Passaggi per integrare Cisco Email Threat Defense (ETD) con Cisco Secure Access:

Sommario

Introduzione

In questo documento viene illustrata la procedura per integrare Cisco Email Threat Defense (ETD) con Cisco Secure Access (SA) per i pacchetti di prevenzione della perdita dei dati tramite posta elettronica in modalità in linea SMTP ETD. In questo modo, tutti i messaggi e-mail in uscita che passano attraverso ETD verranno analizzati alla ricerca di DLP con l'aiuto di Cisco Secure Access (SA).

Panoramica

Negli ambienti di lavoro distribuiti di oggi, la posta elettronica rimane lo strumento di comunicazione principale per le aziende e, di conseguenza, il bersaglio più frequente di attacchi informatici ed esfiltrazione di dati. Per affrontare queste sfide in continua evoluzione, Cisco offre un approccio completo alla sicurezza della posta elettronica tramite Email Threat Defense (ETD) e Secure Access Email Data Loss Prevention (DLP).

Combinando le funzionalità di rilevamento delle minacce di Cisco Email Threat Defense con la solida protezione dei dati di Secure Access Email DLP, le organizzazioni possono stabilire una strategia di difesa multilivello. Questo approccio non solo protegge la casella di posta dagli attori

esterni, ma assicura anche che i dati aziendali sensibili rimangano sotto stretto controllo, indipendentemente dalla posizione dell'utente o dalla modalità di accesso alla posta elettronica.

Prerequisiti

Accedere alla console sottostante.

1. Cisco Email Threat Defense Console (ETD) in modalità inline.

   La console ETD funge da piano di gestione centralizzata per la postura di sicurezza della posta elettronica. L'accesso a questa console è il primo passo nella configurazione dell'ambiente per la protezione da minacce avanzate.

   - Perché la modalità in linea è importante:quando ETD è configurato in modalità in linea, agisce come agente di trasferimento della posta (MTA) o come integrazione diretta che risiede nel percorso del flusso di posta elettronica. Ciò consente al sistema di ispezionare, bloccare o modificare i messaggi prima che vengano recapitati nella cartella Posta in arrivo del destinatario.
2. Cisco Secure Access Console (SA)

Cisco Secure Access è la piattaforma di sicurezza unificata basata su cloud che integra diversi servizi di sicurezza, tra cui Data Loss Prevention (DLP), in un'unica architettura coesiva.

- Perché è necessaria la console SA:la console Secure Access è l'hub di orchestrazione per i criteri di sicurezza dell'organizzazione. Mentre ETD gestisce il flusso e-mail specifico della minaccia, sulla console Secure Access è possibile definire criteri DLP di più ampio respiro che determinano il modo in cui i dati sensibili vengono identificati e gestiti in tutta l'azienda.
- Ruolo della console: questa console consente agli amministratori di creare e applicare regole di classificazione dei dati (ad esempio, identificazione di PII, numeri di carta di credito o codici di progetto interni). Accedendo alla console dell'amministratore di sistema, è possibile garantire la sincronizzazione dei criteri di prevenzione della perdita dei dati e-mail con la strategia di sicurezza generale, consentendo un'applicazione coerente del traffico e-mail.

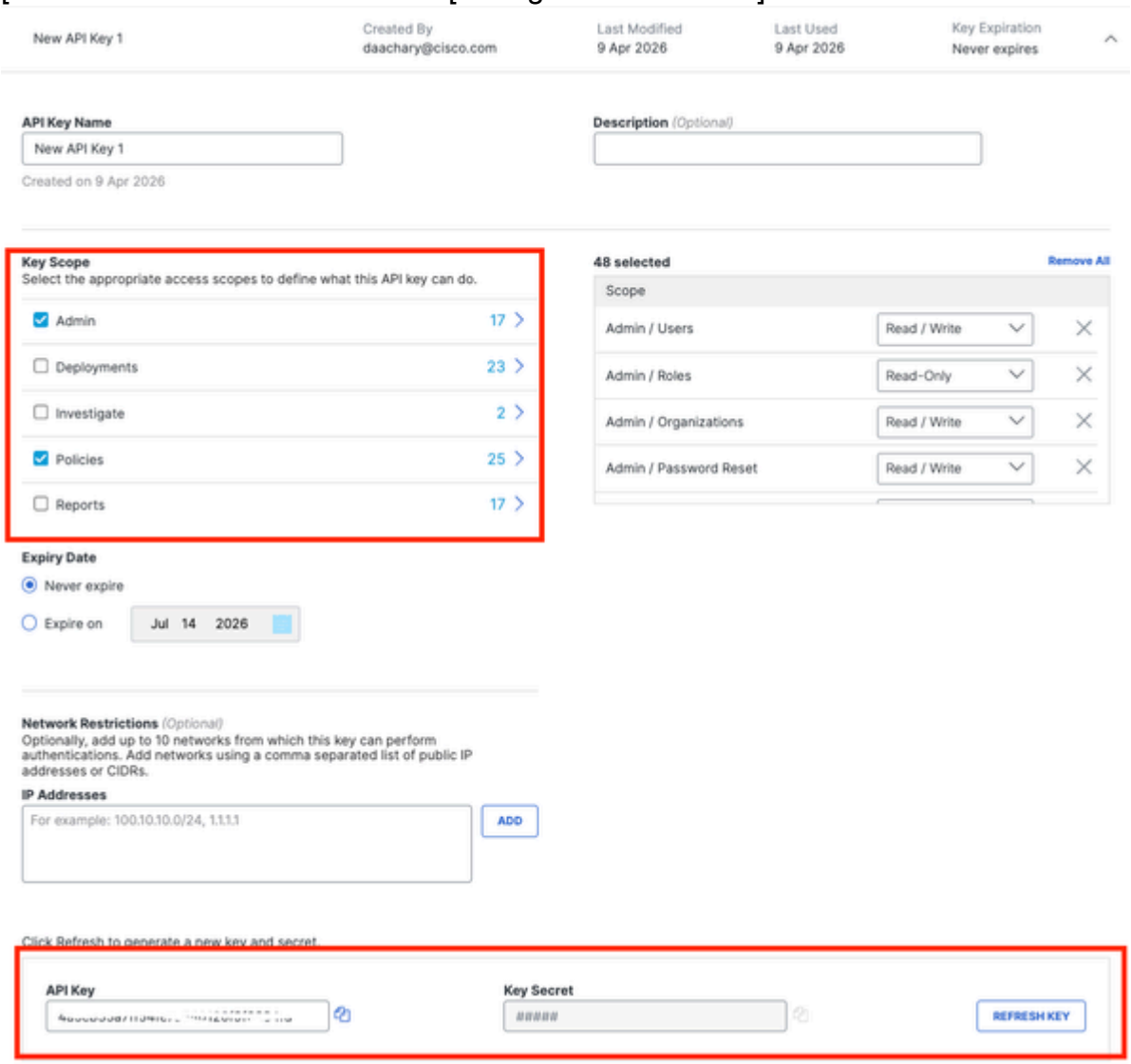
Configurazione

Fasi di integrazione

Passaggio 1: Genera credenziali API in Cisco Secure Access

Per iniziare, è necessario generare le credenziali API necessarie all'interno della console di accesso protetto per autorizzare la connessione.

1. Accedere a Cisco Secure Access dashboard.
2. Selezionare Admin>API Keys.
3. Selezionare l'opzione per creare una nuova chiave API.
4. Assegnare gli ambiti seguenti alla chiave:AdminandPolicy.
    - [Screenshot: Secure Access API [Configurazione chiave]
    -



Passaggio 2: Configura scadenza chiave

Definire il ciclo di vita della chiave API in base ai criteri di sicurezza dell'organizzazione.

- Opzione 1: Nessuna scadenza: fornisce un servizio ininterrotto senza rotazione manuale.
- Opzione 2: Data specifica: imposta una cronologia di scadenza definita.
    - Nota importante: se si sceglie di impostare una data di scadenza, assicurarsi di pianificare un processo di rotazione. È necessario riconfigurare le chiavi API nella console ETD prima della data di scadenza per evitare interruzioni nei servizi DLP.

Passaggio 3: Protezione delle credenziali

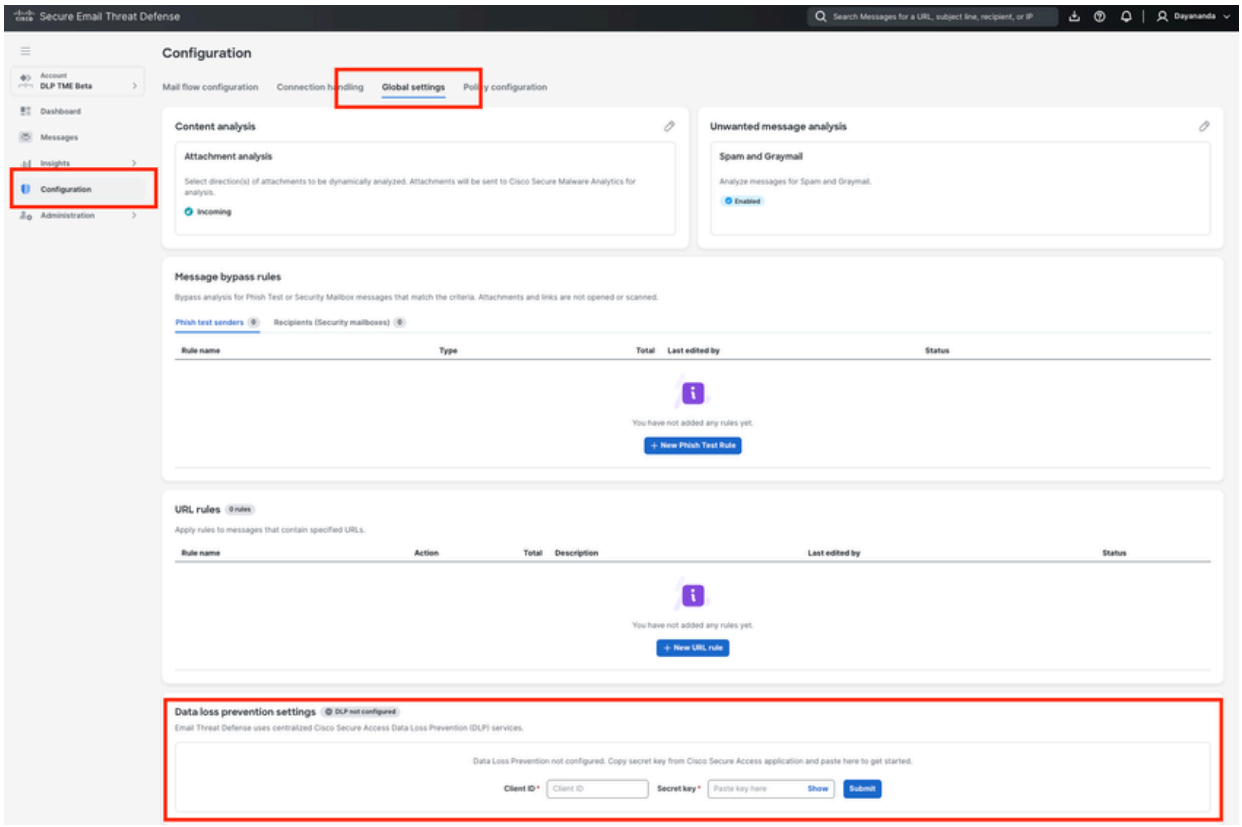
Una volta generata la chiave, il sistema visualizzerà la chiave API e il segreto della chiave.

- Azione: copiare e memorizzare le credenziali in un percorso sicuro, ad esempio un password manager.
- Avviso: il segreto della chiave non sarà visibile dopo l'uscita da questa schermata. In caso di perdita, sarà necessario generare una nuova coppia di chiavi.

Passaggio 4: Accesso alla configurazione ETD

Con le credenziali protette, passare alla console ETD per completare il collegamento.

1. Accedere alla console Cisco ETD.
2. Passare a Configurazione>Impostazioni globali.
    - [Screenshot: ETD [Navigazione impostazioni globali]

- 

Passaggio 5: Completa integrazione

Completare l'handshake immettendo le credenziali ottenute da Secure Access.

1. All'interno del menu Impostazioni globali, individuare la sezione DLP (Data Loss Prevention).
2. Immettere l'ID client (chiave API) e la chiave segreta (chiave segreta) salvati nel passaggio 3.
3. Salvare le modifiche.

Dopo la convalida, l'integrazione tra Cisco ETD e Cisco Secure Access è completata e i criteri di prevenzione della perdita dei dati saranno pronti per essere applicati al traffico e-mail.

Ora l'integrazione di ETD e Secure Access è completata.
NOTA: Per creare i criteri di prevenzione della perdita dei dati in Cisco Secure Access (SA) e Cisco Email Threat Defense (ETD), consultare il documento sulla "Configurazione dei criteri di prevenzione della perdita dei dati di posta elettronica in Cisco Secure Access for Email DLP".

Note sulla risoluzione dei problemi

Se si verificano problemi durante o dopo il processo di integrazione, esaminare i seguenti scenari comuni e i passi di correzione:

1. Credenziali API non accettate in ETD

- Sintomo:quando si immettono l'ID client e la chiave privata in ETD, il sistema restituisce un errore di autenticazione.
- Risoluzione:
  - Verificare che la chiave API sia stata creata con gli esatti ambiti richiesti:"Admin" e"Policy". Se sono stati selezionati altri ambiti o questi non sono stati selezionati, la connessione avrà esito negativo.
  - Assicurarsi che non vi siano spazi iniziali o finali copiati accidentalmente quando si incolla l'ID client o la chiave privata nella console ETD.

2. Segreto chiave perduta o dimenticata

- Sintomo:ci si è allontanati dalla schermata di creazione dell'API Secure Access e non è più possibile visualizzare il segreto della chiave.
- Risoluzione: per motivi di sicurezza, il segreto chiave viene visualizzato una sola volta al momento della creazione. Se non è stata salvata in modo sicuro, è necessario eliminare la chiave API incompleta in Secure Access e generarne una nuova.

3. I criteri di prevenzione della perdita dei dati non vengono applicati al traffico di posta elettronica

- Sintomo: l'integrazione risulta riuscita, ma i criteri di prevenzione della perdita dei dati configurati non sono in grado di rilevare o bloccare i messaggi di posta elettronica sensibili.
- Risoluzione:
  - Verifica scadenza API: se è stato selezionato "Seleziona una data specifica" per la scadenza della chiave API (passaggio 2), verificare che la chiave non sia scaduta. In caso affermativo, è necessario generare e applicare una nuova coppia di chiavi.
  - Verifica modalità di distribuzione ETD: verificare che Cisco ETD sia distribuito in modalità inline. ETD deve trovarsi nel percorso del flusso di posta diretta per bloccare o modificare attivamente i messaggi in base ai verdetti DLP di accesso sicuro.
  - Tempo di sincronizzazione: dopo l'integrazione iniziale, attendere alcuni minuti affinché i sistemi back-end sincronizzino i criteri prima di testare le regole di prevenzione della perdita dei dati.

4. Interruzione del servizio dopo un periodo di stabilità

- Sintomo:l'applicazione del DLP smette improvvisamente di funzionare dopo mesi di funzionamento corretto.
- Risoluzione: in genere il problema è causato da una chiave API scaduta. Selezionare Admin

-> API Key in Cisco Secure Access per controllare lo stato della chiave utilizzata per ETD. Implementare un processo di rotazione delle chiavi per aggiornare le credenziali in ETD prima del raggiungimento della data di scadenza.

Riepilogo

L'integrazione di Cisco Email Threat Defense (ETD) con Cisco Secure Access (SA) è un passo fondamentale per la definizione di una strategia unificata di prevenzione della perdita dei dati (DLP). Generando una chiave API sicura con ambiti "Admin" e "Policy" nella console di accesso sicuro e configurando le credenziali nelle impostazioni globali di ETD, gli amministratori creano un ponte di comunicazione senza interruzioni tra le due piattaforme.

Una volta completato questo handshake, ETD può consegnare attivamente i metadati e-mail al motore DLP di Secure Access. Ciò consente all'organizzazione di gestire tutte le policy di protezione dei dati da un unico dashboard centralizzato (accesso sicuro), mantenendo al contempo una visibilità e un'applicazione complete sul traffico di posta elettronica (ETD).

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).