

Implémenter DLP dans l'accès sécurisé pour limiter l'utilisation de Open AI ChatGPT pour la programmation

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[1. Créer une classification de données pour utiliser l'identificateur de données de code source](#)

[2. Créez une stratégie DLP et appelez-y la classification des données « Code source ».](#)

[3. Assurez-vous que vous avez une politique d'accès à Internet en place pour le trafic vers GPT de conversation avec le décodage activé.](#)

[4. Using Open AI ChatGPT essayer de télécharger ou de télécharger n'importe quel programme.](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment mettre en oeuvre la prévention de perte de données (DLP) dans Secure Access pour limiter l'utilisation de Open AI ChatGPT pour la programmation et le codage.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sécurisé
- DLP
- Ouvrir AI ChatGPT

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Accès sécurisé
- DLP

- Ouvrir AI ChatGPT

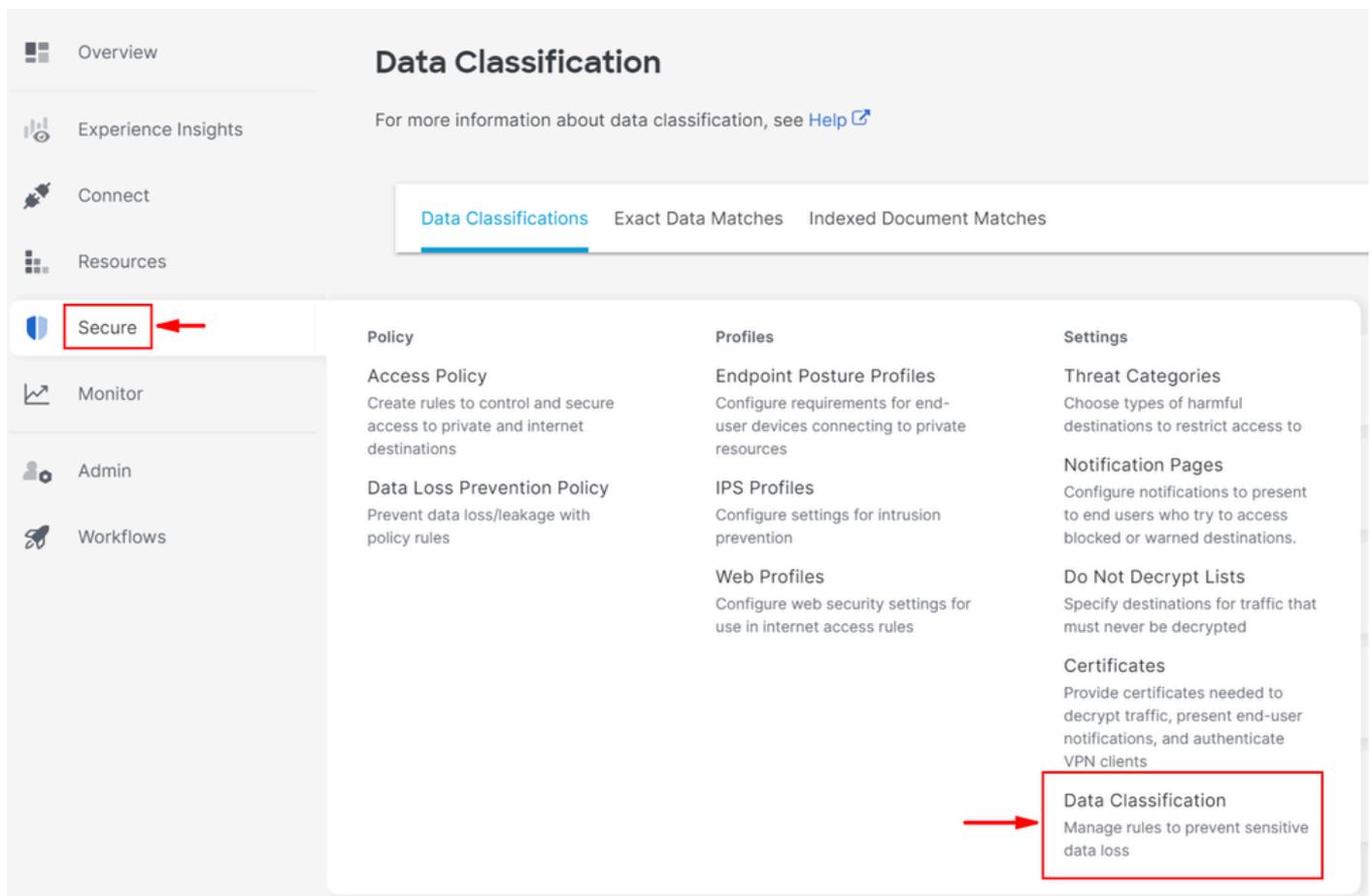
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

1. Créer une classification de données pour utiliser l'identificateur de données de code source

Accédez à [Secure Access Dashboard](#).

- Cliquez sur Secure > Data Classification > Add



- Entrez la commande Data Classification Name > **Select Built-in Data Identifiers** > Search for Source Code et sélectionnez-la

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

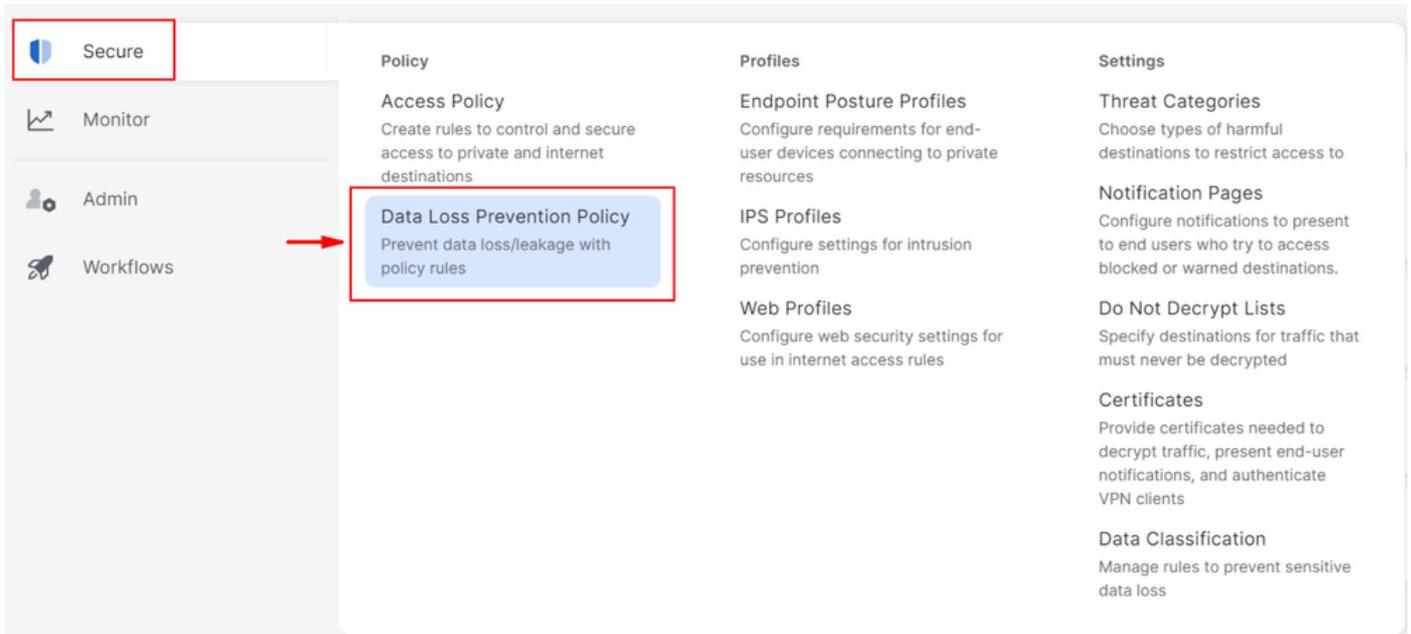
Built-in Data Identifiers

No Data Identifiers found.

Custom Identifiers

2. Créez une stratégie DLP et appelez-y la classification des données « Code source ».

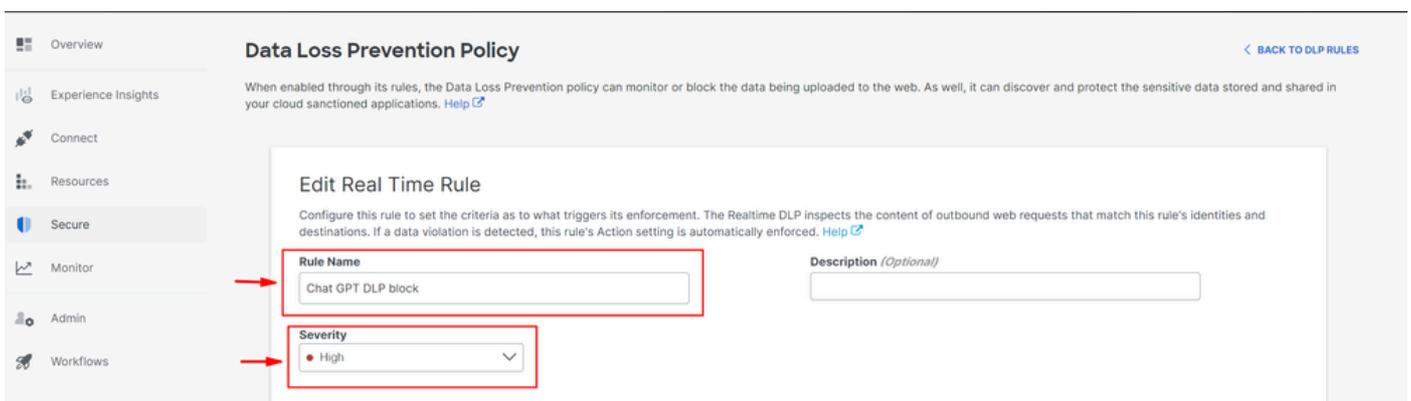
- Cliquez sur Secure > Data Loss Prevention Policy



- Cliquez sur Add Rule > Real Time Rule



- Indiquez un Rule Name > Définir approprié Severity



- Sous Data Classifications sélectionner Content et sélectionner 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

- Sous Identitiessélectionnez les identités souhaitées, le cas échéant

Identities
Select identities to add them to this rule.

Search Identities

All Identities

- AD Groups
- AD Users 4 >
- Network Tunnel Groups 6 >
- Networks 1 >
- Roaming Computers 4 >

5 Selected REMOVE ALL

- Roaming Computers 4
 - onmicrosoft.com)

- Sous Destinations, sélectionnez Select Destination Lists and Applications for Inclusion
- Sélectionnez Application Categories> Sélectionner Generative AI> Sélectionner OpenAI API (Vetted) et OpenAI ChatGPT (Vetted) dans 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



- Sous Actions sélectionner Block

- Sous User Notifications, vous pouvez configurer des notifications par e-mail aux utilisateurs finaux, lorsque la règle est déclenchée (facultatif)

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



- Cliquez sur Save

DELETE

CANCEL

SAVE



3. Assurez-vous que vous avez une politique d'accès à Internet en place pour le trafic vers GPT de conversation avec le décodage activé.

Exemple :

Chat GPT



Internet

General

Action



Allow

Last modified



Rule order

1

Logging

Enabled

Hits

216

Sources

Any

Destinations

2 destinations

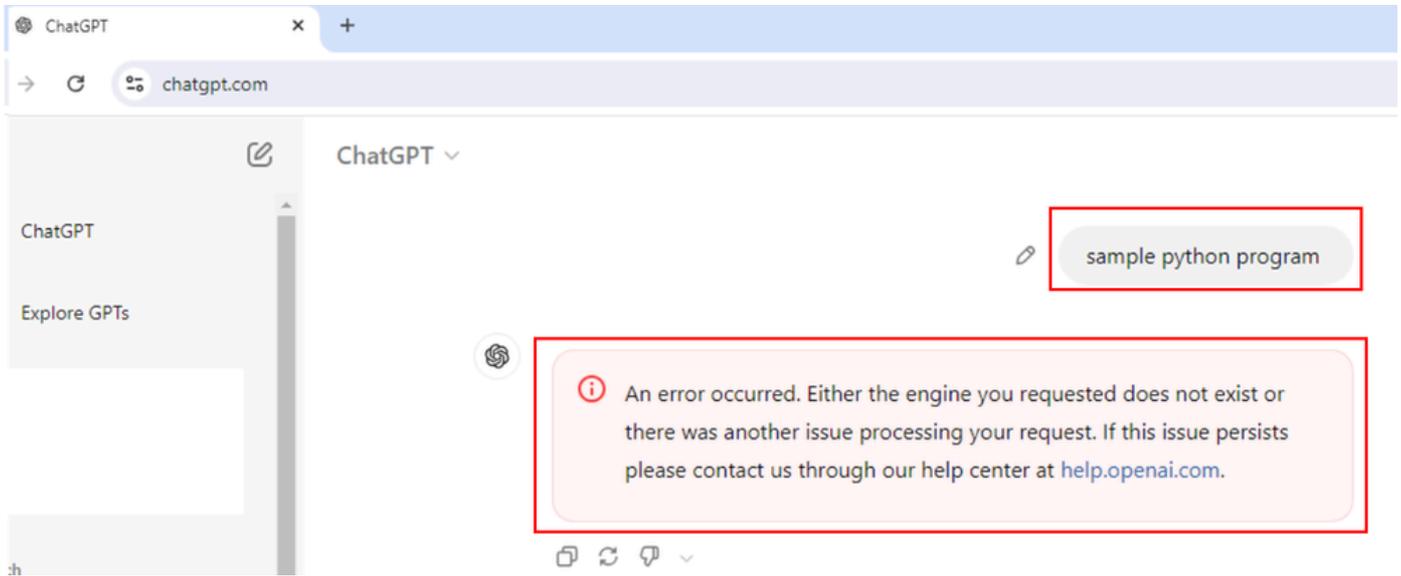


Application Settings (2)

OpenAI API

OpenAI ChatGPT

- Demandez un exemple de programme python et cette requête sera bloquée.



- Demandez si le programme est correct ou non et cette demande est bloquée.



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 >    ▾

Vérifier

Nous pouvons voir quand l'utilisateur essaie de demander à ChatGPT un exemple de programme python, la requête est bloquée. Nous pouvons confirmer qu'un événement DLP a été déclenché dans les journaux Secure Access Data Loss Prevention.

- Accéder à 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

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

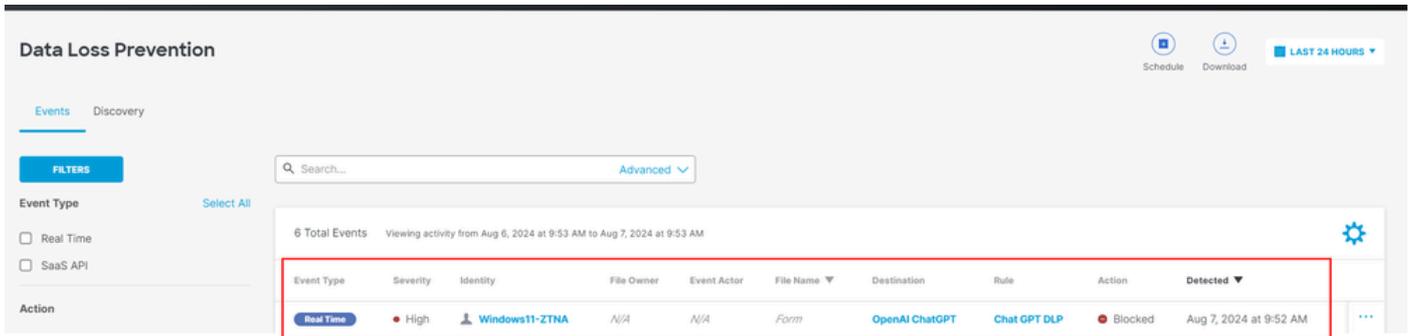
Exported Reports

Scheduled Reports

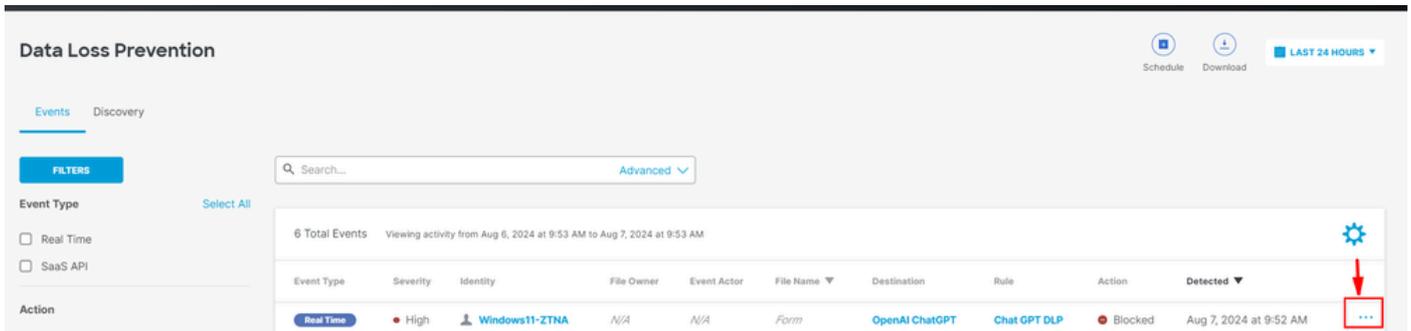
Saved Searches

Admin Audit Log

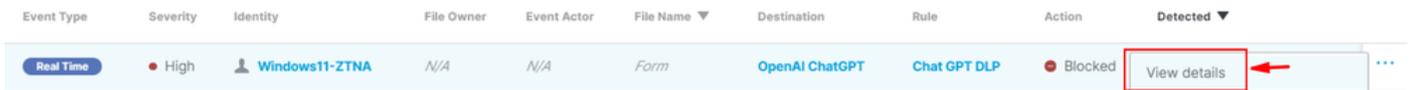
- Nous pouvons voir l'événement DLP.



- Cliquez sur les trois points à la fin du journal des événements pour vérifier plus de détails sur l'événement.



- Cliquez sur View details.



- Nous voyons maintenant l'intégralité des détails de l'événement.

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>

- Développez la classification pour voir quel contenu correspond au classifieur.



Rule

Chat GPT DLP

Severity

● High

Direction

Inbound

Classification

Source Code

8 Matches Source Code

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



- Nous voyons tous les détails du contenu qui correspondait au classifieur / Classification de la politique 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

Dépannage

- Assurez-vous que le déchiffrement est activé pour la stratégie d'accès qui correspond aux requêtes Web pour Open AI ChatGPT.
- Pour vérifier rapidement si SSE décrypte le trafic pour Open AI ChatGPT, vérifiez le certificat du site Web qui affiche le nom commun inclut les mots clés « Cisco Secure Access ».

Certificate Viewer: chatgpt.com



General

Details

Issued To

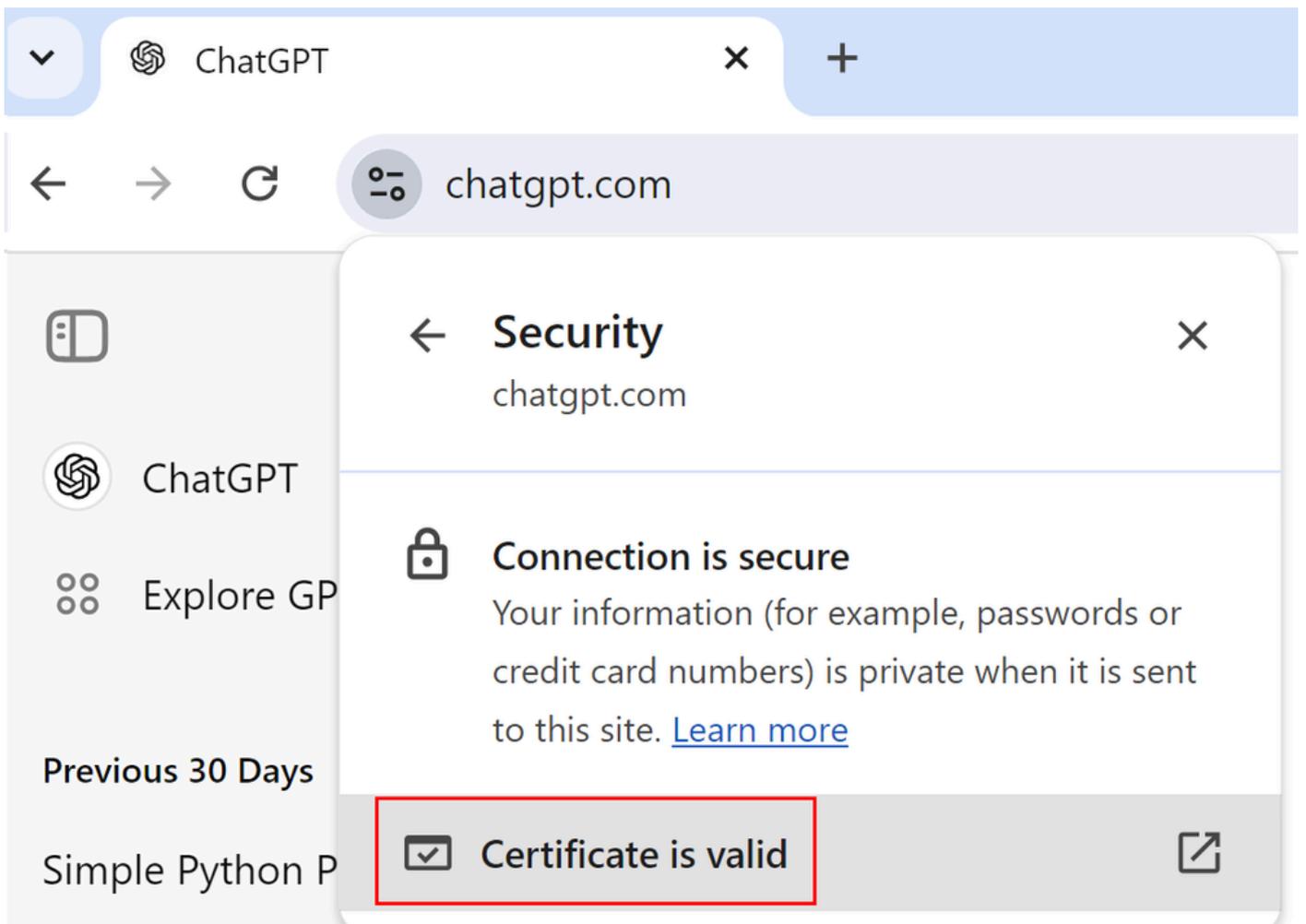
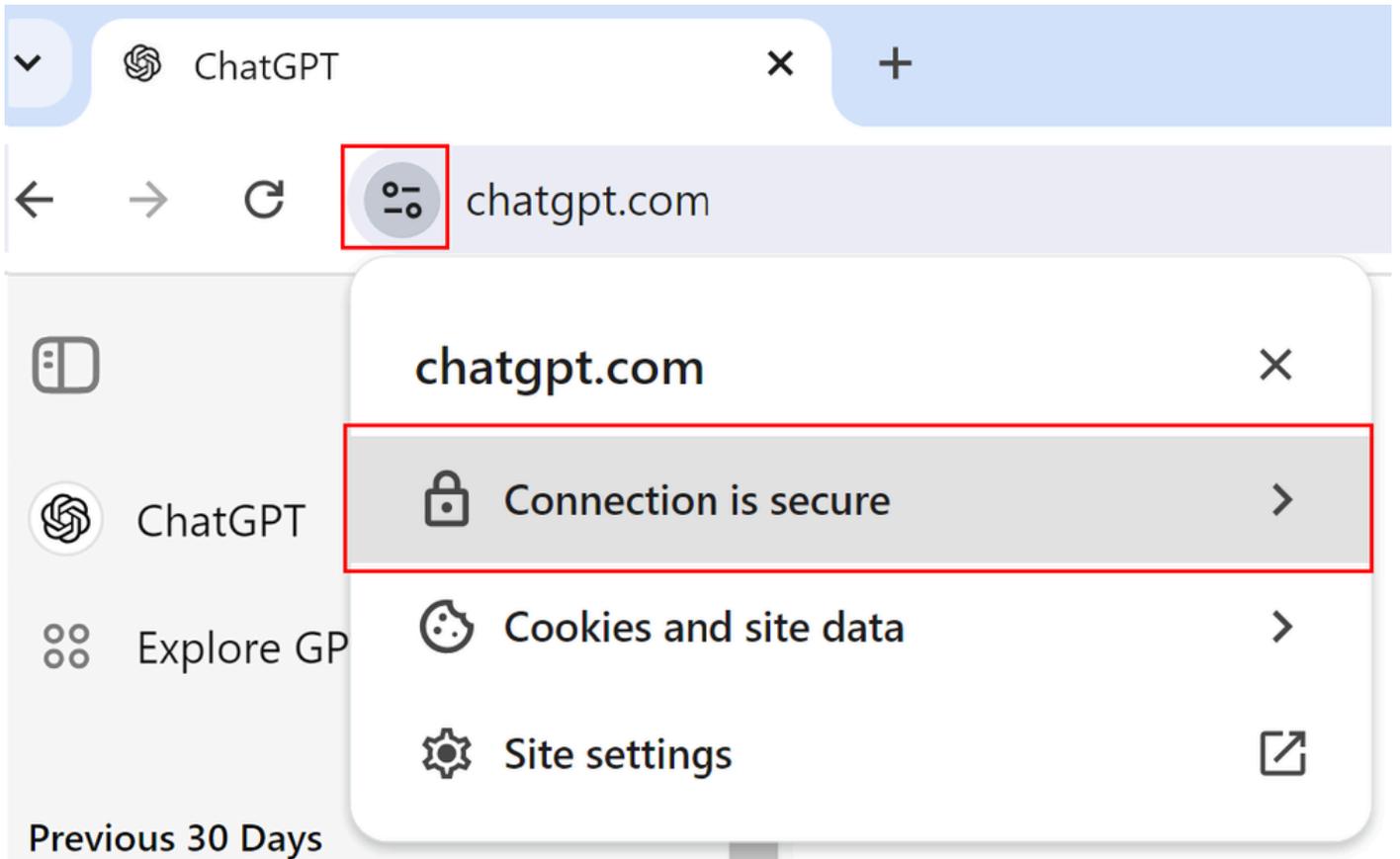
Common Name (CN)	chatgpt.com
Organization (O)	Cisco Systems, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

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>

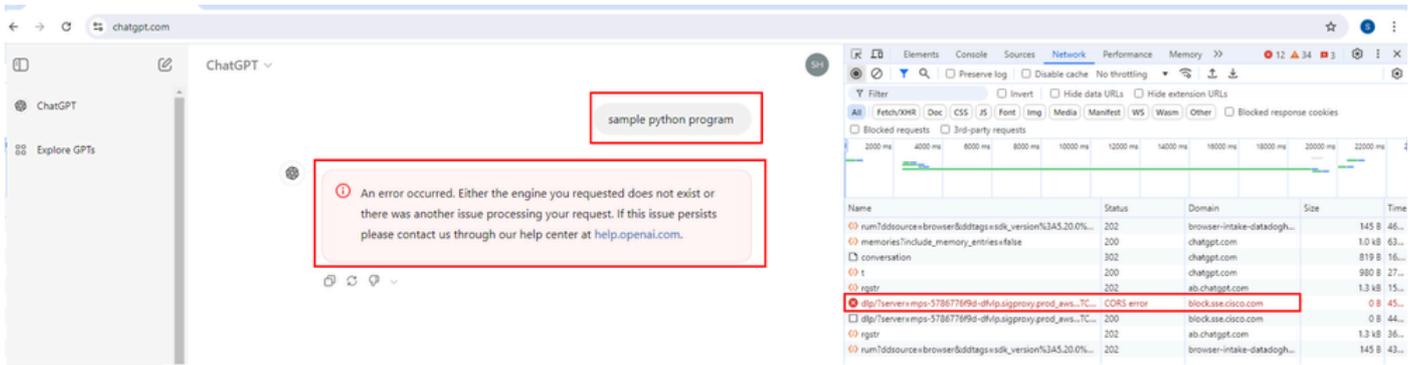
Validity Period

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

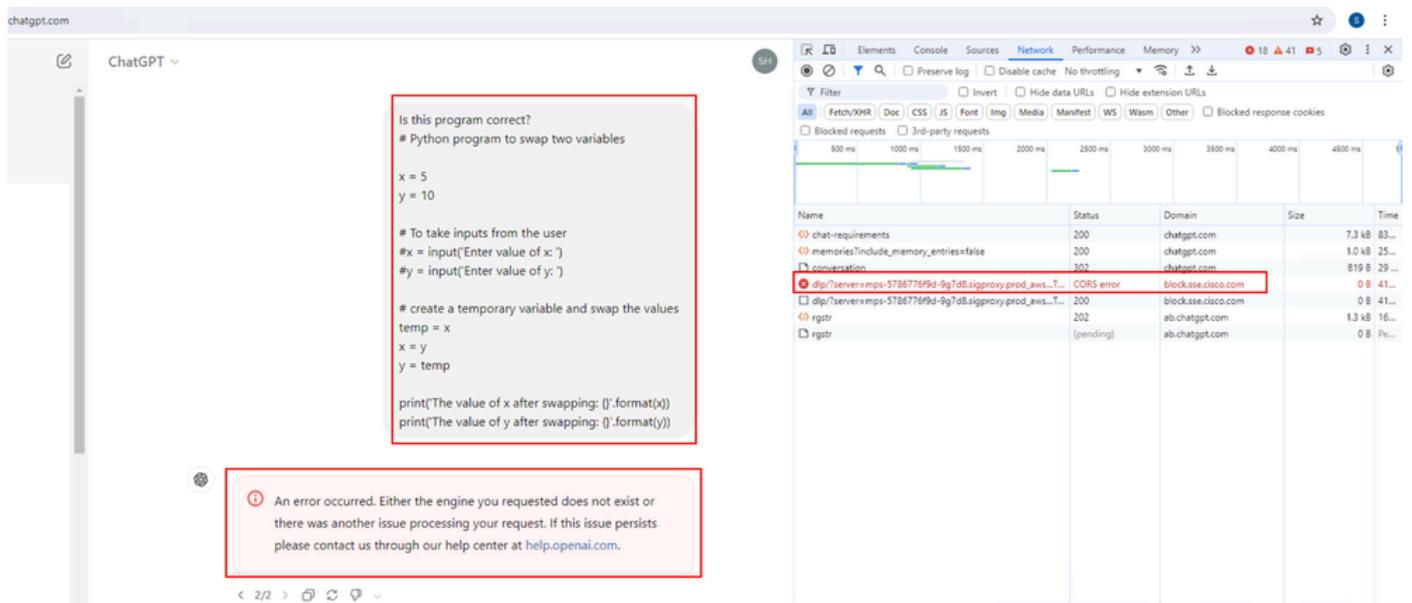
SHA-256 Fingerprints

Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c57647
Public Key	650324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e458b13bd62

- Ouvrez ChatGPT > Ouvrez les outils de développement > Sélectionnez Réseau > Ensuite essayez de demander à ChatGPT un exemple de programme python
- Notez que la requête entraîne un blocage. Sous le domaine, vous voyez « block.sse.cisco.com



- Demandez à ChatGPT si le code du programme est correct.
- Notez que la requête aboutit à un blocage et que sous « domain », vous voyez « block.sse.cisco.com ».



Informations connexes

- [Guide de l'utilisateur Cisco Secure Access](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.