Configurar política de correlação no FMC

Contents

Introdução

Este documento descreve o procedimento para configurar uma política de correlação para conectar eventos e detectar anomalias em sua rede.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes produtos:

- · Centro de gerenciamento seguro de firewall (FMC)
- Defesa contra ameaças de firewall (FTD) segura

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

• Firepower Threat Defense para VMware versão 7.6.0

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As políticas de correlação são usadas para identificar possíveis ameaças à segurança na rede, configurando diferentes tipos de eventos, e são usadas para correção, alertas condicionais e

políticas de tráfego.

Configurar

Configurar regras de correlação

Etapa 1. Navegue até Policies > Correlation e selecione Rule Management.



Imagem 1. Navegação para o menu Política de correlação

Etapa 2. Crie uma nova regra selecionando Criar regra.

Home	Policy Management	Rule Management	Allow List	Traffic Profiles		Alerts Remediations Groups
Overview						Create Rule Create Group
III Analysis	There are no rules currer	ntly defined. To create a rul	le, click "Create R	ule".		

Imagem 2. Criação de Regras no Menu Gerenciamento de Regras

Etapa 3. Selecione um tipo de evento e as condições para corresponder à regra.

Quando a regra contiver várias condições, você deverá vinculá-las a um operador 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 Pr	rotocol v Is v HTTPS v
Add	condition Add complex condition
	Source Country v is not v United Kingdom v
	Source Country

Imagem 3. Menu de Criação de Regra

Observação: as regras de correlação não devem ser genéricas; se a regra for acionada constantemente pelo tráfego normal, isso poderá consumir CPU adicional e afetar o desempenho do FMC.

Configurar alertas

Etapa 1. Navegue até Policies > Actions > Alerts.

Firewall Management Center Policies / Actions / Alerts / Alerts



Imagem 4. Navegação para o menu Alertas

Etapa 2. Selecione Create Alert e crie um Syslog, SNMP ou alerta por e-mail.

Home	Alerts	Impact Flag Alerts	Discovery Event Alerts	Advanced Malware Protection Alerts	Intrusion Email				
Overview								Create	Alert ~
III Analysis	Name					Туре	In Use	Enabled	
8	email					Email	Not Used		00
Policies	syslog					Syslog	Not Used		ØŌ

Imagem 5. Criar Alerta

Etapa 3. Verifique se o alerta está ativado.

Configurar política de correlação

Etapa 1. Navegue até Policies > Correlation.



Navegação para o menu Política de correlação

Imagem 6. Navegação para o menu Política de correlação

Etapa 2. Crie uma nova Política de Correlação. Selecione a prioridade padrão. Use Nenhum para usar as prioridades das regras específicas.

cisco Policie	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
ili] Analysis	There are no policies currently defined. To create a policy, click "Create Policy".		
Analysis			
Policies			
_			

Imagem 7. Criar nova política de correlação

Etapa 3. Adicione regras à política selecionando Add Rules.

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

Imagem 8. Adicionar regras e selecionar prioridade para política de correlação

	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	 Allow List Rules Default Allow List 		
Policy Rules No Rules Currently Active			Add Rules
	(Cancel Add	

Imagem 9. Selecionar regras para adicionar à política de correlação

Etapa 4. Atribua uma resposta à regra a partir dos alertas criados, de modo que, sempre que ela for disparada, o tipo de alerta selecionado seja enviado.

orrelation Policy Inforr	nation	Cancel
Policy Nam	e Correlation	
Policy Description	n	
Default Priorit	y None ~	
olicy Rules		Add
Rule	Responses	Priority
connection	This rule does not have any responses	Default

Imagem 10. Botão Adicionar respostas

Responses for connection					
Assigned Responses					
- A Lingssigned Desponses					
email syslog					
Cancel Update					

Imagem 11. Atribuir respostas à regra de correlação

Etapa 5. Salve e habilite sua Política de correlação.

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

Imagem 12. Resposta Adicionada Corretamente à Regra de Correlação

Policy Management	Rule Management	Allow List	Traffic Profiles		
					Create Policy
Name				Sort by State	~
Correlation					O (

Imagem 13. Habilitar Política de Correlação

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.