

SOCIA: Introducción práctica, herramientas y procesos clave



/ Infraestructura de SOCIA 01

/ *Firewall: ¿qué es y qué hace?* 02

/ SIEM 03

/ Analizando la red 04

/ Trabajando con paneles: Grafana 05

/ *Incident Response* 06

/ *Playbooks* 07

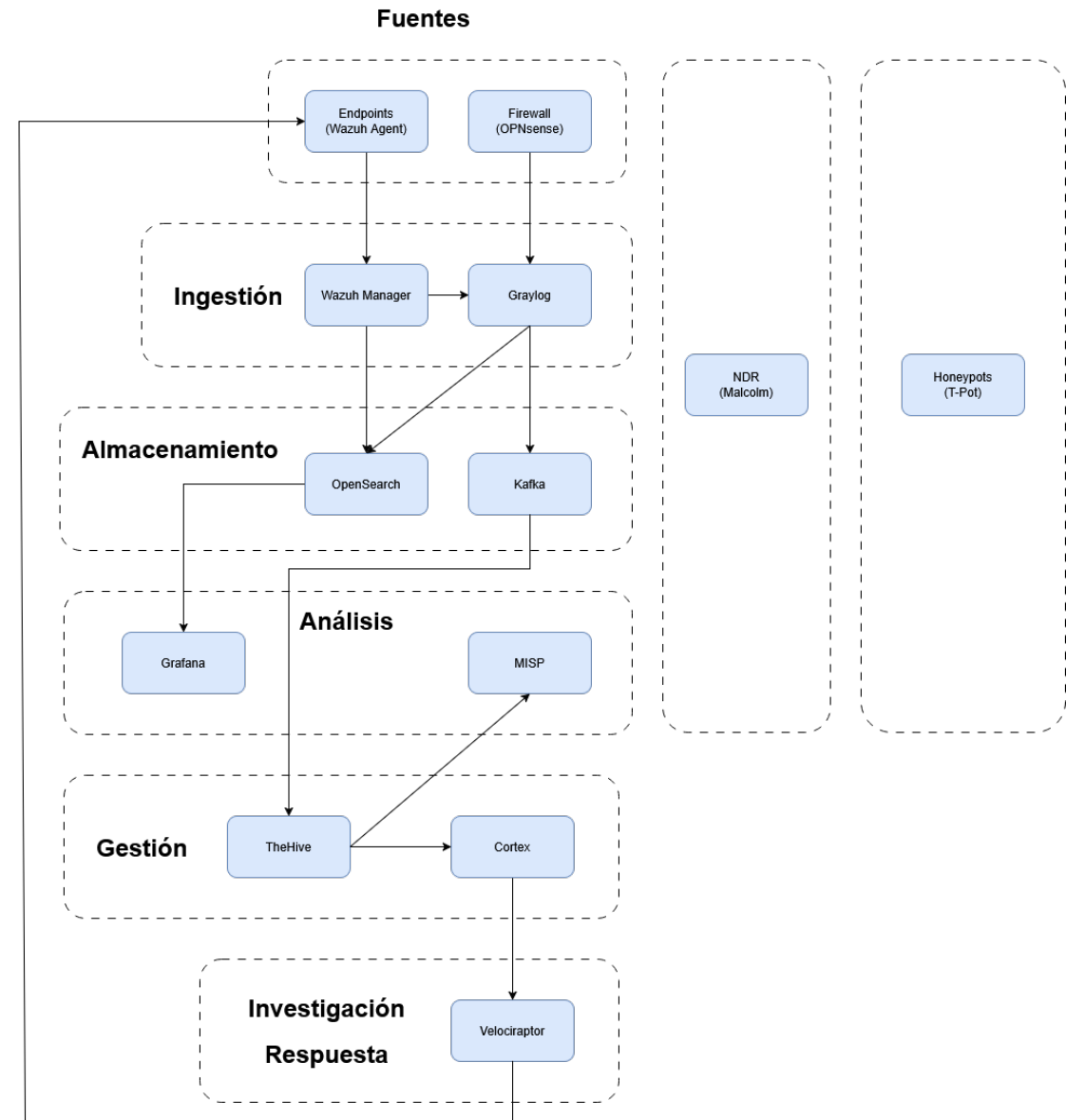
01. Infraestructura de SOCIA

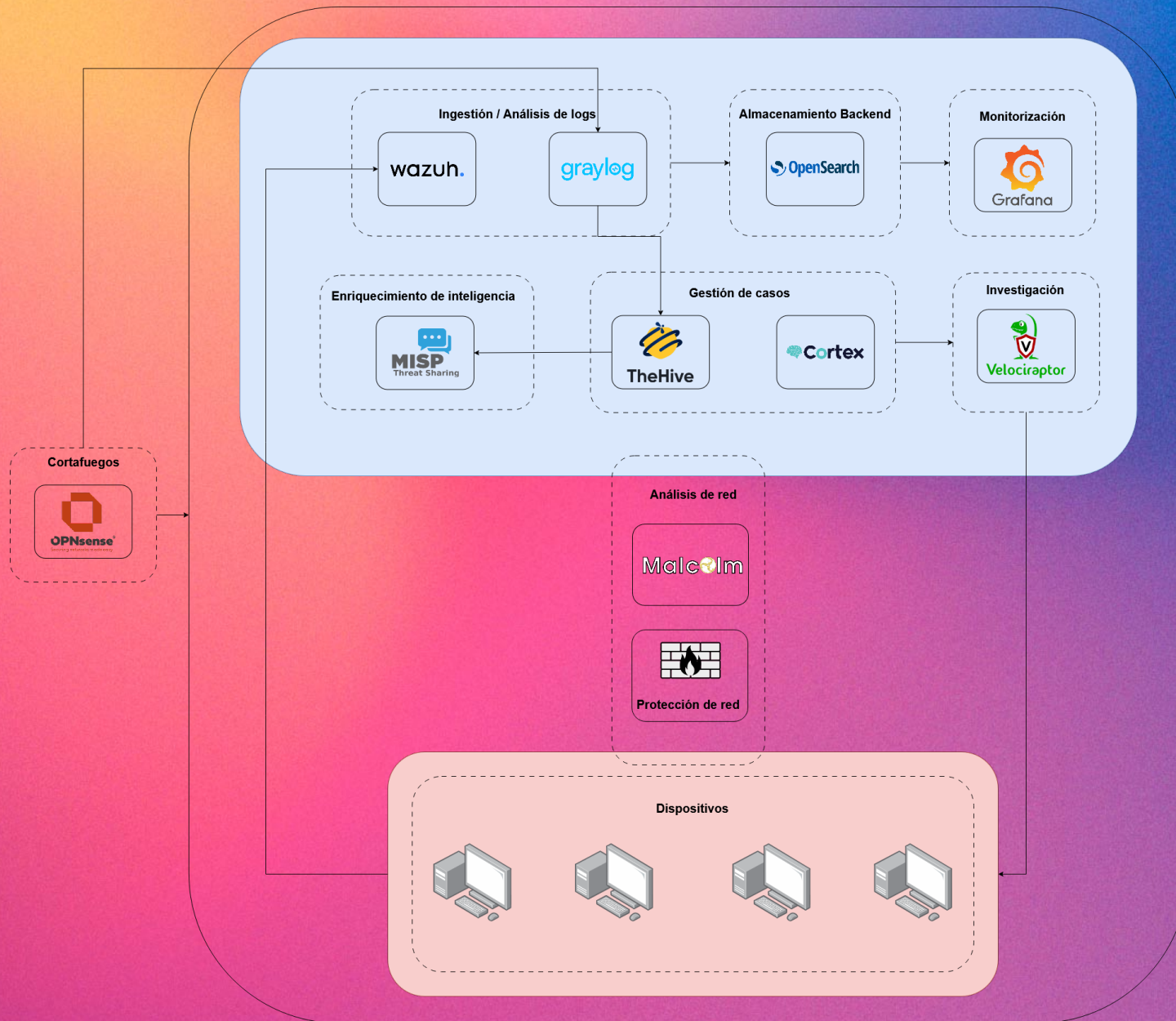
El objetivo de la infraestructura es tener visibilidad total de lo que ocurre en la red y en los sistemas, detectar amenazas y poder responder.

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.



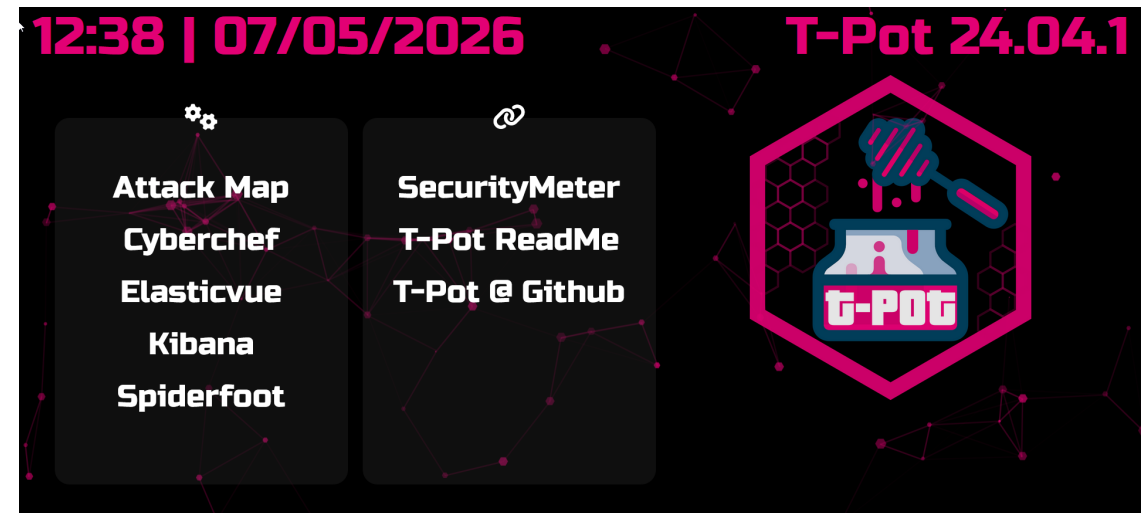


01. Infraestructura de SOCIA: T-Pot

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).



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:

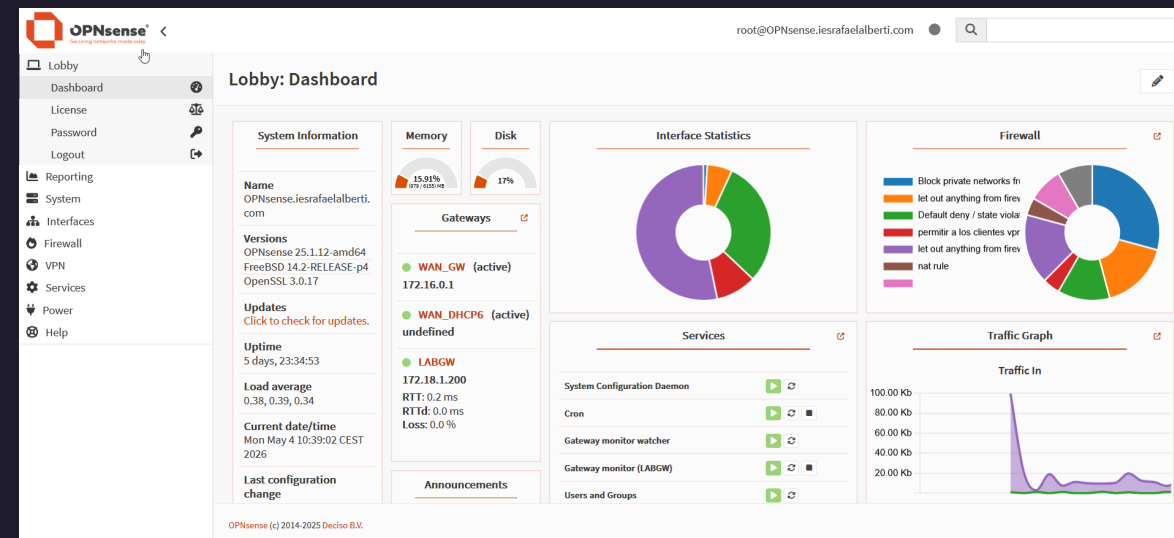
- Control de tráfico.
- Segmentación de redes.
- Protección de servicios.

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.



The screenshot shows the OPNsense Interfaces: Assignments page. The left sidebar is the same as in the dashboard. The main content area is titled 'Interfaces: Assignments' and contains a table of interface assignments:

Interface	Identifier	Device	
[ATTACK]	opt3	vtnet4 (bc:24:11:42:4e:1d)	
[DMZ]	opt1	vtnet2 (bc:24:11:34:7d:bb)	
[LAN]	lan	vtnet0 (bc:24:11:c1:f2:43)	
[SNIF]	opt2	vtnet3 (bc:24:11:51:23:13)	
[WAN]	wan	vtnet1 (bc:24:11:92:b8:d0)	

Below the table is a 'Save' button. Underneath is a section to 'Assign a new interface' with a 'Device' dropdown menu (selected: wg0 (WireGuard - vpnalberti)) and a 'Description' text input field, followed by an 'Add' button.

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

Sin SIEM no hay visibilidad global, solo piezas sueltas.

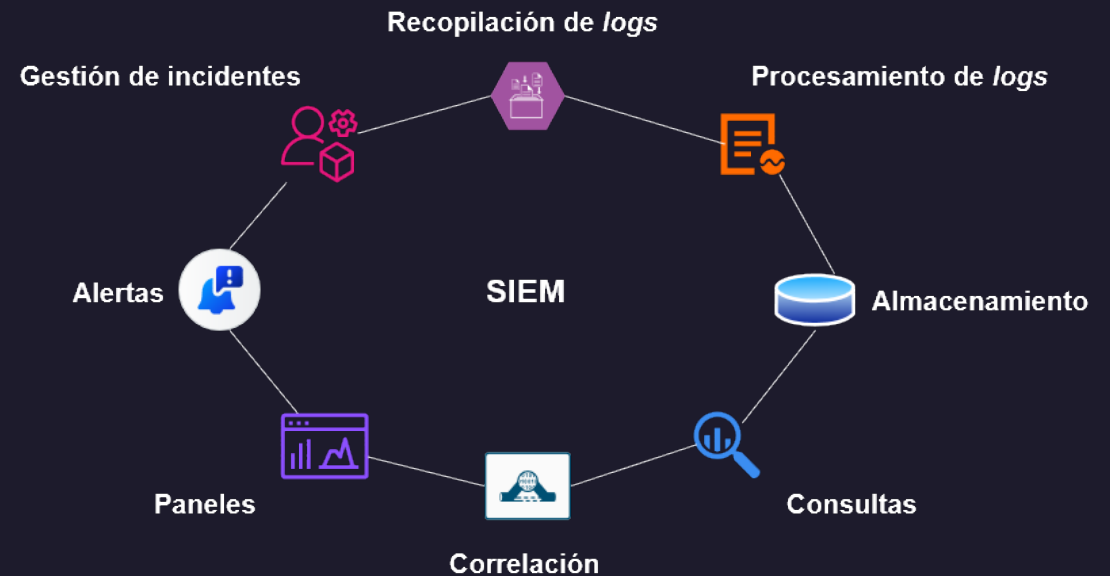
SIEM es el sistema que recoge todos los *logs*, los analiza y permite detectar ataques.

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).



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.

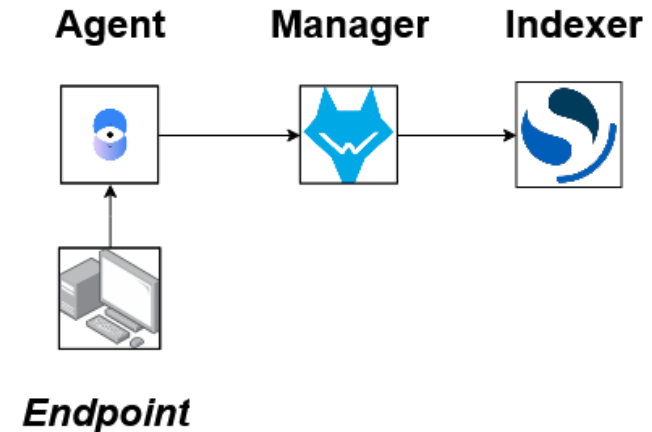
Diferencia con el *firewall*:

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:
  
```

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.

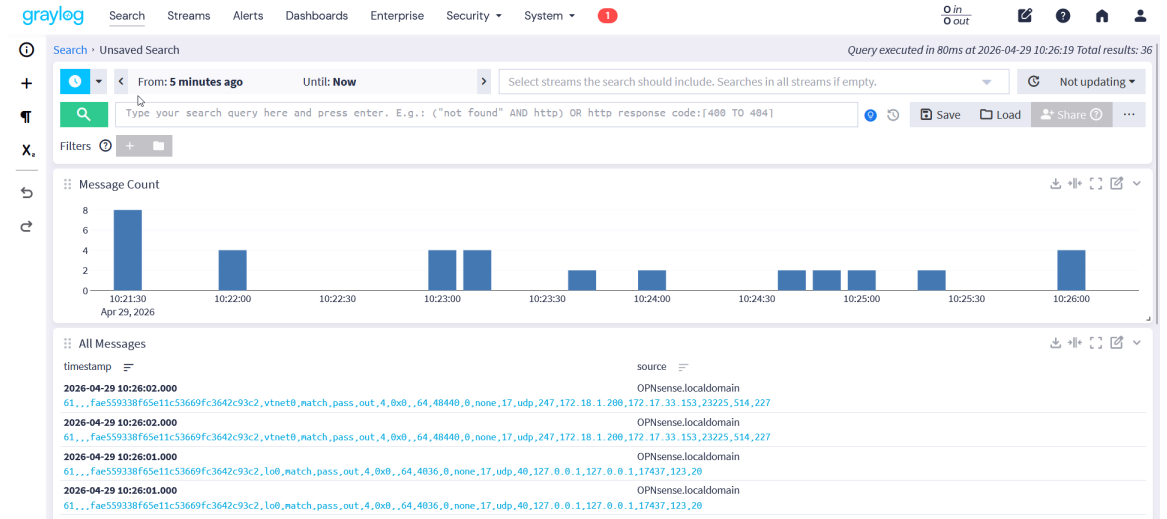
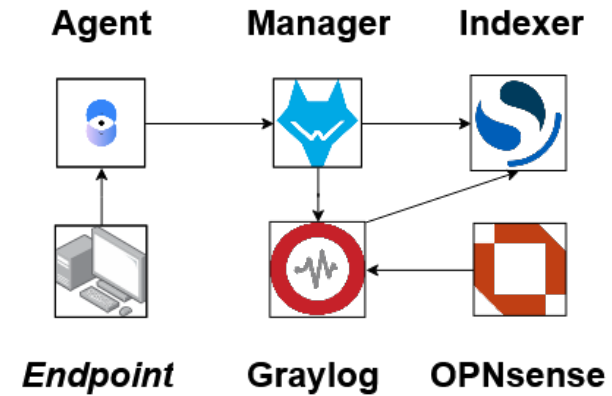
Conceptos:

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

Ejemplo:

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

Graylog es el cerebro del sistema.



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.

OPNsense Firewall: Log Files: Live View

action contains pass + Choose template

Select any of given criteria (or)

Auto refresh
 Lookup hostnames
 25

Interface	Time	Source	Destination	Proto	Label
WAN	→ 2026-05-04T09:16:29	185.200.116.52:52598	172.16.0.100:1080	tcp	Default deny / state violation rule
WAN	→ 2026-05-04T09:16:29	[fe80::d221:9fff:f676:961]:45907	[f02::1]:10001	udp	Block private networks from WAN
WAN	→ 2026-05-04T09:16:29	172.16.0.163:41010	255.255.255.255:10001	udp	Block private networks from WAN
DMZ	← 2026-05-04T09:16:28	45.156.87.253:54864	172.17.34.10:22	tcp	let out anything from firewall host itself
WAN	→ 2026-05-04T09:16:27	64.62.197.34:56351	172.16.0.100:7	udp	Default deny / state violation rule
WAN	→ 2026-05-04T09:16:24	[fe80::d221:9fff:f676:5e1]:59349	[f02::1]:10001	udp	Block private networks from WAN
WAN	→ 2026-05-04T09:16:24	172.16.0.179:39272	255.255.255.255:10001	udp	Block private networks from WAN
DMZ	← 2026-05-04T09:16:23	45.156.87.253:41876	172.17.34.10:22	tcp	let out anything from firewall host itself
WAN	→ 2026-05-04T09:16:19	[fe80::d221:9fff:f676:961]:34463	[f02::1]:10001	udp	Block private networks from WAN
WAN	→ 2026-05-04T09:16:19	172.16.0.163:51210	255.255.255.255:10001	udp	Block private networks from WAN
DMZ	← 2026-05-04T09:16:19	172.16.0.100:55922	89.149.225.137:443	tcp	let out anything from firewall host itself (force gw)
WAN	← 2026-05-04T09:16:19	172.16.0.100:7476	1.1.1.5:3	udp	let out anything from firewall host itself (force gw)
WAN	← 2026-05-04T09:16:19	172.16.0.100:23197	1.1.1.5:3	udp	let out anything from firewall host itself (force gw)
DMZ	← 2026-05-04T09:16:19	45.156.87.253:41866	172.17.34.10:22	tcp	let out anything from firewall host itself
WAN	→ 2026-05-04T09:16:15	91.230.168.31:57308	172.16.0.100:21300	tcp	Default deny / state violation rule

Malcolm Dashboard Overview

Total Number of Logs: 11,299 zeek - Logs

Log Source: malcolm, Last Ingested: May 4, 2026 @ 0: 11,299

Total Log Count Over Time: Bar chart showing log counts over time for zeek.

Data Source	Log Type	Count
zeek	syslog	4,351
zeek	conn	3,720
zeek	ntp	2,282

Application Protocol	Protocol	Count
syslog	-	5,529
ntp	4	2,282
ntp	-	1,167

Protocol	Action	Result	Count
ntp	broadcast/mu...	-	1,219
ntp	conn	peer	1,063
dns	INTERNET A	Success	59

05. Trabajando con paneles: Grafana

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

¿Qué muestra?

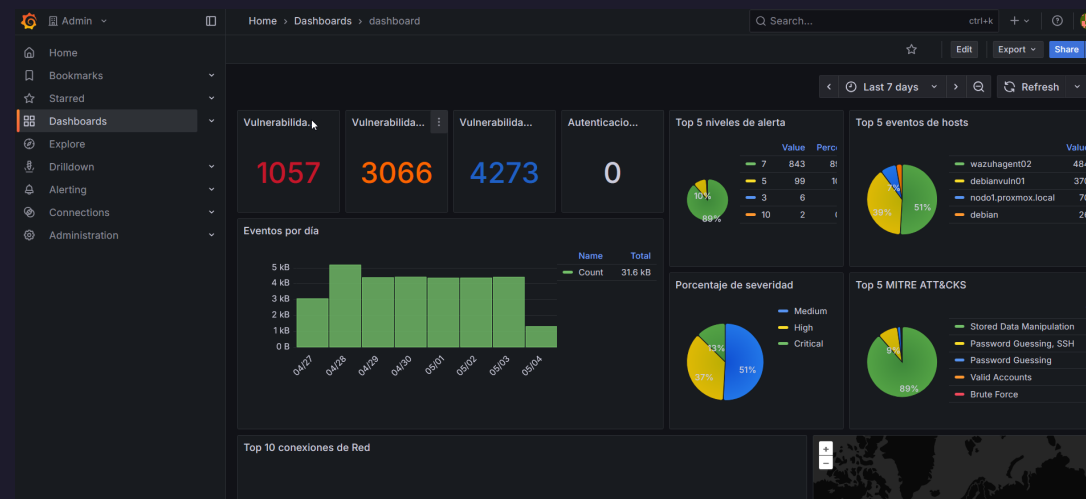
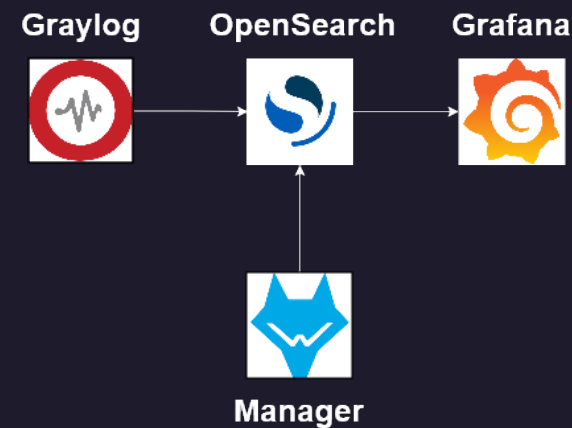
- Número de eventos
- Severidad
- IPs atacantes
- Agentes

Valor:

Permite a un analista ver rápidamente si algo va mal.

Ejemplo:

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

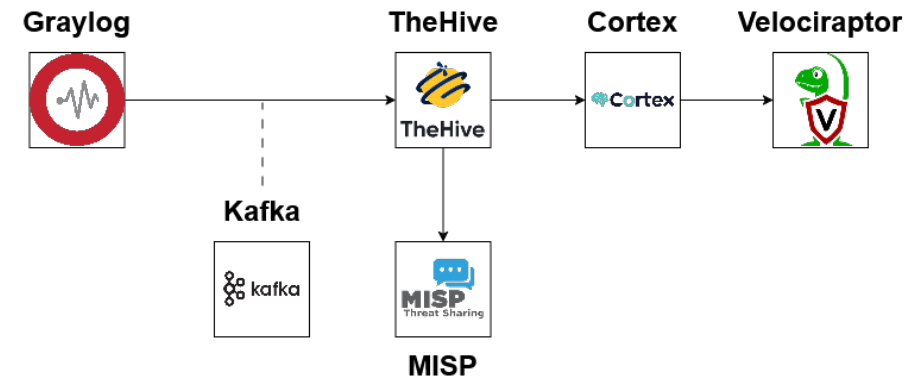
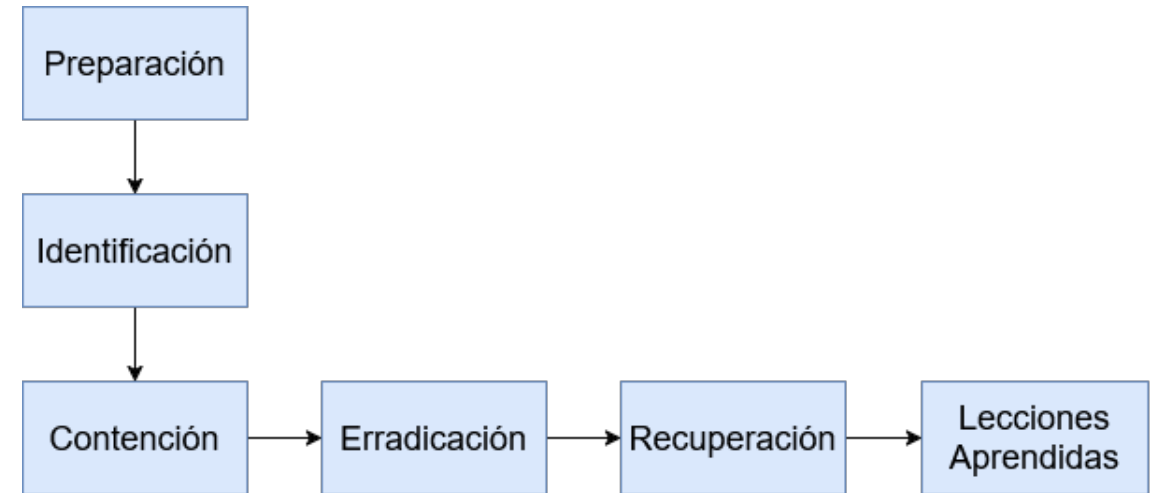


06. IR - ¿qué es?

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.



06. IR - Gestión de casos: TheHive

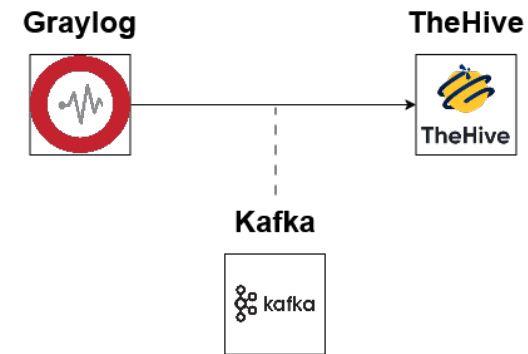
Es una plataforma *open source* utilizada para gestionar y organizar incidentes de seguridad.

Funciones principales:

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

Ejemplo:

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



The screenshot shows the TheHive web interface. At the top, there's a search bar and a '+ Crear un caso' button. Below that, the case details for '#15 #318 Brute Force to debianvuln01 from 172.31.0.2' are visible. The interface includes a sidebar with navigation options like 'Cesionario', 'Estado', 'Fecha de inicio', 'Finalización de tareas', 'Colaboradores', and 'Time metrics'. The main content area displays a table of observables with columns for 'Banderas', 'Tipo de datos', 'Valor / Nombre de archivo', and 'fechas'. The table contains several entries, including one with a 'hash' type and another with an 'other' type, both related to a 'VT:GetReport' action.

06. IR - Gestión de casos: Cortex

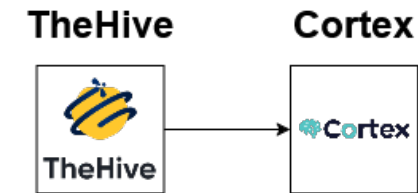
Es una herramienta de automatización utilizada para analizar indicadores de compromiso (IoCs) y ejecutar acciones de respuesta automática. Normalmente trabaja integrado con TheHive.

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.



The screenshot shows the Cortex web interface. At the top, there's a navigation bar with 'Cortex', '+ New Analysis', 'Jobs History', 'Analyzers', 'Responders', and 'SOCIA/aktios'. Below the navigation bar, the main content area is titled 'Analyzers (6)'. There's a search bar with 'Search for analyzer description' and a 'Search' button. Below the search bar, there's a list of analyzers:

Analyzer Name	Version	Author	License	Applies to	Run
AIL_OnionLookup_1_0	Version: 1.0	Author: Fabien Bloume, StrangeBee	License: AGPL-V3	domain, url, fqdn	▶ Run
AbuseIPDB_1_0	Version: 1.0	Author: Matteo Lodi	License: AGPL-V3	ip	▶ Run
AbuseIPDB_1_1	Version: 1.1	Author: Matteo Lodi; Fabien Bloume, StrangeBee	License: AGPL-V3	ip	▶ Run
Abuse_Finder_3_0	Version: 3.0	Author: CERT-BDF	License: AGPL-V3	ip, domain, fqdn, url, mail	▶ Run

06. IR – Actuación: Velociraptor

Velociraptor permite interactuar con las máquinas:

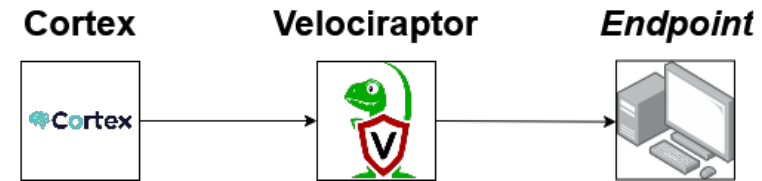
- Ver procesos.
- Analizar conexiones.
- Recoger evidencias.

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.



The screenshot shows the Cortex interface with a search bar containing 'all' and a dropdown menu. The interface is connected to an agent named 'debianvuln01'. The main content area displays the following information:

Client ID	C.556f83ea3c0d4671
Agent Version	0.73.3
Agent Build Time	2024-11-04T04:42:55Z
First Seen At	2025-10-06T16:01:48Z
Last Seen At	2026-05-04T07:34:46.542Z
Last Seen IP	172.18.1.100:34072
Labels	
Operating System	linux
Hostname	debianvuln01
FQDN	debianvuln01
Release	debian12.12
Architecture	amd64
MAC Addresses	bc:24:11:2a:25:7b

The interface also shows navigation options like 'Interrogate', 'VFS', 'Collected', 'Overview', 'SQL Drilldown', and 'Shell'. The bottom right corner displays the timestamp '2026-05-04T07:34:42.920Z'.

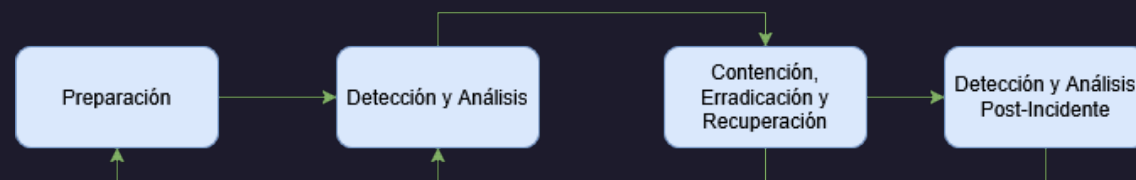
07. Playbooks

¿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.

Fases de un Playbook



Gracias

Contacto

Jose Vila

Responsable de seguridad

jose.vila@aktios.com

Alejandro Díaz

Responsable de infraestructura de seguridad

alejandro.diaz@aktios.com

