FTDでSnort3のカスタムローカルSnortルールを 設定する

内容
<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>ネットワーク図</u>
<u>コンフィギュレーション</u>
<u>方式 1.Snort 2からSnort 3へのインポート</u>
<u>ステップ1:Snortバージョンの確認</u>
<u>ステップ2:Snort 2でのカスタムローカルSnortルールの作成または編集</u>
<u>ステップ 3:Snort 2からSnort 3へのカスタムローカルSnortルールのインポート</u>
<u>ステップ4:ルールの変更アクション</u>
<u>ステップ5:インポートされたカスタムローカルSnortルールの確認</u>
<u> 手順 6:侵入ポリシーとアクセスコントロールポリシー(ACP)ルールの関連付け</u>
<u>手順7: 変更の展開</u>
<u>方式 2.ローカルファイルのアップロード</u>
<u>ステップ1:Snortバージョンの確認</u>
<u>ステップ2:カスタムローカルSnortルールの作成</u>
<u>ステップ3:カスタムローカルSnortルールのアップロード</u>
<u>ステップ4:ルールの変更アクション</u>
<u>ステップ5:アップロードされたカスタムローカルSnortルールの確認</u>
<u> 手順 6:侵入ポリシーとアクセスコントロールポリシー(ACP)ルールの関連付け</u>
<u>手順7: 変更の展開</u>
<u>確認</u>
<u>ステップ1:HTTPサーバでのファイルの内容の設定</u>
<u>ステップ2:初期HTTP要求</u>
<u>ステップ3:侵入イベントの確認</u>
<u>よく寄せられる質問(FAQ)</u>
トラブルシュート

<u>参考</u>

はじめに

このドキュメントでは、ファイアウォール脅威対策(FTD)のSnort3でカスタムローカルSnortルー ルを設定する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Firepower Management Center (FMC)
- 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 7.4.1向けCisco Firepower Management Center
- Cisco Firepower 2120 7.4.1

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

Management Centerを使用した脅威対策におけるSnort 3のサポートは、バージョン7.0以降で開始されます。バージョン7.0以降の新規および再イメージ化デバイスでは、Snort 3がデフォルトのインスペクションエンジンです。

このドキュメントでは、Snort 3用にSnortルールをカスタマイズする方法の例と、実際の検証例 を紹介します。具体的には、特定の文字列(ユーザ名)を含むHTTPパケットをドロップするよ うにカスタマイズされたSnortルールを使用して侵入ポリシーを設定および確認する方法を紹介し ます。



注意:カスタムのローカルSnortルールを作成してサポートを提供することは、TACのサポート対象外です。したがって、このドキュメントは参考資料としてのみ使用でき、これらのカスタムルールは独自の裁量と責任で作成および管理してください。

ネットワーク図

このドキュメントでは、次の図に示すSnort3のカスタムローカルSnortルールの設定および検証に ついて説明します。



ネットワーク図

コンフィギュレーション

これは、特定の文字列(ユーザ名)を含むHTTP応答パケットを検出してドロップするカスタム ローカルSnortルールの設定です。



注:現時点では、FMC GUIのSnort 3 All RulesページからカスタムローカルSnortルール を追加することはできません。このドキュメントで紹介する方法を使用する必要があり ます。

方式 1.Snort 2からSnort 3へのインポート

ステップ1:Snortバージョンの確認

FMCでDevices>Device Managementの順に移動し、Devicetabをクリックします。SnortのバージョンがSnort3であることを確認します。

Firewall Management Center Overview	Analysis Policies De	vices Obje	ects Integration		Deploy Q 💕 🌣	admin v doubo	SECURE
View By: Group						Migrate Deployment H	History
All (1) • Error (0) • Warning (0) • Offline (0) • M	lormal (1) • Deployment Per	nding (0)	Upgrade (0) Snort 3 (1)		C	λ Search Device	Add 🔻
Collapse All						Download Device L	List Report
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (1)							
FPR2120_FTI Snort 3 1.100.0.29 - teored	Firepower 2120 with FTD	7.4.1	N/A	Essentials, IPS (1 more)	acp-rule	49	1

Snortバージョン

ステップ2: Snort 2でのカスタムローカルSnortルールの作成または編集

FMCで、Objects > Intrusion Rules > Snort 2 All Rulesの順に移動します。Create Ruleボタンをク リックしてカスタムローカルSnortルールを追加するか、FMCでObjects > Intrusion Rules > Snort 2 All Rules > Local Rulesの順に選択し、Editボタンをクリックして既存のカスタムローカル Snortルールを編集します。

Snort 2でカスタムローカルSnortルールを作成する方法については、「<u>FTDでSnort2でカスタムロ</u> <u>ーカルSnortルールを設定する</u>」を参照してください。

図に示すように、新しいカスタムローカルSnortルールを追加します。

Firewall Management Center Objects / Intrusion Rules / Snort 2 All Rules	Overview Analysi	Policies	Devices	Objects	Integration	Deploy	Q 📀	¢ 0	admin \lor	cisco SECURE
Snort 2 All Rules Snort 3 All Rules				Object	Management					
< Intrusion Policy				Intrusion	Rules	Search Dele	te Local R	ules	Import Rules	Create Rule

新しいカスタムルールの追加

図に示すように、既存のカスタムローカルSnortルールを編集します。この例では、既存のカスタ ム規則を編集します。

Cipects / Intrus	anagement Ce sion Rules / Snort 2 A	enter Overview Analysis NI Rules	Policies	Devices O	bjects	Integration	Deploy	Q 📀	0	admin 🗸	cisco SECURE
Snort 2 All Rules	Snort 3 All Rules										
< Intrusion Policy							Search Delete	Local Rule	s Imp	ort Rules	Create Rule
Group Rules By		▼ Category (62656)									
Category		▶ app-detect (162)									
		 browser-chrome (234) browser-fragor (107) 									
Q, Filter		 browser-le (2722) 									
		► browser-other (146)									
		 browser-plugins (2552) 									
		 browser-webkit (170) 									
		▶ content-replace (26)									
		 decoder (153) 									
		 deleted (12305) 									
		 exploit-kit (763) 									
		 file-executable (397) 									
		Internation (2225)									
		 file-image (1042) 									
		 file-lava (230) 									
		 file-multimedia (530) 									
		► file-office (1821)									
		► file-other (2603)									
		 file-pdf (1730) 									
		 Indicator-compromise (612) 									
		 Indicator-obfuscation (247) 									
		 indicator-scan (42) 									
		 indicator-shellcode (354) 									
		• Local Rules (1)									
		(1:1000001) custom_http_sig									
		mahware-backboor (871)									

既存のカスタム規則の編集

特定の文字列(ユーザ名)を含むHTTPパケットを検出するためのシグニチャ情報を入力します

- ・メッセージ:custom_http_sig
- アクション:アラート
- ・プロトコル:tcp

o

- フロー:確立、クライアントへ
- コンテンツ:ユーザ名(未加エデータ)

Chiects / Intrusion Rules / Create	erview Analysis Policies Devices Objects Integral	tion	Deploy Q 🚱 🌣 🍘 admin 🗸 🖞
			Search Upload Update Intrusion
Snort 2 All Rules Snort 3 All Rules			
	Edit Rule 1:1000000:3	(Rule Comment)	
	Message custom_http_sig		
	Oleccitestics Unknown Traffic	*	
	Edit Classifications		
	Action alert 👻		
	Protocol tep 👻		
	Direction Bidirectional 🔻		
	Source IPs any Source Po	d any	
	Destination IPs any Destination Po	any any	
	Detection Options		
	flow	×	
	Established 🔻 To Client	*	
	content	×	
	username	0	
	Case Insensitive		
	Raw Data		
	HTTP Header		
	HTTP Cookie		
	HTTP Raw URI		
	HTTP Raw Cookie		
	HTTP Method		
	HTTP Client Body		
	HTTP Status Code		
	Distance		
	Within		
	Offset		
	Denth		
	Use Fast Pattern Matcher		
	Fast Pattern Matcher Only		
	Fast Pattern Matcher Offset and Length		
	ack Add Ontion	Save Save As New	

ルールに必要な情報の入力

ステップ 3: Snort 2からSnort 3へのカスタムローカルSnortルールのインポート

FMCでObjects > Intrusion Rules > Snort 3 All Rules > All Rulesの順に移動し、Convert Snort 2 rules and Import from Tasks プルダウンリストをクリックします。

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	Overvi	iew	Analysis	Policies	Devices	Objects	Integration			Deploy	Q	6 9 K	ł 0	admin \sim	cisco SECURE
Snort 2 All Rules Snort 3 All Rules															
< Intrusion Policy															Back To Top
All Rules		All R	ules												
 Local Rules (1 group) 	0	All rule	s assigned to	current intru	usion policy irresp	pective of ru	le group								
All Snort 2 Converted Global	0	Rule A	Actions	\sim	Y Search by C	CVE, SID, Ref	ference Info, or Rul	e Message							Tasks 🔻
	-	50,094	rules										lpload	Snort 3 rules	
> MITRE (1 group)			GID:SID	Info				Rule Action	Assigne	d Groups		A 9			and import
> Rule Categories (9 groups)	0	•	148:2 📑	(cip) CIP data is non-	conforming to	o ODVA standard	O Disable (Default)	Builtins			N ,	onvert	Snort 2 rules e Groups	and download
		•	133:3 📑	(do	e_smb) SMB - ba	d SMB messa	ige type	🖉 Disable (Default) 🗸	Builtins			Non	e		¶a ≆

警告メッセージをチェックして、OKをクリックします。

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.

Ø



警告メッセージ

FMCでObjects > Intrusion Rules > Snort 3 All Rulesの順に移動し、All Snort 2 Converted Global をクリックして、インポートされたカスタムローカルSnortルールを確認します。

Chief Context	view Analysis Policies Devices Objects Int	egration	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 created for custom rules enabled in snort 2	2 version		
All Snort 2 Converted Global	Rule Actions V Y Search by CVE, SID, Referen	ice Info, or Rule Message		Tasks 💌
> MITRE (1 group)	ſ		Π	
> Rule Categories (9 groups)	l	The custom rules were successfully imported X		
	GID:SID Info	Rule Action	Assigned Groups Alert Configuration	
	> 2000:1000000 custom_http_sig	🖉 Disable (Default) 🗸	All Snort 2 Converted Glo None	/1

インポートされたカスタム規則の確認

ステップ4:ルールの変更アクション

ターゲットカスタムルールのルールアクションに従って、Per Intrusion Policyをクリックします 。

Ę	3	Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	Overvi	iew Analysis Policies	Devices	Objects Inte	gration			Deploy Q	6	° 0	admin \sim	cisco SECURE
s	nort	t 2 All Rules Snort 3 All Rules												
< Ir	ntrus	sion Policy												Back To Top
		All Rules		Local Rules / All Snort 2 (Converted G	lobal								
	~	Local Rules (1 group)	0	Description Group created	or custom rule:	s enabled in snort 2	version							
		All Snort 2 Converted Global	170	Rule Actions 🗸 🗸	Y Search by	CVE, SID, Reference	e Info, or Rule	Message						Tasks 🔻
				1 rule										
-	>	MILKE (1 group)					The custo	m rules were successfull	y imported \times					
1	>	Rule Categories (9 groups)	0											
				GID:SID Inf	0			Rule Action		Assigned Groups	1	Alert Conf	guration	
				> _ 2000:1000000 cu	tom_http_sig			⊘ Disable (Default) ∨	(Overridden)	All Snort 2 Converted	Glo I	None		/1
								Block						
								Alert						
								₽ Drop						
								😫 Pass						
								C Reject						
								 Disable (Default) Bevert to default 						
							I	Per Intrusion Policy	1					

ルールの変更アクション

Edit Rule Action画面で、PolicyとRule Actionに関する情報を入力します。

- ・ポリシー:snort_test
- ・ ルールアクション:BLOCK



注:ルールの処理は次のとおりです。

Block:イベントを生成し、現在の一致するパケットとこの接続の後続のすべてのパケットをブロックします。

Alert:一致するパケットのイベントのみを生成し、パケットや接続をドロップしません。

Rewrite:ルールのreplaceオプションに基づいて、イベントを生成し、パケットの内容を 上書きします。

通過:イベントは生成されず、後続のSnortルールによる評価を受けずにパケットの通過 が許可されます。

ドロップ:イベントを生成し、一致するパケットをドロップします。この接続ではこれ 以上トラフィックをブロックしません。

Reject:イベントを生成し、一致するパケットをドロップします。この接続で今後のトラフィックをブロックし、それがTCPプロトコルである場合はTCP resetを送信元ホストと

宛先ホストに送信します。

Disable:このルールに対してトラフィックを照合しません。イベントは生成されません。

デフォルト-システムのデフォルトのアクションに戻します。

Edit Rule Action	0	
2000:100 custom_http_sig		*
All Policies Per Intrusion Policy		
Policy snort_test Add Another Rule Action BLOCK		
Comments (optional)		_
Provide a reason to change if applicable		
Cancel Sar	ve)	
ルールアクションの編集		

ステップ 5:インポートされたカスタムローカルSnortルールの確認

FMCでPolicies > Intrusion Policiesの順に移動し、行のターゲット侵入ポリシーに対応するSnort 3 Versionをクリックします。

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Policies	licies Overview An	alysis Policies	Devices	Objects Integration	on Dep	ploy Q	6 0	admin ~	cisco SECURE
Intrusion Policies Network Analysis Policies									
Hide Snort 3 Sync status 🌒 🔍 Search by Intrusic	n Policy, Description, or Base Po		All IPS Rules IPS	S Mapping 🕕	Comp	are Policies	Create Policy		
Intrusion Policy Description		Base Policy		Usage Information					
snort_test → Snort 3 is in sync with Snort 2. 2024-01-12		Balanced Security and	I Connectivity	1 Access Control Po No Zero Trust Applic 1 Device	licy ation Policy	Snort 2	Version	Snort 3 Versi	on 🖊 🖥 🕑 🗑

インポートされたカスタム規則の確認

Local Rules > All Snort 2 Converted Globalの順にクリックして、カスタムローカルSnortルールの 詳細を確認します。

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Policie	Overview Analys	sis Policies D	evices Objects	Integration	Deploy	९ 🗳 🕯	🗘 🕜 admin	cisco SECURE
A Policies / Intrusion / snort_test Base Balanced Security and Policy: Connectivity Mode: Pre	evention 🗸	Y		Used by:	1 Access Control	Policy No Z	ero Trust Application	n Policy 1 Device Alert 478 Block 9333
Base Policy \rightarrow Group Overrides \rightarrow	Recommendations Not	in use →	Rule Overrides	Summary				
Rule Overrides @								Back To Top
103 items All X V	Local Rules / All Snort : Description Group create	2 Converted Globa d for custom rules enat	 bled in snort 2 version					Include
All Rules	Rule Action	V Search by C	VE, SID, Reference Info	, or Rule Message				
Overriden Rules	1 rule	Presets: Alert (0) Block (1) Disa	abled (0) Overridder	n (1) Advanced F	ilters		
> MITRE (1 group)	GID:SID Rule De	itails	Rule Action	Set	Ву		Assigned Groups	
 Local Rules (1 group) 	2000:10 custon	n_http_sig	Block	√ «> Rule	e Override		All Snort 2 Converte	
All Snort 2 Converted Global		alert tcp any any <> a msg:"custom_http_si	ny any (sid:1000000; g*; classtype:unknown	gid:2000; flow:establ ; rev:3;)	ished,to_client; raw	v_data; conten	nt:"username";	

インポートされたカスタム規則の確認

手順6:侵入ポリシーとアクセスコントロールポリシー(ACP)ルールの関連付け

FMCでPolicies>Access Controlの順に移動し、侵入ポリシーをACPに関連付けます。

1 Citing Rule ftd_acp					Mandatory 🛛 🗙
Name [ftd_acp 1 Action	n 🖸 Allow	Logging ON	Time Rang	ge None V	Rule Enabled
• Int	trusion Policy	y snort_test X V	Set X	V File Policy None	¥
Q Zones (2) Networks Ports Applications 🛕 Users	URLs	Dynamic Attributes VLAN Ta	igs		
Q Search Security Zone Objects Showing 2 out of 2		Selected Sources: 1		Selected Destinations and Ap	plications: 1
inside_zone (Routed Security Zone)		Collapse All	Remove All	Collapse All	Remove All
dutside_zone (Routed Security Zone)		ZONE V 1 Object		ZONE V 1 Object	•

ACPルールとの関連付け

手順7:変更の展開

変更をFTDに展開します。

Firewall Management Center Policies / Access Control / Policy Editor Overvie	ew Analysis	Policies	Devices	Objects	Integration	_		Deploy	० 💿 ३	0	$\text{admin} \sim $	cisco S	SECURE
↔ Return to Access Control Policy Management							۹	Advanced Deploy	🔺 🗌 Ignore	warning	B Deploy A	JI	Legacy UI Savo
Packets O Prefilter Rules O Decryption O Security Intelligence O Identity O Access Control O More							FPR2120_FTD		Rea	by for Dep	ployment		1 device

変更の展開

方式 2.ローカルファイルのアップロード

ステップ1:Snortバージョンの確認

方法1のステップ1と同じです。

ステップ2:カスタムローカルSnortルールの作成

カスタムローカルSnortルールを手動で作成し、custom-rules.txtという名前のローカルファイルに 保存します。

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

ステップ3:カスタムローカルSnortルールのアップロード

FMCでObjects > Intrusion Rules > Snort 3 All Rules > All Rulesの順に移動し、Tasks プルダウン リストからUpload Snort 3 rules をクリックします。

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	Iverview Analysis Policie	es Devices Objects Integration		Deploy Q 💰	admin 🗸 📲	SECURE
Snort 2 All Rules Snort 3 All Rules						
< Intrusion Policy						Back To Top
All Rules	All Rules					
 Local Rules (1 group) 	 All rules assigned to current 	t intrusion policy irrespective of rule group				
All Snort 2 Converted Global	Rule Actions	✓ Y Search by CVE, SID, Reference Info, or Refe	ule Message			Tasks 🔻
 MITRE (1 group) 	GID:SID	Info	Rule Action	Assigned Groups	Upload Snort 3 rules A Convert Snort 2 rules and	i import
 ATT&CK Framework (1 group) 	• 148:2 🗹	(cip) CIP data is non-conforming to ODVA standard	O Disable (Default)	Builtins	Convert Snort 2 rules and N Add Rule Groups	d download
> Enterprise (13 groups)	• 133:3 🗹	(dce_smb) SMB - bad SMB message type	🖉 Disable (Default) 🗸	Builtins	None	¶₂ ≆

カスタムルールのアップロード

Add Custom Rules画面で、ローカルのcustom-rules.txtファイルをドラッグアンドドロップし、 Rule Groups(この例ではMerge Rules)と適切なアクション(この例ではMerge Rules)を選択 して、Nextボタンをクリックします。

Add Custom Rules	0	Add Custom Rules
	×	File Name custom-rules.txt Replace File Associate Rules to Rule Groups 1 Selected Search Image: Search Image: All Snort 2 Converted Global Image: Search Image: Create New Custom Rule Group Image: Search Image: Create New Custom Rule Group Image: Search Image: Merge Rules Image: Search Image: Merge Rules Image: Search Image: Search Image: Se
		Cancel Next

Add Custom Rules Summary 1 new rule 2000:1000000 Download the summary file. Back Finish

FMCでObjects > Intrusion Rules > Snort 3 All Rulesの順に移動し、All Snort 2 Converted Global をクリックして、アップロードされたカスタムローカルSnortルールを確認します。

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	rview Analysis Polici	es 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 Snor	t 2 Converted Global				
 Local Rules (1 group) 	Description Group crea	ted for custom rules enabled i	n snort 2 version			
All Snort 2 Converted Global	Rule Actions	 Search by CVE, SID, 	Reference Info, or Rule 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 ar	y (sid:1000000; gid:2000; flow:established.to_clien	t; raw_data; content:"username"; msg	:"custom_http_sig";	
> Rule Categories (9 groups)		classtype:unknown; rev:3;)			

カスタム規則の詳細

ステップ4:ルールの変更アクション

方法1のステップ4と同じです。

ステップ5:アップロードされたカスタムローカルSnortルールの確認

方法1のステップ5と同じです。

手順6:侵入ポリシーとアクセスコントロールポリシー(ACP)ルールの関連付け

方法1のステップ6と同じです。

アップロード結果の確認

手順7:変更の展開

方法1のステップ7と同じです。

確認

ステップ1:HTTPサーバでのファイルの内容の設定

HTTPサーバ側のtest.txtファイルの内容をusernameに設定します。

ステップ2:初期HTTP要求

クライアント(192.168.10.1)のブラウザからHTTPサーバ(192.168.20.1/test.txt)にアクセスし、 HTTP通信がブロックされていることを確認します。

) 192.168.20.1	×	+	-	٥	2	×
\leftrightarrow \rightarrow \times	(i) 192.168.20.1/test	.txt	ž	•	•	:

囧

初期HTTP要求

ステップ3:侵入イベントの確認

Analysis>Intrusions>Eventson FMCに移動し、侵入イベントがカスタムローカルSnortルールによって生成されることを確認します。

Firewall Man Analysis / Intrusio	agement Cen Is / Events	ter _{Ove}	erview	Analysis	Policies	Devices	Objects	ntegration				Dep	oloy Q	0	E 🕜 adm	nin v duala SE	CURE
									Bookmark This	Page Reportin	g Dashbo	ard View	Bookmarks	Search	Predefine	d Searches	×
Events By Priority and Classification (auto-workford)																	
No Search Constraints (dit Search)															Expa	anding
Drilldown of Event, Price	rity, and Classificat	ion Table V	/iew of Ev	ents Pac	kets												
Jump to																	
□ ↓ Time X	Priority X	Impact X	Inline Result ×	Reason X	Source IP X	Source Country X	Destination IP X	Destination x Country	Source Port / ICMP X Type	Destination Port / ICMP X Code	SSL Status X	VLAN x	Message 3			Classification X	General
	4:30:48 low	O Unknown	Block		9 192.168.20	1	192.168.10.	1	80 (http) / tcp	50103 / tcp			custom_h	ttp_sig (20	000:1000000:3]) Unknown Traffic	Standa

侵入イベント

Packetstabをクリックし、侵入イベントの詳細を確認します。

Firewall Manage Analysis / Intrusions / E	nent Center Overview Analysis Policies Devices Objects Integration Deploy Q S 🌣 🕢 admin v 🖏 SEC	URE
	Bookmark: This Page Reporting Dashboard View Bookmarks Search Predefined Searches	•
Events By Priority	Ind Classification (auto: accident)	2:46
No Search Constraints (Edit S	arch)	ung
Drilldown of Event, Priority,	d Classification Table View of Events Packets	
Event Information Message Time Classification Priority	custom_http_sig (2000:1000000:3) 2024-04-05 14:31:26 Unknown Traffic Iow	
Egress Security Zone	Vuising zone	
Device	FPR2120_FTD	
Ingress Interface	outside	
Egress Interface	inside	
Source IP	192.168.20.1	
Source Port / ICMP Type	80 (http://tcp	
Destination IP	192168.10.1	
Destination Port / ICMP Code	50105 / tcp	
HTTP Hostname	192.168.20.1	
HTTP URI	7651 bd	
Access Control Policy	Short_rest	
Access Control Dule	auprise Bol ann	
Rule	alert tep any any ⊙ any any (sids1000000);gids2000;flowtestablished.to_client; raw_data: content:"username": msg:"custom_http_sig": classtymetunknomn: rev:8;)	
 Actions 		

侵入イベントの詳細

よく寄せられる質問(FAQ)

Q:Snort 2とSnort 3のどちらが推奨されますか。

A:Snort 2と比較して、Snort 3は処理速度の向上と新機能を備えているため、より推奨されるオプ ションです。

Q:7.0より前のバージョンのFTDから7.0以降のバージョンにアップグレードした後、Snortのバー ジョンは自動的にSnort 3に更新されますか。

A:いいえ。インスペクションエンジンはSnort 2上に残ります。アップグレード後にSnort 3を使用するには、明示的に有効にする必要があります。Snort 2は今後のリリースで廃止される予定であり、今すぐ使用しないことを強く推奨します。

Q:Snort 3では、既存のカスタムルールを編集できますか。

A:いいえ、編集できません。特定のカスタム規則を編集するには、関連する規則を削除して再 作成する必要があります。

トラブルシュート

system support traceコマンドを実行して、FTDの動作を確認します。この例では、HTTPトラフィックはIPSルール (2000:1000000:3)によってブロックされます。

<#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

参考

Cisco Secure Firewall Management Center Snort 3コンフィギュレーションガイド

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。