Detección de vulnerabilidades

Detección de vulnerabilidades

Monitorización de vulnerabilidades

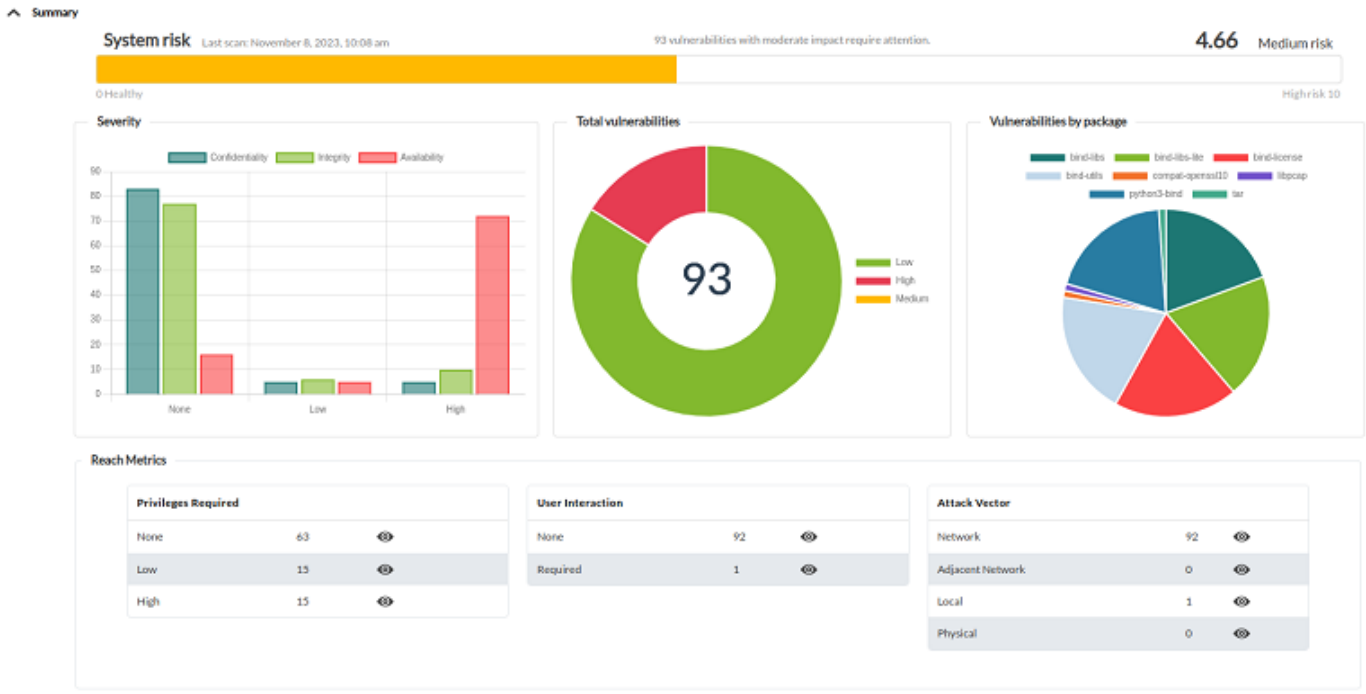
De manera similar a como se realiza la evaluación de *hardening*, los EndPoints de Pandora FMS y el motor de descubrimiento remoto buscarán información sobre el software instalado en el sistema, luego contrastará esta información con la BB.DD. central de vulnerabilidades que dispone Pandora FMS (descargada de NIST, Mitre y otras fuentes) y proporcionará una lista de paquetes de software con vulnerabilidades conocidas.

Esta funcionalidad está disponible tanto si dispone de EndPoints (y estos EndPoints tienen activado el inventario de software) como si no dispone de EndPoints y tiene que hacer el descubrimiento a través de la red. Si el descubrimiento es a través de la red, la información proporcionada será mucho menor. Se recomienda utilizar un EndPoint.

Para ell se puede utilizar cualquier EndPoint de la versión 7 siempre y cuando tenga el inventario de software activado. Este sistema funciona para sistemas Linux® y MS Windows®.

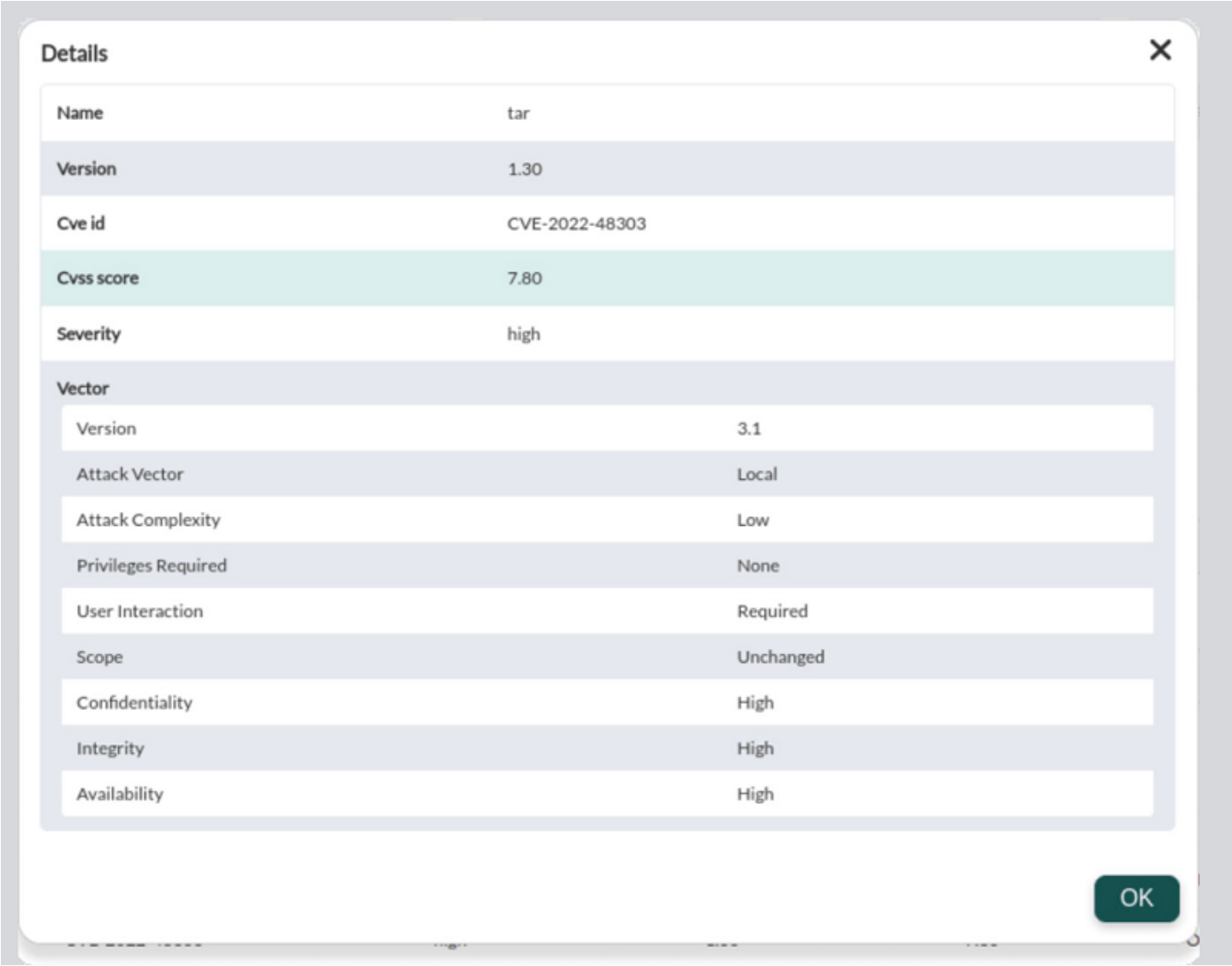
De manera similar a como funciona el *hardening*, Pandora FMS ofrecerá un indicador de riesgo único para cada sistema, basado en el número de vulnerabilidades y su peligrosidad.

Aportará un panel informativo de las vulnerabilidades del sistema, indicando la evolución del riesgo a lo largo del tiempo, las vulnerabilidades ordenadas por diferentes criterios, tales como complejidad del ataque, gravedad, tipo de vulnerabilidad, vector de ataque, interacción de usuario, tipo de privilegios requerido, etc.



Podrá navegar por el panel de control para filtrar la información y llegar a un nivel de detalle donde se especifique cada paquete de software vulnerable, la vulnerabilidad (con código CVE) que le aplica y la descripción del problema:

Name	CVE	Severity	Version	Score	Detection Time	Details
tar	CVE-2022-48303	high	1.30	7.80	October 16, 2023, 8:55 am	
python3-bind	CVE-2022-38177	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2022-38178	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2021-25219	low	9.11.36	5.30	October 16, 2023, 8:55 am	
python3-bind	CVE-2021-25215	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2020-8625	high	9.11.36	8.10	October 16, 2023, 8:55 am	
python3-bind	CVE-2020-8623	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2020-8616	low	9.11.36	8.60	October 16, 2023, 8:55 am	
python3-bind	CVE-2020-8617	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2019-6477	low	9.11.36	7.50	October 16, 2023, 8:55 am	
python3-bind	CVE-2019-6465	low	9.11.36	3.70	October 16, 2023, 8:55 am	
python3-bind	CVE-2019-6471	low	9.11.36	5.90	October 16, 2023, 8:55 am	
python3-bind	CVE-2018-5743	low	9.11.36	8.60	October 16, 2023, 8:55 am	
libpcap	CVE-2019-15165	low	1.9.1	7.50	October 16, 2023, 8:55 am	
compat-openssl10	CVE-2022-0778	low	1.0.2o	7.50	October 16, 2023, 8:55 am	
bind-utils	CVE-2022-38177	low	9.11.36	7.50	October 16, 2023, 8:55 am	
bind-utils	CVE-2022-38178	low	9.11.36	7.50	October 16, 2023, 8:55 am	
bind-utils	CVE-2021-25219	low	9.11.36	5.30	October 16, 2023, 8:55 am	
bind-utils	CVE-2021-25215	low	9.11.36	7.50	October 16, 2023, 8:55 am	



¿Qué es un CVE?

Common Vulnerabilities and Exposures (CVE) es una identificación única y estandarizada para una vulnerabilidad de seguridad en software o hardware. Los CVE son un sistema de nomenclatura y seguimiento que se utiliza en todo el mundo para identificar y enumerar vulnerabilidades de seguridad específicas. Este sistema fue creado para facilitar la organización, comunicación y referencia de información sobre vulnerabilidades, lo que permite a la comunidad de seguridad informática y a los profesionales de TI abordar y solucionar problemas de seguridad de manera más eficiente.

Las características clave de un CVE son las siguientes:

- Identificación única: Cada CVE tiene un número único que lo identifica, lo que facilita su seguimiento y referencia. Por ejemplo, un CVE puede tener un formato como “CVE-2021-12345.”
- Descripción detallada: Cada CVE incluye una descripción detallada de la vulnerabilidad, lo que permite a los usuarios entender mejor la naturaleza y el impacto del problema.
- Referencias cruzadas: Los CVE a menudo incluyen referencias cruzadas a otros recursos y bases de datos de seguridad, como el National Vulnerability Database (NVD) del Instituto Nacional de

Estándares y Tecnología (NIST), para proporcionar información adicional sobre la vulnerabilidad.
- Fecha de publicación: Los CVE suelen incluir la fecha en que se publicó la información sobre la vulnerabilidad.

Los CVE son utilizados por la industria de la seguridad informática, los proveedores de software y hardware, los investigadores de seguridad y los administradores de sistemas para rastrear y gestionar vulnerabilidades. Esta nomenclatura estandarizada es esencial para garantizar que las vulnerabilidades se comuniquen y se aborden de manera coherente en todo el mundo, lo que ayuda a proteger a las organizaciones y a los usuarios finales contra las amenazas de seguridad. Además, la existencia de CVE facilita la creación de bases de datos y herramientas que permiten a las organizaciones mantenerse al día con las últimas amenazas y aplicar parches o soluciones de seguridad cuando sea necesario.

La BB.DD. de vulnerabilidades de Pandora FMS

La base de datos de vulnerabilidades de Pandora FMS se nutre de dos fuentes:

- CVE-Search el cual combina datos de NVD NIST, MITRE y Red Hat.
- Información directa de los repositorios de Canonical, Red Hat, Debian, Arch Linux, NVD NIST, y Microsoft Security Updates.

El servidor de Pandora construye su propia base de datos a partir de estos datos y la segmenta e indexa en memoria para una rápida detección, de modo que únicamente carga las vulnerabilidades correspondientes a los sistemas operativos que reportan los EndPoints de Pandora FMS.

Para la detección de vulnerabilidades mediante EndPoints, se utiliza una base de datos que se distribuye por defecto con el servidor PFMS y asocia nombres de paquetes y aplicaciones con distintos CVE. Para la detección de vulnerabilidades remotas se utiliza una base de datos que asocia los CPE con los CVE. La consola utiliza una base de datos con información sobre los los distintos CVE que se encuentran en la base de datos del servidor para mostrársela al usuario y generar informes. Los datos de los distintos CVE vienen cargados en la tabla `tpandora_cve`, la cual existe desde la versión 774.

Configuración de la auditoría de vulnerabilidades

A nivel de servidor

Para la detección local de vulnerabilidades, debe estar activado el Data Server y los EndPoints

deben enviar información de inventario de software.

Para que funcione la detección remota de vulnerabilidades debe estar activado el Discovery Server.

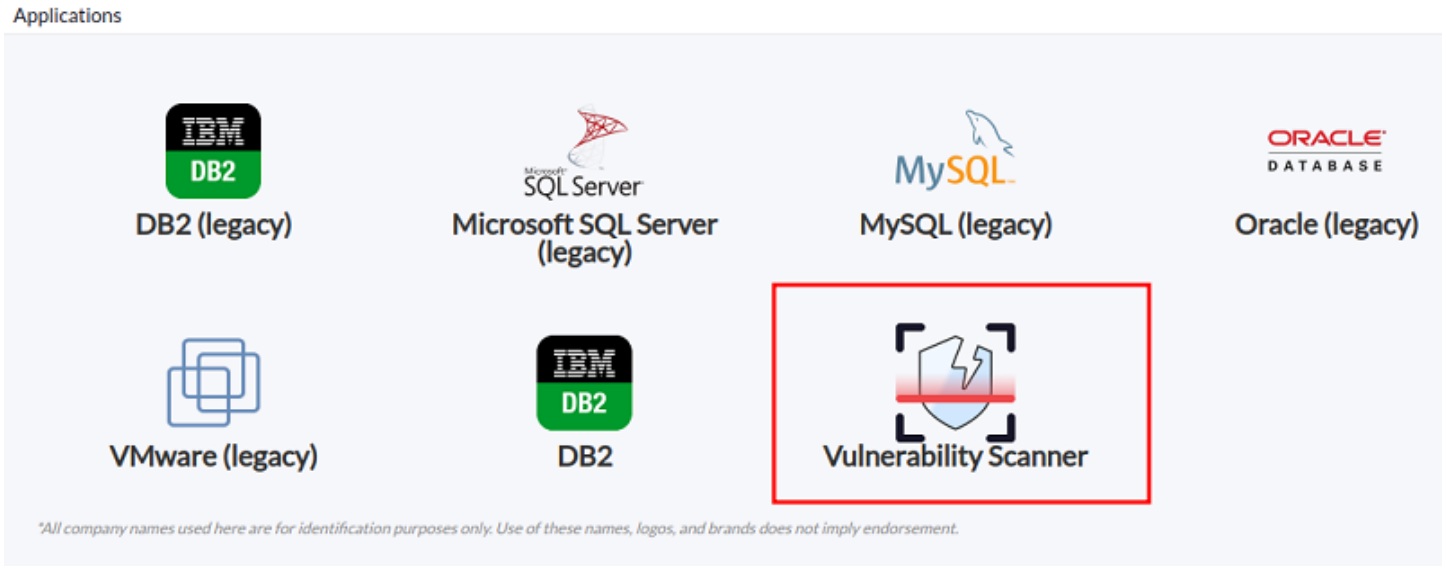
A nivel de agente

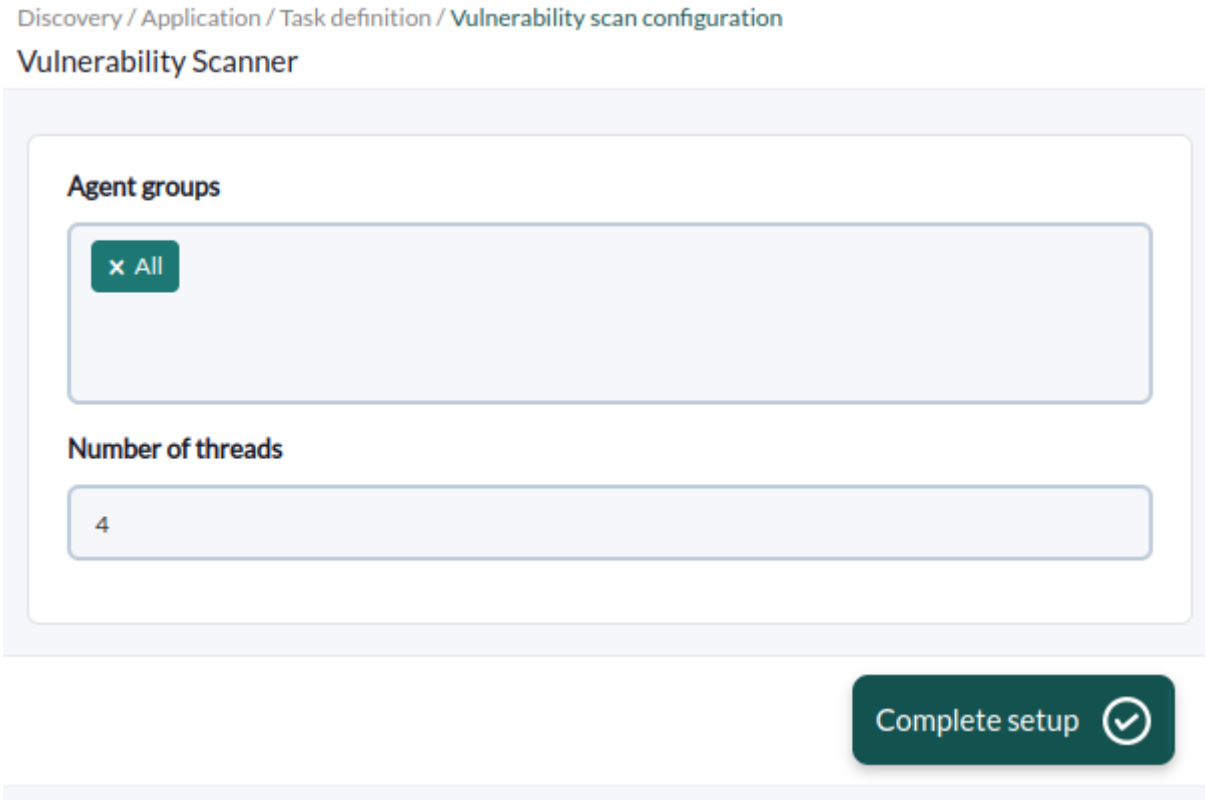
Se puede desactivar o activar manualmente un agente o que utilice (por defecto) la configuración global del *setup*, en la sección de configuración avanzada.

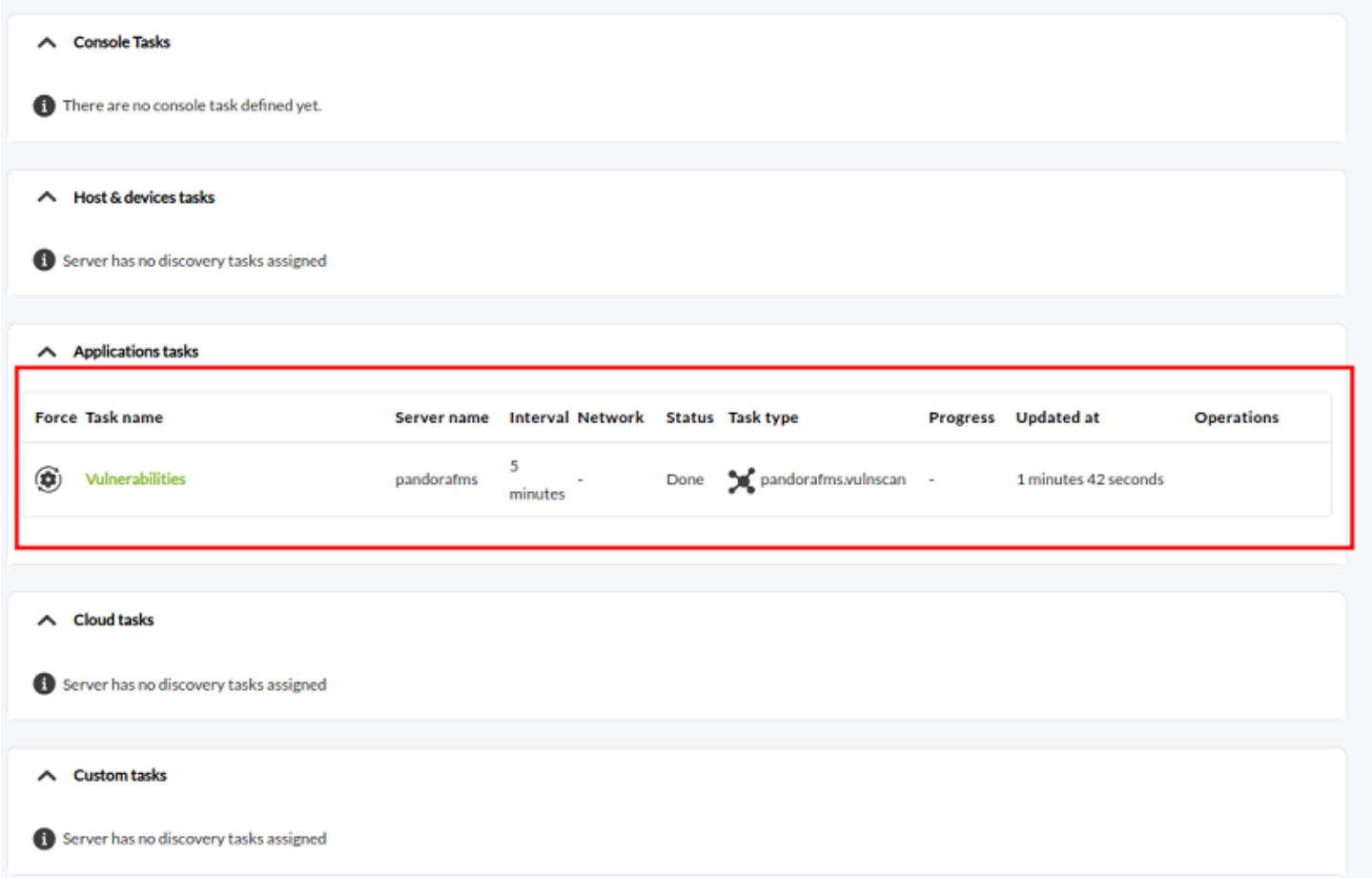
Tareas de escaneo remoto

Para ello debe ir a Discovery y lanzar una nueva tarea de descubrimiento de vulnerabilidades. Se le pedirá uno o varios grupos de máquinas que ya existan en la monitorización para lanzar sobre ellas la detección de vulnerabilidades. Se utilizará la dirección IP principal de dichos agentes para lanzar el escaneo. Si no tiene monitorización o no existen en Pandora FMS, se deben detectar primero con una detección normal de red de discovery.

El escaneo de vulnerabilidades no creará nuevos agentes.


Applications
DB2 (legacy)
Microsoft SQL Server (legacy)
MySQL (legacy)
Oracle (legacy)
VMware (legacy)
DB2
Vulnerability Scanner
*All company names used here are for identification purposes only. Use of these names, logos, and brands does not imply endorsement.


Discovery / Application / Task definition / Vulnerability scan configuration
Vulnerability Scanner
Agent groups
× All
Number of threads
4
Complete setup



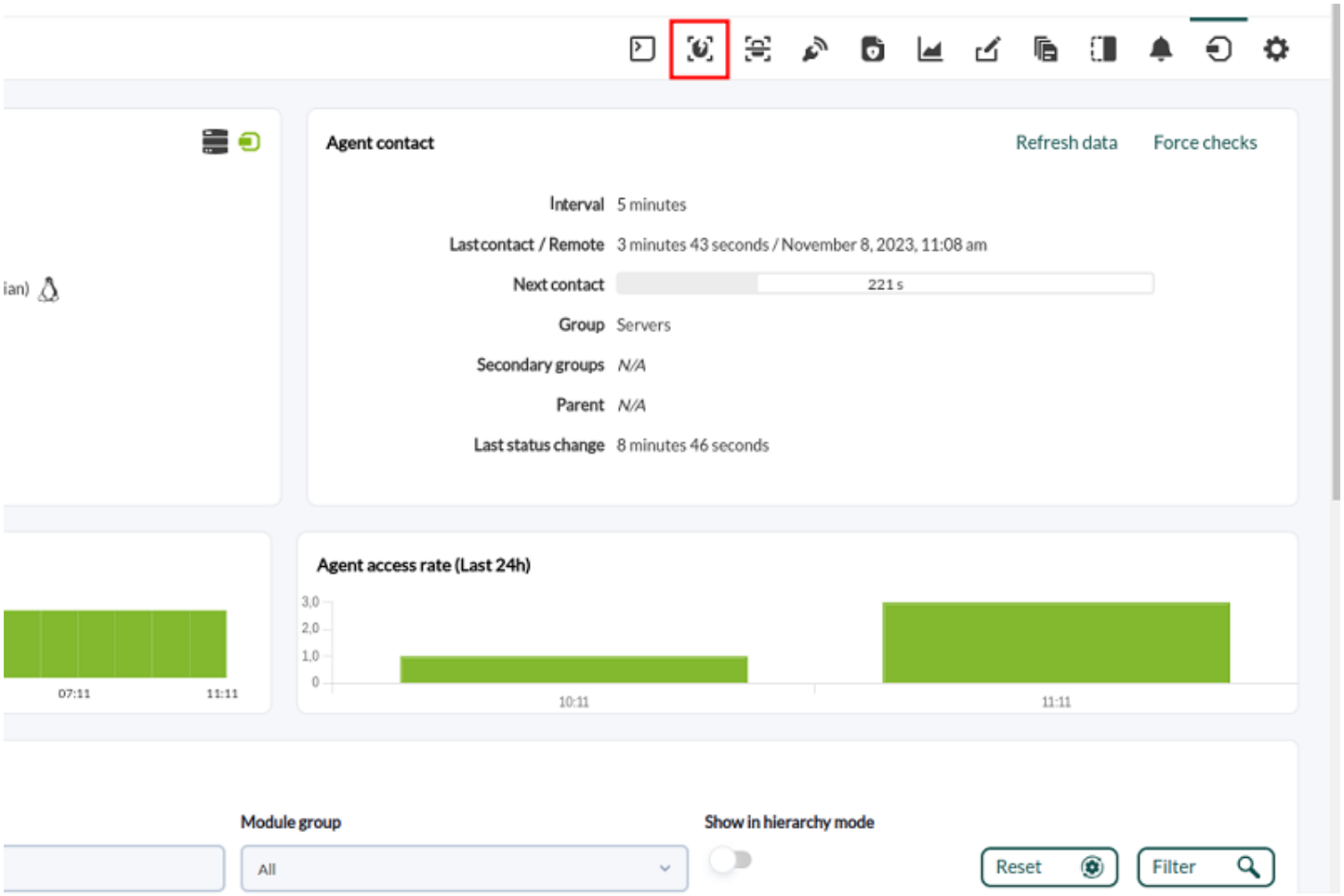
Visualización de los datos de vulnerabilidades

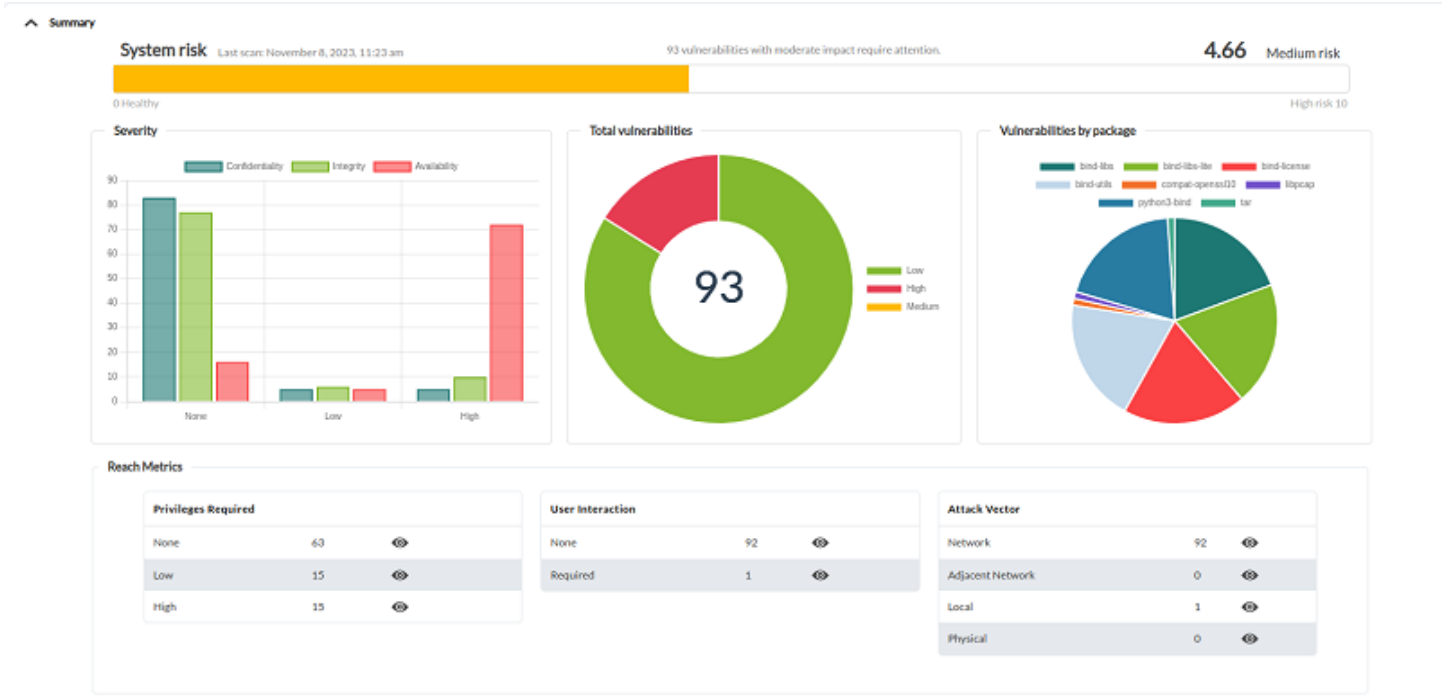
Una vez el sistema disponga de información, esta será mostrada en la pestaña de Vulnerabilidades de cada sistema monitorizado.

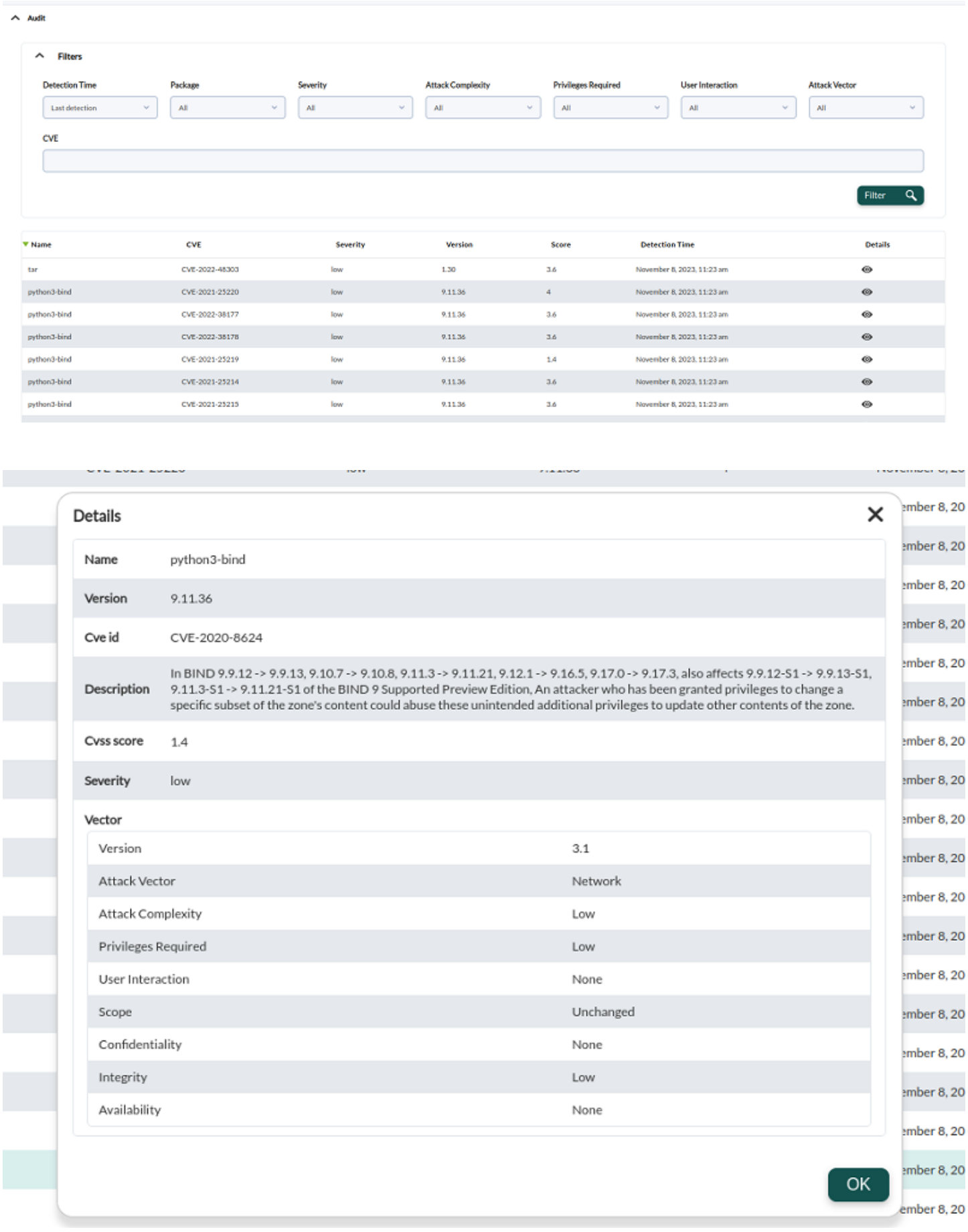
También dispone (a partir de la version 775) de un *dashboard* general, con varias gráficas agregadas, como el Top-10 de sistemas más vulnerables (peor *ranking* de vulnerabilidades), Top-10 vulnerabilities (más frecuentes) y otras agrupaciones.

Estos informes disponen de algunos filtros específicos:

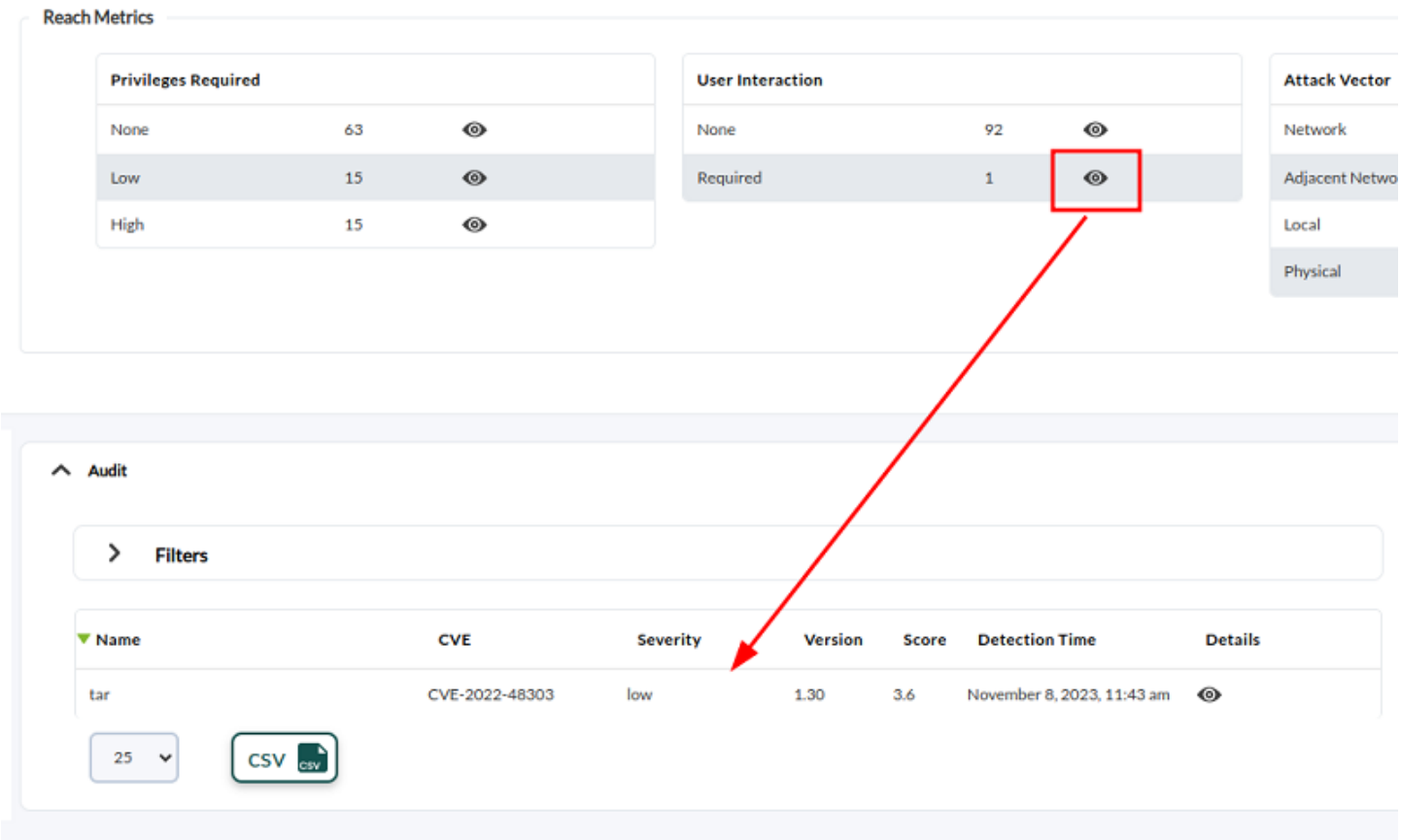
- Por grupo de máquinas.
- Attack complexity (low/high/medium).
- Tipo de vulnerabilidad (confidentiality, integrity, availability...).
- Access vector: Network, Adjacent Network...
- User interaction: none, required, etc.
- Privileges required: None, low...


Agent contact
Refresh data
Force checks
Interval 5 minutes
Last contact / Remote 3 minutes 43 seconds / November 8, 2023, 11:08 am
Next contact 221 s
Group Servers
Secondary groups N/A
Parent N/A
Last status change 8 minutes 46 seconds
Agent access rate (Last 24h)
3,0
2,0
1,0
0
07:11
11:11
10:11
11:11
Module group
All
Show in hierarchy mode
Reset
Filter


Summary
System risk
Last scan: November 8, 2023, 11:23 am
93 vulnerabilities with moderate impact require attention.
4.66
Medium risk
0 Healthy
High risk 10
Severity
Confidentiality
Integrity
Availability
None
Low
High
Total vulnerabilities
93
Low
High
Medium
Vulnerabilities by package
Reach Metrics
Privileges Required
None 63
Low 15
High 15
User Interaction
None 92
Required 1
Attack Vector
Network 92
Adjacent Network 0
Local 1
Physical 0



Las métricas de alcance permiten filtrar de forma rápida las vulnerabilidades:

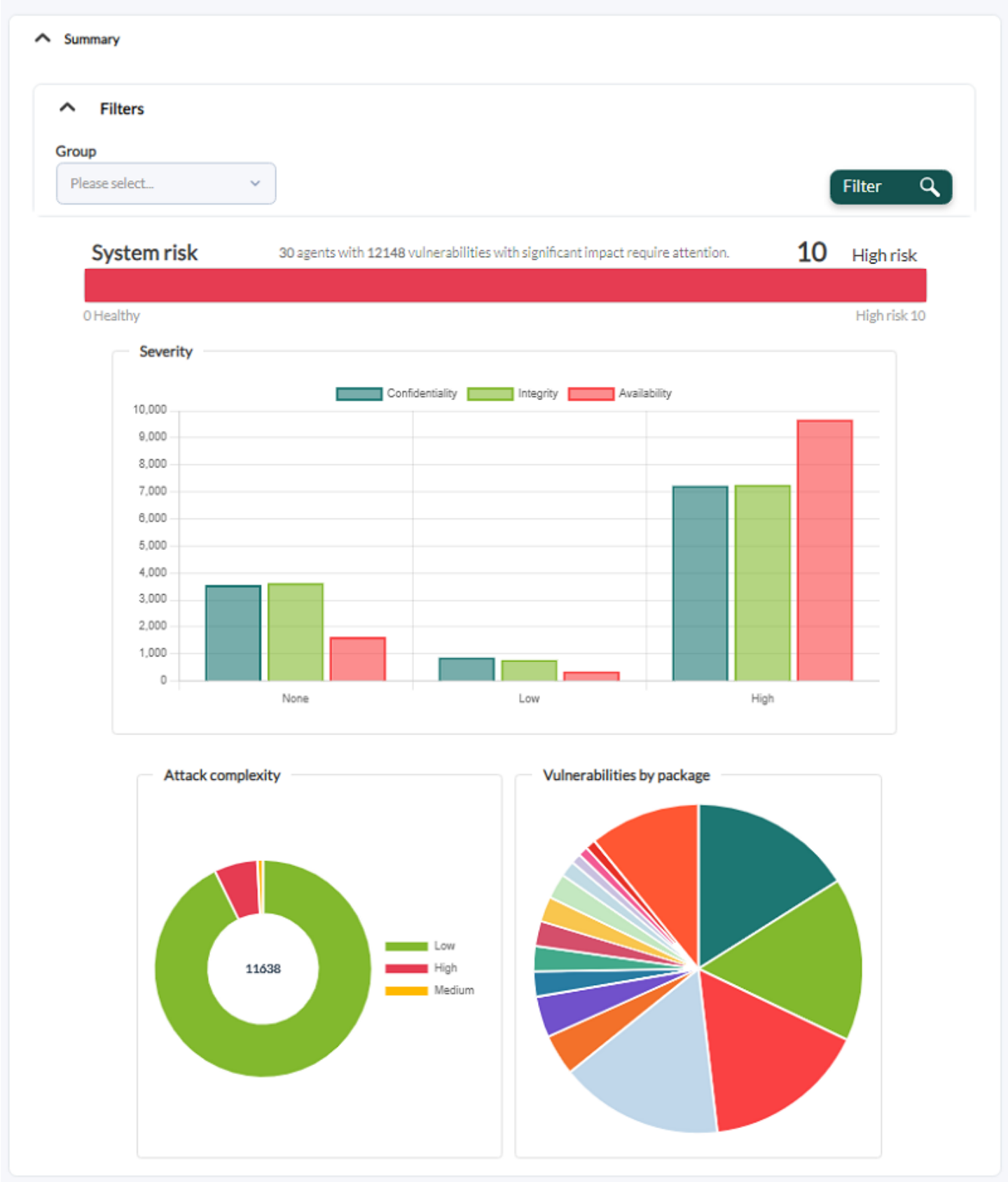


Vista táctica de seguridad

Menú Operation → Security → Vulnerabilities.

Summary

Presenta un panorama global de los agentes, con gráficos que resumen el riesgo total en el sistema como un conjunto, la severidad de la complejidad de los ataques y las vulnerabilidades presentadas por cada paquete de software instalado.

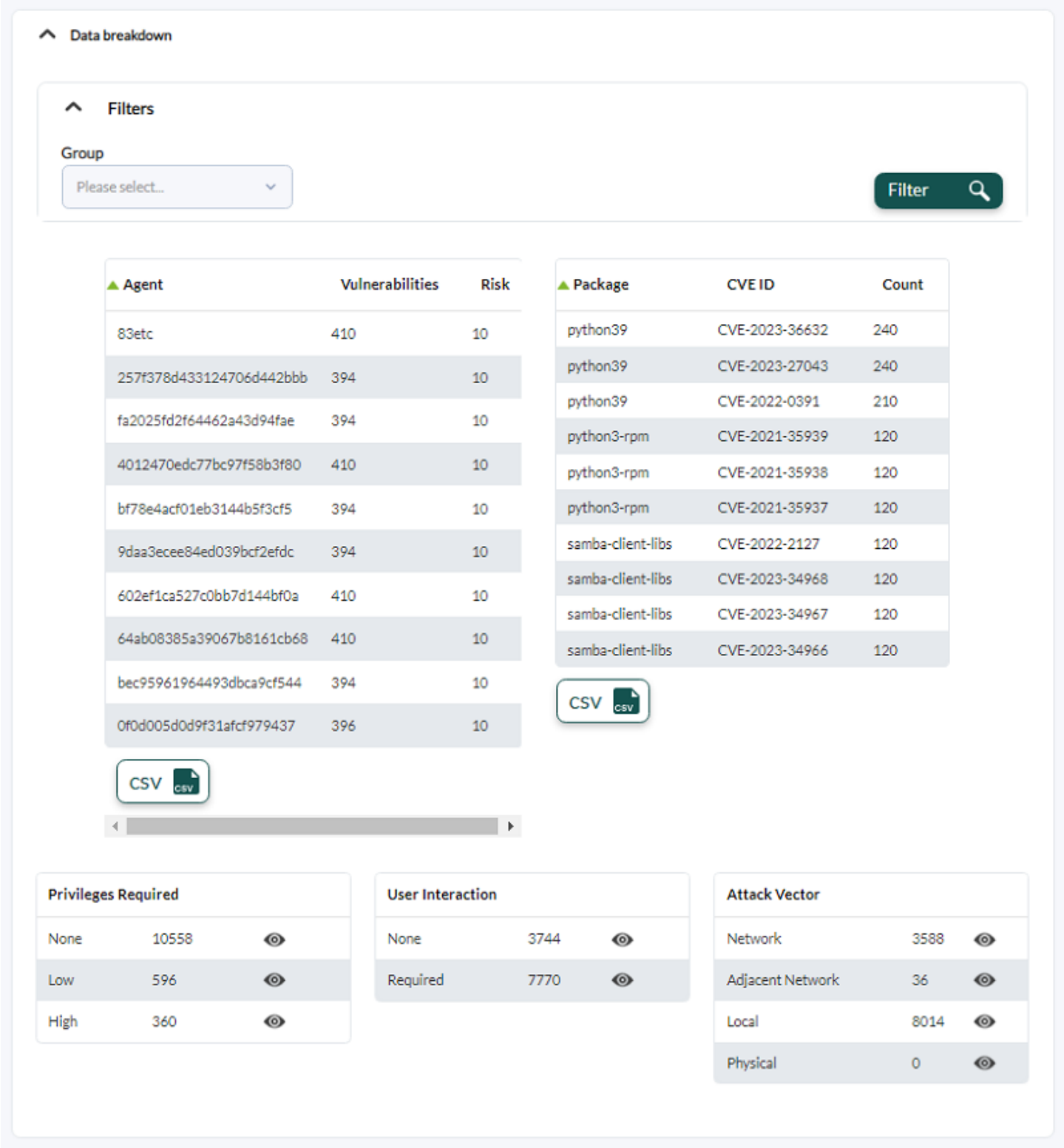


Se puede filtrar por grupo de agentes, por defecto presenta todos los grupos (All).

Data breakdown

Presenta un desglose de los datos de seguridad, mostrando los 10 primeros agentes y 10 primeros

paquetes de software con más vulnerabilidades.



La información se puede filtrar por grupos de agentes y ser exportados en formato CSV. Los resúmenes en los cuadros de privilegios requeridos (Privileges required), interacción del usuario (User Interaction) y vector de ataque (Attack Vector) cuentan con botones de visualización que remiten a la sección de auditoría.

Audit

Por defecto muestra toda la información de vulnerabilidades por lo que puede tardar en cargar. Se podrá filtrar por infinidad de combinaciones en cuanto a las características de las vulnerabilidades, incluyendo números específicos de identificadores de CVE.

Audit

Filters

Agent: All | Package: All | Severity: All | Attack Complexity: All

Privileges Required: All | User Interaction: All | Attack Vector: All

CVE:

Filter

Agent	Name	CVE	Severity	Version	Score	Detection Time	Details
fa2025fd2f64462a43d94fae	python39	CVE-2007-4559	low	3.9.7	6.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2023-32681	low	3.9.7	4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2023-40217	low	3.9.7	1.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2023-24329	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2020-10735	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2022-45061	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2021-28861	low	3.9.7	4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2022-42919	high	3.9.7	5.9	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2015-20107	low	3.9.7	4.7	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2023-36632	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2023-27043	low	3.9.7	1.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39	CVE-2022-0391	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2007-4559	low	3.9.7	6.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2023-32681	low	3.9.7	4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2023-40217	low	3.9.7	1.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2023-24329	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2020-10735	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2022-45061	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2021-28861	low	3.9.7	4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2022-42919	high	3.9.7	5.9	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2015-20107	low	3.9.7	4.7	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2023-36632	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2023-27043	low	3.9.7	1.4	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-libs	CVE-2022-0391	low	3.9.7	3.6	December 7, 2023, 12:00 am	
fa2025fd2f64462a43d94fae	python39-pip	CVE-2023-36632	low	20.7.4	3.6	December 7, 2023, 12:00 am	

Show 25 entries CSV

Previous 1 2 3 4 5 ... 486 Next

Una vez filtrada la información, cada item cuenta con un botón de visualización de detalles (icono con forma de ojo) que presentará a su vez la información detallada correspondiente.

Volver al índice de documentación de Pandora FMS