Risoluzione dei problemi relativi a XDR Device Insights e all'integrazione con Umbrella

Sommario

Introduzione

In questo documento viene descritto come configurare l'integrazione e la risoluzione dei problemi di XDR Device Insights e l'integrazione di Cisco Umbrella.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti.

- XDR
- Umbrella
- Conoscenze base delle API
- strumento API Postman

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware.

- XDR

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

XDR Device Insights fornisce una vista unificata dei dispositivi dell'organizzazione e consolida gli inventari da origini dati integrate.

Umbrella individua automaticamente l'infrastruttura degli utenti malintenzionati messa in scena per le minacce correnti e blocca proattivamente le richieste dannose prima che raggiungano la rete o gli endpoint di un'organizzazione. Grazie all'integrazione, è possibile arrestare le infezioni da malware in anticipo, identificare i dispositivi già infetti più rapidamente e prevenire l'esfiltrazione dei dati. L'integrazione fornisce una visibilità completa dell'attività su Internet tra tutte le sedi e gli utenti e consente di intervenire

con una risposta con due clic per bloccare rapidamente i domini. Sono supportate e collegate più funzioni Umbrella tramite chiavi API generate nella piattaforma Umbrella.

Per ulteriori informazioni sulla configurazione, esaminare i dettagli del modulo di integrazione.

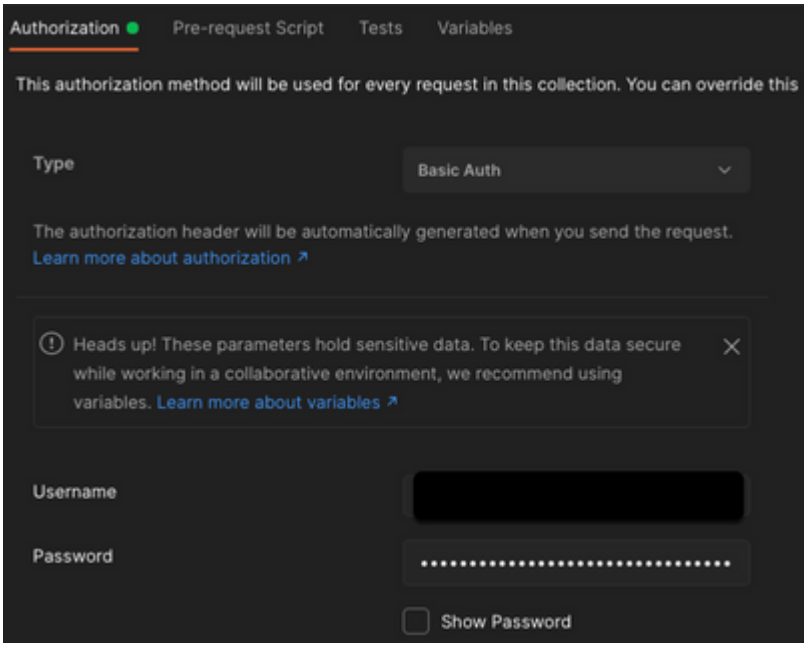
Risoluzione dei problemi

Per risolvere i problemi comuni relativi all'integrazione di XDR e Umbrella, è possibile verificare la connettività e le prestazioni dell'API.

Test di connettività con XDR Device Insights e Umbrella

Passaggio 1. È possibile selezionare Autori di **base** come metodo di autorizzazione, come illustrato nell'immagine.

> **Nota**: Postman non è uno strumento sviluppato da Cisco. Se hai domande sulla funzionalità dello strumento Postman, contatta l'Assistenza Postman.



Passaggio 2. Con questa chiamata API è possibile ottenere **computer in streaming** (il limite di pagina predefinito è 100 voci).

```
https://management.api.umbrella.com/v1/organizations/
```

```
    /roamingcomputers
```

Passaggio 3. In risposta alla prima chiamata, viene restituito il numero totale di oggetti. È possibile utilizzare i parametri limit e page per ottenere le pagine successive.

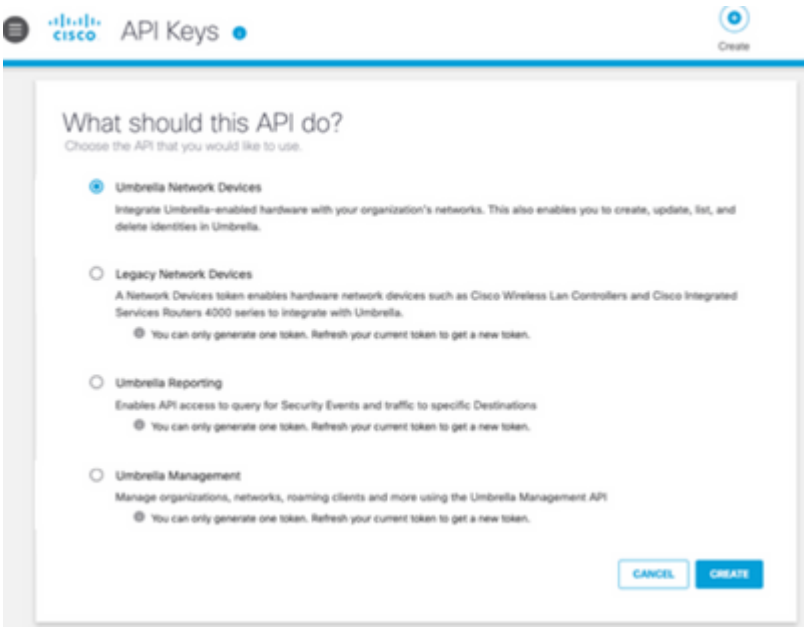
```
https://management.api.umbrella.com/v1/organizations/

      /roamingcomputers?limit=5&page=2
```

Chiave errata

XDR Device Insights non utilizza le stesse chiavi di XDR, quindi è necessario verificare e confermare che le chiavi configurate come chiavi API Umbrella siano corrette, come mostrato nell'immagine.

- Periferiche di rete Umbrella: API utilizzata per conoscere i criteri DNS
- Umbrella Management: API utilizzata per apprendere gli endpoint



Verifica

Una volta che Umbrella è stato aggiunto come origine a XDR Device Insights, è possibile visualizzare lo stato della connessione all'**API REST**.

- È possibile visualizzare la connessione **API REST** con stato verde
- Fare clic su **SYNC NOW** per attivare la sincronizzazione completa iniziale, come mostrato nell'immagine

Se il problema persiste con l'integrazione di Device Insights e Umbrella, raccogli i log HAR dal browser e contatta il supporto TAC per eseguire un'analisi più approfondita.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).