

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

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[1. Crie uma classificação de dados para usar o Identificador de Dados do Código-Fonte](#)

[2. Crie uma Política DLP e chame a Classificação de Dados de "Código-fonte" nela.](#)

[3. Verifique se você tem uma Diretiva de Acesso à Internet em vigor para o tráfego em direção à GPT de Bate-papo com Criptografia habilitada.](#)

[4. Using Open AI ChatGPT tente baixar ou carregar qualquer programa.](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

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

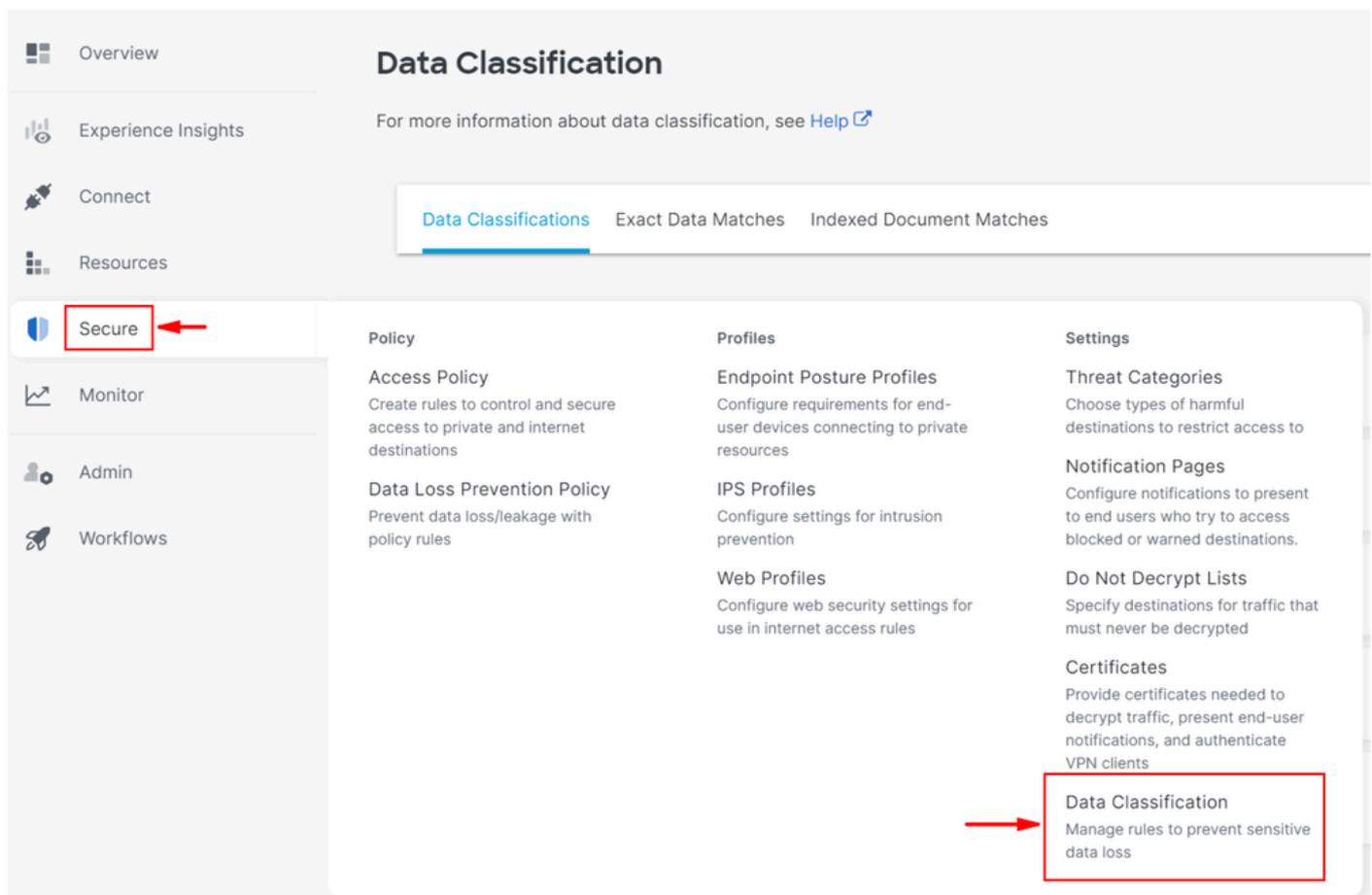
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Data Classifications Exact Data Matches Indexed Document Matches

For more information about data classification, see [Help](#)

[ADD CUSTOM IDENTIFIER](#)

Add New Data Classification

Data Classification Name

Description (Optional)

Select Boolean Operator
 OR AND

Built-in Data Identifiers

Built-in Identifiers
 Source Code

Custom Identifiers

Data Classifications Exact Data Matches Indexed Document Matches

For more information about data classification, see [Help](#)

[ADD CUSTOM IDENTIFIER](#)

Add New Data Classification

Data Classification Name

Description (Optional)

Select Boolean Operator
 OR AND

Selected Data Identifiers
 Source Code

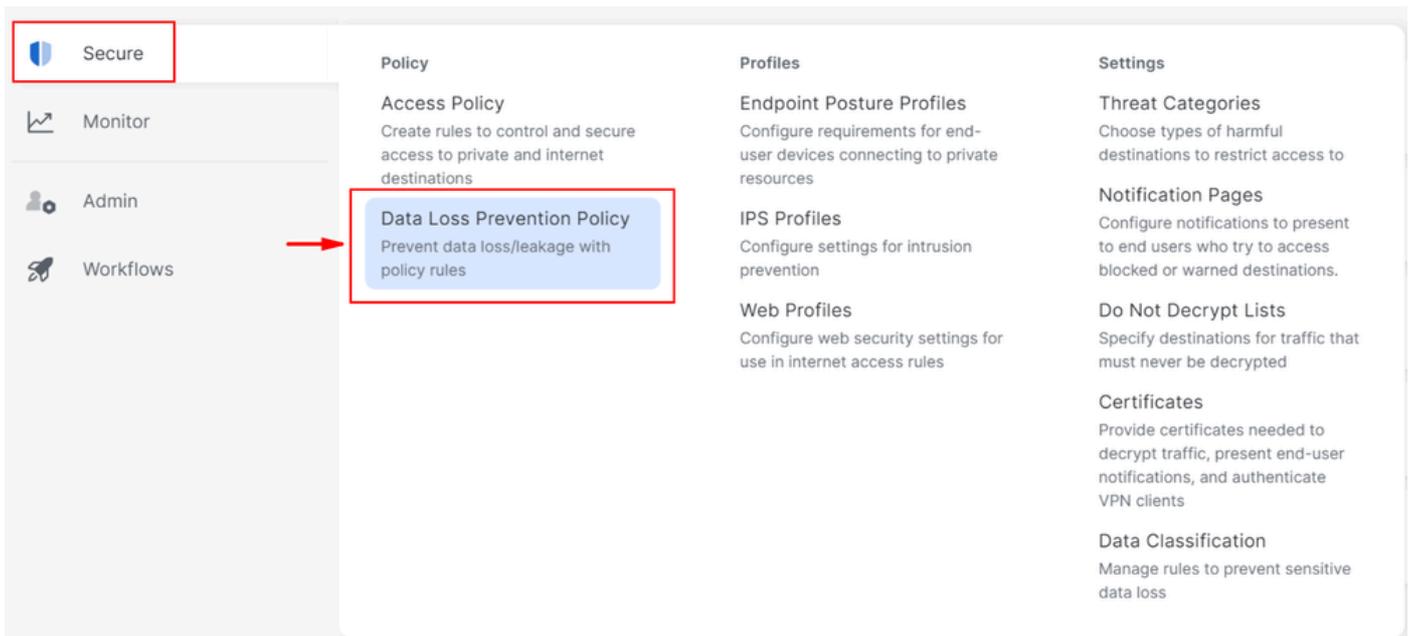
Built-in Data Identifiers

No Data Identifiers found.

Custom Identifiers

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

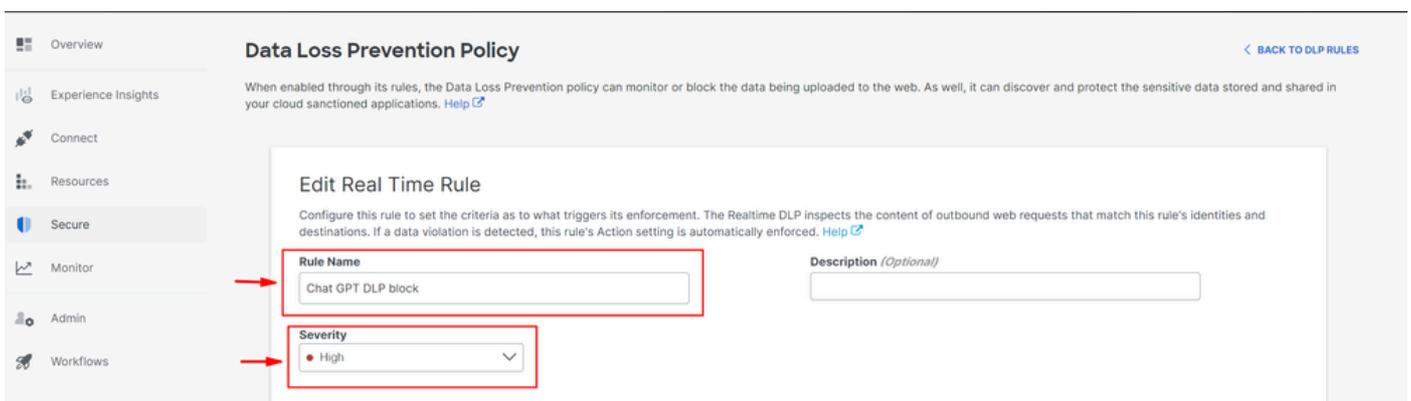
- Clique em Secure > Data Loss Prevention Policy



- Clique em Add Rule > Real Time Rule



- Forneça um Rule Name > Conjunto apropriado Severity



- Em Data Classifications selecione Content e selecione Source Code

Data Classifications

Select where to search for the selected data classifications.

- Content File Name Content and File Name

Select data classifications to add them to this rule.

Search Classifications

<input type="checkbox"/> Built-in GDPR Classification	PREVIEW
<input type="checkbox"/> Built-in HIPAA Classification	PREVIEW
<input type="checkbox"/> Built-in PCI Classification	PREVIEW
<input type="checkbox"/> Built-in PII Classification	PREVIEW
<input checked="" type="checkbox"/> Source Code	PREVIEW

- Em Identitiesselecione as identidades desejadas conforme necessário

Identities
Select identities to add them to this rule.

Search Identities

All Identities

- AD Groups
- AD Users
- Network Tunnel Groups
- Networks
- Roaming Computers

5 Selected REMOVE ALL

- Roaming Computers 4
- onmicrosoft.com)

- 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

Destinations

Manage destination lists and vetted applications for this rule.

All Destinations
Selecting All Destinations will scan the traffic to any application or website the user is browsing to.

Select Destinations Lists and Applications for Inclusion
Scans selected destination lists and vetted applications.

Destinations

Destination Lists [1 >](#)

Application Categories [4802 \(2 SELECTED\) >](#)

2 Selected for Inclusion

[REMOVE ALL](#)

Applications Categories

OpenAI API / Generative AI, Outbound & Inbound [×](#)

OpenAI ChatGPT / Generative AI, Outbound & Inbound [×](#)

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

Action

Choose to monitor or block content for this rule.

Block [▼](#)

The Default Block Page Applied

User Notifications

When enabled, the system sends an email to recipients notifying them that this rule has been triggered.

User Notifications enabled

Email Message

Select the design of the email notification that will be sent to recipients.

Default Email

[Preview Default Email >](#)

Custom Email

Select template [▼](#)

- Clique em Save

DELETE

CANCEL

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 Criptografia habilitada.

Exemplo:

Chat GPT



Internet

General

Action



Allow

Last modified



Rule order

1

Logging

Enabled

Hits

216

Sources

Any

Destinations

2 destinations

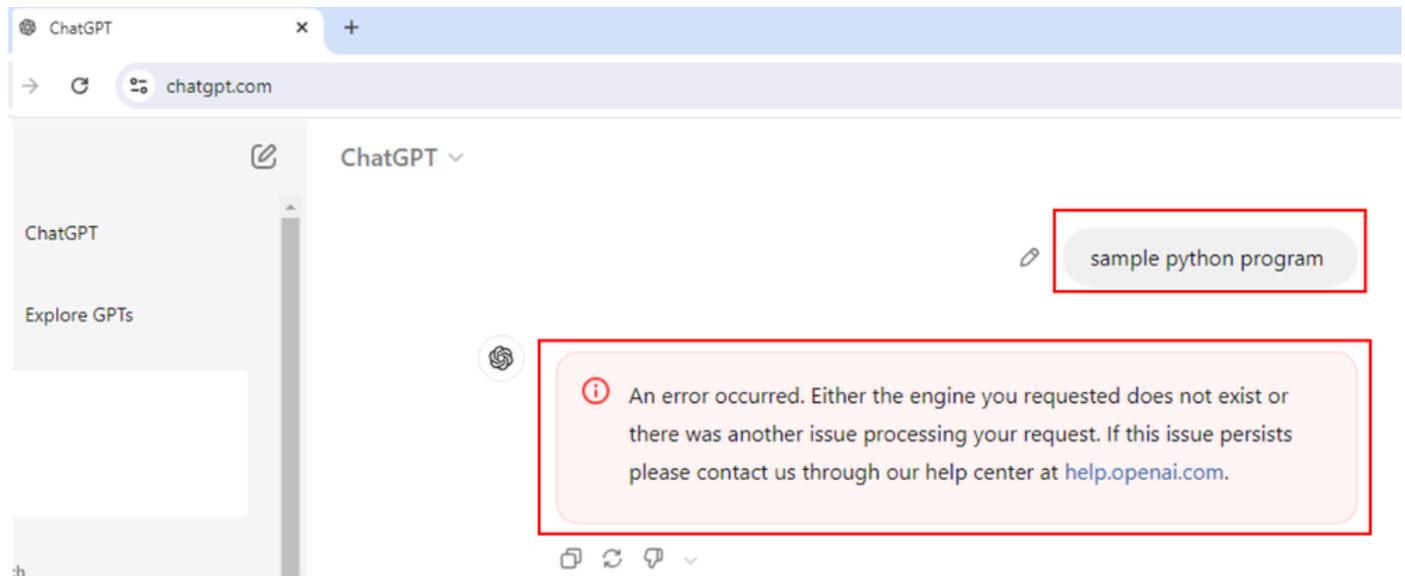


Application Settings (2)

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.



ChatGPT ▾

```
Is this program correct?  
# Python program to swap two variables
```

```
x = 5  
y = 10
```

```
# To take inputs from the user  
#x = input('Enter value of x: ')  
#y = input('Enter value of y: ')
```

```
# create a temporary variable and swap the values  
temp = x  
x = y  
y = temp
```

```
print('The value of x after swapping: {}'.format(x))  
print('The value of y after swapping: {}'.format(y))
```



 An error occurred. Either the engine you requested does not exist or there was another issue processing your request. If this issue persists please contact us through our help center at help.openai.com.

< 2/2 >    ▾

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

Overview

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Activity Search

FILTERS

Search by domain, identity, or URL

Search filters

1,965 Total

View

Response

Select All

Request

Source

Allowed [Advanced](#)

Reports

Remote Access Logs

Activity Search

Traffic logs

Security Activity

Security events and top threats

Total Requests

Activity Volume

App Discovery

Discover and analyze network applications

Top Destinations

Top domains visited by DNS

Top Categories

Top security and content categories by DNS

Third-Party Apps

Cloud Malware

View and manage detected malware events

Data Loss Prevention

Data violations detected through the Real Time and SaaS API rules

Management

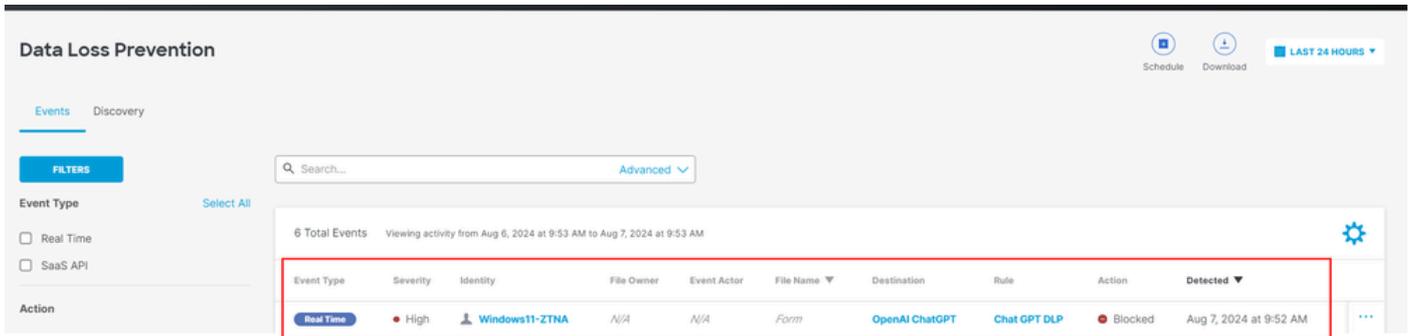
Exported Reports

Scheduled Reports

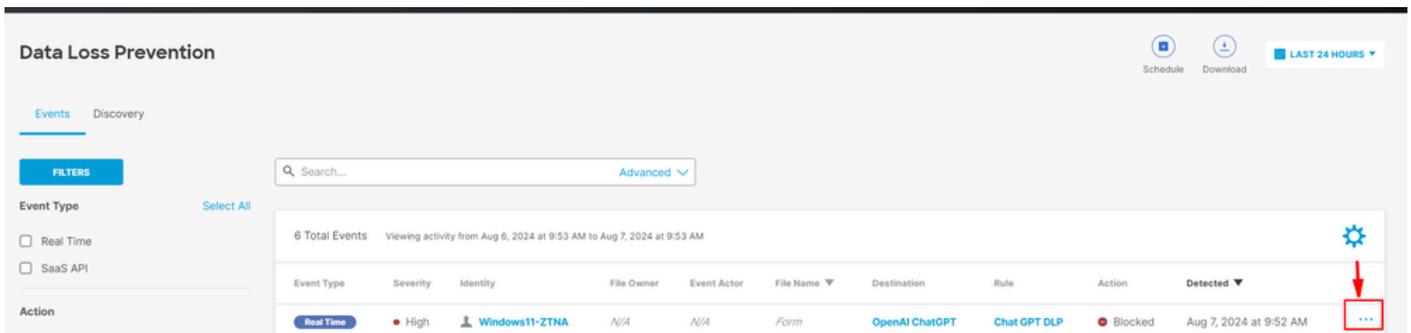
Saved Searches

Admin Audit Log

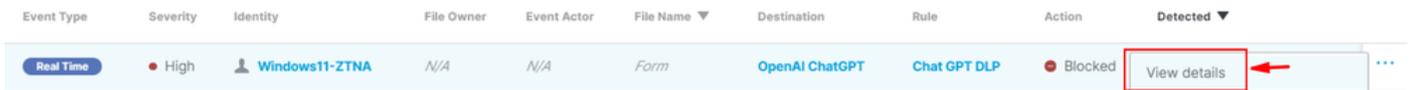
- Podemos ver o evento DLP.



- 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.

Event Details



Detected

Aug 7, 2024 at 9:52 AM

Action

 Blocked

File Name

Form

Identity

 **Windows11-ZTNA**

Application

OpenAI ChatGPT

Application Category

Generative AI

Destination URL

<http://chatgpt.com/backend-api/conversation>

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



Rule

Chat GPT DLP

Severity

● High

Direction

Inbound

Classification

Source Code

8 Matches Source Code

def calculate_year_of_century(age):, def main():...



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

Source Code

8 Matches

Source Code

def calculate_year_of_century(age):, def main():...

age, then calculates the year they will turn 100 years old:\n\n` `python\n**def calculate_year_of_century(age):**\n \"\"\"Calculate the year the user will turn 100. \"\"\"\n current_year =\n = 100 - age\n year_of_century = current_year + years_until_100\n return year_of_century\n\n**def main():**\n # Ask the user for their name and age\n name

Troubleshooting

- Verifique se a política de acesso que corresponde às solicitações da Web para Open AI ChatGPT tem acriptografia habilitada.
- Para verificar rapidamente se o SSE está criptografando 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

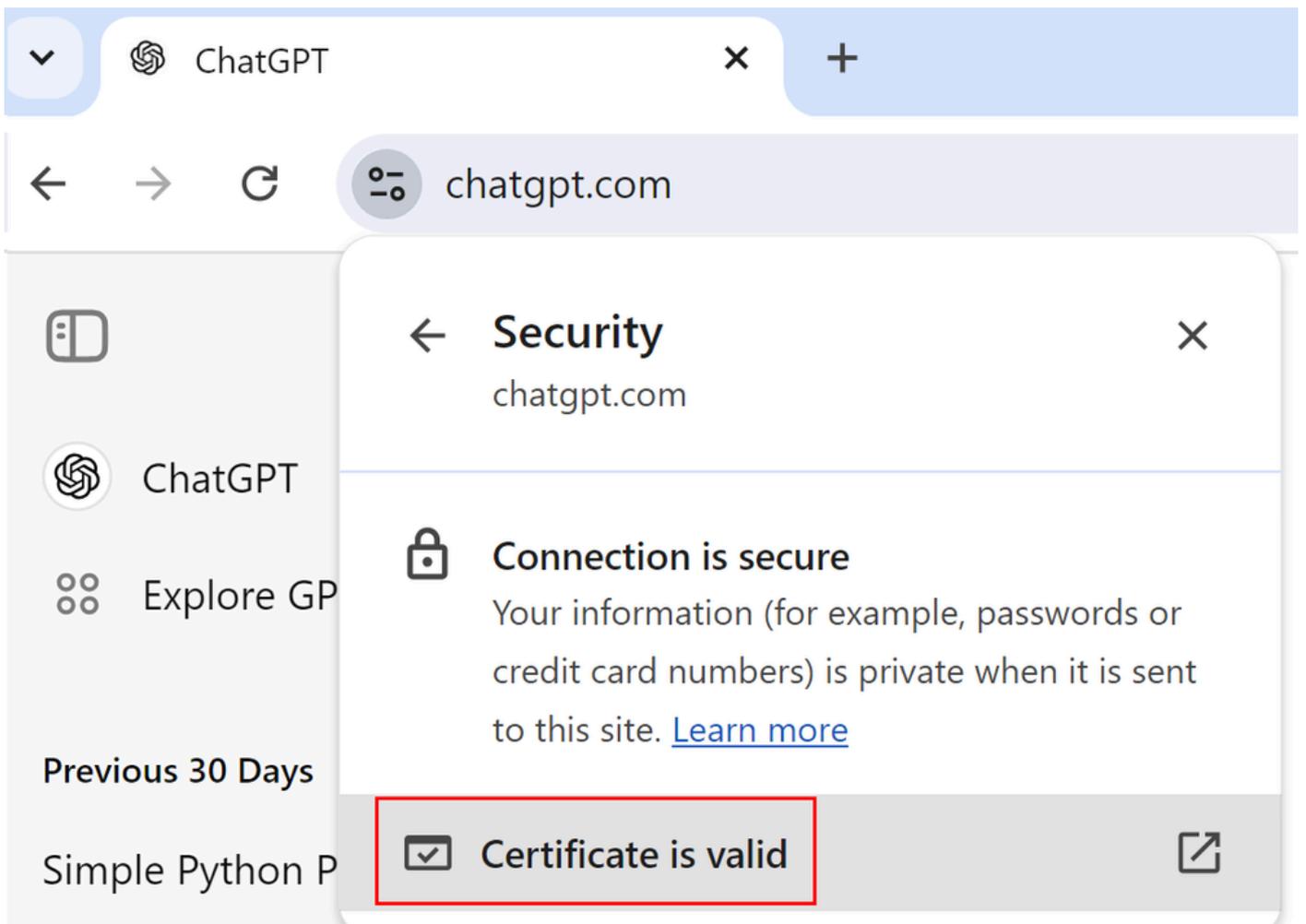
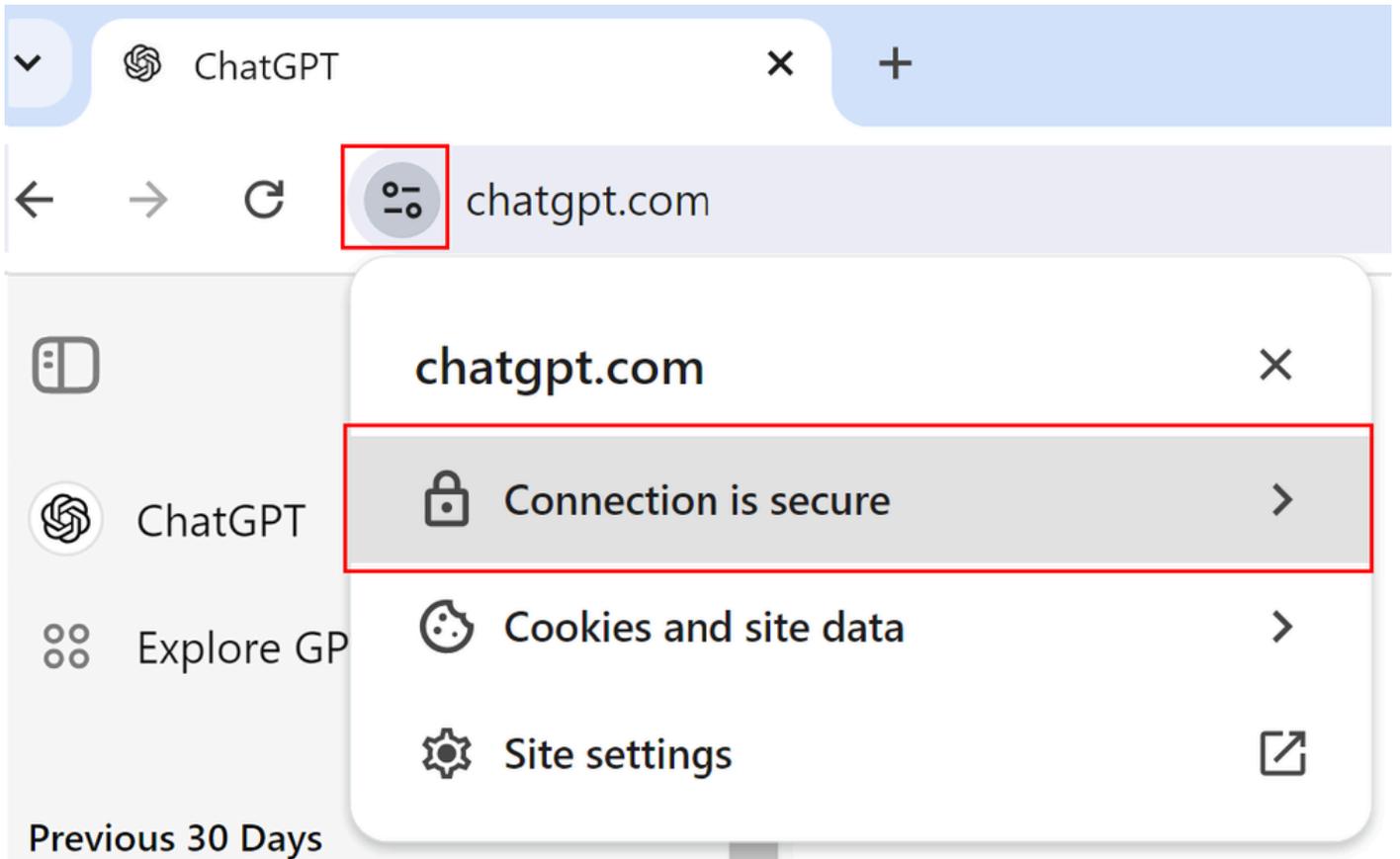
Common Name (CN)	chatgpt.com
Organization (O)	Cisco Systems, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

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



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>

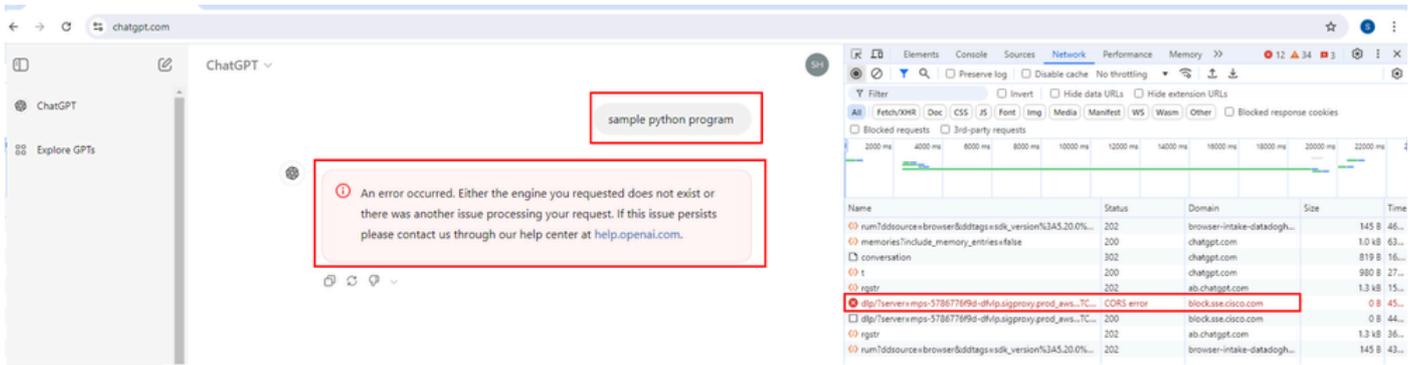
Validity Period

Issued On	Monday, August 12, 2024 at 10:52:16 PM
Expires On	Saturday, August 17, 2024 at 10:52:16 PM

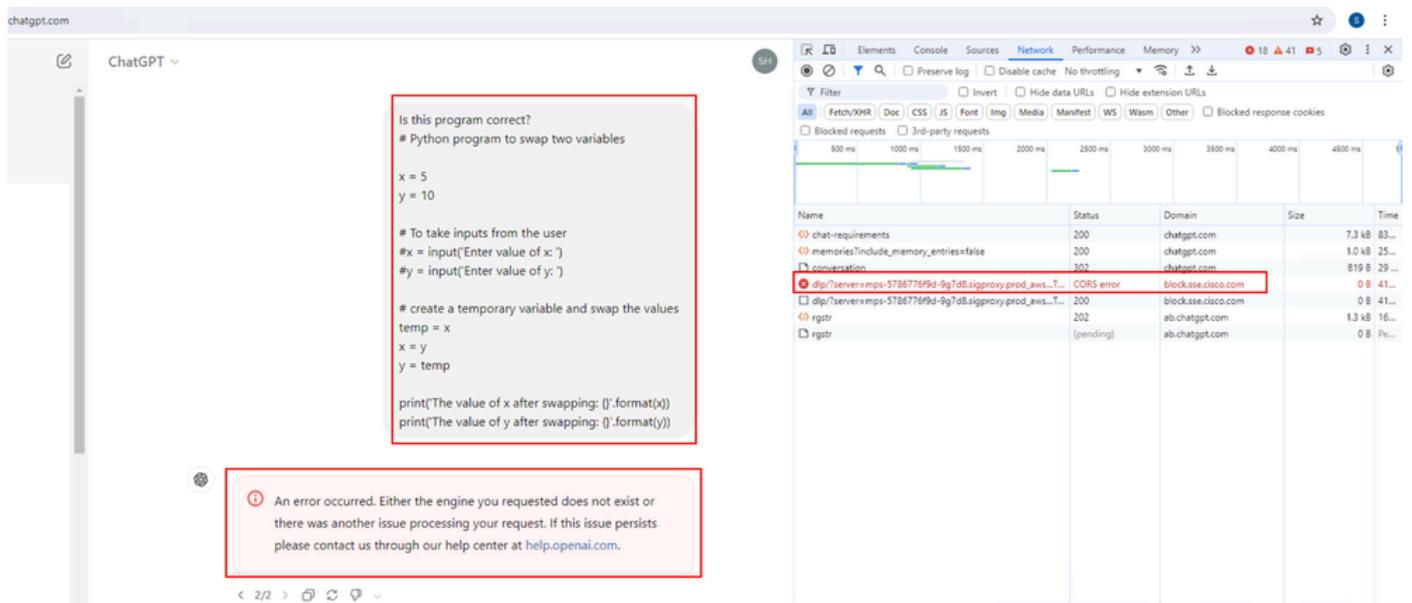
SHA-256 Fingerprints

Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c57647
Public Key	650324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e458b13bd62

- 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.