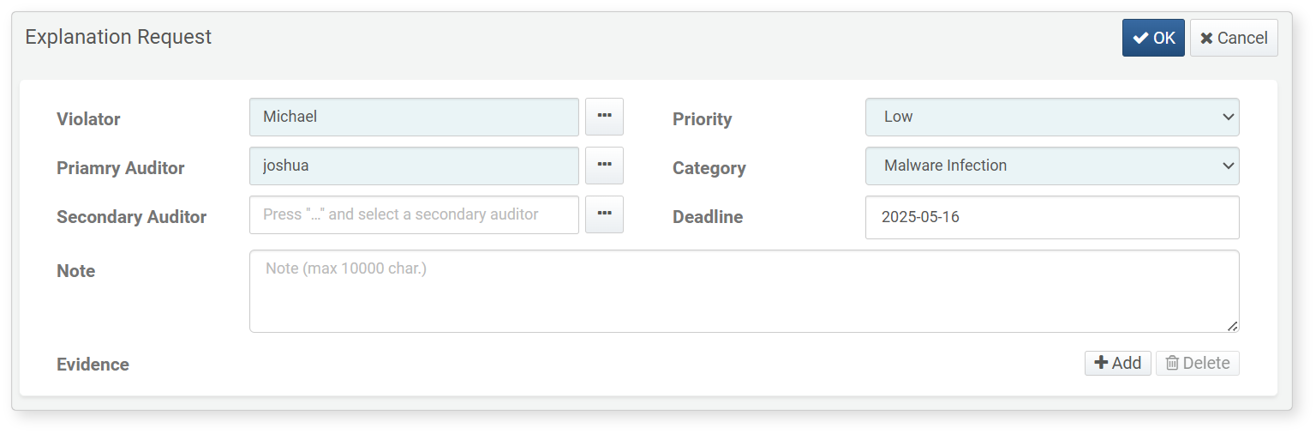
#### 弁明リクエストの作成

弁明リクエストは、ストリーム検出またはバッチ検出によって自動生成されるほか、**チケット**画面または**弁明**画面の**追加**ボタンから手動で追加することもできます。本セクションでは、**チケット**画面および**弁明**画面から弁明リクエストを追加する方法について説明します。



ステップ1：

対象者（違反者）

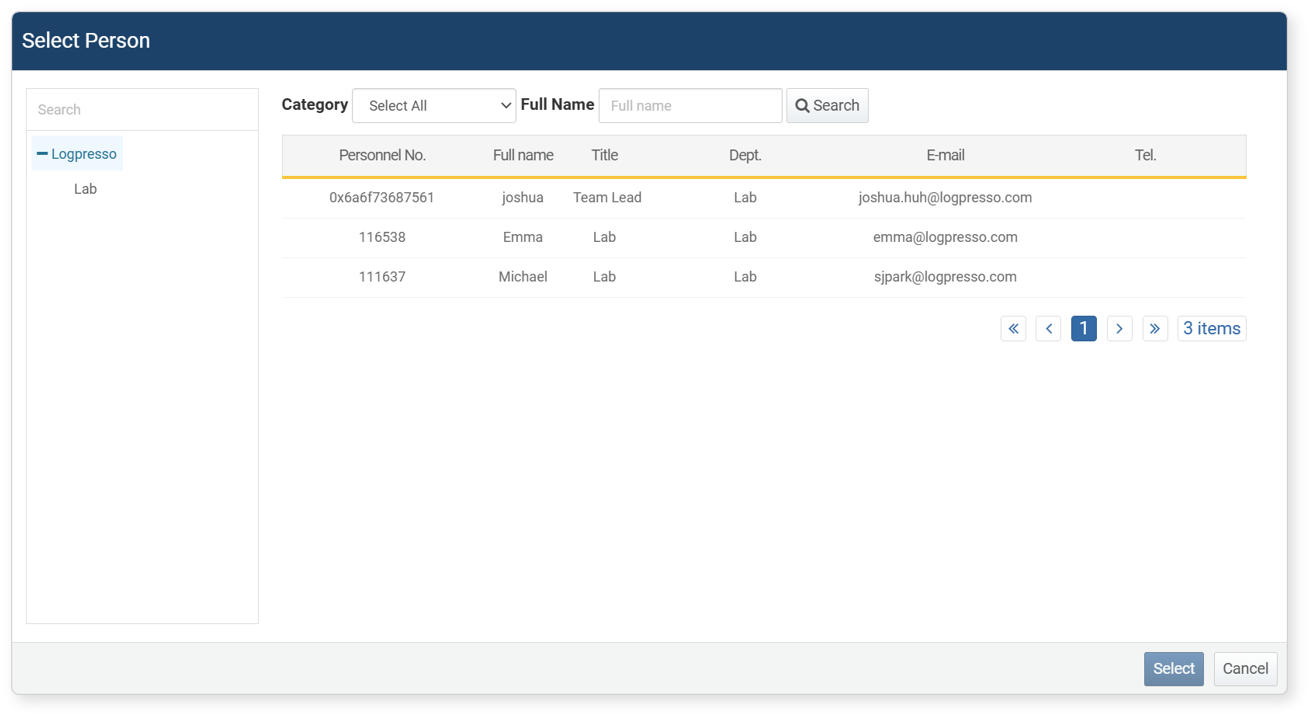
まず、弁明を行う責任者（違反者）を指定します。違反者を選択すると、その所属部門の部門長が一次監査者として自動的に設定されます。必要に応じて二次監査者を追加することも可能です。入力欄に直接名前を入力するか、...ボタンを使用して組織図から違反者や監査者を選択できます。

一次監査者

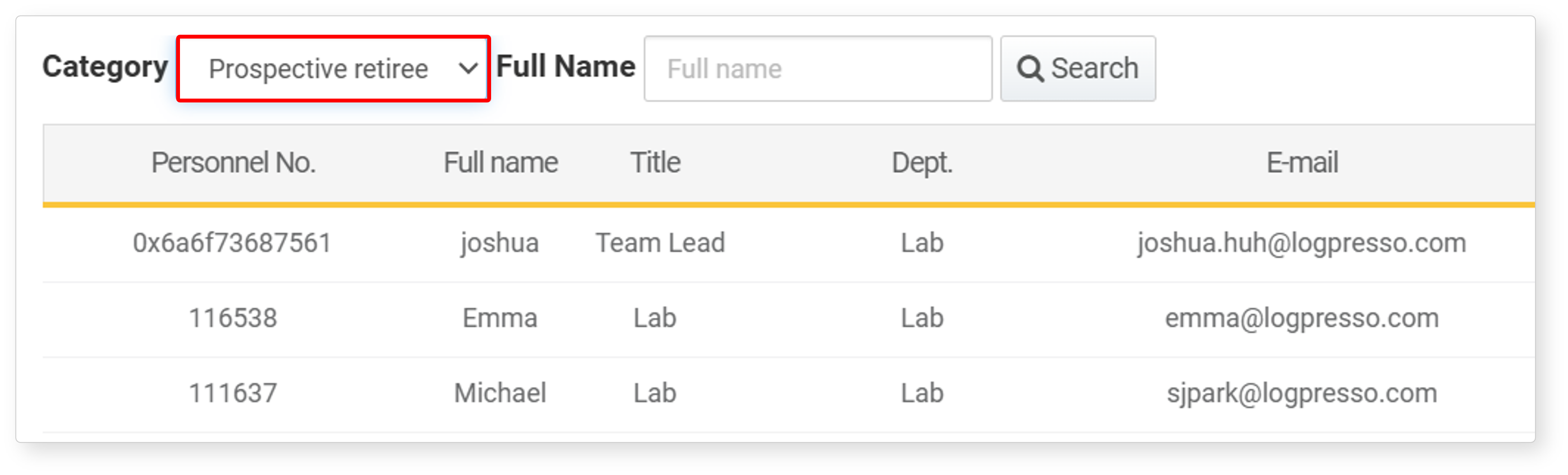
* デフォルトでは、違反者が所属する部門の部門長が一次監査者として割り当てられます。
* 部門長が存在しない場合は、上位部門の部門長が自動的に割り当てられます。
* 最上位部門にも部門長がいない場合は、管理者権限を持つユーザーが一次監査者として指定されます。

違反者が部門長である場合

* 違反者が部門長であり、上位部門に部門長が存在する場合、その人物が一次監査者として指定されます。
* 上位部門にも部門長がいない場合、または違反者が最上位部門に所属している場合は、管理者権限を持つユーザーが一次監査者として指定されます。

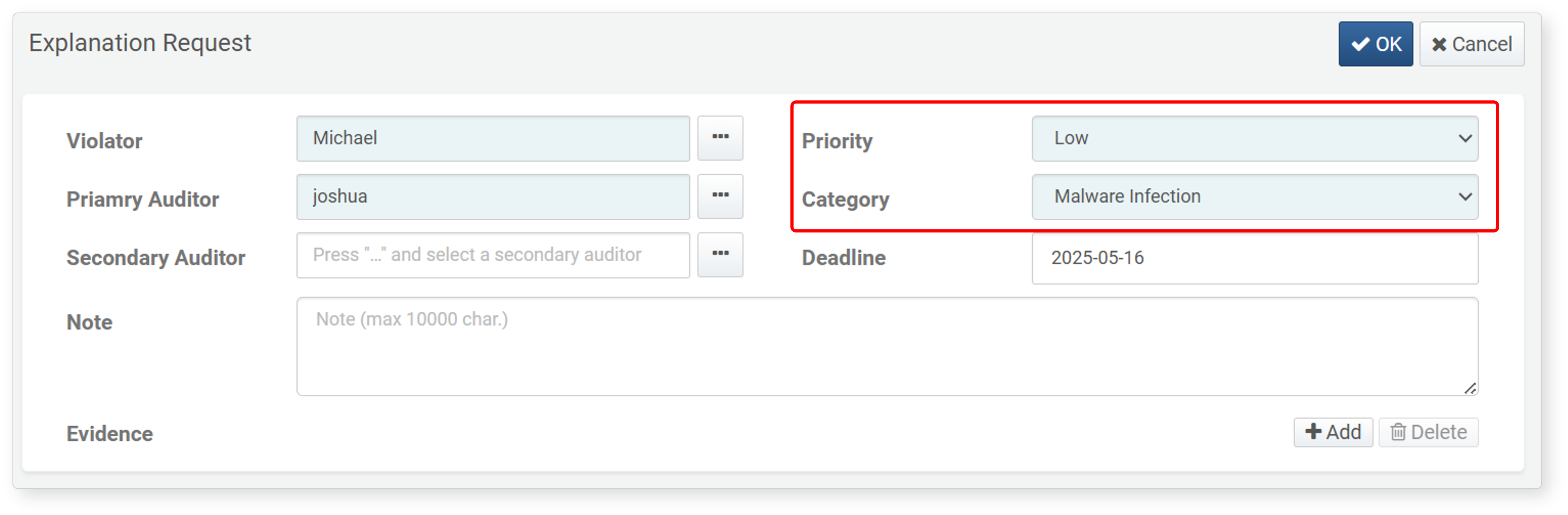


違反者選択画面では、「退職予定者」区分でフィルタリングすることで、退職日が確定している従業員のみを表示できます。



ステップ2：弁明カテゴリ

弁明カテゴリを選択し、重要度を設定します。カテゴリの管理（追加・削除・編集）は**カテゴリ**ページから行えます。



ステップ3：証拠ログの追加

証拠となるログデータを検索します。ログプレッソ・ソナーのロガーで収集されたデータから、対象者によるセキュリティ違反の可能性を示すログを抽出し、弁明リクエストに添付します。

証拠ログを検索する際は、違反者に関連するレコードのみが表示されます。これは、検索時にクエリ対象テーブルのemp\_keyフィールドが従業員番号と一致するレコードのみが返されるためです。そのため、ロガー作成時には、収集データに従業員番号をマッピングし、テーブルに保存しておく必要があります。これにより、弁明リクエスト時に収集データを証拠として利用できます。例えば、収集データ内のIPアドレスやアカウント名をマッピングテーブルやルックアップを用いて従業員番号に紐付け、併せて保存する方法が利用できます。

**テーブル**

証拠ログデータが格納されているテーブルを選択します。

**スキーマ**

データを収集したロガーに関連付けられたスキーマを選択します。クエリおよび結果はこのスキーマに基づきます。

**期間（From/To）**

ログ検索の対象期間を指定します。この期間内に収集されたデータのみが取得されます。

**キーワード／クエリ**

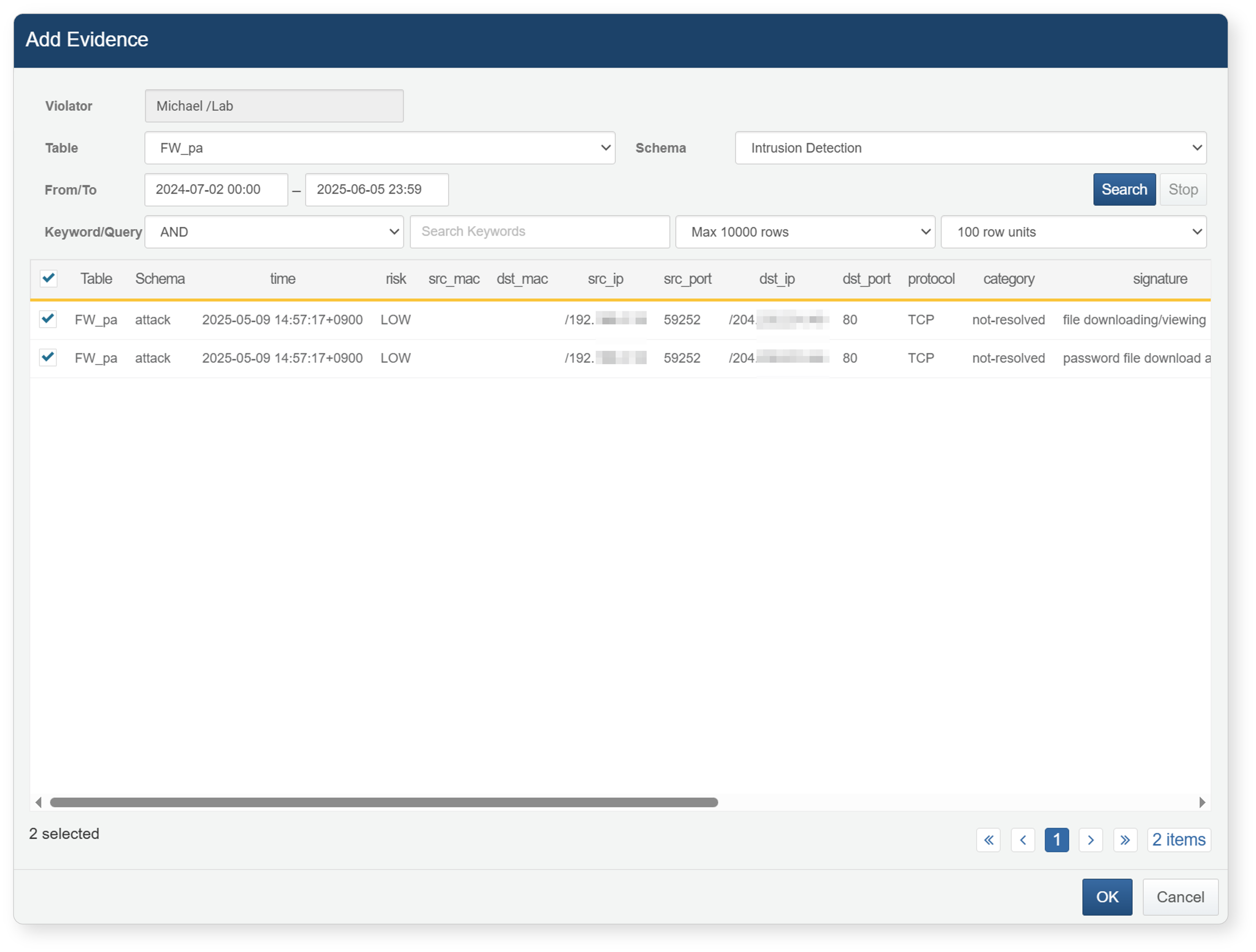
ログ内容を検索するキーワードを入力します。ANDを使用するとすべてのキーワードを含む結果、ORを使用するといずれかのキーワードを含む結果が返されます。クエリエクスプレッション条件を選択した場合は、全文検索のブール式クエリを直接入力できます。

**最大件数**

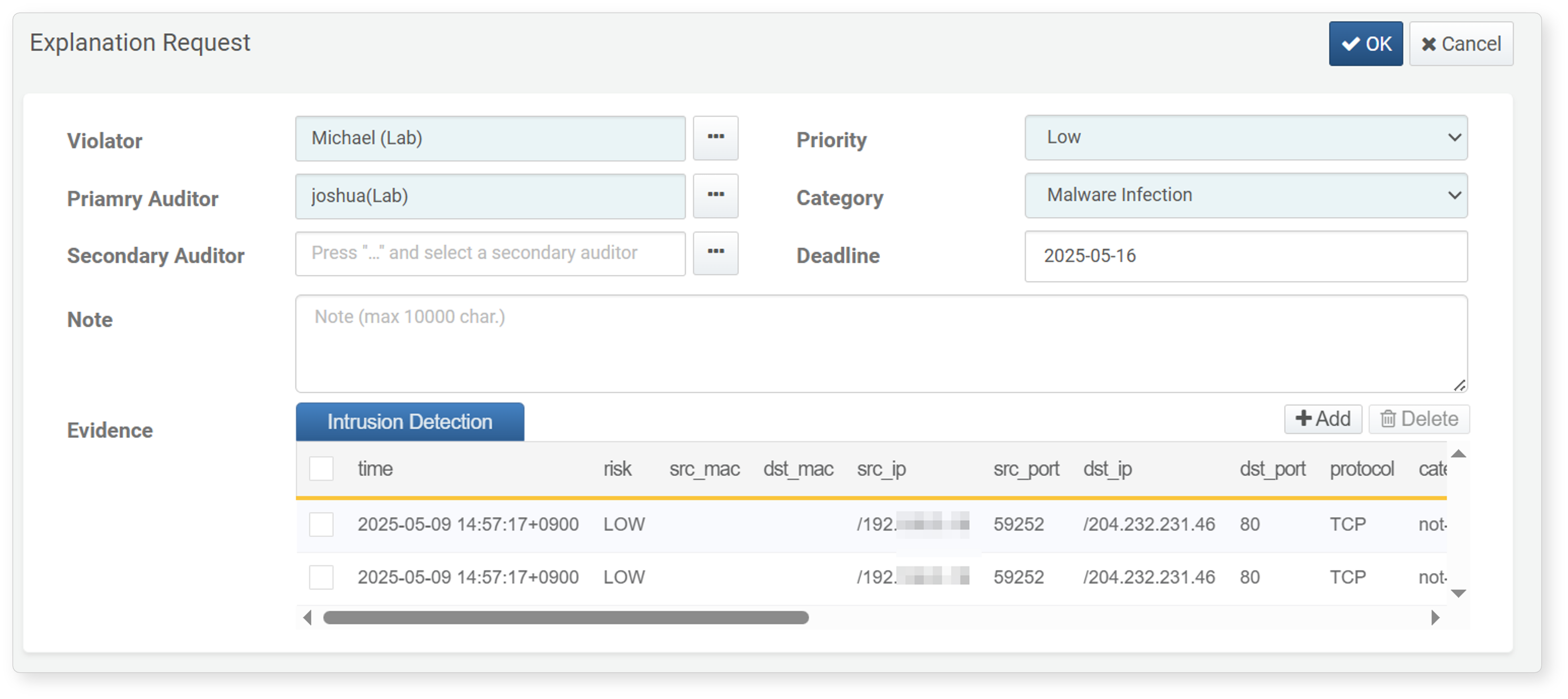
取得するログエントリの最大件数を設定します。

**表示単位**

画面上で1ページに表示する件数を設定します。



選択したログを追加ボタンをクリックすると、選択したログエントリが弁明リクエストに添付されます。



チケット画面から弁明リクエストを作成する場合、そのチケットに紐付けられている証拠ログが自動的にリクエストに追加されます。

ステップ4：弁明リクエストの送信

必要事項の入力が完了したら、画面右上のOKボタンをクリックして弁明リクエストを確定・送信します。