Como configurar uma política DLP de e-mail no Cisco Secure Access (SA) e no Cisco Email Threat Defense (ETD)

Contents

Introdução

O e-mail continua sendo um dos canais mais comuns de exposição de dados não intencional ou não autorizada. Para ajudar as empresas a proteger informações confidenciais compartilhadas por e-mail, a Cisco oferece recursos de prevenção de perda de dados de e-mail (DLP) por meio da integração do Cisco Secure Access (SA) e do Cisco Email Threat Defense (ETD).

Nessa arquitetura, todas as ações de criação, configuração e aplicação da política DLP de e-mail são executadas no Cisco Secure Access. O Cisco Email Threat Defense oferece visibilidade de e-mail e rastreamento de mensagens, enquanto o Cisco Secure Access funciona como mecanismo de política para definir regras de DLP e comportamento de aplicação.

Este artigo explica como criar uma política DLP de e-mail no Cisco Secure Access, usando um modelo DLP predefinido ou um modelo DLP personalizado.

Pré-requisitos

Antes de iniciar o processo de configuração, verifique se os seguintes requisitos foram atendidos:

- Acesso administrativo:Você deve ter privilégios de "Administrador total" para o console em linha do Cisco Email Threat Defense e o console do Cisco Secure Access.
- Assinaturas ativas:verifique se os locatários do Email Threat Defense e do Secure Access estão ativos e provisionados.
- Conectividade:A integração de APIs entre Email Threat Defense e Secure Access deve ser estabelecida com êxito.
- Configuração do fluxo de e-mail: O Email Threat Defense deve ser implantado corretamente no modo in-line para garantir que esteja inspecionando ativamente o tráfego de e-mail.

Importante: Embora essa solução use o Cisco Secure Access e o Cisco Email Threat Defense, todas as etapas de configuração de regra de DLP de e-mail descritas neste artigo são executadas apenas no Cisco Secure Access.

Requisitos e componentes usados

Para implementar com êxito uma política DLP de e-mail, os seguintes componentes são utilizados:

- Cisco Email Threat Defense (ETD):atua como o ponto de inspeção de e-mail. Ele captura o tráfego de e-mail de saída e facilita o fluxo de comunicação necessário para que o

mecanismo DLP execute sua análise.

- Cisco Secure Access (SA) - O mecanismo DLP:este é o componente principal onde residem todas as configurações DLP. Você utilizará o console Secure Access para definir:
    - Identificadores de Dados:Os padrões específicos ou tipos de dados confidenciais (por exemplo, PII, números de cartão de crédito ou códigos de projeto interno) que o sistema deve monitorar.
    - Políticas DLP:as regras que determinam como o sistema deve reagir quando dados confidenciais são detectados (por exemplo, bloquear, criptografar ou notificar).
    - Ações de política:As respostas automatizadas disparadas pelo mecanismo DLP, como impedir que o e-mail seja enviado ou aplicar criptografia obrigatória.
- Estrutura de integração:A conectividade de back-end que permite ao ETD transferir metadados de e-mail para o mecanismo DLP do Secure Access para avaliação de política e aplicação subsequente.

Recursos da Política DLP de Email

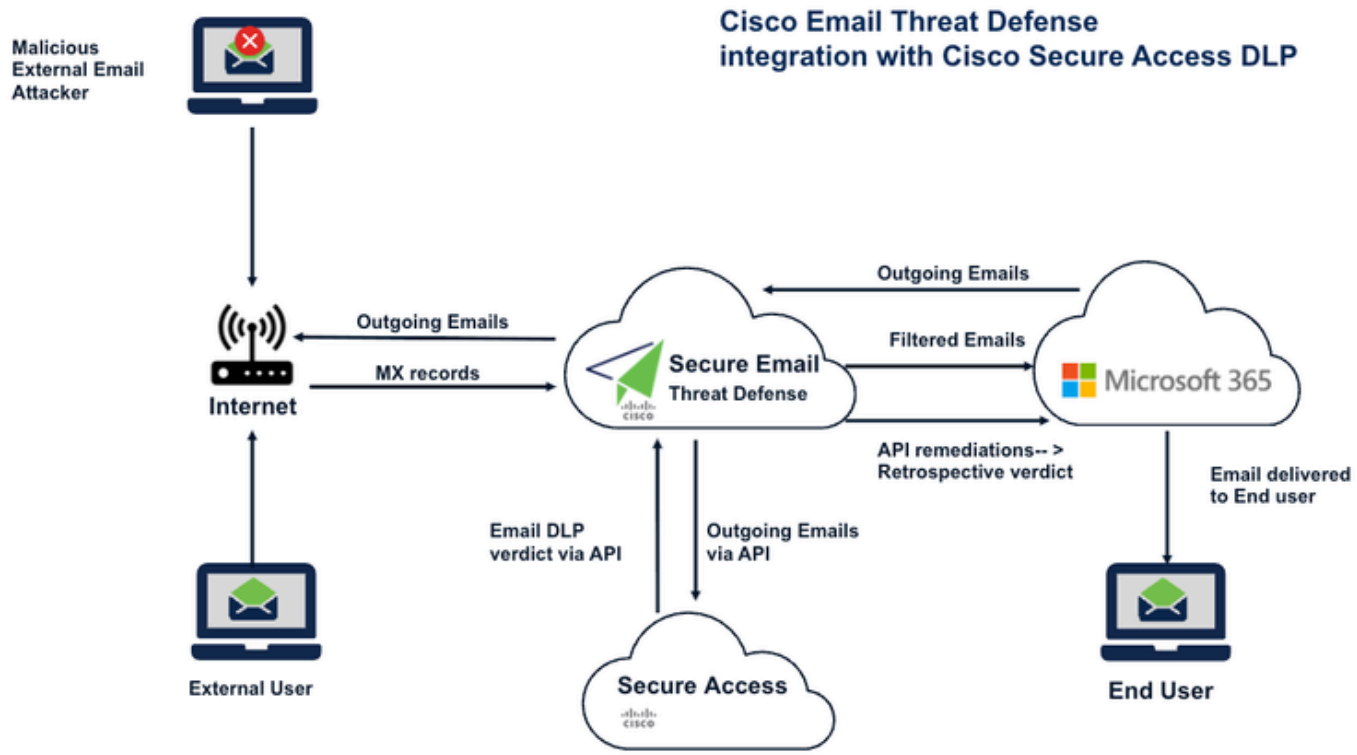
Ao criar uma política DLP de e-mail no Cisco Secure Access, você pode configurar:

- Nome e descrição da regra
- Nível de gravidade
- Classificações de dados
- Âmbito da inspeção, incluindo:
    - Assunto do e-mail
    - Corpo da mensagem
    - Nome do anexo
    - Conteúdo do anexo
- Controles de arquivo, incluindo:
    - Rótulos MIP
    - Rótulos de Tito
- Condições do remetente
- Condições do destinatário
- Ações de política:
    - Monitor
    - Bloqueio
- Notificações opcionais do usuário

Diagrama de Rede

Veja abaixo o diagrama de rede que ilustra a integração da defesa contra ameaças do Cisco Secure Email com o Cisco Secure Access, juntamente com o fluxograma

de tráfego.



NOTE: Na figura acima, o servidor de intercâmbio é O365, mas essa configuração DLP pode ser feita em qualquer servidor de intercâmbio que suporte SMTP.

NOTE: Consulte o artigo "Etapas para integrar o Cisco Email Threat Defense(ETD) com o Cisco Secure Access:" para integrar o Cisco Email Threat Defense e o Cisco Secure Access através da API.

Configurar

Configurar uma política DLP de e-mail no Cisco Secure Access

Passo 1: Faça login no Cisco Secure Access

Inicie a sessão no console Cisco Secure Access (SA) usando uma conta de administrador com as permissões necessárias.

Passo 2: Navegue até Email DLP Rule Creation (Criação de regra DLP de email)

No painel de controle do Secure Access, navegue até:

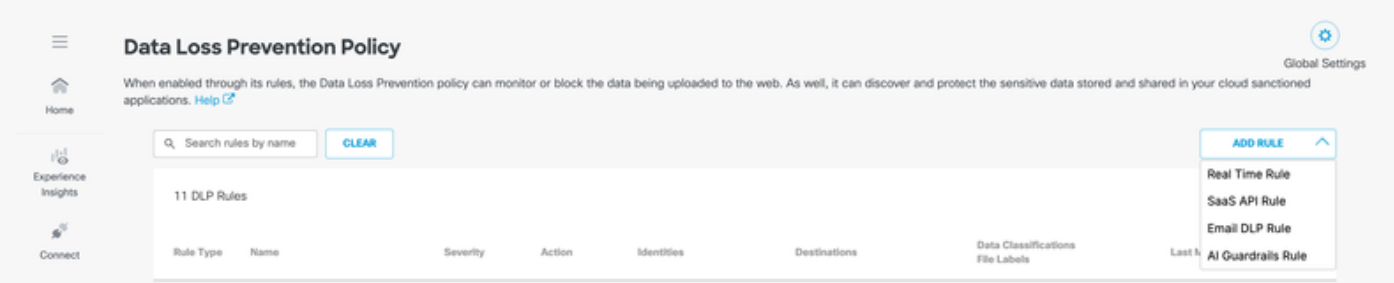
Proteger > Política > Política de prevenção de perda de dados > Adicionar regra > Regra de DLP de e-mail

Isso abre a página Adicionar nova regra de e-mail.

O Cisco Secure Access oferece dois métodos para criar uma regra DLP de e-mail:

- Criar uma regra de DLP de email usando um modelo de DLP predefinido
- Criar uma regra de DLP de email usando um modelo de DLP personalizado

Figura 1. Navegue até Email DLP Rule creation



Opção 1: Criar uma Regra de DLP de Email Usando um Modelo de DLP Predefinido

Passo 3: Configurar Informações Básicas da Regra

Navegue até a janela ADICIONAR REGRA > Regra de DLP de e-mail,

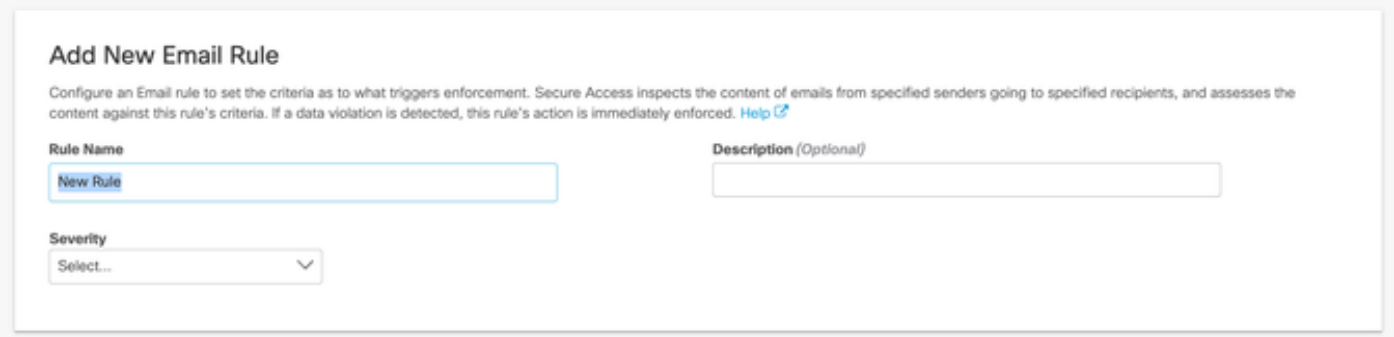
Na janela Adicionar nova regra de e-mail, insira os seguintes detalhes:

- Nome da regra
  Insira um nome descritivo para a regra DLP de email.
- Descrição

Forneça um breve resumo da finalidade da regra.

- Severity
  Selecione o nível de severidade apropriado para a política:
  - Baixa
  - Médio
  - Alto
  - Crítico

Esses campos ajudam a categorizar a regra para administração, geração de relatórios e visibilidade operacional.



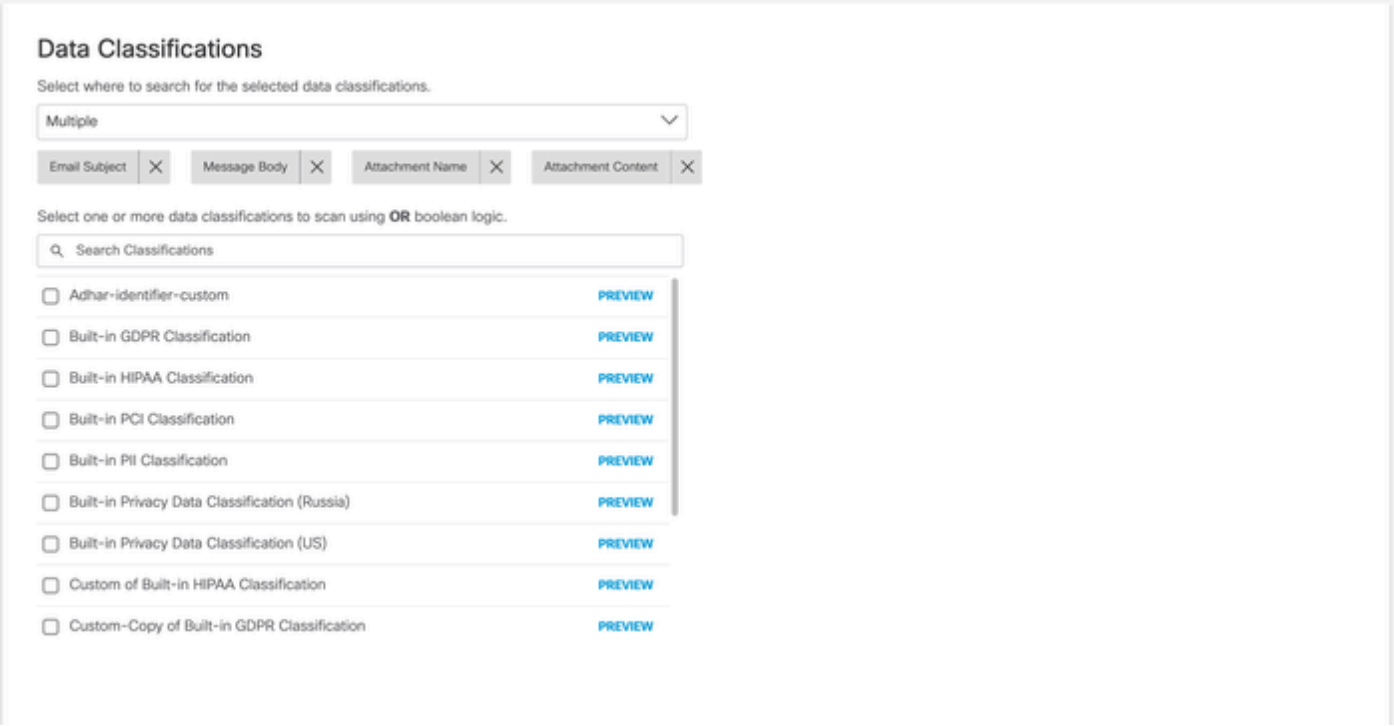
Passo 4: Selecionar Classificações de Dados

Em Classificações de dados, selecione o modelo de DLP predefinido que será usado para inspecionar o conteúdo de e-mail em busca de possíveis violações de DLP.

Em seguida, escolha onde as classificações selecionadas devem ser correspondidas. Os locais de inspeção suportados incluem:

- Assunto do e-mail
- Corpo da mensagem
- Nome do anexo
- Conteúdo do anexo

Isso permite que a política inspecione o conteúdo da mensagem e os anexos em busca de informações confidenciais.



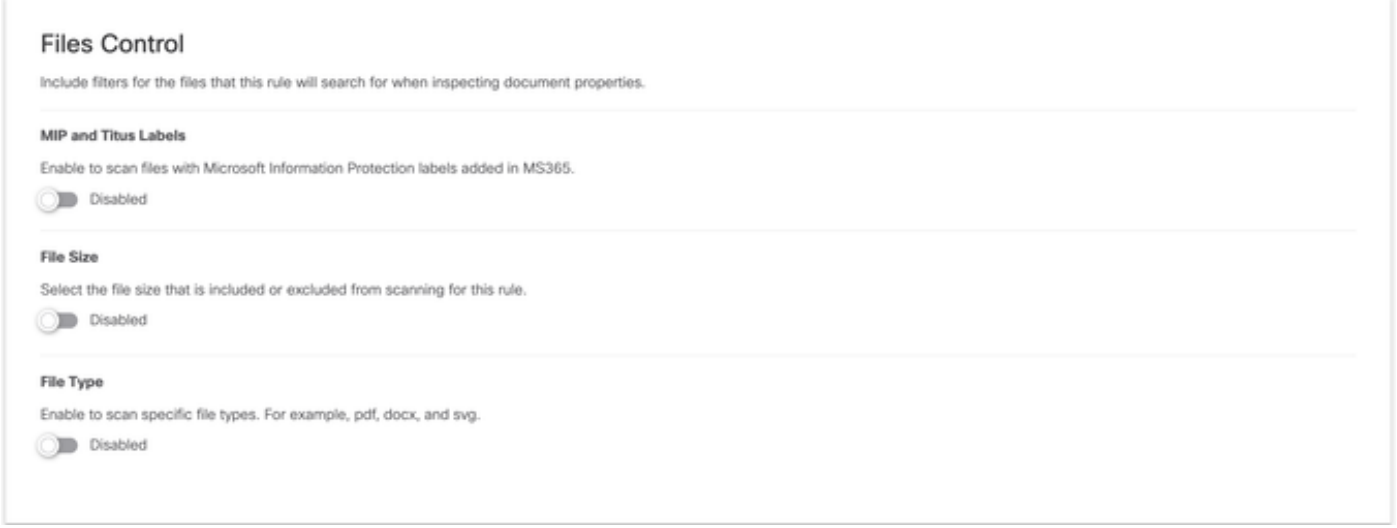
Passo 5: Configurar Controles de Arquivo

Em Controle de Arquivos, configure os critérios de inspeção baseados em arquivos para a regra.

Isso inclui suporte para:

- Rótulos MIP
- Rótulos de Tito

Essas configurações são úteis quando a aplicação de DLP deve considerar rótulos de sensibilidade ou metadados associados a arquivos anexados.



Passo 6: Definir Escopo do Remetente

Na seção Remetentes, especifique a quais remetentes a política se aplica.

As opções disponíveis incluem:

- Todos os remetentes
- Remetentes específicos
- Excluir remetentes específicos

Isso permite aplicar a regra de forma ampla ou restringi-la a usuários ou grupos selecionados.

Passo 7: Definir escopo do destinatário

Na seção Destinatários, escolha os usuários ou grupos que devem ser incluídos ou excluídos da avaliação de política.

As opções disponíveis incluem:

- Incluir todos os usuários
- Incluir usuários específicos
- Excluir usuários específicos

Isso ajuda a personalizar a aplicação de políticas com base nos destinatários pretendidos.

Passo 8: Selecionar a ação da política

Na seção Ação, escolha como o Cisco Secure Access deve tratar os e-mails que são identificados positivamente como violações da regra DLP.

Ações disponíveis:

- Monitor
  O e-mail é permitido e o evento é registrado para visibilidade e geração de relatórios.
- Bloqueio
  O e-mail é descartado para impedir a transmissão de dados confidenciais.

Note: No momento, os e-mails identificados positivamente podem ser permitidos por meio da ação Monitor ou descartados por meio da ação Block.

Importante: As ações de DLP de e-mail são configuradas somente no Cisco Secure Access. Se um e-mail for bloqueado pelo Secure Access, o evento também estará visível no rastreamento de mensagens do Cisco ETD.

Etapa 9: Configurar notificações de usuário

A opção de notificação está disponível apenas para os Destinatários.

Em User Notifications, configure se os usuários devem ser notificados quando um email corresponder à política DLP.
Há uma opção para notificar "Gerente do ator" ou "Destinatário personalizado". Um "Destinatário personalizado" pode ser qualquer pessoa.

Configure o modelo de mensagem de e-mail da notificação Padrão para Personalizada conforme sua necessidade.

Se ativadas, as notificações podem ajudar a aumentar a conscientização do usuário e reduzir as repetidas violações de política. Defina essa configuração de acordo com os requisitos operacionais e de conformidade da sua organização.

Etapa 9: Configurar notificações de usuário

As notificações de usuário são uma ferramenta poderosa para promover a conscientização de segurança e garantir a conformidade. Ao alertar usuários ou administradores quando um e-mail aciona uma política DLP, você pode fornecer feedback e contexto imediatos sobre a violação.

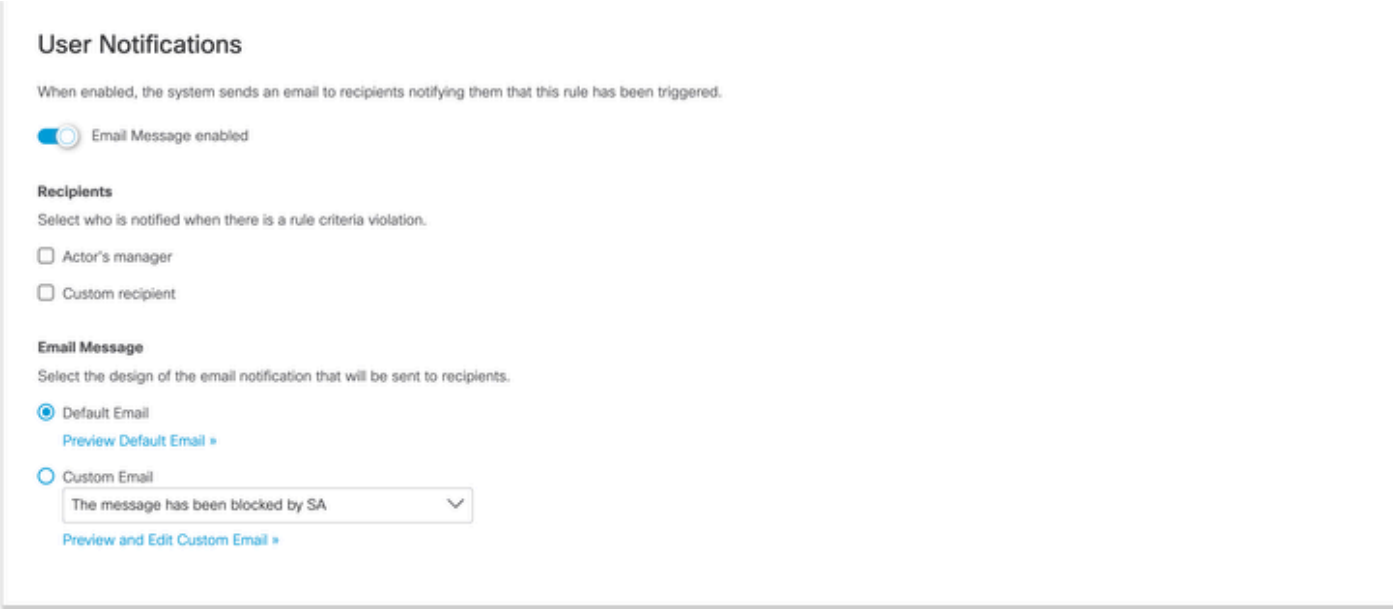
Note: As configurações de notificação destinam-se principalmente aos destinatários de e-mail e às partes interessadas designadas.

Para configurar notificações:

1. Definir destinatários de notificação: Na seção User Notifications, especifique quem deve receber o alerta. Você tem duas opções principais:
    - Gerente do ator: Envia a notificação diretamente ao gerente do usuário que disparou a violação de política.
    - Destinatário personalizado: Permite especificar qualquer endereço de email (por exemplo, um centro de operações de segurança ou um chefe de departamento específico).
2. Selecionar modelo de mensagem: Você pode escolher entre oModelo de notificação

padrãoou umaNotificaçãopersonalizada.
    - Recomendação: Se a sua organização tiver requisitos de marca interna ou mensagens de conformidade específicos, use a opçãoPersonalizarpara personalizar o corpo do e-mail para fornecer instruções claras e práticas ao destinatário.
3. Revisar e salvar: Depois de configuradas, certifique-se de que as configurações estejam alinhadas com as políticas operacionais e de conformidade da sua organização.

Prática recomendada: Habilitar essas notificações é uma maneira eficaz de reduzir violações repetidas de políticas, instruindo os usuários em tempo real sobre procedimentos de tratamento de dados confidenciais.



Note: As opções de notificação podem variar com base na configuração do locatário e nas configurações de política.

Etapa 10: Revisar e salvar a regra

Após concluir a configuração da regra:

1. Revisar todas as configurações definidas.
2. Verifique se as classificações de dados selecionadas, o escopo da inspeção, as condições do remetente e do destinatário e a ação correspondem ao comportamento da política pretendida.
3. Clique emSalvar para criar a regra de DLP de Email.

A política DLP de e-mail agora está ativa no Cisco Secure Access.

Opção 2: Criar uma Regra de DLP de Email Usando um Modelo de DLP Personalizado

A criação de um modelo de DLP personalizado envolve duas fases principais: definição de um identificador personalizado e configuração da classificação de dados.

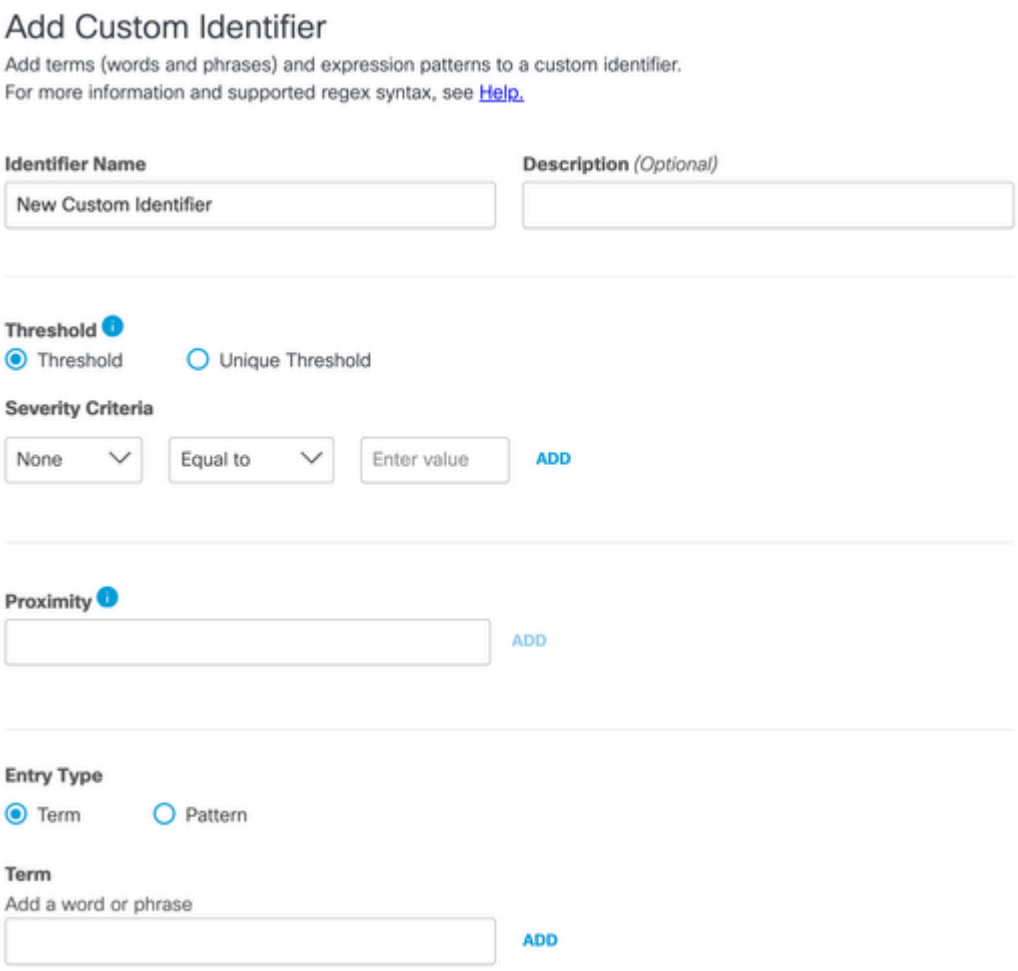
Note: O mecanismo de Classificação de Dados é altamente flexível, permitindo criar políticas usando um único Identificador Personalizado ou uma combinação de Identificadores Personalizado e Predefinido vinculados por operadores E/OU booleanos.

Etapa 11: Criar um identificador personalizado

Para definir um novo padrão de dados para detecção, siga estas etapas:

1. Faça login no painel de acesso seguro.
2. Navegue atéSecure > Data Classification.
3. Clique em Adicionar identificador personalizado.
4. Configure os seguintes parâmetros na janela Adicionar identificador personalizado:

- Nome e Descrição: Forneça um nome exclusivo e uma breve descrição do tipo de dados que você pretende detectar.
- Limite:
    - Limite: Monitora a frequência total dos dados detectados.
    - Limite Exclusivo: Monitora somente o número de ocorrências de funil dos dados, ignorando duplicatas.
- Critérios de severidade: Atribua níveis de gravidade (Muito baixo, Baixo, Médio, Alto) com base na frequência de detecção. Você pode defini-las usando operadores de comparação, comoIgual a, Maior que, Menor que ouIntervalo.
- Proximidade: Defina o limite de proximidade. Isso se aplica a todos os termos e padrões definidos nesse identificador coletivamente, em vez de por termo individual.
- Tipo de entrada: Defina como o sistema identifica os dados:
    - Termo: Uma palavra ou frase específica.
    - Padrão: Uma expressão regular (regex) usada para detectar formatos de dados específicos (por exemplo, números de cartão de crédito ou códigos de projeto internos).



Etapa 12: Configurar Classificação de Dados

Depois que o identificador personalizado for salvo, você poderá integrá-lo a um objeto de classificação de dados:

1. Navegue atéSecure > Data Classification > Add (Proteger > Classificação de dados > Adicionar) (use o botão no canto superior direito)
2. Selecione o identificador personalizado recém-criado na lista disponível.
3. (Opcional) Combine seu identificador personalizado com identificadores predefinidos usando a lógica AND/OR para refinar o escopo de detecção.
4. Salve a configuração para disponibilizá-la para uso em suas políticas de DLP de e-mail.
5. Consulte a captura de tela abaixo para obter mais informações.
6. Agora, siga as mesmas etapas da Etapa 4 à Etapa 10 para criar uma política usando a classificação de dados personalizada.

Essa configuração garante que a sua organização possa detectar informações confidenciais adaptadas especificamente às suas estruturas de dados internas e aos requisitos de conformidade.

Troubleshooting

Se a regra DLP de e-mail não se comportar como esperado, revise o seguinte:

A regra não corresponde aos e-mails

- Confirme se o modelo de classificação de dados correto está selecionado.
- Verifique se os locais de inspeção relevantes estão ativados:
  - Assunto do e-mail
  - Corpo da mensagem
  - Nome do anexo
  - Conteúdo do anexo
- Certifique-se de que os filtros de remetente e destinatário não excluam involuntariamente o e-mail de teste.

Os e-mails não estão bloqueados

- Verifique se a ação da regra está definida como Bloquear e nãoMonitorar.
- Confirme se a regra foi salva e ativada.
- Verifique se o conteúdo do e-mail corresponde positivamente aos critérios de DLP configurados.

Os eventos DLP não estão visíveis no ETD

- Confirme se o Cisco ETD e o Cisco Secure Access estão integrados corretamente.
- Verifique se o ETD está processando ativamente o tráfego de e-mail relevante.
- Verifique se o evento de política está presente primeiro no Cisco Secure Access.

As correspondências baseadas em anexo não são detectadas

- Confirme seAttachment Name e/orAttachment Contentesestão selecionados no escopo de inspeção.
- Verifique as configurações de controle de arquivo se rótulos comoMIPorTitus fizerem parte da lógica da regra.

Melhores práticas

Considere as seguintes práticas recomendadas ao implantar políticas de DLP de e-mail:

- Inicie comMonitormode para validar o comportamento da política antes de enforceBlock.
- Use nomes de regras claros e descritivos para facilitar a administração.
- Defina o escopo das condições do remetente e do destinatário cuidadosamente para reduzir correspondências não intencionais.
- Teste com dados representativos antes de uma implantação ampla.
- Revise o controle de mensagens ETD regularmente para validar atividades de email bloqueadas ou monitoradas.
- Use modelos personalizados onde identificadores de dados específicos da empresa são necessários.

Summary

O Cisco Secure Access é a plataforma central para configurar políticas de DLP de e-mail em uma implantação integrada do Cisco Secure Access e do Cisco Email Threat Defense. Embora o ETD ofereça visibilidade e rastreamento de mensagens, toda a criação de regras DLP, seleção de classificação, ação de aplicação e notificações são configuradas no Secure Access.

Usando modelos DLP predefinidos ou personalizados, os administradores podem inspecionar o conteúdo e os anexos de e-mail, definir o escopo do remetente e do destinatário e aplicar ações de Monitoramento ou Bloqueio para ajudar a evitar a perda de dados confidenciais por e-mail.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.