

配置與Tetration的SecureX整合

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[在Tetration安全控制面板中生成API憑據](#)

[在SecureX中整合Tetration模組](#)

[驗證](#)

[影片指南](#)

簡介

本檔案介紹將Cisco SecureX與Cisco Tetration整合和驗證所需的流程。

作者：Juan Castellero和Uriel Torres，編輯者：Jorge Navarrete，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- 思科終端進階惡意軟體防護
- Tetration安全儀表板
- SecureX控制檯中的基本導航
- 映像的可選虛擬化

採用元件

- Tetrationv安全儀表板
- Tetration管理員帳戶
- SecureX控制檯版本1.54
- SecureX管理員帳戶
- Microsoft Edge版本84.0.522.52

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

Cisco Tetration平台可應對工作負載和應用安全挑戰，這些挑戰可在混合雲基礎設施中提供微分段和基於行為的異常檢測功能，Tetration模組提供3個圖塊。

Tetration易受攻擊的工作負載和庫存：描述具有已知漏洞的工作負載和總庫存計數的指標。

Tetration策略度量：描述配置的分段策略的度量。

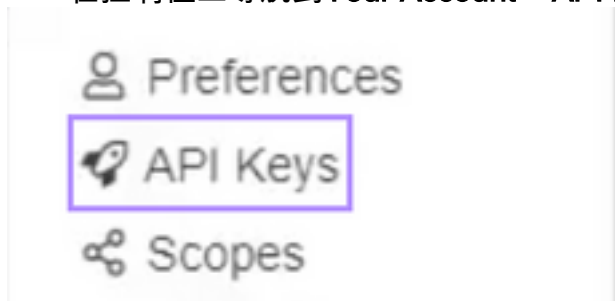
Tetration軟體代理摘要：描述所連線的軟體代理的度量。

設定

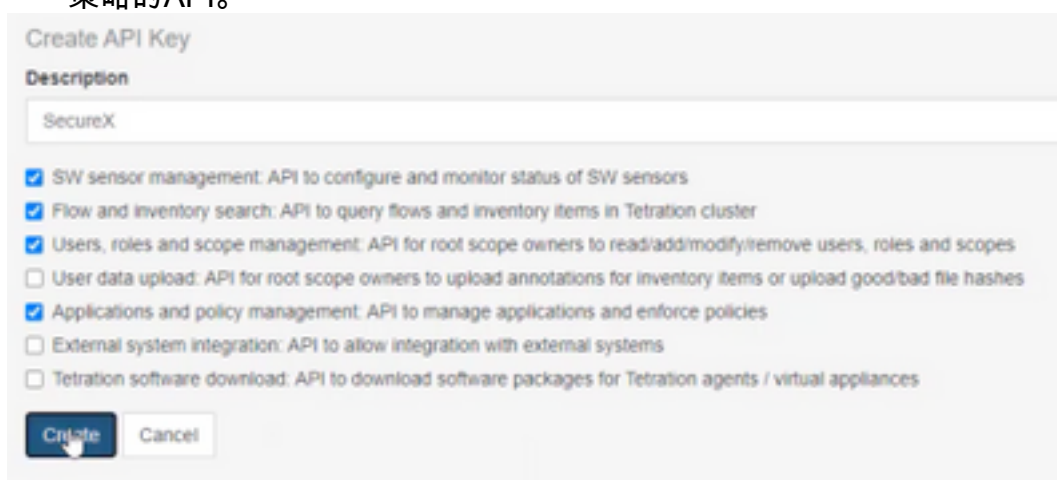
在Tetration安全控制面板中生成API憑據

在Tetration安全控制面板中，建立新的API

- 使用管理許可權登入到Tetration安全儀表板。
- 在控制檯上導航到Your Account > API Keys。



- 按一下**Create API Key**
- 選擇以下元素：
 - SW感測器管理：用於配置和監視SW感測器狀態的API。
 - 流和庫存搜尋：用於查詢Tetration群集中的流和庫存專案的API。
 - 使用者、角色和範圍管理：用於讀取/新增/修改/刪除使用者、角色和作用域的根作用域所有者的API。
 - 應用程式和策略管理：用於管理應用和實施策略的API。

A screenshot of the 'Create API Key' dialog box. The 'Description' field contains the text 'SecureX'. Below the field is a list of checkboxes for different API scopes. The first four checkboxes are checked: 'SW sensor management: API to configure and monitor status of SW sensors', 'Flow and inventory search: API to query flows and inventory items in Tetration cluster', 'Users, roles and scope management: API for root scope owners to read/add/modify/remove users, roles and scopes', and 'Applications and policy management: API to manage applications and enforce policies'. The last two checkboxes are unchecked: 'User data upload: API for root scope owners to upload annotations for inventory items or upload good/bad file hashes' and 'External system integration: API to allow integration with external systems'. At the bottom of the dialog are two buttons: 'Create' and 'Cancel'.

重要資訊：在關閉對話方塊之前檢索這些值；頁籤關閉後，無法檢索生成的API資訊。

- 儲存API憑據
- 若要建立整合權杖，請導覽至tetration-securex.link/setup
- 介紹您的Tetration URL和API憑證

- 按一下「Create Token」
- 複製整合令牌

Use this wizard to setup your Tetraton and SecureX integration.

1. Enable the Tetraton module in your SecureX console

2. Input your Tetraton API credentials

Tetraton URL ^{*}

https://[redacted].com/

API Key ^{*}

cf[redacted]

API Secret ^{*}

[redacted]

Create Token

3. Copy the generated Authentication token to the SecureX console

[redacted]

Copy

在SecureX中整合Tetraton模組

將Tetraton與SecureX整合，以瞭解Tetraton系統的運行狀況、暴露易受攻擊的工作負載、跟蹤分段策略以及對行為偏差做出反應。

- 在SecureX控制檯上，導航到Integrations > Click Add New Module
- 選擇Cisco Tetraton模組，然後按一下Add New Module
- 為模組命名
- 貼上令牌並按一下 儲存

Add New Cisco Tetraton - Application-First Workload Protection Module

Module Name ^{*}

Cisco Tetraton - jesutarr

Authorization Token ^{*}

[redacted]

Save Cancel

Quick Start

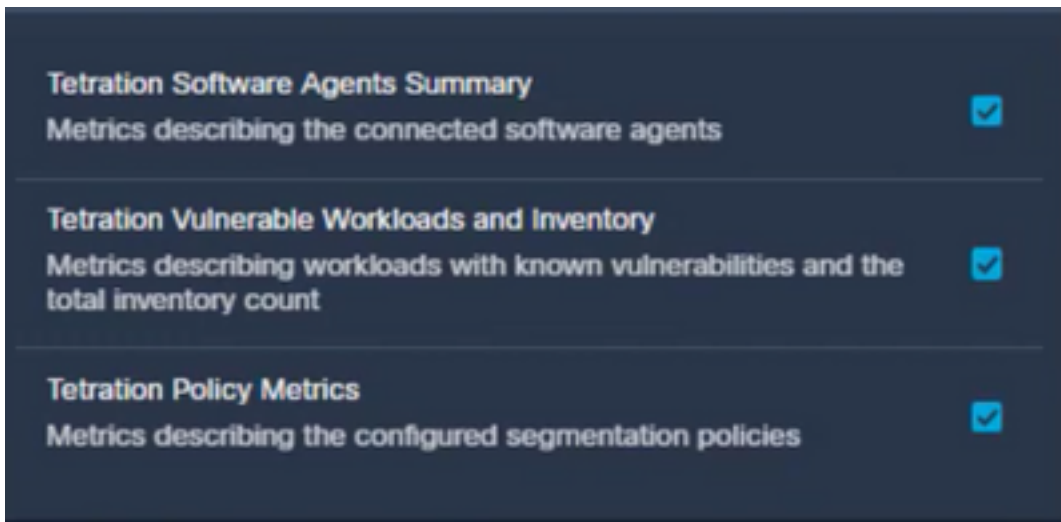
To add a Tetraton module, you must supply an authorization token and cluster.

1. Create a new set of Tetraton API connection credentials:

驗證

驗證Tetraton安全控制面板中的資訊是否顯示在SecureX控制面板中。

- 在SecureX上導航到控制面板
- 按一下New Dashboard並將其命名
- 選擇以前生成的Tetraton模組
- 選擇磁貼，對於本指南，所有磁貼均已新增
- 按一下 儲存



- 選擇Timeframe，並驗證Tetration中的資料是否以安全模式顯示



如果出現問題，並且未顯示任何資料，請檢視API金鑰是否正確應用。如果問題仍然存在，請與支援團隊聯絡。

影片指南