使用ISE配置Firepower 6.1 pxGrid補救

目錄

簡介

本文檔介紹如何使用身份服務引擎(ISE)配置Firepower 6.1 pxGrid補救。 Firepower 6.1+ ISE補救模 組可與ISE端點保護服務(EPS)配合使用,自動在網路訪問層對攻擊者進行排隊/黑名單。

必要條件

需求

思科建議您瞭解以下主題的基本知識:

- Cisco ISE
- Cisco Firepower

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco ISE版本2.0補丁4
- Cisco Firepower 6.1.0
- 虛擬無線LAN控制器(vWLC)8.3.102.0

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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

設定

本文不涉及ISE與Firepower整合的初始配置、ISE與Active Directory(AD)的整合、Firepower與AD的 整合。有關此資訊,請導航到參考部分。Firepower 6.1補救模組允許Firepower系統在匹配關聯規則 時使用ISE EPS功能(隔離、取消隔離、埠關閉)作為補救。

附註:埠關閉不可用於無線部署。

網路圖表



流說明:

- 客戶端連線到網路,使用ISE進行身份驗證並使用授權配置檔案訪問授權規則,授權配置檔案 授予對網路的無限制訪問許可權。
- 2. 來自客戶端的流量隨後通過Firepower裝置。
- 3. 使用者開始執行惡意活動並點選關聯規則,該規則進而觸發Firepower管理中心(FMC)通過 pxGrid執行ISE補救。
- 4. ISE將EPSSstatus Quarantine分配給終端並觸發RADIUS授權更改到網路接入裝置(WLC或交換機)。
- 5. 客戶端點選另一個授權策略,該策略分配受限訪問(更改SGT或重定向到門戶或拒絕訪問)。

附註:網路接入裝置(NAD)應配置為向ISE傳送RADIUS記帳,以便為其提供用於將IP地址對 映到終端的IP地址資訊。

配置Firepower

步驟1.配置pxGrid緩解例項。

導覽至Policies > Actions > Instances,然後新增pxGrid緩解例項,如下圖所示。

Overview Analysis Policies Devices Objects AM	Ρ		Dep	ploy 🧕	System	Help 🔻	admin 🔻
Access Control Network Discovery Application Detectors	Correlation	Actions > Instances					
					Alerts F	Remediations	Groups
	Edit Instanc	e					
	Instance Name	ISE-NEW-INSTANCE					
	Module	pxGrid Mitigation(v1.0)					
	Description						
	Enable Logging	● On ○ Off					
		Create					

步驟2.配置補救。

有兩種型別可用:緩解目的地和緩解源。在此示例中,使用源緩解。選擇修正型別,然後按一下 Add,如下圖所示:

Remediation Name	Reme	diation Type	Descripti	on
No conf	igured re	mediations ava	ila <mark>bl</mark> e	
Add a new remediation	n of type	Mitigate Destir	nation 💌	Ad
		Mitigate Destin	ation	_

將緩解操作分配給補救,如下圖所示:

Edit Remediation	
Remediation Name	QUARANTINE-SOURCE
Remediation Type	Mitigate Source
Description	
Mitigation Action	quarantine 💌
Whitelist (an <i>optional</i> list of networks)	
	Create Cancel

步驟3.配置關聯規則。

導航到**Policies > Correlation > Rule Management**,然後按一下**Create Rule** Correlation rule是進行 補救的觸發器。關聯規則可以包含多個條件。在此範例中,如果發生入侵事件,且目的地IP位址為 192.168.0.121,則會命中Correlation Rule **PingDC**。為了測試的目的,已設定與icmp回應回覆相符 的自訂入侵規則,如下圖所示:

Overview Analysis Policies Devices Objects AMP Dep	oloy 🔑 System Help 🔻 admin 🔻
Access Control V Network Discovery Application Detectors Correlation Actions V	
	Alerts Remediations Groups
Policy Management Rule Management White List Traffic Profiles	
Rule Information	ion O Add Host Profile Qualification
Rule Name PingDC	
Rule Description	
Rule Group Ungrouped 💌	
Select the type of event for this rule	
If an intrusion event occurs 💽 and it meets the following conditions:	
O Add condition O Add complex condition	
X Destination IP is I 192.168.0.121	
Rule Options	O Add Inactive Period
Snooze If this rule generates an event, snooze for hours	
Inactive Periods There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".	

步驟4.配置關聯策略。

導覽至Policies > Correlation > Policy Management,然後按一下Create Policy,將規則新增到策略 並分配對策略的響應,如下圖所示:

Overview Analysis	Policies Devices (Objects AMP)			(Deploy	❶ ₁ Syst	em Help	≠ admin v
Access Control Netwo	ork Discovery Applicat	ion Detectors	Correlation	Actions v						
								Alert	s Remediat	ions Groups
Policy Management	Rule Management	White List	Traffic Profile	es						
Correlation Policy Ir	nformation	You	have unsave	d changes	Save	Cancel				
Policy Name	ise_corellation_policy									
Policy Description										
Default Priority	None -									
Policy Rules										Add Rules
Rule		Responses						F	riority	
PingDC		QUARANTIN	IE-SOURCE (Reme	liation)				[Default 💌	1

啟用關聯策略,如下圖所示:

Overview Analysis Policies Devices Objects AMP	Deploy		Help 🔻 admin 🔻
Access Control Network Discovery Application Detectors Correlation Actions			
		Alerts	Remediations Groups
Policy Management Rule Management White List Traffic Profiles			
			O Create Policy
Name		s	ort by State
ise corellation policy			💌 🦉 🖣 🗄

配置ISE

步驟1.配置授權策略。

導航到Policy > Authorization,然後新增新的授權策略,該策略將在補救發生後命中。使用 Session:EPSStatus等於Quarantine作為條件。因此可使用多個選項:

• 允許訪問並分配不同的SGT(在網路裝置上實施訪問控制限制)

- •拒絕訪問(使用者應該被踢出網路,不能再次連線)
- 重新導向至**黑名單**入口網站(在此案例中,自定義熱點入口網站是為此用途配置的)

cisco Identity S	Services Engine	Home	 Operations 	▼ Policy	Guest Access	Administration	▶ Work Centers		1 License	e Warning 🔺		0	1	\$
Authentication	Authorization Profi	ling Postu	re Client Provi	isioning 🕨 F	Policy Elements									
Authorization Define the Authori For Policy Export	Authorization Policy Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page First Matched Rule Applies													
 Exceptions 	(3)													
Status	Rule Name		Cond	ditions (identity	y groups and other co	onditions)		Permissions						
e 🖉 🔽	AssignSGTBlockOnFF		If Sess	ion:EPSStatu	s EQUALS Quarantir	ne		MaliciousUser AND	PermitAccess			E	dit 🕶	
	BlockOnISE		if Se	ssion:EPSSta	tus EQUALS Quaran	tine	th	en DenyAccess				E	Edit 🔻	
	BlockOnISE_copy		if S	Session:EPSS	tatus EQUALS Quar	antine		then blacklist_redire	ct			E	dit 🕶	

自定義門戶配置

在本示例中,熱點門戶配置為**黑名單**。只有包含自定義文本的「可接受使用策略」(AUP)頁,並且 不可能接受AUP(這通過JavaScript完成)。為此,首先需要啟用JavaScript,然後貼上一個在門 戶自定義配置中隱藏AUP按鈕和控制元件的代碼。

步驟1.啟用JavaScript。

導航到Administration > System > Admin Access> Settings > Portal Customization。選擇Enable Portal Customization with HTML and JavaScript,然後按一下Save。

dentity Services Engine	Home → Operations → Policy → Guest Access → Administration → Work Centers	1	License Warning 🔺	0	0	4	\$						
▼ System → Identity Management →	Network Resources												
Deployment Licensing	s → Logging → Maintenance Upgrade Backup & Restore - Admin Access → Settings												
0													
Authentication	▼ Portal Customization												
➤ Authorization	Enable Portal Customization with HTML												
Administrators	Enable Portal Customization with HTML and JavaScript												
- Settings	Save												
Access													
Session													
Portal Customization													

步驟2.建立熱點門戶。

導覽至Guest Access > Configure > Guest Portals,然後按一下Create,然後選擇熱點型別。

dialo Identity Services Engine	Home ► Operations	► Policy	► Administration	• Work Centers	1	License Warning 🔺	्	0	1	\$		
	Settings											
Overview Guest Portals Guest Ty	pes Sponsor Groups Sp	onsor Portals										
Guest Portals Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for quest access.												
Create Edit Duplicate De	:lete	,								i		

步驟3.配置門戶自定義。

導航到**門戶頁面自定義**並更改標題和內容,為使用者提供適當的警告。

diala cisco	Identi	ty Services En	gine H	ome I	 Operations 	▶ Policy	◄ Guest Access	Administration	Work Centers		1	License Warning 🔺			
▼ Co	nfigure	Manage Accou	unts ► Setti	ngs											
Over	/iew	Guest Portals	Guest Types	Sponso	or Groups S	ponsor Portals									
P	ages				Page	Customization	s								
	▼ Pag	98			Browser Pa	ge Title ED ACCESS						Preview Settings			
	Acc	eptable Use Pol	icy		Optional Co	ntent 1									
	Aut	nentication Suc	cess		Font	Ð	 Size 	• 🛆 • B I !	Į ∷ ∦≣ ∦ •	ci	sco. R	ESTRICTED ACC	ESS		
	Erro	r				2				F	RESTRIC	CTED ACCESS			
	▼ Me	ssages								n	nalicious	s user and blocked			
	Erro	r Messages													
					(text or HTN	1L) Click Previe	w to test HTML rende	ring.							
					Content Titl	e		_							
					RESTRICT	ED ACCESS									
					Instructiona	Text									
					Font		• Size	• 🛆 • 🖪 I	J 🗄 👌 🖉 🕶						
					X - D	Identified a	is a malicious user a	nd blocked							
					iou nave b	con nacritilleu c		na biotica.							

滾動到選項內容2,按一下切換HTML源,然後將指令碼貼上到內部:

按一下**取消切換HTML源。**

Optional Content 2

Font	Size	<u>A</u> ▼ B <i>I</i> <u>U</u> ⊟ <u>∃</u>	Ø -
X - 🔲 🖸			
<script></th><th></th><th></th><th></th></tr><tr><th>(function(){ jQuery('.cisco-is jQuery('.cisco-is setTimeout(function timeout-popup-pop })(); </script> <th>:e-aup-text').hide(); :e-aup-controls').hide(); in(){ jQuery('#portal-session pup, #portal-session-timeou pogus_node="TRUE" /></th> <th>n-timeout-popup-screen, #portal-sess it-popup').remove(); }, 100);</th> <th>ion-</th>	:e-aup-text').hide(); :e-aup-controls').hide(); in(){ jQuery('#portal-session pup, #portal-session-timeou pogus_node="TRUE" />	n-timeout-popup-screen, #portal-sess it-popup').remove(); }, 100);	ion-

(text or HTML) Click Preview to test HTML rendering.

驗證

使用本節提供的資訊以驗證您的組態是否正常運作。

Firepower

觸發補救的是關聯策略/規則的命中。導覽至Analysis > Correlation > Correlation Events,然後驗證 是否已發生關聯事件。

0	verviev	Analysis	Polici	es Devic	es Obje	cts AMP								Deploy	0, System	Help	▼ admin ▼
Co	ntext E	xplorer Con	nections	 Intrus 	sions 🔻	Files 🔻 Ho	osts 🔹 Users	 Vulnerabi 	ities 🔻	Correlation	Correlation Events	Custom 🔻	Lookup 🔻	Search			
												Book	kmark This Pag	e Report Designe	r Dashboard Vie	w Bookm	arks Search
С <u>с</u> с	Correlation Events																
No	Search (Constraints (<u>Edit s</u>	earch)														
	Jump to.																
		▼ <u>Time</u> ×		Impact ×	Inline × Result	Source IP	X <u>Source</u> <u>Country</u>	× Destination IP	×	Destination × Country	Security Intelligence × Category	Source Use	er ×	Destination × User	Source Port / ICMP Type	×	Destination P ICMP Code
-		2017-02-16 13	27:51	1		172.16.1	0.19	i 192.168.	0.121						8 (Echo Request	<u>) / icmp</u>	<u>0 / icmp</u>

ISE

然後ISE應觸發Radius:CoA並重新驗證使用者,可以在操作> RADIUS即時日誌中驗證這些事件。

2017-02-16 13:26:22.894	V	à	alice	E4:B3:18:69:EB:8C	Windows10-Workst Default >> Dot1X >> D Default >> AssignSGT MaliciousUser,PermitAcc v	vWLC
2017-02-16 13:26:21.040	~	à		E4:B3:18:69:EB:8C	v	vWLC
2017-02-16 13:25:29.036	V	o	alice	E4:B3:18:69:EB:8C	Windows10-Workst Default >> Dot1X >> D Default >> Standard R PermitAccess,Administra v	vWLC

在本示例中,ISE為終端分配**了不**同的SGT MaliciousUser。在**Deny Access** authorization profile的 情況下,使用者會丟失無線連線,並且無法再次連線。

使用黑名單門戶進行補救。如果補救授權規則配置為重定向到門戶,則從攻擊者的角度應如下所示 :

e restricted access × +		-	ć	ı ×	
🔶 🛈 🗞 https://vpalkin-ise20-1.example.com.8443/portal/PortalSetup.action?portal=74d92220-e56a-11e6-b87e-005056993cb3&sessionId=b6 🔻 13356 🖉 🔍 Search	☆自	÷	î î		ł
CISCO RESTRICTED ACCESS					^
RESTRICTED ACCESS You have been identified as a malicious user and blocked.					

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

導覽至Analysis > Correlation > Status,如下圖所示。

Overview Analysis Policies Devices Objects AMP Deploy 🍳 System Help 🕶 admin 🔹											
Context Explorer	Connections •	Intrusions 🔻	Files v	Hosts 🔻	Users 🔻	Vulnerabilities v	Correlation • Status	Custom v	Lookup 🔻	Search	
											Bookmark This Page Report Designer View Bookmarks Search
Remediation	Remediation Status 2017-02-16 14:25:00 - 2017-02-16 14:27:00 C Table View of Remediations Static										
No Search Constraints (<u>Edit Search</u>)											
Jump to •											
Time	×	Remediation Name ×			Policy × Rule ×				Result Message ×		
J 2017-02	-16 14:26:19		QUARANTINE-SOURCE			ise_corellation_policy				Successful completion of remediation	
< <page 1="" of="">> Displaying row 1 of 1 rows</page>											
View Delete											

結果消息應返回Successful complete of remediation或特定錯誤消息。驗證系統日誌:System > Monitoring > Syslog並使用pxgrid過濾輸出。可在/var/log/messages中驗證相同的日誌。



- <u>https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-</u> <u>Troubleshoot-ISE-and-FirePOWER-Integrati.html</u>
- <u>https://communities.cisco.com/docs/DOC-68284</u>
- <u>https://communities.cisco.com/docs/DOC-68285</u>
- <u>https://communities.cisco.com/thread/64870?start=0&tstart=0</u>
- <u>http://www.cisco.com/c/en/us/td/docs/security/ise/2-</u> <u>0/admin_guide/b_ise_admin_guide_20.html</u>
- <u>http://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61.html</u>