検証

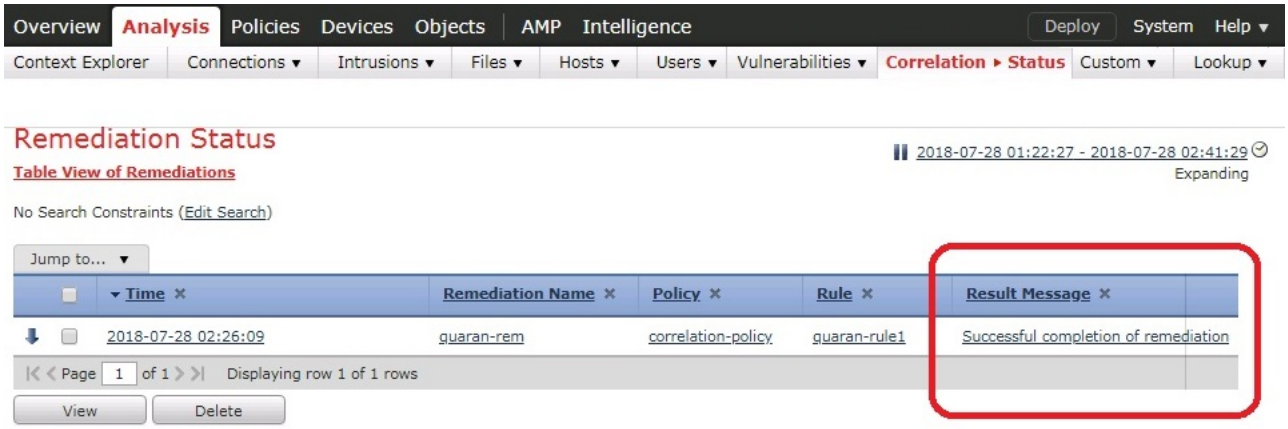
検証

修復はさまざまな理由で失敗することがあるため、次の手順を実行して、修復が成功したことを確認します。

ステップ 1 修復モジュールが関連付けられている相関ルールによってトリガーされた後、FMC GUI で修復実行のステータスを確認します。

ステップ 2 [分析（Analysis）] > [相関（Correlation）] > [ステータス（Status）] に移動します。

ステップ 3 [修復ステータス（Remediation Status）] テーブルで、ポリシーの行を見つけ、結果のメッセージを確認します。

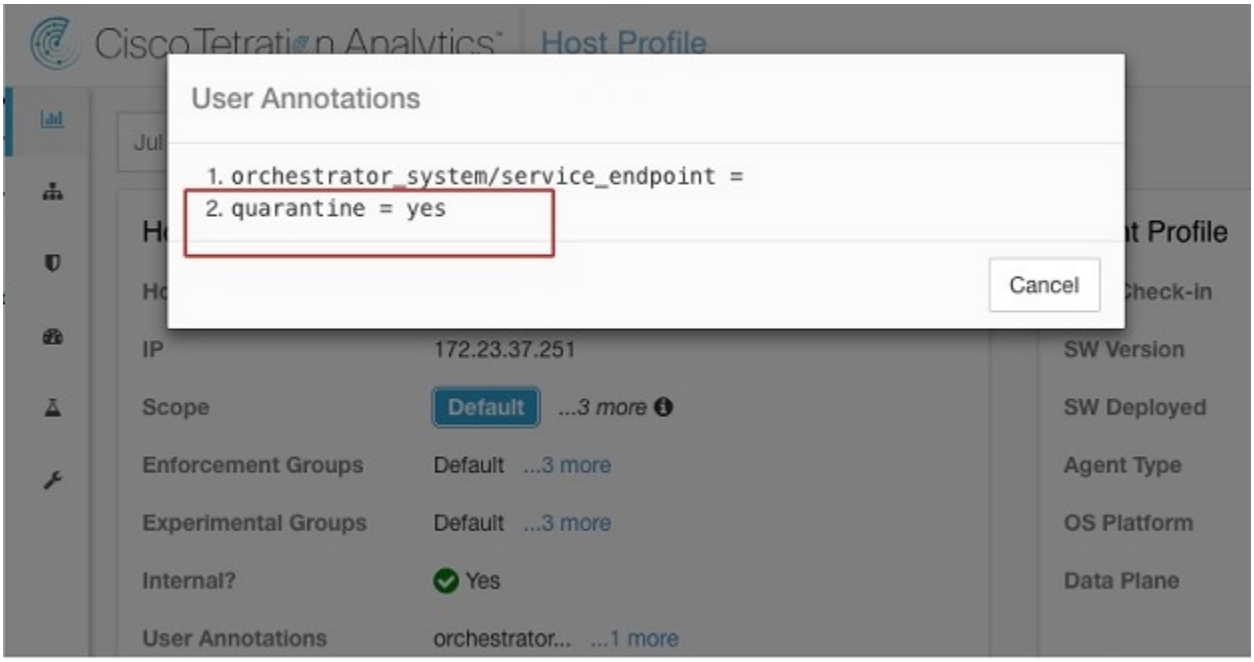


ステップ 4 修復が完了した後、TA GUI に移動します。

1. [可視性（Visibility）] > [インベントリ検索（Inventory Search）] に移動します。
2. 感染したホストの IP アドレスを入力し、[検索（Search）] をクリックします。

検証

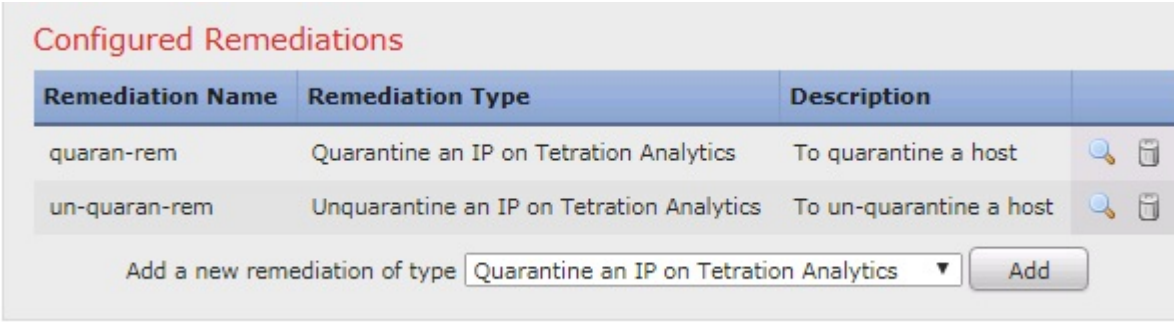
3. [ユーザ注釈（User Annotations）] で、感染したホストの IP アドレスに **quarantine = yes** という注釈が付けられていることを確認します。



次のタスク

隔離されたホストをクリーンにし、感染がなくなった後、TA GUI（推奨）を使用して **quarantine = yes** という注釈を **quarantine = no** に変更するか、または FMC 修復モジュールを使用して次のように隔離を解除します（セキュリティの問題のため、実稼働ネットワークでは非推奨）。

- （「設定：ステップ 1」を参照）隔離解除タイプの修復を使用する新しい修復を追加します。同じインスタンスを編集し、[設定されている修復（Configured Remediations）] で、隔離解除タイプの修復を選択し、追加します（この例では、**un-quaran-rem**）。



検証

- （「設定：ステップ 2」を参照）隔離解除修復をトリガーするために使用できるアクセス コントロール ルール（この例では、**remove-tag**）を同じポリシー（この例では、**rem-policy**）に追加します。
- （「設定：ステップ 3」を参照）アクセス コントロール ルール（この例では、**remove-tag**）を使用する相関ルール（この例では、**unquaran-rule1**）を追加します。
- （「設定：ステップ 4」を参照）隔離解除応答（この例では、**un-quaran-rem**）を相関ルール（この例では、**unquaran-rule1**）に割り当てます。

- このルールに一致すると、隔離解除修復がトリガーされ、隔離注釈が削除されます。

検証