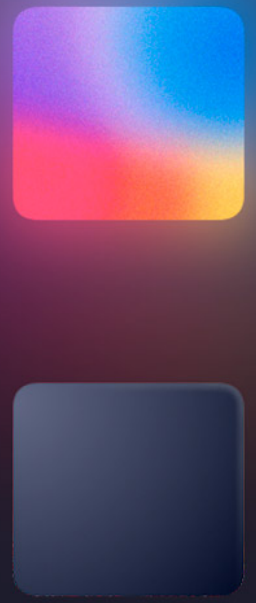
SOCIA: Introducción práctica, herramientas y procesos clave



© 2026 Aktios: Todos los derechos reservados

© 2026 Aktios: Todos los derechos reservados

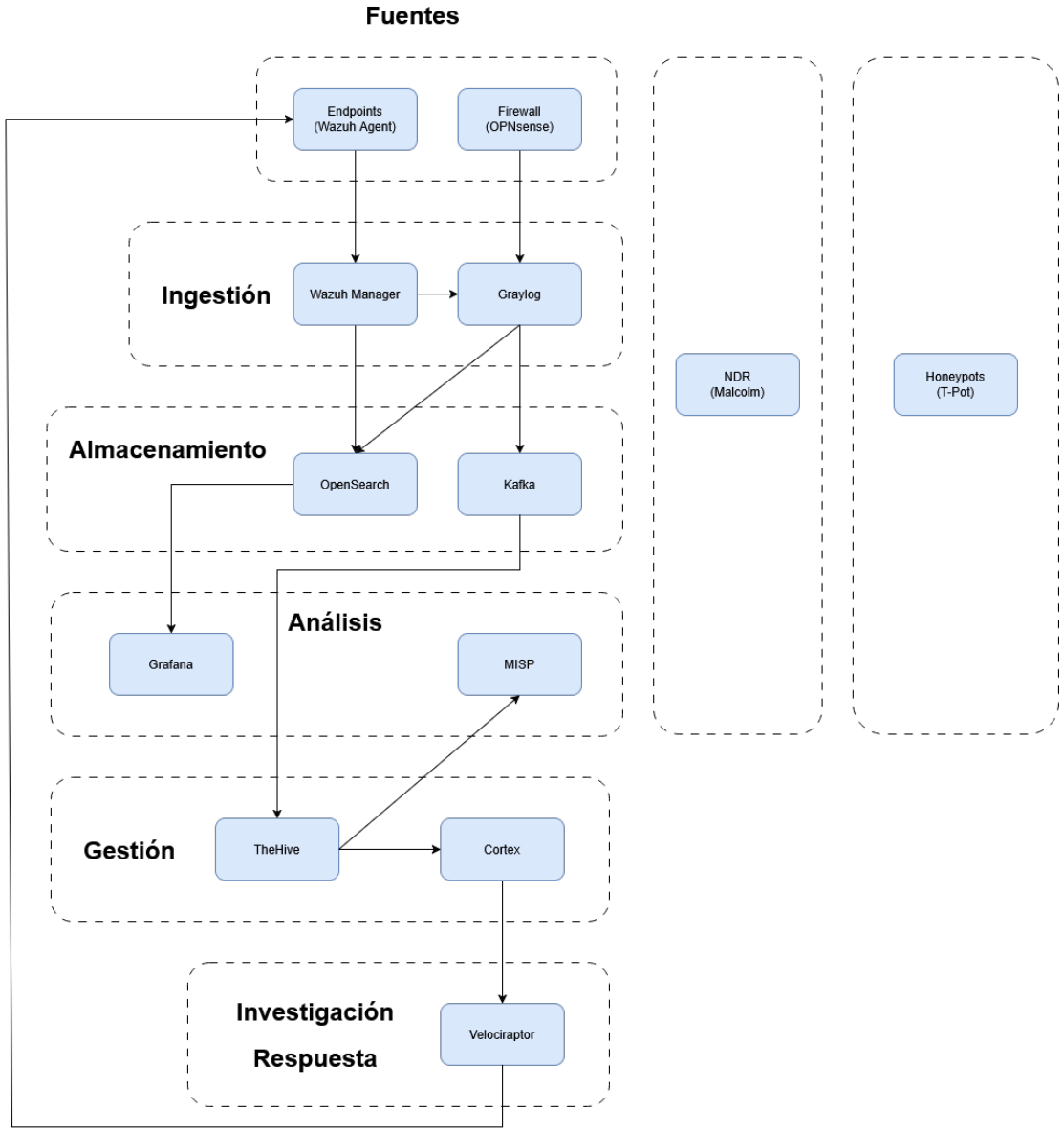
01. Infraestructura de SOCIA

El objetivo de la infraestructura es tener visibilidad total de lo que ocurre en la red y en los sistemas, detectar amenazas y poder responder.

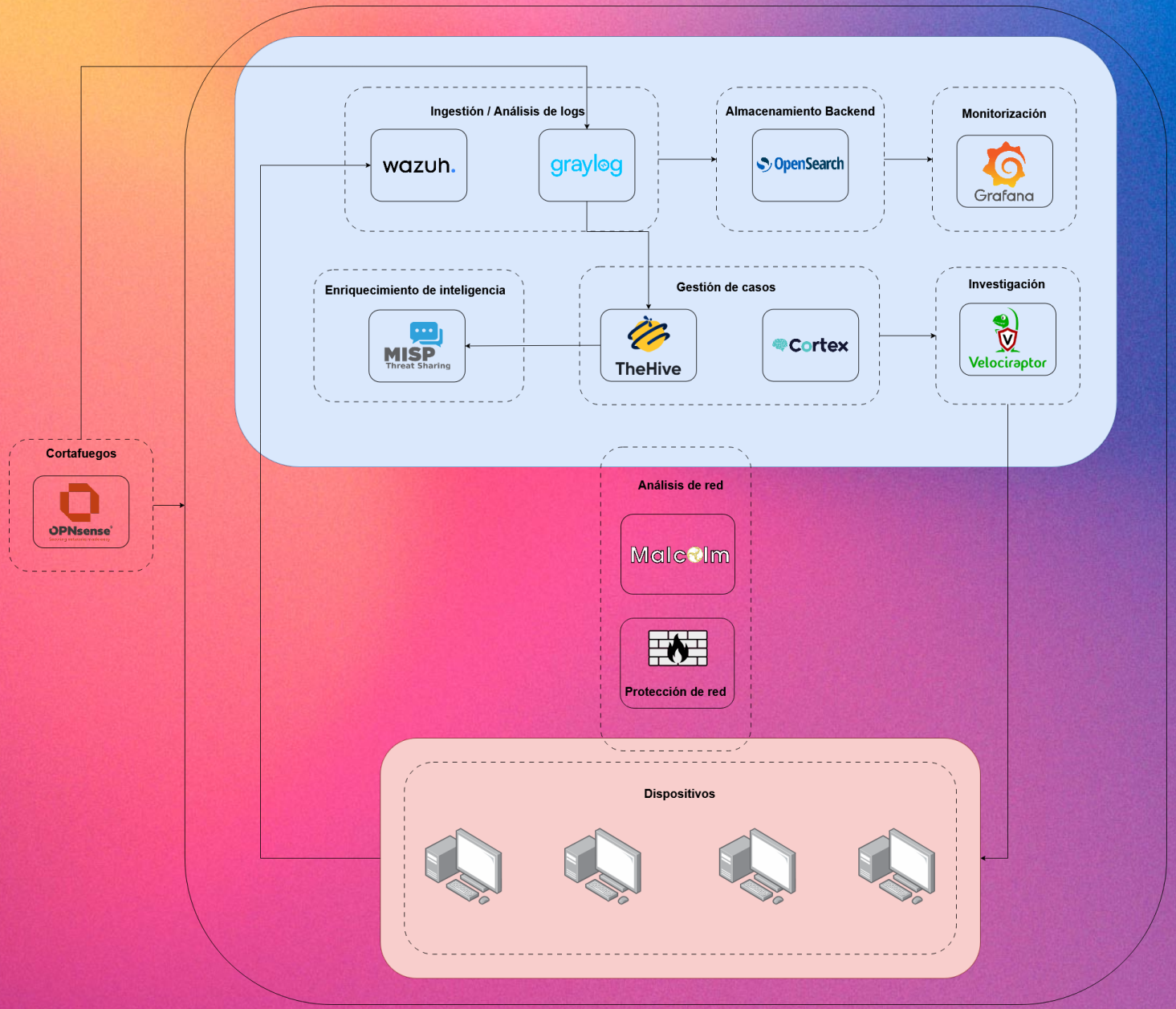
Flujo:

- El *firewall* (OPNsense) genera logs de red.
- Los *endpoints* envían eventos con Wazuh.
- Todo se centraliza en Graylog.
- Grafana se usa para visualizar.
- MISP aporta inteligencia de amenazas.
- TheHive gestiona los incidentes.
- Cortex automatiza análisis.
- Velociraptor permite actuar en las máquinas.

No son herramientas sueltas, es un sistema conectado que sigue un flujo.



© 2026 Aktios: Todos los derechos reservados



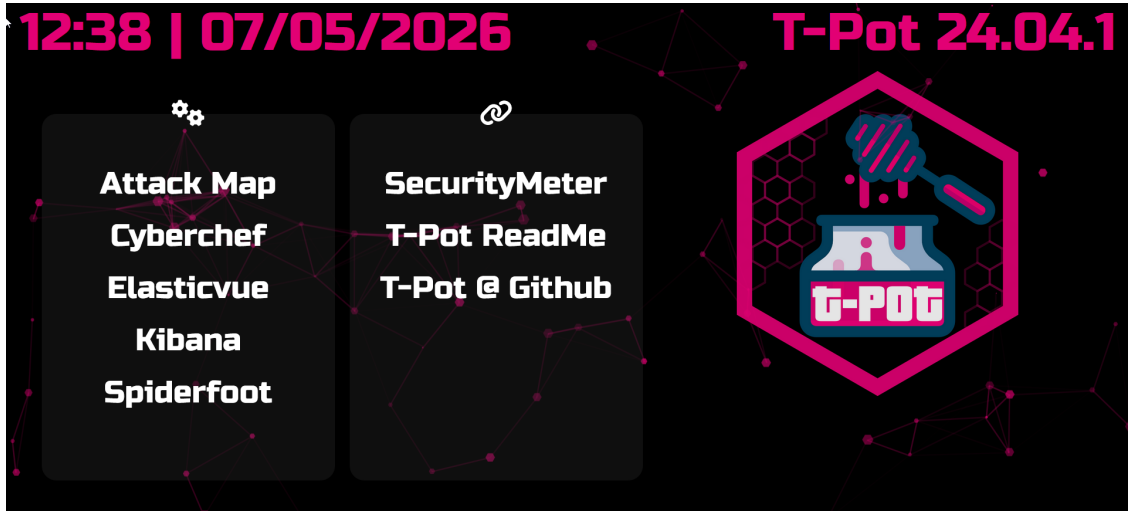
© 2026 Aktios: Todos los derechos reservados

01. Infraestructura de SOCIA: T-Pot

Es una plataforma *open source* que integra múltiples *honeypots* en un único entorno para detectar, registrar y analizar ataques en redes.

Herramientas de análisis:

- **Attack Map**: Muestra en tiempo real los ataques que recibe el sistema, representándolos en un mapa mundial donde se puede ver el origen geográfico de las conexiones maliciosas y la actividad global de los atacantes.
- **Cyberchef**: Sirve para analizar y transformar datos. Permite decodificar en distintos formatos como Base64, Hex, etc.
- **Kibana**: Es el panel principal de visualización de *logs*. Permite analizar los datos generados por los *honeypots* mediante *dashboards* y filtrar la información por IP, país, puerto, etc.
- **Spiderfoot**: Automatiza la recolección de información sobre IPs, dominios, etc. (OSINT).



© 2026 Aktios: Todos los derechos reservados

02. *Firewall*: ¿qué es y qué hace?

Es el primer elemento de seguridad, el que controla qué tráfico entra y sale de la red. Trabaja con reglas que permiten o bloquean conexiones.

Conceptos básicos:

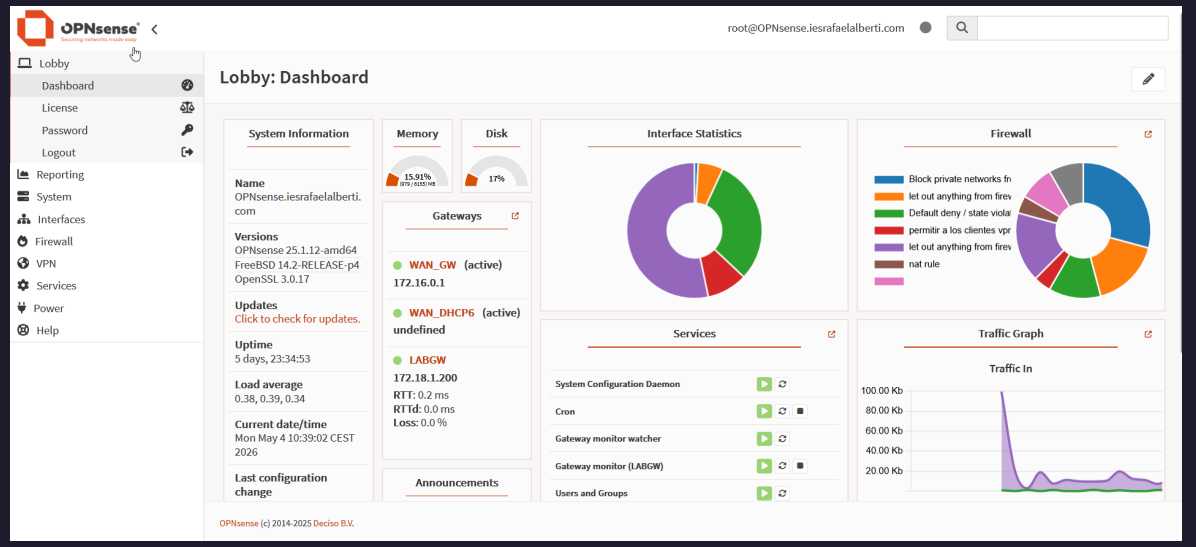
- Control de tráfico.
- Segmentación de redes.
- Protección de servicios.

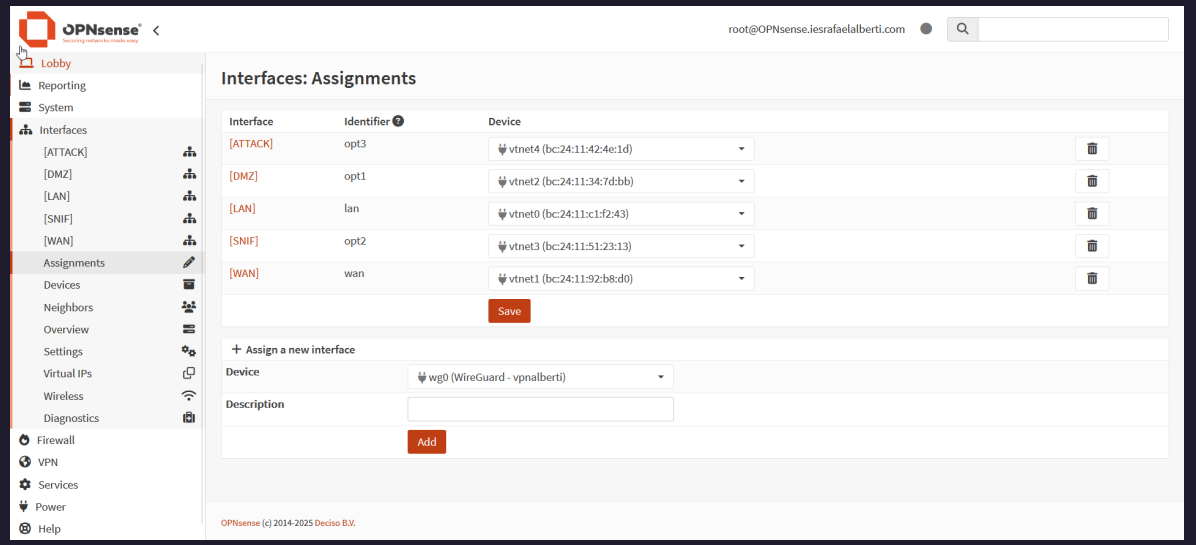
En nuestro entorno:

OPNsense está controlando el tráfico entre redes (*red team* y *blue team*) y registrando todo lo que ocurre.

Ejemplo:

Un equipo intenta acceder a otro → el *firewall* decide si lo permite o lo bloquea y genera un log.





© 2026 Aktios: Todos los derechos reservados

03. SIEM (*Security Information and Event Management*)

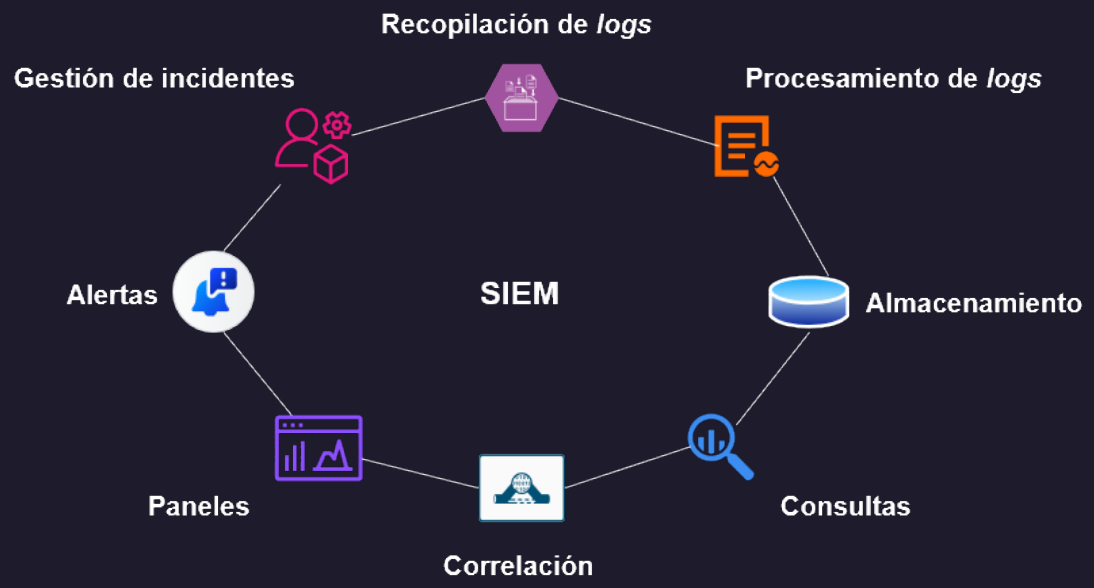
Sin SIEM no hay visibilidad global, solo piezas sueltas.
SIEM es el sistema que recoge todos los *logs*, los analiza y permite detectar ataques.

Problemas que soluciona:

- *Logs* dispersos.
- Difícil correlación.
- Detección manual.

En nuestra arquitectura el SIEM se basa principalmente en:

- Wazuh (eventos de *host*).
- Graylog (centralización y análisis).



© 2026 Aktios: Todos los derechos reservados

03. SIEM: Wazuh en general

Wazuh es un sistema que se instala en las máquinas (agentes) y monitoriza todo lo que ocurre dentro.

¿Qué controla?

- *Logs* del sistema.
- Accesos (como SSH).
- Cambios en archivos.
- Posibles *rootkits*.
- Configuraciones inseguras.

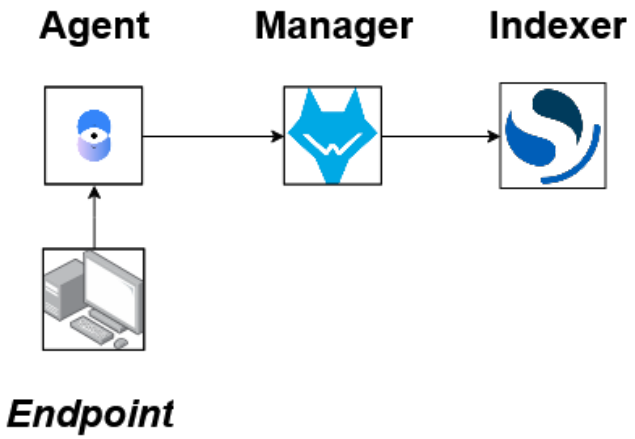
Diferencia con el *firewall*:

Wazuh ve lo que pasa dentro de la máquina.

Ejemplo:

Un atacante intenta entrar por SSH muchas veces → Wazuh lo detecta.

Entramos en detalle de *endpoint*.




```
root@nodo1:~# /var/ossec/bin/agent_control -l

Wazuh agent_control. List of available agents:
   ID: 000, Name: nodo1.proxmox.local (server), IP: 127.0.0.1, Active/Local
   ID: 001, Name: wazuhagent02, IP: any, Active
   ID: 006, Name: debianvuln01, IP: any, Active
   ID: 008, Name: debian, IP: any, Active
   ID: 010, Name: deathnote, IP: any, Disconnected

List of agentless devices:
```

© 2026 Aktios: Todos los derechos reservados

03. SIEM: Graylog en general

Graylog es el núcleo del SIEM, donde llegan todos los *logs*.

¿Qué hace?

- Recibe *logs* de Wazuh y OPNsense.
- Los normaliza.
- Los procesa.
- Permite buscar y correlacionar.

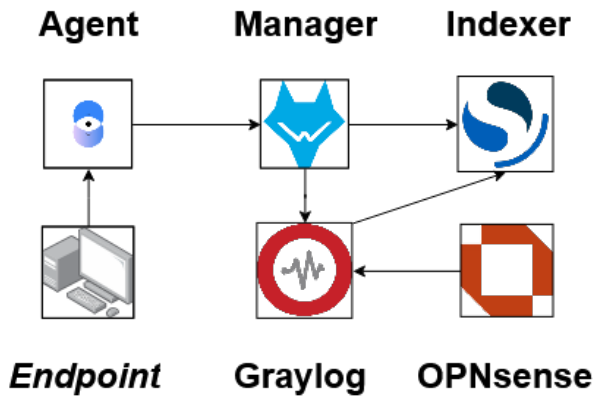
Conceptos:

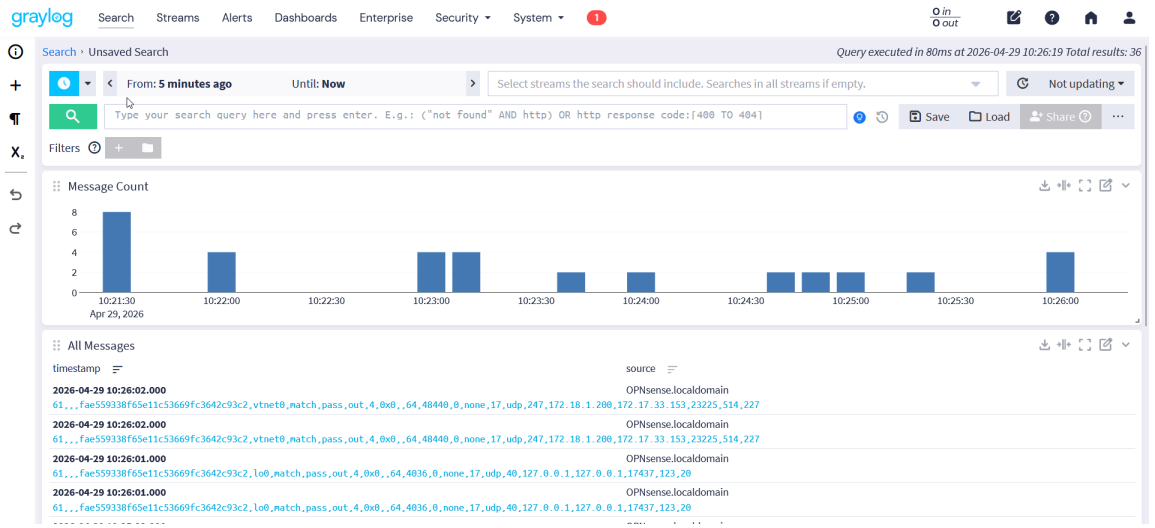
- *Inputs* (entrada de datos).
- *Pipelines* (procesamiento).
- *Streams* (clasificación).

Ejemplo:

Un *login* fallido + una IP sospechosa → Graylog lo junto y genera una alerta más relevante.

Graylog es el cerebro del sistema.





© 2026 Aktios: Todos los derechos reservados

04. Analizando la red: OPNsense + Malcolm

La red te da información que el *host* no ve.

Volvemos al *firewall* pero desde el punto de vista de detección.

Además de bloquear tráfico, también genera información muy valiosa.

OPNsense:

- *Logs* de conexiones.
- IDS/IPS con Suricata.
- Detección de ataques de red.

Malcolm:

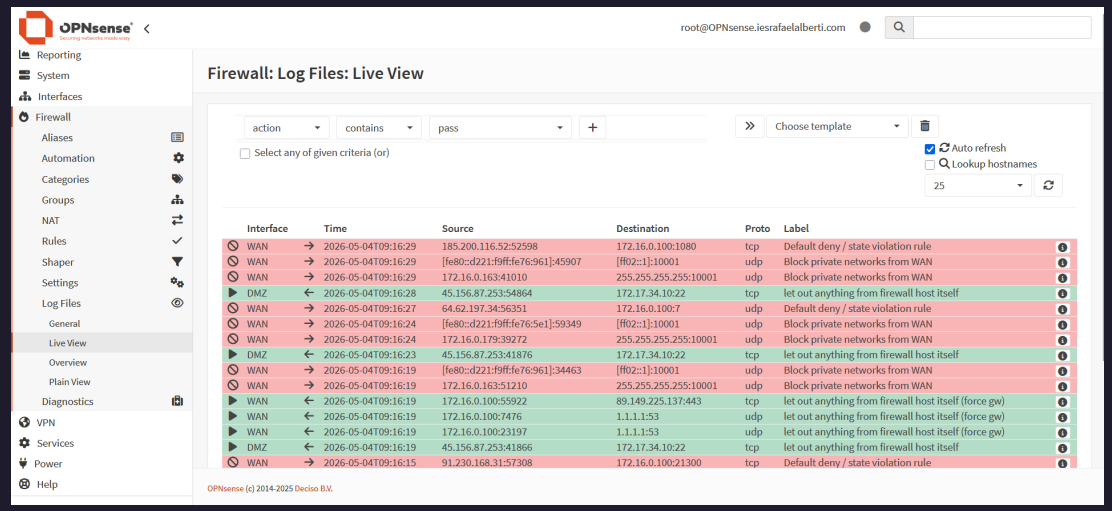
- Análisis profundo de tráfico
- Detección de patrones como DNS sospechoso

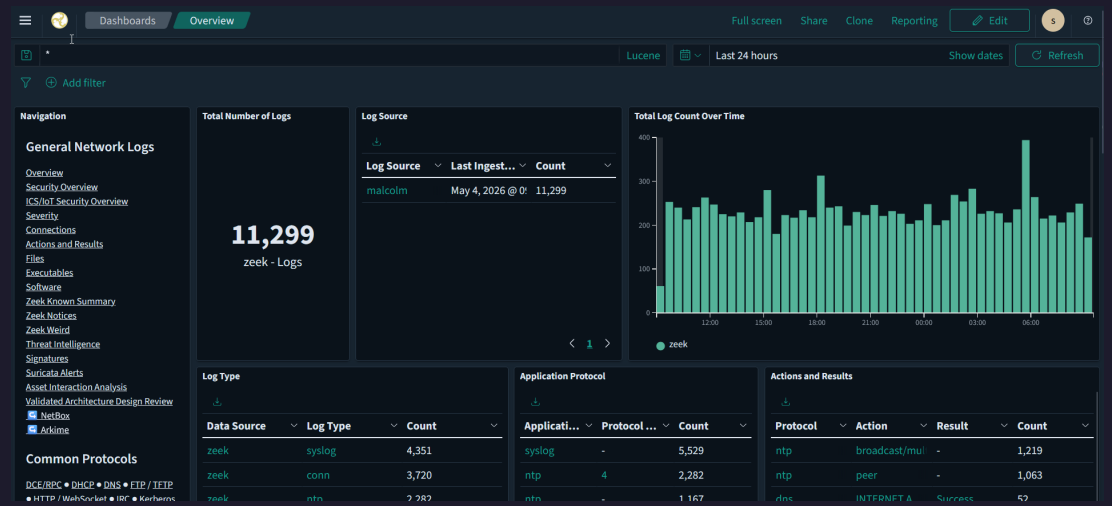
Diferencia importante:

- Wazuh → comportamiento interno
- OPNsense/Malcolm → comportamiento en red

Ejemplo:

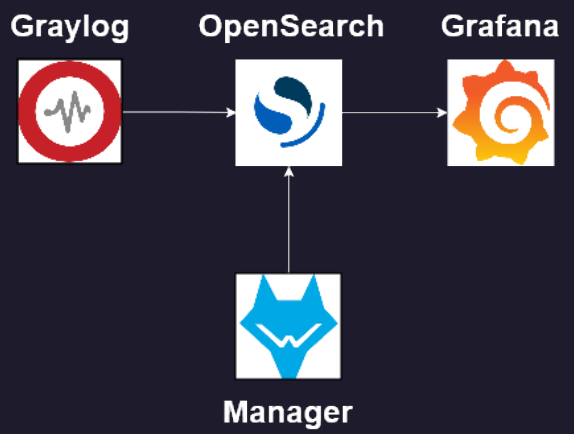
Un equipo se conecta a un servidor raro constantemente → eso puede ser C2.





© 2026 Aktios: Todos los derechos reservados

05. Trabajando con paneles: Grafana



Grafana no detecta nada, pero es clave porque permite ver lo que está pasando.

¿Qué muestra?

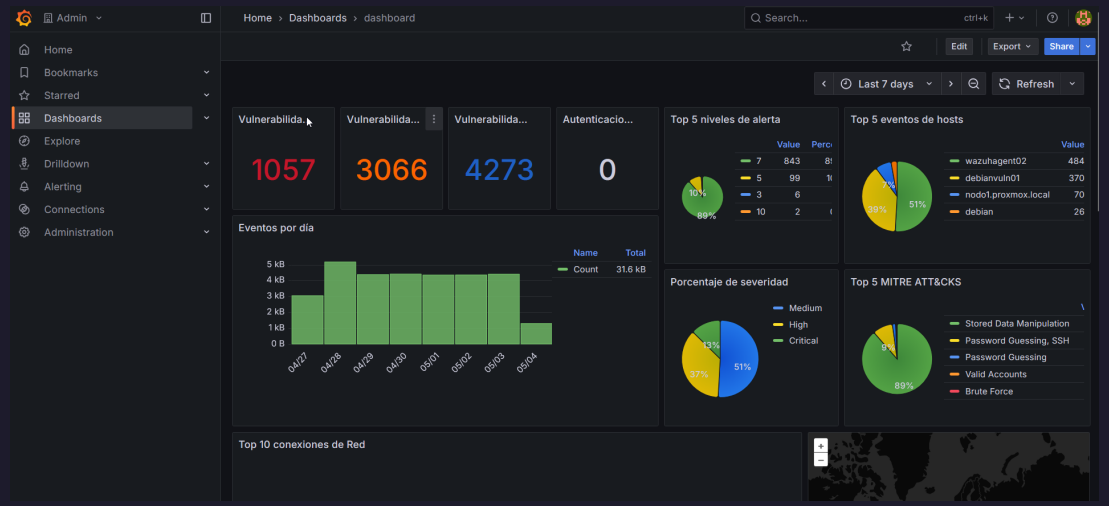
- Número de eventos
- Severidad
- IPs atacantes
- Agentes

Valor:

Permite a un analista ver rápidamente si algo va mal.

Ejemplo:

De repente suben los intentos de SSH → lo ves en un panel.



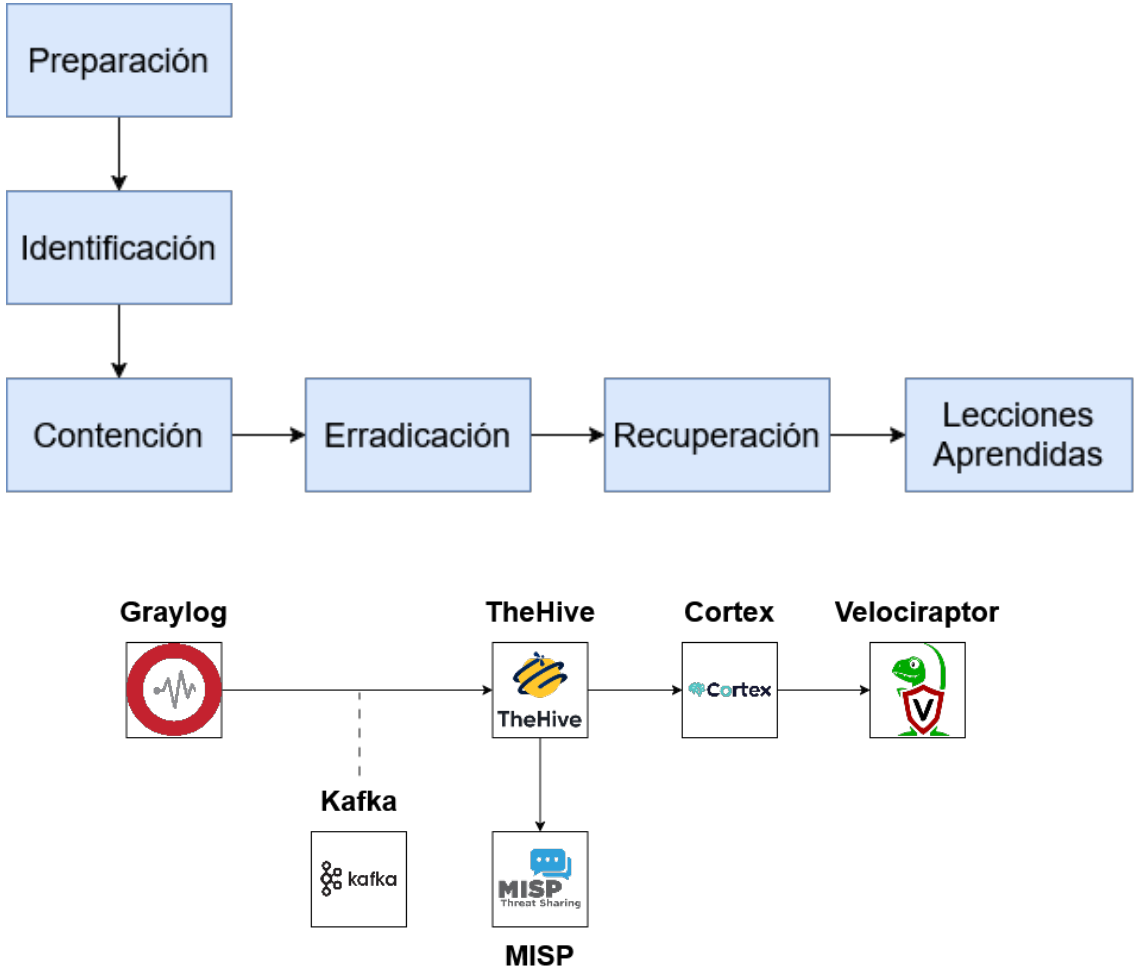
© 2026 Aktios: Todos los derechos reservados

06. IR -¿qué es?

Son el conjunto de acciones que realiza una organización cuando detecta o sospecha que sus sistemas o sus datos han sido comprometidos.

Objetivos:

- Detectar y analizar incidentes .
- Contener y eliminar el ataque en el menor tiempo posible.
- Recuperar los sistemas y reestablecer la operación normal del negocio.
- Analizar lo ocurrido para evitar futuros incidentes.
- Notificar a clientes, usuarios afectados y organismos reguladores.
- Desarrollar capacidades, planes y herramientas que permitan responder eficazmente ante incidentes.



© 2026 Aktios: Todos los derechos reservados

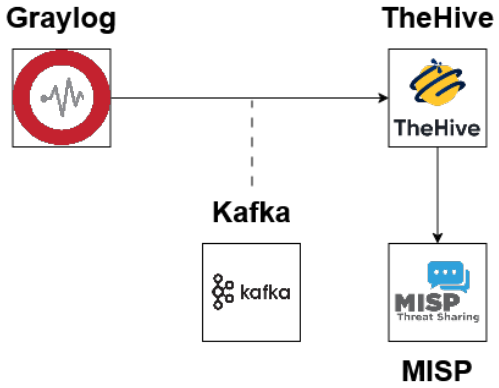
06. IR – *Threat Intelligence*: MISP

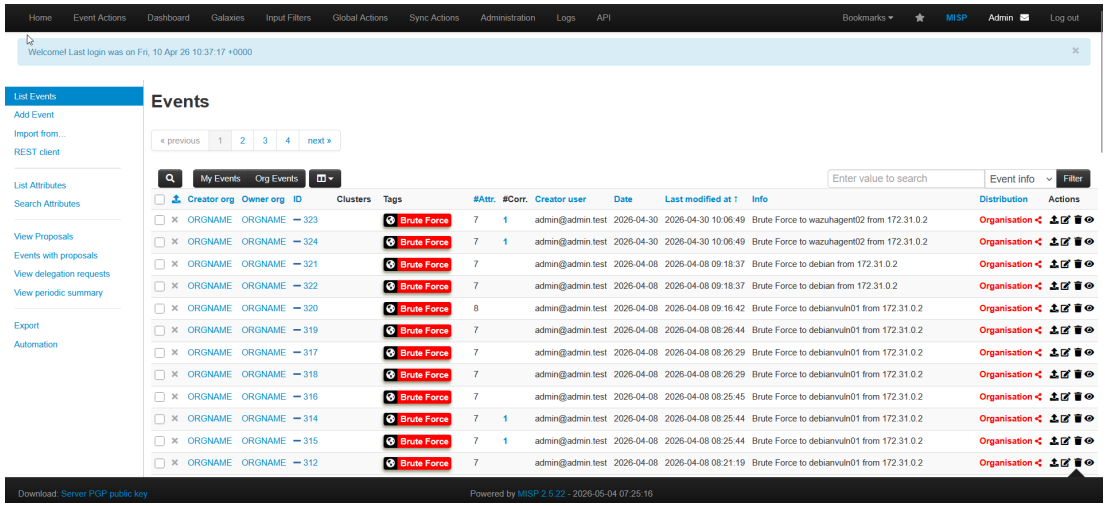
Es una plataforma de código abierto diseñada para compartir, almacenar y correlacionar información sobre amenazas de ciberseguridad.

¿Para qué se utiliza?

- Compartir indicadores de compromiso (IoC), como IP maliciosas, dominios o *hashes* de archivos.
- Analizar y correlacionar datos de amenazas para identificar patrones y campañas.
- Mejorar la colaboración entre empresas, CERTs y equipos de respuesta a incidentes.

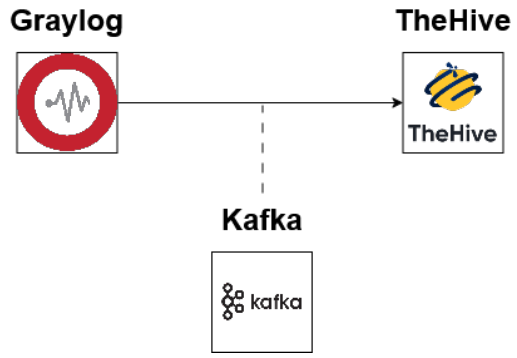
Aquí pasas de detectar a investigar.





© 2026 Aktios: Todos los derechos reservados

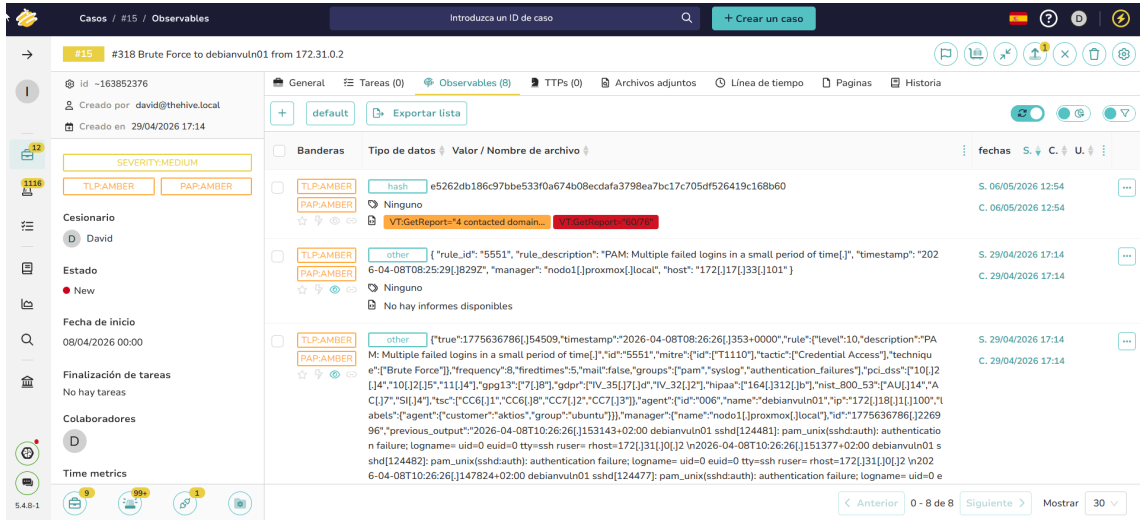
06. IR - Gestión de casos: TheHive



Es una plataforma *open source* utilizada para gestionar y organizar incidentes de seguridad.

Funciones principales:

- Gestión de incidentes (*Cases*).
- Asignación de tareas (trabajo colaborativo).
- Gestión de IoCs.
- Integración con otras herramientas (MISP, Cortex, etc.).

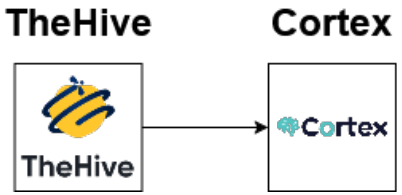


Ejemplo:

1. Graylog genera una alerta.
2. MISP comparte IoCs.
3. TheHive centraliza y organiza la investigación.

© 2026 Aktios: Todos los derechos reservados

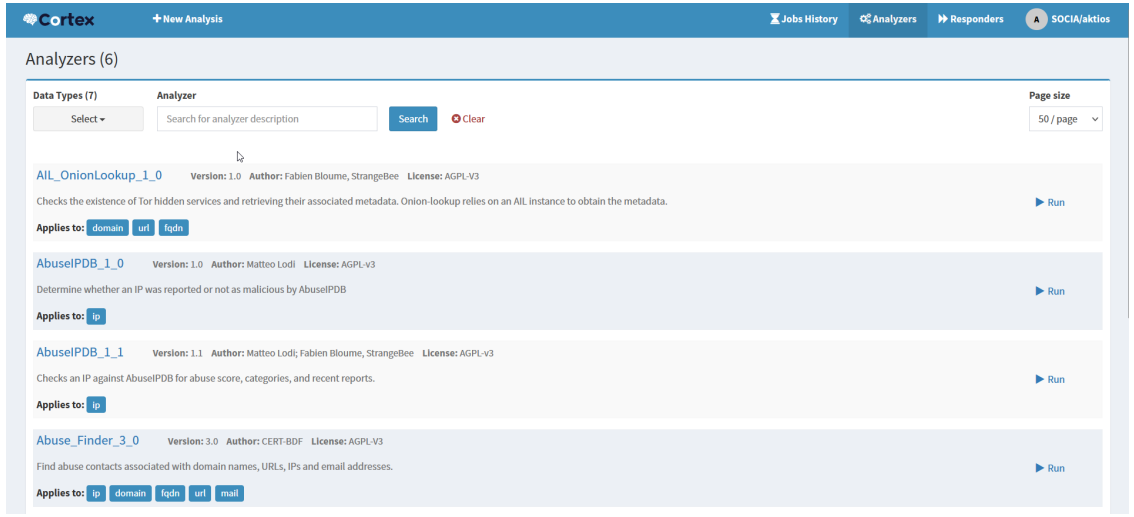
06. IR - Gestión de casos: Cortex



Es una herramienta de automatización utilizada para analizar indicadores de compromiso (IoCs) y ejecutar acciones de respuesta automática. Normalmente trabaja integrado con TheHive.

Funciones principales:

- **Analyzers**: Realizan consultas automáticas sobre indicadores.
  - Consultar VirusTotal.
  - Revisar reputación de IPs.
  - WHOIS de dominios.
  - *Sandbox* de *malware*.
- **Responders**: Ejecutan acciones automáticas.
  - Bloquear una IP.
  - Aislar un equipo.
  - Enviar alertas.
  - Crear tickets.

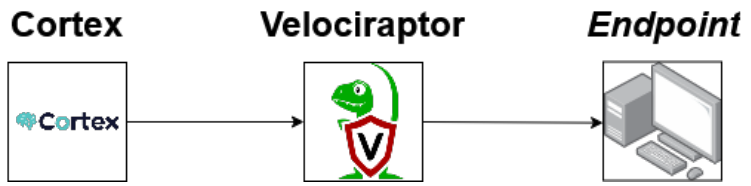


Ejemplo:

1. TheHive crea un *case* a partir de una alerta.
2. El analista añade observables como IPs, *hashes* o URLs.
3. Cortex analiza automáticamente esos indicadores consultando fuentes externas como VirusTotal, etc.

© 2026 Aktios: Todos los derechos reservados

06. IR – Actuación: Velociraptor



Velociraptor permite interactuar con las máquinas:

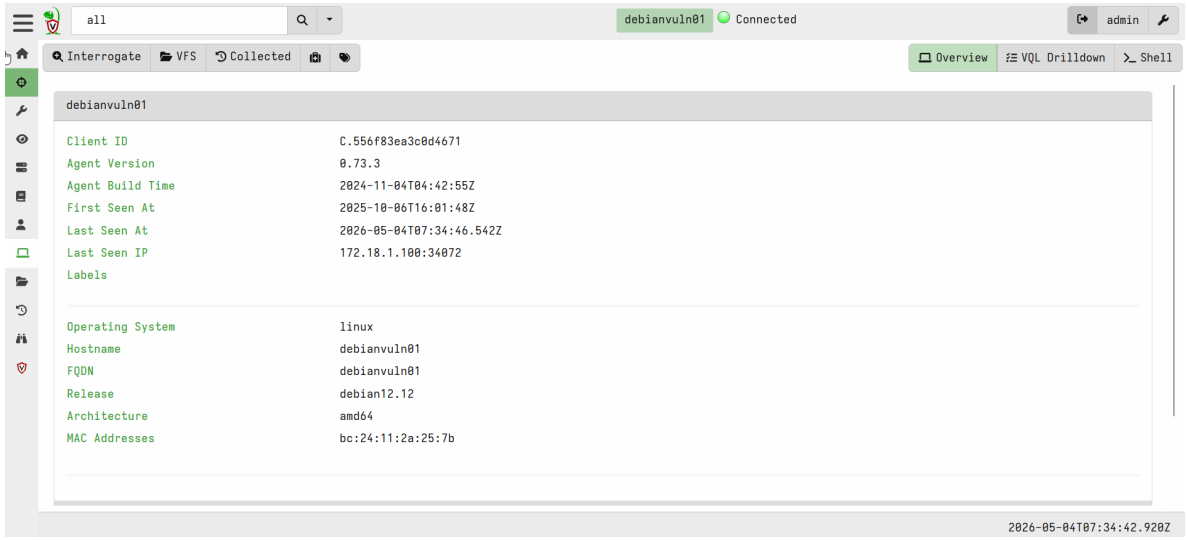
- Ver procesos.
- Analizar conexiones.
- Recoger evidencias.

Se usa cuando ya tienes un incidente confirmado.

Ejemplo:

1. Cortex lanza acciones sobre Velociraptor para recopilar evidencias del equipo afectado.
2. Velociraptor obtiene información como procesos, conexiones de red o archivos sospechosos y la devuelve al *case* para continuar la investigación.

Esto es lo que te permite responder de verdad.



© 2026 Aktios: Todos los derechos reservados

07. *Playbooks*

¿Qué es un *Playbook*?

Es un guía que proporciona un paso a paso de como manejar tipos específicos de amenazas para garantizar una respuesta rápida y coordinada.

Mostrar el archivo con el *playbook* en draw.io.

© 2026 Aktios: Todos los derechos reservados

Gracias

Contacto

Jose Vila
Responsable de seguridad
jose.vila@aktios.com

Alejandro Díaz
Responsable de infraestructura de seguridad
alejandro.diaz@aktios.com

© 2026 Aktios: Todos los derechos reservados