PANDORAFMS

インベントリ

インベントリ

Pandora FMS ドキュメント一覧に戻る

概要

Pandora FMS を使用すると、Pandora FMS によって監視されているデバイスのインベントリを保持できます。このインベントリにより、次のような 一覧およびレポート を管理できます。

-  CPU モデルと速度 (MS Windows®, GNU/Linux®)
-  ストレージとファイルシステム
-  ファームウエアバージョン (ネットワークハードウエア)
-  デバイス設定 (ネットワークハードウエア)
-  シリアル番号およびライセンス (例: MS Office®, MS Windows®).
-  コンピュータにインストールされたアプリケーション (MS Windows®, Android Linux®, GNU/Linux®).
-  ネットワークカードおよび IP アドレスに関連付けられた MAC
-  RAM モジュールおよび容量 (MS Windows®, GNU/Linux®)
-  ルーティング
-  実行中サービス
-  ストレージデバイス (MS Windows®, GNU/Linux®)
-  システムユーザ

インベントリデータ収集

インベントリは監視とは独立しており、次のように取得できます。

- インベントリモジュールを介して、Pandora FMS に統合されたスクリプトで、リモートから WMI クエリを実行したり、または Expect または同様の方法で SSH を実行する方法。
- エージェントプラグインを介してローカルで Pandora FMS エージェントを利用する方法。

インベントリモジュール

インベントリモジュールは、リモートのマシンにコマンドを実行するリモートモジュールです。これらのモジュールは、プラグインと同じように動作します。エージェントを通してデータを取得するローカルモジュールと同じものを定義することができます。

ユーザおよびパスワードでは、_agentcustomfield_n_ (エージェントのカスタムフィールド番号 n) マクロが利用できます。

リモートインベントリ

Pandora FMS では、多数のインベントリ モジュールがデフォルトでインストールされており、インベントリモジュールエディタを使用して新しいインベントリモジュールを作成したり、既存のインベントリモジュールを変更、削除、カスタマイズしたりすることもできます。

リモートモジュールの作成

管理(Management) → 設定(Configuration) → インベントリモジュール(Inventory Modules) メニューから一覧が表示され、作成(Create) ボタンを押すと新規追加できます。

重要なフィールドは次の通りです。

- インタープリタ(Interpreter): ローカルモジュールの場合は空にします。モジュールで使われるコマンドインタープリタを入力するフィールドです。シェルスクリプト、Perl、その他インベントリサーバで実行できるスクリプト言語を利用できます。
- コード(Code): ローカルモジュールの場合は空にします。Perl やシェルスクリプトなどのプログラムを設定します。バイナリの実行ファイルの場合、別途それを呼び出すスクリプトが必要です。
- ブロックモード(Block mode): 設定の 変更を表示・検出します。
- フォーマット(Format): モジュールが返す値を ; で分割したフィールドを入力します。

- フォーマット(Format)では、各フィールドをセミコロンで区切って配置してください。 このフィールドを省略すると、インベントリモジュールを作成または保存できなくなり、行われた変更はすべて失われます。
- インベントリモジュールをエージェントに追加すると、モジュールのオペレーティングシステムがエージェントのオペレーティングシステムと一致するモジュールのみが表示されるため、対応するオペレーティングシステムを選択することが非常に重要です。

リモートモジュールの割当

インベントリモジュールの割り当ては、エージェント自体で実行されます。エージェント管理タブで、インベントリ タブをクリックします。

- モジュール(Module): 追加したいインベントリモジュールを選択します。エージェントのオペレーティングシステムに合うモジュールのみが表示されます。
- 対象(Target): インベントリを取得する対象の IP アドレスもしくはホスト名を設定します。
- 間隔(Interval): インベントリモジュールの実行間隔を設定します。

通常存在するユーザ名とパスワードの代わりにフィールドを定義することができます。そのためには、カスタムフィールドの利用(Use custom fields) を有効化する必要があります。 これを行うと、新しいフィールドを追加するためのコントロールが表示されます (フィールド追加(Add field))

- このコントロールでは、追加する前に希望の名前を入力する必要があります。
- フィールドにパスワードを含めるようにする場合は、It's a password と入力すると、値が難読化された方法でデータベースに保存されます。
- フィールドを作成した後、フィールドに値を指定し、最後にモジュールを追加できます。
- これらのフィールドは、リモートインベントリスクリプトの実行時に作成順に適用されます。

ソフトウエアエージェントによるローカルインベントリ

ソフトウエアエージェントを通してインベントリデータを取得することができます。ソフトウエアエージェントの設定に、必要なインベントリモジュールを適用すれば良いだけです。

リモートモジュールと同様に、これらのモジュールは、管理(Management) → 設定(Configuration) → インベントリモジュール(Inventory modules) でインベントリモジュールとして追加する必要があります。

ローカルモジュールの作成

ローカルモジュールを作成するには、管理(Management) → 設定(Configuration) → インベントリモジュール(Inventory modules) へ行きます。作成済みの全インベントリモジュールが表示されます。エージェント設定内で定義されるすべてのモジュールを作成します。 コンソール上でエージェントに割り当てられた OS は、作成されたモジュールの OS と一致する必要があります。

手順は、インタプリタ(Interpreter) および コード(Code) フィールドを設定すること以外、リモートの場合と同じです。新しく作成したインベントリモジュール (その他すべてのモジュール) を編集するには、名前またはスパナアイコンをクリックします。

ソフトウエアエージェントによる Windows のインベントリモジュール

これらのプラグインは、ソフトウェアエージェントのインストール時にデフォルトで導入されていますが、設定ファイル内でコメントアウトされています。利用する場合はコメントを外し、ソフトウェア エージェントを再起動します (リモート設定によりソフトウェアエージェントを再起動できます)。

MS Windows® の例:

```
#module_begin
#module_plugin cscript.exe B t:20
"%PROGRAMFILES%\Pandora_Agent\util\cpuinfo.vbs"
```

```
#module_crontab * 12-15 * * 1
#module_end
```

追加の設定は、スクリプトコレクション Pandora FMS ライブラリ内 からダウンロードできます。それぞれに使用説明があります。また、ローカルインベントリスクリプトの定期実行は、pandora_agent.conf ファイルの末尾に情報を追加して設定する必要があります。

ソフトウエアエージェントによる UNIX のインベントリモジュール

Unix のソフトウエアエージェントのモジュールは、マシンのソフトウエアおよびハードウエア情報を取得するためにローカルで定義されたプラグインを利用します。

インベントリーを収集するプラグインはディレクトリ /etc/pandora/plugins にあります。

モジュールの書式は次の通りです。

```
module_plugin inventory 1 cpu ram video nic hd cdrom software init_services
filesystem users route
```

モジュールは、次のパラメータを一行で設定します。

- モジュールの有効化

```
"module_plugin inventory" 1 cpu ram video nic hd cdrom software init_services
filesystem users route
```

- モジュールの実行間隔 (日単位) の設定。値が 0 の場合は、エージェントの実行時にインベントリ情報が送信されます。

```
module_plugin inventory "1" cpu ram video nic hd cdrom software init_services
filesystem users route
```

- 収集するインベントリの対象の設定

```
module_plugin inventory 1 "cpu ram video nic hd cdrom software init_services
filesystem users route"
```

利用可能なすべての情報を収集するように指定することもできます。 この例では、すべてのインベントリ情報を毎日収集します。

```
  # Plugin for inventory on the agent
  module_plugin inventory 1
```

インベントリモジュールを有効化するには、上記の設定をソフトウエアエージェントの pandora_agent.conf に記述しエージェントを再起動します。

ローカルモジュールの割当

エージェントで定義したモジュールはコンソールで有効化する必要はありません。

- 設定(Configuration) → インベントリモジュール(Inventory modules) をクリックしてモジュールが作成され、
- ソフトウエアエージェントの設定ファイルに設定された OS が一致すれば、
- コンソール上のエージェントの 表示(view) → インベントリ(inventory) に現れます。

ソフトウエアエージェントでのローカルインベントリモジュールの作成

エージェントにあらかじめ設定されたインベントリシステムに加えてUnix® および MS Windows® システム用のインベントリモジュールを作成できます。 基本的には、次の構造の XML を生成するスクリプトを作成する必要があります。

```
<inventory>
     <inventory_module>
         <name>INVENTORY_MODULE_NAME</name>
         <type>generic_data_string</type>
         <datalist>
             <data>DATA1;DATA2;DATA3....</data>
         </datalist>
     </inventory_module>
</inventory>
```

- INVENTORY_MODULE_NAME: Pandora FMS コンソールのインベントリモジュールに登録したモジュールと同じ名前を入力する必要があります。
- DATA1;DATA2... : これらは抽出されるデータであり、インベントリ モジュールで定義されています。
- ファイル pandora_agent.conf でXML を生成するスクリプトを実行するようにする必要があります。
- ローカル スクリプト実行でインベントリ情報を保存するには、コンソールでインベントリ モジュールを定義し、オペレーティングシステム、モジュール名、および保存するデータを ； で区切って指定する必要があります。
- したがってPandora FMS エージェントを再起動する 前に、Pandora FMS でインベントリモジュールを作成する必要があります。

インベントリのデータ表示

ローカルまたはリモートでシステムから収集されたインベントリデータは、エージェントもしくはコンソールのインベントリメニューから参照することができます。

インベントリメニューでのインベントリデータ表示

操作(Operation) → モニタリング(Monitoring) → インベントリ(Inventory) をクリックすることにより、エージェントのインベントリデータの参照、検索、データの CSV へのエクスポートができます。

デフォルトでは、すべてのエージェントが表示されますが、検索オプションで すべて を選択し、検

索をクリックすると、インベントリを持つすべてのエージェントのモジュールを表示できます。エージェントごとに並べる(Order by agent) オプションをチェックすると、どの検索ケース (グループ、モジュールなど) でもエージェントごとにグループ化できます。

エージェントインベントリの詳細表示では、セレクターを使用して、表示する特定のインベントリレポートの日付 (デフォルトでは 最新) を選択できます。

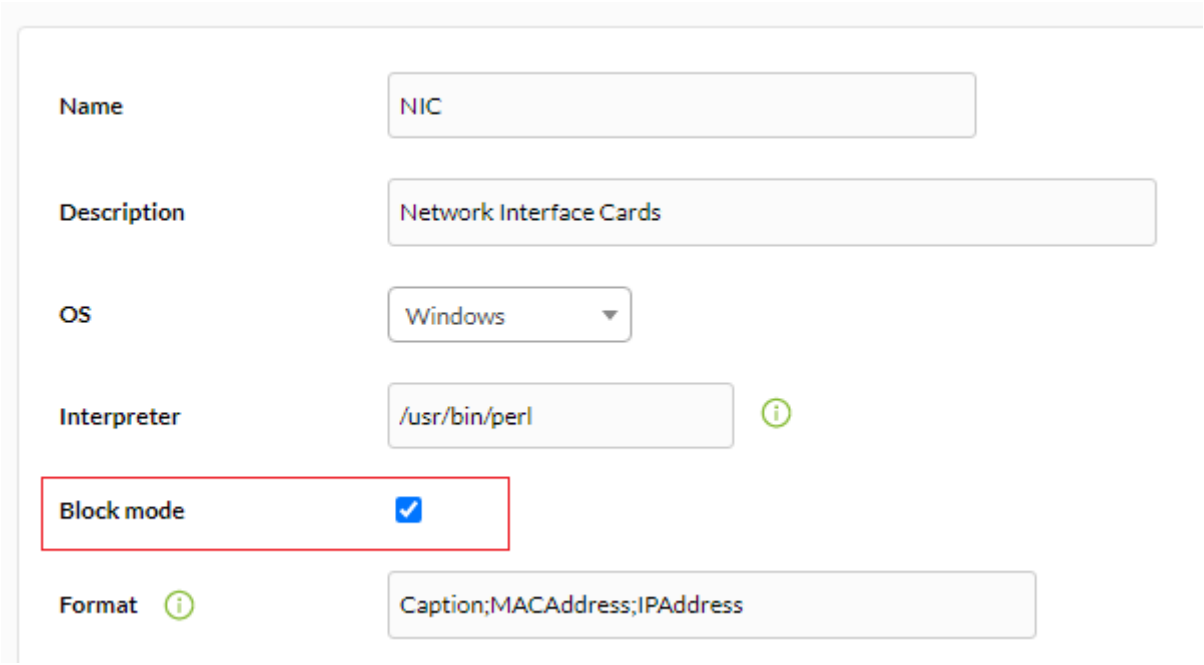
日付が無い場合は、前回のインベントリ実行からデータに変更がないことが原因である可能性があります。 つまりPandora FMS は、インベントリデータが前回の実行と比較して変化した場合にのみ保存します。

インベントリデータの CSV エクスポート

操作(Operation) → モニタリング(Monitoring) → インベントリ(Inventory) をクリックすると、フィルタリングしたあとのインベントリデータを この一覧を CSV へエクスポートする(Export this list to CSV) ボタンを使って CSV ファイルへエクスポートすることができます。CSV 区切り文字 で区切られたインベントリデータを含むファイルが作成およびダウンロードされます。

インベントリ差分

Pandora FMS は、2 つの設定間の違いを視覚的に表示し、違いを確認するために 2 つの列に表示します。 ブロックモードでは、前に見たインベントリモジュールで行われていたように、各行を同じタイプの異なる要素として解釈するのではなく、インベントリモジュールの結果全体を一つとして処理します。 ローカルまたはリモートのインベントリ モジュールを定義するときに設定されます。



インベントリアラート

バージョン NG 751 以降

インベントリアラートは、エージェントグループのインベントリコンテンツに関して特定のアラートを発報するのに役立ちます。SNMPアラートやイベントアラートと同様に、エージェントごとに適用されるのではなく、グローバルに適用されます。この場合、グループごとに適用されます。

これを設定するには、管理(Management) → アラート(Alerts) → インベントリアラート(Inventory alerts) へ行きます。

インベントリアラートには、名前、説明、時間しきい値 、アクションなど、他のアラートと似たフィールドがあります。そのため、他のアラートとの違いに焦点を当てます。

- グループ はアラート条件として機能するため、アラートは、そのグループのエージェントからのデータについて評価されます。
- これらのアラートには、アラートが発報されたときにアラートイベントを生成しないようにするためのイベントの無効化 オプションもあります。インベントリアラートアプリケーションでは、1回の実行で多くのアラートが発報されることがあるため便利です。

アラート発報条件

文字列マッチ

特定のインベントリモジュール内の特定のテキスト文字列(“software” など)を受信すると、設定されたアクションが実行されます。インベントリモジュールには 動的フィールド があることに注意する必要があります。 例えば ソフトウェアインベントリモジュールには、名前、バージョン、および説明のフィールドがあります。これにより、特定のパッケージまたは特定のバージョンのパッケージを探すのに最適な、3つの動的フィールドのいずれかにアラートを設定できます。

これらのフィールドに正規表現を追加して、より複雑な検索を行うことができます。フィールドが空の場合、 .* として扱われます(任意の値にマッチします)。

制限リスト

この場合、インベントリモジュールタイプのフィールドを 1つだけ指定し、文字列リスト(1行ずつ)を指定して、エージェントにそのリストの要素が含まれている場合にアラートが発生するようにします。リストにあるものがある場合、アラートが発生します。

許可リスト

前述のものと似ています。 インベントリフィールドの 1つに要素のリスト (条件(Condition)、ホワイ

トリスト(White list)) を指定します。ただし、今回は、インベントリモジュールの値がリストの要素の 1つにある必要があります。そうでない場合、アラートが発生します。

インベントリアラートの利用

この機能は、デバイスの脆弱なバージョン、マシン内の許可されていないユーザ、またはコンピューター内の許可されていないソフトウェアを検出するのに最適です。

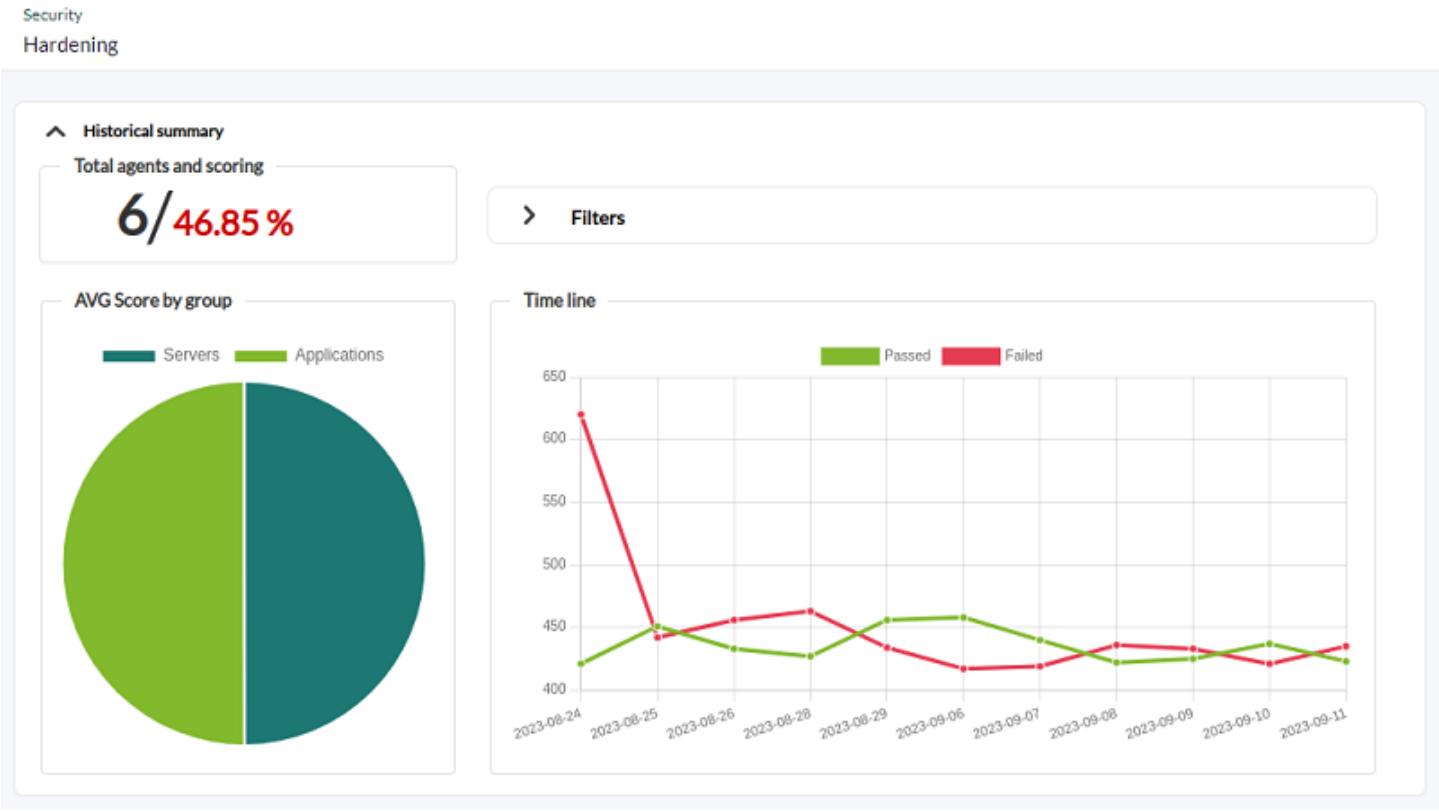
セキュリティ監視

Pandora FMS を使用すると、インベントリデータに加えて、ソフトウェアエージェントを通じて監視される各オペレーティングシステムのその他の重要な値を収集できます。これらすべては、操作(Operation) → セキュリティ(Security) → 強化(Hardening) セクションにあります。

このツールは、監視対象の各デバイスのセキュリティを強化することを目的としており、情報は 3 つの主要なセクションで表示されます。

履歴概要

履歴概要には、セキュリティを目的としたモジュールを監視するエージェントの合計数と合計平均スコア (エージェントの合計とスコア 表) が表示されます。



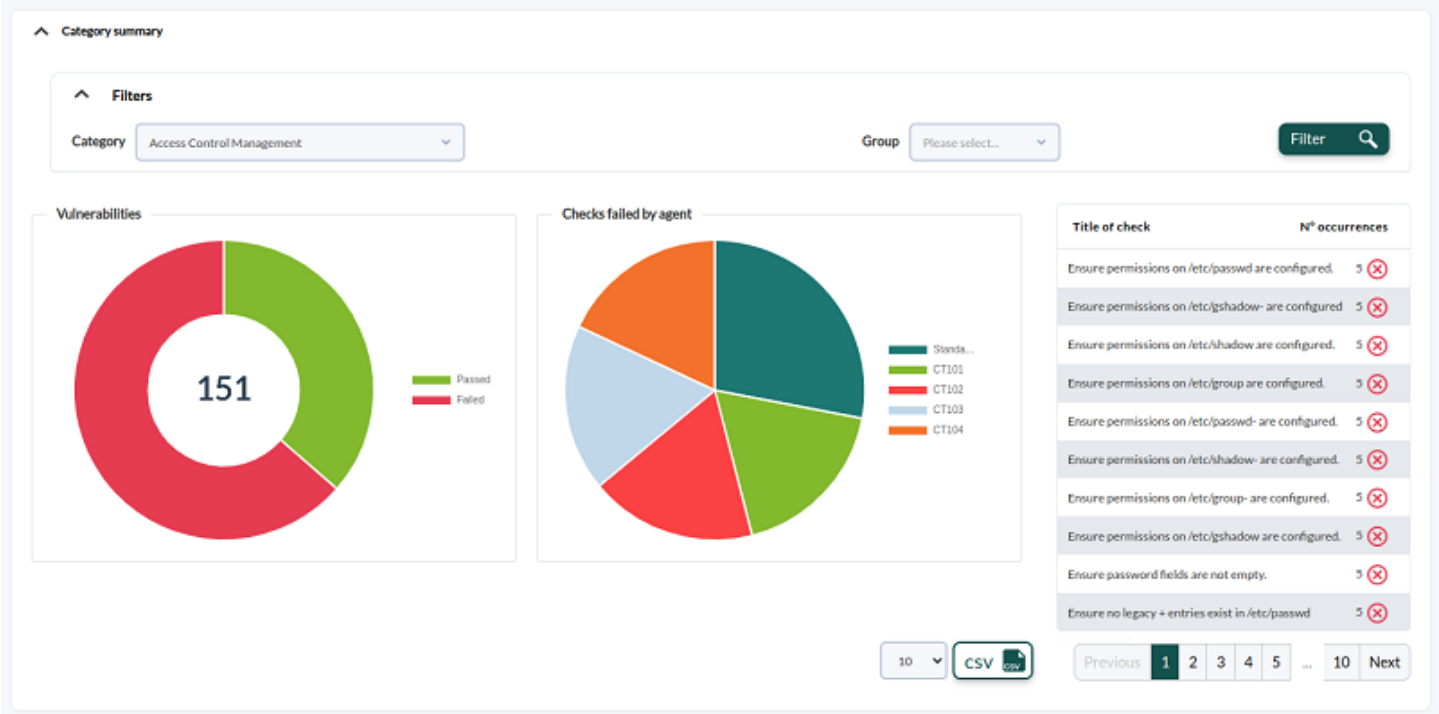
グループ別の AVG スコア 表は、Pandora FMS で定義されている各グループの平均スコアを示してい

ます。

選択した期間に関係なく、失敗したセキュリティチェックと承認されたセキュリティチェックの平均を日ごとにグループ化した履歴グラフ (タイムライン 表) もあります (最大で過去 11 日間)。 フィルタ では、カスタム期間または一般的な値 (先週、先月など) を選択できます。

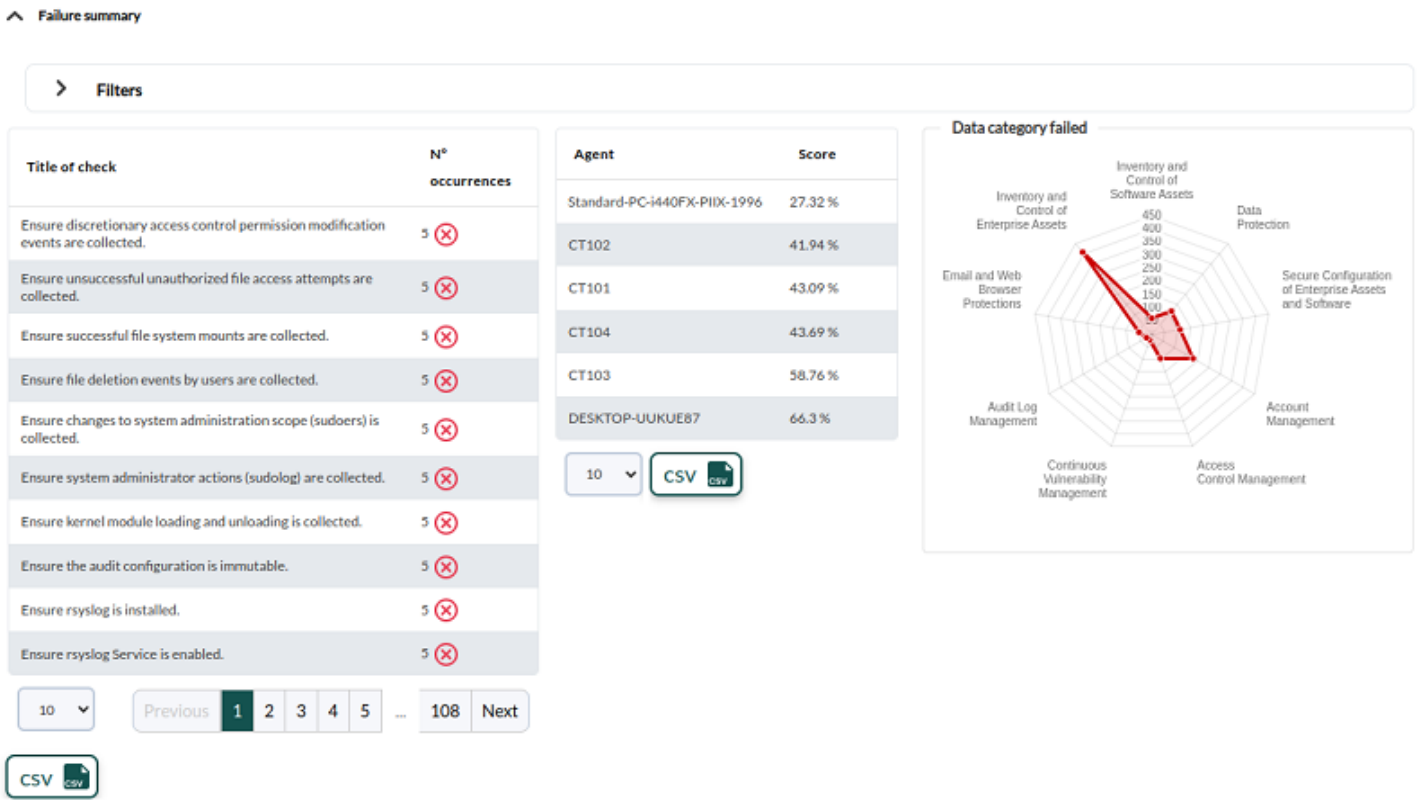
カテゴリ概要

カテゴリ別の概要 では、カテゴリ別、必要に応じてグループ別にフィルタリングして表示する必要があります。 デフォルトでは、アクセス制御管理(Access Control Management) カテゴリが選択されています。



* 脆弱性(Vulnerabilities) ボックスには、問題のある脆弱性と対処された脆弱性の合計数が表示されます。 * エージェントごとに問題のある項目 は、選択したカテゴリの問題のある項目の一覧で、グラフの各セクターをクリックすると、選択した項目と影響を受けるエージェントの詳細が一覧されます。

問題概要



問題の概要が表示されます (確認項目のタイトル): グループおよびインシデントの数によってフィルタリングされた、問題のある項目の一頼です。 フィルタ ボックスを使用して、新しい検索パラメータと表示パラメータを定義します。

また、最も低いセキュリティスコアを持つエージェントの一覧と、クリックすることにより各エージェントのセキュリティビューを表示するオプションも表示されます。

最後に、レーダーグラフにカテゴリ別の問題の分布が表示されます。

Pandora FMS ドキュメント一覧に戻る