

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 De	evices Objects AMP Intel	ligence	Deploy System Help v
Context Explorer Connections •	Intrusions 🔹 Files 🔹 Hosts 🔻	Users • Vulnerabilities •	Correlation ► Status Custom ▼ Lookup ▼
Remediation Status Table View of Remediations No Search Constraints (Edit Search) Jump to			II 2018-07-28 01:22:27 - 2018-07-28 02:41:29 ⊘ Expanding
▼ <u>Time</u> ×	Remediation Name ×	Policy × Rule ×	Result Message ×
2018-07-28 02:26:09	<u>quaran-rem</u>	correlation-policy quaran-r	ule1 Successful completion of remediation
<pre>I of 1 >> I Displaying row</pre>	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。

C	Cisco Tetration Ana	alvtics" Host Profile	_
Lani,	User Annotation	IS	
4	1. orchestrator 2. quarantine =	_system/service_endpoint = yes	t Profile
U	Нс		Cancel Check-in
Ø	IP	172.23.37.251	SW Version
▲	Scope	Default3 more	SW Deployed
×	Enforcement Groups	Default3 more	Agent Type
	Experimental Groups	Default3 more	OS Platform
	Internal?	🔿 Yes	Data Plane
	User Annotations	orchestrator1 more	

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)。

Configured Remediations

Remediation Name	Remediation Type	Description	
quaran-rem	Quarantine an IP on Tetration Analytics	To quarantine a host	9, 8
un-quaran-rem	Unquarantine an IP on Tetration Analytics	To un-quarantine a host	9.6
Add a new rem	ediation of type Quarantine an IP on Tetratio	on Analytics V Add	

2

- (「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。

Rule	Responses
<u>guaran-rule1</u> add tag	quaran-rem (Remediation)
unquaran-rule1	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。

検証

4