



Inventaire



m:
<https://pandorafms.com/manual!/current/>
permanent link:
https://pandorafms.com/manual!/current/fr/documentation/pandorafms/management_and_operation/04_inventory
24/10/03 18:59





Inventaire

Introduction

Pandora FMS vous permet de maintenir un inventaire des appareils surveillés par Pandora FMS. Avec cet inventaire, il est possible de maintenir des **listes et rapports (disponibles dans la version Enterprise)** de :

-  Modèle et vitesse du processeur (MS Windows®, GNU/Linux®).
-  Stockage et systèmes de fichiers.
-  Version du micrologiciel (matériel réseau).
-  Configuration de l'appareil (matériel réseau).
-  Numéros de série et licences (par exemple MS Office®, MS Windows®).
-  Applications installées sur l'ordinateur (MS Windows®, Android Linux®, GNU/Linux®).
-  Cartes réseau et leurs MAC associés aux adresses IP.
-  Modules de mémoire RAM et leur capacité (MS Windows®, GNU/Linux®).
-  Routes installées.
-  Services en cours d'exécution.
-  Périphériques de stockage (MS Windows®, GNU/Linux®).
-  Utilisateurs du système.

Collecte de données pour l'inventaire

L'inventaire est indépendant du suivi et peut être obtenu :

- **Remotely**, via des modules d'inventaire, via des scripts intégrés à Pandora FMS qui exécutent des requêtes WMI, ou des scripts exécutés via SSH avec Expect ou des méthodes similaires.
- **Locally**, avec l'Agent logiciel Pandora FMS, via des plug-ins dans l'Agent.

Modules d'inventaire

Les modules d'inventaire sont des modules distants qui exécutent une commande sur une machine distante. Ces modules fonctionnent de la même manière qu'un plugin. Les mêmes modules peuvent être définis comme locaux lorsqu'ils obtiennent des données via un agent logiciel.

Dans les paramètres User et Password vous pouvez utiliser les **macros** suivants :
`_agentcustomfield_n_` (numéro de champ personnalisé n de l'agent) .

Inventaire à distance

Avec Pandora FMS un bon nombre de modules d'inventaire sont installés par défaut et cela permet également de créer de nouveaux modules d'inventaire, de modifier, supprimer et personnaliser ceux qui existent déjà à l'aide de l'éditeur de module d'inventaire.

Création de modules distants

Dans le menu Gestion → Configuration → Modules d'inventaire vous pouvez voir cette liste, et avec le bouton Créer, ajoutez-en une nouvelle.

Quelques domaines importants:

- **Interprète:** Laissez vide s'il s'agit d'un module local. Champ où est placé l'interpréteur de commandes utilisé dans le module. Il peut s'agir de Shell Script, Perl ou d'un autre interpréteur valide pour le serveur d'inventaire exécuté sur un système GNU/Linux.
- **Code:** Laissez vide s'il s'agit d'un module local. Code des modules ; il s'agit généralement de code Perl ou de Shell Script. S'il s'agissait de code binaire, il faudrait une procédure de chargement différente qui doit être introduite via des scripts auxiliaires.
- **Mode bloc:** **Affiche et détecte les modifications** dans la configuration.
- **Format:** Tapez les champs séparés par ; que le module renverra.

- Dans Format, assurez-vous de placer chaque champ séparé par des points-virgules. Si vous omettez ce champ, vous ne pourrez pas créer ou sauvegarder de module d'inventaire et vous perdrez toutes les modifications apportées.
- Il est très important de choisir le système d'exploitation correspondant car lors de l'ajout de modules d'inventaire à un agent, seuls les modules apparaîtront dans lesquels le système d'exploitation du module correspond à celui de l'agent.

Attribuer des modules distants

L'affectation des Modules d'Inventaire s'effectue dans l'Agent lui-même, dans l'onglet Administration de l'Agent, cliquez sur l'onglet Inventaire.

- **Module:** Choisissez le module d'inventaire qui doit être ajouté. Seuls les modules dont le système d'exploitation correspond à celui de l'agent apparaîtront.
- **Cible:** Adresse IP ou nom du serveur à partir duquel vous souhaitez récupérer l'inventaire.
- **Intervalle:** Choisissez l'intervalle de temps pendant lequel le module d'inventaire s'exécutera.

Il est possible de définir des champs au lieu du nom d'utilisateur et du mot de passe qui existent normalement, il est pour cela nécessaire d'activer le champ Utiliser les champs personnalisés. Après cela, un contrôle apparaîtra pour ajouter de nouveaux champs (Ajouter un champ).

- Dans ce contrôle vous devrez saisir le nom souhaité avant de l'ajouter.
- Si vous indiquez que le champ contiendra un mot de passe, tapez C'est un mot de passe et la valeur sera enregistrée dans la base de données de manière obscurcie.
- Après avoir créé les champs, vous pouvez leur donner une valeur et enfin ajouter le Module.
- Ces champs seront appliqués par ordre de création lors de l'exécution du script d'inventaire distant.

Inventaire local via des agents logiciels

Grâce aux agents logiciels, il est possible d'obtenir des données d'inventaire pour une machine. Il suffira d'appliquer les modules d'inventaire correspondants dans la [Configuration de l'Agent Logiciel](#).

Comme pour les modules distants, il est également nécessaire d'ajouter ces modules en tant que module d'inventaire dans Gestion → Configuration → Modules d'inventaire.

Création de Modules locaux

Pour créer un module local, accédez à Gestion → Configuration → Modules d'inventaire où apparaissent tous les modules d'inventaire créés. Tous les modules qui seront définis dans la configuration de l'Agent doivent être créés ici ; Le système d'exploitation attribué à l'Agent dans la console doit également correspondre à celui du Module créé.

La procédure est la même que celle utilisée pour le cas distant, à l'exception du remplissage des champs Interprète et Code. Pour modifier le module d'inventaire nouvellement créé (ainsi que tous les autres), cliquez sur le nom ou sur l'icône en forme de clé.

Configuration de l'inventaire local pour les agents logiciels

Ces plugins sont livrés par défaut avec l'installation de l'agent logiciel, bien qu'ils soient commentés dans le fichier de configuration, pour les utiliser décommentez ces lignes et redémarrez l'agent logiciel (dans la version Entreprise les agents logiciels peuvent être redémarrés grâce à leur configuration à distance) .

Exemple pour MS Windows® :

```
#module_begin
#module_plugin cscript.exe B t:20
"%PROGRAMFILES%\Pandora_Agent\util\cpuinfo.vbs"
#module_crontab * 12-15 * * 1
#module_end
```

D'autres éléments peuvent être téléchargés à partir de la collection de scripts [dans la bibliothèque Pandora FMS](#). Chacun a son mode d'emploi et l'exécution programmée des scripts d'inventaire local doit être configurée dans le fichier `pandora_agent.conf` en ajoutant l'information à la fin du fichier.

Module d'inventaire sur les systèmes Unix via l'agent logiciel

Le module Unix Software Agent utilise, localement, un plugin pour collecter des informations sur différents aspects de la machine, tant logiciels que matériels.

Le plugin qui récupère l'inventaire se trouve dans le répertoire `/etc/pandora/plugins`

La syntaxe du module est la suivante :

```
module_plugin inventaire 1 cpu ram vidéo nic hd cdrom logiciel init_services
système de fichiers route des utilisateurs
```

Le Module est constitué d'une ligne avec les paramètres suivants :

- Activation des modules :

```
"module_plugin inventaire" 1 cpu ram vidéo nic hd cdrom logiciel init_services
système de fichiers route des utilisateurs
```

- Champ où est établi combien de jours le module sera exécuté. S'il est égal à zéro (0), l'inventaire est renvoyé à chaque exécution de l'agent.

```
module_plugin inventaire "1" cpu ram vidéo nic hd cdrom logiciel init_services
système de fichiers route des utilisateurs
```

- Champ où sont définis les objets d'inventaire collectés.

```
module_plugin inventaire 1 "cpu ram vidéo nic hd cdrom logiciel init_services
système de fichiers utilisateurs route"
```

Vous pouvez aussi simplement préciser qu'il collecte toutes les informations disponibles. Dans cet exemple, vous collecterez quotidiennement toutes les informations d'inventaire :

```
# Plugin pour l'inventaire sur l'agent (Entreprise uniquement)
module_plugin inventaire 1
```

Pour activer le module d'inventaire, copiez le code décrit ci-dessus et ajoutez-le au fichier `pandora_agent.conf` de l'agent logiciel et redémarrez le service.

Attribuer des modules locaux

Il n'est pas nécessaire d'activer les Modules dans les Agents définis dans la Console :

- Si les modules ont été créés dans Configuration → Modules d'inventaire.
- Si le système d'exploitation correspond et que l'exécution est définie dans le fichier de configuration de l'agent logiciel.
- Les données collectées apparaîtront directement dans la section Affichage → Inventaire de l'Agent dans la Console.

Création de modules d'inventaire local avec Software Agent

En plus des systèmes d'inventaire préconfigurés dans l'agent, des modules d'inventaire peuvent être créés pour les systèmes Unix® et MS Windows®. Fondamentalement, vous devez créer un script qui génère un XML avec la structure suivante :

```
<inventaire>
  <module_inventaire>
    <nom>INVENTORY_MODULE_NAME</nom>
    <type>generic_data_string</type>
    <liste de données>
      <données>DONNÉES1;DONNÉES2;DONNÉES3...</données>
    </liste de données>
  </inventory_module>
</inventaire>
```

- `INVENTORY_MODULE_NAME`: Le même nom du module que vous avez enregistré dans les modules d'inventaire de la console Pandora FMS doit être saisi.
- `DATA1;DATA2...` : Ce sont les données à extraire et qui ont été définies dans le module Inventaire.
- Dans le fichier `pandora_agent.conf` le script qui génère le XML doit être exécuté.
- Pour que l'exécution du script local stocke les informations d'inventaire, elle doit avoir un module d'inventaire défini dans la console, spécifiant le système d'exploitation, le nom du module et les données à stocker séparés par ; .
- Par conséquent, le module d'inventaire doit être créé dans Pandora FMS avant de redémarrer l'agent Pandora FMS.

Affichage des données pour l'inventaire

Les données d'inventaire collectées à partir d'un système, que ce soit localement ou à distance, peuvent être visualisées depuis l'agent lui-même ou depuis le menu Inventaire de la console.

Afficher les données d'inventaire dans le menu Inventaire

Depuis Opération → Surveillance → Inventaire, il est possible de visualiser les données d'inventaire de tous les agents, d'effectuer des recherches et d'exporter les données vers un fichier CSV.

Par défaut, tous les agents sont affichés, mais il est possible d'afficher les modules de tous les agents disposant d'un inventaire en choisissant Tous dans les options de recherche et en cliquant sur Rechercher. Dans n'importe quel cas de recherche (groupe, module, etc.) vous pouvez regrouper par agent si vous cochez l'option Ordre par agent.

Dans la vue détaillée de l'inventaire de l'Agent, grâce à un sélecteur, vous pouvez choisir la date du rapport d'inventaire spécifique à visualiser (par défaut Dernier).

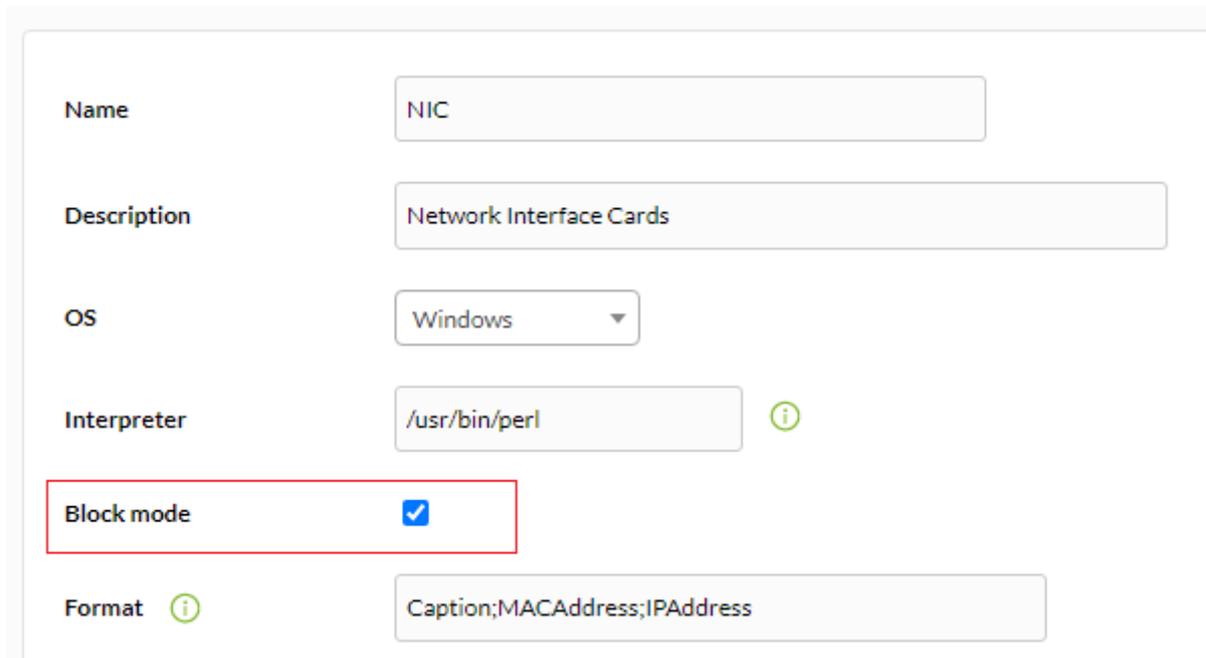
Si vous remarquez des dates manquantes, c'est probablement parce qu'il n'y a aucun changement dans les données depuis le dernier inventaire. Autrement dit, Pandora FMS stocke uniquement les données d'inventaire lorsqu'elles changent par rapport à la dernière exécution.

Exporter les données d'inventaire au format CSV

Depuis Opération → Surveillance → Inventaire, il est possible d'exporter les données d'inventaire, résultat d'un filtre, vers un fichier CSV à l'aide du bouton Exporter cette liste vers CSV. Un fichier avec les données d'inventaire séparées par le **caractère configuré** sera créé et téléchargé dans Setup → Styles visuels → Séparateur CSV.

Différences entre les versions d'inventaire

Pandora FMS peut montrer visuellement les différences entre deux configurations, en l'affichant sur deux colonnes pour voir les différences. Le Mode Bloc précise que le résultat d'un module d'inventaire est un seul élément, au lieu d'interpréter chaque ligne comme différents éléments du même type, comme cela a été fait dans les modules d'inventaire vu précédemment. Configuré lors de la définition d'un module d'inventaire local ou distant :



Name	NIC
Description	Network Interface Cards
OS	Windows
Interpreter	/usr/bin/perl
Block mode	<input checked="" type="checkbox"/>
Format	Caption;MACAddress;IPAddress

Alertes d'inventaire

Version 751 NG ou ultérieure.

Alertes d'inventaire Ils servent pour lancer des alertes spécifiques sur le contenu de l'inventaire d'un groupe d'agents. Comme les alertes SNMP ou les alertes d'événements, elles ne sont pas appliquées agent par agent mais sont globales, dans ce cas, elles sont appliquées par groupes.

Pour configurer les alertes, vous devez vous rendre dans la section Gestion → Alertes → Alertes d'inventaire.

Les alertes d'inventaire comportent des champs similaires à **other alerts** tels que le nom, la description, le seuil de temps et l'action, avec les différences suivantes :

- Le groupe dans ce cas agit comme condition d'alerte, de sorte que les alertes seront évaluées pour toutes les données provenant d'un agent dudit groupe.
- Ces alertes ont également l'option désactiver l'événement qui est utilisée pour que lorsque l'alerte est déclenchée, un événement d'alerte ne soit pas généré. C'est utile car il est possible qu'avec l'application d'alertes d'inventaire de nombreuses alertes soient déclenchées en une seule exécution.

Condition de déclenchement d'alerte

Correspondance de chaîne de texte

De cette façon, lorsqu'une chaîne spécifique arrive dans un module d'inventaire spécifique (par exemple « logiciel ») l'action établie sera déclenchée. Les modules d'inventaire ont des champs dynamiques ; Par exemple, dans le module d'inventaire logiciel, il y a les champs nom, version et description qui peuvent être utilisés. De cette façon, vous pouvez définir une alerte pour l'un des

trois champs dynamiques, par exemple pour surveiller un package d'une version spécifique :

ET Dans ces champs, vous pouvez saisir des expressions régulières pour effectuer des recherches plus complexes. Si un champ est vide, il compte pour .* (il correspondra à n'importe quelle valeur).

Liste restreinte

Dans ce cas (Condition, Liste noire) vous devez spécifier un seul champ de type Module Inventaire, et établir une liste de chaînes (une par ligne) afin que si l'Agent contient un élément de celui-ci liste, l'alerte se déclenchera

Liste autorisée

Similaire [au cas précédent](#) : Une liste d'articles (Condition, Liste blanche) est spécifiée pour l'un des champs d'inventaire, sauf que Dans ce cas, la valeur du Module Inventaire doit toujours se trouver dans un des éléments de la liste, sinon l'alerte apparaîtra.

Utilisations des alertes d'inventaire

Cette fonctionnalité est vraiment utile pour détecter les versions vulnérables des appareils, les utilisateurs non autorisés sur les machines ou les logiciels non autorisés sur les ordinateurs.

Surveillance de la sécurité

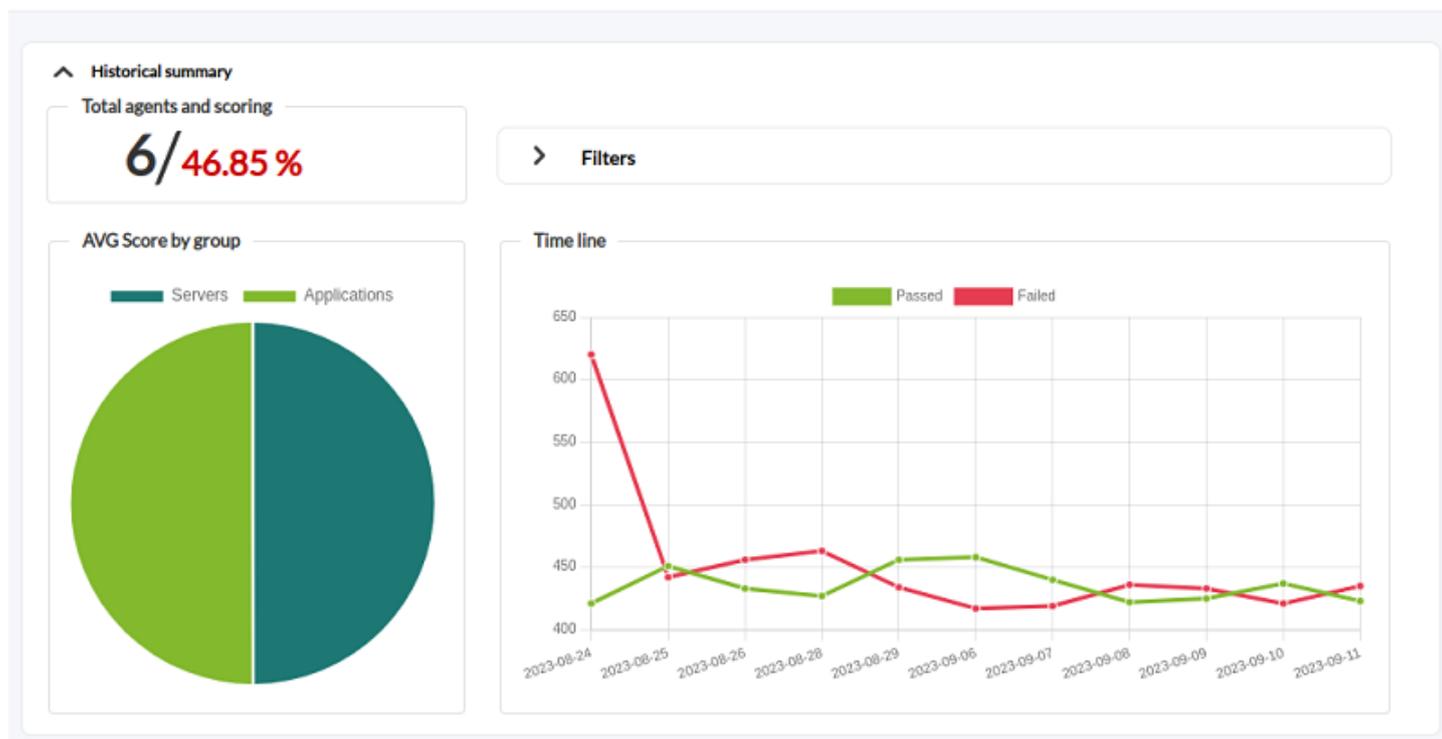
Pandora FMS vous permet de collecter, en plus des données d'inventaire, d'autres valeurs importantes de chaque système d'exploitation surveillées via des agents logiciels. Tout cela est centralisé dans la section Opération → Sécurité → Renforcement.

Cet outil vise à renforcer la sécurité de chacun des appareils surveillés et les informations sont présentées en trois sections principales.

Résumé historique

Le Résumé historique présente le nombre total d'agents qui surveillent les modules destinés à la sécurité et le score moyen total (Tableau Total agents et scoring).

Security
Hardening

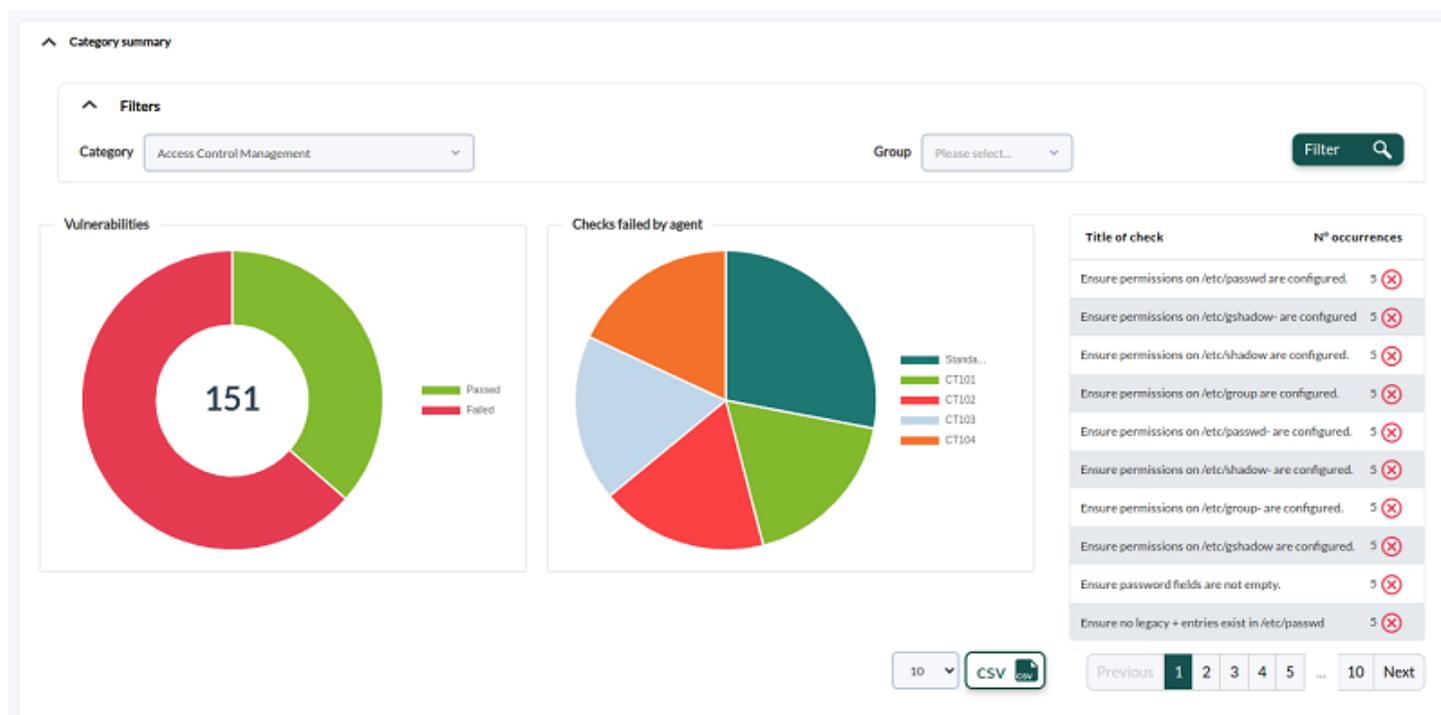


Le tableau AVG Score par groupe présente le score moyen de chaque groupe défini dans PFMS.

Il existe également un graphique historique (tableau Chronologie) avec la moyenne des contrôles de sécurité échoués et approuvés regroupés par jours (maximum les onze derniers jours) quelle que soit la période sélectionnée. Dans Filtres, vous pouvez sélectionner une période personnalisée ou des valeurs communes (la semaine dernière, le mois dernier, etc.).

Résumé de la catégorie

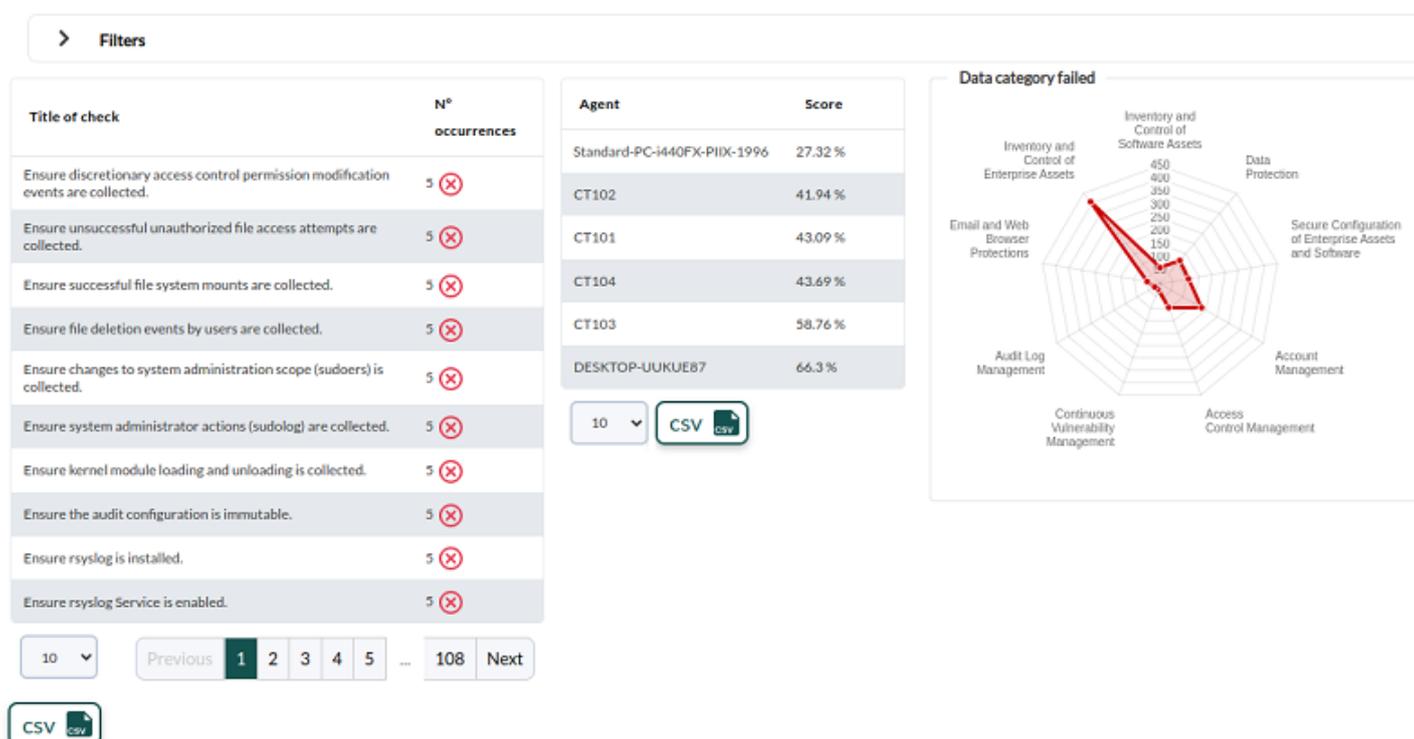
Dans le Résumé par catégories, il doit être filtré par catégorie et éventuellement par groupe pour être affiché. Par défaut, la catégorie Gestion du contrôle d'accès est sélectionnée.



* La case Vulnérabilités affichera le nombre total de vulnérabilités ayant échoué et les vulnérabilités surmontées. * Dans Contrôles échoués par agent, la liste des contrôles échoués pour la catégorie sélectionnée, en cliquant sur chaque secteur du graphique, vous listerez les détails du contrôle sélectionné et les agents concernés.

Résumé des échecs

Failure summary



Le récapitulatif des échecs est présenté (Titre du contrôle) : La liste des contrôles échoués filtrée

par groupe et nombre d'incidents. Utilisez la zone Filtres pour définir de nouveaux paramètres de recherche et d'affichage.

Également la liste des agents avec le pire score de sécurité, avec la possibilité de visualiser la vue de sécurité de chaque agent en cliquant dessus.

Enfin, un graphique radar est présenté avec la répartition des pannes par catégorie.

[Retour à l'index de la documentation Pandora FMS](#)