面向終端的AMP與Splunk整合

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> 設定 疑難排解

簡介

本檔案介紹進階惡意軟體防護(AMP)和Splunk之間的整合程式。

作者:Uriel Islas和Juventino Macias,編輯者:Jorge Navarrete,思科TAC工程師。

必要條件

需求

思科建議您瞭解:

- AMP端點版
- •應用程式開發介面(API)
- 斯普倫克
- Splunk上的管理員使用者

採用元件

- AMP公共雲
- Splunk例項

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

步驟1.導航到AMP控制檯(<u>https://console.amp.cisco.com</u>),然後導航到Accounts>API Credentials,您可以在其中建立事件流。



步驟2。若要執行此整合,請勾選**讀取/寫入**覈取方塊,如下所示:

New API Cre	dential	
Applic	ation name	caisias-amp
	Scope	Read-only Read & Write
	E Alt	ow API access to File Repository download audit logs
An API c AMP for with your	redential v Endpoints r endpoints	with read and write scope can make changes to your configuration that may cause significant problems s.
Some of to the AF	the input ; 71.	protections built into the AMP Console do not apply
		Canical Create

附註:如果您想收集有關事件的詳細資訊,請選中Enable Command Line框,以獲得從檔案 儲存庫生成的稽核日誌,請選中Allow API access to File Repository框。

< API Key [Details
3rd Party A	PI Client ID
	#36a12a390. I
API Key	
	\$3ddr317=essr+42
API credentials (and password, a	API Client ID & API Key) will allow other programs to retrieve and modify your Cisco AMP for Endpoints data. It is functionally equivalent to a use nd should be treated as such.
Delete the API o	redentials for an application if you suspect they have been compromised and create new ones.
Deleting API cre	dentials will lock out any clients using the old ones so make sure to update them to the new credentials.
Your API creden	tials are not stored in plain text and can only be displayed once. If you lose the credentials you will have to generate new ones.
View API Docum	ventation.

注意:此資訊無法以任何方式恢復,如果丟失,必須建立一個新的API金鑰。

步驟4.為了將Splunk與面向終端的AMP整合,請確保Splunk上存在帳戶Admin。

Usemanie	Password	Sign In
-O admin From this website		
**O mex-amp From this website	jed out. Log in to return to the system.	
View Saved Logins		

步驟5.登入Splunk後,繼續從Splunk應用下載AMP。



步驟6.在應用瀏覽器上搜尋思科端點並進行安裝(面向端點的思科AMP事件輸入)。

splunk> Apps ~	Administrator V Messages V Settings V Activity V Help V Find
Browse More Apps	
cisco endpoint	Best Match Newest Popular 7 Apps
CATEGORY DevOps Security, Fraud & Compliance IT Operations Utilities Business Analytics IoT & Industrial Data	****** Cisco AMP for Endpoints CIM Add-On Install The Cisco AMP for Endpoints CIM Add-on provides a mechanism to map data from the Cisco AMP for Endpoints Event Input App for CIM compliant applications. The add-on also provides additional workflow actions so security analysts can go straight from Splunk Events to the Cisco AMP for Endpoints console.
CIM VERSION 4.x 3.x	Category: Security, Fraud & Compliance Author: Samson Nguyen Downloads: 996 Released: 2 years ago Last Updated: a year ago View on Splunkbase
SUPPORT TYPE	Cisco AMP for Endpoints Events Input
Not Supported	The Cisco AMP for Endpoints Events Input provides a mechanism to create, update, and delete event streams in Cisco Advanced Malware Protection (AMP) for Endpoints via the API and index them in your Splunk® instance to make them searchable. All you need to do is provide your API host and credentials from your AMP for Endpoints account and specify the stream parameters. This app has been tested on Splunk v6.6.0
APP CONTENT	Less
Inputs	

步驟7.需要重新啟動會話才能完成Splunk上的安裝。



步驟8.在Splunk下登入後,按一下螢幕左側的Cisco AMP For Endpoints。



步驟9.按一下螢幕頂部的Configuration標籤。

Inputs	New Input	Configuration
Inputs		
Create	a New Input	
Retrieving	g inputs	

步驟10.鍵入以前從AMP控制檯生成的API憑據。

splunk	enterprise	App: Clsco AMP for Endpoints Events Input +
Inputs	New Input	Configuration
Conf Global co	iguration antiguration for	Cisco AMP for Endpoints events input
AMP fo	or Endpoints AF	PLAccess Configuration
AMP to api.ar	r Endpoints API np.cisco.com address of the Ci ent ID *	Host *
Enter the	e Brd Party API Cile	ant ID provided by AMP for Endpoints. Please note that your API Client must have read and write scope
Enter the Save	Configuration	

附註:API主機點可能因組織指向的雲資料中心而異: 北美洲:api.amp.cisco.com 歐洲:api.eu.amp.cisco.com 亞太地區、日本及中國:api.apjc.amp.cisco.com

步驟11.在Splunk控制檯上包含並儲存API憑證,以將其與AMP連結。

splunk	>enterprise	App: Cisco AMP for Endpoints Events Input *
Inputs	New Input	Configuration
Conf	iguration	
Global c	onliguration for 9	Disco AMP for Endpoints events input
0 Co	onfiguration succ	essfully saved
AMP fo	or Endpoints AF	Access Configuration
AMP fo	or Endpoints API	Host *
apilar	mp.cisco.com	
Enter th	e address of the Cr	sco AMP for Endpoints API Server that the application will access for managing event streams. Please refer to the AMP for Endpoints API documentation for the correct hostname
API CI	ent ID 1	
e36c	12c3905be05ca	cb7
Enter th	e 3rd Party API Cite	nt ID provided by AMP for Endpoints. Presse note that your API Client must have read and write scope
API Ke	y.*	
a68f	433e-base-f620	141ct63/b
Enter th	é secrit API key	
Sove	Configuration	

步驟12.返回Input以建立您的事件流。

New Input	
Name *	
caislas	
Index	
main	~
In which index would you like the events to appear?	
Stream Settings	
Stream Name *	
Stream Name * caislas	
Stream Name * caislas Event Types	
Stream Name * caislas Event Types	
Stream Name * caistas Event Types [Groups	
Stream Name * caislas Event Types [Groups Leave this field blank to return all Groups	
Stream Name * coistas Event Types Groups Leave this field blank to return all Groups	

附註:如果要從AMP獲取所有組的所有事件,請將**Event Types**和Groups欄位留空。

Inputs	
Create a New Input	
Name	Index
caislas	main

步驟13.確保已成功建立您的輸入。

如果在建立事件流時,所有欄位都呈灰色顯示,則可能是由於以下某些原因造成的:

nputs	New Input		
New I	nput		
Name."			
		0	
Index			
In which in	idex would you i	to the events to series?	
		ware state a second an address of t	
Stream S	Settings	and the of the first of the papers of a	
Stream Stream N	Settings lame *		
Stream Stream M	Settings lame *		
Stream Stream N Event Typ Leave t	Settings kame * pes his held blank	to return all Event types	0
Stream Stream N Event Typ Leave t Groups	Settings lame * pes his field blank	to return all Event types	

- 1. 連線問題:確保Splunk例項能夠聯絡API主機
- 2. API主機:根據您的業務所在的位置,確保步驟10中配置的API主機與您的AMP組織相匹配。
- 3. API憑據:確保API金鑰和客戶端ID與步驟3中配置的金鑰和客戶端ID匹配。
- 4. 事件流:請確保配置的事件流少於4個。