Hardening

Hardening

Supervision du hardening

Les recommandations du Center for Internet Security (CIS) ont été fusionnées avec la technologie de supervision Pandora FMS pour offrir une solution intégrée système d'audit d'assurance. Cela permet de suivre et d'évaluer l'évolution des mesures de durcissement (renforcement de la sécurité) dans le temps dans les environnements utilisés et supervisés.

Le renforcement du système ou hardening est un processus utilisé pour améliorer la sécurité d'un système informatique en réduisant sa surface d'attaque et en renforçant ses défenses. Elle consiste à rendre plus difficile aux attaquants potentiels l'exploration des erreurs de configuration, qu'elles soient dues à des configurations par défaut, à de mauvaises configurations ou à des configurations inappropriées.

Le renforcement du système est un processus continu à mesure que les menaces de sécurité et les vulnérabilités évoluent au fil du temps.temps. Cela nécessite une supervision constante, des évaluations des risques et des ajustements des configurations de sécurité pour s'adapter à l'évolution des circonstances. De plus, les organisations suivent souvent les normes et les meilleures pratiques spécifiques à l'industrie, telles que les contrôles CIS ou les directives du National Institute of Standards and Technology (NIST), pour garantir un système de hardening intégral.

Pandora FMS utilise plusieurs catégories CIS pour regrouper les contrôles qu'il effectue.

Catégories CIS auditées par Pandora FMS

Nous avons poussé les recommandations du CIS un peu plus loin en mettant en œuvre plus de 1 500 contrôles individuels dans diverses catégories critiques pour la sécurité.

Inventaire et contrôle des actifs matériels et logiciels: Supervisez et gérez tous les appareils et logiciels de votre organisation. Maintenez un inventaire à jour de vos actifs technologiques et utilisez l'authentification pour bloquer les processus non autorisés.

Inventaire et contrôle des appareils: Identifiez et gérez vos appareils matériels afin que seuls les appareils autorisés y aient accès, en bloquant les autres. Le maintien d'un inventaire approprié minimise les risques internes, organise votre environnement et apporte de la clarté à votre réseau.

Gestion des vulnérabilités: Analysez vos actifs en continu au fil du temps pour détecter les vulnérabilités potentielles et les corriger avant qu'elles ne deviennent la porte d'entrée d'une attaque. Renforcez la sécurité du réseau en garantissant que les logiciels et les systèmes d'exploitation de l'organisation sont toujours à jour avec les dernières mesures de sécurité et correctifs. Aidez-nous à gérer votre logiciel pour garantir que seuls les logiciels autorisés sont installés et exécutés. Évitez les vulnérabilités et les risques en maintenant un inventaire précis et en gérant vos logiciels.

Utilisation contrôlée des privilèges administratifs: Supervisez de près les contrôles d'accès et le comportement des utilisateurs disposant de comptes privilégiés pour empêcher tout accès non autorisé aux systèmes critiques. Assurez-vous que seules les personnes autorisées disposent de privilèges élevés pour éviter toute utilisation abusive des privilèges administratifs. Établissez des politiques strictes pour empêcher toute utilisation abusive des privilèges.

Configuration matérielle et logicielle sécurisée: Établissez et maintenez des configurations de sécurité basées sur les normes approuvées par votre organisation. Créez un système de gestion de configuration rigoureux qui détecte et alerte en cas de configuration incorrecte, et établit un processus de contrôle des modifications pour empêcher les attaquants d'exploiter les services et les configurations vulnérables.

Maintenance, surveillance et analyse des journaux et des journaux d'audit: Collectez, gérez et analysez les journaux d'audit des événements pour identifier les anomalies potentielles. Tenez des journaux détaillés pour bien comprendre les attaques et répondre efficacement aux incidents de sécurité.

Défenses contre les logiciels malveillants: Supervisez et contrôlez l'installation et l'exécution de codes malveillants à différents points de votre organisation pour prévenir les attaques. Configurez et utilisez un logiciel anti-malware et tirez parti de l'automatisation pour garantir des mises à jour rapides de la défense et des mesures correctives rapides en cas d'attaques.

Protection de la messagerie et du navigateur Web: Protégez et gérez vos navigateurs Web et systèmes de messagerie contre les menaces en ligne afin de réduire votre surface d'attaque. Désactivez les plugins de messagerie non autorisés et assurez-vous que les utilisateurs accèdent uniquement aux sites Web de confiance à l'aide de filtres d'URL Web. Protégez les portes d’entrée communes des attaques.

Capacités de récupération de données: Établissez des processus et des outils pour garantir que les informations critiques de votre organisation sont correctement sauvegardées. Assurez-vous de disposer d'un système de récupération de données fiable pour restaurer les informations en cas d'attaques compromettant les données critiques. Préparez votre organisation à gérer efficacement la perte de données.

Défense des limites et protection des données: Identifiez et séparez les données sensibles, et établissez une série de processus qui incluent le chiffrement, des plans de protection contre

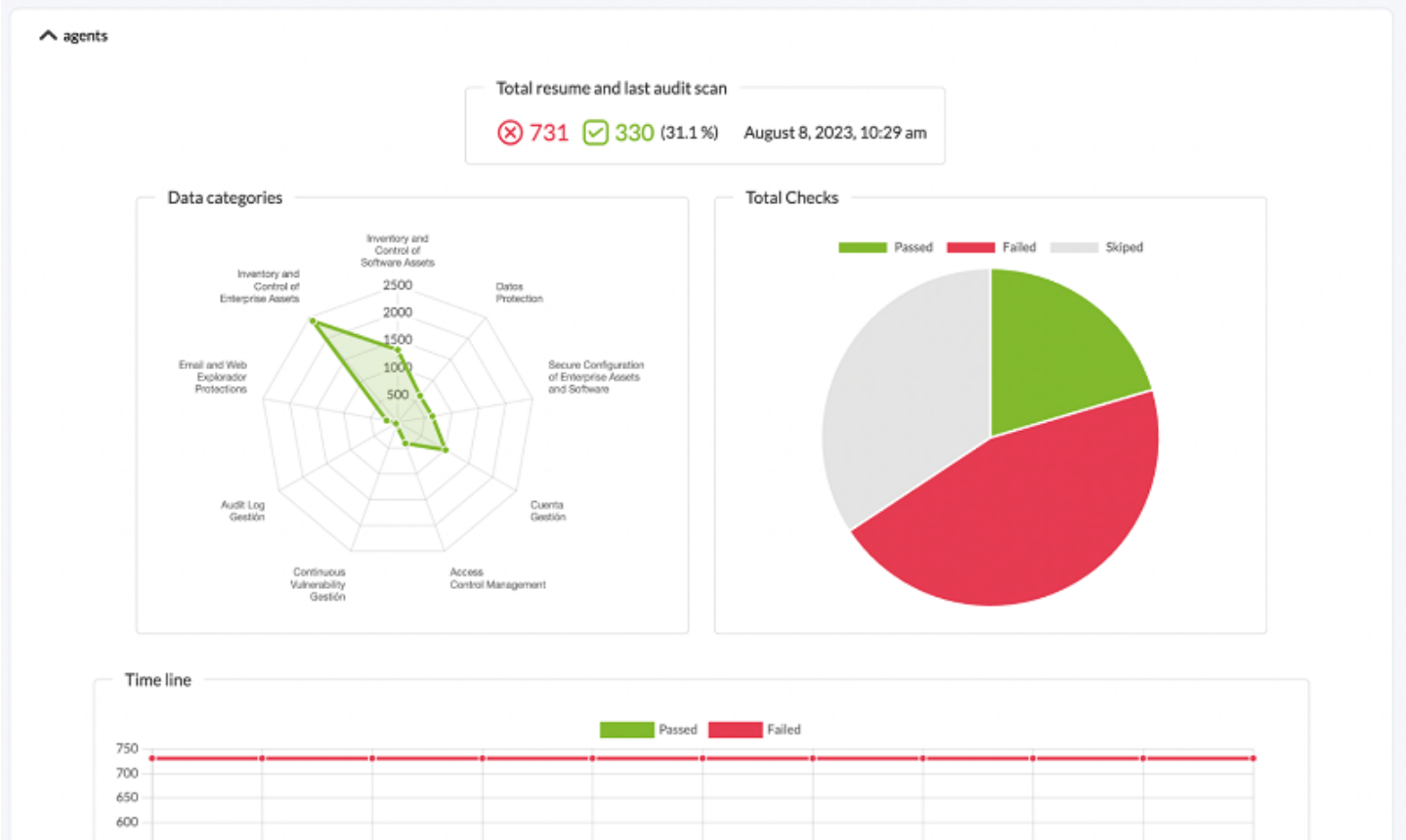
l'infiltration de données et des techniques de prévention des pertes de données. Établissez des barrières solides pour empêcher tout accès non autorisé.

Supervision et contrôle des comptes Elle supervise de près l'ensemble du cycle de vie de vos systèmes et comptes d'applications, de la création à la suppression, en passant par l'utilisation et l'inactivité. Cette gestion active empêche les attaquants d'exploiter les comptes d'utilisateurs légitimes mais inactifs à des fins malveillantes et vous permet de maintenir un contrôle constant sur les comptes et leurs activités.

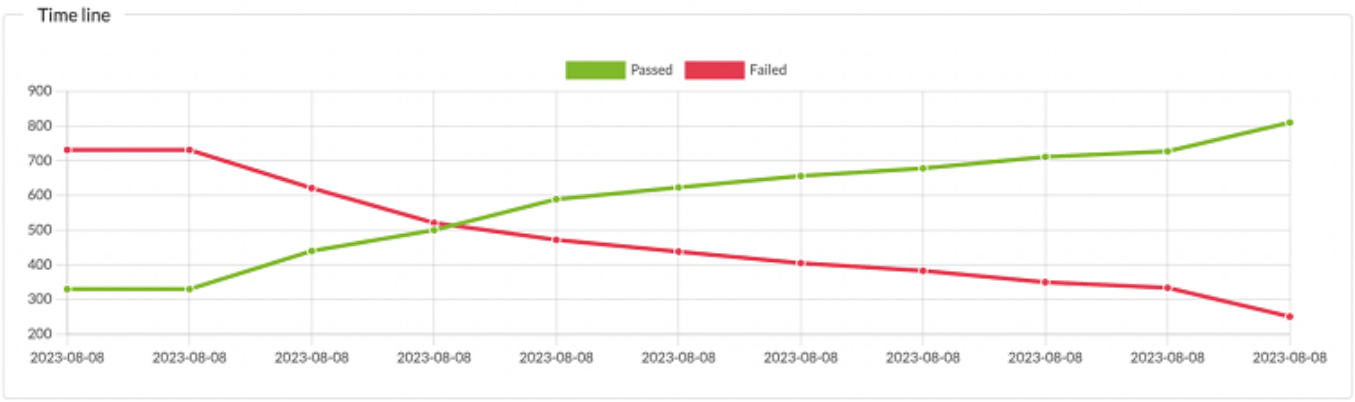
Audits de durcissement détaillés de chaque machine

Les chèques sont effectuées par l'EndPoint qui s'exécute sur chaque machine. Généralement, un audit a lieu chaque semaine, mais cette période peut être fixée à une période plus longue, par exemple un mois. De cette façon, vous pouvez prendre un instantané de la sécurité du système, calculer et attribuer un indice de sécurité (une note numérique, définie comme le pourcentage de contrôles effectués et approuvés par rapport aux contrôles qui ne réussissent pas les tests) et voir l'évolution de cet indice de sécurité au fil du temps.

Exemple de « instantané » de l'état de durcissement d'un système:



Exemple d'évolution du durcissement d'un système dans le temps:



Le système nous permet de voir, ventilés par catégorie, les contrôles qui ont été exécutés:

Summary of categories

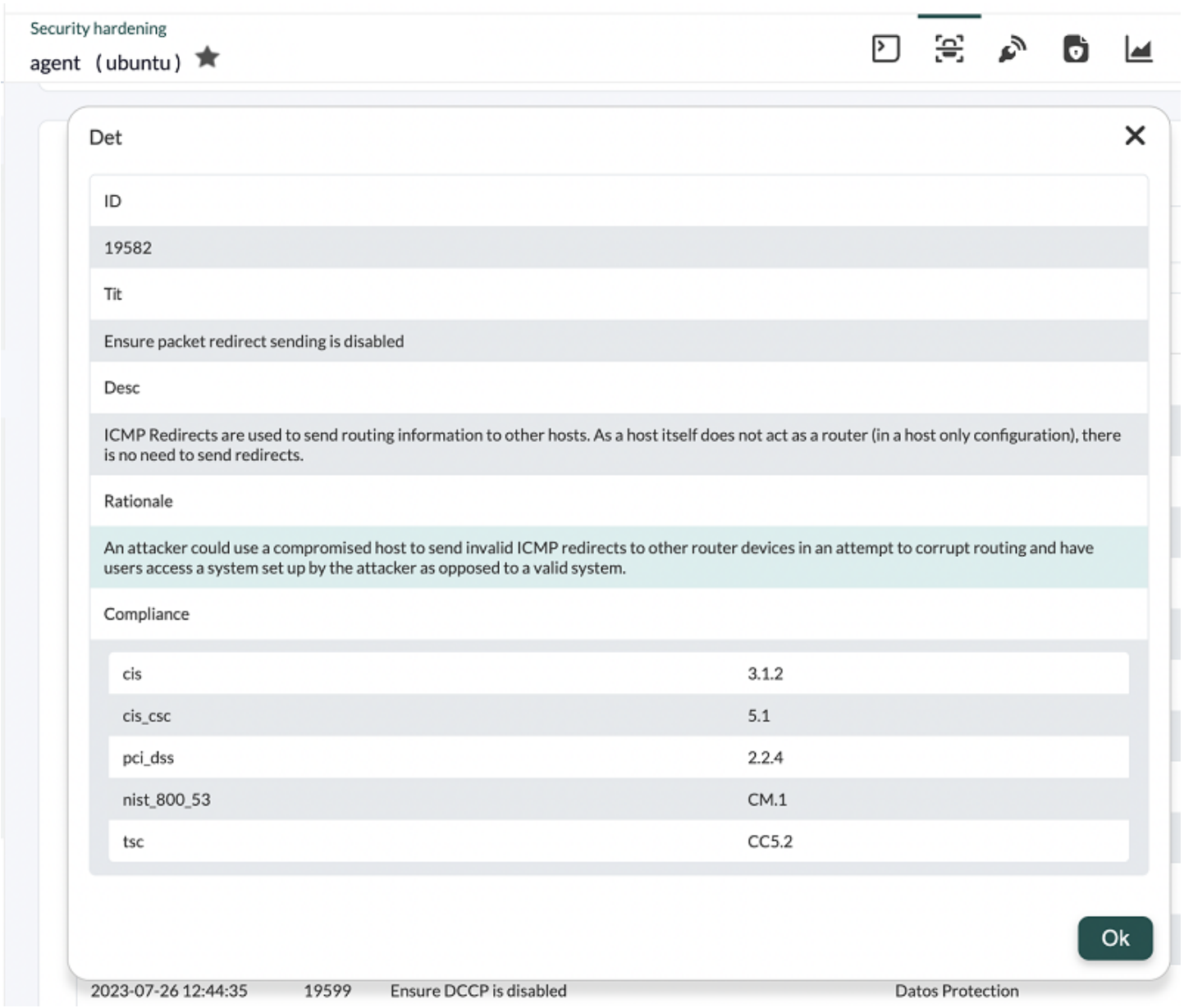
Inventory and Control of Software Assets	14	46	23 %
Data Protection	20	118	14 %
Secure Configuration of Enterprise Assets and Software	21	126	14 %
Account Management	78	193	29 %
Access Control Management	92	16	85 %
Continuous Vulnerability Management	8	14	36 %
Audit Log Management	0	20	0 %
Email and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

Et pour chaque groupe d'éléments, voir le détail, pour pouvoir travailler sa correction:

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		



Configuration de supervision du hardening

Des contrôles ont été développés, en fonction de chaque système s'ils sont applicables, qui aideront à déterminer s'ils sont pertinents dans l'environnement à superviser. Actuellement, cette fonctionnalité est disponible pour les serveurs MS Windows® et Linux®.

Cette fonctionnalité est disponible avec les agents 773 ou version ultérieure. Si les agents sont d'une version antérieure à 773, ils doivent être mis à jour.

Pour ce faire, vous devrez activer le plugin correspondant dans la configuration de l'agent. Cela peut être fait manuellement ou via des supervision des politiques sur des groupes de machines.

Sous MS Windows®:

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

Linux®:

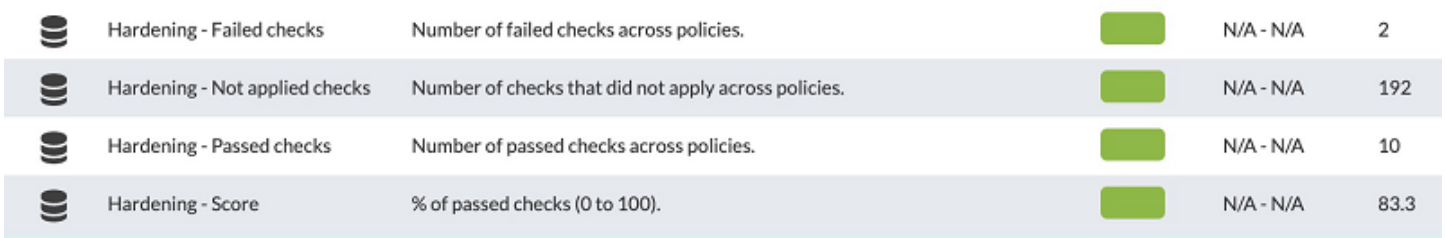
```
module_begin
module_plugin /usr/share/pandora_agent/plugins/pandora_hardening -t 150
module_absoluteinterval 7d
module_end
```

Dans ces exemples, l'audit du hardening sera exécuté tous les 7 jours, avec un timeout de 150 secondes pour chaque commande lancée lors de l'audit. Vous pouvez augmenter cette valeur à 30 jours, mais nous vous déconseillons de le faire tous les quelques jours car cela générerait des données d'inventaire inutiles.

Supervision des données de hardening

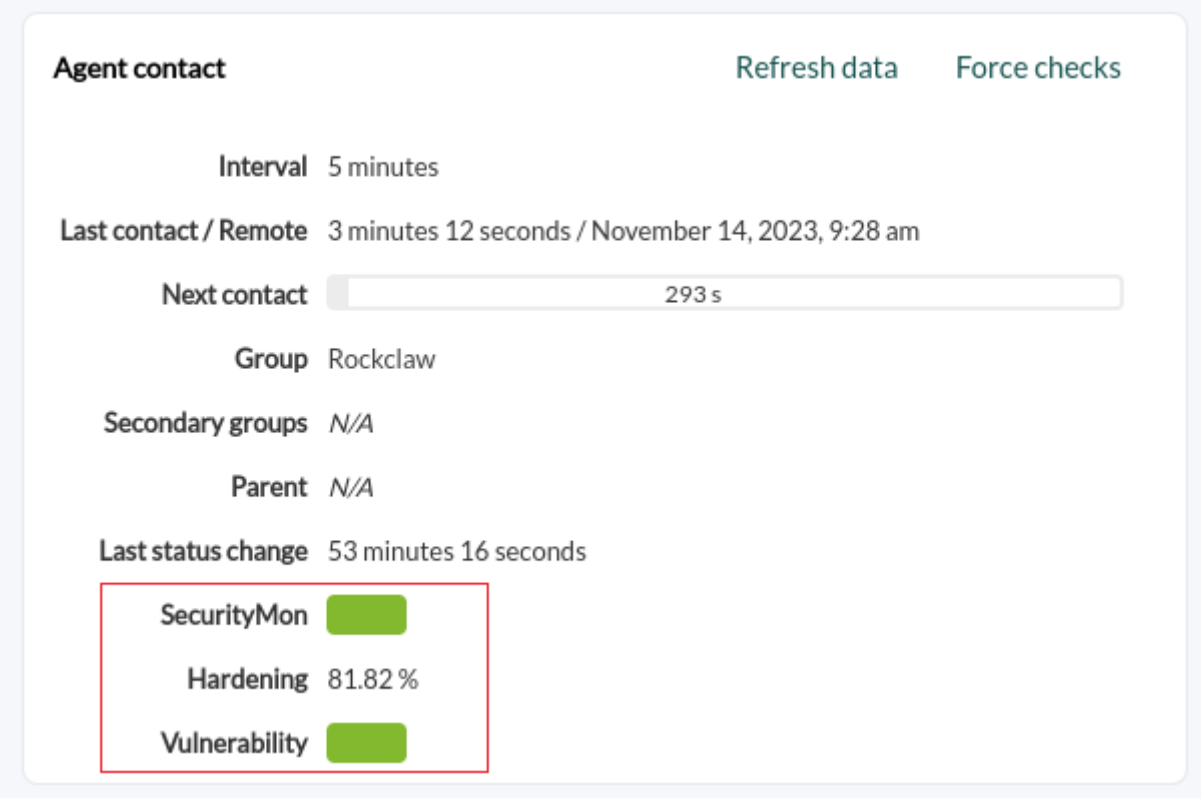
En plus du *dashboards* et des vues spécifiques pour pouvoir analyser ces données dans des systèmes spécifiques ou au niveau global, il existe certains modules générés par le système de hardening qui permettront de traiter les données d'évaluation du hardening comme les autres données Pandora FMS, pour établir des alertes, générer des graphiques ou toute autre utilisation nécessaire. Ces modules sont générés ou mis à jour automatiquement à chaque fois qu'un audit de renforcement est exécuté et appartiennent au Module group appelé Security.

- Durcissement - Échec des contrôles: Il affiche le nombre total de contrôles qui n'ont pas réussi le test de sécurisation.
- Durcissement - Vérifications non appliquées: Il affiche le nombre total de vérifications qui n'ont pas été exécutées parce qu'elles ne s'appliquent pas (par exemple, il vérifie une autre version de votre distribution Linux ou une version de Windows, ou parce qu'elles recherchent un certain composant non installé).
- Durcissement - Contrôles réussis: Il affiche le nombre total de contrôles qui ont réussi le test de sécurisation.
- Durcissement - Score: Il affiche le pourcentage de contrôles réussis. Un seuil peut être défini ici pour indiquer quand le système est dans l'état «Avertissement» ou «Critique» en matière de sécurité.

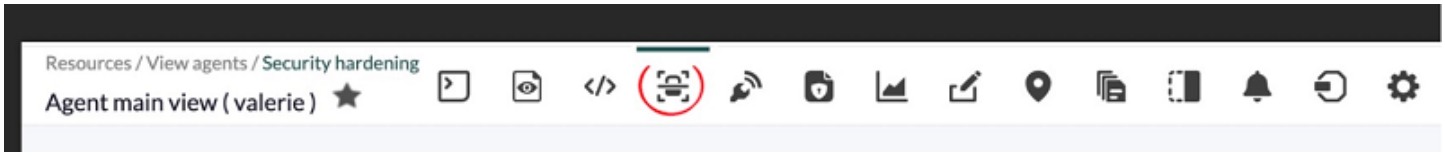


Affichage des données de hardening

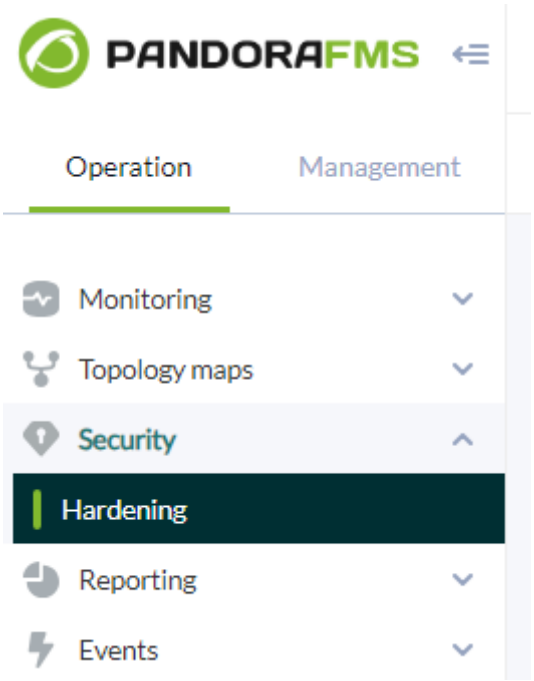
Une fois que les agents ont exécuté le module de durcissement pour la première fois, les informations arrivent et vous pouvez voir dans le détail de chaque agent (Operation → Monitoring views → Agent detail → Agent main view) dans la boîte Agent Contact trois éléments qui résument l'état de la sécurité (SecurityMon, en passant la souris dessus, vous verrez le nombre de modules de sécurité), le pourcentage de sécurité atteint (Hardening) et l'état de la vulnérabilité (Vulnerability, en passant la souris dessus, vous verrez le score atteint):

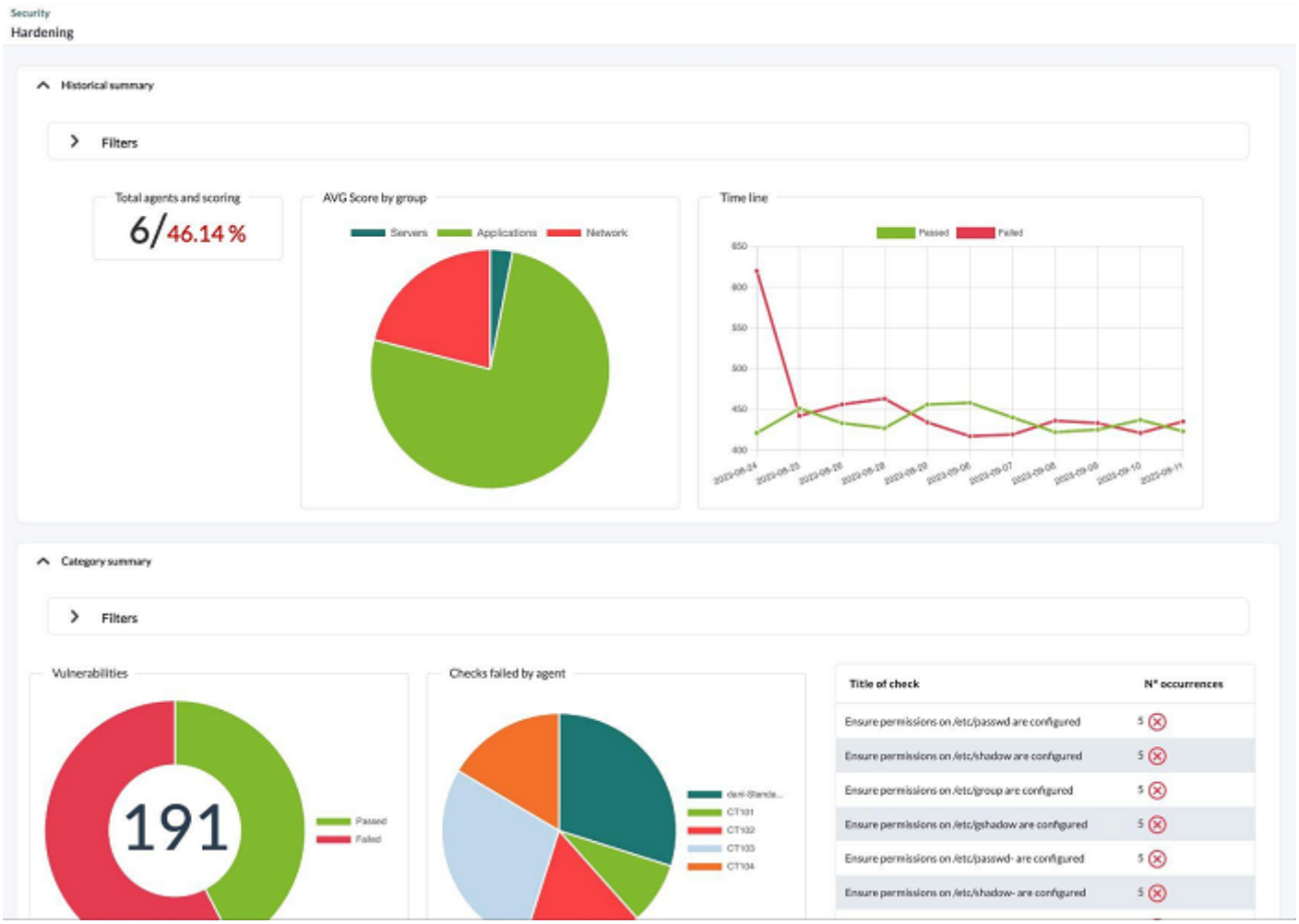


Une section spécifique sera également mise en place pour le durcissement de ces agents :



En outre, vous verrez une section dans le menu d'opération appelée « Sécurité » (Security), où il y a un tableau de bord spécifique pour les données Hardening où vous pouvez filtrer par groupes, agents, catégories CIS et d'autres détails.





Rapports de hardening

De nouveaux report types ont été créés pour afficher les informations de renforcement :

- Top N agents avec le pire score. Filtré par groupes.
- Top N des contrôles qui échouent le plus fréquemment. Filtré par groupes.
- Graphique circulaire avec vulnérabilités par type. En choisissant une catégorie CIS, les échecs, réussites et ignorés (facultatif) de tous les agents sont regroupés (ou uniquement le groupe sélectionnés) par catégorie.
- Les N premiers contrôles ayant échoué par catégorie, les dernières données de tous les agents (ou uniquement du groupe sélectionné) sont regroupées par catégories de renforcement et les catégories avec le plus grand nombre d'échecs parmi tous les agents sont répertoriées.
- Liste des contrôles de sécurité est un rapport technique et exhaustif avec tous les détails, les derniers contrôles d'un agent sont répertoriés, filtrés par groupe, catégorie et état.
- Scoring, le dernier scoring des agents du groupe sélectionné ou de tous dans la plage de temps sélectionnée dans le filtre par défaut des rapports est affiché. Le dernier score de chaque agent dans la plage temporelle est toujours pris en compte, c'est-à-dire que si une plage d'un mois est définie, le dernier score des agents au cours de ce mois sera recherché.
- Évolution, une évolution globale du durcissement est montrée en faisant la moyenne des tests réussis et de ceux qui ont échoué, regroupés par jour, pour tous les agents ou ceux du groupe sélectionné.

Voici quelques exemples de rapports 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

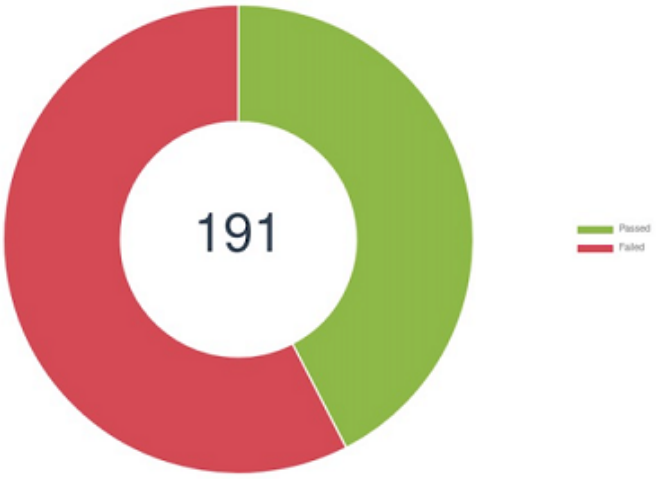
PANDORAFMS ENTERPRISE

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*

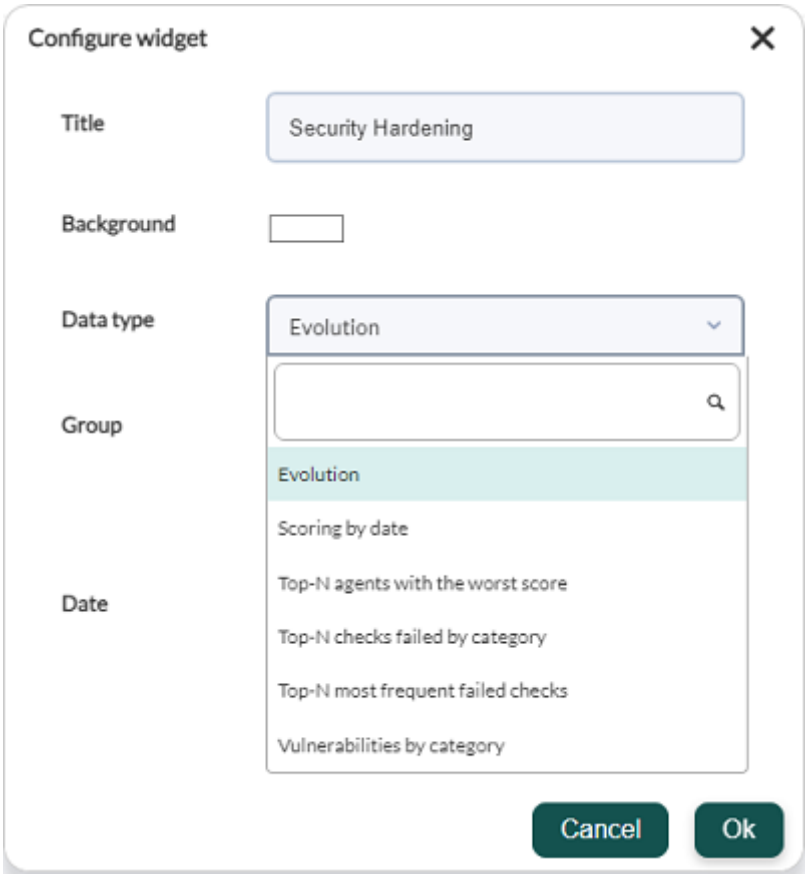
List of checks

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

Tableau de bord de hardening

Un nouveau widget dans le tableau de bord Pandora FMS regroupe les rapports les plus renforcés:

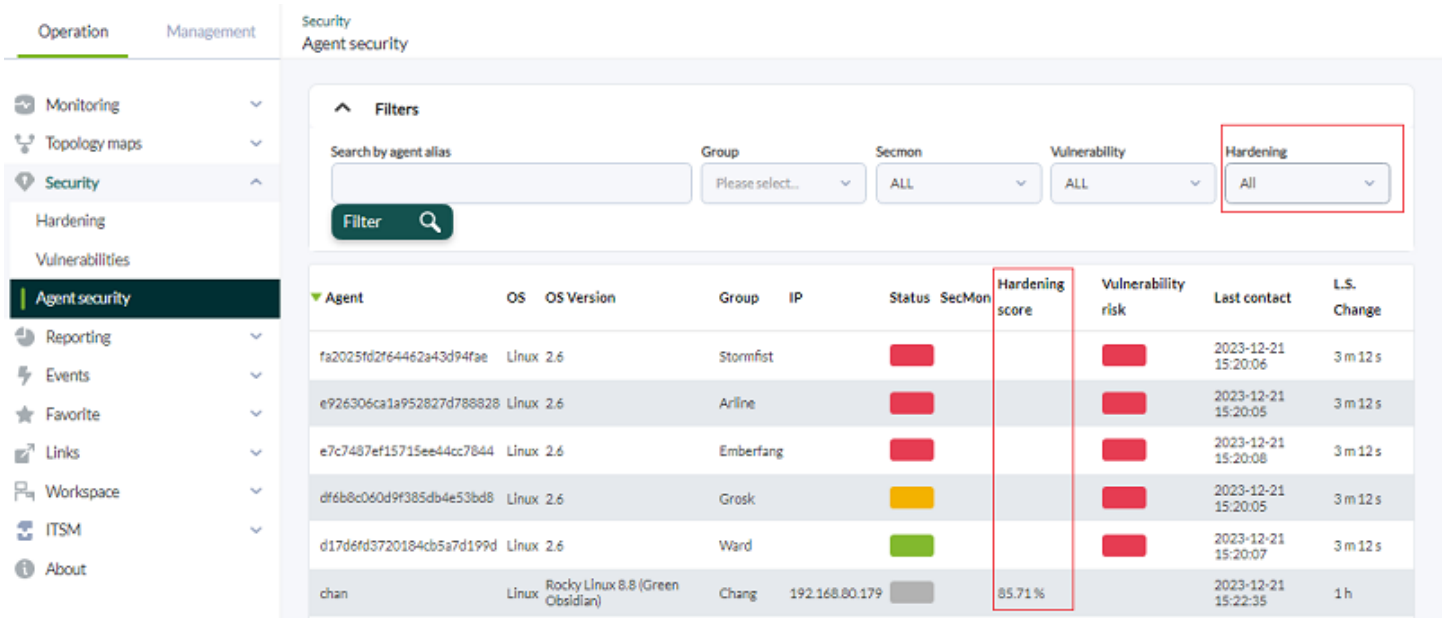
Options de configuration:



Vue de sécurité des agents

Menu Operation → Security → Agent security.

Dans la vue de sécurité des agents, dans la colonne Hardening, vous pourrez voir le score de chaque agent, parmi d'autres données. Vous pouvez filtrer par pourcentage de score de hardening et inclure d'autres champs supplémentaires. Pour afficher les agents sans score de hardening, utilisez l'option All.



Revenir à l'index de la documentation Pandora FMS