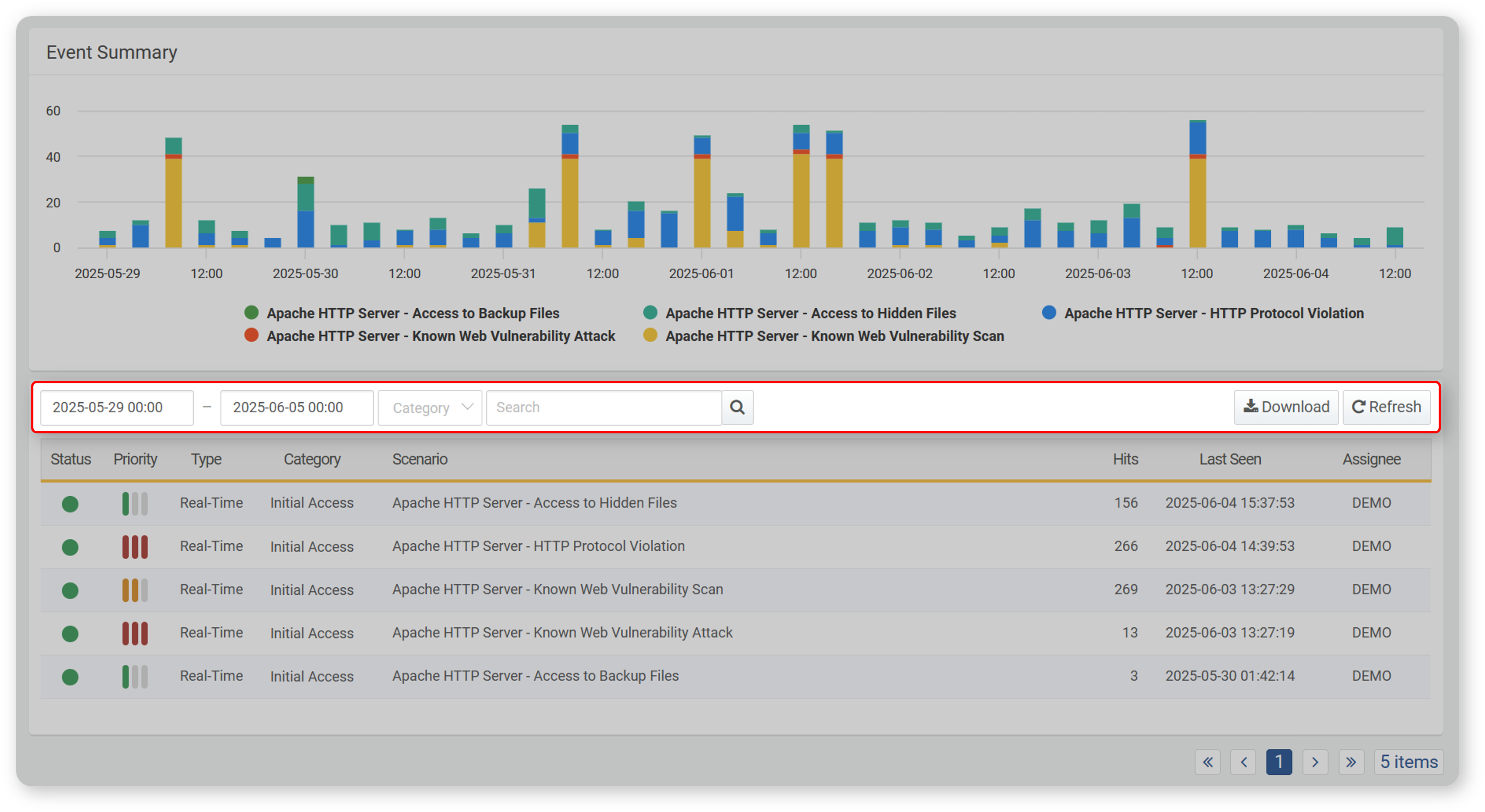
### イベントサマリー

#### 概要

**イベントサマリー**は、シナリオごとのイベント検出状況を視覚的に表示します。検出シナリオごとの検出イベント数を示すチャートと、リストビューで構成されています。ユーザーは期間指定、イベント分類の選択、キーワード入力により、結果を絞り込むことができます。

#### ツールバー

[イベントサマリーリスト](https://docs.logpresso.comnull)の上部には、検出結果のフィルタリングおよび検索を行うためのツールバーがあります。フィルターや検索条件を適用すると、チャートとリストの両方がリアルタイムで更新されます。また、ツールバーから現在のイベントサマリーリストのダウンロードや、最新データへのリフレッシュも可能です。



期間／カテゴリフィルター

期間やイベント分類を指定することで、チャートおよびリストが選択した条件に応じて更新されます。以下の画像は、**期間**フィルター（イベント発生日時の指定）と**カテゴリ**フィルターをリストに適用した例です。

ツールバーで利用可能なフィルターは以下の通りです。

* **期間**: イベント検索のための日付範囲を選択します（デフォルト：当日00:00から翌日00:00まで。ただし翌日00:00は検索対象外）。入力ボックスに直接範囲を入力するか、ボックスをクリックして表示されるタイムピッカーを利用できます。
* **カテゴリ**: フィルタリング対象のイベントカテゴリを選択します（デフォルト：全選択）。イベント分類は検出ルールで定義されたカテゴリに基づきます。これらのカテゴリは、**ポリシー > ストリームルール**または**バッチルール**の[カテゴリ](https://docs.logpresso.comnull)で管理できます。

検索

イベントサマリーリストから特定のイベントを探す場合は、ツールバーにある検索ツールを利用します。このツールは、**シナリオ**フィールドに入力したキーワードを含む検出エントリを検索します。大文字・小文字は区別されません。

より正確な検索結果を得るためには、期間フィルターとカテゴリフィルターを併用してください。期間フィルターは常に検索に適用されます。

ダウンロード

現在のイベントサマリーリストをダウンロードするには、以下の手順を実行します。

ツールバーの**ダウンロード**をクリックします。

**イベントサマリーダウンロード**ウィンドウで、以下のオプションを入力または選択し、**OK**をクリックします。

* **ファイル名**: ダウンロードするファイル名（デフォルト：Ticket）
* **カラム**: ファイルに含めるイベントサマリーのプロパティ。**全選択**をクリックすると、すべての項目を含めることができます。
* **ファイル形式**: ダウンロードするファイルの形式（デフォルト：CSV）
* **CSV**: CSVファイル
* **Excel XML**: Microsoft Excelで開けるXMLファイル
* **Microsoft Word**: DOCXファイル
* **HTML**: HTMLファイル
* **JSON**: JSONファイル
* **PDF**: PDFファイル
* **エンコーディング**: ファイルのエンコーディング（UTF-8、UTF-16 BE、MS949、デフォルト：MS949）
* **範囲**: 含めるイベントサマリーの件数。最新の登録順に指定件数まで逆順で保存されます。

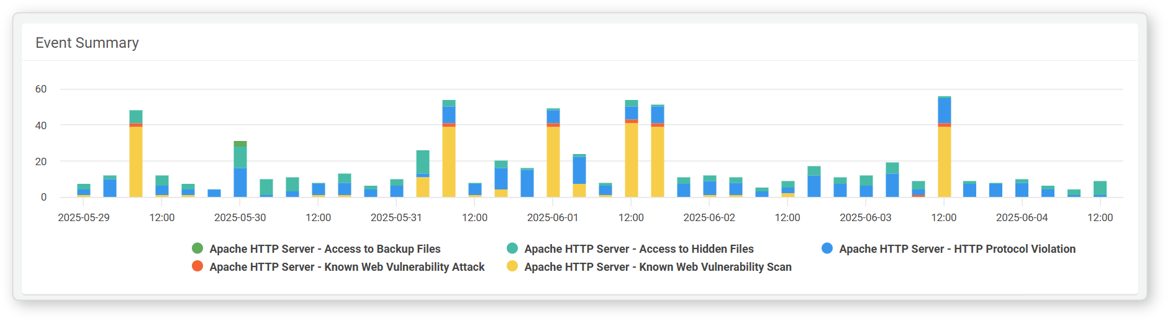
リストのリフレッシュ

最新情報でイベントサマリーリストを表示するには、ツールバーの**リフレッシュ**をクリックします。

#### イベントサマリーチャート

イベントサマリーチャートは、過去7日間のシナリオごとの検出件数を表示します。

* X軸：時間
* Y軸：検出件数



シナリオフィルター

チャート下部にはシナリオの凡例が表示されます。凡例内の特定シナリオをクリックすると、チャート上でそのシナリオの表示／非表示を切り替えることができます。



期間フィルター

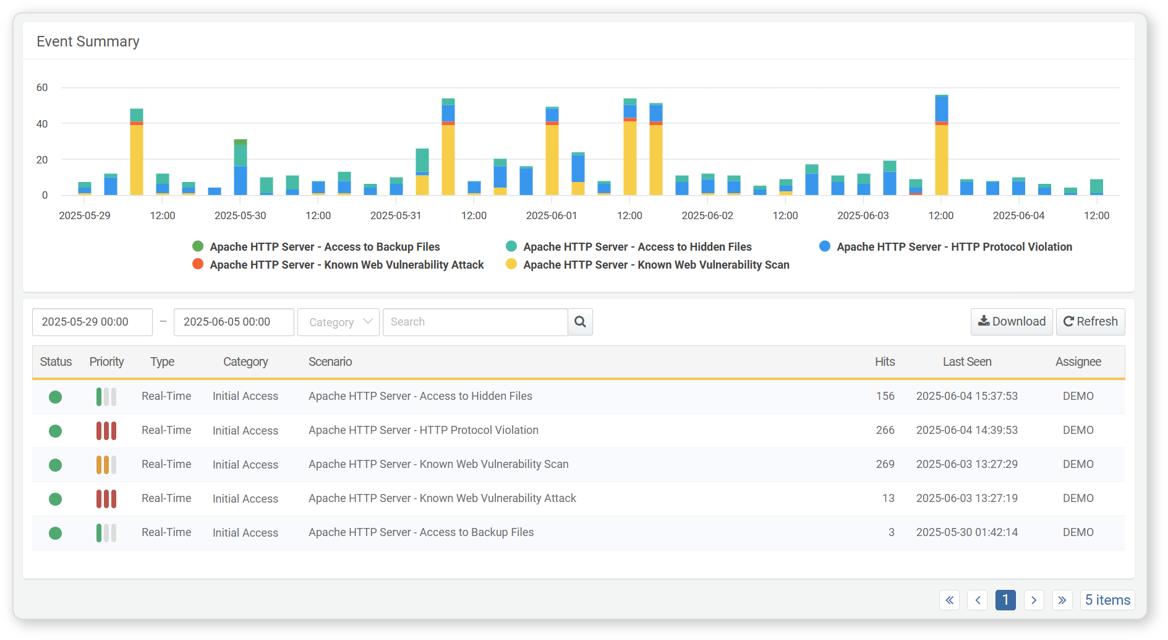
チャートを特定の期間に限定するには、チャート上でマウスをドラッグして時間範囲を選択します。



チャート上の**RESET**をクリックすると、イベント期間フィルターが解除されます。

#### イベントサマリーリスト

イベントサマリーリストは、検出シナリオに基づき、過去7日間に検出されたイベントの分類、発生件数、重要度などの詳細を表示します。リストは最新の検出時刻順に並びます。検出イベントがないシナリオはリストに表示されません。



イベントサマリーリストで確認できる情報は以下の通りです。

* **ステータス**: 検出ルールの状態（**緑**：有効、**グレー**：無効）
* **優先度**: ルールで定義されたイベントの重大度（高／中／低）
* **タイプ**: ルールのタイプ（ストリーム／バッチ）
* **カテゴリ**: シナリオによってイベントに適用された分類情報
* **シナリオ**: イベントを検出したシナリオ名
* **ヒット数**: イベント発生件数
* **最終検出**: 最新の検出発生時刻
* **担当者**: 関連する[チケット](https://docs.logpresso.comnull)の担当者。未割り当ての場合は**未割り当て**と表示されます。

イベントサマリーリストはシナリオ単位で表示されます。ルールが修正された場合、サマリーは該当シナリオの変更内容を反映します。ただし、シナリオ名が変更された場合、旧名称で検出されたイベントはリストから消え、新名称で検出されたイベントのみが表示されます。

#### シナリオごとのイベント詳細表示

イベントの詳細情報を確認するには、以下の手順を実行します。

イベントサマリーリストで、確認したいイベントのシナリオ名をクリックします。

ポップアップウィンドウで、該当シナリオの検出イベントに関する詳細情報を確認できます。

✅ 詳細ビューで利用できる操作は、[イベント](https://docs.logpresso.comnull)セクションと同様です。

このビューで表示されるイベント情報は正規化データです。これに対し、チケットの証拠情報で表示されるイベント情報は、生データ（非正規化データ）となります。