

修復モジュールの設定

次のセクションでは、修復モジュールを設定する手順について説明します。

設定(Configure) (1ページ)

設定(Configure)

FMC にインストールされた修復モジュールを設定するには、次の手順を実行します。

- **ステップ1** FMC で、ネットワーク内の Cisco Secure Workload クラスタごとに修復モジュールのインスタンスを作成します。
 - **1.** [ポリシー (Policies)]>[アクション (Actions)]>[インスタンス (Instances)]に移動します。
 - 2. ドロップダウン リストから修復モジュールを選択し、[追加(Add)]をクリックします。
 - 3. [インスタンス名 (Instance Name)]を入力します (この例では fmc-dev-remediation)。
 - **4.** Cisco Secure Workload サーバーの IP アドレス、API キー、API シークレット、および問題がある可能性のあるホストが含まれる範囲を入力します。[作成(Create)]をクリックします。
 - (注) APIキーとシークレットは、この時点では Cisco Secure Workload サーバーに対して検証され ません。サイト管理者、カスタマーサポート、またはルートスコープオーナーロールは、 APIキーとシークレットを Cisco Secure Workload で最初に作成しておく必要があります。こ こで使用する情報をコピーします。詳細については、関連資料を参照してください。

| Firepower Management Center Policies / Actions / Instance Detail | Overview Analysis Polic | cies Devices Objects | AMP | Deploy Q 🌘 | 🦻 🔅 🕜 DC-North-South \ 📃 🔻 |
|---|--|-----------------------------------|----------------------------|------------|----------------------------|
| | Edit Instance | | | | |
| | Instance Name | fmc-dev-remediation | | | |
| | Module | Secure Workload / Secure Firewall | Remediation Module(v1.0.3) | | |
| | Description | | | | |
| | Secure Workload IP | 10.62.159.4 | | | |
| | Scope(must be root scope, e.g. Default) | Default | | | |
| | API key | | | | |
| | Retype to confirm | | | | |
| | API secret | | | | |
| | hetype to obtain | | | | |
| | | | Cancel Save | | |
| | | | | | |
| | Configured Remediation | ons | | | |
| | Remediation Name Remed | iation Type | Description | | |
| | quarantine-fmc Quaran | tine an IP on Secure Workload | /1 | | |
| | unquarantine-fmc Unquar | rantine an IP on Secure Workload | /1 | | |
| | Add a new remediation of | type Quarantine an IP on Secur | e Wor 🔻 🖌 Add | | |
| | | | | | |

- 5. [設定されている修復(Configured Remediations)]で、修復のタイプ(この例では「Quarantine an IP on Secure Workload」)を選択し、[追加(Add)]をクリックして新しい修復を追加します。
- 6. [修復名 (Remediation Name)] (この例ではquarantine-fmc) を入力し、[作成 (Create)]をクリックします。

| altalta cisco | Firepower Management Center Policies / Actions / Remediation Edit | Overview | Analysis | Policies | Devices | Objects | AMP | | Deploy | ۹ | ¢ | ¢ | DC-North-South \ |
|------------------|--|----------|-----------|---------------|--------------|---------------|-------------|--|--------|---|---|---|--------------------------------|
| | | | | | | | | | | | | | Alerts Remediations Groups |
| | | | Edit Reme | diation | | | | | | | | | |
| | | | Rem | nediation Nam | e quarant | ine-fmc | | | | | | | |
| | | | Rei | mediation Typ | e Quarantine | an IP on Secu | re Workload | | | | | | |
| | | | | Descriptio | n To quaran | tine a host | | | | | | | |
| | | | | | | Cancel | Create | | | | | | |
| | | | | | | | | | | | | | |

7. 設定した修復がテーブルに表示されます。[保存(Save)]をクリックします。

ステップ2 アクセス制御ポリシーを設定します(この例では、rem-policy)。

- [ポリシー(Policies)]>[アクセス制御(Access Control)]を選択し、アクセスコントロールポリシーの[編集(Edit)]アイコンをクリックしてルールを追加します。
- 2. [ルールの追加(Add Rule)]をクリックし、名前(この例ではblock-ssh-add-tag)を入力します。
- 3. [アクション(Action)]で[ブロック(Block)]を選択します。
- 4. [ポート (Ports)]タブで、宛先ポートのプロトコルの一覧から[SSH (SSH)]を選択します。
- 5. [ロギング (Logging)] タブで、[接続開始時のログ (Log at Beginning of Connection)]を選択します。
 - **重要** アクセスルールでロギングが有効になっていることを確認します。これにより、FMC はイ ベント通知を受信します。確認したら [追加(Add)]をクリックします。

6. [保存 (Save)] をクリックします。

| , i | Firepo Policies / | wer Man Access Cor | nagement htrol / Policy E | Center | Overview | Analysis | Policie | s Devic | es Obj | jects AN | IP Intelli | gence | Deploy | a a | 6 < | £ (2) |) Global | Δ., | • |
|--------|-------------------------------|-----------------------|------------------------------|-----------------|---------------|--------------|---------|---------|-----------------|----------------|-----------------|------------------------------|------------------------------|---------------|------------|------------|-----------|---------|-----|
| n E | em-policy nter Description | | | | | | | | | | | | ngs Ana | lyze Hit Co | Gettings | Sa Poli | ve | Cance | el |
| | Rules Secu | rity Intelliger | nce HTTP | P Responses | Logging | Advanc | ed | | | Prefilter P | Policy: Default | Prefilter Poli | cy SSL | Policy: N | one | Ide | entity Po | licy: N | one |
| Fi | ter by Device | T Searc | h Rules | | | | | | | | × | Show R | tule Conflicts | 0 + A | dd Cate | gory | + | Add Ru | ile |
| # | Name | Source Zones | Dest Zones | Source Netwo | Dest Netwo | VLAN Tags | Users | Applic | Source Ports | Dest Ports | URLs | Source Dynamic Attribu | Destin Dynamic Attribu | Action | F6 🛡 | E | 3 🗆 🛙 | j 🗭 | ¢ |
| \sim | Mandatory - rem | -policy (1-1 | 1) | | | | | | | | | | | | | | | | |
| 1 | block-ssh-add | Any | Any | Any | Any | Any | Any | Any | Any | SSH | Any | Any | Any | Block | B | Re S | | 0, | |
| \sim | Default - rem-po | licy (-) | | | | | | | | | | | | | | | | | |
| Th | ere are no rules i | n this sectio | on. Add Rule | or Add Categ | ory | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| Def | ault Action | | | | | | | | | | | Acce | ss Control:Blo | ock all traff | ic | | | , | |
| | | | | | | | | | I | Displaying 1 - | 1 of 1 rules | < Page 1 | of 1 > > | CRule | s per p | age: 1 | 00 | | • |

ステップ3 相関ルールを設定します。

- **1.** [ポリシー (Policies)]>[相関 (Correlation)]>[ルールの管理 (Rule Management)]に移動します。
- 2. [ルールの作成 (Create Rule)]をクリックします。
- **3.** [ルール名 (Rule Name)]を入力し(この例では、quaran-rule1)、説明(オプション)を入力しま す。
- **4.** [このルールのイベントタイプの選択 (Select the type of event for this rule)] セクションで、[接続イベントの発生 (a connection event occurs)]および[接続の開始時または終了時 (at either the beginning or the end of the connection)]を選択します。
- 5. [条件を追加(Add condition)] をクリックし、演算子を OR から AND に変更します。
- 6. ドロップダウンリストで、[アクセスコントロールルール名(Access Control Rule Name)]、[は(is)] を選択し、ステップ2で設定したアクセス コントロール ルールの名前を入力します(この例では、 block-ssh-add-tag)。

| night, Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy Q 💕 🄅 🔕 Global 👘 |
|--|
| Alerts Remediations Group |
| Policy Management Rule Management Allow List Traffic Profiles |
| Rule Information Add Connection Tracker Add User Qualification Add Host Profile Qualification |
| Rule Name quaran-rule1 |
| Rule Description |
| Rule Group Ungrouped • |
| Select the type of event for this rule |
| If a connection event occurs v at the beginning of the connective and it meets the following conditions: |
| Add condition Add complex condition |
| Image: Control Rule Name Image: Second Sec |
| |
| Rule Options |
| Snooze If this rule generates an event, snooze for 0 hours |
| Inactive Periods There are no defined inactive periods. To add an inactive period, click "Add inactive Period", |
| Cancel Save |

- 7. [保存 (Save)]をクリックします。
- ステップ4 相関ルールに、修復モジュールのインスタンスを応答としてアソシエートします。
 - 1. [ポリシー (Policies)]>[相関 (Correlation)]>[ポリシーの管理 (Policy Management)]に移動します。
 - 2. [ポリシーの作成 (Create Policy)]をクリックします。
 - **3.** [ポリシー名 (Policy Name)]を入力し(この例では、correlation-policy)、説明(オプション) を入力します。
 - 4. [ディフォルトのプライオリティ (Default Priority)]ドロップダウンリストから、ポリシーのプライオ リティを選択します。[なし (None)]を選択して、ルールのプライオリティのみ使用します。
 - 5. [ルールの追加(Add Rules)]をクリックし、ステップ3で設定した相関ルールを選択し(この例では、 quaran-rule1)、[追加(Add)]をクリックします。
 - 6. ルールの横にある[応答 (Responses)]アイコンをクリックし、ルールに応答 (この例ではtest_rem) を割り当てます。[更新 (Update)]をクリックします。

| CISCO Firepower Management Center Policies / Correlation / Policy Management | erview Analysis | Policies | Devices | Objects | AMP | Intelligence | Deploy | Q | 6 \$ | 🕜 Glo | bal \ | T |
|---|-----------------------|----------|---------|---------|-----|--------------|----------|---|-------------|-----------|--------------|---|
| | | | | | | | | | Alerts R | emediatic | ins Groups | s |
| Policy Management Rule Management Allow List | Traffic Profiles | | | | | | | | | | | |
| Correlation Policy Information | | | | | | | | | С | ancel | Save | |
| Policy Name correlation-policy | | | | | | | | | | | | |
| Policy Description | | | | | | | | | | | | |
| Default Priority None | • | | | | | | | | | | | |
| Policy Rules | | | | | | | | | | Ad | d Rules | |
| Rule | Responses | | | | | | Priority | | | | | |
| quaran-rule1 | test_rem (Remediation | on) | | | | | Default | | | • | ₩ ¥ | |
| | | | | | | | | | | | | |

7. [保存 (Save)]をクリックします。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては 、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている 場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容につい ては米国サイトのドキュメントを参照ください。