Monitorización de seguridad

Monitorización de seguridad

Introducción

Pandora FMS se puede emplear para monitorizar el estado de infraestructuras de seguridad tales como entornos de *backup*, antivirus, VPN, *firewalls*, IDS/IPS, SIEM, *honeypots*, sistemas de autentificación, sistemas de almacenamiento, recogida de *logs*, etcétera. Además, Pandora FMS incorpora herramientas internas para incrementar la propia seguridad como doble autentificación (2FA), cifrado en la base de datos para las contraseñas, autentificación externa, protocolo Tentacle usando cifrado de datos (SSL/TLS), registro de auditoría propio y otras características para hacer más segura la plataforma. Pandora FMS, como organización, dispone de certificación 27001, y es CNA en Mitre para gestionar sus propios CVE. Tenemos una política de seguridad pública y abierta para auditores de seguridad independientes.

Además de esas funciones Pandora FMS incorpora funcionalidades específicas de seguridad propias desde la versión 773 y se irán añadiendo más funcionalidades en sucesivas versiones.

En la versión 774 Pandora FMS incorpora las siguientes funcionalidades propias de seguridad.

- *Plugin* de monitorización de seguridad, para supervisar la seguridad básica del sistema, diseñado para servidores GNU/Linux® únicamente.
- Sistema de evaluación de *hardening* a lo largo del tiempo (GNU/Linux®, MS Windows®).
- Sistema de evaluación de las vulnerabilidades del sistema (GNU/Linux®, MS Windows® y sistemas remotos).

Plugin de monitorización de seguridad

Este *plugin*, que viene de serie en los agentes GNU/Linux, se encarga de verificar constantemente ciertos aspectos básicos de su entorno. Está diseñado para ser ligero, afectando muy poco al rendimiento del sistema y ser lanzado con el intervalo estándar del agente, cada cinco minutos. Comprueba los siguientes aspectos del sistema:

- Robustez de las contraseñas de todos los usuarios con acceso al sistema. Lo hace a través de un “diccionario de contraseñas”, por defecto compuesto por 100 entradas. Puede personalizar dicho diccionario y añadir sus propias entradas (para reflejar las típicas contraseñas comunes usadas en su organización). El 90% de los ataques habituales tienen como vector de ataque una cuenta de usuario mal protegida en un entorno secundario.
- Estado de SELinux, verificando si está activo o presente.
- Acceso remoto como usuario root, verificando que esté desactivado el inicio de sesión con contraseña para este usuario.
- Acceso remoto automático como root mediante llaves SSH previamente configuradas y establecidas.
- Puertos TCP en escucha activa (que estén fuera de una lista de números de puertos permitidos).
- Modificación de ficheros de configuración esenciales, verificando la integridad de los mismos y si han cambiado (ficheros como `/etc/resolv.conf`, `/etc/hosts/`, `/etc/passwd` y otros).

Son cosas muy básicas pero a la vez muy importantes. Cualquier sistema, sea un entorno de pruebas, una máquina virtual o un VPS en un *hosting* secundario es vulnerable a ataques básicos pero que suelen ser el 80% de los que abren una incidencia más seria en la organización.

Para instalar el *plugin* de seguridad basta con activarlo en el agente GNU/Linux, viene por defecto incluido en versiones 774 o posteriores:

```
module_begin
module_plugin /etc/pandora/plugins/pandora_security_check
module_end
```

Para instalar el plugin en versiones anteriores del agente, se puede descargar de la librería de *plugins* de Pandora FMS:

https://pandorafms.com/library/linux-security-plugin/

Monitorización de hardening

E Se han fusionado las recomendaciones del Center for Internet Security (CIS) con la tecnología de monitorización de Pandora FMS para ofrecer un sistema de auditoría de aseguramiento integrado. Esto permite rastrear y evaluar a lo largo del tiempo la evolución de las medidas de *hardening* (fortalecimiento de la seguridad) en los entornos utilizados y monitorizados.

El *system hardening* (o endurecimiento del sistema) es un proceso que utilizado para mejorar la seguridad de un sistema informático al reducir su superficie de ataque y fortalecer sus defensas. Consiste en hacer más difícil que posibles atacantes exploren fallos de configuración, ya sea por configuraciones por defecto, malas configuraciones o configuraciones indebidas.

El *system hardening* es un proceso continuo ya que las amenazas de seguridad y las vulnerabilidades evolucionan con el tiempo. Requiere un monitoreo constante, evaluaciones de riesgos y ajustes en las configuraciones de seguridad para adaptarse a las circunstancias cambiantes. Además, las organizaciones a menudo siguen estándares y mejores prácticas específicas de la industria, como los controles del CIS o las pautas del National Institute of Standards and Technology (NIST), para garantizar un *system hardening* integral.

Pandora FMS utiliza varias categorías del CIS para agrupar los chequeos que realiza.

Categorías CIS Auditadas por Pandora FMS

Hemos llevado las recomendaciones del CIS un paso más allá al implementar más de 1500 comprobaciones individuales en una variedad de categorías cruciales para la seguridad.

Inventario y control de activos hardware y software: Supervise y gestione todos los dispositivos y software en su organización. Mantenga un inventario actualizado de sus activos tecnológicos y use la autenticación para bloquear los procesos no autorizados.

Inventario y control de dispositivos: identificar y gestionar sus dispositivos de hardware para que solamente los autorizados tengan acceso, bloqueando los demás. Mantener un inventario adecuado minimiza riesgos internos, organiza su entorno y brinda claridad a su red.

Gestión de vulnerabilidades: Analice sus activos de forma continua en el tiempo para detectar vulnerabilidades potenciales y solucionelas antes de que se conviertan en la entrada a un ataque. Refuerce la seguridad de red asegurándose de que el software y los sistemas operativos en la organización estén siempre actualizados con las últimas medidas de seguridad y *parches*. Ayude a gestionar su software para asegurar que solamente el software autorizado esté instalado y sea ejecutado. Evite vulnerabilidades y riesgos al mantener un inventario preciso y gestionar su software.

Uso controlado de privilegios administrativos: Supervise de cerca los controles de acceso y el comportamiento de los usuarios con cuentas privilegiadas para evitar cualquier acceso no autorizado a sistemas críticos. Asegúrese de que solamente las personas autorizadas tengan privilegios elevados para evitar cualquier mal uso de los privilegios administrativos. Establece políticas estrictas para prevenir el uso indebido de privilegios.

Configuración segura de hardware y software: Establezca y mantenga configuraciones de seguridad basadas en los estándares aprobados por su organización. Crea un sistema de gestión de configuraciones riguroso que detecte y alerte sobre cualquier configuración incorrecta, y establece un proceso de control de cambios para evitar que los atacantes se aprovechen de servicios y configuraciones vulnerables.

Mantenimiento, supervisión y análisis de *logs* y registros de auditoría: Recopile, administre y analice los *logs* de auditoría de eventos para identificar posibles anomalías. Mantenga registros detallados para comprender a fondo los ataques y poder responder de manera eficaz a los incidentes de seguridad.

Defensas contra *malware* : Supervise y controle la instalación y ejecución de código malicioso en varios puntos de su organización para prevenir ataques. Configure y utiliza software antimalware y aproveche la automatización para garantizar actualizaciones rápidas de defensas y una acción correctiva ágil en caso de ataques.

Protección del correo electrónico y los navegadores web: Proteja y administre sus navegadores web y sistemas de correo electrónico contra amenazas en línea para reducir su superficie de ataque. Desactive complementos de correo electrónico no autorizados y asegúrese de que los usuarios solo accedan a sitios web de confianza mediante filtros de URL basados en la red. Mantenga seguras las puertas de entrada más comunes para ataques.

Capacidades de recuperación de datos: Establece procesos y herramientas para asegurar que la información crítica de tu organización esté respaldada adecuadamente. Asegúrese de contar con un sistema de recuperación de datos confiable para restaurar la información en caso de ataques que pongan en peligro los datos críticos. Prepare su organización para hacer frente a la pérdida de datos de manera efectiva.

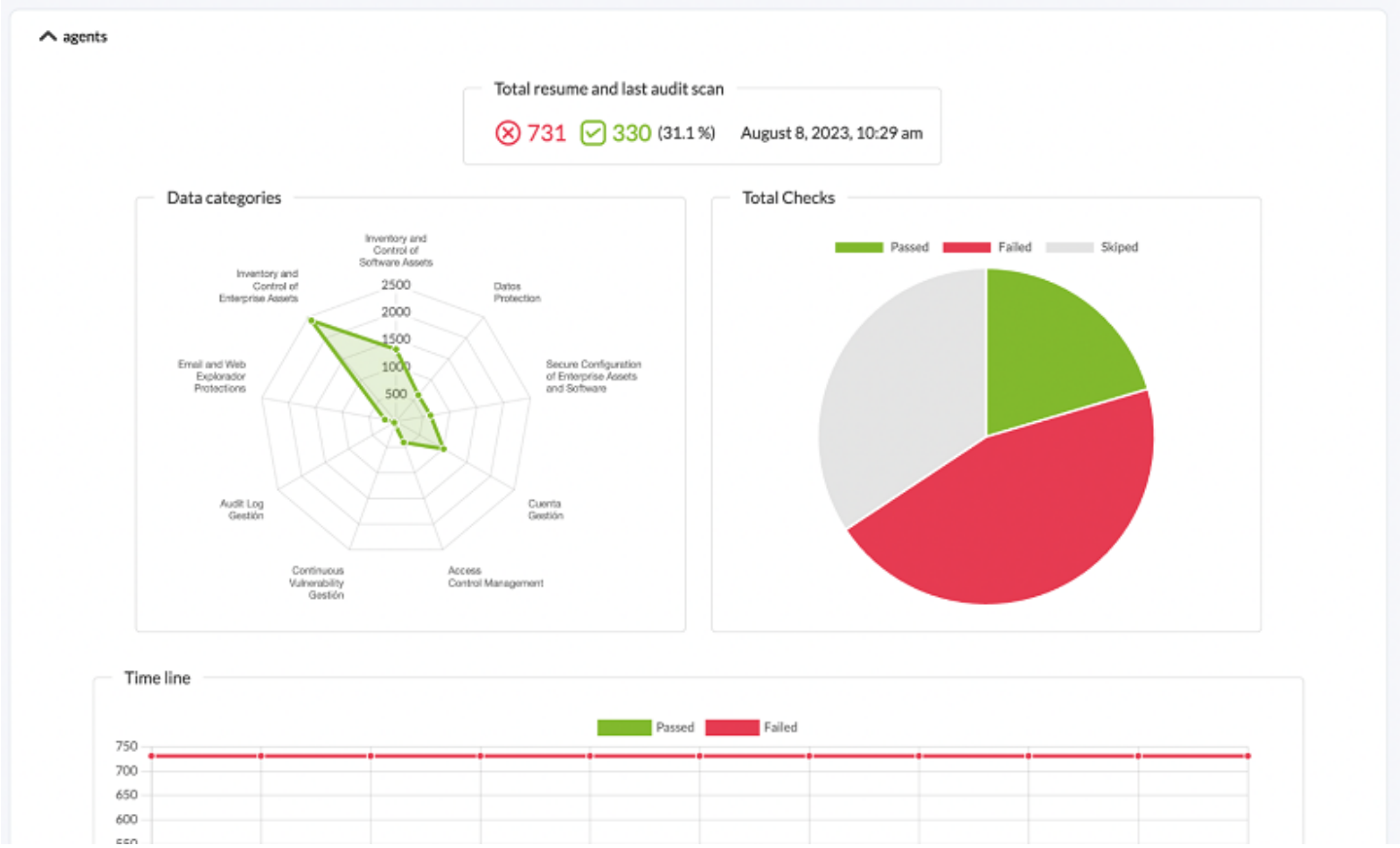
Defensa de límites y protección de datos: Identifica y separa los datos sensibles, y establece una serie de procesos que incluyan la codificación, planes de protección contra la infiltración de datos y técnicas de prevención de pérdida de datos. Establece barreras sólidas para prevenir el acceso no autorizado.

Supervisión y control de cuentas: Supervisa de cerca todo el ciclo de vida de sus sistemas y cuentas de aplicaciones, desde su creación hasta su eliminación, pasando por su uso e inactividad. Esta gestión activa previene que los atacantes se aprovechen de cuentas de usuarios legítimos pero inactivos para fines maliciosos y permite mantener un control constante sobre las cuentas y sus actividades.

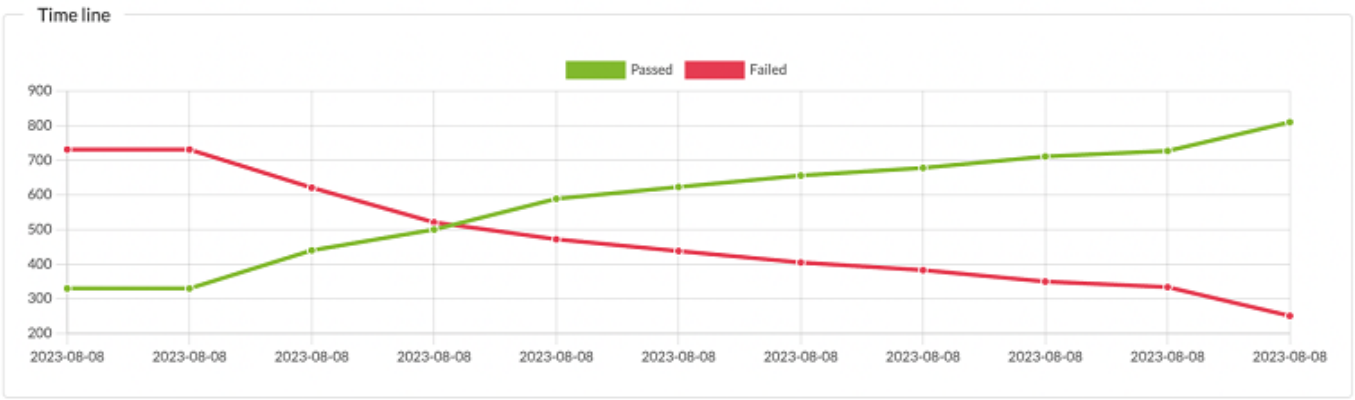
Auditorías de hardening detalladas de cada máquina

Los chequeos son realizados por el agente que corre en cada máquina. Habitualmente toma una auditoría cada semana, pero ese período puede ser configurado a más tiempo, por ejemplo un mes. De esta forma se puede tomar una *fotografía de la securización* del sistema, calcular y asignar un índice de seguridad (una valoración numérica, definida como el porcentaje de chequeos realizados y aprobados versus los chequeos que no pasan las pruebas) y ver la evolución de ese índice de seguridad a lo largo del tiempo.

Ejemplo de una “fotografía” del estado del *hardening* de un sistema:



Ejemplo de evolución del hardening de un sistema a lo largo del tiempo:



El sistema nos permite ver, desglosado por categorías, los chequeos que se han ejecutado:

Summary of categories

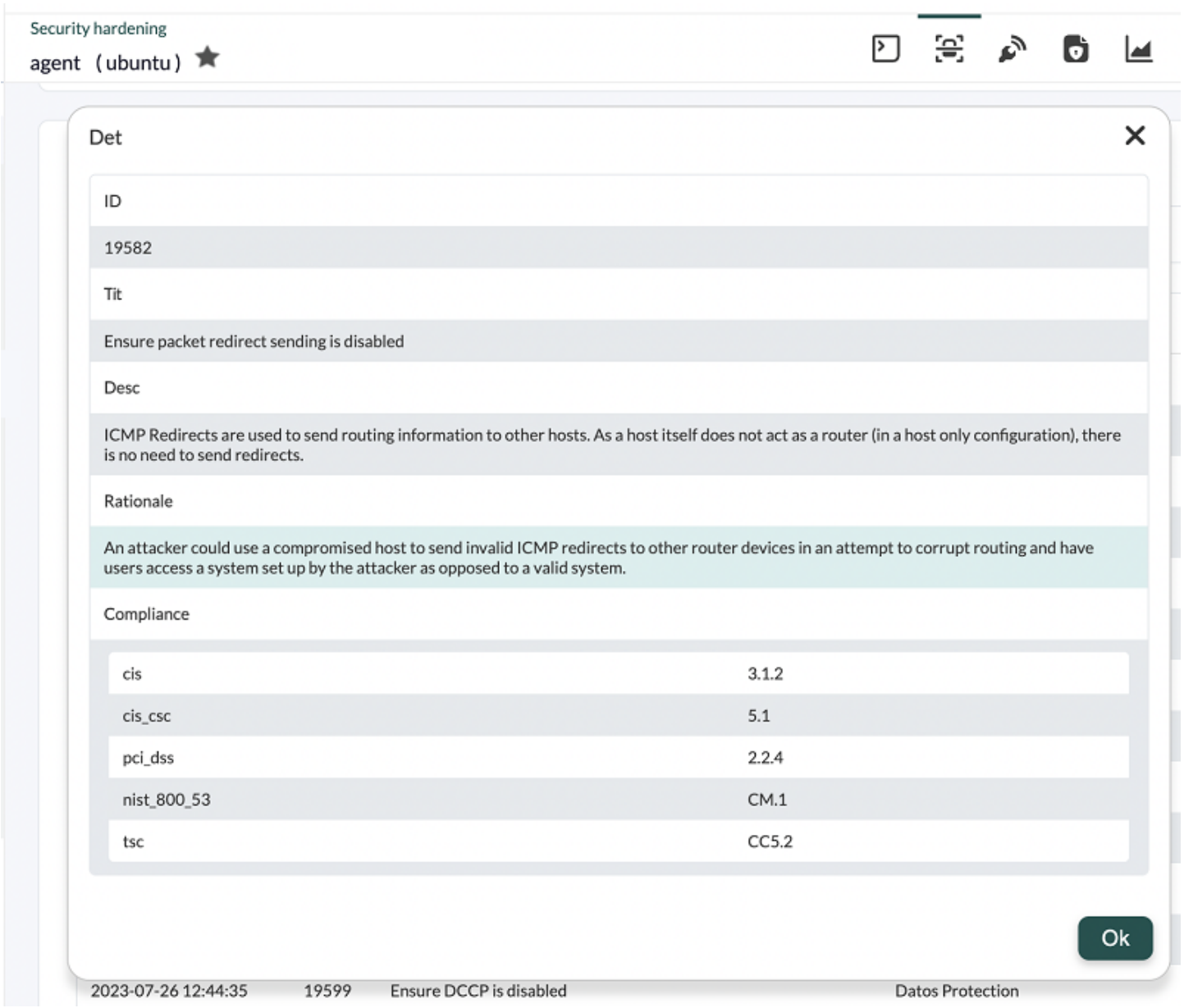
Inventory and Control of Software Assets	14	46	23 %
Data Protection	20	118	14 %
Secure Configuration of Enterprise Assets and Software	21	126	14 %
Account Management	78	193	29 %
Access Control Management	92	16	85 %
Continuous Vulnerability Management	8	14	36 %
Audit Log Management	0	20	0 %
Email and Web Browser Protections	6	20	23 %
Inventory and Control of Enterprise Assets	89	176	34 %

Y de cada grupo de elementos, ver el detalle, para poder trabajar sobre su corrección:

Results for audit on 2023-07-26 12:44:35

Filters

Date	ID	Title	Category	Status	Details
2023-07-26 12:44:35	19581	Ensure IP forwarding is disabled	Datos Protection		
2023-07-26 12:44:35	19582	Ensure packet redirect sending is disabled	Datos Protection		
2023-07-26 12:44:35	19583	Ensure source routed packets are not accepted	Datos Protection		
2023-07-26 12:44:35	19584	Ensure ICMP redirects are not accepted	Datos Protection		
2023-07-26 12:44:35	19585	Ensure secure ICMP redirects are not accepted	Datos Protection		
2023-07-26 12:44:35	19586	Ensure suspicious packets are logged	Datos Protection		
2023-07-26 12:44:35	19589	Ensure Reverse Path Filtering is enabled	Datos Protection		
2023-07-26 12:44:35	19590	Ensure TCP SYN Cookies is enabled	Datos Protection		
2023-07-26 12:44:35	19591	Ensure IPv6 router advertisements are not accepted	Datos Protection		
2023-07-26 12:44:35	19592	Ensure IPv6 redirects are not accepted	Datos Protection		
2023-07-26 12:44:35	19593	Ensure IPv6 is disabled	Datos Protection		
2023-07-26 12:44:35	19596	Ensure /etc/hosts.deny is configured	Datos Protection		
2023-07-26 12:44:35	19599	Ensure DCCP is disabled	Datos Protection		



Configuración de la monitorización de hardening

Se han desarrollado controles, dependiendo de cada sistema si son aplicables, que ayudarán a determinar si son relevantes en el entorno a monitorizar. Actualmente esta funcionalidad está disponible para servidores MS Windows® y GNU/Linux®. Está funcionalidad está disponible con los agentes 773 o posteriores. Si los agentes son de una versión anterior a 773 se deberán actualizar.

Para ello se tendrá que activar el *plugin* correspondiente en la configuración del agente. Se podrá realizar manualmente o a través de políticas de monitorización en grupos de máquinas.

En MS Windows®:

```
module_begin
module_plugin "%PROGRAMFILES%\Pandora_Agent\util\pandora_hardening.exe -t 150"
module_absoluteinterval 7d
module_end
```

GNU/Linux®:

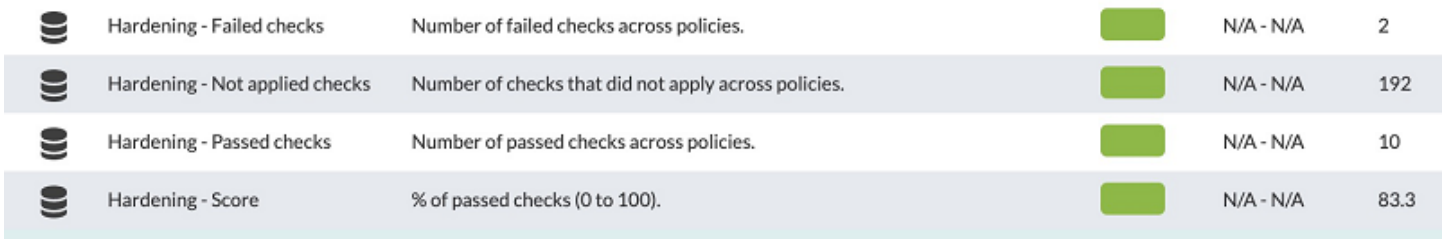
```
module_begin
module_plugin /usr/share/pandora_agent/plugins/pandora_hardening -t 150
module_absoluteinterval 7d
module_end
```

En estos ejemplos se ejecutará la auditoría de *hardening* cada 7 días, con un *timeout* de 150 segundos para cada comando que se lance durante la auditoría. Puede incrementar este valor a 30 días, pero no recomendamos que lo haga cada menos días pues generará datos innecesarios de inventario.

Monitorización de los datos de hardening

Además de *dashboard* y vistas específicas para poder analizar esos datos en sistemas concretos o a nivel global, se dispone de algunos módulos generados por el sistema de *hardening* que permitirán tratar los datos de la evaluación del *hardening* como otros datos de Pandora FMS, para establecer alertas, generar gráficas o cualquier otro uso que se necesite. Estos módulos son generados o actualizados automáticamente cada vez que se ejecuta una auditoría de *hardening* y pertenecen al Module group denominado Security.

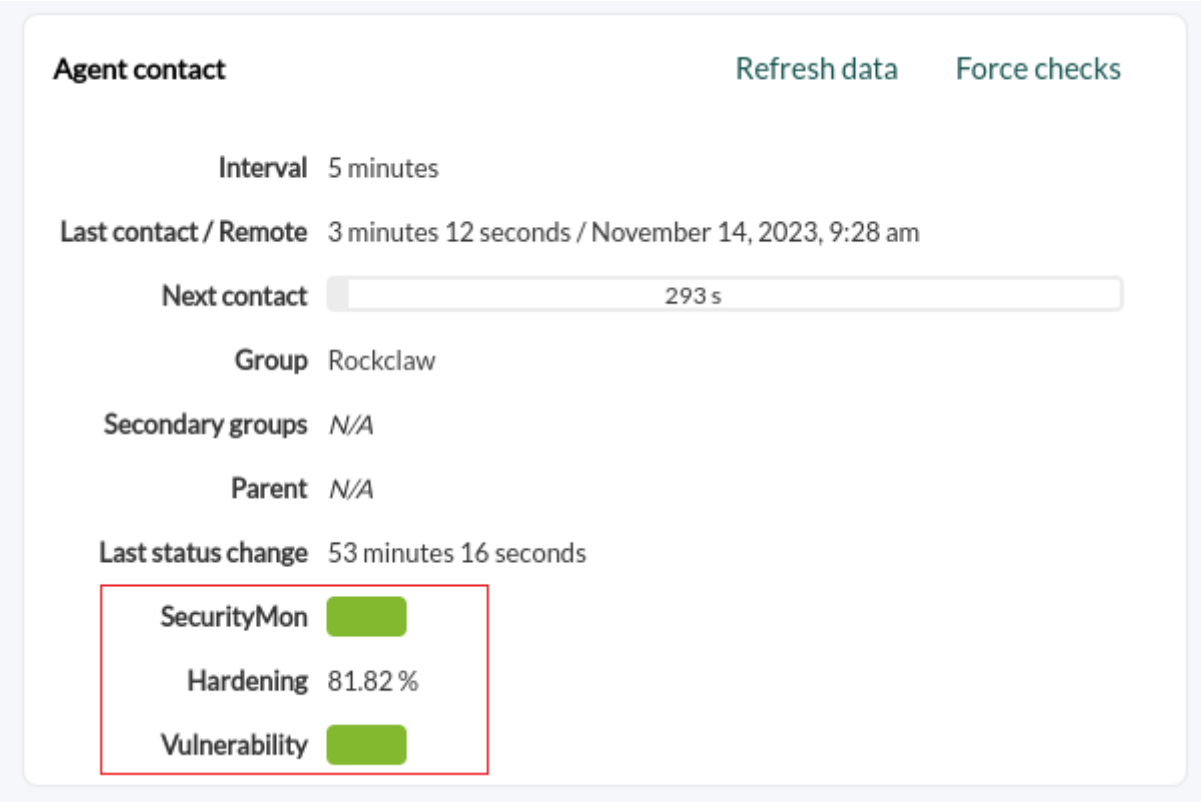
- Hardening - Failed checks: Muestra el número total de chequeos que no han pasado la prueba de *securización*.
- Hardening - Not applied checks:Muestra el número total de chequeos que no se han ejecutado porque no aplican (por ejemplo, chequeos para otra versión de su distribución Linux o versión Windows, o porque buscan un determinado componente que no está instalado).
- Hardening - Passed checks: Muestra el número total de chequeos que han pasado la prueba de *securización*.
- Hardening - Score: Muestra el porcentaje de los chequeos que han pasado. Se puede establecer un umbral aquí para mostrar cuando el sistema está en estado `Warning` o `Critical` respecto a la *securización*.



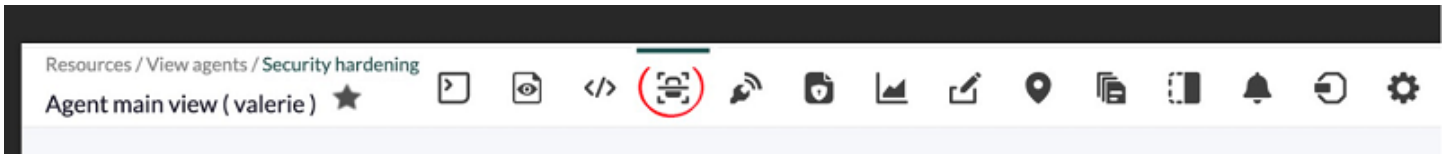
Visualización de los datos de hardening

Una vez que los agentes ejecuten por primera vez el módulo de *hardening*, la información llegará

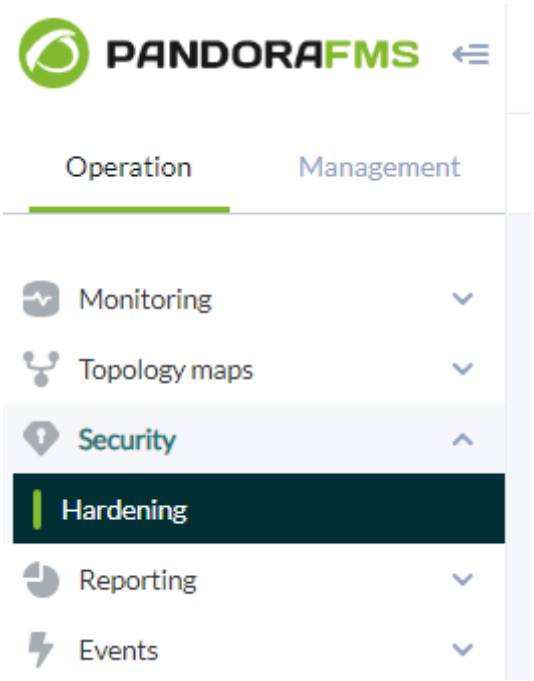
y se podrá ver en el detalle de cada agente (Operation → Monitoring views → Agent detail → Agent main view) en el cuadro Agent Contact tres elementos que resumen el estado de la seguridad (SecurityMon, al colocar el puntero encima mostrará el número de módulos de seguridad), el porcentaje de seguridad alcanzado (Hardening) y el estado de la vulnerabilidad (Vulnerability, al colocar el puntero encima mostrará el puntaje alcanzado):

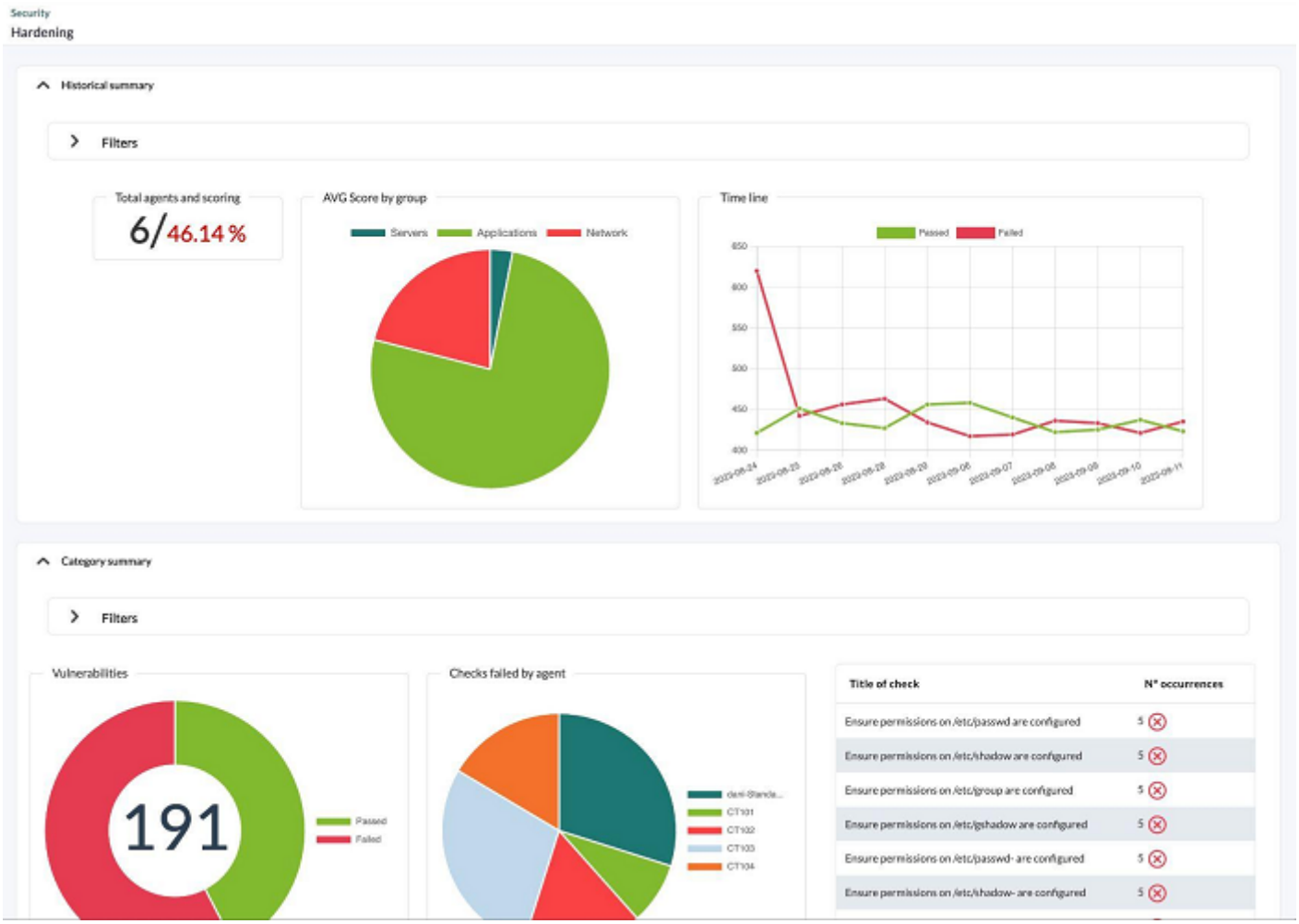


También se habilitará una sección específica para el *hardening* de dichos agentes:



Además, podrá ver una sección en el menú de operación llamada “Seguridad” (Security), donde existe un *dashboard* específico para los datos de Hardening donde podrá filtrar por grupos, agentes, categorías del CIS y otros detalles.





Informes de hardening

Se han creado nuevos tipos de informe para mostrar la información de *hardening*:

- Top N agentes con peor puntuación. Filtrada por grupos.
- Top N de chequeos que no pasan más frecuentes. Filtrada por grupos.

- Gráfica de tarta con Vulnerabilidades por tipo. Eligiendo una categoría CIS, se agrupan los *fails*, *passed* y *skipped* (opcional) de todos los agentes (o solo el grupo seleccionado) por categoría.
- Top N de chequeos que no pasan por categoría, se agrupan los últimos datos de todos los agentes (o solo el grupo seleccionado) por categorías del hardening y se listan las categorías con mayor número de *fails* entre todos los agentes.
- Listado de chequeos de *securización*, es un informe técnico y exhaustivo con todos los detalles, se listan los últimos chequeos de un agente filtrado por grupo, categoría y estado.
- Scoring, se muestran los últimos *scoring* de los agentes del grupo seleccionado o de todos dentro del rango de tiempo seleccionado en el filtro por defecto de los informes. Siempre se coge el último scoring de cada agente dentro del rango temporal, es decir si se coloca un rango de un mes, se buscará el último scoring de los agentes dentro de ese mes.
- Evolution, se muestra una evolución global del *hardening* haciendo la media de los *test* que han pasado y los que han fallado agrupando por día, de todos los agentes o de los que estén dentro del grupo seleccionado.

Estos son algunos ejemplos de informes en PDF:

PANDORAFMS ENTERPRISE

Test

T n agents Hardening: Top number of agents with the worst score

T n agents

Agent	Last audit scan	Score
DESKTOP-UUKUE87	September 21, 2023, 11:25 am	0.7 %
dani-Standard-PC-i440FX-PIIX-1996	September 21, 2023, 9:24 am	4.19 %
CT103	September 21, 2023, 9:24 am	17.06 %
CT104	September 21, 2023, 9:24 am	48.48 %
CT102	September 21, 2023, 9:23 am	54.21 %
CT101	September 21, 2023, 9:26 am	82.02 %

T most frequent Hardening: Top number most frequent failed checks

T most frequent

Title	Total Failed	Description
Ensure /etc/hosts.deny is configured	5	The /etc/hosts.deny file specifies which IP addresses are not permitted to connect to the host. It is intended to be used in conjunction with the /etc/hosts.allow file.
Verify permissions on /etc/hosts.allow	5	The /etc/hosts.allow file contains network information that is used by many system applications and therefore must be readable for these applications to operate.
Verify permissions on /etc/hosts.deny	5	The /etc/hosts.deny file contains network information that is used by many system applications and therefore must be readable for these applications to operate.
Ensure default deny firewall policy	5	A default deny all policy on connections ensures that any unconfigured network usage will be rejected.
Ensure loopback traffic is configured	5	Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8).
Ensure audit log storage size is configured	5	Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.
Ensure system is disabled when audit logs are full	5	The auditd daemon can be configured to halt the system when the audit logs are full.
Ensure audit logs are not automatically deleted	5	The max_log_file_action setting determines how to handle the audit log file reaching the max file size. A value of keep_logs will rotate the logs but never delete old logs.
Ensure events that modify date and time information are collected	5	Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimeofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier "time-change"
Ensure rsyslog default file permissions configured	5	rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.

Top n checks Hardening: Top number most frequent failed checks by category

Top n checks

Id	Category	Total Failed
1	Inventory and Control of Enterprise Assets	991
5	Account Management	777

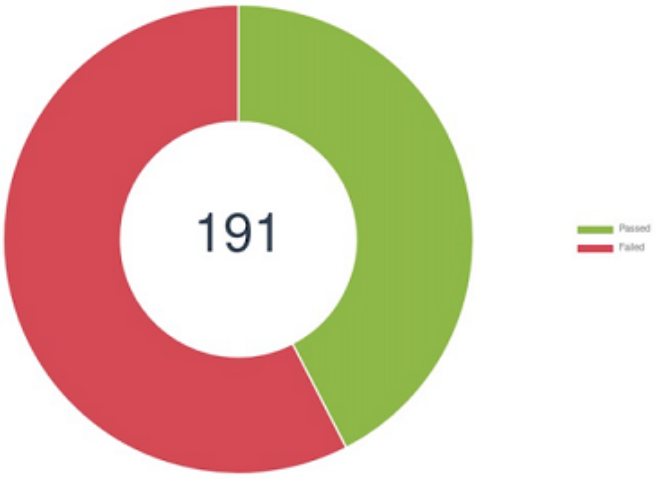
PANDORAFMS ENTERPRISE

Test

Top n checks

Id	Category	Total Failed
4	Secure Configuration of Enterprise Assets and Software	422
3	Data Protection	403
6	Access Control Management	328
2	Inventory and Control of Software Assets	261
9	Email and Web Browser Protections	104
8	Audit Log Management	45
7	Continuous Vulnerability Management	44

Vulnerabilities Hardening: Vulnerabilities of Access Control Management



List of checks Hardening: Checks of agent DESKTOP-UUKUE87 *September 21, 2023, 11:25 am*

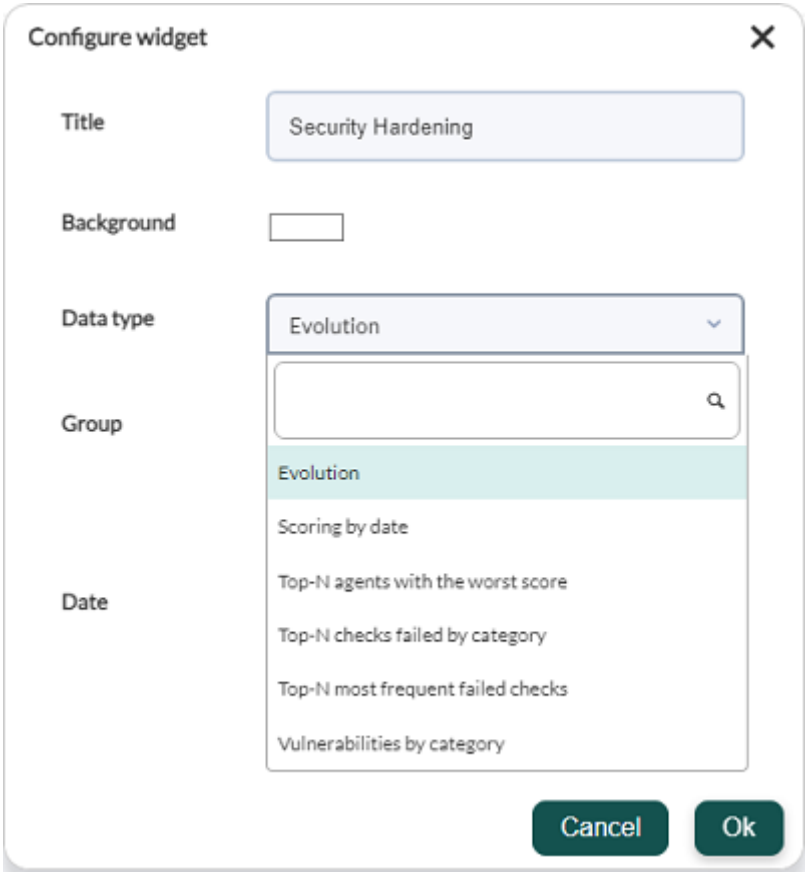
List of checks

Id	Title	Category	Status
12522	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies	Access Control Management	Skiped
13521	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies	Access Control Management	Skiped
12022	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies	Access Control Management	Skiped
11522	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies	Access Control Management	Skiped
13022	Ensure 'CLR Assembly Permission Set' is set to 'SAFE_ACCESS' for All CLR Assemblies	Access Control Management	Skiped
24533	Ensure 'EXECUTE' is revoked from 'PUBLIC' on File System Packages.	Access Control Management	Skiped
24536	Ensure 'EXECUTE' is revoked from 'PUBLIC' on Job Scheduler Packages.	Access Control Management	Skiped
24561	Ensure the 'USER' Audit Option Is Enabled.	Access Control Management	Skiped
24562	Ensure the 'ROLE' Audit Option Is Enabled.	Access Control Management	Skiped
24563	Ensure the 'SYSTEM GRANT' Audit Option Is Enabled.	Access Control Management	Skiped
24564	Ensure the 'PROFILE' Audit Option Is Enabled.	Access Control Management	Skiped
24565	Ensure the 'DATABASE LINK' Audit Option Is Enabled.	Access Control Management	Skiped
24566	Ensure the 'PUBLIC DATABASE LINK' Audit Option Is Enabled.	Access Control Management	Skiped
24567	Ensure the 'PUBLIC SYNONYM' Audit Option Is Enabled.	Access Control Management	Skiped

Dashboard de hardening

Un nuevo *widget* en los Dashboard de Pandora FMS agrupa la mayoría de informes de *hardening*:

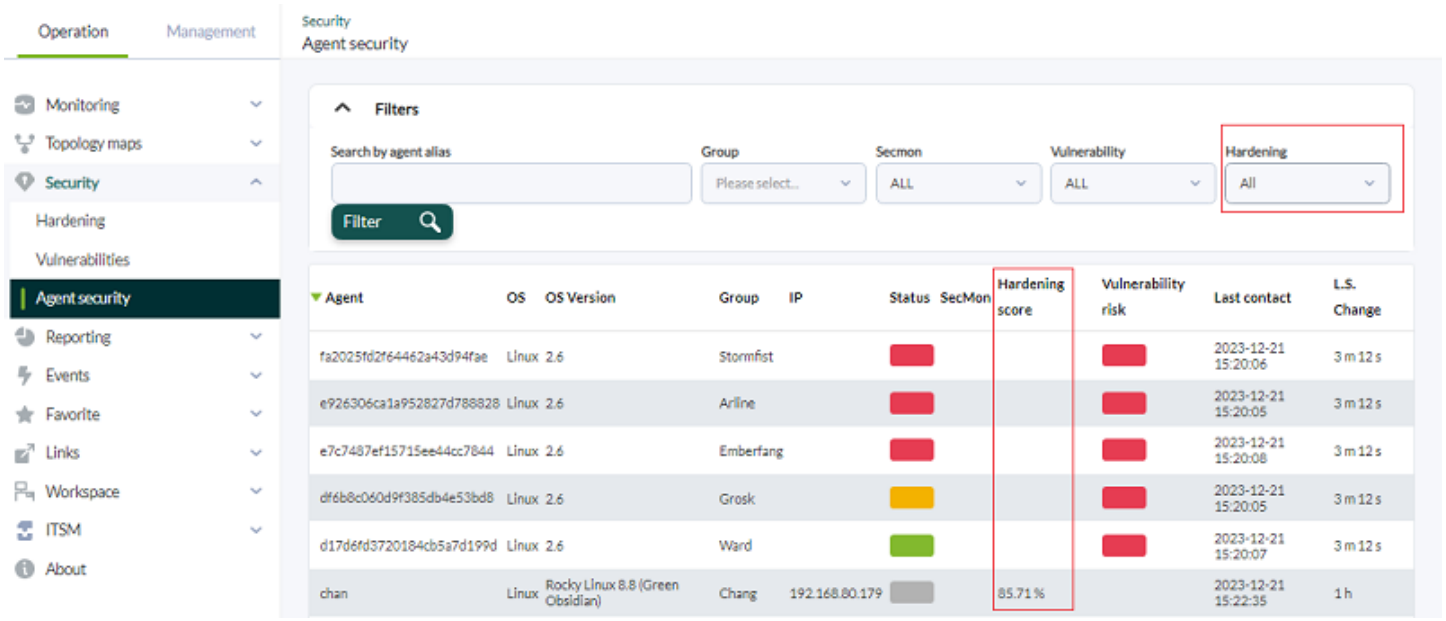
Opciones de configuración:



Vista de seguridad de los agentes

Menú Operation → Security → Agent security.

En la vista de seguridad de los agentes, columna Hardening, se podrá observar la puntuación de cada agente, entre otros datos. Se puede filtrar por porcentaje de puntuación de *hardening* e incluir otros campos adicionales. Para mostrar los agentes sin puntuación de *hardening* se utiliza la opción All.



Monitorización de vulnerabilidades

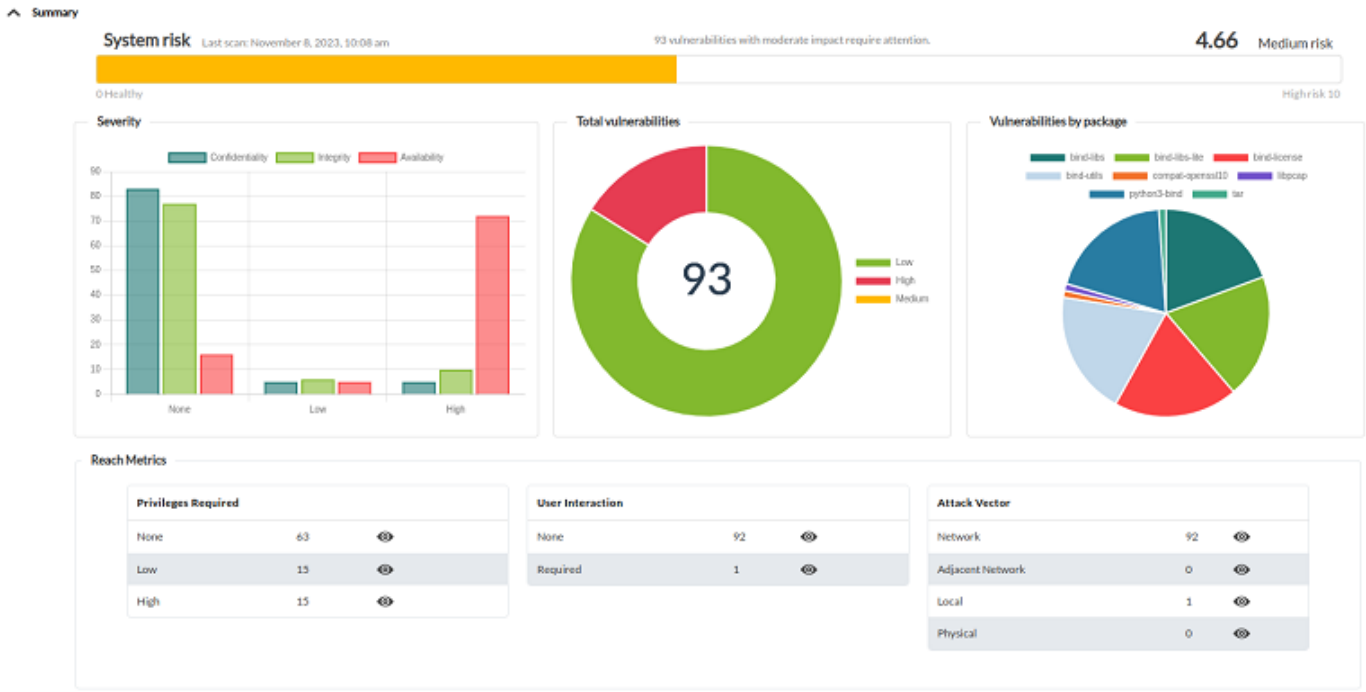
De manera similar a como se realiza la evaluación de *hardening*, los agentes de Pandora FMS y el motor de descubrimiento remoto buscarán información sobre el software instalado en el sistema, luego contrastará esta información con la BBDD central de vulnerabilidades que dispone Pandora FMS (descargada 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 agentes software (y estos agentes tienen activado el inventario de software) como si no dispone de agentes 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 agente.

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

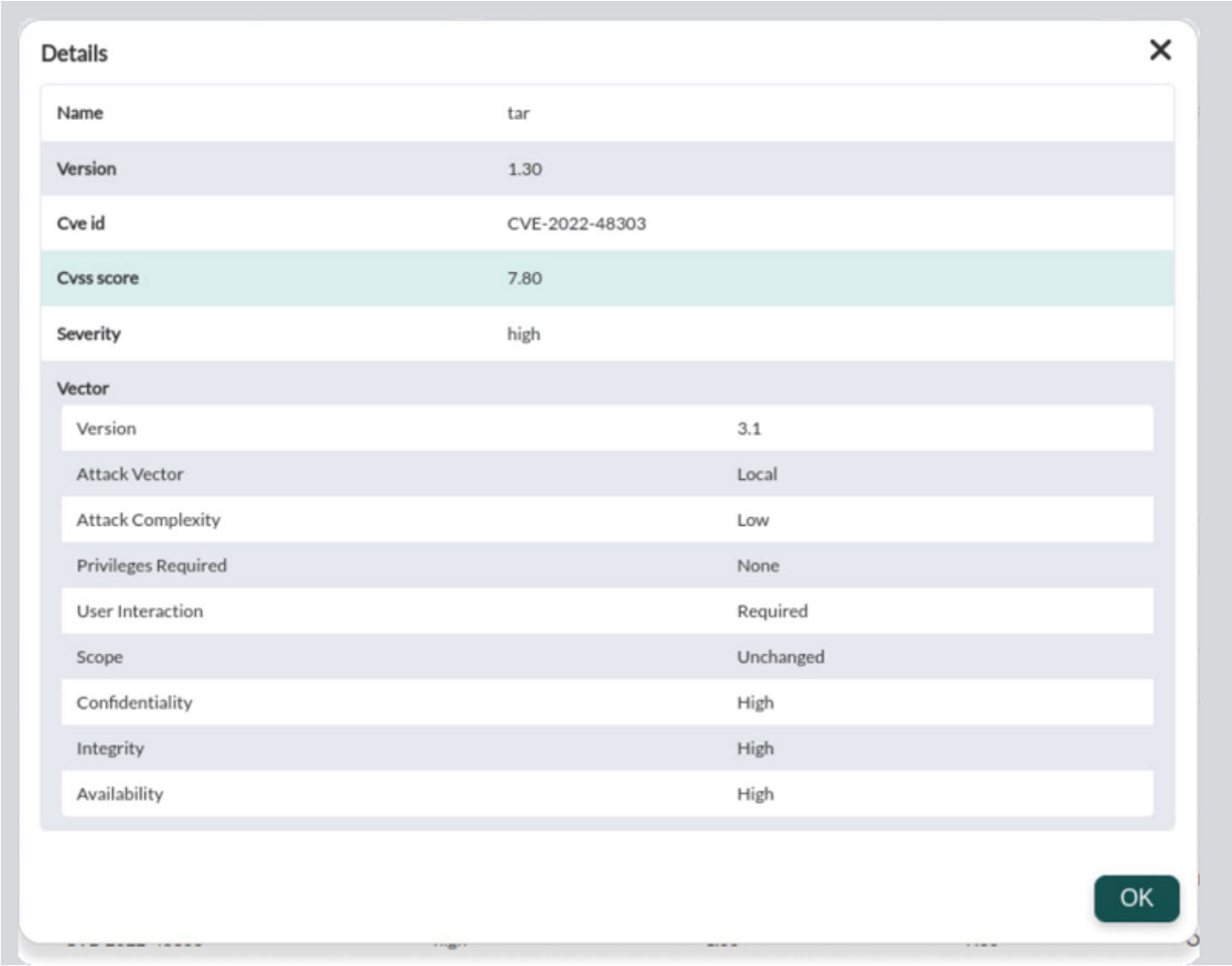
De manera similar a como funciona el *hardening*, Pandora FMS ofrecerá un indicador de riesgo único para cada sistema, basado en el número de vulnerabilidades y su peligrosidad.

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 BBDD 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 agentes de Pandora FMS.

Para la detección de vulnerabilidades mediante agentes, se utiliza una base de datos que se distribuye por defecto con el servidor Enterprise 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

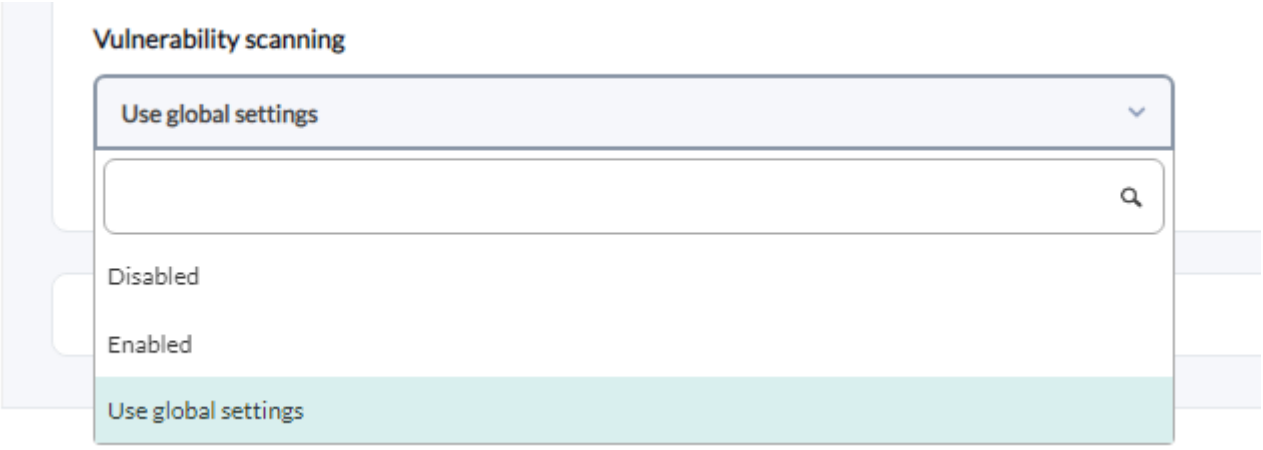
A nivel de servidor

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

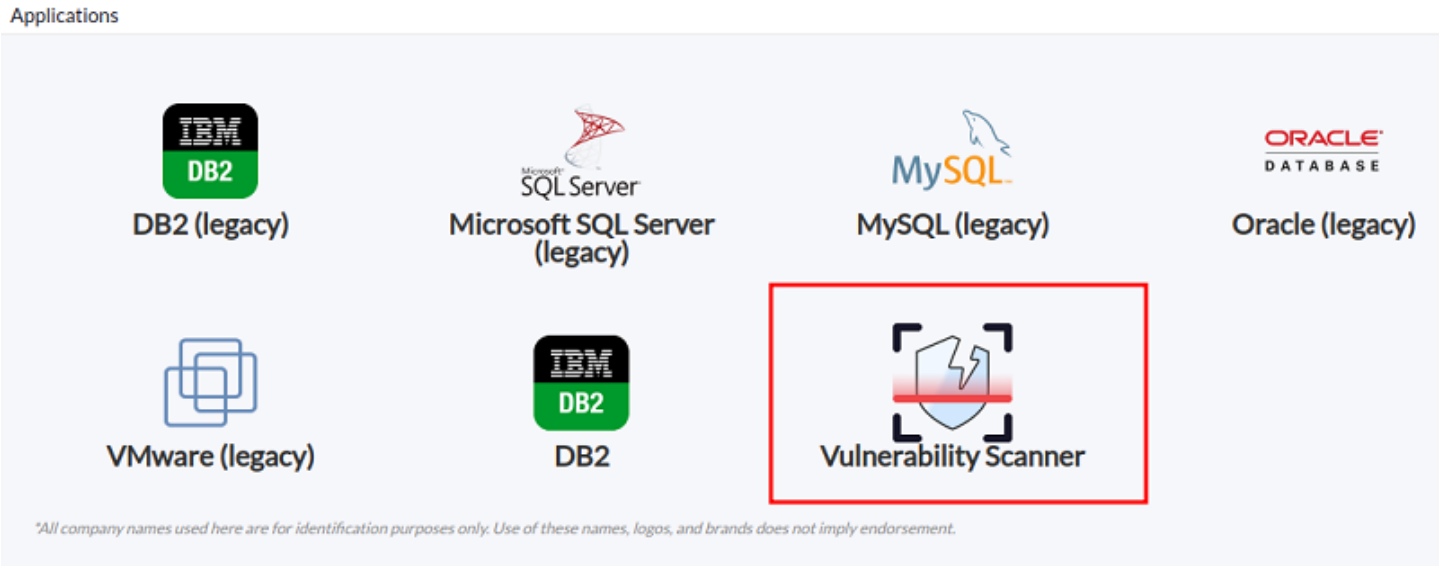
La configuración por defecto (global) se hace en el *setup*. Se puede desactivar o activar manualmente un agente o que utilice la configuración global del *setup*, en la sección de configuración avanzada.

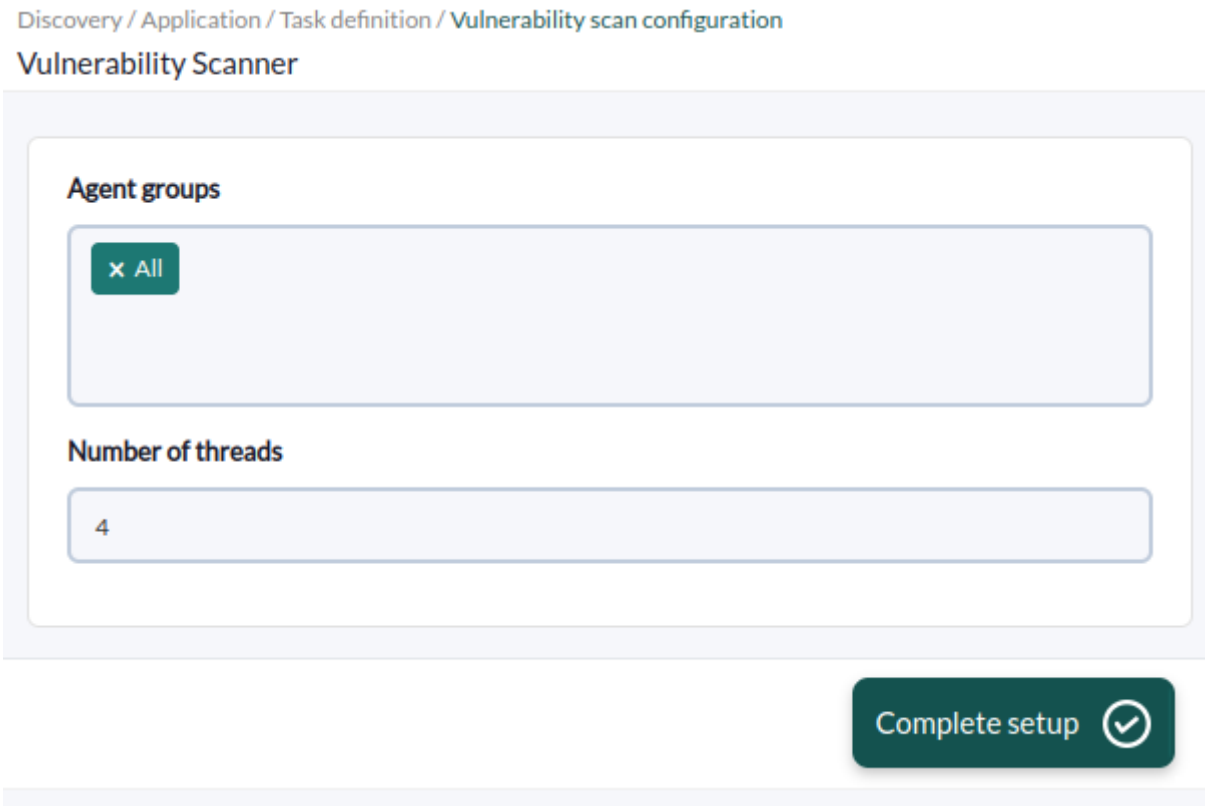


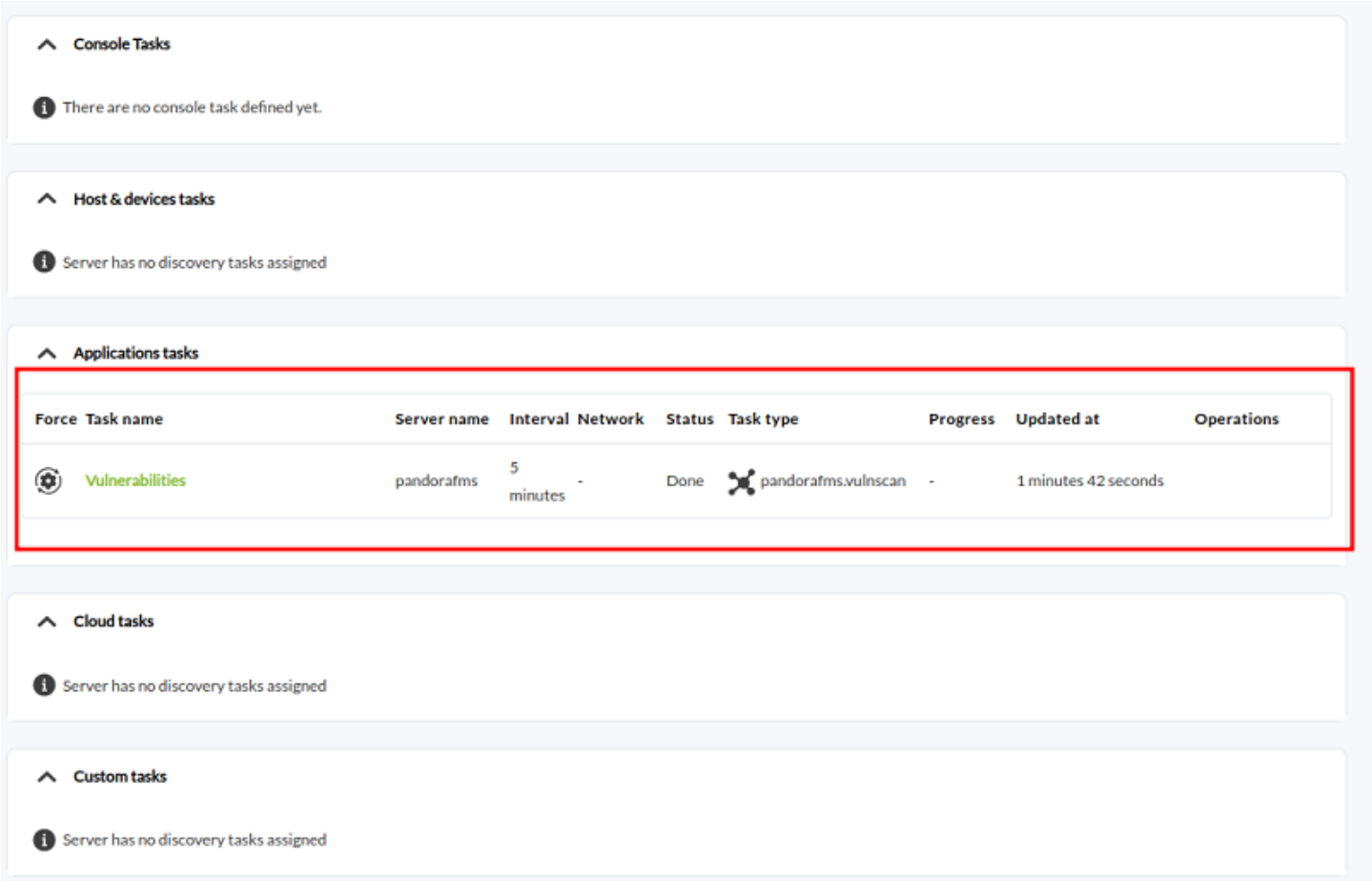
Tareas de escaneo remoto

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.







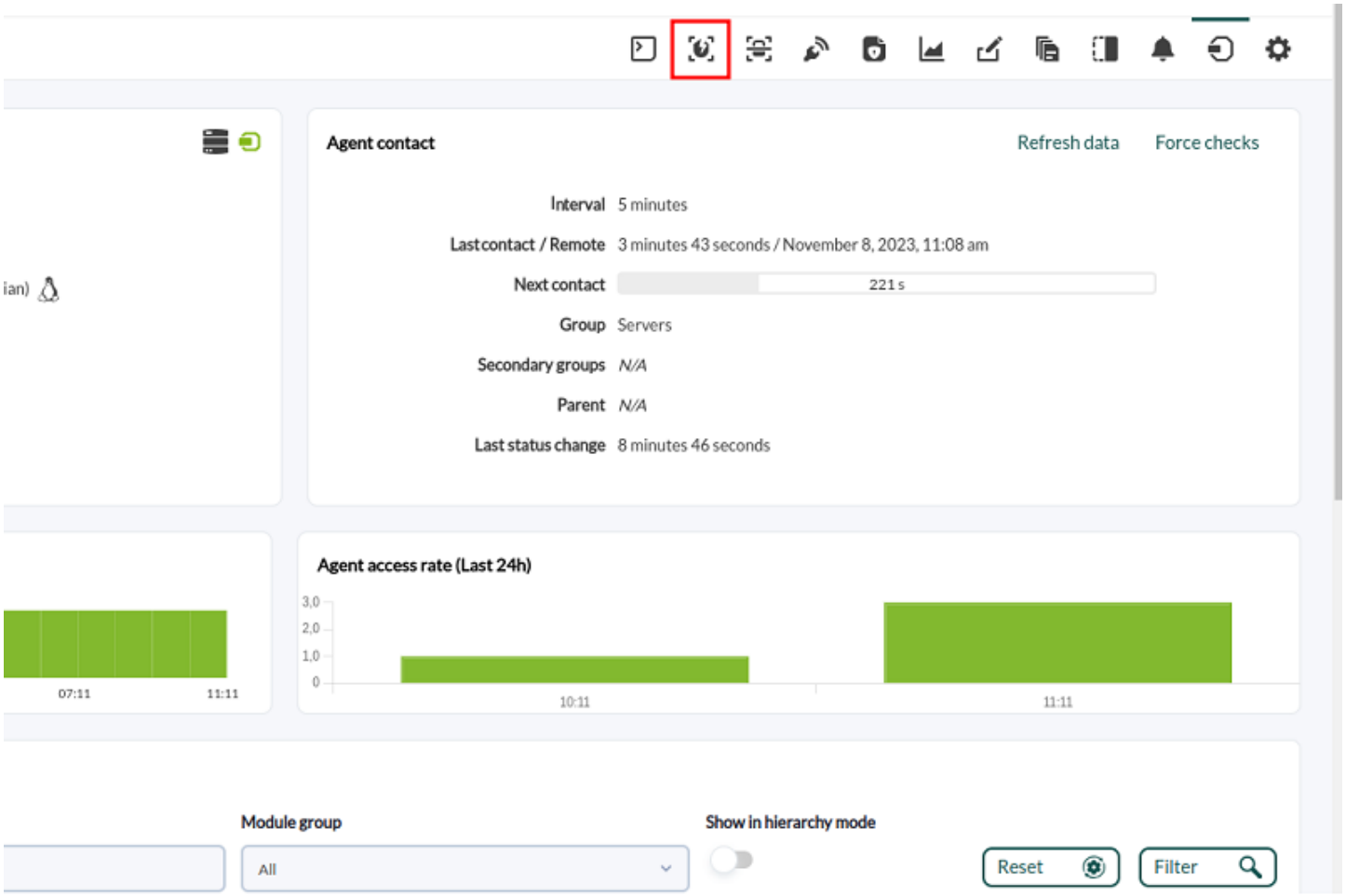
Visualización de los datos de vulnerabilidades

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...



Summary

System risk Last scan: November 8, 2023, 11:23 am

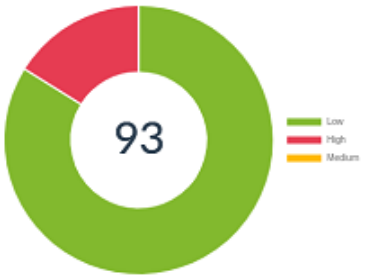
93 vulnerabilities with moderate impact require attention.

4.66 Medium risk

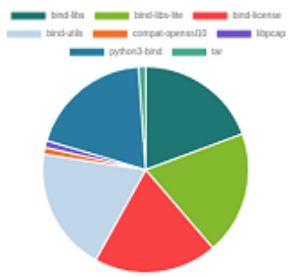
0 Healthy High risk 10

Severity

Total vulnerabilities



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	

Audit

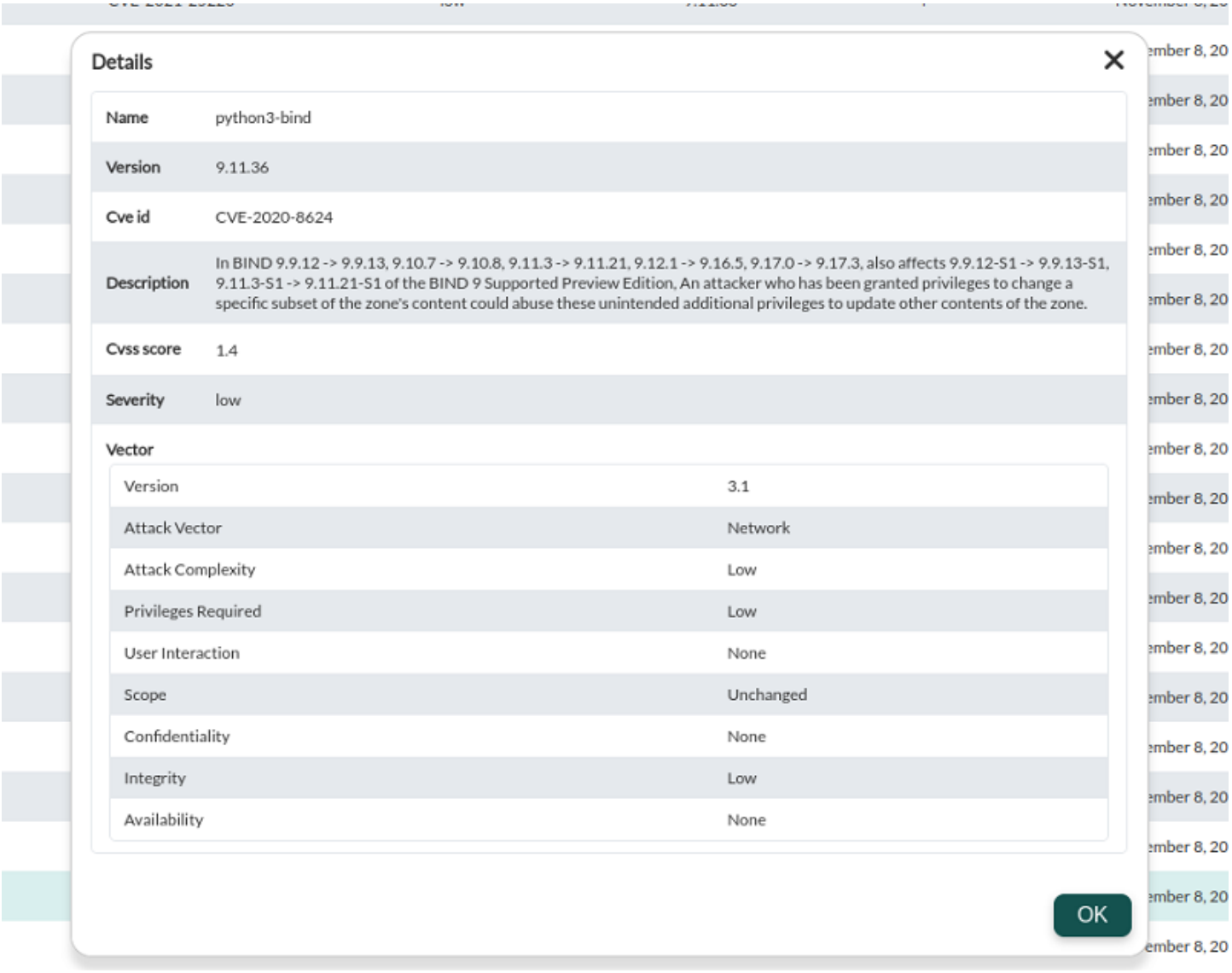
Filters

Detection Time: Last detection | Package: All | Severity: All | Attack Complexity: All | Privileges Required: All | User Interaction: All | Attack Vector: All

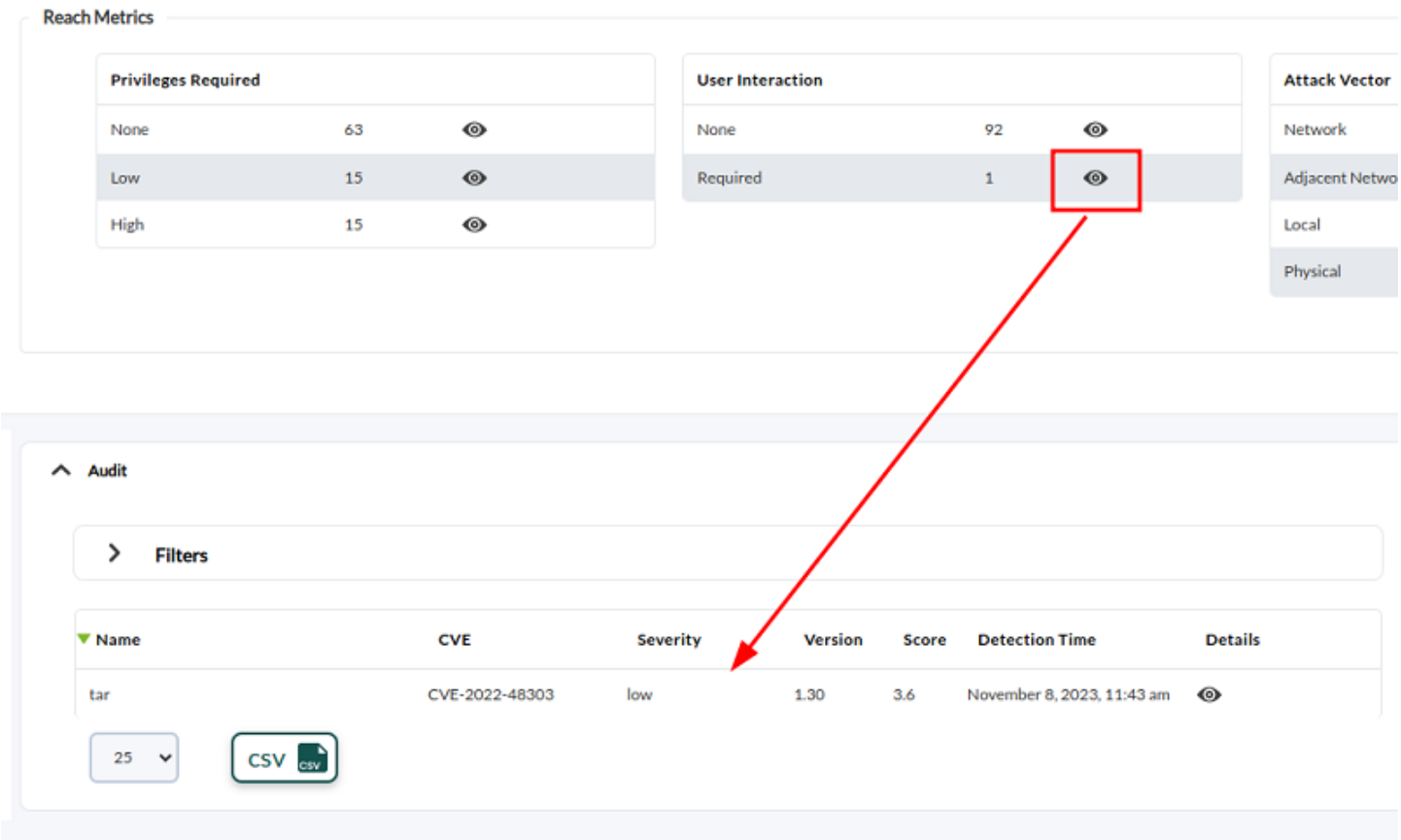
CVE

Filter

Name	CVE	Severity	Version	Score	Detection Time	Details
tar	CVE-2022-48303	low	1.30	3.6	November 8, 2023, 11:23 am	
python3-bind	CVE-2021-25220	low	9.11.36	4	November 8, 2023, 11:23 am	
python3-bind	CVE-2022-38177	low	9.11.36	3.6	November 8, 2023, 11:23 am	
python3-bind	CVE-2022-38178	low	9.11.36	3.6	November 8, 2023, 11:23 am	
python3-bind	CVE-2021-25219	low	9.11.36	1.4	November 8, 2023, 11:23 am	
python3-bind	CVE-2021-25214	low	9.11.36	3.6	November 8, 2023, 11:23 am	
python3-bind	CVE-2021-25215	low	9.11.36	3.6	November 8, 2023, 11:23 am	



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

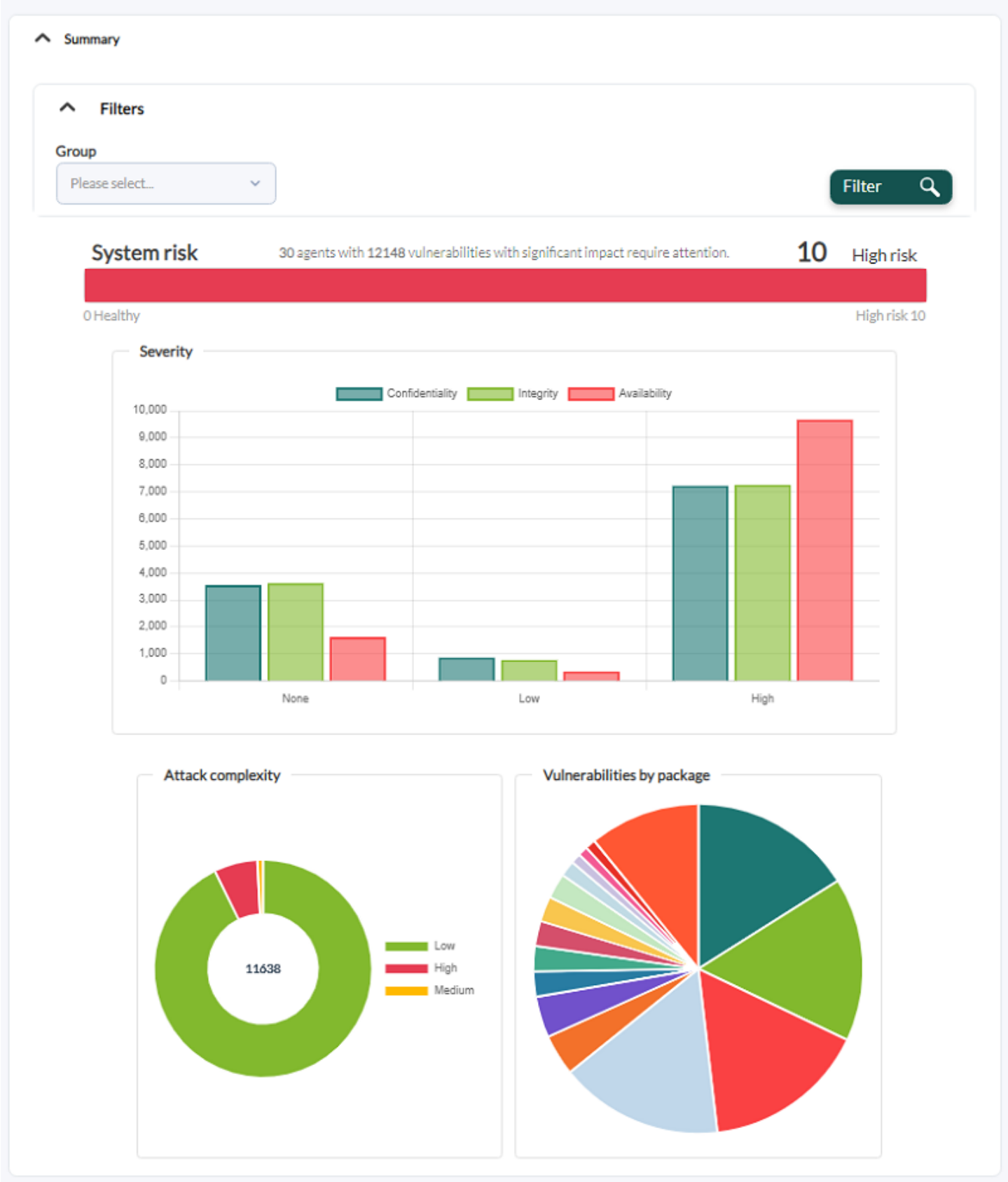


Vista táctica de seguridad

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.

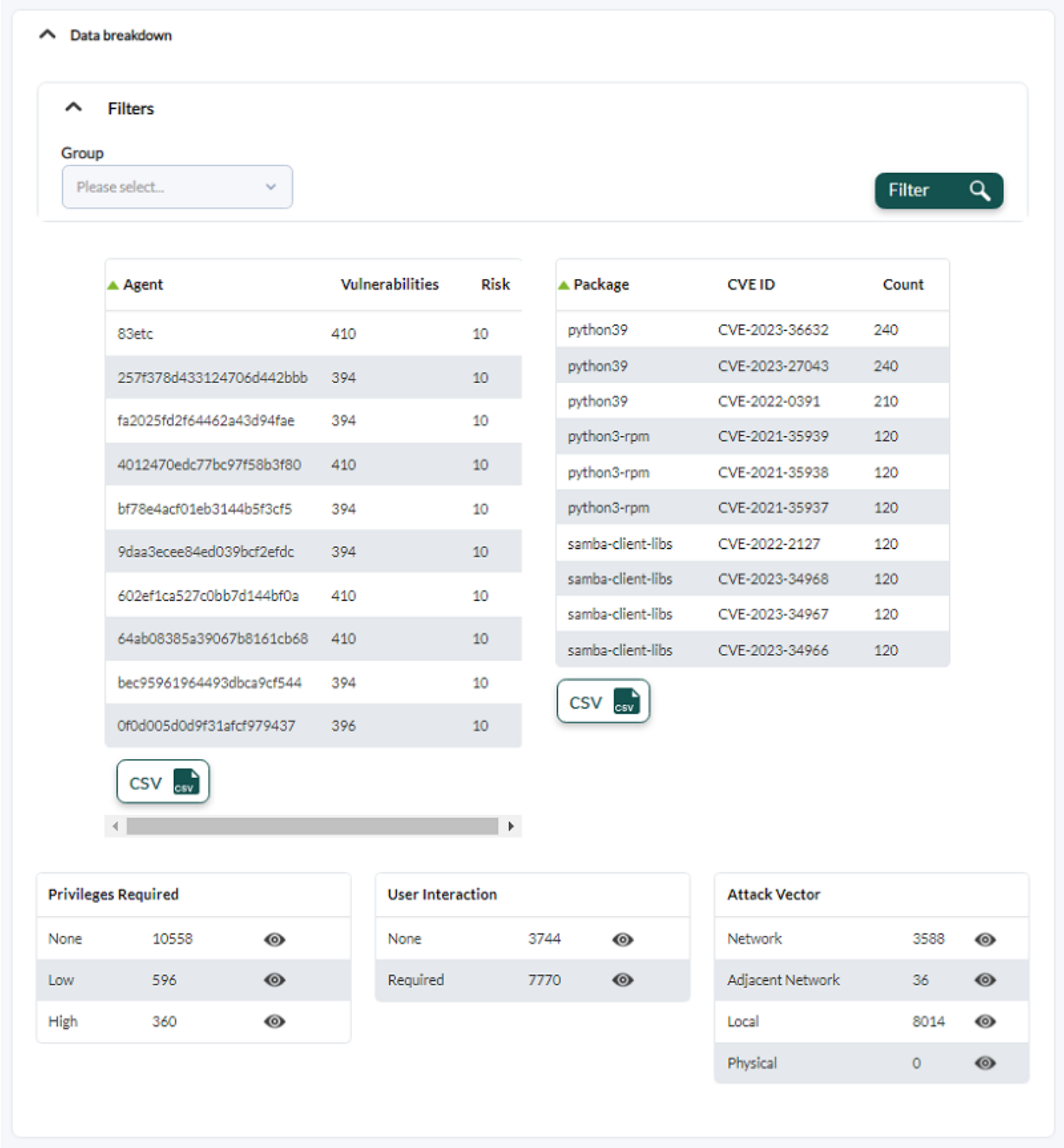


Se puede filtrar por grupo de agentes, por defecto presenta todos los grupos (All).

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