Configurar la política de correlación en FMC

Contenido

Introducción	
Prerequisites	
Requirements	
Componentes Utilizados	
Antecedentes	
Configurar	
Configurar reglas de correlación	
Configurar alertas	
Configurar política de correlación	

Introducción

Este documento describe el procedimiento para configurar una política de correlación para conectar eventos y detectar anomalías en su red.

Prerequisites

Requirements

Cisco recomienda que conozca estos productos:

- Centro de gestión de firewall seguro (FMC)
- Protección frente a amenazas de firewall (FTD)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

• Firepower Threat Defense para VMware versión 7.6.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Las políticas de correlación se utilizan para identificar posibles amenazas de seguridad en la red

mediante la configuración de diferentes tipos de eventos, y se utilizan para la remediación, alertas condicionales y políticas de tráfico.

Configurar

Configurar reglas de correlación

Paso 1. Navegue hasta Políticas > Correlación y seleccione Administración de reglas.

cisco Policie	wall Management (es / Correlation / Policy Ma	Center magement		
Home	Policies			×
E Overview	Access Control	Network Discovery	Actions	
ilil Analysis	Intrusion	Correlation V	Scanners	
Policies	Malware & File DNS		Groups Modules	
Devices	Identity Decryption		Instances	
©_≡ Objects	Prefilter Zero Trust Application			
3 Integration				

Imagen 1. Navegación al menú Política de correlación

Paso 2. Cree una nueva regla seleccionando Create Rule.

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

Imagen 2. Creación de reglas en el menú Administración de reglas

Paso 3. Seleccione un tipo de evento y las condiciones para que coincidan con la regla.

Cuando la regla contiene varias condiciones, debe vincularlas con AND o con un operador 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

Imagen 3. Menú de creación de reglas

Nota: Las reglas de correlación no deben ser genéricas. Si el tráfico normal activa constantemente la regla, esto puede consumir CPU adicional y afectar al rendimiento de FMC.

Configurar alertas

Paso 1. Vaya a Políticas > Acciones > Alertas.

Firewall Management Center Policies / Actions / Alerts / Alerts



Imagen 4. Navegación al menú Alertas

Paso 2. Seleccione Create Alert y cree un Syslog, SNMP o alerta de correo electrónico.

\sim				i oneleo initiasorritateo	Allow List Humorrollics			oups (mo	
Home	Alerts	Impact Flag Alerts	Discovery Event Alerts	Advanced Malware Protection Alerts	Intrusion Email				
Overview								Create	Alert ~
⊣III Analysis	Name					Туре	In Use	Enabled	
2	email					Email	Not Used		00
Policies	syslog					Syslog	Not Used		00
-									

Imagen 5. Crear alerta

Paso 3. Verifique que la alerta esté habilitada.

Configurar política de correlación

Paso 1. Vaya a Políticas > Correlación.



Navegación al menú Política de correlación

Imagen 6. Navegación al menú Política de correlación

Paso 2. Cree una nueva política de correlación. Seleccione la prioridad predeterminada. Utilice None para utilizar las prioridades de las reglas 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			
_			

Imagen 7. Crear nueva política de correlación

Paso 3. Agregue reglas a la directiva seleccionando Add Rules.

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

Imagen 8. Agregar reglas y seleccionar prioridad para la política de correlación

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

Imagen 9. Seleccionar reglas para agregar a la directiva de correlación

Paso 4. Asigne una respuesta a la regla desde las alertas que ha creado, de modo que siempre que se active, enviará el tipo de alerta seleccionado.

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

Imagen 10. Botón Agregar respuestas

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

Imagen 1. Asignar respuestas a regla de correlación

Paso 5. Guarde y active la política de correlación.

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 ~ 🗆 🗆

Imagen 12. Respuesta agregada correctamente a la regla de correlación

Policy Management	Rule Management	Allow List	Traffic Profiles		
					Create Policy
Name				Sort by State	~
Correlation					Ū 🖗 💭 Ū

Imagen 13. Habilitar política de correlación

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).