FMCでの相関ポリシーの設定

内容

<u>はじめに</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>背景説明</u> <u>設定</u> <u>相関ルールの設定</u> <u>アラートの設定</u> <u>相関ポリシーの設定</u>

はじめに

このドキュメントでは、イベントを接続し、ネットワーク上の異常を検出するために相関ポリシ ーを設定する手順について説明します。

前提条件

要件

次の製品に関する知識があることが推奨されます。

- セキュアファイアウォール管理センター(FMC)
- セキュアファイアウォール脅威対策(FTD)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

VMware向けFirepower Threat Defenseバージョン7.6.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

相関ポリシーは、さまざまなタイプのイベントを設定してネットワーク上の潜在的なセキュリテ ィ脅威を特定するために使用され、修復、条件付きアラート、およびトラフィックポリシーに使 用されます。

設定

相関ルールの設定

ステップ1: Policies > Correlationに移動し、Rule Managementを選択します。



画像 1.相関ポリシーメニューへのナビゲーション

ステップ2: Create Ruleを選択して、新しいルールを作成します。

Home	Policy Management	Rule Management	Allow List	Traffic Profiles		Alerts Ren	nediations Groups
Overview						Create Rule	Create Group
III Analysis	There are no rules curren	ntly defined. To create a rui	e, click "Create Ru	ile".			

画像 2.ルール管理メニューでのルールの作成

ステップ3:ルールに一致するイベントタイプと条件を選択します。

ルールに複数の条件が含まれている場合は、それらの条件をAND演算子またはOR演算子でリン クする必要があります。

Rule Information		Add Connection Tracker	Add User Qualification	Add Host Profile Qualification
Rule Name	connection			
Rule Description				
Rule Group	Ungrouped v			
Select the type of event for	r this rule			
If a connection event occurs	~] at any point of the connection ~] and it meets the follow	ing conditions:		
Add condition	Add complex condition			
Application	Protocol v lis v HTTPS	~		
Ad	d condition Add complex condition			
	Source Country	om ~		
	Source Country	~		

画像 3.ルール作成メニュー

◆ 注:相関ルールは汎用的なものにしないでください。ルールが常に通常のトラフィックによってトリガーされる場合、追加のCPUを消費し、FMCのパフォーマンスに影響を与える可能性があります。

アラートの設定

ステップ1: [Policies] > [Actions] > [Alerts] の順に移動します。

Firewall Management Center Policies / Actions / Alerts / Alerts



図 4.[Alerts]メニューへのナビゲーション

ステップ 2: Create Alertを選択し、Syslog、SNMP、または電子メールアラートのいずれかを作 成します。

					Allow List Harris Fromes	Alerta Kellieur	auona j on	oups (Wo	nitor Alerta
Home	Alerts	Impact Flag Alerts	Discovery Event Alerts	Advanced Malware Protection Alerts	Intrusion Email				
- 53									
Overview								Create	Alert 🗸
ul.									_
Analysis	Name					Туре	In Use	Enabled	
8	email					Email	Not Used		00
Policies	email syslog					Email Syslog	Not Used Not Used		00 00

図 5.アラートの作成

ステップ3:アラートが有効になっていることを確認します。

相関ポリシーの設定

ステップ1: Policies > Correlationの順に移動します。



相関ポリシーメニューへのナビゲーション

図 6.相関ポリシーメニューへのナビゲーション

ステップ2:新しい相関ポリシーを作成します。デフォルトの優先度を選択します。特定のルールの優先度を使用するには、Noneを使用します。

cisco Polici	wall Management Center es / Correlation / Policy Management		Q Search	Deploy 🧳 🛞 🕐 admin v
Home	Policy Management Rule Management Allow List	Traffic Profiles		Alerts Remediations Groups
Overview				Create Policy
III Analysis	There are no policies currently defined. To create a policy, click "Create	e Policy".		
Policies				

図 7.新しい相関ポリシーの作成

ステップ 3: Add Rulesを選択して、ポリシーにルールを追加します。

Home		Alerts Remediations Groups
	Policy Management Rule Management Allow List Traffic Profiles	
Overview	Correlation Policy Information	Cancel Save You have unsaved changes
III Analysis	Policy Name Correlation	
, maryono	Policy Description	
Policies	Default Priority None ~	
	Policy Rules	Add Rules
Devices	No Rules Currently Active	
•_=		
Objects		

図 8.相関ポリシーのルールの追加と優先度の選択

	Available Rules		Alerts Remediations Groups
Policy Management Rule Manager Correlation Policy Informatio Policy Name	Select the rules you wish to add to this policy, then click "Add". Vungrouped Rules connection		Cancel Save
Policy Description	 Allow List Rules Default Allow List 	. 1	
Policy Rules No Rules Currently Active			Add Rules
	Can	el Add	

図 9.相関ポリシーに追加するルールの選択

ステップ 4: 作成したアラートからルールに応答を割り当てると、トリガーされるたびに選択し たアラートタイプが送信されます。

orrelation Policy Informa	tion		Cancel
Policy Name	Correlation		
Policy Description			
Default Priority	None ~		
licy Rules			Add
Rule	Responses	Priority	
connection	This rule does not have any responses.	Default	v) r

図 10.[返信の追加]ボタン

Responses for connection							
Assigned Responses							
Unassigned Responses							
email syslog							
Cancel Update							

図 11.相関ルールへの応答の割り当て

ステップ5:相関ポリシーを保存して有効にします。

Policy Management Rule Manag	gement Allow List Traffic Profiles	
Correlation Policy Information	tion	Cancel Save You have unsaved changes
Policy Name	Correlation	
Policy Description		
Default Priority	None ~	
Policy Rules		Add Rules
Rule	Responses	Priority
connection	email (Email)	Default v 🗆 🗆

図 12.相関ルールに正しく追加された応答

Policy Management	Rule Management	Allow List	Traffic Profiles		
					Create Policy
Name				Sort by State	~
Correlation					ā 🖞 💭

図 13.相関ポリシーの有効化

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。