

Configurazione dell'integrazione SecureX con Tetration

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Genera le credenziali API nel dashboard di Tetration Security](#)

[Integrazione del modulo Tetration in SecureX](#)

[Verifica](#)

[Guida video](#)

Introduzione

Questo documento descrive il processo richiesto per integrare e verificare Cisco SecureX con Cisco Tetration.

Contributo di Juan Castellero e Uriel Torres, a cura di Jorge Navarrete, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco AMP for Endpoints
- Dashboard di Tetration Security
- Navigazione di base nella console SecureX
- Virtualizzazione delle immagini opzionale

Componenti usati

- Dashboard Tetration vSecurity
- account Tetration Administrator
- SecureX Console versione 1.54
- Account amministratore SecureX
- Microsoft Edge versione 84.0.522.52

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

La piattaforma Cisco Tetration risolve i problemi di sicurezza del carico di lavoro e delle applicazioni fornendo funzionalità di micro-segmentazione e rilevamento delle anomalie basate sul comportamento in infrastrutture cloud ibride. Il modulo Tetration fornisce 3 tessere.

Carichi di lavoro e inventario vulnerabili di Tetration: Metriche che descrivono i carichi di lavoro con vulnerabilità note e il conteggio totale dell'inventario.

Metriche dei criteri di Tetration: Metriche che descrivono i criteri di segmentazione configurati.

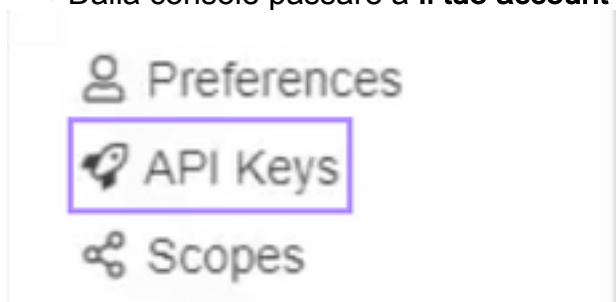
Riepilogo degli agenti software Tetration: Metriche che descrivono gli agenti software connessi.

Configurazione

Genera le credenziali API nel dashboard di Tetration Security

Nel dashboard di Tetration Security vengono create nuove API

- Accedere a **Tetration Security Dashboard** con privilegi di amministrazione.
- Dalla console passare a **Il tuo account > Chiavi API**.



- Fare clic su **Crea chiave API**
- Selezionare gli elementi seguenti: Gestione dei sensori software: API per configurare e monitorare lo stato dei sensori software. Ricerca flusso e inventario: API per eseguire query su flussi e articoli di magazzino nel cluster Tetration. Utenti, ruoli e gestione degli ambiti: API per la lettura/aggiunta/modifica/rimozione di utenti, ruoli e ambiti da parte dei proprietari degli ambiti radice. Gestione delle applicazioni e delle policy: API per la gestione delle applicazioni e l'applicazione dei criteri.

Create API Key

Description

SecureX

- 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
- User data upload: API for root scope owners to upload annotations for inventory items or upload good/bad file hashes
- Applications and policy management: API to manage applications and enforce policies
- External system integration: API to allow integration with external systems
- Tetration software download: API to download software packages for Tetration agents / virtual appliances

Create Cancel

Importante: recuperare questi valori prima di chiudere la finestra di dialogo. una volta chiusa la scheda, non è possibile recuperare le informazioni API generate.

- Salva le credenziali API
- Per creare il token di integrazione, accedere a tetration-securex.link/setup
- Introdurre l'URL Tetration e le credenziali API
- Fare clic su **Crea token**
- Copia il token di integrazione

Use this wizard to setup your Tetration and SecureX integration.

1. Enable the Tetration module in your SecureX console

2. Input your Tetration API credentials

Tetration URL *

https://[redacted].com/

API Key *

[redacted]

API Secret *

[redacted]

Create Token

3. Copy the generated Authentication token to the SecureX console

[redacted] Copy

Integrazione del modulo Tetration in SecureX

Integrare Tetration con SecureX per ottenere visibilità sullo stato del sistema Tetration, esporre carichi di lavoro vulnerabili, tenere traccia delle regole di segmentazione e reagire alle deviazioni di comportamento.

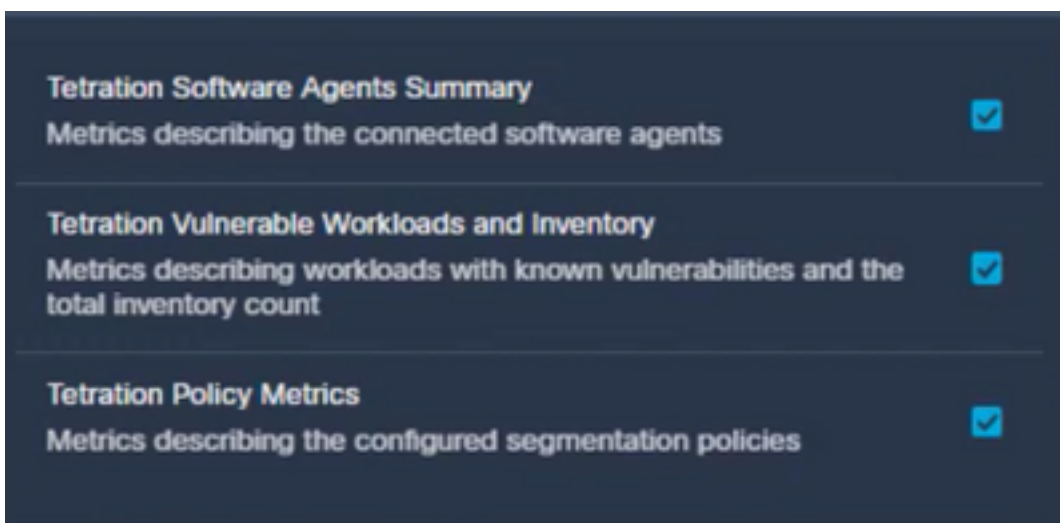
- Su console SecureX passare a **Integrations > Fare clic su Add New Module**
- Selezionare il modulo **Cisco Tetration** e fare clic su **Add New Module**

- Assegnare un nome al modulo
- Incollare il token e fare clic su **Salva**

Verifica

Verificare che le informazioni del dashboard Tetration Security vengano visualizzate nel dashboard SecureX.

- In SecureX passare a **Dashboard**
- Fare clic su **Nuovo dashboard** e denominarlo
- Selezionare il modulo Tetration generato in precedenza
- Selezionare i riquadri, per questa guida tutti sono aggiunti
- Clic **Salva**



- Selezionare l'**intervallo temporale** e verificare se i dati di Tetration vengono visualizzati in Secure (Protetto)



Se si verificano problemi e non vengono visualizzati dati, verificare che le chiavi API siano applicate correttamente. Se il problema persiste, rivolgersi al team di supporto.

Guida video