Détection des vulnérabilités

Détection des vulnérabilités

Supervision des vulnérabilités

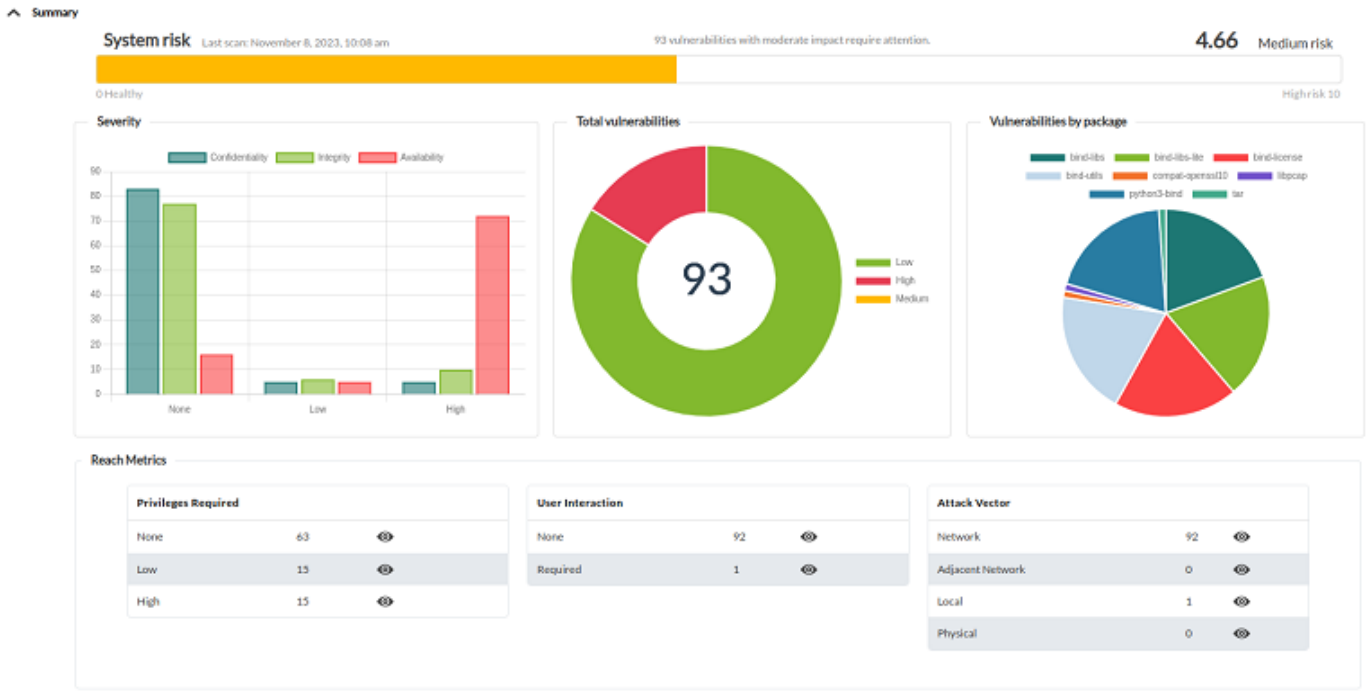
De la même manière que l'évaluation du renforcement est effectuée, les agents Pandora FMS et le moteur de découverte à distance rechercheront des informations sur les logiciels installés sur le système, puis compareront ces informations avec la base de données centrale de vulnérabilités de Pandora FMS (téléchargée depuis NIST, Mitre et autres sources) et fournira une liste de progiciels présentant des vulnérabilités connues.

Cette fonctionnalité est disponible que vous disposiez d'EndPoints (et que l'inventaire logiciel soit activé sur ces agents) ou si vous n'avez pas d'agents et devez effectuer une découverte sur le réseau. Si la découverte se fait via le réseau, les informations fournies seront bien moindres. Il est recommandé d'utiliser un agent.

N'importe quel agent version 7 peut être utilisé pour cela à condition que son inventaire logiciel soit activé. Ce système fonctionne pour les systèmes Linux® et MS Windows®.

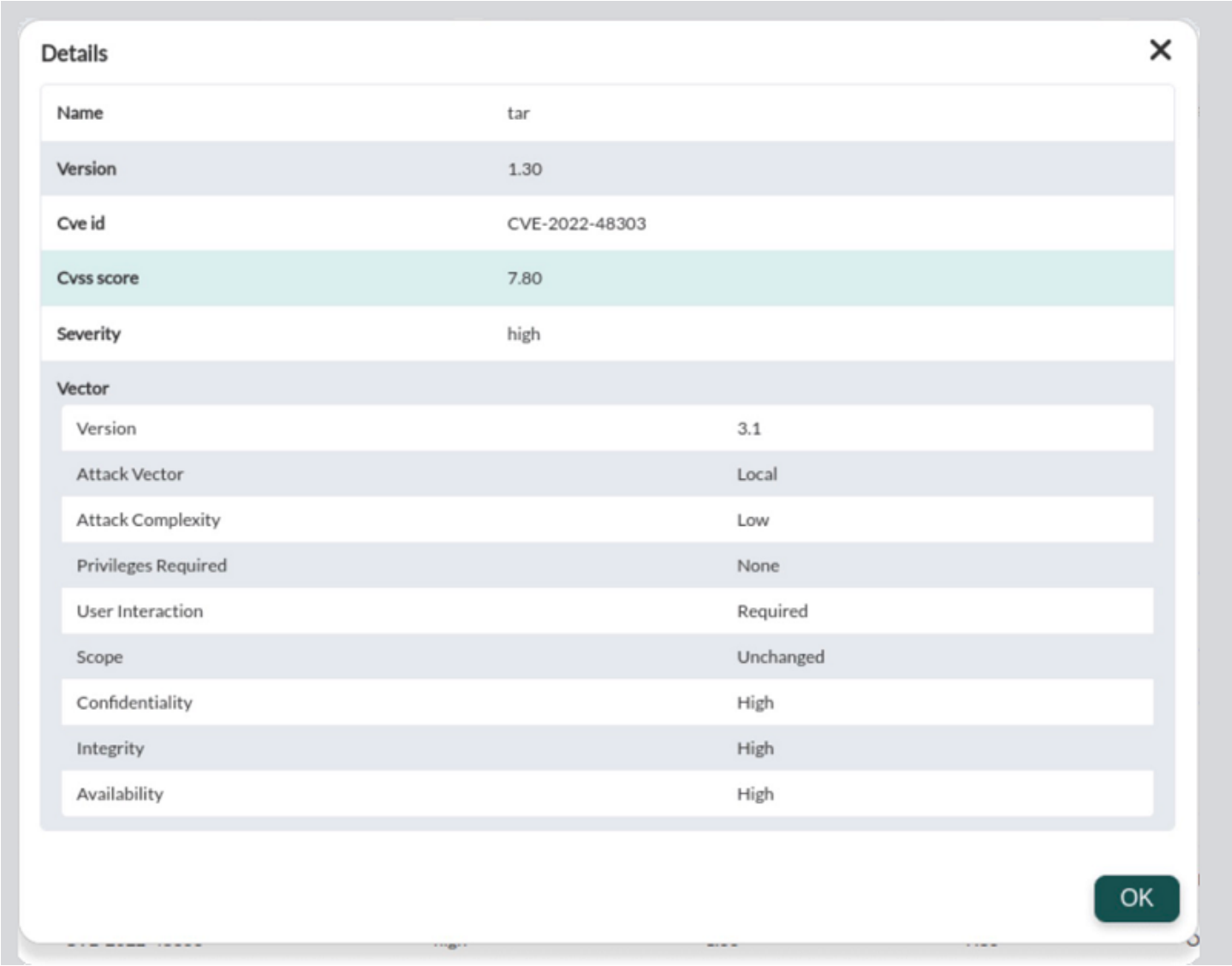
De la même manière que le renforcement, Pandora FMS proposera un indicateur de risque unique pour chaque système, basé sur le nombre de vulnérabilités et leur dangerosité.

Il fournira un panneau d'information sur les vulnérabilités du système, indiquant l'évolution du risque dans le temps, les vulnérabilités classées selon différents critères, tels que la complexité de l'attaque, la gravité, le type de vulnérabilité, le vecteur d'attaque, l'interaction de l'utilisateur, le type de privilèges requis, etc.



Vous pouvez naviguer dans le panneau de configuration pour filtrer les informations et atteindre un niveau de détail où est spécifié chaque progiciel vulnérable, la vulnérabilité (avec code CVE) qui s'y applique et la description du problème:

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	



Qu'est-ce qu'un CVE ?

Les Common Vulnerabilities and Exposures (CVE) sont une identification unique et standardisée d'une vulnérabilité de sécurité logicielle ou matérielle. Les CVE sont un système de nommage et de suivi utilisé dans le monde entier pour identifier et répertorier des vulnérabilités de sécurité spécifiques. Ce système a été créé pour faciliter l'organisation, la communication et la référence des informations sur les vulnérabilités, permettant ainsi à la communauté de la cybersécurité et aux professionnels de l'informatique d'aborder et de résoudre les problèmes de sécurité plus efficacement.

Les principales caractéristiques d’un CVE sont les suivantes:

- Identification unique: Chaque CVE possède un numéro unique qui l'identifie, ce qui facilite son suivi et sa référence. Par exemple, un CVE peut avoir un format tel que « CVE-2021-12345 ».
- Description détaillée: Chaque CVE comprend une description détaillée de la vulnérabilité, permettant aux utilisateurs de mieux comprendre la nature et l'impact du problème.
- Références croisées: Les CVE incluent souvent des références croisées à d'autres ressources et bases de données de sécurité, telles que la Institut national des normes et de la technologie (NIST) National

Vulnerability Database (NVD), pour fournir des informations supplémentaires sur la vulnérabilité.
- Date de publication: Les CVE incluent généralement la date à laquelle les informations sur la vulnérabilité ont été publiées.

Les CVE sont utilisés par l'industrie de la sécurité informatique, les fournisseurs de logiciels et de matériel et les chercheurs en sécurité et les administrateurs système pour suivre et gérer les vulnérabilités. Cette nomenclature standardisée est essentielle pour garantir que les vulnérabilités sont communiquées et traitées de manière cohérente dans le monde entier, contribuant ainsi à protéger les organisations et les utilisateurs finaux contre les menaces de sécurité. De plus, l'existence de CVE facilite la création de bases de données et d'outils permettant aux organisations de se tenir au courant des dernières menaces et d'appliquer des correctifs ou des solutions de sécurité si nécessaire.

La base de données des vulnérabilités Pandora FMS

La base de données de vulnérabilités Pandora FMS s'appuie sur deux sources:

- CVE-Search qui combine les données de NVD NIST, MITRE et Red Hat.
- Informations directes des référentiels de mises à jour de sécurité Canonical, Red Hat, Debian, Arch Linux, NVD NIST et Microsoft.

Le serveur Pandora construit sa propre base de données à partir de ces données, les segmente et les indexe en mémoire pour une détection rapide, afin de charger uniquement les vulnérabilités correspondant aux systèmes d'exploitation signalées par les agents Pandora FMS.

Pour détecter les vulnérabilités à l'aide d'agents, on utilise une base de données distribuée par défaut avec le serveur PFMS et qui associe les noms de packages et d'applications à différents CVE. Pour détecter les vulnérabilités à distance, une base de données est utilisée qui associe les CPE aux CVE. La console utilise une base de données contenant des informations sur les différents CVE trouvés dans la base de données du serveur pour les afficher à l'utilisateur et générer des rapports. Les données des différents CVE sont chargées dans la table `tpandora_cve`, qui existe depuis la version 774.

Configuration de l'audit de vulnérabilité

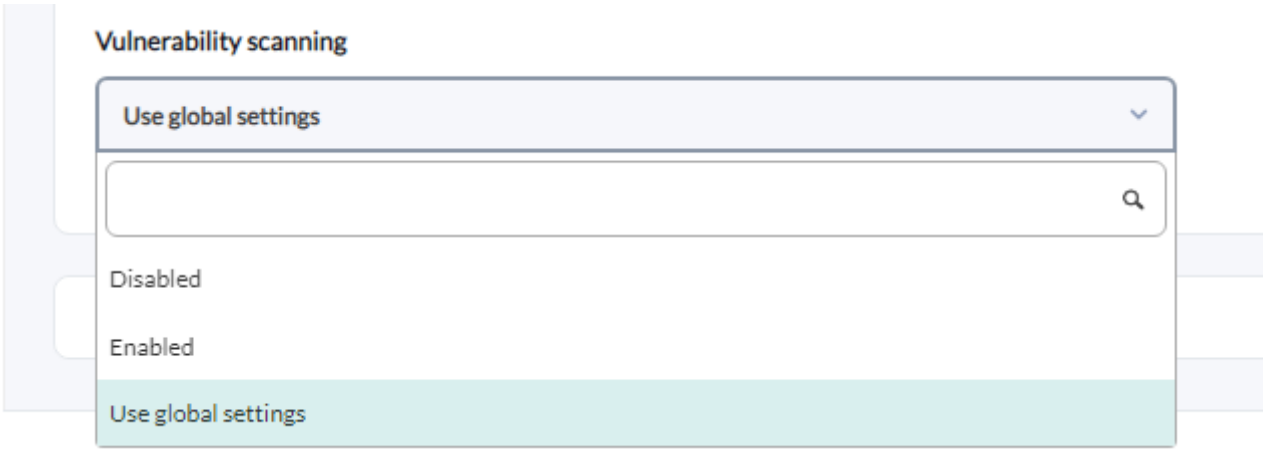
Au niveau du serveur

Pour la détection locale des vulnérabilités, le Data Server doit être activé et les agents doivent envoyer un logiciel d'informations d'inventaire.

Pour que la détection des vulnérabilités à distance fonctionne, le serveur Discovery doit être activé.

Au niveau de l'agent

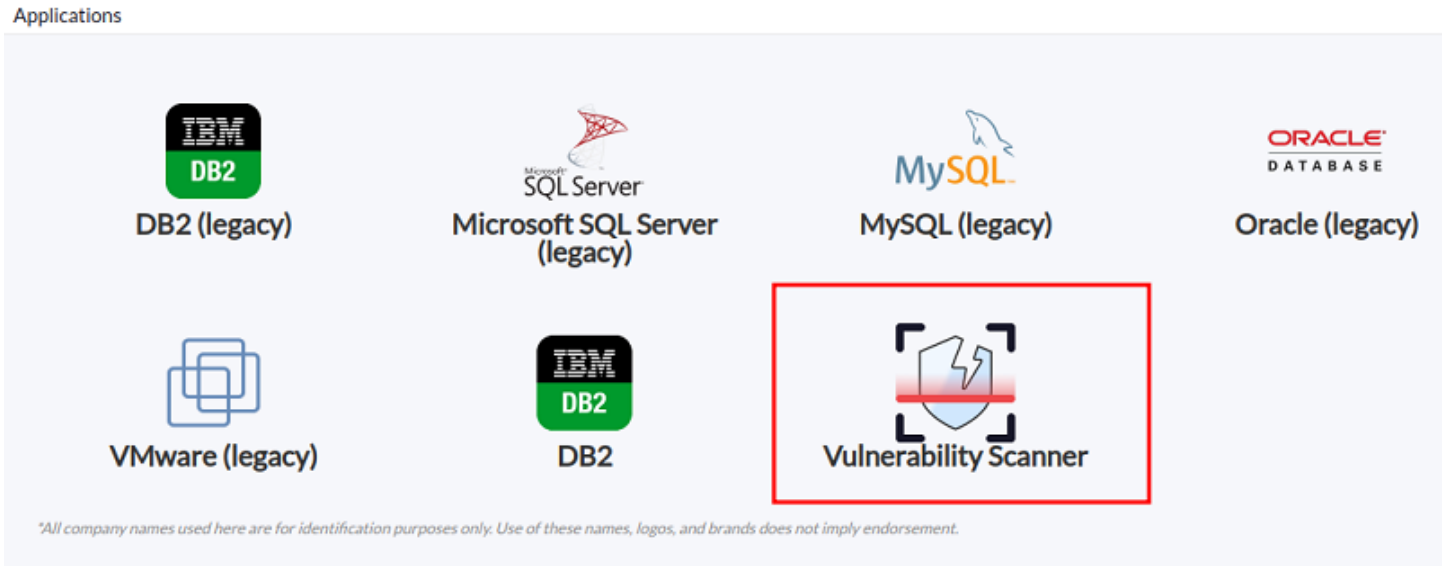
Vous pouvez désactiver ou activer manuellement un agent ou utiliser (par défaut) la configuration globale du *setup*, dans la section de configuration avancée.

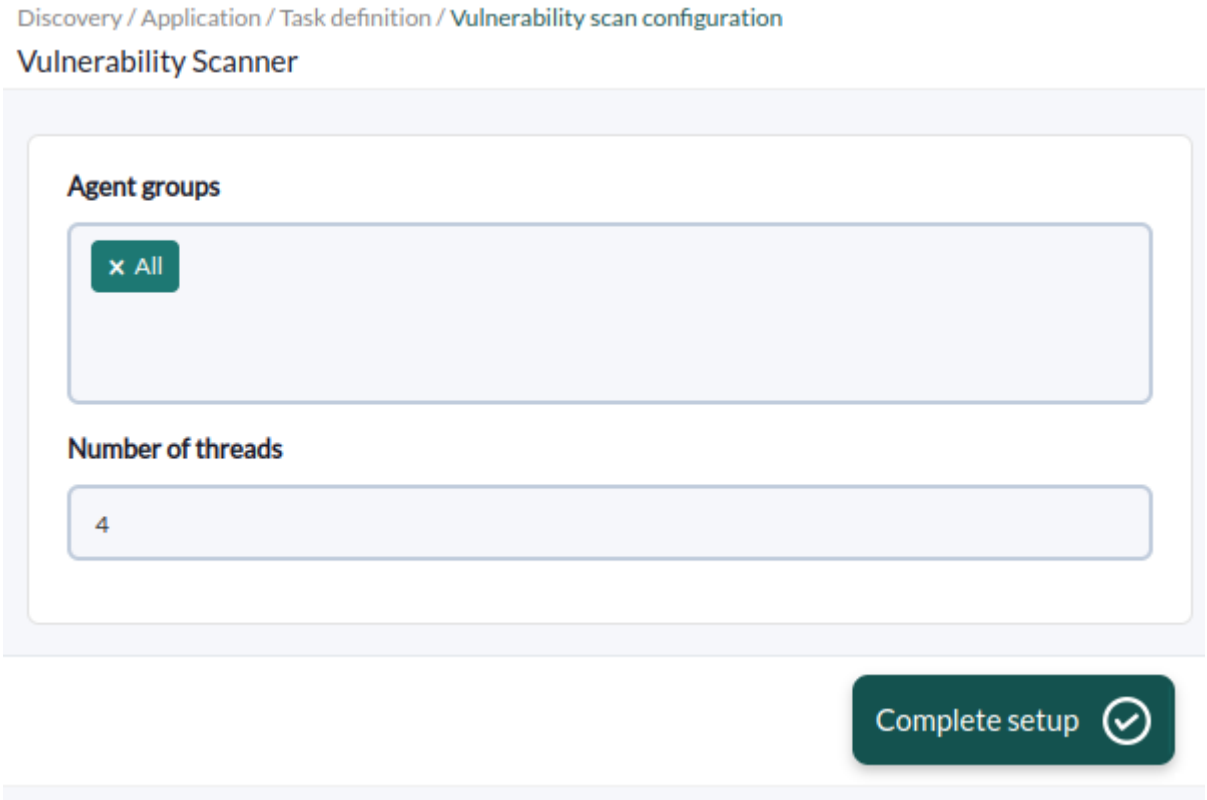


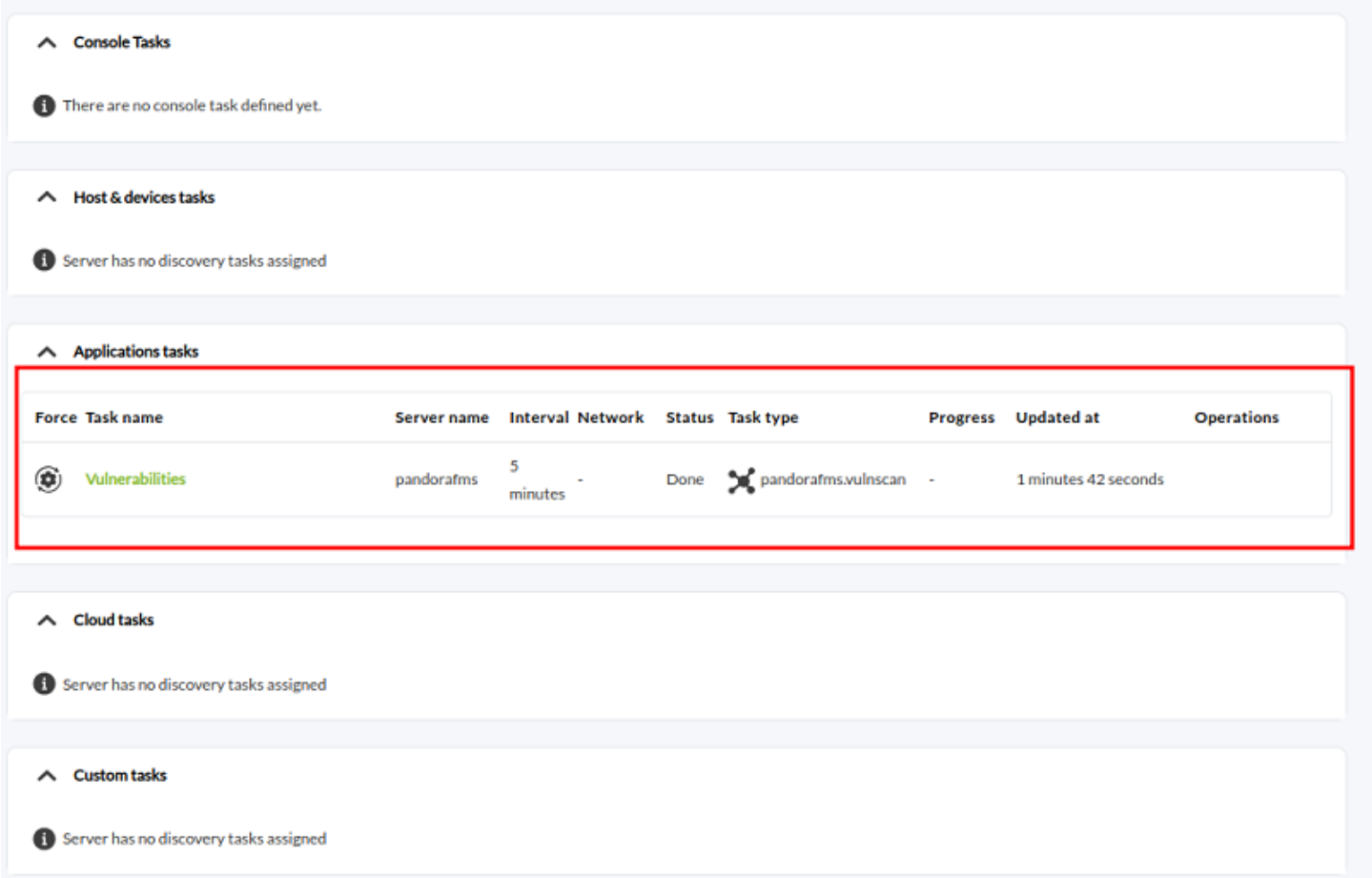
Tâches d'analyse à distance

Pour ce faire, vous devez vous rendre sur Discovery et lancer une nouvelle tâche de découverte de vulnérabilité. Il vous sera demandé un ou plusieurs groupes de machines déjà existantes dans la supervision pour lancer la détection de vulnérabilités sur celles-ci. L'adresse IP principale de ces agents sera utilisée pour lancer le scan. Si vous n'avez pas de supervision ou s'ils n'existent pas dans Pandora FMS, ils doivent d'abord être détectés avec une détection de réseau de découverte normale.

L'analyse des vulnérabilités ne créera pas de nouveaux agents.


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



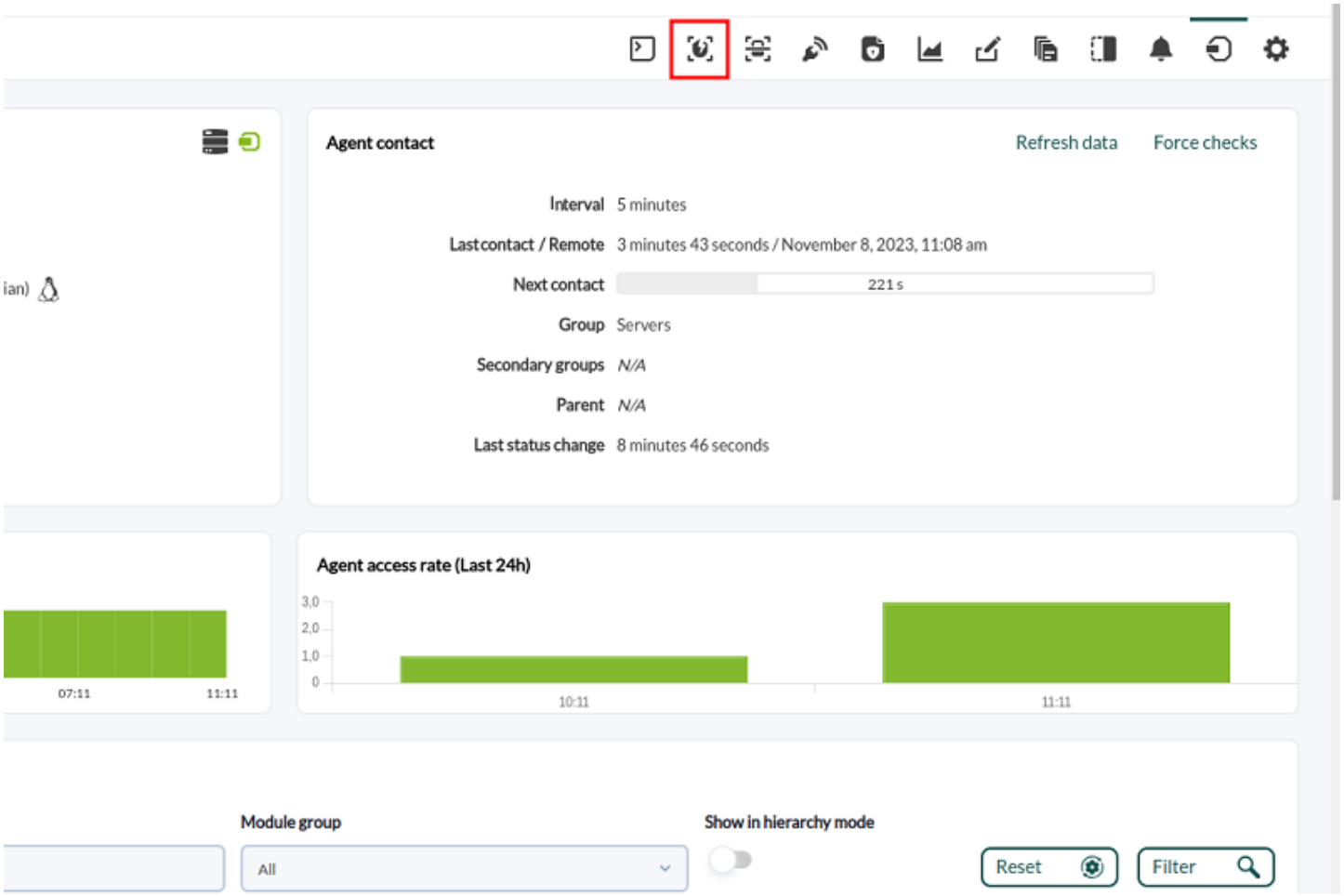
Affichage des données de vulnérabilité

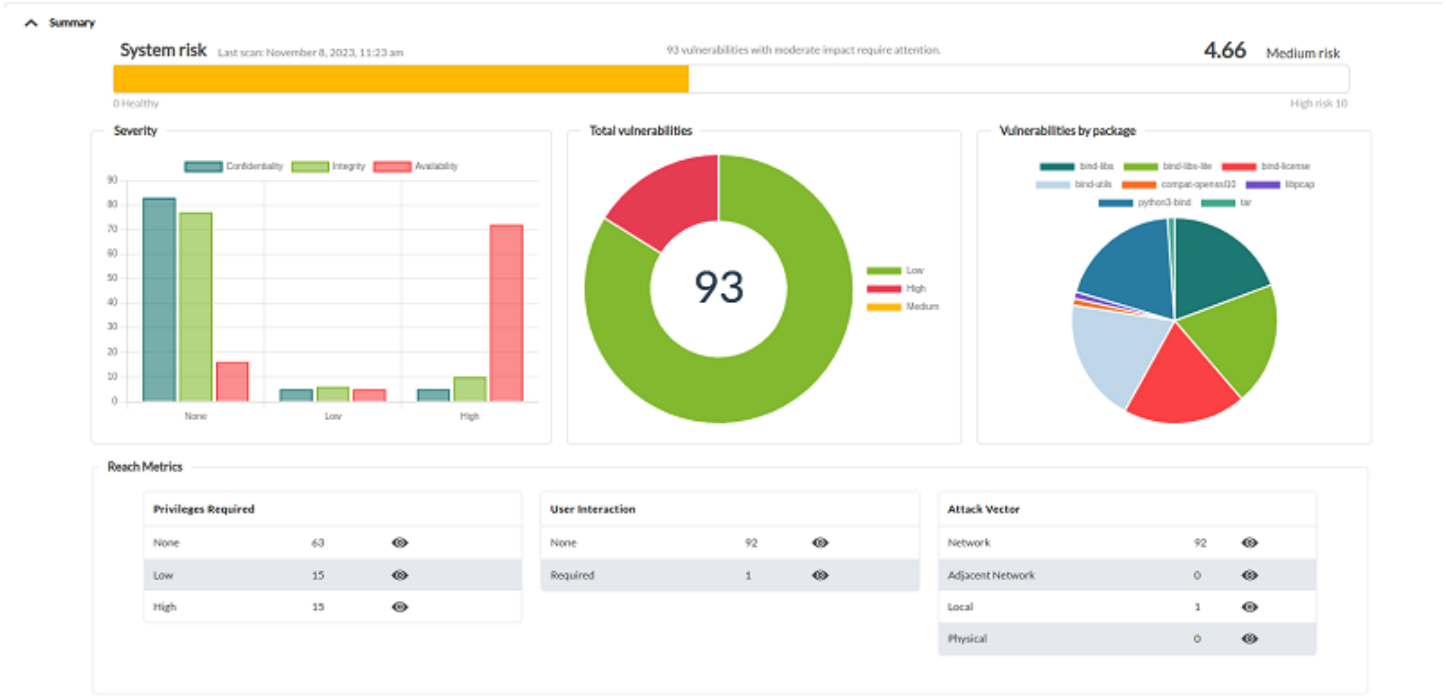
Une fois que le système dispose d'informations, celles-ci seront affichées dans l'onglet Vulnérabilités de chaque système supervisé.

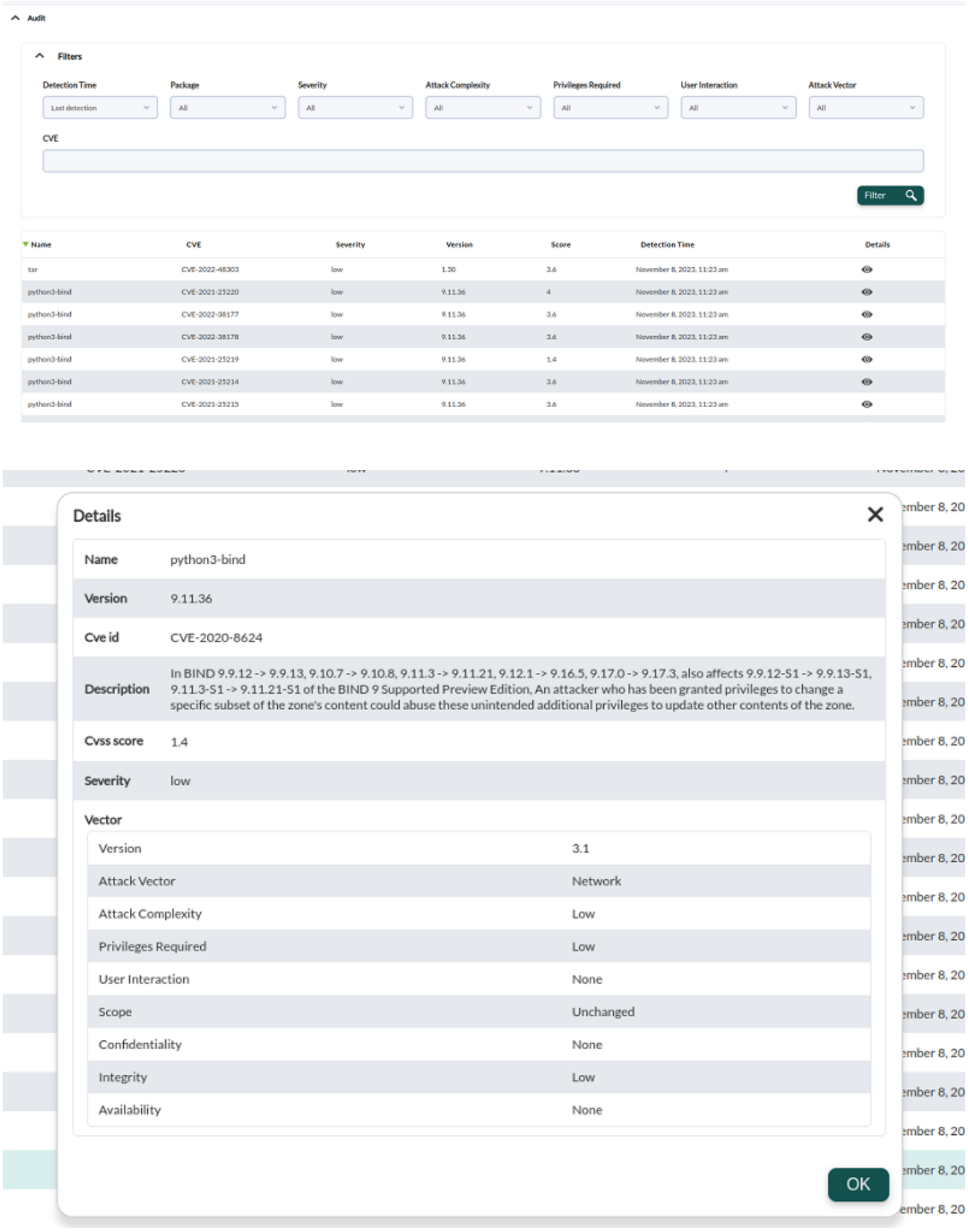
Il dispose également (à partir de la version 775) d'un tableau de bord général, avec plusieurs graphiques ajoutés, comme le Top-10 des systèmes les plus vulnérables (pire classement des vulnérabilités), le Top-10 vulnerabilities (les plus fréquents) et autres regroupements.

Ces rapports comportent des filtres spécifiques:

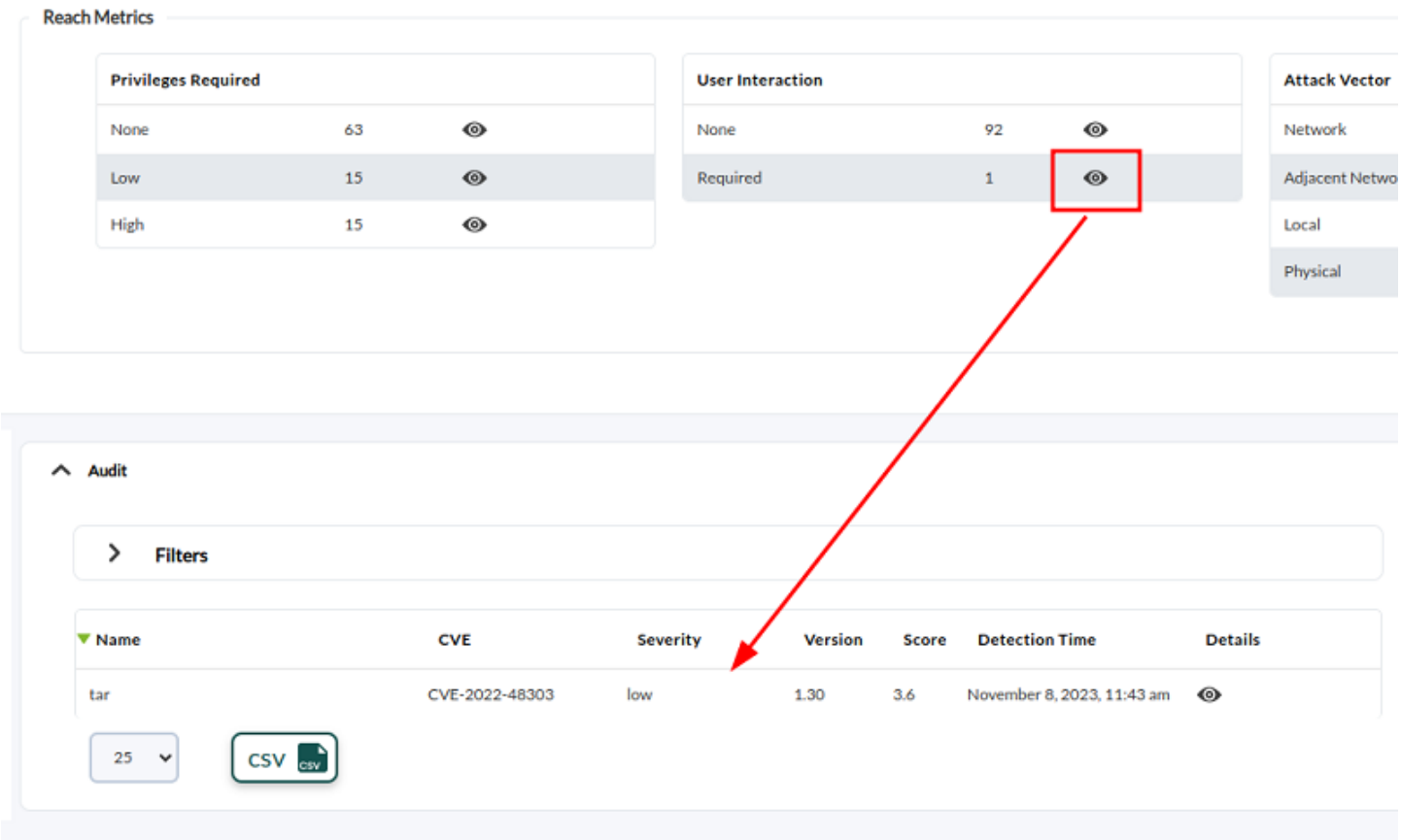
- Par groupe de machines.
- Attack complexity (low/high/medium).
- Type de vulnérabilité (confidentiality, integrity, availability...).
- Access vector: Network, Adjacent Network...
- User interaction: none, required, etc.
- Privileges required: None, low...


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



Les métriques de portée vous permettent de filtrer rapidement les vulnérabilités:

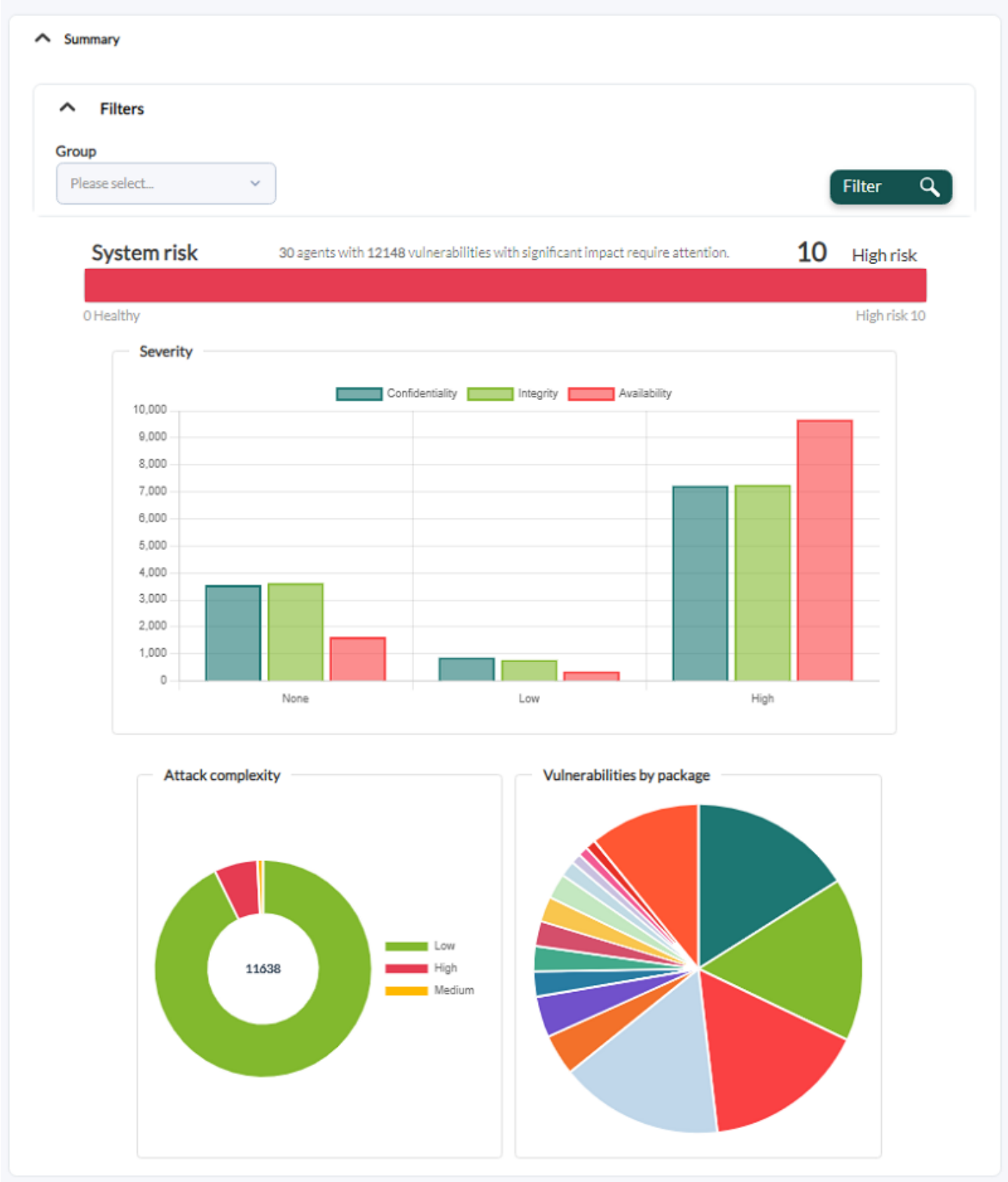


Vision tactique de la sécurité

Menu Operation → Security → Vulnerabilities.

Summary

Il présente une image globale des agents, avec des graphiques résumant le risque total dans le système dans son ensemble, la gravité de la complexité des attaques et les vulnérabilités présentées par chaque logiciel installé.

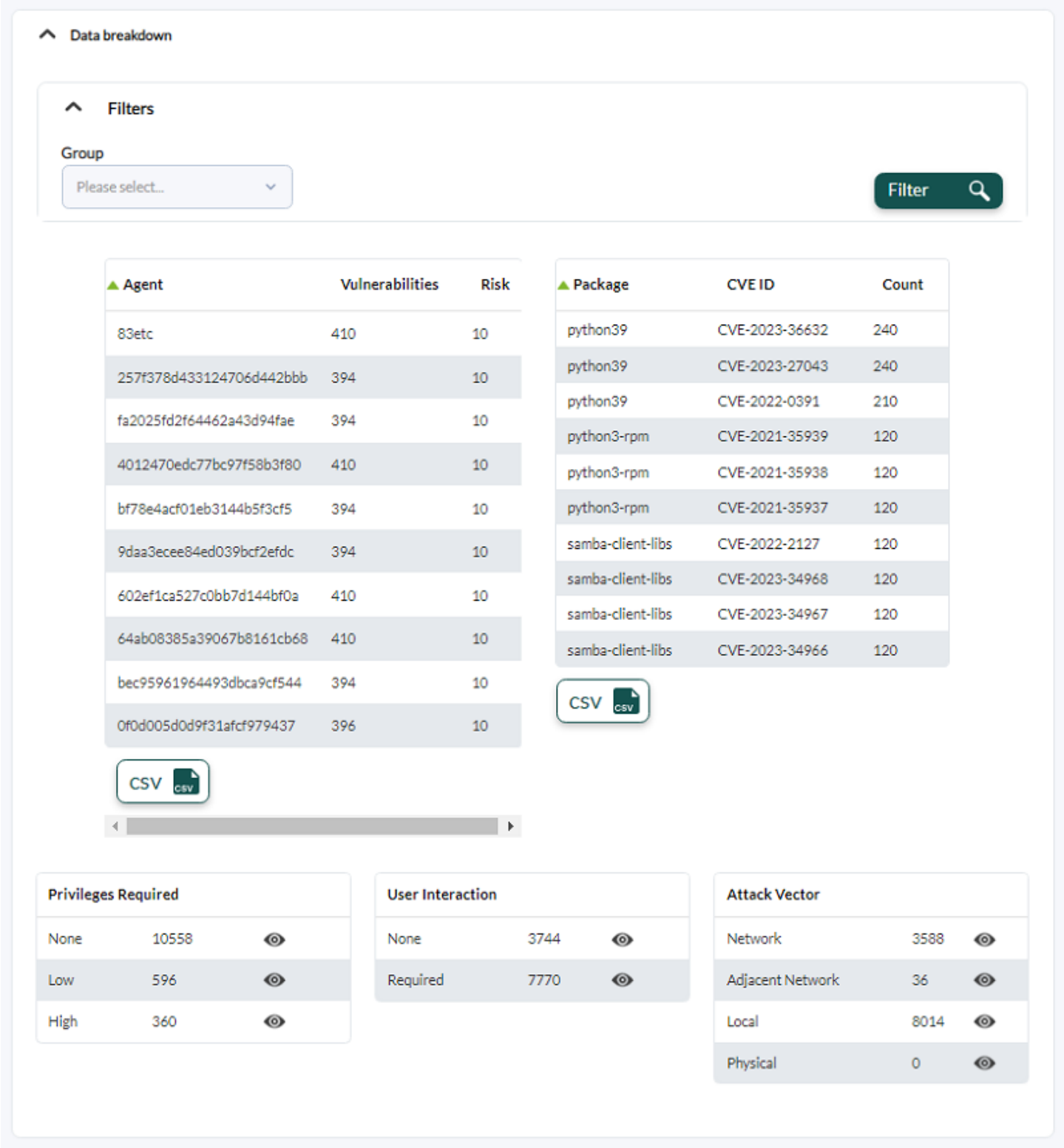


Vous pouvez filtrer par groupe d'agents; par défaut, tous les groupes sont affichés (All).

Data breakdown

Il présente une ventilation des données relatives à la sécurité, en indiquant les 10 principaux

agents et les 10 principaux logiciels présentant le plus grand nombre de vulnérabilités.



Les informations peuvent être filtrées par groupe d'agents et exportées au format CSV. Les résumés dans les cases Privileges required, User Interaction et Attack Vector ont des boutons d'affichage qui renvoient à la section audit.

Audit

Par défaut, il affiche toutes les informations sur les vulnérabilités, ce qui peut prendre un certain temps de chargement. Vous pouvez filtrer par un nombre quelconque de combinaisons de caractéristiques de vulnérabilité, y compris des numéros d'identification CVE spécifiques.

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

Une fois les informations filtrées, chaque élément dispose d'un bouton d'affichage détaillé (icône en forme d'œil) qui permet d'afficher les informations détaillées correspondantes.

Revenir à l'index de la documentation Pandora FMS