在FTD的Snort2中設定自訂本機Snort規則

```
目錄
簡介
必要條件
  <u>需求</u>
  <u>採用元件</u>
<u>背景資訊</u>
設定
  網路圖表
  組態
    步驟 1.確認Snort版本
    步驟 2.在Snort 2中建立自定義本地Snort規則
    步驟 3.確認自定義本地Snort規則
    步驟 4.變更規則動作
    步驟 5.將入侵策略與訪問控制策略(ACP)規則關聯
    步驟 6.部署變更
<u>驗證</u>
  <u>未觸發自定義本地Snort規則</u>
    步驟 1.設定HTTP伺服器中的檔案內容
    步驟 2.初始HTTP請求
  <u>已觸發自定義本地Snort規則</u>
    步驟 1.設定HTTP伺服器中的檔案內容
```

<u>步驟 2.初始HTTP請求</u> 步驟 3.確認入侵事件

<u>疑難排解</u>

簡介

本檔案介紹在防火牆威脅防禦(FTD)的Snort2中設定自訂本機Snort規則的程式。

必要條件

需求

思科建議您瞭解以下主題:

- Cisco Firepower管理中心(FMC)
- 防火牆威脅防禦(FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 適用於VMWare的Cisco Firepower管理中心7.4.1
- Cisco Firepower 2120 7.4.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

自訂本機Snort規則是指使用者定義規則,您可以在整合至FTD的Snort入侵偵測與防禦系統中建立 及實作。在Cisco FTD中建立自訂本機Snort規則時,基本上就是定義了Snort引擎可以注意的新模式 或條件集。如果網路流量符合自定義規則中指定的條件,Snort可以採取規則中定義的操作,例如生 成警報或丟棄資料包。管理員使用自定義本地Snort規則處理一般規則集未涵蓋的特定威脅。

本文檔介紹了如何配置和驗證用於檢測和丟棄包含特定字串(使用者名稱)的HTTP響應資料包的 自定義本地Snort規則。



注意:建立自定義本地Snort規則並為其提供支援不屬於TAC支援範圍。因此,本文檔只能 用作參考,並要求您自行斟酌決定並自行負責建立和管理這些自定義規則。

設定

網路圖表

本文檔介紹此圖中Snort2自定義本地Snort規則的配置和驗證。



組態

這是自訂本機Snort規則的組態,可偵測和捨棄包含特定字串(使用者名稱)的HTTP回應封包。

步驟 1.確認Snort版本

導航到裝置 > FMC上的裝置管理,點選裝置頁籤。確認snort版本為Snort2。

Firewall Management C Devices / Secure Firewall Device	Center Overview Analysis	Policies Devices Objects	Integration	Deploy	Q 🥝 🌣 🚱 admin 🗸 🖏	ECU			
FPR2120_FTD Cisco Firepower 2120 Threat Defense Device Routing Interfaces	Inline Sets DHCP VTEP SN	MP							
General	/ <u>+</u> +	License	1	System	8 G				
Name:	FPR2120_FTD	Essentials:	Yes	Model:	Cisco Firepower 2120 Threat Defense				
Transfer Packets:	Yes	Export-Controlled Features:	Yes	Serial:	JUNDA11707U2				
Troubleshoot:	Logs CLI Download	Malware Defense:	Yes	Time:	2024-04-06 01:26:12				
Mode:	Routed	IPS:	Yes	Time Zone:	UTC (UTC+0:00)				
Compliance Mode:	None	Carrier:	No	Version:	7.4.1				
TLS Crypto Acceleration:	Enabled	URL:	No	Time Zone setting for Time	LITC (LITC+0:00)				
		Secure Client Premier:	No	based Rules:					
Device Configuration:	Import Export Download	Secure Client Advantage:	No	Inventory:	View				
OnBoarding Method:	Registration Key	Secure Client VPN Only:	No						
Inspection Engine		Health		Management	/ 🕥				
Inspection Engine:	Snort 2	Status:	0	Remote Host Address:	1.10%0.25				

Snort版本

步驟 2.在Snort 2中建立自定義本地Snort規則

在FMC上導航到Objects > Intrusion Rules > Snort 2 All Rules,然後按一下Create Rule按鈕。



建立自訂規則

輸入自定義本地Snort規則的必要資訊。

- 入侵(客戶端/惡意客戶端): custom_http_sig
- 操作:警報
- 協定:tcp
- flow: Established, 到客戶端
- 內容:使用者名稱(原始資料)

Clijects / Intrusion Rules / Create Overview Analysis Policies Devices Objects Integration	Deploy Q 🙆 🌣 🚱 admin 🗸 🖏 SECURE
	Search Upload Update Intrusion
Snort 2 All Rules Snort 3 All Rules	
Create New Rule	
Message custom_http_sig	
Classification Unknown Traffic •	
Action alert v	
Protocol tep •	
Direction Bidirectional •	
Source IPs any Source Port any	
Destination IPs any Destination Pot any	
Detection Options	
flow ×	
content ×	
Case insensitive	
Not	
Rear Data	
ИТТР Невоег	
HTTP COORD	
NTTP Raw Header	
HTTP Raw Cooke	
HTTP Client Body	
HTTP Status Message	
Distance	
Within	
Official	
Depth	
Use Fast Pattern Matcher	
Fast Pattern Matcher Only	
content Add Option Save As New	
輸入規則的必要資訊	

步驟 3.確認自定義本地Snort規則

導航到FMC上的Policies > Intrusion Policies,點選Snort 2 Version按鈕。

Firewall Management Center Policies / Access Control / Intrusion Policies	Overview Analysis Policies	Devices Objects Int	itegration Deploy	० 💿 🌣 (admin v diada SE	CURE	
Intrusion Policies Network Analysis Policies							
Hide Snort 3 Sync status 🌒 🔍 Search by Intrusion Policy	, Description, or Base Policy		All IPS Rules IPS Map	ping O Com	pare Policies Create Po	olicy	
Intrusion Policy Description	Base Policy	Usage Infor	rmation				
snort_test → Snort 3 is in sync with Snort 2. 2024-01-12	Balanced Security and	2000 2000 2000 2000 2000 2000 2000 200	antrol Policy st Application Policy	Snort 2 Version Snort 3 Version 🖌 🖬 💽 🗑			

確認自定義規則

導航到FMC上的規則 >類別>本地,確認自定義本地Snort規則的詳細資訊。

Firewall Management Center Policies / Access Control / Intrusion / Edit Policy	Overview Analysis Policies	Devices Objects Integration	Deploy Q 🤣 🌣 🕲 admin ~ 🖓
Intrusion Policies Network Analysis Policies			
Policy Information Rules			< Back
Cisco Recommendations Rule Configuration > Advanced Settings Category	Filter: Category:"local"		0 (X
Policy Layers indicator-compromise indicator-cofuscation indicator-cofuscation	 0 selected rules of 1 Rule State Event Filtering 	namic State • Alerting • Comments •	Policy
indicator-shellcode	GID SID Message +	sig	→ @▼⊙ 9 ₩
malware-enc malware-other malware-tools netbios	Hide details		< < <u>1</u> of 1 > >
os-linux - m-mhile	Suppressions (0) Dynamic State (0)		Add
Classifications Microsoft Vulnerabiliti Microsoft Worms Platform Specific	> Alerts (0) > Comments (0)		Add SNMP Alert
Preprocessors Priority Rule Update	✓ Documentation rule at	slert top any any <> any any (sid:1000001; gid:1; flow:established.to	o_client; content.*username*; rawbytes; msg.*custom_http_sig*; classtype:unknown; rev:1;)

自定義規則的詳細資訊

步驟 4.變更規則動作

按一下State按鈕,將State設定為Drop and Generate Events,然後按一下OK按鈕。

Firewall Manageme Policies / Access Control / In	nt Center ntrusion / Edit Policy	Overview	Analysis	Policies	Devices	Objects	Integration			Deploy	۹ (•	0	admin 🗸	cisco S	SECURE	
Intrusion Policies Network A	nalysis Policies																
Policy Information Rules	Rules															< Back	
Cisco Recommendations > Advanced Settings	Rule Configuration Rule Content Category	Filter: Catego	ilter: Category:"local"												ר		
> Policy Layers	file-pdf indicator-compromise indicator-obfuscation indicator-scan indicator-shellcode	O selecte Rule Sta Gat	0 selected rules of 1 Rule State + Event Filtering + Dynamic State + Alerting + Comments + GRD SID Message +									Policy → ●▼ ⊙ €		•			
	makurare-backdoor makurare-other makurare-other makurare-other makurare-other makurare-other classifications Microsoft Vulnerabilities Microsoft Worms Platform Specific Provoncessors	•	1000001	custom_ht	Set rule s State Disabled Drop and Disabled	tate for "cu Events Generato Ever	stom_http_sig" @					Γ	-]			

變更規則動作

依次按一下Policy Information 按鈕和Commit Changes 按鈕以儲存更改。



提交更改

步驟 5.將入侵策略與訪問控制策略(ACP)規則關聯

導航到策略 > 訪問控制(在FMC上),將入侵策略與ACP關聯。

1 Cliting Rule ftd_acp	Mandatory 🛛 🗙
Name ftd_acp	dlow V Logging ON Time Range None V Rule Enabled
Intrusion	olicy snort_test X V Default-Set X V File Policy None V
Q Zones (2) Networks Ports Applications 🛕 Users UF	s Dynamic Attributes VLAN Tags
Q Search Security Zone Objects Showing 2 out of 2	Selected Sources: 1 Selected Destinations and Applications: 1
inside_zone (Routed Security Zone)	Collapse All Remove All Collapse All Remove All
dutside_zone (Routed Security Zone)	ZONE 1 Object 1 object 1 object 1 outside_zone I outside_zone I outside_zone I outside_zone

與ACP規則關聯

步驟 6.部署變更

將變更部署到FTD。



部署變更

驗證

未觸發自定義本地Snort規則

步驟 1.設定HTTP伺服器中的檔案內容

將HTTP伺服器端的test.txt檔案內容設定為使用者。

步驟 2.初始HTTP請求

從使用者端(192.168.10.1)的瀏覽器存取HTTP伺服器(192.168.20.1/test.txt),並確認允許HTTP通訊 。

	3	192.1	168.20.	1/test	txt	×	+	-	٥	×
<	<u>.</u>	\rightarrow	G	▲			192.168.20.1/test.txt	☆	Θ	:
use	er									

初始HTTP請求

已觸發自定義本地Snort規則

步驟 1.設定HTTP伺服器中的檔案內容

將HTTP伺服器端的test.txt檔案內容設定為username。

步驟 2.初始HTTP請求

從使用者端(192.168.10.1)的瀏覽器存取HTTP伺服器(192.168.20.1/test.txt),並確認已封鎖HTTP通 訊。

) 192.168.20.1	× +			<u> </u>	٥	×
\leftrightarrow \rightarrow X (1) 192.10	58.20.1/test.txt			☆	Θ	:
	Γ Ά					
初始HTTP請求						

步驟 3.確認入侵事件

在FMC上導航到分析 >入侵 >事件,確認入侵事件由自定義本地Snort規則生成。

Firewall Man Analysis / Intrusion	agement Cen s / Events	ter ov	verview	Analysis	Policies	Devices	Objects In	ntegration				Deploy	v Q	o 🌣 🛛	admin v diado	SECURE
								B	ookmark This Pa	ge Reporting	Dashboard	I View Bo	okmarks	Search Prede	ined Searches	Ŧ
Events By Priority and Classification (wetch workford)																
Search Constraints (Edit Search Save Search)																
Drilldown of Event, Prio	Drilldown of Event, Priority, and Classification Table View of Events Packets															
Jump to																
□ ↓ Time ×	Priority X	Impact X	Inline Result ×	Reason X	Source IP X	Source x	Destination IP X	Destination x	Source Port / ICMP X Type	Destination Port / ICMP X Code	SSL Status X	ULAN x	Messag	e X	Classification	General
× 2024-04-06 1	:05:13 low	O Unknown	Dropped		9192.168.20.1		9 192.168.10.1		80 (http) / tcp	50057 / tcp			custom	_http_sig (1:100000	1:1) Unknown Traf	lc Standar

按一下Packets頁籤,確認入侵事件的詳細資訊。

Bookmark: This Page Reporting Dashboard View Bookmarks Searche Predefined Searches	•
	7.15
Events By Priority and Classification instances and the section instan	nding
Search Constraints (Edit Search Save Search)	
Drilldown of Event, Priority, and Classification Table View of Events Packets	
← Event Information Message custom_http_sig (1:1000001:1) Time 2024-04-06 11:06:34	
Classification Unknown Traffic	
Priority low	
Ingress Security Zone outside_zone	
Egress Security Zone inside_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 192.168.10.1	
Destination Port / ICMP Code 50061 / tcp	
HTTP Hostname 192.168.20.1	
HTTP URI /test.txt	
Intrusion Policy snort_test	
Access Control Policy acp-rule	
Access Control Rule ftd_acp	
Rule alert top any any ⇔ any (sid:1000001; gid:1; flor:established.to_client; content:"username"; rambytes; msg:"custom_http_sig"; classtype:unknown; rev:1;) > Actions	

入侵事件的詳細資訊

疑難排解

運行system support trace命令以確認FTD上的行為。在本示例中,HTTP流量被IPS規則阻止(gid 1, sid 1000001)。

<#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 server IP address: 192.168.20.1
Please specify a server port:
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '
ftd_acp
', allow
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0
IPS Event
:
gid 1
,
sid 1000001
```

, drop

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW 192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ===>

Blocked by IPS

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。