將Cisco SecureX與VirusTotal整合

目錄

<u>簡介</u> <u>必要條件</u> <u>需求用元件</u> 設設 設 難 <u>疑</u> 業 上

簡介

本文檔介紹將Cisco SecureX與VirusTotal整合的步驟。

必要條件

需求

思科建議您瞭解以下主題:

- API金鑰
- SecureX控制檯

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。

設定

要配置新的VirusTotal增強模組,必須先在VirusTotal中生成API金鑰,然後新增VirusTotal模組。

步驟1. InVirusTotal,點選VirusTotal使用者圖示並選擇設定。

步驟2. ClickAPI Keyword並儲存金鑰值,如下圖所示。

	6	Yeraldin San		
		Profile		
		API key		
		Settings		
		Sign out		
< → C ■	virustotal.com	l/gui/uset/leisanch/apikey		
	address, dornai	n, or file hash		
		APIKey		
		fb5b7becda	1577e	

步驟3.在SecureX門戶上,導航到Integrations,然後點選Add New Module,如下圖所示

cisco Secure×	Dashboard	Integrations	Orchestration Beta	Administration	
Settings Your Account Devices API Clients	Integrations SecureX uses modules to integrate with other Cisco security products and third-part Your Configurations				
> Integrations Users			Add New Module		

步驟4.在VirusTotal部分,按一下Add New module,如下圖所示。



VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of...

Add New Module

Learn More · Free Trial

步驟5.在此部分輸入VirusTotalAPI 金鑰,然後按一下Save,如下圖所示。

cisco SecureX	Dashboard	Integrations	Orchestration Beta	Administration	
Settings Your Account Devices API Clients	Add New VirusTotal Module Module Name* VirusTotal				
 Integrations Available Integrations 	API Key*				
Users					

附註:公共API限製為每1分鐘時間幀最多4個請求。VirusTotal富集模組為每個可觀察對象發出一個API請求。VirusTotal還提供<u>一個</u>Private API,可提供更高的請求速率。

驗證

使用本節內容,確認您的組態是否正常運作。

若要驗證模組是否按預期運作,請導覽至**思科威脅回應**入口網站並進行調查,結果會顯示已擴充的 模組,如下圖所示。

22 Presidences manager incomes managere						 Number for the second se
Recorder Terror. 1						Address Cauch
Balayers Artest	011 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0	B	No. of Concession, Name	10 · · · · ·	3 · · · · · · ·
Interplate 1 of Leadershow Corpus			Payment Payment <t< td=""><td>B B B D Toplet, 1780 B B</td></t<>			B B B D Toplet, 1780 B B
			Cinco.com ¹⁰ Institute Without Cinco Million Cinco Millio	an an an ana ana ana ana ana ana ana ana	daari ^a raa daarai	

疑難排解

本節提供的資訊用於對組態進行疑難排解。

步驟1.確保API憑據已正確從SecureX門戶的模組部分複製。

步驟2.驗證API憑據是否具有正確的許可權且當前可用。

附註:如果出現任何意外錯誤,請參閱VirusTotal API錯誤文檔。

影片

您可以在此影片中找到本文中包含的配置步驟。