Schritte zur Integration von Cisco Email Threat Defense (ETD) in Cisco Secure Access:

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Integration von Cisco Email Threat Defense (ETD) in Cisco Secure Access (SA) für E-Mail DLP im ETD SMTP Inline-Modus erläutert. Auf diese Weise wird sichergestellt, dass alle ausgehenden E-Mails, die über ETD geleitet werden, mithilfe von Cisco Secure Access (SA) auf DLP gescannt werden.

Überblick

In der verteilten Arbeitsumgebung von heute sind E-Mails nach wie vor das wichtigste Kommunikationstool für Unternehmen und damit das häufigste Ziel von Cyberangriffen und Datendiebstahl. Um diesen neuen Herausforderungen zu begegnen, bietet Cisco einen umfassenden Ansatz für E-Mail-Sicherheit durch E-Mail-Bedrohungsschutz (ETD) und Schutz vor E-Mail-Datenverlust (DLP).

Durch die Kombination der Bedrohungserkennungsfunktionen von Cisco Email Threat Defense mit dem zuverlässigen Datenschutz von Secure Access Email DLP können Unternehmen eine mehrschichtige Abwehrstrategie entwickeln. Dieser Ansatz schützt nicht nur den Posteingang vor externen Akteuren, sondern stellt auch sicher, dass vertrauliche Unternehmensdaten unter

strenger Kontrolle bleiben, unabhängig davon, wo sich der Benutzer befindet oder wie er auf seine E-Mails zugreift.

Voraussetzungen

Zugriff auf die Konsole unten.

1. Cisco Email Threat Defense Console (ETD) im Inline-Modus

   Die ETD-Konsole dient als zentrale Managementebene für Ihren E-Mail-Sicherheitsstatus. Der Zugriff auf diese Konsole ist der erste Schritt bei der Konfiguration Ihrer Umgebung zum Schutz vor komplexen Bedrohungen.

   - Bedeutung des "Inline Mode":Wenn ETD im Inline Mode konfiguriert ist, fungiert es als Mail Transfer Agent (MTA) oder als direkte Integration, die im Pfad des E-Mail-Flusses stattfindet. Auf diese Weise kann das System Nachrichten überprüfen, blockieren oder ändern, bevor sie an den Posteingang des Empfängers gesendet werden.
2. Cisco Secure Access Console (SA)

Cisco Secure Access ist die einheitliche, über die Cloud bereitgestellte Sicherheitsplattform, die verschiedene Sicherheitsservices, einschließlich Data Loss Prevention (DLP), in einer einheitlichen Architektur integriert.

- Warum die SA-Konsole erforderlich ist:Die Secure Access-Konsole ist der zentrale Orchestrierungspunkt für die Sicherheitsrichtlinien Ihres Unternehmens. Während der bedrohungsspezifische E-Mail-Fluss von ETD verwaltet wird, können Sie mit der Konsole für sicheren Zugriff die umfassenderen DLP-Richtlinien definieren, die festlegen, wie sensible Daten im gesamten Unternehmen identifiziert und behandelt werden.
- Konsolenrolle:Diese Konsole ermöglicht es Administratoren, Datenklassifizierungsregeln zu erstellen und anzuwenden (z. B. zur Identifizierung von PII, Kreditkartennummern oder internen Projektcodes). Mit dem Zugriff auf die SA-Konsole können Sie sicherstellen, dass Ihre DLP-E-Mail-Richtlinien mit Ihrer allgemeinen Sicherheitsstrategie synchronisiert sind, sodass eine konsistente Durchsetzung über beide E-Mail-Traffics hinweg möglich ist.

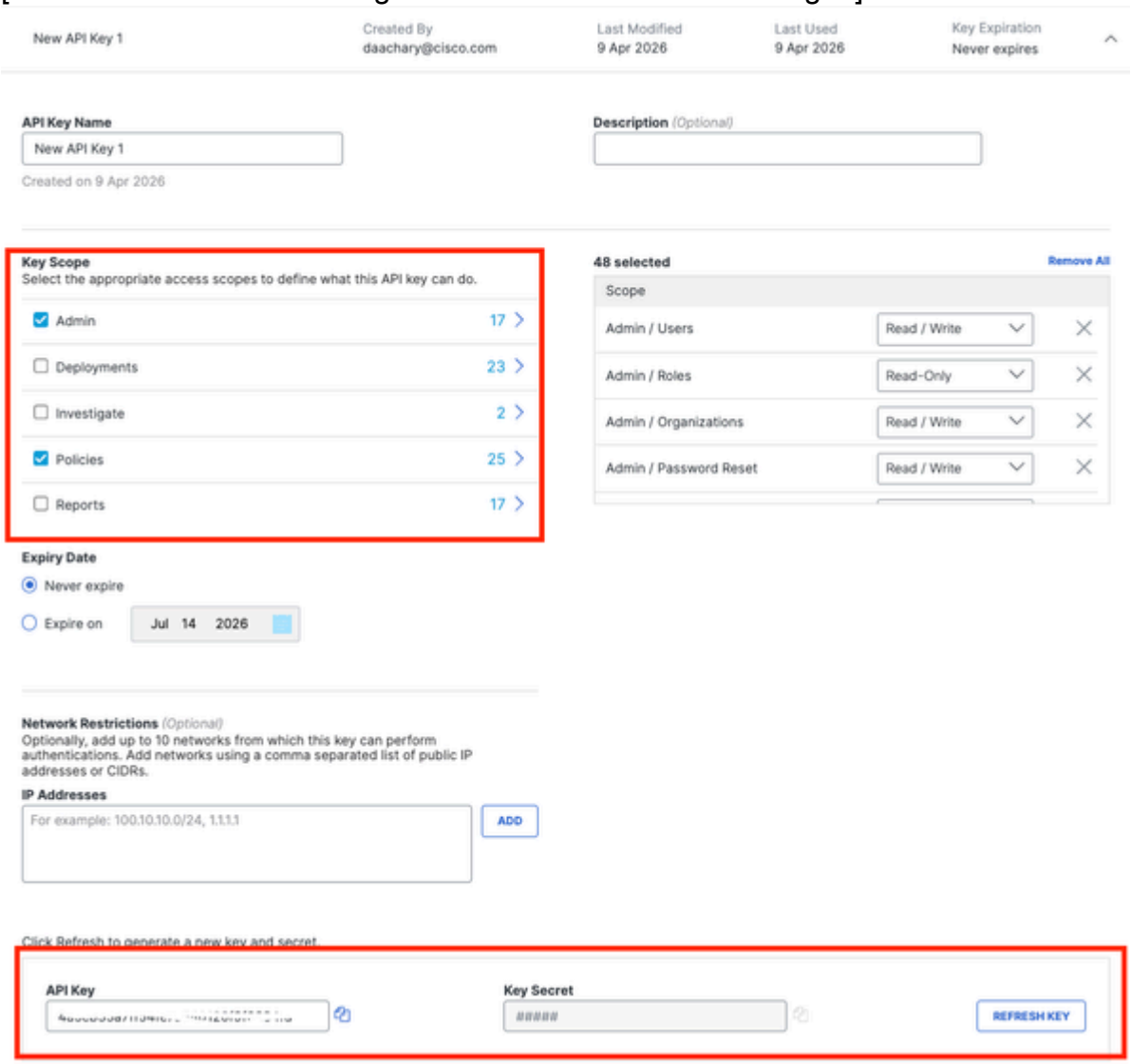
Konfigurieren

Integrationsschritte

Schritt 1: API-Anmeldeinformationen in Cisco Secure Access generieren

Zu Beginn müssen Sie die API-Anmeldeinformationen in der Konsole für sicheren Zugriff generieren, um die Verbindung zu autorisieren.

1. Melden Sie sich beim Cisco Secure Access Dashboard an.
2. Navigieren Sie zuAdmin>API Keys.
3. Wählen Sie die Option zum Erstellen eines neuen API-Schlüssels aus.
4. Weisen Sie dem Schlüssel die folgenden Bereiche zu:AdminandPolicy.
    - [Screenshot: Schlüsselkonfiguration der API für sicheren Zugriff]
    -



Phase 2: Ablauf von Schlüsseln konfigurieren

Definieren Sie den Lebenszyklus Ihres API-Schlüssels basierend auf den Sicherheitsrichtlinien Ihres Unternehmens.

- Option 1: Läuft nie ab - Unterbrechungsfreier Service ohne manuelle Rotation
- Option 2: Spezifisches Datum: Legt einen definierten Ablaufzeitplan fest.
    - Wichtiger Hinweis: Wenn Sie ein Ablaufdatum festlegen, müssen Sie einen Rotationsprozess einplanen. Sie müssen die API-Schlüssel in der ETD-Konsole vor dem Ablaufdatum neu konfigurieren, um eine Unterbrechung Ihrer DLP-Dienste zu verhindern.

Schritt 3: Schützen Sie Ihre Anmeldeinformationen

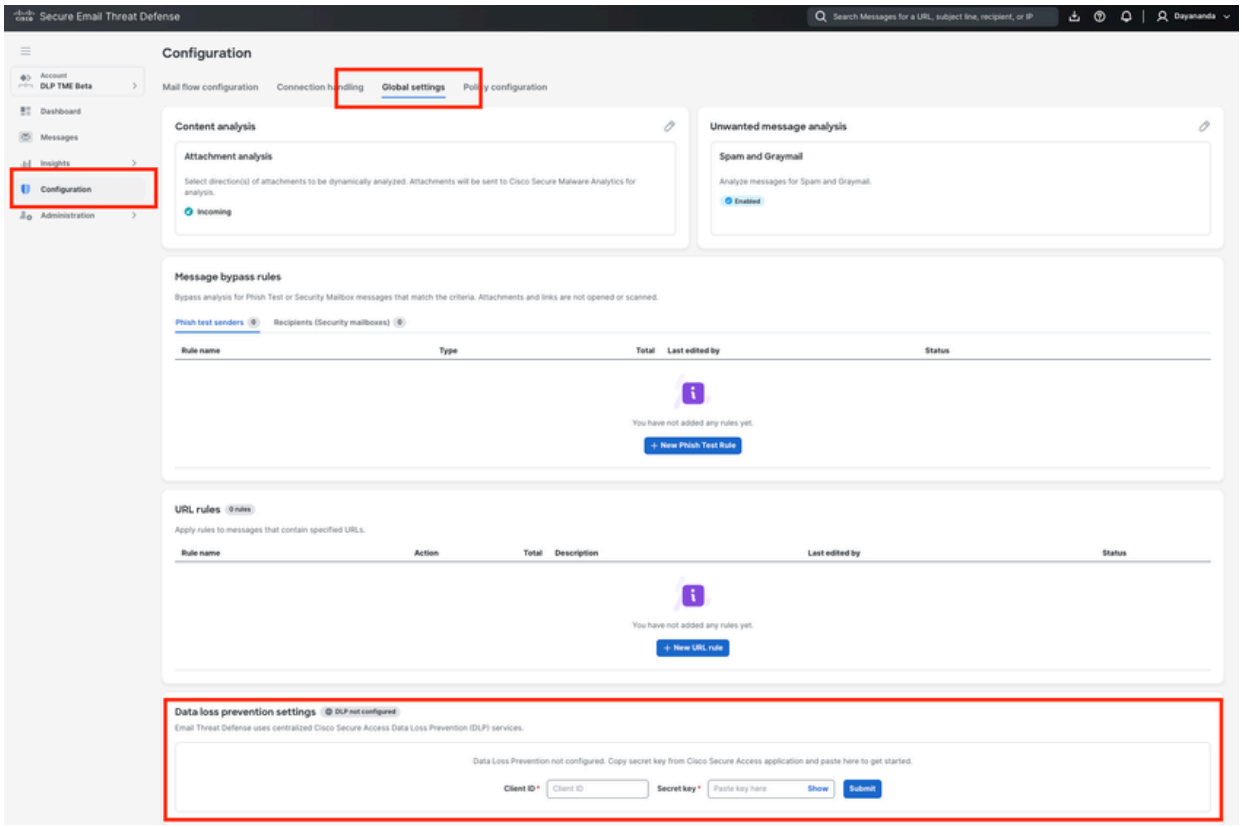
Sobald der Schlüssel generiert wurde, zeigt das System den API-Schlüssel und den Schlüsselgeheimnis an.

- Aktion: Kopieren Sie diese Anmeldeinformationen, und speichern Sie sie an einem sicheren Ort (z. B. einem Passwort-Manager).
- Warnung: Der Schlüsselsekretär wird nicht angezeigt, wenn Sie diesen Bildschirm verlassen. Wenn Sie verloren gehen, müssen Sie ein neues Schlüsselpaar generieren.

Schritt 4: Zugriff auf die ETD-Konfiguration

Fahren Sie mit gesicherten Anmeldeinformationen zur ETD-Konsole fort, um die Verknüpfung abzuschließen.

1. Melden Sie sich bei der Cisco ETD-Konsole an.
2. Navigieren Sie zuKonfiguration>Globale Einstellungen.
    - [Screenshot: Navigation zu globalen ETD-Einstellungen]

- 

Schritt 5: Abschließen der Integration

Schließen Sie den Handshake ab, indem Sie die von Secure Access erhaltenen Anmeldeinformationen eingeben.

1. Suchen Sie im Menü Globale Einstellungen den Abschnitt Schutz vor Datenverlust (DLP).
2. Geben Sie die Client-ID (API-Schlüssel) und den geheimen Schlüssel (Key Secret) ein, die Sie in Schritt 3 gespeichert haben.
3. Speichern Sie Ihre Änderungen.

Nach der erfolgreichen Validierung ist die Integration zwischen Cisco ETD und Cisco Secure Access abgeschlossen, und Ihre DLP-Richtlinien können für den gesamten E-Mail-Verkehr durchgesetzt werden.

Die Integration von ETD und Secure Access ist damit abgeschlossen.
HINWEIS: Informationen zum Erstellen einer DLP-Richtlinie in Cisco Secure Access for Email DLP finden Sie unter "How to configure an Email DLP policy in Cisco Secure Access (SA) and Cisco Email Threat Defense (ETD)".

Hinweise zur Fehlerbehebung

Wenn während oder nach dem Integrationsprozess Probleme auftreten, überprüfen Sie die folgenden gängigen Szenarien und Schritte zur Problembehebung:

1. API-Anmeldeinformationen in ETD nicht akzeptiert

- Symptom: Bei Eingabe der Client-ID und des geheimen Schlüssels in ETD gibt das System einen Authentifizierungsfehler zurück.
- Auflösung:
  - Überprüfen Sie, ob der API-Schlüssel mit den exakt erforderlichen Bereichen "Admin" und "Policy" erstellt wurde. Wenn andere Bereiche ausgewählt wurden oder diese fehlten, schlägt die Verbindung fehl.
  - Stellen Sie sicher, dass beim Einfügen der Client-ID oder des geheimen Schlüssels in die ETD-Konsole keine vor- oder nachgestellten Leerzeichen versehentlich kopiert werden.

2. Verlorener oder vergessener Schlüssel Geheimnis

- Symptom: Sie haben den Erstellungsbildschirm der API für sicheren Zugriff verlassen und können den Schlüssel-Schlüssel nicht mehr anzeigen.
- Auflösung: Aus Sicherheitsgründen wird der Schlüssel-Schlüssel nur einmal zum Zeitpunkt der Erstellung angezeigt. Wenn Sie sie nicht sicher gespeichert haben, müssen Sie den unvollständigen API-Schlüssel in Secure Access löschen und einen neuen generieren.

3. SvD-Policys werden für E-Mail-Verkehr nicht durchgesetzt

- Symptom: Die Integration wird als erfolgreich angezeigt, aber konfigurierte SvD-Richtlinien fangen oder blockieren keine vertraulichen E-Mails.
- Auflösung:
  - API-Ablaufdatum überprüfen: Wenn Sie "Wählen Sie ein bestimmtes Datum aus" für das Ablaufdatum des API-Schlüssels ausgewählt haben (Schritt 2), stellen Sie sicher, dass der Schlüssel nicht abgelaufen ist. Wenn dies der Fall ist, müssen Sie ein neues Schlüsselpaar generieren und anwenden.
  - Überprüfen des ETD-Bereitstellungsmodus: Stellen Sie sicher, dass Cisco ETD im Inline-Modus bereitgestellt wird. ETD muss sich im Direktmailpfad befinden, um Nachrichten aktiv basierend auf SvD-Verdicts des sicheren Zugriffs zu blockieren oder zu ändern.
  - Synchronisierungszeit: Lassen Sie den Backend-Systemen nach der Erstintegration einige Minuten Zeit, um Richtlinien zu synchronisieren, bevor Sie SvD-Regeln testen.

4. Service-Unterbrechung nach einer Phase der Stabilität

- Symptom:Die DLP-Durchsetzung funktioniert plötzlich nicht mehr, nachdem sie monatelang ordnungsgemäß funktioniert hat.
- Auflösung: Dies wird in der Regel durch einen abgelaufenen API-Schlüssel verursacht. Navigieren Sie zuAdmin -> API-Schlüssel in Cisco Secure Access, um den Status des Schlüssels für ETD zu überprüfen. Implementieren Sie einen Schlüsselrotationsprozess, um die Anmeldeinformationen in ETD zu aktualisieren, bevor das Ablaufdatum erreicht wird.

Zusammenfassung

Die Integration von Cisco Email Threat Defense (ETD) mit Cisco Secure Access (SA) ist ein wichtiger Schritt auf dem Weg zu einer einheitlichen Strategie zum Schutz vor Datenverlust (DLP). Durch die Generierung eines sicheren API-Schlüssels mit "Admin"- und "Policy"-Bereichen in der Secure Access-Konsole und die Konfiguration dieser Anmeldeinformationen in den globalen ETD-Einstellungen erstellen Administratoren eine nahtlose Kommunikationsbrücke zwischen den beiden Plattformen.

Nach Abschluss dieses Handshakes kann ETD E-Mail-Metadaten aktiv an die Secure Access DLP-Engine übergeben. So können Sie alle Datenschutzrichtlinien über ein zentrales Dashboard (Secure Access) verwalten und gleichzeitig umfassenden Überblick über den E-Mail-Verkehr haben.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.