XIX JORNADAS REDIMADRID 2024

Martes, 15 de octubre de 2024

EducaMadrid

Servicio de Plataformas Educativas
Subdirección General de Transformación Educativa
Dirección General de Estrategia Digital Consejería de Digitalización

Equipo técnico de implantación

wazuh.
Overview

Adolfo Sanz de Diego

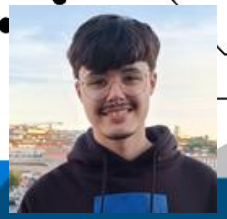
Jefe de Servicio en EducaMadrid.

Sergio Lobo del Olmo

Coordinador de Ciberseguridad en EducaMadrid.

David Navarro Iborra

Consultor de Ciberseguridad en EducaMadrid.



Rubén García-Rosell Gallego

Técnico de Sistemas (Wazuh) en EducaMadrid.

XDR Y SIEM

Wazuh es una plataforma gratuita de código abierto, (Opensource) que se utiliza para la prevención, detección y respuesta a amenazas. Básicamente consta de 3 componentes:

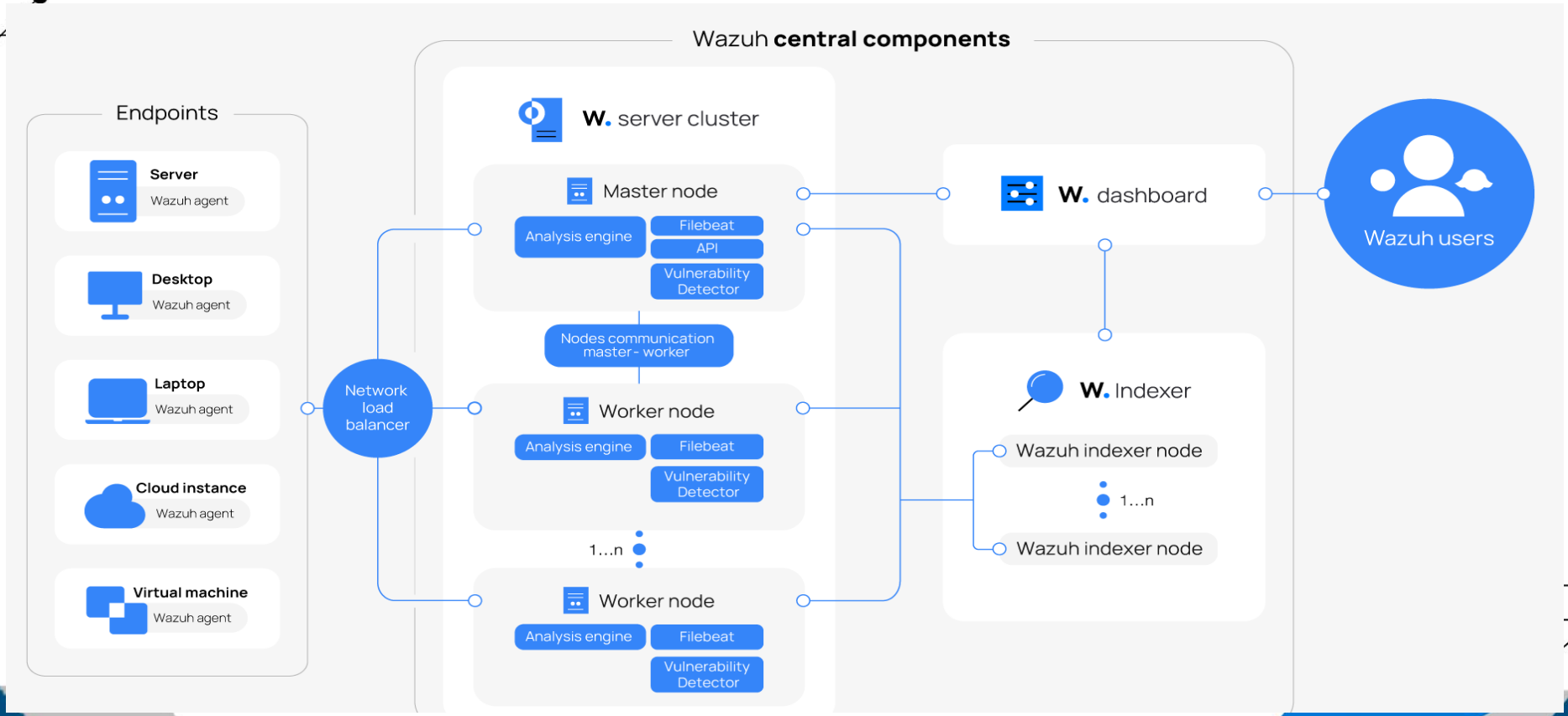
OSSEC HIDS: Sistema de detección de intrusos(HIDS) que es usado para la detección, visibilidad y monitorización del cumplimiento de eventos de seguridad.

OpenSCAP: Intérprete que se usa para chequear configuraciones del sistema y detectar aplicaciones vulnerables. Herramienta diseñada para cumplimiento de seguridad y el bastionado de sistemas empresariales o corporativos.

Elastic Stack: Software (Elasticsearch, Kibana y Filebeat) usado para recolectar, comparar, almacenar, indexar, buscar y mostrar datos de logs. Proporciona interfaz web para mostrar los datos a través de dashboard.

Lo explicaremos mas en profundidad a continuación….

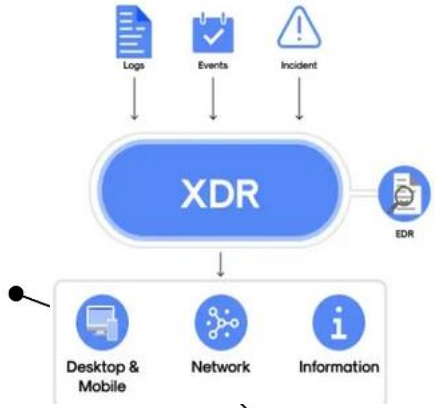
Estructura de Wazuh



Funciones implementadas

SIEM (Security Information and Event Management)
Es una tecnología que recopila, analiza y correlaciona datos de diferentes fuentes en tiempo real para identificar y responder a amenazas de seguridad. Las fuentes pueden ser registros (logs) de sistemas, aplicaciones o dispositivos de Red o finales. Utiliza técnicas de correlación y análisis para identificar patrones de comportamiento malicioso y así generar alertas cuando se detecten estas actividades sospechosas. Incorpora también funciones de generación de informes, así como formas gráficas de representación visual.

XDR (Extended Detection and Response)
Va más allá, puesto que amplía su alcance, llegando a una gama más amplia de dispositivos y/o servicios (fuentes).Además, no solo tiene un papel pasivo de detección, sino que también dispone de la capacidad de respuesta activa automatizada, que permite actuar en caso de detectar comportamientos maliciosos. Wazuh incorpora, pues, toda una serie de características y funcionalidades que le permiten trabajar como SIEM y XDR



Infraestructura implementada

Desde EducaMadrid hemos optado por tener la infraestructura del CPD principal de este modo:

•Un balanceador de carga nginx, que actué como intermediario entre las máquinas con Wazuh Manager y los servidores con agentes.

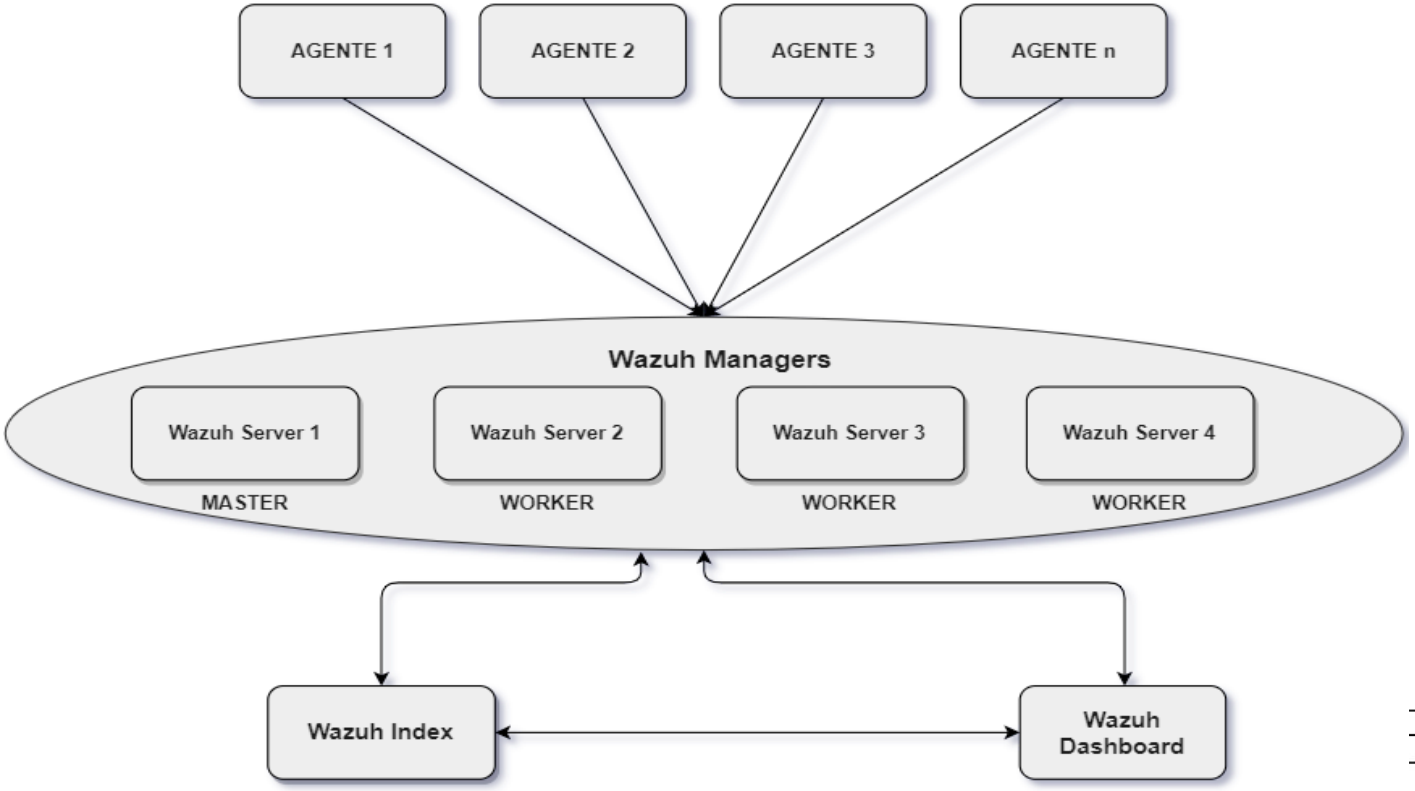
•3 servidores en los que se instalara Wazuh Manager. Estos 3 servidores recibirán los datos y las peticiones de los agentes desde el balanceador de carga.

•2 servidores con Wazuh Indexer instalado. Cada uno con 100G en la partición /var para guardar los índices que crea Wazuh.

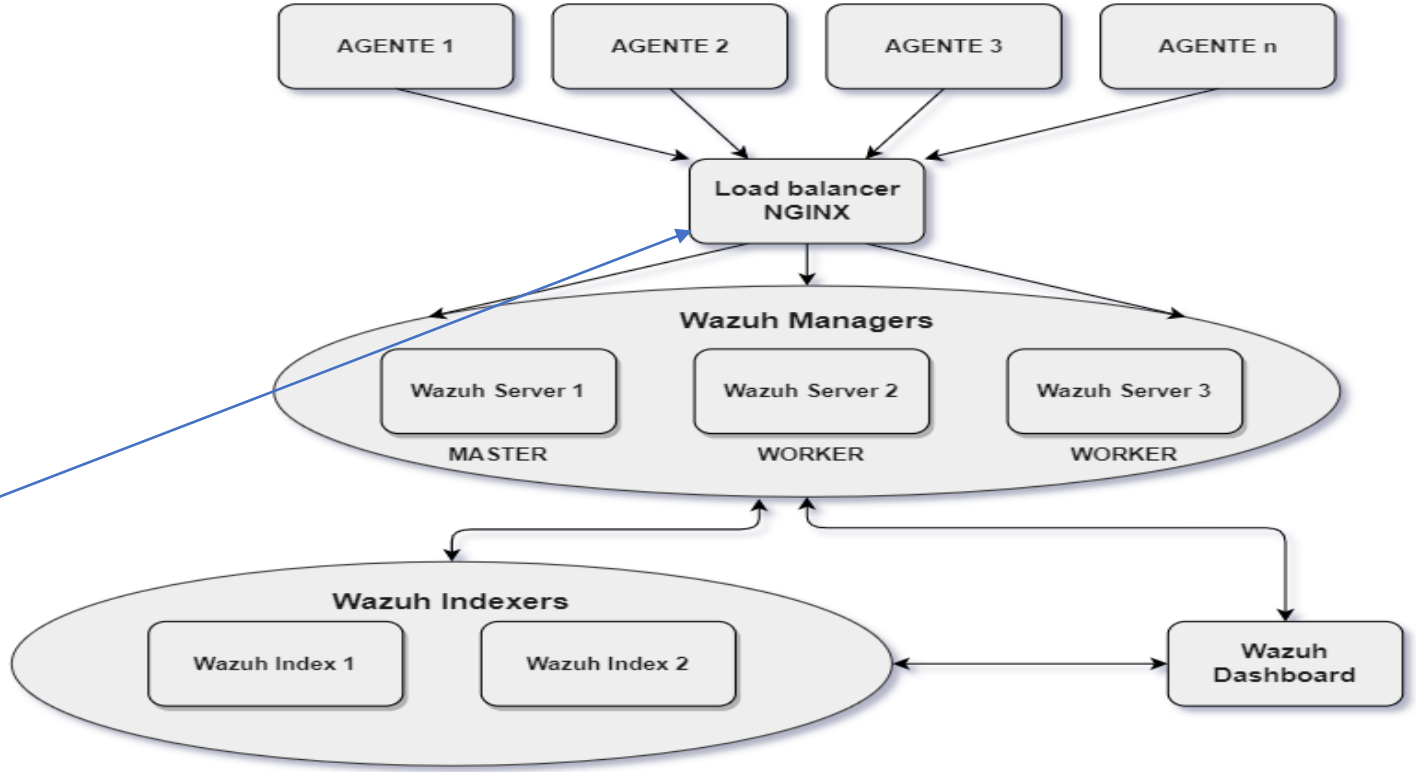
•1 servidor con Wazuh Dashboard instalado.

•Especificaciones --> 8GB RAM/8 Cores y entre 500 y 100 GB de almacenamiento en /var

Infraestructura CPD 1



Infraestructura CPD 2



Algunas lecciones aprendidas

Funcionalidades y capacidades

SCA (Security Configuration Assessment):

Wazuh supervisa la configuración del sistema y de las aplicaciones para garantizar el cumplimiento de las normas y políticas de seguridad. Los agentes de Wazuh realizan escaneos periódicos para detectar errores de configuración o agujeros de seguridad en los dispositivos finales que podrían ser explotados por actores maliciosos. Estos controles de configuración pueden configurarse para adaptarlos a las necesidades de la organización.

Detección de malware:

Wazuh detecta la actividad maliciosa y genera IOC,s (indicadores de compromiso) que se producen en los dispositivos finales como resultado de infecciones de malware o ciberataques.

FIM (File Integrity Monitoring):

Wazuh monitoriza el sistema de carpetas, identificando cambios en el contenido, permisos, propiedad y atributos de los archivos a monitorizar.

Funcionalidades y capacidades

Threat detection (Detección de amenazas) / Inteligencia de amenazas (Threat intelligence):

Wazuh ofrece una visibilidad completa de los dispositivos finales y de la infraestructura supervisada. Dispone de funciones de conservación de registros, indexación y consulta que ayudan a investigar amenazas que pueden haber eludido los controles de seguridad iniciales.

Log Data Analysis:

Los agentes de Wazuh recopilan registros del sistema operativo y las aplicaciones y los envían de forma segura al servidor de Wazuh para su análisis y asignación basados en reglas. Sysmon.
Análisis de registro de dispositivos, syslog, sensores IDS, FW (por syslog). Registro herramientas terceros (Maltrail), Office365, MISP…

Detección de vulnerabilidades:

Los agentes de Wazuh recogen los datos del inventario del programa y envían esta información al servidor de Wazuh. Los datos de inventario recopilados se correlacionan con bases de datos CVE actualizadas continuamente para identificar software vulnerable conocido. (NIST)

Funcionalidades y capacidades

Respuesta a incidentes: Wazuh tiene respuestas activas predefinidas para llevar a cabo diversas contramedidas contra las amenazas en curso.

Cumplimiento normativo: Wazuh ofrece algunos de los controles de seguridad necesarios para el cumplimiento de las normas y reglamentos del sector, como GDPR, NIST, TSC e HIPAA, que también se logran a través de las funciones SCA (Software Composition Analysis) y FIM (File Integrity Monitoring)

Higiene de TI: Wazuh construye un inventario actualizado del sistema de todos los dispositivos finales monitorizados. Este inventario ayuda a las organizaciones a optimizar la visibilidad de los activos y a mantener una buena higiene informática.

Integración de terceros : Contenedores (Docker) / Nube.

Análisis del comportamiento: Qué está haciendo en cada momento el usuario, procesos, archivos de trabajo, aplicaciones, inicios de sesión / bloqueos, errores logon, etc

Síntesis de servicios

Análisis de seguridad: Wazuh es utilizado para recolectar, agregar, indexar y analizar información de seguridad, ayudando a las organizaciones a detectar intrusos, amenazas y anomalías de comportamiento.

Detección de intrusos: Los agentes de Wazuh monitorizan los sistemas buscando malware, rootkits y anomalías sospechosas. Puede detectar archivos ocultos, procesos ocultos, listeners de red no registrados o inconsistencias en respuestas de llamadas al sistema. Además, el servidor usa un enfoque basadoen firmas para la detección usando un motor de expresiones regulares para analizar la información de los logs recolectados.

Análisis de logs: Los agentes de Wazuh leen el S.O y los logs de las aplicaciones, y los envían de manera segura al administrador central para ser analizados y almacenados. Las reglas de Wazuh ayudan a mantener la consistencia frente a errores de aplicación, sistemas, malas configuraciones, intentos de actividades maliciosas, violación de políticas de operación y otros referidos a la seguridad.

Monitorización de la integridad de los Archivos: Wazuh monitorea el sistema de archivos, identificando cambios en el contenido, permisos, propiedad, y los atributos que necesitas mantener bajo control.

Detección de vulnerabilidades: Los agentes de Wazuh envían información referida al servidor, donde es correlacionada con la base de datos de actualizaciones continuas de CVE (Common Vulnerabilities and Exposure), para identificar las vulnerabilidades de software conocidas.

Síntesis de servicios

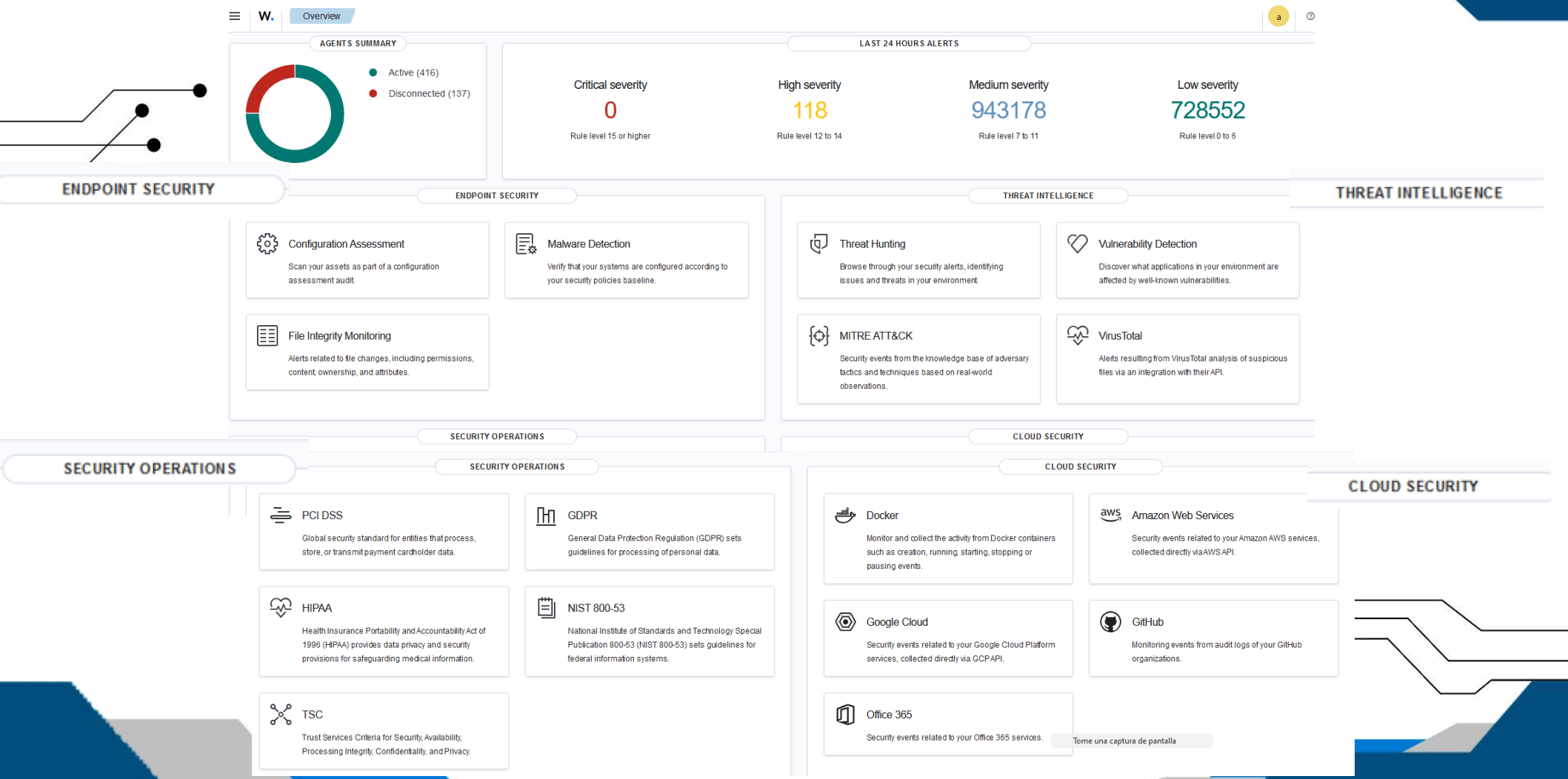
Configuración de Evaluación de sistema: Wazuh monitorea los ajustes de configuración y las aplicaciones para asegurar que se alinean con las políticas de seguridad. Los agentes actúan escaneando periódicamente para detectar aplicaciones que son conocidas como vulnerables, no parcheadas o configuradas inseguramente. Adicionalmente, la configuración puede ser personalizada, adaptándose para ser alineadas con las propiedades de la institución u organización. Las alertas incluyen recomendaciones para mejorar la configuración, referencias y mapeo con cumplimiento normativo.

Respuesta ante incidentes: Wazuh provee respuestas activas «out-of-the-box» para accionar varias contramedidas para la dirección de amenazas activas, como bloquear acceso al sistema para las fuentes de amenazas cuando cumpla ciertos criterios. Aparte, Wazuh permite introducir comandos remotamente o solicitudes del sistema, identificando (IOCs) y ayudando a realizar otras tareas forenses o tareas automatizadas en respuestas a incidentes

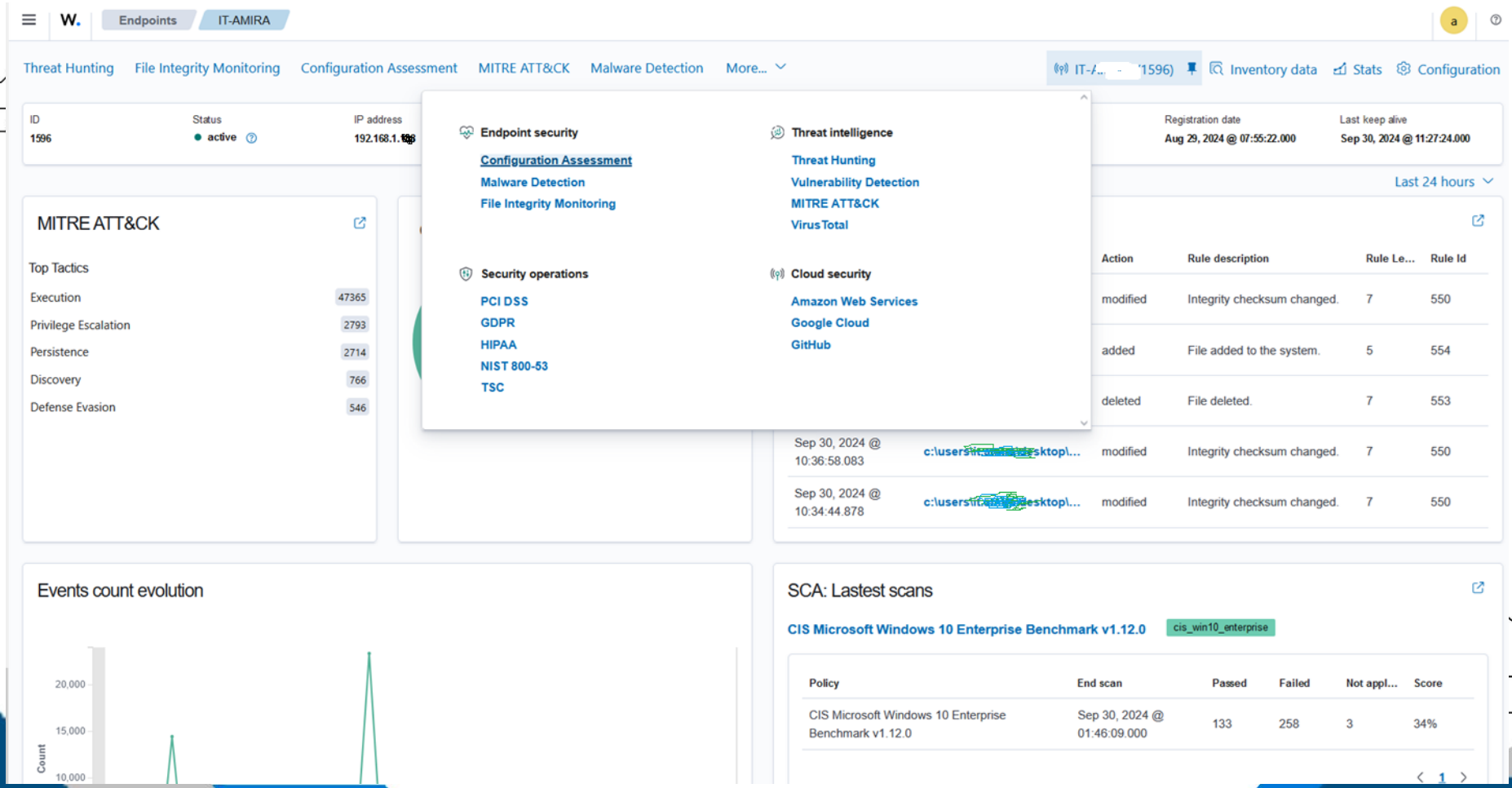
Cumplimiento Normativo: Wazuh provee algunos de los controles de seguridad necesarios para cumplir con los estándares y regulaciones de la industria. Estas características combinadas con su escalabilidad y soporte multiplataforma ayuda a las organizaciones al cumplimiento técnico de los requerimientos.

Seguridad en la nube/ Contenedores : Wazuh ayuda a monitorear infraestructuras en la nube a nivel API, usando integración de módulos que capaces de enviar datos de manera segura desde proveedores como Amazon AWS, Azure o Google Cloud o para contenedores tipo Docker, Wazuh provee seguridad en los host y monitoriza su comportamiento y detecta amenazas y anomalías. El agente Wazuh tiene integración nativa con el motor de Docker permitiendo a los usuarios monitorizar las imágenes, volúmenes,modo configuraciones de red, y contenedores corriendo.

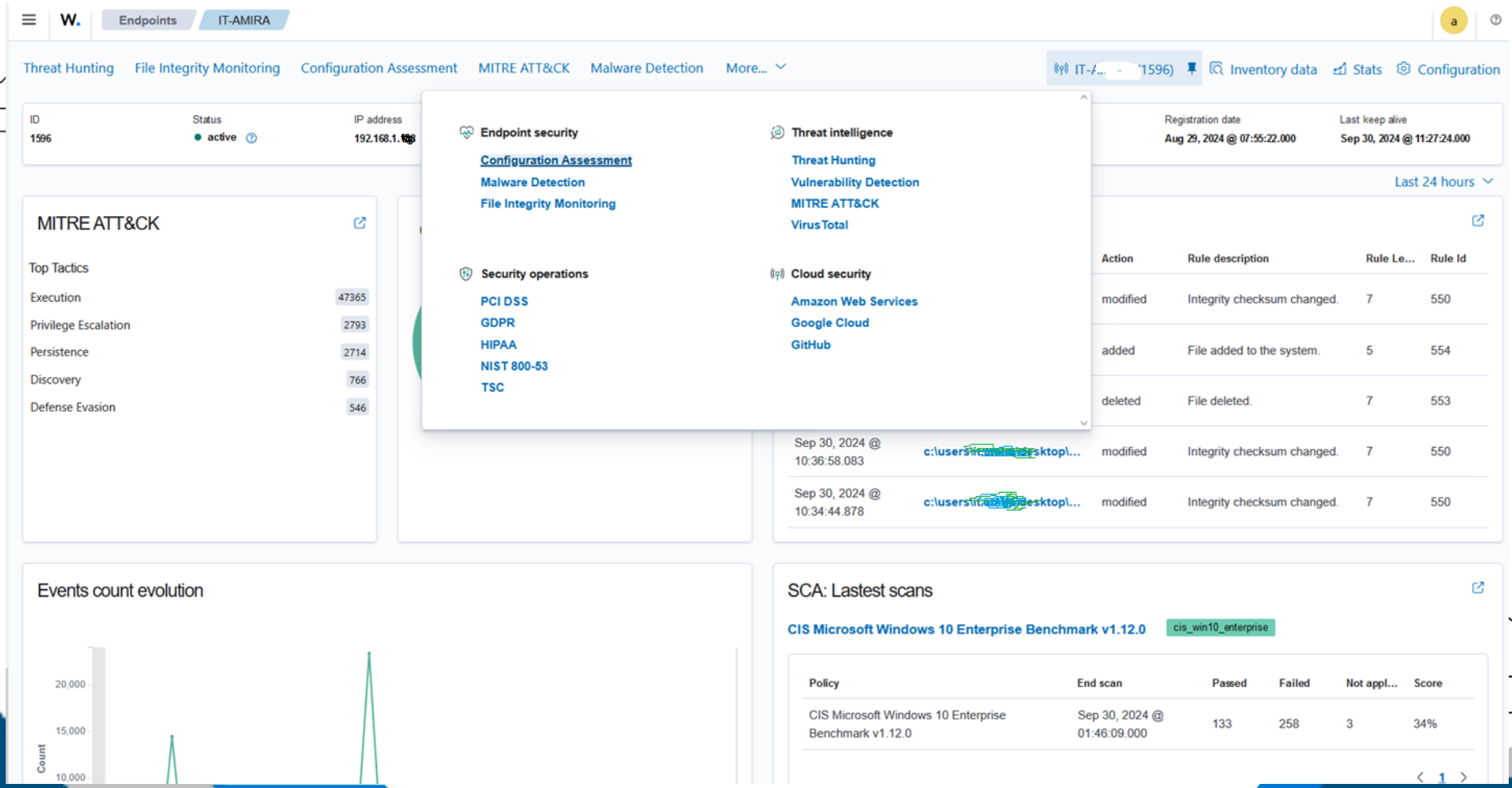
Panel Central



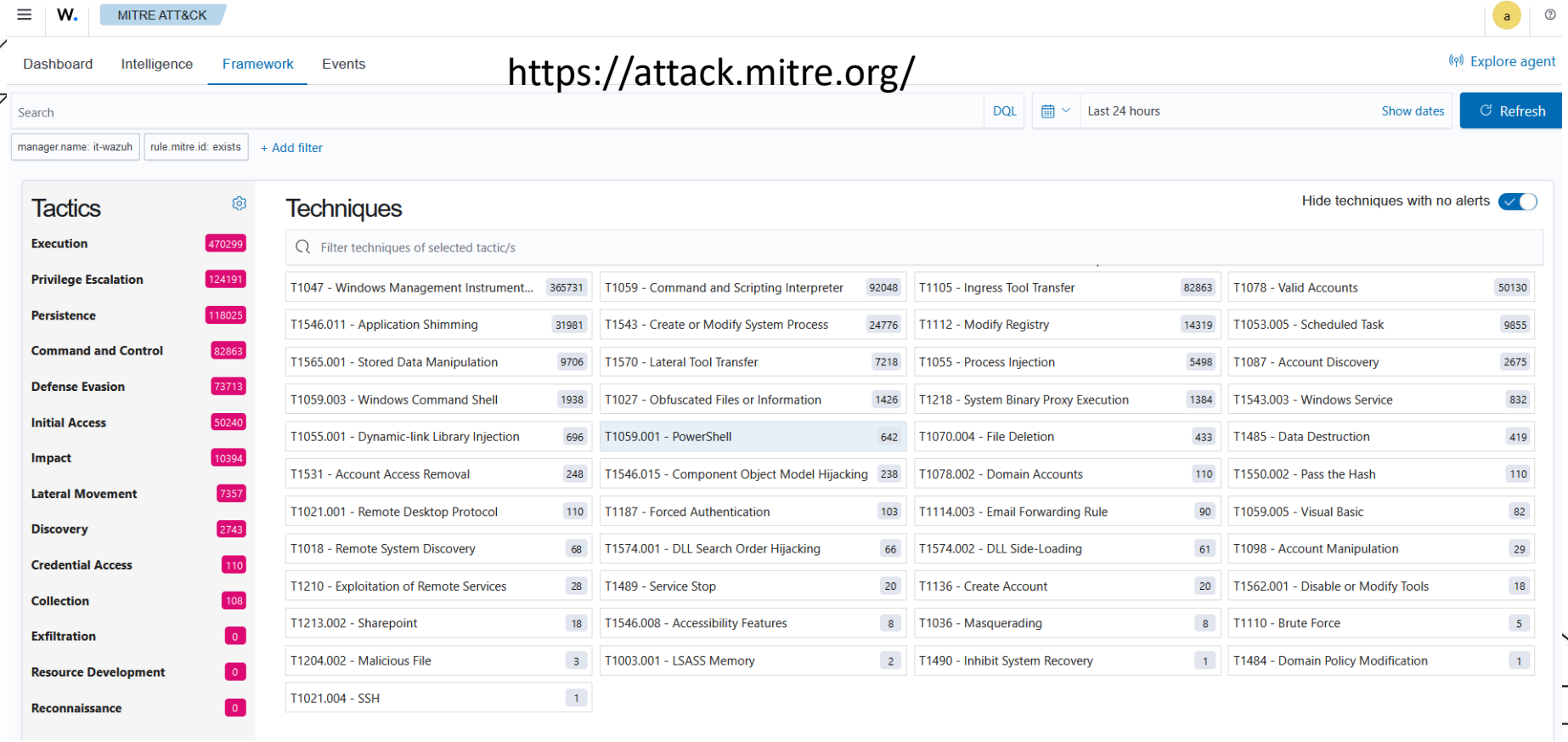
Subpaneles


Endpoints
IT-AMIRA
Threat Hunting
File Integrity Monitoring
Configuration Assessment
MITRE ATT&CK
Malware Detection
More...
Inventory data
Stats
Configuration
ID
1596
Status
active
IP address
Registration date
Aug 29, 2024 @ 07:55:22.000
Last keep alive
Sep 30, 2024 @ 11:27:24.000
Endpoint security
Configuration Assessment
Malware Detection
File Integrity Monitoring
Threat intelligence
Threat Hunting
Vulnerability Detection
MITRE ATT&CK
VirusTotal
Security operations
PCI DSS
GDPR
HIPAA
NIST 800-53
TSC
Cloud security
Amazon Web Services
Google Cloud
GitHub
Last 24 hours
MITRE ATT&CK
Top Tactics
Execution 47365
Privilege Escalation 2793
Persistence 2714
Discovery 766
Defense Evasion 546
Action
Rule description
Rule Le...
Rule Id
modified
Integrity checksum changed.
7
550
added
File added to the system.
5
554
deleted
File deleted.
7
553
Sep 30, 2024 @ 10:36:58.083
modified
Integrity checksum changed.
7
550
Sep 30, 2024 @ 10:34:44.878
modified
Integrity checksum changed.
7
550
Events count evolution
20,000
15,000
10,000
Count
SCA: Lastest scans
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0
cis_win10_enterprise
Policy
End scan
Passed
Failed
Not appl...
Score
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0
Sep 30, 2024 @ 01:46:09.000
133
258
3
34%

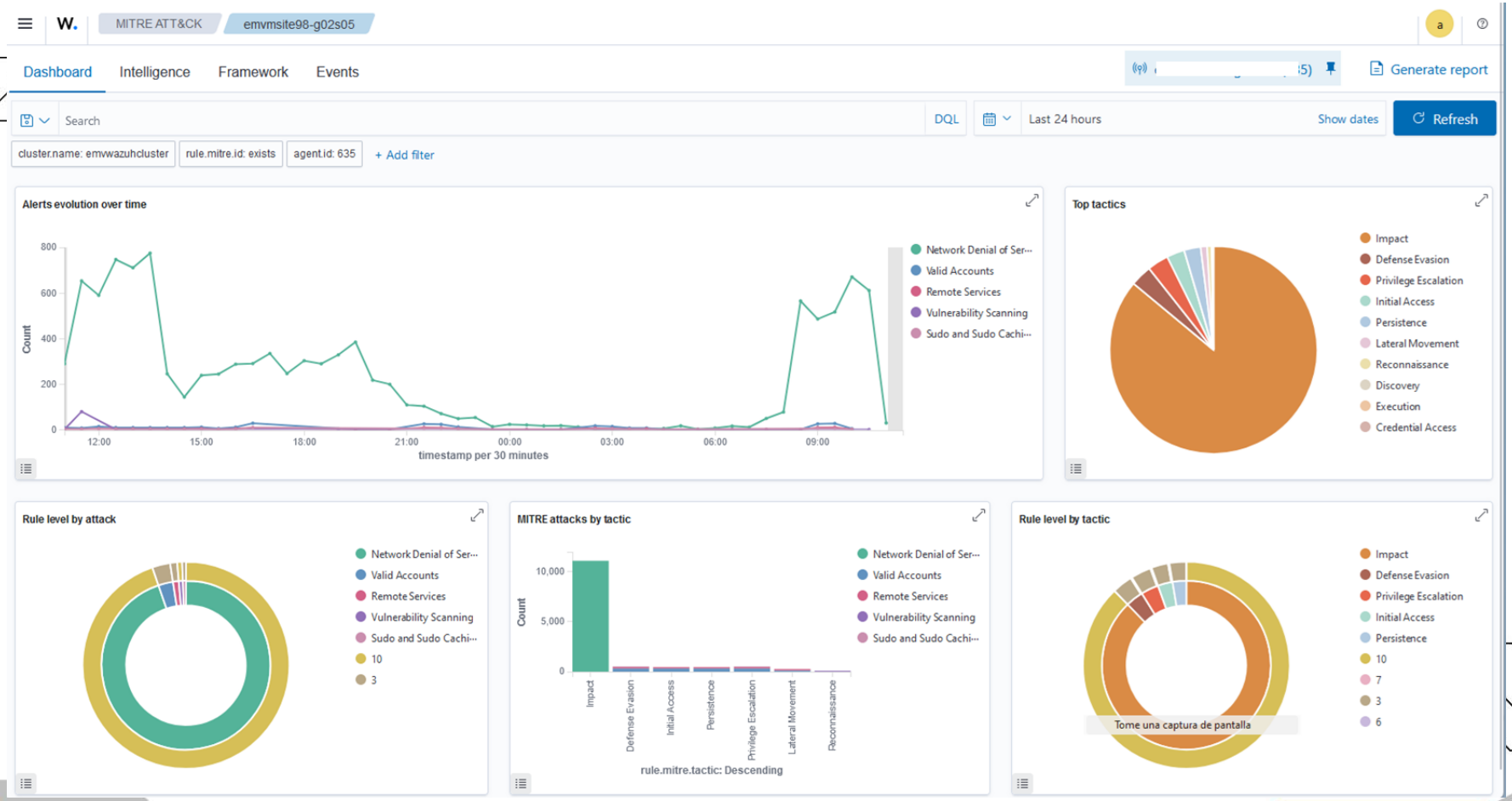
Subpaneles


Endpoints
IT-AMIRA
Threat Hunting
File Integrity Monitoring
Configuration Assessment
MITRE ATT&CK
Malware Detection
More...
Inventory data
Stats
Configuration
ID
1596
Status
active
IP address
Registration date
Aug 29, 2024 @ 07:55:22.000
Last keep alive
Sep 30, 2024 @ 11:27:24.000
Endpoint security
Configuration Assessment
Malware Detection
File Integrity Monitoring
Threat intelligence
Threat Hunting
Vulnerability Detection
MITRE ATT&CK
VirusTotal
Security operations
PCI DSS
GDPR
HIPAA
NIST 800-53
TSC
Cloud security
Amazon Web Services
Google Cloud
GitHub
Last 24 hours
MITRE ATT&CK
Top Tactics
Execution 47365
Privilege Escalation 2793
Persistence 2714
Discovery 766
Defense Evasion 546
Action
Rule description
Rule Le...
Rule Id
modified
Integrity checksum changed.
7
550
added
File added to the system.
5
554
deleted
File deleted.
7
553
Sep 30, 2024 @ 10:36:58.083
modified
Integrity checksum changed.
7
550
Sep 30, 2024 @ 10:34:44.878
modified
Integrity checksum changed.
7
550
Events count evolution
20,000
15,000
10,000
Count
SCA: Lastest scans
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0
cis_win10_enterprise
Policy
End scan
Passed
Failed
Not appl...
Score
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0
Sep 30, 2024 @ 01:46:09.000
133
258
3
34%

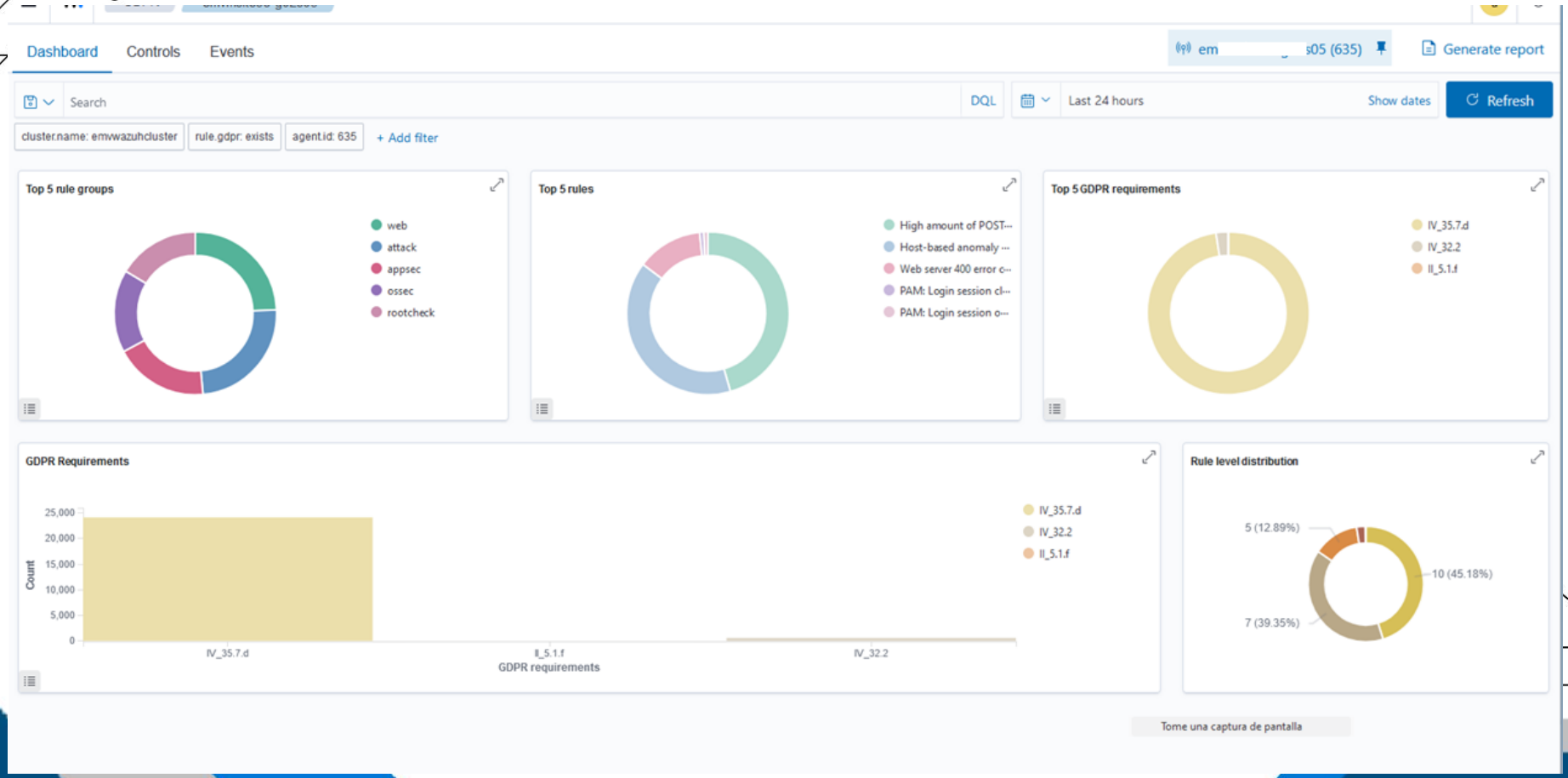
Subpaneles


MITRE ATT&CK
Dashboard
Intelligence
Framework
Events
Explore agent
https://attack.mitre.org/
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: it-wazuh
rule.mitre.id: exists
+ Add filter
Tactics
Execution 470299
Privilege Escalation 124191
Persistence 118025
Command and Control 82863
Defense Evasion 73713
Initial Access 50240
Impact 10394
Lateral Movement 7357
Discovery 2743
Credential Access 110
Collection 108
Exfiltration 0
Resource Development 0
Reconnaissance 0
Techniques
Hide techniques with no alerts
Filter techniques of selected tactic/s
T1047 - Windows Management Instrument... 365731
T1059 - Command and Scripting Interpreter 92048
T1105 - Ingress Tool Transfer 82863
T1078 - Valid Accounts 50130
T1546.011 - Application Shimming 31981
T1543 - Create or Modify System Process 24776
T1112 - Modify Registry 14319
T1053.005 - Scheduled Task 9855
T1565.001 - Stored Data Manipulation 9706
T1570 - Lateral Tool Transfer 7218
T1055 - Process Injection 5498
T1087 - Account Discovery 2675
T1059.003 - Windows Command Shell 1938
T1027 - Obfuscated Files or Information 1426
T1218 - System Binary Proxy Execution 1384
T1543.003 - Windows Service 832
T1055.001 - Dynamic-link Library Injection 696
T1059.001 - PowerShell 642
T1070.004 - File Deletion 433
T1485 - Data Destruction 419
T1531 - Account Access Removal 248
T1546.015 - Component Object Model Hijacking 238
T1078.002 - Domain Accounts 110
T1550.002 - Pass the Hash 110
T1021.001 - Remote Desktop Protocol 110
T1187 - Forced Authentication 103
T1114.003 - Email Forwarding Rule 90
T1059.005 - Visual Basic 82
T1018 - Remote System Discovery 68
T1574.001 - DLL Search Order Hijacking 66
T1574.002 - DLL Side-Loading 61
T1098 - Account Manipulation 29
T1210 - Exploitation of Remote Services 28
T1489 - Service Stop 20
T1136 - Create Account 20
T1562.001 - Disable or Modify Tools 18
T1213.002 - Sharepoint 18
T1546.008 - Accessibility Features 8
T1036 - Masquerading 8
T1110 - Brute Force 5
T1204.002 - Malicious File 3
T1003.001 - LSASS Memory 2
T1490 - Inhibit System Recovery 1
T1484 - Domain Policy Modification 1
T1021.004 - SSH 1

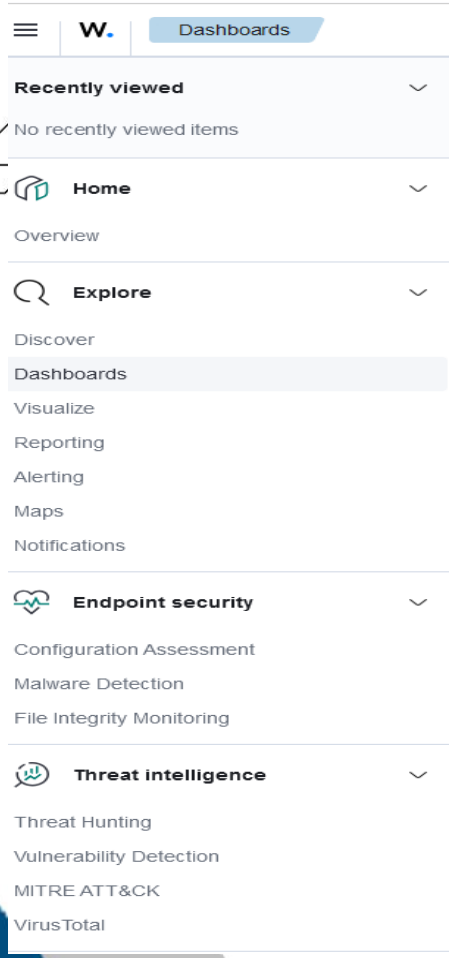
Subpaneles

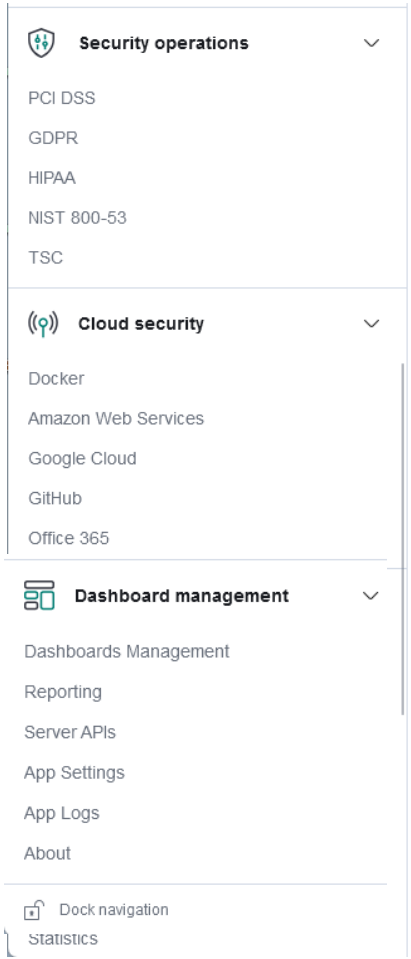

MITRE ATT&CK
emvmsite98-g02s05
Dashboard
Intelligence
Framework
Events
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
cluster.name: emvwazuhcluster
rule.mitre.id: exists
agent.id: 635
+ Add filter
Alerts evolution over time
Count
timestamp per 30 minutes
Network Denial of Ser···
Valid Accounts
Remote Services
Vulnerability Scanning
Sudo and Sudo Cachi···
Top tactics
Impact
Defense Evasion
Privilege Escalation
Initial Access
Persistence
Lateral Movement
Reconnaissance
Discovery
Execution
Credential Access
Rule level by attack
10
3
MITRE attacks by tactic
rule.mitre.tactic: Descending
Rule level by tactic
7
6
Tome una captura de pantalla

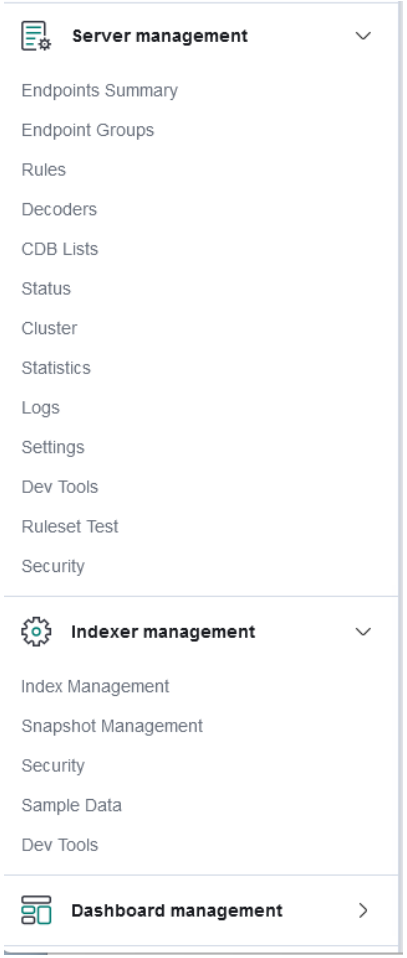
Subpaneles

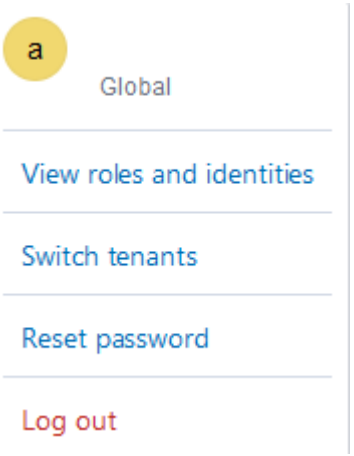

Dashboard
Controls
Events
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
cluster.name: emwwazuhcluster
rule.gdpr: exists
agent.id: 635
+ Add filter
Top 5 rule groups
web
attack
appsec
ossec
rootcheck
Top 5 rules
High amount of POST...
Host-based anomaly ...
Web server 400 error c...
PAM: Login session cl...
PAM: Login session o...
Top 5 GDPR requirements
IV_35.7.d
IV_32.2
II_5.1.f
GDPR Requirements
25,000
20,000
15,000
10,000
5,000
0
Count
IV_35.7.d
II_5.1.f
IV_32.2
GDPR requirements
Rule level distribution
5 (12.89%)
10 (45.18%)
7 (39.35%)
Tome una captura de pantalla

Menú lateral de Wazuh



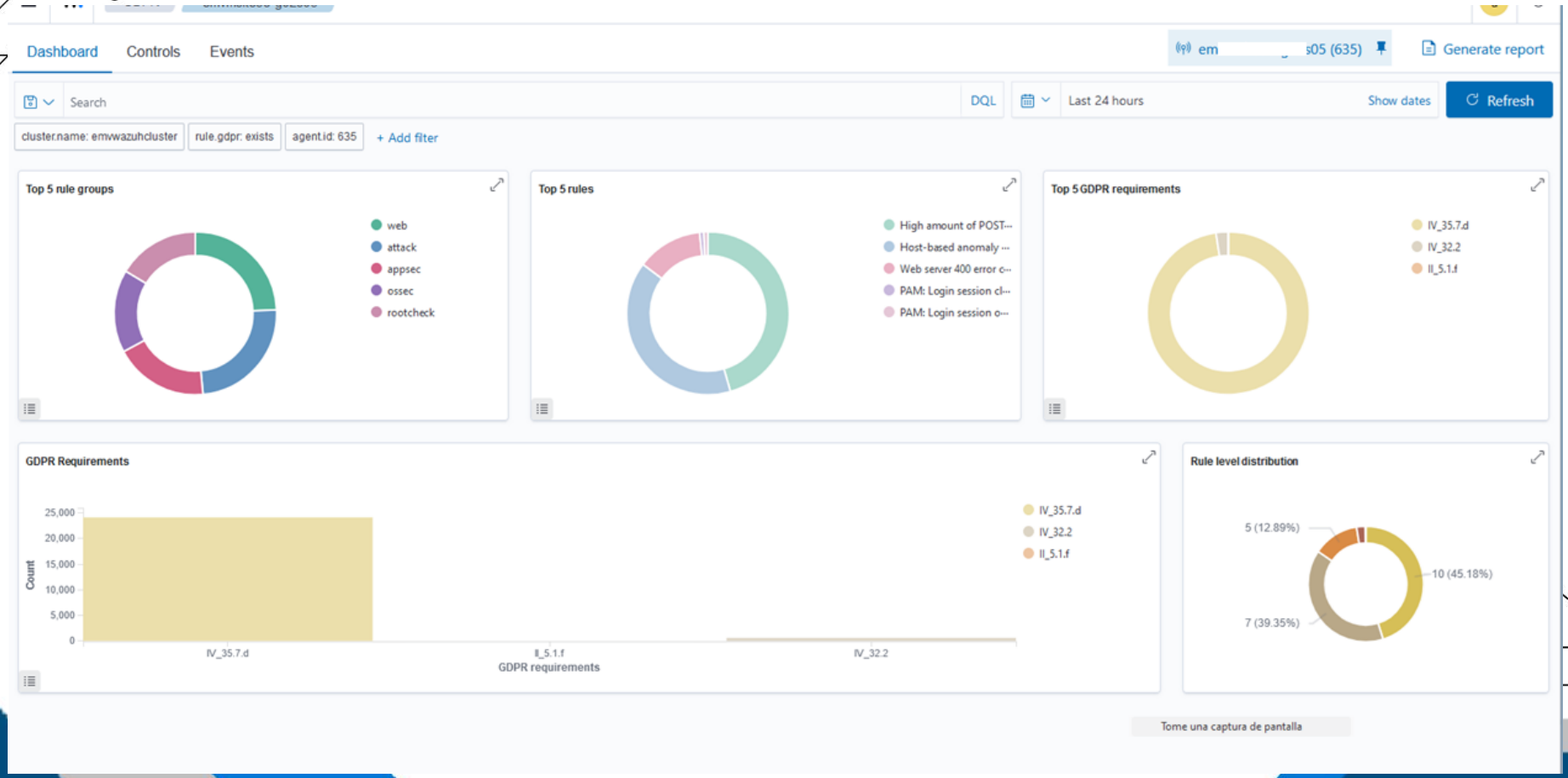






https://documentation.wazuh.com/current/user-manual/wazuh-dashboard/settings.html

Subpaneles


Dashboard
Controls
Events
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
cluster.name: emwwazuhcluster
rule.gdpr: exists
agent.id: 635
+ Add filter
Top 5 rule groups
web
attack
appsec
ossec
rootcheck
Top 5 rules
High amount of POST...
Host-based anomaly ...
Web server 400 error c...
PAM: Login session cl...
PAM: Login session o...
Top 5 GDPR requirements
IV_35.7.d
IV_32.2
II_5.1.f
GDPR Requirements
25,000
20,000
15,000
10,000
5,000
0
Count
IV_35.7.d
II_5.1.f
IV_32.2
GDPR requirements
Rule level distribution
5 (12.89%)
10 (45.18%)
7 (39.35%)
Tome una captura de pantalla

Control Vulnerabilidades

- Por agente
- Por CVE
- CVE solucionados

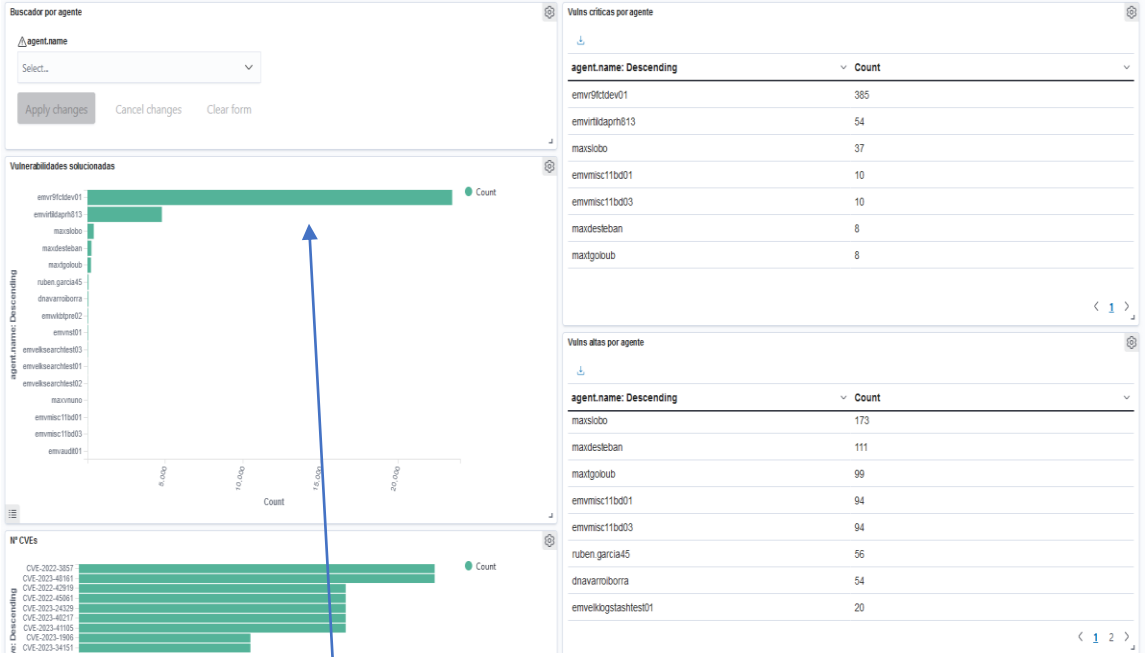
Common Vulnerabilities and Exposures

¿Qué es CVE?

Vulnerabilidades y exposiciones comunes

CVE - 2019 - 1214

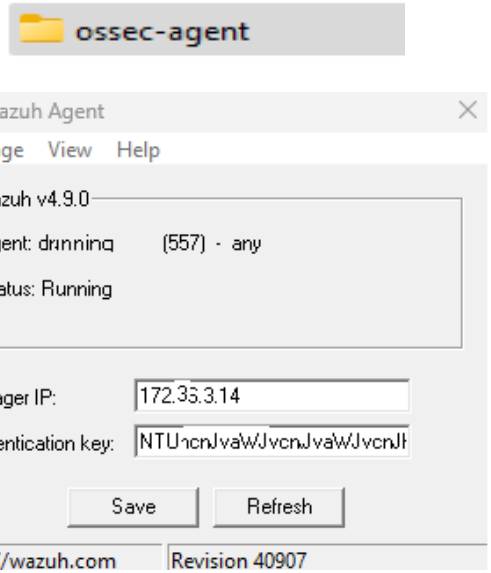
Prefix	Year	Numbering
Identical for each ID	Four digits, year of publication	Ongoing: four, five or seven digits



Vulnerabilidades solucionadas

Supervisión Agentes

Por agente



The agent was developed considering the need to monitor a wide variety of different endpoints without impacting their performance. It is supported on the most popular operating systems, and it requires 35 MB of RAM on average.

The Wazuh agent provides key features to enhance your system's security.

Log collector	Command execution
File integrity monitoring (FIM)	Security configuration assessment (SCA)
System inventory	Malware detection
Active response	Container security
Cloud security	

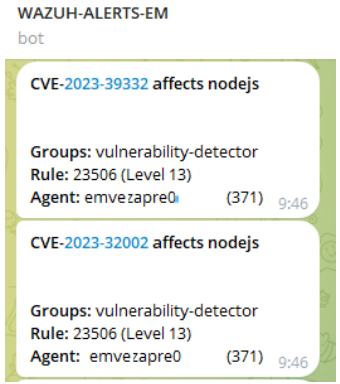
To install a Wazuh agent, select your operating system and follow the instructions.

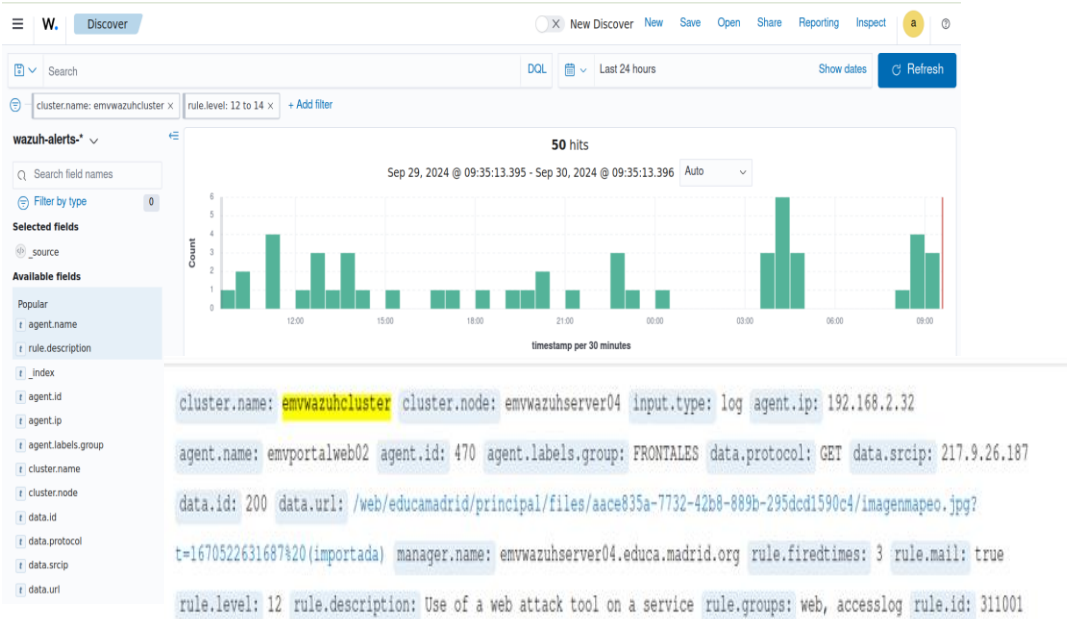
- Puerto 1514: se usa para los logs, los eventos... el grueso de los datos.
- Puerto 1515: se emplea para la autenticación.

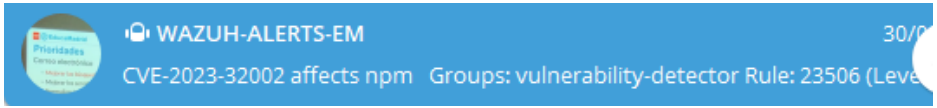
XDR estado agentes

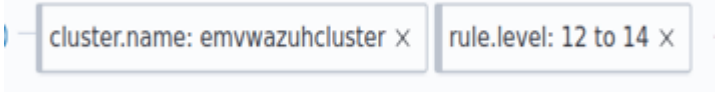
Extended Detection and Response (XDR)

- **Eventos**
- **Alertas**
  - **Comportamientos**
  - **Virus**
  - **Telegram**









Futuro y opciones adicionales

- **Comunicaciones (Logs Fortinet)**
- **Ajustes de funcionamiento (Calibrar reglas)**
- **Integración con IDS (maltrail)**
- **¿Posibilidades?**
- **¿I.A sobre Wazuh?**
- **¿Modulo ENS??**
- **Muchas opciones .....**

IRIS-WAZUH Foro para el intercambio de experiencias con WAZUH

https://listserv.rediris.es/cgi-bin/wa?SUBED1=IRIS-WAZUH&A=1

IRIS-WAZUH@LISTSERV.REDIRIS.ES

¿ Por qué Wazuh ?

EducaMadrid ha optado por implementar Wazuh a nuestra infraestructura por varios motivos:

- **Somos totalmente PRO Open source, encaja con nuestros valores.**
- **Nos ayuda a cumplir con necesidades básicas, como por ejemplo tener un servidor de logs centralizado**
- **Nos ayuda a cumplir gran parte de los requerimientos del ENS.**

CPD en **Madrid------- Hardware** propio---- **Software Libre**

Plataforma Libre

Segura, Soberana, Sostenible

Durante el curso 22/23…

1.8 millones de cuentas.

16 servidores LDAP.

CPD ISO 50.001 (energía) e ISO 14.001 (medio ambiente).

Energía 100% renovable.

ENS y LOPD.

Ni huella digital ni perfiles.

Casi 400 millones de correos.

Casi 35 servidores para operativa del correo electrónico.

¡¡¡ 8000 millones de páginas Servidas ¡¡¡

Menos de 2 € usuario al año.

Y mucho más…

¡¡¡ La colaboración público privada funciona ¡¡¡

9 funcionarios

26 trabajadores empresa privada.

CAU.

Desarrollo.

Diseño.

Sistemas.

Redes/ciber.

+ Personal en practicas

XIX JORNADAS REDIMADRID 2024

Martes, 15 de octubre de 2024

¡Muchas gracias!
¿Preguntas?

cibersec@educa.madrid.org