Implemente o DLP no acesso seguro para restringir o uso do ChatGPT de IA aberta para programação

Contents

Introdução

Este documento descreve como implementar a Prevenção de Perda de Dados (DLP - Data Loss Prevention) no Acesso Seguro para restringir o uso do Open AI ChatGPT para programação e codificação.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso seguro
- DLP
- Abra o AI ChatGPT

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Acesso seguro
- DLP

- Abra o AI ChatGPT

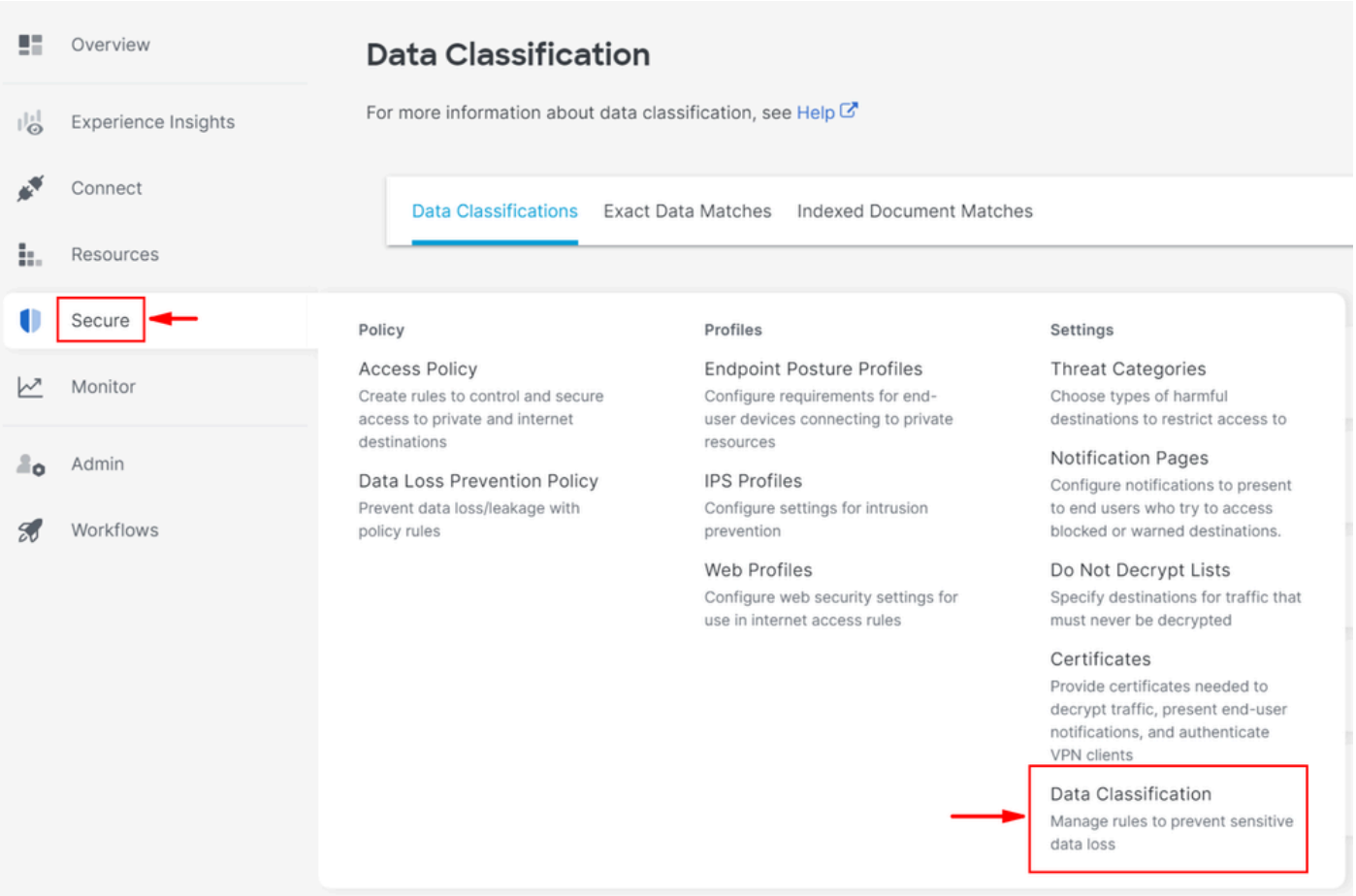
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

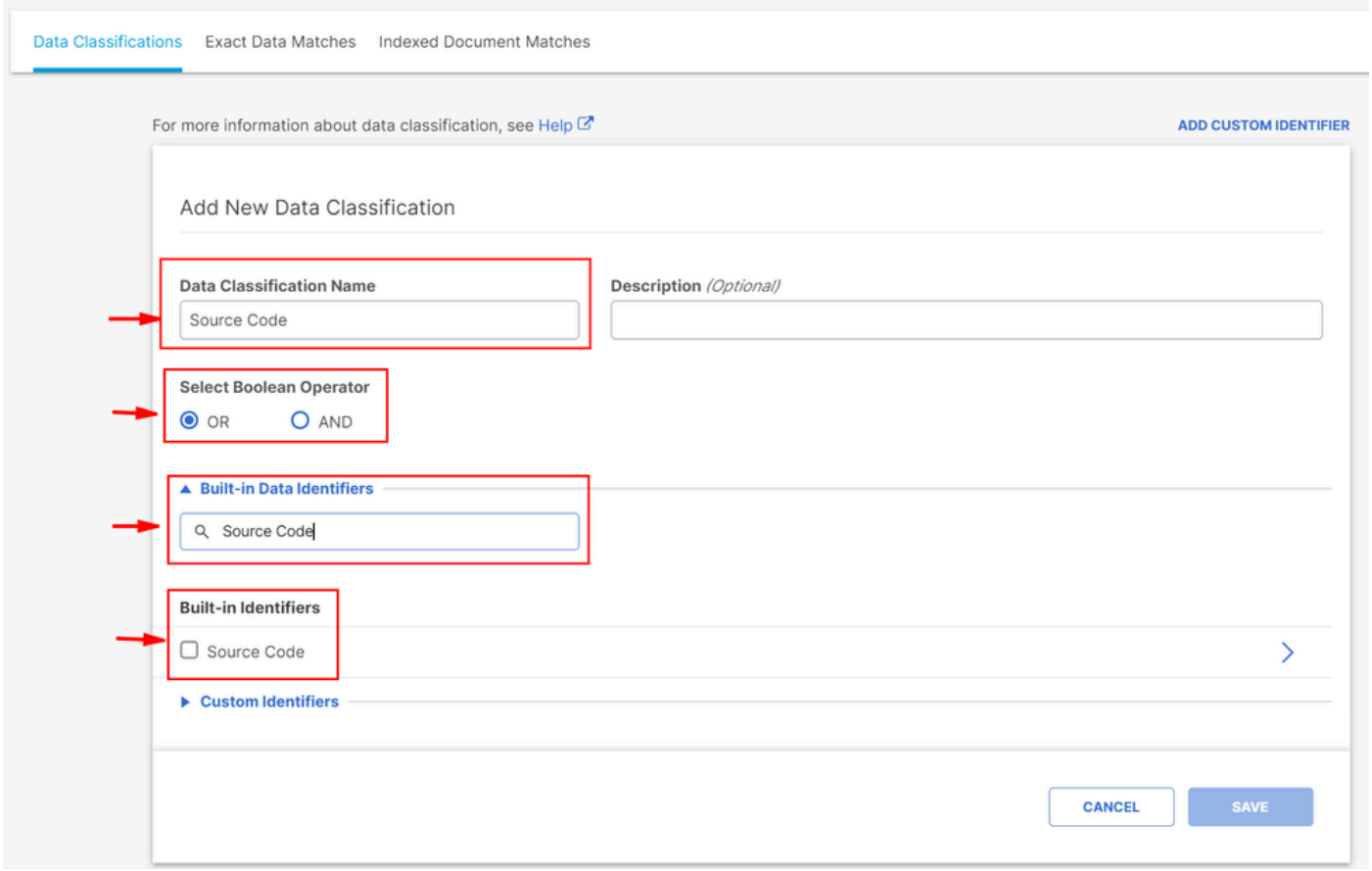
1.Crie uma classificação de dados para usar o Identificador de Dados do Código-Fonte

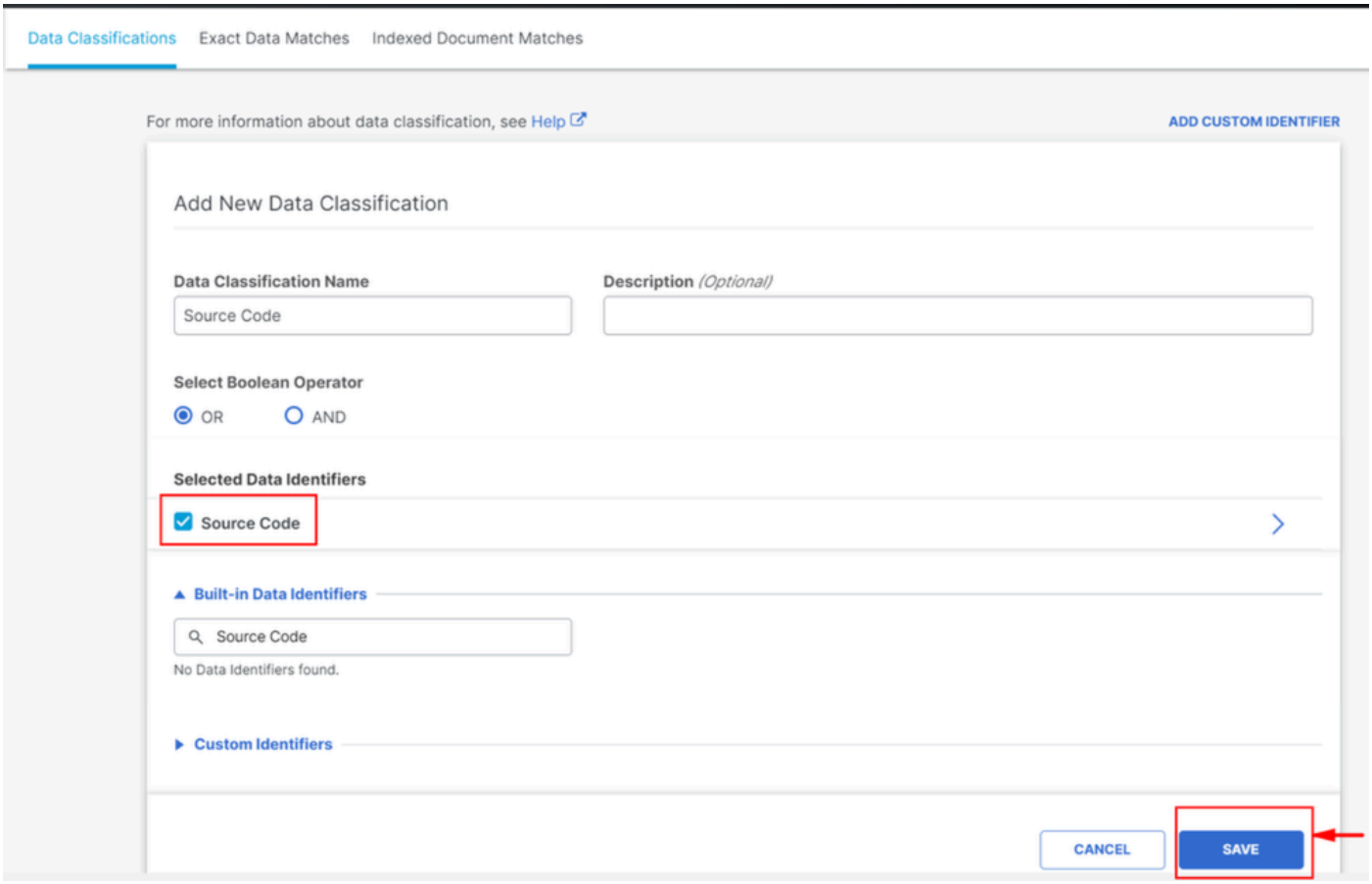
Navegue até [Painel de controle de acesso seguro.]

- Clique em Secure > Data Classification > Add



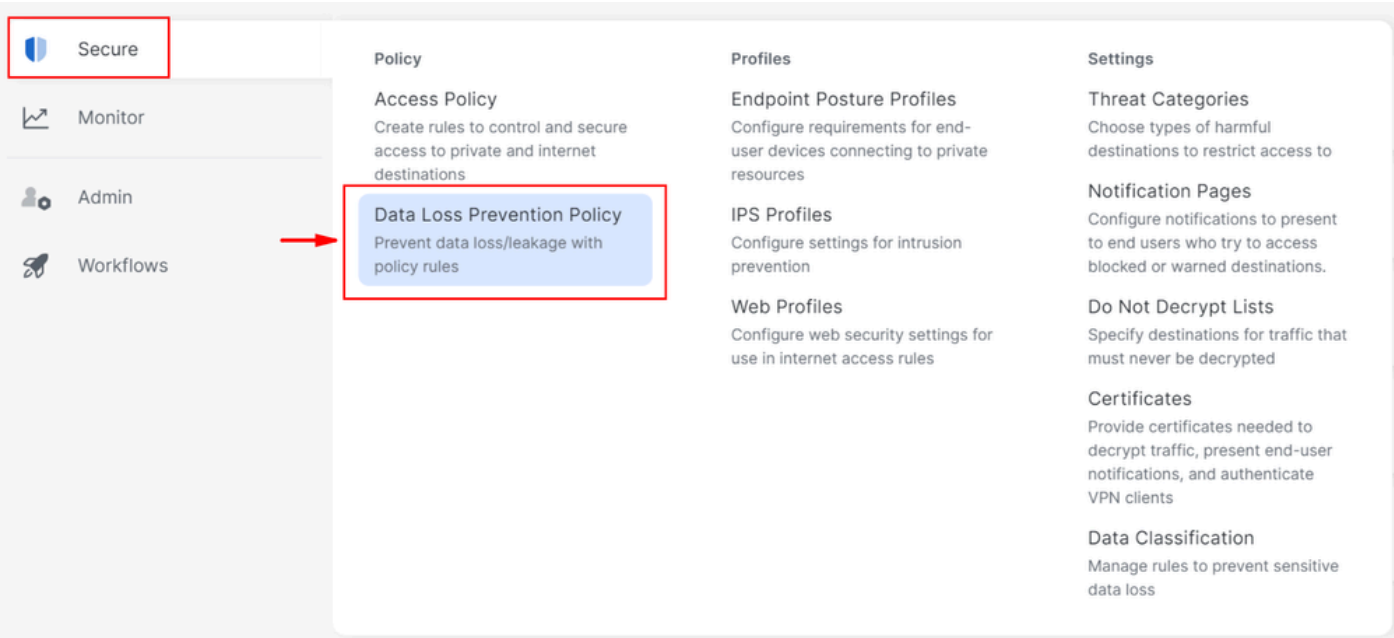
- Insira Data Classification Name > Selecionar Built-in Data Identifiers > Pesquisar Source Code e selecione-o



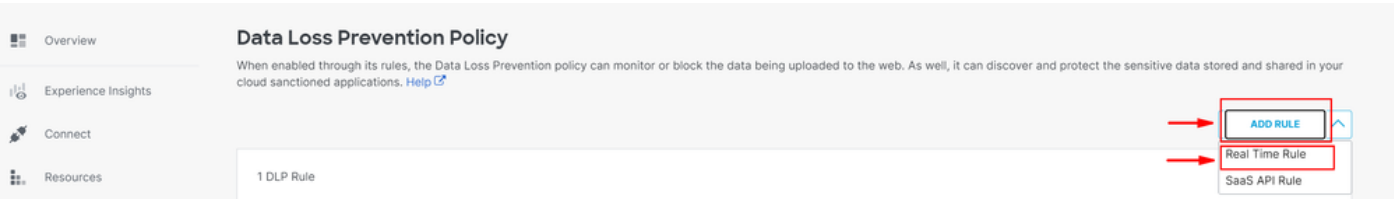


2.Crie uma Política DLP e chame a Classificação de Dados de "Código-fonte" nela.

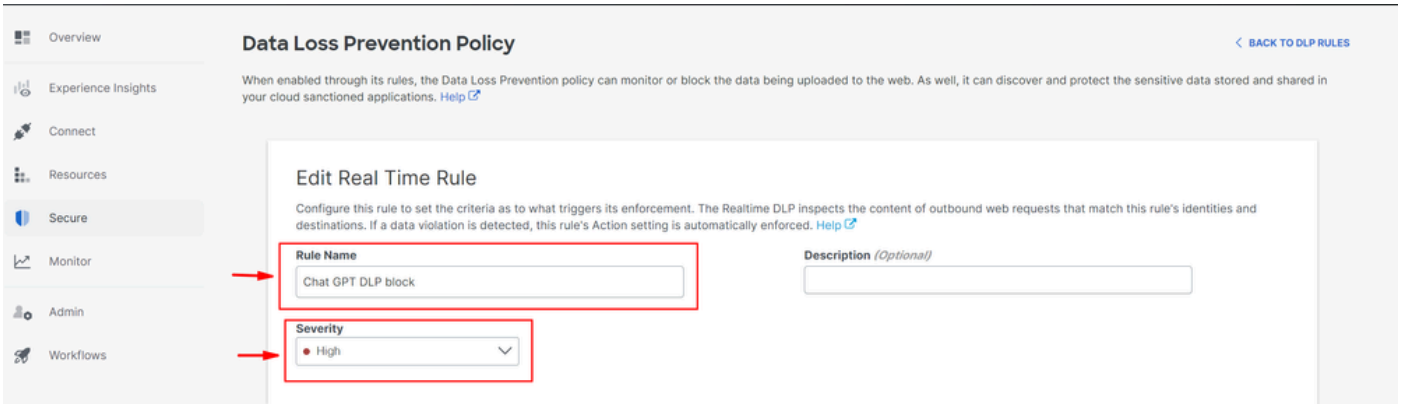
- Clique em Secure > Data Loss Prevention Policy



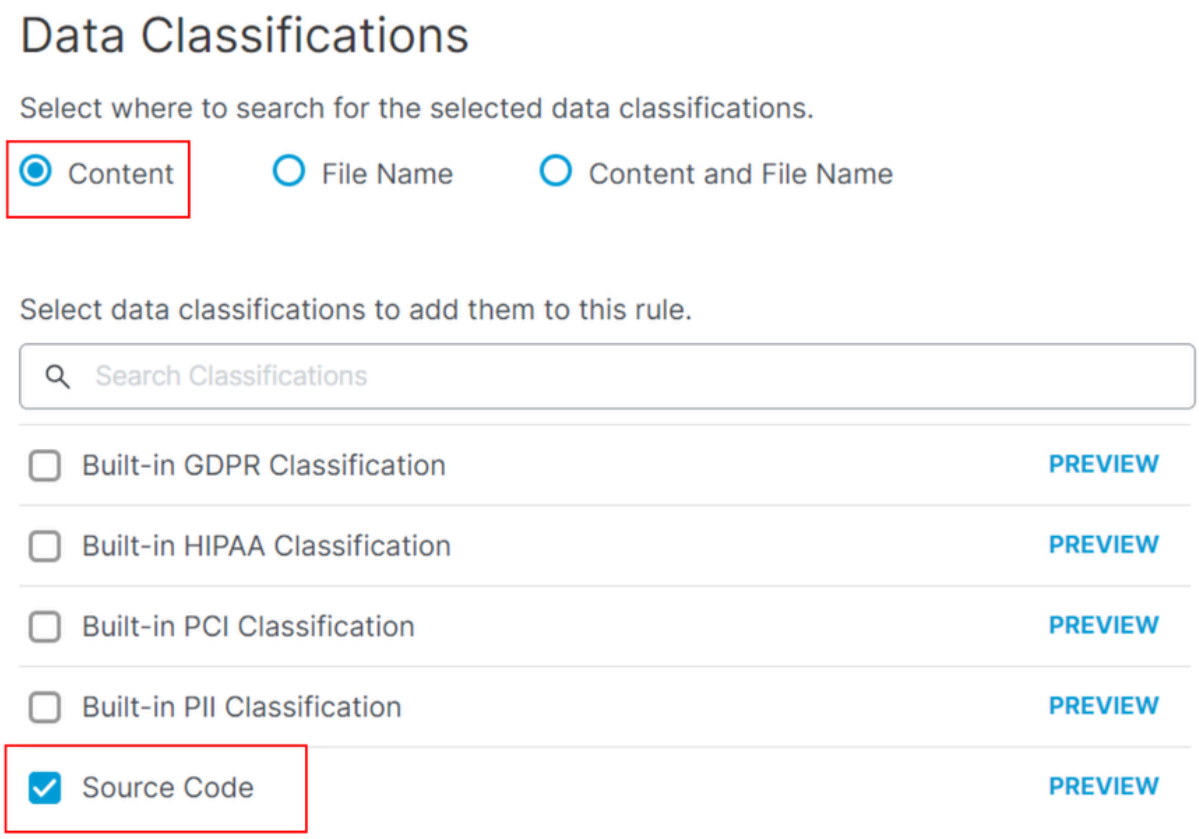
- Clique em Add Rule > Real Time Rule



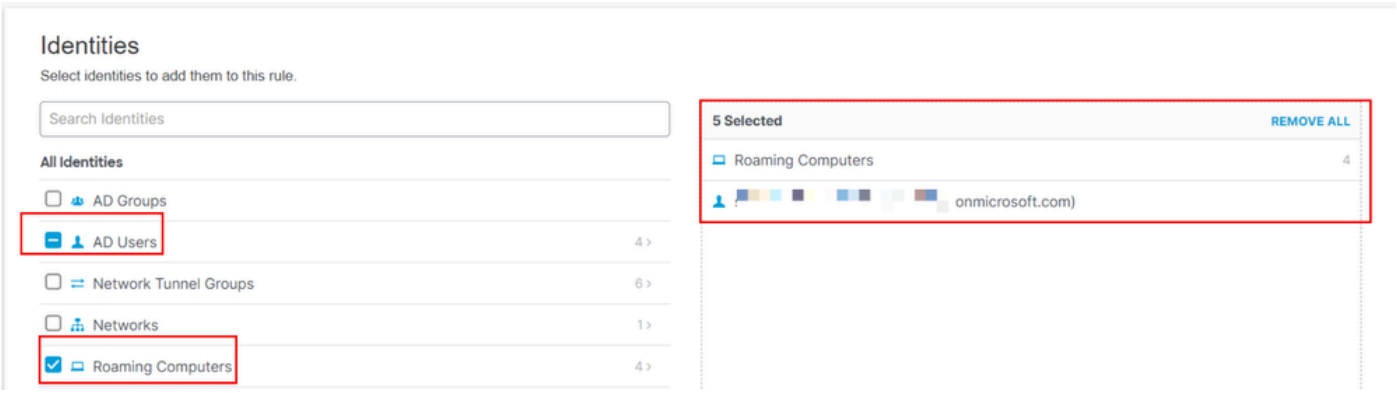
- Forneça um Rule Name > Conjunto apropriado Severity



- Em Data Classifications selecioneContent e selecione Source Code

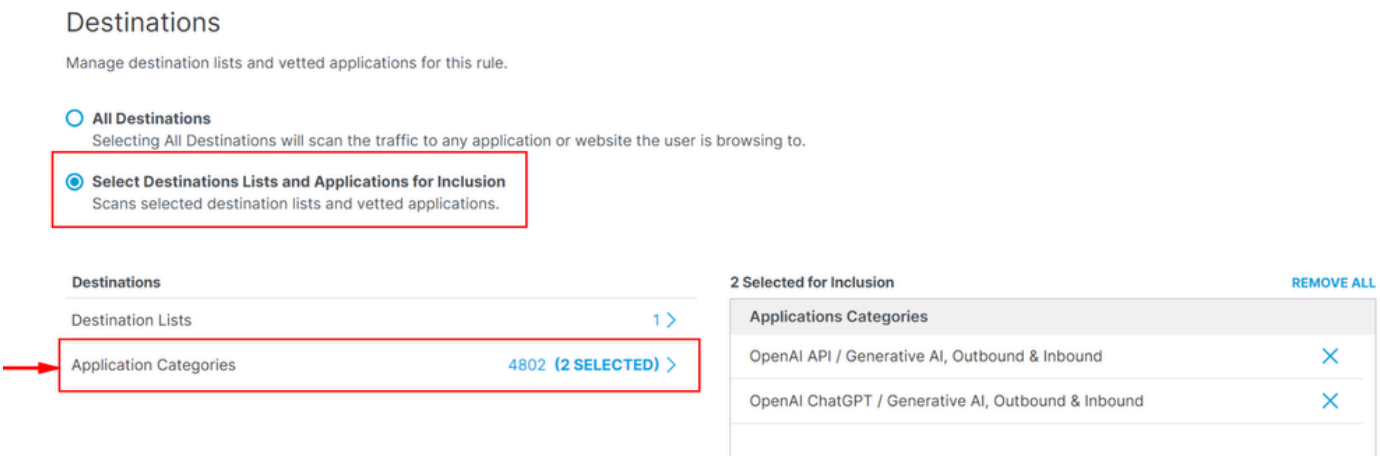


- Em Identitiesselecione as identidades desejadas conforme necessário

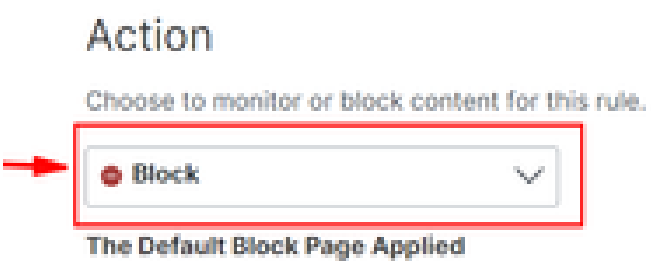


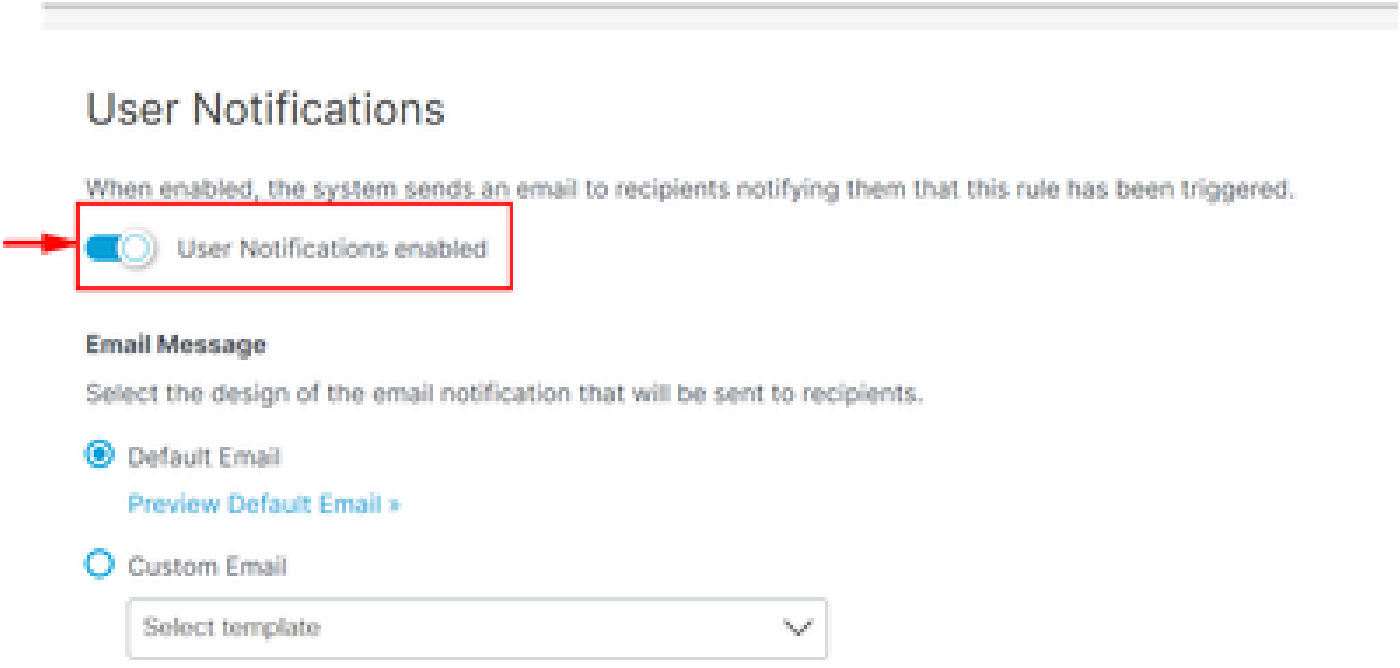
- Em Destinos, selecione Select Destination Lists and Applications for Inclusion

- Selecione Application Categories> Selecionar Generative AI > Selecionar OpenAI API (Vetted) e OpenAI ChatGPT (Vetted) em Outbound and InboundDirection

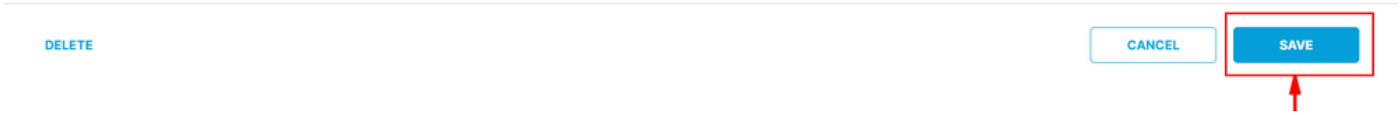


- Em Actionselecione Block
- Em User Notifications, você pode configurar notificações por e-mail para usuários finais quando a regra for acionada (opcional)





- Clique em Save



3. Verifique se você tem uma Diretiva de Acesso à Internet em vigor para o tráfego em direção à GPT de Bate-papo com Descriptografia habilitada.

Exemplo:

Chat GPT

Internet

General

Action	Allow
Last modified	[redacted]
Rule order	1
Logging	Enabled
Hits	216

Sources

Any

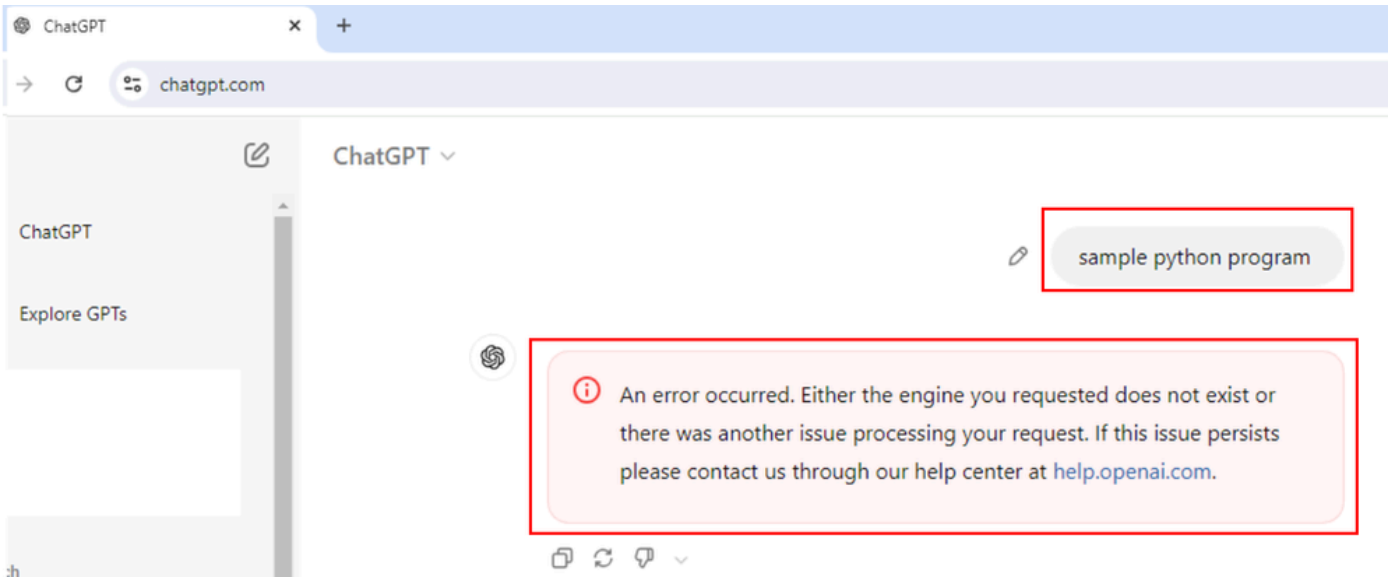
Destinations

2 destinations

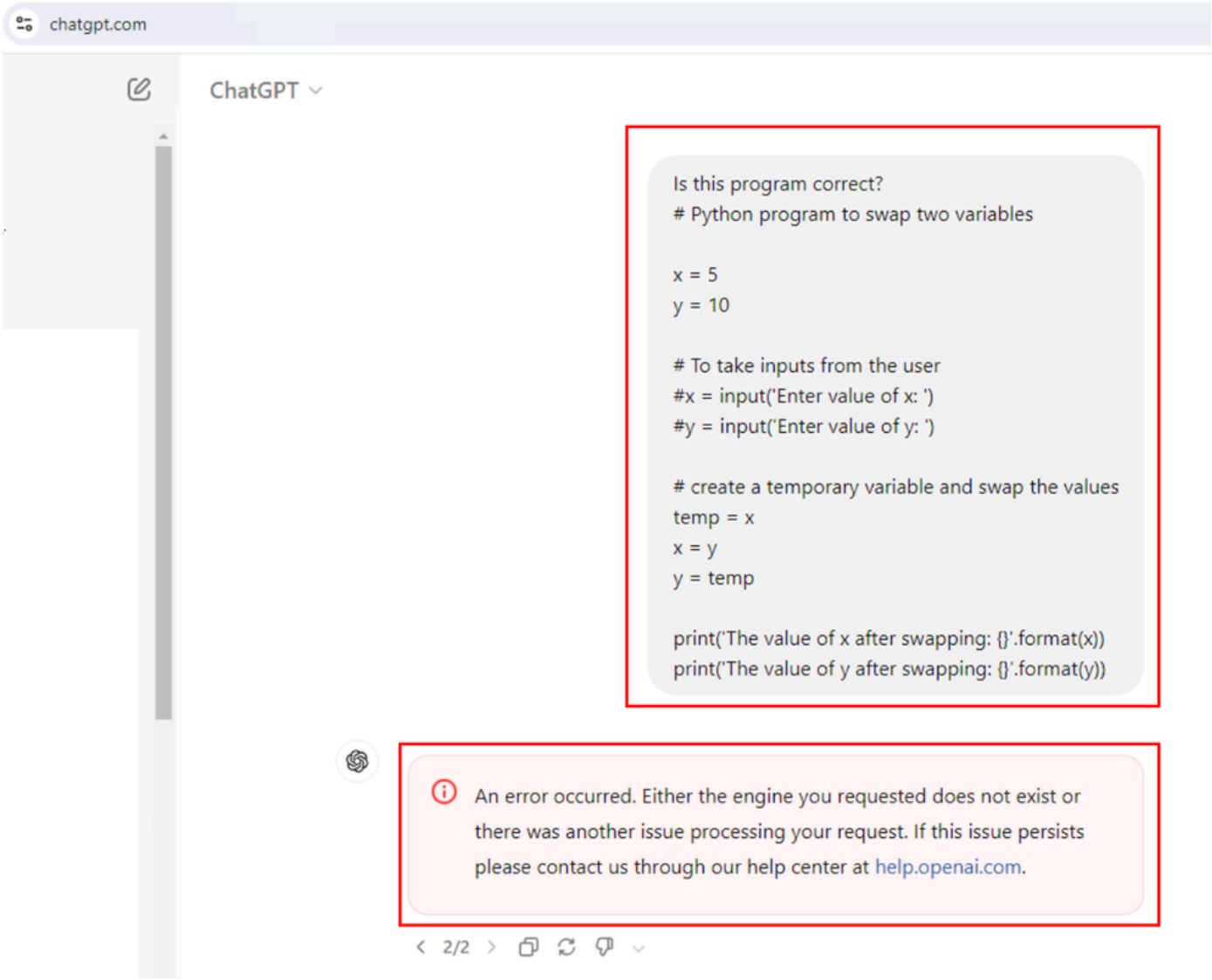
Application Settings (2)

OpenAI API OpenAI ChatGPT

- Peça um programa python de exemplo e esta solicitação será bloqueada.



- Pergunte se o programa está correto ou não e esta solicitação será bloqueada.

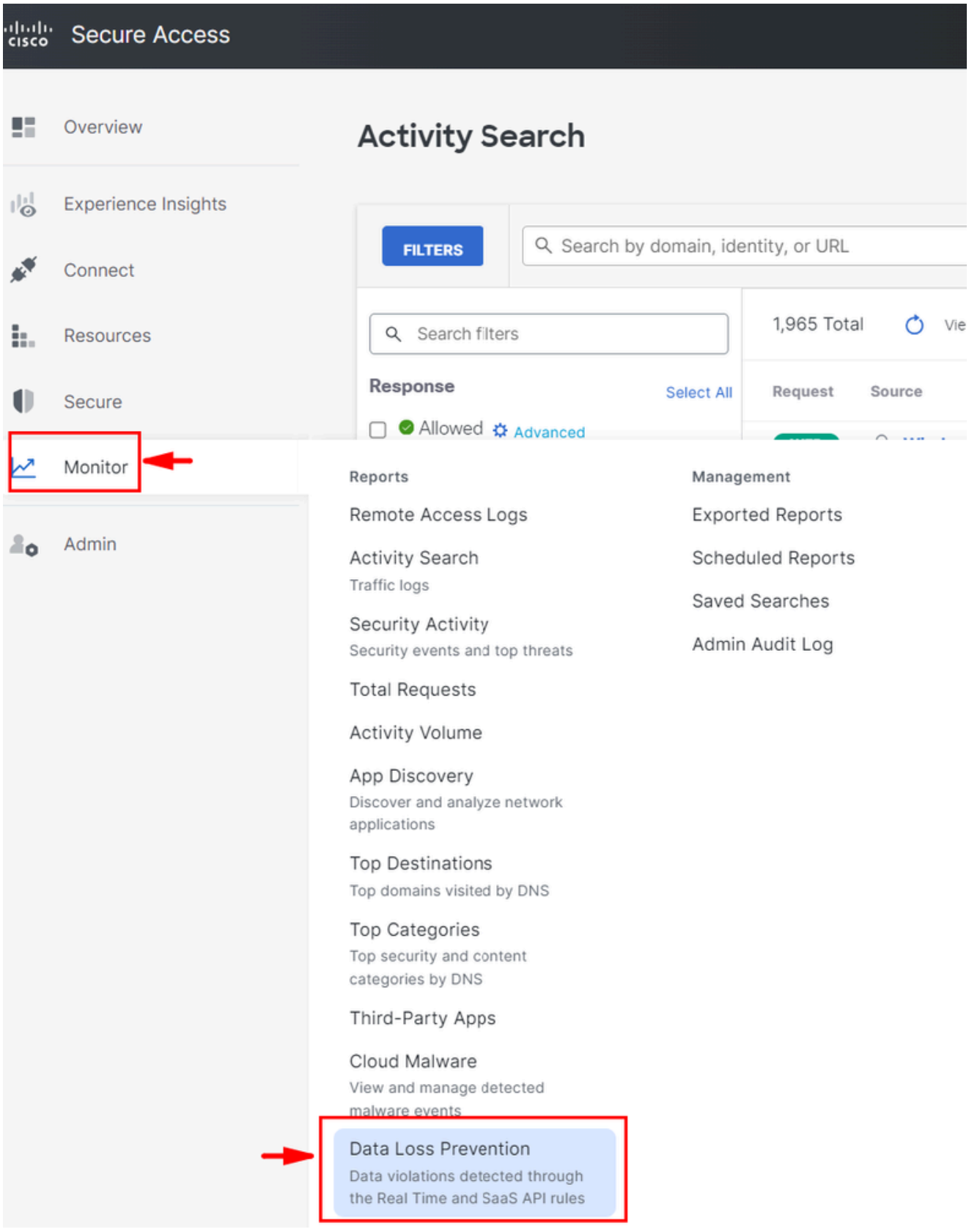


Verificar

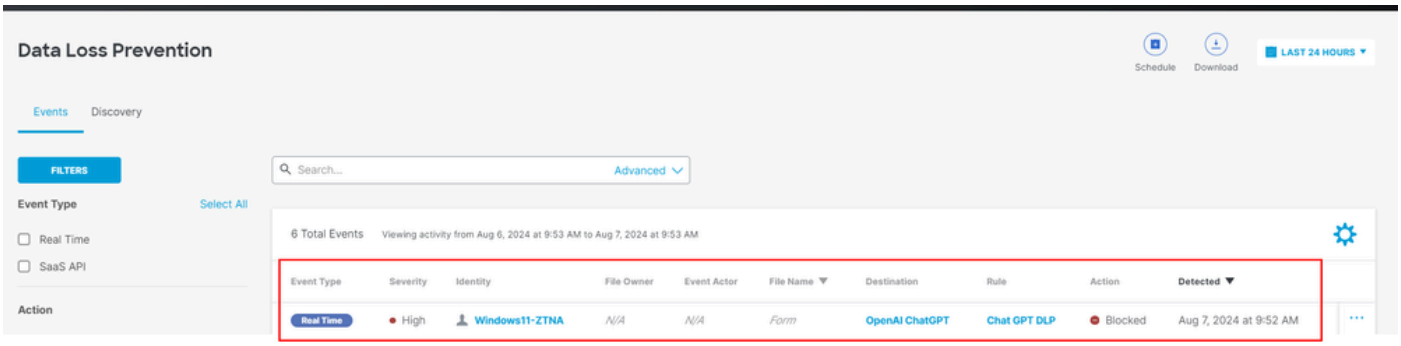
Podemos ver quando o usuário tenta pedir ao ChatGPT um programa python de exemplo, a solicitação é bloqueada.

Podemos confirmar se um evento DLP foi disparado nos logs de Prevenção de Perda de Dados de Acesso Seguro.

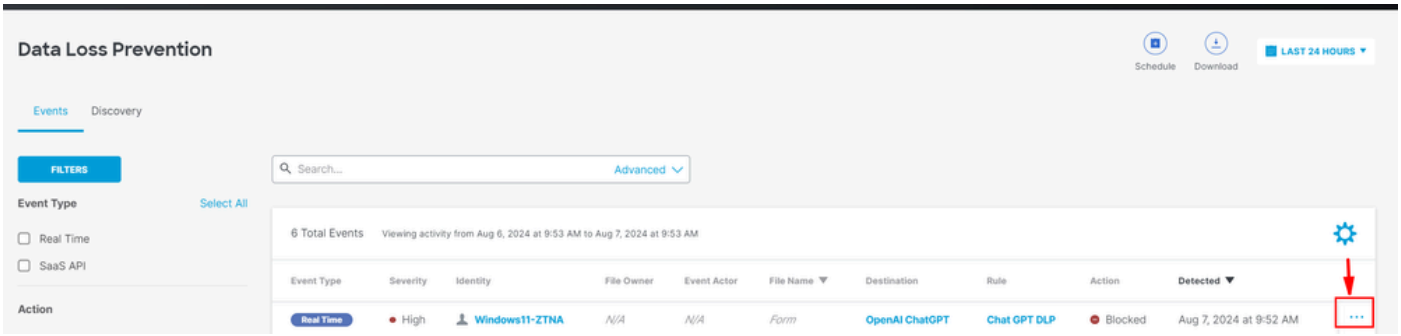
- Vá para Monitor> Data Loss Prevention



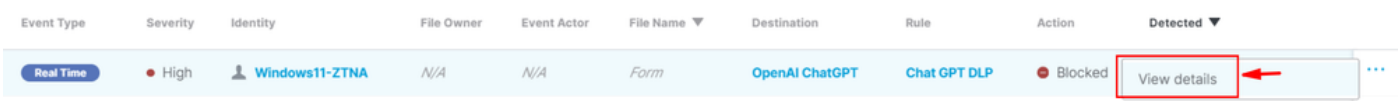
- Podemos ver o evento DLP.



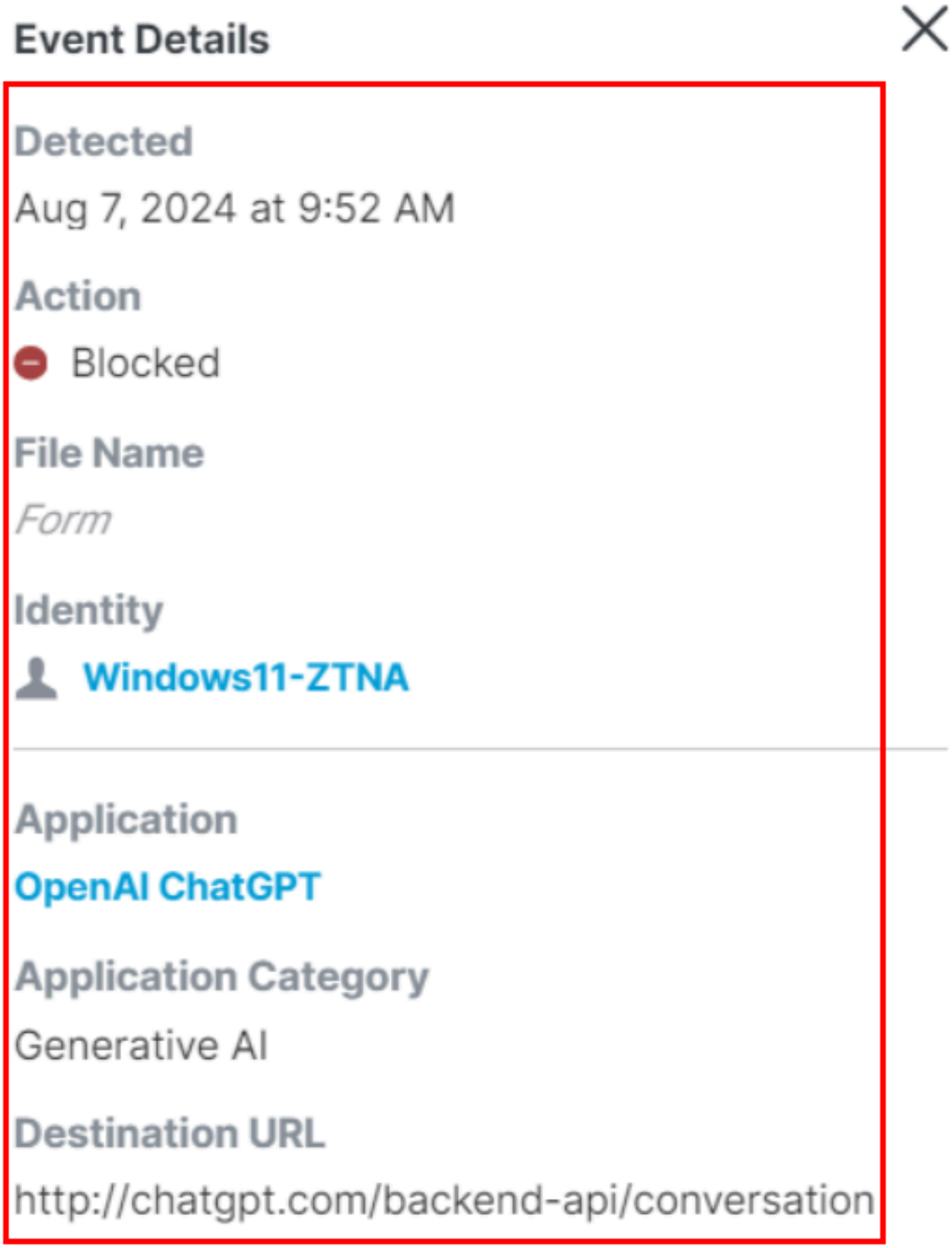
- Clique nos três pontos no final do registro de eventos para ver mais detalhes sobre o evento.



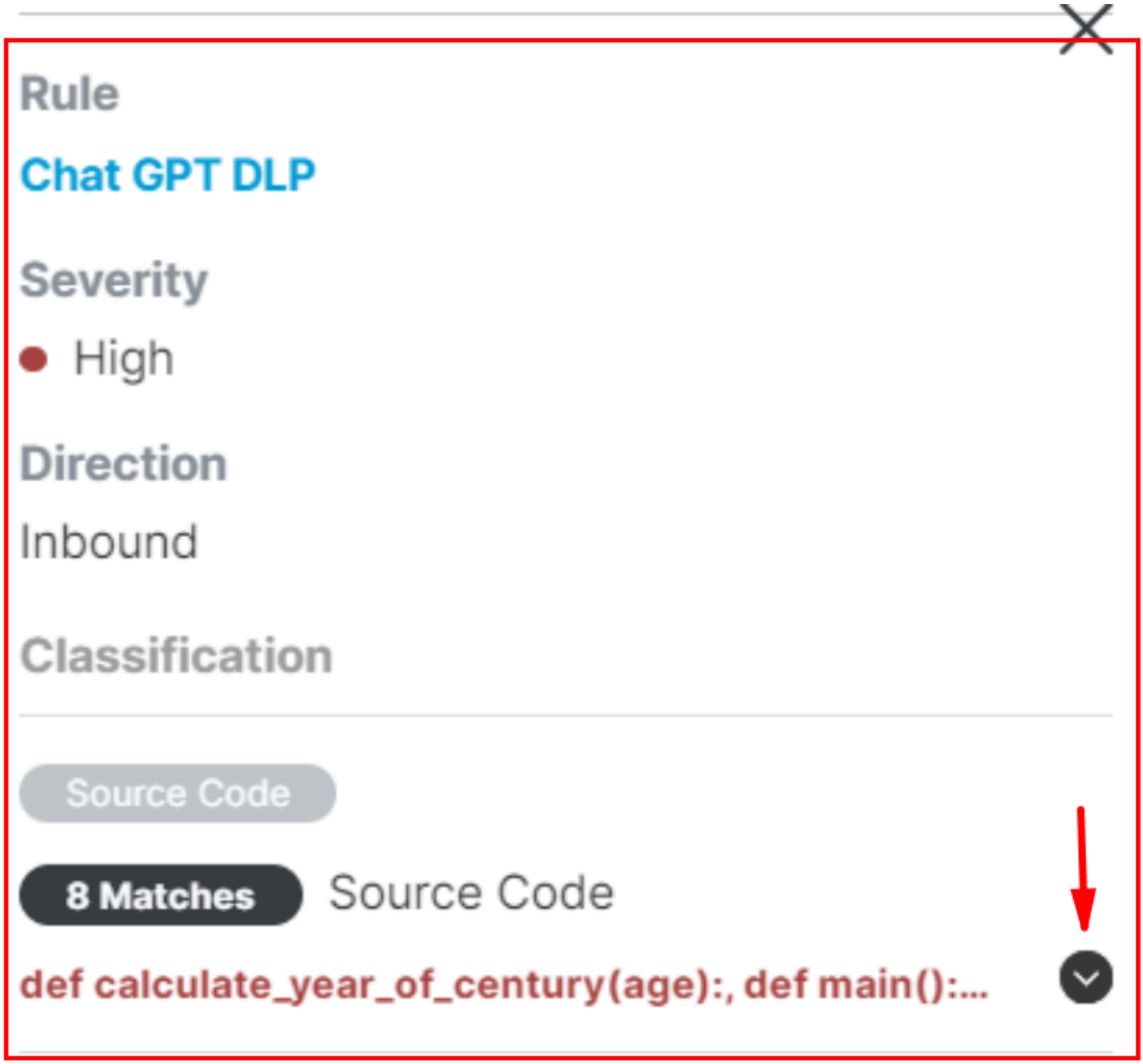
- Clique em View details.



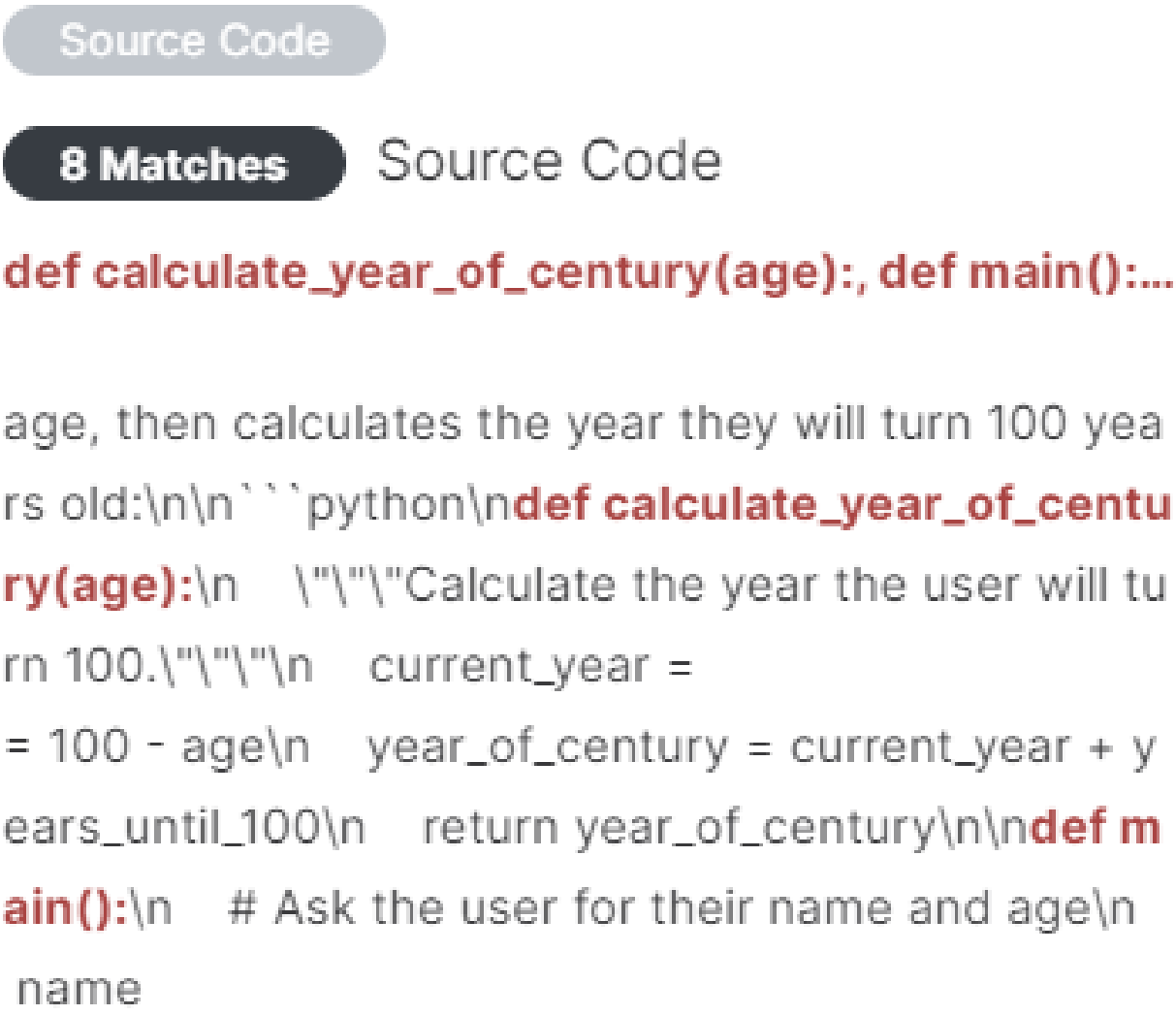
- Agora, vemos todos os Detalhes do evento.



- Expanda a classificação para ver qual conteúdo correspondeu ao classificador.

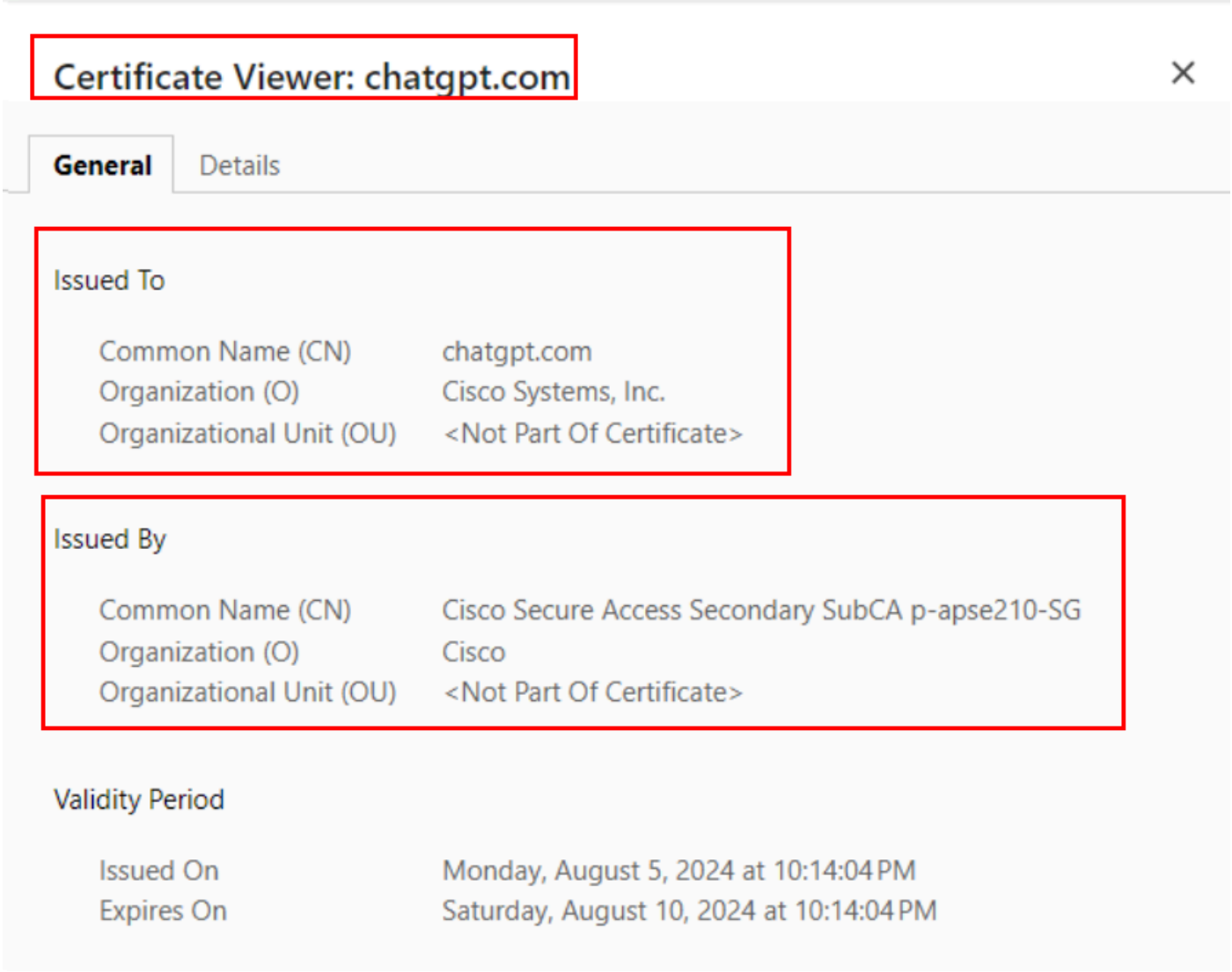


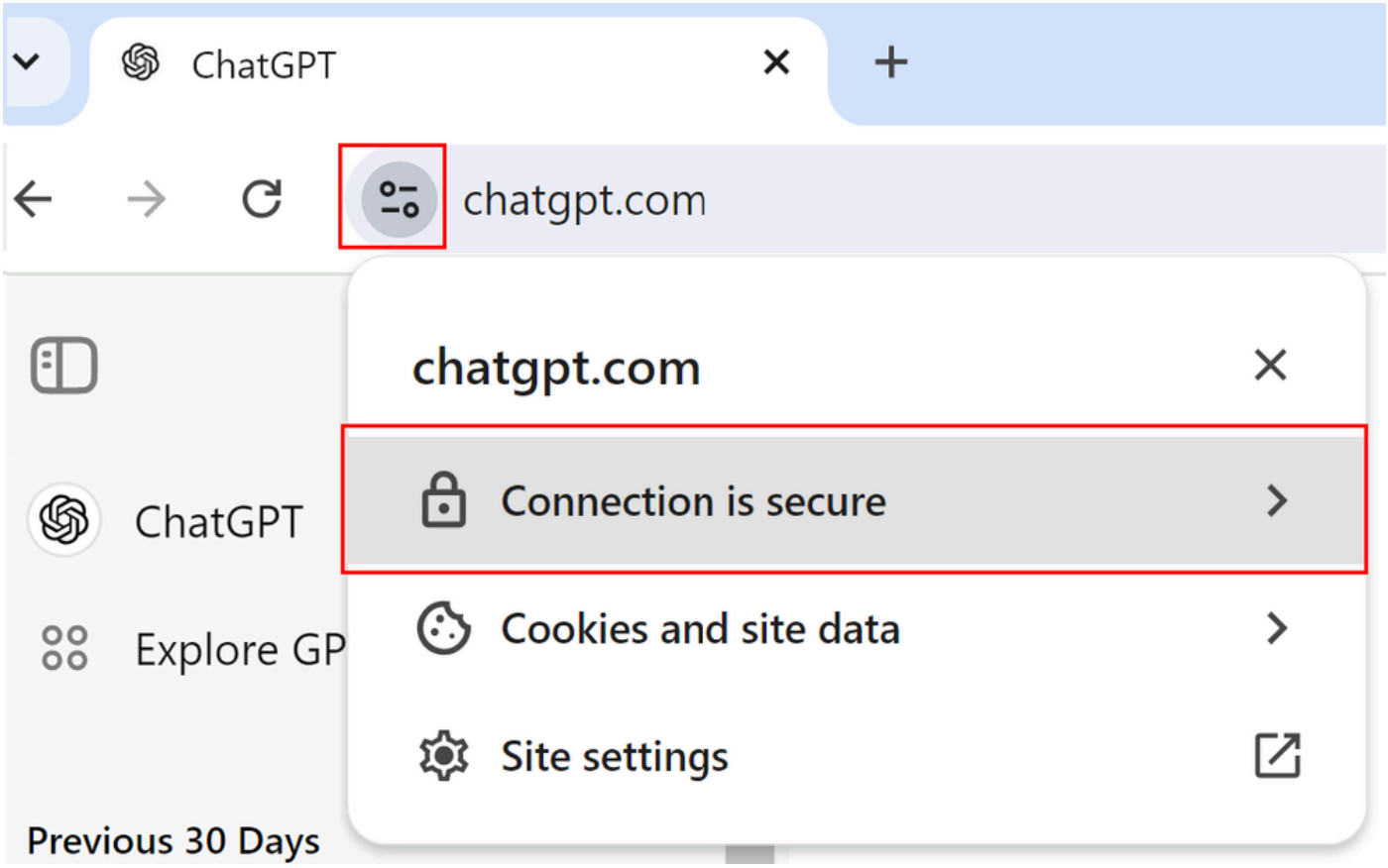
- Vemos todos os detalhes do conteúdo que correspondeu ao classificador/Classificação da política DLP.

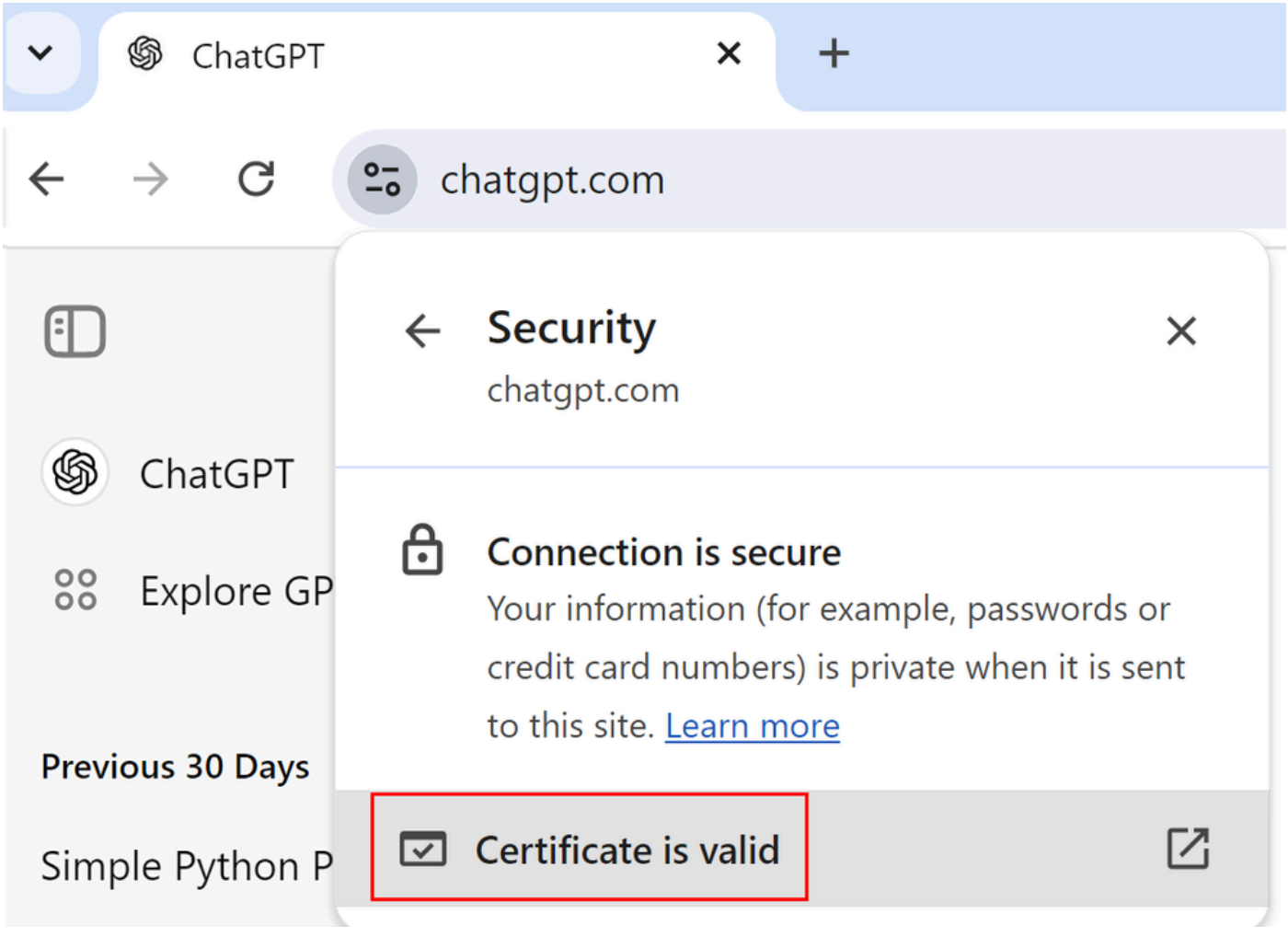


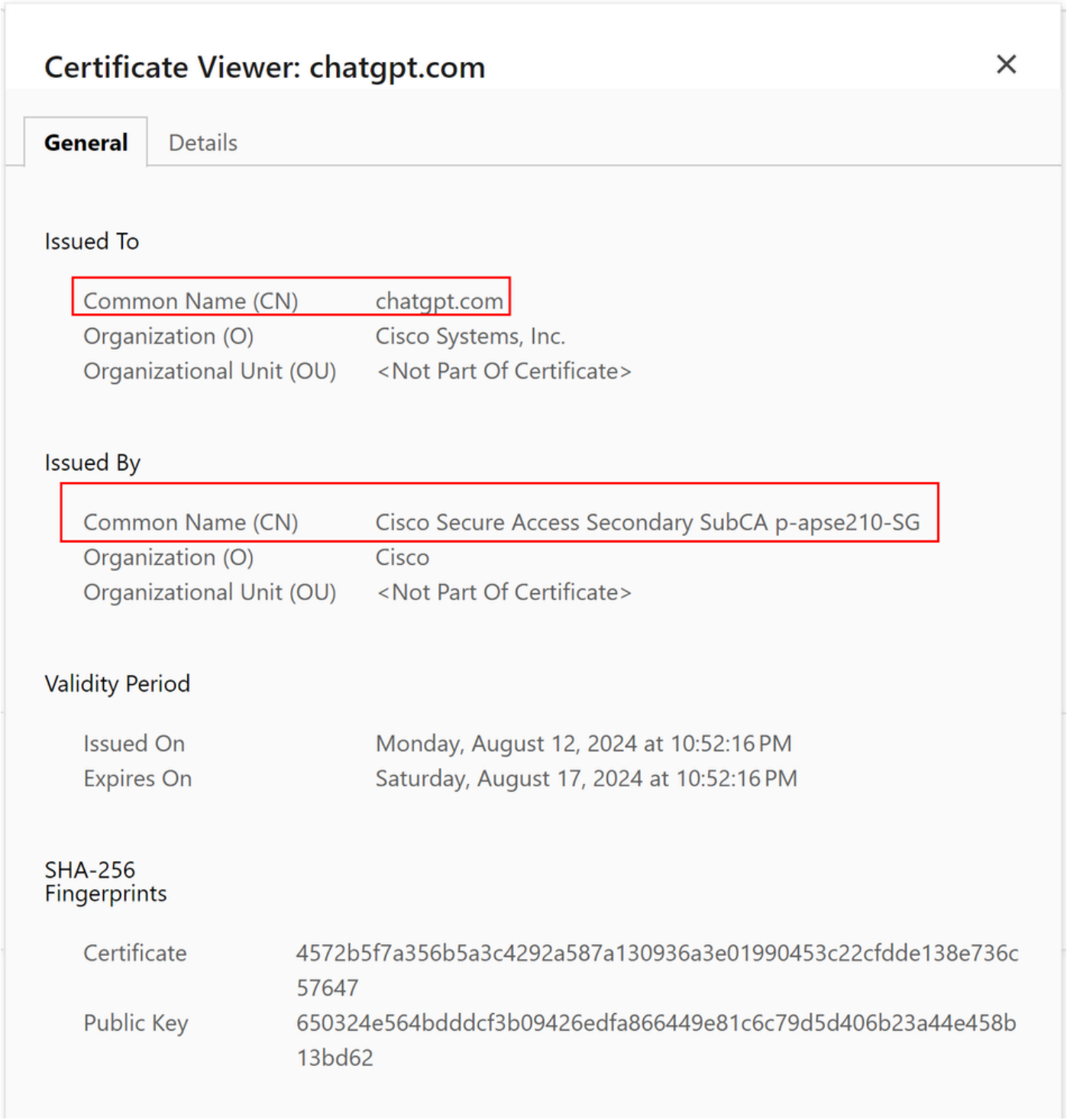
Troubleshooting

- Verifique se a política de acesso que corresponde às solicitações da Web para Open AI ChatGPT tem a descriptografia habilitada.
- Para verificar rapidamente se o SSE está descriptografando o tráfego para Open AI ChatGPT, verifique o certificado do site que mostra o nome comum inclui palavras-chave "Cisco Secure Access" nele.


Certificate Viewer: chatgpt.com
General
Details
Issued To
Common Name (CN) chatgpt.com
Organization (O) Cisco Systems, Inc.
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) Cisco Secure Access Secondary SubCA p-apse210-SG
Organization (O) Cisco
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Monday, August 5, 2024 at 10:14:04 PM
Expires On Saturday, August 10, 2024 at 10:14:04 PM

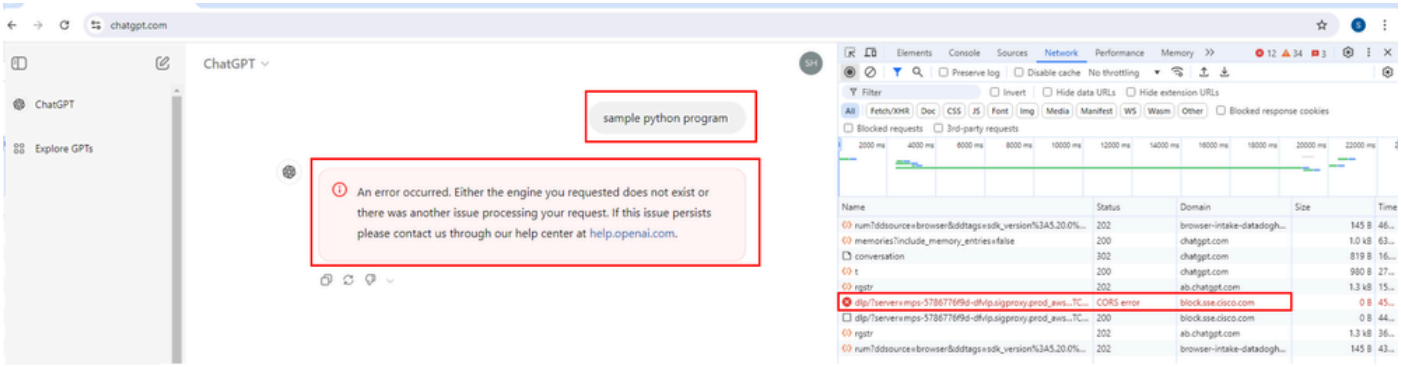

ChatGPT
chatgpt.com
chatgpt.com
Connection is secure
Cookies and site data
Site settings
ChatGPT
Explore GP
Previous 30 Days


ChatGPT
chatgpt.com
Security
chatgpt.com
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more
Certificate is valid
ChatGPT
Explore GP
Previous 30 Days
Simple Python P

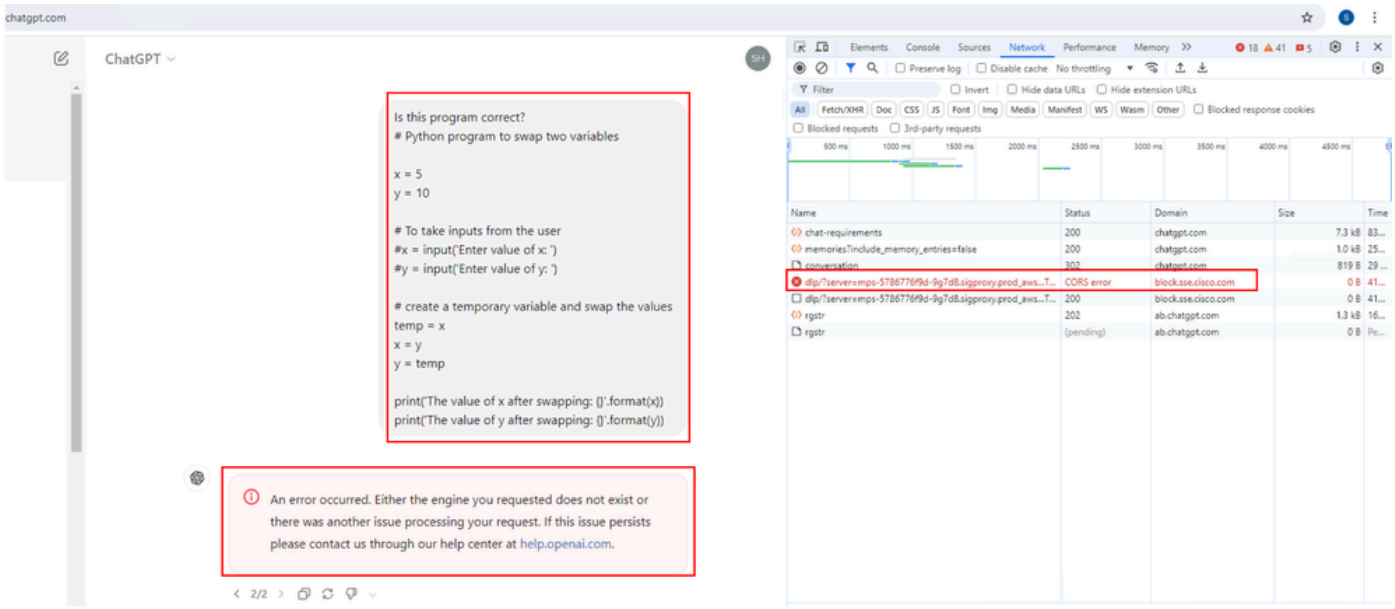


- Abra o ChatGPT > Abra as ferramentas do desenvolvedor > Selecione a rede > Em seguida, tente pedir ao ChatGPT um programa python de exemplo

- Observe que a solicitação resulta em um bloco. No domínio, você verá "block.sse.cisco.com



- Pergunte ao ChatGPT se o código do programa está correto.
- Observe que a solicitação resulta em um bloco e em "domínio" você vê "block.sse.cisco.com".



Informações Relacionadas

- Guia do usuário do Cisco Secure Access
- Suporte técnico e downloads da Cisco

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.