Artículo original/ Original article
ISSN 2953-6553

Implementar un sistema de gestión y análisis de seguridad con la herramienta Wazuh, en el Instituto Superior Universitario Tecnológico del Azuay.

Implement a security management and analysis system with the Wazuh tool, at the Instituto Superior Universitario Tecnológico del Azuay.

Marcelo Monteros 0000-0002-8095-8109 , José Fabián-Chuqui Quille 0009-0005-4182-3112 ,Nayeli Benitez-Cacao, Pablo Velez-Guerrero
ruben.monteros@tecazuay.edu.ec , jose.chuqui@tecazuay.educ, nayeli.benitez.est@tecazuay.edu.ec, pabloa.velez.est@tecazuay.edu.ec

[1]Afiliación, Provincia/Ciudad, País.

DOI 10.36500/atenas.3.006

Resumen

El objetivo de este proyecto consiste en proponer una plataforma de seguridad y monitoreo de amenazas utilizando el software Wazuh. Durante el desarrollo de este trabajo, se ha realizado un estudio exhaustivo de la herramienta, abarcando los conceptos teóricos necesarios, su funcionamiento y las características de las herramientas de detección de vulnerabilidades.
Se ha planificado e implementado la instalación de Wazuh en un entorno virtual utilizando el sistema operativo Ubuntu. Se ha proporcionado una guía detallada que explica paso a paso la configuración necesaria para su instalación y configuración.
Una vez que se han configurado estos sistemas, se ha llevado a cabo la monitorización durante un día y una noche en una serie de computadoras con sistema operativo Windows, ubicadas en los laboratorios 3 y 4 del TEC-Azuay.
Posteriormente, se ha realizado un análisis de los resultados obtenidos de los módulos de vulnerabilidades y se ha comparado con la guía CIS, correspondiente a nuestros equipos. Además, se han descubierto una serie de soluciones ofrecidas por este software de código abierto.
Finalmente, se han analizado los resultados y se puede concluir que Wazuh es una herramienta muy completa, ya que brinda un análisis exhaustivo de seguridad y alertas; así como, recomendaciones para solucionar los problemas identificados en los informes generados.

Abstract

The objective of this project is to propose a comprehensive security and threat monitoring platform utilizing Wazuh software. This work involved an in-depth analysis of the tool, covering its theoretical underpinnings, operational capabilities, and features pertinent to vulnerability detection.
The implementation of Wazuh in a virtualized environment running the Ubuntu operating system was meticulously planned and executed. A detailed installation and configuration guide was developed, providing step-by-step instructions necessary for deployment.
Post-configuration, a 24-hour monitoring session was conducted on a network of computers operating on the Windows OS, situated in laboratories 3 and 4 of TEC-Azuay. The data collected from Wazuh's vulnerability detection modules were subsequently analyzed and benchmarked against the CIS standards applicable to our equipment.
Furthermore, various solutions and remediation strategies offered by this open-source software were identified and evaluated for effectiveness in enhancing the security posture of the monitored systems.

Palabras Claves – Wazuh, SIEM, TEC-AZUAY, IDS/IPS, SCA-CIS
Keywords – Wazuh, SIEM, TEC-AZUAY, IDS/IPS, SCA-CIS

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

I. INTRODUCCIÓN

En los últimos cuatro años, entre 2019 y 2022, se han detectado tres ataques en la infraestructura de tecnología y comunicación, del Instituto Superior Universitario Tecnológico del Azuay (TEC. AZUAY). Estos ataques consisten en dos casos de fuerza bruta y uno de malware; sin embargo, no se han establecido ni aplicado políticas de seguridad para proteger la información de los datos académicos y personales de los estudiantes y docentes de esta institución de educación superior. El primer ataque ocurrió en febrero de 2019, afectando al router principal; en esta ocasión, se obtuvo acceso al router utilizando credenciales de administrador. El equipo de Tecnología y Comunicación del Instituto solucionó este incidente mediante la implementación de una regla de firewall. El segundo ataque, de tipo malware, se descubrió el 18 de septiembre de 2020, gracias a la acción de un antivirus; el software malicioso ingresó a través del puerto 2085; sin embargo, se logró mitigar el incidente cerrando dicho puerto. El tercer evento de ataque por fuerza bruta tuvo lugar el 7 de mayo de 2022, afectando nuevamente al router principal; para solucionar este incidente de seguridad, se añadieron reglas al firewall para bloquear las direcciones IP desde las cuales se originó el ataque.

El monitoreo de la red de datos ha sido un aspecto poco atendido en el TEC. AZUAY durante mucho tiempo. Se ha priorizado brindar un servicio de conexión a los usuarios, dejando de lado la seguridad de la misma.

Es importante tener en cuenta que, el monitoreo de las vulnerabilidades y amenazas de los equipos es una tarea importante, ya que por medio de ella podemos detectar posibles ataques y pérdidas de información.

II. MARCO TEÓRICO

La ejecución del mencionado proyecto se realiza con base en la documentación oficial de la página de Wazuh, que se detalla a continuación.

Wazuh. (s.f.). Wazuh - Open Source Security Monitoring Platform. Recuperado de https://wazuh.com/

¿Qué es la herramienta Wazuh?

Wazuh se emplea para la prevención, detección y respuesta ante amenazas, salvaguardando las cargas de trabajo en diversos entornos, ya sean locales, virtualizados, en contenedores o basados en la

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

nube. Esta herramienta goza de una amplia adopción en todo el mundo, siendo utilizada por miles de organizaciones, desde pequeñas empresas hasta grandes corporaciones.

Considerada como una de las soluciones de seguridad más destacadas, Wazuh resulta invaluable para empresas de todos los tamaños. Su efectiva detección y respuesta ante amenazas, junto con la capacidad de supervisar la integridad de los sistemas, le otorgan un alto nivel de confiabilidad como solución de seguridad. Además, cabe destacar que, esta herramienta se basa en código libre, lo que implica que su implementación no conlleve costos onerosos.

Características de Wazuh

- Código Abierto

Inicialmente, la expresión open source (código abierto) hacía referencia exclusivamente al software open source (OSS). Dicho software se caracteriza por su accesibilidad al público, permitiendo a todos visualizar, modificar y distribuir el código de acuerdo con sus necesidades y preferencias.

El desarrollo del software open source se lleva a cabo de forma colaborativa y descentralizada, basándose en la revisión entre pares y la contribución de la comunidad. Además, este tipo de software tiende a ser más económico, flexible y perdurable en comparación con alternativas de propiedad, ya que su creación depende de comunidades, en lugar de un único autor o empresa.

- Seguridad de la información

La seguridad de la información abarca un conjunto de técnicas y medidas que se aplican para salvaguardar la privacidad de los datos e información de una institución, evitando su divulgación a personas no autorizadas. Estas acciones y medidas se basan en el conocimiento de las nuevas tecnologías. Asimismo, la seguridad de la información se encargará de proteger los datos almacenados en el sistema de la empresa, limitando el acceso a usuarios con autorización.

Además de proteger la información, también es crucial asegurar que cualquier modificación se realice únicamente por personas con los permisos adecuados. La seguridad de la información reconoce que los datos representan un valioso activo en la actualidad y su mal uso podría tener consecuencias catastróficas para gobiernos, empresas y personas que manejan datos sensibles en línea.

- Monitoreo de seguridad

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

Según Fortra (2023), sugiere monitorear el sistema de manera constante para detectar cualquier cambio no autorizado y para identificar y eliminar posibles amenazas de seguridad, evitando así el daño o la exposición de información crítica. La supervisión de los cambios en el sistema permite una respuesta inmediata ante actividades sospechosas, lo que ayuda a minimizar o prevenir posibles daños. Normalmente, las iniciativas de monitoreo de la integridad de la seguridad buscan proporcionar visibilidad sobre varios aspectos, incluyendo qué usuario inició un cambio, qué aplicación o función sufrió el cambio, cuándo se llevó a cabo el cambio y cuál fue el valor antes y después de dicho cambio. También, se busca determinar si el cambio estaba autorizado o no.

- Gestión de eventos e información de seguridad

Las plataformas para gestión de eventos e información de seguridad, o SIEM, ofrecen análisis en tiempo real de eventos de seguridad y capacidades de respuesta para automatizar el despliegue de contramedidas. Según Rangel Méndez (2021), los sistemas de respuesta actuales no realizan un análisis de impacto completo de los ataques y escenarios de respuesta.

La herramienta de gestión de eventos e información de seguridad (SIEM) es fundamental en las empresas para proteger la información sensible y diferenciar entre amenazas de bajo y alto riesgo. Esto la convierte en una herramienta importante en la detección y respuesta ante posibles amenazas.

- Sistemas de Detección y Prevención de Intrusiones

Según Coyla Jarita (2019), un sistema de detección de intrusos (IDS) es un sistema que monitorea el tráfico de la red en busca de actividad sospechosa y emite alertas cuando se detecta alguna acción (falsos positivos).

Por otro lado, según la misma fuente, un sistema de prevención de intrusiones (IPS) es una tecnología de seguridad de red que examina los flujos de tráfico de la red para detectar y prevenir vulnerabilidades.

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

Tabla 1.

Arquitectura de Wazuh

Arquitectura	Descripción
Indexador Wazuh	El indexador de Wazuh es un potente motor de análisis y búsqueda de texto completo, diseñado para escalar eficientemente. Además, proporciona capacidades avanzadas de análisis y búsqueda de datos casi en tiempo real.
Servidor Wazuh	El servidor de Wazuh examina los datos enviados por los agentes de Wazuh y genera alertas, en caso de detectar amenazas o anomalías. Además, se emplea para la gestión remota de la configuración de los agentes y para supervisar su estado de funcionamiento.
Agente Wazuh	Agente de Wazuh es multiplataforma que se ejecuta en los puntos finales seleccionados por el usuario para su monitoreo. Establece una comunicación con el servidor de Wazuh y transmite datos casi en tiempo real, a través de un canal encripta y autenticado.
Wazuh Dashboard	Es otro componente central de la arquitectura de Wazuh porque es una interfaz web versátil e intuitiva diseñada para extraer, analizar y visualizar datos de seguridad.

Nota. La tabla establece la arquitectura que se utiliza en la instalación de Wazuh con su respectiva descripción 2024.

III. METODOLOGÍA

Para la implementación del proyecto mencionado, se adoptó el enfoque analítico, que consiste en emplear teorías o estudios previos que brinden información relevante para la investigación. Inicialmente, se llevó a cabo una investigación bibliográfica de tipo documental, en concordancia con los requisitos de desarrollo y avances en el tema, enfocada en fortalecer la seguridad de la información en el TEC. AZUAY, a través de la adopción y configuración de una solución de monitoreo de seguridad.

El enfoque cuantitativo de la investigación para la instalación de Wazuh está directamente vinculado al objetivo de proporcionar a la institución visibilidad sobre sus activos tecnológicos, tal como lo indica el estudio de Bello Vieda (2019). La implementación de Wazuh permite obtener una visión en tiempo real del comportamiento de los puntos finales (endpoints), lo que proporciona los datos e inteligencia necesarios para detectar, contener y eliminar amenazas cibernéticas. La planificación detallada, configuración del entorno, instalación de Wazuh y configuración de los agentes, facilitan el

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

monitoreo y recopilación de información de los sistemas a proteger, lo que a su vez agiliza la toma de decisiones y acciones en situaciones de crisis.

IV. RESULTADOS

A. Requisitos de Hardware

En la instalación mencionada, tanto el servidor de Wazuh; así como, el Inicio rápido de Wazuh se instalan en el mismo host. En este entorno, se implementaron 13 agentes.

Tabla 2.

Sistema operativo del servidor

Servidor Wazuh	RAM (GB)	CPU (cores)
Ubuntu 22.04 LS	5	3

Nota Características del servidor Wazuh 2024.

Nota. Lo recomendado son 32 GB de RAM y 8 núcleos de CPU. El uso de sistema operativo de 64 bits

B. Requisitos de Comunicación Wazuh Server

Para la comunicación de los componentes de Wazuh se emplean varios servicios, los cuales hacen uso de una serie de puertos predeterminados. A continuación, se presenta una tabla que detalla la lista de dichos puertos.

Tabla 3.

Puertos de comunicación Wazuh

Componente	Software	Puerto	Protocolo	Propósito
Wazuh server	Wazuh manager	1514	TCP (default)	Agents connection service
		1514	UDP	Agents connection service
		1515	TCP	Agents registration service
		1516	TCP	Wazuh clúster daemon
		514	UDP (default)	Wazuh syslog collector (disabled by default)

Nota Descripción de los puertos y protocolo 2024.

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

C. Requisitos para la inicialización rápida de Wazuh

La tabla presenta los requisitos de hardware necesarios para la implementación del inicio rápido de Wazuh; así como, la capacidad de almacenamiento de los datos capturados por Wazuh a lo largo del tiempo.

Tabla 4.

Inicialización rápida de Wazuh

Agentes	UPC	RAM	Almacenamiento (90 días)
1-25	3 vCPU	4 GB	20GB

Nota. Descripción de las características de los agentes 2024.

D. Resultado del nivel de severidad de las vulnerabilidades

El análisis de las vulnerabilidades y las políticas SCA-CIS de los equipos se llevó a cabo en los laboratorios 3 y 4. A continuación, se presentan detalladamente los resultados obtenidos a partir del análisis de vulnerabilidades identificadas, mediante el uso del software Wazuh.

Tabla 5.

Nivel de severidad de las vulnerabilidades

Nivel de severidad	Cuenta de Severidad
High	1063
Low	28
Medium	283
Total general	**1374**

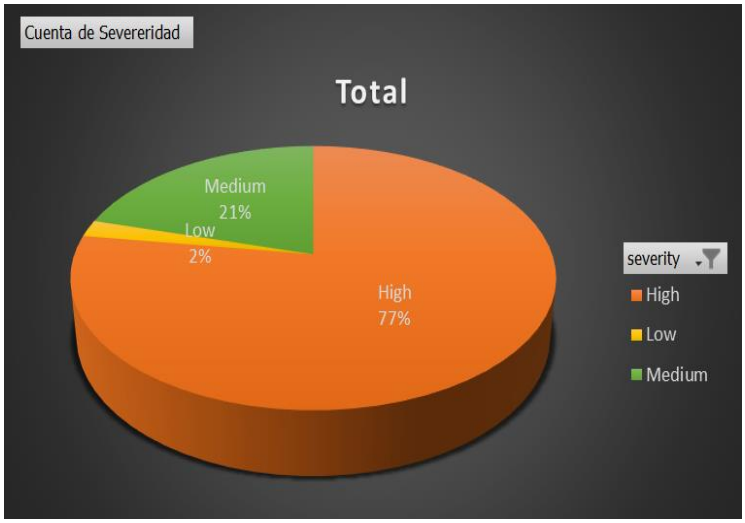
Nota. Cuadro de severidad 2024.

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

Las vulnerabilidades de alta importancia son prioritarias en cuanto a su resolución, ya que representan una de las debilidades más preocupantes. Su existencia puede dar lugar a ataques o al robo de información. Por otro lado, las vulnerabilidades de impacto medio requieren atención gradual; sin embargo, no deben ser ignoradas. Aunque no afecten significativamente al instituto TEC. AZUAY, si se les permite persistir con el tiempo, podrían volverse críticas. Finalmente, las vulnerabilidades de baja prioridad aún no afectan la seguridad del Instituto, pero se debe estar alerta ante cualquier indicio mínimo de riesgo.

Figura 1

Nivel de severidad de las vulnerabilidades



Nota. Cuadro de severidad de vulnerabilidades del análisis realizado 2024.

E. Análisis de las vulnerabilidades en aplicaciones y sistema operativo

En cambio, en este apartado se presentan de manera detallada los resultados del análisis de vulnerabilidades encontradas en aplicaciones y sistema operativo, las cuales fueron obtenidas a partir del mismo informe de debilidades, generado por el software Wazuh.

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

Tabla 6.

Vulnerabilidades en aplicaciones y sistema operativo

Vulnerabilidades en aplicaciones y sistema operativo	Cuenta de CVE
Microsoft Office Professional Plus 2016 - es-es	1287
Python 2.7.18 (64-bit)	27
Windows 10	4
Oracle VM VirtualBox 7.0.4	16
Oracle VM VirtualBox 7.0.6	40
Total general	**1374**

Nota. Cuadro de vulnerabilidades por aplicaciones 2024.

En el informe, se identificó un mayor número de vulnerabilidades en el software Microsoft Office Professional Plus 2016 es-es y Windows 10. Se observó que no se han aplicado los parches disponibles desde la página oficial, lo cual indica una falta de actualizaciones en dichas aplicaciones. Por otro lado, otras aplicaciones como Python 2.7.18 (64-bit), Oracle VM VirtualBox 7.0.4 y Oracle VM VirtualBox 7.0.6 presentan un riesgo mediano de vulnerabilidad debido a que se trata de versiones antiguas, las cuales ya han sido objeto de vulnerabilidades conocidas. Es por esta razón que, se han lanzado nuevas versiones que solucionan estos problemas.

F. Análisis de los años de la publicación de los parches para cada vulnerabilidad

En el informe generado por el software Wazuh, se proporcionan los años de publicación de los parches destinados a corregir los errores encontrados. La información detallada incluye las fechas en que estos parches fueron lanzados para solucionar las vulnerabilidades identificadas.

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

Tabla 7.

Años de publicación de los parches

Años de publicación de los parches	Cuenta de CVE
2016	66
2017	146
2018	300
2019	275
2020	146
2021	267
2022	97
2023	77
Total general	**1374**

Nota. Cuadro de publicación de los parches 2024.

Es posible observar el progreso anual de los atacantes, ya que desde 2017 hasta 2021 ha habido un crecimiento exponencial en el número de actualizaciones de parches destinados a contrarrestar la inseguridad. Desde 2022 hasta la fecha actual, se puede afirmar que las organizaciones están tomando con mayor seriedad la protección de la integridad, confidencialidad y disponibilidad de sus usuarios.

G. Resultado del análisis de eventos de seguridad

La plataforma Wazuh genera un informe de eventos de seguridad que provee información detallada sobre las alertas; así como, la evolución de los grupos de alerta, evidenciando cambios significativos a lo largo del tiempo. Además, brinda una visión general de las alertas generadas durante un período específico, con el propósito de evaluar el cumplimiento de los estándares de seguridad del CIS.

Tabla 8.

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

Políticas SCA-CIS

Resultado	**Cuenta de Resultado**
Aprobado	111
Fallido	280
No aplica	4
Total general	**395**

Nota. Cuadro de resultados 2024.

A través de la utilización de la guía CIS como punto de referencia, Wazuh tiene la capacidad de analizar la configuración del sistema y detectar cualquier desviación o vulnerabilidad en relación con las recomendaciones de seguridad establecidas. Durante el escaneo realizado en el TEC. AZUAY, se aprobaron únicamente 111 puntos, mientras que se identificaron 280 fallos en total. Este resultado es motivo de preocupación, ya que no se logra superar la cantidad de puntos aprobados. Para mejorar la seguridad de los sistemas, se han recopilado en el Anexo G una serie de soluciones que siguen los estándares establecidos por la Guía CIS. Asimismo, se identificaron 4 estándares que no se aplican en esta institución.

Figura 2.

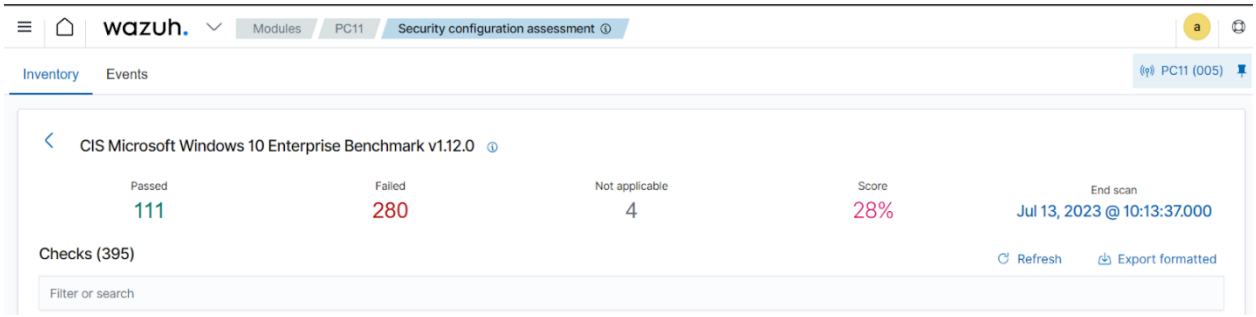
Políticas SCA-CIS

Nota. Cuadro de resultados políticas 2024.

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

Figura 3.

Reporte CIS que muestra en la plataforma de Wazuh



Nota. Cuadro de resultados reporte CIS.2024

En la imagen adjunta, se pueden observar deficiencias de cumplimiento en la guía de CIS. Se detallan minuciosamente las falencias en el cumplimiento de los estándares establecidos por la guía, junto con las soluciones propuestas para abordar cada una de estas deficiencias.

V. CONCLUSIONES

Mediante la adopción de la solución de código abierto, TEC. AZUAY ha mejorado su capacidad para monitorear en tiempo real los eventos relacionados con los equipos de los laboratorios. Esto permite a los responsables de la seguridad de la información tomar decisiones rápidas y oportunas, implementando acciones preventivas ante la detección de comportamientos anómalos. La implementación de Wazuh ha generado una oportunidad de mejora en el manejo de eventos, brindando a TEC. AZUAY una herramienta que facilita el tratamiento de los riesgos evaluados mediante la detección preventiva, evitando así la materialización de dichos riesgos.

Se logró identificar las vulnerabilidades y el incumplimiento de los estándares de seguridad establecidos por el CIS. Estas acciones son fundamentales para fortalecer la seguridad en TEC. AZUAY, ya que se obtuvo un reporte detallado de las vulnerabilidades críticas, altas, medias y bajas presentes en los equipos de los laboratorios. Además, se realizó un análisis de las guías de incumplimiento de estándares de seguridad, identificando cuáles se están cumpliendo, cuáles no y cuáles no son aplicables.

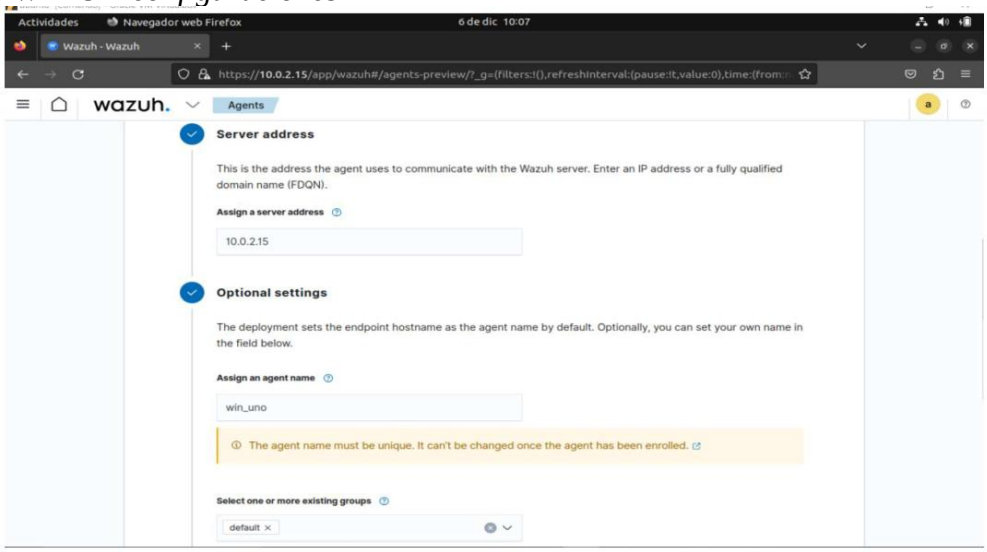
Teniendo en cuenta todas las inseguridades y vulnerabilidades identificadas en la Institución, la implementación de estas políticas y medidas ayudará a fortalecer la seguridad de TEC.AZUAY, protegiendo sus sistemas, datos y usuarios contra amenazas cibernéticas y asegurando un entorno seguro para todos. Se pueden aplicar las soluciones necesarias para mejorar la seguridad de TEC.AZUAY.

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

VI. ANEXO CONFIGURACIONES Y ALERTAS

Figura 4

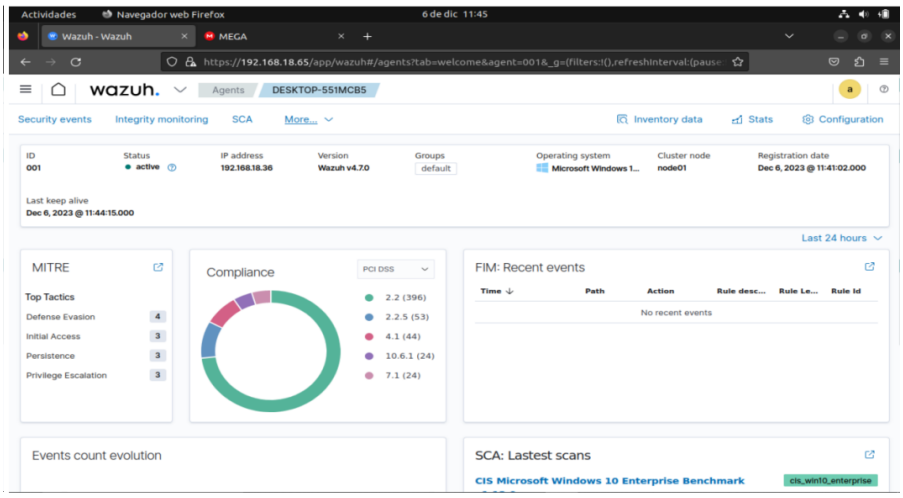
Reporte WAZUH configuraciones



Nota. Visualización de configuraciones.2024

Figura 5

Reporte WAZUH indicadores

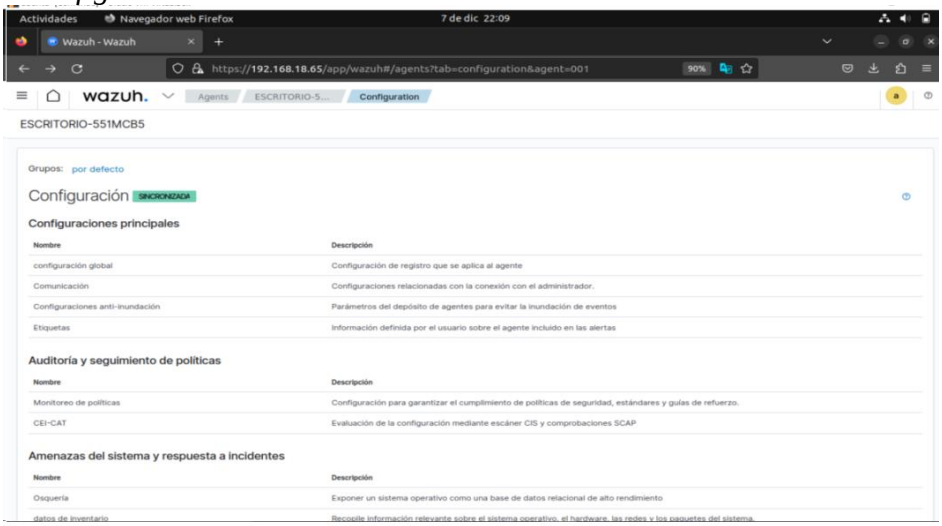


Nota. Visualización de indicadores de Wazuh.2024

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

Figura 6

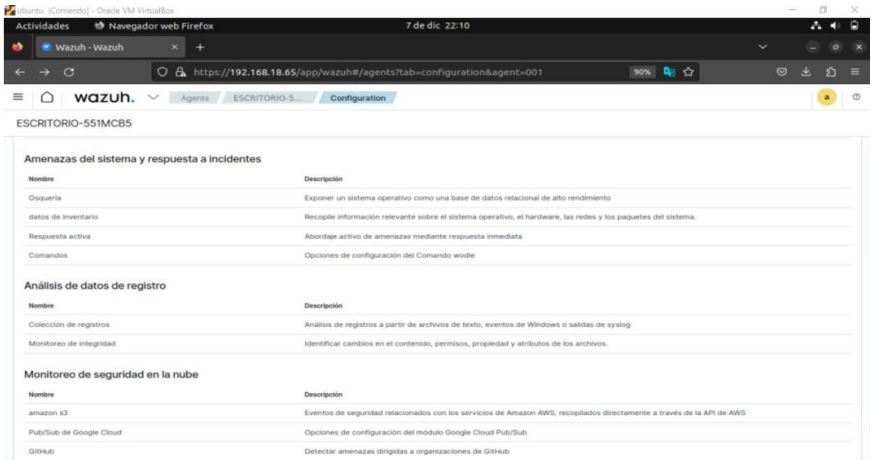
Reporte WAZUH configuración de auditorías



Nota. Visualización de configuraciones de Wazuh.2024

Figura 7

Reporte WAZUH configuración de análisis



Nota. Visualización de configuraciones de amenazas de sistemas, análisis de datos y monitoreo de seguridad. 2024

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

REFERENCIAS BIBLIOGRÁFICAS

Farinango Endara, H. P. (29 de Diciembre de 2020). *Detección de anomalías con Elastic Stack.* Obtenido de Universitat Oberta de Catalunya (UOC): https://openaccess.uoc.edu/bitstream/10609/126629/6/hfarinangoTFM1220memoria.pdf

Cabello, R. R. (01 de Junio de 2021). *Implementación del SIR Open Source.* Obtenido de Universitat Oberta de Catalunya (UOC): https://openaccess.uoc.edu/bitstream/10609/132147/6/rromerocTFM0621memoria.pdf

Becerra Acosta, G., & Paramo Calderon, C. A. (03 de Diciembre de 2021). *Implementación de un sistema de correlación de eventos basadosen software libre para la empresa sistemas integrales de informpatica SISA S.A. Enfocado al área del SOC SISAMAX.* Obtenido de Universidad Piloto de Colombia: http://repository.unipiloto.edu.co/handle/20.500.12277/11530

Polo Cózar, J. (Junio de 2020). *IMPLEMENTACIÓN DE WAZUH.* Obtenido de Universitat Oberta de Catalunya (UOC): http://hdl.handle.net/10609/117787

Tómas Guerra, J. (27 de Diciembre de 2019). *Monitorización de seguridad con Wazuh.* Obtenido de Universitat Oberta de Catalunya (UOC): http://hdl.handle.net/10609/107166

Fernández Ameijeiras, J. Á. (4 de Enero de 2022). *Implementación de un SIEM para la auditoría de eventos de seguridad sobre cluster de Kubernetes en un entorno multicloud.* Obtenido de Universitat Oberta de Catalunya (UOC): http://hdl.handle.net/10609/138095

Figueroa Suárez, J. A., Rodriguez Andrade, R. F., Bone Obando, C. C., & Saltos Gómez, J. A. (15 de Diciembre de 2017). La seguridad informática y la seguridad de la información. *Casa del Polo del Conocimiento*, 147. Obtenido de La seguridad informática y la seguridad de la información: https://polodelconocimiento.com/ojs/index.php/es/article/view/420

Rangel Méndez, J. A. (24 de Noviembre de 2021). *Sistemas de detección de intrusiones y gestión de eventos e información de seguridad basados en nuevas tecnologías de código abierto.* Obtenido de Universidad Autónoma del Estado de Quintana Roo: http://hdl.handle.net/20.500.12249/2782

Coyla Jarita, Y. (26 de Mayo de 2019). Implementación de un sistema de detección y prevención de intrusos (IDS/IPS), basado en la norma ISO 27001, para el monitoreo perimetral de la seguridad informática, en la red de la Universidad Peruana Unión – Filial Juliaca. *Repositorio de Tesis*, 24 - 26. Obtenido de http://hdl.handle.net/20.500.12840/2002

CSIRT DE GOBIERNO. (7 de Septiembre de 2021). *La Implementación del Mes | No. 3 Seguridad Aplicada: Wazuh.* Obtenido de CSIRT: https://www.csirt.gob.cl/media/2021/09/La_Implementacion_del_Mes_-_Seguridad_Aplicada_-_Septiembre_2021_v2.pdf

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22

Barquero Pastor, A. (2022). *Estudio comparativo entre OpenVas y Wazuh.* Obtenido de Universidad Politécnica de Cartagena: http://hdl.handle.net/10317/11663

Bello Vieda, J. A. (31 de Diciembre de 2019). *Soluciones Endpoint Detection and Response Open-Source. Estado del arte, propuesta de medición, análisis y evaluación para determinar su implementación y aplicabilidad en ambientes empresariales.* Obtenido de Universitat Oberta de Catalunya (UOC): http://hdl.handle.net/10609/107609

Wazuh Inc. (2023). *Wazuh Documentation*. Obtenido de Wazuh: https://wazuh.com

ISO 27001. (17 de Julio de 2023). *A12 SEGURIDAD DE LAS OPERACIONES*. Obtenido de ISO 27001: https://normaiso27001.es/a12-seguridad-de-las-operaciones/

¿Qué es el open source o código abierto? (s/f). Redhat.com. Recuperado el 1 de agosto de 2023, de https://www.redhat.com/es/topics/open-source/what-is-open-source

¿Qué es La Seguridad de la Información y cuál es su importancia? (2020, julio 10). IBERO Posgrados | Blog. https://blog.posgrados.ibero.mx/seguridad-de-la-informacion/

Fortra. (31 de Julio de 2023). *Monitoreo de Seguridad e integridad*. Obtenido de Fortra: https://www.fortra.com/es/soluciones/seguridad-informatica/infraestructura/monitoreo-de-seguridad-e-integridad#:~:text=Monitoree%20su%20sistema%20para%20detectar,da%C3%B1e%20o%20exponga%20informaci%C3%B3n%20cr%C3%ADtica.

Recibido: 2024-04-26, Aprobado tras revisión: 2024-08-22