🚀 De cero a seguro

Instalá Wazuh y detectá amenazas en minutos

wazuh.

flisol CABA 2025

Sultanovich

$ whoami

@sultanovich (Pablo)

- Sysadmin veterano y SecOps por adopción
- Arranqué en GNU/Linux con Mandrake 7 y Debian 3
- Entré en seguridad por casualidad y terminé quedándome a vivir
- Uso software libre y una consola para resolver casi todo (a veces con una Raspberry Pi)
- Colaboro con las comunidades BairesNorteLug y OpenSSF
- Ayudo a proteger infra cloud (hoy, desde Wazuh)
- A veces doy charlas... como esta 😅

El problema en muchas empresas

- Tenés servidores, pero `no sabés qué está pasando`
- Querés `ver vulnerabilidades`, sin licencias ni dolores de cabeza
- No todos los equipos tienen un `especialista en seguridad`
- Lo ideal: `algo fácil, abierto y que te avise` cuando algo anda mal

¿Qué es Wazuh?

> *Wazuh es una plataforma de seguridad (XDR / SIEM) open source, que permite **monitorear, detectar y responder ante amenazas** en entornos locales, virtualizados, contenedores y basados en la nube.*

- Centraliza logs, alertas y vulnerabilidades
- Dashboard web unificado
- Agente multiplataforma
- Sin costos de licencia
- Comunidad muy activa

¿Qué ofrece?

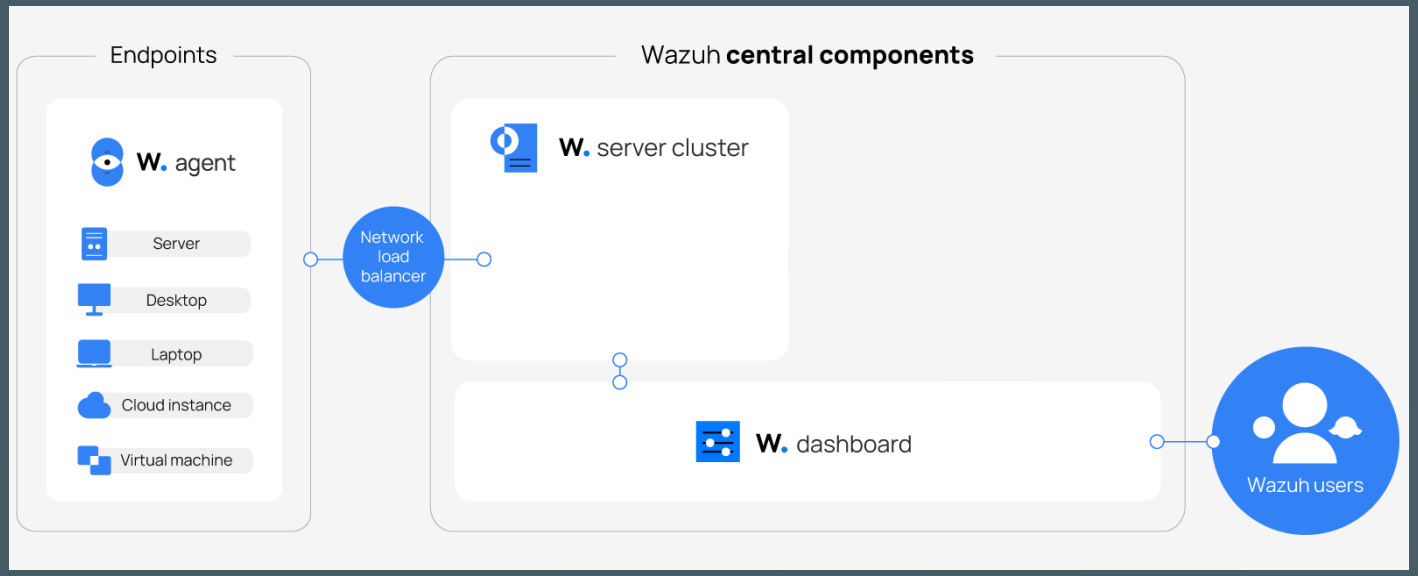
➡️ Desde el inicio:

- `Detecta` accesos y escaladas de privilegio
- Comprueba `integridad de archivos` (FIM)
- `Identifica CVEs` del software instalado
- `Mide qué tan alineado estás` a estándares (PCI, NIST, etc)

➡️ Si lo configurás a fondo:

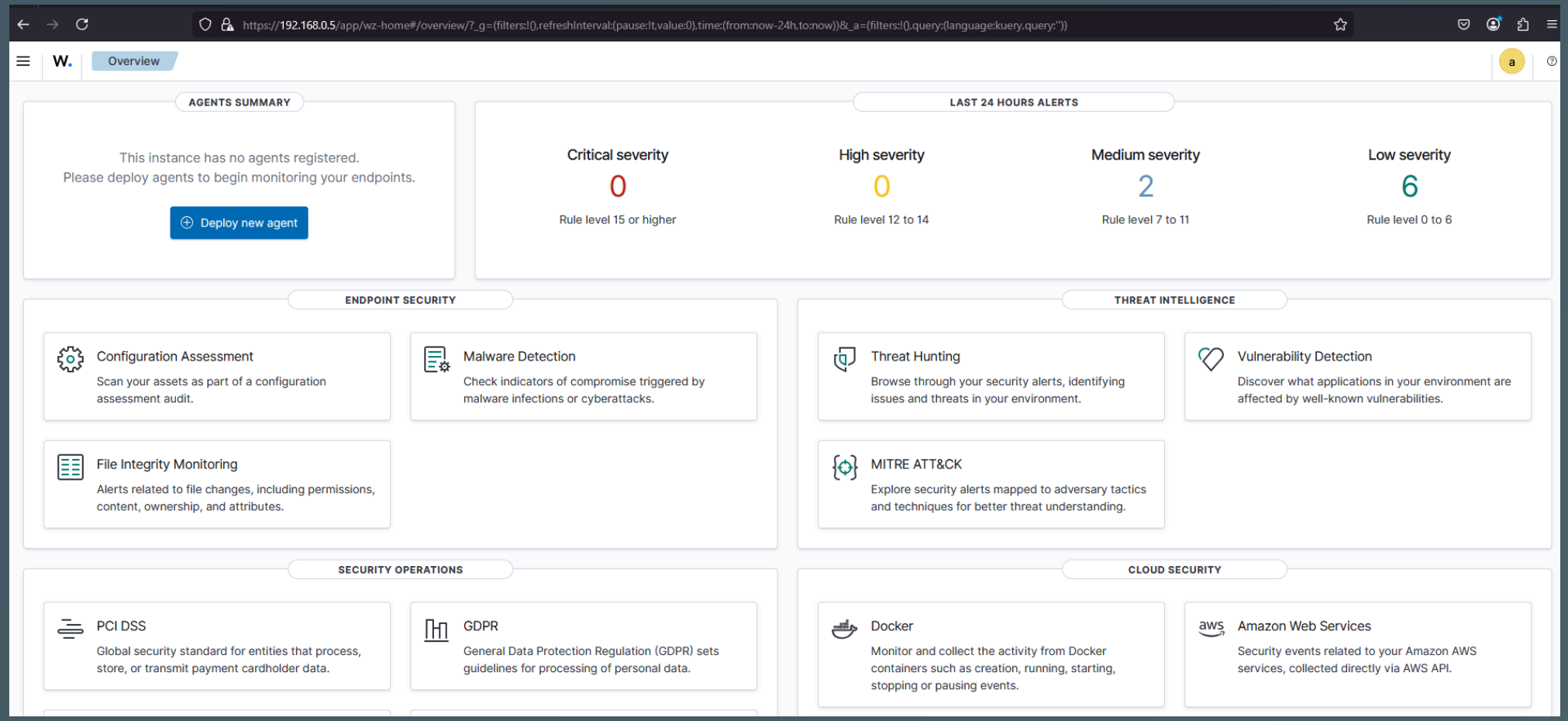
- Se integra con `Slack`, `AWS`, `VirusTotal` y más
- Puede `reaccionar automáticamente` ante ciertos eventos

Arquitectura simplificada de Wazuh

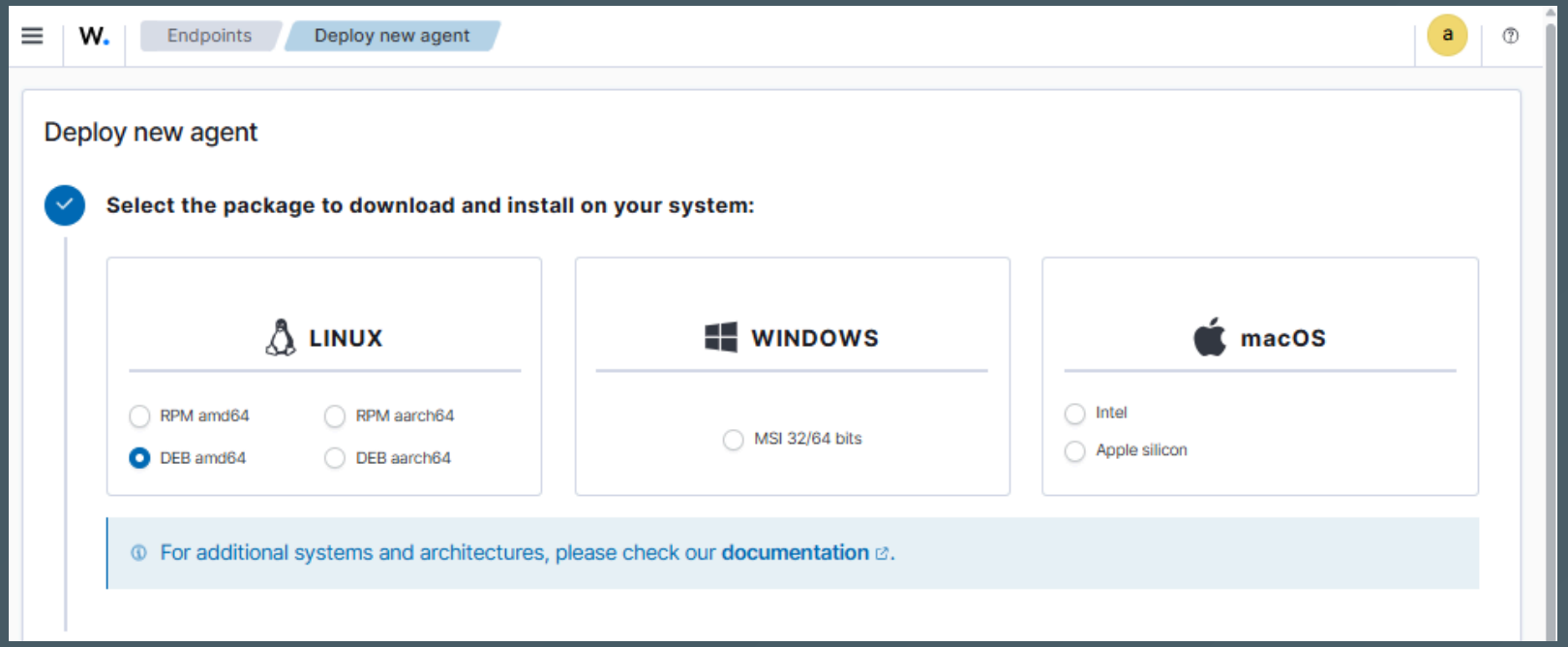


- Modelo `Cliente / Servidor`
- `Eventos Centralizados`
- `Se gestiona desde una Web` (Dashboard)

Wazuh Dashboard

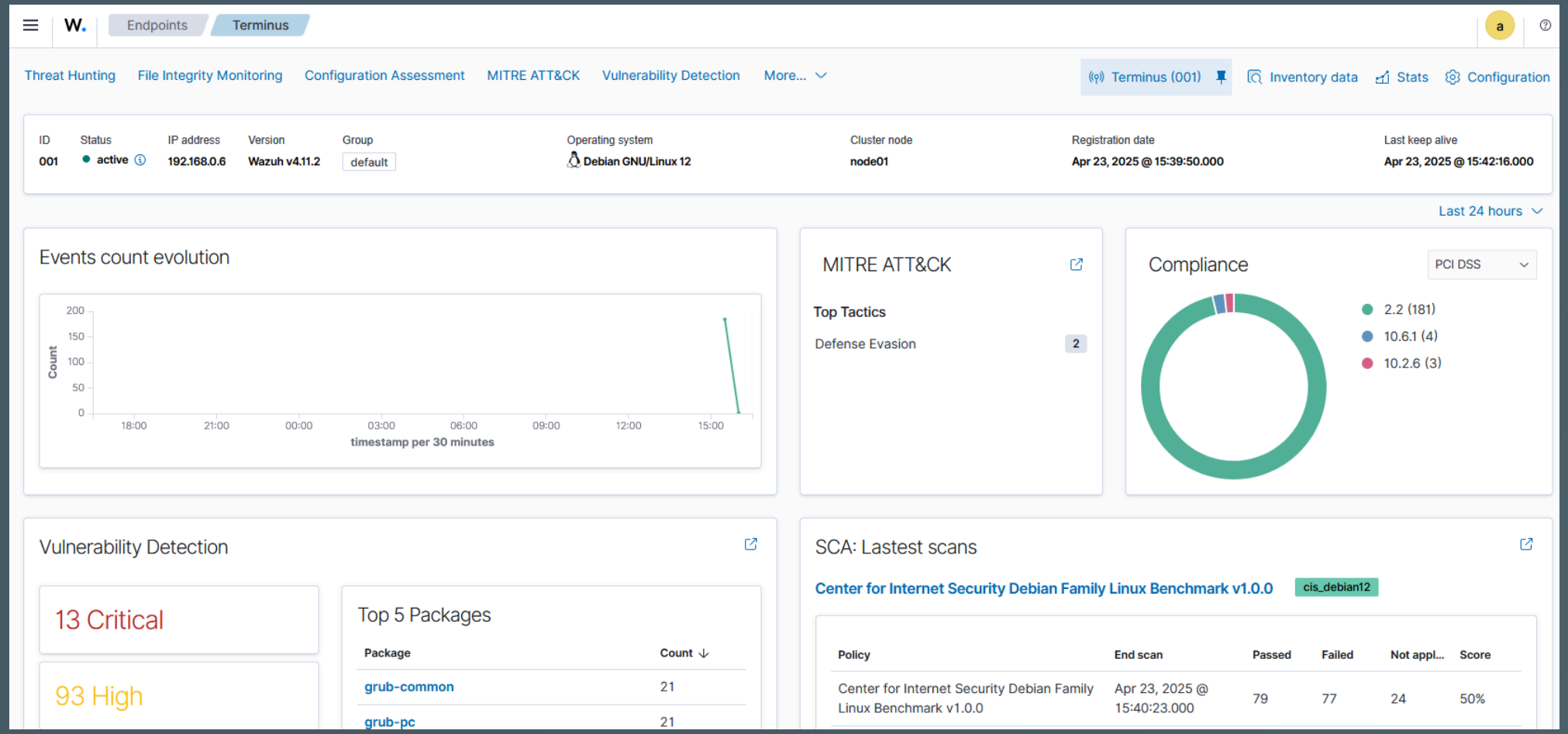


Instalar un agente en GNU/Linux

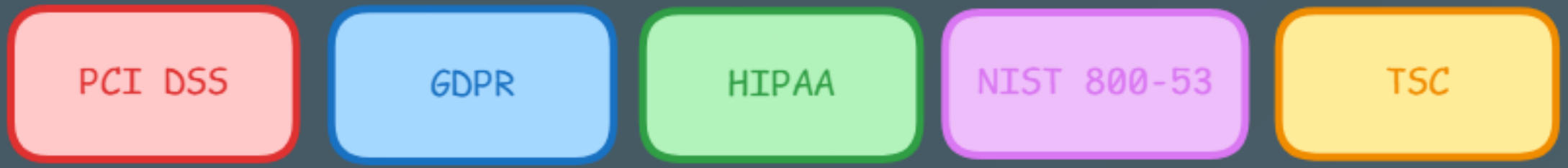



```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.11.2-1_amd64.deb \
&& sudo WAZUH_MANAGER='192.168.0.5' dpkg -i ./wazuh-agent_4.11.2-1_amd64.deb
```

¿Qué veo cuando instalo un agente?

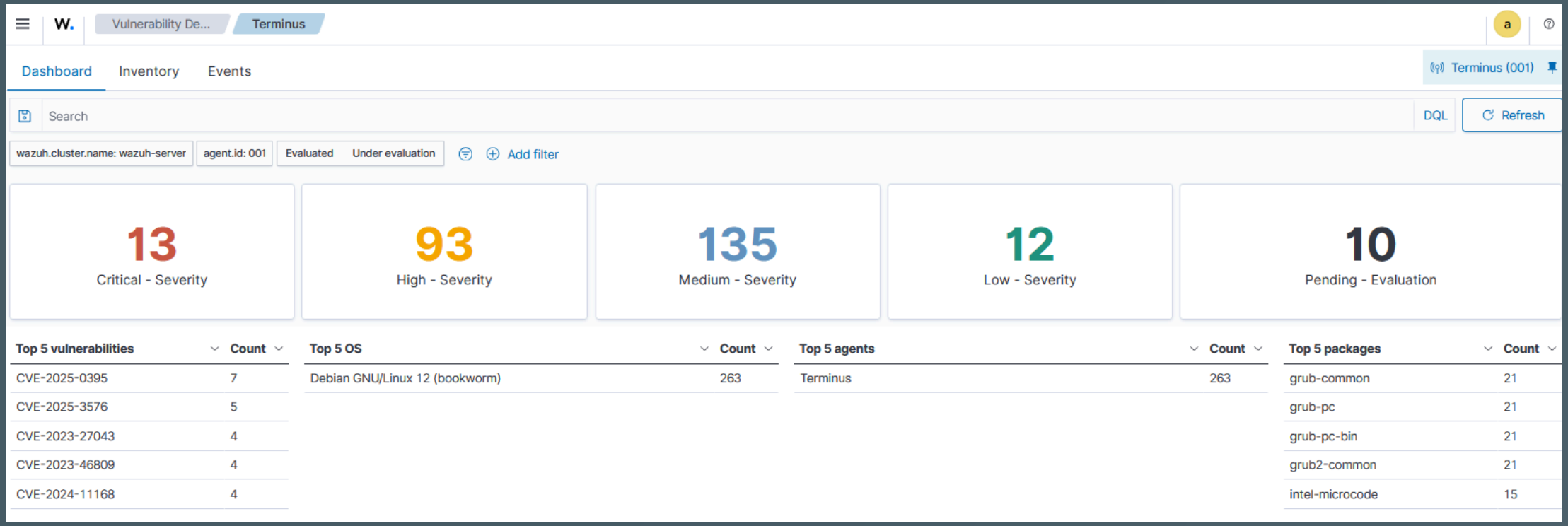


Cumplimiento Normativo



- Vista simple que muestra `qué controles se cumplen`
- Ideal para auditar servidores `sin herramientas pagas`

Detección de vulnerabilidades



¿Cómo instalar Wazuh?

> *Wazuh ofrece múltiples métodos de instalación, según tu entorno y experiencia.*

Te permite iniciar con un entorno simple y escalarlo a despliegues complejos en producción

Instalación rápida (OVA)

Descargar OVA

Importar OVA

Abrir Navegador

Iniciar Sesión

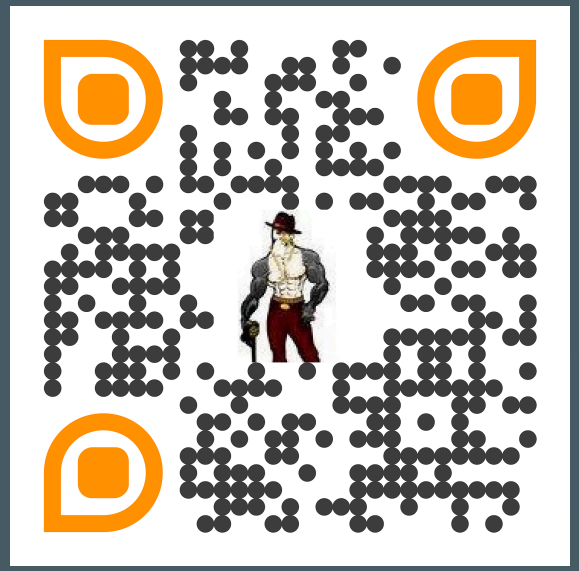
Instalación rápida (OVA)

¿Qué vimos hoy?

- Qué es y qué hace Wazuh
- Qué información tenemos cuando lo instalamos
- Cómo ayuda a cumplir normas de seguridad
- Cómo instalarlo rápidamente
- Cómo agregar un agente (Desktop/Server)

¿Preguntas?

¿Preguntas, ideas o ganas de seguir charlando?



🌐 linktr.ee/sultanovich.sh | 🐙 github.com/sultanovich

```
$ echo  "despedida.txt"
                    Gracias por quedarte hasta el final 🙏
```