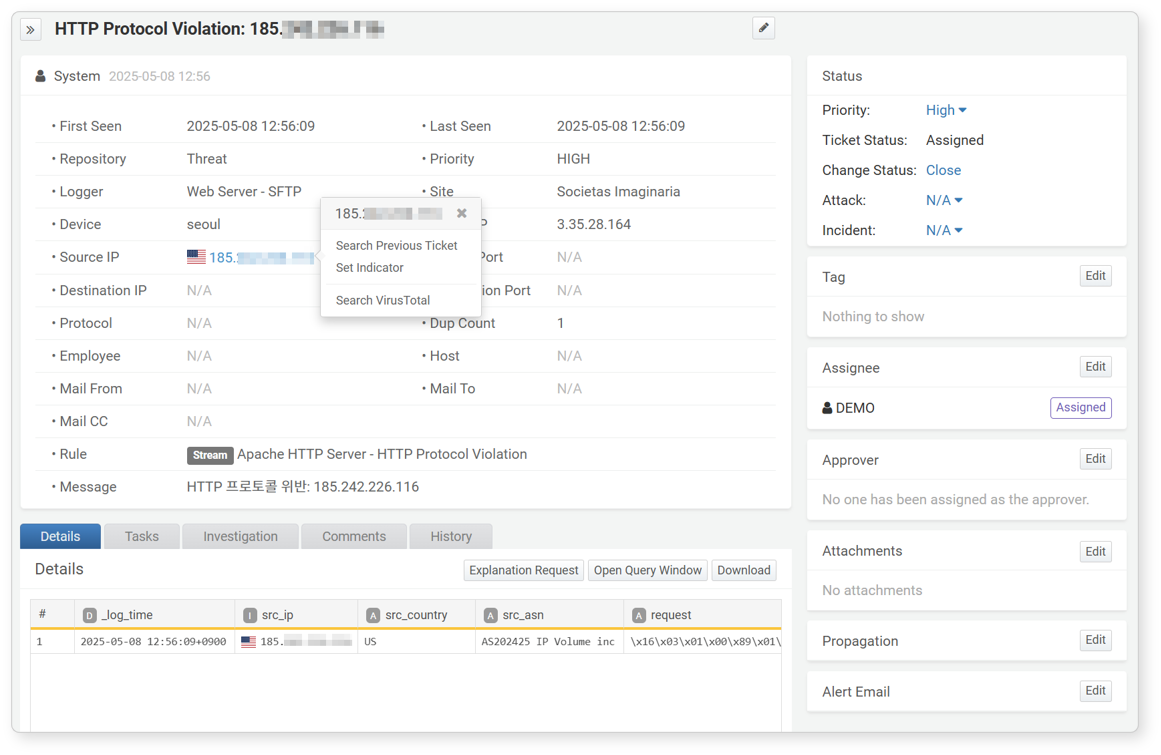
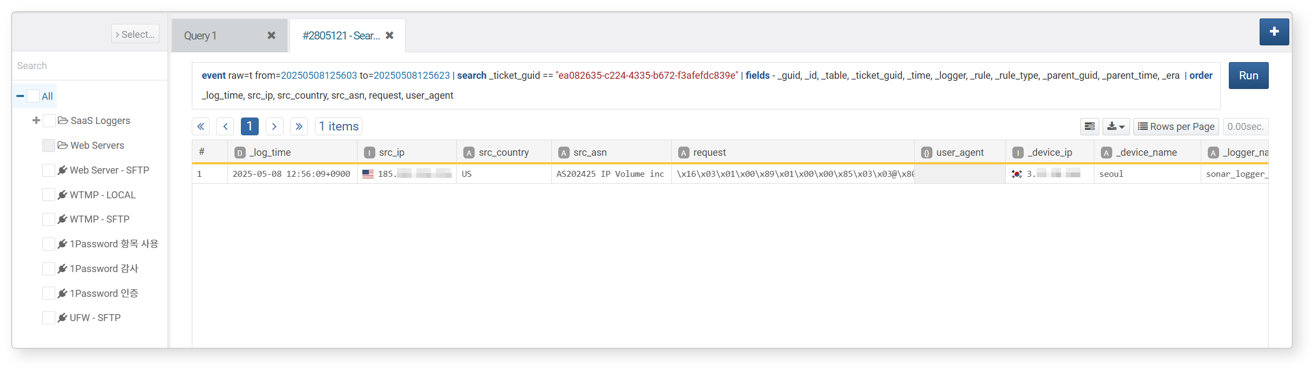
#### チケットの閲覧

チケットリストでチケットタイトルをクリックすると、その詳細およびステータスを確認できます。



チケットが検出ルールによって自動生成された場合、上記のようにチケット本文にイベントの詳細が表示されます。下部の証拠欄には、イベントをトリガーした元のログやチケットに関連するデータが含まれます。たとえば、ホストスキャンが検出された場合、証拠欄にはスキャンを試みた宛先IPやポートなどの情報が、下記の例のように表示されます。証拠欄のスペースが狭い場合は、**クエリウィンドウを開く**ボタンをクリックして、別画面でデータを確認できます。

また、ユーザーは送信元IP、宛先IP、またはホストに関連する過去のチケット履歴を検索したり、VirusTotalで悪意のある活動がないか確認することも可能です。



アナリストは証拠を精査し、実際に脅威や異常が存在するかを判断します。その後、対応内容を記録し、チケットのステータスを更新して完了とします。