Configurer la politique de corrélation sur FMC

Table des matières

ntroduction	
Conditions préalables	
Exigences	
Composants utilisés	
nformations générales	
Configurer	
Configurer les règles de corrélation	
Configurer les alertes	
Configurer la politique de corrélation	

Introduction

Ce document décrit la procédure de configuration d'une politique de corrélation pour connecter des événements et détecter des anomalies sur votre réseau.

Conditions préalables

Exigences

Cisco vous recommande d'avoir connaissance des produits suivants :

- · Centre de gestion du pare-feu sécurisé (FMC)
- · Protection pare-feu contre les menaces (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

• Firepower Threat Defense pour VMware version 7.6.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les politiques de corrélation permettent d'identifier les menaces de sécurité potentielles sur votre réseau en configurant différents types d'événements. Elles sont utilisées pour la correction, les

alertes conditionnelles et les politiques de trafic.

Configurer

Configurer les règles de corrélation

Étape 1. Accédez à Politiques > Corrélation et sélectionnez Gestion des règles.



Image 1. Navigation jusqu'au menu Correlation Policy

Étape 2. Créez une nouvelle règle en sélectionnant Créer une règle.

Home	Policy Management	Rule Management	Allow List	Traffic Profiles		Alerts Remediations Groups
Overview						Create Rule Create Group
II Analysis	There are no rules curre	ntly defined. To create a rui	e, click "Create R	ıle".		

Image 2. Création de règle dans le menu Gestion des règles

Étape 3. Sélectionnez un type d'événement et les conditions qui correspondent à la règle.

Lorsque votre règle contient plusieurs conditions, vous devez les lier à l'opérateur AND ou OR.

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	- this rule
If a connection event occurs	at any point of the connection
Add condition	Add complex condition
Application P	Protocol
Add	d condition Add complex condition
	Source Country
	Source Country

Image 3. Menu Création de règle

Remarque : les règles de corrélation ne doivent pas être génériques. Si la règle est constamment déclenchée par le trafic normal, cela peut consommer davantage de CPU et affecter les performances FMC.

Configurer les alertes

Étape 1. Accédez à Politiques > Actions > Alertes.

Firewall Management Center Policies / Actions / Alerts / Alerts



Image 4. Navigation vers le menu Alertes

Étape 2. Sélectionnez Create Alert et créez une alerte Syslog, SNMP ou une alerte par e-mail.

Home	Alerts	Impact Flag Alerts	Discovery Event Alerts	Advanced Malware Protection Alerts	Intrusion Email				
Overview								Create	Alert ~
dil.									
Analysis	Name					Туре	In Use	Enabled	
Anaiysis	email					Type	In Use Not Used	Enabled	Ø Ū
Policies	email syslog					Type Email Syslog	In Use Not Used Not Used	Enabled	0 0 0 0

Image 5. Créer une alerte

Étape 3. Vérifiez que l'alerte est activée.

Configurer la politique de corrélation

Étape 1. Accédez à Politiques > Corrélation.



Navigation jusqu'au menu Correlation Policy

Image 6. Navigation jusqu'au menu Correlation Policy

Étape 2. Créez une nouvelle politique de corrélation. Sélectionnez la priorité par défaut. Utilisez None pour utiliser les priorités des règles spécifiques.

cisco Policie	vall Management Center Q Search	Deploy	🧳 🛞 🕐 🛛 admin ~
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 Policy".		
Policies			

Image 7. Créer une nouvelle stratégie de corrélation

Étape 3. Ajoutez des règles à la stratégie en sélectionnant Ajouter des règles.

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	
	Policy Description	
Policies	Default Priority None ~	
=	Policy Rules	Add Rules
Devices	No Rules Currently Active	
•=		
Objects		

Image 8. Ajouter des règles et sélectionner la priorité pour la stratégie de corrélation

	Available Rules		Alerts Remediations Groups
Policy Management Rule Managen Correlation Policy Informatio Policy Name	Select the rules you wish to add to this policy, then click "Add". ~ Ungrouped Rules _ connection		Cancel
Policy Description Default Priority t	 Allow List Rules Default Allow List 		Add Rules
No Rules Currently Active			
		Cancel	

Image 9. Sélectionner les règles à ajouter à la politique de corrélation

Étape 4. Affectez une réponse à la règle à partir des alertes que vous avez créées, de sorte que chaque fois qu'elle est déclenchée, elle envoie le type d'alerte sélectionné.

orrelation Policy Inform	ation	Cancel
Policy Name	Correlation	
Policy Description		
Default Priority	None ~	
blicy Rules		A
Rule	Responses	Priority
connection	This rule does not have any responses	Default

Image 10. Bouton Ajouter des réponses

Responses for connection						
Assigned Responses						
Unassigned Responses	Unassianed Responses					
email syslog						
Cancel Update						

Image 11. Affecter des réponses à la règle de corrélation

Étape 5. Enregistrez et activez votre politique de corrélation.

Policy Management Rule Manag	gement Allow List Traffic Profiles		
Correlation Policy Information	tion	Cancel Save You have unsave	d changes
Policy Name	Correlation		
Policy Description			
Default Priority	None ~		
Policy Rules			dd Rules
Rule	Response	s Priority	
connection	email (Em	il) Default ~	οŌ

Image 12. Réponse ajoutée correctement à la règle de corrélation

Policy Management	Rule Management	Allow List	Traffic Profiles		
					Create Policy
Name				Sort by State	~
Correlation					Ū (1) (1)

Image 13. Activer la stratégie de corrélation

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.