CENTRO DE POSGRADOS

Tema:

GESTIÓN DE EVENTOS CON TECNOLOGÍA XDR PARA ASEGURAR LA INFRAESTRUCTURA DE COMUNICACIÓN DEL GAD COLTA

Proyecto de investigación previo a la obtención del título de Magíster en Ciberseguridad

Línea de investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

Patricio Fabián Ashqui Cuvi

Director:

Mg. Alberto Leopoldo Arellano Aucancela

Ambato – Ecuador

Septiembre 2024

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **PATRICIO FABIÁN ASHQUI CUVI**, con cédula de ciudadanía **1500621485**, autor del trabajo de graduación intitulado: “GESTIÓN DE EVENTOS CON TECNOLOGÍA XDR PARA ASEGURAR LA INFRAESTRUCTURA DE COMUNICACIÓN DEL GAD COLTA”, previa a la obtención del título profesional de **MAGÍSTER EN CIBERSEGURIDAD**, en el centro de **POSGRADOS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, septiembre 2024

Firmado electrónicamente por:
PATRICIO FABIAN ASHQUI CUVI

Patricio Fabian Ashqui Cuvi

CC. 1500621485

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

GESTIÓN DE EVENTOS CON TECNOLOGÍA XDR PARA ASEGURAR LA INFRAESTRUCTURA DE COMUNICACIÓN DEL GAD COLTA

Línea de investigación:

SEGURIDAD DE LA INFORMACIÓN

Autor:

Patricio Fabián Ashqui Cuvi

Alberto Leopoldo Arellano Aucancela, Ing. Mg. f._____

Firmado electrónicamente por: ALBERTO LEOPOLDO ARELLANO AUCANCELA

CC. 0602523383

CALIFICADOR

David Omar Guevara Aulestia, Ing. Mg. f._____

Firmado electrónicamente por: DAVID OMAR GUEVARA AULESTIA

CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. f._____

Firmado electrónicamente por: JOSE MARCELO BALSECA MANZANO

CALIFICADOR

Teresa Milena Freire Aillón, Ing. Mg. f._____

TERESA MILENA FREIRE AILLON

Firmado digitalmente por TERESA MILENA FREIRE AILLON
Fecha: 2024.10.04 16:39:36 -05'00'

DIRECTORA CENTRO DE POSGRADOS

Diego Gonzalo Coca Chanalata, Dr. f._____

DIEGO GONZALO COCA CHANALATA

Firmado digitalmente por DIEGO GONZALO COCA CHANALATA
Fecha: 2024.10.04 14:48:14 -05'00'

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Septiembre 2024

DEDICATORIA

El presente proyecto de investigación y desarrollo está dedicado a:

A Dios Padre Todopoderoso, por haberme dado Fuerza de voluntad y vida para poder concluirlo.

A mi padre, por toda la sabiduría que me entrego, a mi madre, en muestra de amor y gratitud que tengo a ella, y en reciprocidad a su esfuerzo que hace por todos sus hijos, para que cada día sean mejores.

A mis hermanos, por su confianza, amistad, paciencia, comprensión y apoyo que me dan en todo momento.

A mis hijos Kelyta, Dany y Martin quienes son la razón de mí vivir, quien con su amor y comprensión en cada momento me ha dado inspiración para la culminación de este trabajo.

A todos los docentes quienes con su amplia experiencia supieron impartir sus conocimientos y me orientaron al correcto desenvolvimiento académico, personal y profesional y a través de ellos a la Pontificia Universidad Católica del Ecuador sede Ambato, autoridades, personal administrativo y docentes.

Muchas gracias a todos.

AGRADECIMIENTO

Agradezco a mi DIOS todo poderoso por darme la oportunidad de vivir esta vida maravillosa llena de bendiciones y permitirme llegar a este día.

A mi padre, el mejor, tú eres parte importante de mi esfuerzo porque me enseñaste a luchar para conseguir mis propósitos con mucha valentía, como no podía faltar a mi madre, la mejor amiga, la mejor madre eres una de las causas principales por las que yo soy mejor cada día, gracias por todo tu amor, por tus esfuerzos, por tu apoyo incondicional.

A todos mis hermanos por su invaluable apoyo comprensión y cariño que me dieron en los momentos más importantes de mi vida.

A las autoridades y funcionarios del Gobierno Autónomo Descentralizado Municipal del Cantón Colta, gracias por darme la apertura y proporcionarme los recursos y herramientas que fueron necesarios para llevar a cabo el proceso de investigación.

A mi tutor, el Magister. Alberto Arellano, por compartir su experiencia, su tiempo y sus conocimientos aportados al presente trabajo.

Patricio Fabián Ashqui Cuvi
Maestrante

RESUMEN

Uno de los requerimientos de mayor importancia en toda organización pública o privada, es poder contar con información respecto de potenciales acciones maliciosas que afecta a los sitios webs y sistemas de información institucionales, y no necesariamente relacionados únicamente al ámbito web, sino que también a otros componentes críticos como lo son los servidores de DNS, los servidores de correo institucional, las bases de datos eventualmente expuestas a Internet, los puertos de acceso para administración o transferencia segura de archivos entre otros.

En este contexto es fundamental que todos los dispositivos finales de usuario, así como los dispositivos de red y aplicativos registren de manera segura las actividades propias de su operación y seguridad. En estos registros debieran estar las señales que anuncien alguna actividad maliciosa o sospechosa, y que interpretadas de manera oportuna por las personas correctas podrían permitir responder ante este incidente lo más rápido posible, minimizando así su impacto.

El presente trabajo de investigación tiene como objetivo principal implementar una herramienta SIEM (sistema de Gestión de Eventos e Información de Seguridad) con tecnología XDR basada en plataforma open source para la detección temprana de amenazas y vulnerabilidades.

El desarrollo de esta investigación está basado en la metodología MAGERIT, misma que se enfoca en la evaluación de las principales características de la plataforma de seguridad opensource WAZUH, que integra protección XDR y SIEM unificada para endpoints, dichas características serán evaluadas en la infraestructura tecnológica del GAD del cantón Colta de la provincia de Chimborazo.

Palabras clave: siem, xdr, gestión de eventos, ataques, detección, respuestas.

ABSTRACT

One of the most important requirements in any public or private organization is to have information regarding potential malicious actions that may be affecting institutional websites and information systems, and not necessarily related only to the web environment, but also to other critical components such as DNS servers, institutional mail servers, databases eventually exposed to the Internet, access ports for administration or secure file transfer, among others.

In this context, it is essential that all end-user devices as well as network and application devices securely record their operation and security activities. These logs should contain the signals that announce any malicious or suspicious activity, which, if interpreted in a timely manner by the right people, could allow responding to such an incident as quickly as possible, thus minimizing its impact.

The main objective of this research is to implement a SIEM tool (Security Information and Event Management System) with XDR technology based on an open source platform for early detection of threats and vulnerabilities.

The development of this research is based on the MAGERIT methodology, which focuses on the evaluation of the main features of the open source security platform WAZUH, which integrates XDR protection and unified SIEM for endpoints, these features will be evaluated in the technological infrastructure of the GAD of the canton Colta in the province of Chimborazo.

***Keywords**: siem, xdr, event management, attacks, detection, responses.*

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

La ciberseguridad es un campo en constante evolución que se enfoca en proteger los sistemas informáticos, las redes y los datos de ataques, daños o accesos no autorizados. Con el crecimiento exponencial de las amenazas cibernéticas, la ciberseguridad se ha vuelto crucial para individuos, empresas y gobiernos. Según (Steinberg, 2022) la ciberseguridad abarca una amplia gama de tecnologías, procesos y prácticas diseñadas para proteger los sistemas y datos.

En la práctica, las violaciones de datos y los ciberataques han tenido un impacto significativo en organizaciones y gobiernos a nivel internacional. Por ejemplo, el ataque cibernético a Equifax en 2017 comprometió la información personal de millones de personas, lo que resultó en consecuencias legales y financieras significativas para la empresa (Thenault, 2017)

Según, (CEPAL, 2020), La información es considerado como uno de los activos más importantes para todas las entidades públicas o privadas sin importar su área de incidencia o tamaño. Entre estos están considerado los datos personales, información de propiedad intelectual, datos sensibles, estadísticas del mercado, etc. A su vez estos son recopilados, normalizados, procesados, transmitidos y almacenados en medios tecnológicos. Por lo que es fundamental implementar medidas para proteger la información y con esto evitar ataques y delitos informáticos que puedan afectar el normal funcionamiento y entrega de servicios por parte de las instituciones.

En el contexto internacional, (Dirección Nacional de Ciberseguridad de Israel, 2022) existen diversas recomendaciones y mejores prácticas que ayudar a reducir los riesgos cibernéticos. Algunas de estas prácticas incluyen asignar un rol dedicado a las amenazas internas, instalar un firewall, un software antimalware, crear una política clara sobre gestión de contraseñas, realizar copias de seguridad de datos, estas soluciones son efectivos para prevenir ataques informáticos. Dado que, actualmente se presentan varios desafíos como: 1) Múltiples interfaces de administración. 2) registros de eventos generados por las soluciones de

seguridad, sistemas operativos y aplicaciones. 3) Visibilidad limitada del ciclo del ataque, 4) Falta de profesional capacitado en la gestión de ciberseguridad.

El uso de múltiples vectores de ataque dificulta su monitoreo, identificación y respuesta oportunas, amenazas que no son detectadas oportunamente por las soluciones tradicionales de seguridad.

El auge del internet ha provocado un crecimiento exponencial en la cantidad de información que se transmite actualmente, lo que ha llevado a que las infraestructuras se vuelvan cada vez más complejas e integren una mayor cantidad de herramientas tecnológicas. Esto ha dificulta la gestión y protección de la infraestructura tecnológica, lo que a su vez aumenta el riesgo de amenazas cibernéticas. Para abordar estos desafíos, según Polanco (2018) las plataformas SIEM (*Security Information and Event Management*) son herramientas amigables que permiten la recopilación, correlación y análisis de información de seguridad de diferentes fuentes en tiempo real, con el objetivo de detectar y responder a amenazas de seguridad de manera eficiente.

XDR (*Extended Detection and Response*) es una solución de seguridad que combina la detección y respuesta de amenazas en diferentes fuentes de datos, como *endpoints*, redes y nubes. XDR utiliza la correlación de datos para identificar patrones de comportamiento y detectar amenazas avanzadas. (Valcárcel, 2023)

Si bien es cierto la plataforma SIEM ha sido una herramienta fundamental para la gestión de la seguridad de la información, la tecnología XDR ha surgido como una solución más específica y holística que permite la detección y respuesta más eficientes y automáticas frente a las amenazas cibernéticas.

La presente investigación, se centra en analizar la siguiente problemática: En la infraestructura de comunicaciones del GAD COLTA existe posibles amenazas que afectan la seguridad de la información, como son ataques de acceso a la red ya sea interna o externamente (internet), esto generar vulnerabilidades y filtrado de la información.

El riesgo de no aplicar un monitoreo de seguridad en la infraestructura de comunicaciones ocasionara que los usuarios no autorizados accedan a la información de la infraestructura de comunicación, causando fallas de seguridad que afectan el correcto funcionamiento de los servicios y posibles fugas de información, que conllevaría a la paralización de los servicios dentro de la institución.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

En el presente capítulo, se analizan los principales conceptos que ayudan a comprender el procedimiento y fases que involucran la gestión y monitoreo de seguridad, así como las ventajas de utilizar la tecnología XDR para asegurar la infraestructura de comunicación del GAD COLTA.

ESTADO DEL ARTE

Para Kaspersky (2023) la protección de las infraestructuras tecnológicas corporativas contra los ataques cibernéticos requiere cada vez más recursos, tanto en términos de plataformas de seguridad como de personal especializado. Esto sucede por cuanto la superficie de ataque se ha ampliado exponencialmente, lo que ha generado un aumento del riesgo digital. Por lo tanto, es fundamental saber cómo gestionar las ciberamenazas de forma integral.

- Los actores maliciosos dedican tiempo a investigar a sus posibles víctimas. Esto les permite saber a quién atacar, qué procedimiento usar y el mejor momento para actuar. Esta etapa de reconocimiento y planificación hace que los ataques sean más difíciles de detectar, más sofisticados y, por lo tanto, más efectivos.

- Los atacantes trabajan en equipo para aprovechar sus diferentes habilidades. Algunos se especializan en identificar vulnerabilidades, mientras que otros se centran en la exfiltración de información sensible.

- Los ciberataques se aprovechan del eslabón más débil de la cadena de seguridad: el usuario final. Los atacantes utilizan una variedad de métodos para engañar o manipular a los usuarios para que hagan clic en un enlace malicioso, abran un archivo adjunto infectado o proporcionen sus credenciales. Una vez que un usuario ha sido comprometido, el atacante estaría accediendo a la red de la organización.

- Los atacantes utilizan herramientas propias del sistema operativo para ejecutar procesos maliciosos. Estas actividades son difíciles de detectar por herramientas tradicionales de seguridad, utilizan las mismas funciones que los procesos legítimos.

Para monitorear de manera eficiente a los ataques cibernéticos, se han desarrollado múltiples plataformas de gestión y administración de eventos de seguridad (SIEM). Plataformas que permiten a las organizaciones tomar medidas proactivas y unificadas para detectar, investigar y responder a los incidentes de seguridad. (Gómez, 2023)

En la actualidad los sistemas SIEM, han evolucionado hasta llegar a ser más que una herramienta de análisis en tiempo real sobre las amenazas y las alertas de seguridad en el negocio. Controla el almacenamiento, la manipulación, el análisis y la generación de informes de diferentes datos de seguridad, nos permitirá correlacionar diferentes eventos y alertas, llevando así la seguridad de la organización a otro nivel. (Ramiro, 2021)

1.1. Centro de operaciones de seguridad (SOC)

Según Kanade (2023) un SOC es una unidad especializada dentro de una organización responsable de supervisar, detectar, analizar y responder a incidentes y amenazas de seguridad.

En el panorama actual de las amenazas cibernéticas, las organizaciones se enfrentan a muchos riesgos, como las filtraciones de datos, los ataques de *ransomware*, las amenazas internas y los sofisticados ataques a los estados-nación. En septiembre de 2022, Statista publicó un informe en el que destacaba el impacto financiero de las filtraciones de datos en Estados Unidos y en todo el mundo. Según el informe, el coste medio de una filtración de datos en Estados Unidos aumentó a 9,44 millones de dólares desde los 9,05 millones del año anterior. Además, el informe reveló que el coste medio mundial por violación de datos en 2022 fue de 4,35 millones de dólares. Este aumento de los costes refleja

los crecientes retos a los que se enfrentan las organizaciones a la hora de salvaguardar la información sensible. (Kanade, 2023)

Funcionalidades de los centros de operaciones de seguridad (SOC)

Según Kanade (2023) los Centros de Operaciones de Seguridad poseen las siguientes funcionalidades:

- **Monitoreo continuo y detección de amenazas**, esto implica examinar varias fuentes de datos, incluido el tráfico de red, los registros del sistema, los dispositivos de seguridad y el comportamiento del usuario, en tiempo real.

- **Respuesta y contención de incidentes**, es un proceso bien definido destinado a contener y mitigar rápidamente el impacto de la amenaza.

- **Integración de inteligencia de amenazas**, incorpora activamente la inteligencia de amenazas en sus operaciones. Esto implica recopilar datos sobre amenazas cibernéticas emergentes, técnicas de ataque y vulnerabilidades de diversas fuentes.

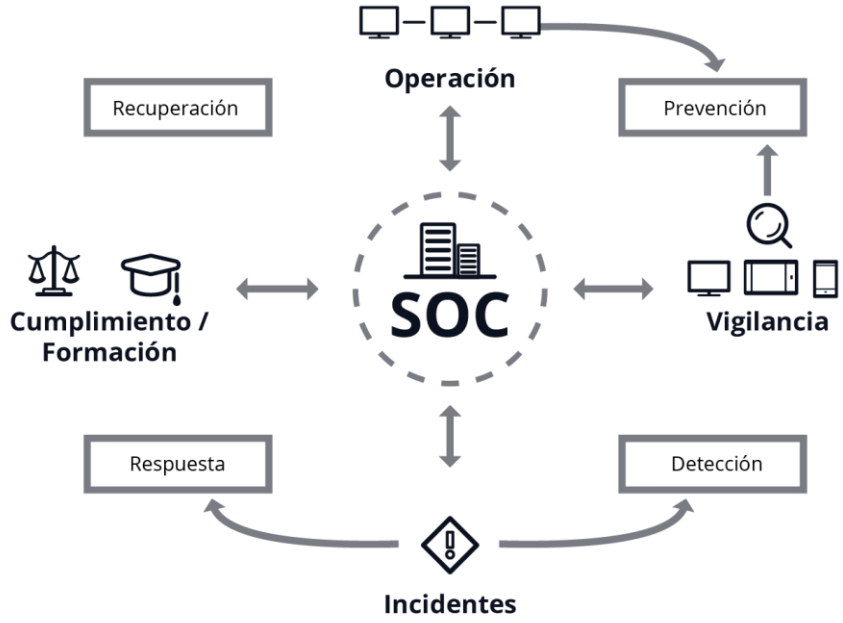
- **Gestión de vulnerabilidades**, realizan evaluaciones periódicas de vulnerabilidades para identificar las debilidades y los posibles puntos de entrada para los ciberatacantes. Trabajan con los equipos de TI para priorizar y remediar estas vulnerabilidades con prontitud.

- **Análisis forense y notificación de incidentes**. Después de resolver los incidentes de seguridad, los equipos de SOC realizan un análisis forense en profundidad. Esta investigación ayuda a determinar la causa raíz del incidente, el alcance del compromiso y cualquier posible violación de datos. Se generan informes detallados de incidentes, que documentan el cronograma, el impacto y las lecciones aprendidas del incidente.

- **Mejoras de seguridad proactivas**. Los SOC no solo responden a incidentes; También desempeñan un papel crucial en las mejoras proactivas de la seguridad. Mediante el análisis de datos históricos, la identificación de tendencias y la realización de evaluaciones de riesgos, los equipos de SOC realizan recomendaciones de mejoras de seguridad y cambios en las políticas para proteger de mejor manera los activos de la organización.

La ilustración 1, muestra una visión sobre el funcionamiento de un centro de operaciones de seguridad (SOC).

Ilustración 1. Eje y funciones de un SOC



Fuente**:** tomada a partir de centro criptológico nacional (s.f)

Los Centros de Operaciones de Seguridad (SOC) desempeñan un papel crucial en la protección de las organizaciones contra amenazas cibernéticas y en la supervisión y respuesta a incidentes de ciberseguridad. Estas funcionalidades permiten a las empresas garantizar la **disponibilidad**, **confiabilidad** e **integridad** de sus sistemas y datos, cumplir con las normativas y regulaciones aplicables y mejorar la confianza de sus clientes.

1.2. Gestión de eventos e información de seguridad (SIEM)

Según Lorenzo (2021) SIEM es una tecnología capaz de detectar rápidamente, responder y neutralizar las amenazas informáticas. Su objetivo principal es el de proporcionar una visión global de la seguridad de la tecnología de la información.

Según el informe realizado por Insiders (2022), el 85% de las organizaciones que tienen un SIEM como parte de su estrategia de seguridad se encuentran satisfechos con su efectividad, menciona que esta satisfacción se centra en tres elementos.

- Detección y respuesta de incidentes más rápida.
- Mayor eficiencia en las operaciones de seguridad.
- Mejora de la visibilidad de amenazas.

De la misma forma, el informe indica que el 78% de las organizaciones pudieron detectar eventos de seguridad en pocas horas y el 50% en varios minutos, mostrando así, la importancia de utilizar este tipo de plataformas.

En cuanto a la efectividad en la detección de ataques, el informe muestra que con la utilización de herramientas SIEM, se logró detectar el 66% de accesos no autorizados, el 61% de malware (virus, gusanos y troyanos) y el 52% de ataques a aplicaciones web.

Arquitectura de un SIEM

Los pilares esenciales de un sólido sistema de gestión de eventos e información de seguridad (SIEM), abarcan una diversidad tan amplia como la gama de datos que procesa. Desde los elementos centrales encargados de recopilar y analizar información hasta las capacidades avanzadas que optimizan la detección y respuesta ante amenazas, comprender las características cruciales de un SIEM resulta fundamental para tomar decisiones informadas al seleccionar medidas de seguridad y proteger la organización contra riesgos en ciberseguridad. En este

contexto en general un sistema SIEM está conformado por los siguientes componentes:

1. Gestión de Registros (*Log Management*):

- Recopila, almacena y gestiona registros o logs de eventos generados por sistemas, aplicaciones y dispositivos en toda la red.

- Proporciona una visión completa de las actividades y eventos en la infraestructura, permitiendo la identificación de patrones, anomalías y actividades sospechosas.

2. Inteligencia y Detección de Amenazas (*Threat Intelligence and Detection*):

- Utiliza bases de datos de inteligencia de amenazas para correlacionar eventos y detectar patrones asociados a amenazas conocidas.

- Mejora la capacidad de identificar y responder a amenazas al integrar información actualizada sobre tácticas, técnicas y procedimientos utilizados por actores maliciosos.

3. Notificaciones y Alertas (*Alerting and Notifications*):

- Genera alertas y notificaciones en tiempo real ante eventos de seguridad significativos o incidentes que requieren atención inmediata.

- Facilita una respuesta rápida al proporcionar alertas inmediatas, permitiendo a los analistas abordar las amenazas de manera oportuna.

4. Identificación Inteligente de Incidentes (*Incident Identification*):

- Utiliza técnicas de correlación avanzadas para identificar incidentes de seguridad y agrupar eventos relacionados, permitiendo una comprensión más completa de las amenazas.

- Ayuda a los analistas a priorizar y enfocarse en incidentes relevantes, reduciendo el ruido y mejorando la eficiencia de la respuesta.

5. Análisis Forense (*Forensic Analysis*):

- Permite investigar a fondo incidentes de seguridad, analizando datos recopilados para determinar el alcance y la naturaleza de la brecha.

- Facilita la comprensión de cómo ocurrió un incidente, qué sistemas se vieron afectados y qué acciones se llevaron a cabo, lo que es crucial para la mejora continua de la postura de seguridad.

6. Informes, Auditorías y Paneles (*Reports, Audits, and Dashboards*):

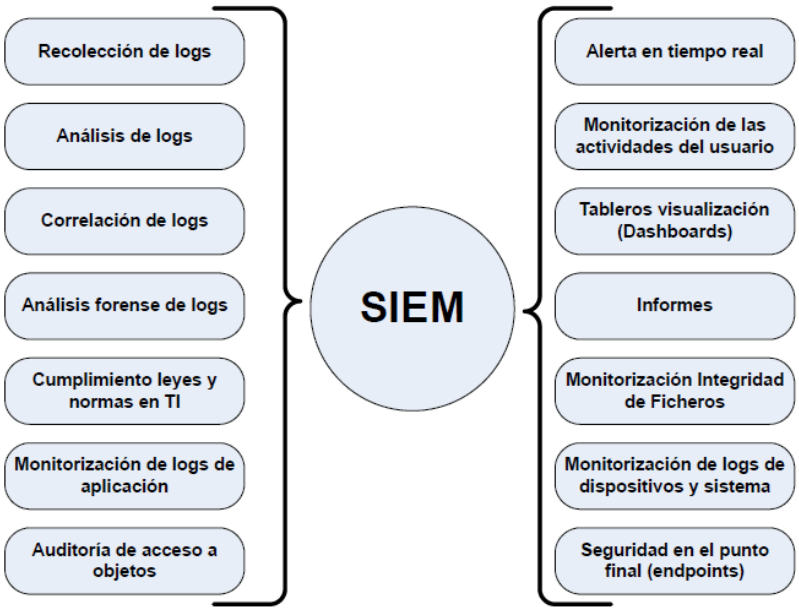
- Genera informes detallados, realiza auditorías de seguridad y proporciona paneles visuales para resumir la actividad de seguridad y el cumplimiento normativo.

- Facilita la comunicación de la postura de seguridad a partes interesadas internas y externas, respalda la conformidad con regulaciones y proporciona una visión clara de los aspectos clave de la seguridad de la información.

Estos componentes trabajan de manera conjunta para ofrecer una solución completa de gestión de eventos e información de seguridad, permitiendo a las organizaciones detectar, analizar y responder eficazmente a amenazas cibernéticas.

La ilustración 2, muestra una visión general sobre la arquitectura (SIEM).

Ilustración 2. Arquitectura de un sistema SIEM



Fuente: modificado a partir de SECURE-OPS (2020)

1.3. Detección y respuesta del punto final (EDR)

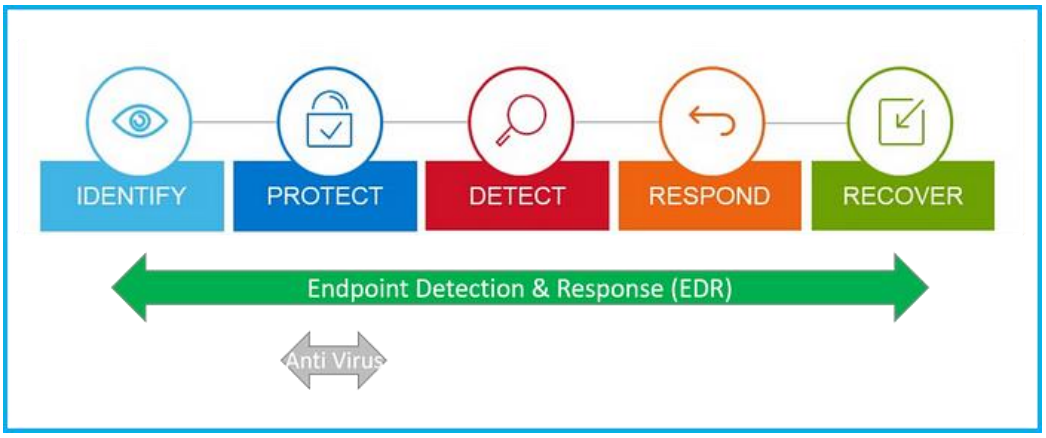
Según González (2023) un sistema EDR es una herramienta de protección y monitorización diseñada para salvaguardar la red, los dispositivos y la infraestructura tecnológica de una organización. El término EDR proviene del inglés "*Endpoint Detection Response*" (detección y respuesta de punto final).

Los sistemas EDR no son software antivirus, aunque estarían en las capacidades de antivirus. El software antivirus se centra en la protección contra amenazas conocidas, mientras que los sistemas EDR detectan amenazas nuevas como *exploits* y amenazas desconocidas en tiempo real. Esta capacidad para detectar amenazas en tiempo real hace que los sistemas EDR sean una parte importante de la última generación de productos de ciberseguridad.

En la siguiente ilustración 2 según Solo (2021) se evidencia que EDR tiene más funciones que un antivirus, que incluye capacidades como la identificación, la

protección, la detección, la respuesta, etc., mientras que un antivirus solo proporciona una función de recuperación.

Ilustración 3. Comparación Antivirus y EDR



Fuente: tomado a partir de Solo (2021)

Funcionalidades de un (EDR)

- **Identificación**: Cuando un programa se está ejecutando, conoceríamos su malicia y reputación. Por lo tanto, antes de implementar actividades en los puntos finales, EDR identificaría si esas actividades son maliciosas o no, para luego ejecutar de forma segura en un espacio separado.

- **Protección**: Esto implica bloquear los programas que se consideran maliciosos o mover los archivos a un lugar seguro para mantenerlos en cuarentena.

- **Detección**: Supervisión de las actividades y el comportamiento en los puntos de conexión para detectar malware.

- **Respuesta**: Responder al comportamiento detectado, como bloquear la actividad para evitar daños en áreas específicas del sistema que, de otro modo, provocarían un error en el arranque de la computadora, y hacer una copia de seguridad instantánea de imágenes, videos, documentos, etc. que están a punto de ser cifrados por *ransomware* en un área protegida.

- **Recuperación**: Recuperación de archivos que de otro modo no podrían abrirse debido al cifrado por *malware* mediante el uso de los archivos respaldados durante la etapa de respuesta.

1.4. Detección y respuesta extendida (XDR)

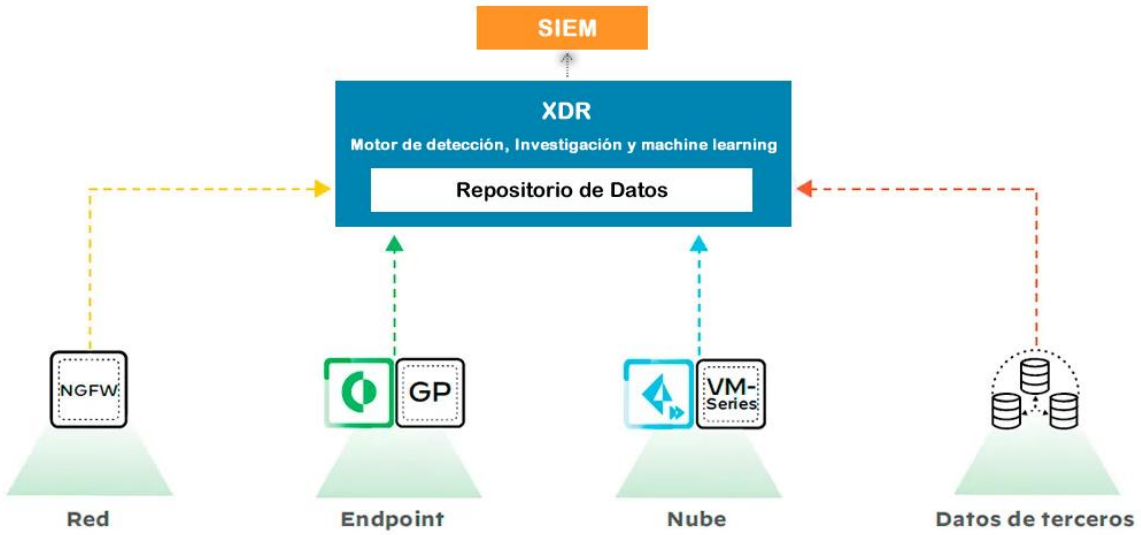
Según Ballejos (2023) un sistema de Detección y Respuesta Extendida o XDR ("*Extended Detection and Response*" en inglés), es un conjunto integrado de productos de seguridad que unifica el control y la visibilidad en todos los vectores de amenazas, incluidas redes, correos electrónicos, servidores, cargas de trabajo en la nube y usuarios finales. La XDR aprovecha la inteligencia artificial y la automatización para detectar, investigar y responder a las amenazas en toda una infraestructura de TI.

La detección y respuesta extendidas recopila y correlaciona automáticamente datos de múltiples capas de seguridad (*endpoint*, red y nube) para identificar actividades sospechosas. Gracias al aprendizaje automático y al análisis del comportamiento, la detección y respuesta extendidas, estarán en la capacidad de detectar amenazas potenciales y eliminarlas antes de que causen daños.

Arquitectura de un XDR

La ilustración 4, muestra los principales componentes de la arquitectura general de un sistema de detección y respuesta extendida.

Ilustración 4. Arquitectura de un XDR



Fuente: modificado a partir de (S3CURETASUN, 2022)

Funcionalidades de un (XDR)

Según (Ballejos (2023), las principales funcionalidades que posee las soluciones de XDR son:

1. **Detección y respuesta mejoradas**: el enfoque unificado de la XDR permite una detección y respuesta más rápidas a las amenazas mediante la correlación de datos procedentes de diversas fuentes.
2. **Mayor eficiencia**: al automatizar las tareas rutinarias, la XDR permite a que tu equipo de seguridad disponga de más tiempo para centrarse en problemas más complejos.

3. **Pila de seguridad simplificada**: la XDR integra varias soluciones de seguridad en una sola plataforma, lo que reduce la complejidad y mejora la capacidad de gestión.

4. **Mejor visibilidad**: la XDR proporciona una visión holística de tu entorno de TI, así comprender todo el alcance y el impacto de los incidentes de seguridad.

Wazuh

Según (Delgado, 2023), Wazuh es una plataforma SIEM diseñada para recopilar, analizar y correlacionar eventos de seguridad en tiempo real. Su arquitectura flexible y extensible lo convierte en una herramienta altamente efectiva tanto para pequeñas empresas como para grandes organizaciones, además ofrece capacidades unificadas XDR y SIEM. Proporciona una vista centralizada para supervisar, detectar y alertar sobre eventos e incidentes de seguridad en puntos finales supervisados, cargas de trabajo en la nube, contenedores y servidores.

Componentes

De acuerdo a (Wazuh, 2023), la plataforma se basa en el agente Wazuh, que se implementa en los puntos finales monitoreados, y en tres componentes centrales: el servidor Wazuh, el indexador Wazuh y el panel de control Wazuh.

Indexador Wazuh: El indexador Wazuh es un motor de búsqueda y análisis de texto completo altamente escalable. Este componente central de Wazuh indexa y almacena las alertas generadas por el servidor de Wazuh y proporciona capacidades de búsqueda y análisis de datos casi en tiempo real. El indexador Wazuh se configurar como un clúster de un solo nodo o multinodo, proporcionando escalabilidad y alta disponibilidad.

El indexador de Wazuh almacena datos como documentos JSON. Cada documento correlaciona un conjunto de claves, nombres de campo o propiedades, con sus valores correspondientes que consiguen ser cadenas, números, booleanos, fechas, matrices de valores, geolocalizaciones u otros tipos de datos.

Wazuh utiliza cuatro índices diferentes para almacenar los tipos de eventos, la tabla 1 detalla estos índices.

Tabla 1. Índices de Wazuh

Índice	Descripción
wazuh-alertas	Almacena alertas generadas por el Servidor wazuh. Estos se crean cada vez que un evento dispara una regla con una prioridad lo suficientemente alta (este umbral es configurable).
wazuh-archivos	Almacena todos los eventos (datos de archivo) recibidos por el Servidor wazuh, si disparan o no una regla.
wazuh-monitoreo	Almacena datos relacionados con el estado del Agente wazuh a lo largo del tiempo. Es utilizado por la interfaz web para representar cuando los agentes individuales son o han sido Activos, Desconectados, o nunca conectado.
wazuh-estadísticas	Almacena datos relacionados con el Servidor wazuh rendimiento. Es utilizado por la interfaz web para representar las estadísticas de rendimiento.

Fuente: tomado a partir de (Wazuh, 2023)

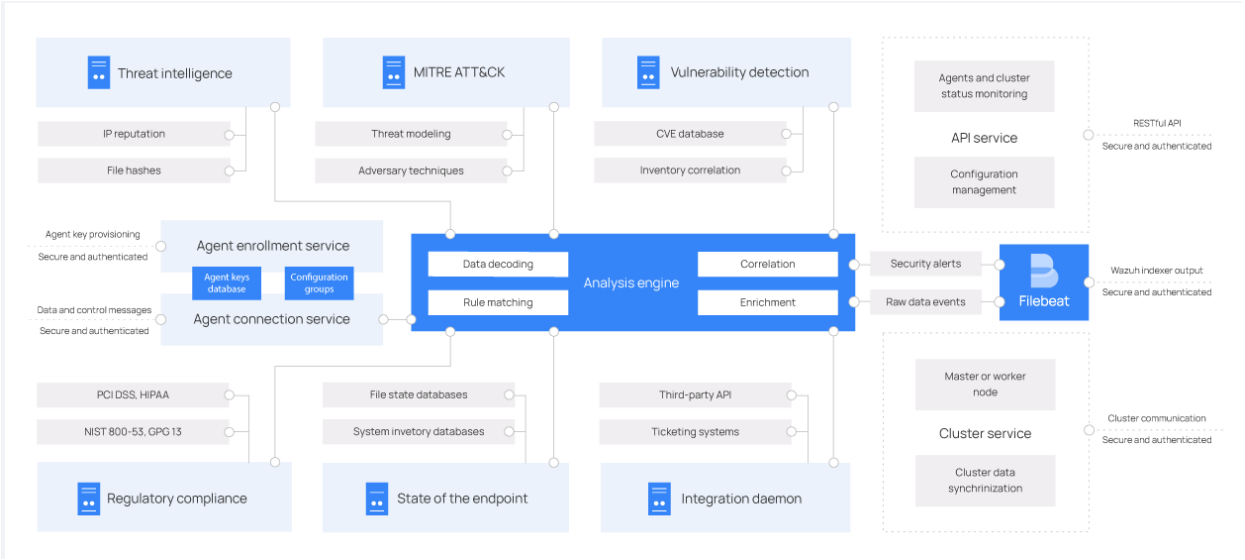
- **Servidor Wazuh:** El servidor Wazuh analiza los datos recibidos de los agentes, activa alertas cuando se detectan amenazas o anomalías. También se utiliza para administrar la configuración de los agentes de forma remota y monitorear su estado.

  El servidor Wazuh utiliza fuentes de inteligencia de amenazas para mejorar sus capacidades de detección. También enriquece los datos de las alertas utilizando el *framework* MITRE ATT&CK y los requisitos de cumplimiento normativo como PCI DSS, GDPR, HIPAA, CIS y NIST 800-53, proporcionando un contexto útil para el análisis de seguridad.

  El servidor de Wazuh ejecuta el motor de análisis, la API RESTful de Wazuh, el servicio de inscripción de agentes, el servicio de conexión de agentes, el demonio de clúster de Wazuh y Filebeat. El servidor se instala en un sistema operativo Linux y por lo general se ejecuta en una máquina física independiente, máquina virtual, contenedor *docker*, o instancia en la nube.

  La siguiente ilustración 5 representa la arquitectura del servidor y sus componentes:

Ilustración 5. Arquitectura del Servidor Wazuh



Fuente: tomado a partir de (Wazuh, 2023)

La tabla 2, detalla los principales componentes de la arquitectura de un servidor wazuh.

Tabla 2. Componentes de Wazuh

COMPONENTE	DESCRIPCIÓN
Servicio de inscripción de agentes	Se utiliza para inscribir nuevos agentes. Este servicio proporciona y distribuye claves de autenticación únicas a cada agente. El proceso se ejecuta como un servicio de red y admite la autenticación mediante certificados TLS/SSL o proporcionando una contraseña fija.
Servicio de conexión de agentes	Este servicio recibe datos de los agentes. Utiliza las claves compartidas por el servicio de inscripción para validar la identidad de cada agente y encriptar las comunicaciones entre el agente Wazuh y el servidor Wazuh. Además, este servicio proporciona una gestión centralizada de la configuración, lo que le permite empujar nuevos ajustes del agente de forma remota.
Motor de análisis	Es el componente del servidor que realiza el análisis de los datos. Utiliza decodificadores para identificar el tipo de información que se está procesando (eventos de Windows, registros SSH, registros del servidor web y otros). Estos decodificadores también extraen elementos de datos relevantes de los mensajes de registro, como la dirección IP de origen, el ID del evento o el nombre de usuario. A continuación, mediante el uso de reglas, el motor identifica patrones específicos en los eventos decodificados que podrían activar alertas y, posiblemente, incluso solicitar contramedidas automatizadas (por ejemplo, prohibir una dirección IP, detener un proceso en ejecución o eliminar un malware).
API RESTful de Wazuh	Este servicio proporciona una interfaz para interactuar con la infraestructura Wazuh. Se utiliza para gestionar los ajustes de configuración de agentes y servidores, monitorizar el estado de la infraestructura y la salud general, gestionar y editar decodificadores y reglas Wazuh, y consultar sobre el estado de los puntos finales monitorizados. El panel de control Wazuh también lo utiliza.
Demonio de cluster Wazuh	Este servicio se utiliza para escalar servidores Wazuh horizontalmente como un clúster. Este tipo de configuración, combinada con un

	balanceador de carga de red, proporciona alta disponibilidad y balanceo de carga. El demonio del cluster Wazuh es lo que los servidores Wazuh usan para comunicarse entre ellos y mantenerse sincronizados.
Filebeat	Se utiliza para enviar eventos y alertas al indexador Wazuh. Lee la salida del motor de análisis de Wazuh y envía eventos en tiempo real. También provee balanceo de carga cuando se conecta a un cluster de indexadores Wazuh de múltiples nodos.

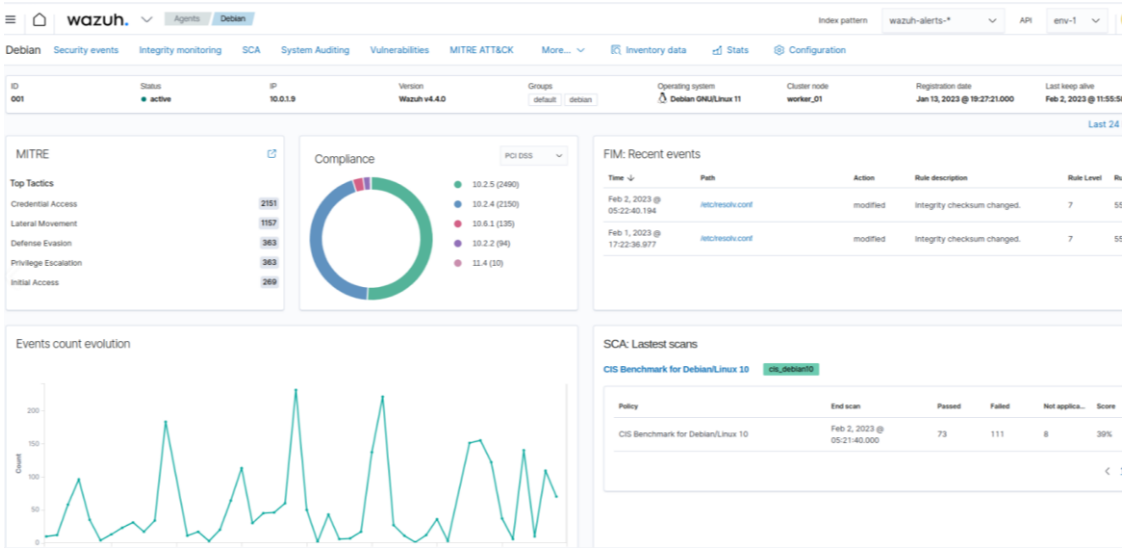
Fuente: tomado a partir de (Wazuh, 2023)

- **Panel de Control Wazuh**: El panel de control de Wazuh es una interfaz de usuario web flexible e intuitiva para extraer, analizar y visualizar datos de eventos y alertas de seguridad. También se utiliza para la gestión y supervisión de la plataforma Wazuh. Además, proporciona funciones para el control de acceso basado en roles (RBAC) y el inicio de sesión único (SSO).

  La interfaz web ayuda a los usuarios a navegar por los distintos tipos de datos recogidos por el agente Wazuh, así como por las alertas de seguridad generadas por el servidor Wazuh. Los usuarios también logran generar informes y crear visualizaciones y cuadros de mando personalizados.

  La ilustración 6, muestra la información referente a un usuario activo.

Ilustración 6. Panel de Control Wazuh de un Usuario



Fuente: tomado a partir de (Wazuh, 2023)

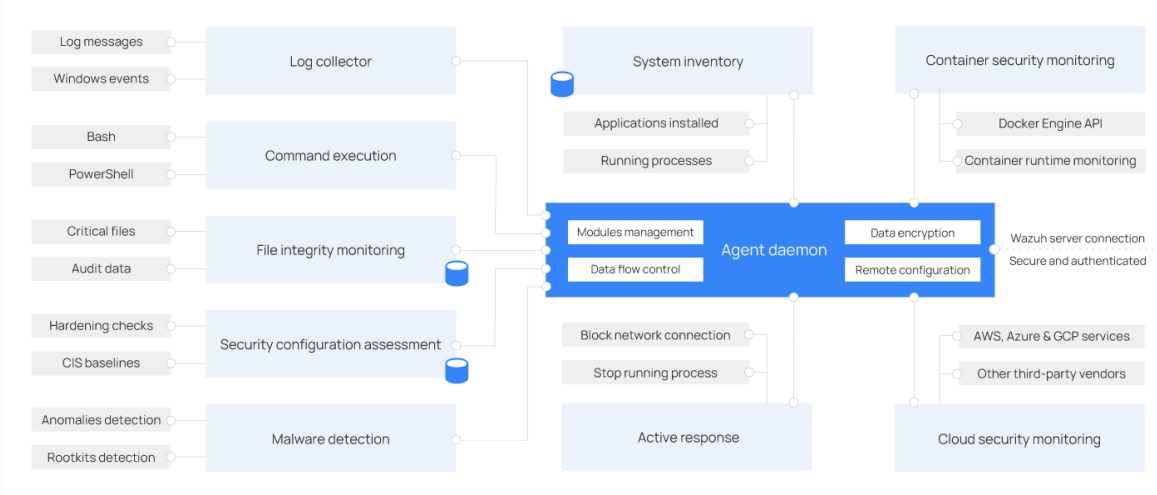
- **Agente Wazuh:** El agente Wazuh funciona en Linux, Windows, macOS, Solaris, AIX y otros sistemas operativos. Permite desplegar en portátiles,

computadores de sobremesa, servidores, instancias en la nube, contenedores o máquinas virtuales. El agente ayuda a proteger el sistema proporcionando funciones de prevención, detección y respuesta ante amenazas. También se utiliza para recopilar diferentes tipos de datos de sistemas y aplicaciones que reenvía al servidor Wazuh a través de un canal cifrado y autenticado.

El agente Wazuh tiene una arquitectura modular. Cada componente se encarga de sus propias tareas, entre las que se incluyen la supervisión del sistema de archivos, la lectura de mensajes de registro, la recopilación de datos de inventario, el análisis de la configuración del sistema y la búsqueda de malware. Los usuarios gestionan los módulos del agente a través de los ajustes de configuración, adaptando la solución a sus casos de uso particulares.

La ilustración 7, muestra la arquitectura y los componentes del agente.

Ilustración 7. Arquitectura y Componentes del Agente Wazuh



Fuente: tomado a partir de (Wazuh, 2023)

Todos los módulos del agente son configurables y realizan diferentes tareas de seguridad. Esta arquitectura modular le permite activar o desactivar cada componente en función de sus necesidades de seguridad.

La tabla 3 detalla las funciones de cada uno de estos componentes.

Tabla 3. Funciones de los componentes del agente wazuh

COMPONENTE	DESCRIPCIÓN
Recopilador de registros	Este componente del agente puede leer archivos de registro planos y eventos de Windows, recopilando mensajes de registro del sistema operativo y de las aplicaciones. Admite filtros XPath para eventos de Windows y reconoce formatos multilínea como los registros de auditoría de Linux. También puede enriquecer los eventos JSON con metadatos adicionales.
Ejecución de comandos	Los agentes ejecutan comandos autorizados periódicamente, recogiendo su salida y lo reporta al servidor Wazuh para su posterior análisis. Puede usar este módulo para diferentes propósitos, como monitorizar el espacio restante en el disco duro u obtener una lista de los últimos usuarios conectados.
Supervisión de la integridad de los archivos (FIM - File Integrity Monitoring)	Este módulo supervisa el sistema de archivos, informando cuando se crean, borran o modifican archivos. Realiza un seguimiento de los cambios en los atributos, permisos, propiedad y contenido de los archivos. Cuando se produce un evento, captura los detalles de quién, qué y cuándo en tiempo real. Además, el módulo FIM crea y mantiene una base de datos con el estado de los archivos supervisados, lo que permite realizar consultas de forma remota.
Evaluación de la configuración de seguridad (SCA)	Este componente proporciona una evaluación continua de la configuración, utilizando comprobaciones listas para usar basadas en los puntos de referencia del Centro de Seguridad de Internet (CIS). Los usuarios también pueden crear sus propias comprobaciones SCA para supervisar y aplicar sus políticas de seguridad.
Inventario del sistema	Este módulo del agente ejecuta periódicamente escaneos, recopilando datos de inventario como la versión del sistema operativo, interfaces de red, procesos en ejecución, aplicaciones instaladas y una lista de puertos abiertos. Los resultados de los análisis se almacenan en bases de datos SQLite locales que pueden consultarse de forma remota.
Detección de malware	Utilizando un enfoque no basado en firmas, este componente es capaz de detectar anomalías y la posible presencia de rootkits. Además, busca procesos ocultos, archivos y puertos ocultos mientras supervisa las llamadas al sistema.
Respuesta activa	Este módulo ejecuta acciones automáticas cuando se detectan amenazas, activando respuestas para bloquear una conexión de red, detener un proceso en ejecución o eliminar un archivo malicioso. Los usuarios también pueden crear respuestas personalizadas cuando sea necesario y personalizar, por ejemplo, las respuestas para ejecutar un binario en un sandbox, capturar el tráfico de red y analizar un archivo con un antivirus.
Supervisión de la seguridad de los contenedores	Este módulo de agente se integra con la API del motor Docker para supervisar los cambios en un entorno de contenedores. Por ejemplo, detecta cambios en las imágenes de los contenedores, en la configuración de la red o en los volúmenes de datos. Además, alerta sobre contenedores que se ejecutan en modo privilegiado y sobre usuarios que ejecutan comandos en un contenedor en ejecución.
Supervisión de la seguridad en la nube	Este componente monitoriza proveedores de nube como Amazon AWS, Microsoft Azure o Google GCP. Se comunica de forma nativa con sus API. Es capaz de detectar cambios en la infraestructura de la nube (por ejemplo, se crea un nuevo usuario, se modifica un grupo de seguridad, se detiene una instancia de la nube, etc.) y recopilar datos de registro de servicios en la nube (por ejemplo, AWS Cloudtrail, AWS Macie, AWS GuardDuty, Microsoft Entra ID, etc.).

Fuente: tomado a partir de (Wazuh, 2023)

Es importante recalcar, en base a la referencia del sitio oficial, Wazuh se distribuye bajo la licencia GPLv2, licencia Open Source que permite a los usuarios utilizar, modificar y distribuir el software de forma gratuita, así usar Wazuh en tu organización sin costo alguno, y también adaptar el software a tus necesidades específicas; adicionalmente, Wazuh ofrece servicios comerciales como soporte técnico, consultoría y formación a través de su empresa homónima.

Requerimientos de hardware para Wazuh

Según (Delgado, 2023), dimensionar un servidor SIEM como Wazuh en base a Eventos por Segundo (EPS) y tráfico, esto cambia según la carga de trabajo y los requisitos específicos de cada entorno. A continuación, se presentó una tabla con ejemplos de dimensionamiento aproximado basado en diferentes niveles de EPS y tráfico, estos valores son solo estimaciones y se ajusta en función de las necesidades y características particulares de tu infraestructura. La tabla 4 detalla el dimensionamiento del servidor basado en eventos por segundo (EPS) y tráfico (Mbps).

Tabla 4. Dimensionamiento del servidor basado en eventos por segundo

Nivel de Carga	Eventos por segundo (EPS)	Tráfico (Mbps)	Recursos Recomendados		
			CPU	RAM	DISCO
Muy Baja	Hasta 50 EPS	Hasta 0,5 Mbps	2 núcleos	4 GB	100 GB SSD
Baja	50-200 EPS	0,5 - 2 Mbps	4 núcleos	8 GB	200 GB SSD
Media Baja	200-500 EPS	2 - 5 Mbps	4 núcleos	16 GB	500 GB SSD
Media	500-1000 EPS	5 - 10 Mbps	8 núcleos	16 GB	1 TB SSD
Media Alta	1000-2000 EPS	10 - 20 Mbps	12 núcleos	32 GB	2 TB SSD
Alta	2000-5000 EPS	20 - 50 Mbps	16 núcleos	64 GB	4 TB SSD
Muy Alta	5000-10000 EPS	50 - 100 Mbps	24 núcleos	128 GB	8 TB SSD
Extrema	Más de 10000 EPS	Más de 100 Mbps	Escalabilidad y Configuración Personalizada según requerimientos		

Fuente: modificado a partir de (Wazuh, 2023)

Los Eventos por Segundo (EPS), es una métrica que se utiliza para medir la cantidad de eventos o registros de seguridad que un sistema, herramienta o componente de seguridad procesado en un segundo.

La métrica EPS es importante para evaluar la capacidad y el rendimiento de sistemas y herramientas de seguridad, como sistemas de detección de intrusiones

(IDS), sistemas de prevención de intrusiones (IPS), servidores de registro (log servers), sistemas de gestión de información y eventos de seguridad (SIEM) y otros componentes similares.

Por lo que es importante realizar pruebas de carga y ajustar los recursos según sea necesario para asegurarse de que el servidor esté adecuadamente dimensionado para satisfacer las necesidades de seguridad de cada organización.

CAPÍTULO II. DISEÑO METODOLÓGICO

Este capítulo, comprende la metodología y técnicas de investigación utilizadas para la GESTIÓN DE EVENTOS CON TECNOLOGÍA XDR PARA ASEGURAR LA INFRAESTRUCTURA DE COMUNICACIÓN DEL GAD COLTA; para determinar la importancia y nivel de impacto por parte del personal de la unidad de Tecnologías de la información TICs. El estudio ayudara a obtener información detallada y confiable, para proseguir con el presente proyecto, y a través de ello ejecutar un adecuado plan de implementación y garantizar no ser víctima de ciberdelincuentes.

2.1. Caracterización de la institución

Colta es un cantón de la Provincia de Chimborazo en el Ecuador. Se sitúa en una altitud promedio de 3.212 m s. n. m. Villa La Unión (Cajabamba) es considerada una de las ciudades más altas del país. La temperatura media es de 12 °C. Su proximidad a la ciudad de Riobamba está a solo 18 km, hace de ella una ciudad turística importante.

En la siguiente tabla 5 se resume la información concerniente al Cantón Colta.

Tabla 5. Datos generales del cantón Colta

Datos	Descripción
Nombre del Cantón	Colta
Denominación del GAD	Gobierno Autónomo Descentralizado Municipal del Cantón Colta
Origen Constitucional	27 de febrero 1884
Promulgación Registro Oficial	2 de agosto 1884
Poblacional (INEC 2020)	44.838 habitantes
Extensión (ha)	81.957,01 hectáreas
Temperatura promedio	12° C
Latitud	1°39´a 1°54´sur
Longitud	78° 36´a 78° 59´occidente
Rango altitudinal	1400-4300 m.s.n.m.
Precipitación	475-1639 milímetros de agua
Límites	
Norte	El Cantón Riobamba, con sus parroquias San Juan y Licán.
Sur	El Cantón Pallatanga y el Cantón Guamote.
Este	El Cantón Riobamba, con sus parroquias rurales Cacha, Punín y Flores. El Cantón Guamote, con su parroquia Cebadas.
Oeste	El Cantón Chillanes y el Cantón San Miguel (Provincia de Bolívar)

Fuente: tomado a partir de plan de ordenamiento territorial cantón Colta 2019

Misión

Promover el bienestar y la prosperidad de todas las familias Coltenses tanto del área rural y urbana, con la participación activa de todos los ciudadanos en los procesos de planeamiento y ejecución de todas las acciones del desarrollo local y el afianzamiento de la democracia con participación ciudadana real y efectiva de veedurías, para garantizar la administración de los recursos públicos con honradez, honestidad y transparencia; que permita la proyección de una nueva imagen a nivel nacional e internacional.

Visión

Colta será un modelo de desarrollo y de convivencia social donde se pueda vivir con dignidad y seguridad, que brinde oportunidades para el desarrollo pleno de las capacidades físicas y espirituales de sus pobladores; fomentando el desarrollo del empleo, la educación, la salud, las actividades productivas, la vivienda, el espacio público, equipamiento, tecnificación, eficiencia y eficacia.

2.2. Metodología de investigación

Tipo de investigación

El proceso de investigación bibliográfica es muy importante para el trabajo debido a que nos permite dar relevancia al tema y asegurar su originalidad, para ello se contó con material informativo como libros, revistas de divulgación o de investigación científica, sitios web; información necesaria para iniciar el estudio, la búsqueda de información bibliográfica se desarrolló en tesis similares, artículos científicos relacionados con la gestión de eventos de seguridad en repositorios como: Mendeley, Redalyc, IEEE Explore y otras fuentes.

Además, en el presente trabajo también se utilizó la investigación experimental. Por esta razón, se implementó y configuró la plataforma de monitoreo de eventos de seguridad de software libre Wazuh en su versión 4.7.1 en la infraestructura real

del GAD Colta, misma que permitió realiza el diagnóstico de vulnerabilidades y otras amenazas comunes en la red de comunicaciones.

Enfoque de investigación

En el presente trabajo de investigación, se usó un tipo de enfoque cuantitativo, debido a que este enfoque es un método estructurado que utiliza la recolección de datos para probar hipótesis con base a la medición numérica y el análisis estadístico, con el fin de establecer pautas de comportamiento (Hernández Sampieri 2006); de manera específica este es el método utilizado por la herramienta de monitoreo de eventos de seguridad seleccionada para determinar un posible ataque o amenaza a la red de comunicaciones del GAD Colta.

Población y muestra

La población que se tomó en la presente investigación es de 93 computadores personales asignados a cada uno de los funcionarios que son los que conforman el personal de todos los departamentos del GAD Colta. Ver Tabla 6.

Tabla 6. Población Computadores del GAD Colta

Departamento	# Computadores	%
ADMINISTRATIVO	17	18,28
ALCALDIA	4	4,301
CONCEJALES	5	5,376
FINANCIERO	16	17,20
JURIDICO	4	4,301
OBRAS PUBLICAS	11	11,83
PLANIFICACIÓN	15	16,13
REGISTRO PROPIEDAD	6	6,452
SECRETARIA DE CONCEJO	5	5,376
SERVICIOS PUBLICOS	10	10,75
TOTAL	**93**	**100**

Fuente: elaboración propia

Además, el centro de datos del Gobierno Autónomo Descentralizado del Cantón Colta está formado por 6 servidores como se detalla en la tabla 7.

Tabla 7. *Servidores GAD Colta*

Servidores
Zimbra
Sinat
Eset
Directorio Activo
Central IP
Quipux
TOTAL = 6

Fuente: elaboración propia

Para calcular los valores de la muestra por cada uno de los departamentos que conforman el GAD Colta, se utilizó la fórmula de poblaciones finitas, los resultados se presentan en la siguiente tabla 8.

Tabla 8. Numero de muestras por departamento GAD Colta

Departamento	Muestra
Administrativo	16
Alcaldía	2
Concejales	2
Financiero	15
Jurídico	2
Obras Públicas	10
Planificación	14
Registro de la Propiedad	2
Secretaria del Concejo	2
Servicios Públicos	10
TOTAL	**75**

Fuente: elaboración propia

En estos 75 computadores personales asignado a cada uno de los funcionarios del GAD Colta, así como en los 6 servidores del Centro de Datos, se instala la versión 4.7.1 del agente wazuh.

El software agente wazuh se utiliza para almacenar diferentes tipos de datos provenientes de sistemas o aplicaciones. Los datos son transmitidos desde el agente hacia el servidor de Wazuh por medio de un canal encriptado y autenticado.

2.3. Metodología de desarrollo

Para la elaboración de un proyecto es necesario tener un enfoque claro de secuencias sistemáticas y definir una metodología de desarrollo, que permita elaborar a partir de un marco definido por uno o varios ciclos de vida en todas sus fases.

En este contexto, **MAGERIT** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), es una metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica de España a finales de 1990. Su objetivo principal es identificar, analizar y gestionar los riesgos relacionados con la información y los sistemas de información en las organizaciones, especialmente en el ámbito de la administración pública, aunque su aplicación puede extenderse a cualquier tipo de organización. MAGERIT se centra en la protección de los activos de información, considerando tanto las amenazas que podrían comprometer dichos activos como las vulnerabilidades que podrían facilitar su materialización.

En el presente trabajo, el objetivo principal de la metodología MAGERIT, es proteger la información que se transmite en la infraestructura de comunicaciones del GAD Colta, teniendo en cuenta las dimensiones de seguridad.

Disponibilidad: La disponibilidad de todos los servicios informáticos que presta el GAD Colta es fundamental y se tiene que identificar adecuadamente, la falta de esta, se supone una interrupción del servicio reduce drásticamente la productividad y la imagen corporativa de la entidad.

Integridad: La información generada dentro de los sistemas de información del GAD Colta sea manipulada, lo que provocaría que esta información se corrompa, afectando directamente al correcto funcionamiento de los sistemas informáticos existentes.

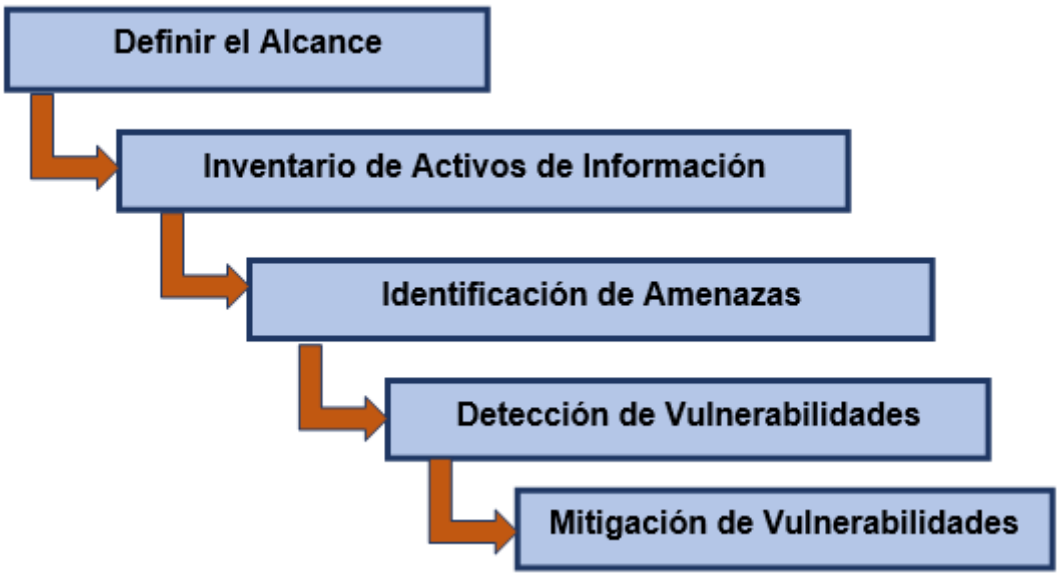
Confidencialidad: De acuerdo con el tipo de información que se maneja en el GAD Colta, será accedida solamente por las personas autorizadas, para evitar fugas o filtraciones de información de carácter confidencial.

Autenticidad: Esta propiedad de la seguridad de la información garantiza la veracidad de la fuente que procesan los datos, el monitoreo en tiempo real de los eventos que suceden en la red del GAD Colta evita la manipulación del origen o del contenido de los datos.

Trazabilidad: La trazabilidad se refiere a la capacidad de rastrear y registrar las acciones y eventos que afectan a la información y los sistemas de información, permitiendo reconstruir quién hizo, qué, cuándo, cómo y desde dónde. Esta capacidad es fundamental para asegurar la integridad, confidencialidad, y disponibilidad de la información, así como para el cumplimiento de políticas de seguridad, auditorías internas y externas, y regulaciones legales.

MAGERIT maneja un esquema sencillo de todas sus etapas como se muestra a continuación en la ilustración 8.

Ilustración 8. Etapas de la metodología MAGERIT



Fuente: elaboración propia

ETAPA 1. Definir el alcance

La infraestructura de comunicaciones del GAD Colta está conformada por 10 departamentos como se indica en la tabla 6, en la misma existen 93 computadores personales que utilizan como sistema operativo Windows 7, Windows 8.1, Windows 10 y 11; además de 40 impresoras, 80 teléfonos IP, 12 *switchs* administrables, 30 cámaras IP de vídeo vigilancia, 17 puntos de acceso inalámbrico, 6 servidores de aplicaciones y un equipo de seguridad perimetral.
Adicional la infraestructura cuenta con acceso a Internet mediante el proveedor de servicios CNT mediante un enlace de fibra óptica con una tasa de transmisión de 800 Mbps.

El alcance del presente trabajo define los dispositivos de la infraestructura tecnológica del GAD Colta que serán monitoreados y que son 75 computadores personales y 6 servidores de aplicaciones, en los que se instalan un software agente que se encarga de enviar toda la información del dispositivo al servidor de WAZUH; además se monitorea mediante el protocolo SYSLOG el switch principal de la infraestructura, así como el equipo de seguridad perimetral.

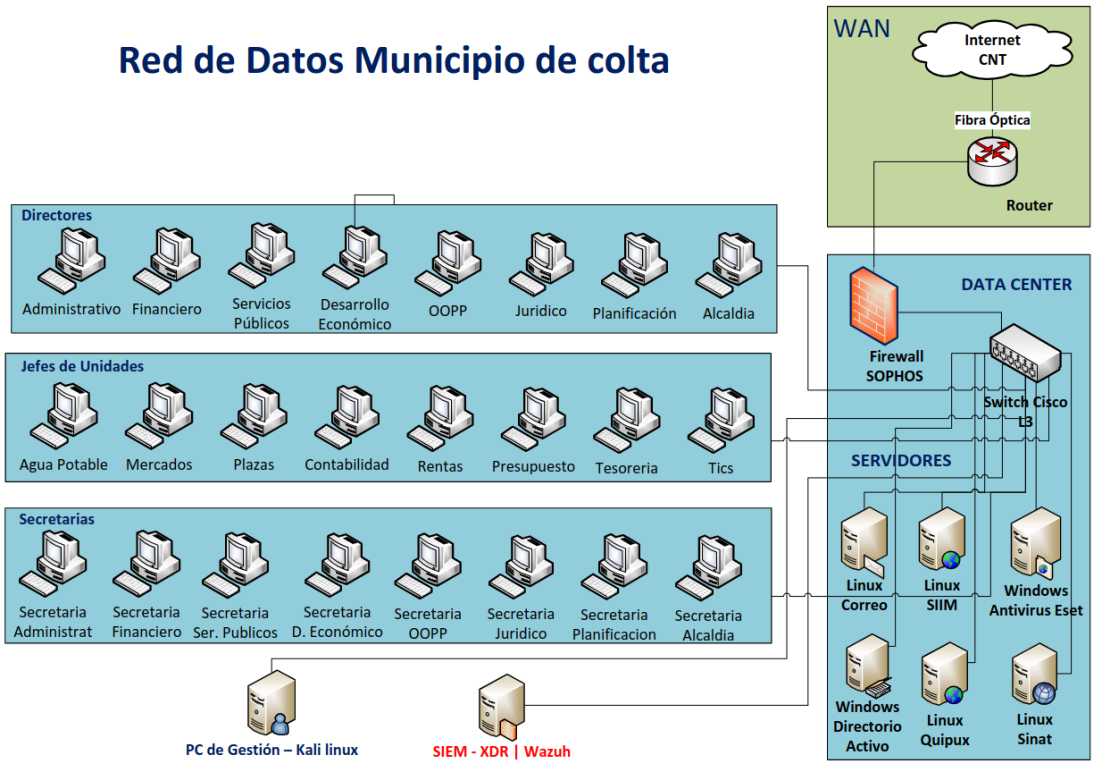
ETAPA 2. Inventario de Activos de Información

El inventario de activos de información implica identificar, documentar y clasificar todos los activos de información relevantes de una organización. Estos activos son tanto físicos (como servidores, dispositivos de almacenamiento, dispositivos de red) así como lógicos (como bases de datos, aplicaciones, documentos).
En el presente trabajo de investigación se toman 3 fuentes para el inventario de Activos de Información:

1. Diagrama Lógico de la red
2. Inventario Hardware de los servidores
3. Inventario de los sistemas de información existentes

El diagrama lógico de la infraestructura de comunicaciones del GAD Colta se detalla a continuación en la ilustración 9.

Ilustración 9. Diagrama Lógico de la Red GAD Colta



Fuente: elaboración propia

A continuación, en la tabla 9 se detalla las principales características de los servidores físicos y virtualizados de los que dispone el GAD Colta y en los que se encuentran instalados los sistemas de información que se detallan más adelante.

Tabla 9. Inventario de los servidores del GAD Colta

Servidor	Tipo	Marca	Modelo	Sistema Operativo	Software Instalado
Zimbra	Físico	HP Proliant	ML 370 G5	Linux Centos 6.6	Zimbra
SINAT	Físico	DELL	PowerEdge T710	Centos 6.5	Sinat
SIIM	Virtualizado	HP Proliant	DL 380 G9	Linux Centos 7	Registro SIIM
Directorio Activo	Virtualizado	HP Proliant	DL 380 G9	Windows Server 2012	Directorio Activo, SQL ServerWin Server Eset Antivirus
Central IP	Físico	HP Proliant	Proliant DL 120 G9	Linux Centos 7.0	Elastix
QUIPUX	Físico	HP Proliant	ML 350 G6	Linux Centos 6.5	QUIPUX Base Datos Posgress Aplicación Web

Fuente: elaboración propia

Según Mosquera (2020), los sistemas de información pueden definirse como un conjunto integrado de componentes cuyo objetivo es recolectar, almacenar, procesar y proporcionar datos o cualquier producto digital. Los componentes principales de un Sistema de información son:

1. El hardware o componentes físicos
2. El software o código fuente
3. Las telecomunicaciones
4. Bases de datos y servidores
5. Recursos humanos y procedimientos

En la infraestructura del GAD Colta existen los sistemas de información que se detalla en la tabla 10.

Tabla 10. Sistemas de Información del GAD Colta

Sistema de información	Descripción	Software utilizado
Sistema Integral de Catastro - SIC	Sistema contempla todas las funciones básicas necesarias para Ingresar la Información de los Predios Urbano/Rural, correspondiente a la parte alfanumérica.	Windows SIC 5.0 SQL server 2008 10.50.16
Sistema Integral de Catastro Rural - SINAT	Sistema de gestión de catastro Rural georreferenciado para el levantamiento de planimetrías de Predios.	Windows SINAT Ver 17 2022.07.08 Postgres 9.05.19
Sistemas Administrativo Financiero - SIGAME	Facilita la automatización de las tareas de gestión y análisis de los Gobiernos Autónomos Descentralizados, con el fin de agilizar las tareas obligatorias y proporcionar absoluta seguridad en el manejo de operaciones en las áreas tales como: Talento humano, Contabilidad, Presupuesto, Tesorería, Bodega, Activos fijos y Proyectos	Windows SIGAME 1.2.7 SQL server 2008 10.50.16
Sistema de administración de tributos - SAT	Herramienta informática que facilita la automatización del proceso de Catastro, emisión y cobro de títulos, esta funcionalidad está orientada a planificar, programar, dirigir y controlar los recursos del Municipio: Contribución especial de mejoras, Patentes Alcabalas, Ocupación de vías, Impuesto al rodaje, Tasas, Gestión de agua potable.	Windows SAT 2.0 SQL server 2008 10.50.16
Sistema integral multifinalitario de automatización de procesos del registro de la propiedad - SIIM	Sistema Integral Multi-Finalitario del registro de la propiedad, completamente alineado y basado en las directrices de la DINARDAP, maneja todo el proceso desde solicitud, facturación, recaudación, creación de índices y repertorios, revisión, aprobación y registro de trámites.	Web SIIM 6.0 Postgres 9.05.19

Sistema de gestión de Correo/Mail institucional – ZIMBRA	Sistema de Mensajería de colaboración que permite enviar/recibir documentos, almacenar y organizar mensajes de correo electrónico, citas, contactos, tareas, documentos; que está disponible desde la web, facilitando tener presencia institucional ante los organismos públicos nacionales e internacionales	Zimbra 8.8.15-GA 4562.FOSS
Sistema de Portal Web Institucional – WEB	Portal www.municipiodecolta.gob.ec por el cual a través del internet se tiene como objetivo general, proveer a usuario externo e internos el acceso a la información pública de la municipalidad de forma fácil e integrada el acceso a una serie de recursos y de servicios, entre los que podrá encontrar Información relevante a las actividades, documentos, Noticias & Eventos, etc.	Joomla 2.5.28
Sistema de Gestión Documental - QUIPUX	Sistema web utilizado para la gestión de correspondencia interna y externa tales como: creación, envío, recepción, almacenamiento, recuperación y clasificación de memorandos, oficios, circulares y anexos.	Quipux 3.0 Postgres 9.05.19
Sistema Electrónico de facturación – SitacE	Facilita el procesamiento y emisión de documentos electrónicos (Facturas, Retenciones, Anexos y Formularios) con conexión al *web service* de SRI para el envió automático de documentos electrónicos al mail de los clientes y proveedores, en línea autorizados y solicitados por el Servicio de Rentas Internas	Windows SitacE 2024 SQL server 2008 10.50.16
Sistema de gestión de precios unitarios – PUNIS.	Sistema para la elaboración de Análisis de Precios Unitarios, Presupuestos de obras, Cronogramas Valorados de Trabajos, Insumos: Equipo y Mano de Obra, Formula de Reajuste y Cuadrilla Tipo, Desagregación Tecnológica. Fácil de usar, compatible 100% con APU y modelos de Formularios del SERCOP (Ecuador).	Excel, Macros Punis 2024

Fuente: elaboración propia

ETAPA 3. Identificación de amenazas

Según menciona Tejena Macías (2018) en su artículo científico, las amenazas suelen ser internas como externas que ocasionan robo de identidad o información, bases de datos, información sensible de clientes, pérdida de credibilidad y daños financieros que afectarían la sostenibilidad de la entidad pública o privada.

Durante el proceso de identificación de amenazas, las organizaciones buscan indicadores de ataques (IoA), que permiten determinar la intención y las acciones

de los posibles atacantes. Un IoA es una acción o un conjunto de acciones que un atacante realiza para completar con éxito un ataque específico.

En este contexto, La gestión de la información y eventos de seguridad es una tecnología crucial para las instituciones públicas por varias razones fundamentales, de manera específica la plataforma WAZUH instalada en la infraestructura de comunicaciones del Gad Colta ha permitido realizar un monitoreo permanente de las posibles amenazas que se puedan presentar y que afecten al normal desenvolvimiento de las actividades diarias.

Para determinar estas posibles amenazas en la infraestructura de comunicaciones del GAD Colta se procedió a monitorear en tiempo real los servidores de la institución que alojan los sistemas de información que se indican en detalle en la tabla 10, así como a los computadores de cliente final; el monitoreo se realizó durante 120 días, desde el 1 de diciembre del 2023 hasta el 1 de abril del 2024.

La tabla 11 detalla los servidores y clientes de la infraestructura tecnológica del GAD Colta seleccionados para el análisis e identificación de amenazas.

Tabla 11. Servidores y Clientes seleccionados

Agente	Dirección IP	Sistema Operativo	Tipo
Servidor	192.168.100.2	Microsoft Windows Server 2012 R2 Standard 6.3.9600.21620	Servidor
Zimbra	192.168.100.4	CentOS Linux 7.9	Servidor
Siim	192.168.100.12	Ubuntu 16.04.6 LTS	Servidor
Sinat	192.168.100.7	CentOS Linux 6.5	Servidor
Quipux	192.168.100.5	CentOS Linux 6.5	Servidor
Central-VozIP	192.168.40.2	CentOS Linux 7.0	Servidor
Facturación	192.168.100.132	Microsoft Windows 7 Professional Service Pack 1 6.1.7601	Cliente
Yachay	192.168.100.8	Microsoft Windows 11 Pro 10.0.22621.1702	Cliente
Tesorería	192.168.100.248	Microsoft Windows 11 Pro 10.0.22621.2134	Cliente
Contador	192.168.100.178	Microsoft Windows 10 Pro 10.0.19045.3324	Cliente
Lap-Compras2	192.168.100.79	Microsoft Windows 10 Home 10.0.19045.4046	Cliente
Presupuesto	192.168.100.41	Microsoft Windows 8.1 Pro 6.3.9600.20778	Cliente

Fuente: elaboración propia

En el periodo de tiempo indicado y en los dispositivos seleccionados que se indican en la tabla 11, se realizó el monitoreo de los siguientes indicadores de ataques por ser los más comunes en la identificación de amenazas.

- **Eventos de seguridad** (*Security events*) mediante la recopilación y el análisis efectivo de los datos de registro (logs) de cada uno de los agentes.

- **Detección de malware** (Virus Total) y archivos maliciosos a través de la integración con VirusTotal (https://www.virustotal.com/gui/home/upload), una poderosa plataforma que agrega múltiples productos antivirus y un motor de escaneo en línea, proporcionando una forma efectiva de inspeccionar archivos en busca de contenido malicioso.

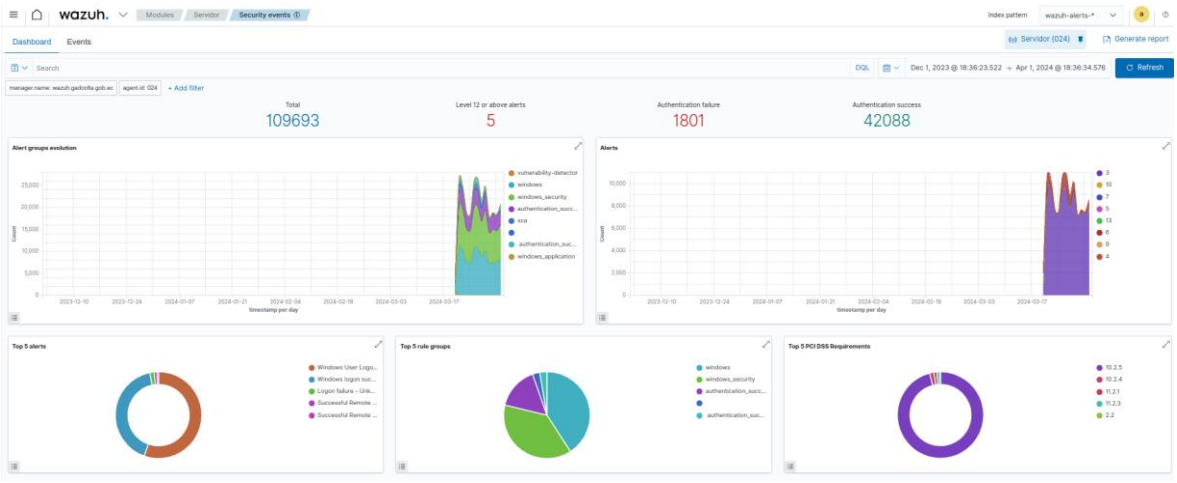
- **Evaluación de las mejores prácticas de configuración de seguridad** (*Security configuration assessment*) mediante el testeo de las políticas CIS *Benchmarks* preinstaladas en la plataforma Wazuh, un CIS *Benchmak* es un conjunto de prácticas recomendadas, reconocidas y consensuadas a nivel mundial para ayudar a los profesionales de la seguridad a aplicar y administrar medidas adecuadas de seguridad informática.

A continuación, se detallan los resultados obtenidos en cada uno de los servidores y clientes seleccionados.

Servidor Base de Datos (Windows Server 2012)

Como se observa en la ilustración 10, durante el periodo de monitoreo indicado se registraron 109693 eventos de seguridad, de estos 5 es decir el 0,045% son de nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

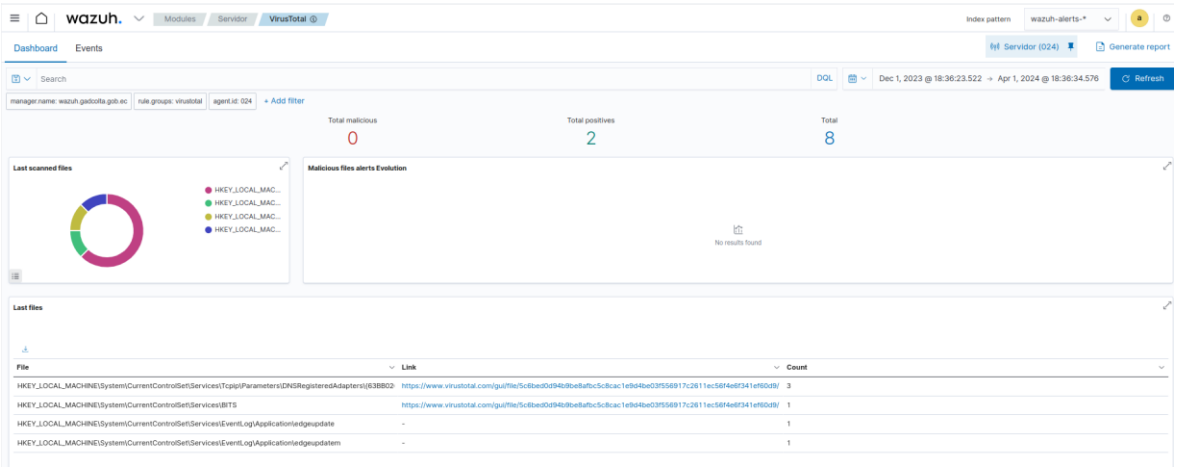
Ilustración 10. Eventos de Seguridad (Windows Server 2012)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 11 muestra que en el periodo de monitoreo no se detectaron archivos maliciosos.

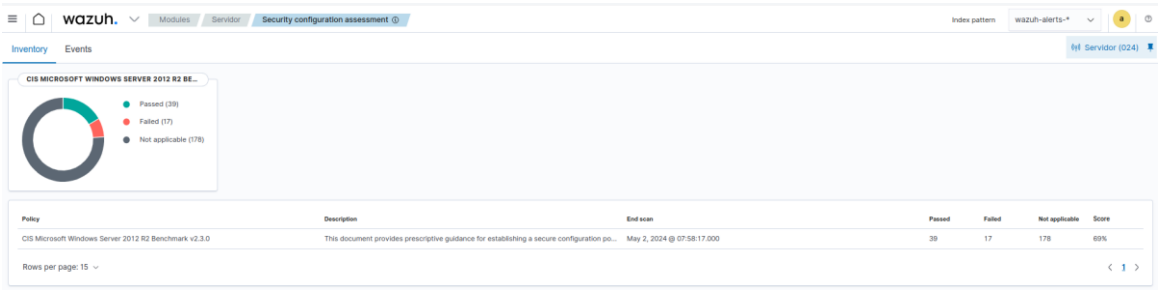
Ilustración 11. Detección de Malware (Windows Server 2012)



Fuente: elaboración propia

Con respecto a la evaluación de la configuración de seguridad de este servidor, la ilustración 12 indica que 39 de las 56 mejores prácticas de configuración segura pasaron exitosamente las pruebas, dando finalmente un puntaje de 69/100.

Ilustración 12. Evaluación de la configuración de seguridad (Windows Server 2012)

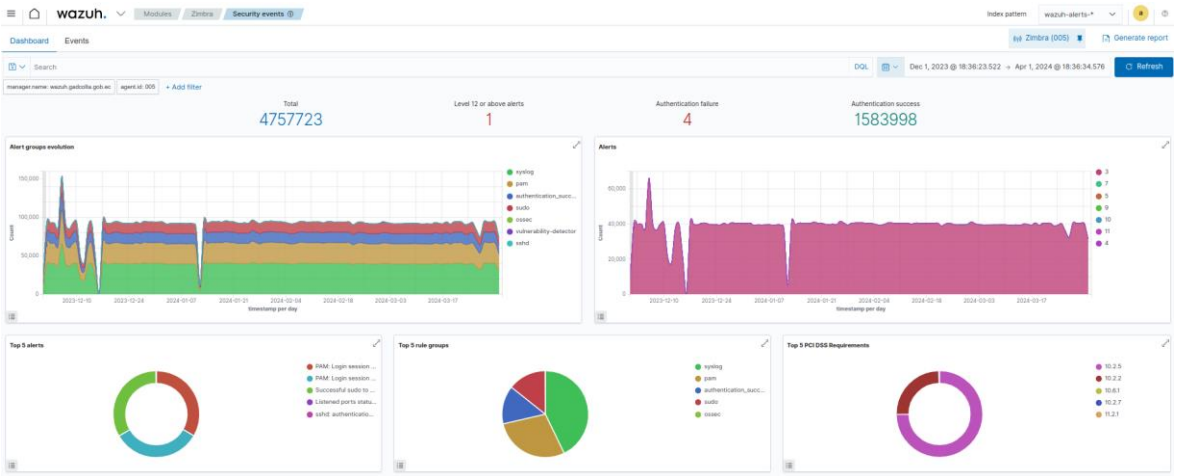


Fuente: elaboración propia

Servidor ZIMBRA (Centos 7.9)

Como se observa en la ilustración 13, durante el periodo de monitoreo indicado se registraron 4757723 eventos de seguridad, de estos 1 es decir el 0,00021% son de nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

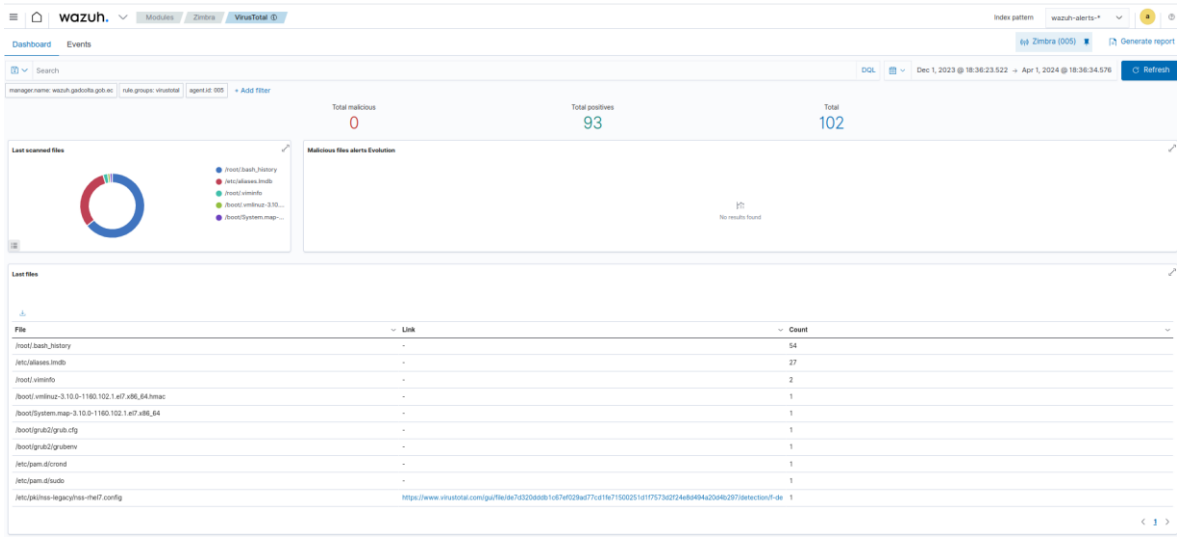
Ilustración 13. Eventos de Seguridad (Centos 7.9)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 14 muestra que en el periodo de monitoreo no se detectaron archivos maliciosos.

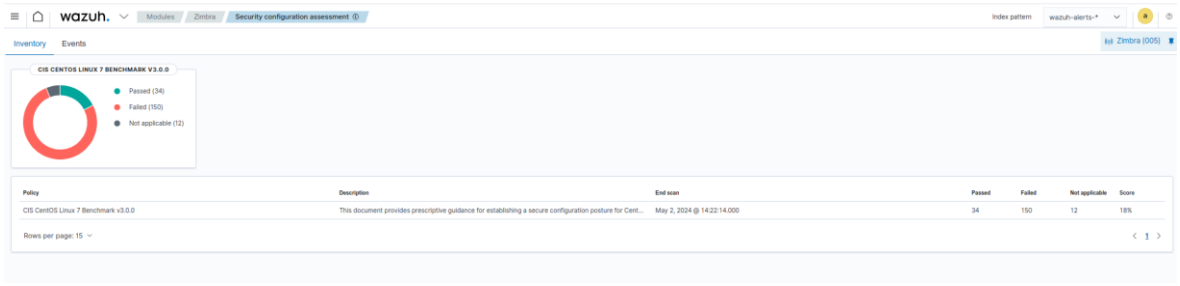
Ilustración 14. Detección de Malware (Centos 7.9)



Fuente: elaboración propia

Con respecto a la evaluación de la configuración de seguridad de este servidor, la ilustración 15 indica que solo 34 de las 184 mejores prácticas de configuración segura pasaron exitosamente las pruebas, dando finalmente un puntaje de 18/100.

Ilustración 15. Evaluación de la configuración de seguridad (Centos 7.9)

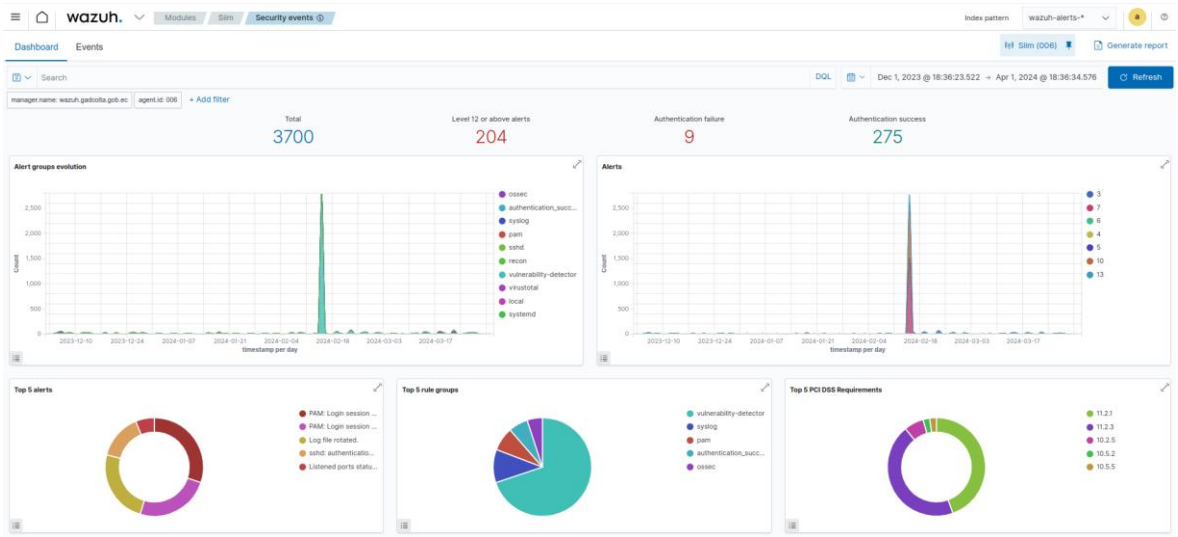


Fuente: elaboración propia

Servidor SIIM (Ubuntu 16.04)

Como se observa en la ilustración 16, durante el periodo de monitoreo indicado se registraron 3700 eventos de seguridad, de estos 204 es decir el 5,225% son de nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

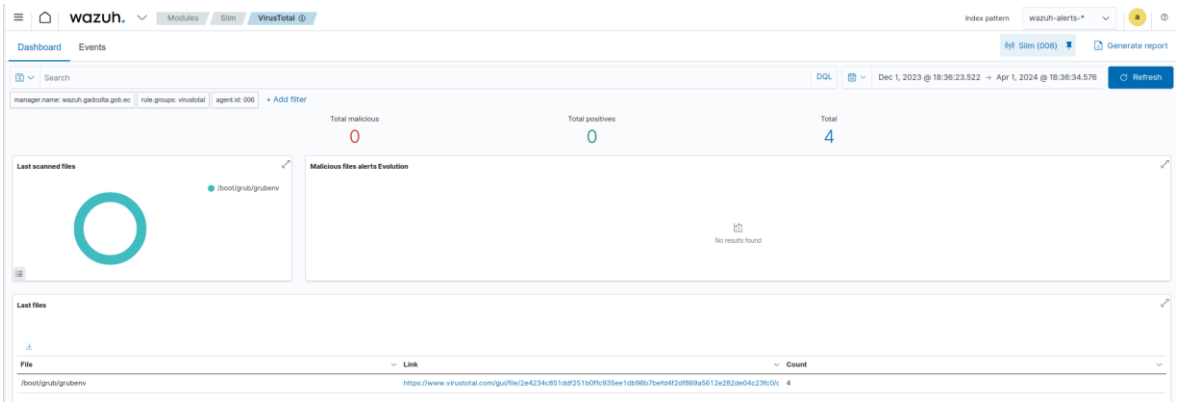
Ilustración 16. Eventos de Seguridad (Ubuntu 16.04)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 17 muestra que en el periodo de monitoreo no se detectaron archivos maliciosos.

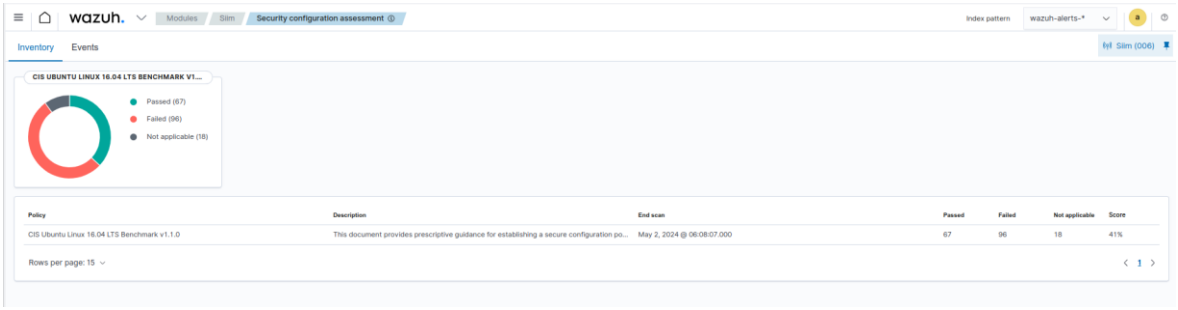
Ilustración 17. Detección de Malware (Ubuntu 16.04)



Fuente: elaboración propia

Con respecto a la evaluación de la configuración de seguridad de este servidor, la ilustración 18 indica que solo 67 de las 163 mejores prácticas de configuración segura pasaron exitosamente las pruebas, dando finalmente un puntaje de 41/100.

Ilustración 18. Evaluación de la configuración de seguridad (Ubuntu 16.04)

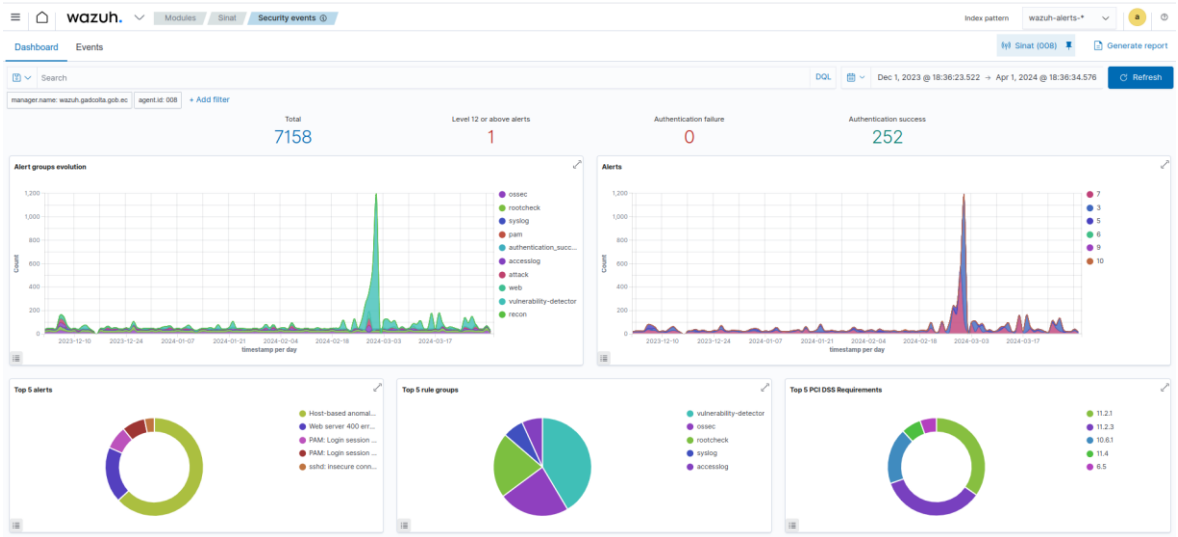


Fuente: elaboración propia

Servidor SINAT (Centos 6.5)

Como se observa en la ilustración 19, durante el periodo de monitoreo indicado se registraron 7158 eventos de seguridad, de estos 1 es decir el 0,014% son de nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

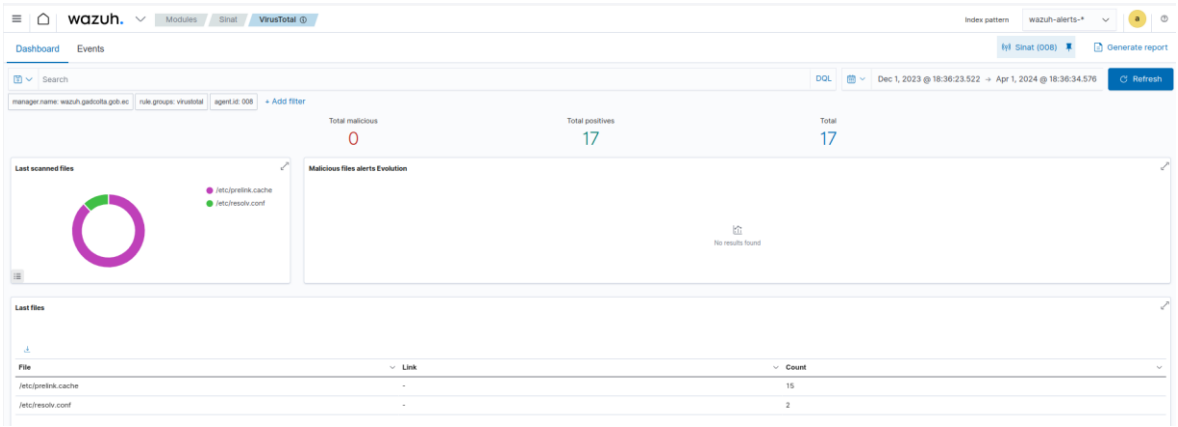
Ilustración 19. Eventos de Seguridad (Centos 6.5)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 20 muestra que en el periodo de monitoreo no se detectaron archivos maliciosos.

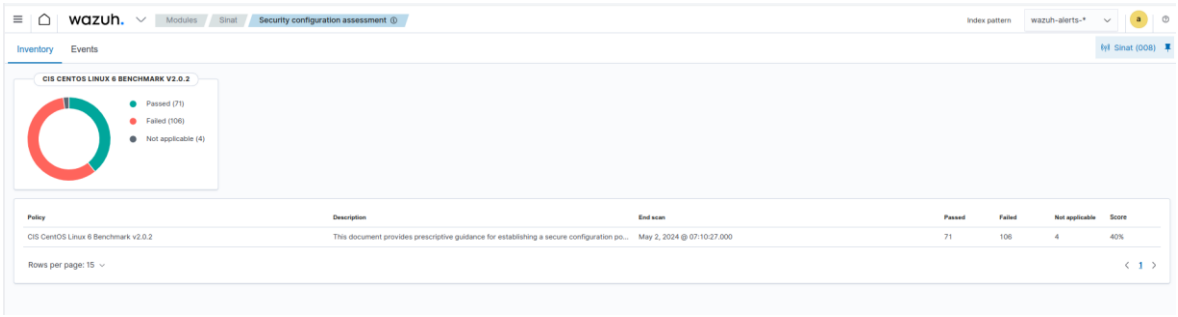
Ilustración 20. Detección de Malware (Centos 6.5)



Fuente: elaboración propia

Con respecto a la evaluación de la configuración de seguridad de este servidor, la ilustración 21 indica que solo 71 de las 177 mejores prácticas de configuración segura pasaron exitosamente las pruebas, dando finalmente un puntaje de 40/100.

Ilustración 21. Evaluación de la configuración de seguridad (Centos 6.5)

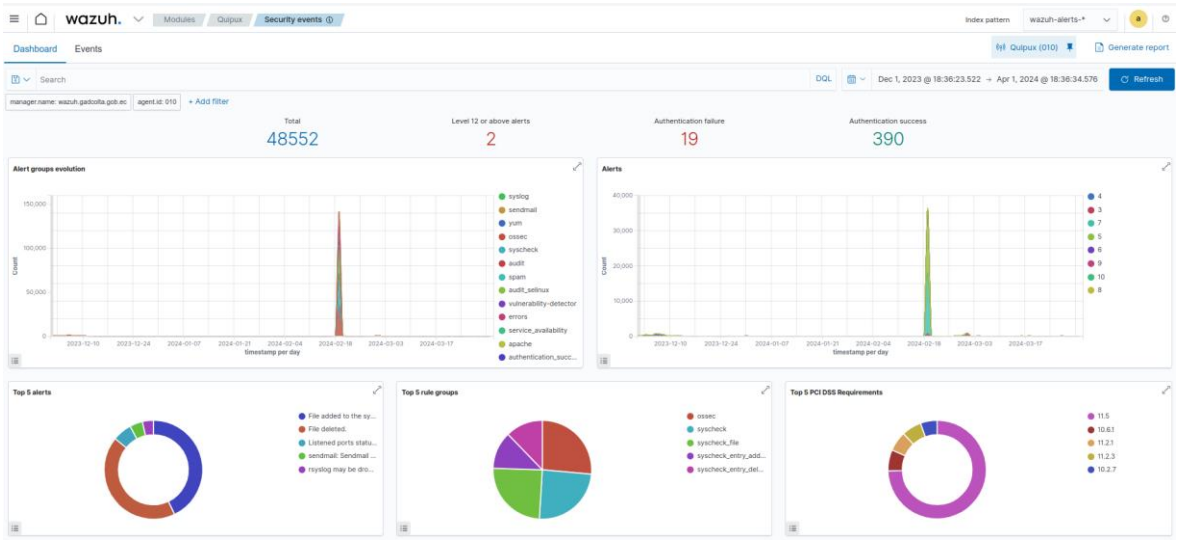


Fuente: elaboración propia

Servidor QUIPUX (Centos 6.5)

Como se observa en la ilustración 22, durante el periodo de monitoreo indicado se registraron 48552 eventos de seguridad, de estos 2 es decir el 0,004% son de nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

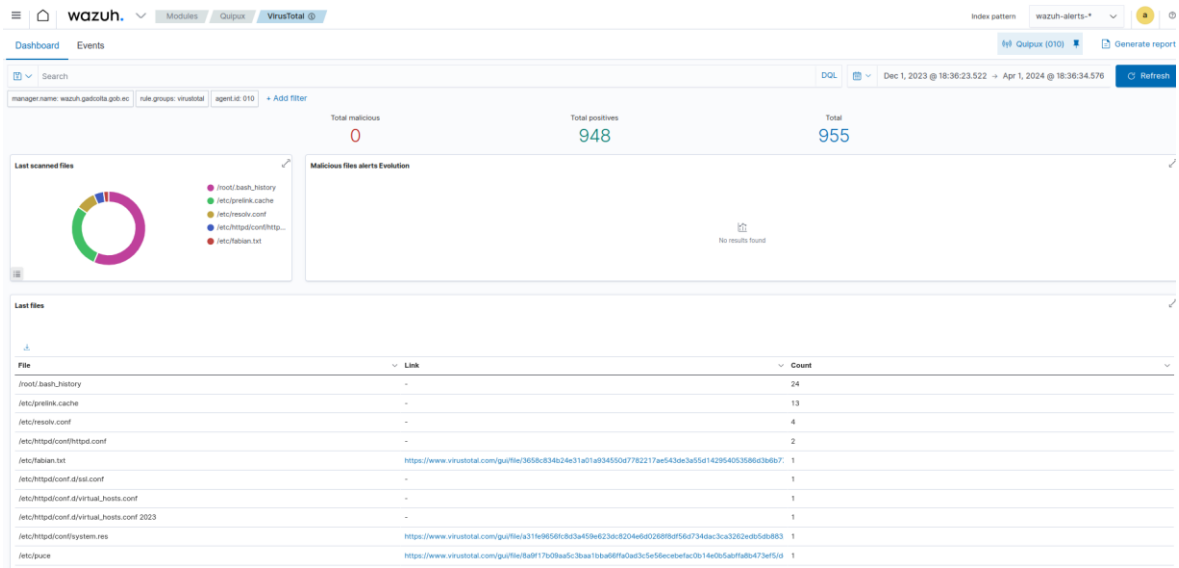
Ilustración 22. Eventos de Seguridad (Centos 6.5)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 23 muestra que en el periodo de monitoreo no se detectaron archivos maliciosos.

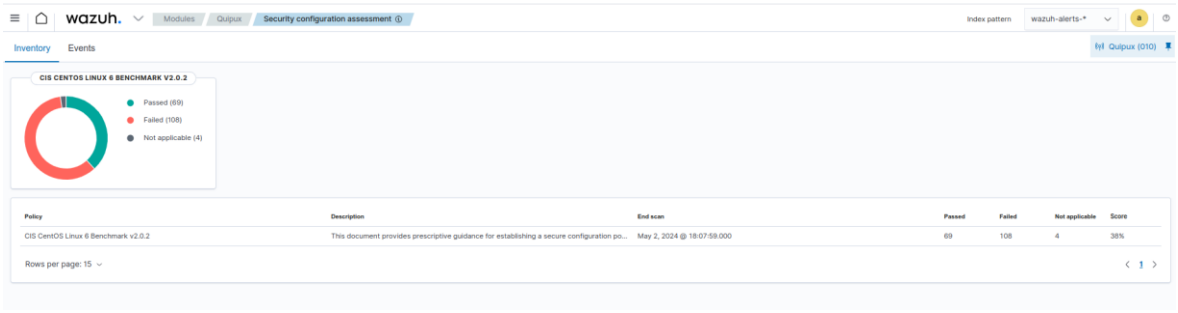
Ilustración 23. Detección de Malware (Centos 6.5)



Fuente: elaboración propia

Con respecto a la evaluación de la configuración de seguridad de este servidor, la ilustración 24 indica que solo 69 de las 177 mejores prácticas de configuración segura pasaron exitosamente las pruebas, dando finalmente un puntaje de 38/100.

Ilustración 24. Evaluación de la configuración de seguridad (Centos 6.5)

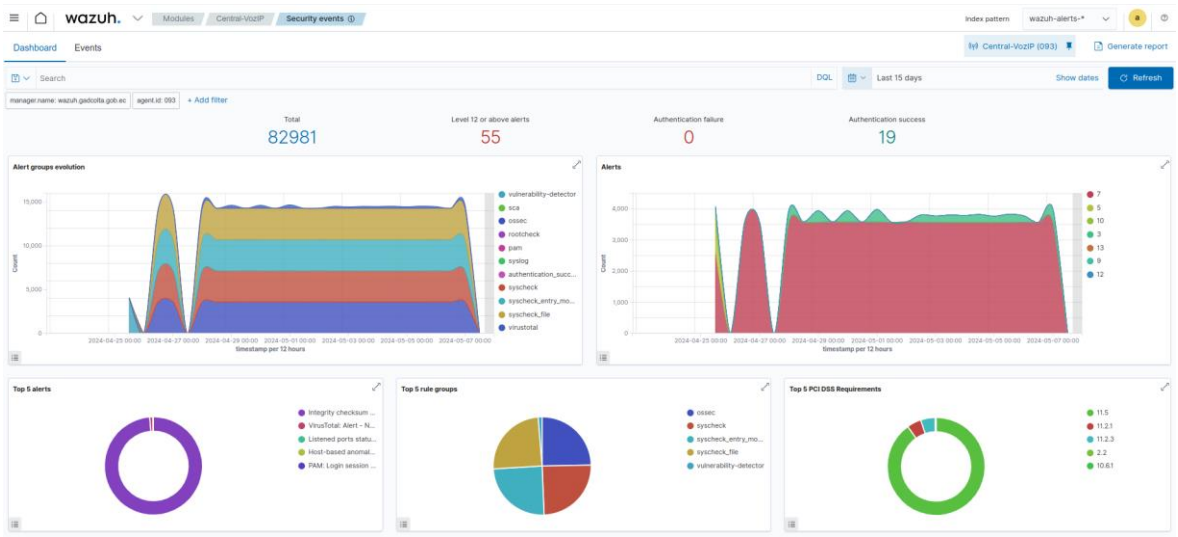


Fuente: elaboración propia

Servidor Central-VozIP (Centos 7)

Como se observa en la ilustración 25, durante el periodo de monitoreo indicado se registraron 82981 eventos de seguridad, de estos 55 es decir el 0,07% son de nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

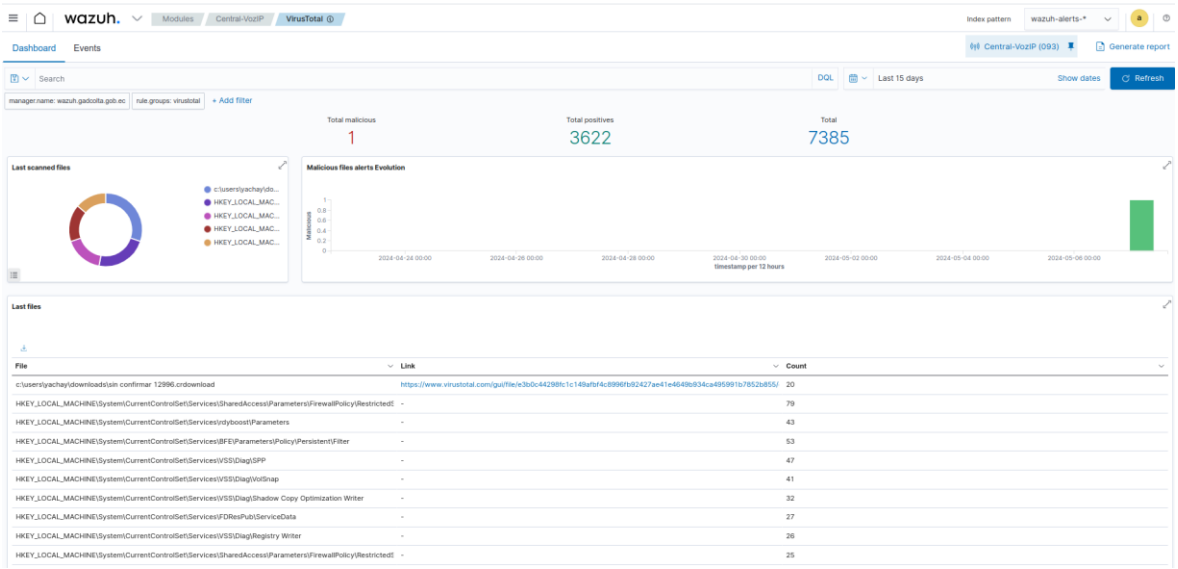
Ilustración 25. Eventos de Seguridad (Centos 7)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 26 muestra que en el periodo de monitoreo se detectó 1 archivo malicioso.

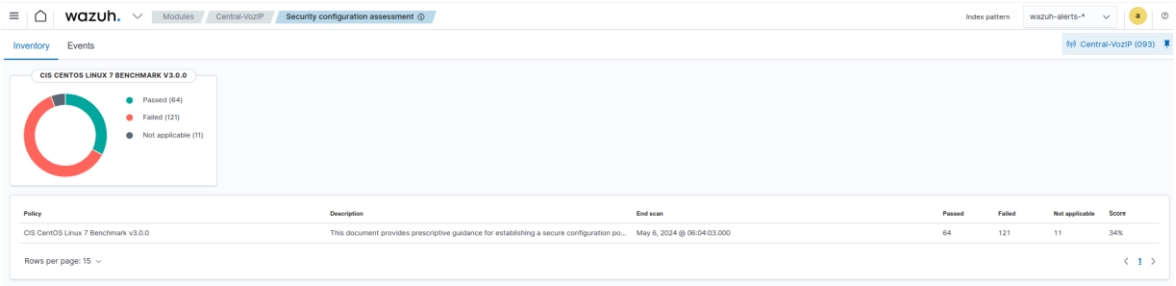
Ilustración 26. Detección de Malware (Centos 7)



Fuente: elaboración propia

Con respecto a la evaluación de la configuración de seguridad de este servidor, la ilustración 27 indica que solo 64 de las 185 mejores prácticas de configuración segura pasaron exitosamente las pruebas, dando finalmente un puntaje de 34/100.

Ilustración 27. Evaluación de la configuración de seguridad (Centos 7)

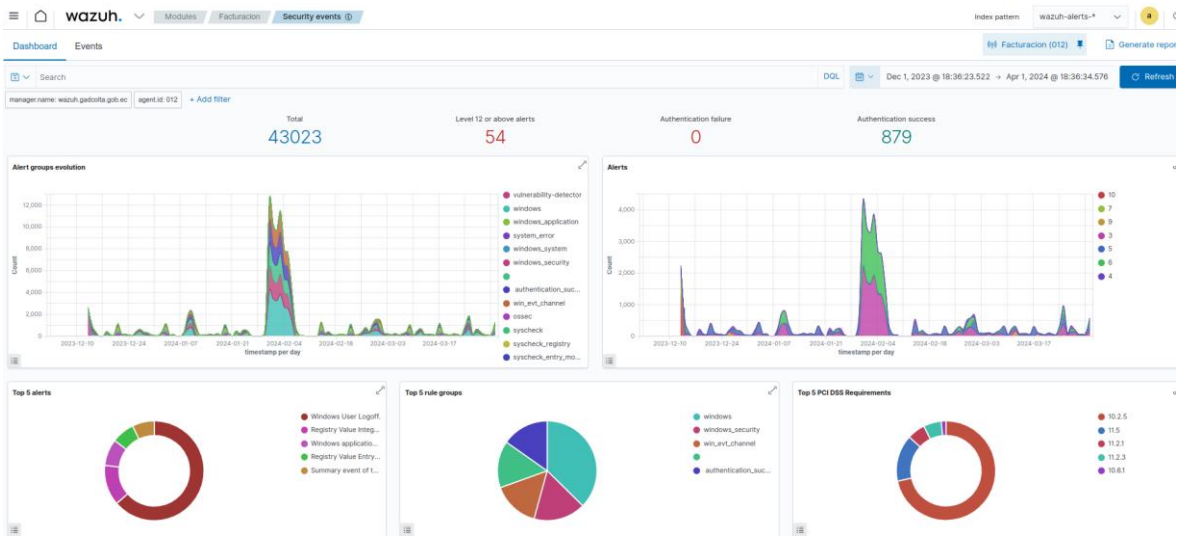


Fuente: elaboración propia

Cliente FACTURACIÓN (Windows 7 SP 1)

Como se observa en la ilustración 28, durante el periodo de monitoreo indicado se registraron 43023 eventos de seguridad, de estos 54 es decir el 0,13% son de nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

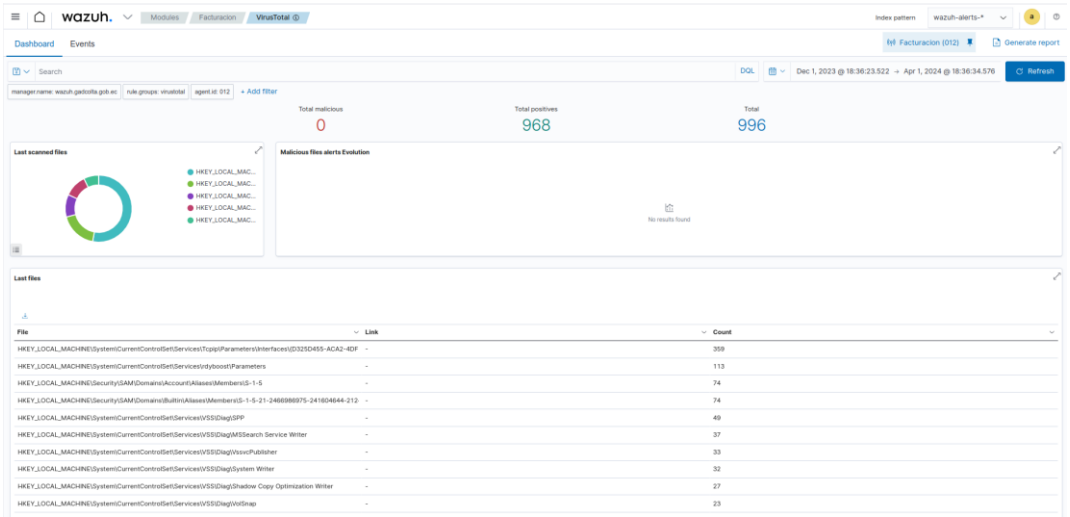
Ilustración 28. Eventos de Seguridad (Windows 7 SP 1)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 29 muestra que en el periodo de monitoreo no se detectaron archivos maliciosos.

Ilustración 29. Detección de Malware (Windows 7 SP 1)



Fuente: elaboración propia

Con respecto a la evaluación de la configuración de seguridad de este servidor, la documentación de la plataforma indica que no dispone de políticas SCA para los sistemas operativos Windows 7 y Windows 8, la ilustración 30 detalla las versiones del sistema operativo soportadas hasta la fecha actual.

Ilustración 30. Políticas SCA para el sistema operativo windows

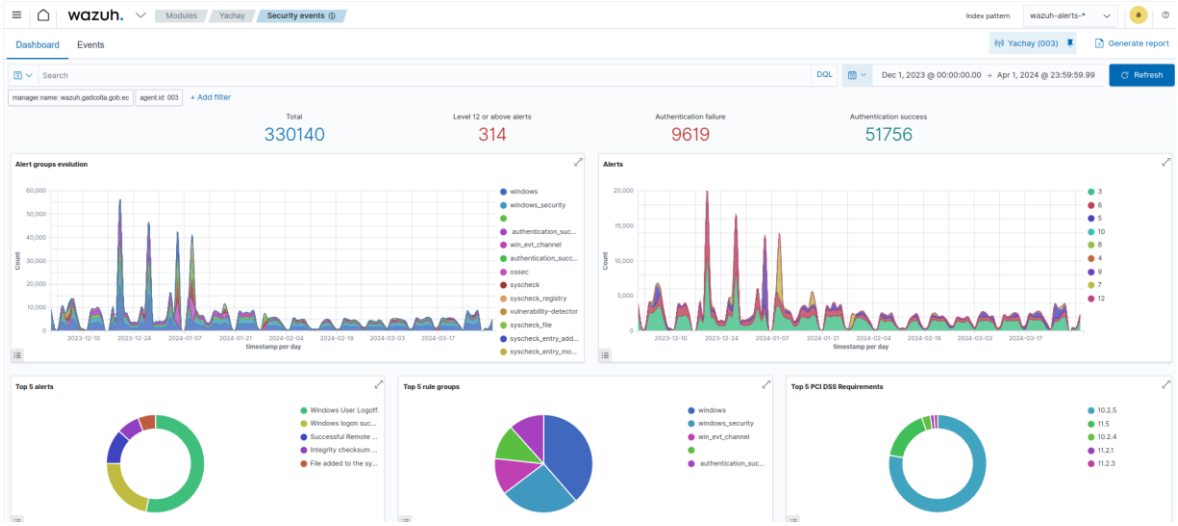
Available SCA policies		
Policy	**Name**	**Target**
cis_win2012r2	CIS Benchmark for Windows 2012 R2	Windows Server 2012 R2
cis_win10_enterprise	CIS Benchmark for Windows 10 Enterprise	Windows 10
cis_win11_enterprise	CIS Benchmark for Windows 11 Enterprise	Windows 11
cis_win2016	CIS Benchmark for Windows Server 2016	Windows Server 2016
cis_win2019	CIS Benchmark for Windows Server 2019 RTM	Windows Server 2019
cis_win2022	CIS Benchmark for Windows Server 2022	Windows Server 2022

Fuente: tomado a partir de Wazuh

Cliente YACHAY (Windows 11 Pro)

Como se observa en la ilustración 3**1**, durante el periodo de monitoreo indicado se registraron 330140 eventos de seguridad, de estos 314 es decir el 0,095% son de nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

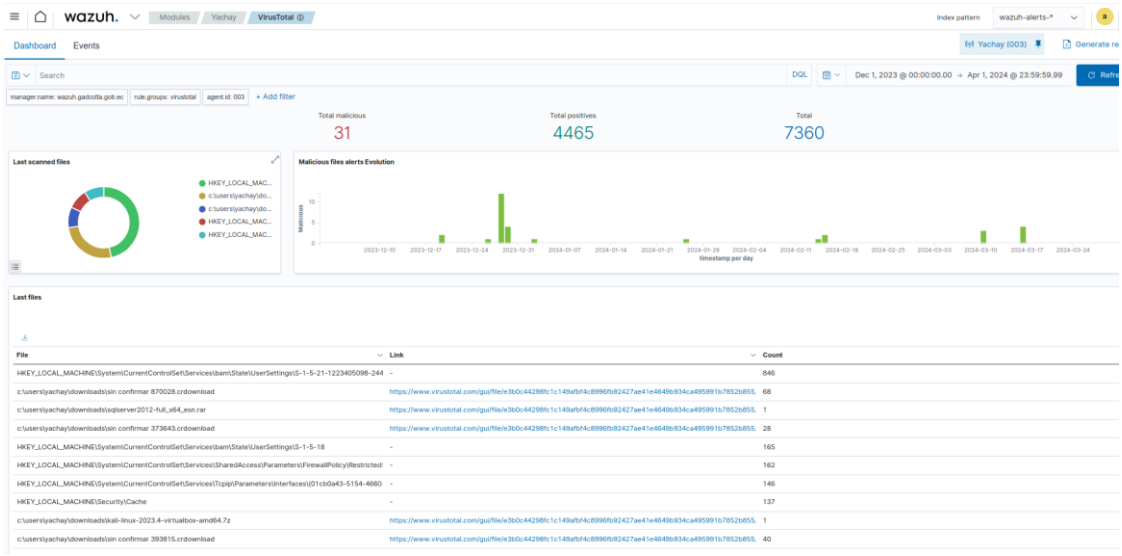
Ilustración 31. Eventos de Seguridad (Windows 11 Pro)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 32 muestra que en el periodo de monitoreo se detectaron 31 archivos maliciosos, que según VirusTotal se debe a la presencia de los troyanos: Trojan.Malware.300983.susgen y Trojan.JPotato.fx.

Ilustración 32. Detección de Malware (Windows 11 Pro)



Fuente: elaboración propia

Con respecto a la evaluación de la configuración de seguridad de este servidor, la ilustración 33 indica que solo 112 de las 392 mejores prácticas de configuración segura pasaron exitosamente las pruebas, dando finalmente un puntaje de 28/100.

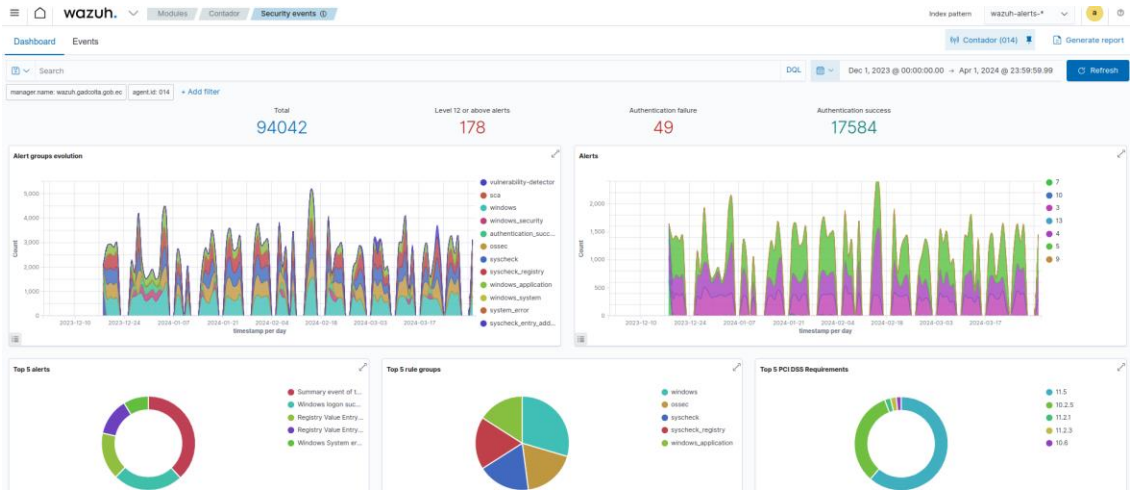
Ilustración 33. Evaluación de la configuración de seguridad (Windows 11 Pro)

Fuente: elaboración propia

Cliente Contador (Windows 10 Pro)

Como se observa en la ilustración 34, durante el periodo de monitoreo indicado se registraron 94042 eventos de seguridad, de estos 178 es decir el 0,19% son de nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

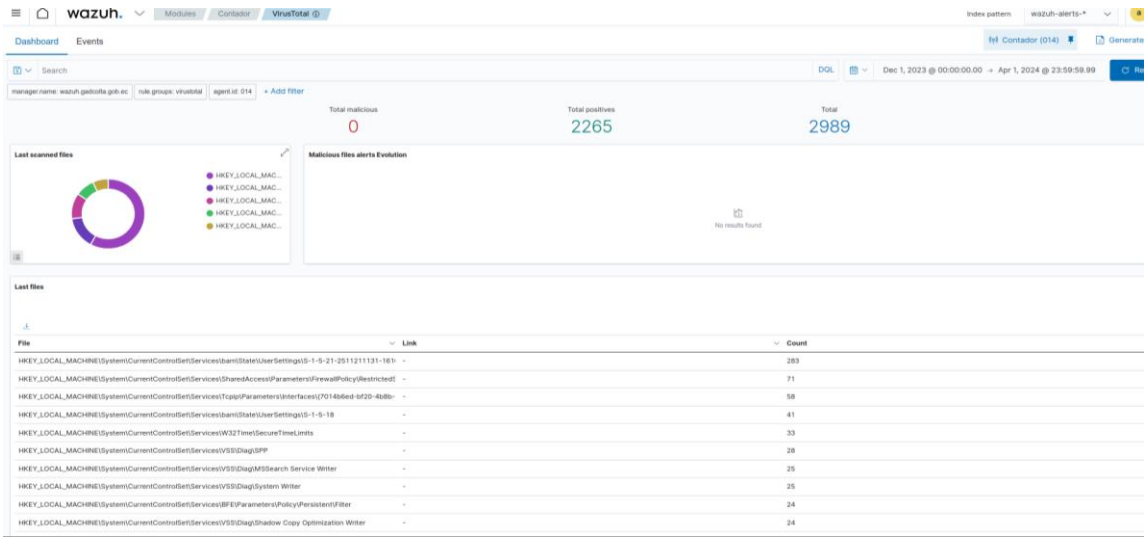
Ilustración 34. Eventos de Seguridad (Windows 10 Pro)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 35 muestra que en el periodo de monitoreo no se detectaron archivos maliciosos.

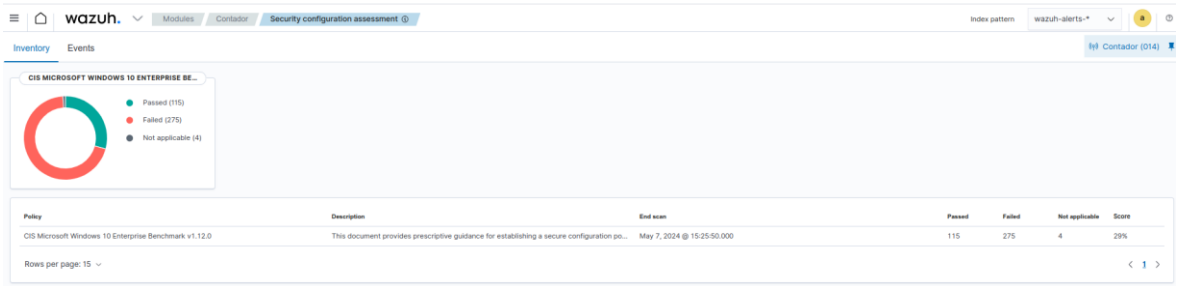
Ilustración 35. Detección de Malware (Windows 10 Pro)



Fuente: elaboración propia

Con respecto a la evaluación de la configuración de seguridad de este servidor, la ilustración 36 indica que solo 115 de las 390 mejores prácticas de configuración segura pasaron exitosamente las pruebas, dando finalmente un puntaje de 29/100.

Ilustración 36. Evaluación de la configuración de seguridad (Windows 10 Pro)

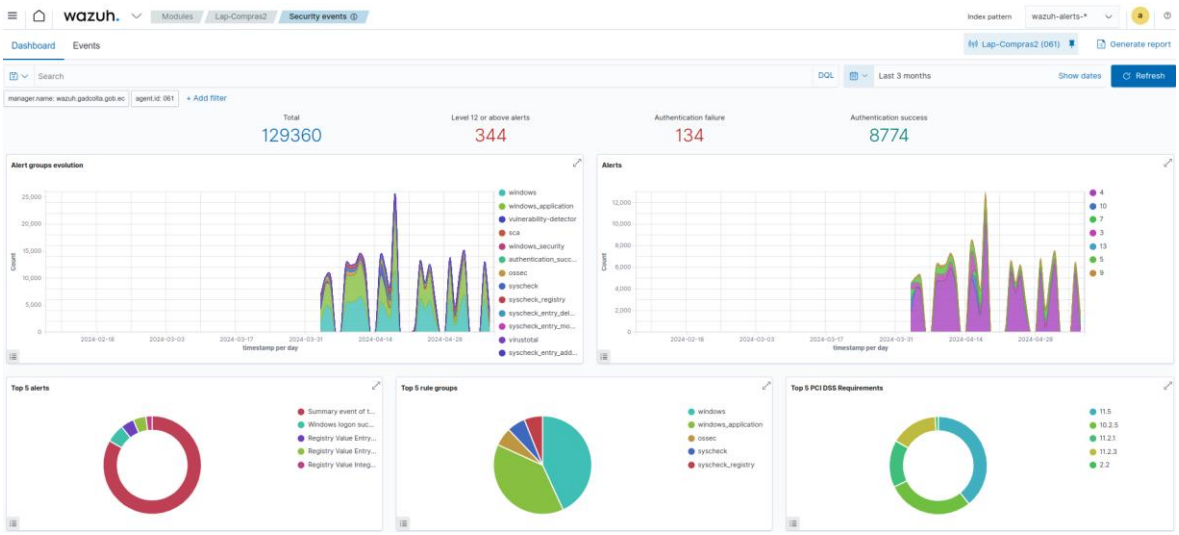


Fuente: elaboración propia

Cliente Lap-Compras2 (Windows 10 Home)

Como se observa en la ilustración 37, durante el periodo de monitoreo indicado se registraron 129360 eventos de seguridad, de estos 344 es decir el 0,27% son de nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

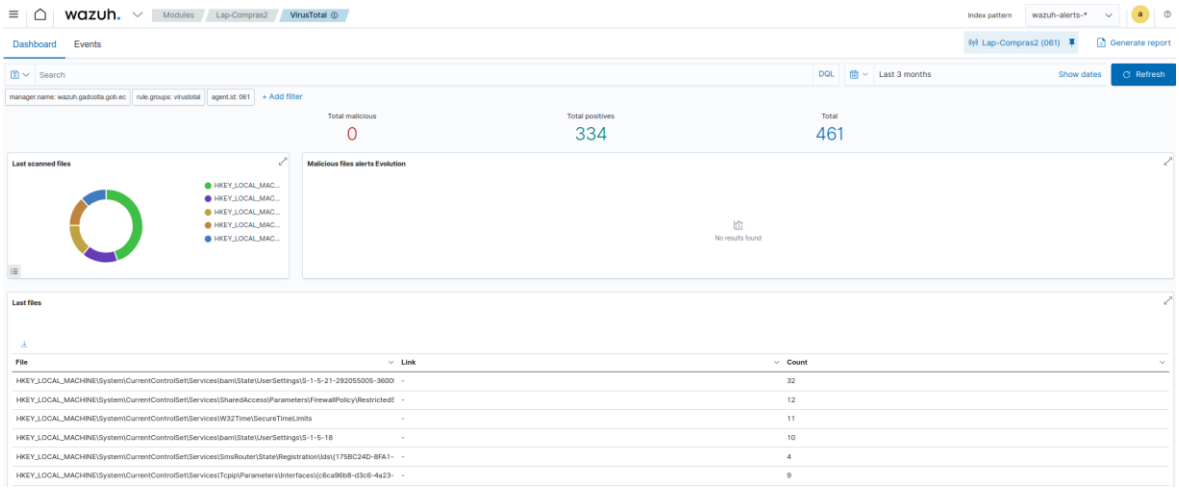
Ilustración 37. Eventos de Seguridad (Windows 10 Home)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 38 muestra que en el periodo de monitoreo no se detectaron archivos maliciosos.

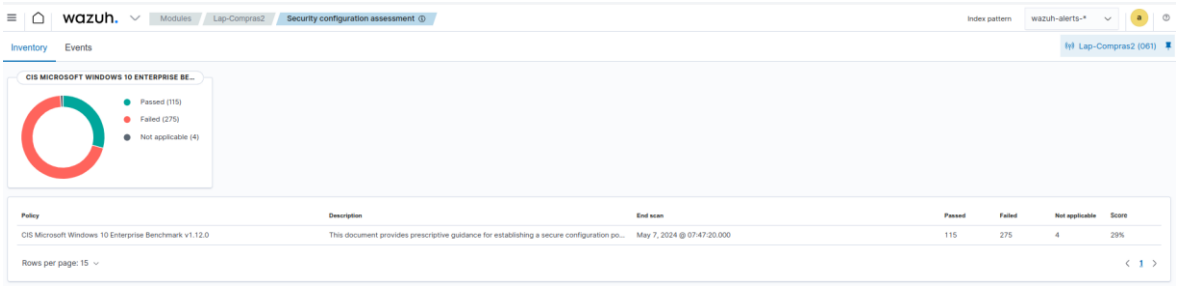
Ilustración 38. Detección de Malware (Windows 10 Home)



Fuente: elaboración propia

Con respecto a la evaluación de la configuración de seguridad de este servidor, la ilustración 39 indica que solo 115 de las 390 mejores prácticas de configuración segura pasaron exitosamente las pruebas, dando finalmente un puntaje de 29/100.

Ilustración 39. Evaluación de la configuración de seguridad (Windows 10 Home)



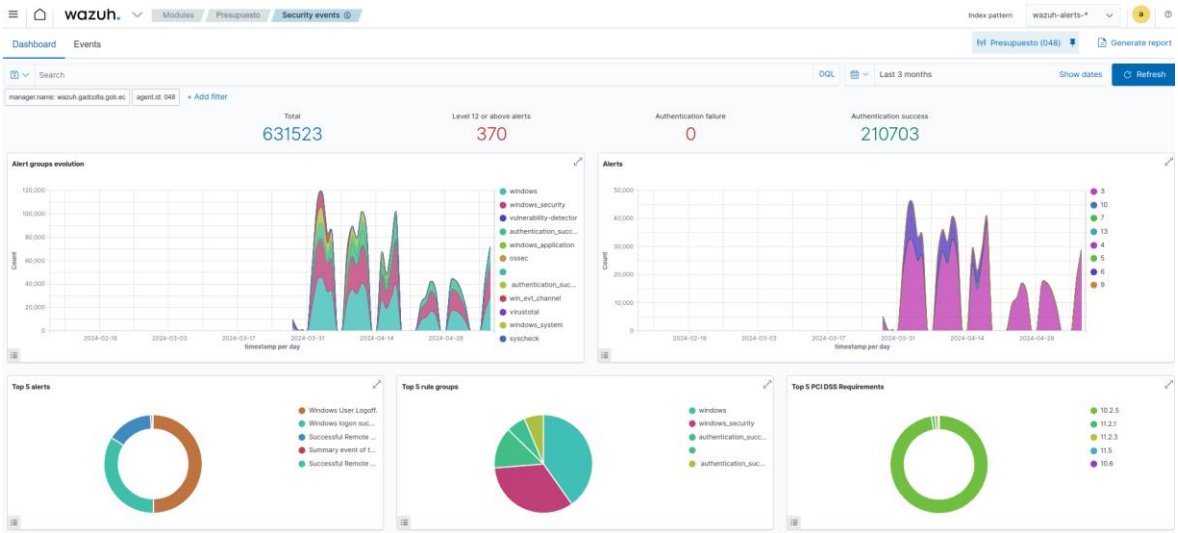
Fuente: elaboración propia

Cliente Presupuesto (Windows 8.1 Pro)

Como se observa en la ilustración 40, durante el periodo de monitoreo indicado se registraron 631523 eventos de seguridad, de estos 370 es decir el 0,06% son de

nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

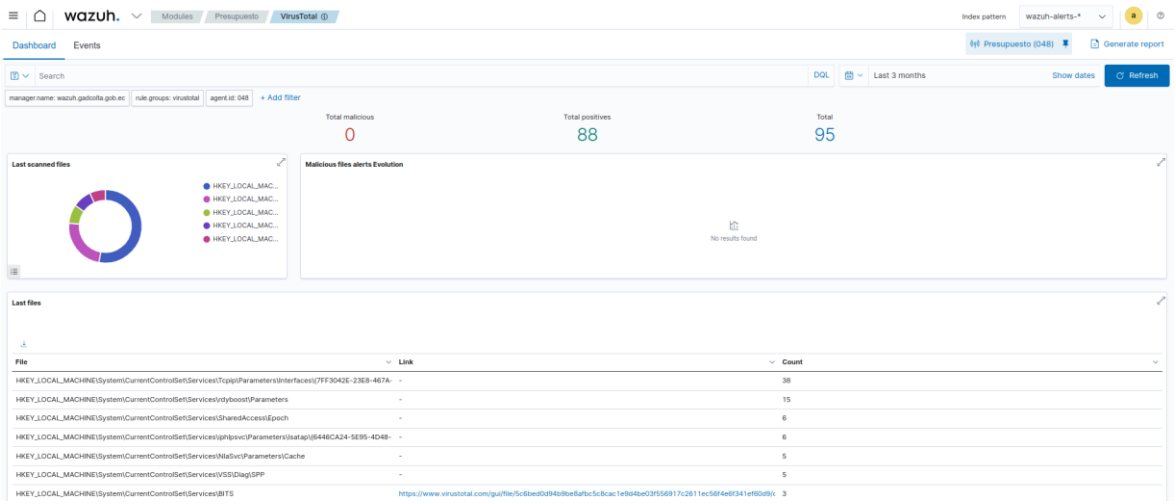
Ilustración 40. Eventos de Seguridad (Windows 8.1 Pro)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 41 muestra que en el periodo de monitoreo no se detectaron archivos maliciosos.

Ilustración 41. Detección de Malware (Windows 8.1 Pro)



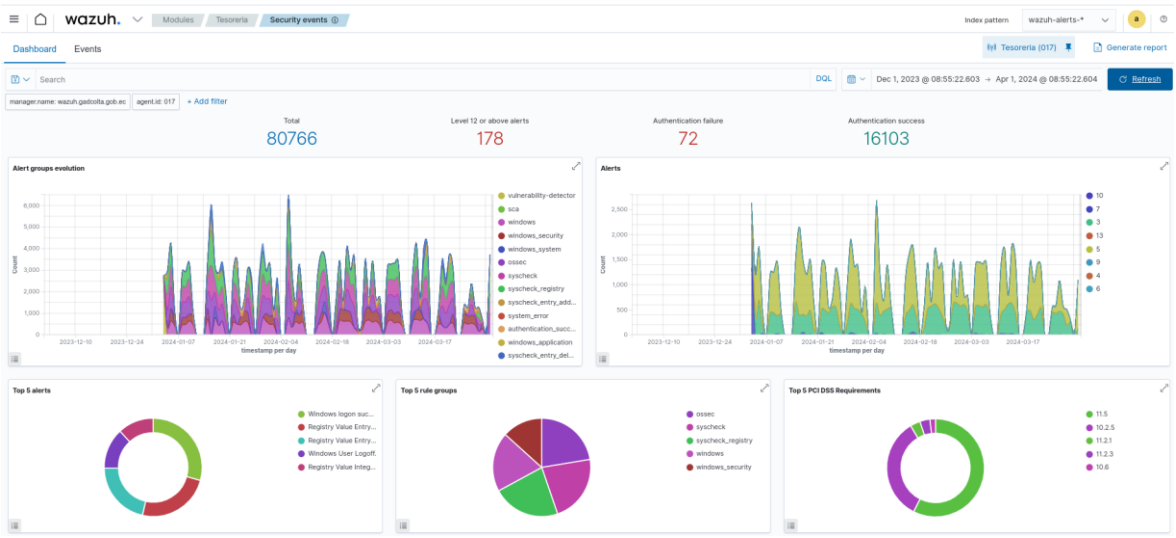
Fuente: elaboración propia

Finalmente, con respecto a la evaluación de la configuración de seguridad, la documentación de la versión actual de la plataforma Wazuh, indica que no dispone de políticas SCA para los sistemas operativos Windows 7 y Windows 8.

Cliente Tesorería (Windows 11 Pro)

Como se observa en la ilustración 42, durante el periodo de monitoreo indicado se registraron 80766 eventos de seguridad, de estos 178 es decir el 0,22% son de nivel 13 que se consideran alertas de alta importancia generalmente asociadas con un patrón de ataque común.

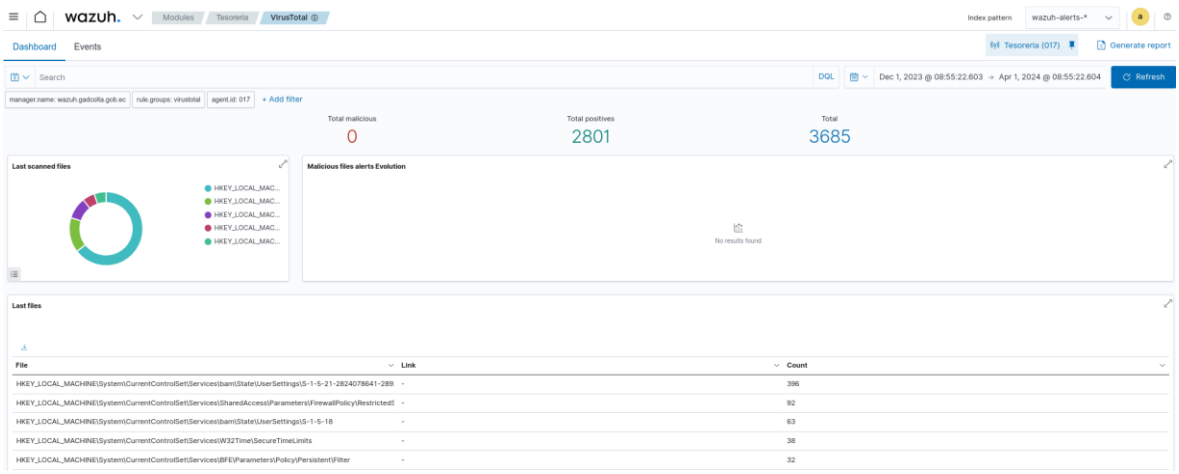
Ilustración 42. Eventos de Seguridad (Windows 11 Pro)



Fuente: elaboración propia

En cuanto a la detección de malware, la ilustración 43 muestra que en el periodo de monitoreo no se detectaron archivos maliciosos.

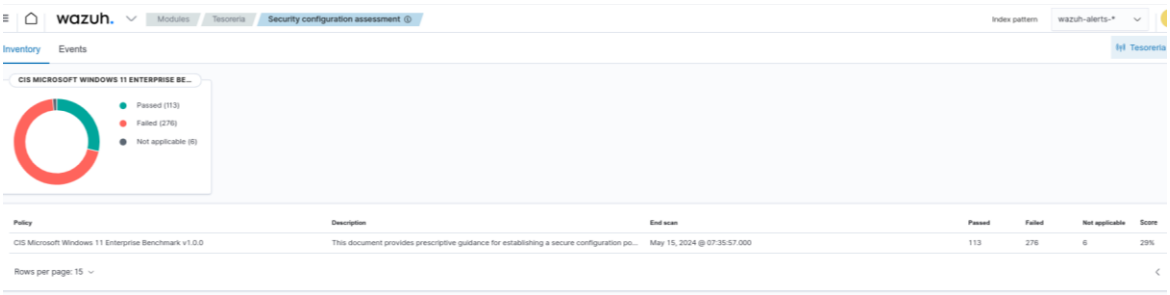
Ilustración 43. Detección de Malware (Windows 11 Pro)



Fuente: elaboración propia

Con respecto a la evaluación de la configuración de seguridad de este servidor, la ilustración 44 indica que solo 113 de las 389 mejores prácticas de configuración segura pasaron exitosamente las pruebas, dando finalmente un puntaje de 29/100.

Ilustración 44. Evaluación de la configuración de seguridad (Windows 11 Pro)



Fuente: elaboración propia

ETAPA 4. Detección de vulnerabilidades

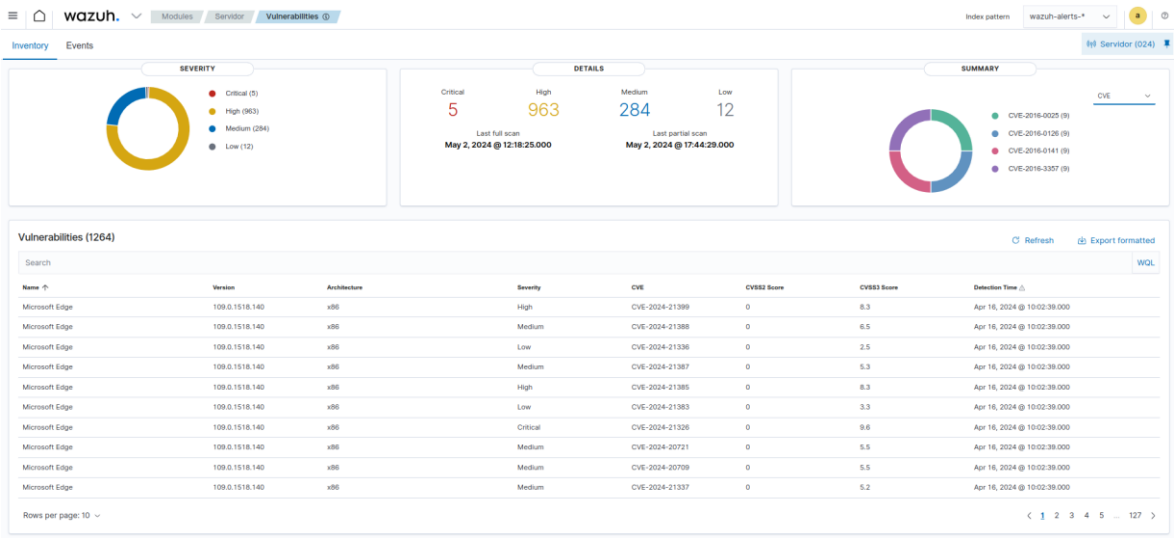
Wazuh es capaz de detectar vulnerabilidades en las aplicaciones instaladas en cada uno de los servidores y clientes de la infraestructura del GAD Colta, utilizando el módulo Vulnerability Detector. Esta auditoría de software se realiza a través de la integración de fuentes de vulnerabilidades indexadas por Canonical, Debian, Red Hat y la base de datos nacional de vulnerabilidades (NVD), que se actualiza cada hora para garantizar que se buscará los CVEs más recientes.

A continuación, se indican los resultados obtenidos mediante el detector de vulnerabilidades de WAZUH en cada uno de los servidores de la institución.

Servidor - Base de Datos

El análisis de vulnerabilidades de este servidor indica que existen 1264 vulnerabilidades de las cuales 5 son de severidad crítico y 963 de alta severidad, como se indica en la ilustración 45.

Ilustración 45. Reporte de Vulnerabilidades - Base de Datos

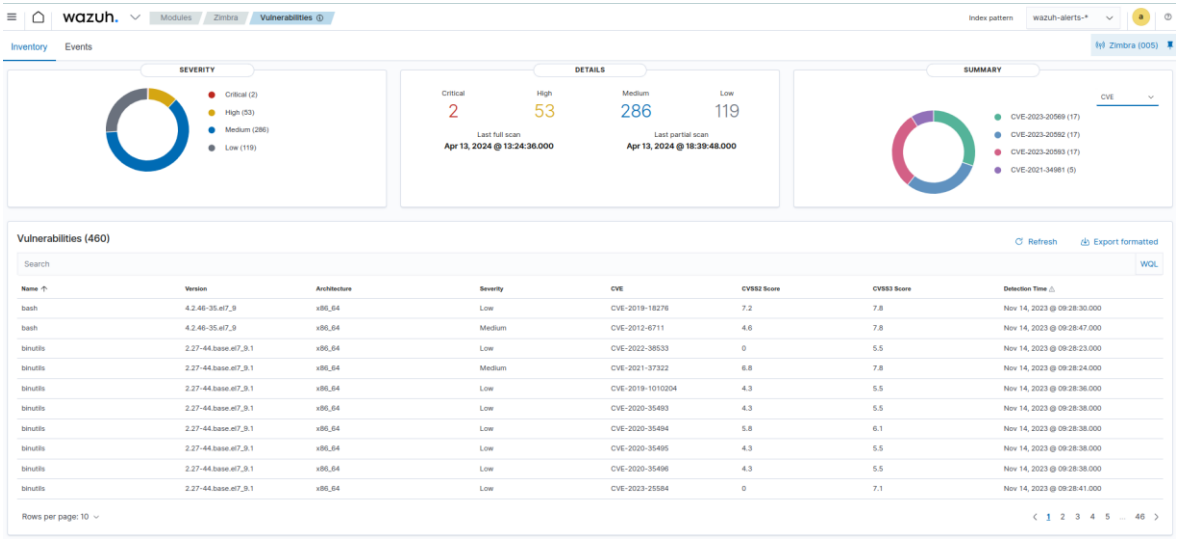


Fuente: elaboración propia

Servidor - ZIMBRA

El análisis de vulnerabilidades de este servidor indica que existen 460 vulnerabilidades de las cuales 2 son de severidad crítico y 53 de alta severidad, como se indica en la ilustración 46.

Ilustración 46. Reporte de Vulnerabilidades - Zimbra

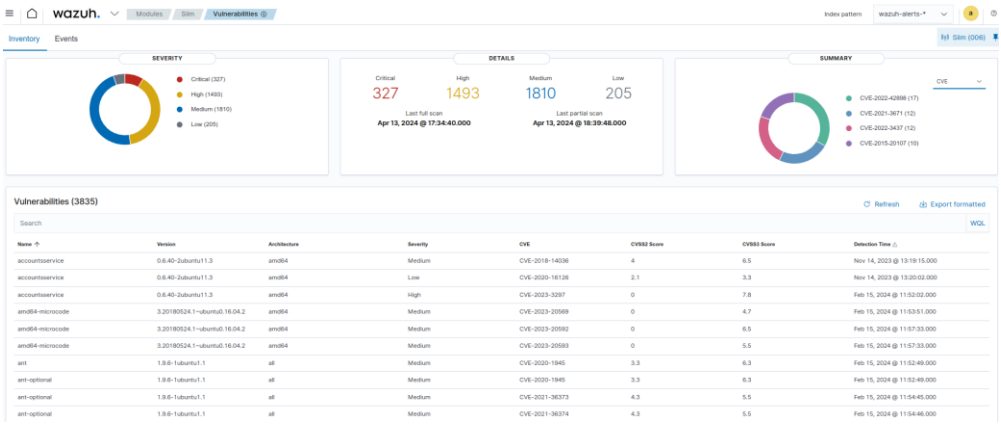


Fuente: elaboración propia

Servidor - SIIM

El análisis de vulnerabilidades de este servidor indica que existen 3835 vulnerabilidades de las cuales 327 son de severidad crítico y 1493 de alta severidad, como se indica en la ilustración 47.

Ilustración 47. Reporte de Vulnerabilidades - SIIM

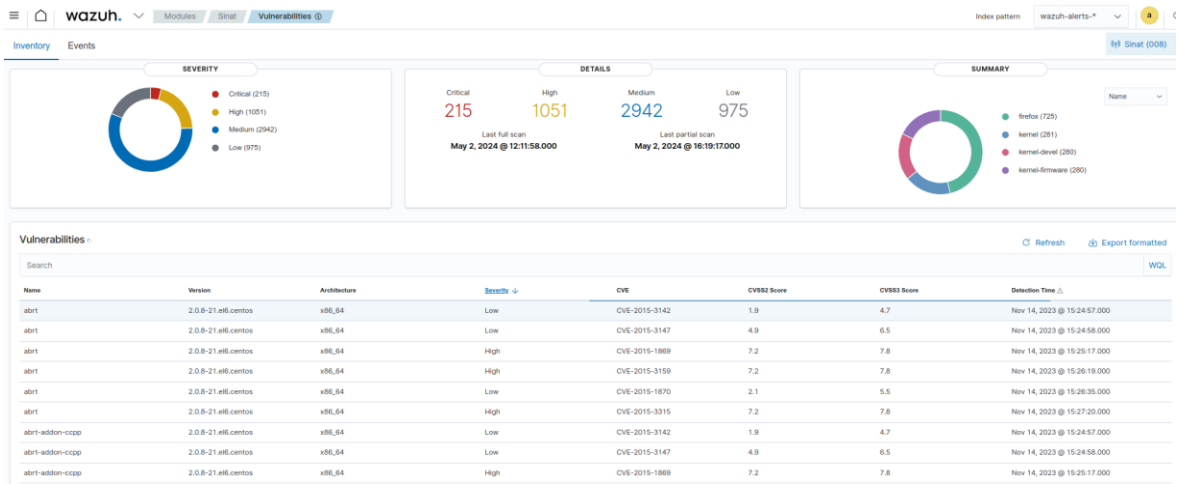


Fuente: elaboración propia

Servidor - SINAT

El análisis de vulnerabilidades de este servidor indica que existen 5183 vulnerabilidades de las cuales 215 son de severidad crítico y 1051 de alta severidad, como se indica en la ilustración 48.

Ilustración 48. Reporte de Vulnerabilidades - SINAT

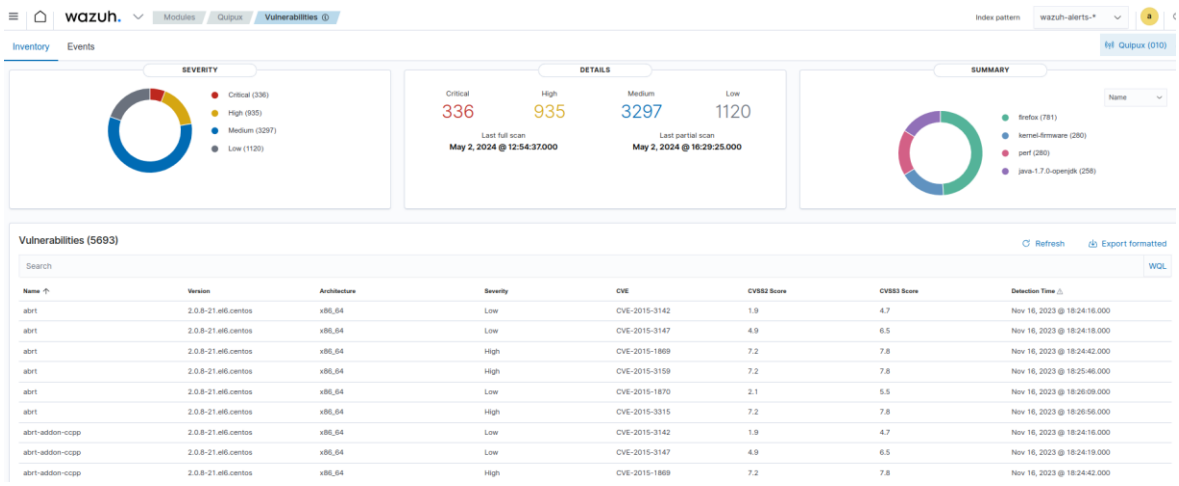


Fuente: elaboración propia

Servidor - QUIPUX

El análisis de vulnerabilidades de este servidor indica que existen 5688 vulnerabilidades de las cuales 336 son de severidad crítico y 935 de alta severidad, como se indica en la ilustración 49.

Ilustración 49. Reporte de Vulnerabilidades - QUIPUX

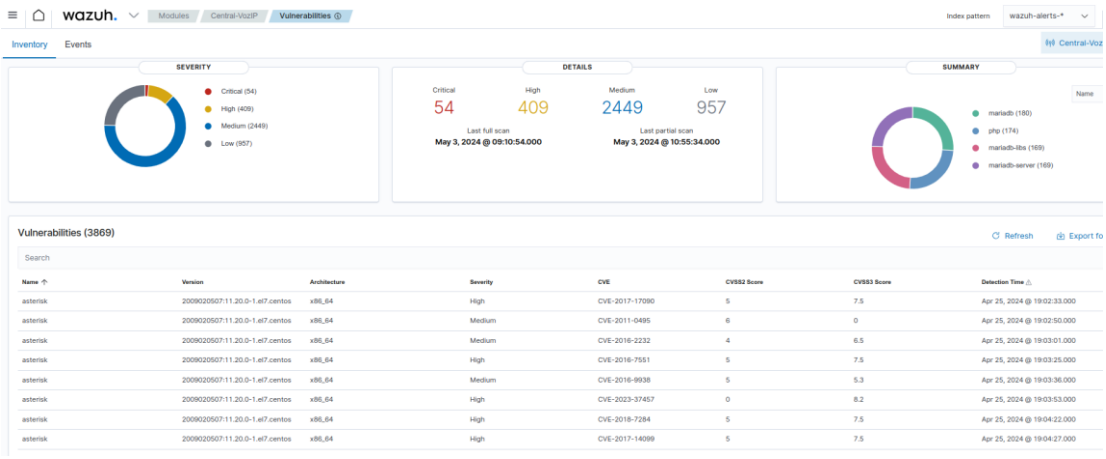


Fuente: elaboración propia

Servidor Central-VozIP

El análisis de vulnerabilidades de este servidor indica que existen 3869 vulnerabilidades de las cuales 54 son de severidad crítico y 409 de alta severidad, como se indica en la ilustración 50.

Ilustración 50. Reporte de Vulnerabilidades - Central-VozIP

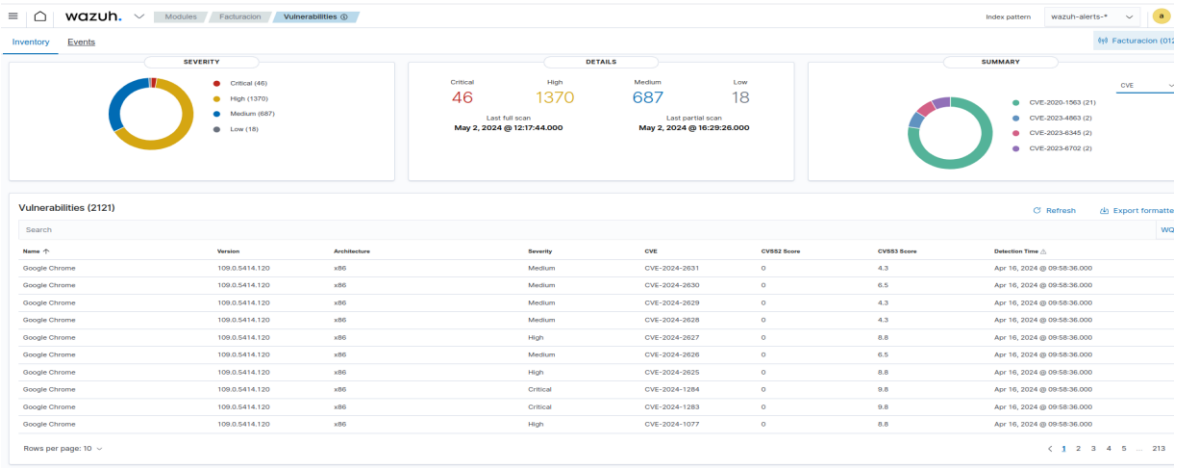


Fuente: elaboración propia

Cliente - Facturación

El análisis de vulnerabilidades de este cliente indica que existen 2121 vulnerabilidades de las cuales 46 son de severidad crítico y 1370 de alta severidad, como se indica en la ilustración 51.

Ilustración 51. Reporte de Vulnerabilidades - Facturación

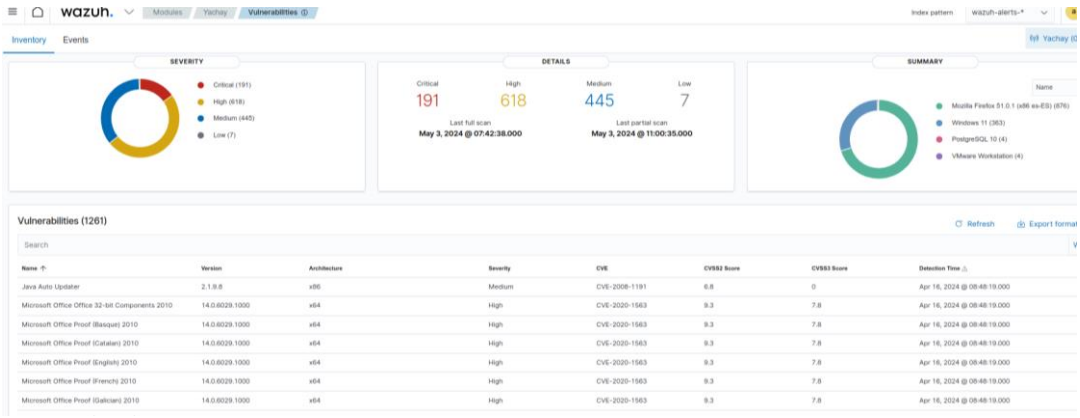


Fuente: elaboración propia

Cliente - Yachay

El análisis de vulnerabilidades de este cliente indica que existen 1261 vulnerabilidades de las cuales 191 son de severidad crítico y 618 de alta severidad, como se indica en la ilustración 52.

Ilustración 52. Reporte de Vulnerabilidades - Yachay

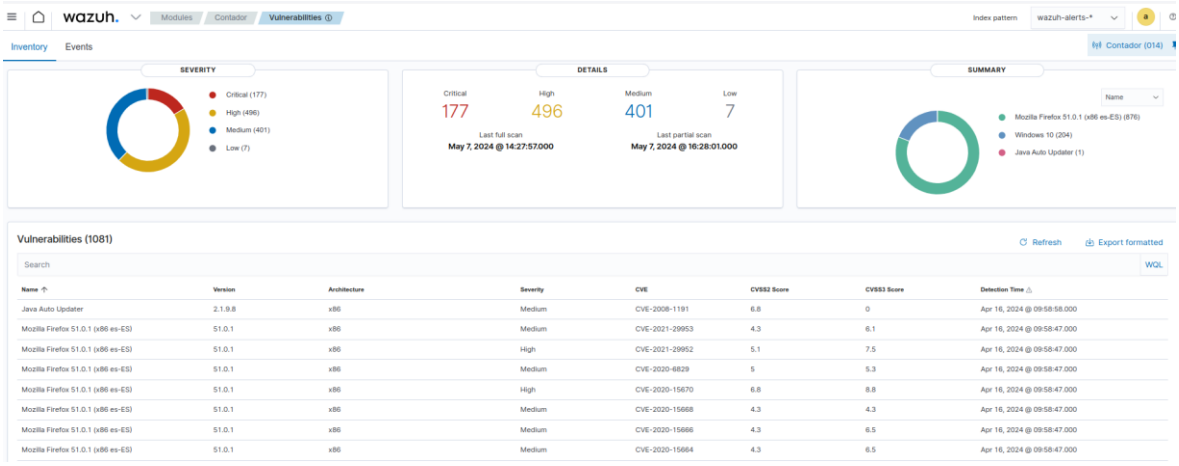


Fuente: elaboración propia

Cliente - Contador

El análisis de vulnerabilidades de este cliente indica que existen 1081 vulnerabilidades de las cuales 177 son de severidad crítico y 496 de alta severidad, como se indica en la ilustración 53.

Ilustración 53. Reporte de Vulnerabilidades - Contador

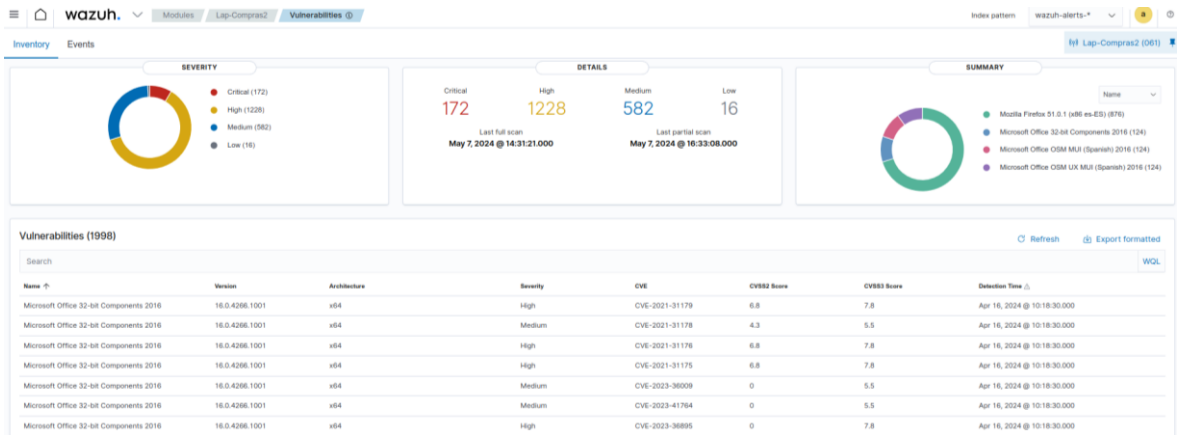


Fuente: elaboración propia

Cliente Lap-Compras2

El análisis de vulnerabilidades de este cliente indica que existen 1998 vulnerabilidades de las cuales 172 son de severidad crítico y 1228 de alta severidad, como se indica en la ilustración 54.

Ilustración 54. Reporte de vulnerabilidades - Lap-Compras2

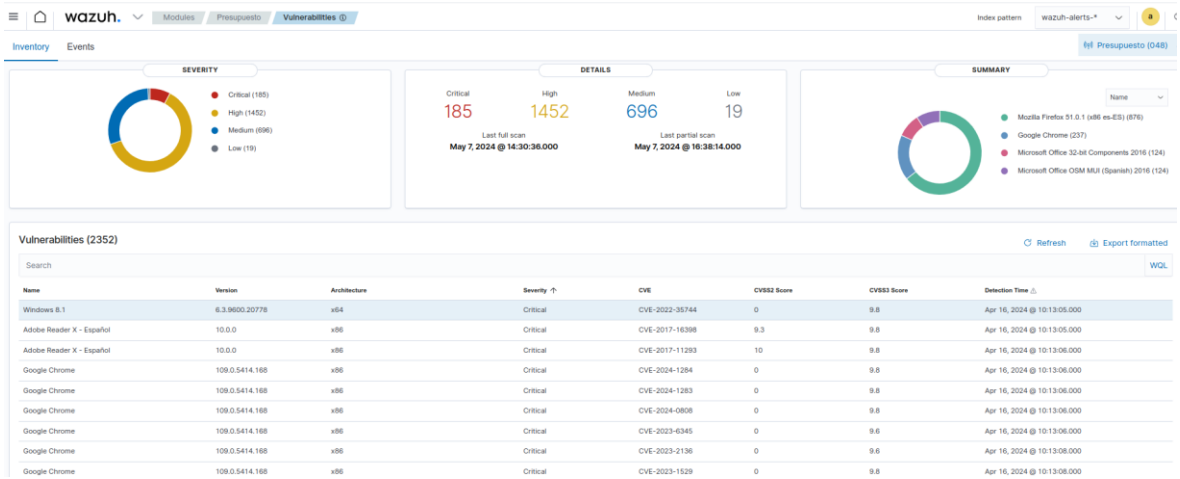


Fuente: elaboración propia

Cliente - Presupuesto

El análisis de vulnerabilidades de este cliente indica que existen 2352 vulnerabilidades de las cuales 185 son de severidad crítico y 1452 de alta severidad, como se indica en la ilustración 55.

Ilustración 55. Reporte de Vulnerabilidades - Presupuesto

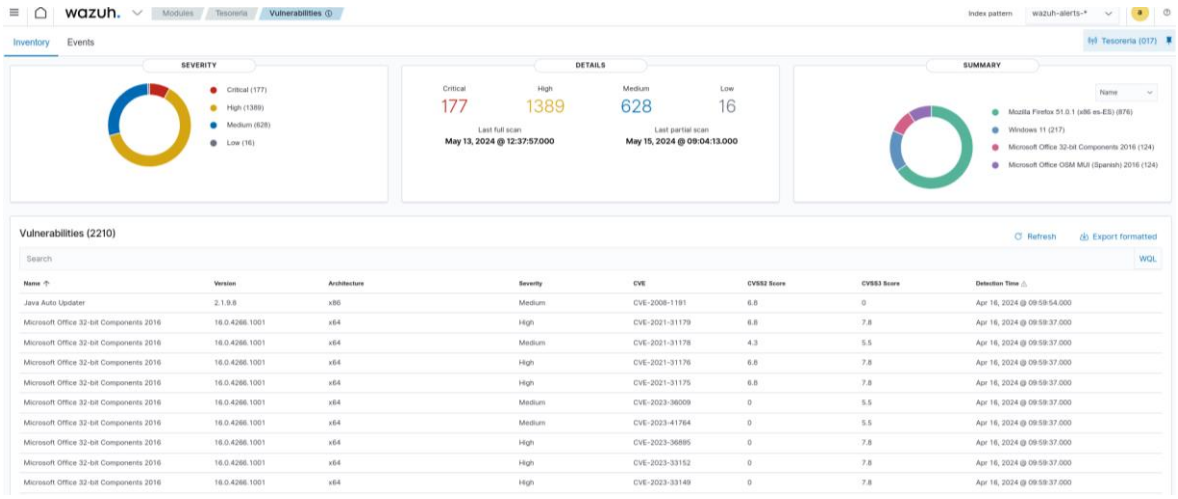


Fuente: elaboración propia

Cliente - Tesorería

El análisis de vulnerabilidades de este cliente indica que existen 2210 vulnerabilidades de las cuales 177 son de severidad crítico y 1389 de alta severidad, como se indica en la ilustración 56.

Ilustración 56. Reporte de Vulnerabilidades - Tesorería



Fuente: elaboración propia

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Luego de realizar el análisis y detección de amenazas y vulnerabilidades en los servidores y clientes de la infraestructura tecnológica del GAD Colta, la tabla 12 muestra los resultados de las vulnerabilidades de severidad crítica y de severidad alta, que podrían impactar directamente en la seguridad de los sistemas de información de la institución.

Adicional a los servidores la tabla 12 detalla las vulnerabilidades encontradas en seis clientes, que, a juicio del autor de la investigación, son los más representativos por sus actividades cotidianas relacionadas al área financiera del GAD Colta.

Tabla 12. Resumen de vulnerabilidades (01-Dic-2023 / 01-Abr-2024)

AGENTE	TIPO	NÚMERO DE VULNERABILIDADES	
		SEVERIDAD CRÍTICA	SEVERIDAD ALTA
Servidor	Servidor	5	963
Zimbra	Servidor	2	53
Siim	Servidor	327	1493
Sinat	Servidor	215	1051
Quipux	Servidor	336	935
Central-VozIP	Servidor	54	409
Facturación	Cliente	46	1370
Yachay	Cliente	191	6182
Contador	Cliente	177	496
Lap-Compras2	Cliente	172	1228
Presupuesto	Cliente	185	1452
Tesorería	Cliente	177	1389

Fuente: elaboración propia

3.1. Mitigación de vulnerabilidades

A continuación**,** se detalla las recomendaciones que se estarán ejecutando en los servidores de la infraestructura tecnológica del GAD Colta para mitigar las vulnerabilidades, de manera prioritaria, las de severidad crítico, estas requieren remediación inmediata debido a que ponen en riesgo la confidencialidad, disponibilidad e integridad de los datos de los usuarios.

Servidor de Base de Datos

Luego de analizar detenidamente las vulnerabilidades y exposiciones comunes (CVE) de severidad crítica de este servidor, la tabla 13 detalla la descripción y la solución de cada una de estas CVEs.

Tabla 13. CVE - descripción y mitigación - Servidor de base de datos

CVE	Descripción	Solución Propuesta
CVE-2024-21326	Vulnerabilidad de elevación de privilegios en Microsoft Edge (basado en Chromium)	Actualización inmediata del navegador web
CVE-2023-35618	Vulnerabilidad de elevación de privilegios en Microsoft Edge (basado en Chromium)	Actualización inmediata del navegador web
CVE-2023-6345	El desbordamiento de enteros en Skia en Google Chrome anterior a 119.0.6045.199 permitió a un atacante remoto que había comprometido el proceso de renderizado realizar potencialmente un escape de la zona de pruebas a través de un archivo malicioso	Actualización inmediata del navegador web
CVE-2023-36735	Vulnerabilidad de elevación de privilegios en Microsoft Edge (basado en Chromium)	Actualización inmediata del navegador web
CVE-2023-36397	Vulnerabilidad de ejecución remota de código (RCE) en el protocolo Pragmatic General Multicast de Windows para transportar datos de multidifusión.	Instalación inmediata de las actualizaciones de seguridad del Sistema Operativo de noviembre 2023.

Fuente: elaboración propia

Servidor Zimbra

De la misma forma, luego de analizar detalladamente las vulnerabilidades y exposiciones comunes (CVE) de severidad crítica de este servidor, la tabla 14 detalla la descripción y la solución de este CVE.

Tabla 14. CVE - Descripción y mitigación - Servidor Zimbra

CVE	Descripción	Solución Propuesta
CVE-2021-23418	Los paquetes glance anteriores a 3.2.1 son vulnerables a la inyección de entidades externas XML (XXE) mediante el uso de Fault para analizar datos XML no fiables, que se sabe que son vulnerables a ataques XML.	Actualización inmediata de la versión del programa de monitoreo glance.

Fuente: elaboración propia

Servidor SIIM

Debido a que este servidor tiene la versión 16.04.06 LTS de Ubuntu, y esta versión en abril del 2021 finalizó el soporte de las actualizaciones de seguridad, parches y nuevas funcionalidades, se recomienda actualizar de manera urgente al menos a la versión 20.04 del sistema operativo.

Servidor SINAT

De igual manera, este servidor tiene la versión 6.5 de Centos, y esta versión en noviembre del 2020 finalizó el soporte de las actualizaciones de seguridad, parches y nuevas funcionalidades, se recomienda actualizar de manera urgente a la versión 8 o 9 de Alma Linux o Rocky Linux que son sistemas operativos totalmente compatibles a Centos.

Servidor QUIPUX

De la misma forma, este servidor también tiene la versión 6.5 de Centos, y esta versión en noviembre del 2020 finalizó el soporte de las actualizaciones de seguridad, parches y nuevas funcionalidades, se recomienda actualizar de manera urgente a la versión 8 o 9 de Alma Linux o Rocky Linux que son sistemas operativos totalmente compatibles a Centos.

Servidor Central-VozIP

Luego de analizar detenidamente las vulnerabilidades y exposiciones comunes (CVE) de severidad crítica de este servidor, la tabla 15 detalla la descripción y la solución de cada una de estas CVEs.

Tabla 15. CVE - Descripción y Mitigación - Servidor Central-VozIP

CVE	Descripción	Solución Propuesta
CVE-2017-14491	Un desbordamiento de búfer basado en memoria dinámica (heap) en dnsmasq en versiones anteriores a la 2.78 permite a los atacantes provocar una denegación de servicio (cierre inesperado) o ejecutar código arbitrario utilizando una respuesta DNS manipulada.	Actualización inmediata de la versión del programa dnsmasq.
CVE-2021-45967	Problema en Pascom Cloud Phone System antes de la versión 7.20.x. Un error de configuración entre NGINX y un servidor Tomcat backend conduce a un path traversal en el servidor Tomcat, exponiendo endpoints no deseados.	Actualización inmediate del programa de mensajería instantánea openfire.
CVE-2014-1544	La vulnerabilidad Use-after-free en la función CERT_DestroyCertificate en libnss3.so en Mozilla Network Security Services (NSS) 3.x, tal como se utiliza en Firefox antes de 31.0, Firefox ESR 24.x antes de 24.7, y Thunderbird antes de 24.7, permite a atacantes remotos ejecutar código arbitrario a través de vectores que desencadenan cierta eliminación incorrecta de una estructura NSS Certificate de un dominio de confianza.	Actualización inmediata del navegador web firefox.

Fuente: elaboración propia

Además, es importante recalcar que este servidor tiene la versión 7.0 de Centos, y esta versión finalizará el soporte de las actualizaciones de seguridad, parches y nuevas funcionalidades, el 30 de junio de 2024, por lo que se recomienda actualizar el servidor a la versión 8 o 9 de Alma Linux o Rocky Linux que son sistemas operativos totalmente compatibles a Centos.

Servidor Facturación

Debido a que este servidor tiene la versión Microsoft Windows 7 Profesional SP 1, y esta versión en enero del 2020 finalizó el soporte de las actualizaciones de seguridad y parches, se recomienda actualizar de manera urgente a la versión 10 u 11 del sistema operativo.

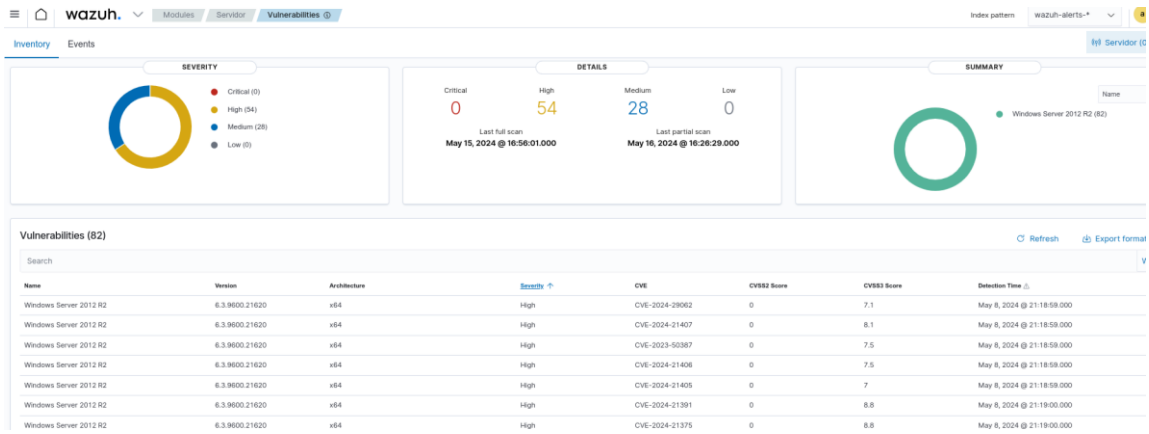
Finalmente, es muy importante recalcar que existen 65 computadores personales en la infraestructura tecnológica del GAD Colta, mismas que corresponde al 70% del total de equipos, que tienen instalado como sistema operativo, Microsoft Windows en sus versiones 7 y 8, mismas para las que el fabricante finalizó el

soporte de las actualizaciones de seguridad y parches, en enero del 2020 y en enero del 2023 respectivamente; por lo que se sugiere que a la brevedad posible se actualice este sistema operativo a su versión 10 u 11.

3.2. Validación de la propuesta de mitigación

Después de proceder a implementar cada una de las soluciones propuestas para mitigar las vulnerabilidades de los servidores y clientes seleccionados de la infraestructura tecnológica del GAD Colta, entre el **14 y el 17 de mayo del 2024**, se ejecutó nuevamente la detección de vulnerabilidades en el servidor Wazuh y se verifico que las de severidad crítica se minimizaron al máximo y en algunos casos desaparecieron, como se observa en las siguientes ilustraciones.

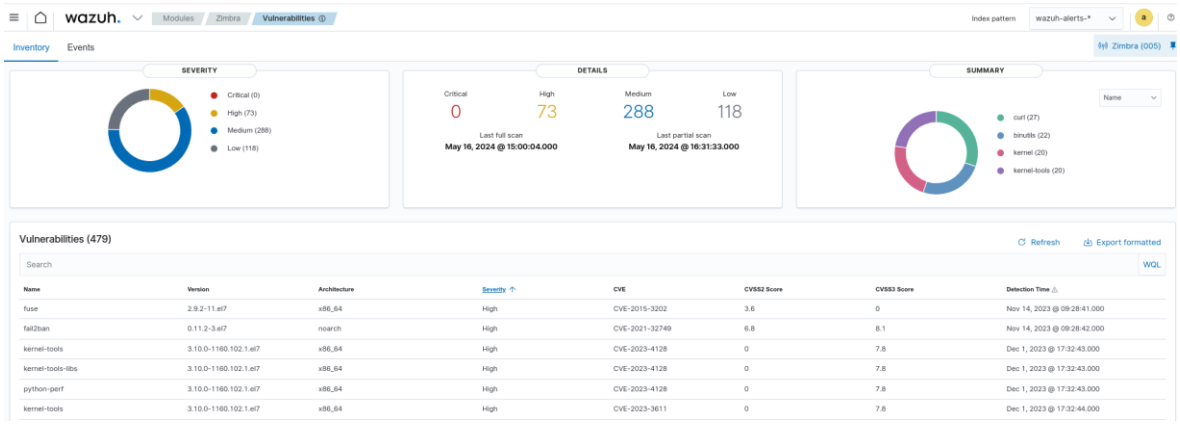
Ilustración 57. Reporte de mitigación - Servidor de Base de Datos



Fuente: elaboración propia

Como se observa en la ilustración 57, el 100% de las vulnerabilidades de severidad crítica se solucionaron.

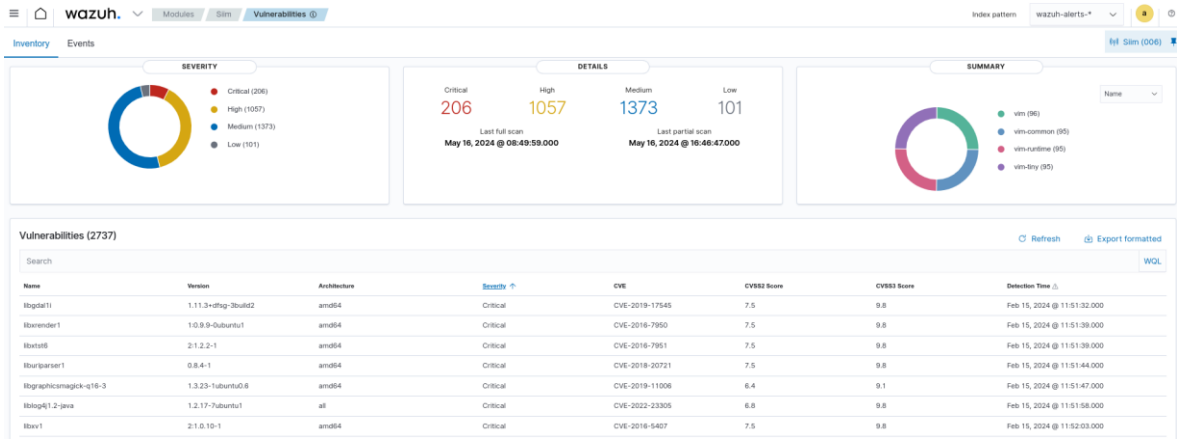
Ilustración 58. Reporte de mitigación - Servidor Zimbra



Fuente: elaboración propia

De igual forma, ilustración 58 demuestra que, el 100% de las vulnerabilidades de severidad crítica se solucionaron.

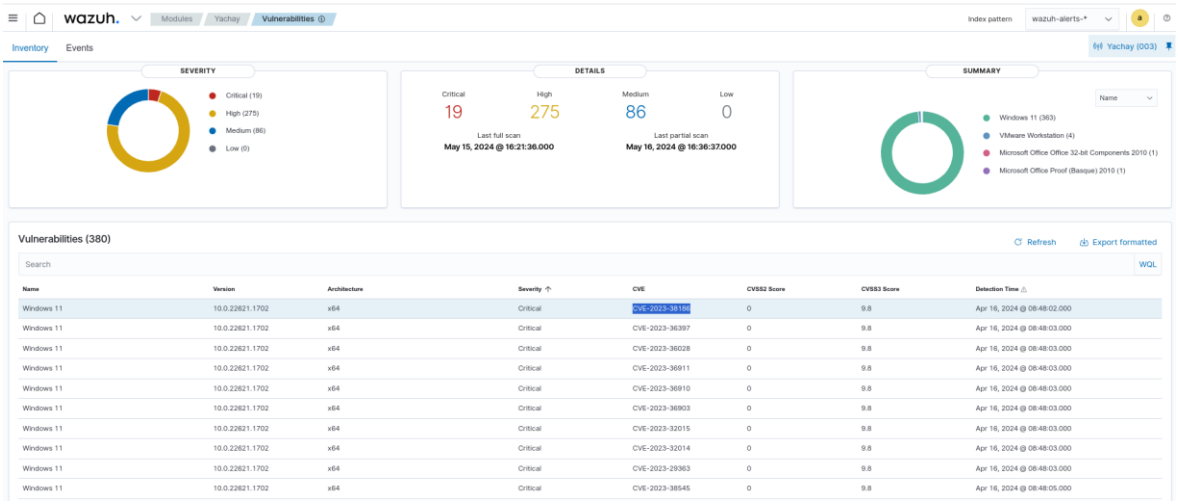
Ilustración 59. Reporte de mitigación - Servidor SIIM



Fuente: elaboración propia

En el caso de este servidor, la ilustración 59 demuestra que el 37% de las vulnerabilidades de severidad crítica, se solucionaron.

Ilustración 60. Reporte de mitigación - Cliente Yachay

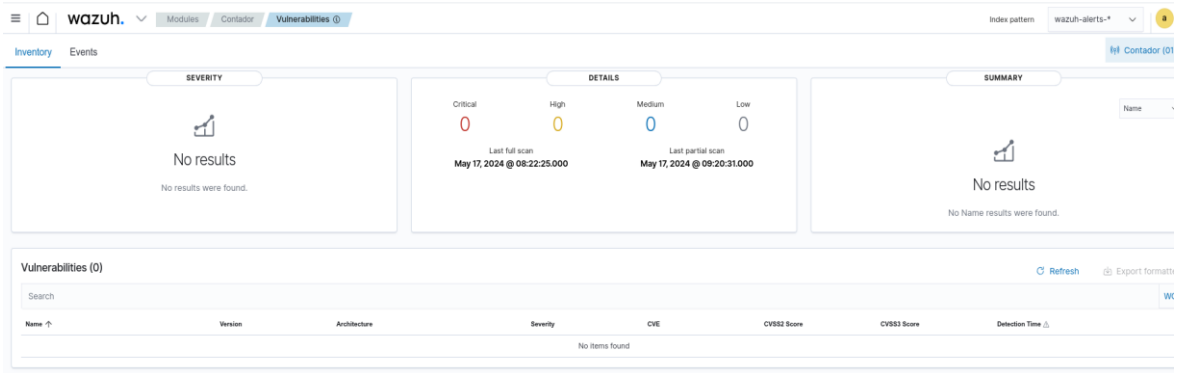


Fuente: elaboración propia

En cuanto a los resultados del cliente Yachay, en la ilustración 60 se observa que el 90 % de las vulnerabilidades de severidad crítica, se solucionaron.

Finalmente, como se observa en la ilustración 61, el 100% de las vulnerabilidades del Cliente Contador se solucionaron luego de instalar todas las actualizaciones de seguridad recomendadas por el fabricante.

Ilustración 61. Reporte de Mitigación - Cliente Contador



Fuente: elaboración propia

3.3. Respuestas activas de Wazuh

Las respuestas activas son acciones automatizadas que Wazuh ejecuta en respuesta a eventos o alertas de seguridad específicas. Estas acciones están

diseñadas para mitigar amenazas, prevenir ataques y mantener la seguridad del sistema sin intervención manual.

La funcionalidad de Extended Detection and Response (XDR) en la plataforma Wazuh y las respuestas activas están estrechamente relacionadas, ambas trabajan juntas para mejorar la capacidad de detección y respuesta ante amenazas de seguridad.

Por ejemplo, en el escenario que Wazuh se detectó múltiples intentos fallidos de inicio de sesión SSH desde una misma IP (indicando un posible ataque de fuerza bruta), se activan dos procesos en la plataforma de seguridad:

a) Proceso de Detección (XDR)

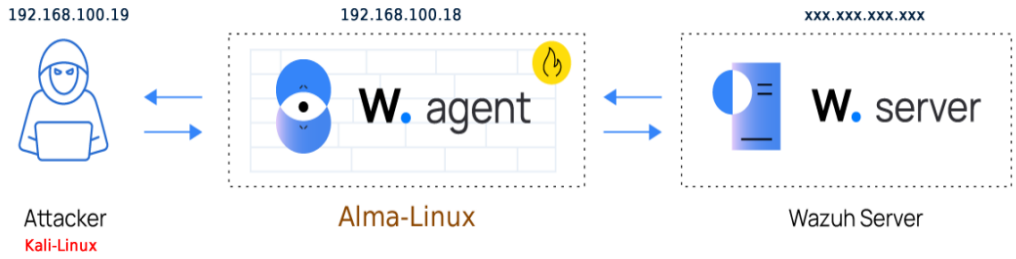
- Wazuh recoge los registros de intentos fallidos de inicio de sesión SSH.
- Analiza y correlaciona estos eventos, detectando un patrón de fuerza bruta.

b) Respuesta Activa

- Basado en la detección de XDR, Wazuh activa una respuesta activa predefinida.
- Ejecuta un script que bloquea automáticamente la IP sospechosa utilizando iptables en el servidor víctima del ataque.

Como se aprecia en la ilustración 62, para demostrar esta funcionalidad, se procedió a instalar en la infraestructura tecnológica del GAD Colta, un servidor web adicional con el sistema operativo Alma Linux 8.9 (Victima 192.168.100.18) y un cliente con la versión 2024 de Kali Linux (Atacante 192.168.100.19), posteriormente desde este dispositivo se ejecutaron ataques a este nuevo servidor, y mediante la configuración de respuestas activas en el Servidor Wazuh, se logró detectar y mitigar estos patrones de tráfico malicioso, bloqueando de manera automática la dirección IP del dispositivo atacante.

Ilustración 62. Escenario de pruebas de la tecnología XDR



Fuente: elaboración propia

La información recopilada de la ejecución exitosa de estas pruebas de concepto se detalla a continuación en la “Guía de Implementación de la Tecnología XDR en Wazuh”.

Guía de Implementación de la Tecnología XDR en Wazuh.

Objetivo

Proveer un marco detallado para la implementación de la tecnología XDR con Wauzh, en la infraestructura tecnológica del GAD COLTA, para mejorar sustancialmente la detección y respuesta a incidentes de seguridad.

Alcance

Esta guía detalla el paso a paso del proceso de instalación y configuración de la herramienta SIEM Wazuh con tecnología XDR, incluyendo pruebas y validaciones finales para la detección de los siguientes ataques más frecuentes:

1. Ataque de fuerza bruta por SSH.
2. Ataque de escaneo de puertos mediante NMAP.
3. Ataque de denegación de servicio al protocolo HTTP.

Instalación de Wazuh con tecnología XDR

Para la instalación de la plataforma WAZUH en la infraestructura tecnológica del GAD Colta, se provisiono un servidor virtual con las características indicadas en la tabla 16.

Tabla 16. Características del Servidor Wazuh

DETALLE	CARACTERÍSTICAS
Procesadores asignados	4
Memoria RAM	10 GB
Disco Duro	300 GB
Sistema operativo de 64 bits	Rocky Linux 8.8

Fuente: elaboración propia

Una vez instalado el sistema operativo recomendado, se procede a la instalación mediante CLI de las librerías y programas requeridos para la implementación y configuración de la versión 4.7 de WAZUH como se indica en la documentación oficial.

Paso 1: Actualización del sistema

Asegúrese que el sistema esté actualizado, para el mismo que se estarán ejecutando los siguientes comandos:

```
$ sudo dnf update -y
$ sudo dnf upgrade -y
```

Paso 2: Instalación de dependencias

Ejecute el siguiente comando:

```
$ sudo dnf install curl apt-transport-https unzip wget libcap2-bin software-properties-common lsb-release gnupg2
```

Paso 3: Descarga del asistente de instalación de Wazuh

Para esto ejecute el siguiente comando:

```
$ curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
```

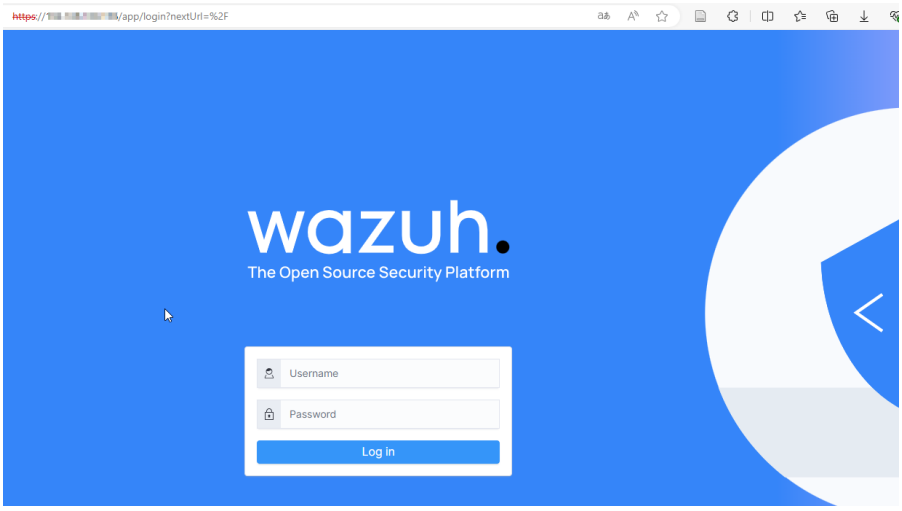
Paso 4: Ejecución del asistente de instalación de Wazuh
Ejecute el siguiente comando:

```
sudo bash ./wazuh-install.sh -a
```

El argumento -a se utiliza para que el proceso de instalación instale directamente Wazuh Indexer, Wazuh Server y Wazuh Dashboard.

El proceso de instalación automatizado se inicia de inmediato y luego al finalizar la instalación de manera exitosa, mostrara los datos de inicio de sesión; seguidamente se accederá a través de un navegador web ingresando la dirección https://<direccion-ip-wazuh-server>, evidencia conforme la ilustración 63.

Ilustración 63. Inicio de sesión de Wazuh



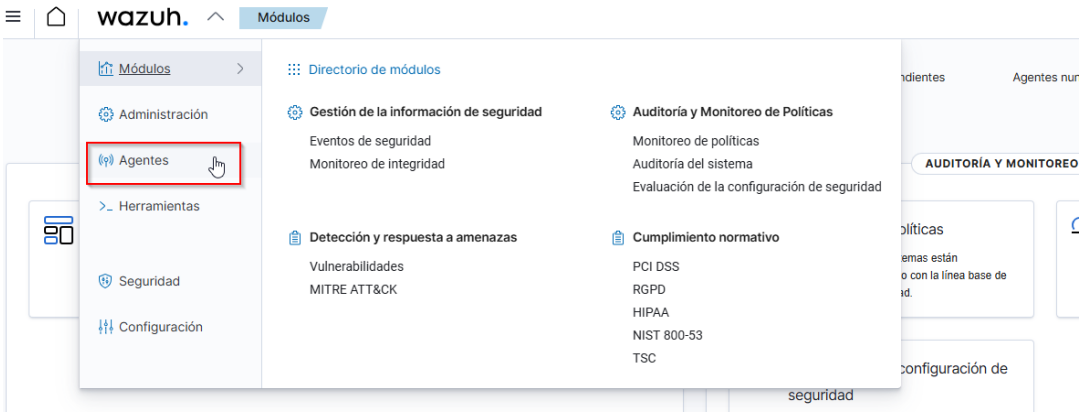
Fuente: elaboración propia

Instalación del agente Wazuh linux

Antes de instalar software agente en cada uno de los clientes a monitorear, asegúrese que el servidor Wazuh se esté ejecutando correctamente; Luego de esto se procede a la instalación del agente, siguiendo los pasos que se detallan a continuación:

1. Conforme la ilustración 64, en el panel de control de Wazuh, haga clic en el menú desplegable en la esquina superior izquierda junto al logotipo de Wazuh, luego, haga clic en "Agente".

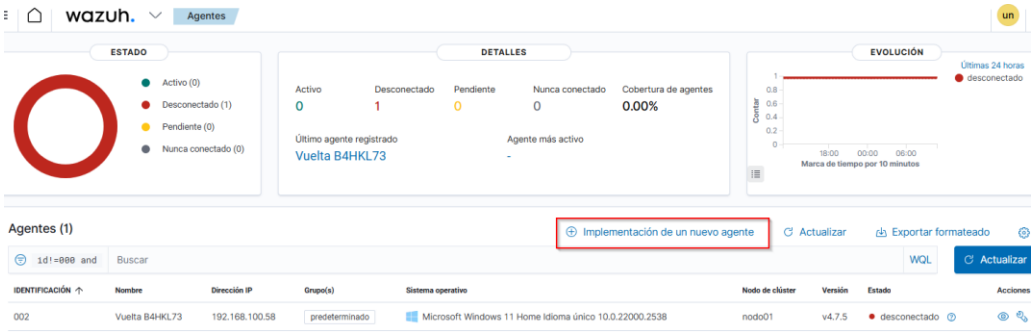
Ilustración 64. Agregar agente linux



Fuente: elaboración propia

2. Conforme la ilustración 65, haga clic en "Implementar nuevo agente".

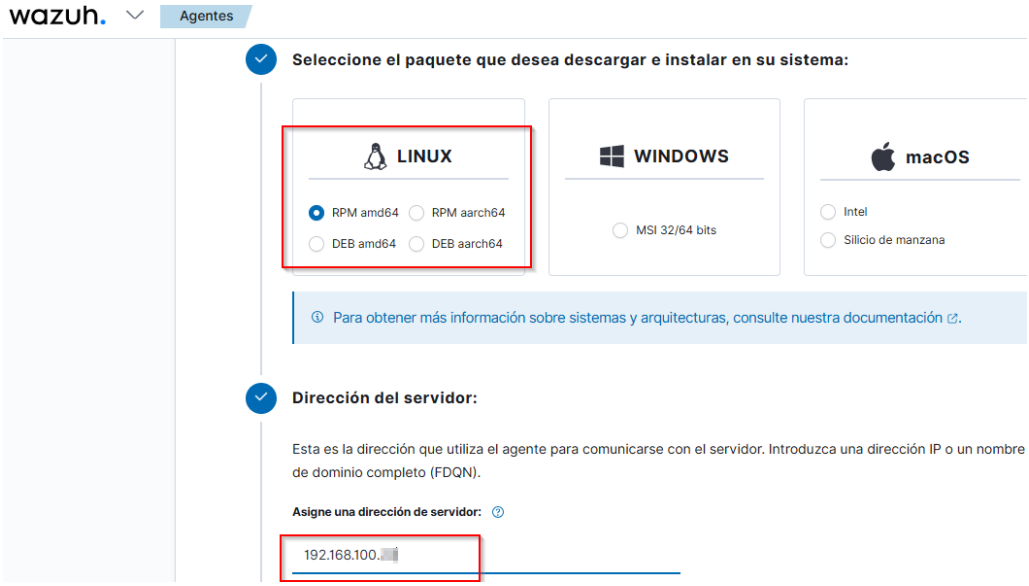
Ilustración 65. *Agregar nuevo agente en linux*



Fuente: elaboración propia

3. Conforme la ilustración 66, elija el sistema operativo del cliente en el que se desea instalar el agente wazuh, seleccione la arquitectura, especifique la dirección IP del Servidor Wazuh al que va a conectarse el agente.

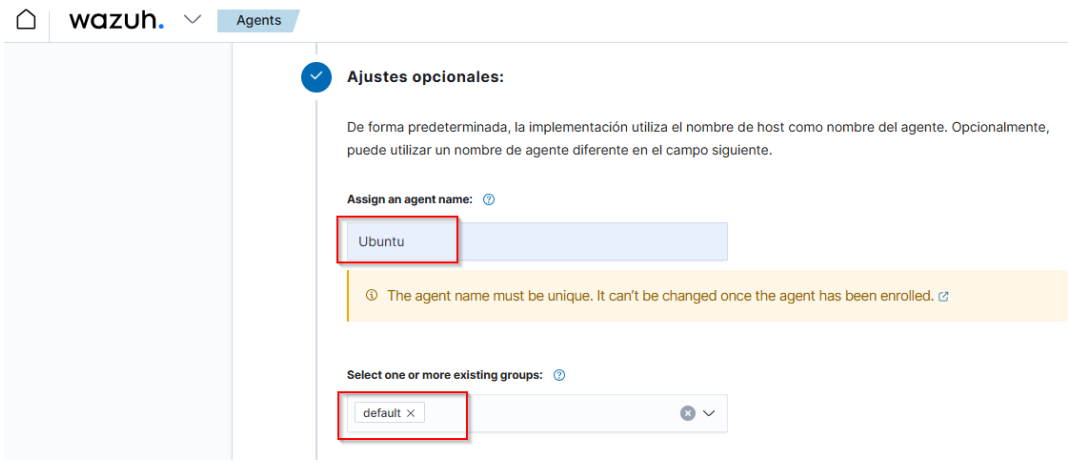
Ilustración 66. Elección de la arquitectura y servidor linux



Fuente: elaboración propia

4. Conforme la ilustración 67, especifique el nombre del agente y el grupo al que pertenece.

Ilustración 67. Definiendo el nombre y grupo del agente linux



Fuente: elaboración propia

5. Abra una consola de línea de comandos en el computador (linux) en el que va a instalar el agente y ejecute el siguiente comando:

```
curl -o wazuh-agent-4.7.4-1.x86_64.rpm
https://packages.wazuh.com/4.x/yum/wazuh-agent-4.7.4-1.x86_64.rpm && sudo
WAZUH_MANAGER='192.168.100.X' WAZUH_AGENT_GROUP='default'
WAZUH_AGENT_NAME='Ubuntu' rpm -ihv wazuh-agent-4.7.4-1.x86_64.rpm
```

6. Configure el servicio wazuh para que se ejecute cada vez que el sistema arranque, para esto ejecute los siguientes comandos:

```
$ sudo systemctl daemon-reload
$ sudo systemctl enable wazuh-agent
$ sudo systemctl start wazuh-agent
```

7. Verifique que en el panel de control del Servidor Wazuh, se muestre el nombre del agente instalado.

Instalación del agente Wazuh en Windows

De manera similar para desplegar el agente Wazuh en un cliente Windows siga los pasos que se detallan a continuación:

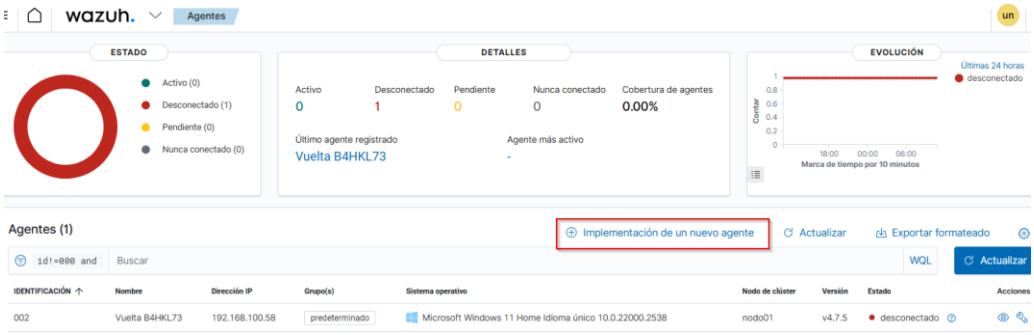
1. Conforme la ilustración 68, en el panel de control de Wazuh, haga clic en el menú desplegable en la esquina superior izquierda junto al logotipo de Wazuh, luego, haga clic en "Agente".

Ilustración 68. Agregar agente Windows

Fuente: elaboración propia

2. Conforme la ilustración 69, haga clic en "Implementar nuevo agente".

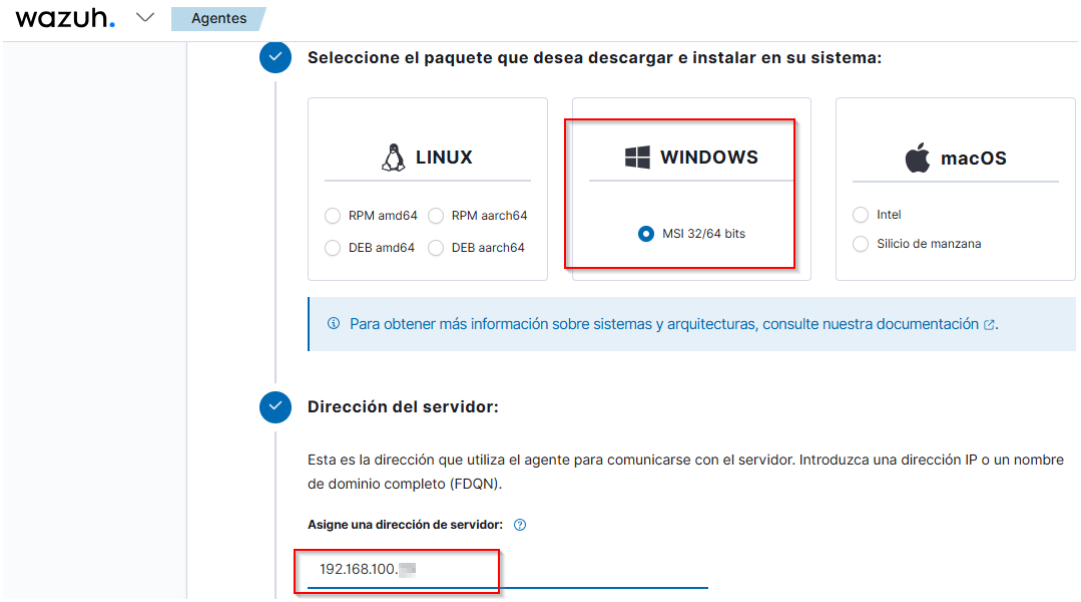
Ilustración 69. Agregar nuevo agente Windows



Fuente: elaboración propia

3. Conforme la ilustración 70, elija el sistema operativo del cliente en el que se desea instalar el agente wazuh, seleccione la arquitectura, especifique la dirección IP del Servidor Wazuh al que va a conectarse el agente.

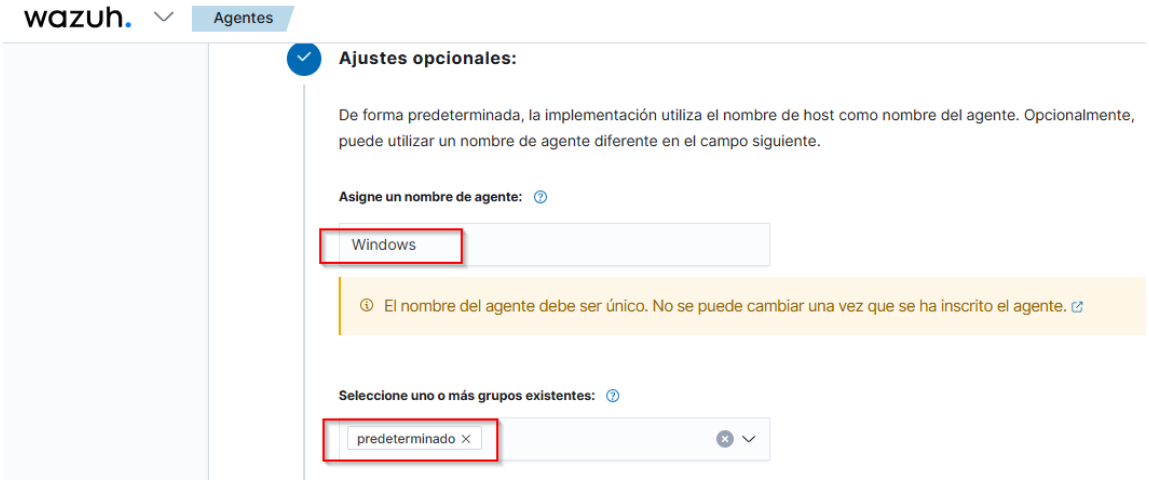
Ilustración 70. Elección de la arquitectura y servidor Windows



Fuente: elaboración propia

4. Conforme la ilustración 71, especifique el nombre del agente y el grupo al que pertenece.

Ilustración 71. Definiendo el nombre y grupo del agente Windows



Fuente: elaboración propia

5. Abra una consola de línea de comandos de Powershell en el computador (Windows) en el que va a instalar el agente y ejecute el siguiente comando:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.4-1.msi -OutFile ${env.tmp}\wazuh-agent; msiexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.100.X WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Windows' WAZUH_REGISTRATION_SERVER='192.168.100.X'
```

6. Configure el servicio wazuh para que se ejecute cada vez que el sistema arranque, para esto ejecute los siguientes comandos:

```
NET START WazuhSvc
```

7. Verifique que en el panel de control del Servidor Wazuh, se muestre el nombre del agente instalado.

Integración con API Slack

La integración de Slack con Wazuh permite recibir notificaciones en tiempo real de los eventos y alertas de seguridad generados por Wazuh directamente en los canales de Slack. A continuación, se detallan los pasos necesarios para configurar esta integración:

1. Acceder a la API de Slack

   - ✓ Ingrese al sitio web https://api.slack.com/apps y haga clic en "Create New App

2. Configurar la Aplicación

   - ✓ Seleccione "From scratch".
   - ✓ Dele un nombre a la aplicación y seleccione el espacio de trabajo donde quiere integrarla.
   - ✓ Haz clic en "Create App".

3. Configurar el Webhook entrante

   - ✓ Seleccione "Incoming Webhooks",
   - ✓ Active la opción "Activate Incoming Webhooks".
   - ✓ Haga clic en "Add New Webhook to Workspace".
   - ✓ Seleccione el canal de Slack donde desea recibir las notificaciones de Wazuh y haga clic en "Allow".

4. Obtenga el URL del Webhook

   - ✓ Copie la URL del Webhook generado. Este será necesario para configurar Wazuh.

5. Configuración de la Integración en Wazuh

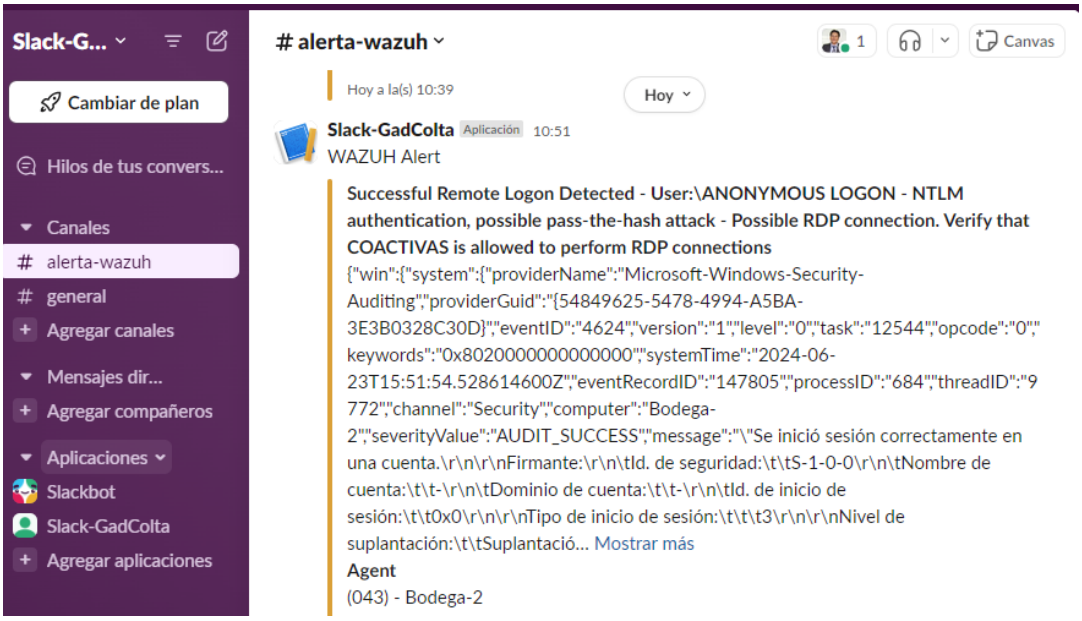
- ✓ Acceda al panel de control de Wazuh
- ✓ Edite el archivo de configuración de Wazuh server: /var/ossec/etc/ossec.conf e incluya un bloque de configuración como el siguiente.

```
<integration>
 <name>slack</name>
<hook_url>https://hooks.slack.com/services/nombre_servicio</hook_url>
 <level>10</level>
 <alert_format>json</alert_format>
 <group>ossec</group>
 </integration>
```

Reemplace https://hooks.slack.com/services/nombre_del_servicio, con la URL del “webhook entrante”.

Después de unos segundos empezará a llegará al canal configurado, por ejemplo, #Alertas-Wazuh, del espacio de trabajo las notificaciones con el nivel de alerta indicado, como podemos ver en la siguiente ilustración.

Ilustración 72. Panel de alertas con Slack



Fuente: elaboración propia

Integración con API Virustotal

Integrar VirusTotal con Wazuh le permitirá analizar archivos y URLs sospechosos detectados por Wazuh mediante los servicios de escaneo y análisis de VirusTotal. A continuación, se describen los pasos necesarios para configurar esta integración:

1. Obtener el API key de Virustotal

   - ✓ Acceda a https://www.virustotal.com y regístrece o inicie sesión en su cuenta.
   - ✓ Vaya la sección de "API Key".
   - ✓ Copie el API Key, dato necesario para configurar Wazuh.

2. Configure la integración de VirusTotal en el Server Wazuh, para ello, edite el archivo /var/ossec/etc/ossec.conf y añada las siguientes líneas:

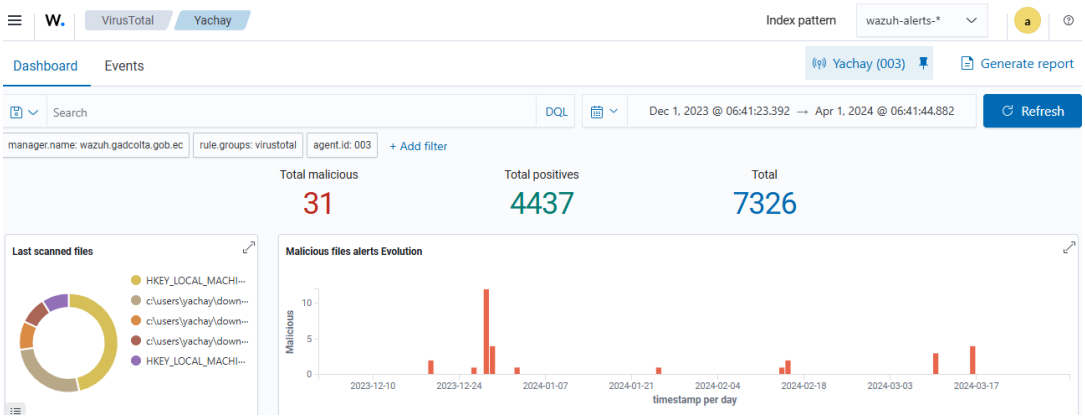
```
<integration>
 <name>virustotal</name>
 <api_key>API_KEY</api_key>
 <group>syscheck</group>
 <alert_format>json</alert_format>
</integration>
```

3. Reinicie el servicio wazuh-manager, para ello ejecute el siguiente comando:

```
$ sudo systemctl restart wazuh-manager
```

   Posteriormente conforme la ilustración 73, en el panel de control de wazuh server podemos evidenciar las detecciones realizadas por Virutotal.

Ilustración 73. Módulo de detección de alertas con Virustotal



Fuente: elaboración propia

Ataque de fuerza bruta al protocolo SSH

1. En el servidor Wazuh, se verifica que el bloque de configuración del script firewall-drop este en activo en el archivo /var/ossec/etc/ossec.conf.

```
<command>
<name>firewall-drop</name>
<executable>firewall-drop</executable>
<timeout_allowed>yes</timeout_allowed>
</command>
```

2. Añada el bloque **<active-response>** como se muestra a continuación, en el archivo de configuración /var/ossec/etc/ossec.conf del servidor Wazuh:

```
<ossec_config>
 <active-response>
 <command>firewalld-drop</command>
 <location>local</location>
 <rules_id>5763</rules_id>
 <timeout>3600</timeout>
 </active-response>
</ossec_config>
```

La configuración anterior especifica cuánto tiempo estará vigente la acción de respuesta activa. En este caso específico, el módulo bloquea durante 60 minutos la dirección IP del dispositivo que está llevando a cabo el ataque de fuerza bruta al protocolo SSH, y que está definido en la regla 5763.

3. Acceda al dispositivo atacante (Kali Linux) y verifica conectividad hasta el servidor víctima del ataque (Server Alma-Linux), como se muestra en la ilustración 74.

Ilustración 74. Prueba de conectividad

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.100.18 -c 10
PING 192.168.100.18 (192.168.100.18) 56(84) bytes of data.
64 bytes from 192.168.100.18: icmp_seq=1 ttl=64 time=0.483 ms
64 bytes from 192.168.100.18: icmp_seq=2 ttl=64 time=0.317 ms
64 bytes from 192.168.100.18: icmp_seq=3 ttl=64 time=0.314 ms
64 bytes from 192.168.100.18: icmp_seq=4 ttl=64 time=0.323 ms
64 bytes from 192.168.100.18: icmp_seq=5 ttl=64 time=0.323 ms
64 bytes from 192.168.100.18: icmp_seq=6 ttl=64 time=0.316 ms
64 bytes from 192.168.100.18: icmp_seq=7 ttl=64 time=0.344 ms
64 bytes from 192.168.100.18: icmp_seq=8 ttl=64 time=0.332 ms
64 bytes from 192.168.100.18: icmp_seq=9 ttl=64 time=0.294 ms
64 bytes from 192.168.100.18: icmp_seq=10 ttl=64 time=0.320 ms

--- 192.168.100.18 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9204ms
rtt min/avg/max/mdev = 0.294/0.336/0.483/0.050 ms

┌──(kali㉿kali)-[~]
```

Fuente: elaboración propia

4. Ejecute el ataque de fuerza bruta utilizando la herramienta hydra como se muestra en la ilustración 75.

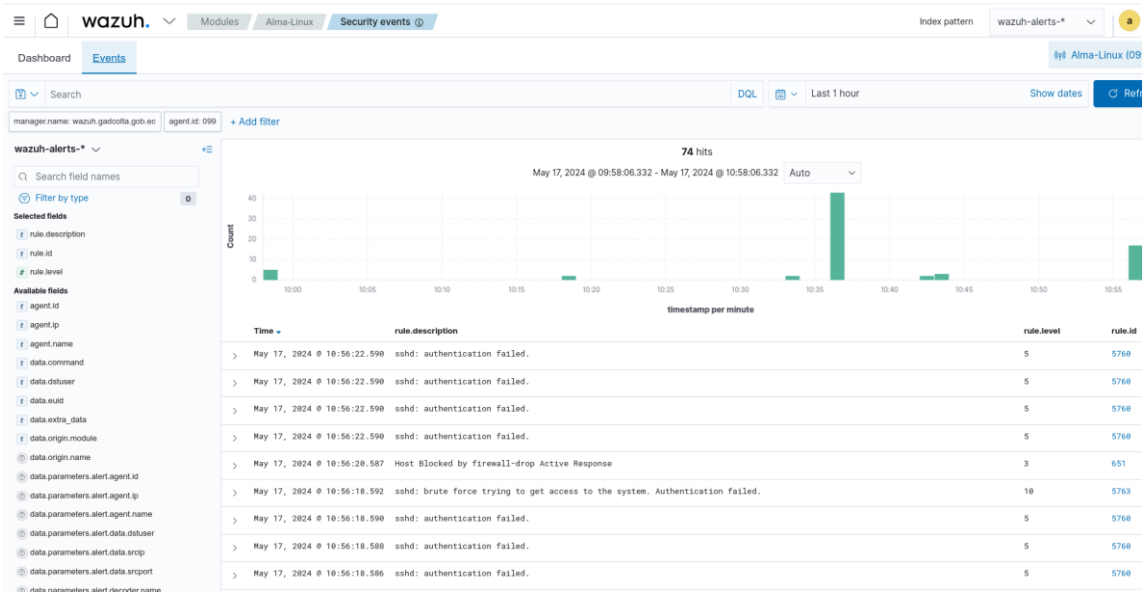
Ilustración 75. Ataque de fuerza bruta al protocolo SSH

```
┌──(kali㉿kali)-[~]
└─$ sudo hydra -t 4 -l root -P passlist.txt 192.168.100.18 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
 for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-17 10:56:12
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14 login tries (l:1/p:14), ~4 tries per task
[DATA] attacking ssh://192.168.100.18:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-17 10:56:53

┌──(kali㉿kali)-[~]
```

Fuente: elaboración propia

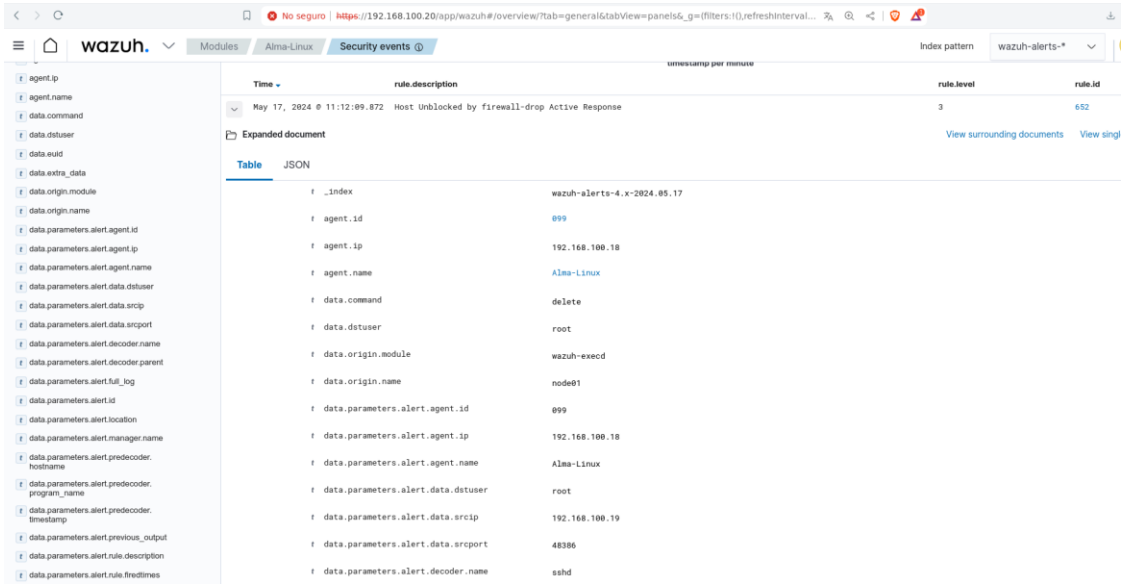
5. Como se observa en las ilustraciones 76, 77, 78, 79 y 80; Wazuh detecto el evento de seguridad y ejecuto inmediatamente la respuesta activa que se configuro en el paso # 2.

Ilustración 76. Detección del evento de seguridad



Fuente: elaboración propia

Ilustración 77. Detalle del patrón de tráfico detectado



Fuente: elaboración propia

Ilustración 78. *Prueba de conectividad al servidor no exitosa*

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.100.18 -c 10
PING 192.168.100.18 (192.168.100.18) 56(84) bytes of data.

--- 192.168.100.18 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9208ms


┌──(kali㉿kali)-[~]
```

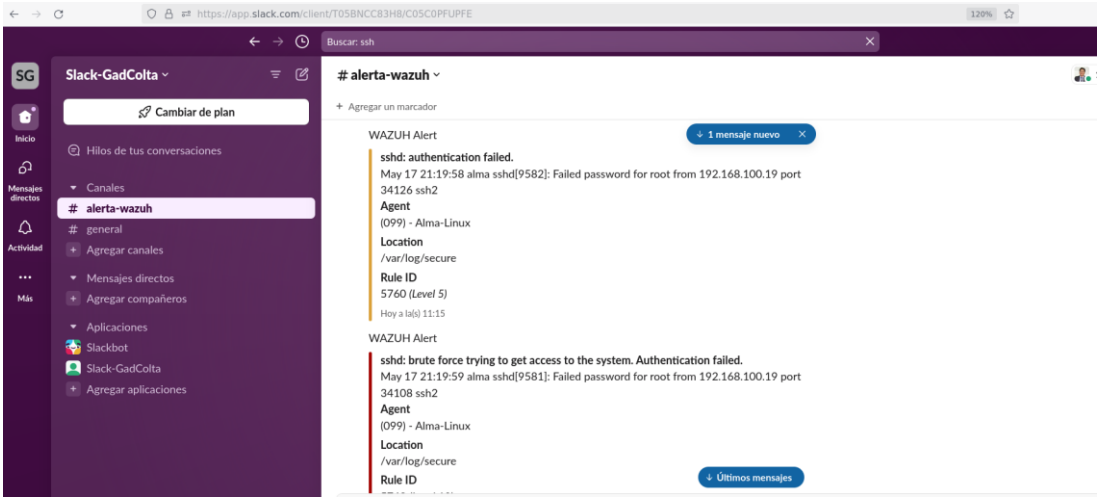
Fuente: elaboración propia

Ilustración 79. Reglas Creadas Automáticamente en el Firewall

```
[root@alma ~]#
[root@alma ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.100.19       anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.100.19       anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@alma ~]#
```

Fuente: elaboración propia

Ilustración 80. Alerta de Detección del Ataque en la plataforma Slack



Fuente: elaboración propia

Ataques de escaneo de puertos mediante NMAP y Denegación de Servicios

Para la detección de los ataques de denegación de servicio y del escaneo de puertos con NMAP, se integró Suricata a Wazuh. Suricata es un sistema de detección de intrusiones (IDS) y prevención de intrusiones (IPS) de código abierto que analiza el tráfico de red en tiempo real. Detectar una amplia gama de actividades sospechosas, incluidas las firmas de ataques DoS y las técnicas de escaneo de puertos.

Una vez instalado Suricata y actualizada sus reglas de detección, se procedió a realizar lo que a continuación se detalla:

1. En el servidor Wazuh, se crea un grupo de agentes llamado Suricata, ejecutando la siguiente instrucción:

```
$ sudo /var/ossec/bin/agent_groups -a -g Suricata -q
```

2. Determine la identificación (ID) de cada uno de los agentes que se requiere añadir al grupo Suricata, para ello ejecute la siguiente instrucción:

```
$ sudo /var/ossec/bin/manage_agents -l
```

3. Incluya el identificador del agente al grupo Suricata utilizando el siguiente comando.

```
$ sudo /var/ossec/bin/agent_groups -a -i <AGENT_ID> -g Suricata -q
```

4. Añada la siguiente configuración al archivo de configuración del agente compartido del grupo Suricata.

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

5. Configurar un decodificador personalizado en Wazuh para mapear el campo src_ip de los logs de suricata al campo srcip del script firewalld-drop. Añada esta configuración en el archivo /var/ossec/etc/decoders/local_decoder.xml.

```
<decoder name="json">
 <prematch>^{\s*"</prematch>
</decoder>
<decoder name="json_child">
 <parent>json</parent>
 <regex type="pcre2">"src_ip":"([^"]+)"</regex>
 <order>srcip</order>
</decoder>
<decoder name="json_child">
 <parent>json</parent>
 <plugin_decoder>JSON_Decoder</plugin_decoder>
</decoder>
```

6. Añada en el servidor Wazuh reglas personalizadas para detectar el uso del motor de scripting Nmap, y el ataque GoldenEye DoS desde las alertas de Suricata. Estas reglas serán utilizadas por el módulo de respuesta activa para ejecutar el script firewall-drop en el agente Alma-Linux. Este script añade la dirección IP maliciosa a la lista de bloqueos del firewall en el agente monitoreado.

   Estas reglas personalizadas se añaden en el archivo de configuración /var/ossec/etc/rules/local_rules.xml, como se muestra a continuación.

```
<group name="custom_active_response_rules,">
 <rule id="100200" level="12">
 <if_sid>86600</if_sid>
 <field name="event_type">^alert$</field>
 <match>ET DOS Inbound GoldenEye DoS attack</match>
 <description>El Ataque DOS GoldenEye se ha detectado </description>
 <mitre>
 <id>T1498</id>
 </mitre>
 </rule>

 <rule id="100201" level="12">
 <if_sid>86600</if_sid>
 <field name="event_type">^alert$</field>
 <match>ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)</match>
 <description>Detectado el motor de scripting de NMAP. </description>
 <mitre>
 <id>T1595</id>
 </mitre>
 </rule>
</group>
```

7. En el servidor Wazuh, se verifica que el bloque de configuración del script firewall-drop este en activo en el archivo /var/ossec/etc/ossec.conf.

```
<command>
<name>firewall-drop</name>
<executable>firewall-drop</executable>
<timeout_allowed>yes</timeout_allowed>
</command>
```

8. Añada el bloque **<active-response>** como se muestra a continuación, en el archivo de configuración /var/ossec/etc/ossec.conf.

```
<ossec_config>
 <active-response>
 <command>firewalld-drop</command>
 <location>local</location>
 <rules_id>5763, 10200, 102001</rules_id>
 <timeout>3600</timeout>
 </active-response>
</ossec_config>
```

9. Acceda al dispositivo atacante (Kali Linux) y verifica conectividad hasta el servidor víctima del ataque (Server Alma-Linux), como se muestra en la ilustración 81.

Ilustración 81. Prueba de conectividad

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.100.18 -c 10
PING 192.168.100.18 (192.168.100.18) 56(84) bytes of data.
64 bytes from 192.168.100.18: icmp_seq=1 ttl=64 time=0.483 ms
64 bytes from 192.168.100.18: icmp_seq=2 ttl=64 time=0.317 ms
64 bytes from 192.168.100.18: icmp_seq=3 ttl=64 time=0.314 ms
64 bytes from 192.168.100.18: icmp_seq=4 ttl=64 time=0.323 ms
64 bytes from 192.168.100.18: icmp_seq=5 ttl=64 time=0.323 ms
64 bytes from 192.168.100.18: icmp_seq=6 ttl=64 time=0.316 ms
64 bytes from 192.168.100.18: icmp_seq=7 ttl=64 time=0.344 ms
64 bytes from 192.168.100.18: icmp_seq=8 ttl=64 time=0.332 ms
64 bytes from 192.168.100.18: icmp_seq=9 ttl=64 time=0.294 ms
64 bytes from 192.168.100.18: icmp_seq=10 ttl=64 time=0.320 ms
```

Fuente: elaboración propia

10. Desde el cliente Kali Linux ejecute el escaneo de puertos mediante el motor de la herramienta NMAP contra el servidor Alma-Linux como se muestra en la ilustración 82.

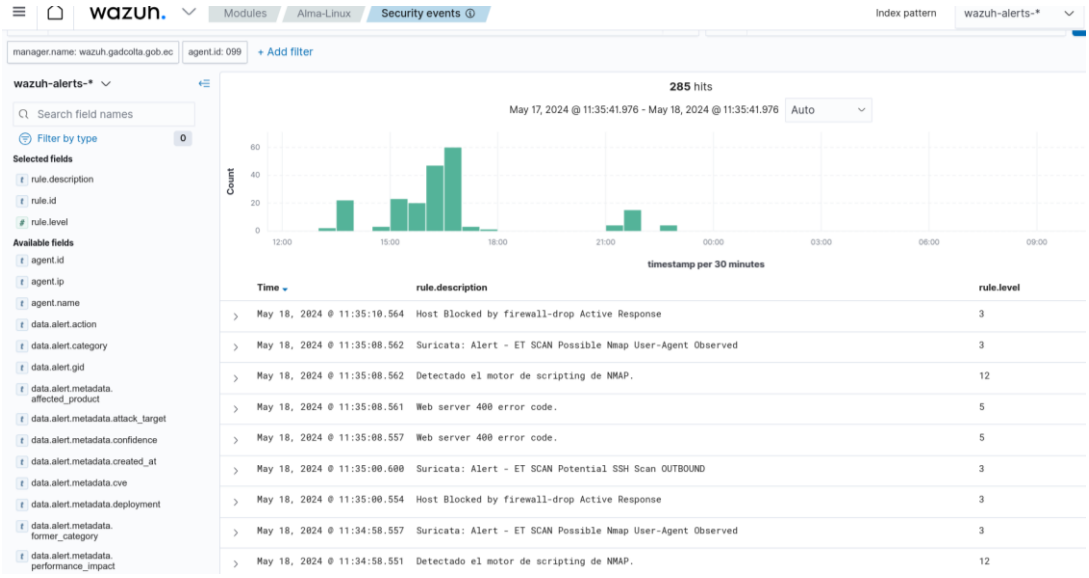
Ilustración 82. Escaneo de puertos con NMAP

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS --script=vuln 192.168.100.18
[sudo] contraseña para kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 11:34 -05
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 192.168.100.18
Host is up (0.00028s latency).
Not shown: 986 filtered tcp ports (no-response), 10 filtered tcp ports (admin-prohibited)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp  open   https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-trace: TRACE is enabled
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
9090/tcp closed zeus-admin
MAC Address: 00:0C:29:1F:C0:19 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 251.81 seconds
```

Fuente: elaboración propia

11. Como se observa en las ilustraciones 83, 84, 85 y 86; Wazuh detecto el evento de seguridad y ejecuto inmediatamente la respuesta activa que se configuro en el paso # 8.

Ilustración 83. Detección del escaneo de puertos con NMAP



Fuente: elaboración propia

Ilustración 84. Prueba de conectividad al servidor no exitosa

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.100.18 -c 10
PING 192.168.100.18 (192.168.100.18) 56(84) bytes of data.

--- 192.168.100.18 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9208ms


┌──(kali㉿kali)-[~]
```

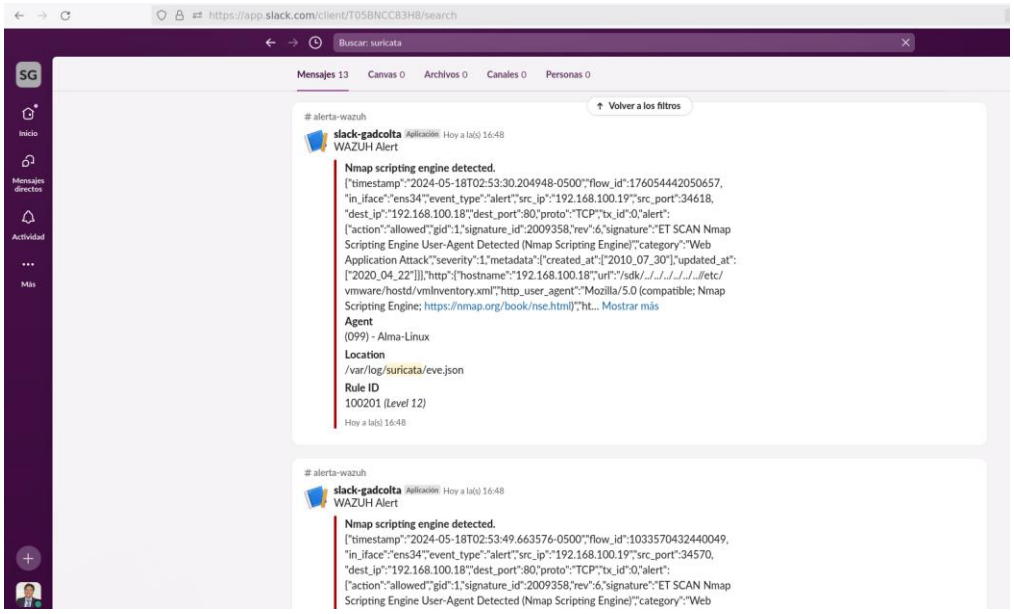
Fuente: elaboración propia

Ilustración 85. Reglas Creadas Automáticamente en el Firewall

```
[root@alma ~]#
[root@alma ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.100.19       anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  192.168.100.19       anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[root@alma ~]#
[root@alma ~]#
```

Fuente: elaboración propia

Ilustración 86. Alerta de Detección del Ataque en la plataforma Slack



Fuente: elaboración propia

12. Para realizar el **Ataque de Denegación de Servicio**, desde el cliente Kali Linux ejecute la herramienta *goldeneye*, contra el servidor Alma-Linux como se muestra en la ilustración 87.

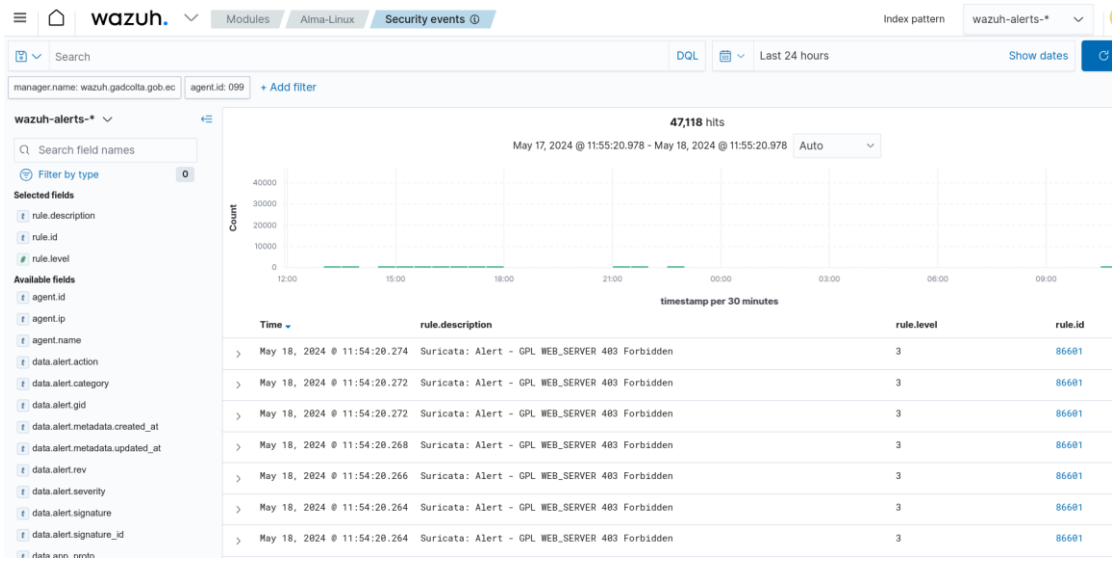
Ilustración 87. Ataque de denegación de Servicios al protocolo HTTP

```
┌──(kali㉿kali)-[~/GoldenEye]
└─$ ./goldeneye.py http://192.168.100.18

GoldenEye v2.1 by Jan Seidl <jseidl@wroot.org>

Hitting webserver in mode 'get' with 10 workers running 500 connections each. Hit CTRL+C to cancel
2985 GoldenEye strikes hit. (176 Failed)
2985 GoldenEye strikes hit. (6412 Failed)
        Server may be DOWN!
3985 GoldenEye strikes hit. (16798 Failed)
4985 GoldenEye strikes hit. (28401 Failed)
8151 GoldenEye strikes hit. (31963 Failed)
8151 GoldenEye strikes hit. (35449 Failed)
        Server may be DOWN!
8151 GoldenEye strikes hit. (38499 Failed)
        Server may be DOWN!
```

Fuente: elaboración propia

13. Como se observa en las ilustraciones 88; Wazuh detecto el evento de seguridad y ejecuto inmediatamente la respuesta activa que se configuro en el paso # 8.

Ilustración 88. Detección del ataque DOS al protocolo HTTP



Fuente: elaboración propia

CONCLUSIONES

- Se estudió exhaustivamente la arquitectura de la plataforma SIEM con tecnología XDR, Wazuh, mediante una revisión bibliográfica detallada, que incluyo artículos científicos indexados, trabajos de titulación académicos y la documentación oficial de la plataforma de seguridad. Esta revisión incluyó conceptos claves, beneficios y limitaciones de la tecnología XDR aplicada a las plataformas SIEM. La información recopilada proporcionó una base teórica sólida para la implementación de esta tecnología en la infraestructura del GAD COLTA, destacando su capacidad para mejorar sustancialmente la visibilidad de las amenazas y la eficiencia en la respuesta a incidentes.

- El análisis detallado de detección y respuesta extendidas en la infraestructura del GAD Colta, reveló varias deficiencias en la detección temprana de amenazas y en la capacidad de respuesta automática a incidentes. Se identificaron áreas y equipamiento crítico que requieren mejoras a la brevedad posible, como la actualización del sistema operativo Windows 7 y Windows 8.1 en los equipos finales de usuario de las áreas estratégicas del GAD Colta, así como en cuatro servidores que tienen instalado el sistema operativo Linux con versiones que ya no existe soporte de actualizaciones de seguridad y parches. Estos hallazgos subrayan la necesidad de adoptar una solución SIEM con tecnología XDR para fortalecer la postura de seguridad del GAD COLTA.

- Las pruebas ejecutadas con la herramienta SIEM Wazuh en la infraestructura del GAD COLTA demostraron la eficacia de la tecnología XDR en la mejora de la detección y respuesta a amenazas. Los resultados mostraron una reducción muy significativa en el tiempo de respuesta a incidentes y una mayor precisión en la identificación de amenazas. Esto confirma que la implementación de la herramienta seleccionada es viable y beneficiosa para el GAD COLTA, mejorando su capacidad para enfrentar amenazas cibernéticas de manera proactiva.

- La guía de implementación elaborada proporciona un marco paso a paso para la adopción de la herramienta SIEM WAZUH con tecnología XDR en la infraestructura del GAD COLTA. Esta guía incluye recomendaciones prácticas, configuraciones óptimas y procedimientos operativos que facilitan la integración y uso efectivo de la herramienta. La disponibilidad de esta guía asegura que el personal del GAD COLTA pueda implementar y gestionar la solución de manera eficiente, maximizando los beneficios de la tecnología XDR.

RECOMENDACIONES

- Se recomienda a la brevedad posible actualizar las versiones del sistema operativo de los servidores: QUIPUX, SIIM, SINAT, Zimbra y Central-VozIP; las versiones actuales del sistema representan un riesgo de seguridad inminente a la infraestructura tecnológica del GAD Colta.

- De igual manera se recomienda actualizar a la brevedad posible los 65 dispositivos finales de usuario que están operativos en los diferentes departamentos del GAD Colta y que tienen como sistema operativo Windows 7 y Windows 8.1.

- Se recomienda también, extender las configuraciones XDR de las respuestas activas a los servidores institucionales que operan con Windows Server 2012 y Windows Server 2022.

- Finalmente, se recomienda realizar eventos de capacitación y concientización con el personal interno del GAD COLTA, para explicarles los conceptos claves y beneficios de utilizar la tecnología XDR en la infraestructura tecnológica del GAD Colta.

BIBLIOGRAFÍA

Advance Networks. (23 de 09 de 2021). *¿Qué es XDR en Ciberseguridad y para qué sirve?* Obtenido de https://advance-nt.com/2021/09/23/que-es-xdr-en-ciberseguridad-y-para-que-sirve/

Ballejos, L. (s/f). ¿Qué es la XDR (detección y respuesta extendidas)? NinjaOne. Recuperado el 12 de enero de 2024, de https://www.ninjaone.com/es/blog/que-es-la-xdr/

Carlos Lunar, G. P. (noviembre de 2014). *Proyecto Sociotecnologico*. Obtenido de http://proyecto-plataformadespachos7022.blogspot.com/p/metodologia-de-red_14.html

CEPAL, N. U. (23 al 26 de Noviembre de 2020). *Informe sobre la Séptima Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe*. Obtenido de www.cepal.org: https://repositorio.cepal.org/server/api/core/bitstreams/0509131c-7ca8-40a4-ae2d-755df6a68cb1/content

CIO-PERU. (16 de 1 de 2023). *Herramientas XDR y cómo evaluarlas*. Obtenido de https://cioperu.pe/articulo/35893/las-11-mejores-herramientas-xdr-y-como-evaluarlas/

Clusit. (10 de 2023). *Informe Clusit 2023 sobre ciberseguridad global*. Obtenido de https://clusit.it/rapporto-clusit/

Criollo Rimaycuna, G. (28 de Octubre de 2022). *Lan de Cámaras IP de Monitoreo para los Protocolos de Bioseguridad Mediante la Metodología de Diseño de Red PPDIOO – Cisco en la I.E. José Carlos Mariátegui – La Oroya*. Obtenido de https://hdl.handle.net/20.500.12848/4806

CrowdStrike. (28 de 6 de 2023). Obtenido de https://www.crowdstrike.com/cybersecurity-101/what-is-xdr/open-xdr-vs-native-xdr/

Dirección Nacional de Ciberseguridad de Israel. (Julio de 2022). *https://www.iadb.org/es*. Obtenido de http://dx.doi.org/10.18235/0004378

Delgado, M. F. (2023, agosto 13). Wazuh como herramienta SIEM esencial para la Seguridad de tu Infraestructura. Linkedin.com. https://es.linkedin.com/pulse/wazuh-como-herramienta-siem-esencial-para-la-de-tu-maurice

Dragora. (6 de 3 de 2023). *Wazuh: una plataforma de código abierto, SIEM y XDR*. Obtenido de https://blog.underc0de.org/wazuh-una-plataforma-de-codigo-abierto-siem-y-xdr/#:~:text=Wazuh%20es%20una%20plataforma%20de%20seguridad%20gratuita%20y,trabajo%20en%20entornos%20locales%20y%20en%20la%20nube.

Gartner, T. L. (17 de Agosto de 2023). *Guía de mercado para la detección y respuesta extendidas*. Obtenido de https://www.gartner.com/doc/reprints?id=1-2EOYTQA6&ct=230811&st=sb

Geovanny, M. L. E. (2012). Analisis y Gestion de Riesgos Implementando La Metodologia Magerit. Eae Editorial Academia Espanola.

Gómez, J. A. (25 de Julio de 2023). *SIEM: Qué es y cómo puede optimizar la ciberseguridad de tu empresa*. Obtenido de https://www.deltaprotect.com/blog/siem-que-es

González, L. P. (1 de 9 de 2023). *Sistemas EDR: que son y cómo ayudan a proteger los activos OT*. Obtenido de https://www.mytra.es/blog-post/sistemas-edr-que-son-y-como-ayudan-a-proteger-los-activos-ot

Hernández Sampieri, R. (2006). Metodologia de La Investigación. McGraw-Hill Companies.

Insiders, C. (2019). *SIEM REPORT*. Obtenido de https://cdn2.hubspot.net/hubfs/4620545/PDF/SIEM%20Report%202019.pdf?utm_campaign=INFORME%20SIEM&utm_source=hs_automation&utm_medium=email&utm_content=79716239&_hsenc=p2ANqtz--rXp3bACnTqgsj3sxbvAHRoZJ-dcoBuUyX5PgxRL9k1Xhp3BErZADh2VgzTsNX05lP0o8uskxSMw6hX9z

Kanade, V. (8 de 11 de 2023). *¿Qué es un Centro de Operaciones de Seguridad (SOC)? Significado, componentes, configuración y beneficios*. Obtenido de spiceworks: https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-soc/

Kaspersky. (s.f.). *¿Qué es la detección y respuesta ampliadas (XDR)?* Obtenido de kaspersky: https://www.kaspersky.es/resource-center/definitions/what-is-xdr

Kaspersky. (15 de Febrero de 2023). *Predice cambios en el panorama de amenazas para el sector industrial*. Obtenido de https://latam.kaspersky.com/about/press-releases/2023_kaspersky-predice-cambios-en-el-panorama-de-amenazas-para-el-sector-industrial

Lorenzo, A. R. (1 de 7 de 2021). *SIEM, gestión de eventos e información de seguridad*. Obtenido de https://www.mytra.es/blog-post/siem-gestion-de-eventos-e-informacion-de-seguridad

Mosquera Rodríguez , Cedeño Troya (2020). Sistemas de Información como herramienta para la toma de decisiones. https://www.uteg.edu.ec/wp-content/uploads/2022/10/L2-2020.pdf

Muguira, A. (2016). *¿Qué es la investigación descriptiva?* Obtenido de https://www.questionpro.com/blog/es/investigacion-descriptiva/

Ocampo, D. S. (3 de Diciembre de 2019). *Investigalia*. Obtenido de https://investigaliacr.com/investigacion/investigacion-bibliografica/

Paloalto Networks. (7 de 2021). *¿Cuál es la diferencia entre XDR y SIEM?* Obtenido de https://www.paloaltonetworks.com/cyberpedia/what-is-xdr-vs-siem

Polanco, C. (14 de Mayo de 2018). *sofecom*. Obtenido de https://sofecom.com/: https://sofecom.com/que-es-un-siem/

Ramiro, R. (7 de Marzo de 2021). *Las mejores prácticas para implementar una estrategia SIEM*. Obtenido de https://ciberseguridad.blog/las-mejores-practicas-para-implementar-una-estrategia-siem/

S3CURETASUN. (8 de 7 de 2022). Obtenido de https://s3curetasun.net/que-es-un-xdr/

SECURE-OPS. (1 de 1 de 2020). Obtenido de https://secureops.com/blog/blog-what-is-a-siem/

Solo, H. (24 de 2 de 2021). *¿Qué es EDR (Endpoint Detection & Response)?* Obtenido de https://zombiezero.medium.com/what-is-edr-endpoint-detection-response-d4e399aec970

Steinberg, J. (Marzo de 2022). *Cybersecurity For Dummies, 2nd Edition*. Obtenido de https://www.wiley.com/en-in/Cybersecurity+For+Dummies,+2nd+Edition-p-9781119867180

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. Polo Del Conocimiento, 3(4), 230. https://doi.org/10.23857/pc.v3i4.809

Thenault, F. (13 de Noviembre de 2017). *https://www.syneidis.com/*. Obtenido de https://www.syneidis.com/es/the-equifax-case-causes-and-consequences/

TREND. (s.f). *¿Qué es XDR?* Obtenido de https://www.trendmicro.com/es_es/what-is/xdr.html#:~:text=XDR%20(detecci%C3%B3n%20y%20respuesta%20extendidas)%20recopila%20y%20correlaciona%20autom%C3%A1ticamente%20datos,mediante%20un%20an%C3%A1lisis%20de%20seguridad.

Valcárcel, L. J. (28 de Abril de 2023). *LinKedin*. Obtenido de https://www.linkedin.com: https://www.linkedin.com/pulse/siem-vs-soar-xdr-cuáles-son-las-diferencias-y-cuál-es-luis-josé/?originalSubdomain=es

Wazuh. (2023). *Protección XDR activa frente a amenazas modernas*. Obtenido de https://wazuh.com/platform/xdr/?gclid=Cj0KCQiAsvWrBhC0ARIsAO4E6f-uqtl6GtVlsPvaCUyfjZN2N-er_dskGicOL2LhcysmSry8GpfcMrsaAgOTEALw_wcB#open-source