

eman ta zabal zazu



Universidad  
del País Vasco

Euskal Herriko  
Unibertsitatea

# WAZUH PLATAFORMA DE SEGURIDAD-OPEN SOURCE, EN LA UPV/EHU

Monitorización de la seguridad de  
los servidores.

[www.ehu.eus](http://www.ehu.eus)

# SITUACIÓN DE PARTIDA



- Sin SIEM, ni EDR/XDR, → antivirus (apex-one) solo en windows
- Sobre los servidores:
  - ¿en qué estado están?
  - ¿están actualizados?
  - ¿controlamos los accesos?
  - ¿están todos vivos?
  - .....
- Necesidad de una herramienta para controlar el estado real de los activos:
  - Versión del SO real, no la de la CMDB
  - ¿están actualizados?
  - ¿Tienen vulnerabilidades los SOs o las aplicaciones instaladas (las reconocidas y con CVS) ?
  - ¿Se detectan ataques en ellos? → ¿Funcionan las medidas de los FW de perímetro?
  - .....

# HERRAMIENTA SELECCIONADA

**wazuh.**  
The Open Source Security Platform

## Razones:

- Open-source
- Escalable
- Compatible con la mayoría de los SO

 **LINUX**

---

RPM amd64  RPM aarch64  
 DEB amd64  DEB aarch64

 **WINDOWS**

---

MSI 32/64 bits

 **macOS**

---

Intel  
 Apple silicon

## ¿Qué es Wazuh?

- Wazuh, plataforma Open-Source de seguridad , capacidades de:
  - XDR
  - SIEM
  - Solución basada en agente ( y sin agente) HIDS

## ¿Qué ofrece Wazuh?



Detección de intrusos



Análisis de Información de los Logs



Monitorización Integridad de Archivos



Detección de vulnerabilidades



Evaluación de la Configuración



Cumplimiento Normativo



Seguridad en la nube



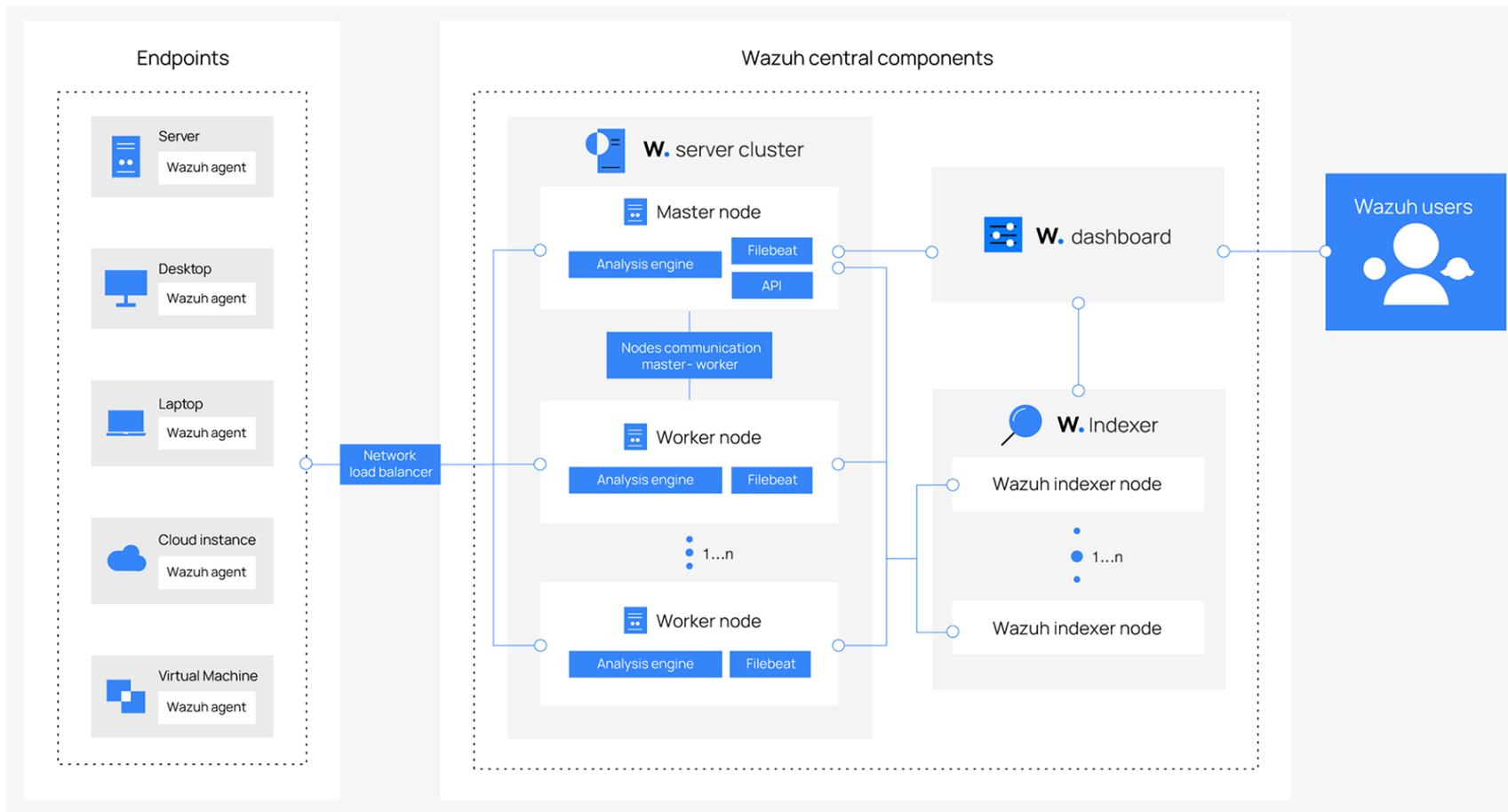
Seguridad en contenedores

# WAZUH EN LA UPV/EHU: PRIMEROS PASOS (1)



- Crear la infraestructura de servidores ... (PoC pequeño)
  - Configuramos:
    - 1 Servidor de Dashboard
    - 2 servidores de Master/Worker+ indexer
- Instalar el Agente en los equipos de producción.
  - Proceso lento y dependiente de los técnicos...  
(Conclusión)→Necesidad de herramienta para estas instalaciones ....
- Agrupar los equipos por áreas y subáreas.
- Muchos Logs.... 😞 Nos hemos quedado cortos en el dimensionamiento:
  - Añadimos más servidores a la infraestructura . Y la adaptamos a las especificaciones dadas por Wazuh.

# WAZUH EN LA UPV/EHU: PRIMEROS PASOS (2)



1 Servidor de Dashboard  
4 Servidores de Master/Worker  
4 Servidores de Indexer

# WAZUH EN LA UPV/EHU

## ¿QUÉ ESTAMOS MONITORIZANDO?



- 558 Servidores con agente (servidores Web, BD, etc)
- M365
- Cisco Umbrella y DNSs internos
- Fw Perimetral
- Antivirus (Apex-One)
- VPNs (Cisco ASA y Forti)
- Logs de Aruba (WiFi)
- .....

Total agents  
**558**

Active agents  
**532**

Disconnected agents  
**25**

Pending agents  
**0**

Never connected agents  
**1**

**SECURITY INFORMATION MANAGEMENT**

 **Security events**

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

 **Integrity monitoring**

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

 **Office 365**

Security events related to your Office 365 services.

**AUDITING AND POLICY MONITORING**

 **Policy monitoring**

Verify that your systems are configured according to your security policies baseline.

 **System auditing**

Audit users behavior, monitoring command execution and alerting on access to critical files.

 **Security configuration assessment**

Scan your assets as part of a configuration assessment audit.

**THREAT DETECTION AND RESPONSE**

 **Vulnerabilities**

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

 **VirusTotal**

Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

 **MITRE ATT&CK**

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

**REGULATORY COMPLIANCE**

 **PCI DSS**

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

 **NIST 800-53**

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

 **GDPR**

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





Total agents  
558

Active agents  
532

Disconnected agents  
25

Pending agents  
0

Never connected agents  
1

SECURITY INFORMATION MANAGEMENT



Security events

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



Integrity monitoring

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



Office 365

Security events related to your Office 365 services.

AUDITING AND POLICY MONITORING



Policy monitoring

Verify that your systems are configured according to your security policies baseline.



System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.



Security configuration assessment

Scan your assets as part of a configuration assessment audit.

THREAT DETECTION AND RESPONSE



Vulnerabilities

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



VirusTotal

Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.



MITRE ATT&CK

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

REGULATORY COMPLIANCE



PCI DSS

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



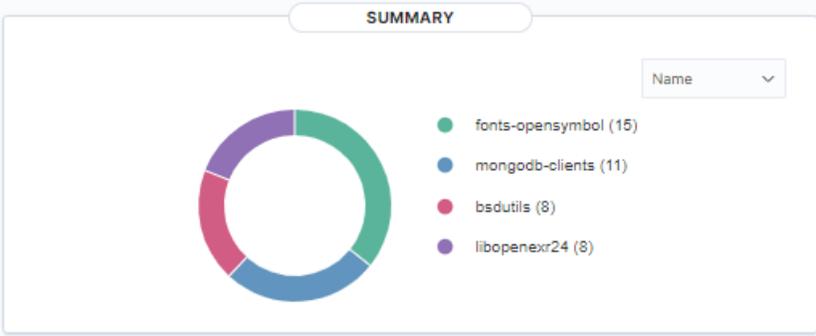
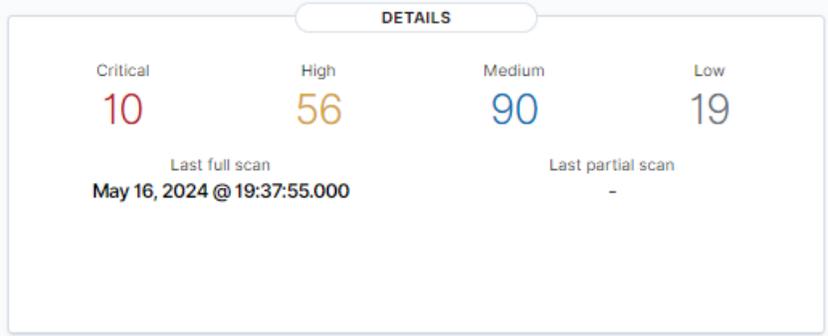
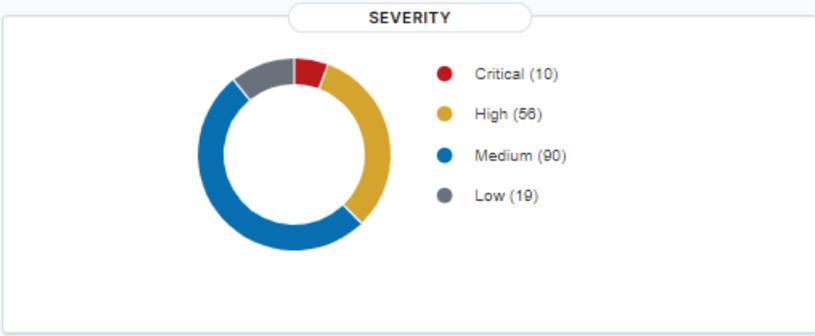
NIST 800-53

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



GDPR

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

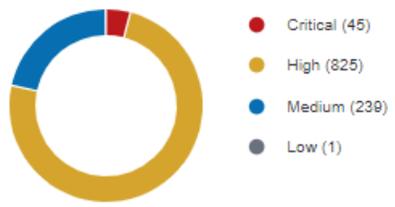


Vulnerabilities (175) Refresh Export formatted

Name ↑	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time ▲
apparmor	2.13.3-7ubuntu5.3	amd64	Critical	CVE-2016-1585	7.5	9.8	May 16, 2024 @ 19:37:46.000
apport	2.20.11-0ubuntu27.27	all	Low	CVE-2022-28653	0	0	May 16, 2024 @ 19:37:50.000
apport-gtk	2.20.11-0ubuntu27.27	all	Low	CVE-2022-28653	0	0	May 16, 2024 @ 19:37:50.000
binutils-common	2.34-6ubuntu1.9	amd64	Medium	CVE-2022-48064	0	5.5	May 16, 2024 @ 19:37:47.000
binutils-x86-64-linux-gnu	2.34-6ubuntu1.9	amd64	Medium	CVE-2022-48064	0	5.5	May 16, 2024 @ 19:37:47.000
bsdutils	2.34-0.1ubuntu9.6	amd64	High	CVE-2018-7738	7.2	7.8	May 16, 2024 @ 19:37:43.000
bsdutils	2.34-0.1ubuntu9.6	amd64	Low	CVE-2013-0157	2.1	0	May 16, 2024 @ 19:37:46.000
bsdutils	2.34-0.1ubuntu9.6	amd64	Medium	CVE-2016-5011	4.9	4.6	May 16, 2024 @ 19:37:46.000
bsdutils	2.34-0.1ubuntu9.6	amd64	High	CVE-2014-9114	7.2	7.8	May 16, 2024 @ 19:37:48.000
bsdutils	2.34-0.1ubuntu9.6	amd64	Medium	CVE-2024-28085	0	0	May 16, 2024 @ 19:37:50.000

Ubuntu 20.04.1 actualizado pero con vulnerabilidades

SEVERITY



DETAILS



SUMMARY



Vulnerabilities (1110)

[Refresh](#) [Export formatted](#)

Name ↑	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time ▲
Windows Server 2008	6.0.6003	x86	Medium	CVE-2024-20692	0	5.7	Mar 8, 2024 @ 21:44:12.000
Windows Server 2008	6.0.6003	x86	High	CVE-2024-20683	0	7.8	Mar 8, 2024 @ 21:44:12.000
Windows Server 2008	6.0.6003	x86	Medium	CVE-2024-20680	0	6.5	Mar 8, 2024 @ 21:44:12.000
Windows Server 2008	6.0.6003	x86	High	CVE-2024-20674	0	8.8	Mar 8, 2024 @ 21:44:12.000
Windows Server 2008	6.0.6003	x86	Medium	CVE-2024-20684	0	6.5	Mar 8, 2024 @ 21:44:12.000

Windows 2008 → 14 de febrero de 2020, Microsoft puso fin al soporte → solución Virtual Patching de Trend



Total agents  
558

Active agents  
532

Disconnected agents  
25

Pending agents  
0

Never connected agents  
1

SECURITY INFORMATION MANAGEMENT



Security events

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



Integrity monitoring

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



Office 365

Security events related to your Office 365 services.

AUDITING AND POLICY MONITORING



Policy monitoring

Verify that your systems are configured according to your security policies baseline.



System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.



Security configuration assessment

Scan your assets as part of a configuration assessment audit.

THREAT DETECTION AND RESPONSE



Vulnerabilities

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



VirusTotal

Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.



MITRE ATT&CK

Security events from the knowledge base of adversary tactics and techniques based on real-world observations

REGULATORY COMPLIANCE



PCI DSS

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



NIST 800-53

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



GDPR

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

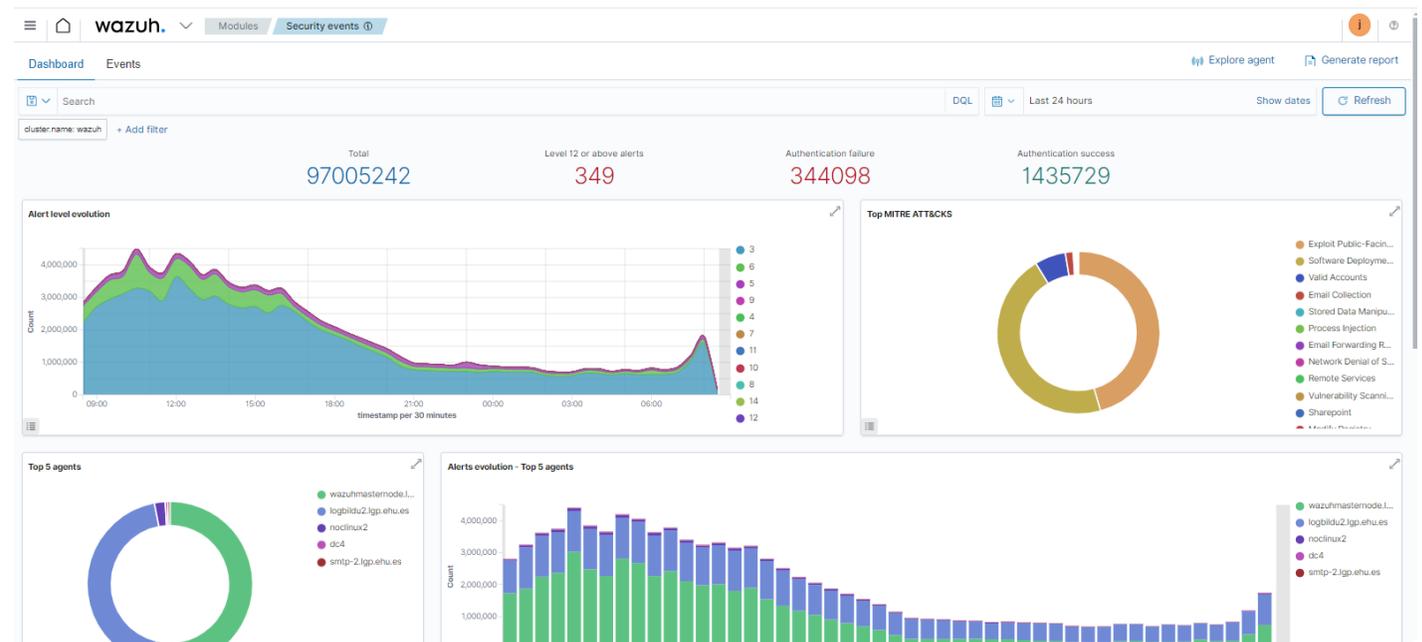
# WAZUH EN LA UPV/EHU: MUCHOS DATOS (2) EVENTOS DE SEGURIDAD



# WAZUH EN LA UPV/EHU: MUCHOS DATOS Y ¿AHORA QUÉ?

Según vemos los logs y las alertas en Wazuh:

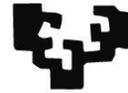
- Creamos Dashboard específicos, según servicio o alertas (opensearch)
  - Fallos de auth : top de usuarios de Ips origen, ....
  - Ataques
  - .....
- Creamos Alertas según los datos:
  - Email
  - Integración con Telegram
- Filtrado en los FWs corporativos (WebHooks):
  - Ataques VPN (ya implementada)
  - Fallos de autenticación x en 1 minuto
  - Ataques Web





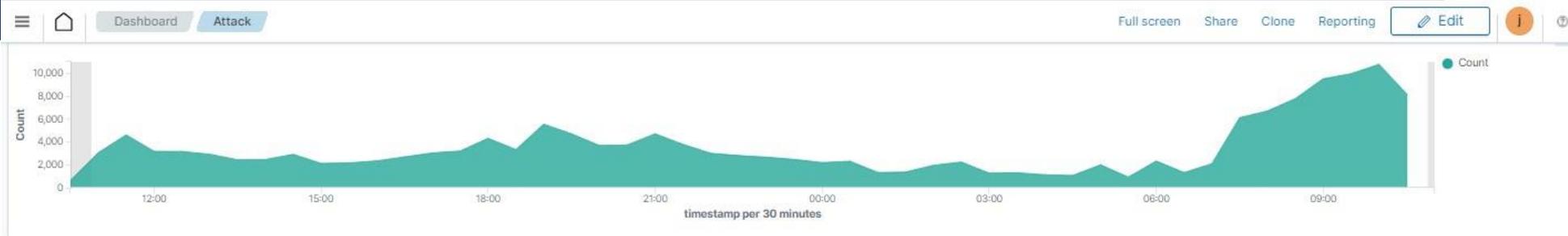
# EJEMPLOS

eman ta zabal zazu



Universidad del País Vasco

Euskal Herriko Unibertsitatea



data.scrip	Count
66.249.93.7	6,461
66.249.93.8	6,416
66.249.93.9	5,981
10.0.11.115	5,640
185.125.50.183	3,465
37.28.157.152	1,650
156.146.63.176	1,553
143.284.41.152	1,545
10.227.122.217	1,360

Rule_description	Count
Web server 400 error code.	148,412
High amount of POST requests in a s...	20,365
A web attack returned code 200 (suc...	317
Common web attack.	281
CMS (WordPress or Joomla) login att...	279
SQL injection attempt.	222
PHP internal error (missing file).	36
Multiple common web attacks from si...	23
Fortigate attack detected.	13

Agent.Name	Count
stweb72	40,257
stweb71	30,775
stweb73	22,123
fronteggiprodflw2 lgg.ehu	15,960
fronteggiprodflw1 lgg.ehu	15,048
web7desa1	5,660
web72	4,606
ad03.ehu.eus	3,751
web71	3,725

data.id	Count
404	110,736
405	22,588
200	20,792
400	7,279
403	3,738
401	2,278
410	858
416	814
409	212

Time	agent.name	data.scrip	rule.description	data.url	full_Log	data.id
May 20, 2024 @ 10:52:25.848	fronteggiprodflw1 lgg.ehu	67.16.162.8	Web server 400 error code.	/theme/image.php/ehu/assign/1715671474/icon	67.16.162.8 - [20/May/2024:10:52:25 -0200] "HEAD /theme/image.php/ehu/assign/1715671474/icon HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Linux; Android 11; SM-A505FN Build/RP1A.200720.012; wv AppleWebKit/537.36; HTML; like Gecko) Vers... 2024 Chrome/124.0.6307.123 Mobile Safari/537.36 Mozilla/5.0 (Linux; ..."	405
May 20, 2024 @ 10:52:24.792	fronteggiprodflw2 lgg.ehu	10.244.44.78	High amount of POST requests in a...	/lib/aiav/service.php?ceeskuv-&CaHnTTD...	10.244.44.78 - [20/May/2024:10:52:24 -0200] "POST /lib/aiav/service.php?ceeskuv-&CaHnTTD...info-cvva fetch notifical... 200	200

# WAZUH EN LA UPV/EHU : SIGUIENTES PASOS



## ■ Integración con terceros:

- AbuseIPDB (Implementada)
- MISP (por ahora de pruebas, con Reyes-CCN-CERT)
- Virustotal (Licencia limitada)

## Futuro (cercano???)

- Filtrado de ataques en el endpoint
- SCA (evaluación de la configuración de seguridad) ejemplo, longitudes de password,
- (Muchas más integraciones disponibles y documentadas en la web de Wazuh)
- Añadir más hosts (servidores departamentales, laboratorios, etc etc...)

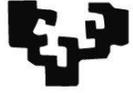
# CONCLUSIONES



- PROS:
  - Fácil de implantar
  - Escalable
  - Comunidad viva con integraciones nuevas, reglas y decodificadores
  - Cambios de configuración en los agentes desde el Dashboard (ejemplo, directorio a monitorizar)
  - GRATIS... x ahora 😊
- CONTRAS:
  - Algo dura la configuración de reglas y decodificadores (ficheros, pero mediante de la GUI)
    - No todos los decodificadores llaman igual a los campos: ip, ip\_address,... (Pero se puede solucionar sin tocar los decodificadores THANKS COMUNIDAD)
  - Consume recursos HW (sobre todo disco, dependerá de lo que almacenes y periodo de retención)
  - Se necesitan manos de seguridad para ir implementado nuevas acciones,... INTEGRACIONES



eman ta zabal zazu



Universidad  
del País Vasco

Euskal Herriko  
Unibertsitatea

