Come configurare i criteri di prevenzione della perdita dei dati di posta elettronica in Cisco Secure Access (SA) e Cisco Email Threat Defense (ETD)

Sommario

Introduzione

La posta elettronica rimane uno dei canali più comuni per l'esposizione non intenzionale o non autorizzata dei dati. Per aiutare le organizzazioni a proteggere le informazioni riservate condivise tramite e-mail, Cisco offre funzionalità di prevenzione della perdita dei dati tramite l'integrazione di Cisco Secure Access (SA) e Cisco Email Threat Defense (ETD).

In questa architettura, tutte le azioni di creazione, configurazione e applicazione dei criteri di prevenzione della perdita dei dati di posta elettronica vengono eseguite in Cisco Secure Access. Cisco Email Threat Defense fornisce visibilità e monitoraggio dei messaggi di posta elettronica, mentre Cisco Secure Access funge da motore delle policy per la definizione delle regole di prevenzione della perdita dei dati e del comportamento di imposizione.

In questo articolo viene spiegato come creare i criteri di prevenzione della perdita dei dati per la posta elettronica in Cisco Secure Access, utilizzando un modello di prevenzione della perdita dei dati predefinito o un modello di prevenzione della perdita dei dati personalizzato.

Prerequisiti

Prima di iniziare il processo di configurazione, verificare che siano soddisfatti i seguenti requisiti:

- Accesso amministrativo:è necessario disporre dei privilegi di "amministratore completo" sia per la console in linea Cisco Email Threat Defense che per la console Cisco Secure Access.
- Sottoscrizioni attive: verificare che i tenant Email Threat Defense e Secure Access siano attivi e dotati di provisioning.
- Connettività: l'integrazione API tra Email Threat Defense e Secure Access deve essere stabilita correttamente.
- Configurazione flusso di posta: Email Threat Defense deve essere implementato correttamente in modalità inline per garantire l'ispezione attiva del traffico di posta elettronica.

Importante: Sebbene questa soluzione utilizzi sia Cisco Secure Access che Cisco Email Threat Defense, tutti i passaggi di configurazione delle regole di prevenzione della perdita dei dati dei messaggi di posta elettronica descritti in questo articolo vengono eseguiti solo in Cisco Secure Access.

Requisiti e componenti utilizzati

Per implementare correttamente i criteri di prevenzione della perdita dei dati tramite e-mail, vengono utilizzati i seguenti componenti:

- Cisco Email Threat Defense (ETD):agisce come punto di ispezione e-mail. Acquisisce il traffico e-mail in uscita e semplifica il flusso di comunicazione necessario al motore di prevenzione della perdita dei dati per eseguire l'analisi.
- Cisco Secure Access (SA) - Il motore DLP:è il componente principale in cui risiedono tutte le configurazioni DLP. La console Secure Access consente di definire:
    - Identificativi dati:i modelli specifici o i tipi di dati sensibili (ad esempio PII, numeri di carta di credito o codici di progetto interni) che il sistema deve monitorare.
    - Criteri di prevenzione della perdita dei dati:le regole che determinano la modalità di reazione del sistema quando vengono rilevati dati sensibili (ad esempio, blocco, crittografia o notifica).
    - Azioni criteri:le risposte automatizzate attivate dal motore di prevenzione della perdita dei dati, ad esempio il blocco dell'invio dell'e-mail o l'applicazione della crittografia obbligatoria.
- Integration Framework:connettività back-end che consente a ETD di consegnare i metadati e-mail al motore DLP di accesso sicuro per la valutazione dei criteri e la successiva applicazione.

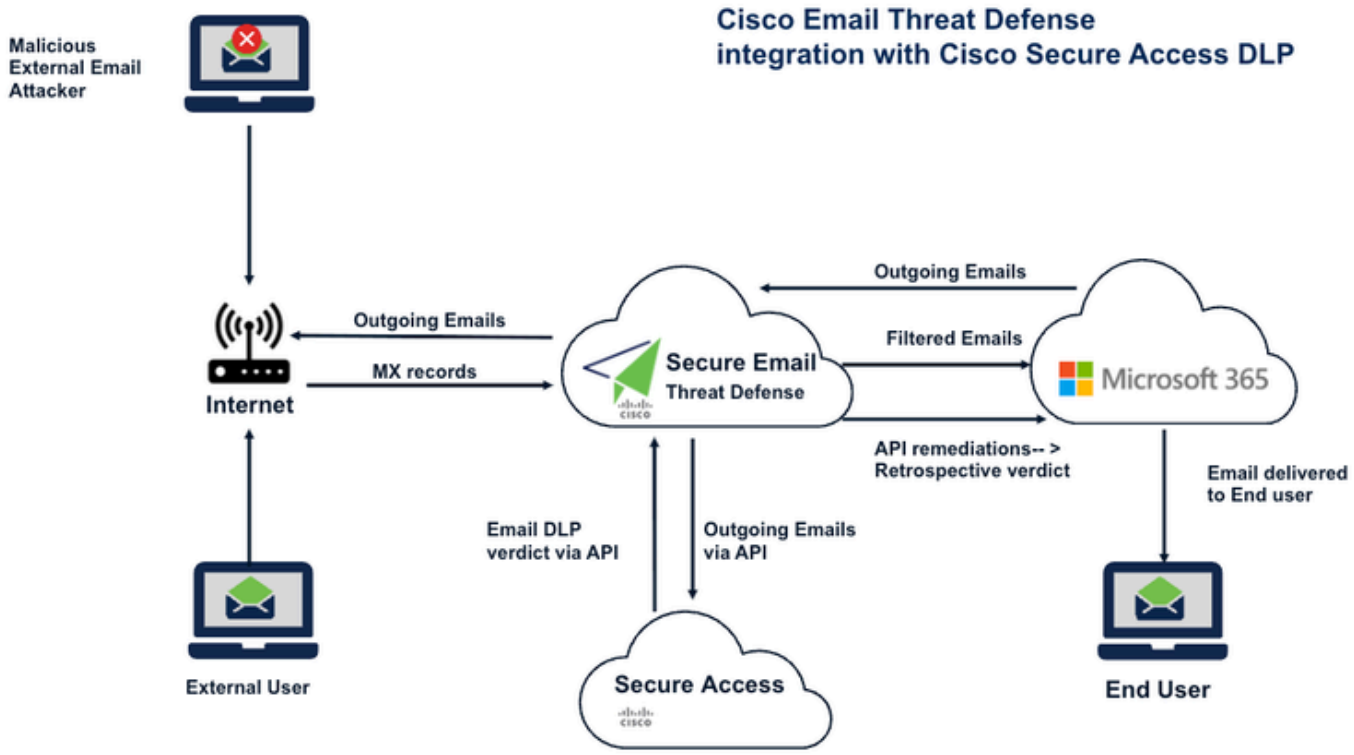
Funzionalità dei criteri di prevenzione della perdita dei dati tramite e-mail

Quando si creano i criteri di prevenzione della perdita dei dati per la posta elettronica in Cisco Secure Access, è possibile configurare:

- Nome e descrizione regola
- Livello di gravità
- Classificazioni dei dati
- Ambito dell'ispezione, compresi:
    - Oggetto e-mail
    - Corpo del messaggio
    - Nome allegato
    - Contenuto degli allegati
- Controlli file, tra cui:
    - Etichette MIP
    - Etichette Titus
- Condizioni mittente
- Condizioni destinatario
- Azioni politiche:
    - Monitor (Monitora)
    - Block (Blocca)
- Notifiche utente facoltative

Esempio di rete

Di seguito è riportato il diagramma di rete che illustra l'integrazione di Cisco Secure Email threat defense con Cisco Secure Access insieme al diagramma del flusso del traffico.



NOTA: Nell'immagine precedente, il server Exchange è O365, ma questa configurazione DLP può essere eseguita su qualsiasi server Exchange che supporti SMTP.

NOTA: Per integrare Cisco Email Threat Defense e Cisco Secure Access tramite API, consultare l'articolo "Passaggi per l'integrazione di Cisco Email Threat Defense (ETD) con Cisco Secure Access:".

Configurazione

Configurare i criteri di prevenzione della perdita dei dati per la posta elettronica in Cisco Secure Access

Passaggio 1: Accedi a Cisco Secure Access

Accedere alla console di Cisco Secure Access (SA) utilizzando un account amministratore con le autorizzazioni richieste.

Passaggio 2: Passa alla creazione di regole di prevenzione della perdita dei dati tramite posta elettronica

Dal dashboard Accesso sicuro, passare a:

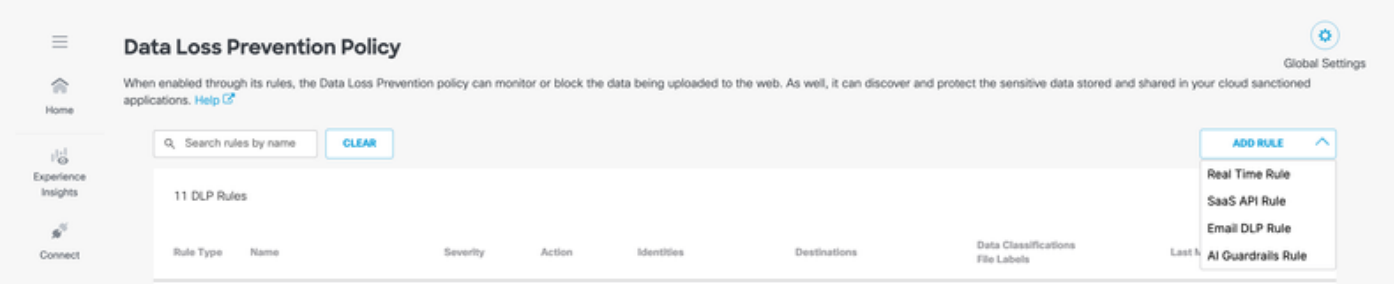
Protezione > Criteri > Criteri di prevenzione della perdita dei dati > Aggiungi regola > Regola di prevenzione della perdita dei dati tramite posta elettronica

Verrà visualizzata la pagina Aggiungi nuova regola di posta elettronica.

Cisco Secure Access offre due metodi per creare una regola di prevenzione della perdita dei dati per la posta elettronica:

- Crea una regola di prevenzione della perdita dei dati tramite posta elettronica utilizzando un modello di prevenzione della perdita dei dati predefinito
- Crea una regola di prevenzione della perdita dei dati tramite posta elettronica utilizzando un modello di prevenzione della perdita dei dati personalizzato

Figura 1. Passare alla creazione di regole di prevenzione della perdita dei dati tramite posta elettronica



Opzione 1: Crea una regola di prevenzione della perdita dei dati tramite posta elettronica utilizzando un modello di prevenzione della perdita dei dati predefinito

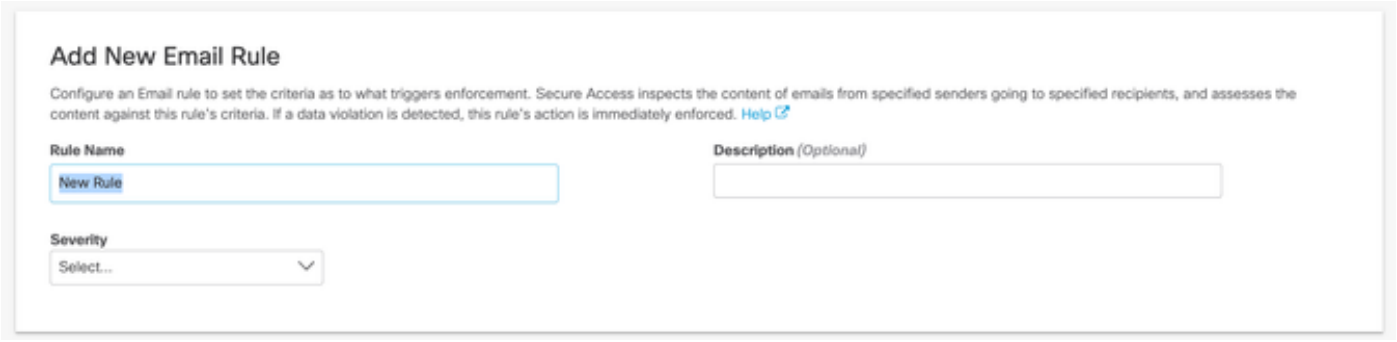
Passaggio 3: Configura informazioni di base sulle regole

Passare alla finestra AGGIUNGI REGOLA > Invia regola di prevenzione della perdita dei dati tramite posta elettronica,

Nella finestra Aggiungi nuova regola e-mail, immettere i dettagli riportati di seguito.

- Nome regola
  Immettere un nome descrittivo per la regola di prevenzione della perdita dei dati tramite posta elettronica.
- Descrizione
  Fornire un breve riepilogo dello scopo della regola.
- Gravità
  Selezionare il livello di gravità appropriato per il criterio:
  - Bassa
  - Media
  - Alta
  - Critico

Questi campi consentono di suddividere in categorie le regole per l'amministrazione, la creazione di report e la visibilità operativa.



Passaggio 4: Seleziona classificazioni dati

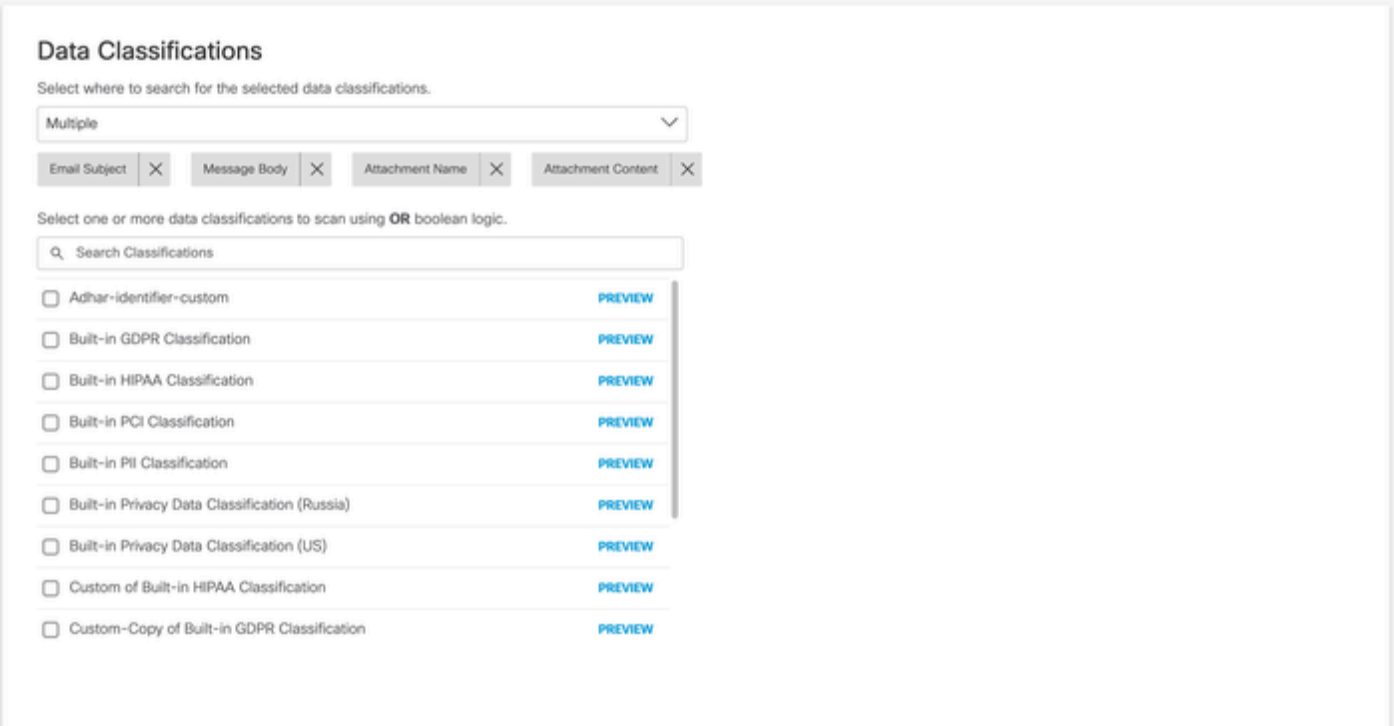
In Classificazioni dati, selezionare il modello di prevenzione della perdita dei dati predefinito che verrà utilizzato per ispezionare il contenuto della posta elettronica per individuare potenziali violazioni della prevenzione della perdita dei dati.

Scegliere quindi la corrispondenza tra le classificazioni selezionate. I siti di ispezione supportati

includono:

- Oggetto e-mail
- Corpo del messaggio
- Nome allegato
- Contenuto degli allegati

In questo modo il criterio può ispezionare il contenuto e gli allegati dei messaggi per individuare informazioni riservate.



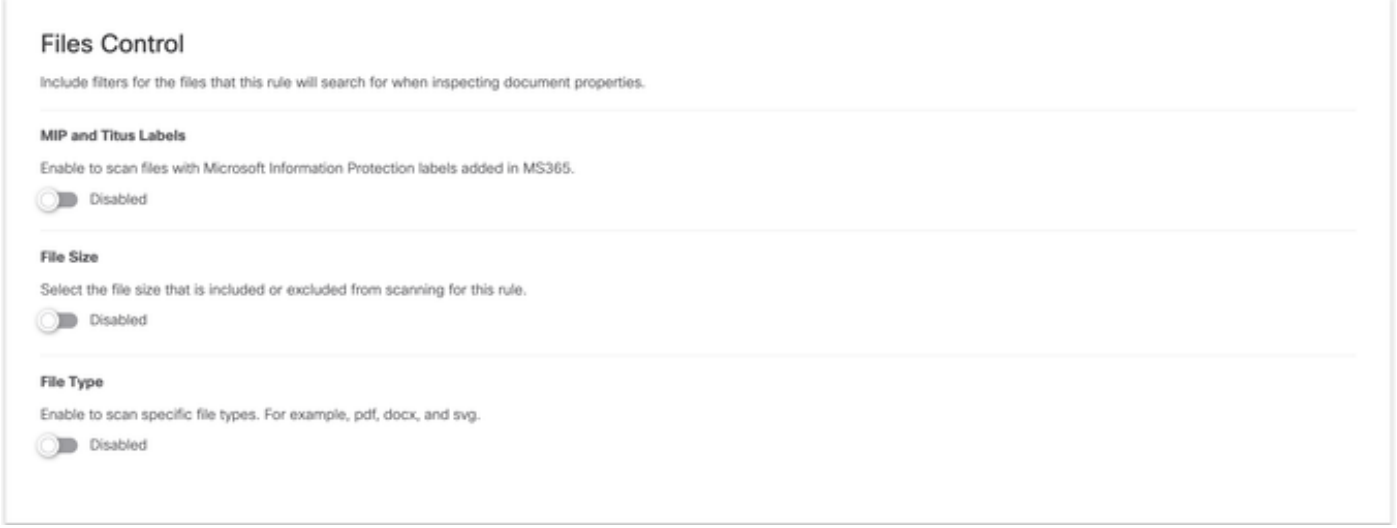
Passaggio 5: Configura controlli file

In Controllo file configurare i criteri di ispezione basati su file per la regola.

Ciò include il supporto per:

- Etichette MIP
- Etichette Titus

Queste impostazioni sono utili quando l'imposizione DLP deve considerare le etichette di riservatezza o i metadati associati ai file allegati.



Passaggio 6: Definisci ambito mittente

Nella sezione Mittenti specificare i mittenti a cui si applica il criterio.

Le opzioni disponibili includono:

- Tutti i mittenti
- Mittenti specifici
- Escludi mittenti specifici

In questo modo è possibile applicare la regola in modo ampio o limitarla a utenti o gruppi selezionati.

Passaggio 7: Definisci ambito destinatario

Nella sezione Destinatari scegliere gli utenti o i gruppi da includere o escludere dalla valutazione

dei criteri.

Le opzioni disponibili includono:

- Includi tutti gli utenti
- Includi utenti specifici
- Escludi utenti specifici

Ciò consente di personalizzare l'applicazione dei criteri in base ai destinatari previsti.

Passaggio 8: Selezionare l'azione criterio

Nella sezione Azione, scegli in che modo Cisco Secure Access deve gestire i messaggi di posta elettronica che sono stati identificati come violazioni della regola di prevenzione della perdita dei dati.

Le azioni disponibili sono:

- Monitor (Monitora)
  L'e-mail è consentita e l'evento viene registrato per la visibilità e la creazione di report.
- Block (Blocca)
  L'e-mail viene eliminata per impedire la trasmissione di dati sensibili.

Nota: Al momento, le e-mail identificate positivamente possono essere permesse tramite l'azione Monitor o scartate tramite l'azione Block.

Importante: Le azioni DLP per posta elettronica sono configurate solo in Cisco Secure Access. Se un'e-mail è bloccata da Secure Access, l'evento è visibile anche nel monitoraggio dei messaggi ETD di Cisco.

Passaggio 9: Configura notifiche utente

L'opzione di notifica è disponibile solo per i destinatari.

In Notifiche utente specificare se gli utenti devono ricevere una notifica quando un messaggio di posta elettronica corrisponde ai criteri di prevenzione della perdita dei dati.
C'è un'opzione per notificare "Responsabile attore" o "Destinatario personalizzato". Un "Destinatario personalizzato" può essere chiunque.

Configurare il modello di messaggio e-mail da predefinito a notifica personalizzata in base alle proprie esigenze.

Se abilitate, le notifiche possono contribuire a migliorare la consapevolezza degli utenti e a ridurre le ripetute violazioni dei criteri. Configurare questa impostazione in base ai requisiti operativi e di conformità dell'organizzazione.

Passaggio 9: Configura notifiche utente

Le notifiche degli utenti sono uno strumento potente per promuovere la consapevolezza della sicurezza e garantire la conformità. Avvisando gli utenti o gli amministratori quando un messaggio e-mail attiva un criterio di prevenzione della perdita dei dati, puoi fornire un feedback e un contesto immediati riguardo alla violazione.

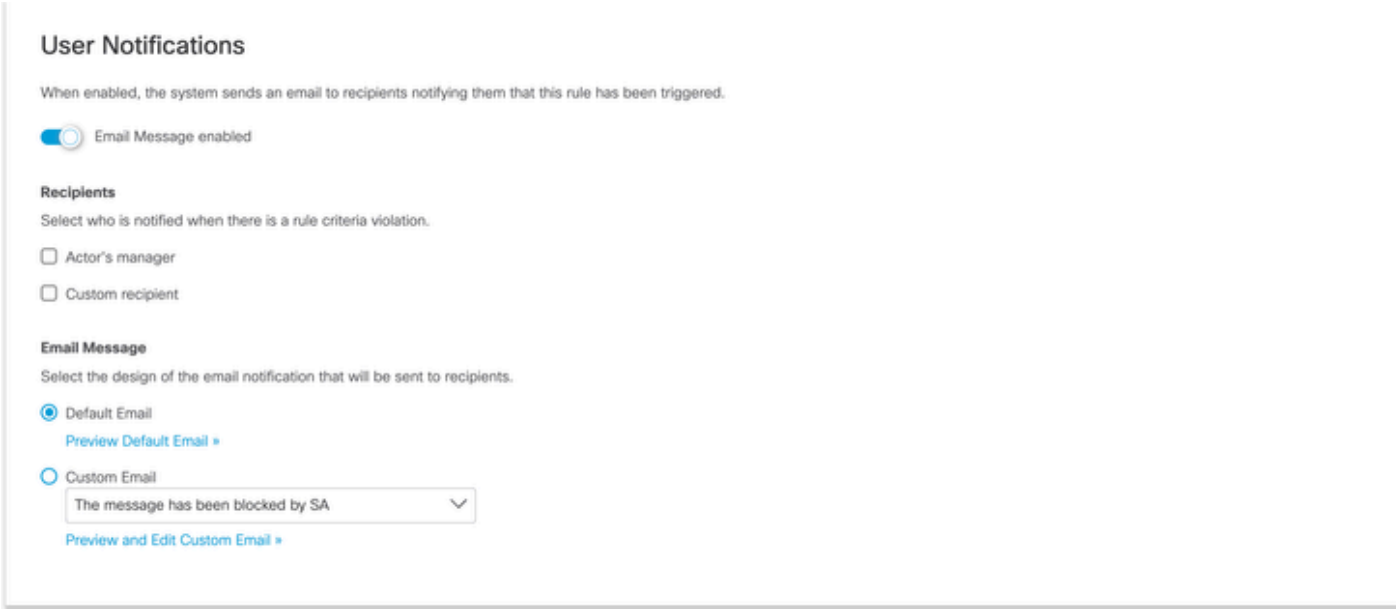
Nota: Le impostazioni di notifica sono principalmente destinate ai destinatari di posta elettronica e alle parti interessate designate.

Per configurare le notifiche:

1. Definisci destinatari notifica: Nella sezione Notifiche utente specificare gli utenti che devono ricevere l'avviso. Sono disponibili due opzioni principali:
    - Responsabile attore: Invia la notifica direttamente al responsabile dell'utente che ha attivato la violazione dei criteri.

    - Destinatario personalizzato: Consente di specificare qualsiasi indirizzo e-mail (ad esempio, un centro operazioni di sicurezza o un responsabile di reparto specifico).
2. Seleziona modello messaggio: È possibile scegliere tra il modello di notifica predefinito o una notifica personalizzata.
    - Consiglio: Se l'organizzazione ha specifici requisiti di conformità o di branding interno, utilizzare l'opzione Personalizza per personalizzare il corpo dell'e-mail in modo da fornire al destinatario istruzioni chiare e pratiche.
3. Revisione e salvataggio: Una volta configurate, verificare che le impostazioni siano in linea con le politiche operative e di conformità della propria organizzazione.

Procedura ottimale: L'attivazione di queste notifiche è un modo efficace per ridurre le violazioni ripetute delle regole, poiché consente di informare in tempo reale gli utenti sulle procedure di gestione dei dati sensibili.



Nota: Le opzioni di notifica possono variare in base alla configurazione del tenant e alle impostazioni dei criteri.

Passaggio 10: Revisione e salvataggio della regola

Dopo aver completato la configurazione della regola:

1. Controllare tutte le impostazioni configurate.
2. Verificare che le classificazioni dei dati, l'ambito di ispezione, le condizioni del mittente e del destinatario e l'azione selezionati corrispondano al comportamento previsto per i criteri.
3. Fare clic su Salva per creare la regola di prevenzione della perdita dei dati tramite posta elettronica.

I criteri di prevenzione della perdita dei dati per la posta elettronica sono ora attivi in Cisco Secure Access.

Opzione 2: Creare una regola di prevenzione della perdita dei dati tramite posta elettronica utilizzando un modello di prevenzione della perdita dei dati personalizzato

La creazione di un modello di prevenzione della perdita dei dati personalizzato prevede due fasi principali: definizione di un identificatore personalizzato e configurazione della classificazione dati.

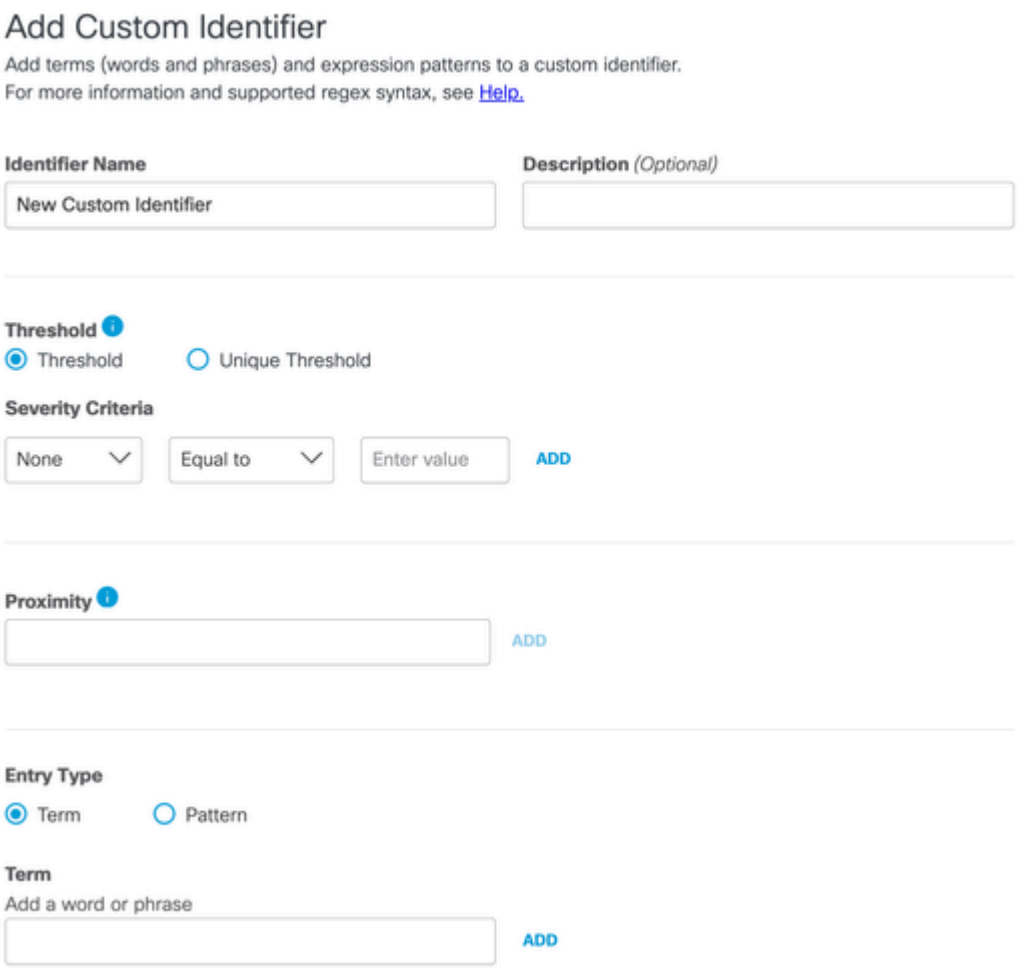
Nota: Il motore di classificazione dei dati è estremamente flessibile e consente di creare criteri utilizzando un singolo identificatore personalizzato o una combinazione di identificatori personalizzati e predefiniti collegati da operatori booleani AND/OR.

Passaggio 11: Creare un identificatore personalizzato

Per definire un nuovo modello di dati per il rilevamento, eseguire la procedura seguente:

1. Accedere a Secure Accessdashboard.
2. Passare aProtezione > Classificazione dati.
3. Fare clic su Aggiungi identificatore personalizzato.
4. Configurare i seguenti parametri nella finestra Aggiungi identificatore personalizzato:

- Nome e descrizione: Fornire un nome univoco e una breve descrizione del tipo di dati che si desidera rilevare.
- Soglia:
    - Soglia: Esegue il monitoraggio della frequenza totale dei dati rilevati.
    - Soglia univoca: Esegue il monitoraggio solo del numero di occorrenze dei dati, ignorando i duplicati.
- Criteri di gravità: Assegnare i livelli di gravità (Molto basso, Basso, Medio, Alto) in base alla frequenza di rilevamento. È possibile definirli utilizzando operatori di confronto quali Uguale a, Maggiore di, Minore di o Intervallo.
- Prossimità: Impostare la soglia di prossimità. Ciò si applica a tutti i termini e modelli definiti all'interno di questo identificatore collettivamente, piuttosto che per singolo termine.
- Tipo voce: Definire il modo in cui il sistema identifica i dati:
    - Termine: Parola o frase specifica.
    - Motivo: Espressione regolare (regex) utilizzata per rilevare formati di dati specifici, ad esempio numeri di carta di credito o codici di progetto interni.



Passaggio 12: Configura classificazione dati

Dopo aver salvato l'identificatore personalizzato, è possibile integrarlo in un oggetto Classificazione dati:

1. Selezionare Secure (Protetto) > Data Classification (Classificazione dati) > Add (Aggiungi) (utilizzare la parte inferiore nell'angolo superiore destro)
2. Selezionare il nuovo identificatore personalizzato dall'elenco disponibile.
3. (Facoltativo) Combinare l'identificativo personalizzato con identificativi predefiniti utilizzando la logica AND/OR per definire meglio l'ambito di rilevamento.
4. Salvare la configurazione per renderla disponibile per l'uso nei criteri di prevenzione della perdita dei dati e-mail.
5. Per ulteriori informazioni, fare riferimento alla schermata seguente.
6. Seguire ora gli stessi passaggi dal Passaggio 4 al Passaggio 10 per creare un criterio utilizzando la classificazione dei dati personalizzata.

Questa configurazione garantisce all'organizzazione la possibilità di rilevare informazioni sensibili personalizzate in base alle strutture di dati interne e ai requisiti di conformità.

Risoluzione dei problemi

Se il comportamento della regola di prevenzione della perdita dei dati tramite posta elettronica non è quello previsto, verificare quanto segue:

La regola non corrisponde ai messaggi di posta elettronica

- Confermare che il modello di classificazione dei dati corretti sia selezionato.
- Verificare che i siti di ispezione pertinenti siano abilitati:
  - Oggetto e-mail
  - Corpo del messaggio
  - Nome allegato
  - Contenuto degli allegati
- Assicurarsi che i filtri mittente e destinatario non escludano involontariamente il messaggio di posta elettronica di prova.

Le e-mail non sono bloccate

- Verificare che l'azione della regola sia impostata su Blocco e non su Monitor.
- Confermare che la regola sia stata salvata e attivata.
- Verificare che il contenuto dell'e-mail corrisponda correttamente ai criteri di prevenzione della perdita dei dati configurati.

Gli eventi DLP non sono visibili in ETD

- Confermare che Cisco ETD e Cisco Secure Access siano integrati correttamente.
- Verificare che ETD stia elaborando attivamente il traffico e-mail rilevante.
- Verificare se l'evento criterio è presente prima in Cisco Secure Access.

Non sono state rilevate corrispondenze basate su allegati

- Confermare che nell'ambito di ispezione sono selezionati il nome e/o il contenuto dell'allegato.
- Verificare le impostazioni di controllo file se etichette quali MIPorTitus fanno parte della logica della regola.

Procedure ottimali

Quando si distribuiscono i criteri di prevenzione della perdita dei dati per la posta elettronica, è necessario tenere presenti le procedure consigliate seguenti:

- Iniziare con Monitormode per convalidare il comportamento dei criteri prima di enforceBlock.
- Utilizzare nomi di regola chiari e descrittivi per semplificare l'amministrazione.
- Definire con attenzione le condizioni del mittente e del destinatario per ridurre le corrispondenze non intenzionali.
- Test con dati rappresentativi prima di un'implementazione estesa.
- Esaminare regolarmente il monitoraggio dei messaggi ETD per convalidare l'attività di posta elettronica bloccata o monitorata.
- Utilizzare modelli personalizzati in cui sono richiesti identificatori di dati specifici dell'azienda.

Riepilogo

Cisco Secure Access è la piattaforma centrale per la configurazione dei criteri di prevenzione della perdita dei dati e-mail in un'implementazione integrata di Cisco Secure Access e Cisco Email Threat Defense. Mentre ETD fornisce visibilità e verifica dei messaggi, tutte le operazioni di creazione delle regole di prevenzione della perdita dei dati, selezione della classificazione, azione di imposizione e notifiche vengono configurate in Accesso sicuro.

Utilizzando modelli di prevenzione della perdita dei dati predefiniti o personalizzati, gli amministratori possono ispezionare il contenuto e gli allegati dei messaggi di posta elettronica,

definire l'ambito del mittente e del destinatario e applicare azioni di monitoraggio o di blocco per evitare la perdita di dati riservati tramite e-mail.

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).