Wazuh

¿Qué es Wazuh?

Wazuh es una **plataforma de seguridad de código abierto y gratuita** (Open Source) que ofrece capacidades unificadas de **XDR** (Detección y Respuesta Extendida) y **SIEM** (Gestión de Eventos e Información de Seguridad).

Es una solución integral que ayuda a las organizaciones a **detectar amenazas, supervisar la seguridad** de sus sistemas, **prevenir intrusiones** y **responder a incidentes** de forma centralizada y eficiente.

Su arquitectura principal se basa en:

- **Agentes:** Pequeños programas que se instalan en los *endpoints* (servidores, portátiles, escritorios, contenedores, instancias en la nube, etc.) y se encargan de recopilar datos de seguridad (logs, cambios en archivos críticos, inventario de software, etc.).
- **Servidor Wazuh (Wazuh Manager):** Recibe los datos de los agentes, los analiza utilizando reglas y motores de correlación, detecta amenazas y genera alertas. También gestiona las configuraciones y permite ejecutar acciones de respuesta activa.
- **Indexador:** Almacena, indexa y permite la búsqueda rápida de las alertas y los datos recopilados (a menudo utilizando OpenSearch, antes conocido como Elasticsearch).
- **Dashboard (Interfaz Web):** Una interfaz visual (basada en OpenSearch Dashboards o Kibana) que permite visualizar las alertas, monitorear el estado de los agentes, ver gráficos de seguridad y acceder a informes de cumplimiento normativo.

2. ¿Para qué se usa Wazuh? (Funcionalidades Clave)

Wazuh se utiliza para mejorar significarivamente la postura de ciberseguridad de una organización a través de varias funciones clave:

- **Detección de Intrusiones (HIDS):** Monitoriza la actividad en los *endpoints* en busca de malware, rootkits, anomalías y patrones de comportamiento malicioso.
- **Análisis y Gestión de Logs (SIEM):** Recolecta, agrega, indexa y analiza los *logs* (registros) de sistemas y

aplicaciones para detectar errores, configuraciones incorrectas, actividades maliciosas y violaciones de políticas.

- **Monitorización de la Integridad de Archivos (FIM):** Rastrea cambios en archivos y directorios críticos (contenido, permisos, propiedad) para alertar sobre modificaciones no autorizadas que podrían indicar un compromiso.
- **Evaluación de Vulnerabilidades:** Recopila el inventario de software de los agentes y lo compara con bases de datos de vulnerabilidades conocidas (CVE) para identificar software desactualizado o vulnerable.
- **Evaluación de la Configuración (Hardening):** Monitorea la configuración del sistema operativo y las aplicaciones para asegurar que cumplen con políticas de seguridad internas o estándares de la industria (como CIS Benchmarks).
- **Cumplimiento Normativo:** Proporciona los controles de seguridad y los informes necesarios para ayudar a cumplir con normativas como PCI DSS, GDPR, HIPAA, ISO 27001, entre otras.
- **Respuesta a Incidentes:** Permite ejecutar respuestas activas y automatizadas (como bloquear una IP, eliminar archivos sospechosos o detener un proceso) para mitigar amenazas de forma rápida.
- **Seguridad en la Nube y Contenedores:** Se integra con plataformas como AWS, Azure, GCP y monitorea el comportamiento y la seguridad de los contenedores Docker.

Instalación de Wazuh 4.13 en Ubuntu 24.04

Paso 0: Preparación de la Máquina Virtual (VM)

Asegúrate de que tu nueva VM tenga esta configuración **antes de arrancar Ubuntu 24.04**:

1. **RAM: Mínimo 8 GB** (para la instalación Todo-en-Uno).
2. **CPU: Mínimo 2 vCPUs** (4 es ideal).
3. **Red:** Configurada como **Adaptador Puente** (Bridge Adapter) para obtener una IP local accesible.

Paso 1: Instalación de Dependencias Esenciales

Abre la terminal de tu nueva VM y actualiza la lista de paquetes. Instala las herramientas básicas necesarias para la instalación de Wazuh:

sudo apt update

sudo apt install -y curl wget apt-transport-https software-properties-common

Paso 2: Ejecución del Instalador Asistido de Wazuh

Usaremos el *script* de instalación asistida de Wazuh (wazuh-install.sh) con la opción Todo-en-Uno (-a).

1. **Descargar el Script y Ejecutar la Instalación Todo-en-Uno:**

sudo snap install curl

curl -sO https://packages.wazuh.com/4.13/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

*(**Nota:** Este proceso instalará el Indexer, el Manager y el Dashboard. Puede tardar varios minutos).*

Eliminar archivos de bloqueo de APT

sudo rm /var/lib/dpkg/lock-frontend

sudo rm /var/lib/dpkg/lock

sudo rm /var/cache/apt/archives/lock

2. Guardar Contraseñas:

El script te mostrará una contraseña generada para el usuario admin. ¡Anótala! También puedes verla después:

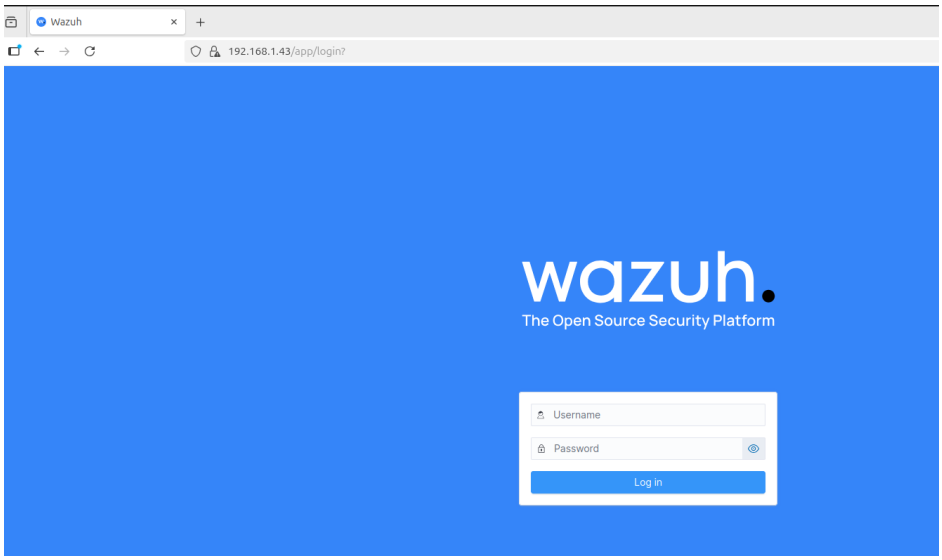
sudo tar -xOf wazuh-install-files.tar wazuh-passwords.txt

```
06/11/2025 16:09:28 INFO: --- Summary ---
06/11/2025 16:09:28 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: Gt1TIDig5aaRCNDNyNjRA0sO*RlRHNXc
06/11/2025 16:09:28 INFO: --- Dependencies ----
06/11/2025 16:09:28 INFO: Removing gawk.
06/11/2025 16:09:39 INFO: Installation finished.
```

User: admin

Password: Gt1TIDig5aaRCNDNyNjRA0sO*RlRHNXc

https://192.168.1.43:443



Paso 3: Configuración Final para Acceso Remoto

Aunque el instalador debería configurar el Dashboard para escuchar todas las interfaces, vamos a verificar y corregir la configuración de acceso.

1. **Editar el Archivo de Configuración del Dashboard:**

sudo nano /etc/wazuh-dashboard/opensearch_dashboards.yml

2. Añadir la Línea Clave:

Asegúrate de que la línea server.host esté configurada como "0.0.0.0" para que el Dashboard escuche en tu IP local:

YAML

```
# Asegúrate de que esta línea esté presente y sin comentarios:
server.host: "0.0.0.0"
```

Guarda y cierra el archivo (Ctrl+O, Enter, Ctrl+X).

3. Reiniciar el Servicio:

Reinicia el Dashboard para aplicar la configuración:

```
sudo systemctl restart wazuh-dashboard
```

Paso 4: Verificación y Acceso

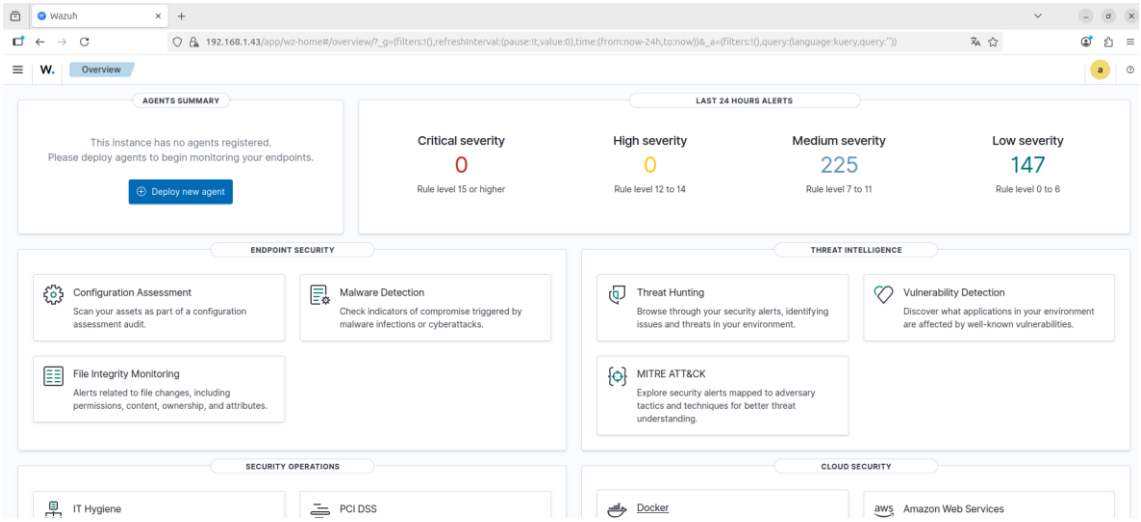
1. Verificar Servicios:

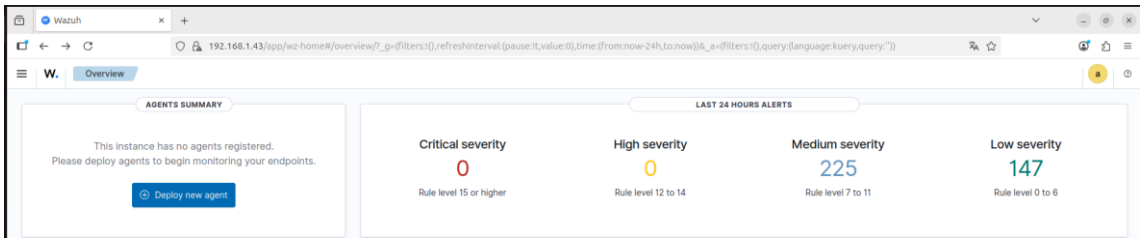
Asegúrate de que los tres servicios están activos:

```
sudo systemctl status wazuh-indexer
sudo systemctl status wazuh-manager
sudo systemctl status wazuh-dashboard
```

2. Acceso al Dashboard:

Abre tu navegador en la máquina host y navega a la dirección IP de tu VM (por ejemplo, https://192.168.1.41/). Acepta la advertencia de certificado no seguro y usa la contraseña que guardaste en el Paso 2 para iniciar sesión como admin.





Análisis del Panel de Resumen de Wazuh

El panel de resumen se divide en dos secciones principales, que te dan una instantánea del estado de seguridad y operativo de tu plataforma.

1. Resumen de Agentes (Agents Summary)

Esta sección te indica el estado de tus *endpoints* monitorizados.

Elemento	Información Mostrada	Lo que debes observar
"This instance has no agents registered."	Es el estado actual de tu instalación.	**Estado Inicial:** Indica que la plataforma Wazuh está funcionando, pero **aún no está protegiendo ningún sistema.**
Contador de Agentes	Normalmente, mostraría el número de agentes activos, desconectados o pendientes.	**Próximo Paso:** Debes usar el botón **"Deploy new agent"** para instalar agentes en tus servidores, estaciones de trabajo o contenedores.

2. Alertas de Últimas 24 Horas (Last 24 Hours Alerts)

Esta es la sección de seguridad más importante, ya que muestra las alertas de seguridad generadas por el **Wazuh Manager** en el último día, clasificadas por su nivel de severidad.

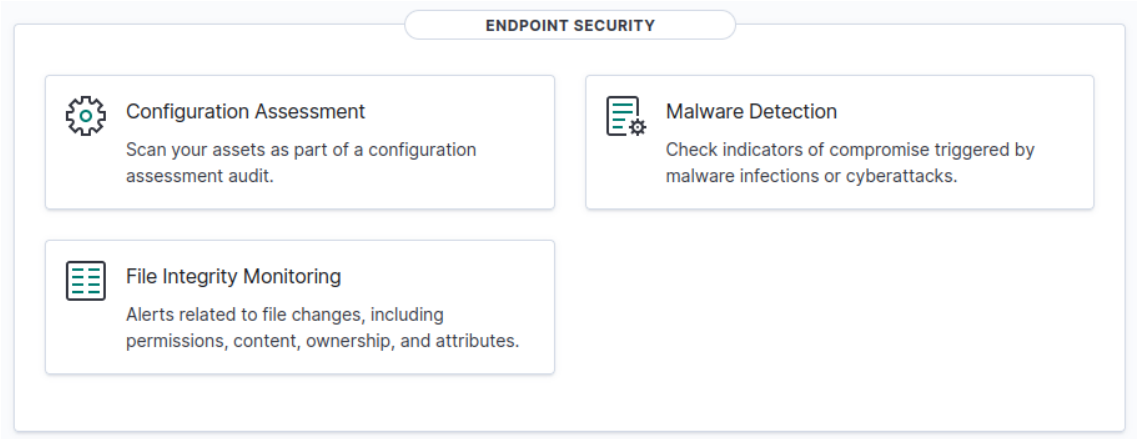
Severidad	Nivel de Regla	Recuento en la Imagen	Significado
Critical	Regla nivel 15	**0**	Alertas de máxima prioridad. Indican intrusiones activas,

Severidad	Nivel de Regla	Recuento en la Imagen	Significado
	o superior		*rootkits*, o actividad altamente maliciosa.
High	Regla nivel 12 a 14	**0**	Alertas serias. Indican posible actividad maliciosa, fallos de autenticación persistentes, o posibles vulnerabilidades.
Medium	Regla nivel 7 a 11	**225**	Alertas de importancia media. Indican cambios en archivos de configuración, fallos de *logins* ocasionales o eventos de auditoría que requieren seguimiento.
Low	Regla nivel 0 a 6	**147**	Alertas de baja prioridad. Son eventos informativos, actividad normal del sistema, o resultados de chequeos de integridad de archivos no críticos.

Lo que Indican las Alertas

La presencia de **372 alertas (225 Medium + 147 Low)**, incluso sin agentes instalados, indica que:

- **Alertas Internas (Monitorización):** Es completamente normal. Estas alertas son generadas por el propio **Wazuh Manager** sobre el sistema operativo en el que está instalado. Son eventos relacionados con el servicio, la monitorización interna del propio Manager, la conexión con el Indexer y el estado de la máquina VM.
- **Prueba de Funcionamiento:** Confirman que el **Manager está procesando logs, el Indexer está recibiendo y almacenando datos, y el Dashboard está consultando el Indexer.** Es una señal de que toda la cadena de datos está operando correctamente.



Funciones Clave de Seguridad del *Endpoint*

1. Configuration Assessment (Evaluación de la Configuración)

Este módulo se centra en el **Hardening de la Configuración** (endurecimiento de la seguridad).

- **Función:** Wazuh escanea regularmente las configuraciones de seguridad de tus *endpoints* (agentes) para determinar si cumplen con las **mejores prácticas** y **estándares de seguridad** (como CIS Benchmarks, por ejemplo).
- **Lo que verifica:** Comprueba políticas de contraseñas, configuraciones de servicios innecesarios, ajustes de permisos y otras configuraciones que podrían ser explotadas si están mal establecidas.
- **Valor:** Ayuda a **reducir la superficie de ataque** al identificar y alertarte sobre configuraciones débiles o riesgosas *antes* de que ocurra un incidente de seguridad.

2. Malware Detection (Detección de Malware)

Este módulo se enfoca en la identificación de actividad maliciosa en tiempo real.

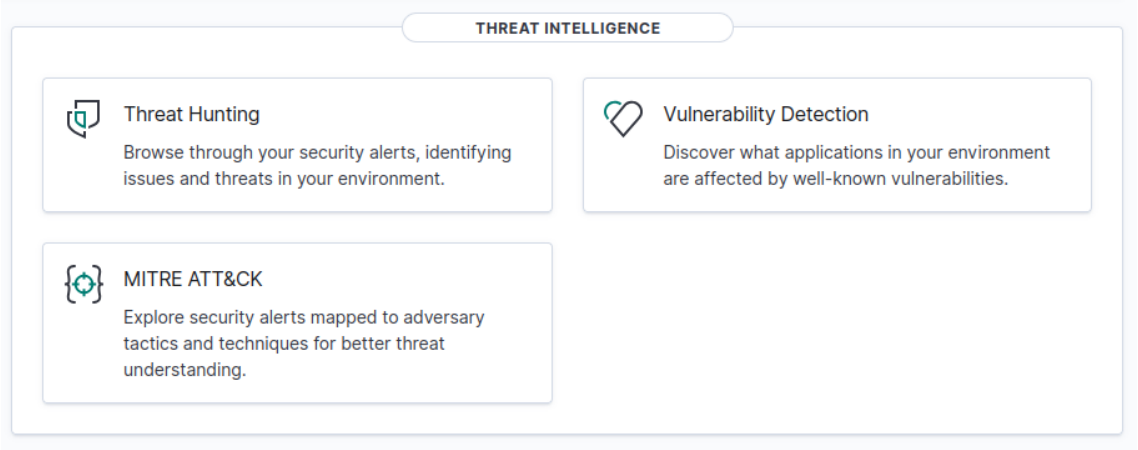
- **Función:** Wazuh analiza los **Indicadores de Compromiso (IOCs)** en los *logs* y la actividad del sistema para detectar patrones asociados con *malware*, *ransomware* o ataques cibernéticos activos.
- **Lo que verifica:** Busca eventos como la ejecución de archivos sospechosos, conexiones de red inusuales a direcciones IP maliciosas conocidas, y procesos que exhiben comportamiento anómalo.

- **Valor:** Proporciona **detección temprana** y visibilidad de que un *endpoint* puede haber sido comprometido, permitiendo una acción de respuesta rápida.

3. File Integrity Monitoring (FIM - Monitorización de la Integridad de Archivos)

FIM es una de las funciones más antiguas y críticas de Wazuh, centrada en la protección de archivos y directorios sensibles.

- **Función:** Monitoriza archivos y directorios clave en tiempo real. Cuando un archivo es modificado, se accede, se cambia su propietario, o se alteran sus permisos, Wazuh genera una alerta.
- **Lo que verifica:** El módulo FIM comprueba cambios en el **contenido** (usando *hashes* como MD5/SHA1), **permisos**, **propiedad** y **atributos** de archivos críticos (como /etc/passwd o archivos de configuración de aplicaciones).
- **Valor:** Es esencial para la **detección de intrusiones** y el **cumplimiento normativo** (como PCI DSS). Si un atacante accede al sistema y modifica archivos de configuración o crea *backdoors*, FIM lo detectará inmediatamente.



Funciones de Inteligencia y Análisis de Amenazas

1. Threat Hunting (Caza de Amenazas)

Este módulo es una herramienta proactiva que te permite buscar activamente amenazas que podrían haber pasado desapercibidas para las alertas automáticas.

- **Función:** Te da acceso directo a la consola de búsqueda de la plataforma, permitiéndote **navegar y filtrar** todas las alertas de seguridad e *logs* que Wazuh ha recopilado.
- **Valor:** En lugar de esperar una alerta, puedes formular tus propias hipótesis de seguridad (por ejemplo: "¿Se conectó algún servidor a esta IP maliciosa ayer?") y usar el **buscador** para encontrar evidencia que confirme o descarte esa actividad. Es la esencia de la ciberseguridad proactiva.

2. Vulnerability Detection (Detección de Vulnerabilidades)

Este módulo es crucial para la gestión de riesgos y el cumplimiento normativo.

- **Función:** Los agentes de Wazuh escanean periódicamente el *software* instalado en cada *endpoint* y lo comparan con las bases de datos públicas de vulnerabilidades (como la **NVD - National Vulnerability Database**).
- **Lo que verifica:** Identifica qué aplicaciones, librerías o sistemas operativos en tu entorno contienen **CVEs** (*Common Vulnerabilities and Exposures*) conocidas y graves.
- **Valor:** Te permite tener un **inventario centralizado de riesgos**. Puedes priorizar qué sistemas deben ser parchados (actualizados) inmediatamente para eliminar las vulnerabilidades más explotables.

3. MITRE ATT&CK

Este es un marco de referencia de conocimiento globalmente reconocido que describe las **tácticas y técnicas** que usan los atacantes.

- **Función:** Wazuh toma las alertas de seguridad que genera (por ejemplo, "Ejecución de un script sospechoso") y las **mapea automáticamente** a las técnicas específicas dentro del marco MITRE ATT&CK (por ejemplo, T1059: Command and Scripting Interpreter).
- **Valor:** Proporciona un **contexto táctico** al incidente. En lugar de ver una alerta aislada, ves cómo se relaciona con el ciclo de vida del ataque (Acceso Inicial, Movimiento Lateral, Persistencia, etc.). Esto mejora tu **capacidad de respuesta** y te ayuda a entender la intención del atacante.

Funciones de Operaciones de Seguridad y Cumplimiento

1. IT Hygiene (Higiene de TI)

Esta función es un concepto amplio que Wazuh aplica para asegurar que tus sistemas mantienen un estado de seguridad saludable a lo largo del tiempo.

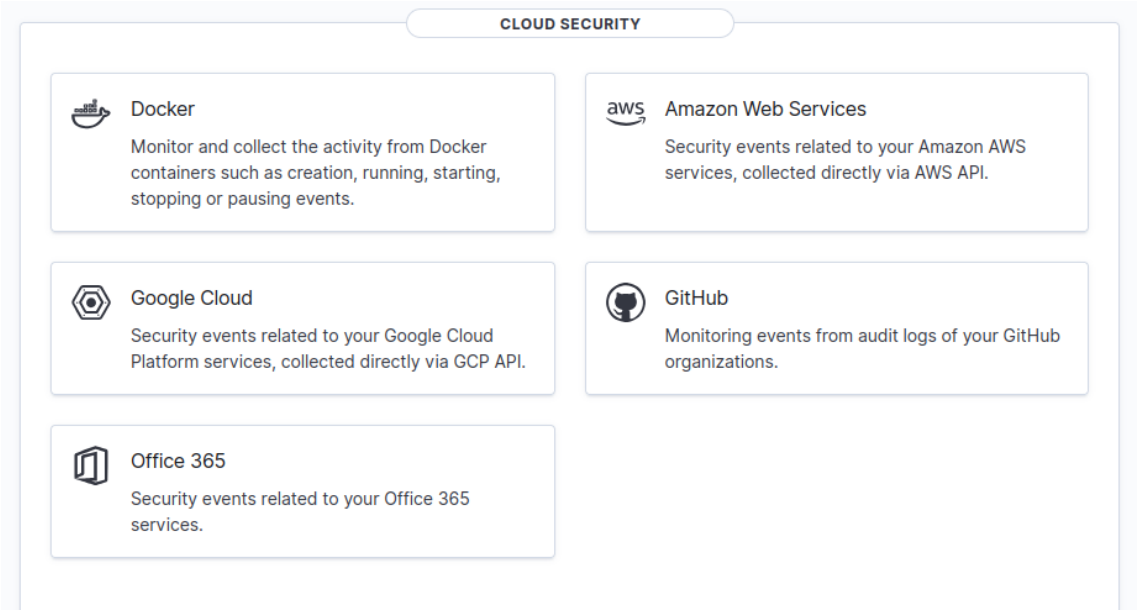
- **Función:** Se basa en la **monitorización continua** de la configuración, el *software* y los procesos para detectar desviaciones del estado de seguridad esperado.
- **Valor:** Ayuda a prevenir que los sistemas caigan en un estado de riesgo (por ejemplo, *software* desactualizado, servicios innecesarios activos o permisos modificados) al alertar sobre **malas configuraciones, cambios no autorizados y anomalías** en la red y los sistemas.

2. Normativas de Cumplimiento (Compliance Standards)

Wazuh correlaciona sus alertas con los requisitos específicos de las principales normativas globales, permitiendo a las organizaciones auditar su postura de seguridad contra estos estándares.

Norma	Nombre Completo y Contexto	Lo que Wazuh Ayuda a Cumplir
PCI DSS	**Payment Card Industry Data Security Standard.** Estándar de seguridad global para entidades que procesan, almacenan o transmiten datos de titulares de tarjetas de pago.	Monitorización de la integridad de archivos (FIM), auditoría de *logs* de seguridad y detección de intrusiones, que son requisitos obligatorios para manejar datos de tarjetas.
GDPR	**General Data Protection Regulation.** Reglamento general de protección de datos de la Unión Europea que establece pautas para el procesamiento de datos personales.	Auditoría de acceso y procesamiento de datos, detección de intrusiones (*breaches*), y monitorización de seguridad de los sistemas que almacenan Información de Identificación Personal (PII).
HIPAA	**Health Insurance Portability and Accountability Act of 1996.** Ley de EE. UU. que proporciona disposiciones de privacidad y seguridad para salvaguardar la información médica.	Protección de la Información de Salud Protegida (PHI) a través de controles de acceso, FIM en registros de salud y auditoría de eventos de seguridad.
NIST 800-53	**National Institute of Standards and Technology Special Publication 800-53.** Conjunto de directrices y requisitos para sistemas de información federales en EE. UU.	Mapeo de controles de seguridad (como control de acceso, auditoría y evaluación continua) a los requisitos específicos de esta compleja regulación.
TSC	**Trust Services Criteria** (Criterios de Servicios de Confianza). Marco utilizado en auditorías SOC (Service Organization Control) que se centra en cinco áreas: Seguridad, Disponibilidad,	Proporciona la monitorización y la evidencia (*logs*) necesarias para demostrar el cumplimiento de la seguridad, la disponibilidad del sistema y la integridad de los

Norma	Nombre Completo y Contexto	Lo que Wazuh Ayuda a Cumplir
	Integridad del Procesamiento, Confidencialidad y Privacidad.	datos, que son pilares de las auditorías SOC.



Funciones de Seguridad en la Nube y Contenedores

Componente	Descripción de la Función	Valor Clave
Docker	Monitorea y recopila la **actividad en tiempo real** de los contenedores Docker. Esto incluye eventos como la creación, inicio, detención o pausa de contenedores.	Proporciona **visibilidad** del ciclo de vida de la aplicación en el entorno de contenedores, detectando configuraciones de seguridad débiles o actividades anómalas dentro del *host* de Docker.
Amazon Web Services (AWS)	Recopila eventos de seguridad relacionados con tus servicios de AWS (como EC2, S3, IAM, CloudTrail, etc.),	Monitorea **cambios críticos** en la infraestructura de la nube, como la creación de nuevos usuarios con privilegios elevados, cambios en políticas de

Componente	Descripción de la Función	Valor Clave
	utilizando la **API de AWS**.	acceso de S3, o eventos de API sospechosos.
Google Cloud	Recopila eventos de seguridad de los servicios de Google Cloud Platform (GCP), utilizando la **API de GCP**.	Proporciona control sobre los entornos de GCP, detectando configuraciones incorrectas o actividades que violan las políticas de seguridad en servicios como GKE o Cloud Storage.
GitHub	Monitorea los eventos de los **logs de auditoría** de tus organizaciones de GitHub.	Asegura la **cadena de suministro de software (Software Supply Chain)**. Detecta accesos no autorizados a repositorios, cambios en los permisos de los colaboradores, o eliminaciones críticas de código.
Office 365	Recopila eventos de seguridad y actividad relacionados con los servicios de Office 365 (ahora conocido como Microsoft 365), como Exchange, SharePoint, y Azure AD.	Monitorea la **actividad de los usuarios en la nube**, detectando *logins* sospechosos, acceso a datos sensibles o cambios en la configuración de seguridad del correo electrónico.

El Siguiente Paso: Despliegue de Agentes

Tu plataforma ya está lista. El siguiente paso lógico es la **instalación de tu primer agente**.

1. Haz clic en el botón **"Deploy new agent"**.

2. Sigue las instrucciones que aparecen en pantalla para seleccionar el sistema operativo de tu *endpoint* (por ejemplo, Windows o Linux) y el Dashboard te proporcionará el comando exacto de instalación que incluye la dirección IP de tu Manager (192.168.1.41).

¿Qué Implica el Despliegue de Agentes?

El despliegue de agentes es el proceso de instalar un *software* ligero (el Agente Wazuh) en cada sistema que deseas monitorizar.

Componente	**Rol**
Agente (Instalado en el *Endpoint*)	Recopila datos de seguridad (logs del sistema, eventos de integridad de archivos, cambios de configuración) en tiempo real.
Manager (Tu VM Wazuh)	Recibe los datos, los analiza, los correlaciona con reglas de seguridad y genera alertas.

¿Debes Desplegar un Agente en Cada Máquina a Controlar?

Para que Wazuh pueda monitorizar, proteger y auditar un servidor, estación de trabajo o máquina virtual, debe haber un **Agente Wazuh instalado y activo** en esa máquina. Cada agente reporta exclusivamente a tu Manager central.

Excepción: Wazuh puede monitorizar dispositivos de red (como *routers* o *firewalls*) y servicios en la nube (AWS, Google Cloud) **sin un agente**, extrayendo directamente los *logs* a través de Syslog o de la API del proveedor de la nube.

¿Cómo Funciona el Despliegue de Agentes?

El flujo de despliegue es muy sencillo gracias a la herramienta que te ofrece el Dashboard:

1. El Dashboard Genera el Script

Cuando haces clic en **"Deploy new agent"** en el Dashboard, sigues estos pasos:

- **Seleccionas el Sistema Operativo** (e.g., Windows, RHEL, Debian, macOS).

- **Seleccionas la Arquitectura** (e.g., 64 bits).

El Dashboard utiliza la IP de tu Manager (192.168.1.41) y genera un **comando único de instalación**. Este comando contiene toda la información de configuración necesaria (principalmente, la dirección IP del Manager) para que el agente sepa dónde enviar sus datos.

2. Ejecución en el *Endpoint*

Tú tomas ese comando generado y lo ejecutas en la máquina que deseas monitorizar.

- El comando descarga e instala el agente.
- El agente se configura automáticamente para apuntar a **192.168.1.41**.
- El agente se registra en el Manager, y el Manager le asigna un ID único.

3. Conexión Cifrada y Monitorización

- El agente inicia su servicio y establece una **conexión cifrada** (segura) con el Manager.
- Comienza a recopilar datos de la máquina (*logs*, FIM, inventario de *software*) y a enviarlos al Manager para su análisis en tiempo real.

Una vez que el agente está instalado, la pestaña **Agents Summary** en tu Dashboard pasará de mostrar "0" agentes a mostrar "1" agente activo.