



検証

- 検証 (1 ページ)

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。

Overview **Analysis** Policies Devices Objects AMP Intelligence Deploy System Help ▾

Context Explorer Connections ▾ Intrusions ▾ Files ▾ Hosts ▾ Users ▾ Vulnerabilities ▾ **Correlation ▶ Status** Custom ▾ Lookup ▾

Remediation Status

Table View of Remediations 2018-07-28 01:22:27 - 2018-07-28 02:41:29 Expanding

No Search Constraints ([Edit Search](#))

Jump to... ▾

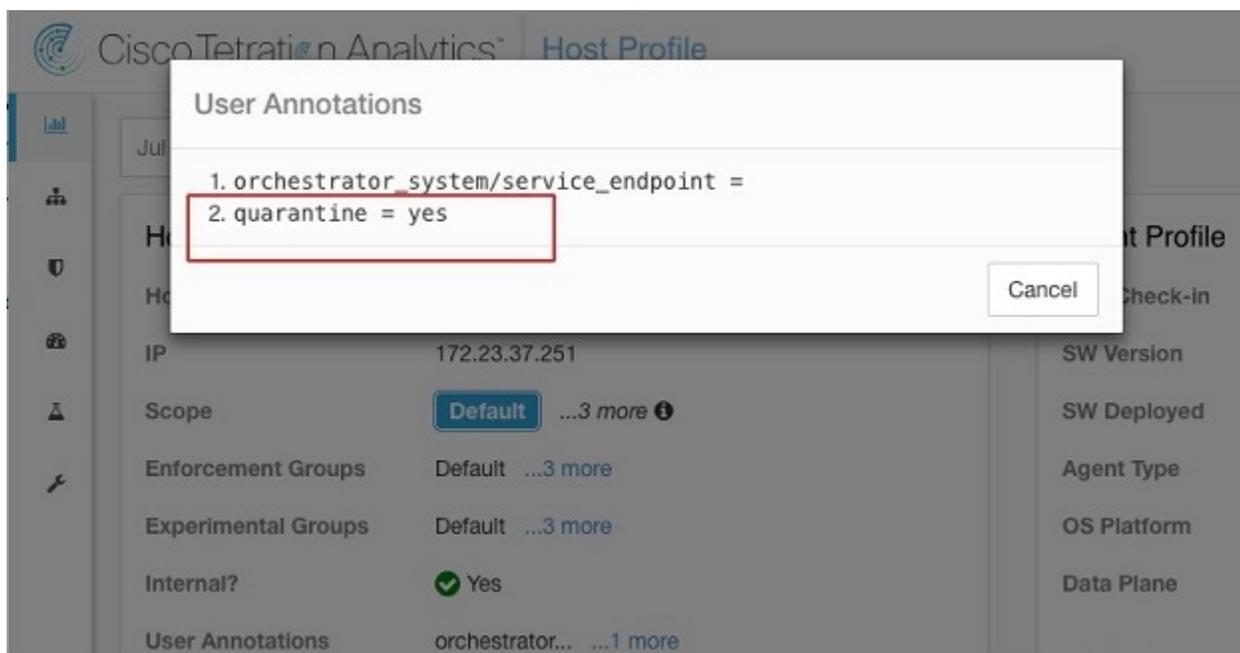
Time ×	Remediation Name ×	Policy ×	Rule ×	Result Message ×
2018-07-28 02:26:09	guaran-rem	correlation-policy	guaran-rule1	Successful completion of remediation

Page 1 of 1 | Displaying row 1 of 1 rows

View Delete

- 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。

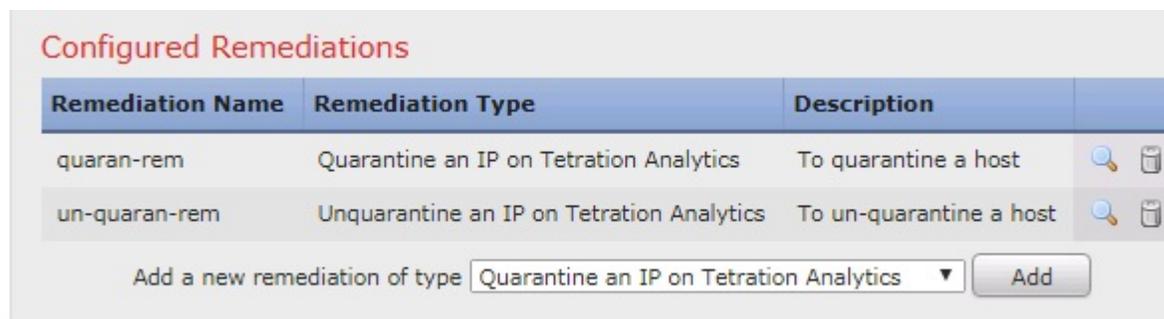
3. [ユーザ注釈 (User Annotations)] で、感染したホストの IP アドレスに **quarantine = yes** という注釈が付けられていることを確認します。



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**)。



- (「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**) を使用する関連ルール (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**) を関連ルール (この例では、**unquaran-rule1**) に割り当てます。

Policy Rules	
Rule	Responses
<u>quaran-rule1</u> add tag	quaran-rem (Remediation)
<u>unquaran-rule1</u> removing tag	un-quaran-rem (Remediation)

- 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。

