

Wazuh

**Andres Valdivieso

Introducción

Este write-up documenta el proceso de instalación, configuración y puesta en marcha de **Wazuh** mediante su imagen virtual (OVA), como parte integral de un **entorno de laboratorio de ciberseguridad** diseñado para investigación, práctica defensiva y ofensiva, así como para la integración de herramientas de análisis avanzado y automatización.

El laboratorio está compuesto por múltiples máquinas que cumplen funciones complementarias, incluyendo:

- **Kali Linux Básico y Purple** para pruebas de penetración y ejercicios de Red/Blue Team.
- **OpenCTI** para la gestión y correlación de inteligencia de amenazas.
- **ElasticSearch, Kibana y Filebeat** como stack de análisis y visualización de eventos.
- **Redmux** para administración de herramientas y acceso remoto consolidado.

En este ecosistema, **Wazuh actúa como un eje central de monitoreo y detección**, permitiendo la recolección de eventos desde diversos sistemas, análisis de integridad, correlación de comportamientos sospechosos y gestión de agentes en endpoints clave. Su integración con herramientas como Elastic y Filebeat fortalece la visibilidad sobre la infraestructura, mientras que su interoperabilidad con sistemas como OpenCTI permite enriquecer alertas con inteligencia contextual.

Esta implementación no solo refuerza la postura defensiva del laboratorio, sino que también permite simular escenarios reales de ataques, evaluar tiempos de detección y respuesta, y probar mecanismos de defensa proactivos, consolidando un entorno técnico completo orientado al **aprendizaje, experimentación y desarrollo de capacidades en ciberseguridad**.

Resumen Máquina Virtual (OVA) - Wazuh

Descripción general

Wazuh ofrece una máquina virtual en formato OVA que incluye **Amazon Linux 2023** y los componentes centrales de Wazuh 4.12.0:

- **Wazuh Manager**
- **Wazuh Indexer**
- **Wazuh Dashboard**
- **Filebeat OSS 7.10.2**

Importante:

- **Compatible solo con sistemas de 64 bits (x86_64/AMD64).**
- **No ofrece alta disponibilidad ni escalabilidad por defecto, pero se puede adaptar mediante una implementación distribuida.**

Requisitos y configuración

Requisitos del sistema:

- Sistema operativo host de 64 bits (x86_64/AMD64 o AARCH64/ARM64).
- Virtualización habilitada en BIOS/UEFI.
- Plataforma como **VirtualBox** instalada.

Especificaciones predeterminadas:

Componente	CPU	RAM	Almacenamiento
OVA v4.12.0	4 núcleos	8 GB	50 GB

Configuración en VirtualBox:

1. Importar el archivo `wazuh-4.12.0.ova` .
2. Ir a **Configuración > Pantalla > Controlador gráfico** y seleccionar **VMSVGA**.
3. Ajustar el reloj del hardware a **UTC** para evitar problemas de sincronización.

Accesos y comandos útiles

Acceso a la VM:

- **Usuario:** `wazuh-user`
- **Contraseña:** `admin`
- Acceso root: `sudo -i`

Acceso al panel Wazuh:

- **URL:** `https://<wazuh_server_ip>`
- **Usuario:** `admin`
- **Contraseña:** `admin`
- Obtener IP: `ip a`

Archivos de configuración:

- **Manager:** `/var/ossec/etc/ossec.conf`
- **Indexer:** `/etc/wazuh-indexer/opensearch.yml`
- **Filebeat:** `/etc/filebeat/filebeat.yml`
- **Dashboard:**
 - `/etc/wazuh-dashboard/opensearch_dashboards.yml`
 - `/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml`

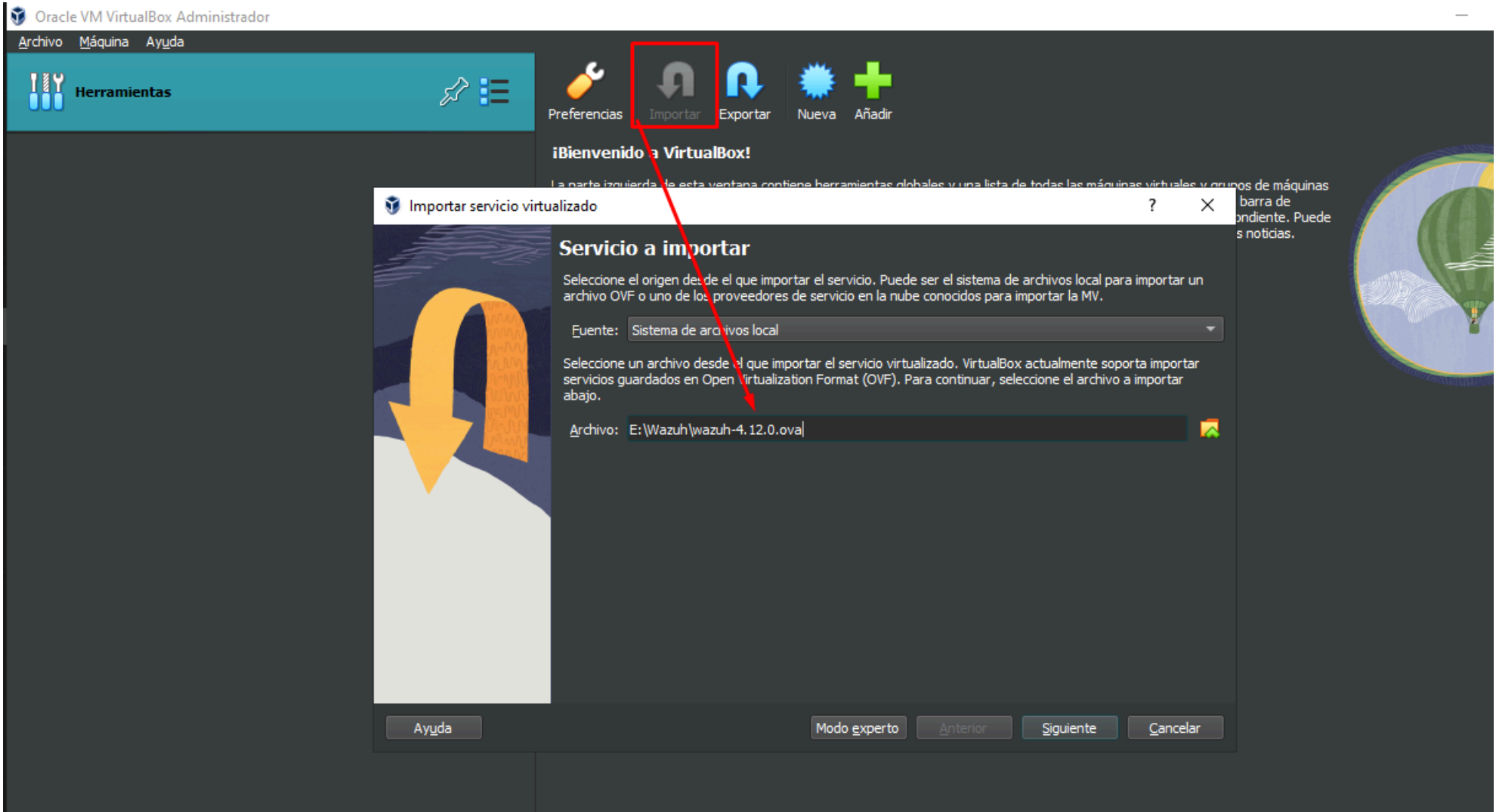
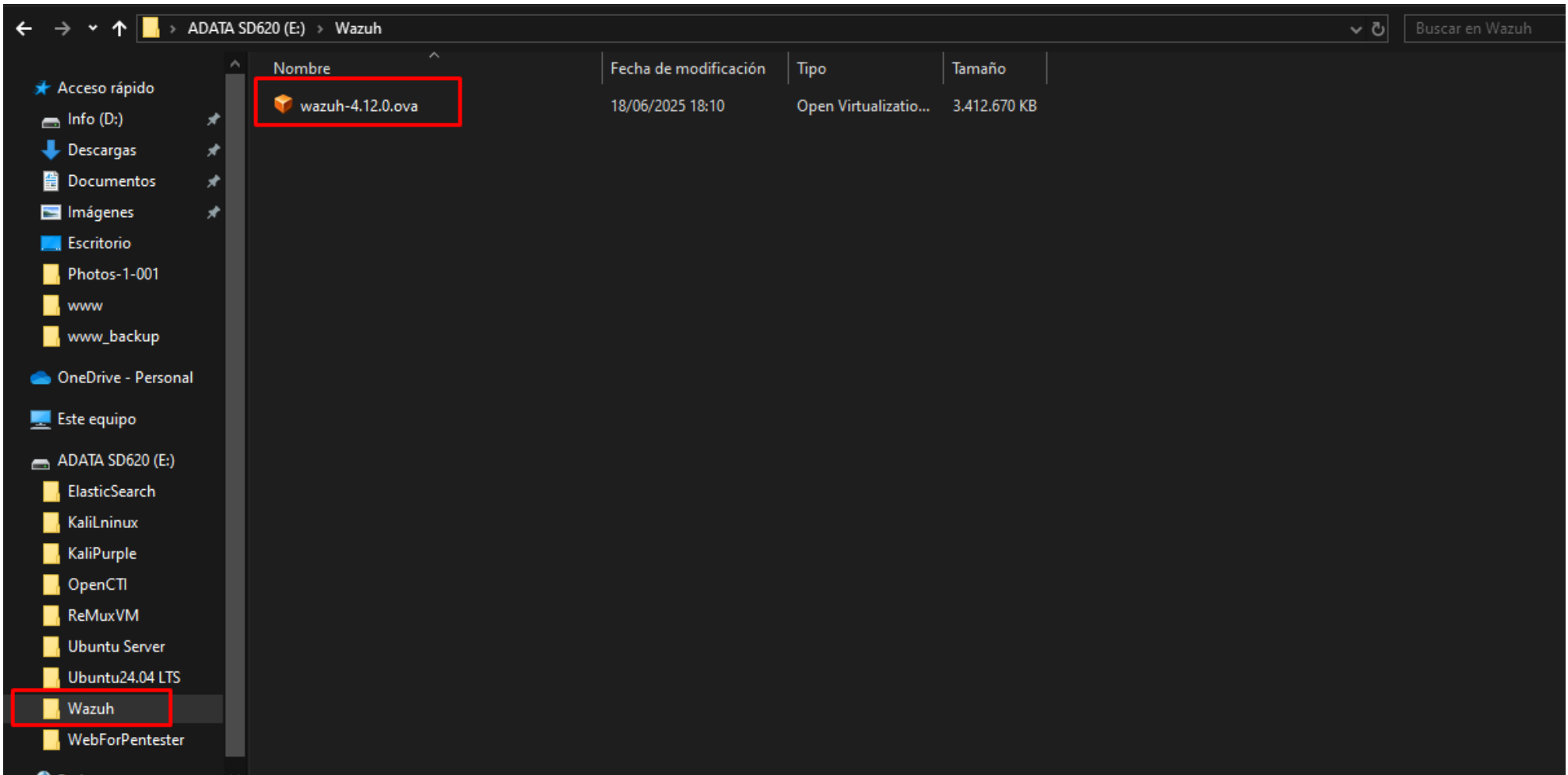
Consideraciones adicionales

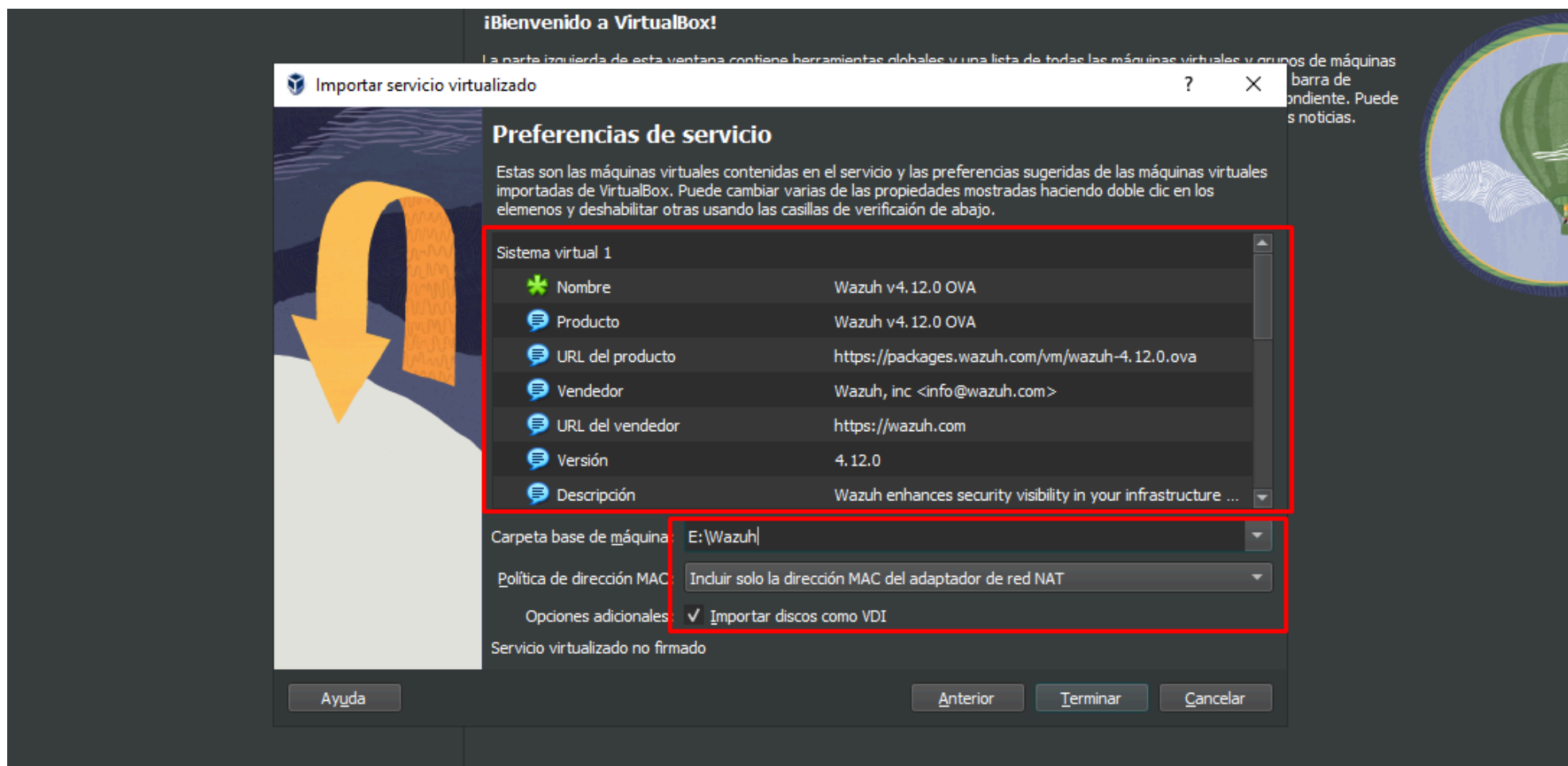
Red:

- Por defecto, la interfaz de red es tipo **Adaptador en puente** (IP por DHCP).
- Se puede configurar IP estática desde los archivos de red del sistema.

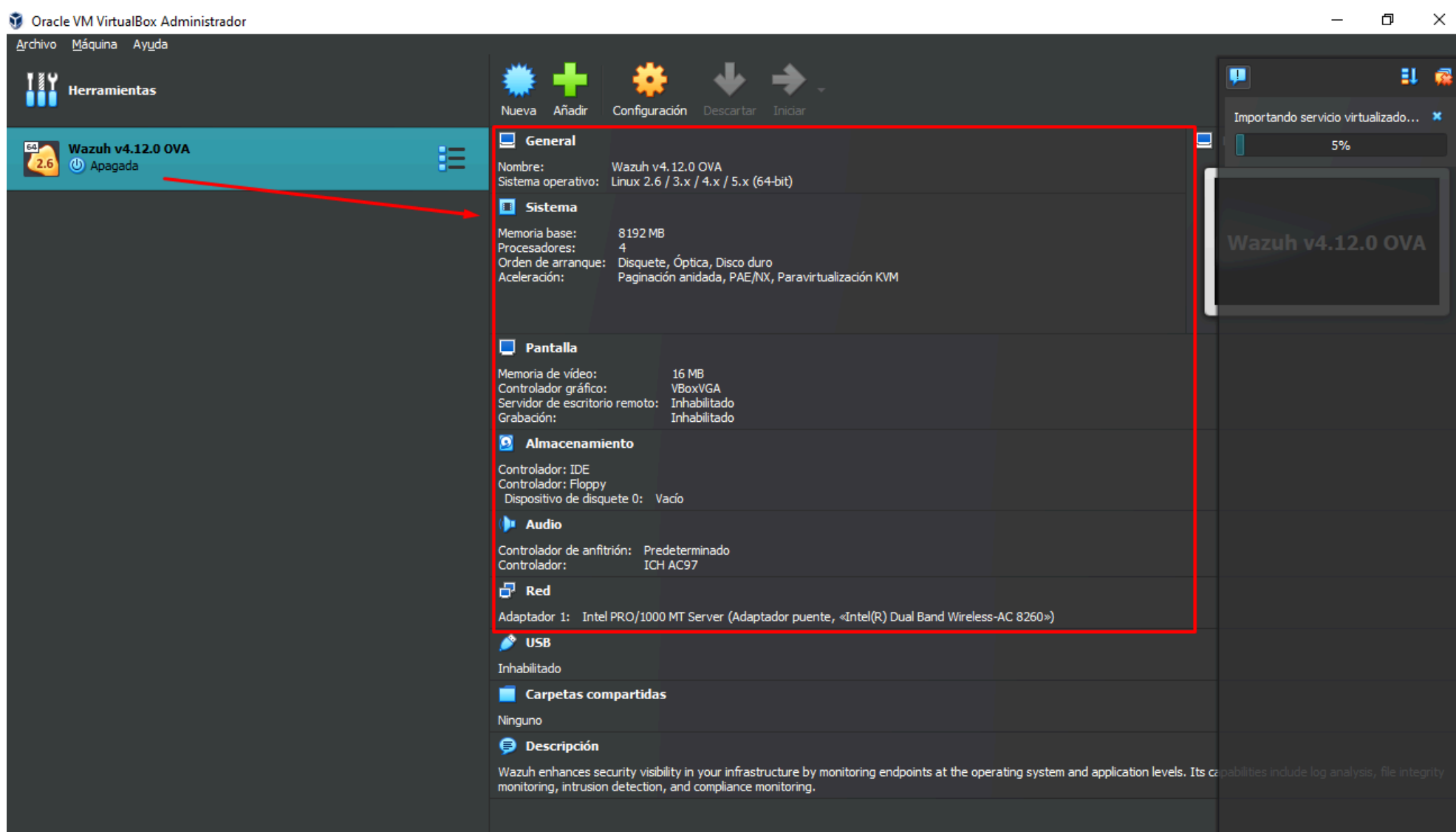
Instalación Wazuh

Descargar el OVA, importarlo y luego configurar según los recursos del equipo en cuestión, esto para un despliegue en VM de Laboratorio:

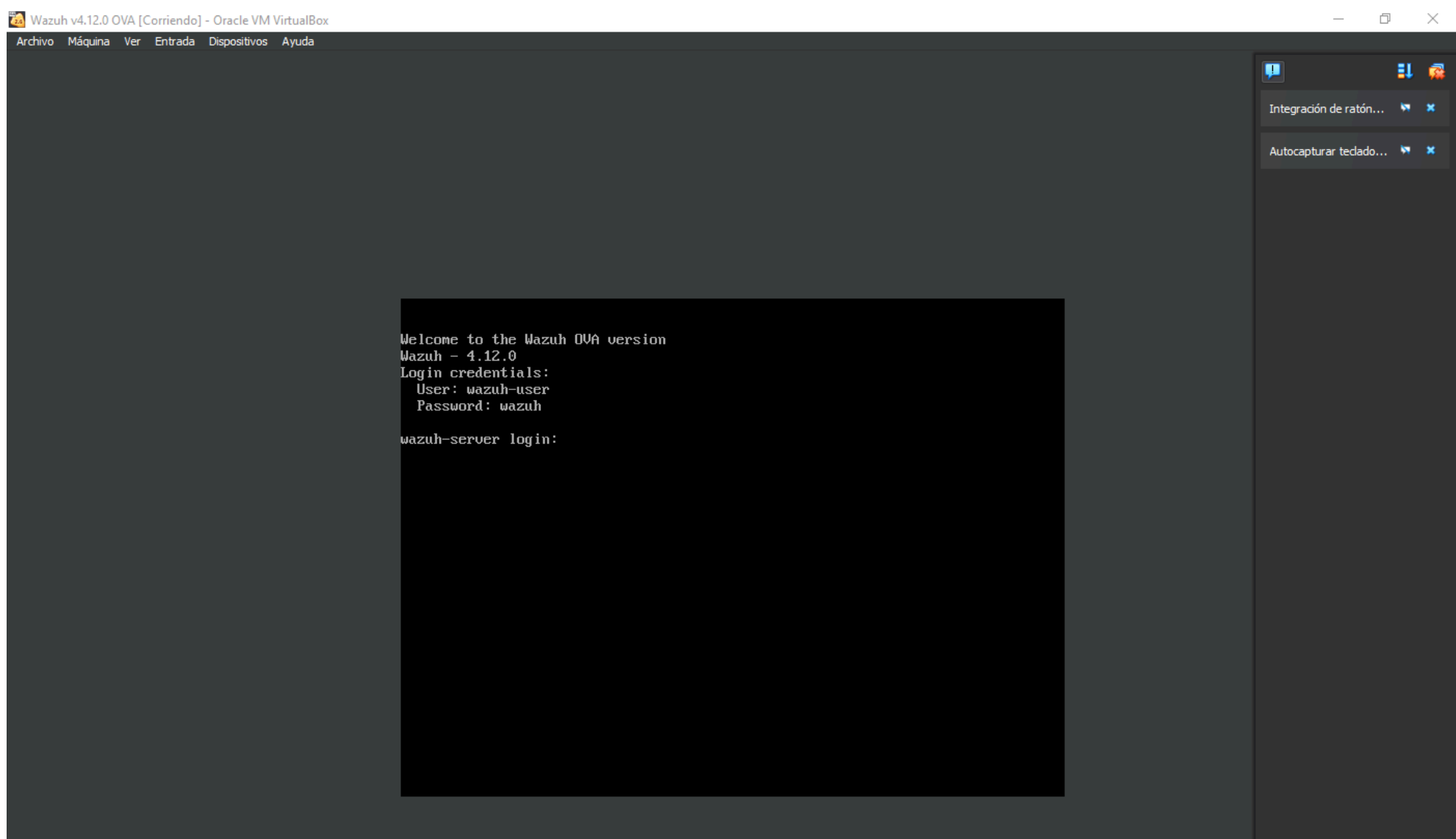
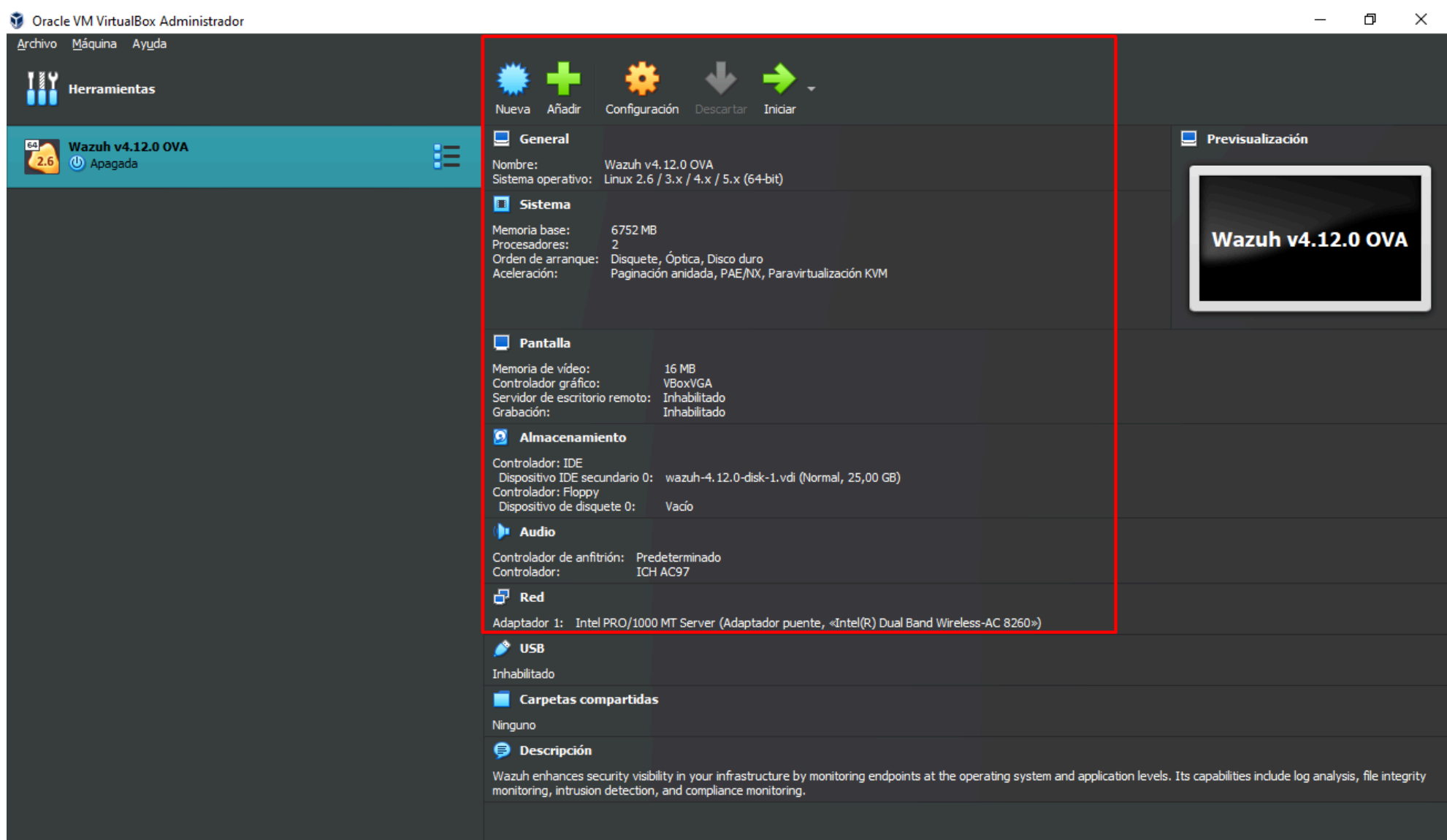




Como base trae estos valores:



Para mi uso personal y por recursos se dejan lo siguientes:



Se hace uso del comando

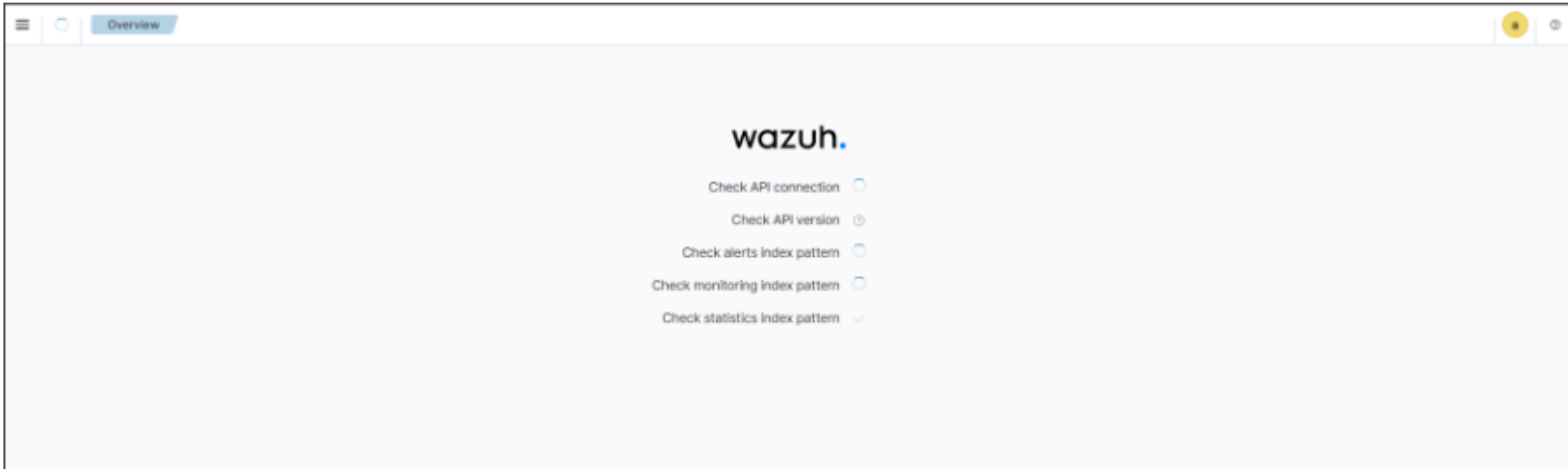
```
ip a
```

Pra encontrar la IP del wazuh y asi poder ingresar a la herrameinta

- URL: <https://IP>
- User: admin
- Password: admin

wazuh.

Loading ...



Overview

W.

AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.
[Deploy new agent](#)

LAST 24 HOURS ALERTS

Critical severity
0
Rule level 15 or higher

High severity
0
Rule level 12 to 14

Medium severity
3
Rule level 7 to 11

Low severity
40
Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment

Scan your assets as part of a configuration assessment audit.

Malware Detection

Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring

Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting

Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection

Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK

Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

PCI DSS

Global security standard for entities that process, store, or transmit payment cardholder data.

GDPR

General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.

HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security provisions for safeguarding medical information.

NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

CLOUD SECURITY

Docker

Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.

Amazon Web Services

Security events related to your Amazon AWS services, collected directly via AWS API.

Google Cloud

Security events related to your Google Cloud Platform services, collected directly via GCP API.

GitHub

Monitoring events from GitHub organizations.

Default API has been updated.

lo primero es configurar los agentes para que le reporten a wazuh:

W. Overview

AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

[Deploy new agent](#)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	3	40
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

- Configuration Assessment**
Scan your assets as part of a configuration assessment audit.
- Malware Detection**
Check indicators of compromise triggered by malware infections or cyberattacks.
- File Integrity Monitoring**
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

- Threat Hunting**
Browse through your security alerts, identifying issues and threats in your environment.
- Vulnerability Detection**
Discover what applications in your environment are affected by well-known vulnerabilities.
- MITRE ATT&CK**
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS

- PCI DSS**
Global security standard for entities that process, store, or transmit payment cardholder data.
- GDPR**
General Data Protection Regulation (GDPR) sets guidelines for processing of personal data.
- HIPAA**
Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides data privacy and security.
- NIST 800-53**
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

CLOUD SECURITY

- Docker**
Monitor and collect the activity from Docker containers such as creation, running, starting, stopping or pausing events.
- Amazon Web Services**
Security events related to your Amazon AWS services, collected directly via AWS API.
- Google Cloud**
Security events related to your Google Cloud Platform services, collected directly via GCP API.
- GitHub**
Monitoring events from audit logs of your GitHub organizations.

<https://192.168.0.12/app/endpoints-summary#/agents-preview/deploy>

W. Endpoints Deploy new agent

Deploy new agent

Select the package to download and install on your system:

LINUX

☐ RPM x86_64 ☐ RPM x86_64
☐ DEB x86_64 ☐ DEB x86_64

WINDOWS

☒ MSI x64 x64

macOS

☐ Intel ☐ Apple silicon

[For additional systems and architectures, please check our documentation.](#)

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address [?](#)

☒ Remember server address

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: [?](#)

W. Endpoints Deploy new agent

☒ Remember server address

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name: [?](#)

[The agent name must be unique. It can't be changed once the agent has been enrolled.](#)

Select one or more existing groups: [?](#)

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.nsi -OutFile $env:tmp\wazuh-agent; nsisexec.exe /s $env:tmp\wazuh-agent /q /AZUL_MANAGER=192.168.0.12 /AZUL_AGENT_NAME="Window_AgentWazuh"
```

[Requirements](#)

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

Start the agent:

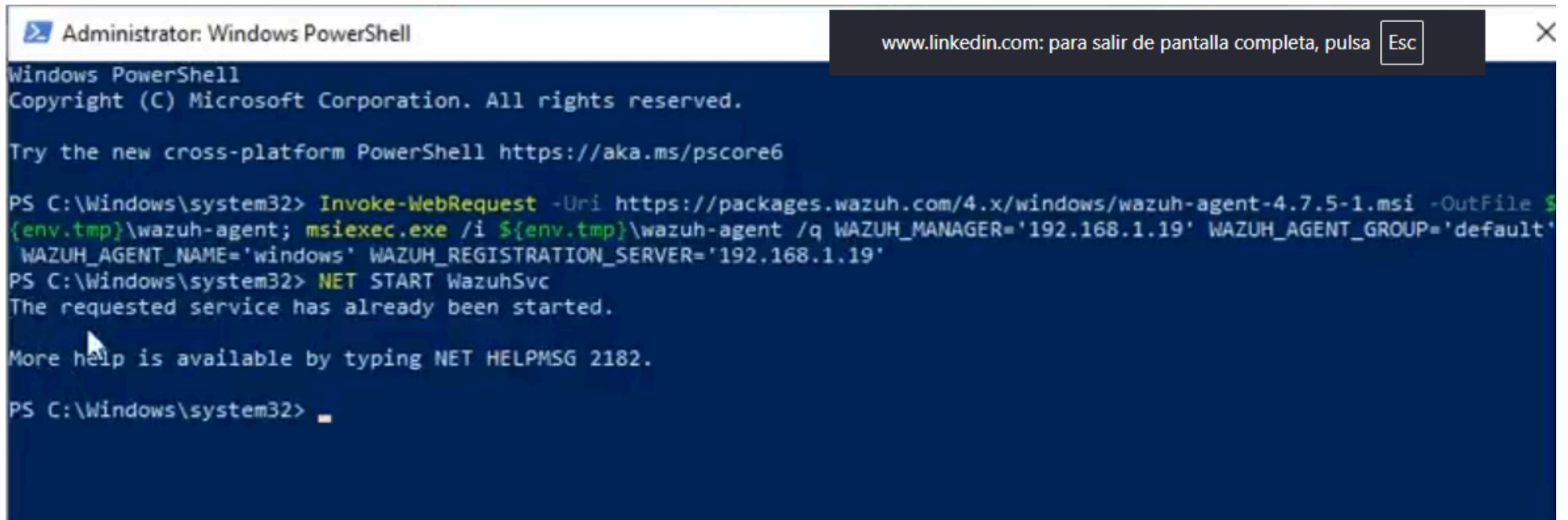
Para instalar el agente esta este comando que sale en la configuración del agente esto se corre desde PowerShell con permisos de admin:


```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msixexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='IP_Server' WAZUH_AGENT_NAME='Window_AgentWazuh'
```

Luego desde la maquina a la que se le instale se corre el iniciador del wazuh:

```
NET START WazuhSvc
```

Debería verse así:



The screenshot shows an Administrator Windows PowerShell window. The title bar reads "Administrator: Windows PowerShell". The window content displays the following text:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

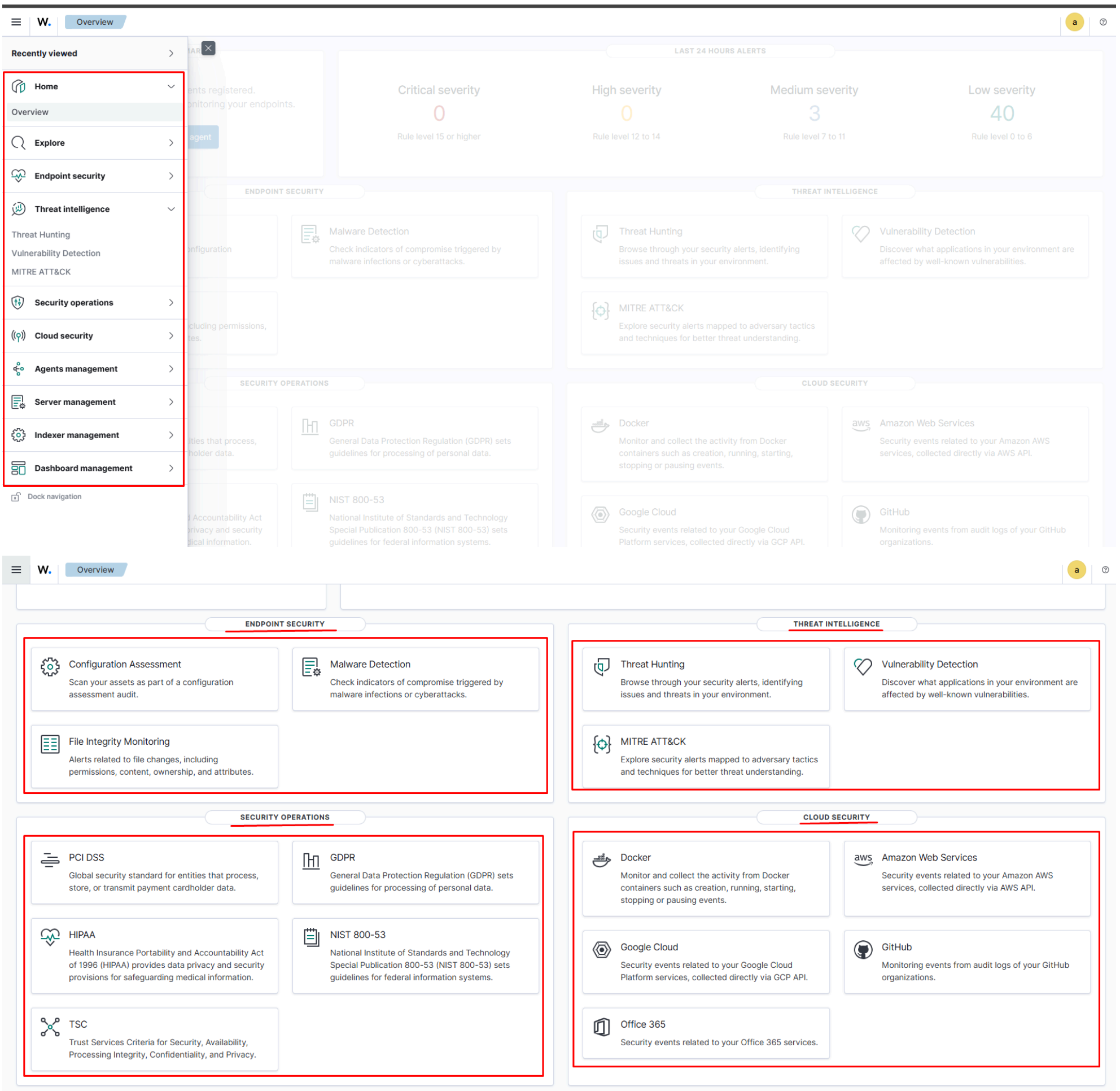
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.7.5-1.msi -OutFile $
{env.tmp}\wazuh-agent; msixexec.exe /i ${env.tmp}\wazuh-agent /q WAZUH_MANAGER='192.168.1.19' WAZUH_AGENT_GROUP='default'
WAZUH_AGENT_NAME='windows' WAZUH_REGISTRATION_SERVER='192.168.1.19'
PS C:\Windows\system32> NET START WazuhSvc
The requested service has already been started.

More help is available by typing NET HELPMSG 2182.

PS C:\Windows\system32>
```

A notification bar at the top right of the window states: "www.linkedin.com: para salir de pantalla completa, pulsa Esc".

Paneles



Conclusión tras la instalación y despliegue de Wazuh

Implementar Wazuh a través de su imagen OVA representa un paso sólido hacia la consolidación de una estrategia de **monitoreo, detección y respuesta ante amenazas** de seguridad en infraestructuras modernas. Su arquitectura modular permite contar en pocos minutos con un entorno completo que incluye gestión centralizada de agentes, análisis de logs, correlación de eventos, monitoreo de integridad, y visualización avanzada de datos desde su panel web.








Con la instalación realizada, se habilita un ecosistema de **detección proactiva**, donde es posible supervisar servidores, estaciones de trabajo, dispositivos de red y contenedores, permitiendo identificar amenazas, comportamientos anómalos y posibles brechas de seguridad.

Sin embargo, uno de los aspectos más relevantes es que **el verdadero potencial de Wazuh no solo reside en la visibilidad que ofrece, sino en su capacidad para integrarse con otras soluciones** (SIEM, herramientas de ticketing, correo, Slack, etc.), automatizar respuestas, aplicar políticas de cumplimiento normativo (como PCI DSS, HIPAA o GDPR), y escalarse según las necesidades del entorno.

No obstante, es importante resaltar que **tener el servidor Wazuh en una máquina virtual local y no mantenerlo encendido permanentemente puede limitar seriamente su eficacia operativa**, ya que la recolección y correlación de

eventos se interrumpe, reduciendo la capacidad de generar alertas en tiempo real y mantener una postura de seguridad continua.

Aspectos más relevantes a destacar:

-  **Despliegue rápido y funcional desde OVA.**
 -  **Visibilidad centralizada de seguridad** en endpoints.
 -  **Análisis y correlación avanzada** de eventos.
 -  **Cumplimiento normativo** y políticas de integridad.
 -  **Alta personalización** y automatización de respuestas.
 -  **Interoperabilidad con múltiples herramientas externas.**
 -  **Dependencia de disponibilidad constante del servidor** para un monitoreo continuo y efectivo.
-

En definitiva, Wazuh se presenta como una solución poderosa, gratuita y escalable que bien implementada y mantenida, puede elevar significativamente el nivel de seguridad operativa de una organización o entorno personal/profesional. Mantenerla activa y alineada con una estrategia de ciberseguridad permanente es clave para aprovechar al máximo su potencial.