Konfigurieren einer E-Mail-DLP-Richtlinie in Cisco Secure Access (SA) und Cisco Email Threat Defense (ETD)

Inhalt

Einleitung

Voraussetzungen

- Anforderungen und verwendete Komponenten
- E-Mail-DLP-Richtlinienfunktionen

Netzwerkdiagramm

- Nachfolgend finden Sie das Netzwerkdiagramm, das die Integration von Cisco Secure Email Threat Defense in Cisco Secure Access veranschaulicht, sowie das Datenverkehrsflussdiagramm.

Konfigurieren

- Schritt 1: Bei Cisco Secure Access anmelden
- Phase 2: Navigieren zur Erstellung von E-Mail-SvD-Regeln

Option 1: Erstellen einer E-Mail-SvD-Regel mithilfe einer vordefinierten SvD-Vorlage

- Schritt 3: Grundlegende Regelinformationen konfigurieren
- Schritt 4: Datenklassifizierungen auswählen
- Schritt 5: Konfigurieren von Dateisteuerelementen
- Schritt 6: Absenderbereich definieren
- Schritt 7: Empfängerbereich definieren
- Schritt 8: Richtlinienaktion auswählen
- Schritt 9: Benutzerbenachrichtigungen konfigurieren
- Schritt 9: Benutzerbenachrichtigungen konfigurieren
- Phase 10: Regel überprüfen und speichern

Option 2: Erstellen einer E-Mail-SvD-Regel mithilfe einer benutzerdefinierten SvD-Vorlage

- Phase 11: Erstellen eines benutzerdefinierten Bezeichners
- Phase 12: Datenklassifizierung konfigurieren

Fehlerbehebung

- Regel stimmt nicht mit E-Mails überein
- E-Mails werden nicht blockiert
- DLP-Ereignisse sind in ETD nicht sichtbar.
- Übereinstimmungen auf Anlagenbasis wurden nicht erkannt

Best Practices

Zusammenfassung

Einleitung

E-Mails sind nach wie vor einer der häufigsten Kanäle für unbeabsichtigte oder nicht autorisierte Datenzugriffe. Cisco bietet Email Data Loss Prevention (DLP)-Funktionen für den Schutz sensibler, per E-Mail weitergegebener Informationen durch die Integration von Cisco Secure Access (SA) und Cisco Email Threat Defense (ETD).

In dieser Architektur werden alle Aktionen zum Erstellen, Konfigurieren und Durchsetzen von E-Mail-DLP-Richtlinien in Cisco Secure Access ausgeführt. Cisco Email Threat Defense bietet Transparenz für E-Mails und Nachrichtenverfolgung, während Cisco Secure Access als Policy Engine für die Definition von DLP-Regeln und Durchsetzungsverhalten dient.

In diesem Artikel wird erläutert, wie Sie in Cisco Secure Access eine E-Mail-DLP-Richtlinie erstellen, entweder mit einer vordefinierten DLP-Vorlage oder einer benutzerdefinierten DLP-Vorlage.

Voraussetzungen

Stellen Sie vor Beginn des Konfigurationsprozesses sicher, dass die folgenden Anforderungen erfüllt sind:

- Administrator-Zugriff:Sie müssen sowohl für die Cisco Email Threat Defense Inline-Konsole als auch für die Cisco Secure Access-Konsole über die Berechtigung "Vollständiger Administrator" verfügen.
- Aktive Abonnements:Stellen Sie sicher, dass sowohl Ihre E-Mail Threat Defense- als auch Ihre Secure Access-Tenants aktiv sind und bereitgestellt werden.
- Konnektivität:Die API-Integration zwischen Email Threat Defense und Secure Access muss erfolgreich hergestellt werden.
- Mail Flow-Konfiguration: E-Mail Threat Defense muss im Inline-Modus korrekt bereitgestellt werden, um sicherzustellen, dass der E-Mail-Verkehr aktiv untersucht wird.

Wichtig: Obwohl diese Lösung sowohl Cisco Secure Access als auch Cisco Email Threat Defense verwendet, werden alle in diesem Artikel beschriebenen Konfigurationsschritte für E-Mail-SvD-Regeln nur in Cisco Secure Access ausgeführt.

Anforderungen und verwendete Komponenten

Um eine E-Mail-DLP-Richtlinie erfolgreich zu implementieren, werden die folgenden Komponenten verwendet:

- Cisco Email Threat Defense (ETD):Fungiert als E-Mail-Prüfpunkt. Es erfasst den ausgehenden E-Mail-Verkehr und vereinfacht den Kommunikationsfluss, der für die DLP-Engine zur Durchführung der Analyse erforderlich ist.
- Cisco Secure Access (SA) - Die DLP-Engine: Dies ist die Hauptkomponente, in der alle DLP-Konfigurationen gespeichert sind. Verwenden Sie die Secure Access-Konsole, um Folgendes zu definieren:
    - Daten-IDs: Die spezifischen Muster oder sensiblen Datentypen (z. B. PII, Kreditkartennummern oder interne Projektcodes), die vom System überwacht werden sollen.
    - SvD-Policys: Die Regeln, die festlegen, wie das System reagieren soll, wenn sensible Daten erkannt werden (z. B. blockieren, verschlüsseln oder benachrichtigen).
    - Richtlinienaktionen: Die von der SvD-Engine ausgelösten automatisierten Antworten, z. B. das Verhindern des Versands von E-Mails oder das Anwenden einer obligatorischen Verschlüsselung.
- Integrations-Framework: Die Backend-Konnektivität, mit der ETD E-Mail-Metadaten zur Richtlinienauswertung und anschließenden Durchsetzung an die SvD-Engine für sicheren Zugriff übergeben kann.

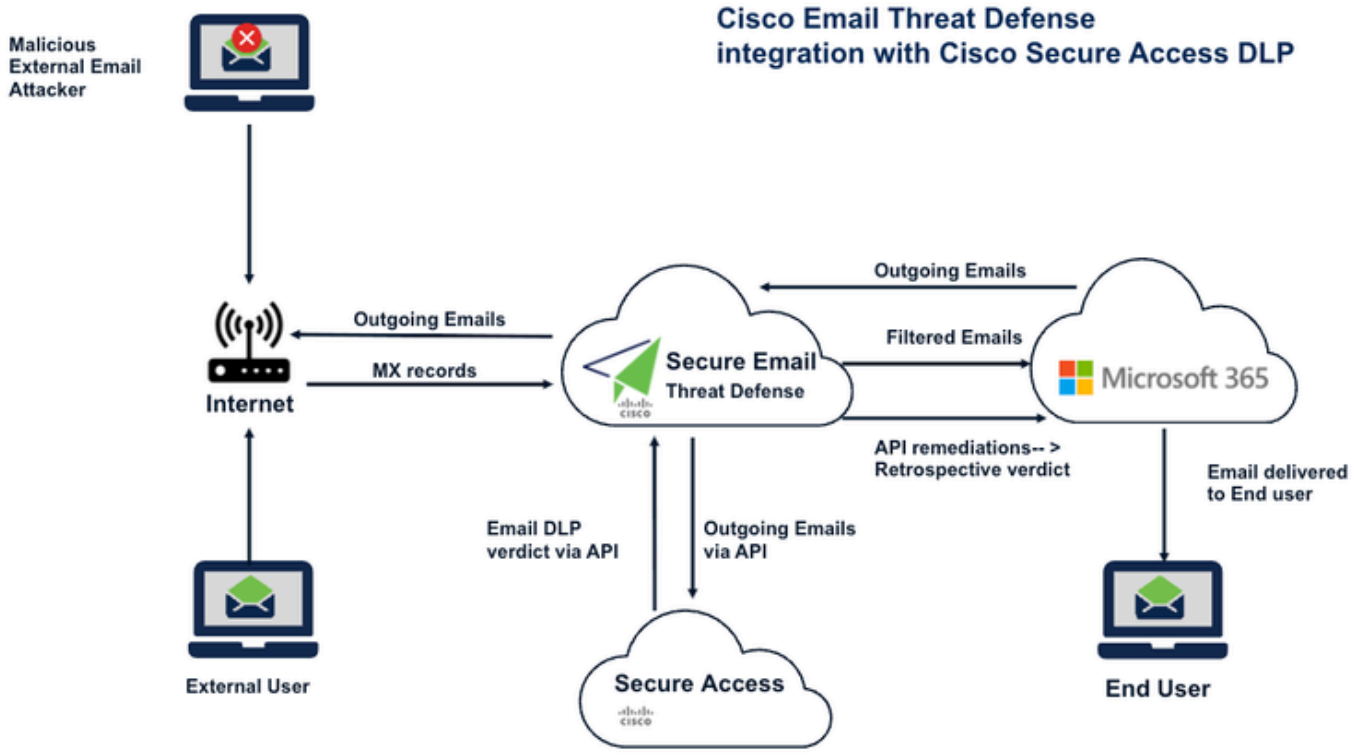
E-Mail-DLP-Richtlinienfunktionen

Beim Erstellen einer E-Mail-DLP-Richtlinie in Cisco Secure Access können Sie Folgendes konfigurieren:

- Regelname und -beschreibung
- Schweregrad
- Datenklassifizierungen
- Umfang der Inspektion, einschließlich:
    - Betreff der E-Mail
    - Nachrichtentext
    - Name des Anhangs
    - Inhalt des Anhangs
- Dateisteuerelemente, einschließlich:
    - MIP-Labels
    - Titus-Etiketten
- Absenderbedingungen
- Empfängerbedingungen
- Politische Maßnahmen:
    - Überwachung
    - Blockieren
- Optionale Benutzerbenachrichtigungen

Netzwerkdiagramm

Nachfolgend finden Sie das Netzwerkdiagramm, das die Integration von Cisco Secure Email Threat Defense in Cisco Secure Access veranschaulicht, sowie das Datenverkehrsflussdiagramm.



HINWEIS: Im obigen Bild ist der Exchange-Server O365, diese SvD-Konfiguration kann jedoch auf jedem Exchange-Server vorgenommen werden, der SMTP unterstützt.

HINWEIS: Weitere Informationen finden Sie im Artikel "Steps to integration Cisco Email Threat Defense (ETD) with Cisco Secure Access:" (Schritte zur Integration von Cisco Email Threat Defense (ETD) in Cisco Secure Access:), um Cisco Email Threat Defense und Cisco Secure Access über die API zu integrieren.

Konfigurieren

Konfigurieren einer E-Mail-DLP-Richtlinie in Cisco Secure Access

Schritt 1: Bei Cisco Secure Access anmelden

Melden Sie sich bei der Cisco Secure Access (SA)-Konsole mit einem Administratorkonto mit den erforderlichen Berechtigungen an.

Phase 2: Navigieren zur Erstellung von E-Mail-SvD-Regeln

Navigieren Sie im Dashboard für sicheren Zugriff zu:

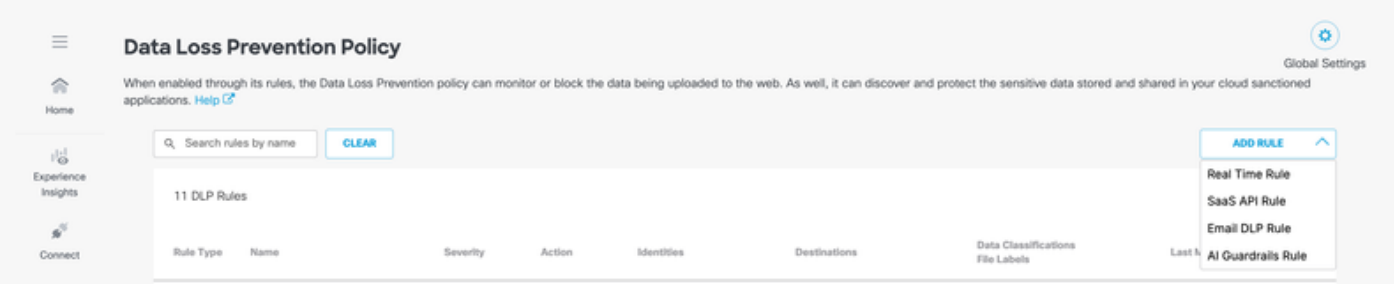
Sicher > Richtlinie > Richtlinie zum Schutz vor Datenverlust > Regel hinzufügen > E-Mail-SvD-Regel

Daraufhin wird die Seite Neue E-Mail-Regel hinzufügen geöffnet.

Cisco Secure Access bietet zwei Methoden zum Erstellen einer E-Mail-DLP-Regel:

- Erstellen einer E-Mail-SvD-Regel mithilfe einer vordefinierten SvD-Vorlage
- Erstellen einer E-Mail-SvD-Regel mithilfe einer benutzerdefinierten SvD-Vorlage

Abbildung 1. Navigieren zur Erstellung der E-Mail-SvD-Regel



Option 1: Erstellen einer E-Mail-SvD-Regel mithilfe einer vordefinierten SvD-Vorlage

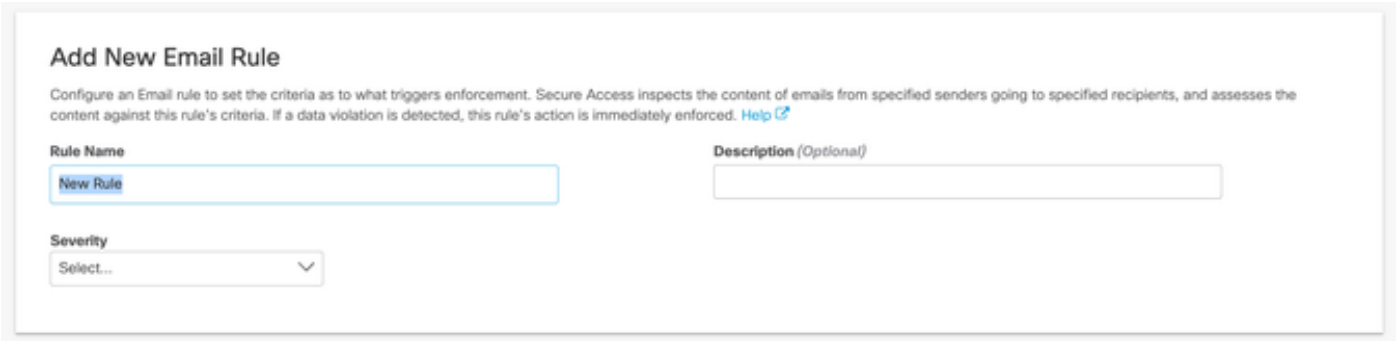
Schritt 3: Grundlegende Regelinformationen konfigurieren

Navigieren Sie in das Fenster REGEL HINZUFÜGEN > E-Mail-SvD-Regel,

Geben Sie im Fenster Neue E-Mail-Regel hinzufügen die folgenden Details ein:

- Regelname
  Geben Sie einen beschreibenden Namen für die E-Mail-SvD-Regel ein.
- Beschreibung
  Kurze Zusammenfassung des Zwecks der Regel
- Schweregrad
  Wählen Sie den entsprechenden Schweregrad für die Richtlinie aus:
    - Niedrig
    - Mittel
    - Hoch
    - Critical (Kritisch)

Mithilfe dieser Felder können Sie Regeln für Administration, Berichterstellung und betriebliche Transparenz kategorisieren.



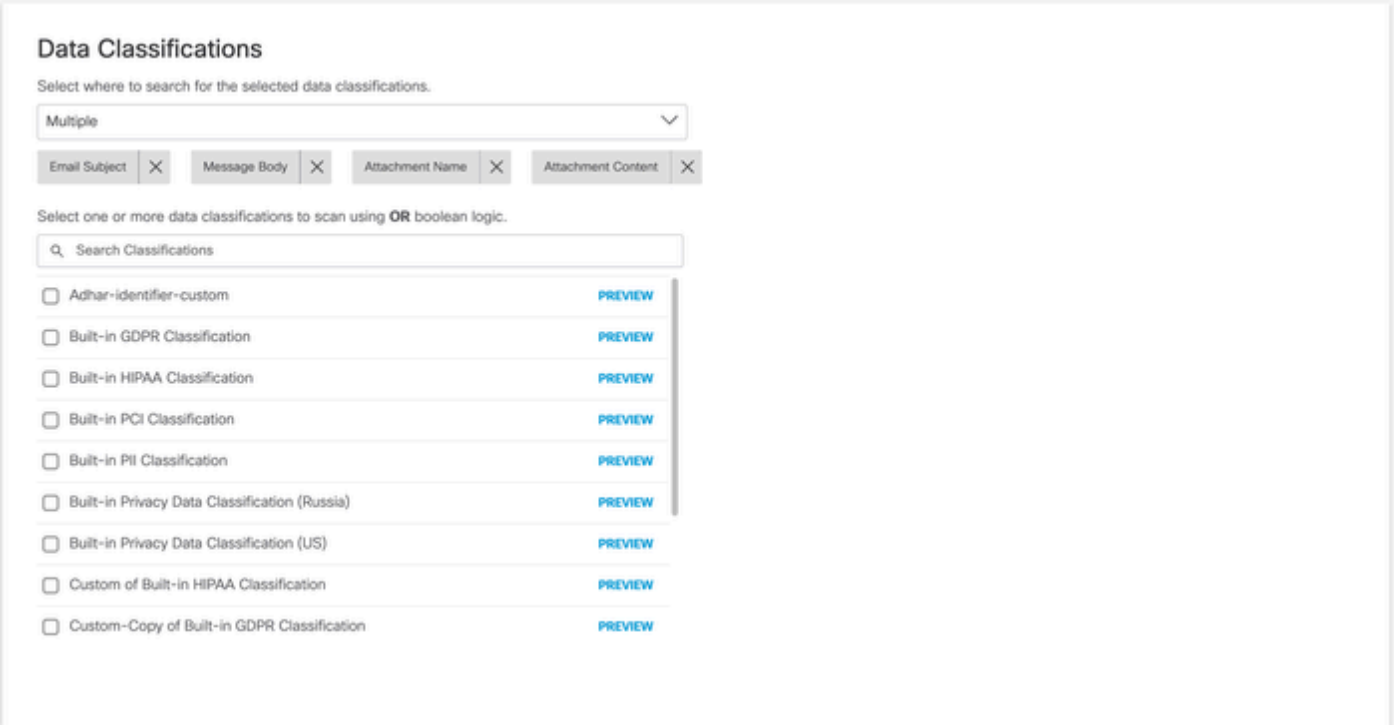
Schritt 4: Datenklassifizierungen auswählen

Wählen Sie unter Datenklassifizierungen die vordefinierte SvD-Vorlage aus, die verwendet wird, um E-Mail-Inhalte auf potenzielle SvD-Verletzungen zu prüfen.

Wählen Sie als Nächstes aus, wo die ausgewählten Klassifikationen zugeordnet werden sollen. Folgende Prüfpunkte werden unterstützt:

- Betreff der E-Mail
- Nachrichtentext
- Name des Anhangs
- Inhalt des Anhangs

Auf diese Weise kann die Richtlinie sowohl den Nachrichteninhalt als auch Anhänge auf vertrauliche Informationen überprüfen.



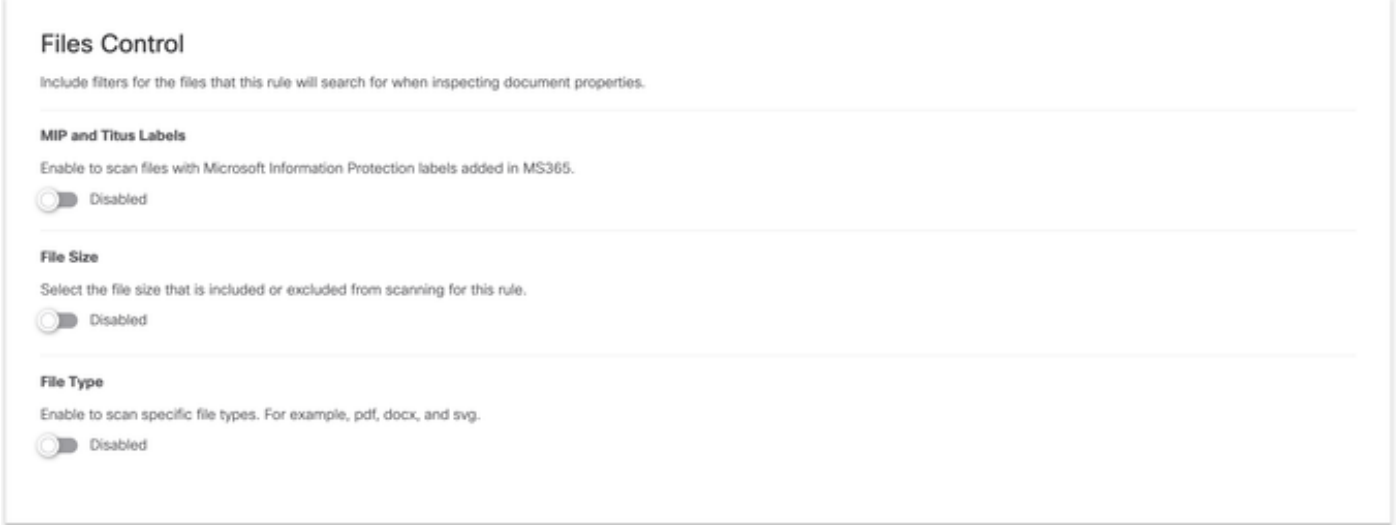
Schritt 5: Konfigurieren von Dateisteuerelementen

Konfigurieren Sie unter Dateikontrolle die dateibasierten Prüfkriterien für die Regel.

Dies umfasst Unterstützung für:

- MIP-Labels
- Titus-Etiketten

Diese Einstellungen sind nützlich, wenn bei der SvD-Erzwingung Vertraulichkeitslabel oder Metadaten berücksichtigt werden müssen, die angehängten Dateien zugeordnet sind.



Schritt 6: Absenderbereich definieren

Geben Sie im Abschnitt Absender an, auf welche Absender die Richtlinie angewendet wird.

Verfügbare Optionen:

- Alle Absender
- Bestimmte Absender
- Bestimmte Absender ausschließen

So können Sie die Regel umfassend anwenden oder auf ausgewählte Benutzer oder Gruppen beschränken.

Schritt 7: Empfängerbereich definieren

Wählen Sie im Abschnitt Empfänger die Benutzer oder Gruppen aus, die in die

Richtlinienbewertung einbezogen oder von ihr ausgeschlossen werden sollen.

Verfügbare Optionen:

- Alle Benutzer einschließen
- Spezifische Benutzer einbeziehen
- Bestimmte Benutzer ausschließen

So lässt sich die Richtliniendurchsetzung besser an die beabsichtigten Empfänger anpassen.

Schritt 8: Richtlinienaktion auswählen

Wählen Sie im Abschnitt Action (Aktion) aus, wie Cisco Secure Access E-Mails handhaben soll, die eindeutig als Verstoß gegen die DLP-Regel identifiziert wurden.

Verfügbare Aktionen:

- Überwachung
  Die E-Mail ist zulässig, und das Ereignis wird protokolliert, um für Transparenz zu sorgen und Berichte zu erstellen.
- Blockieren
  Die E-Mail wird verworfen, um die Übertragung vertraulicher Daten zu verhindern.

Anmerkung: Derzeit können positiv identifizierte E-Mails entweder durch die Aktion Überwachen oder durch die Aktion Blockieren blockiert werden.

Wichtig: E-Mail-SvD-Aktionen werden nur in Cisco Secure Access konfiguriert. Wenn eine E-Mail von Secure Access blockiert wird, wird die Veranstaltung auch in der Cisco ETD-Nachrichtenverfolgung angezeigt.

Schritt 9: Benutzerbenachrichtigungen konfigurieren

Die Benachrichtigungsoption steht nur für die Empfänger zur Verfügung.

Konfigurieren Sie unter User Notifications (Benutzerbenachrichtigungen), ob Benutzer benachrichtigt werden sollen, wenn eine E-Mail mit der SvD-Policy übereinstimmt.
Es besteht die Möglichkeit, "Actor's Manager" oder einen "Custom Recipient" zu benachrichtigen. Ein "benutzerdefinierter Empfänger" kann jeder sein.

Konfigurieren Sie die E-Mail-Nachrichtenvorlage von der Standard- zur benutzerdefinierten Benachrichtigung nach Ihren Anforderungen.

Wenn diese Funktion aktiviert ist, können Benachrichtigungen dazu beitragen, die Benutzer besser zu informieren und wiederholte Richtlinienverletzungen zu reduzieren. Konfigurieren Sie diese Einstellung entsprechend den betrieblichen und Compliance-Anforderungen Ihres Unternehmens.

Schritt 9: Benutzerbenachrichtigungen konfigurieren

Benutzerbenachrichtigungen sind ein leistungsstarkes Tool zur Erhöhung des Sicherheitsbewusstseins und zur Gewährleistung der Compliance. Indem Sie Benutzer oder Administratoren benachrichtigen, wenn eine E-Mail eine DLP-Richtlinie auslöst, können Sie sofortiges Feedback und Kontext zu der Verletzung geben.

Anmerkung: Die Benachrichtigungseinstellungen richten sich in erster Linie an die E-Mail-Empfänger und die benannten Beteiligten.

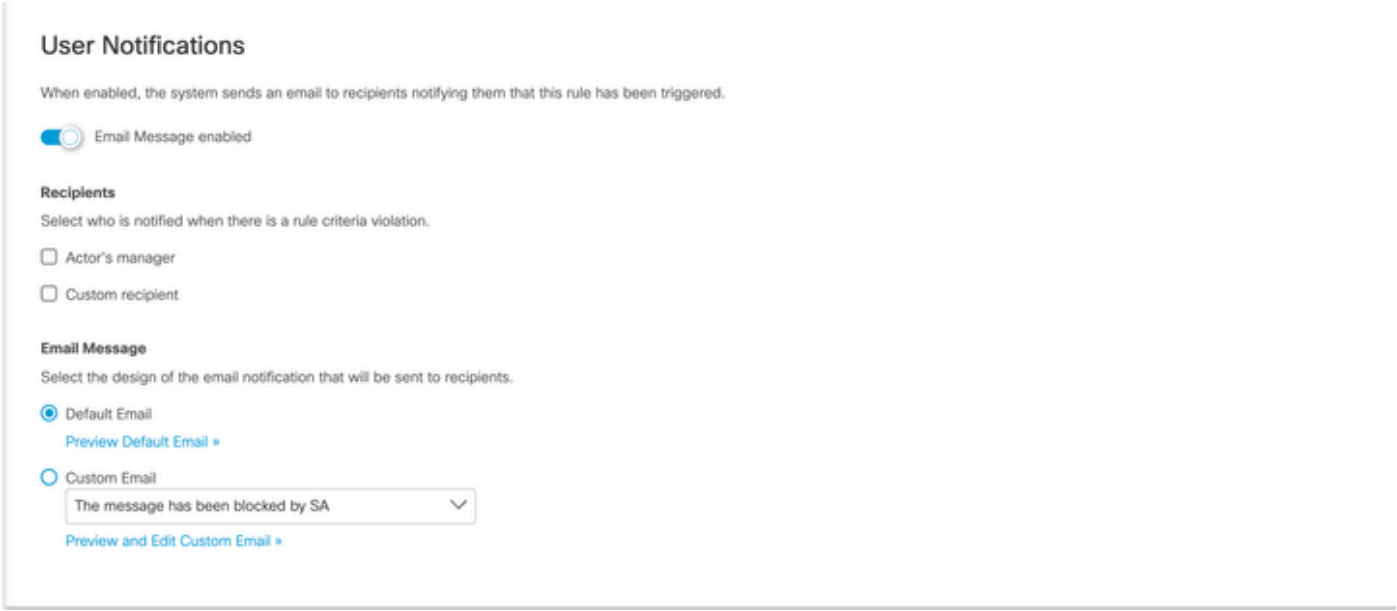
So konfigurieren Sie Benachrichtigungen:

1. Benachrichtigungsempfänger definieren: Geben Sie im Abschnitt "Benutzerbenachrichtigungen" an, wer die Warnung erhalten soll. Sie haben zwei primäre Optionen:

- Schauspieler-Manager: Sendet die Benachrichtigung direkt an den Manager des Benutzers, der die Richtlinienverletzung ausgelöst hat.
- Benutzerdefinierter Empfänger: Ermöglicht die Angabe beliebiger E-Mail-Adressen (z. B. eine Security Operations Center oder ein bestimmter Abteilungsleiter).

2. Nachrichtenvorlage auswählen: Sie können zwischen der Standardbenachrichtigungsvorlage und einer benutzerdefinierten Benachrichtigung wählen.
    - Empfehlung: Wenn in Ihrem Unternehmen bestimmte Compliance-Anforderungen oder interne Branding-Anforderungen bestehen, können Sie den E-Mail-Text mit der Option Benutzerdefiniert anpassen, um dem Empfänger klare, umsetzbare Anweisungen zu geben.
3. Prüfen und speichern: Stellen Sie nach der Konfiguration sicher, dass die Einstellungen den Betriebs- und Compliance-Richtlinien Ihres Unternehmens entsprechen.

Best Practice: Die Aktivierung dieser Benachrichtigungen ist eine effektive Methode, um wiederholte Richtlinienverletzungen zu reduzieren, indem Benutzer in Echtzeit über Verfahren zur Verarbeitung vertraulicher Daten informiert werden.



Anmerkung: Die Benachrichtigungsoptionen können je nach Tenant-Konfiguration und Richtlinieneinstellungen variieren.

Phase 10: Regel überprüfen und speichern

Nach Abschluss der Regelkonfiguration:

1. Überprüfen Sie alle konfigurierten Einstellungen.
2. Überprüfen Sie, ob die ausgewählten Datenklassifizierungen, der Prüfungsumfang, die

Absender- und Empfängerbedingungen und die Aktion mit dem beabsichtigten Richtlinienverhalten übereinstimmen.
3. Klicken Sie auf Speichern, um die E-Mail-SvD-Regel zu erstellen.

Die DLP-Richtlinie für E-Mail ist jetzt in Cisco Secure Access aktiviert.

Option 2: Erstellen einer E-Mail-SvD-Regel mithilfe einer benutzerdefinierten SvD-Vorlage

Das Erstellen einer benutzerdefinierten SvD-Vorlage umfasst zwei primäre Phasen: Definieren eines benutzerdefinierten Bezeichners und Konfigurieren der Datenklassifizierung.

Anmerkung: Die Datenklassifizierungs-Engine ist äußerst flexibel und ermöglicht Ihnen die Erstellung von Richtlinien mithilfe einer einzelnen benutzerdefinierten Kennung oder einer Kombination aus benutzerdefinierten und vordefinierten, durch UND/ODER-Boolesche Operatoren verknüpften Bezeichnern.

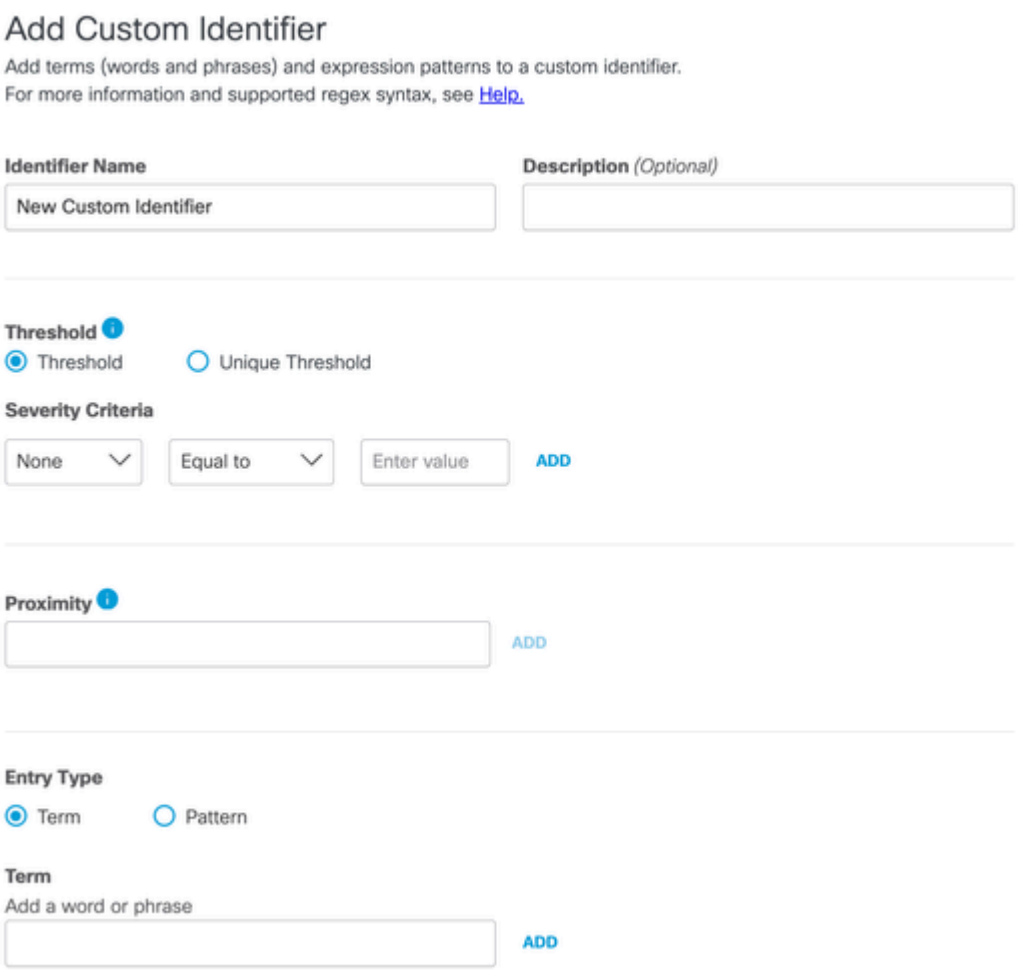
Phase 11: Erstellen eines benutzerdefinierten Bezeichners

Führen Sie die folgenden Schritte aus, um ein neues Datenmuster für die Erkennung zu definieren:

1. Melden Sie sich beim Secure AccessDashboard an.
2. Navigieren Sie zuSicher > Datenklassifizierung.
3. Klicken Sie auf Benutzerdefinierten Bezeichner hinzufügen.
4. Konfigurieren Sie die folgenden Parameter im Fenster Benutzerdefinierten Identifikator hinzufügen:

- Name und Beschreibung: Geben Sie einen eindeutigen Namen und eine kurze Beschreibung des Datentyps an, den Sie erkennen möchten.
- Schwellenwert:
    - Schwellenwert: Überwacht die Gesamtfrequenz der erkannten Daten.
    - Eindeutiger Schwellenwert: Überwacht nur die Anzahl eindeutiger Datenvorkommen und ignoriert Duplikate.
- Schweregradkriterien: Weisen Sie Schweregrade zu (Sehr niedrig, Niedrig, Mittel, Hoch), basierend auf der Häufigkeit der Erkennung. Sie können diese mithilfe von Vergleichsoperatoren wieEqual to, Greater Than, Less Than oderRange definieren.
- Nähe: Legen Sie den Näherungsgrenzwert fest. Dies gilt für alle Begriffe und Muster, die in diesem Bezeichner gemeinsam und nicht pro einzelnen Begriff definiert werden.

- Eintragstyp: Legen Sie fest, wie das System die Daten identifiziert:
  - Begriff: Ein bestimmtes Wort oder eine bestimmte Phrase.
  - Muster: Ein regulärer Ausdruck (regulärer Ausdruck), der zum Erkennen bestimmter Datenformate (z. B. Kreditkartennummern oder interne Projektcodes) verwendet wird.

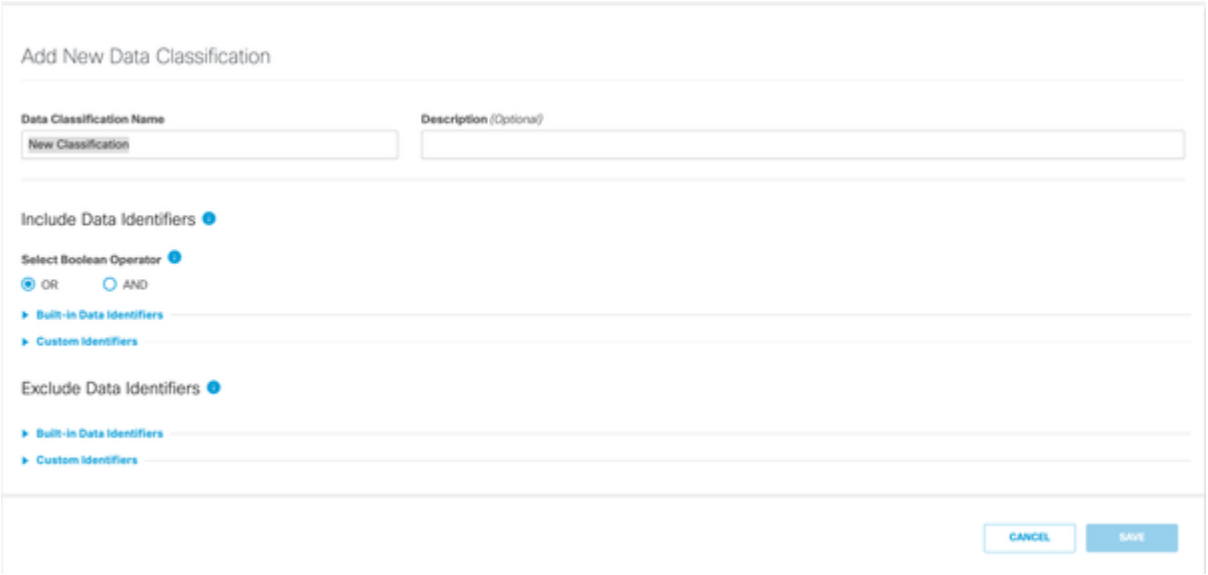


Phase 12: Datenklassifizierung konfigurieren

Nachdem der benutzerdefinierte Bezeichner gespeichert wurde, können Sie ihn in ein Datenklassifizierungsobjekt integrieren:

1. Navigieren Sie zuSicher > Datenklassifizierung > Hinzufügen (verwenden Sie die Schaltfläche oben rechts).
2. Wählen Sie Ihre neu erstellte benutzerdefinierte Kennung aus der verfügbaren Liste aus.
3. (Optional) Kombinieren Sie Ihren benutzerdefinierten Bezeichner mit vordefinierten Bezeichnern, indem Sie die AND/OR-Logik verwenden, um den Erkennungsbereich zu verfeinern.
4. Speichern Sie die Konfiguration, um sie für die Verwendung in Ihren E-Mail-SvD-Policys verfügbar zu machen.
5. Weitere Informationen finden Sie im folgenden Screenshot.

6. Befolgen Sie nun die gleichen Schritte von Schritt 4 bis Schritt 10, um eine Richtlinie mit benutzerdefinierter Datenklassifizierung zu erstellen.



Diese Konfiguration stellt sicher, dass Ihr Unternehmen sensible Informationen erkennen kann, die speziell auf Ihre internen Datenstrukturen und Compliance-Anforderungen zugeschnitten sind.

Fehlerbehebung

Wenn sich die E-Mail-SvD-Regel nicht wie erwartet verhält, überprüfen Sie Folgendes:

Regel stimmt nicht mit E-Mails überein

- Bestätigen Sie, dass die richtige Datenklassifizierungsvorlage ausgewählt ist.
- Überprüfen Sie, ob die relevanten Prüfplätze aktiviert sind:
  - Betreff der E-Mail
  - Nachrichtentext
  - Name des Anhangs
  - Inhalt des Anhangs
- Stellen Sie sicher, dass Absender- und Empfängerfilter die Test-E-Mail nicht unbeabsichtigt ausschließen.

E-Mails werden nicht blockiert

- Vergewissern Sie sich, dass die Regelaktion auf Blockund nichtÜberwachen festgelegt ist.
- Bestätigen Sie, dass die Regel gespeichert und aktiviert ist.
- Stellen Sie sicher, dass der E-Mail-Inhalt die konfigurierten SvD-Kriterien erfüllt.

DLP-Ereignisse sind in ETD nicht sichtbar.

- Bestätigen Sie, dass Cisco ETD und Cisco Secure Access ordnungsgemäß integriert sind.
- Überprüft, ob der relevante E-Mail-Verkehr aktiv von ETD verarbeitet wird.
- Überprüfen Sie, ob das Richtlinienereignis zuerst in Cisco Secure Access vorhanden ist.

Übereinstimmungen auf Anlagenbasis wurden nicht erkannt

- Bestätigen Sie, dass im Prüfbereich Name und/oder Inhalt des Anhangs ausgewählt sind.
- Überprüfen Sie die Dateisteuerungseinstellungen, wenn Labels wie MIP oder Titus Teil der Regellogik sind.

Best Practices

Berücksichtigen Sie die folgenden Best Practices bei der Bereitstellung von E-Mail-DLP-Richtlinien:

- Beginnen Sie mit Überwachungsmodus, um das Richtlinienverhalten zu überprüfen, bevor Sie Block erzwingen.
- Verwenden Sie eindeutige und beschreibende Regelnamen, um die Administration zu vereinfachen.
- Richten Sie die Absender- und Empfängerbedingungen sorgfältig aus, um unbeabsichtigte Übereinstimmungen zu vermeiden.
- Führen Sie vor der breiten Bereitstellung einen Test mit repräsentativen Daten durch.
- Überprüfen Sie die ETD-Nachrichtenverfolgung regelmäßig, um blockierte oder überwachte E-Mail-Aktivitäten zu validieren.
- Verwenden Sie benutzerdefinierte Vorlagen, wenn unternehmensspezifische Daten-IDs erforderlich sind.

Zusammenfassung

Cisco Secure Access ist die zentrale Plattform für die Konfiguration von Email DLP-Richtlinien in einer integrierten Bereitstellung von Cisco Secure Access und Cisco Email Threat Defense. Während ETD Transparenz und Nachrichtenverfolgung bietet, werden alle SvD-Regelerstellung, Klassifizierungsauswahl, Durchsetzungsaktionen und Benachrichtigungen in Secure Access konfiguriert.

Mithilfe vordefinierter oder benutzerdefinierter SvD-Vorlagen können Administratoren E-Mail-Inhalte und -Anhänge überprüfen, den Absender- und Empfängerbereich definieren und Aktionen zur Überwachung oder Blockierung anwenden, um vertrauliche Daten vor dem Verlust durch E-Mail zu schützen.

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.