

設定(Configure)

・設定 (1ページ)

設定

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、FMC GUI で次の手順を実行します。

ステップ1 ネットワーク内の Tetration Analytics (TA) サーバ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。

Overview Ana	alysis Policies	Devices Objects	AMP	Intelligence	Deploy	System
Access Control •	Network Discover	ry Application Det	ectors	Correlation	Actions •	Instanc
					Alerts Ren	nediations
Configured In	stances					
Instance Name		Module Name		Version		
		No instances o	onfigured			
Add a New In:	stance					
	Select a module type	Tetration/FirePOWER	Remediatio	n Module(v1.0.1)	▼ Add	
インスタンス名(Instance Name)]を入	力します(この例では	. rem-in	nstance)		

- 4. TA サーバの IP アドレス、API キー、API シークレット、および問題の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TAサーバ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TA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、『TA API Configuration Guide』を参照してください。

設定

Overview	w Analysis	Policies De	evices (Objects	AMP	Intelligen	ce Deploy	Syster
Access Co	ontrol 🔹 Ne	twork Discovery	Applic	ation Dete	ectors	Correlation	Actions •	Instanc
							Alerts Rem	ediations
						×		
		Created new	instance re	em-instance	e			
	Edit Instar	nce						
	Instance Nam	e		,	rem-instar	nce		
	Module			-	Tetration/I	FirePOWER Rer	mediation Module	e(v1.0.1)
	Description							
	Tetration Anal	ytics IP		[172.26.46	.68		
	Scope(e.g. De	fault)			SBG			
	API key				•••••			
	Retype to confirm	n			•••••	•••••	•••••	
	API secret	-			•••••	•••••	•••••	
	Relype to comm			t			**********	
					Save	Cancel		
	Configured	d Remediations	5					
	Remediatio	n Name	Ren	nediation	Туре	D	escription	
			No config	ured remed	liations av	ailable		
	Add a	new remediation o	f type Qua	arantine an	IP on Tet	ration Analytics	s 🔻 🗛 Add	

- 5. [設定されている修復(Configured Remediations)]で、修復のタイプを選択し(この例では、Quarantine an IP on Tetration Analytics)、[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)]を入力し(この例では、quaran-rem)、[作成 (Create)]をクリック します。

Overview	Analysis	Policies D	evices Objects	AMP	Intelligence	Deploy	System		
Access Cont	Access Control Network Disc		Application De	etectors	Correlation	Actions •	Instances		
					Ale	rts Remediat	ions Groups		
		Edit Re	emediation						
		Remedia	ion Name		quaran-rem				
		Remedia	ion Type		Quarantine an IP on Tetration Analytics				
					To quarantine	a host			
		Descripti	n						
					Create	Cancel			

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。

設定

verview A	nalysis Polic	ies Devices	6 Objects	AMP	Intelligence	e Deploy	S	yster
cess Control	 Network D 	iscovery Ap	plication Dete	ctors	Correlation	Actions	Inst	tanc
					Al	erts Remedia	tions	Grou
E	dit Instance							
In	stance Name			rem-instar	nce			
Mo	odule			Tetration/F	FirePOWER Rer	mediation Mod	ule(v1	.0.1)
De	escription							
Те	tration Analytics IP			172.26.46	.68			
Sc	cope(e.g. Default)			SBG				
AP	PI key			•••••		•••••		
Ret	type to confirm			•••••	•••••	•••••		
AP	I secret			•••••	•••••	•••••		
Rei	type to contirm			•••••				
				Save	Cancel			
C	onfigured Rem	ediations						
R	emediation Nam	e Remediati	on Type		Descrip	otion		
a	luaran-rem	Quarantine	an IP on Tetrat	ion Analytic	s To quar	antine a host	0,	8
							_	

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)。

- 1. [ポリシー (Policies)]>[アクセス制御 (Access Control)]>[ルール (Rules)]に移動します。
- 2. [ルールの追加(Add Rule)]をクリックします(たとえば、block-ssh-add-tag)。
- 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]を選択し、[追加 (Add)]をクリックします。
- 5. [保存 (Save)] をクリックします。

設定

- 6. [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。
- 7. [保存 (Save)]をクリックします。

Ove	erview Analys	is Policies	Devices Ol	bjects	AMP In	telligence							Deploy	/ System	Help 🔻	test 🔻
Acc	ess Control 🕨 A	ccess Control	Network Dis	covery	Applicatio	on Detectors	Corr	elation	Actions •							
rer for te	rem-policy															
Prefi	Prefilter Policy: Default Prefilter Policy: None Identity Policy: None															
Ru	les Security I	ntelligence H	TTP Responses	Advance	:d							Ĩ∎ I	nheritance Se	ettings 📑 Polic	y Assignm	ents (1)
曲	Filter by Device									Show Rule Conflic	ts 🕑	🗿 Add	Category	Add Rule	Search R	ules 💥
#	Name	Source Zo	Dest Zones	Source	Dest	VLAN Tags	Users	Apps	Source Ports	Dest Ports	URLs	ISE/	Action	U 🗅 🔏 🕈	2 🔲 🛡	
-	Mandatory - rem	-policy (1-2)														
1	remove-tag	a external-zon∉ ゐ internal-zone	🚠 internal-zone 🏦 external-zone	Any	Any	Any	Any	Any	Any	👷 TCP (6):500	Any	Any	🖋 Allow	U D 2 t	j 🔲 o	6
2	block-ssh-add-ta	a external-zon∉ ゐ internal-zone	🚠 internal-zone	Any	Any	Any	Any	Any	Any	<i>∲</i> SSH	Any	Any	🗙 Block	0021	0 🛄	0
-	Default - rem-po	licy (3-3)														
3	allow-any	🚠 external-zone	🚠 internal-zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	UD.81	0 🗐	<i>⊘</i> ₿

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。
- [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。
- 4. [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。
- 5. 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)。

6.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	e	Deploy
Access Cont	rol 🔻 N	letwork Discov	very App	lication Det	ectors	Correlation	Actio	ns 🔻
								Alerts
Policy Ma	nagemen	t Rule M	lanagemen	t White	e List	Traffic Prof	iles	
Rule Info	ormation		O Add Co	nnection Trac	ker 🔇	Add User Qua	lification	Add Hos
Rule Name		quaran-rule1						
Rule Descri	iption	add tag						
Rule Group		Ungrouped	▼.					
Select th	ne type o	of event for	this rule					
If a con	nection eve	nt occurs 🔻 🛛 a	t either the b	eginning or th	ne end of t	he connection 🔻	and it	meets the fol
	O Add	condition	Add compl	ex condition)			
	X Acc	cess Control Rul	e Name		• i	s	▼ bl	ock-ssh-add-tag
Rule Opt	tions							
Snooze		If this rule ge	enerates an ev	vent, snooze	for0	hours 🔻		
Inactive Per	riods	There are no	defined inact	ive periods. T	io add an i	nactive period, o	lick "Add	Inactive Period".
[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. [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。

(Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	System
A	Access Cont	rol 🔻 Net	twork Discov	ery App	lication Dete	ectors	Correlation	Actions 🔻	
								Aler	ts Remedia
1	Policy Ma	anagement	Rule M	lanagemer	t White	e List	Traffic Profil	es	
	Correlat	tion Policy	Informatio	on					Save
	Policy Nam	ie	correlat	tion-policy					
	Policy Desc	cription	correlat	tion policy for	testing				
	Default Pri	ority	None 1	•					
	Policy R	ules							0
	Rule				R	esponses	5		Priority
	guaran-i add tag	rule1			т	his rule do	es not have any re	esponses.	Default 🔻

6. ルールの横にある [応答 (Responses)] アイコンをクリックし、ルールに応答を割り当てます (この例 では、quaran-rem)。[更新 (Update)] をクリックします。

(Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	System
4	Access Cont	rol 🔻 Ne	twork Discov	ery App	lication Dete	ectors	Correlation	Actions 🔻	
								Ale	rts Remedia
1	Policy Ma	anagemen	t Rule M	lanagemen	t Whit	e List	Traffic Profil	es	
	Correlat	ion Policy	Informatio	on					Save
	Policy Nam	e	correlat	ion-policy					
	Policy Desc	cription	correlat	ion policy for	testing				
	Default Pri	ority	None 1	•					
	Policy R	ules							0
	Rule				R	esponses	5		Priority
	guaran-i add tag	rule1			q	uaran-rem	(Remediation)		Default 🔻

設定

7. [保存 (Save)]をクリックします。

I

I