Guida all'integrazione di SecureX con Oracle Advanced Search

Sommario

Introduzione

Questo documento descrive il processo richiesto per integrare e verificare Cisco SecureX con Cisco Orbital Advanced Search.

Contributo di Yeraldin Sanchez e Uriel Torres, a cura di Jorge Navarrete, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco AMP for Endpoints Essentials con licenza Orbital, Advantage o Premier
- Cisco Orbital Advanced Search
- Navigazione di base nella console SecureX
- Virtualizzazione delle immagini opzionale

Componenti usati

- AMP for Endpoints Console versione 5.4.2020804
- Account amministratore AMP for Endpoints
- Orbital Advanced Search Console versione 1.7
- 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

Orbital è una funzionalità avanzata di Cisco AMP for Endpoints progettata per semplificare le indagini di sicurezza e la ricerca di minacce. Fornisce un'implementazione della potente tecnologia Osquery su ciascuno degli endpoint AMP. Orbital consente di creare query personalizzate per cercare informazioni di interesse nella rete, ma include anche oltre un centinaio di query predefinite, che consentono di eseguire rapidamente query complesse su uno o tutti gli endpoint.

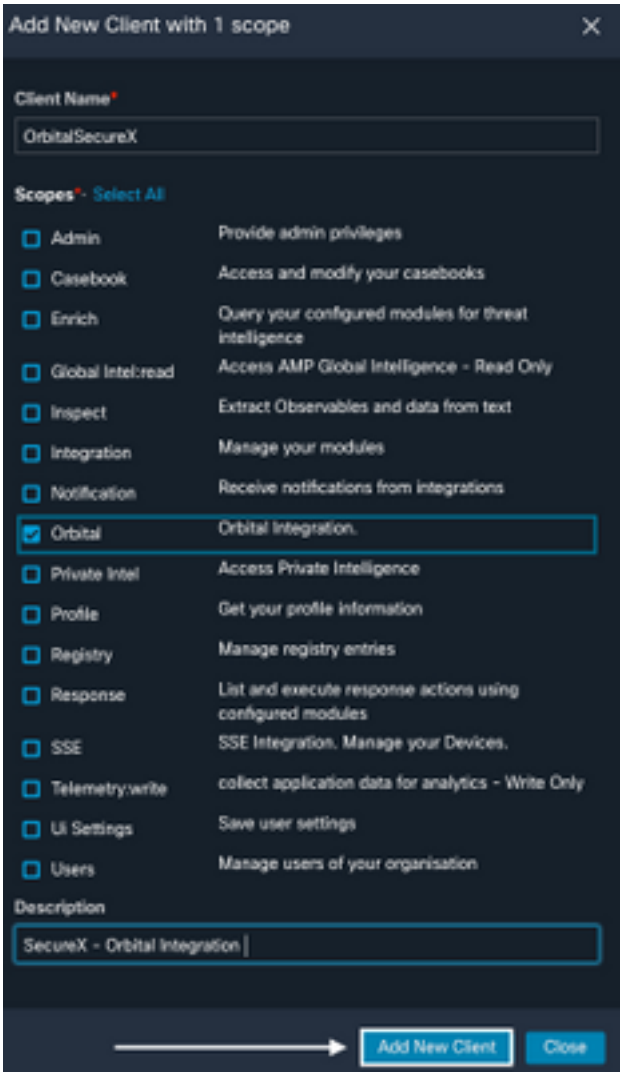
Il modulo Orbital dispone di 4 tessere che è possibile aggiungere a un dashboard SecureX.

- **Statistiche query organizzazione e risultati:**un set di metriche che descrive le query organizzazione e i risultati
- **Statistiche catalogo utente:** un set di metriche che descrive le query di catalogo utilizzate con maggiore frequenza per questo utente
- **Statistiche catalogo organizzazione:** una serie di metriche che descrivono le query di catalogo più utilizzate per questa organizzazione
- **Statistiche query utente e risultati:** un set di metriche che descrive le query utente e i risultati

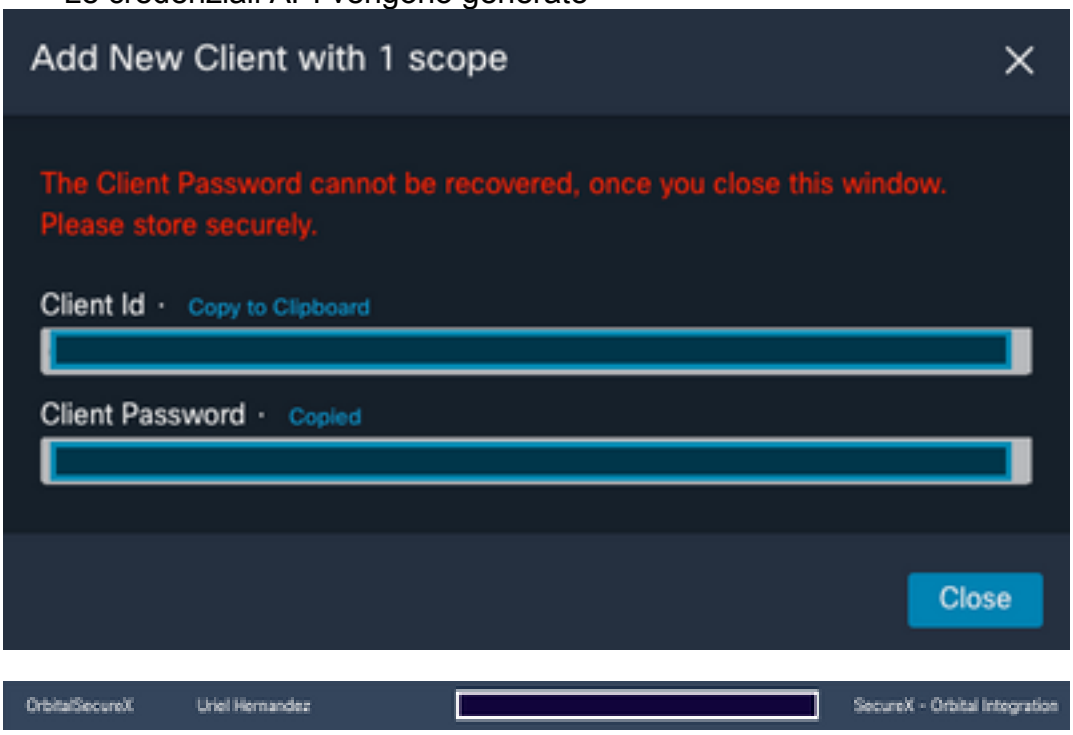
Configurazione

Genera le credenziali API nella console SecureX

- Accedere a SecureX
- Passare a **Integrazioni > Impostazioni > Client API**
- Fare clic su **Generate API Client**
- Assegnare un nome al client, selezionare **Orbital,** descrivere l'API e fare clic su **Aggiungi nuovo client**



- Le credenziali API vengono generate



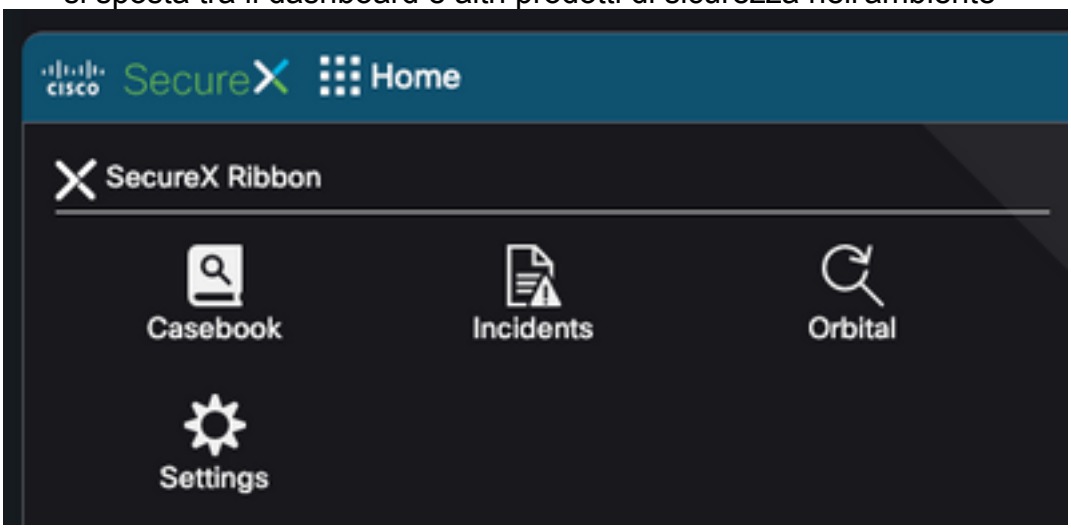
Nota: Queste informazioni sono disponibili solo in questa finestra. Salvare le credenziali in un file di backup.

Abilitare la barra multifunzione SecureX nella console AMP

SecureX è una console centralizzata e una serie distribuita di funzionalità che unificano la visibilità, consentono l'automazione, accelerano i flussi di lavoro di risposta agli incidenti e migliorano la ricerca di minacce. Queste funzionalità distribuite sono presentate sotto forma di applicazioni (app) e strumenti nella barra multifunzione SecureX, la barra multifunzione SecureX può essere abilitata nella console orbitale.

- Accedi a Console orbitale
- Sulla console orbitale
- Passare a **<Utente giovane> > Impostazioni**
- Abilitare la barra multifunzione SecureX

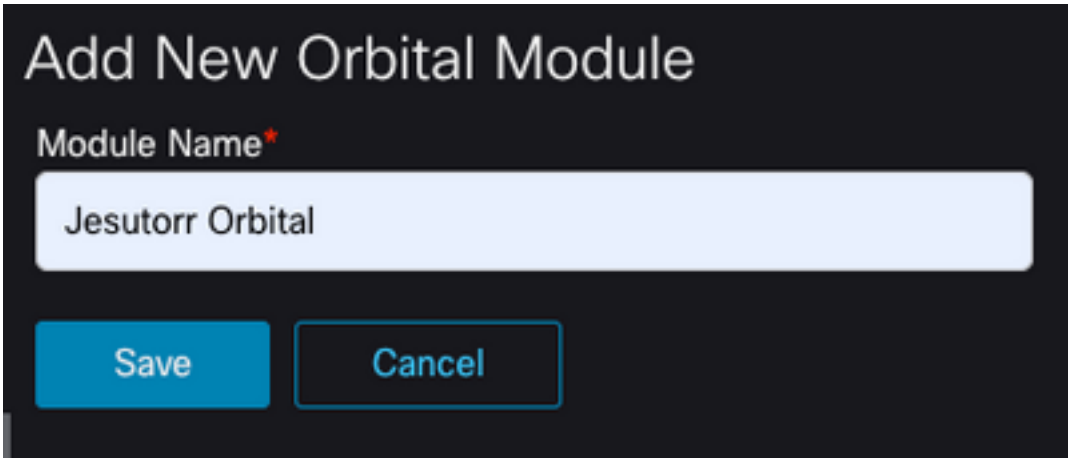
- La barra multifunzione si trova nella parte inferiore della pagina e viene mantenuta quando ci si sposta tra il dashboard e altri prodotti di sicurezza nell'ambiente



Integrazione del modulo orbitale in SecureX

Orbital può arricchire le informazioni presentate nel grafico delle relazioni di risposta alle minacce se si entra in Orbital per eseguire query e raccogliere informazioni aggiuntive su host, IP, IP4, IP6, MAC e OS, ecc. L'app Orbital è disponibile sulla barra multifunzione SecureX e consente di eseguire una query in tempo reale. È inoltre possibile visualizzare le metriche e le query recenti nel riquadro di destra.

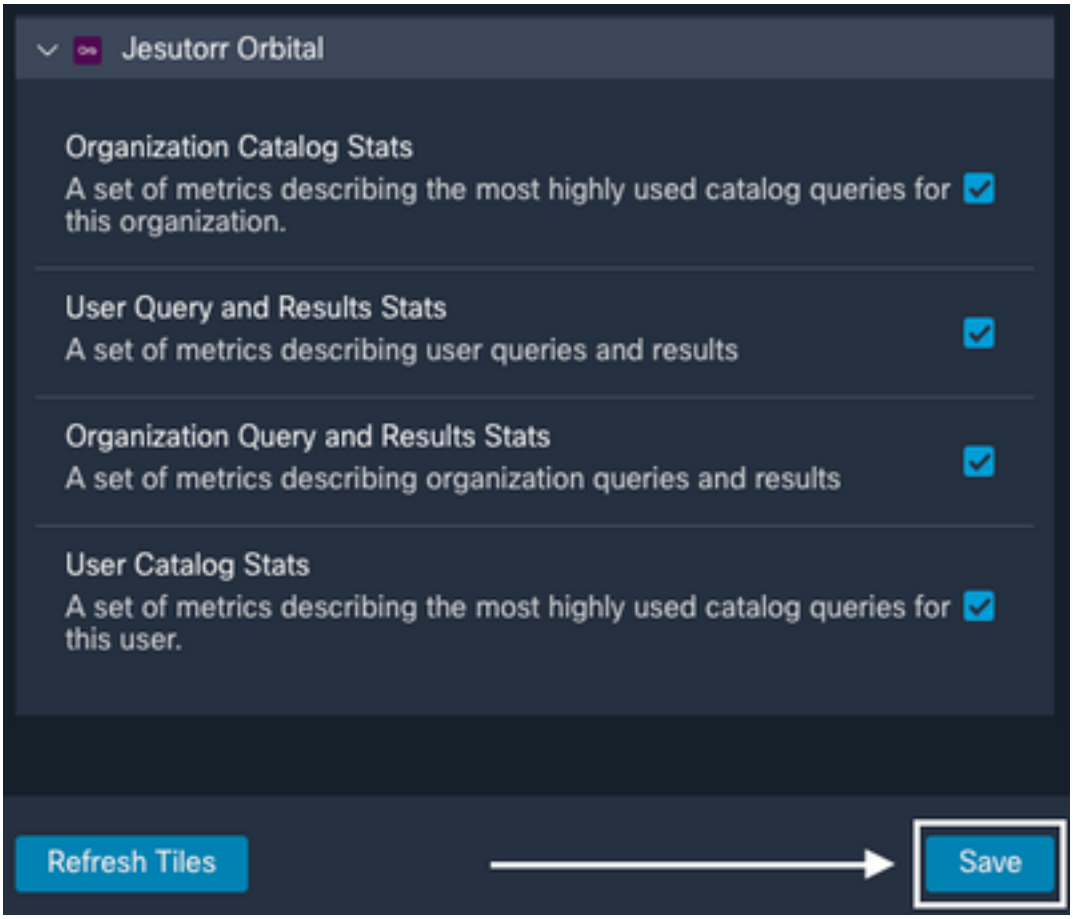
- Su SecureX
- Passare a **Integrazioni > Aggiungi nuovo modulo**
- Selezionare Orbital e fare clic su **Add New Module**
- Assegnare un nome al modulo e fare clic su **Salva**



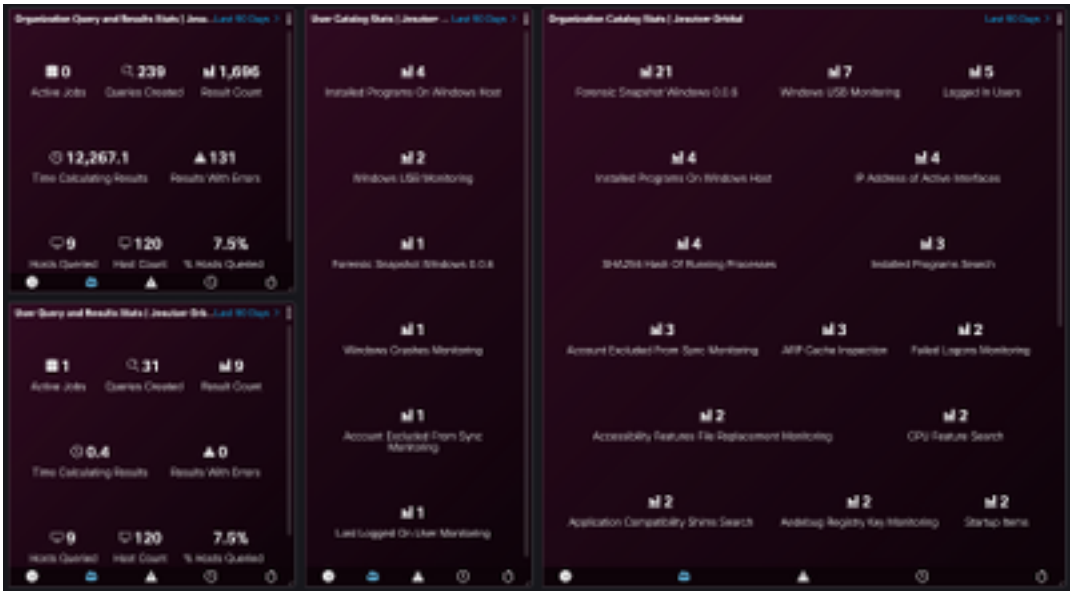
Verifica

Verificare che le informazioni di Oracle Advanced Set Console siano visualizzate nel dashboard SecureX.

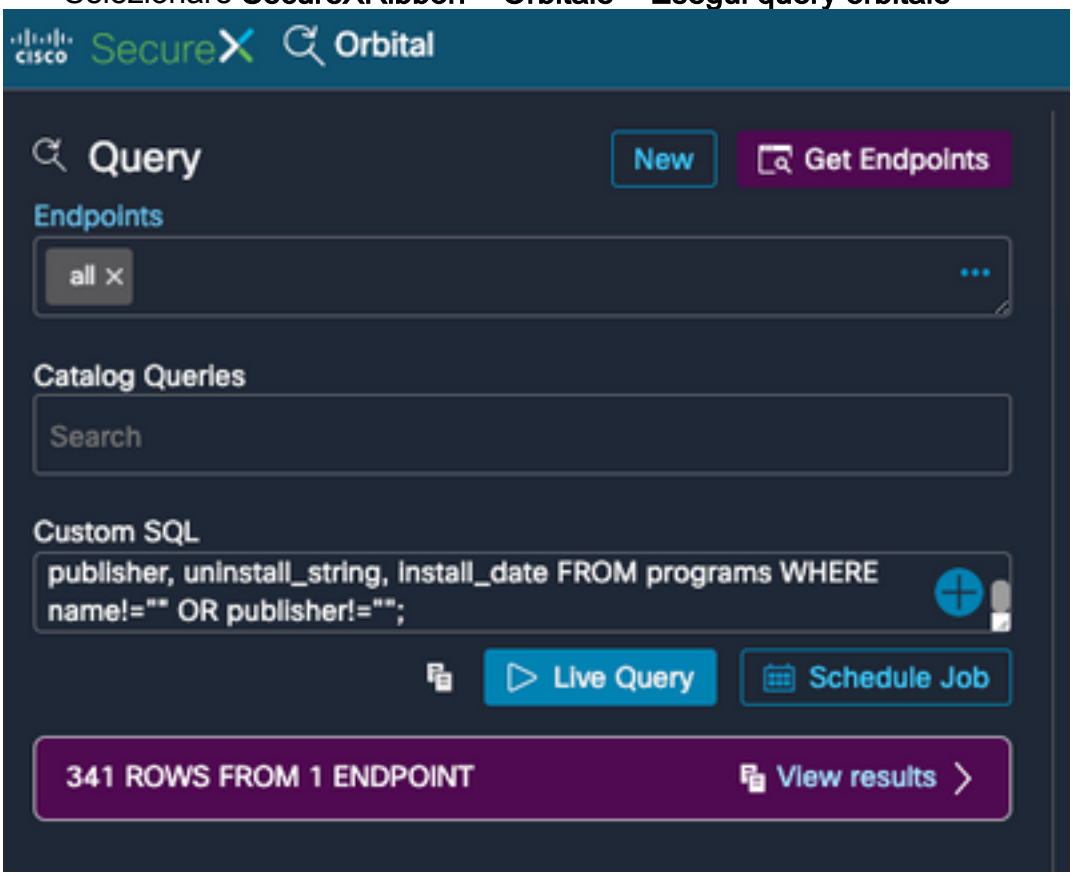
- In SecureX passare a **Dashboard**
- Fare clic **su Nuovo dashboard** e denominarlo
- Selezionare il modulo orbitale generato in precedenza
- Selezionare i riquadri, per questa guida tutti sono aggiunti
- Fare clic su Salva.



- Selezionare l'**intervallo di tempo** e verificare se i dati di Orbital vengono visualizzati in SecureX



- Èpossibile avviare un'indagine dalla barra multifunzione SecureX
- Selezionare **SecureXRibbon > Orbitale > Esegui query orbitale**



Informazioni correlate

- Qui sono disponibili video su come configurare le integrazioni dei prodotti.
- Documentazione e supporto tecnico – Cisco Systems

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).