Überprüfen Sie den Supportbereich für SecureX.

Inhalt

Einleitung

In diesem Dokument wird der Support-Umfang für SecureX von verschiedenen Cisco Organisationen beschrieben.

Hintergrund

Ziel des Dokuments ist es, die verschiedenen Services und Supportleistungen von Cisco im Zusammenhang mit SecureX zu erläutern und Erwartungen zu verdeutlichen.

Berechtigung

Alle Mitarbeiter mit einem aktiven Vertrag für ein Cisco Security-Produkt sind berechtigt, ein Ticket beim TAC für SecureX-Support zu erstellen. Im Abschnitt "SecureX" finden Sie die Informationen, die vom Berechtigungsteam für die Validierung und das Erstellen von Tickets mit dem TAC verwendet wurden, und folgende Meldung:

> The customer is entitled if a contract covers any of the security solutions integrated into SecureX, like AMP for Endpoints, Cisco Umbrella, Email Security, Web Security, Stealthwatch, DUO, Tetration, Meraki, and ThreatGRID. For Umbrella, DUO, and Meraki that do not operate within CSOne, if the customer is not having any other integrated products with entitlement, choose “SecureX” as a bypass option.

SecureX Single Sign-On

Cisco TAC unterstützt alle Probleme im Zusammenhang mit SecureX Single Sign-On, Anmeldung oder Account Management. Für alle Anfragen im Zusammenhang mit der Integration einer Drittanbieter-ID (Identity Provider) verwenden Sie bitte dieses Handbuch:

[Cisco SecureX Sign-On Integrationsleitfaden für Identitätsanbieter von Drittanbietern](#)

Um eine METADATA-Datei zu erstellen, gehen Sie folgendermaßen vor:

[Wie laden wir die IDP.XML Metadatendatei von einer SAML Template App herunter?](#)

Dashboard, Kacheln und Analyseprobleme für die Reaktion auf Bedrohungen

Das Cisco TAC unterstützt alle Probleme im Zusammenhang mit der Erstellung von Dashboards und Kacheln, der Datenbestückung und der Modulintegration auf der SecureX-Konsole. Bei Untersuchungen zur Reaktion auf Bedrohungen kann Ihnen das Cisco TAC helfen, alle mit den integrierten Produkten durchgeführten Untersuchungen zu verstehen oder zu klären und bei Problemen, Fehlern oder Warnungen, die Teil der Untersuchung sein können, behilflich zu sein.

Integrationsprobleme bei Cisco Security-Produkten

Das Cisco TAC bietet umfassenden Support bei Problemen im Zusammenhang mit den in SecureX integrierten Cisco Security-Produkten. Dies gilt für Geräte am Standort mit indirekter Integration in SecureX (Security Services Exchange (SSE) und Cisco Security Services Proxy (CSSP)-Server) oder eine direkte (Cloud-to-Cloud) Integration für ein Cisco Security-Produkt.

Probleme mit der Integration von Drittanbietern

Bei Integrationsproblemen mit Drittanbietern überprüft das Cisco TAC, ob die für die Integration erforderlichen APIs mit allen Parametern und Anforderungen der Dokumentation zu den SecureX Integrationsmodulen korrekt konfiguriert sind.

Wenn die Probleme nach der Validierung der API-Parameter und -Anforderungen weiterhin bestehen, muss der Support des Drittanbieterprodukts in Anspruch genommen werden, um das Problem gemeinsam mit dem TAC lösen zu können.

APIs und benutzerdefinierte Scripts

Cisco TAC unterstützt die korrekte Funktionsweise dokumentierter APIs. TAC unterstützt jedoch nicht die von Benutzern angewendete benutzerdefinierte Verwendung, wie z. B. die Verwendung einer API in einem Python-Skript.

Wenden Sie sich für individuelle Anfragen an Ihren Cisco Account Manager, um Informationen über dieAbonnementservices, die vom Cisco Professional Services Team (PS) bereitgestellt werden.

Wenn Sie Fragen zum TAC Scope-Support für SecureX haben, senden Sie eine E-Mail an ats-cxtls@cisco.com.