Implementación de un centro de operaciones de seguridad (SOC) de código abierto

Definición

Un centro de operaciones de seguridad (SOC) es un centro de mando para un equipo de profesionales de IT con experiencia en seguridad de la información que supervisa, analiza y protege a una organización de los ciberataques.

Los SOC son una parte integral para minimizar los costos de una posible violación de datos, ya que no sólo ayudan a las organizaciones a responder a las intrusiones con rapidez, sino que también mejoran constantemente los procesos de detección y prevención.

Existen diferentes tipos de SOC que pueden ser implementados según las necesidades y características de la empresa:

• SOC dedicado o autogestionado. Este modelo tiene una instalación en las instalaciones con personal interno.
• SOC distribuido. También conocido como SOC cogestionado, este modelo cuenta con miembros del equipo semidedicados a tiempo completo o parcial que son contratados internamente para trabajar junto a un proveedor de servicios de seguridad gestionados por terceros (MSSP).
• SOC gestionado. Este modelo cuenta con MSSPs que proporcionan todos los servicios SOC a una empresa.
• SOC de mando. Este modelo proporciona conocimientos de inteligencia sobre amenazas y experiencia en seguridad a otros centros de operaciones de seguridad, normalmente dedica dos. Un SOC de mando no participa en las operaciones o procesos de seguridad reales, sólo en la parte de inteligencia.
• Centro de fusión. Este modelo supervisa cualquier instalación o iniciativa centrada en la seguridad, incluidos otros tipos de SOC o departamentos de TI. Los centros de fusión se consideran SOCs avanzados y trabajan con otros equipos de la empresa, como operaciones de TI, DevOps y desarrollo de productos.
• SOC multifunción. Este modelo tiene una instalación dedicada y personal interno, pero sus funciones y responsabilidades se extienden a otras áreas críticas de la gestión de IT, como los centros de operaciones de red (NOC).
• SOCaaS. Este modelo basado en la suscripción o en el software subcontrata algunas o todas las funciones del SOC a un proveedor en la nube.

En el SOC, el tráfico de Internet, las redes, los equipos de cómputo de escritorio, los servidores, los dispositivos *endpoint*, las bases de datos, las aplicaciones y otros sistemas se examinan continuamente en busca de signos de un ***incidente de seguridad***. El personal del SOC puede trabajar con otros equipos o departamentos, pero este suele ser autónomo, con empleados que tienen conocimientos de alto

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

nivel de IT y ciberseguridad, o se subcontratan estos roles a proveedores de servicios externos. La mayoría de los SOC funcionan las 24 horas del día, con empleados que trabajan por turnos para registrar constantemente la actividad y mitigar las amenazas.

Funciones del SOC

La función de un equipo de operaciones de seguridad y, con frecuencia, de un centro de operaciones de seguridad (SOC), es vigilar, detectar, investigar y responder a las **ciberamenazas** las 24 horas del día. Los equipos de operaciones de seguridad se encargan de supervisar y proteger tanto los activos, como la propiedad intelectual, los datos del personal, los sistemas empresariales y la integridad de la marca. Como componente de implementación del marco general de ciberseguridad de una organización, los equipos de operaciones de seguridad actúan como punto central de colaboración en los esfuerzos coordinados para supervisar, evaluar y defenderse de los ciberataques.

Las responsabilidades básicas de un equipo SOC son las siguientes:

• **El descubrimiento y la gestión de activos**. Estas tareas implican obtener un alto conocimiento de todas las herramientas, el software, el hardware y las tecnologías utilizadas en la organización. También se centran en garantizar que todos los activos funcionen correctamente y sean parcheados y actualizados con regularidad.

• **La supervisión continua** del comportamiento incluye el examen de todos los sistemas las 24 horas del día, los 7 días de la semana, durante todo el año. Esto permite a los SOC dar la misma importancia a las medidas reactivas y proactivas, ya que cualquier irregularidad en la actividad se detecta al instante. Los modelos de comportamiento entrenan a los sistemas de recogida de datos sobre qué actividades son sospechosas y pueden utilizarse para ajustar la información que podría registrarse como falsos positivos.

• **Mantener registros de actividad**. Esto permite a los miembros del equipo SOC retroceder o localizar acciones anteriores que puedan haber dado lugar a una anomalía. El SOC debe registrar todas las comunicaciones y actividades de una empresa.

• **La clasificación de la gravedad de las alertas** ayuda a los equipos a garantizar que las alertas más graves o urgentes se traten primero. Los equipos deben clasificar regularmente las amenazas de ciberseguridad en términos de daño potencial.

• **El desarrollo y la evolución de las medidas de seguridad** es importante para ayudar a los equipos del SOC a estar al día. Los equipos deben crear un plan de respuesta a incidentes (IRP) para defender los sistemas contra ataques nuevos y antiguos. Los equipos también deben ajustar el plan según sea necesario cuando se obtenga nueva información.

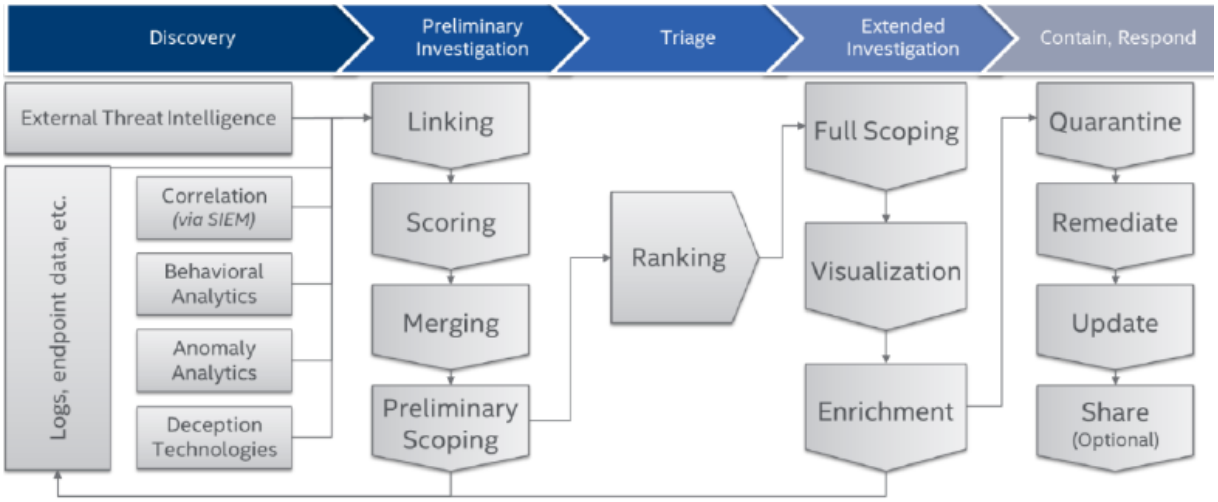
• **La recuperación de incidentes** mediante copias de seguridad permite a una organización recuperar los datos comprometidos. Esto incluye reconfigurar, actualizar o hacer copias de seguridad de los sistemas.

• **El mantenimiento del cumplimiento** es clave para garantizar que los miembros del equipo del SOC y la empresa sigan las normas reglamentarias y organizativas al llevar a cabo los planes de negocio.

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

Normalmente, un miembro del equipo supervisa la legislación y la adecuación del cumplimiento de las medidas legales necesarias.
• Las capacidades adicionales del SOC podrían incluir la ingeniería inversa, el análisis forense, la telemetría de red y el criptoanálisis, según las necesidades específicas de la organización.

En la siguiente figura se puede ver de forma esquematizada el funcionamiento de un SOC tras la detección de una amenaza teniendo en cuenta las diferentes fuentes y activos anteriormente nombrados.



Herramientas de monitorización

Las herramientas empleadas como parte de la capacidad de un SOC son fundamentales para garantizar su capacidad de vigilar y detectar activamente las últimas amenazas. Constantemente surgen nuevas tecnologías para las diferentes áreas de los SOC, por lo que es probable que las tecnologías que actualmente proporcionan mejores resultados terminen quedando obsoletas en un periodo corto de tiempo.

Las herramientas desplegadas por el SOC deben mantenerse actualizadas y gestionarse adecuadamente para asegurar el correcto funcionamiento de este. El conjunto de herramientas no sólo debe tener en cuenta los avances tecnológicos del mercado, sino, lo que es más importante, los cambios en las necesidades de la empresa. La implementación de una herramienta específica dentro del SOC se deberá considerar:

• Las razones empresariales y técnicas de la implementación de nueva tecnología y el impacto de estos cambios sobre la organización.
• La compatibilidad de las nuevas herramientas con las otras ya implementadas en la empresa.
• Hay que asegurar que el personal del SOC está formado en el uso de las nuevas herramientas.
• El equipo SOC ha de tener una comprensión estratégica de cómo las nuevas herramientas contribuyen a las necesidades generales del SOC

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

Tecnología de gestión de eventos e información de seguridad- SIEM

SIEM son las siglas en inglés de la **gestión de eventos e información de seguridad** y proporciona a las organizaciones la detección, el análisis y la respuesta ante las posibles amenazas de seguridad en la empresa.

El software SIEM combina la gestión de la información de seguridad (SIM) y la gestión de eventos de seguridad (SEM) para proporcionar un análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones y el hardware de la red. El software SIEM coteja los eventos con las reglas de los motores de análisis y los indexa para realizar búsquedas en menos de un segundo con el fin de detectar y analizar las amenazas avanzadas utilizando la inteligencia recopilada globalmente. Esto proporciona a los equipos de seguridad tanto una visión como un registro de las actividades dentro de su entorno de IT, proporcionando la capacidad de análisis de datos, correlación de eventos, agregación, informes y gestión de registros.

El software SIEM proporciona una serie de características y beneficios, entre ellos:

- Agregación en un único punto de múltiples fuentes de datos.
- Cuadros de mando personalizados y gestión del flujo de trabajo de las alertas.
- Integración con otros productos.

Las principales funciones de un SIEM son las siguientes:

- **Agregación de datos:** Las soluciones SIEM necesitan datos de múltiples fuentes como parte de la agregación de datos, trasladando la información a un único lugar. Los sistemas SIEM recogen los datos por sí mismos o utilizan reenviadores para enviar los registros de otros sistemas al sistema SIEM.
- **Colectores SIEM**: Los colectores pueden configurarse para obtener datos de registro de los equipos de la red, pudiendo conectarse directamente al sistema y obtener los registros.
- **Transmisores SIEM**: Los SIEM Forwarders pueden enviar datos de registro a la solución SIEM desde el equipo, ya que implican una instalación de software, conocida como agente que puede reenviar eventos a la solución SIEM.
- **Correlación de eventos de seguridad:** La correlación de eventos de seguridad consiste en tratar de detectar patrones en los datos recogidos por los sistemas para encontrar identificadores de actividad maliciosa en la red. Si se descubren patrones sospechosos, se marcan, lo que permite a los analistas de seguridad investigar más a fondo y tomar medidas correctivas.
- **Análisis avanzado**: El análisis avanzado puede incluir el análisis del comportamiento mediante el análisis de los datos recogidos en el SIEM para detectar cambios de comportamiento inesperados dentro de la red empresarial o el estudio de una serie de acciones realizadas por un usuario consideradas como indicadores de un posible ataque.
- **Automatización del SOC**: Las capacidades de automatización del SOC de un sistema SIEM pueden actuar sobre los eventos de seguridad haciendo el análisis como lo haría el analista del SOC, pudiendo así dar un resultado. Por ejemplo, un evento de seguridad es analizado por la solución SIEM y,

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

basándose en criterios, la solución SIEM determina que este evento es un incidente grave y, en consecuencia, plantea un incidente en el sistema de gestión de incidentes con una prioridad crítica.

• **Cuadros de mando e informes**: Todas las soluciones SIEM disponen de cuadros de mando para facilitar la visualización del panorama de las amenazas y ofrecerles indicadores de lo que está ocurriendo en los sistemas de los que el SIEM está recopilando datos. Estos cuadros de mando también permiten la elaboración de informes para poder ver el número de amenazas identificadas durante un periodo definido, lo que permite a las organizaciones determinar el nivel de amenazas al que se han enfrentado a lo largo del tiempo.
• **Búsqueda de amenazas**: Utilizando las herramientas de análisis de búsqueda proporcionadas por el SIEM, los analistas de seguridad pueden consultar los datos del SIEM y determinar el impacto en la organización durante los últimos meses o incluso años permitiendo la búsqueda de nuevos patrones y amenazas que van surgiendo diariamente con las publicaciones de nuevos exploits y vulnerabilidades.
• **Análisis forense o respuesta a incidentes:** Cuando las organizaciones descubren que han sufrido un ataque, necesitan determinar rápidamente cuándo se produjo la brecha, qué acciones se llevaron a cabo y si los responsables siguen dentro de la red, es decir, siguen dentro de los sistemas de la organización. El análisis forense permite analizar los datos recogidos durante un periodo de tiempo e intentar determinar la gravedad de los acontecimientos que condujeron a la violación, incluidos los ataques iniciales, el momento de la primera violación y las actividades realizadas después de entrar en los sistemas de la organización.

Software de monitorización de seguridad
Mientras que la monitorización de la red proporciona una recopilación de datos para el análisis de los flujos de tráfico básicos, la estructura general y la integridad de sus sistemas, la monitorización de la seguridad de la red protege de las numerosas vulnerabilidades y explotaciones.
Incluso más importante que la monitorización general, la supervisión de la seguridad analiza una multitud de factores complejos (carga útil de la red, protocolos de red, comunicaciones cliente-servidor, sesiones de tráfico cifrado, patrones de tráfico y flujo de tráfico) para alertar a los analistas de actividades maliciosas conocidas en un intento de contener un ataque.
La herramienta de supervisión adecuada le ofrece un servicio permanente de vigilancia a un entorno empresarial en busca de amenazas y comportamientos sospechosos. Los administradores y analistas pueden entonces investigar y calibrar los patrones anormales de los usuarios y tomar las medidas adecuadas.

A diferencia de la supervisión operativa de la red, la supervisión de la seguridad de la red y los analistas que la utilizan también deben ser capaces de detectar intrusiones y todas las formas de ataque incluidas las amenazas nuevas, de día cero y de última generación, para poder tomar decisiones basadas en estas acciones anómalas.
Ningún experto en seguridad puede garantizar una protección del 100% frente a los ataques, pero las nuevas tecnologías de supervisión y análisis continuos de la red proporcionan niveles de apoyo a la

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

detección y mitigación que pueden disminuir considerablemente la posibilidad de un ataque o una brecha. Aquellos que puedan aprovechar la supervisión, el análisis y la corrección continuos de la seguridad de la red en tiempo real también se beneficiarán de una reducción del tiempo de detección y de la capacidad de reducir o evitar drásticamente los daños resultantes.
Es importante señalar que un atacante tarda sólo unos minutos en comprometer y exfiltrar datos. Por lo tanto, la calidad de un sistema de supervisión de la seguridad de la red equivale a la velocidad con la que se notifica el tráfico sospechoso a los analistas.
Los elementos de monitorización de seguridad se pueden dividir principalmente entre elementos de monitorización de red y elementos de monitorización de equipos.

Los principales elementos de monitorización de red son:
• Cortafuegos: Es un dispositivo de seguridad de red que supervisa el tráfico de red entrante y saliente y permite o bloquea los paquetes de datos basándose en un conjunto de reglas de seguridad. Su objetivo es establecer una barrera entre la red interna y el tráfico entrante de fuentes externas como Internet para bloquear el tráfico malicioso. [
• IDS/IPS: Es un sistema que supervisa el tráfico de la red en busca de actividad sospechosa y alerta cuando se descubre dicha actividad. Aunque la detección de anomalías y la elaboración de informes son las funciones principales, algunos sistemas de detección de intrusiones (IPS) son capaces de tomar medidas cuando se detecta actividad ilícita o tráfico anómalo, llegando a provocar el bloqueo del tráfico enviado desde direcciones IP maliciosas. Un IDS únicamente supervisa los paquetes de red en busca de tráfico de red potencialmente malicioso sin ejecutar acciones sobre este.
• Proxy de navegación: Herramienta que traduce el tráfico entre redes o protocolos. Es un servidor intermediario que separa a los usuarios de los destinos por los que navegan. Los servidores proxy ofrecen diferentes niveles de inspección de red, privacidad y seguridad según el tipo de tráfico, la política o las necesidades de la empresa.
• Sondas: Es la tecnología encargada de monitorizar la red y detectar comportamientos maliciosos. Detecta ataques y programas malignos mediante el análisis red en tiempo real por medio de las reglas implementadas en la misma. Para su correcto funcionamiento necesitará un duplicado del tráfico que se desee analizar, habitualmente se encuentran en elementos críticos de las redes industriales ya que permiten el análisis detallado a bajo nivel de los protocolos utilizados por componentes de este tipo de redes.

Por otro lado, las principales herramientas de monitorización de equipos de punto final son:
• Detección y respuesta a los puntos finales (EDR): También conocida como detección y respuesta a las amenazas en los puntos finales (ETDR), es una solución de seguridad integrada para los puntos finales que combina la supervisión continua en tiempo real y la recopilación de datos de los puntos finales con capacidades de respuesta y análisis automatizados basados en reglas. Investiga actividades sospechosas en los equipos, empleando un alto grado de automatización para permitir a los analistas de seguridad identificar y responder rápidamente a las amenazas.

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

• Sistema de monitorización de procesos: Permite en equipos Windows la monitorización y el registro de la actividad del sistema en el registro de eventos de Windows. Proporciona información detallada sobre la creación de procesos, las conexiones de red y los cambios en el tiempo de creación de archivos del equipo.

Fase de diseño

Durante la fase de diseño se ha buscado garantizar la mayor securización en la red del Call Center mediante la manera más sencilla de implementación de los activos y modificaciones necesarias para conseguirlo.

Para ello se ha dividido en dos puntos claves Diseño de la segmentación de la red del Call Center y Diseño de la centralización, visualización y monitorización de logs

Finalmente se detallarán las especificaciones técnicas necesarias para tener en cuenta durante el dimensionamiento de las herramientas durante el proceso de introducción de la red del call center en el apartado Especificaciones técnicas de las herramientas.

Diseño de la segmentación de la red del call center

• Arquitectura de red: La piedra angular del diseño de una red de call center segura es emplear un enfoque de defensa en profundidad que incluya zonas y comunicaciones seguras entre las diferentes subredes. Diseñar un acceso remoto seguro y fiable se está convirtiendo rápidamente en una necesidad desde un punto de vista práctico.

• Configuración segura de los dispositivos: Con las redes convergentes de hoy en día, la configuración de los dispositivos de la red de un call center es cada vez más complicada, y las funciones de seguridad se desactivan con frecuencia para facilitarla. Como resultado, las redes LAN y WAN son vulnerables a violaciones tanto deliberadas como involuntarias.

• Gestión de la seguridad de la red: Un sistema competente de gestión de la seguridad de la red no sólo le ayudará a implantar y hacer cumplir las políticas de seguridad en la red, sino que también le permitirá supervisar y registrar los eventos de la red, así como proporcionar alertas de eventos de seguridad en tiempo real.

Una arquitectura de defensa en profundidad puede diseñarse en tres pasos:

• La segmentación de la red: La división de la red en zonas físicas o lógicas con requisitos de seguridad similares se conoce como segmentación de la red. La ventaja de segmentar la red es que cada componente puede centrarse en los problemas de seguridad individuales a los que se enfrenta cada sección de la red. Debido a que cada dispositivo es responsable de un área específica de la red, en lugar de ser responsable de la seguridad de toda la red, el uso de la estrategia de segmentación es aconsejable.

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

• Definir las interacciones entre zonas: El tráfico no autorizado se puede filtrar mediante cortafuegos una vez que se haya definido el tráfico preciso que debe pasar por las zonas seguras. La lista blanca del tráfico que debe pasar entre cada zona y el bloqueo del resto del tráfico es una práctica habitual. La inspección profunda de paquetes se utiliza habitualmente en los IDS para filtrar los protocolos industriales a un nivel más fino que los cortafuegos normales. Muchos IDS también incluyen un modo transparente que permite instalarlos en redes existentes sin necesidad de modificar el esquema IP de la red.

- Otra buena práctica de seguridad para vincular las redes del CC a las redes informáticas de la empresa o a Internet es utilizar un cortafuegos para crear una zona desmilitarizada (DMZ). Aunque no hay conexión directa entre la red CC protegida y la red de la empresa cuando se utiliza una DMZ, ambas pueden acceder al servidor de datos. Al eliminar la conexión directa entre las redes de CC y de la empresa, se reduce en gran medida el riesgo de que el tráfico ilegal viaje a través de las zonas, lo que podría poner en peligro la seguridad de toda la red.

• Acceso remoto seguro: Por último, en el mercado de los sistemas de control y automatización industrial hay una creciente demanda de supervisión y mantenimiento de las instalaciones a distancia. Esto aumenta en gran medida las posibilidades de que un usuario hostil acceda a la red. Las redes que requieren que el sitio remoto esté conectado al CC en todo momento deben emplear una red privada virtual (VPN) que utilice un mecanismo de cifrado seguro, como IPsec u OpenVPN, para evitar que usuarios no autorizados accedan a la red. El uso de una VPN tiene tres ventajas principales.

• La trasmisión de datos va cifrada extremo a extremo.

• Se exige que tanto el remitente como el destinatario de la sesión verifiquen sus identidades, lo que garantiza que los datos sólo se transfieren entre dispositivos verificados.

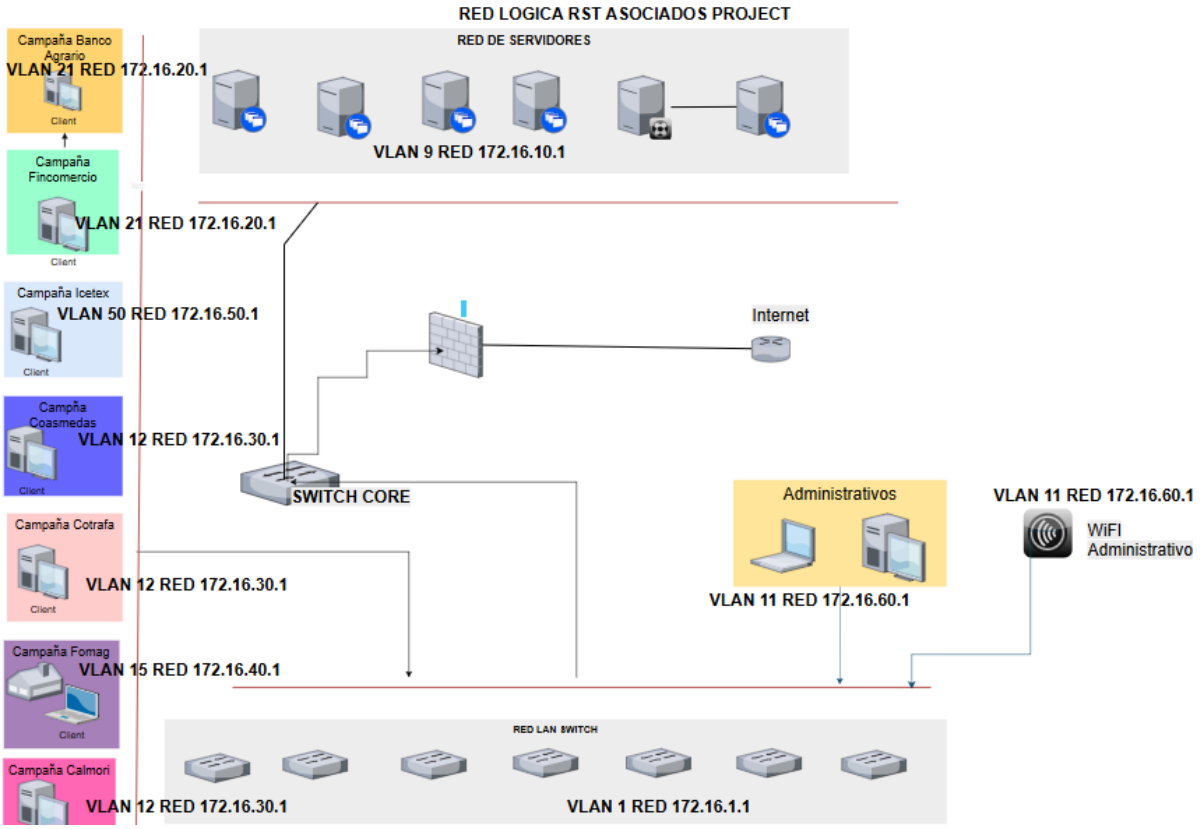
• Puede proteger la integridad de los datos al exigir el cifrado y la autenticación.

Siguiendo estas normas y basándonos en un marco teórico de una red industrial simple determinada por tres zonas.

• Zona de red corporativa de usuarios administrativos
• Zona de red corporativa de servidores
• Zona de red corporativa Usuarios Home Office
• Red operacional de usuarios de campañas
• Red operacional de SWITCH Capa II
• Red operacional Desarrollo de Software.
• Red operacional WiFi

Se ha desarrollado la siguiente topología de red con elementos de seguridad y segmentaciones basándose en los criterios anteriormente citados.

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Los componentes necesarios y segmentaciones de la red de la Figura anterior, Diseño seguro de red operacional se detallan a continuación:

• Perímetro: router de entrada y salida a Internet y firewall Fortinet para la segmentación de las redes en la organización

• Red corporativa de servidores: servicios de la empresa como Directorio Activo, servidores de Archivos, Servidor de Backup, Servidor de telefonía: Neotel-Ucontact-Anw, Servidores de BD, servidores de Aplicaciones, que contienen toda la información sensible para la empresa

• Red corporativa de usuarios administrativos: red de uso habitual para empleados de la empresa que no tengan un rol operacional, por ejemplo: financiera, gestión humana, calidad y formación...

• Red operacional de campañas: red de uso habitual para empleados de la empresa que tengan un rol operacional, por ejemplo: Campaña Banco Agrario, Icetex, Cotrafa... proporciona conectividad con el entorno OT aislado del resto de redes

• Red operacional home office: red de usuarios que trabajan desde su casa.

• IDS01: monitorización de entrada y salida a Internet y monitorización inter-VLANs en toda la red

• IDS02: monitorización intra-VLAN de la red de servidores

• IDS03: monitorización de la conexión entre la red IT y la red OT

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

Diseño de la centralización, visualización y monitorización de logs

Una solución de centralización de logs aporta la visión centralizada de todo lo que está ocurriendo en los sistemas de la empresa, y va a permitir tanto generar alertas automáticas basadas en una sucesión de eventos considerados anómalos, como tener disponible toda la información pasada para poder llevar a cabo investigaciones futuras.

Esta solución debe cumplir los siguientes requisitos para ser confiable:

- Garantizar la disponibilidad de los datos en todo momento.
- Ser escalable a cualquier tamaño de la empresa.
- Restringir el acceso a los datos únicamente a personal autorizado.
- Cifrar los datos at-rest y on-transit para evitar acceso ilegítimo a la información.
- Establecer diferentes periodos de retención de los datos y tipos de almacenamiento para los mismos.
- Generar alertas en pseudo tiempo real basadas en reglas previamente esta
- Normalizar los datos de las diferentes fuentes en un único esquema.

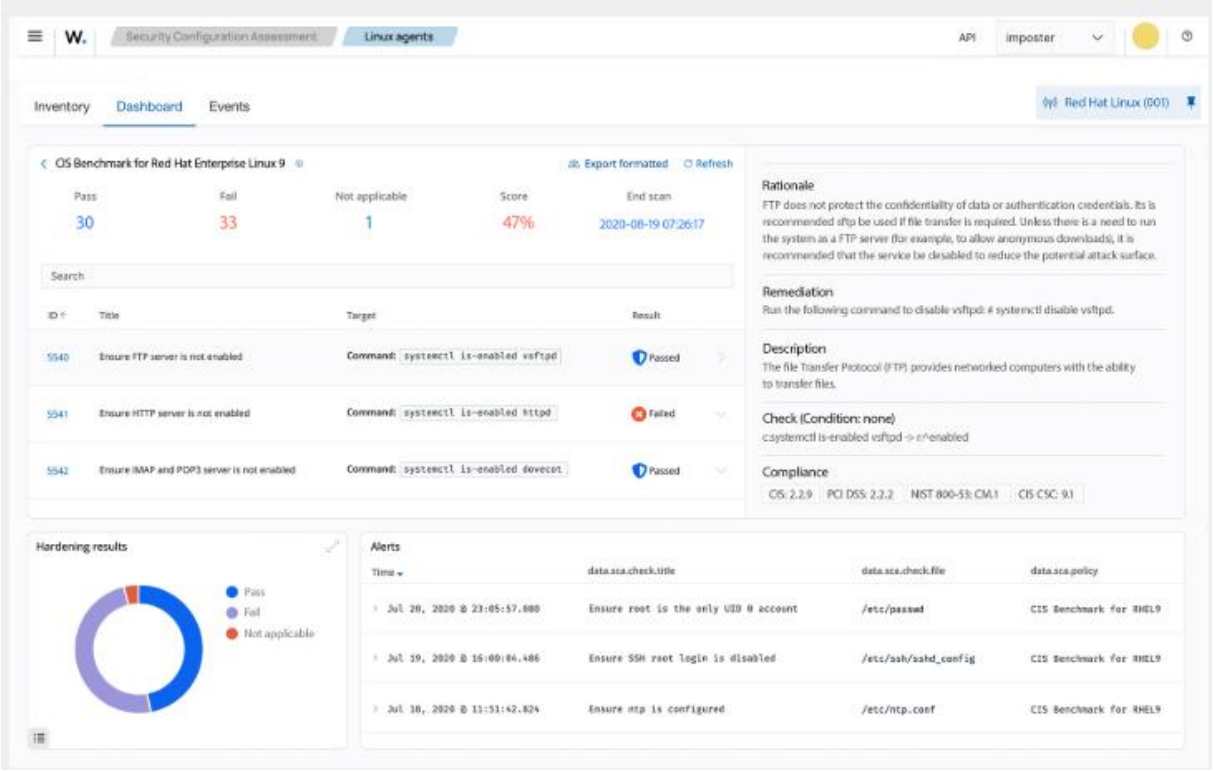
En base a estos puntos se considera **Wazuh**, como herramienta de centralización, gestión, visualización y monitorización de eventos. Esta solución es de código abierto y ofrece licencias libres para su uso gratuito, Wazuh ofrece una sólida monitorización y protección de seguridad para los activos de TI de RST ASOCIADOS PROJECT mediante sus capacidades de Gestión de Información y Eventos de Seguridad **(SIEM)** y Detección y Respuesta Extendidas (XDR). Los casos de uso de Wazuh están diseñados para proteger los activos digitales y mejorar la ciberseguridad de la empresa.

Casos de uso

Evaluación de la configuración

Wazuh supervisa la configuración del sistema y de las aplicaciones para garantizar que cumpla con sus políticas de seguridad, estándares y guías de refuerzo. Los agentes de Wazuh realizan análisis periódicos para detectar errores de configuración o vulnerabilidades de seguridad en los endpoints que puedan ser explotadas por actores de amenazas. Además, puede personalizar estas comprobaciones de configuración para que se ajusten a las necesidades de su organización. Las alertas de seguridad incluyen recomendaciones para una mejor configuración, referencias y compatibilidad con el cumplimiento normativo.

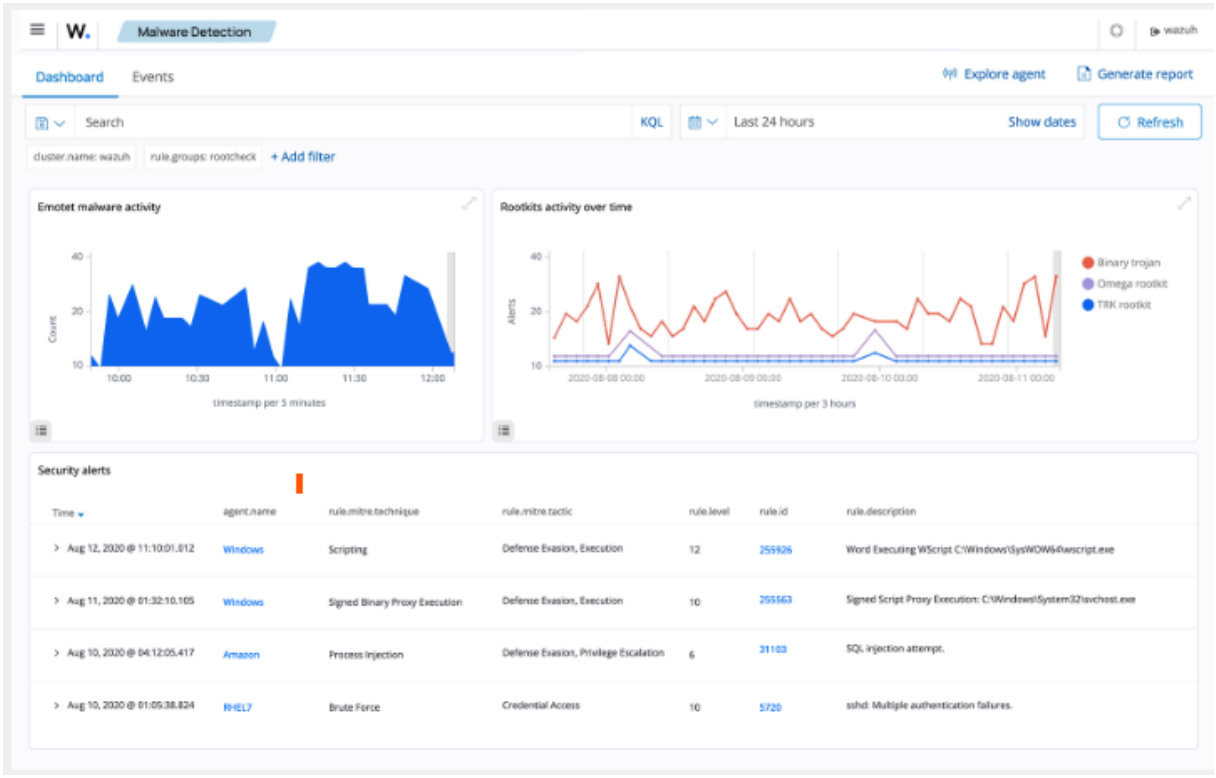
NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Detección de malware

Wazuh detecta actividades maliciosas e indicadores de vulnerabilidad que ocurren en los endpoints como resultado de una infección de malware o un ciberataque. El conjunto de reglas preconfiguradas de Wazuh y las funciones como la Evaluación de la Configuración de Seguridad (SCA), Rootcheck y la Supervisión de la Integridad de Archivos (FIM) ayudan a detectar actividades maliciosas y anomalías. Puede configurar y personalizar estas funciones de Wazuh para adaptarlas a las necesidades de su organización.

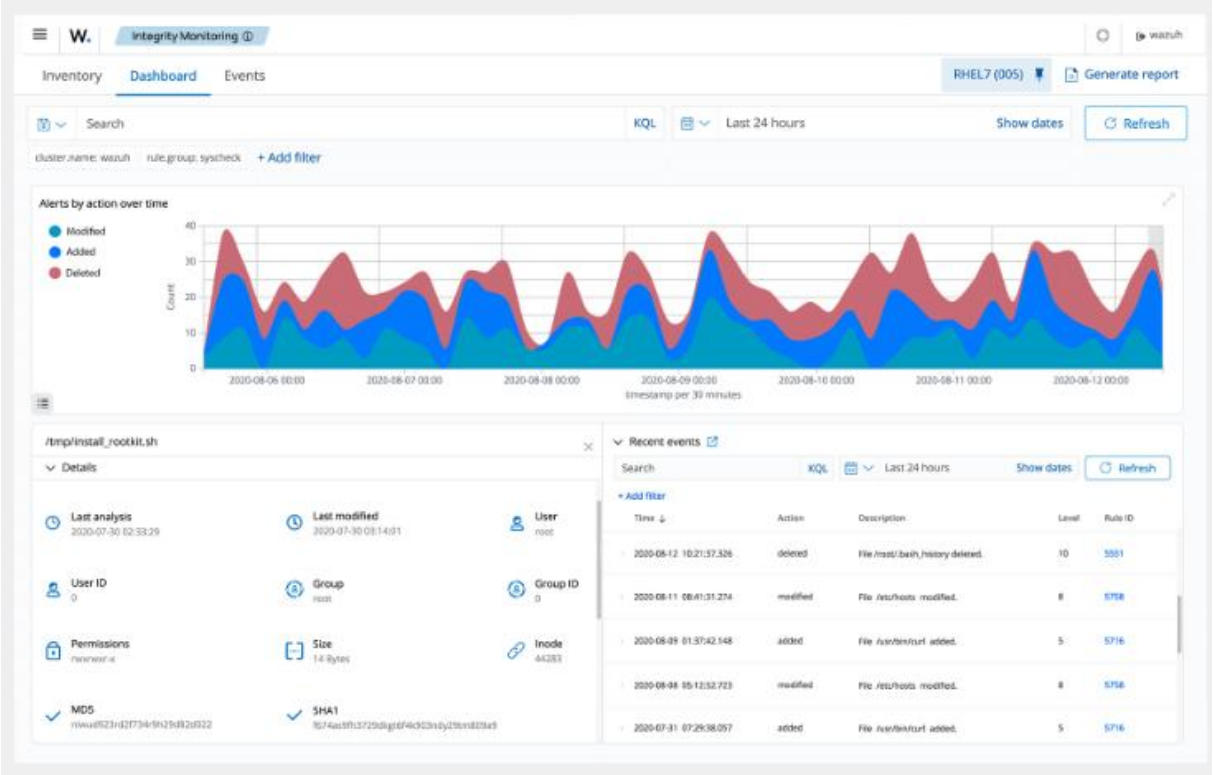
NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Monitoreo de la integridad de los archivos

Wazuh monitorea el sistema de archivos, identificando cambios en el contenido, los permisos, la propiedad y los atributos de los archivos que necesita monitorear. Además, identifica de forma nativa a los usuarios y las aplicaciones que se utilizan para crear o modificar archivos. Puede usar la función de Monitoreo de Integridad de Archivos de Wazuh junto con la inteligencia de amenazas para identificar amenazas o endpoints comprometidos. Además, FIM ayuda a cumplir con diversas normas de cumplimiento normativo, como PCI DSS, NIST y otras.

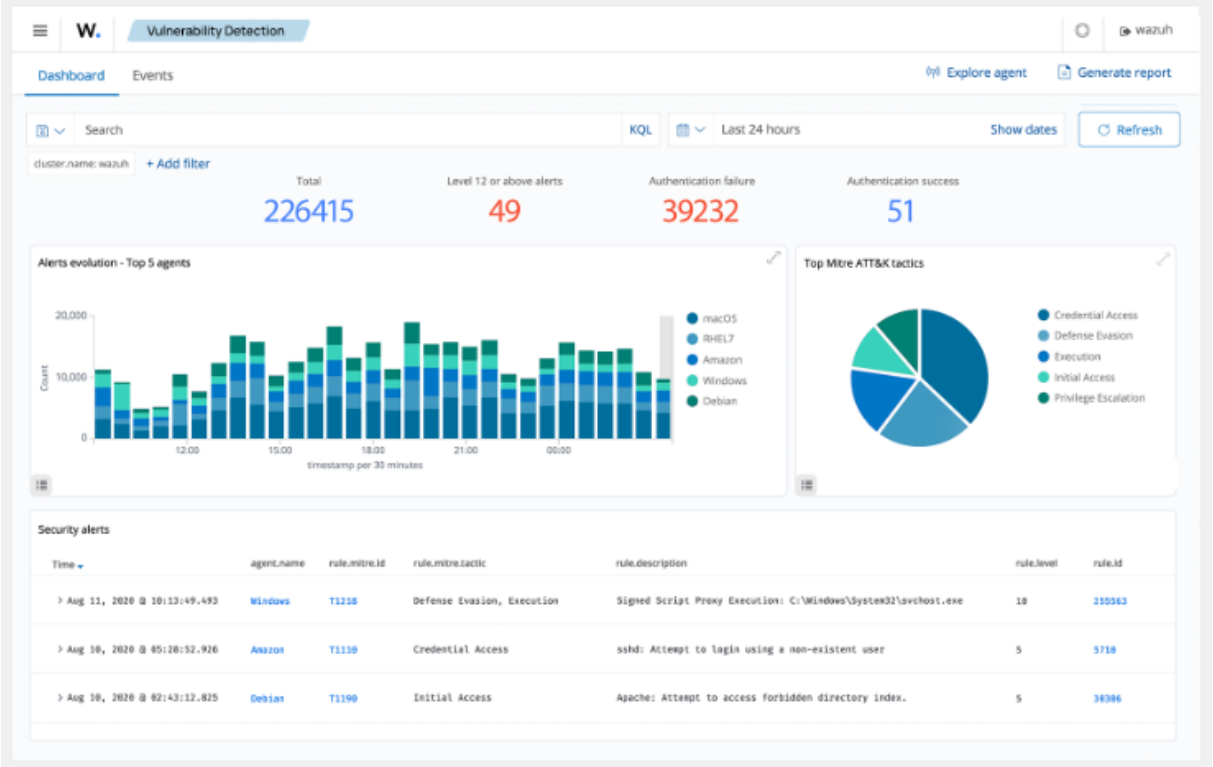
NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Caza de amenazas

Wazuh ofrece visibilidad completa de los endpoints e infraestructura monitoreados. Ofrece funciones de retención de registros, indexación y consulta que nos ayudan a investigar amenazas que puedan haber eludido los controles de seguridad iniciales. Las reglas de detección de amenazas se mapean con el marco MITRE ATT&CK para facilitar la investigación y la referenciación de tácticas, técnicas y procedimientos comúnmente utilizados por los atacantes. Wazuh también se integra con fuentes y plataformas de inteligencia de amenazas de terceros para una mejor detección de amenazas.

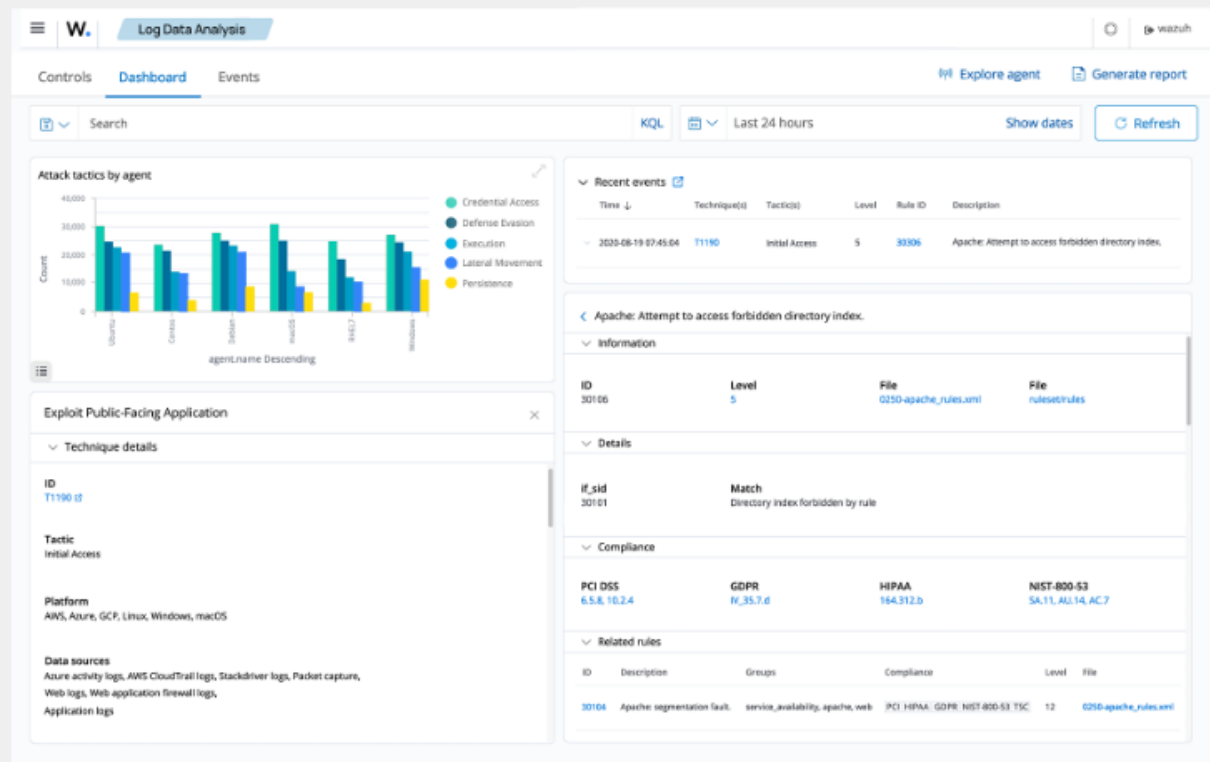
NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Análisis de datos de registro

Los agentes de Wazuh recopilan registros del sistema operativo y de las aplicaciones, y los reenvían de forma segura al servidor de Wazuh para su análisis y almacenamiento basado en reglas. Las reglas de Wazuh detectan errores de la aplicación o del sistema, configuraciones incorrectas, actividades maliciosas, infracciones de políticas y otros problemas de seguridad y operativos.

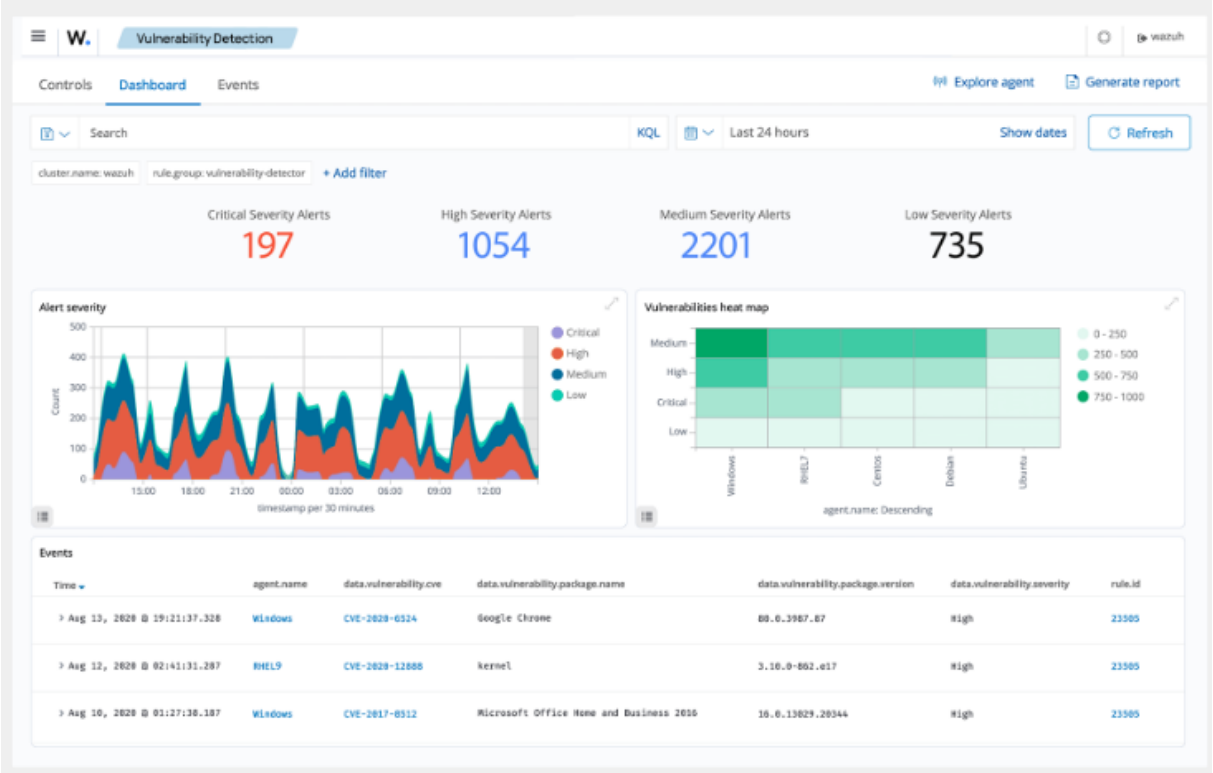
NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Detección de vulnerabilidades

Los agentes de Wazuh extraen datos del inventario de software y los envían al servidor de Wazuh. Estos datos se correlacionan con bases de datos CVE (vulnerabilidades y exposiciones comunes) que se actualizan constantemente para identificar software vulnerable conocido. La detección automatizada de vulnerabilidades le ayuda a encontrar las fallas en sus activos críticos y a tomar medidas correctivas antes de que los atacantes las exploten con fines maliciosos.

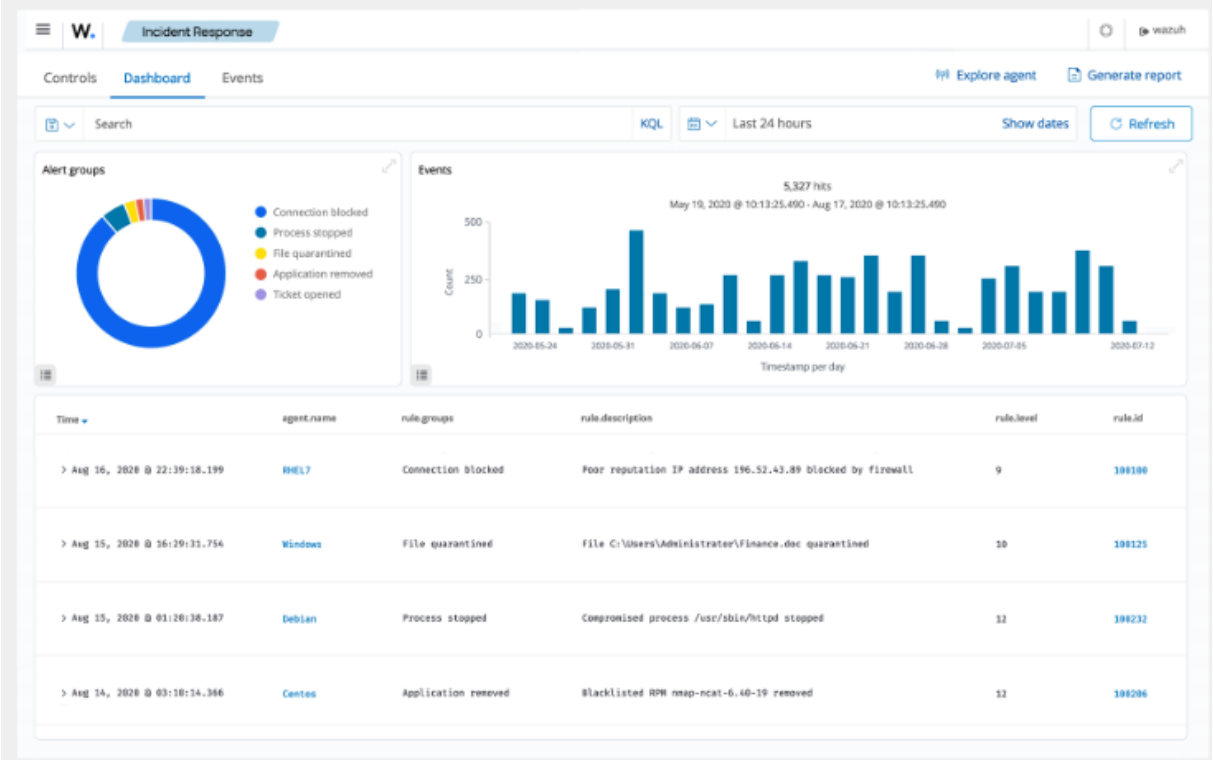
NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Respuesta a incidentes

Wazuh ofrece respuestas activas listas para usar para implementar diversas contramedidas contra amenazas en curso. Estas respuestas se activan cuando se cumplen ciertos criterios, incluyendo acciones como bloquear el acceso de red a un endpoint desde la fuente de la amenaza, entre otras. Además, Wazuh puede utilizarse para ejecutar comandos o consultas del sistema de forma remota, identificar indicadores de compromiso (IOC) y facilitar la respuesta a incidentes.

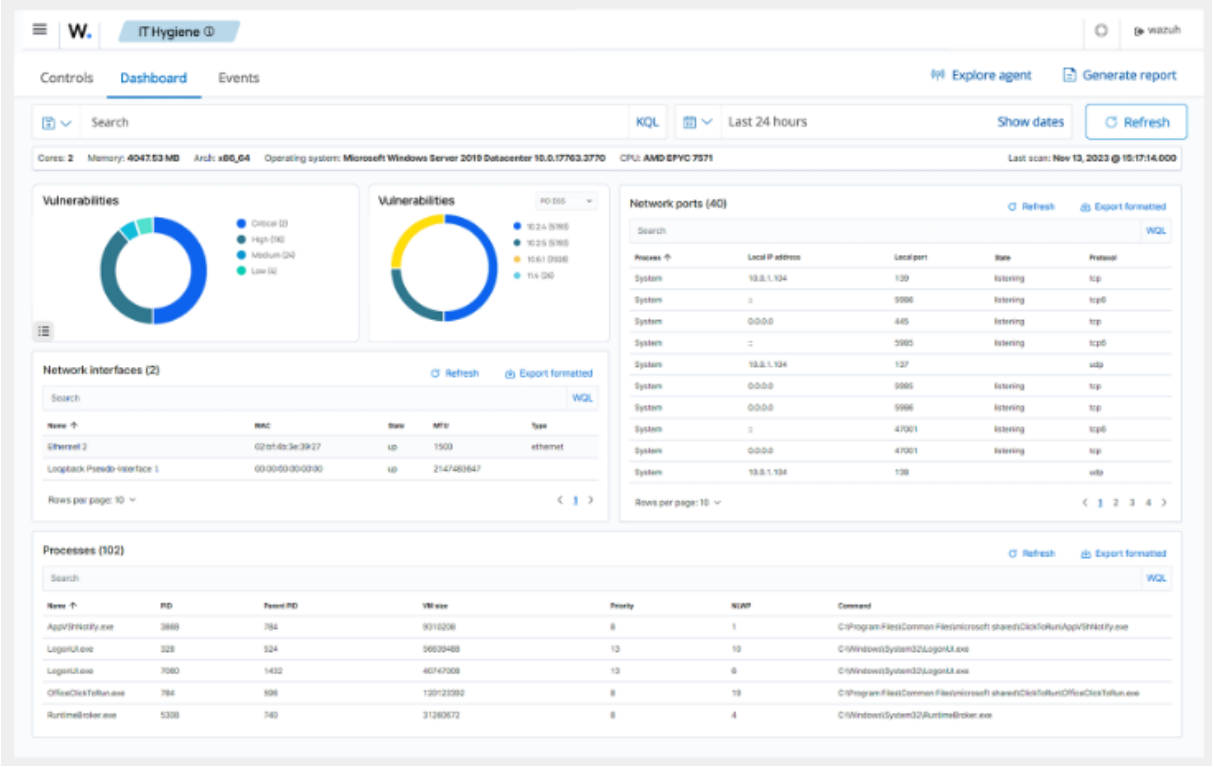
NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Higiene de TI

Wazuh crea un inventario actualizado del sistema de todos los endpoints monitoreados. Este inventario contiene datos como aplicaciones instaladas, procesos en ejecución, puertos abiertos, información de hardware y sistema operativo, entre otros. Recopilar esta información ayuda a las organizaciones a optimizar la visibilidad de los activos y a mantener una buena higiene de TI. Otras funciones de Wazuh, como la detección de vulnerabilidades, la evaluación de la configuración de seguridad y la detección de malware, ayudan a proteger los endpoints monitoreados y a mejorar la higiene de TI.

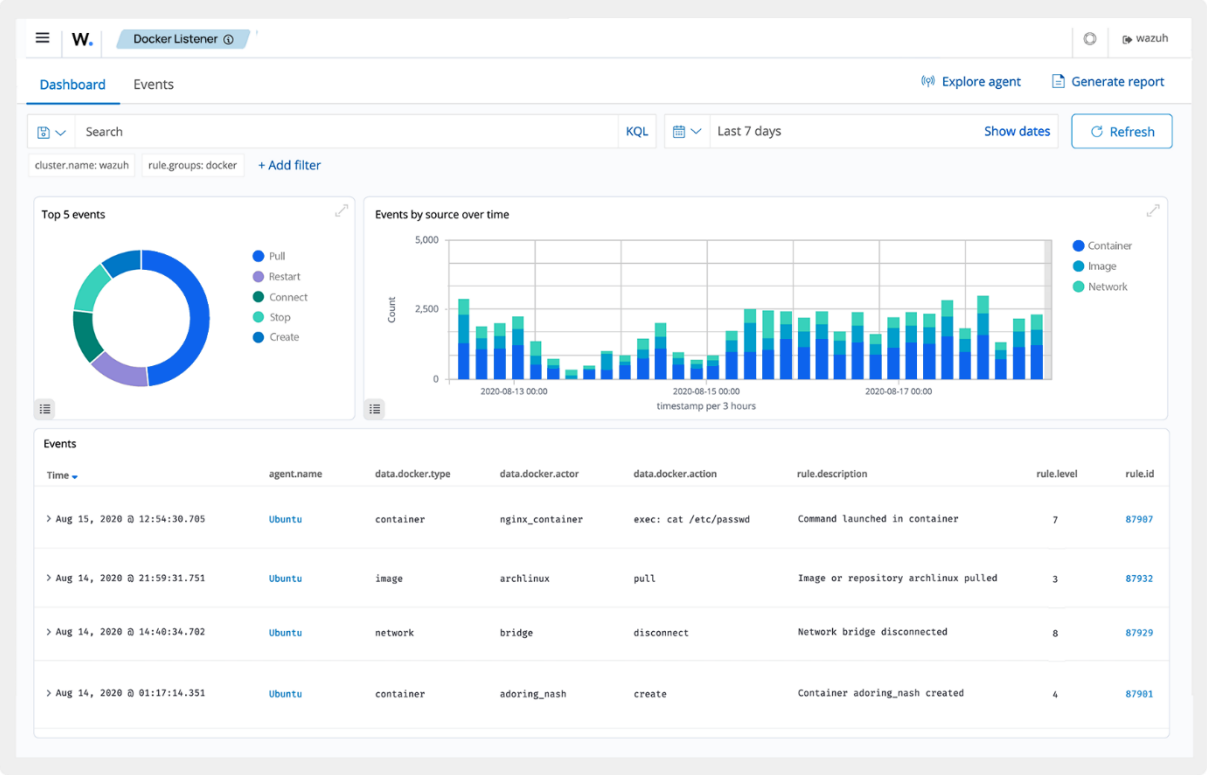
NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Seguridad de los contenedores

Wazuh proporciona visibilidad de seguridad en hosts y contenedores Docker, monitorizando su comportamiento y detectando amenazas, vulnerabilidades y anomalías. El agente de Wazuh se integra de forma nativa con el motor Docker, lo que permite a los usuarios monitorizar imágenes, volúmenes, configuraciones de red y contenedores en ejecución. Wazuh recopila y analiza continuamente información detallada del tiempo de ejecución. Por ejemplo, alerta sobre contenedores ejecutándose en modo privilegiado, aplicaciones vulnerables, un shell ejecutándose en un contenedor, cambios en volúmenes o imágenes persistentes y otras posibles amenazas.

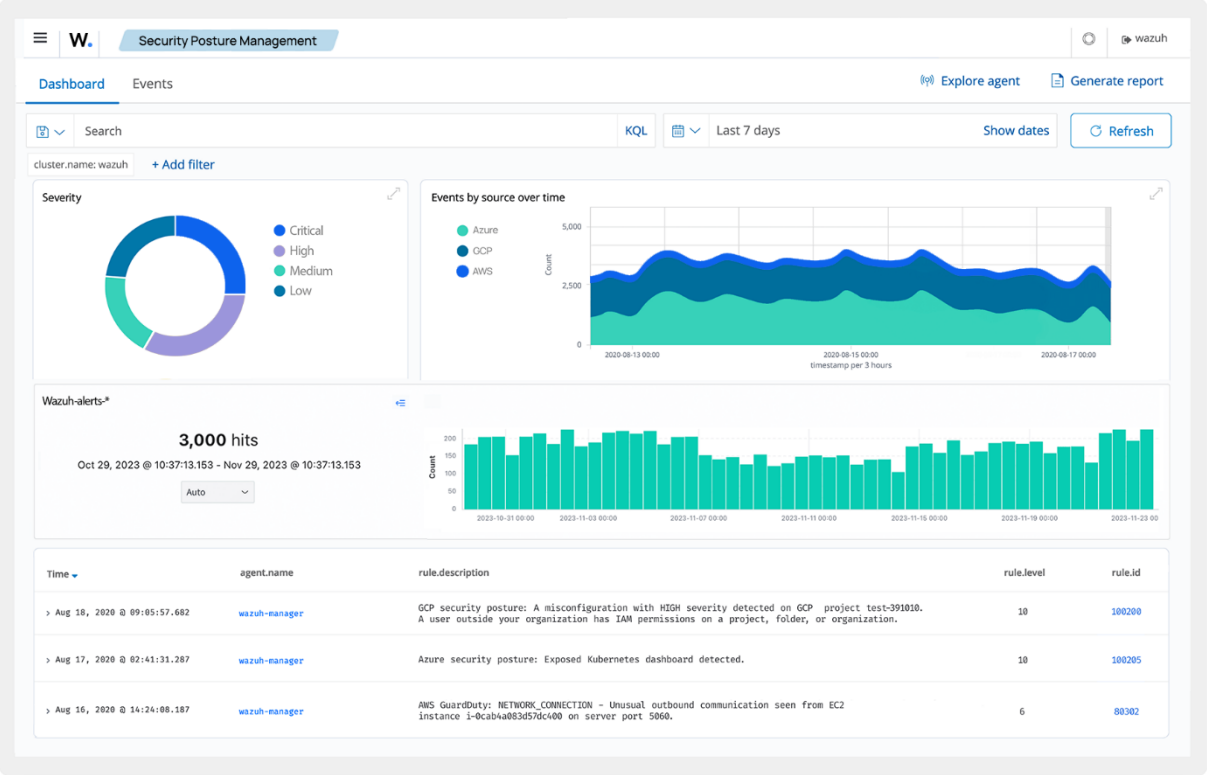
NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Manejo de la postura

Wazuh se integra con plataformas en la nube, recopilando y agregando datos de seguridad. Alerta sobre riesgos y vulnerabilidades de seguridad detectados para garantizar la seguridad y el cumplimiento de las normas regulatorias.

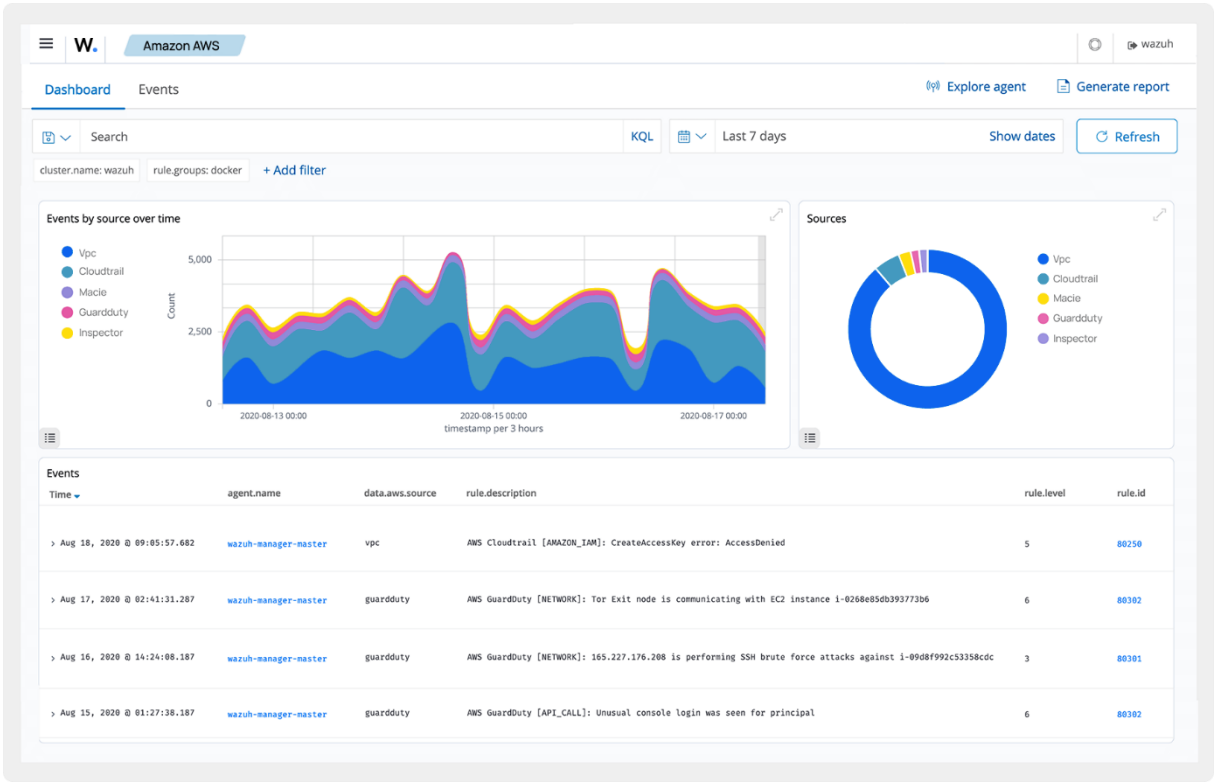
NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Protección de la carga de trabajo

Wazuh supervisa y protege las cargas de trabajo tanto en entornos de nube como locales. Puede integrar Wazuh con plataformas en la nube como AWS, Microsoft Azure, GCP, Microsoft 365 y GitHub para supervisar servicios, máquinas virtuales y las actividades que ocurren en estas plataformas. La gestión centralizada de registros de Wazuh ayuda a las organizaciones que utilizan estas plataformas en la nube a cumplir con los requisitos normativos.

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Componentes centrales

Indexador Wazuh

El indexador Wazuh es un motor de búsqueda y análisis de texto completo altamente escalable. Se encarga de indexar y almacenar las alertas generadas por el servidor Wazuh. Puede instalarse como un clúster de uno o varios nodos, según las necesidades del entorno.

Servidor Wazuh

El servidor gestiona los agentes, configurándolos y actualizándolos remotamente cuando es necesario. Este componente analiza los datos recibidos de los agentes, procesándolos mediante decodificadores y reglas, y utiliza inteligencia de amenazas para buscar indicadores de vulnerabilidad.

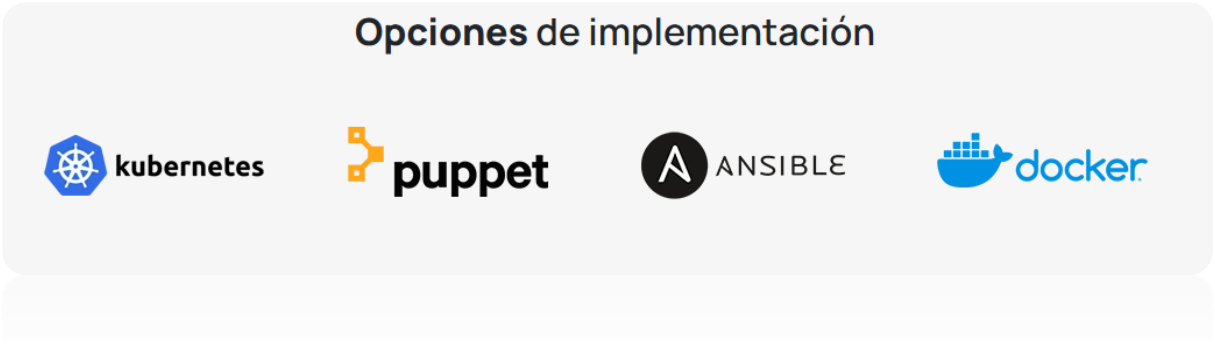
Panel de control de Wazuh

Una interfaz web flexible e intuitiva para la minería, el análisis y la visualización de datos. El panel de control permite gestionar la configuración de Wazuh y supervisar su estado.

Agente de seguridad de endpoints

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

El agente Wazuh es un componente multiplataforma que se ejecuta en los endpoints que se van a monitorear. Ofrece capacidades de prevención, detección y respuesta.



Arquitectura

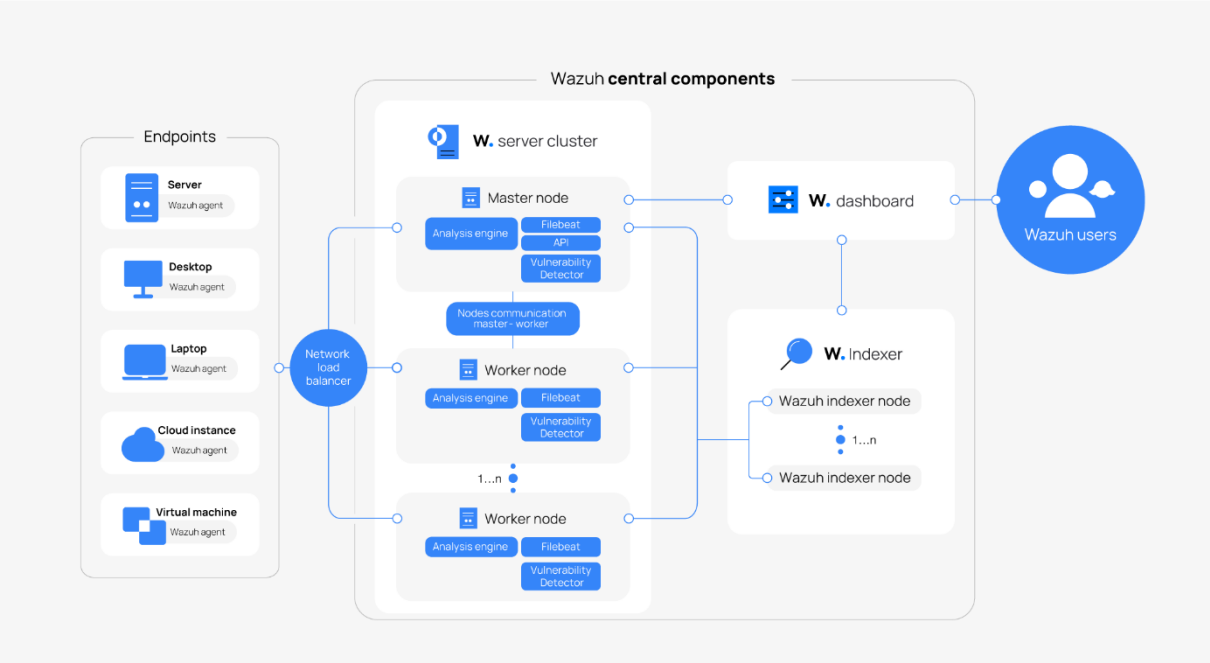
La arquitectura de Wazuh se basa en agentes que se ejecutan en los endpoints monitoreados y que reenvían datos de seguridad a un servidor central. Se admiten dispositivos sin agente, como firewalls, switches, routers y puntos de acceso, que pueden enviar datos de registro de forma activa mediante Syslog, SSH o su API. El servidor central decodifica y analiza la información entrante y envía los resultados al indexador de Wazuh para su indexación y almacenamiento.

El clúster de indexadores de Wazuh es un conjunto de uno o más nodos que se comunican entre sí para realizar operaciones de lectura y escritura en índices. Las implementaciones pequeñas de Wazuh, que no requieren el procesamiento de grandes cantidades de datos, pueden gestionarse fácilmente con un clúster de un solo nodo. Se recomiendan los clústeres multinodo cuando se monitorizan muchos endpoints, se anticipa un gran volumen de datos o se requiere alta disponibilidad.

En entornos de producción, se recomienda implementar el servidor y el indexador de Wazuh en hosts diferentes. En este caso, se utiliza Filebeat para reenviar de forma segura las alertas y los eventos archivados de Wazuh al clúster del indexador de Wazuh (de un solo nodo o multinodo) mediante cifrado TLS.

El diagrama a continuación representa una arquitectura de implementación de Wazuh. Muestra los componentes de la solución y cómo el servidor y los nodos indexadores de Wazuh pueden configurarse como clústeres, lo que proporciona equilibrio de carga y alta disponibilidad.

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co



Comunicación entre el agente de Wazuh y el servidor de Wazuh

El agente de Wazuh envía continuamente eventos al servidor de Wazuh para su análisis y detección de amenazas. Para comenzar a enviar estos datos, el agente establece una conexión con el servicio del servidor para la conexión del agente, que escucha en el puerto 1514 por defecto (configurable). El servidor de Wazuh decodifica y verifica las reglas de los eventos recibidos mediante el motor de análisis. Los eventos que activan una regla se complementan con datos de alerta, como el ID y el nombre de la regla. Los eventos se pueden almacenar en uno o ambos archivos, dependiendo de si se activa o no una regla

- El archivo /var/ossec/logs/archives/archives.jsoncontiene todos los eventos independientemente de si activaron una regla o no.
- El archivo /var/ossec/logs/alerts/alerts.jsoncontiene solo eventos que activaron una regla con prioridad suficientemente alta (el umbral es configurable).

El protocolo de mensajes Wazuh utiliza cifrado AES por defecto, con 128 bits por bloque y claves de 256 bits. El cifrado Blowfish es opcional.

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

Comunicación entre el servidor Wazuh y el indexador Wazuh

El servidor Wazuh utiliza Filebeat para transmitir de forma segura datos de alertas y eventos al indexador Wazuh mediante cifrado TLS. Filebeat monitoriza los datos de salida del servidor Wazuh y los reenvía al indexador Wazuh, que escucha en el puerto 9200/TCP por defecto. Una vez indexados, puede analizar y visualizar los datos a través del panel de control de Wazuh.
El módulo de Detección de Vulnerabilidades actualiza el inventario de vulnerabilidades. También genera alertas que proporcionan información sobre las vulnerabilidades del sistema.
El panel de control de Wazuh consulta la API RESTful de Wazuh (que escucha por defecto en el puerto 55000/TCP del servidor Wazuh) para mostrar información de configuración y estado del servidor y los agentes de Wazuh. También permite modificar la configuración de los agentes o del servidor mediante llamadas a la API. Esta comunicación se cifra con TLS y se autentica con nombre de usuario y contraseña.

Puertos requeridos
Se utilizan varios servicios para la comunicación entre los componentes de Wazuh. A continuación, se muestra la lista de puertos predeterminados que utilizan estos servicios. Los usuarios pueden modificar estos números de puerto cuando sea necesario.

Componente	Puerto	Protocolo	Objetivo
Servidor Wazuh	1514	TCP (predeterminado)	Servicio de conexión de agentes
	1514	UDP (opcional)	Servicio de conexión del agente (deshabilitado de forma predeterminada)
	1515	TCP	Servicio de inscripción de agentes
	1516	TCP	Demonio de clúster Wazuh
	514	UDP (predeterminado)	Recopilador de Syslog de Wazuh (deshabilitado de forma predeterminada)
	514	TCP (opcional)	Recopilador de Syslog de Wazuh (deshabilitado de forma predeterminada)

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

Componente	Puerto	Protocolo	Objetivo
	55000	TCP	API RESTful del servidor Wazuh
Indexador Wazuh	9200	TCP	API RESTful del indexador Wazuh
	9300-9400	TCP	Comunicación del clúster de indexadores de Wazuh
Panel de control de Wazuh	443	TCP	Interfaz de usuario web de Wazuh

Almacenamiento de datos de archivo

Tanto las alertas como los eventos que no son alertas se almacenan en archivos en el servidor de Wazuh, además de enviarse al indexador de Wazuh. Estos archivos pueden estar en formato JSON (.json) o en texto plano (.log). Estos archivos se comprimen y firman diariamente con sumas de comprobación MD5, SHA1 y SHA256. La estructura del directorio y el nombre de archivo es la siguiente: root@wazuh-manager:/var/ossec/logs/archives/2022/Jan# ls -l

Output

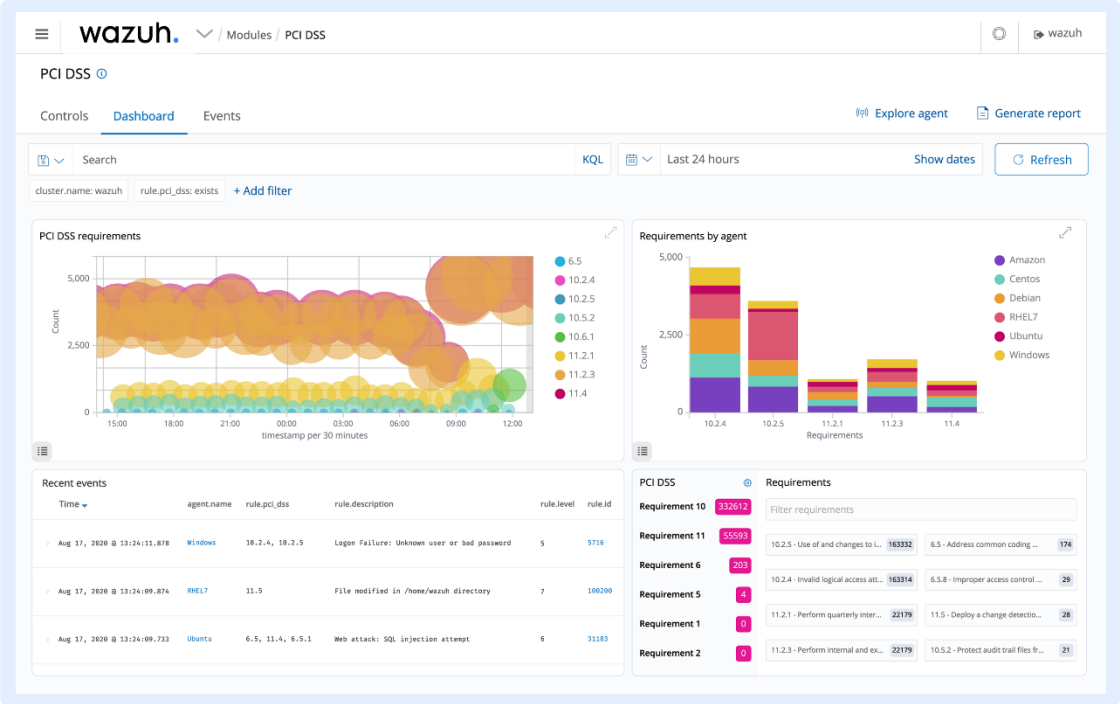
```
total 176
-rw-r----- 1 wazuh wazuh 234350 Jan  2 00:00 ossec-archive-01.json.gz
-rw-r----- 1 wazuh wazuh    350 Jan  2 00:00 ossec-archive-01.json.sum
-rw-r----- 1 wazuh wazuh 176221 Jan  2 00:00 ossec-archive-01.log.gz
-rw-r----- 1 wazuh wazuh    346 Jan  2 00:00 ossec-archive-01.log.sum
-rw-r----- 1 wazuh wazuh 224320 Jan  2 00:00 ossec-archive-02.json.gz
-rw-r----- 1 wazuh wazuh    350 Jan  2 00:00 ossec-archive-02.json.sum
-rw-r----- 1 wazuh wazuh 151642 Jan  2 00:00 ossec-archive-02.log.gz
-rw-r----- 1 wazuh wazuh    346 Jan  2 00:00 ossec-archive-02.log.sum
-rw-r----- 1 wazuh wazuh 315251 Jan  2 00:00 ossec-archive-03.json.gz
-rw-r----- 1 wazuh wazuh    350 Jan  2 00:00 ossec-archive-03.json.sum
-rw-r----- 1 wazuh wazuh 156296 Jan  2 00:00 ossec-archive-03.log.gz
-rw-r----- 1 wazuh wazuh    346 Jan  2 00:00 ossec-archive-03.log.sum
```

Se recomienda rotar y realizar copias de seguridad de los archivos comprimidos según la capacidad de almacenamiento del servidor Wazuh . Mediante tareas cron, puede gestionar fácilmente solo un período específico de archivos comprimidos localmente en el servidor, por ejemplo, el año pasado o los últimos tres meses.

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

Por otro lado, puede optar por prescindir del almacenamiento de archivos y simplemente confiar en el indexador de Wazuh para el almacenamiento de archivos. Esta alternativa podría ser la mejor opción si ejecuta copias de seguridad periódicas de instantáneas del indexador de Wazuh o si tiene un clúster de indexadores de Wazuh de varios nodos con réplicas de fragmentos para alta disponibilidad. Incluso podría usar una tarea cron para mover los índices generados a un servidor de almacenamiento de datos final y firmarlos con algoritmos de hash MD5, SHA1 y SHA256.

Cumplimiento Normativo



Wazuh emplea su tecnología SIEM para consolidar, examinar y enriquecer la información relacionada con la seguridad. Asimismo, ofrece múltiples funcionalidades de seguridad, tales como la identificación de intrusiones, evaluación de ajustes de sistema, análisis detallado de registros y descubrimiento de vulnerabilidades, todo ello alineado con los criterios técnicos de los marcos de cumplimiento normativo.

Las directrices de Wazuh se alinean meticulosamente con las exigencias de cumplimiento normativo para ofrecer un sólido soporte en esta área. De este modo, cada vez que se activa una alerta (es decir, cuando se satisface una condición de una regla de detección de amenazas), esta lleva consigo automáticamente datos relevantes para el cumplimiento de normativas. Actualmente, Wazuh ofrece soporte para los siguientes estándares:

- Normativa de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS)

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

- Regulación General de Protección de Datos (GDPR)
- Norma Especial Publicada por el NIST 800-53 (NIST 800-53)
- Guía de Buenas Prácticas 13 (GPG13)
- **ISO 27001**
- Criterios para Servicios de Confianza (TSC SOC2)
- Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA)

Tipos de Auditoría y su Relevancia

La importancia de realizar auditorías de seguridad de forma periódica no puede ser subestimada. Dependiendo de los requisitos de su industria, es posible que necesite diferentes tipos de auditoría.

1. **Auditorías Internas**: Estas son realizadas por el personal interno o terceros contratados para evaluar la eficacia de las políticas y sistemas de gestión internos. Wazuh facilita la realización de auditorías internas al permitir un seguimiento en tiempo real de la actividad en los sistemas y redes.
2. **Auditorías Externas**: Se trata de revisiones llevadas a cabo por entidades externas con el objetivo de verificar que una empresa cumple con estándares específicos, como el **ISO 27001**. Wazuh ofrece la capacidad de generar informes de cumplimiento que pueden ser usados como prueba en auditorías externas.

Auditoría de Seguridad Informática con Wazuh

1. **Hacking Ético y Test de Intrusión**: Wazuh también es útil en el contexto de hacking ético y test de intrusión, prácticas que buscan identificar vulnerabilidades en los sistemas antes de que sean explotadas por agentes maliciosos.
2. **Medidas de Seguridad y Control de Acceso**: Un aspecto clave para garantizar la seguridad es el control de acceso. Wazuh permite configurar quién tiene acceso a qué información, asegurando que solo las personas autorizadas puedan acceder a datos sensibles.

Importancia de los Informes de Cumplimiento

Un aspecto crucial en cualquier estrategia de seguridad es la capacidad de generar informes de cumplimiento detallados. Estos informes son vitales para el Oficial de Seguridad de la Información y otros encargados de garantizar que RST ASOCIAFOS PROJECT cumpla con todas las regulaciones y leyes aplicables.
En resumen, Wazuh es una herramienta versátil que no solo ayuda a garantizar la seguridad sino también a facilitar el proceso de auditorías de seguridad informática, control de acceso, y mucho más. No solo es una solución para garantizar el cumplimiento normativo, sino que también es una estrategia proactiva para mantener la integridad y seguridad de los sistemas de gestión en una organización.

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co

En un mundo donde las amenazas de seguridad son constantes y siempre evolucionan, garantizar el cumplimiento y la seguridad de la organización es más que una necesidad; es una obligación.

El consumo de recursos de Wazuh (RAM, CPU y disco duro) depende del número de agentes, la carga de trabajo y el tipo de sistema que se esté monitoreando. Se recomienda al menos 4 GB de RAM y 8 núcleos de CPU, pero para entornos más grandes o con 1000 agentes, se pueden necesitar 32 núcleos de CPU y 64 GB de RAM. El uso de disco duro también variará según la cantidad de datos que se generen y se almacenen, con recomendaciones que van desde 1 TB hasta un escalado horizontal para grandes clústers.

Requisitos mínimos:

- **RAM:** 2 GB
- **CPU:** 2 vCPU

Recomendaciones:

- **RAM:** 4 GB
- **CPU:** 8 núcleos

Entornos grandes:

- **CPU:** 32 núcleos o más
- **RAM:** 64 GB o más
- **Disco duro:** 1 TB o más, con escalado horizontal para clústers

Monitoreo del uso de recursos:

- Wazuh permite monitorear el uso de CPU, memoria y disco duro en los agentes.
- Se pueden usar alertas y reglas para detectar usos excesivos de recursos.

Consideraciones adicionales:

- La carga de trabajo del sistema afectará el consumo de recursos.
- La cantidad de agentes y el tipo de datos que se estén monitoreando también influirán en el uso de recursos.
- Wazuh ofrece opciones de escalado vertical e horizontal para adaptarse a diferentes necesidades.

NIT 900.264.538-8 - TEL: (601) 9180404-7446565
OFICINA OPERATIVA: CALLE 130ª # 58A-29 PISO 3
OFICINA ADMINISTRATIVA: AUTOPISTA NORTE # 122-35 OFICINA 302
info@rstasociados.com.co