CS-MARS — 新增並配置IPS感測器作為報告裝置

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>相關產品</u> <u>慣例</u> <u>設定</u> <u>在MARS中新增和配置Cisco IPS 6.x或7.x裝置</u> <u>驗證MARS是否從Cisco IPS裝置獲取事件</u> <u>疑難排解</u> <u>相關資訊</u>

<u>簡介</u>

本文檔介紹如何準備思科安全入侵防禦系統(IPS)裝置和任何已配置的虛擬感測器,以充當思科安全 監控、分析和響應系統(CS-MARS)的報告裝置。

<u>必要條件</u>

<u>需求</u>

對於Cisco IPS 5.x、6.x和7.x裝置,MARS使用SSL上的SDEE獲取日誌。因此,MARS必須能夠通 過HTTPS訪問感測器。為了準備感測器,必須在感測器上啟用HTTP伺服器,啟用TLS以允許 HTTPS訪問,並確保MARS的IP地址被定義為允許的主機,該主機可以訪問感測器並獲取事件。如 果已將感測器配置為允許從網路上的有限主機或子網訪問,可以使用access-list ip_address/netmask命令啟用此訪問。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- 運行軟體版本4.2.x及更高版本的Cisco Secure MARS裝置
- 運行軟體版本6.0及更高版本的Cisco 4200系列IPS裝置

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。

<u>相關產品</u>

此配置也可用於以下感測器:

- IPS-4240
- IPS-4255
- IPS-4260
- IPS-4270-20

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

<u>設定</u>

本節提供有關如何向思科安全監控、分析和響應系統(CS-MARS)裝置新增和配置Cisco Secure Intrusion Prevention System(IPS)感測器的資訊。

在MARS中新增和配置Cisco IPS 6.x或7.x裝置

在MARS中定義Cisco IPS 6.x或7.x裝置時,可以發現裝置上配置的任何虛擬感測器。當您發現這些 虛擬感測器時,這允許MARS按虛擬感測器分離報告的事件。它還允許您調整每個虛擬感測器的受 監控網路清單,從而提高所需報告的準確性。

完成以下步驟,以便在MARS中新增和配置Cisco IPS 6.x或7.x裝置:

- 1. 選擇Admin > System Setup > Security and Monitor Devices。然後,按一下Add。
- 2. 從Device Type清單中選擇Cisco IPS 6.x或Cisco IPS 7.x。現在在Device Name欄位中輸入感 測器的主機名,如下所示。IPS1是本示例中使用的裝置名稱。「Device Name(裝置名稱)」 值必須與配置的感測器名稱相同。

*Device Name:	IPS1			
Reporting IP:	10 10 10	10		
*Access Type:	SSL			
Login:				
Password:				
Port:	443			
Monitor Resource Usage:	NO 💌			
Pull IP Logs:	NO 🛩			

⇔Back Test Connectivity

Submit

現在,在Reporting IP欄位中輸入管理IP地址。報告IP地址與管理IP地址相同。

3. 在登入欄位中,輸入與用於訪問報告裝置的管理帳戶關聯的使用者名稱。現在,在 Password欄位中,輸入與Login欄位中指定的使用者名稱相關聯的密碼。在此範例中,使用者 名稱為cisco,而使用密碼為cisco123。在Port欄位中輸入感測器上運行的Web伺服器監聽的

TCP埠號。預設HTTPS埠為443。

→ "Device Name:	FS1
→ Reporting IP:	10 10 10 10
→ *Access Type:	SSL
Login:	cisco'
Password:	
Port:	443
→ Monitor Resource Usage:	NO V
Pull IP Logs:	NO 🛩

🗢 Back

Back

Submit

Submit

Test Connectivity

Test Connectivity

注意:雖然可以僅配置HTTP,但MARS需要HTTPS。

4. 現在驗證在**Monitor Resource Usage**清單中是否選擇了**NO**。當Monitor Resource Usage選項 出現在此頁面上時,它對Cisco IPS不起作用。

•	*Device Name:	PS1]
+	Reporting IP:	10	10	10	10	כ
+	Access Type:	SSL				
	Login:	cisc	o'			1
	Password: Port:	443]
+	Monitor Resource Usage:	- NO		-		
1555	Pull IP Logs:	NO	v			

5. 要從感測器提取IP日誌,請從**提取IP日誌**清單中選擇**Yes**。這是一項可選功能,可在需要時使 用。

→ ~1	Device Name;	PS1			
→ 1	Reporting IP:	10	1/10	10][
÷ "1	Access Type:	551.			
	Login:	ciso	10"		
	Password:			•	
	Port:	443			
-> P	tonitor Resource Usage:	NO	~		
P	ull IP Logs:	NO	v	1	

◆Back Test Connectivity Submit 此設定適用於整個感測器,包括為虛擬感測器警報生成的日誌。 6. 按一下Test Connectivity以驗證配置並啟用虛擬感測器的發現。

→ "Device Name;	PS1	
→ Reporting IP:	10 10	10
→ *Access Type:	55L	
Login:	cisco'	
Password:		
Port:	443	
→ Monitor Resource U	age: NG 🗸	
Pull IP Logs:	NO V	

Back

Test Connectivity

Submit

7. 按一下「Discover」以發現任何已定義的虛擬感測器。

Reporting IP: 10 *Access Type: SSL Login: cisco Password: eeneeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	Reporting IP: 10 10 10 *Access Type: SSL Login: Cisco Password: exerces Port: 443 Monitor Resource Usage: NO * Pull IP Logs: NO *	Reporting IP: 10 10 10 *Arcess Type: SSI Login: cisco Password: exercese Port: 443 Moitor Resource Usage: NO	Reporting IP: f0_f0_f0_f0 *Access Type: SSI Login: cisco Password: exereme Port: 443 Monitor Resource Usage: NO Pull IP Logs: NO	Reporting IP: fg_f0_f0_f0_f0 "Access Type: SSI Login: cisco Password: evereve Port: 443 Noitor Resource Usage: No Pull IP Logs: NO Discover Edit Virtual Sensor Name Monitoring Networks	Reporting IP: http://titual Sensor Name	Reporting IP: 'Access Type: Login: Password: Port:	ta 10 10 10 SSL cisco	J	
*Access Type: SSL Login: Cisco Password: e******* Port: 443 Monitor Resource Usage: NO *	*Access Type: SSL Login: Cisco Password: ******** Port: 443 Monitor Resource Usage: NO * Pull IP Logs: NO *	*Access Type: SSL Login: cisco Password: e******* Port: 443 Monitor Resource Usage: NO × Pull IP Logs: NO ×	*Access Type: SSL Login: Cisco Password: eeneeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	*Access Type: SSI Login: Cisco Password: exerner Port: 443 Monitor Resource Usage: NO Pull IP Logs: NO	*Access Type: SSI Login: cisco Password: eeeeeee Port: 443 Monitor Resource Usage: NO Pull IP Logs: NO Discover Edit	'Access Type: Login: Password: Port:	SSI cisco		
Login: cisco Password: e Port: 443 Monitor Resource Usage: NO NO	Login: Cisco Password: eeeeeee Port: 443 Monitor Resource Usage: NO V Pull IP Logs: NO V	Login: cisco Password: e++++++ Port: 443 Monitor Resource Usage: NO V Pull IP Logs: NO V	Login: cisco Password: eeeeeee Port: 443 Monitor Resource Usage: NO Pull IP Logs: Edit	Login: cisco Password: exerce Port: 443 Monitor Resource Usage: No Pull IP Logs: No Discover Edit	Login: cisco Password: eeeeeee Port: 443 Monitor Resource Usage: NO NO Pull IP Logs: NO NO Discover Edit	Login: Password: Port:			
Password: exerce 443 Monitor Resource Usage: NO V Pull IP Logs: NO V	Password: exerce 443 Monitor Resource Usage: NO V Pull IP Logs: NO V	Password: exerce 443 Port: 443 Monitor Resource Usage: NO V Pull IP Logs: NO V	Password: exerce Port: 443 Monitor Resource Usage: NO X Pull IP Logs: NO X Edit Edit	Password: exerce Port: 443 Monitor Resource Usage: NO V Pull IP Logs: NO V NO V Edit Virtual Sensor Name Monitoring Networks	Password: 443 Port: 443 Monitor Resource Usage: NO V Pull IP Logs: NO V Discover Edit Virtual Sensor Name Monitoriog Networks	Password: Port:	******		120012120121200000000000000000000000000
Monitor Resource Usage: NO V Pull IP Logs: NO V	Monitor Resource Usage: NO V Pull IP Logs: NO V	Monitor Resource Usage: NO V Pull IP Logs: NO V	Monitor Resource Usage: NO Pull IP Logs: NO V Discover	Monitor Resource Usage: NO	Monitor Resource Usage: NO		443		
Pull IP Logs: NO 💌	Pull IP Logs: NO 💌		Pull IP Logs: NO S Discover Edit	Pull IP Logs: NO V Discover Edit Virtual Sensor Name Monitoring Networks	Pull IP Logs: NO NO Discover Edit Virtual Sensor Name Monitoring Networks	Monitor Resource Usag	8: NO 💌		
			Discover	Discover Edit Virtual Sensor Name Monitoring Networks	Discover Edit Virtual Sensor Name Monitoring Networks	Pull IP Logs:	NO 💌		

注意:MARS不知道對感測器所做的更改。無論何時更改虛擬感測器設定,您都必須在該感測 器配置頁面上按一下**Discover**才能刷新MARS中的虛擬感測器詳細資訊。

8. 選擇「Virtual Sensor Name(虛擬感測器名稱)」旁邊的覈取方塊,然後按一下**Edit**,為每個 虛擬感測器定義受監控的網路。此時會顯示「IPS模組」頁面,如下所示。

+	*Device Name:	[IPSt	
->	Reporting IP:	10 (10 10	10
÷	*Access Type:	55L	
	Login: Password; Port:	cisco ••••••	
+	Monitor Resource Usage: Pull IP Logs:	NO V	
	Discover	Edit	
	Virtual Sensor Name	Monitorin	Networks
	N LOI		122222222222

9. 要計算和緩解攻擊路徑,請指定感測器所監視的網路。選擇定義網路單選按鈕以手動定義網路。然後完成以下步驟以定義網路:在Network IP欄位中輸入網路地址。在Mask欄位中輸入相應的網路掩碼值。按一下「Add」將指定的網路移到「Monitored Networks」欄位中。如果需要定義更多網路,請重複前面的步驟。

Back

Test Connectivity

Submit

*Device Name: P\$1		
ional: for attack path calculation and mitigation e Monitored Networks:	Add	tworks information] C Select a Network: 10.10.00/255.255.255.0(n-10.10.10.00/24)
		Define a Network: Network IP: 10 10 10 0 Mask: 255 255 255 0

Cancel Submit

注意:這是一個可選功能,如果需要,可以跳過此功能。

10. 按一下Select a Network單選按鈕以選擇連線到裝置的網路。然後完成以下步驟以選擇網路 : 從Select a Network(選擇網路)清單中選擇網路。按一下「Add」將指定的網路移到「 Monitored Networks」欄位中。如果需要選擇更多網路,請重複前面的步驟。

* Device Name: PS1	
ptional: for attack path calculation and n	Al Add (* Select a Network: Remove (* 10.10.10.0/255.255.0(n-10.10.10.0/24))
	C Define a Network: Network IP: 10 10 10 0 Mask: 255 255 0

注意:這是一個可選功能,如果需要,可以跳過此功能。

- 11. 對每個虛擬感測器重複步驟8到步驟10。
- 12. 按一下「Submit」以儲存變更內容。裝置名稱顯示在Security and Monitoring Information清 單下。提交操作在資料庫表中記錄更改。但是,它不會將更改載入到MARS裝置的工作記憶 體中。啟用操作將提交的更改載入到工作記憶體中。

Cancel

Submit

13. 按一下Activate以啟用MARS以開始從此裝置對事件進行會話化。MARS開始設定此模組生成 的事件的會話,並使用定義的檢查和丟棄規則評估這些事件。裝置在啟用之前向MARS發佈 的任何事件都可以以裝置的報告IP地址作為匹配條件進行查詢。請參閱<u>啟用報告和緩解裝置</u> 。有關啟用操作的詳細資訊。

<u>驗證MARS是否從Cisco IPS裝置獲取事件</u>

在網路中建立良性事件以驗證資料流是很常見的。完成以下步驟,驗證Cisco IPS裝置和MARS之間 的資料流:

- 1. 在Cisco IPS裝置上, 啟用2000和2004簽名並發出警報。特徵碼監控ICMP消息(ping)。
- 2. 對Cisco IPS裝置偵聽的子網上的裝置執行Ping操作。這些事件由MARS生成和拉動。
- 3. 驗證事件是否顯示在MARS Web介面中。您可以使用Cisco IPS裝置執行查詢。
- 4. 驗證資料流後,您可以在Cisco IPS裝置上禁用2000和2004簽名。注意:如果在MARS Web介面中配置Cisco IPS裝置期間,測試連線操作未失敗,則通訊已啟用。使用此任務可以進一步 驗證警報是否正確生成和提取。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 思科安全監控、分析和回應系統支援頁面
- <u>思科入侵防禦系統支援頁面</u>
- 思科安全監控、分析和響應系統 相容性資訊
- <u>要求建議 (RFC)</u>
- 技術支援與文件 Cisco Systems