

보안 액세스에서 DLP를 구현하여 프로그래밍 시 개방형 AI 채팅GPT 사용 제한

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[1. 소스 코드 데이터 식별자를 사용할 데이터 분류 만들기](#)

[2. DLP 정책을 생성하고 데이터 분류 "소스 코드"를 호출합니다.](#)

[3. 암호 해독이 활성화된 채팅 GPT로 향하는 트래픽에 대한 인터넷 액세스 정책이 있는지 확인합니다.](#)

[4. Open AI ChatGPT를 사용하여 프로그램을 다운로드하거나 업로드합니다.](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 프로그래밍 및 코딩을 위해 Open AI ChatGPT 사용을 제한하기 위해 Secure Access에서 DLP(Data Loss Prevention)를 구현하는 방법을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 보안 액세스
- DLP
- AI ChatGPT 열기

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 보안 액세스
- DLP
- AI ChatGPT 열기

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

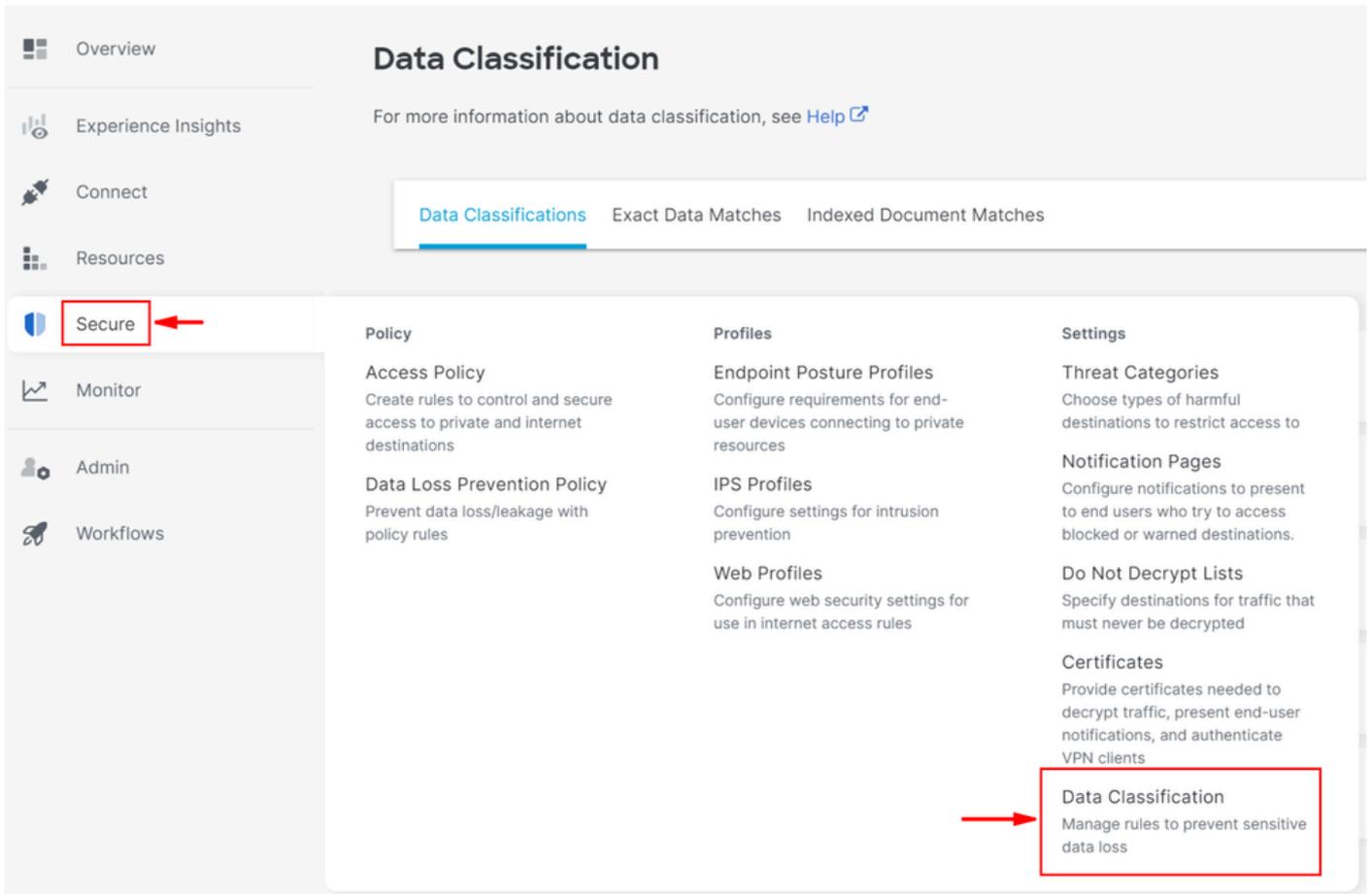
이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

1. 소스 코드 데이터 식별자를 사용할 데이터 분류 만들기

Secure [Access Dashboard\(보안 액세스 대시보드\)](#)로 이동합니다.

- Secure > Data Classification 를 클릭합니다. Add Data Classification Name



- > **선택** Built-in Data Identifiers > 검색 대상을 Source Code 입력하고 선택합니다

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

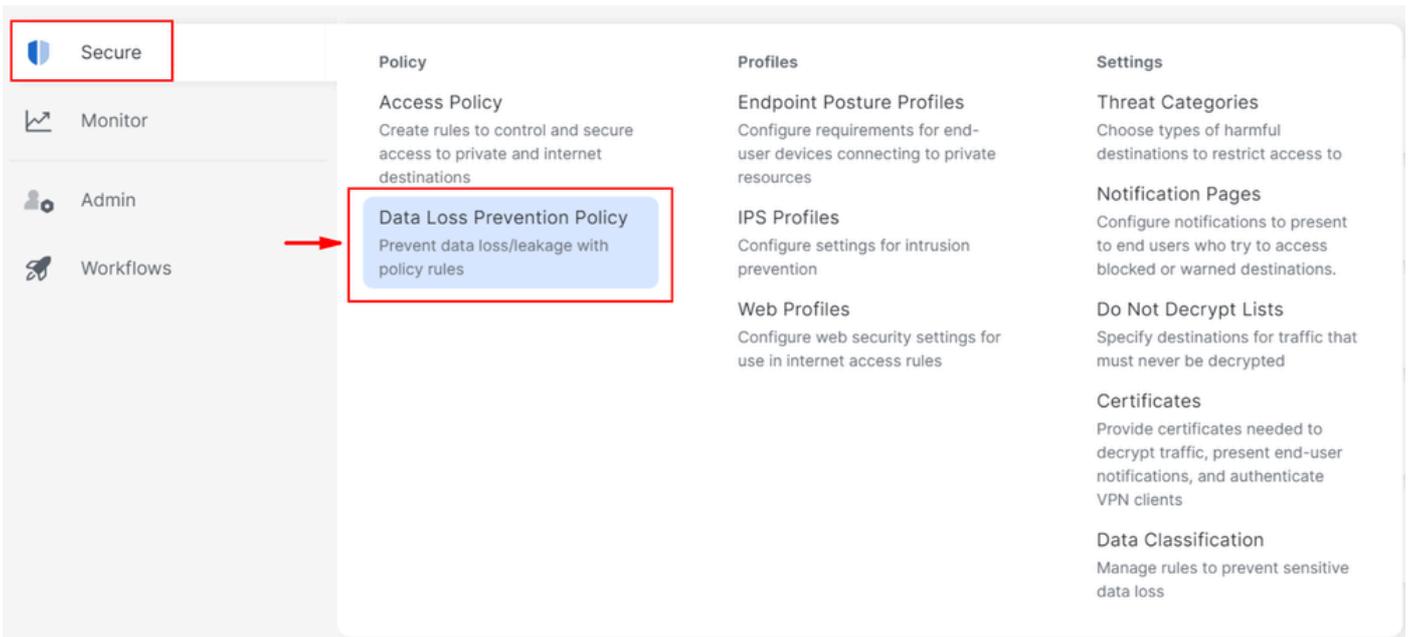
No Data Identifiers found.

Custom Identifiers

2. DLP 정책을 생성하고 데이터 분류 "소스 코드"를 호출합니다.

- Secure > 를 클릭합니다. Data Loss Prevention Policy

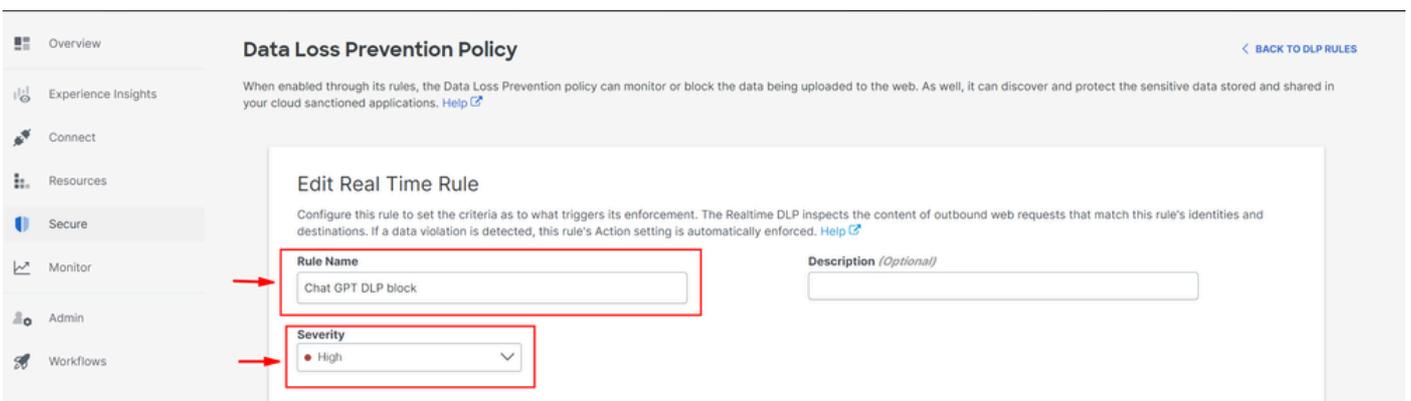
Add Rule



- > 를 클릭합니다. Real Time Rule



- > 적절한 Rule Name 설정 제공 Severity



- 선택 Data Classifications 아래에서 Content 다음을 선택합니다 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

- 에서 Identities 필요에 따라 원하는 ID를 선택합니다

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)

- 대상 아래에서 Select Destination Lists and Applications for Inclusion
- 선택 Application Categories > 선택 Generative AI OpenAI API (Vetted) > 선택 및 OpenAI ChatGPT (Vetted) 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



- 아래에서 Action선택 Block
- 에서User Notifications, 규칙이 트리거될 때 최종 사용자에게 이메일 알림을 설정할 수 있습니다(선택 사항)

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

- 클릭 Save

DELETE

CANCEL

SAVE

3. 암호 해독이 활성화된 채팅 GPT로 향하는 트래픽에 대한 인터넷 액세스 정책이 있는지 확인합니다.

예:

Chat GPT



Internet

General

Action

 Allow

Last modified



Rule order

1

Logging

Enabled

Hits

216

Sources

Any

Destinations

2 destinations

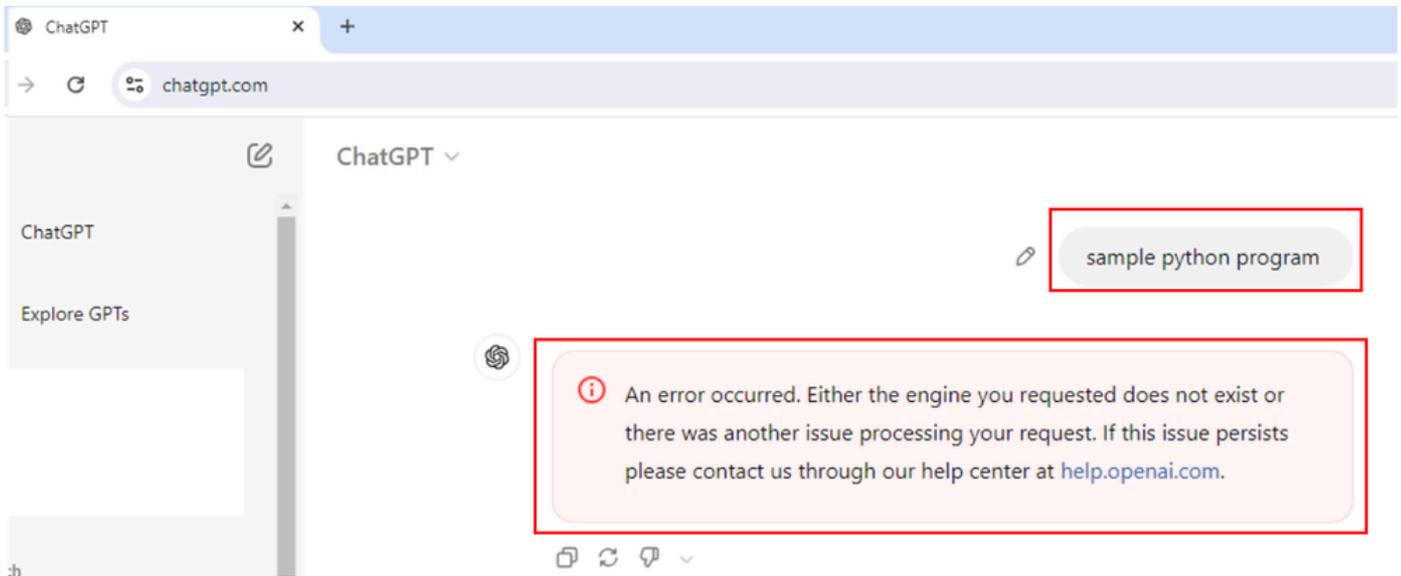


Application Settings (2)

OpenAI API

OpenAI ChatGPT

- 샘플 python 프로그램을 요청하면 이 요청이 차단됩니다.



- 프로그램이 정확한지 물어보고 이 요청을 차단합니다.



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 >    ▾

다음을 확인합니다.

사용자가 ChatGPT에 샘플 python 프로그램을 요청하려고 하면 요청이 차단되는 것을 확인할 수 있습니다.
DLP 이벤트가 Secure Access Data Loss Prevention 로그에서 트리거되었음을 확인할 수 있습니다.

- 이동 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

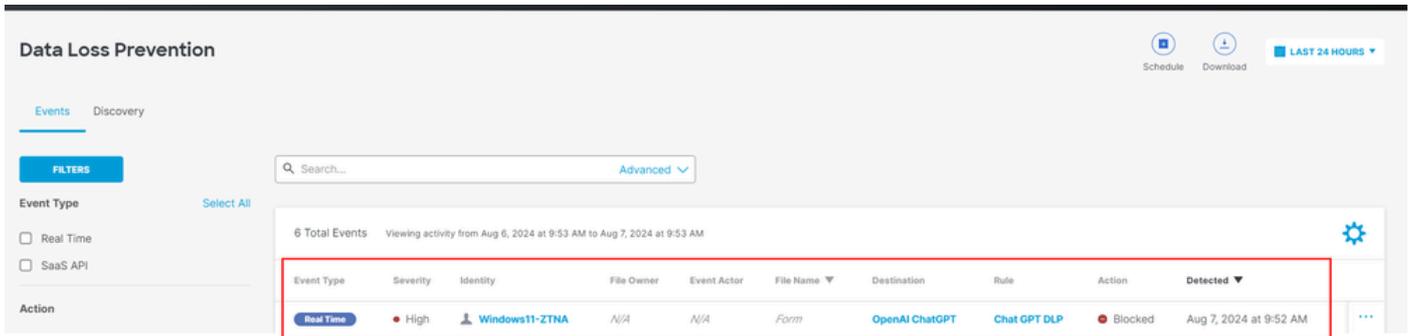
Exported Reports

Scheduled Reports

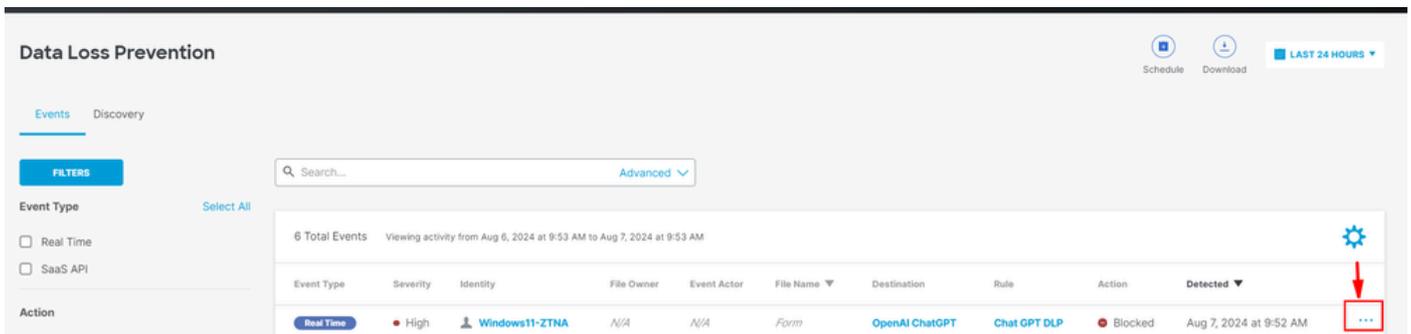
Saved Searches

Admin Audit Log

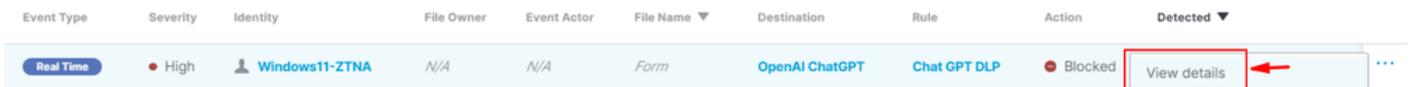
- DLP 이벤트를 볼 수 있습니다.



- 이벤트 로그의 끝에 있는 세 개의 점을 클릭하여 이벤트에 대한 자세한 내용을 확인합니다.



- 클릭 View details.



- 이제 전체 Event Details(이벤트 세부 정보)가 표시됩니다.

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>

- 분류자를 확장하여 어떤 콘텐츠가 분류자와 일치하는지 확인합니다.



Rule

Chat GPT DLP

Severity

- High

Direction

Inbound

Classification

Source Code

8 Matches Source Code

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



- DLP 정책의 분류자/분류와 일치하는 모든 콘텐츠 세부사항이 표시됩니다.

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`
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

문제 해결

- Open AI ChatGPT에 대한 웹 요청과 일치하는 액세스 정책에 암호 해독이 활성화되어 있는지 확인합니다.
- SSE가 Open AI ChatGPT에 대한 트래픽을 해독하고 있는지 신속하게 확인하려면 "Cisco Secure Access" 키워드가 포함된 공용 이름이 표시된 웹 사이트의 인증서를 확인하십시오.

Certificate Viewer: chatgpt.com



General

Details

Issued To

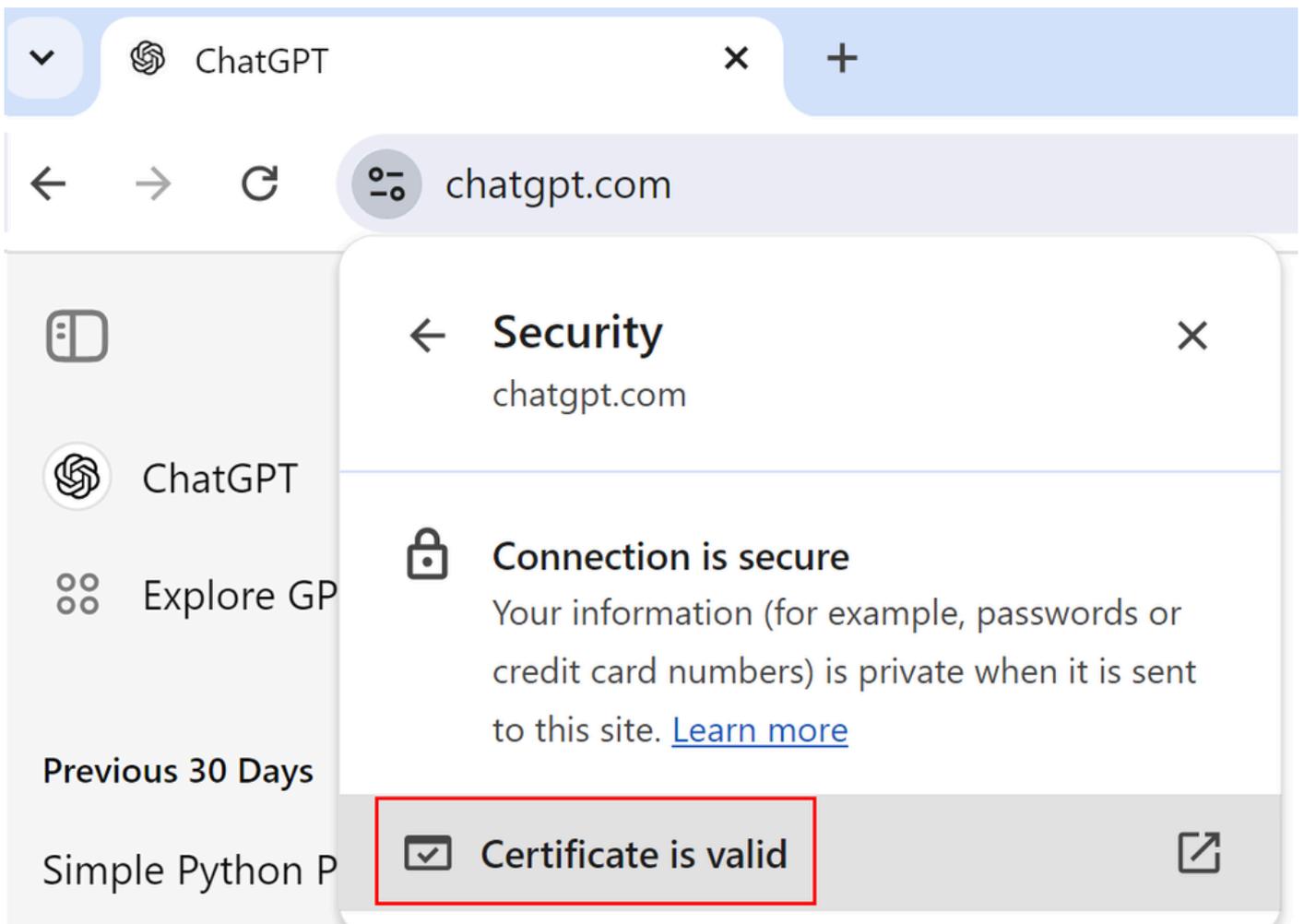
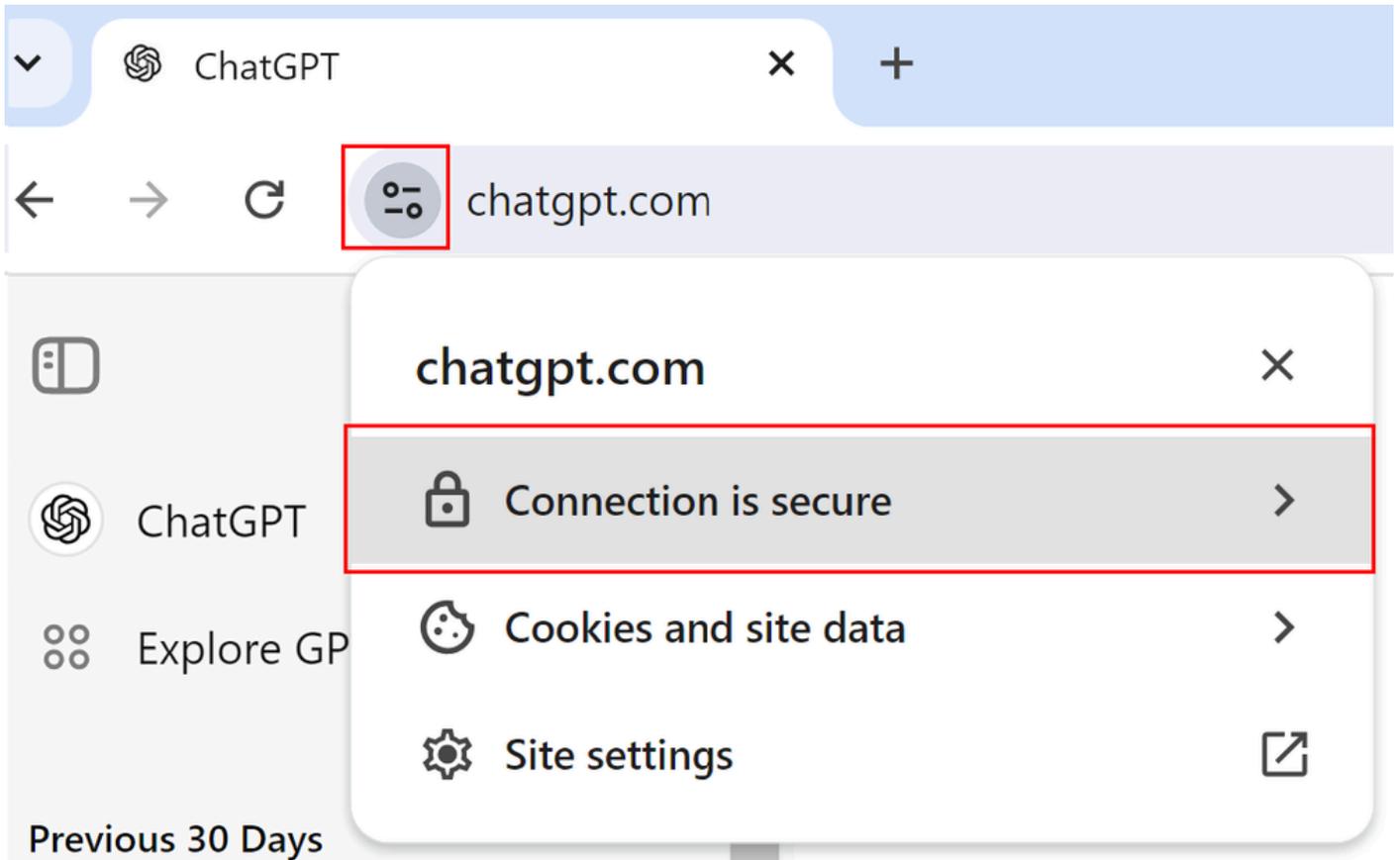
Common Name (CN)	chatgpt.com
Organization (O)	Cisco Systems, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

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>

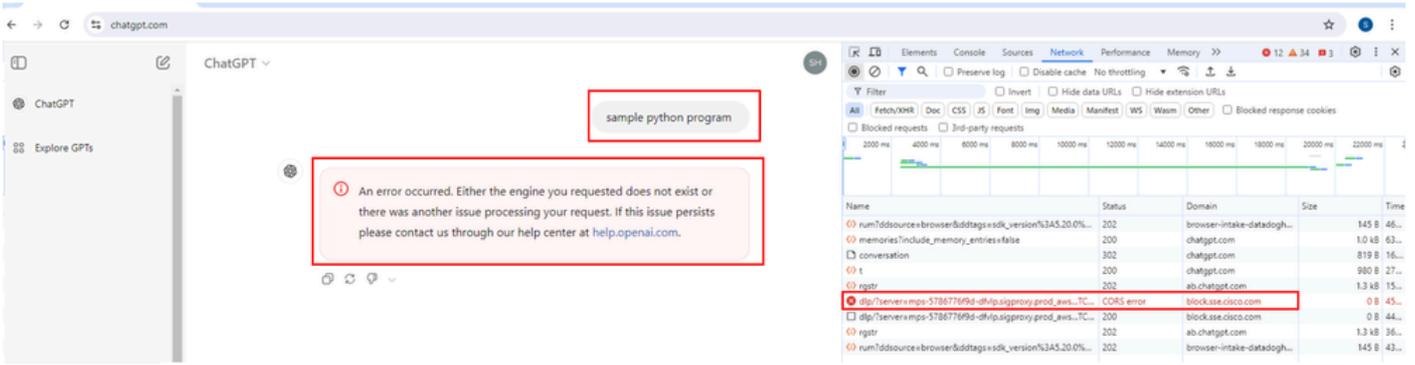
Validity Period

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

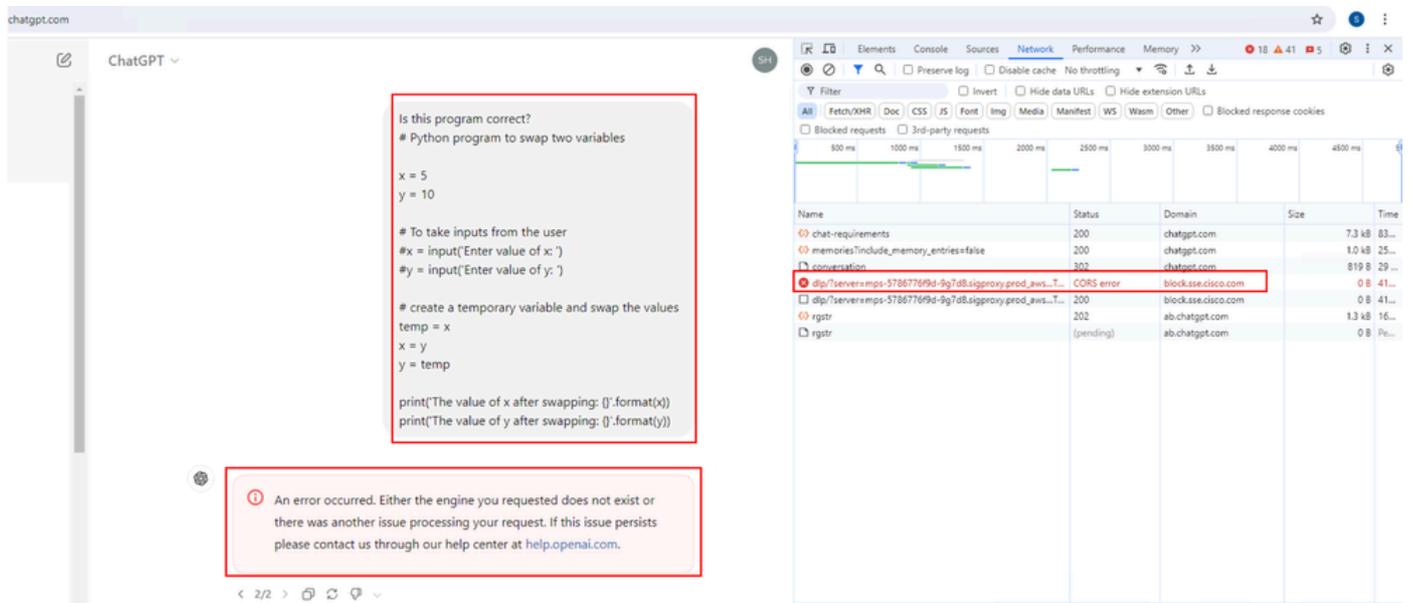
SHA-256 Fingerprints

Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c57647
Public Key	650324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e458b13bd62

- ChatGPT > Open developer tools > Select Network > Next try to ask ChatGPT for a sample python program
- 요청이 차단되는지 확인합니다. 도메인 아래에 "block.sse.cisco.com"이 표시됩니다.



- 프로그램 코드가 정확한지 ChatGPT에 문의하십시오.
- 요청이 블록으로 나타나는지 확인하고 "domain" 아래에 "block.sse.cisco.com"이 표시됩니다.



관련 정보

- [Cisco Secure Access 사용 설명서](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.