Regras de tamanho de arquivo DLP de acesso seguro sem classificação de dados Não gerar eventos de monitoramento para arquivos de texto

Contents

Problema

Uma política do Cisco Secure Access Web DLP configurada somente com critérios de tamanho de arquivo (sem Classificação de Dados) não gera eventos de monitor DLP para carregamentos de arquivo .txt, enquanto a mesma política aciona corretamente eventos de monitor para outros tipos de arquivo, como arquivos .xlsx, .png e .pdf. A política afetada Política de Gerenciamento Sênior - Web é configurada com:

- Controle de arquivos com tamanho de arquivo personalizado entre 1 KB e 49 MB
- Nenhum critério de classificação de dados
- Ação definida para Monitorar

Os testes revelaram que:

- Os carregamentos de arquivos TXT não aparecem em eventos DLP quando Action = Monitor.
- Os mesmos arquivos TXT geram eventos DLP corretamente quando Action = Block.
- Os registros de atividades mostram todos os carregamentos de arquivos, inclusive arquivos TXT.
- Outros formatos de arquivo (PNG, PDF, XLSX) geram eventos DLP conforme esperado com a ação Monitorar.

Além disso, quando nenhuma Classificação de dados é configurada em regras DLP, os eventos DLP registrados sempre mostram a severidade Média, independentemente da configuração de

severidade de regra configurada.

Ambiente

- Cisco Secure Access (antigo Cisco Umbrella)
- Políticas da Web de DLP (Prevenção de perda de dados)
- Políticas de acesso à Internet com descriptografia HTTPS habilitada
- Teste de carregamento de arquivo realizado através de aplicativos da Web

Resolução

Este comportamento não está documentado, mas é esperado pelo projeto. Os tipos MIME, como texto/sem formatação, são ignorados do monitoramento DLP ao usar critérios somente de tamanho de arquivo com a ação Monitorar para evitar sobrecarga de log. A equipe de desenvolvimento confirmou que este é um comportamento intencional que não é documentado externamente.

Opções de solução

Opção 1 (Recomendada): Adicionar classificação de dados

Adicione quaisquer critérios amplos de Classificação de Dados à regra DLP enquanto mantém Ação = Monitorar.

Isso restaura:

- Geração de evento DLP de arquivo TXT
- Manipulação correta da severidade com base na configuração da regra

Opção 2: Alterar Ação para Bloquear

Altere a ação da regra de Monitor para Bloquear. Isso gera eventos DLP para arquivos TXT, mas também impõe o bloqueio, que não pode ser desejado para casos de uso somente de monitoramento.

Resultados dos testes de laboratório

Testes de laboratório abrangentes confirmaram os padrões de comportamento.

Cenário de teste 1: Regra de DLP com classificação de dados e tamanho de arquivo (1 KB a 49 MB), ação = bloquear

- Arquivo TXT com PII: Bloqueado e registrado
- Arquivo PDF: Bloqueado e registrado
- Arquivo TXT sem PII: Permitido (esperado)
- PNG com PII: Permitido (esperado com base na classificação)

Cenário de teste 2: Regra DLP com tamanho de arquivo apenas (sem classificação de dados), ação = bloquear

- Todos os tipos de arquivos (TXT, PDF, PNG): Bloqueado e registrado
- A gravidade mostra como Média apesar da regra configurada como Baixa

Cenário de teste 3: Regra DLP somente com tamanho de arquivo (sem classificação de dados), Ação = Monitor

- Arquivos TXT: Permitido, mas NÃO registrado em eventos DLP
- Arquivos PDF e PNG: Eventos DLP permitidos e conectados
- Os registros de atividades mostram todos os carregamentos, inclusive arquivos TXT

Causa

Esse é um comportamento intencional, mas não documentado, no Cisco Secure Access DLP. O sistema ignora o log de eventos DLP para tipos MIME de texto/sem formatação ao usar regras somente de tamanho de arquivo com a ação Monitorar para evitar a geração excessiva de logs. O comportamento depende da ação e é específico do tipo MIME:

- Monitorar ação com critérios somente de tamanho de arquivo: Arquivos TXT ignorados do registro
- Ação de bloqueio com critérios somente de tamanho de arquivo: Arquivos TXT registrados normalmente
- Qualquer ação com classificação de dados presente: Arquivos TXT registrados normalmente

O problema de gravidade ocorre porque os eventos DLP derivam a gravidade dos metadados de Classificação de Dados, em vez das configurações de regra, ao operar no modo sensível a conteúdo. Sem a Classificação de dados, o sistema assume como padrão a gravidade "Média", independentemente da gravidade da regra configurada.

Conteúdo relacionado

- Configuração do tamanho do arquivo DLP do Cisco Secure Access

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.