### パターングループ

#### 概要

パターングループは、パターンをトピックごとに管理し、検出ポリシーに統合するための機能です。たとえば、IPSログルールやシグネチャ名を基にした脆弱性スキャンの識別や、SQLインジェクションなど特定の攻撃タイプのグループ化に活用できます。

ログプレッソ・ソナーはAho-Corasickアルゴリズムを採用しており、数千のキーワードを同時に検出することが可能です。これは、侵入防止システム（IPS）と同様の動作です。入力文字列をパターングループ内のすべてのキーワードと一括で照合し、該当するパターンに対して検証式を順次実行することで、パターンに一致するイベントを検出します。

パターン例

|  |  |  |  |
| --- | --- | --- | --- |
| # | パターン名 | パターン（必須）：一次高速検出 | 検証式（任意）：二次フィルター |
| 1 | xp\_cmdshell | "sp\_addextendedproc" and "xp\_cmdshell" |  |
| 2 | zb\_now\_connect | "REMOTE\_ADDR" and ("fputs" or "fwrite") | path == "lib.php" |

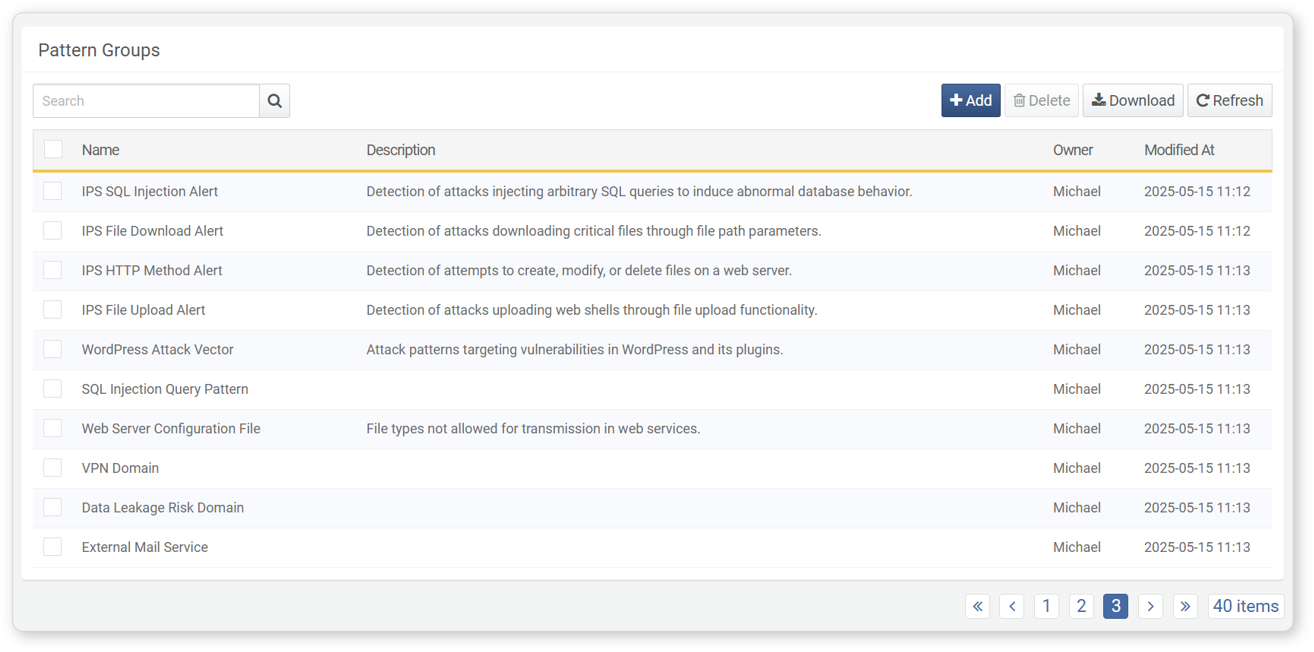
パターンは、文字列パターンとブール型の検証式で構成されます。検証式は任意です。

パターン1「**xp\_cmdshell**」では、sp\_addextendedprocとxp\_cmdshellはMicrosoft SQL Serverで頻繁に使用されるコマンドです。攻撃者はSQLインジェクションを利用してsp\_addextendedproc経由でxp\_cmdshellを登録し、システムコマンドを実行して悪意のある活動を行う場合があります。このパターンは検証式なしの例として提供されています。

パターン2「**zb\_now\_connect**」は、[ZeroBoard 4.1 pl7 - 'now\_connect()' リモートコード実行](https://www.exploit-db.com/exploits/9590)の脆弱性を悪用し、lib.php経由で任意コードをリモート実行する攻撃を検出します。このパターンは、入力フィールドにREMOTE\_ADDRとfputsまたはfwriteの両方が含まれているかを確認し、さらにpathフィールドの値がlib.phpであるかを検証します。

#### パターングループの検索

**ポリシー > パターングループ**で、パターングループの一覧を確認できます。



* **名前**: パターングループの一意な名称
* **説明**: パターングループの説明
* **所有者**: パターングループを追加したユーザー
* **更新日時**: パターングループの作成または最終更新日時

特定のパターングループを検索するには、ツールバーの検索ツールを利用します。検索ツールは、**名前**、**説明**、**パターン名**、**パターン**、**フィルター式**に入力したキーワードが含まれるパターングループを検索します。大文字・小文字は区別されません。

パターングループ一覧のダウンロード

パターングループ一覧をローカルPCにファイルとしてダウンロードするには、ツールバーの**ダウンロード**をクリックします。

パターングループ一覧の更新

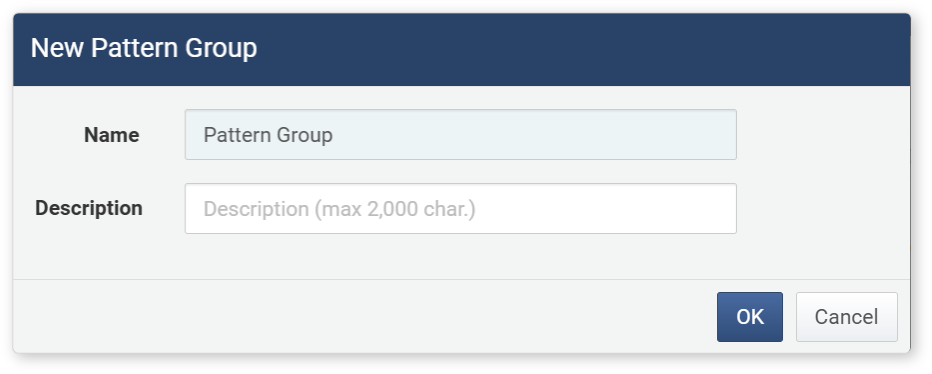
パターングループ一覧を最新情報に更新するには、ツールバーの**更新**をクリックします。

#### パターングループの追加

パターングループを追加するには、以下の手順を実行します。

**ポリシー > パターングループ**で、ツールバーの**追加**をクリックします。

**パターングループ追加**ダイアログが表示されたら、必要事項を入力し、**OK**をクリックします。



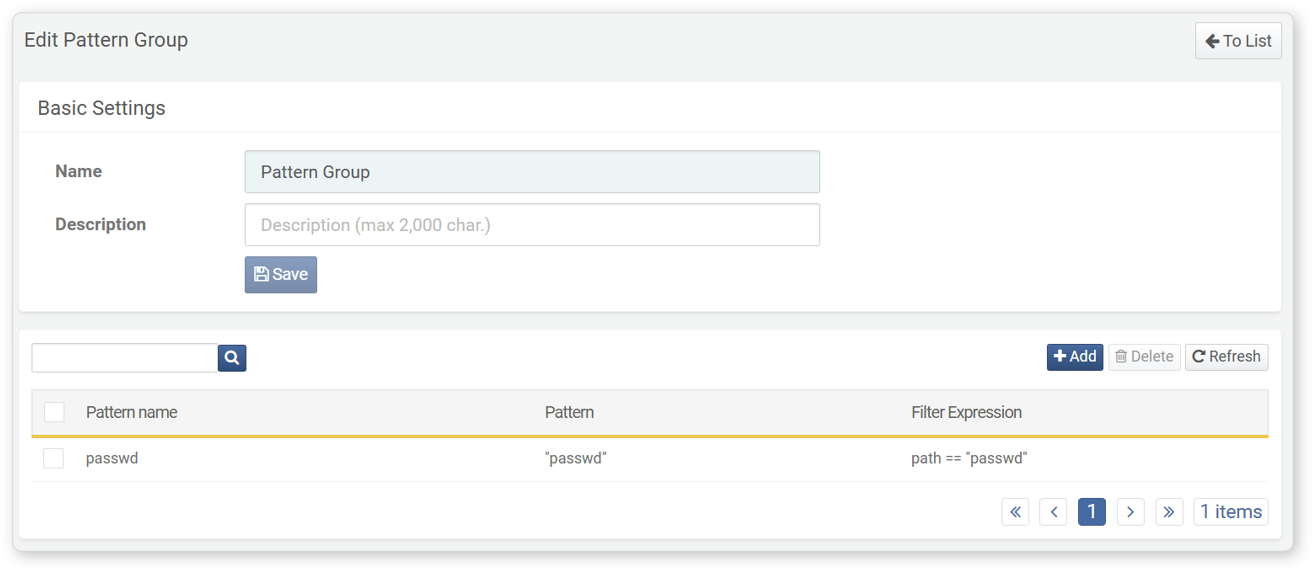
* **名前**: パターングループの名称（最大50文字）
* **説明**: パターングループの詳細説明（最大2,000文字）

#### パターングループの編集

パターングループを編集するには、以下の手順を実行します。

**パターングループ**一覧で、編集したいパターングループ名をクリックします。

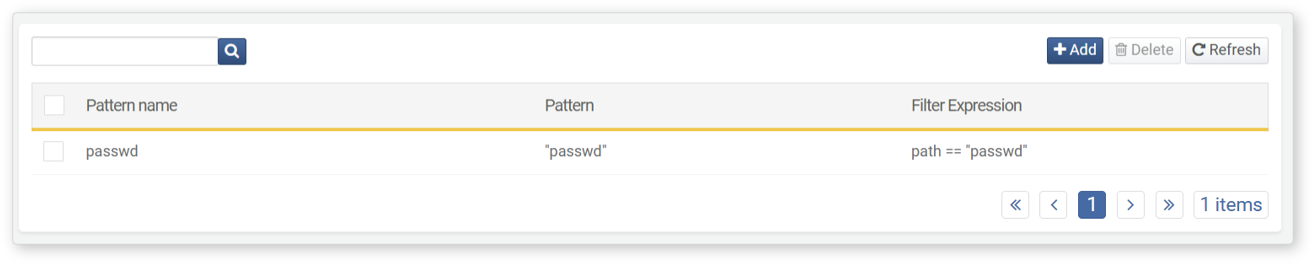
**パターングループ編集**画面で情報を修正し、**保存**をクリックします。



パターンの検索

パターングループに登録されている特定のパターンを検索するには、以下の手順を実行します。

**パターングループ**一覧で、検索したいパターングループをクリックします。



**パターングループ編集**画面でパターン一覧を確認します。

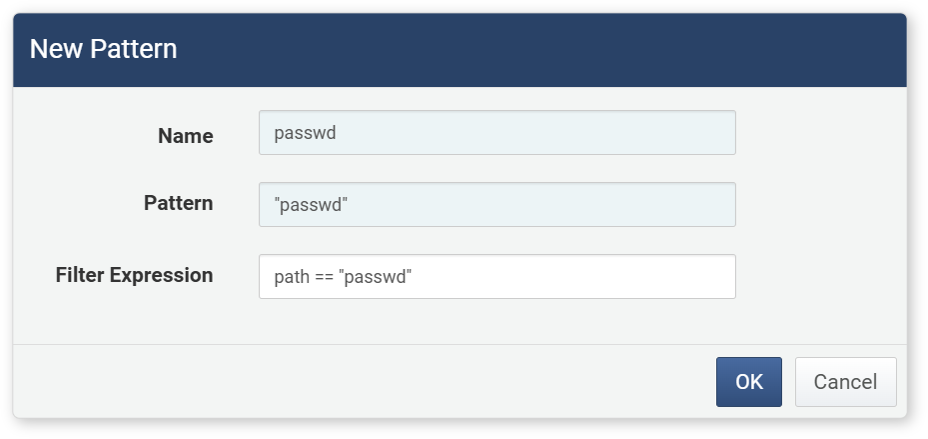
* **名前**: 登録済みパターンの名称
* **パターン**: 検出対象の文字列パターン
* **検証式**: 追加の検証・検索条件

パターンの追加

パターングループにパターンを追加するには、以下の手順を実行します。

**[パターングループ編集](section-pattern-group#outline8)** 画面で、ツールバーの**追加**をクリックします。

**パターン追加**ダイアログが表示されたら、パターンの詳細を入力し、**OK**をクリックします。



* **パターン名**: パターンの一意な名称（最大1,000文字）
* **パターン**: 検索対象の文字列をダブルクォーテーション（"）で囲んで入力します。andやorで複数キーワードを組み合わせることができます（3文字以上、最大1,000文字、スペース含む）。
* **フィルター式**: パターン検出時の追加検証・フィルタ条件（最大1,000文字）。
* フィルター式は「フィールド」「演算子（==または!=）」「値」から構成されます（例：path == "lib.php"）。

|  |  |  |
| --- | --- | --- |
| 対象フィールド | 条件 | 値 |
| path | == | "lib.php" |

* ワイルドカード（\*）は「値」の先頭または末尾に使用できます。
* 検証式は任意です。

パターンの編集

パターングループに登録されているパターンを編集するには、以下の手順を実行します。

**[パターングループ編集](section-pattern-group#outline8)** 画面で、編集したいパターン名をクリックします。

**パターン編集**ダイアログが表示されたら、情報を修正し、**OK**をクリックします。

パターンの削除

パターングループから登録済みパターンを削除するには、以下の手順を実行します。

**[パターングループ編集](section-pattern-group#outline8)** 画面で、削除したいパターンのチェックボックスを選択します。

ツールバーの**削除**をクリックします。

**パターン削除**ダイアログで削除対象のパターンを確認し、**削除**をクリックします。削除しない場合は**キャンセル**をクリックします。

#### パターングループの活用

パターングループは、以下の方法で利用できます。

シナリオビルダー

**ポリシー > ストリームルール**で検出ルールを追加・修正する際に、パターングループを利用できます。

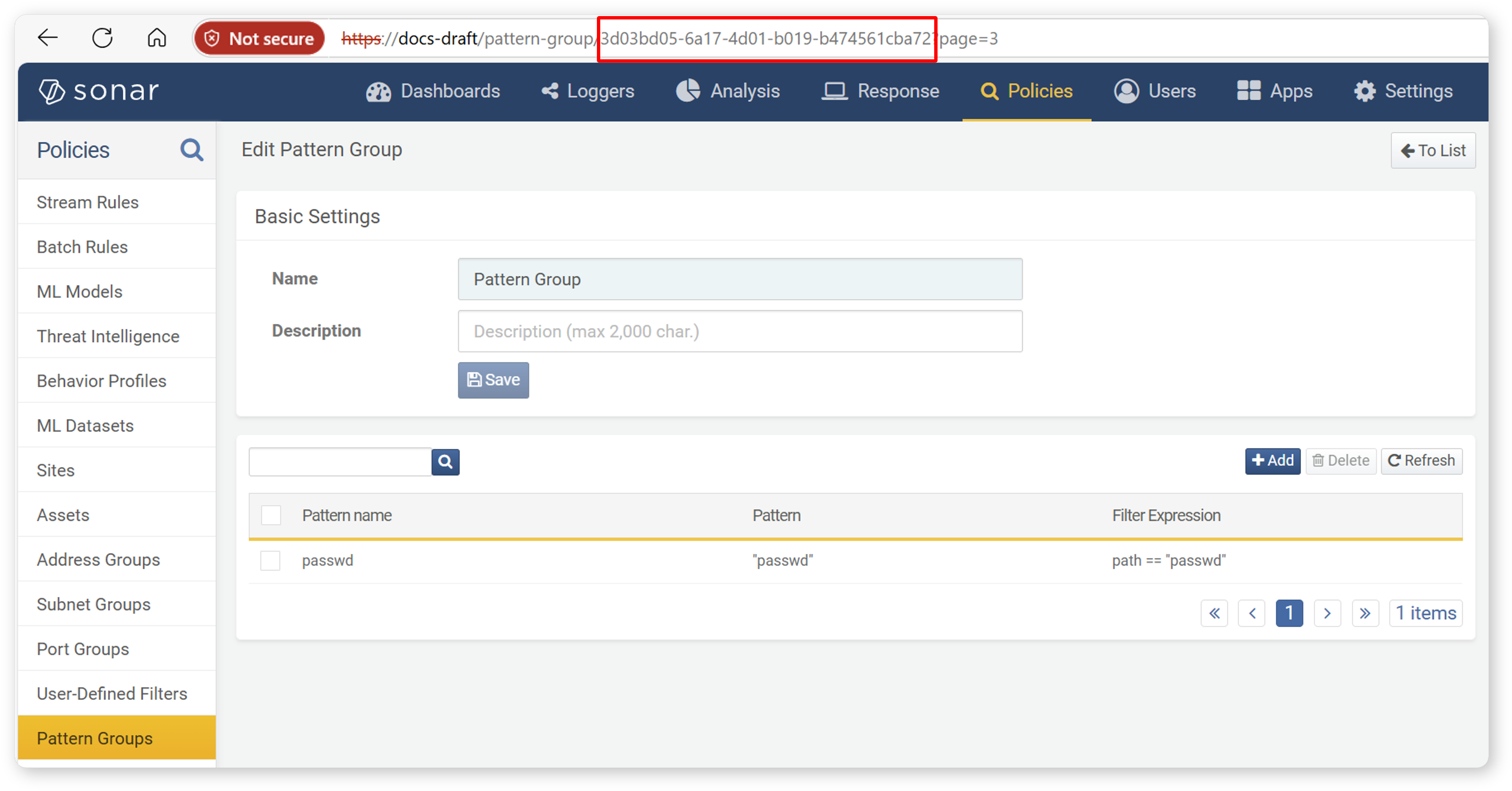
以下の表は、入力フィールドタイプが**STRING**の場合のパターングループ利用方法をまとめたものです。詳細は[フィールドタイプ別ルールとパラメータ](https://docs.logpresso.comnull)を参照してください。

|  |  |  |  |
| --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 説明 |
| シグネチャパターン検出 | 対象シグネチャグループ | シグネチャグループを選択 | シグネチャに一致するフィールド値をフィルタします。 |

クエリ

**ポリシー > ストリームルール**または**ポリシー > バッチルール**で検出ルールを追加・修正する際、[matchsig](https://docs.logpresso.comnull)コマンドや[matchsig()](https://docs.logpresso.comnull)関数を利用してパターングループを適用できます。パターングループは、クエリ入力を受け付ける任意の関数でも利用可能です。

[matchsig](https://docs.logpresso.comnull)コマンドや[matchsig()](https://docs.logpresso.comnull)関数を利用するには、パターングループのGUIDが必要です。GUIDはブラウザのアドレスバーで確認できます。



#### パターングループの削除

パターングループを削除するには、以下の手順を実行します。

パターングループ一覧で、削除したいパターングループのチェックボックスを選択します。

ツールバーの**削除**をクリックします。

**パターングループ削除**ダイアログで削除対象のパターングループを確認し、**削除**をクリックします。削除しない場合は**キャンセル**をクリックします。

ストリームルールやバッチルールで参照されているパターングループを削除すると、該当ルールが正常に動作しなくなる場合があります。