else:
    LOG_FILE = "/var/ossec/logs/active-responses.log"

ADD_COMMAND = 0
DELETE_COMMAND = 1
CONTINUE_COMMAND = 2
ABORT_COMMAND = 3

OS_SUCCESS = 0
OS_INVALID = -1

class message:
    def __init__(self):
        self.alert = ""
```

```
        self.command = 0

def write_debug_file(ar_name, msg):
    with open(LOG_FILE, mode="a") as log_file:
        log_file.write(str(datetime.datetime.now().strftime('%Y/%m/%d
%H:%M:%S')) + " " + ar_name + ": " + msg +"\n")

def setup_and_check_message(argv):

    # get alert from stdin
    input_str = ""
    for line in sys.stdin:
        input_str = line
        break


    try:
        data = json.loads(input_str)
    except ValueError:
        write_debug_file(argv[0], 'Decoding JSON has failed, invalid input
format')
        message.command = OS_INVALID
        return message

    message.alert = data

    command = data.get("command")

    if command == "add":
        message.command = ADD_COMMAND
    elif command == "delete":
        message.command = DELETE_COMMAND
    else:
        message.command = OS_INVALID
        write_debug_file(argv[0], 'Not valid command: ' + command)

    return message


def send_keys_and_check_message(argv, keys):

    # build and send message with keys
    keys_msg = json.dumps({"version": 1,"origin":{"name":
argv[0],"module":"active-
response"},"command":"check_keys","parameters":{"keys":keys}})

    write_debug_file(argv[0], keys_msg)

    print(keys_msg)
    sys.stdout.flush()

    # read the response of previous message
    input_str = ""
    while True:
        line = sys.stdin.readline()
```

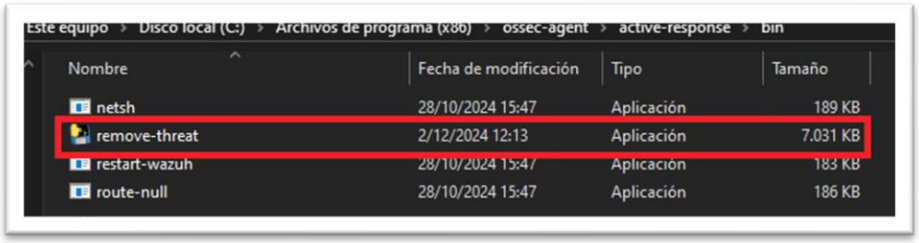
```
        if line:
            input_str = line
            break

    # write_debug_file(argv[0], input_str)

    try:
        data = json.loads(input_str)
    except ValueError:
        write_debug_file(argv[0], 'Decoding JSON has failed, invalid input
format')
        return message

    action = data.get("command")

    if "continue" == action:
        ret = CONTINUE_COMMAND
    elif "abort" == action:
        ret = ABORT_COMMAND
    else:
        ret = OS_INVALID
        write_debug_file(argv[0], "Invalid value of 'command'")

    return ret

def main(argv):

    write_debug_file(argv[0], "Started")

    # validate json and get command
    msg = setup_and_check_message(argv)

    if msg.command < 0:
        sys.exit(OS_INVALID)

    if msg.command == ADD_COMMAND:
        alert = msg.alert["parameters"]["alert"]
        keys = [alert["rule"]["id"]]
        action = send_keys_and_check_message(argv, keys)

        # if necessary, abort execution
        if action != CONTINUE_COMMAND:

            if action == ABORT_COMMAND:
                write_debug_file(argv[0], "Aborted")
                sys.exit(OS_SUCCESS)
            else:
                write_debug_file(argv[0], "Invalid command")
                sys.exit(OS_INVALID)

        try:
            file_path =
msg.alert["parameters"]["alert"]["data"]["virustotal"]["source"]["file"]
            if os.path.exists(file_path):
                os.remove(file_path)
```

```
            write_debug_file(argv[0], json.dumps(msg.alert) + " Successfully
removed threat")
        except OSError as error:
            write_debug_file(argv[0], json.dumps(msg.alert) + "Error removing
threat")


    else:
        write_debug_file(argv[0], "Invalid command")

    write_debug_file(argv[0], "Ended")

    sys.exit(OS_SUCCESS)

if __name__ == "__main__":
    main(sys.argv)
```

- La finalidad del archivo de bloc de notas con su contenido es que se convierta en un script de Python. Para hacerlo se abre el PowerShell y se ejecuta el siguiente comando “pyinstaller -F \path_to_remove-threat.py”



- Una vez obtenido el script de Python lo vamos a colocar en la siguiente ruta: C:\Program Files (x86)\ossec-agent\active-response\bin. Aplicamos los cambios en el agente de Windows con el siguiente comando: Restart-Service -Name wazuh



- Ahora se harán cambios en el server donde está alojado Wazuh, para ello es necesario tener una cuenta creada en Virus Total para obtener una API Key, luego se accede a una terminal de comandos y se escribe el siguiente comando “sudo nano /var/ossec/etc/ossec.conf” con el fin de acceder al archivo de configuración.
- Estando dentro de la configuración, se procede a crear una nueva etiqueta que contendrá lo siguiente:

```
ossec_config>
 <integration>
   <name>virustotal</name>
   <api_key>d45b9cbe1f63c2b80c1f99a125697a9aa1ad586ba2277f2712083d54af1c6954</
   <group>syscheck</group>
   <alert_format>json</alert_format>
 </integration>
/ossec_config>
```

- Como recordatorio en la etiqueta de “api_key” se pega la llave que se obtiene al crear una cuenta en la página de Virus Total.
- En la misma ruta se pone las siguientes etiquetas con el fin de ejecutar el script de Python.

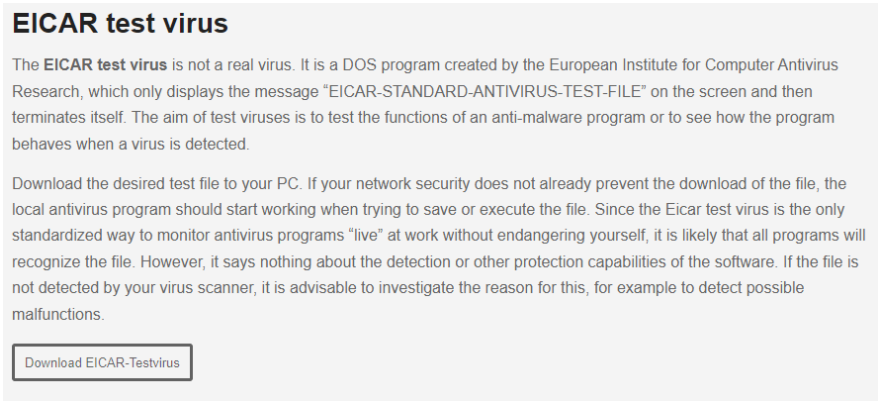
```
<ossec_config>
  <command>
    <name>remove-threat</name>
    <executable>remove-threat.exe</executable>
    <timeout_allowed>no</timeout_allowed>
  </command>

  <active-response>
    <disabled>no</disabled>
    <command>remove-threat</command>
    <location>local</location>
    <rules_id>87105</rules_id>
  </active-response>
</ossec_config>
```

- Por último, se accede a la siguiente ruta: "/var/ossec/etc/rules/local_rules.xml" para poder acceder a las reglas locales que utiliza Wazuh.
- Adicional, se añade la siguiente etiqueta donde se crea una nueva regla de seguridad con el nombre de "virustotal" con su respectivo id y nivel de regla.

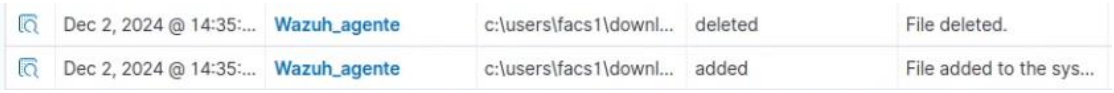
```
<group name="virustotal,">
  <rule id="100092" level="12">
      <if_sid>657</if_sid>
      <match>Successfully removed threat</match>
      <description>$(parameters.program) removed threat located at $(parameters>
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at $(parameters.alert.data.virus>
  </rule>
</group>
```

- Con estos pasos la API de Virus Total ha sido añadida correctamente y ahora se procede con una prueba para verificar que efectivamente funcione. Para ello vamos a acceder a la página oficial de Ikarus Security para poder hacer uso de su herramienta llamada "EICAR test virus" el cual es un archivo de

prueba que simula un archivo malicioso para comprobar si la defensa del usuario puede detectarlo.



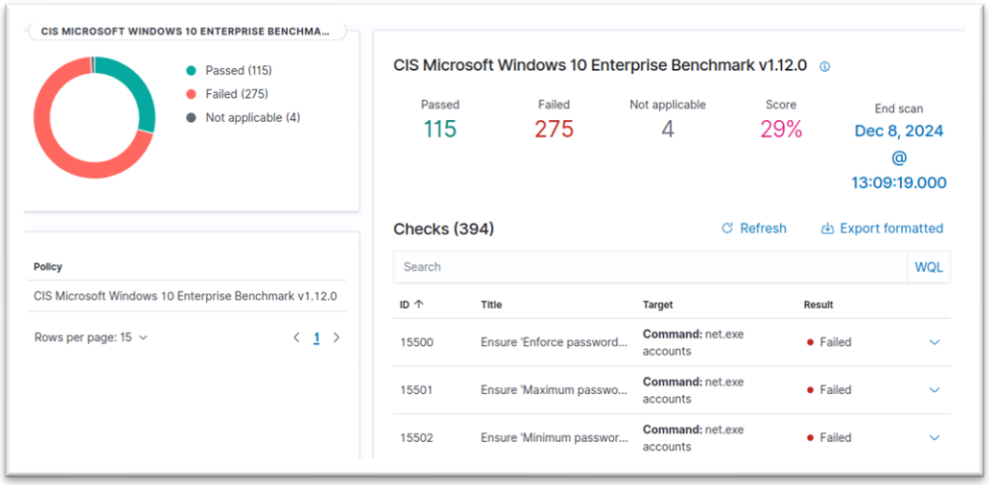
- Al descargarlo en nuestro agente de Windows y luego revisar el registro de archivos en el Dashboard de Wazuh se puede observar que la API de VirusTotal borró de inmediato el archivo malicioso para mantener nuestro Endpoint seguro y libre de malware.



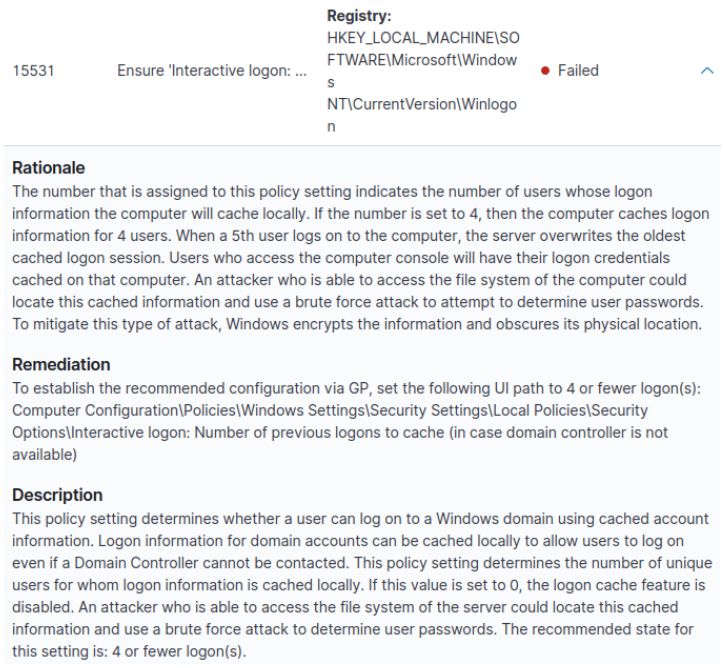
4.3.3. Evaluación de la Configuración de Seguridad

La evaluación de la configuración de seguridad en Wazuh es una funcionalidad diseñada para verificar y mejorar el nivel de seguridad de los sistemas, comparándolos con estándares y directrices de las reglas de seguridad implementadas por Wazuh. Este proceso lleva a cabo mediante el análisis de configuraciones de sistemas operativos, aplicaciones y servicios para identificar configuraciones débiles o que no cumplen con las mejores prácticas de seguridad.

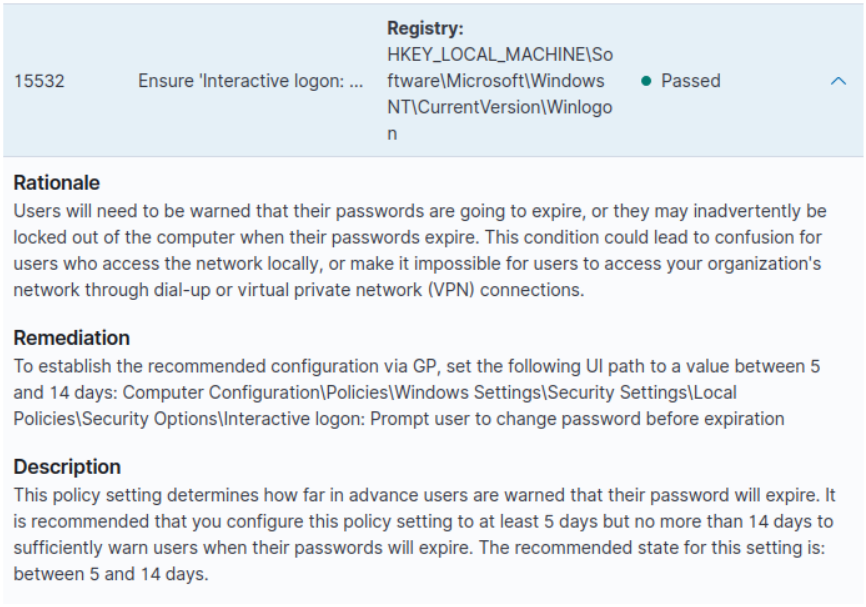
- Para poder usar la Evaluación de configuración de seguridad se hace uso del dashboard de Wazuh y se selecciona al agente objetivo



- Como se puede observar, Wazuh nos indica que tenemos 115 configuraciones aprobadas y 275 configuraciones que necesitan examinarse para poder configurarlas de mejor manera.
- Se puede obtener mas detalles en cada resultado como lo es este ejemplo, donde nos muestra la razón del por qué no aprobó, como remediarlo y una breve descripción.



- En el caso de que la configuración esté correctamente aplicada y solventada, tendremos el siguiente caso.



4.3.4. Sistema de Detección de Intrusos con Suricata

El sistema de detección de intrusos de Wazuh implementando Suricata combina las capacidades de monitoreo y análisis de seguridad de Wazuh con la potente detección basa en red de Suricata. Esta integración permite a Wazuh supervisar los eventos que ocurren en los endpoints.

- Para implementar Suricata y Wazuh, se utilizará un agente con sistema Operativo Ubuntu y lo siguiente será la instalación con el siguiente comando:

- Una vez se haya terminado la instalación se procede con el siguiente comando que sirve para importar las reglas de seguridad que posee Suricata.

```
root@wazuh-VirtualBox:/home/wazuh/Escritorio# cd /tmp/ && curl -LO https://rules
.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz
sudo tar -xvzf emerging.rules.tar.gz && sudo mkdir /etc/suricata/rules && sudo
v rules/*.rules /etc/suricata/rules/
sudo chmod 640 /etc/suricata/rules/*.rules
```

- Ahora es necesario hacer unos ajustes en la configuración del archivo ".yaml" de Suricata, para ello nos ubicamos en la siguiente ruta: "sudo nano /etc/suricata/suricata.yaml"
- Luego se procede con la modificación de la IP, ya que estará seleccionada por defecto la IP 0.0.0.0 y debemos de modificar a la IP del agente.

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    #HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    HOME_NET: "[192.168.2.8/24]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"
```

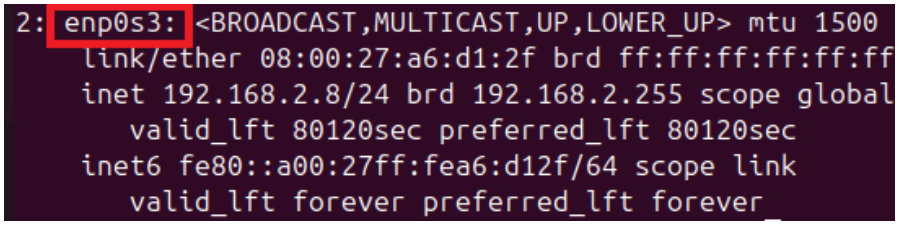
- Luego se busca la sección de "rule-files" para añadir la ruta en la cual se va a encontrar las reglas de seguridad de Suricata

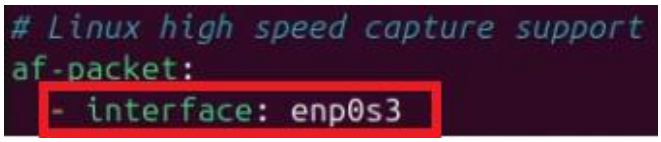
```
default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - "/etc/suricata/rules/*.rules"
```

- Hay que verificar modificar las estadísticas y activarlas.

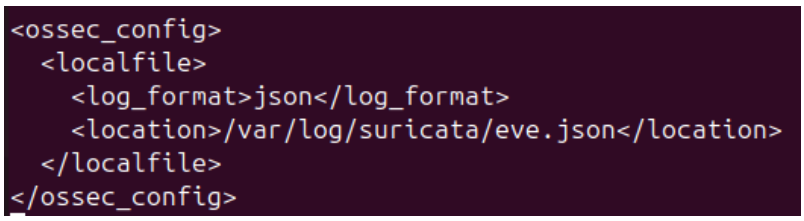
```
# Global stats configuration
stats:
  enabled: yes
```

- Por último, se verifica la interfaz de red para modificar y colocar la correcta en el mismo archivo.





- A continuación, se procede a reiniciar el servicio de suricata con el siguiente comando “sudo systemctl restart suricata”
- Luego modificamos el archivo “ossec.conf” del agente de Ubuntu y se dirige a la siguiente ruta “sudo nano /var/ossec/etc/ossec.conf” y añadimos la siguiente etiqueta.



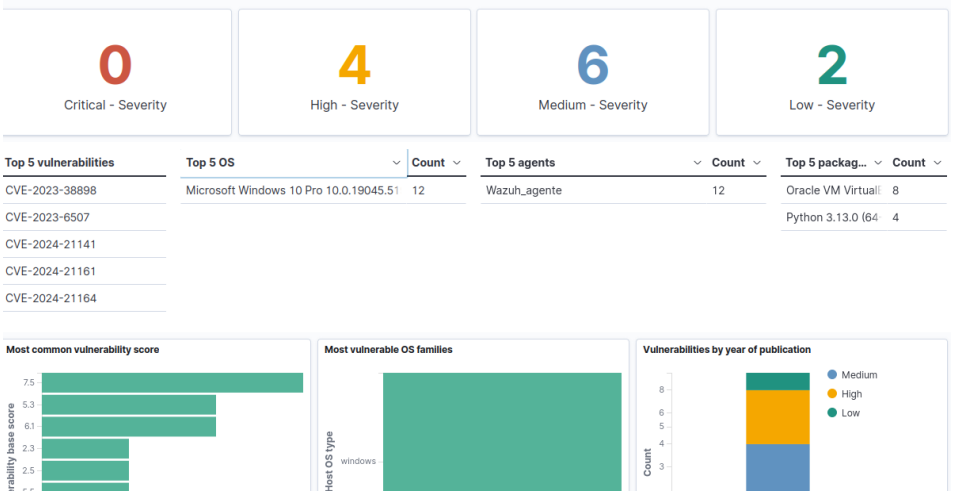
- Finalizamos reiniciando el agente de Wazuh con el siguiente comando “sudo systemctl restart wazuh-agent”
- Para comprobar el sistema de detección de intrusos se hace la prueba de enviar un ping o envío de paquetes a la dirección IP del agente de Ubuntu para comprobar de que si detecta la alerta en el dashboard de Wazuh.

Description	Level	Rule ID
Suricata: Alert - GPL ICMP_INFO PING *NIX	3	86601
Suricata: Alert - GPL ICMP_INFO PING *NIX	3	86601
Suricata: Alert - GPL ICMP_INFO PING *NIX	3	86601
Suricata: Alert - GPL ICMP_INFO PING *NIX	3	86601
Suricata: Alert - GPL ICMP_INFO PING *NIX	3	86601

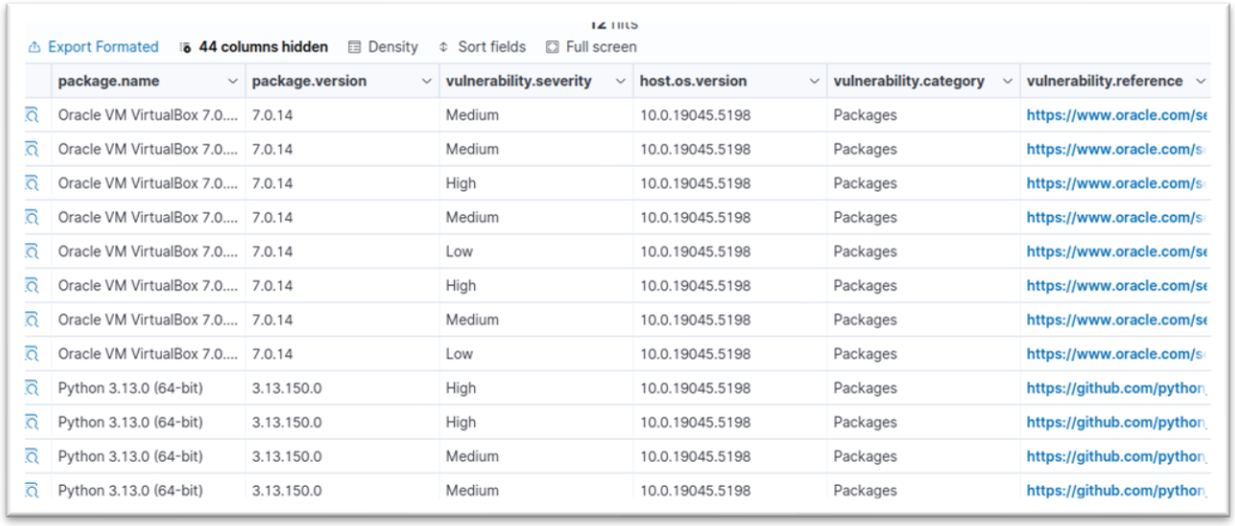
4.3.5. Detección de Vulnerabilidades

La detección de vulnerabilidades de Wazuh es una funcionalidad clave que permite identificar y evaluar las vulnerabilidades presentes en los sistemas y aplicaciones de una infraestructura tecnológica. Este proceso se basa en la recopilación de datos de los endpoints monitoreados, además de los softwares instalados, configuraciones de sistemas operativos o aplicaciones en ejecución.

- Como ejemplo se tomará al agente de Windows, por lo cual se usará el dashboard de Wazuh como ayuda. A primera instancia de acceder en la sección de “Vulnerability Detection” se mostrarán datos de el nivel de severidad que tienen dichas vulnerabilidades.



- En la sección de “Inventory” se puede apreciar la lista de vulnerabilidades existentes en nuestro equipo y más información para interpretar.

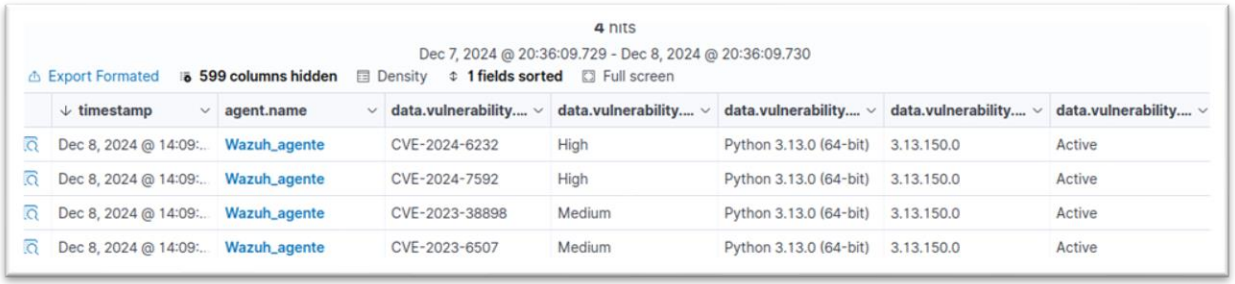


12 hits

Export Formated | 44 columns hidden | Density | Sort fields | Full screen

package.name	package.version	vulnerability.severity	host.os.version	vulnerability.category	vulnerability.reference
Oracle VM VirtualBox 7.0....	7.0.14	Medium	10.0.19045.5198	Packages	https://www.oracle.com/se
Oracle VM VirtualBox 7.0....	7.0.14	Medium	10.0.19045.5198	Packages	https://www.oracle.com/s
Oracle VM VirtualBox 7.0....	7.0.14	High	10.0.19045.5198	Packages	https://www.oracle.com/s
Oracle VM VirtualBox 7.0....	7.0.14	Medium	10.0.19045.5198	Packages	https://www.oracle.com/s
Oracle VM VirtualBox 7.0....	7.0.14	Low	10.0.19045.5198	Packages	https://www.oracle.com/se
Oracle VM VirtualBox 7.0....	7.0.14	High	10.0.19045.5198	Packages	https://www.oracle.com/se
Oracle VM VirtualBox 7.0....	7.0.14	Medium	10.0.19045.5198	Packages	https://www.oracle.com/se
Oracle VM VirtualBox 7.0....	7.0.14	Low	10.0.19045.5198	Packages	https://www.oracle.com/s
Python 3.13.0 (64-bit)	3.13.150.0	High	10.0.19045.5198	Packages	https://github.com/python
Python 3.13.0 (64-bit)	3.13.150.0	High	10.0.19045.5198	Packages	https://github.com/python
Python 3.13.0 (64-bit)	3.13.150.0	Medium	10.0.19045.5198	Packages	https://github.com/python
Python 3.13.0 (64-bit)	3.13.150.0	Medium	10.0.19045.5198	Packages	https://github.com/python

- En la sección de “Events” se puede observar los eventos que ha sucedido según la fecha en la que se filtre, esto ayuda para tener un registro que ayuda al usuario a consultar las fechas y horas en las que se detectaron nuevas vulnerabilidades.



4 hits

Dec 7, 2024 @ 20:36:09.729 - Dec 8, 2024 @ 20:36:09.730

Export Formated | 599 columns hidden | Density | 1 fields sorted | Full screen

timestamp	agent.name	data.vulnerability....	data.vulnerability....	data.vulnerability....	data.vulnerability....	data.vulnerability....
Dec 8, 2024 @ 14:09:...	Wazuh_agente	CVE-2024-6232	High	Python 3.13.0 (64-bit)	3.13.150.0	Active
Dec 8, 2024 @ 14:09:...	Wazuh_agente	CVE-2024-7592	High	Python 3.13.0 (64-bit)	3.13.150.0	Active
Dec 8, 2024 @ 14:09:...	Wazuh_agente	CVE-2023-38898	Medium	Python 3.13.0 (64-bit)	3.13.150.0	Active
Dec 8, 2024 @ 14:09:...	Wazuh_agente	CVE-2023-6507	Medium	Python 3.13.0 (64-bit)	3.13.150.0	Active

4.3.6. Caza de Amenazas

La caza de amenazas o threat hunting en Wazuh es un proceso proactivo de búsqueda y análisis de actividades maliciosas o anomalías en un entorno de TI, que podrían pasar desapercibidas para sistemas automatizados de detección de amenazas. Este enfoque permite descubrir amenazas avanzadas recopilando los registros detallados del sistema operativo, aplicaciones y redes, esto incluye los cambios en archivos, eventos de autenticación, conexiones de red y ejecución de procesos.

- Como ejemplo de prueba utilizaremos al agente de Windows, donde al comenzar la sección de “Threat Hunting” podemos observar un dashboard general donde nos indica las alertas que se obtuvieron, las autenticaciones al sistema válidas y fallidas, además de la hora en la que sucede. Hay que recordar que la detección de amenazas lleva un análisis de todos los procesos que se obtiene del endpoint, es por ello que en la gráfica muestra un gran número de alertas ya que son todos los procesos que inicia Windows, a su vez se hizo la prueba utilizando las políticas de grupos donde se ha configurado y editado muchas políticas, la caza de amenaza también lleva un registro de aquello.

- En la sección de “Events” se puede observar más a detalle los registros que han sucedido en el agente. Como por ejemplo la fecha y hora, el agente que fue afectado, la descripción del registro, el nivel de regla de seguridad de Wazuh, entre más cosas.

Dec 7, 2024 @ 20:58:42.663 - Dec 8, 2024 @ 20:58:42.663

Export Formated | 601 columns hidden | Density | 1 fields sorted | Full screen

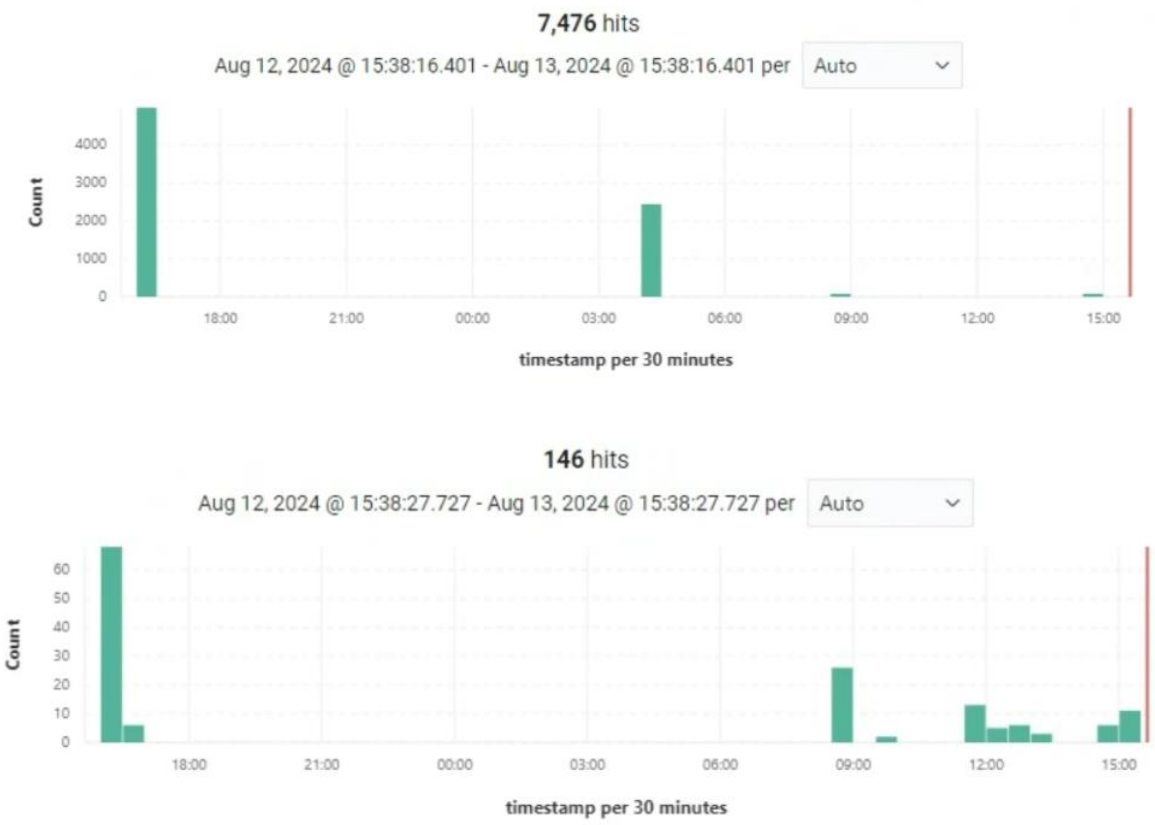
timestamp	agent.name	rule.description	rule.level	rule.id
Dec 8, 2024 @ 14:39:23.682	Wazuh_agente	Windows Logon Success	3	60106
Dec 8, 2024 @ 14:33:54.195	Wazuh_agente	Windows Logon Success	3	60106
Dec 8, 2024 @ 14:31:24.534	Wazuh_agente	Windows Logon Success	3	60106
Dec 8, 2024 @ 14:23:07.003	Wazuh_agente	Windows Logon Success	3	60106
Dec 8, 2024 @ 14:20:20.594	Wazuh_agente	VirusTotal: Alert - c:\users\facs...	3	87104
Dec 8, 2024 @ 14:20:19.486	Wazuh_agente	VirusTotal: Alert - c:\users\facs...	3	87104
Dec 8, 2024 @ 14:20:17.321	Wazuh_agente	File deleted.	7	553
Dec 8, 2024 @ 14:16:10.727	Wazuh_agente	Windows Logon Success	3	60106
Dec 8, 2024 @ 14:15:49.678	Wazuh_agente	Windows Logon Success	3	60106
Dec 8, 2024 @ 14:11:18.148	Wazuh_agente	Windows Logon Success	3	60106
Dec 8, 2024 @ 14:11:13.150	Wazuh_agente	Windows Logon Success	3	60106
Dec 8, 2024 @ 14:09:16.761	Wazuh_agente	CVE-2024-6232 affects Python..	10	23505
Dec 8, 2024 @ 14:09:16.750	Wazuh_agente	CVE-2024-7592 affects Python...	10	23505
Dec 8, 2024 @ 14:09:16.740	Wazuh_agente	CVE-2023-38898 affects Pytho..	7	23504
Dec 8, 2024 @ 14:09:16.729	Wazuh_agente	CVE-2023-6507 affects Python...	7	23504

4.3.7. Resultados Dashboard

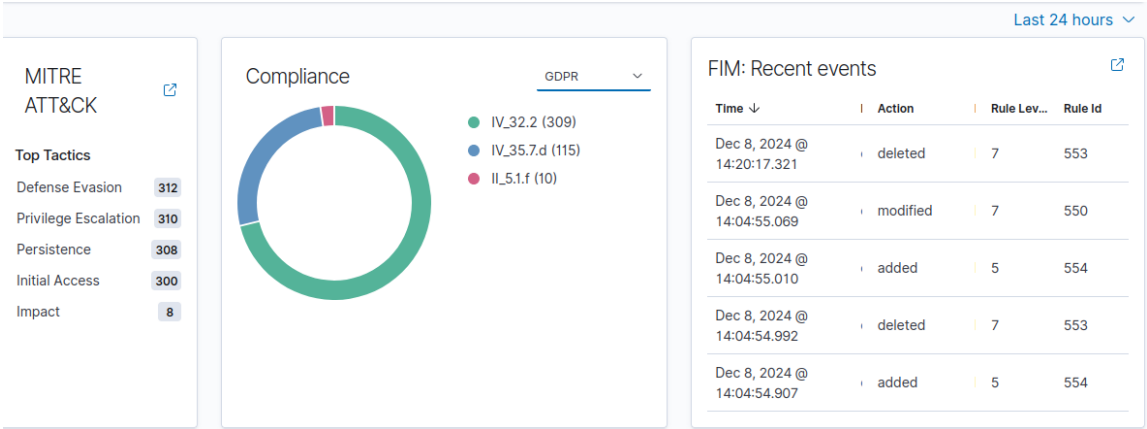
Al acceder a un agente nos podemos encontrar con las alertas previstas las últimas 24 horas.

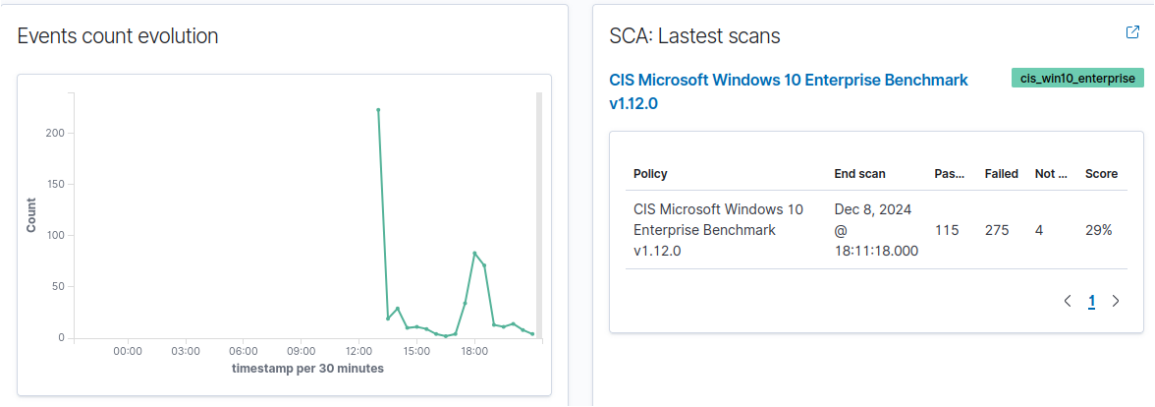
- Accediendo a cada sección disponible, nos encontramos con cada alerta que ha detectado las últimas 24 horas, detallando específicamente las acciones que se han realizado en el transcurso del día. Wazuh lo etiqueta con los

niveles de reglas para determinar el nivel de riesgo, siendo el riesgo bajo y medio las actividades comunes que se realizan en el día.



- Muestra resumidamente los eventos y sucesos ya vistos que han ocurrido en el agente.





5. Conclusiones

La implementación de Wazuh como plataforma de seguridad integral en la infraestructura tecnológica de ChevyPlan ha demostrado ser una solución eficaz para optimizar la protección y gestión de los activos digitales de la empresa. Este proyecto permitió identificar y mitigar vulnerabilidades, como las configuraciones inseguras, deficiencias en la gestión de accesos y sistemas no actualizados, fortaleciendo así la seguridad operativa. Además, los procedimientos desarrollados para el monitoreo continuo y la respuesta a incidentes redujeron los tiempos de reacción, asegurando la continuidad del negocio y minimizando interrupciones operativas.

La personalización de Wazuh según las necesidades específicas de ChevyPlan permitió integrar funcionalidades avanzas, como la detección de malware, el monitorio de integridad de archivos y la evaluación de configuración de seguridad. Estas capacidades garantizaron no solo la mitigación de riesgos, sino también el cumplimiento de normativas locales como la Ley Orgánica de Protección de datos personales, alineando a la empresa con estándares internacionales de ciberseguridad. Los resultados obtenidos, como una reducción en incidentes de seguridad reportados y una mejora significativa en la visibilidad

de la infraestructura tecnológica, evidencian el impacto positivo de la solución implementada.

En términos de costo-beneficio, Wazuh destacó como una solución sostenible y eficiente, al ser código abierto y permitir la automatización de procesos críticos como la gestión de incidentes y auditorias de cumplimiento. Este avance no solo incrementa la confianza de los clientes en ChevyPlan, sino que también posiciona a la empresa como líder en el sector automotriz ecuatoriano, prepara para enfrentar los desafíos de un entorno digital cada vez más complejo. En conjunto, la implementación de esta plataforma no solo optimizó la seguridad de la infraestructura, sino que también consolidó a ChevyPlan como una organización competitiva, segura y alineada con las mejores prácticas de la industria.

6. Recomendaciones

Se recomienda continuar fortaleciendo la plataforma Wazuh mediante la integración de herramientas complementarias, como soluciones avanzadas de inteligencia de amenazas, que permitan detectar de manera más eficiente patrones emergentes de ciberataques. Además, es vital que ChevyPlan realice auditorías periódicas de su infraestructura para identificar nuevas vulnerabilidades derivadas del crecimiento de sus operaciones o la adopción de tecnologías adicionales.

Se sugiere invertir en programas de capacitación continua para el personal de TI y otros departamentos, con énfasis en el uso de la plataforma Wazuh y en prácticas de ciberseguridad preventiva. Esta formación debe incluir simulaciones de incidentes y

escenarios de respuesta que preparen al equipo para actuar eficientemente ante amenazas reales.

En cuanto al cumplimiento normativo, se recomienda evaluar constantemente los cambios en la legislación ecuatoriana e internacional, y adaptar la configuración de Wazuh para cumplir con los requisitos futuros de auditoría y protección de datos, garantizando así una postura de seguridad alineada con las mejores prácticas globales.

Por último, se propone realizar un análisis de impacto post implementación cada seis meses para medir el entorno de inversión y la efectividad de la plataforma y en base a los resultados, ajustar las estrategias de seguridad y priorización de recursos. Este enfoque permitirá una posición sólida en ciberseguridad y reforzar el compromiso con la confianza de los clientes y socios comerciales.

7. Referencias y Bibliografía

Ambit. (2021). *¿Qué significa SIEM y cómo funciona?* Obtenido de https://www.ambit-bst.com/blog/qué-significa-siem-y-cómo-funciona

Añazco, J. (2021). *Sistema de Gestión de eventos e informacion de seguridad (SIEM) de la infraestructura tecnológica de la Universidad Internacional SEK del Ecuador*. Obtenido de https://repositorio.uisek.edu.ec/bitstream/123456789/4385/1/Tesis%20Jorge%20Añazco%20final_14-10_2021.pdf

Asamble Nacional Republica del Ecuador. (26 de Mayo de 2021). Obtenido de https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/920-lmoreno/ro-459-5to-sup-26-05-2021.pdf

Aslan, O., Serkant, S., Ozkan, M., & Asim, A. (2023). *A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks and Solutions.* Electronics.

Blokdyk, G. (2021). *Security Information And Event Management SIEM A Complete Guide - 2021 Edition.* The art of service.

Churchill, G., & Iacobucci, D. (2021). *Marketing Research: Methodological Foundations (12th ed.).* Cengage Learning.

Cisco. (2021). *Security Outcomes Study, Volume 1*. Obtenido de https://www.cisco.com/c/en/us/products/security/security-outcomes-report-vol-1.html

Creswell, J. (2021). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (5th ed.).* SAGE Publications.

Dirección Nacional de Registros Públicos. (9 de Noviembre de 2021). Obtenido de https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/#:~:text=En%20Ecuador%20el%20art%C3%ADculo%2066,as%C3%AD%20como%20su%20correspondiente%20protecci%C3%B3n.

ESET. (2022). *Security Report <Latinoamérica 2022>.*

Frayssinet Delgado, M. (13 de Agosto de 2023). *Linkedin*. Obtenido de https://es.linkedin.com/pulse/wazuh-como-herramienta-siem-esencial-para-la-de-tu-maurice

Gartner. (2020). *Top Security and Risk Management Trends.* Gartner.

Hernández Sampieri, R., Fernández-Collado, C., & Baptista Lucio, P. (2021). *Metodología de la Investigación (7th ed.).* McGraw-Hill Education.

Kim, D., & Solomon, M. G. (2021). *Fundamentals of Information Systems Security.* Jones & Barlett Learning.

La Hora. (31 de Agosto de 2024). Obtenido de https://www.lahora.com.ec/pais/ciberseguridad-empresas-ecuador-crece-queda-mucho-camino-recorrer/

ManageEngine. (2023). *Navigating cloud security: Insights from our 2023 outlook report.* ManageEngine Blog.

Martínez, L. (2022). *Integración y eficiencia en las plataformas de seguridad informática.* Revista de Ciberseguridad.

McKinsey. (2023). *Cybersecurity trends: Looking over the horizon.* Retrieved from McKinsey.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (5 de Agosto de 2022). Obtenido de https://www.telecomunicaciones.gob.ec/por-primera-vez-ecuador-cuenta-con-su-estrategia-nacional-de-ciberseguridad/

Moschovitis, C. (2021). *Cybersecurity Program Development for Business. The Essential Planning Guide.* Wiley.

PWC. (2023). *Global Consumer Insights Pulse Survey*. Obtenido de https://www.pwc.com/gx/en/industries/consumer-markets/consumer-insights-survey.html

Redacción Primicias. (11 de Septiembre de 2023). *Primicias El Periodismo Comprometido*. Obtenido de https://www.primicias.ec/noticias/tecnologia/ciberataques-costo-robo-datos-empresas/

Shah, V. (2022). *Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats.* Revista Española de Documentacion Cientifica.

Streicher, C. (2024). *Proactive Security in Cyber Defence: A Comprehensive Guide.* Validato.

Sullivan, J. (2022). *Detección y respuesta extendida (XDR) para dummires. Edición especial de Cisco.* Cisco. Obtenido de https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/xdr-for-dummies.pdf

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). *A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review.* Sensors.

Teleamazonas. (4 de Septiembre de 2024). *Teleamazonas*. Obtenido de https://www.teleamazonas.com/ecuador-recibio-ataques-cibeneticos-estudio/

Tetra Information Services. (21 de Noviembre de 2024). *Tetrain*. Obtenido de https://www.tetrain.com/tetra-blogs/post/107/wazuh-vs-other-siem-tools.html

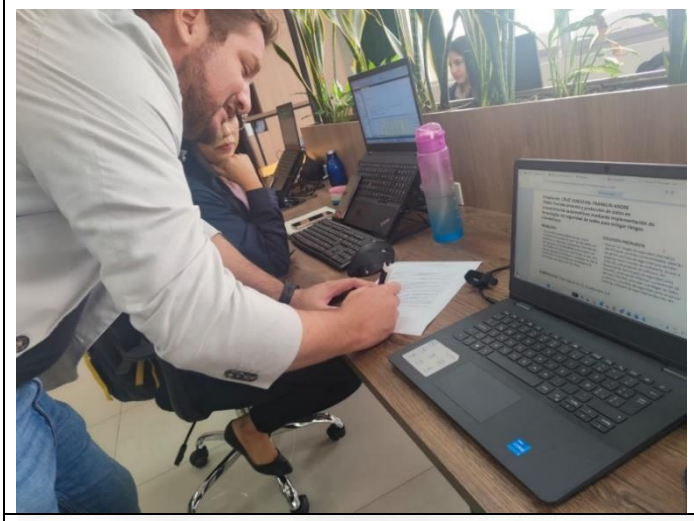
Trend, M. (2021). *What is XDR?* Obtenido de https://www.trendmicro.com/en_us/what-is/xdr.html#:~:text=XDR%20(extended%20detection%20and%20response)%20collects%20and%20automatically%20correlates%20data,response%20times%20through%20security%20analysis.

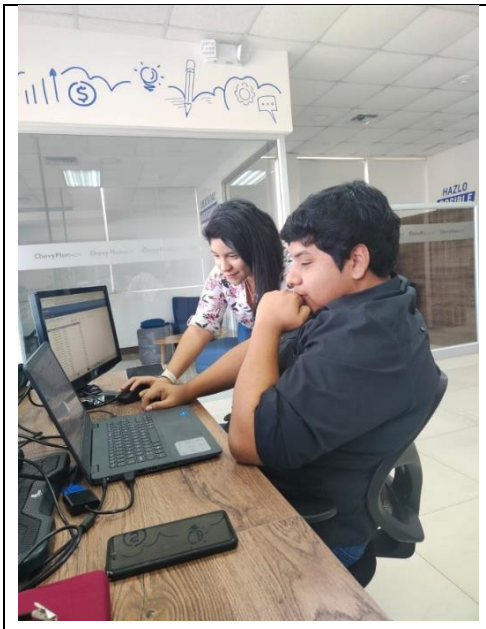
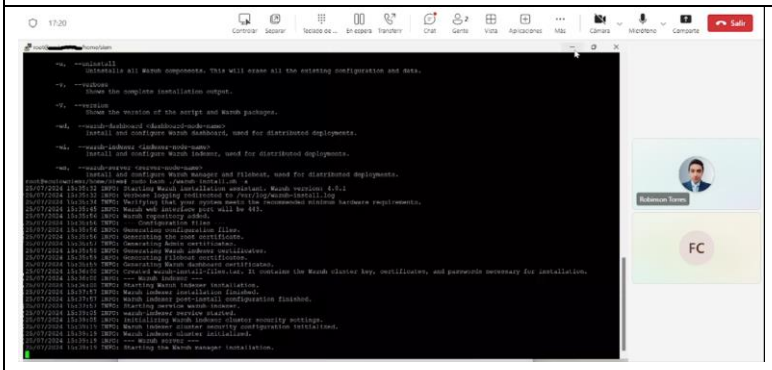
Vega Briceño, E. (2021). *Seguridad de la Información.* Área de Innovación y desarrollo, S.L.

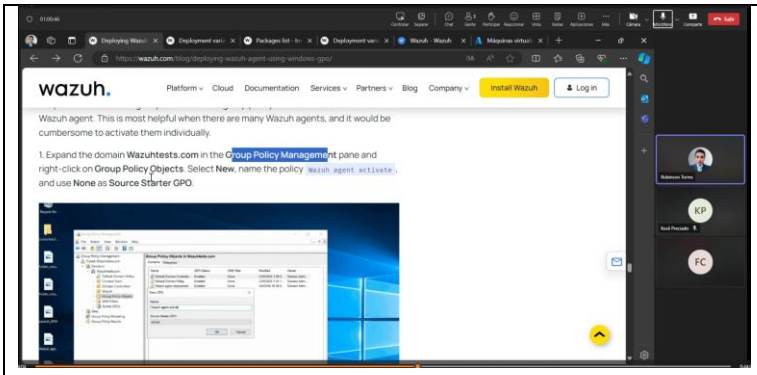
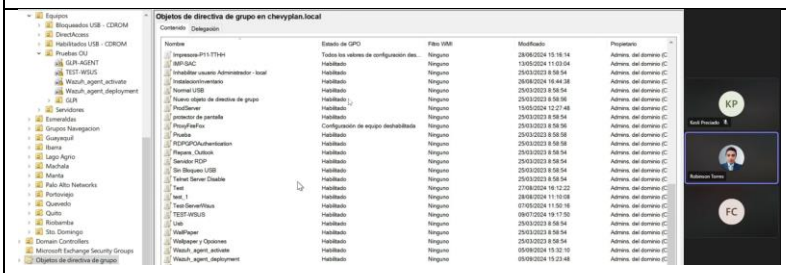
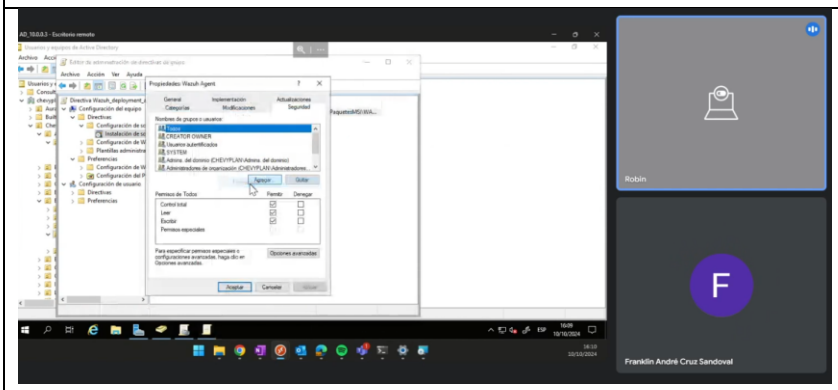
Wazuh. (2024). *The Open Source Security Platform.* Obtenido de https://www.wazuh.com

Williams, B. K., & Sawyer, S. C. (2023). *Using Information Technology: A Practical Introduction to Computers & Communications.* Hill Education.

8. Anexos

	Firma de la autorización de proyecto por el Ing. Marco Guerrero el cual desempeña el cargo de jefe de Tecnologías de la información en la empresa Plan Automotor Ecuatoriano S.A
PLAN AUTOMOTOR ECUATORIANO S.A AV DE LAS AMERICAS EDIFICIO MECANOS PISO 6 Guayaquil, 23 de Mayo de 2024 Estimado Franklin Cruz: Es un placer para nosotros en Plan Automotor Ecuatoriano S.A comprometernos a apoyar su proyecto integrador curricular titulado "Implementación y gestión de una plataforma de seguridad integral para la infraestructura ChevyPlan", que se lleva a cabo como parte de sus estudios en el área de Sistemas Inteligentes de la Universidad Ecotec. Conscientes de la complejidad que implica comprender las necesidades y requerimientos específicos para el desarrollo de soluciones tecnológicas eficaces, nuestro compromiso se centrará en: • Explicación de necesidades y requerimientos: Ofreceremos nuestra experiencia para detallar y clarificar las necesidades y requerimientos específicos que su proyecto pretende abordar, asegurando una comprensión profunda de los problemas a solucionar. • Análisis de procesos a sistematizar: Nuestro equipo brindará una visión clara sobre los procesos actuales que podrían beneficiarse de la sistematización, ayudándole a identificar las oportunidades de mejora y optimización mediante soluciones de TI. • Planificación de servicios o soluciones de TI: Asistiremos en la planificación estratégica para el desarrollo de servicios o soluciones tecnológicas que respondan eficientemente a los requerimientos identificados. • Evaluación de metodologías: Evaluar las metodologías empleadas en el desarrollo del proyecto para asegurar que son apropiadas y efectivas en el contexto de los objetivos planteados. • Pruebas y validación de resultados: Probar y validar los resultados del proyecto, incluyendo productos o servicios desarrollados, para asegurar que cumplen con los estándares de calidad y funcionalidad esperados. • Provisión de datos anonimizados: En caso de ser relevante para análisis de datos, proporcionaremos acceso a conjuntos de datos anonimizados, asegurándonos de cumplir con todas las leyes y regulaciones vigentes sobre protección de datos. Entendemos que este tipo de orientación es crucial para el éxito de proyectos que buscan implementar soluciones tecnológicas innovadoras y efectivas. Para discutir cómo podemos comenzar a colaborar o para cualquier detalle específico, por favor no dude en ponerse en contacto con Carolina Pérez en carolina.perez@chevyplan.com.ec o Kesli Preciado en kesli.preciado@chevyplan.com.ec. Agradecemos la oportunidad de ser parte de su trayectoria educativa y profesional, y quedamos a la espera de contribuir significativamente a su proyecto. Cordialmente, Marco Guerrero Jefe de Tecnologías de la Información 23 MAY 2024 Marco G ChevyPlan Jefe de marco.guerrero@chevyplan.com.ec	Autorización Firmada por el jefe de Tecnologías de la información Ing. Marco Guerrero

	Primera Reunión – 16 de Julio 2024 Reunión con Kesli Preciado – Líder de infraestructura y seguridad Tema por tratar: Beneficios de implementar una plataforma de seguridad integral
	Segunda reunión – 23 Julio 2024 Reunión con Kesli Preciado – Líder de infraestructura y seguridad Temas por tratar: Términos y condiciones para poder hacer la implementación
	Tercera reunión – 25 Julio 2024 Robinson Torres – Analista IT Tema por tratar: Instalación de Wazuh en el servidor

	Cuarta reunión – 19 Agosto 2024 Robinson Torres – Analista IT y Kesli Preciado – Líder de infraestructura y seguridad Tema por tratar: Instalación del agente de wazuh por medios de políticas GPO
	Quinta reunión – 18 Septiembre 2024 Robinson Torres – Analista IT y Kesli Preciado – Líder de infraestructura y seguridad Tema por tratar: Solucionar errores encontrados al implementar los agentes por políticas GPO
	Sexta reunión 10 Octubre 2024 Robinson Torres – Analista IT Tema por tratar: Revisión de todos los agentes de Wazuh que han sido implementados recientemente para luego hacer pruebas