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

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?
  - .....

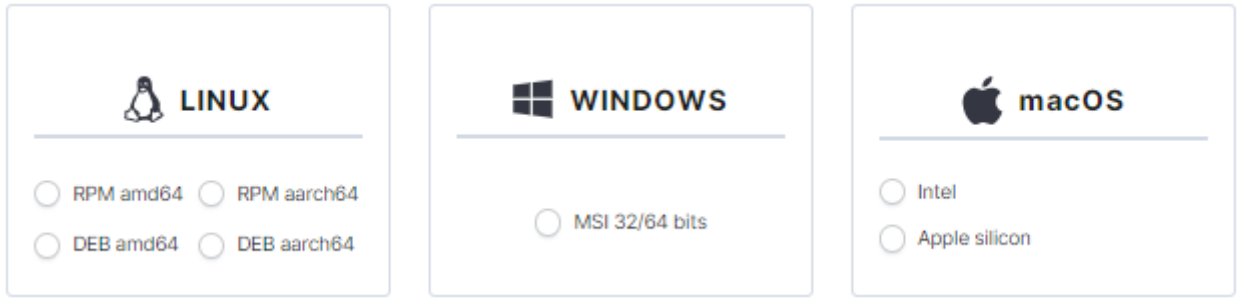
HERRAMIENTA SELECCIONADA

Universidad del País Vasco · Euskal Herriko Unibertsitatea

wazuh.
The Open Source Security Platform

Razones:

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



WAZUH

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

¿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)

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

- 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...

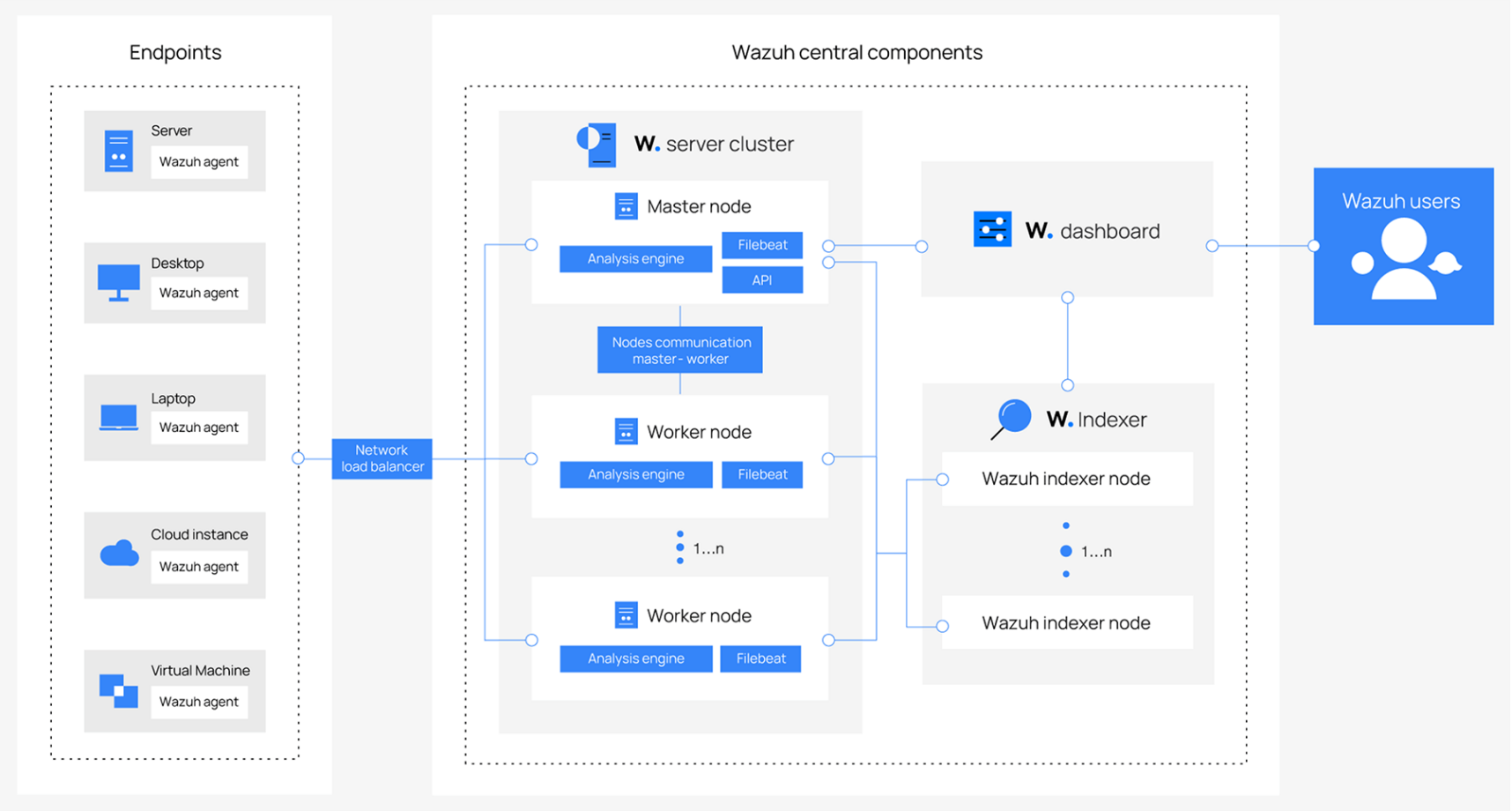
  (Conclusión)→Necesidad de herramienta para estas instalaciones ....

- 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)

Universidad del País Vasco — Euskal Herriko Unibertsitatea

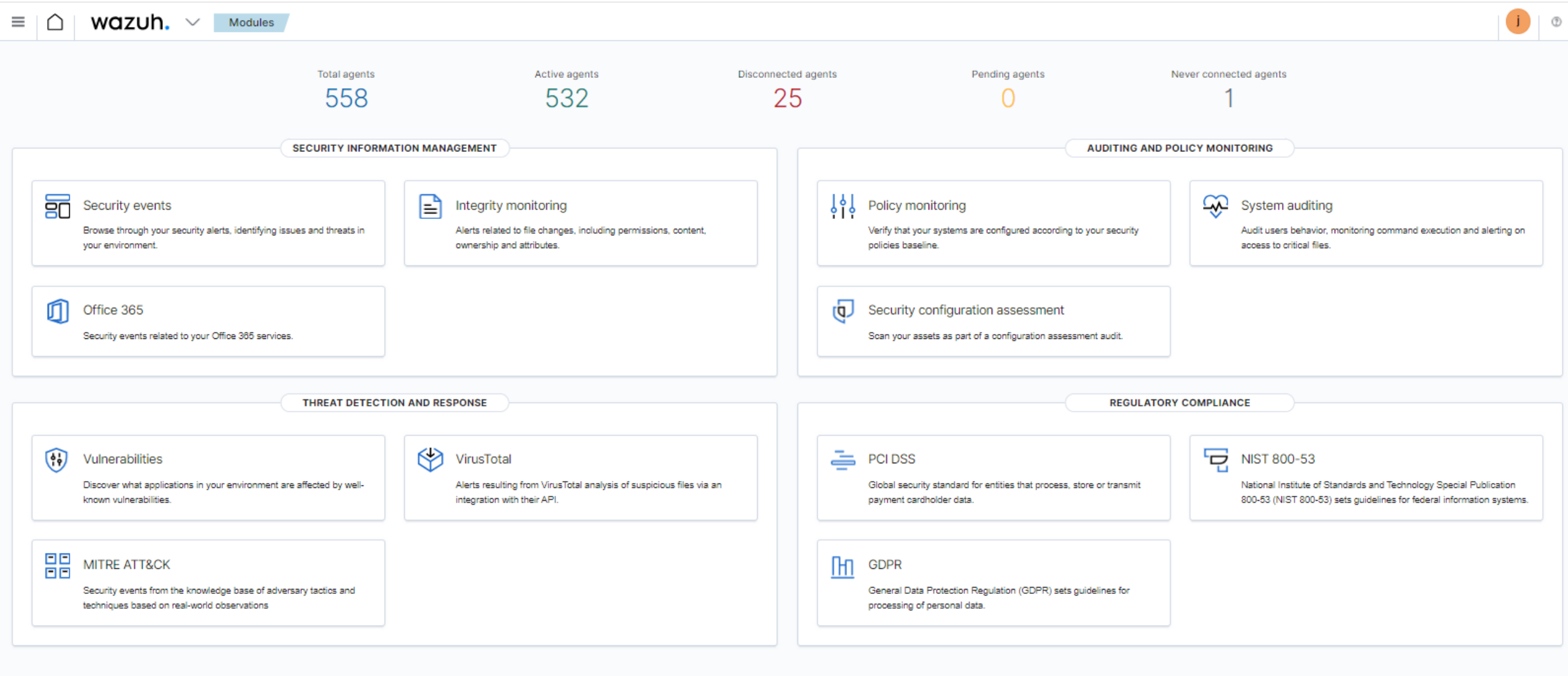


1 Servidor de Dashboard
4 Servidores de Master/Worker
4 Servidores de Indexer

WAZUH EN LA UPV/EHU
¿QUÉ ESTAMOS MONITORIZANDO?

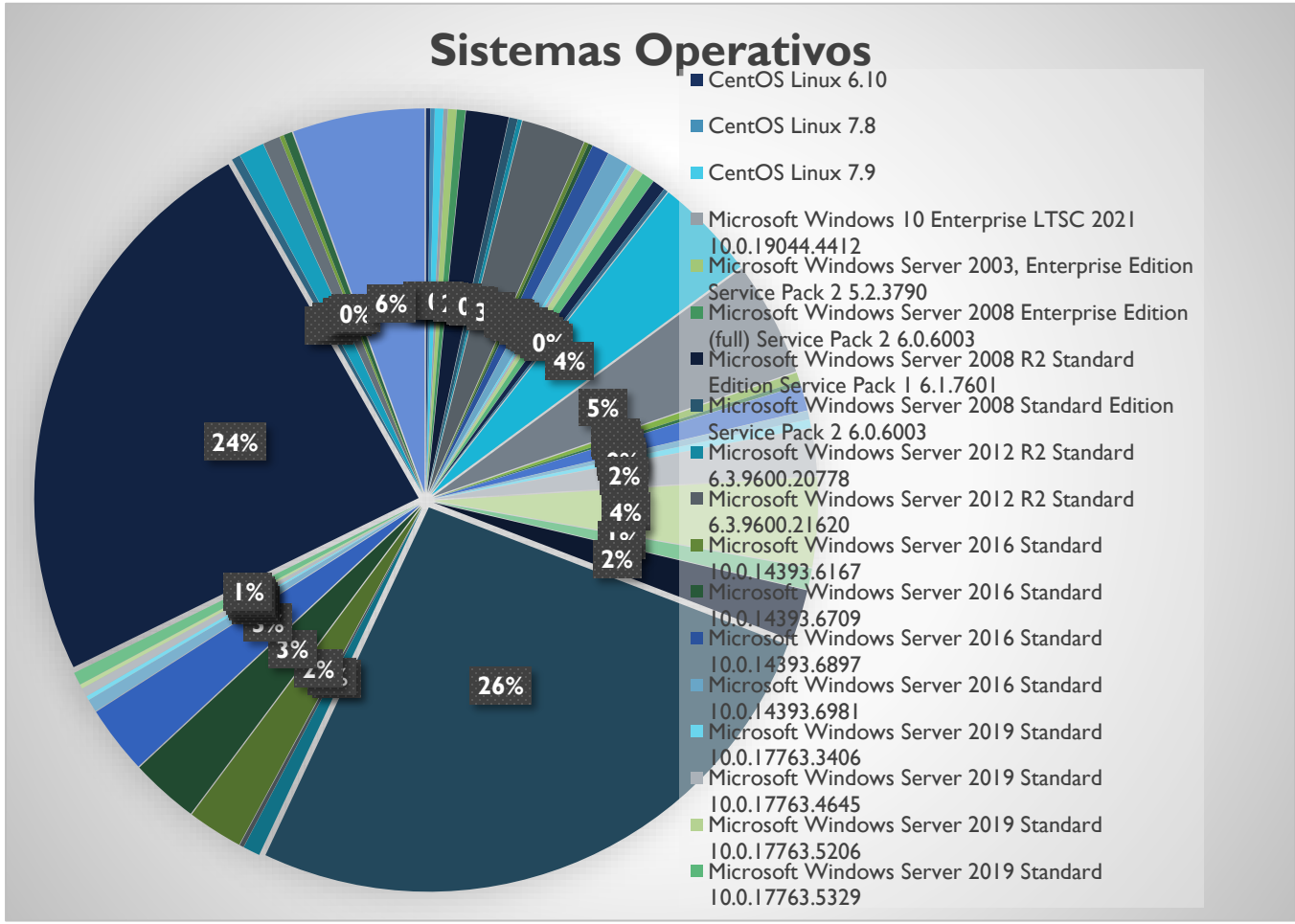
eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

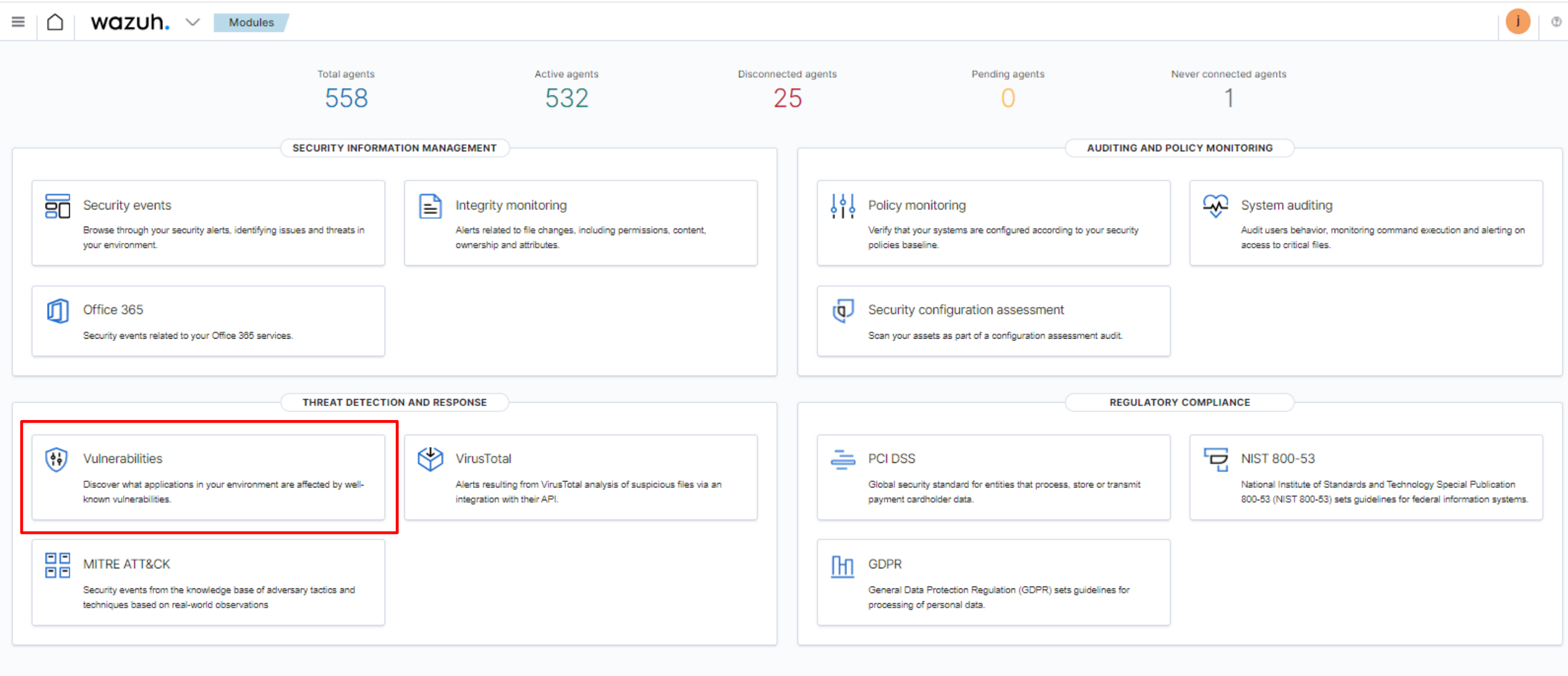
- 558 Servidores con agente (servidores Web, BD, etc)
- M365
- Cisco Umbrella y DNSs internos
- Fw Perimetral
- Antivirus (Apex-One)
- VPNs (Cisco ASA y Forti)
- Logs de Aruba (WiFi)
- .....

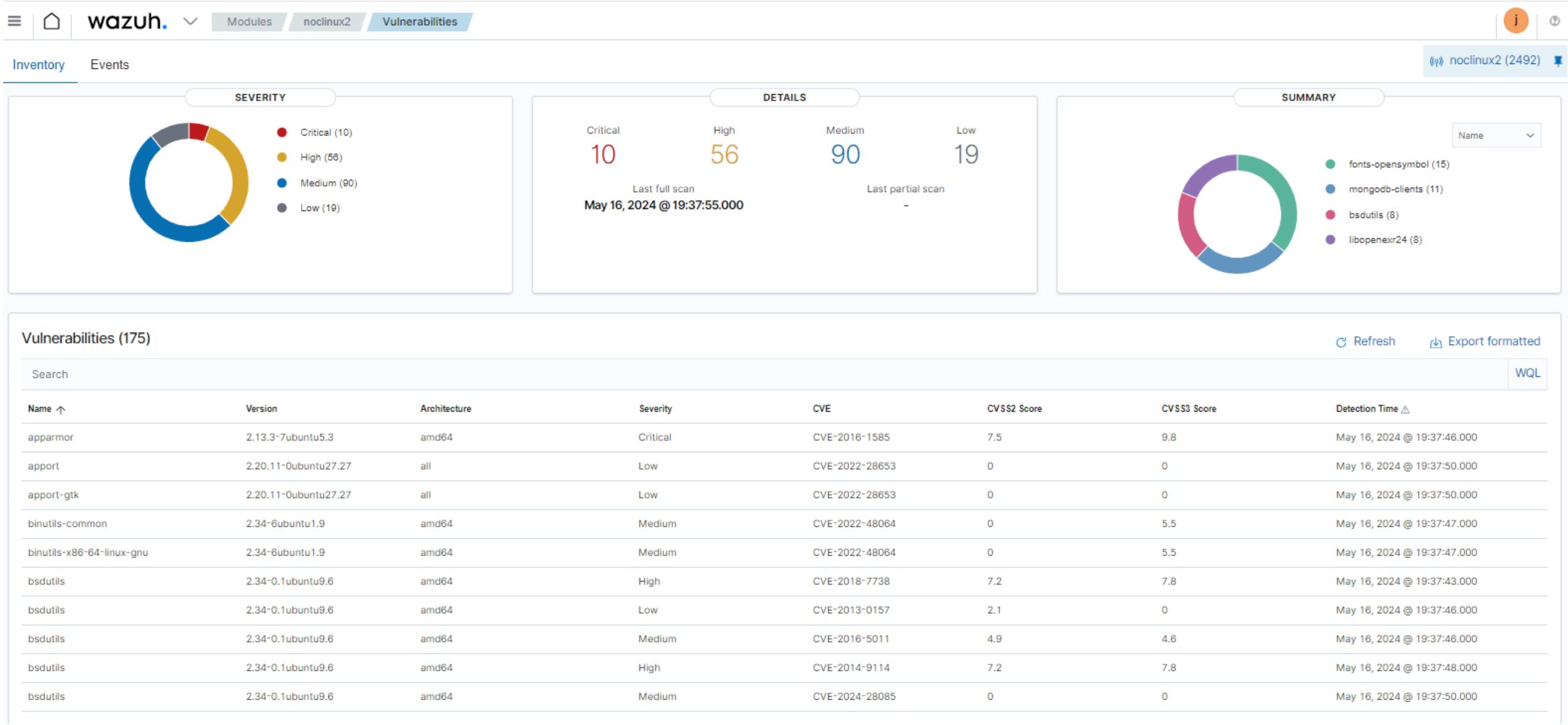

wazuh.
Modules
j
Total agents
558
Active agents
532
Disconnected agents
25
Pending agents
0
Never connected agents
1
SECURITY INFORMATION MANAGEMENT
Security events
Browse through your security alerts, identifying issues and threats in your environment.
Integrity monitoring
Alerts related to file changes, 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: PRIMEROS DATOS

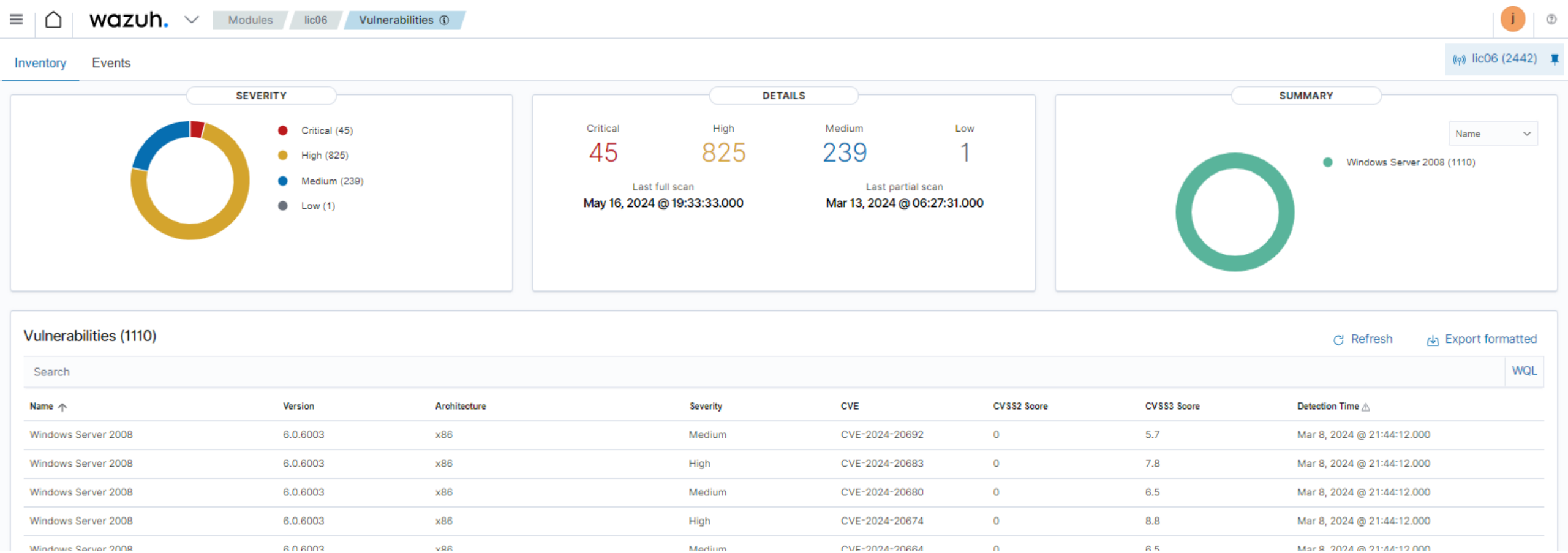
- Visibilidad de Versiones de SOs.
  - Algunos muy obsoletos
- Equipos sin actualizar.
- Equipos actualizados, pero con “Falsa” creencia de seguridad.
- Visibilidad de los LOGs de los propios Servidores de forma centralizada y catalogada.



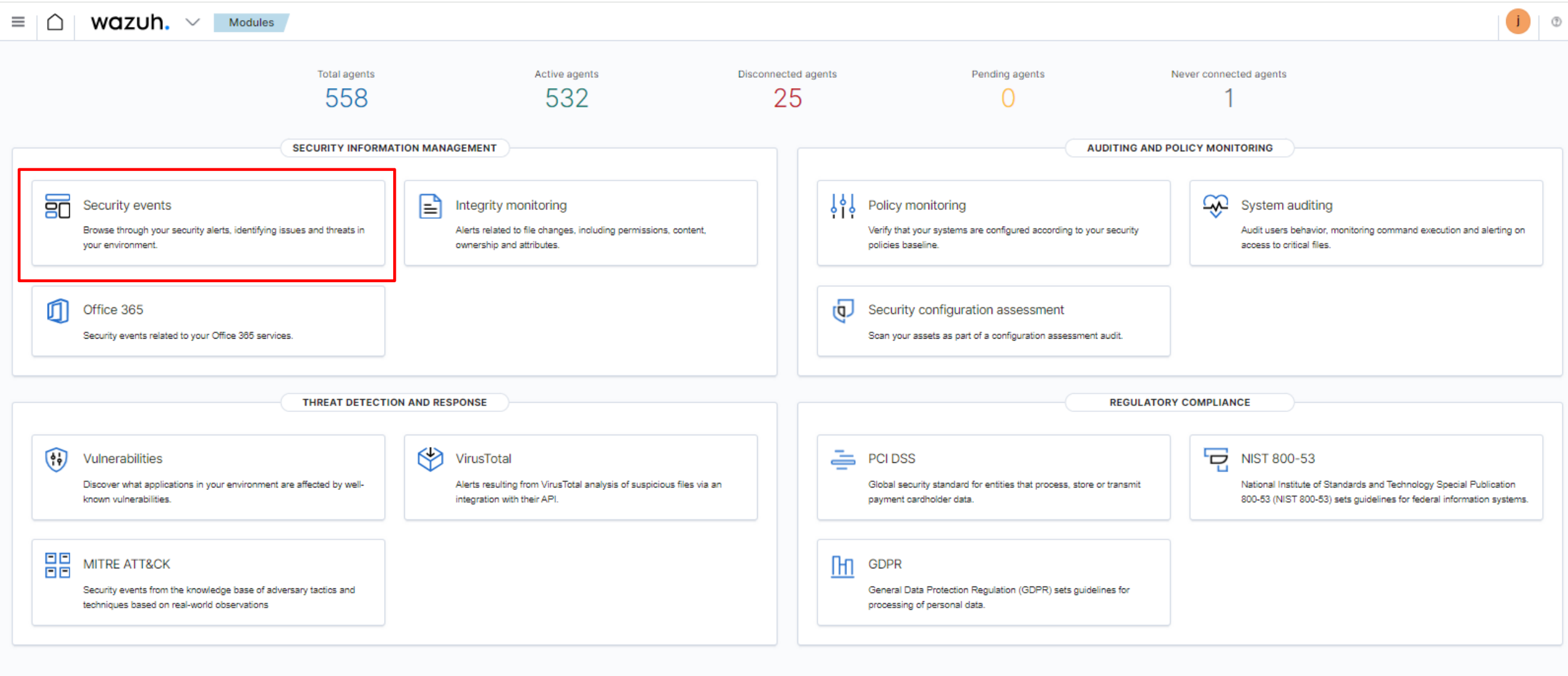

wazuh.
Modules
Total agents
558
Active agents
532
Disconnected agents
25
Pending agents
0
Never connected agents
1
SECURITY INFORMATION MANAGEMENT
Security events
Browse through your security alerts, identifying issues and threats in your environment.
Integrity monitoring
Alerts related to file changes, 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.



Ubuntu 20.04.1 actualizado pero con vulnerabilidades



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


wazuh.
Modules
j
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

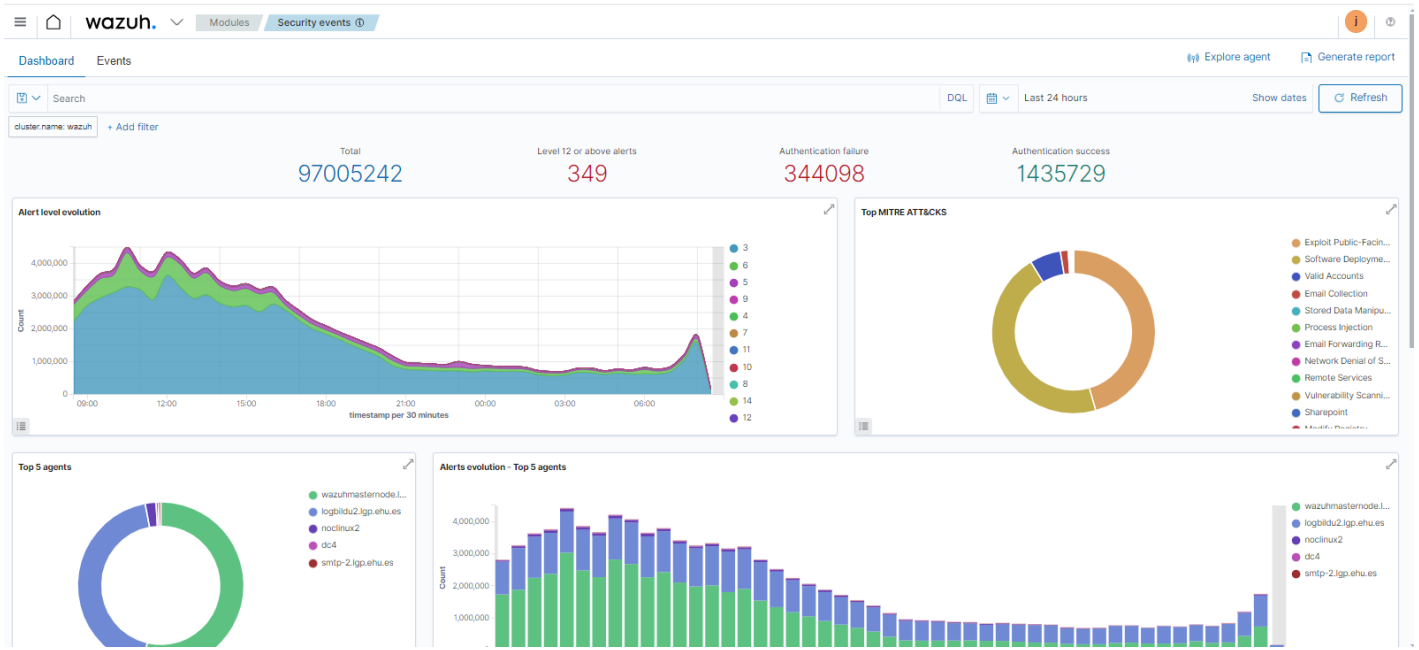
eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

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

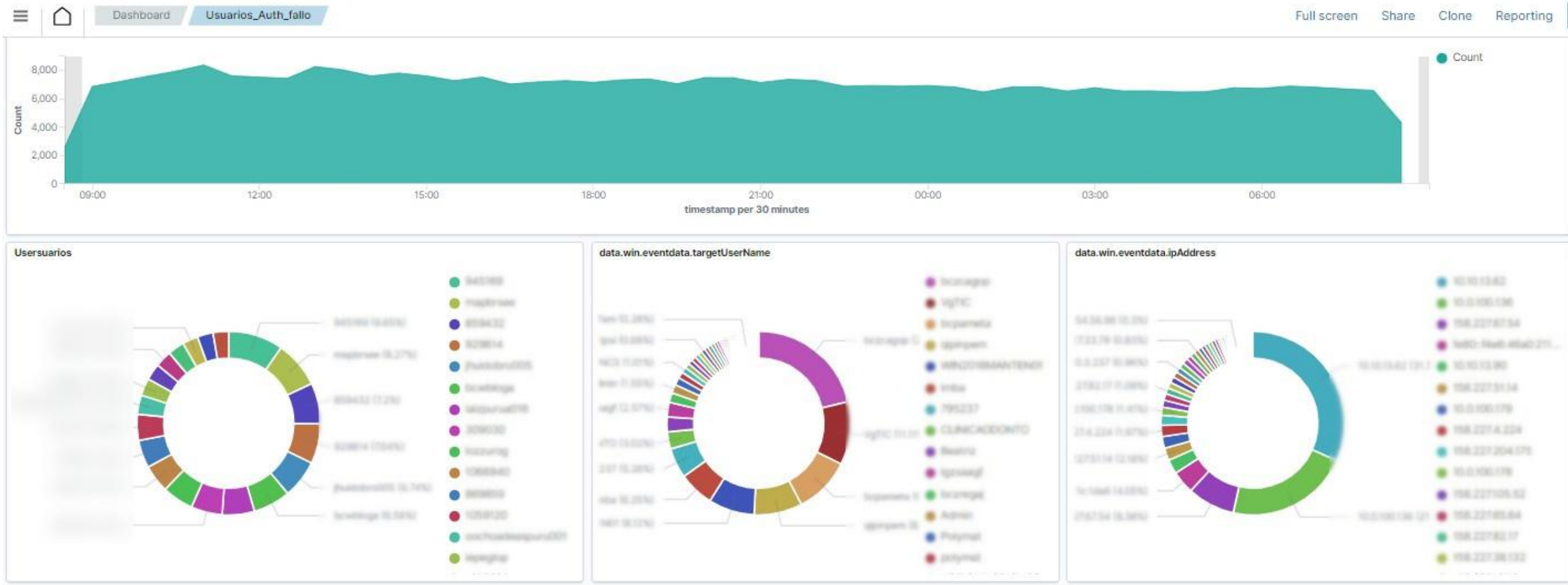
eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

Según vemos los logs y las alertas en Wazuh:

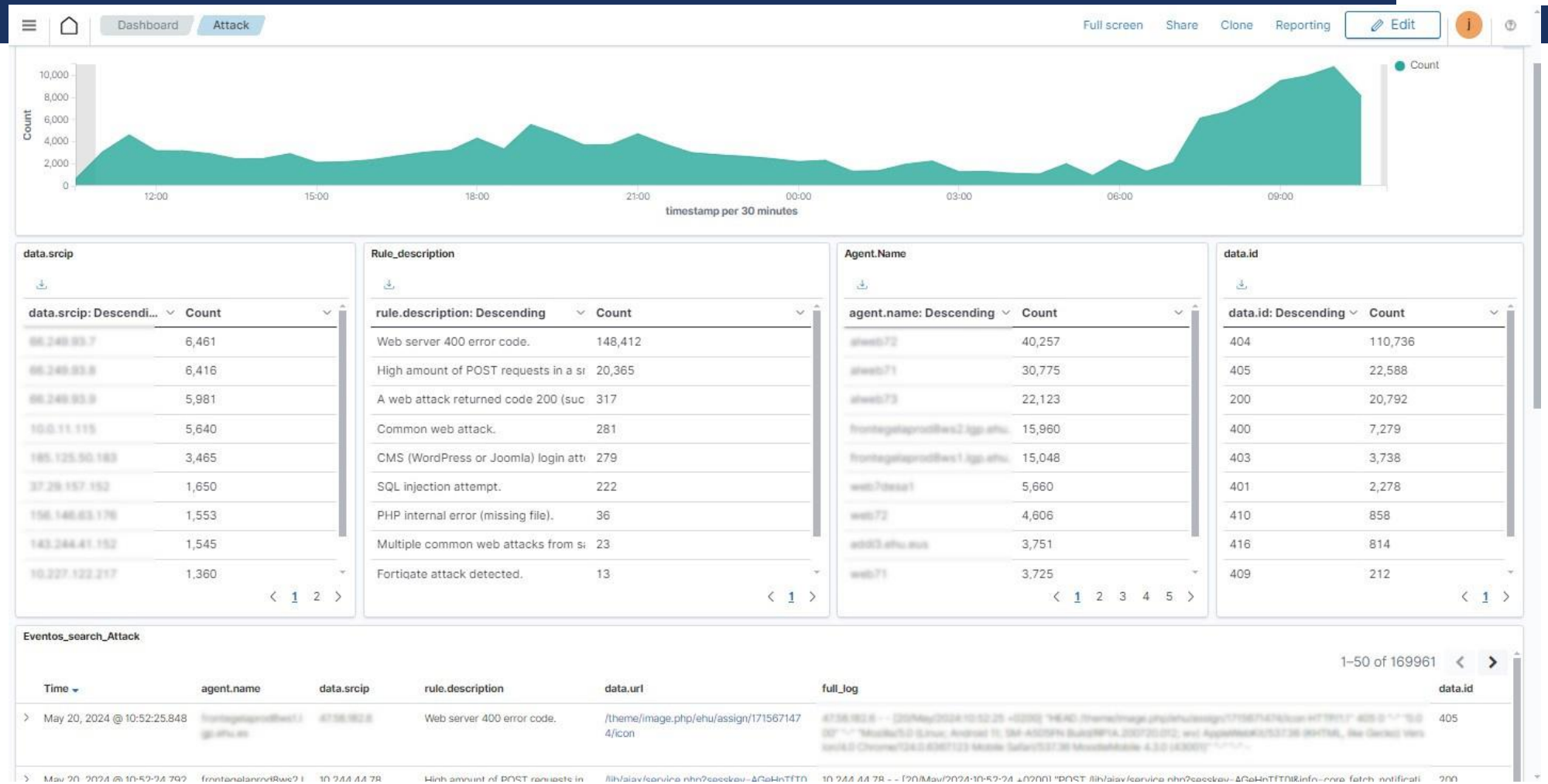
- Creamos Dashboard específicos, según servicio o alertas (opensearch)
  - Fallos de auth : top de usuarios de Ips origen, ...
  - Ataques
  - .....
- Creamos Alertas según los datos:
  - Email
  - Integración con Telegram
- Filtrado en los FWs corporativos (WebHooks):
  - Ataques VPN (ya implementada)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



EJEMPLOS


Dashboard
Usuarios_Auth_fallo
Full screen
Share
Clone
Reporting
Count
8,000
6,000
4,000
2,000
0
09:00
12:00
15:00
18:00
21:00
00:00
03:00
06:00
timestamp per 30 minutes
Usersuarios
data.win.eventdata.targetUserName
data.win.eventdata.ipAddress

EJEMPLOS


Dashboard
Attack
Full screen
Share
Clone
Reporting
Edit
Count
timestamp per 30 minutes
data.srcip
Rule_description
Agent.Name
data.id
Eventos_search_Attack
1–50 of 169961

WAZUH EN LA UPV/EHU : SIGUIENTES PASOS

Universidad del País Vasco · Euskal Herriko Unibertsitatea

- 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

Universidad del País Vasco — Euskal Herriko Unibertsitatea

- 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