Configurer des règles de sniffage local personnalisées dans Snort3 sur FTD

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Diagramme du réseau
Configuration
Méthode 1. Importer de Snort 2 vers Snort 3
Étape 1. Confirmer la version Snort
Étape 2. Créer ou modifier une règle de sniffage local personnalisée dans Snort 2
Étape 3. Importer des règles de sniffage locales personnalisées de Snort 2 vers Snort 3
Étape 4. Action Modifier la règle
Étape 5. Confirmer la règle de sniffage local personnalisée importée
Étape 6. Associer une politique d'intrusion à une règle de politique de contrôle d'accès (ACP)
Étape 7. Déployer les modifications
Méthode 2. Télécharger un fichier local
Étape 1. Confirmer la version de Snort
Étape 2. Créer une règle de détection locale personnalisée
Étape 3. Télécharger la règle de détection locale personnalisée
Étape 4. Action Modifier la règle
Étape 5. Confirmer la règle de détection locale personnalisée téléchargée
Étape 6. Associer une politique d'intrusion à une règle de politique de contrôle d'accès (ACP)
Étape 7. Déployer les modifications
Vérifier
Étape 1. Définition du contenu du fichier dans le serveur HTTP
Étape 2. Requête HTTP initiale
Étape 3. Confirmer l'incident
Foire aux questions (FAQ)
<u>Dépannage</u>
Référence

Introduction

Ce document décrit la procédure pour configurer des règles de détection locale personnalisées dans Snort3 sur Firewall Threat Defense (FTD).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Management Center (FMC)
- Protection contre les menaces par pare-feu

Composants utilisés

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

- Cisco Firepower Management Center pour VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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

La prise en charge de Snort 3 dans la défense contre les menaces avec le centre de gestion commence dans la version 7.0. Pour les nouveaux périphériques et les périphériques réimagés des versions 7.0 et ultérieures, Snort 3 est le moteur d'inspection par défaut.

Ce document fournit un exemple de personnalisation des règles Snort pour Snort 3, ainsi qu'un exemple pratique de vérification. En particulier, vous apprendrez à configurer et à vérifier une stratégie d'intrusion avec une règle Snort personnalisée pour abandonner les paquets HTTP qui contiennent une certaine chaîne (nom d'utilisateur).



Attention : la création de règles Snort locales personnalisées et leur prise en charge ne sont pas prises en charge par le TAC. Par conséquent, ce document ne peut être utilisé qu'à titre de référence et vous demandez de créer et de gérer ces règles personnalisées à votre discrétion et sous votre responsabilité.

Diagramme du réseau

Ce document présente la configuration et la vérification de la règle de sniffage local personnalisée dans Snort3 sur ce schéma.



Diagramme du réseau

Configuration

Il s'agit de la configuration de la règle de détection locale personnalisée pour détecter et supprimer les paquets de réponse HTTP contenant une chaîne spécifique (nom d'utilisateur).



Remarque : il n'est pas possible d'ajouter des règles Snort locales personnalisées à partir de la page Toutes les règles Snort 3 de l'interface utilisateur graphique FMC. Vous devez utiliser la méthode présentée dans ce document.

Méthode 1. Importer de Snort 2 vers Snort 3

Étape 1 : confirmation de la version Snort

Accédez àPériphériques>Gestion des périphériques sur FMC, cliquez sur l'onglet Périphérique. Vérifiez que la version de Snort est Snort3.

þ	Firewall Management Center Overview Devices / Device Management	Analysis Policies D	evices Obje	ects Integration		Deploy Q 💕 🌣	admin v duala	SECURE
View E	8y: Group 🔻						Migrate Deployment	History
All	(1) • Error (0) • Warning (0) • Offline (0) • N	ormal (1) • Deployment P	ending (0)	Upgrade (0) Snort 3 (1)		a	Search Device	Add 🔻
Collaps	se All						Download Device	List Report
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
	V Ungrouped (1)							
	FPR2120_FTI 5.000 Short 3 1.126.029 - Noted	Firepower 2120 with FTD	7.4.1	N/A	Essentials, IPS (1 more)	acp-rule	4 9	1

Version Snort

Étape 2. Créer ou modifier une règle de sniffage local personnalisée dans Snort 2

Accédez à Objets > Règles d'intrusion > Snort 2 All Rules sur FMC. Cliquez sur le bouton Créer une règle pour ajouter une règle de sniffage local personnalisée, ou accédez à Objets > Règles d'intrusion > Toutes les règles de sniffage 2 > Règles locales sur FMC, cliquez sur le bouton Modifier pour modifier une règle de sniffage local existante.

Pour des instructions sur la façon de créer des règles de Snort local personnalisées dans Snort 2, veuillez vous référer à <u>Configurer des règles de Snort local personnalisées dans Snort2 sur FTD</u>.

Ajoutez une nouvelle règle d'analyse locale personnalisée comme illustré dans l'image.

Firewall Management Center Objects / Intrusion Rules / Snort 2 All Rules	Overview Anal	sis Policies	Devices	Objects Integra	gration [Deploy	۹ 📀	¢ 0	$\operatorname{admin} \lor $	cisco SECURE
Snort 2 All Rules Snort 3 All Rules				Object Manageme	ment					
< Intrusion Policy				Intrusion Rules	Search	Delete	Local Ru	les In	nport Rules	Create Rule

Ajouter une nouvelle règle personnalisée

Modifiez une règle de sniffage local personnalisée existante comme indiqué dans l'image. Dans cet exemple, modifie une règle personnalisée existante.



Modifier une règle personnalisée existante

Entrez les informations de signature pour détecter les paquets HTTP contenant une chaîne

spécifique (nom d'utilisateur).

- Message : custom_http_sig
- Action : alerte
- Protocole : TCP
- flux : établi, au client
- content : username (Raw Data)

Firewall Management Center Objects / Intrusion Rules / Create	iew Analysis Policies Devices Objects	Integration	Deploy Q 🚱 🌣 🕢 admin 🗸 🐝 SECURE
Snort 2 All Rules Snort 3 All Rules		-	Search Upload Update Intrusion
	Edit Rule 1:1000000:3 Message custom_http_sig Classification Action alert Protocol tcp Direction Bidirectional Source IPs any Destination IPs any Detection Options flow Established To Client Case Insensitive NTP Raw URI HTTP Status Code HTTP Status Message HTTP Status Code Distance Within Offset Depth Use Fast Pattern Matcher Only Fast Pattern Matcher Offset and Length	(Rule Comment)	
Informations requises pour la règ	e Add Option	Save As New	

Étape 3. Importer des règles de sniffage locales personnalisées de Snort 2 vers Snort 3

Accédez à Objets > Règles d'intrusion > Snort 3 Toutes les règles > Toutes les règles sur FMC, cliquez sur Convertir les règles Snort 2 et Importer à partir de la liste déroulante Tâches.

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	Overv	iew	Analysis	Policies	Devices	Objects	Integration		C	eploy	Q	6 ° ¢	F @	ədmin \backsim	cisco SECURE
Snort 2 All Rules Snort 3 All Rules															
< Intrusion Policy															Back To Top
All Rules		All F	Rules												
 Local Rules (1 group) 	Local Rules (1 group)														
All Snort 2 Converted Global	0	Rule	e Actions V Search by CVE, SID, Reference Info, or Rule Message							Tasks 🔻					
		50,09	50,094 rules Upload Snort 3 rules												
> MITRE (1 group)	0		GID:SID	Info				Rule Action	Assigned	Groups			Convert	Snort 2 rules	and import
> Rule Categories (9 groups)	0	•	148:2	(cip) CIP data is non-o	conforming to	o ODVA standard	Ø Disable (Default)	Builtins			N	onvert	Snort 2 rules	and download
												A	dd Rul	e Groups	
		•	133:3 🖸	(dc	e_smb) SMB - bad	SMB messa	age type	🖉 Disable (Default) 🗸	Builtins			Non	e		¶a ≆

Vérifiez le message d'avertissement et cliquez sur OK.

Convert Snort 2 rule:	and import	3

The Snort 2 local rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. This action will convert all Snort 2 local rules to Snort 3 rules. All the enabled rules per the Snort 2 version of the policy will be added into different groups and enabled in the corresponding Snort 3 version of the policy.



Message d'avertissement

Accédez à Objets > Règles d'intrusion > Snort 3 All Rules sur FMC, cliquez sur All Snort 2 Converted Global pour confirmer la règle de snort locale personnalisée importée.

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	Overvier	w Analysis	Policies	Devices	Objects	Integration		Deploy	९ 🌀	° 0	admin \vee	cisco SECURE
Snort 2 All Rules Snort 3 All Rules												
< Intrusion Policy												Back To Top
All Rules		Local Rules / A	All Snort 2	Converted (Global							
 Local Rules (1 group) 	0	Description G	roup created	for custom rule	es enabled in s	nort 2 version						
All Snort 2 Converted Global	/ 70	Rule Actions	~	Y Search b	by CVE, SID, Re	ference Info, or Rule Me	ssage					Tasks 🔻
> MITRE (1 group)	0											
> Rule Categories (9 groups)	0					The custom r	ules were successfully importer	d ×				
		GID:SID	Inf	fo		Rule	e Action	Assigned Group	5	Alert Conf	guration	
		> 🗌 2000:10	100000 cu	istom_http_sig		0	Disable (Default)	All Snort 2 Com	verted Glo.	None		/1

Confirmer la règle personnalisée importée

Étape 4. Action Modifier la règle

Cliquez sur Per Intrusion Policy selon l'action de règle de la règle personnalisée cible.

Ę	Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	Overvi	ew Analysis Policies	Devices Of	bjects Integration			Deploy Q 🚱	🗘 🕜 admin	 aliadia SECURE
Sno	rt 2 All Rules Snort 3 All Rules									
< Intr	usion Policy									Back To Top
	All Rules		Local Rules / All Snort 2 C	Converted Globa	al					
~	Local Rules (1 group)	0	Description Group created f	or custom rules ena	abled in snort 2 version					
	All Coart O Converted Clabal	120	Rule Actions 🗸 🗸	Y Search by CVE	, SID, Reference Info, or Rule	Message				Tasks 🔻
	All Short 2 Converted Global	<u> </u>	1 rule							
>	MITRE (1 group)	0			O The sure	an adap ware supposed it	in mented V			
>	Rule Categories (9 groups)	0			O The cust	m rules were successful	iy imported X			
			GID:SID Infe			Rule Action		Assigned Groups	Alert Configuration	
			> 2000:1000000 cus	tom_http_sig		🖉 Disable (Default) 🗸	(Overridden)	All Snort 2 Converted Glo	None	/1
						Block				
						Alert				
						A Rewrite				
						© Drop				
						Reject				
						Oisable (Default)				
						Cevert to default				
						Per Intrusion Policy				

Action Modifier la règle

Dans l'écran Modifier l'action de règle, entrez les informations relatives à la stratégie et à l'action de règle.

- Stratégie : snort_test
- Action de la règle : BLOCK



Remarque : les actions de règle sont les suivantes :

Block : génère un événement, bloque le paquet correspondant actuel et tous les paquets suivants de cette connexion.

Alerte : génère uniquement des événements pour le paquet correspondant et ne supprime pas le paquet ou la connexion.

Rewrite : génère un événement et écrase le contenu du paquet en fonction de l'option replace de la règle.

Pass : aucun événement n'est généré, permet au paquet de passer sans autre évaluation par les règles Snort suivantes.

Drop : génère un événement, abandonne le paquet correspondant et ne bloque pas le trafic supplémentaire dans cette connexion.

Reject : génère un événement, abandonne le paquet correspondant, bloque le trafic supplémentaire dans cette connexion et envoie la réinitialisation TCP s'il s'agit d'un

protocole TCP aux hôtes source et de destination.

Disable : ne fait pas correspondre le trafic avec cette règle. Aucun événement n'est généré.

Par défaut : rétablit l'action par défaut du système.

Edit Rule Action	0
2000:100 custom_http_sig	Í
All Policies Per Intrusion Policy	- 1
Policy snort_test	
Comments (optional) Provide a reason to change if applicable	- 1
Cancel Sa	ve

Action Modifier la règle

Étape 5. Confirmer la règle de sniffage local personnalisée importée

Accédez à Policies > Intrusion Policies sur FMC, cliquez sur Snort 3 Version correspondant à la stratégie d'intrusion cible dans la ligne.

Firewall Management Center Policies / Access Control / Intrusion / Int	er Overview a	Analysis Policies	Devices	Objects	Integration	Deploy	۹ (¢ 🎙	admin v	cisco SECURE	
Intrusion Policies Network Analysis Polici	ies										
Hide Snort 3 Sync status 🜒 🔍 Search by Intrusion Policy, Description, or Base Policy Create Policy Create Policy Create Policy Create Policy											
Intrusion Policy De	escription	Base Policy		Usage In	formation						
snort_test → Snort 3 is in sync with Snort 2, 2024-01-12		Balanced Security an	d Connectivity	1 Access No Zero 7 1 Device		Snort 2	Version	Snort 3 Versio	on 🖊 🖥 🕑 🗑		

Confirmer la règle personnalisée importée

Cliquez sur Local Rules > All Snort 2 Converted Global pour vérifier les détails de la règle de snort local personnalisée.

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Policie	Overview Analysis	Policies Devices	Objects Integration	Deploy	Q 🗳 🌣 🙆 admin	o ∽ secure
<pre></pre>	revention v	v	Use	ed by: 1 Access Control F	Policy No Zero Trust Applicati Active Rules 9811	Alert 478 Block 9333
Base Policy \rightarrow Group Overrides \rightarrow	Recommendations Not in us	se → Rule Ove	errides Summ	ary		
Rule Overrides						Back To Top
103 items All X V	Local Rules / All Snort 2 Co Description Group created for	onverted Global r custom rules enabled in sn	ort 2 version			Include
All Rules	Rule Action	Y Search by CVE, SID, R	teference Info, or Rule Messa	ge		
Overriden Rules	1 rule	Presets: Alert (0) Blo	ck (1) Disabled (0) Ove	erridden (1) Advanced Fi	Iters	
> MITRE (1 group)	GID:SID Rule Details	Ru	le Action 0	Set By	Assigned Groups	
✓ Local Rules (1 group)	2000:10 custom_http	p_sig	Block 🗸 🗸	Rule Override	All Snort 2 Conve	rte 🖊 🗭
All Snort 2 Converted Global	ale	ert tcp any any <> any any (s sg:"custom_http_sig"; classt	sid:1000000; gid:2000; flow: ype:unknown; rev:3;)	established,to_client; raw	_data; content:"username";	
Rule Categories (9 groups)						



Étape 6. Associer une politique d'intrusion à une règle de politique de contrôle d'accès (ACP)

Accédez à Politiques>Contrôle d'accès sur FMC, associez la politique d'intrusion à ACP.

Editing Rule ftd_acp					Mandatory 🛛 🗙
Name ftd_acp 1 Action	n 🕒 Allow	Logging ON	🌇 Time Ran	ge None 🗸 🗸	Rule Enabled 🔵
• Int	trusion Policy	v snort_test X ∨ Defaul	t-Set X	File Policy None	¥
Q Zones (2) Networks Ports Applications 🛕 Users	URLs	Dynamic Attributes VLAN	lags		
Q Search Security Zone Objects Showing 2 out of 2		Selected Sources: 1		Selected Destinations and App	lications: 1
<u>hiside_zone</u> (Routed Security Zone)		Collapse All	Remove All	Collapse All	Remove All
discrete (Routed Security Zone)		ZONE V 1 Object		ZONE v 1 Object	

Associer à la règle ACP

Étape 7. Déployer les modifications

Déployez les modifications sur FTD.

Firewall Management Center Overview Analysis Policies Devices Objects Integration		Deploy Q 🥝 🔅 🕜 admin 🗸 deficience	SECURE
→ Return to Access Control Policy Management. In acp-rule ✓	٩	Advanced Deploy 🔺 🗋 Ignore warnings Deploy All	Legacy UI Sovo
Packets → O Prefilter Rules → Decryption → O Security Intelligence → Identity → O Access Control O More	FPR2120_FTD	Ready for Deployment	1 device

Déployer les modifications

Méthode 2. Télécharger un fichier local

- Étape 1. Confirmer la version de Snort
- Identique à l'étape 1 de la méthode 1.
- Étape 2. Créer une règle de détection locale personnalisée

Créez manuellement une règle d'analyse locale personnalisée et enregistrez-la dans un fichier local nommé custom-rules.txt.

alert tcp any any <> any any (sid:1000000; flow:established,to_client; raw_data; content:"username"; m

Étape 3. Télécharger la règle de détection locale personnalisée

Accédez à Objets > Règles d'intrusion > Snort 3 All Rules > All Rules sur FMC, cliquez sur Upload Snort 3 rules from Tasks pulldown list.

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	Overv	iew	Analysis	Policies	Devices	Objects	Integration			Deploy	Q	6	0 ¢	admin \checkmark	cisco SECUI	RE
Snort 2 All Rules Snort 3 All Rules																
< Intrusion Policy															Back To	Гор
All Rules		All F	Rules													
 Local Rules (1 group) 	0	All rul	les assigned to	o current intr	usion policy im	espective of n	ule group									
All Snort 2 Converted Global	0	Rule	Actions	~	Y Search b	y CVE, SID, Re	eference Info, or Rul	le Message					Iloload	Soort 2 pulse	Tasks 🔻	ļ
 MITRE (1 group) 	0	0	GID:SID	Info	0			Rule Action	Assig	med Groups		A	Convert	Snort 2 rules a	nd import	1
 ATT&CK Framework (1 group) 	0	> (148:2 📫	(ci	p) CIP data is no	n-conforming t	to ODVA standard	O Disable (Default)	Builti	ns		N	Convert Add Ruí	Snort 2 rules a	nd download	*
> Enterprise (13 groups)	0	•	133:3 🖸	(dc	e_smb) SMB -	bad SMB mess	age type	🖉 Disable (Default) 🔍	Built	ns		No	ne		¶3 ₩	

Télécharger une règle personnalisée

Dans l'écran Ajouter des règles personnalisées, faites glisser le fichier custom-rules.txt local, sélectionnez Groupes de règles et l'action appropriée (Fusionner les règles dans cet exemple), puis cliquez sur le bouton Suivant.

Add Custom Rules	Add Custom Rules	0
T	File Name	
Drag and drop a file here or click to browse .rules and .txt files are supported	Associate Rules to Rule Groups 1	Selected
Cancel O	Q. Search All Snort 2 Converted Global	
	Create New Custom Rule Group	
	Choose the appropriate action. Merge Rules	
	Merges any extra rules with the existing rules in the rule group. Replace all rules in the group with file contents Replaces the rules which are already present in a custom intrusion rule group new rules	p with the
	Cancel	Next

Vérifiez que le fichier de règle locale a bien été téléchargé.

Add Custom Rules		0
Summary		
2000:1000000		
Download the summary file.		
	Back	Finish

Confirmer le résultat du téléchargement

Accédez à Objects > Intrusion Rules > Snort 3 All Rules sur FMC, cliquez sur All Snort 2 Converted Global pour confirmer la règle de détection locale personnalisée téléchargée.

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	view Analysis Policie:	s Devices Objects Integration		Deploy Q 💕	🔅 🞯 🛛 admin 🗸	cisco SECURE
Snort 2 All Rules Snort 3 All Rules						
< Intrusion Policy						Back To Top
All Rules	Local Rules / All Snort	2 Converted Global				
 Local Rules (1 group) 	Description Group creat	ed for custom rules enabled in snort 2 version				
All Snort 2 Converted Global	Rule Actions V	 Search by CVE, SID, Reference Info, or Rule 	ile Message			Tasks 🔻
 MITRE (1 group) 	GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration	
 ATT&CK Framework (1 group) 	✓ □ 2000:1000000	custom_http_sig	🖉 Disable (Default) 🗸	All Snort 2 Converted Glo	None	11
> Enterprise (13 groups)		alert tcp any any <> any any (sid:1000000; gid	2000; flow:established,to_client; raw_dat	a; content:"username"; msg	g:"custom_http_sig";	
> Rule Categories (9 groups)		classtype:unknown; rev:3;)				

Détail de la règle personnalisée

Étape 4. Action Modifier la règle

Identique à l'étape 4 de la méthode 1.

Étape 5. Confirmer la règle de détection locale personnalisée téléchargée

Identique à l'étape 5 de la méthode 1.

Étape 6. Associer une politique d'intrusion à une règle de politique de contrôle d'accès (ACP)

Identique à l'étape 6 de la méthode 1.

Étape 7. Déployer les modifications

Identique à l'étape 7 de la méthode 1.

Vérifier

Étape 1. Définition du contenu du fichier dans le serveur HTTP

Définissez le contenu du fichier test.txt côté serveur HTTP sur username.

Étape 2. Requête HTTP initiale

Accédez au serveur HTTP (192.168.20.1/test.txt) à partir du navigateur du client (192.168.10.1) et vérifiez que la communication HTTP est bloquée.

) 192.168.20.1	× +		<u> </u>	٥	×
\leftrightarrow \rightarrow X (i) 192.16	58.20.1/test.txt		☆	θ	:
	E				

Requête HTTP initiale

Étape 3. Confirmer l'incident

Accédez àAnalyse>Intrusions>ÉvénementsDans FMC, vérifiez que l'événement d'intrusion est généré par la règle de détection locale personnalisée.

Firewall Managemen Analysis / Intrusions / Events	t Center	Overview Ana	lysis Policies	Devices	Objects Ir	ntegration				Dep	oloy Q 🥑	🗘 🕜 adm	in v diala SEC	CURE
							Bookmark This	Page Reportin	g Dashbo	ard View	Bookmarks Se	earch Predefine	d Searches	٣
Events By Priority and	Classificatio	n (switch workflow)									II 202	24-04-06 13:26:03	- 2024-04-06_14:	31:12
No Search Constraints (Edit Search)													Expa	inding
Drilldown of Event, Priority, and Cla	assification Table	View of Events	Packets											
Jump to														
□ ↓ Time X Pr	iority X Impact X	Inline Result × Reas	on X Source IP X	Source x	Destination IP X	Destination x Country	Source Port / ICMP X Type	Destination Port / ICMP X Code	SSL Status X	VLAN x	Message X		Classification X	General
▼ 2024-04-06 14:30:48 lo	w 🔘 Unknow	Block	192.168.20	0.1	192.168.10.1		80 (http) / tcp	50103 / tcp			custom_http_s	sig (2000:1000000:3)	Unknown Traffic	Standa

Événement D'Intrusion

Cliquez sur l'onglet Paquets, confirmez les détails de l'événement Intrusion.

Firewall Manage Analysis / Intrusions / E	ent Center Overview Analysis Policies Devices Objects Integration Deploy Q 📀 🌣 🕢 admin v 🖏 SECURE
	Bookmark: This Page Reporting Dashboard View Bookmarks Search Predefined Searches •
Events By Priority	1d Classification (sunta) 12 2024-04-06 13:26:03 - 2024-04-06 14:32:46 Expanding
No Search Constraints (Edit S	ct)
Drilldown of Event, Priority, a	Classification Table View of Events Packets
Event Information Message Time Classification Priority	ustom_http_sig (2000:1000000:3) 028-04-05 14:31:26 hknown Traffic ov
Ingress Security Zone	utside_zone
Egress Security Zone	uside_zone
Device	PR2120_FTD
Ingress Interface	diside
Egress Interface Source ID	awe 02168201
Source Port / ICMP Type	Su House A
Destination IP	92.168.10.1
Destination Port / ICMP Code	0105 / tcp
HTTP Hostname	92.168.20.1
HTTP URI	lest.bt
Intrusion Policy	nort_test
Access Control Policy	cp-rule
Access Control Rule	
Rule	lert tçp any any ⇔ any any i sidsiUUUUUU; gidsi2UUUI flowiestablished.lo_client; raw_data; content; username ; mag; custom_http_sig; classiypeiunknorm; rev:3;)
 Actions 	

Détail de l'incident

Foire aux questions (FAQ)

Q : Lequel est recommandé ? Snort 2 ou Snort 3 ?

R : Par rapport à Snort 2, Snort 3 offre des vitesses de traitement améliorées et de nouvelles fonctionnalités, ce qui en fait l'option la plus recommandée.

Q : Après la mise à niveau d'une version de FTD antérieure à 7.0 vers une version 7.0 ou ultérieure, la version de Snort est-elle automatiquement mise à jour vers Snort 3 ? R : Non, le moteur d'inspection reste sur Snort 2. Pour utiliser Snort 3 après la mise à niveau, vous devez l'activer explicitement. Notez que Snort 2 est prévu pour être déconseillé dans une prochaine version et il est fortement recommandé d'arrêter de l'utiliser maintenant.

Q : Dans Snort 3, est-il possible de modifier une règle personnalisée existante ?

R : Non, vous ne pouvez pas le modifier. Pour modifier une règle personnalisée spécifique, vous devez la supprimer et la recréer.

Dépannage

Exécutez system support trace la commande pour confirmer le comportement sur FTD. Dans cet exemple, le trafic HTTP est bloqué par la règle IPS (2000:1000000:3).

<#root>

>

system support trace

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
```

Please specify a client port: Please specify a server IP address: 192.168.20.1 Please specify a server port: 192.168.10.1 50104 -> 192.168.20.1 80 6 AS=0 ID=4 GR=1-1 Firewall: allow rule, ' ftd_acp ', allow 192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Event : 2000:1000000:3 , Action block 192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist 192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist 192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist 192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist 192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist 192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist 192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist

Référence

Guide de configuration de Cisco Secure Firewall Management Center Snort 3

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.