セキュリティ強化の監視

セキュリティ強化の監視

Pandora FMS ドキュメント一覧に戻る

強化監視

インターネットセキュリティセンター (CIS) の推奨事項を、Pandora FMS の監視技術 と統合し、統合された保証監査システムを提供します。これにより、使用および監視対象の環境におけるセキュリティ強化策の進捗状況を、時間の経過とともに追跡および評価できます。

システム強化とは、攻撃対象領域を縮小し、防御を強化することでコンピュータシステムのセキュリティを向上させるプロセスです。これは、デフォルト設定、間違った設定、あるいは不適切な設定など、潜在的な攻撃者が設定の問題を見つけることをより困難にすることを意味します。

セキュリティの脅威と脆弱性は時間とともに進化するため、システムの強化は継続的なプロセスです。状況の変化に適応するためには、継続的な監視、リスク評価、そしてセキュリティ設定の調整が必要です。さらに、組織は、CIS 管理策や 米国国立標準技術研究所 (NIST) ガイドラインなど、業界固有の標準やベストプラクティスに従い、システムの総合的な強化を図ることがよくあります。

Pandora FMS は、実行するチェックをグループ化するために複数の CIS カテゴリを使用します。

Pandora FMS で監査される CIS カテゴリ

当社では、安全性が極めて重要なさまざまなカテゴリにわたって 1,500 を超える個別のチェックを実施することで CIS の推奨事項をさらに一歩進めています。

ハードウェアおよびソフトウェア資産のインベントリと管理：組織内のすべてのデバイスとソフトウェアを監視および管理します。テクノロジー資産の最新のインベントリを維持し、認証を使用して不正なプロセスをブロックします。

デバイスのインベントリと管理：ハードウェアデバイスを識別・管理し、許可されたデバイスのみがアクセスできるようにし、それ以外のデバイスはブロックします。適切なインベントリを維持することで、内部リスクを最小限に抑え、環境を整理し、ネットワークの透明性を確保できます。

脆弱性管理：資産を継続的に分析し、潜在的な脆弱性を検出して、攻撃の入り口となる前に修正します。組織内のソフトウェアとオペレーティングシステムを常に最新のセキュリティ対策とパッチで更新することで、ネットワークセキュリティを強化します。ソフトウェア管理を支援し、承認されたソフトウェアのみがインストールおよび実行されるようにします。正確なインベントリを維持し、ソフトウェアを管理することで、脆弱性とリスクを回避します。

管理者権限の適切な使用：アクセス制御と特権アカウントを持つユーザーの行動を綿密に監視し、重要なシステムへの不正アクセスを防止します。管理者権限の不正使用を防ぐため、適切な権限を付与されたユーザーのみがアクセスできるようにします。権限の不正使用を防ぐための厳格なポリシーを確立します。

ハードウェアとソフトウェアの構成をセキュリティで保護する：組織が承認した標準に基づいてセキュリティ構成を確立し、維持します。不適切な構成を検出して警告する厳格な構成管理システムを構築し、攻撃者が脆弱なサービスや構成を悪用するのを防ぐための変更管理プロセスを確立します。

ログと監査ログの維持、監視、分析：イベント監査ログを収集、管理、分析し、潜在的な異常を特定します。詳細なログを維持することで、攻撃を完全に理解し、セキュリティインシデントに効果的に対応できます。

マルウェア対策：組織内の様々なポイントにおける悪意のあるコードのインストールと実行を監視・制御し、攻撃を防止します。マルウェア対策ソフトウェアを設定・使用し、自動化を活用することで、迅速な防御アップデートと攻撃発生時の迅速な是正措置を確実に実施できます。

メールとウェブブラウザの保護：ウェブブラウザとメールシステムをオンラインの脅威から保護・管理し、攻撃対象領域を縮小します。許可されていないメールプラグインを無効化し、ウェブベースのURLフィルターを使用して、ユーザーが信頼できるウェブサイトにのみアクセスできるようにします。共通の入口を攻撃から守ります。

データ復旧能力：組織の重要な情報が適切にバックアップされていることを確認するためのプロセスとツールを確立します。重要なデータが侵害されるような攻撃が発生した場合でも、情報を復元できる信頼性の高いデータ復旧システムを確保します。組織がデータ損失に効果的に対処できるよう準備を整えます。

境界防御とデータ保護：機密データを特定・分離し、暗号化、データ侵入防止計画、データ損失防止技術を含む一連のプロセスを確立します。不正アクセスを防止するための強固な障壁を構築します。

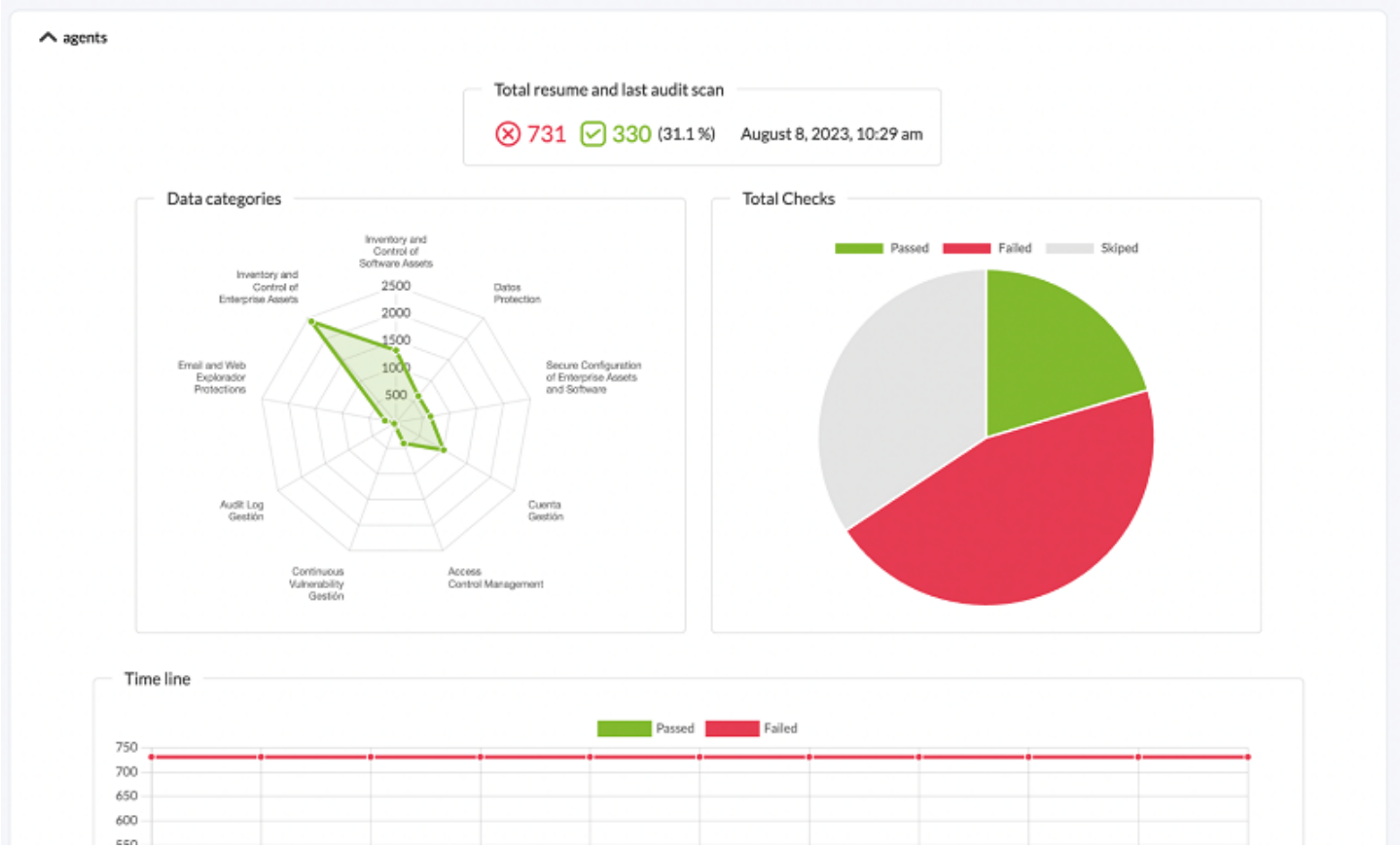
監視とアカウント制御：システムとアプリケーションアカウントのライフサイクル全体、つまり作成から削除、使用中、そして非アクティブ状態に至るまでを綿密に監視します。この積極的な管理により、攻撃者が正当なユーザアカウントを悪意のある目的で悪用するのを防ぎ、アカウントとそのアクティビティを常に制御できます。

各マシンの詳細な強化監査

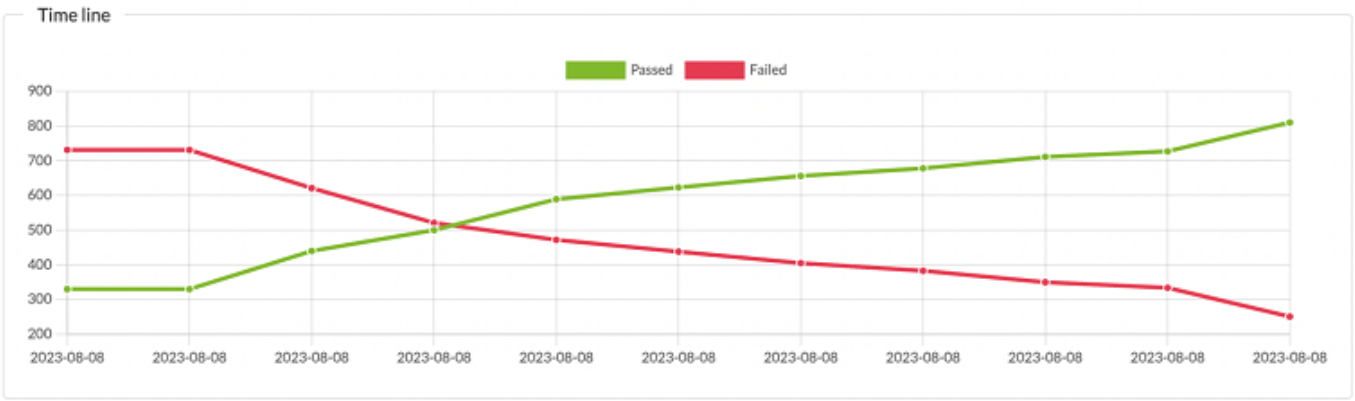
チェックは、各マシンで実行される エンドポイント によって実行されます。通常、監査は毎週行われますが、1か月など、より長い期間に設定することもできます。これにより、システムのセキュリティのスナップショットを取得し、セキュリティインデックス（実行され承認されたチェックとテ

ストに合格しなかったチェックの割合として定義される数値評価）を計算して割り当て、その安全性インデックスの経時的な変化を確認できます。

システムの強化状態の「スナップショット」の例:



システムの強化が時間の経過とともにどのように進化するかの例:



システムでは、実行されたチェックをカテゴリ別に分類して確認できます。

Summary of categories

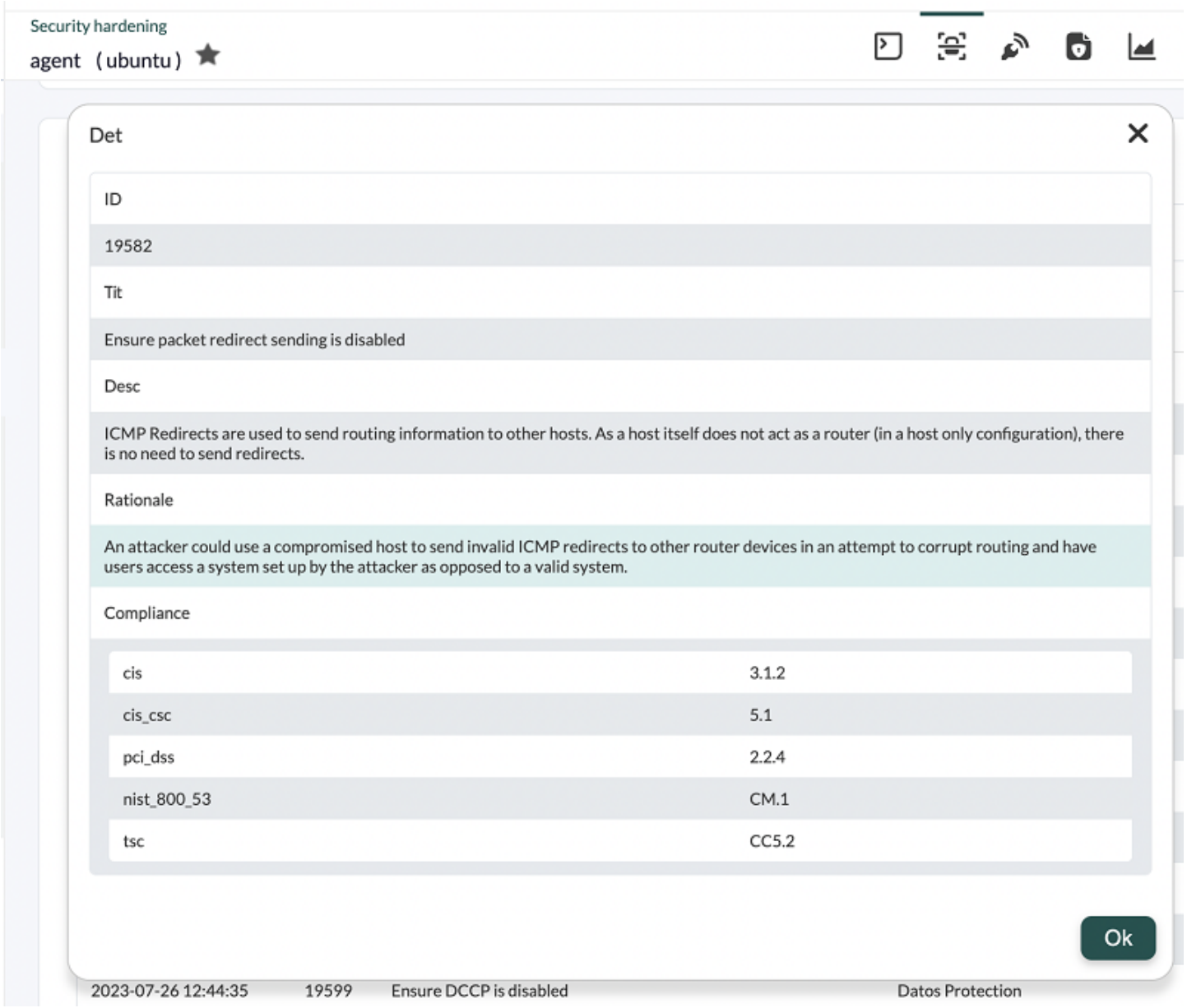
Inventory and Control of Software Assets	14	46	23 %
Data Protection	20	118	14 %
Secure Configuration of Enterprise Assets and Software	21	126	14 %
Account Management	78	193	29 %
Access Control Management	92	16	85 %
Continuous Vulnerability Management	8	14	36 %
Audit Log Management	0	20	0 %
Email and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

それぞれの要素グループの詳細を確認し、修正作業を行うことができます。

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		



強化監視設定

各システム（該当する場合）に応じて、監視対象環境における適切な制御方法を開発しました。現在、この機能はMS Windows® および Linux® サーバで利用可能です。

この機能は 773 以降のエンドポイントで利用できます。エンドポイントが 773 より前のバージョンの場合は、更新する必要があります

そのためには、エンドポイント設定で対応するプラグインを有効化します。これは手動で行うことも、マシングループの監視ポリシーを通じて行うこともできます。

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
```

これらの例では、強化監査は7日ごとに実行され、監査中に実行される各コマンドのタイムアウトは 150秒です。この値を 30日に増やすことも可能ですが、不要なインベントリデータが生成されるため、数日ごとに実行することはお勧めしません。

強化データ監視

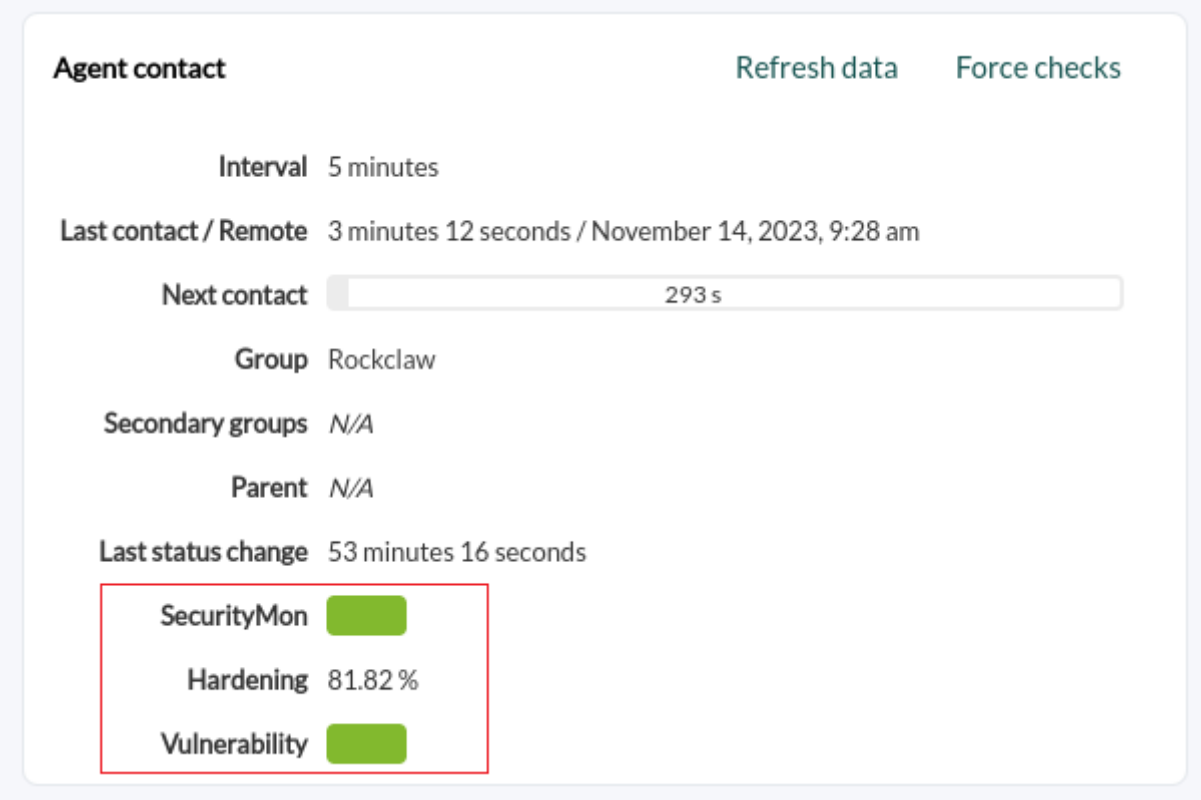
特定のシステムまたはグローバルレベルでこのデータを分析するための ダッシュボード と特定のビューに加えて、強化システムによって生成されるいくつかのモジュールがあり、強化評価データを他の Pandora FMS データと同様に処理して、アラートを生成したり、グラフを生成したり、その他の必要な用途に使用したりできます。これらのモジュールは、強化監査が実行されるたびに自動的に生成または更新され、モジュールグループ の セキュリティ に属します。

- 強化 - 失敗したチェック(Hardening - Failed checks): セキュリティテストに合格しなかったチェックの総数が表示されます。
- 強化 - 適用されなかったチェック(Hardening - Not applied checks): 適用されないため実行されなかったチェックの総数が表示されます（例: Linuxディストリビューションの別のバージョンや Windows バージョンのチェック、またはインストールされていない特定のコンポーネントを探すチェックなど）。
- 強化 - 合格したチェック(Hardening - Passed checks): セキュリティテストに合格したチェックの総数が表示されます。
- 強化 - スコア(Hardening - Score): 合格したチェックの割合が表示されます。ここでしきい値を設定することで、システムがセキュリティに関して「警告」または「障害」状態にあるかどうかを確認できます。

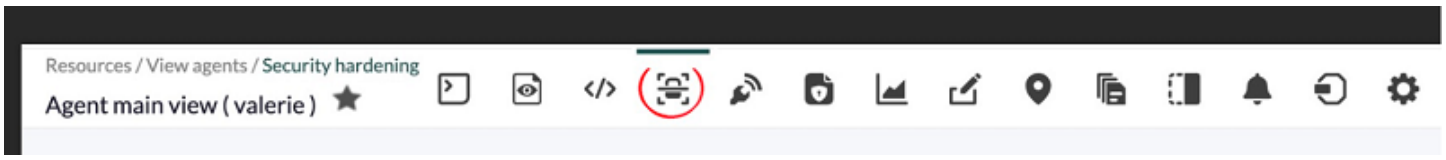
Hardening - Failed checks	Number of failed checks across policies.		N/A - N/A	2
Hardening - Not applied checks	Number of checks that did not apply across policies.		N/A - N/A	192
Hardening - Passed checks	Number of passed checks across policies.		N/A - N/A	10
Hardening - Score	% of passed checks (0 to 100).		N/A - N/A	83.3

強化データ表示

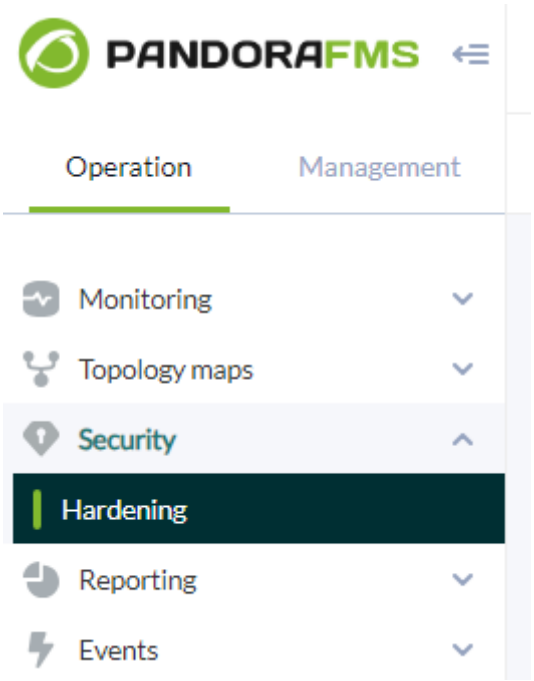
エンドポイントが強化モジュールを初めて実行すると、情報が到着し、各エンドポイントの詳細 (操作(Operation) → 表示(Monitoring views) → エージェント詳細(Agent detail) → エージェントメイン画面) の エージェント接続 ボックスに、セキュリティステータス (SecurityMon、ポインターを合わせるとセキュリティモジュールの数が表示されます)、達成されたセキュリティのパーセンテージ (強化(Hardening))、および脆弱性ステータス (脆弱性(Vulnerbility)、ポインターを合わせると達成されたスコアが表示されます) を要約した 3 つの要素が表示されます。

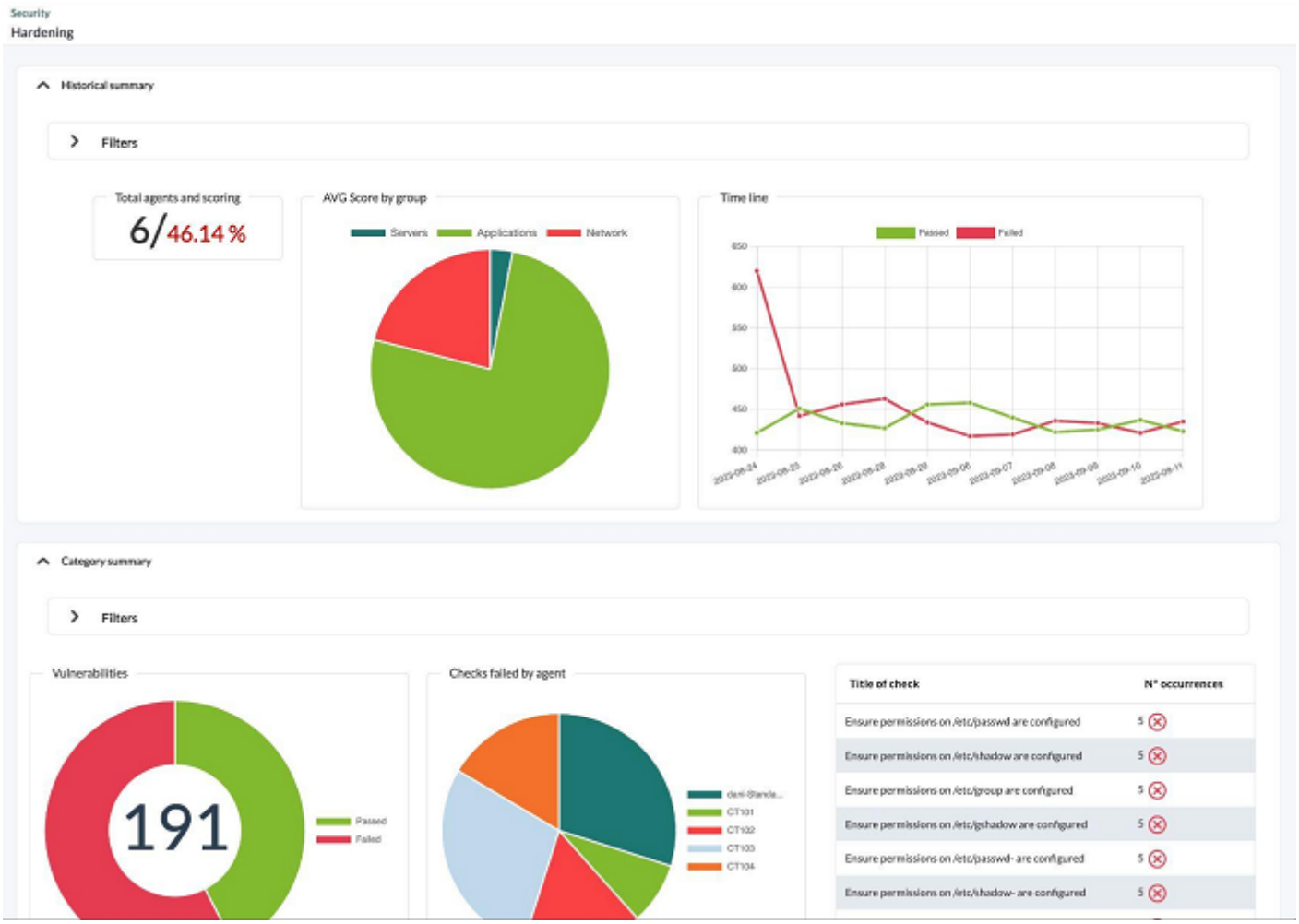


これらのエージェントの強化のために、特定のセクションも有効になります。



さらに、操作メニューに セキュリティ(Security)(というセクションが表示されます。ここには、強化(Hardening) データ用の 特定のダッシュボード があり、グループ、エージェント、CIS カテゴリ、その他の詳細でフィルタリングできます。





強化レポート

強化情報を表示するための新しい レポートタイプ があります。

* スコアが最も低い上位Nのエージェント(Top N agents with the worst score)。グループ別にフィルタリングされます。 * 最も頻繁に失敗するチェックの上位N(Top N of checkups that fail most frequently)。グループ別にフィルタリングされます。 * 脆弱性の種類別円グラフ(Pie chart with Vulnerabilities by type)CISカテゴリを選択すると、すべてのエージェント（または選択したグループのみ）の不合格、合格、スキップ（オプション）がカテゴリ別にグループ化されます。 * カテゴリ別に失敗するチェックの上位N(Top N of checks that fail by category)。すべてのエージェント（または選択したグループのみ）の最新データが強化カテゴリ別にグループ化され、すべてのエージェントの中で不合格数が最も多いカテゴリがリストされます。 * セキュリティチェックのリスト(List of security checks)。すべての詳細を含む技術的かつ包括的なレポートで、エージェントの最新のチェックがグループ、カテゴリ、ステータス別にフィルタリングされてリストされます。 * スコアリング(Scoring)。選択したグループのエージェント、またはレポートのデフォルトフィルタで選択された期間内のすべてのエージェントの最新のスコアリングが表示されます。時間範囲内の各エージェントの最新のスコアリングが常に取得されます。つまり、1か月の範囲が設定されている場合、その月内のエージェントの最新のスコアリングが検索されます。 * 進化(Evolution) では、すべてのエージェントまたは選択したグループ内のエージェントについて、合格したテストと不合格のテストを日ごとにグループ化して平均することで、強化の全体的な進化が表示されます。

PDF レポートの例をいくつか示します。

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

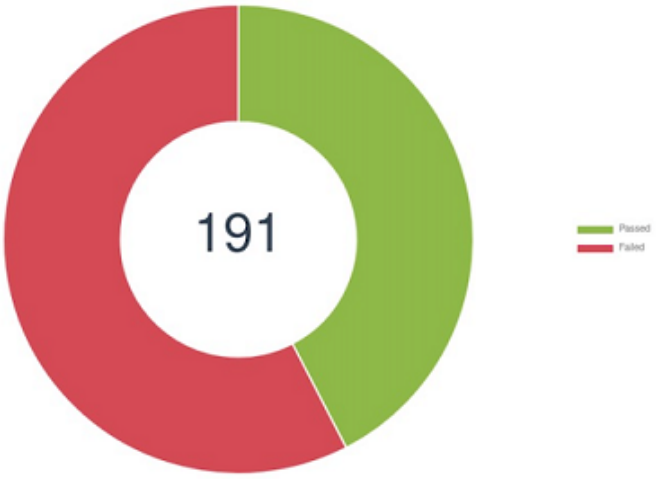
PANDORAFMS ENTERPRISE

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*

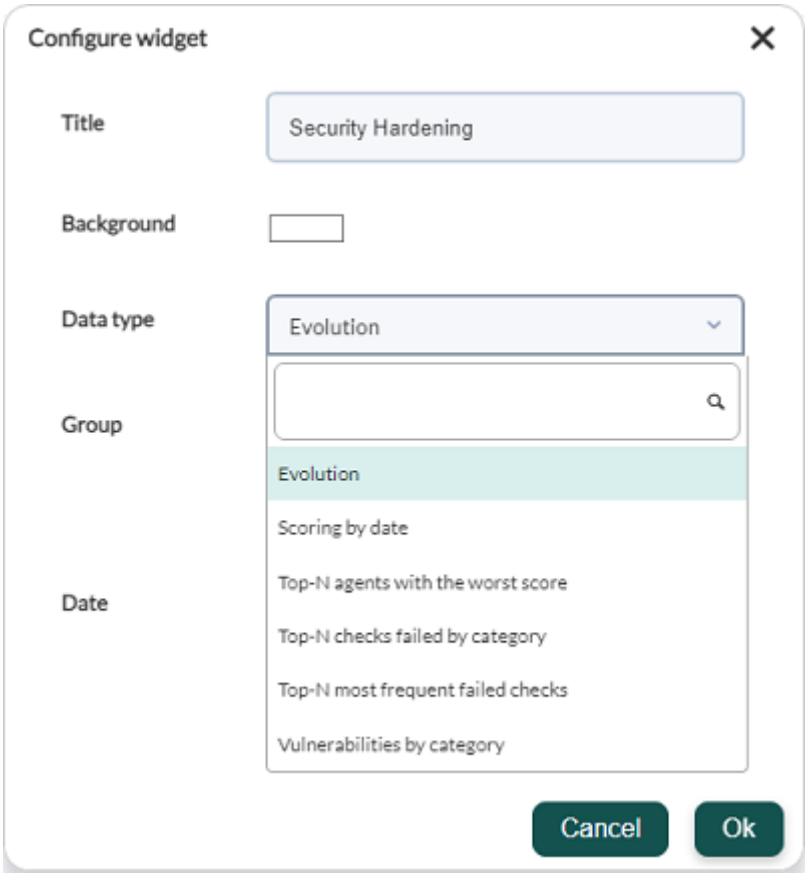
List of checks

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

強化ダッシュボード

Pandora FMS ダッシュボードの新しいウィジェットは、ほとんどの強化レポートをグループ化します。

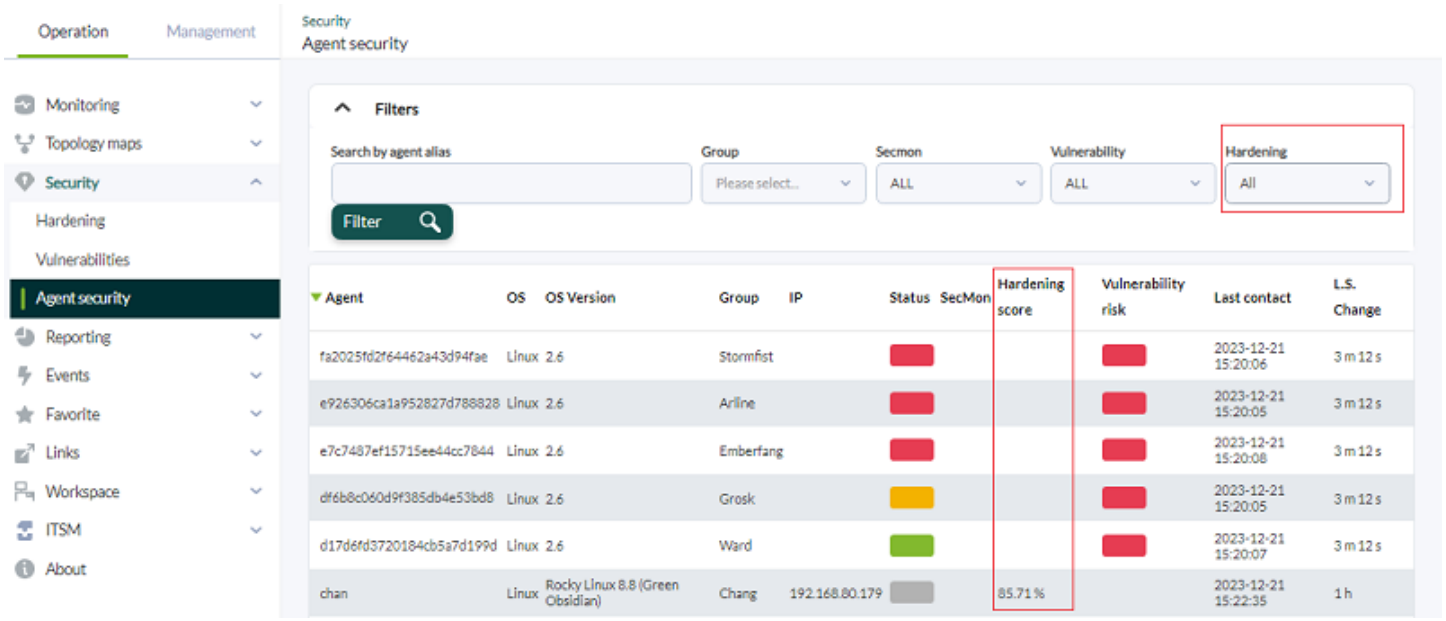
設定オプション:



エージェントのセキュリティ表示

操作(Operation) → セキュリティ(Security) → エージェントセキュリティ(Agent security) メニュー。

エージェントのセキュリティ表示の強化(Hardening)列では、各エージェントのスコアをはじめとするデータを確認できます。強化スコアのパーセンテージでフィルタリングしたり、その他の追加フィールドを含めたりすることも可能です。強化スコアのないエージェントを表示するには、すべて(All)オプションを使用してください。



Pandora FMS ドキュメント一覧に戻る