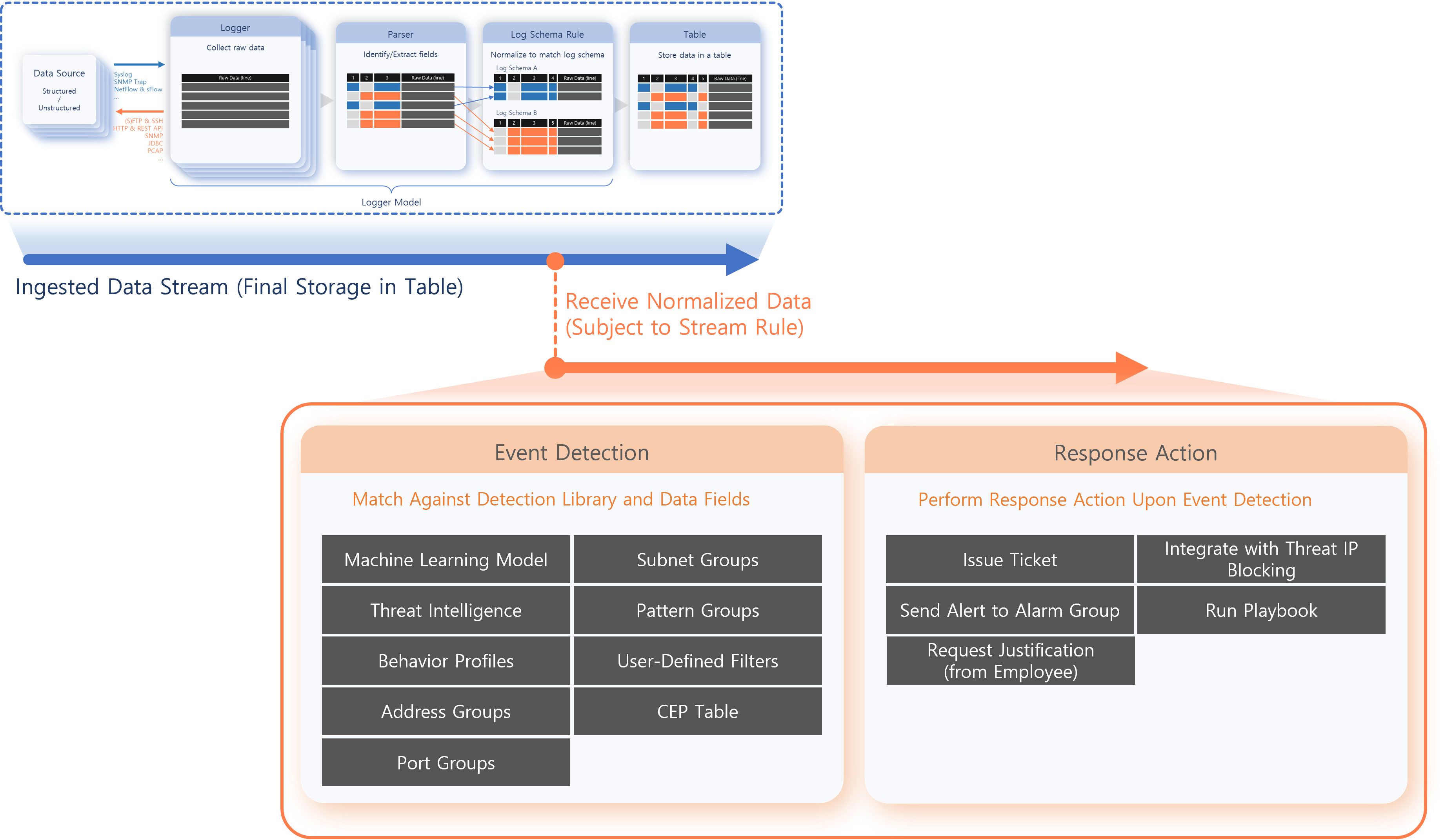
### ストリームルール

#### 概要

ストリームルールは、あらかじめ定義されたパターンや条件に基づき、リアルタイムデータを相関分析して脅威を即時に検出するために使用されます。例えば、IPSログ内の特定パターンを識別して高リスク攻撃を検出したり、外向きトラフィック量が定義された閾値を超えた場合にデータ流出を検知したりできます。

以下の図は、ストリームルールの動作イメージを示しています。ストリームルールは、インジェスト段階で正規化されたデータに適用されます。ストリームルールを作成する際は、必ず[ログスキーマ](https://docs.logpresso.comnull)に従って正規化されたフィールド名を使用してください。



ストリームルールは、主に以下のアクションを実行します。

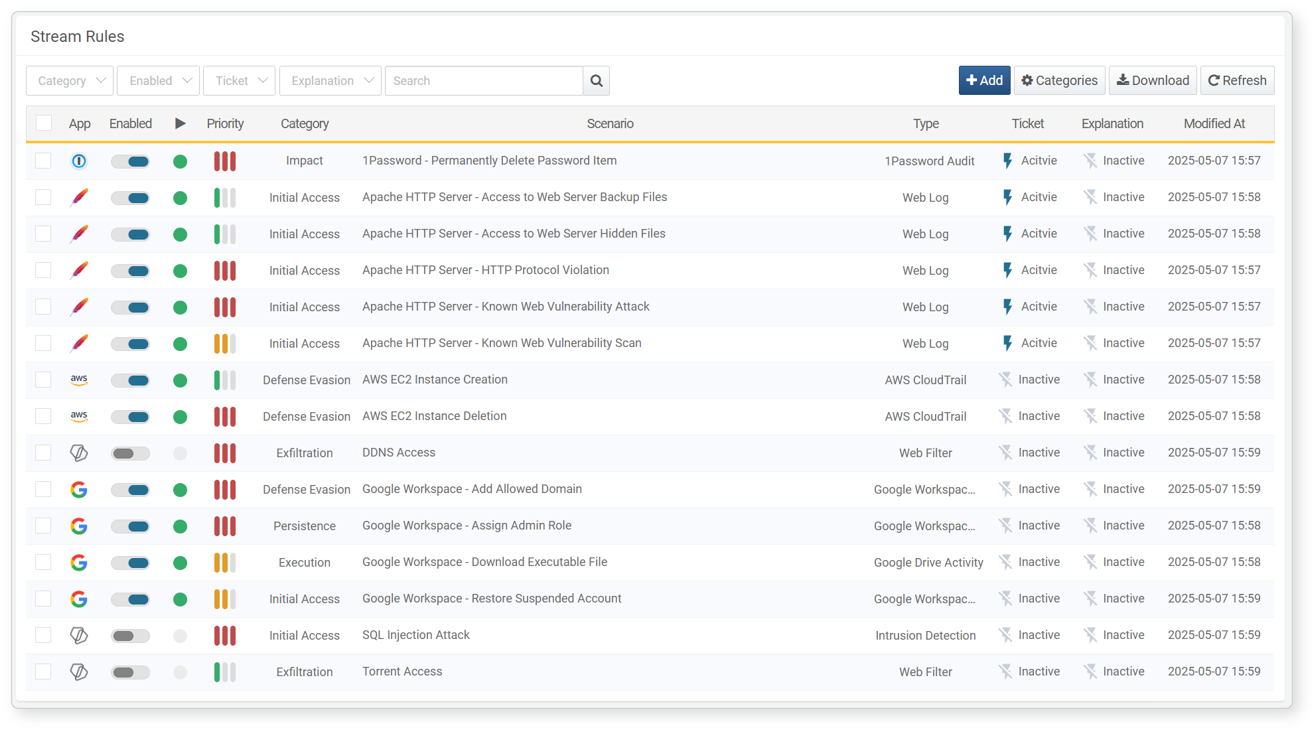
* イベント検出:
* 正規化されたフィールド値に対して検出ライブラリを照合します。
* レスポンスアクション:
* 検出されたイベントに対してチケットを発行し、アラームを送信します。
* アクターが従業員の場合は[弁明](https://docs.logpresso.comnull)を要求します。
* イベントに関連するIPアドレスをアドレスグループに登録します。
* 必要に応じて、接続されたデバイスに対してトラフィック遮断コマンドを送信します。
* プレイブックの実行をトリガーします。

プレイブックの実行は、ストリームルール自体が直接行うレスポンスアクションではありません。ただし、ストリームルールによってプレイブックがトリガーされるよう設定されている場合、プレイブックに基づいたレスポンスアクションが自動的に実行されます。

通常、ストリームルールはイベント検出時にチケットを発行したり、関係者に弁明を要求します。アナリストやセキュリティ担当者が重複したチケットで圧迫されないよう、重複発行を最小限に抑えることが重要です。ログプレッソ・ソナーは、アラートメッセージやチケット件名、または指定された重複判定フィールドに基づき、同一イベントを1つのチケットに統合します。

#### ストリームルールの検索

**ポリシー** > **ストリームルール** で、ストリームルールの一覧を閲覧・検索できます。



* **アプリ**: 関連アプリを示すアイコン。デフォルトルールやユーザー追加ルールはログプレッソアイコン、インストール済みアプリのルールは各アプリアイコンで表示されます。
* **有効化**: ルールの有効/無効を切り替えるトグルボタン (: 有効, : 無効)
* **状態**: **有効化**設定に応じたルールの状態（**緑**: 有効、**グレー**: 無効）
* **優先度**: ルールの重要度（高・中・低）
* **カテゴリ**: カテゴリ情報
* **ルール**: ストリームルール名
* **タイプ**: ルールに設定された[ログスキーマ](https://docs.logpresso.comnull)
* **最終変更日**: ストリームルールの最終変更日（または作成日）

特定のストリームルールを検索するには、ツールバーの検索ツールを利用します。検索ツールは、入力したキーワードがルールの**名前**、**説明**、**クエリ**フィールドに含まれているルールを検索します。大文字・小文字は区別されません。

ストリームルールの有効化・無効化

ストリームルールの**有効化**列にあるトグルボタンをクリックして、ルールを有効/無効に切り替えます（: 有効, : 無効）。

ストリームルール一覧のダウンロード

ストリームルール一覧をローカルPCに保存するには、ツールバーの**ダウンロード**をクリックし、希望するファイル形式を選択してください。

ストリームルール一覧の更新

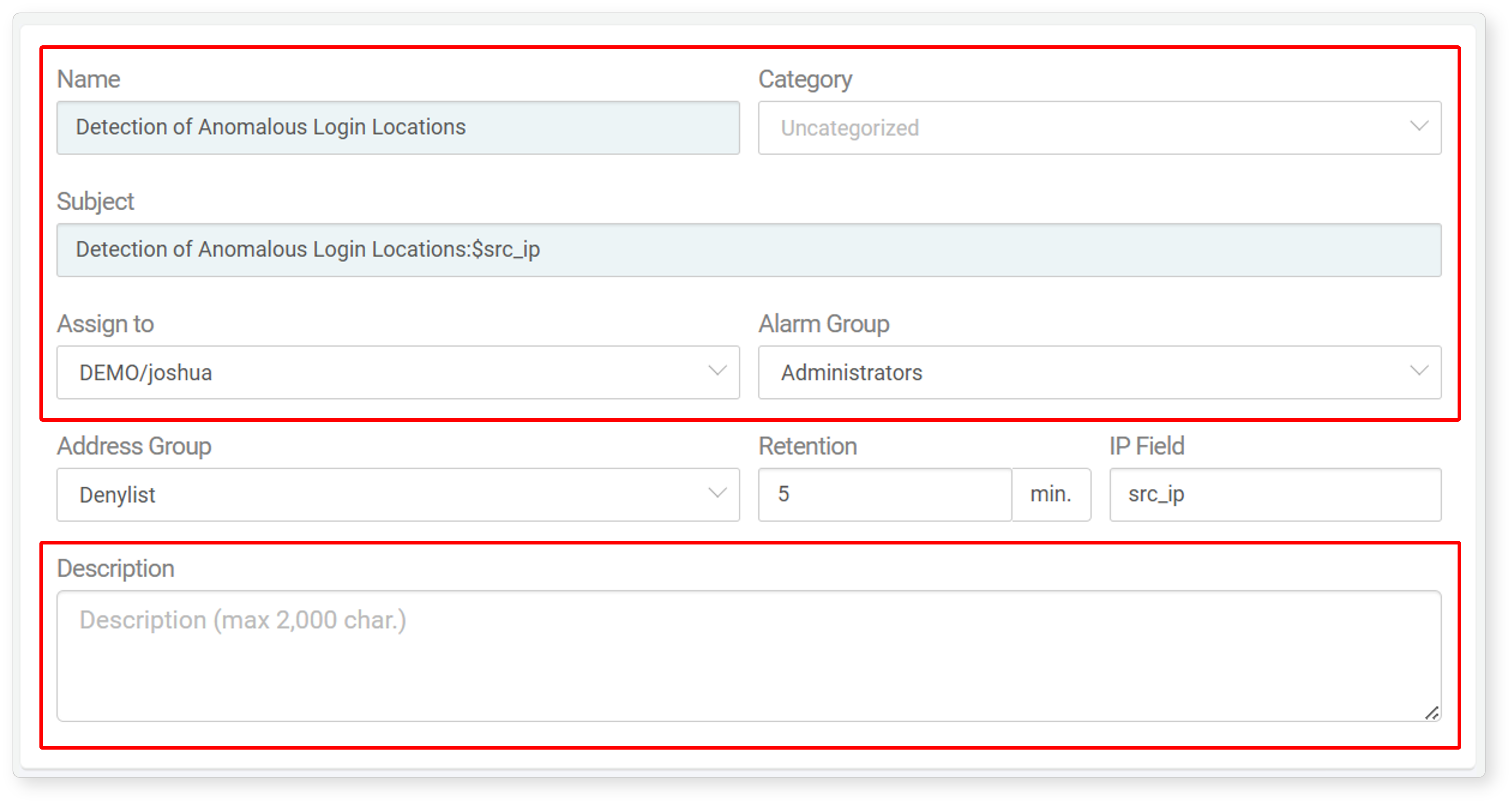
最新のストリームルール一覧を表示するには、ツールバーの**更新**をクリックします。

#### ストリームルールの追加

ストリームルールを追加するには:

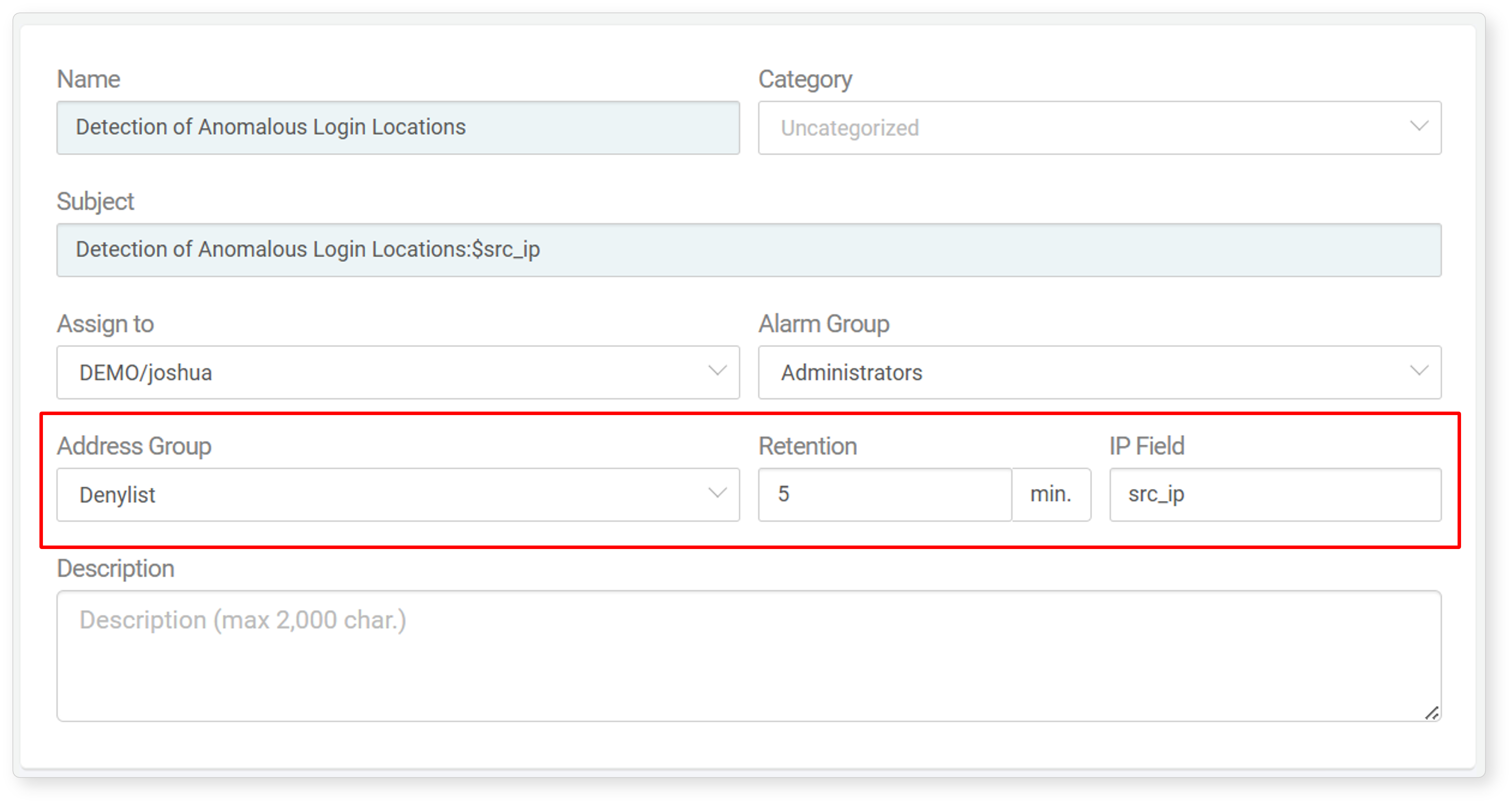
**ポリシー** > **ストリームルール** に移動し、ツールバーの**追加**をクリックします。

**ストリームルール追加**画面で、以下の基本設定を入力します。



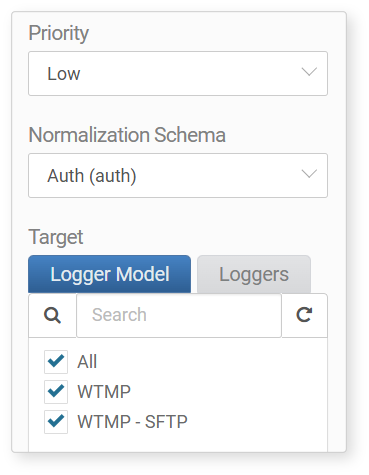
* **名前**: ストリームルールの一意な名称（最大50文字）。ルール名は重複できません。
* **カテゴリ**: ストリームルールのカテゴリ。ツールバーの**カテゴリ**からカテゴリを追加できます。カテゴリが未設定の場合、チケットは発行されません。
* **メッセージ**: イベント検出時にチケットへ割り当てるタイトル
* [ログスキーマ](https://docs.logpresso.comnull)で定義されたフィールド名を$fieldまたは$field$形式で使用します。イベント検出の基となったログからフィールド値を取得してメッセージが生成されます（例: $src\_ip）。韓国語を含むフィールドは必ず$FieldName$形式を使用してください。
* **詳細設定**の**重複判定フィールド**が未指定の場合、生成されたメッセージ（最大2,000文字）が同一かどうかで重複チケットの発行を防止します。
* **担当者**: 発行されたチケットを割り当てる[ユーザー](https://docs.logpresso.comnull)アカウント。複数選択可能。未指定の場合、担当者なしでチケットが作成されます。
* **アラームグループ**: イベント検出時にアラームを受信する[アラームグループ](https://docs.logpresso.comnull)。
* アラームの受信設定は、選択したアラームグループ内で構成する必要があります。
* **説明**: ストリームルールの詳細説明（最大2,000文字）。

攻撃者IPや異常アクターIPを個別管理したり、アドレスグループ情報をファイアウォールやIPSへ転送する場合は、以下の設定を行います。



* **アドレスグループ**: **IPフィールド**で指定したフィールド値（IPアドレス）を追加する[アドレスグループ](https://docs.logpresso.comnull)。
* **保持期間**: **アドレスグループ**内にIPアドレスを保持する期間（分単位）。指定した遮断期間が経過すると、IPアドレスは自動的にアドレスグループから削除されます。未指定の場合は恒久的に保持されます（範囲: 1～100,000,000）。
* **IPフィールド**: イベント検出時に**アドレスグループ**へ追加するIPアドレスを含むフィールド名。ログスキーマで定義されたIP関連フィールド名を入力します（例: src\_ip, dst\_ip）（最大50文字）。
* サードパーティ製セキュリティシステムとの連携による遮断アクションについては、「システム > レスポンスターゲット」を参照してください。

ロガー（またはロガーモデル）に対する検出イベントの優先度を設定します。



* **優先度**: 検出イベントの重大度（高・中・低）。
* **正規化スキーマ**: ストリームルールに適用するログスキーマ。**シナリオビルダー**で利用可能なフィールドは、選択したログスキーマに依存します。
* **ターゲット**: ストリームルールを適用するロガーモデル（またはロガー）。選択したログスキーマに関連付けられたロガーモデルおよびロガーのみが表示されます。

ロガーモデルが「Raw」正規化ルールのみでログスキーマを参照していない場合、検出ターゲット一覧に表示されません。必ずロガーモデルがログスキーマを参照していることを確認してください。

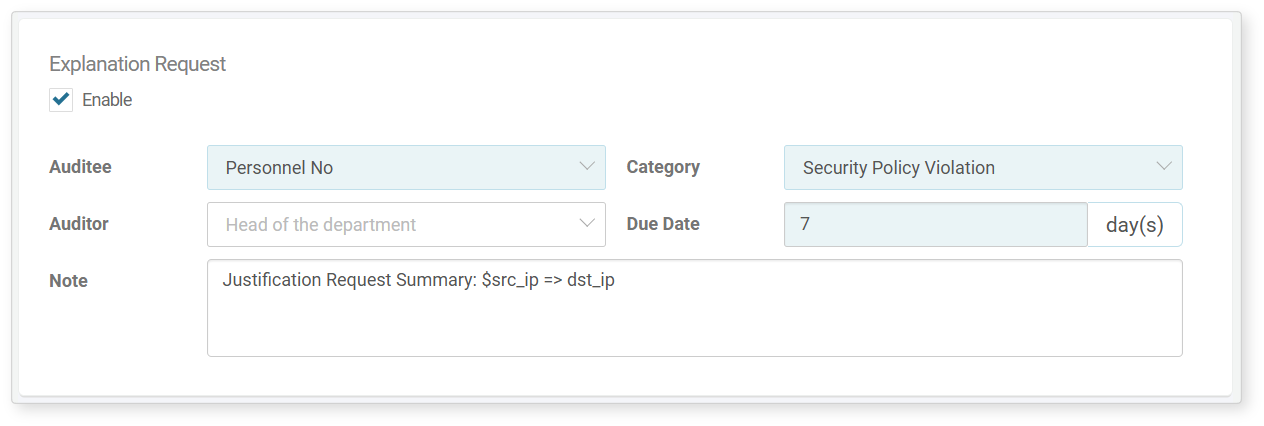
脅威検出シナリオを作成します。**シナリオビルダー**を利用するか、**クエリ**フィールドに直接クエリを入力して検出シナリオを定義します。**シナリオビルダー**の詳細は[フィールドタイプ別ルールとパラメータ](https://docs.logpresso.comnull)を参照してください。

シナリオは最低1つのルールで構成され、シナリオリスト上部から順に適用されます。選択したターゲットからデータが収集されると、ルール順に照合されます。前のシナリオが成立しないと次のシナリオは実行されません。シナリオの実行順序はシステムパフォーマンスに影響するため、単純かつ高速な条件を先に設定し、不要なログを早期にフィルタリングすることを推奨します。

無効または実行不可能なクエリ（例: 存在しないアドレスグループやパターングループを参照）を入力した場合、検出ルールは追加できません。

* **シナリオビルダー**: **条件**、**フィールド**、**ルール**で構成される検出シナリオエディタ。シナリオ入力後、**追加**をクリックしてシナリオリストに登録します。最低1つのシナリオ登録が必要です。
* **条件**: シナリオ適用条件（AND、NOT；デフォルト: AND）。- **AND**: 一致した場合true。- **NOT**: 一致しない場合true。
* **フィールド**: ログスキーマから**ルール**と比較するフィールド
* **ルール**: **フィールド**に適用するルール。選択した**フィールド**によって利用可能なルールが異なります。
* **クエリ**: フィルタ条件を手動で定義したい場合に直接クエリを入力（最大10,000文字）。
* **ストリームクエリ**: **シナリオビルダー**または**クエリ**で入力したフィルタルールをストリームクエリとして表示。

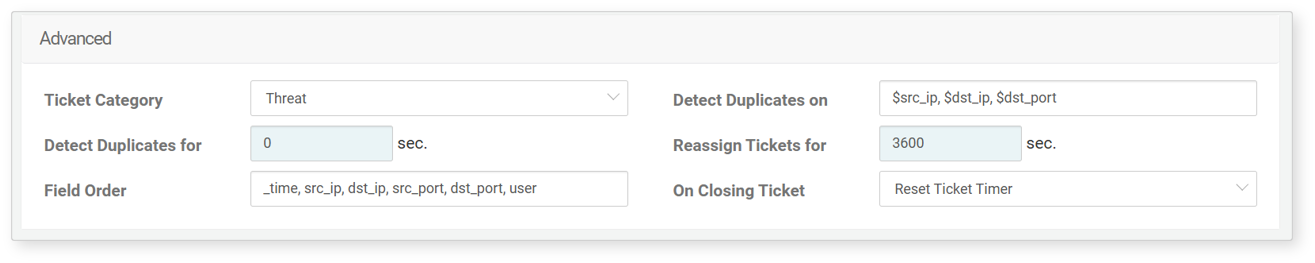
検出イベントが組織内の従業員に関連する場合、従業員に**弁明**を要求できます。



* **弁明要求**: 検出された脅威やイベントに関与した従業員または関係者に弁明を要求するかどうか（デフォルト: 無効）。
* **従業員**: 検出イベントの責任者である従業員の従業員IDを含むフィールド。
* 脅威が検出されると、指定した従業員IDにマッピングされた従業員へ自動的に弁明要求メールが送信されます。この場合、従業員情報（従業員ID、アカウント、メール）が**ポリシー** > **従業員**で設定されていることを確認してください。
* **カテゴリ**: 弁明要求の分類。必要に応じて、**レスポンス** > **弁明** > **カテゴリ**で追加カテゴリを設定できます。
* **監査者**: 提出された弁明の二次審査者（未設定時は「部門長」がデフォルト）。一次・二次審査者の詳細は[弁明](https://docs.logpresso.comnull)を参照してください。
* **期限**: 弁明提出の締切日（デフォルト: 7日）。期限を過ぎると、従業員は弁明を提出できなくなります。
* **備考**: 弁明要求メールに含める追加情報。入力したテキストはメール/SMSテンプレートの$user\_noteマクロ位置に挿入されます。ログスキーマで定義されたフィールド名を$FieldNameマクロ形式で挿入すると、フィールド値がメッセージ内で置換されます。追加備考は**レスポンス** > **弁明**の詳細画面で確認できます（最大10,000文字）。

弁明要求を行うには、「emp\_key」というフィールドが必要です。このフィールドが存在しない場合は、手順5の\*\*クエリ\*\*をクリックし、ユーザーアカウントやIPアドレスを従業員IDにマッピングするクエリを作成して「emp\_key」フィールドを生成してください。

イベント検出時にチケットを発行する場合は、**詳細設定**を構成します。



* **チケット分類**: セキュリティ運用時にチケットを分類するための[チケット分類](https://docs.logpresso.comnull)（デフォルト: なし）

チケット発行は、イベントでトリガーされるプレイブック内でも制御できます。プレイブック内でチケット発行を制御する場合は、ここでこのオプションを設定しないでください。```

* **重複判定フィールド**: 重複チケット検出に使用するフィールドをマクロ形式（例: $field\_name）でカンマ区切りで指定します（最大2,000文字）。未指定の場合は**メッセージ**文字列がデフォルト基準となります。
* **重複判定期間**: チケット発行後、重複イベントを無視する期間（デフォルト: 0、範囲: 0～86,400秒）。
* 「0」に設定時: **チケット統合期間**設定に従います。
* 0以外の場合: 指定期間中は重複イベントを無視し、チケットの補足データには含まれません。
* **チケット統合期間**: 同一イベントが繰り返し発生した際、新規チケットを作成せず、既存チケットに補足データと発生回数を追加する期間（デフォルト: 3,600秒、範囲: 0～86,400秒）- 「0」に設定時: イベント発生ごとに同一タイトルの新規チケットを作成します。- 0以外の場合: 指定期間中は既存チケットに補足データと発生回数を追加します。
* **フィールド順序**: チケットの補足データに表示するログデータフィールドの順序。カンマ区切りでフィールド名を入力（最大2,000文字）。特殊文字やパイプ（|）は使用不可。
* **チケットクローズ時の動作**: **チケット統合期間**有効時、チケットクローズ後の処理方法（デフォルト: タイマーリセット）。- **タイマー維持**: チケットクローズ後も、統合タイマー有効期間内に同一脅威イベントが発生した場合、補足データと発生回数をクローズ済みチケットに追加します。- **タイマーリセット**: チケットクローズ時に統合タイマーも失効し、以降の同一脅威イベントには新規チケットが作成されます。

**OK**をクリックしてストリームルールの追加を完了します。作成後、ストリームルールは即時有効化されます。

フィールドタイプ別ルールとパラメータ

シナリオビルダーでは、[ログスキーマ](https://docs.logpresso.comnull)で定義されたフィールドタイプに応じてルールを設定できます。各フィールドのデータ型ごとに利用可能なルールとパラメータは以下の通りです。

**STRING**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 負荷 | 説明 |
| 文字列一致 | 対象文字列 | 最大255文字 | 低 | フィールド値が対象文字列と一致するデータを抽出します。 |
| 部分一致 | 部分文字列 | 最大255文字 | 低 | フィールド値に指定した部分文字列が含まれるデータを抽出します。 |
| シグネチャパターン検出 | 対象シグネチャパターン | シグネチャグループ | 中 | シグネチャパターンに基づきフィールド値を抽出します。 |

**BOOL**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 負荷 | 説明 |
| 真偽値 | 条件 | True または False | 低 | 真偽条件に基づきフィールド値を抽出します。 |

**SHORT/INT/LONG/DOUBLE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 負荷 | 説明 |
| 等しい | 対象値 | -9007199254740991 ~ 9007199254740991 | 低 | 指定値と一致するフィールド値を抽出します。 |
| 範囲内 | 開始値, 終了値 | -9007199254740991 ~ 9007199254740991 | 低 | 指定範囲内のフィールド値を抽出します。 |
| より大きい | 対象値 | -9007199254740991 ~ 9007199254740991 | 低 | 指定値より大きいフィールド値を抽出します。 |
| 以上 | 対象値 | -9007199254740991 ~ 9007199254740991 | 低 | 指定値以上のフィールド値を抽出します。 |
| より小さい | 対象値 | -9007199254740991 ~ 9007199254740991 | 低 | 指定値より小さいフィールド値を抽出します。 |
| 以下 | 対象値 | -9007199254740991 ~ 9007199254740991 | 低 | 指定値以下のフィールド値を抽出します。 |

**DATE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 負荷 | 説明 |
| 曜日 | 選択曜日 | 日～土から複数選択 | 低 | 指定曜日に生成されたデータを抽出します。 |
| 週末 | - | - | 低 | 週末に生成されたデータを抽出します。 |
| 平日 | - | - | 低 | 平日に生成されたデータを抽出します。 |
| 時間範囲 | 開始時刻, 終了時刻 | 0～23時 | 低 | 指定時間帯に生成されたデータを抽出します。 |

**COUNTRY**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 負荷 | 説明 |
| 国コード | 対象国コード | 国コード選択 | 低 | 指定国コードと一致するフィールド値を抽出します。 |

**PORT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 負荷 | 説明 |
| ポート番号 | 対象ポート番号 | 0～65535 | 低 | 指定ポートと一致するフィールド値を抽出します。 |
| ポートグループ内 | 対象ポートグループ | 事前定義済みポートグループから選択 | 低 | 指定ポートグループに属するフィールド値を抽出します。 |

**IP**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 負荷 | 説明 |
| IPアドレス一致 | 対象IP | IPv4形式アドレス | 低 | 指定IPアドレスと一致するフィールド値を抽出します。 |
| ネットワーク範囲内 | 対象ネットワーク範囲 | ネットワーク範囲選択 | 低 | 指定ネットワーク範囲に含まれるフィールド値を抽出します。 |
| アドレスグループ内 | 対象アドレスグループ | アドレスグループ選択 | 低 | 指定アドレスグループに含まれるフィールド値を抽出します。 |
| 特定レピュテーションDBに登録 | レピュテーションDB | 脅威インテリジェンスソース選択 | 中 | 指定レピュテーションDBに登録されたフィールド値を抽出します。 |
| IPアドレスでイベントコンテキスト作成 | イベント名, タイムアウト | 最大255文字、0～86400（分/時/秒） | 高 | IPアドレスをキーとしてイベントコンテキストを作成し、指定タイムアウト期間内で追跡登録します。 |
| IPアドレスでイベント相関 | イベント名 | 最大255文字 | 高 | 指定イベントコンテキストに登録されたIPアドレスに関連するイベントを検索します。 |
| イベント閾値超過 | イベント名, 閾値 | 最大255文字、閾値は0～9007199254740991 | 高 | 指定イベント閾値を超えたIPアドレスを抽出します。 |
| いずれかのレピュテーションDBに登録 | - | - | 中 | いずれかの脅威インテリジェンスDBに出現したフィールド値を抽出します。 |

**MD5/SHA1/SHA256**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 負荷 | 説明 |
| ハッシュ値一致 | ハッシュ | 最大255文字 | 低 | 指定ハッシュ値と一致するフィールド値を抽出します。 |
| レピュテーションDBに登録 | - | - | 中 | いずれかのレピュテーションDBに出現したフィールド値を抽出します。 |
| 特定レピュテーションDBに登録 | レピュテーションDB | 脅威インテリジェンス選択 | 中 | 指定レピュテーションDBに登録されたフィールド値を抽出します。 |

**URL**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 負荷 | 説明 |
| レピュテーションDBに登録 | - | - | 中 | いずれかのレピュテーションDBに出現したフィールド値を抽出します。 |
| 特定レピュテーションDBに登録 | レピュテーションDB | 脅威インテリジェンスソース選択 | 中 | 指定レピュテーションDBに登録されたフィールド値を抽出します。 |

**DOMAIN**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 負荷 | 説明 |
| ドメイン一致 | 対象文字列 | 最大255文字 | 低 | 指定文字列と一致するフィールド値を抽出します。 |
| レピュテーションDBに登録 | - | - | 中 | いずれかのレピュテーションDBに出現したフィールド値を抽出します。 |
| 特定レピュテーションDBに登録 | レピュテーションDB | 脅威インテリジェンスソース選択 | 中 | 指定レピュテーションDBに登録されたフィールド値を抽出します。 |

**その他（例: BLOB）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ルール | パラメータ | 範囲 | 負荷 | 説明 |
| その他 | 行動プロファイル検出 | 行動プロファイル選択 | 低 | 行動プロファイルのキーとなるフィールド値を抽出します。 |

#### ストリームルールの複製

既存のストリームルールを複製するには:

ストリームルール一覧で、複製したいルールのチェックボックスを選択します。

ツールバーにアクションメニューが表示されるので、**複製**をクリックします。

**ストリームルール複製**ダイアログで選択ルールを確認し、**複製**をクリックします。キャンセルする場合は**キャンセル**をクリックします。

* 複製されたルールは「Copy of 元のルール名」という名前で無効状態で追加されます。

#### ストリームルールの編集

ストリームルールを編集するには:

ストリームルール一覧で、編集したいルール名をクリックします。

**ストリームルール編集**画面で情報を更新し、**OK**をクリックします。編集可能なプロパティの説明は[ストリームルールの追加](https://docs.logpresso.comnull)を参照してください。

#### ストリームルールの削除

ストリームルールを削除するには:

ストリームルール一覧で、削除したいルールのチェックボックスを選択します。

ツールバーにアクションメニューが表示されるので、**削除**をクリックします。

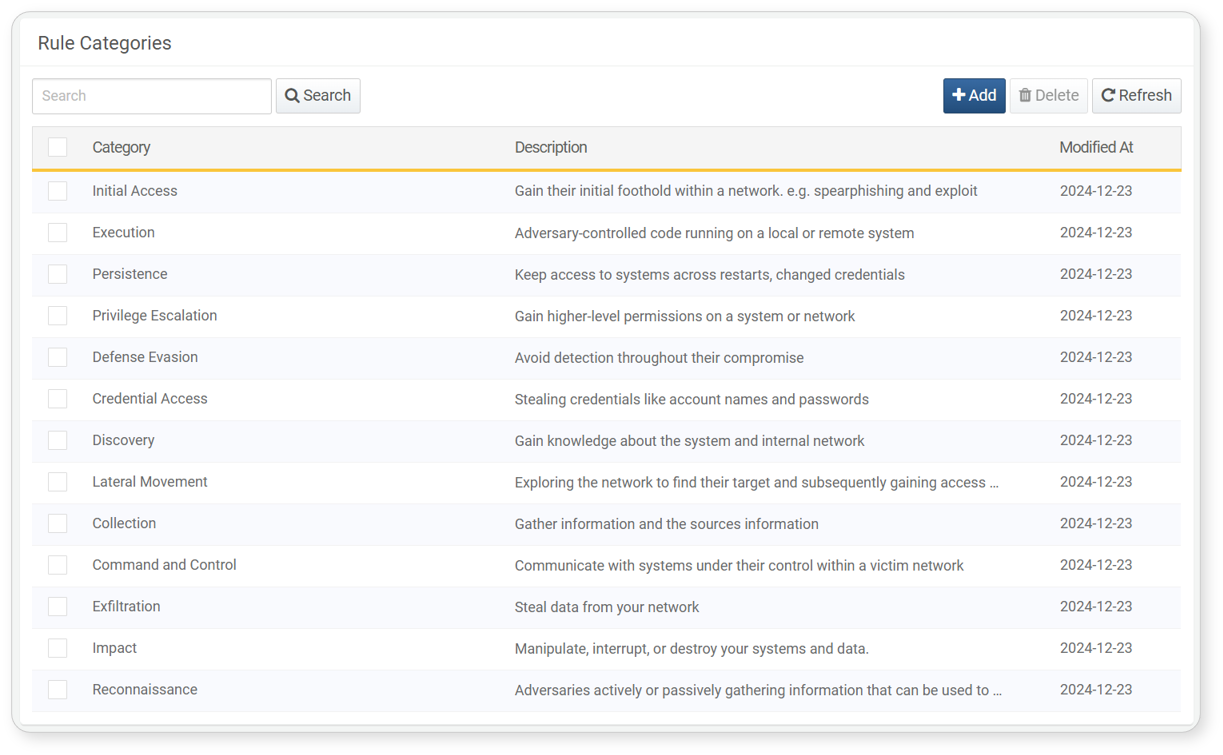
**ストリームルール削除**ダイアログで選択ルールを確認し、**削除**をクリックします。キャンセルする場合は**キャンセル**をクリックします。

#### ルールカテゴリ

ルールカテゴリは、攻撃タイプに基づいて検出イベントを管理するために使用されます。ルール追加時にカテゴリを定義できます。デフォルトカテゴリはMITRE ATT&CKマトリクスに基づいています。

|  |  |
| --- | --- |
| カテゴリ | MITRE ATT&CK戦術 |
| Initial Access | Initial Access |
| Execution | Execution |
| Persistence | Persistence |
| Privilege Escalation | Privilege Escalation |
| Defense Evasion | Defense Evasion |
| Credential Access | Credential Access |
| Discovery | Discovery |
| Lateral Movement | Lateral Movement |
| Collection | Collection |
| C&C | Command and Control |
| Exfiltration | Exfiltration |
| Impact | Impact |
| Reconnaissance | Reconnaissance |

ルールカテゴリの追加・編集・削除は、**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、ツールバーの**カテゴリ**をクリックして行います。



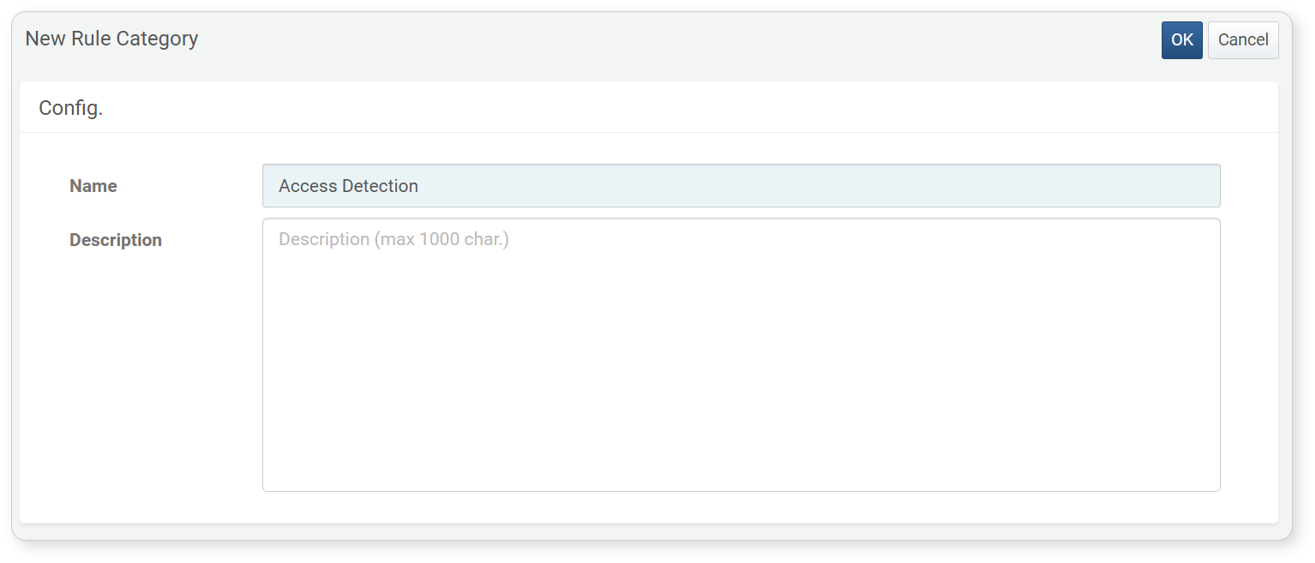
* **カテゴリ**: ルールカテゴリ名
* **説明**: ルールカテゴリの詳細説明
* **最終変更日**: カテゴリの最終変更日時

ルールカテゴリの追加

ルールカテゴリを追加するには:

**カテゴリ管理**ウィンドウで**追加**をクリックします。

**新規ルールカテゴリ**ページでカテゴリ詳細を入力し、**OK**をクリックします。



* **名前**: ルールカテゴリの一意な名称（最大50文字）
* **説明**: ルールカテゴリの詳細説明（最大1,000文字）

ルールカテゴリの編集

ルールカテゴリを編集するには:

**カテゴリ管理**ウィンドウで、編集したいカテゴリ名をクリックします。

**ルールカテゴリ編集**ページで詳細を更新し、**OK**をクリックします。

ルールカテゴリの削除

ルールカテゴリを削除するには:

**カテゴリ管理**ページで、削除したいカテゴリのチェックボックスを選択します。

ツールバーで**削除**をクリックします。

**ルールカテゴリ削除**ダイアログで選択カテゴリを確認し、**削除**をクリックします。キャンセルする場合は**キャンセル**をクリックします。