Implement DLP in Secure Access to Restrict Open AI ChatGPT Usage for Programming

Contents

Introduction

This document describes how to implement Data Loss Prevention (DLP) in Secure Access to restrict Open AI ChatGPT usage for programming and coding.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Access
- DLP
- Open AI ChatGPT

Components Used

The information in this document is based on these software and hardware versions:

- Secure Access
- DLP
- Open AI ChatGPT

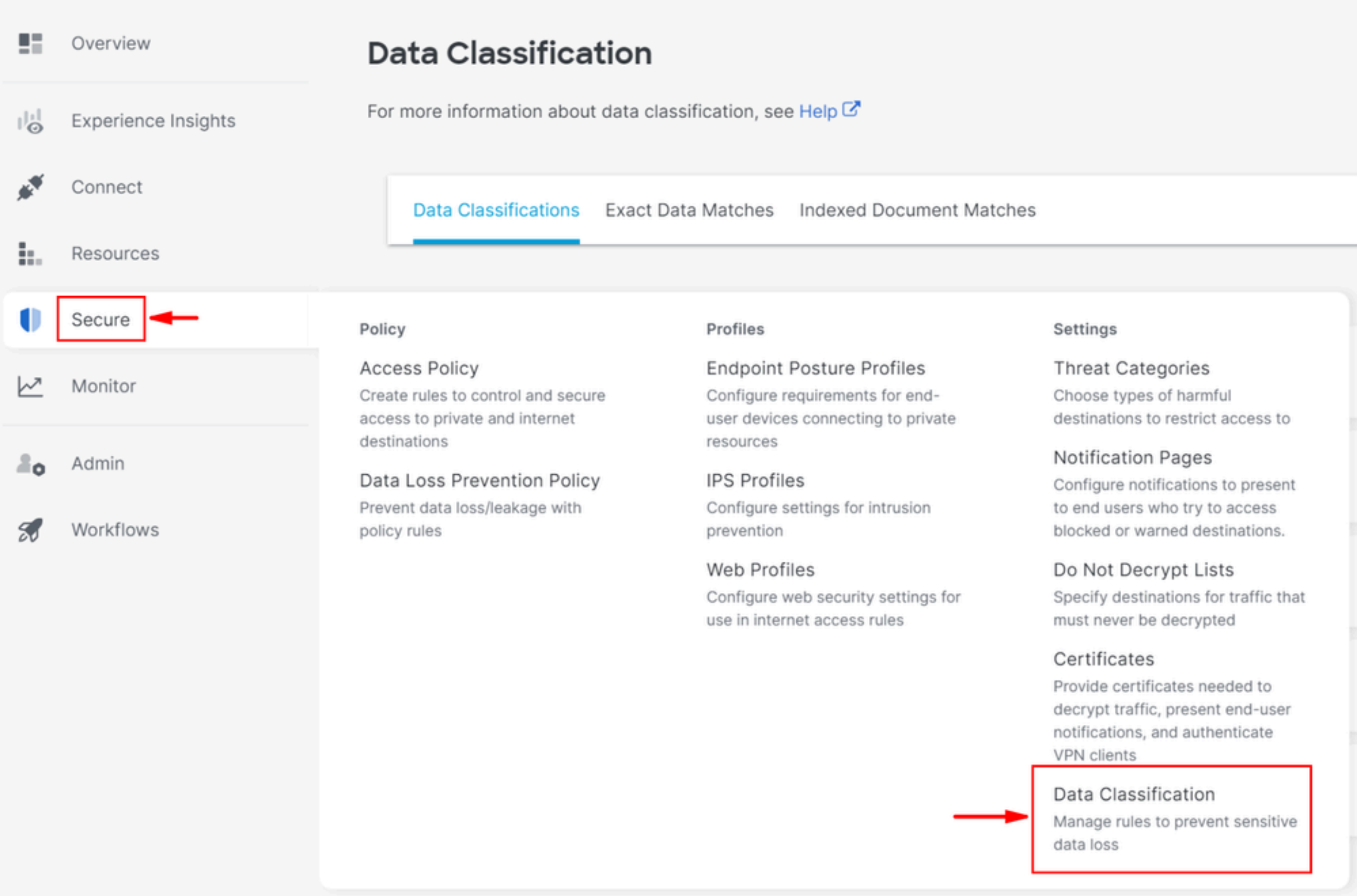
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

1.Create a data classification to use Source Code Data Identifier

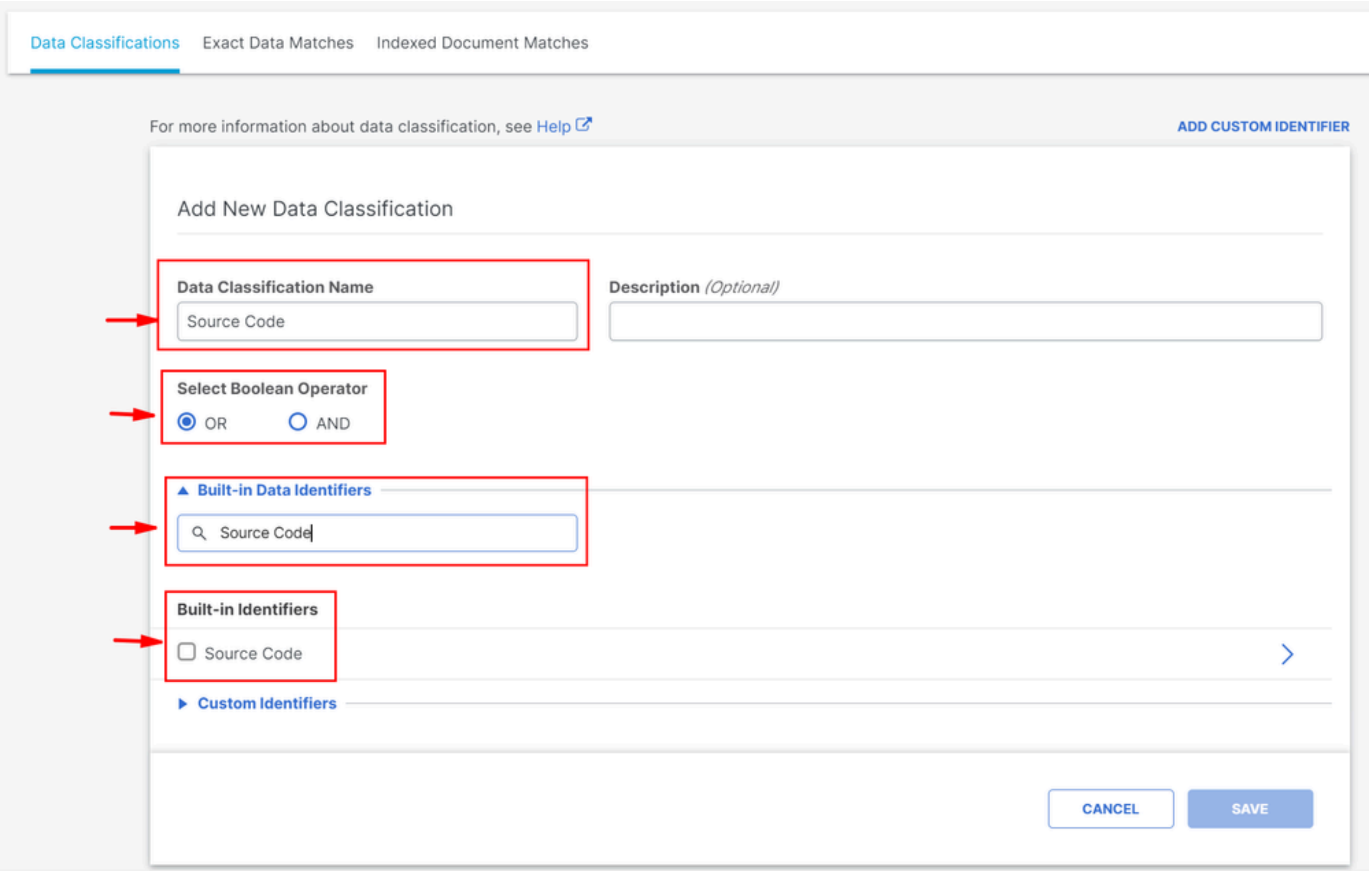
Navigate to Secure Access Dashboard.

- Click on Secure > Data Classification > Add



Overview
Experience Insights
Connect
Resources
Secure
Monitor
Admin
Workflows
Data Classification
For more information about data classification, see Help
Data Classifications
Exact Data Matches
Indexed Document Matches
Policy
Access Policy
Create rules to control and secure access to private and internet destinations
Data Loss Prevention Policy
Prevent data loss/leakage with policy rules
Profiles
Endpoint Posture Profiles
Configure requirements for end-user devices connecting to private resources
IPS Profiles
Configure settings for intrusion prevention
Web Profiles
Configure web security settings for use in internet access rules
Settings
Threat Categories
Choose types of harmful destinations to restrict access to
Notification Pages
Configure notifications to present to end users who try to access blocked or warned destinations.
Do Not Decrypt Lists
Specify destinations for traffic that must never be decrypted
Certificates
Provide certificates needed to decrypt traffic, present end-user notifications, and authenticate VPN clients
Data Classification
Manage rules to prevent sensitive data loss

- Enter the Data Classification Name > **Select** Built-in Data Identifiers > Search for Source Code and select it



For more information about data classification, see Help

Add New Data Classification

Data Classification Name: Source Code

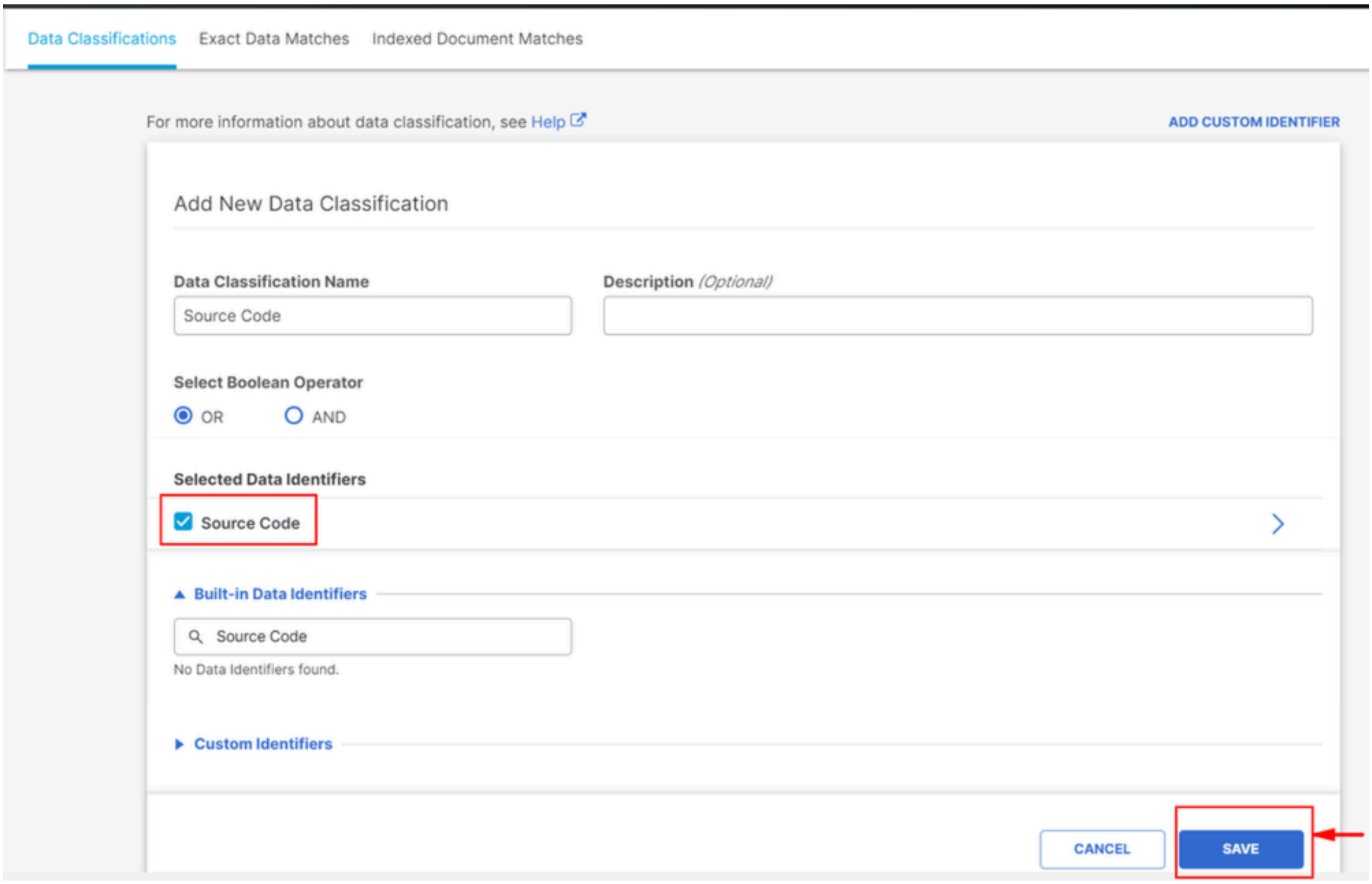
Description *(Optional)*:

Select Boolean Operator: ● OR ○ AND

▲ Built-in Data Identifiers: Source Code

Built-in Identifiers

☐ Source Code



For more information about data classification, see Help

Add New Data Classification

Data Classification Name: Source Code

Description *(Optional)*:

Select Boolean Operator: ● OR ○ AND

Selected Data Identifiers

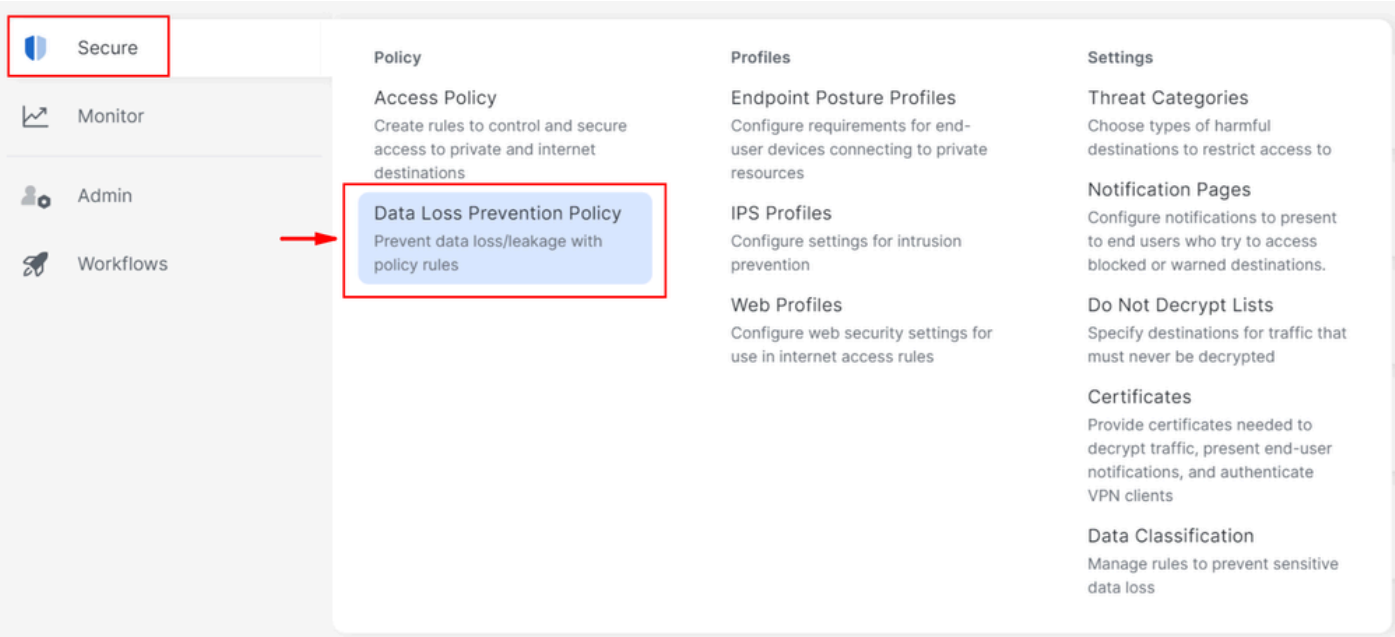
☑ Source Code

▲ Built-in Data Identifiers: Source Code

No Data Identifiers found.

2.Create a DLP Policy and call the Data Classification "Source Code" in it.

- Click on Secure > Data Loss Prevention Policy



Policy

Access Policy
Create rules to control and secure access to private and internet destinations

Data Loss Prevention Policy
Prevent data loss/leakage with policy rules

Profiles

Endpoint Posture Profiles
Configure requirements for end-user devices connecting to private resources

IPS Profiles
Configure settings for intrusion prevention

Web Profiles
Configure web security settings for use in internet access rules

Settings

Threat Categories
Choose types of harmful destinations to restrict access to

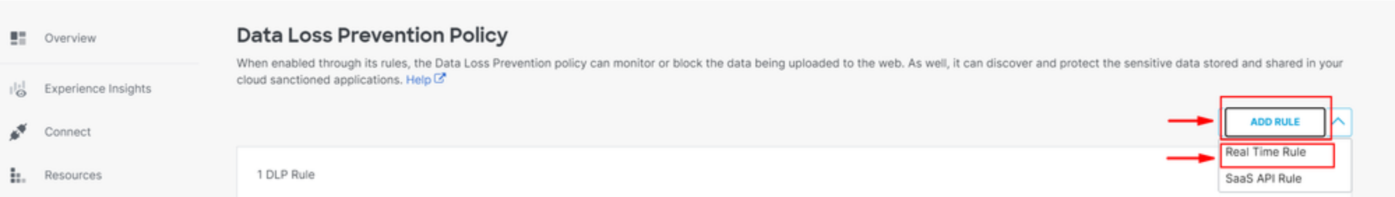
Notification Pages
Configure notifications to present to end users who try to access blocked or warned destinations.

Do Not Decrypt Lists
Specify destinations for traffic that must never be decrypted

Certificates
Provide certificates needed to decrypt traffic, present end-user notifications, and authenticate VPN clients

Data Classification
Manage rules to prevent sensitive data loss

- Click on Add Rule > Real Time Rule

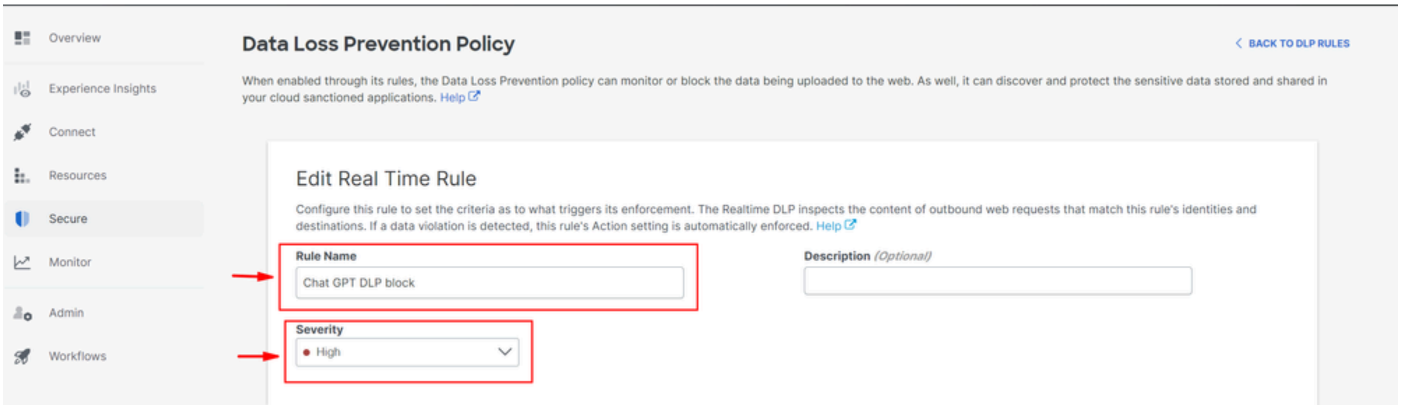


Data Loss Prevention Policy

When enabled through its rules, the Data Loss Prevention policy can monitor or block the data being uploaded to the web. As well, it can discover and protect the sensitive data stored and shared in your cloud sanctioned applications. Help

1 DLP Rule

- Provide a Rule Name > Set appropriate Severity



Data Loss Prevention Policy

When enabled through its rules, the Data Loss Prevention policy can monitor or block the data being uploaded to the web. As well, it can discover and protect the sensitive data stored and shared in your cloud sanctioned applications. Help

Edit Real Time Rule

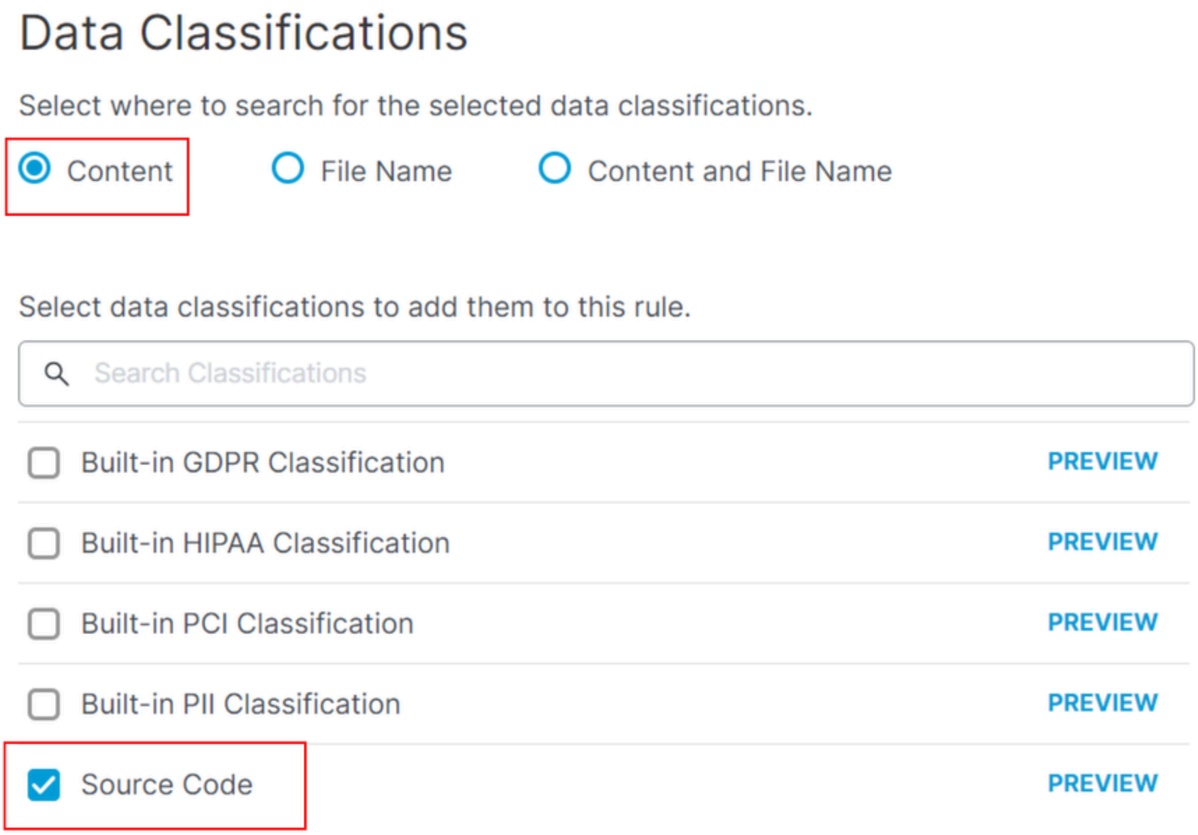
Configure this rule to set the criteria as to what triggers its enforcement. The Realtime DLP inspects the content of outbound web requests that match this rule's identities and destinations. If a data violation is detected, this rule's Action setting is automatically enforced. Help

Rule Name: Chat GPT DLP block

Description *(Optional)*:

Severity: ● High

- Under Data Classifications select Content and select 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.

□ Built-in GDPR Classification PREVIEW

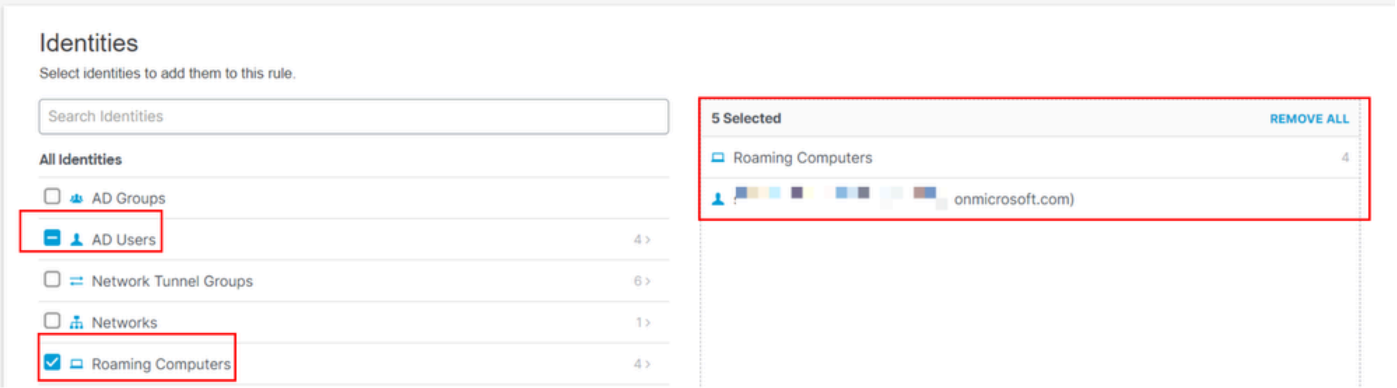
□ Built-in HIPAA Classification PREVIEW

□ Built-in PCI Classification PREVIEW

□ Built-in PII Classification PREVIEW

☑ Source Code PREVIEW

- Under Identitiesselect desired identities as required



Identities

Select identities to add them to this rule.

All Identities

□ AD Groups

■ AD Users 4 >

□ Network Tunnel Groups 6 >

□ Networks 1 >

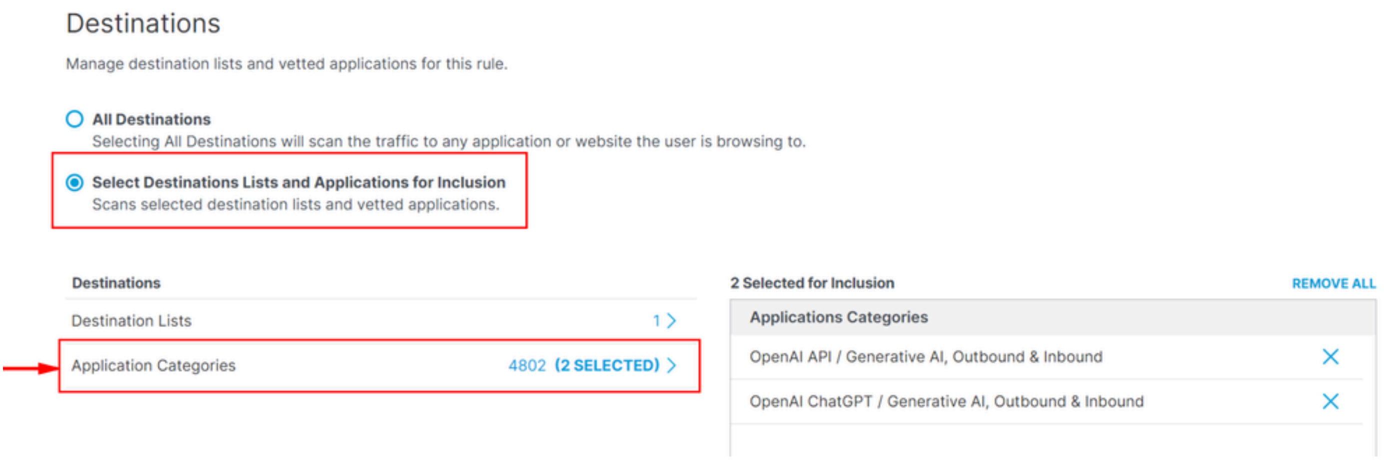
☑ Roaming Computers 4 >

5 Selected REMOVE ALL

Roaming Computers 4

[redacted]onmicrosoft.com)

- Under Destinations select Select Destination Lists and Applications for Inclusion
- Select Application Categories> Select Generative AI > Select OpenAI API (Vetted) and OpenAI ChatGPT (Vetted) in 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.

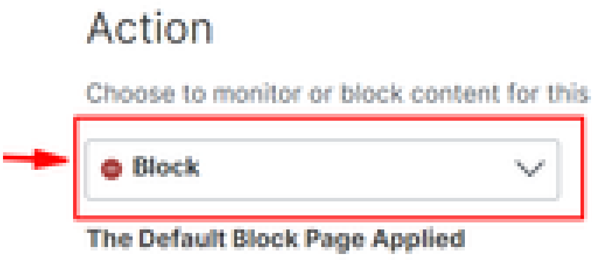
● **Select Destinations Lists and Applications for Inclusion**
Scans selected destination lists and vetted applications.

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	×

- Under Action select Block
- Under User Notifications, you can setup email notifications to end users, when the rule is triggered (optional)

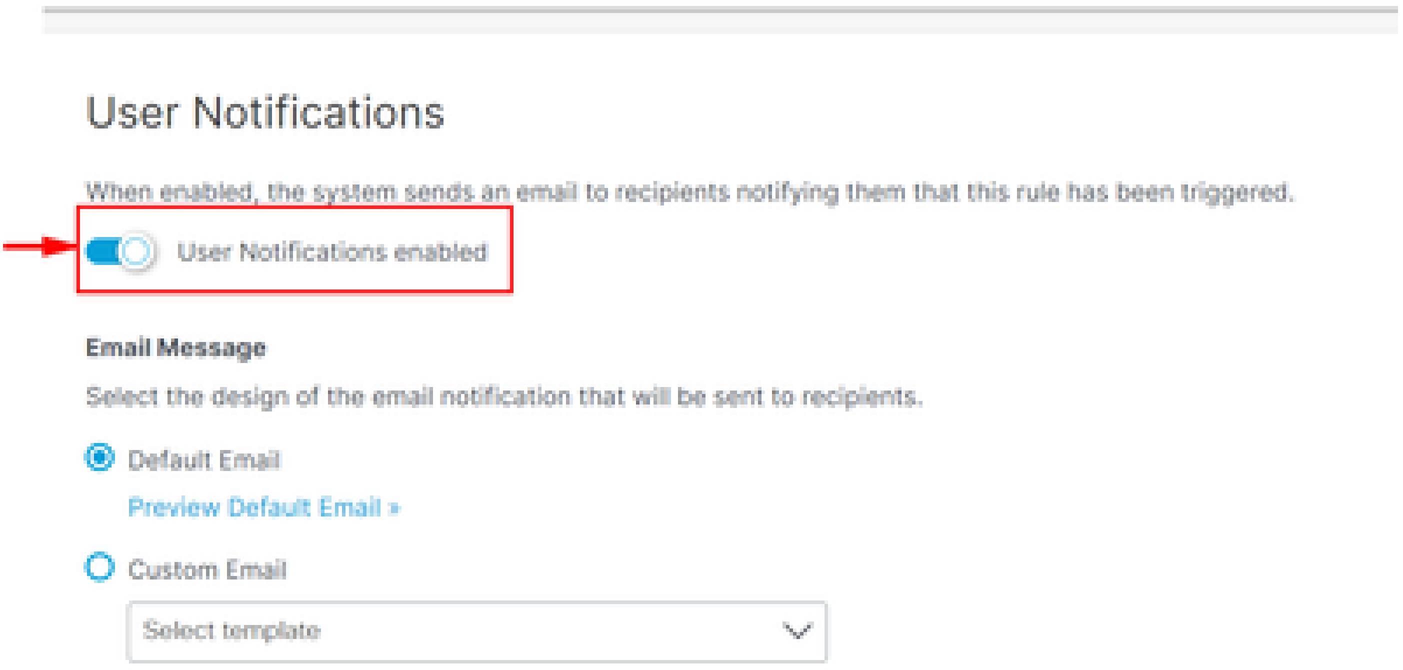


Action

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

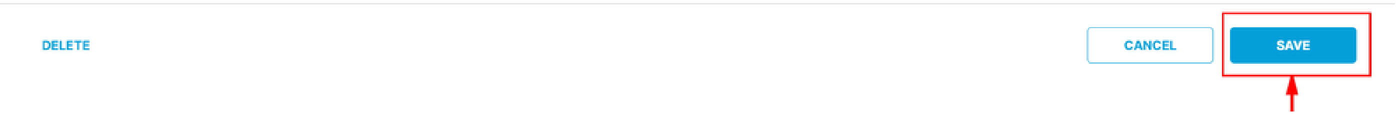
Email Message

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

● Default Email
Preview Default Email »

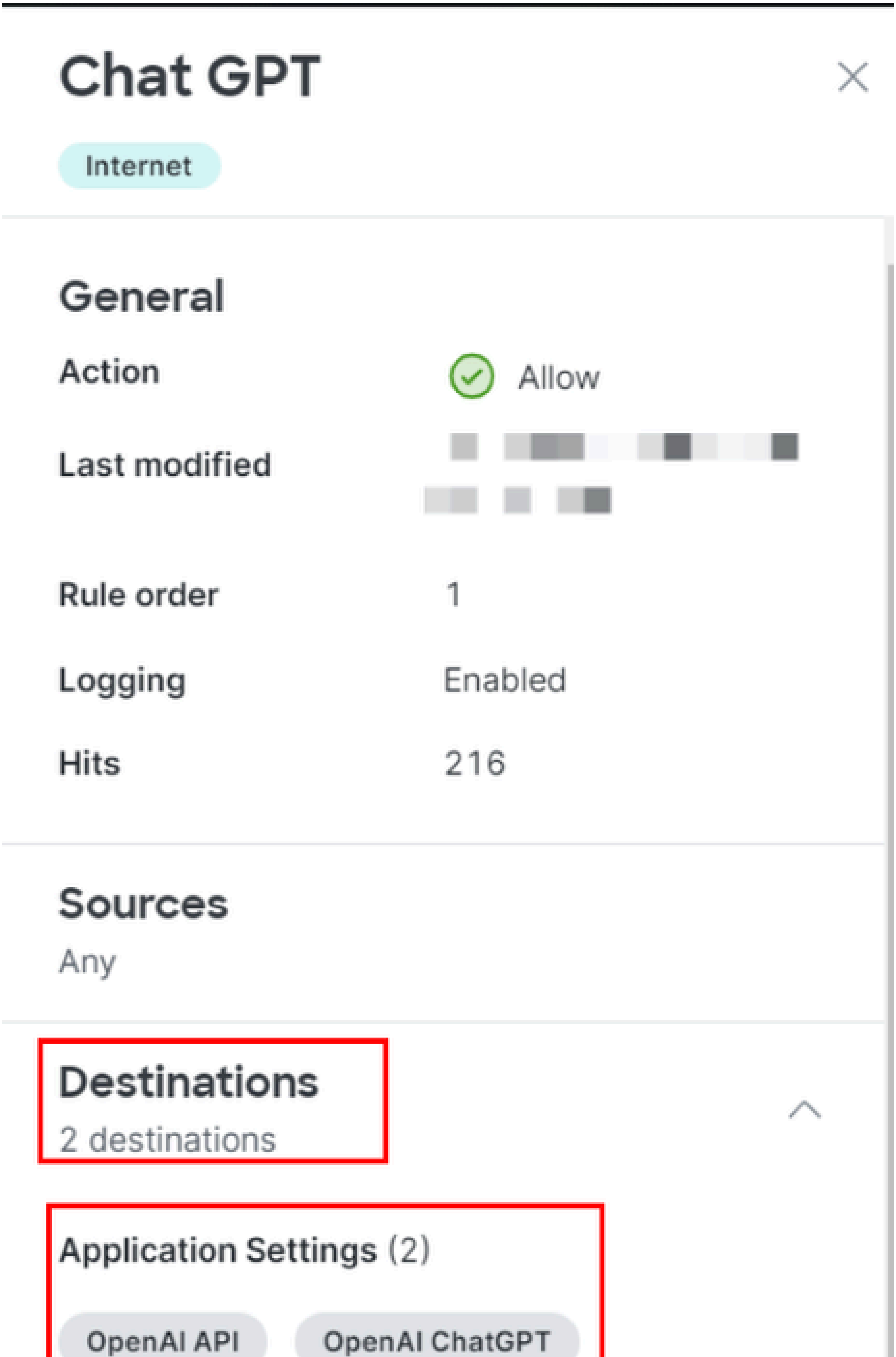
○ Custom Email
Select template

- Click on Save



3.Ensure you have an Internet Access Policy in place for traffic towards Chat GPT with Decryption enabled.

Example:



Chat GPT

Internet

General

Action ✓ Allow

Last modified [redacted]

Rule order 1

Logging Enabled

Hits 216

Sources

Any

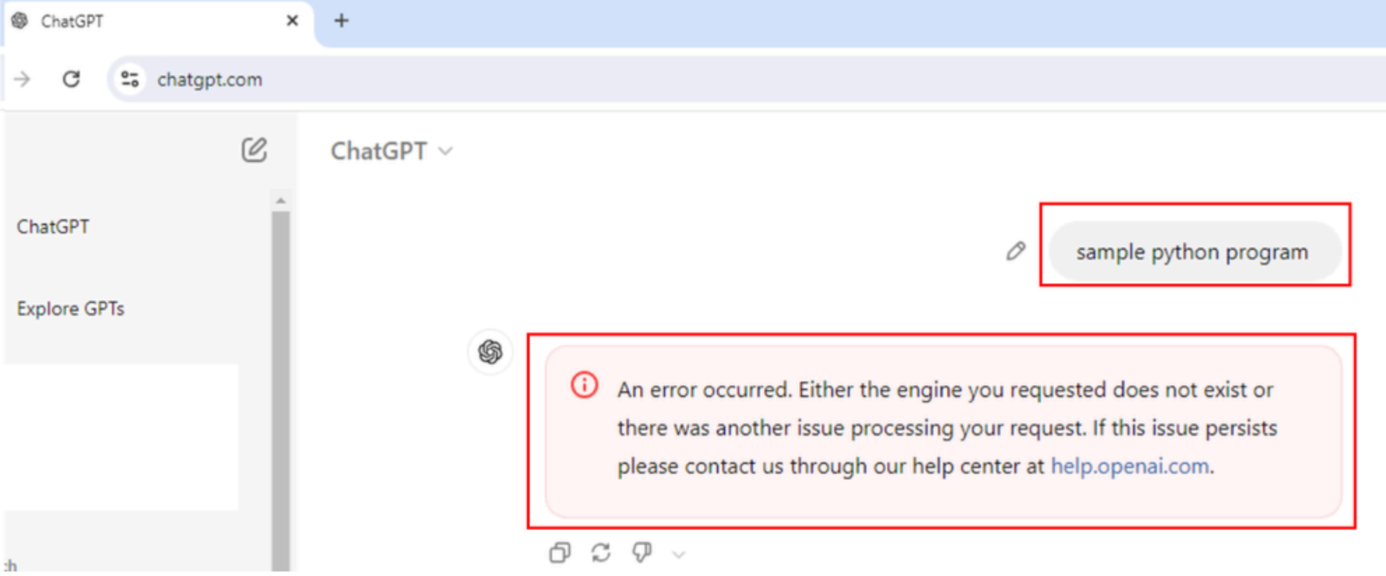
Destinations

2 destinations

Application Settings (2)

OpenAI API OpenAI ChatGPT

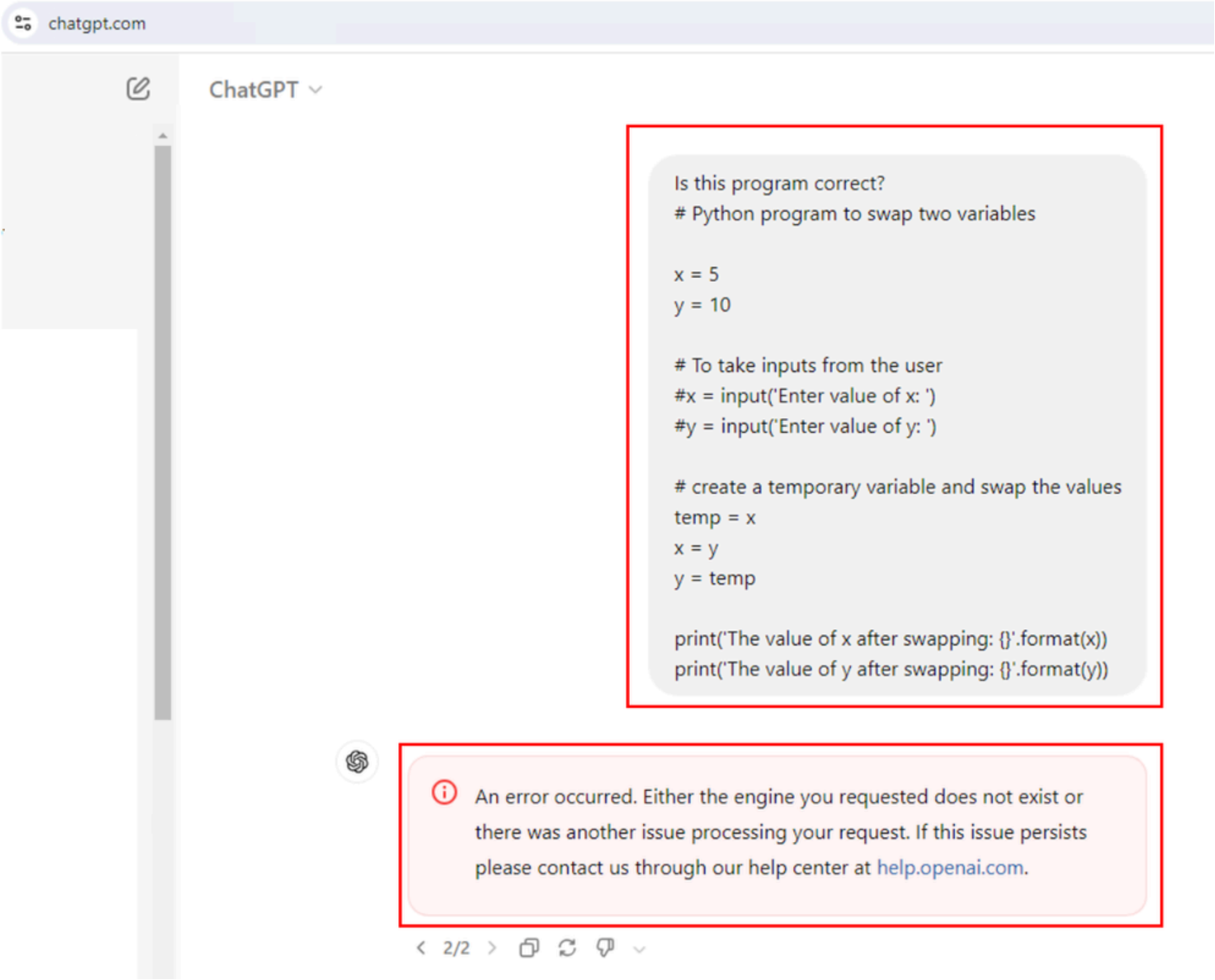
- Ask for a sample python program and this request gets blocked.



sample python program

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.

- Ask if the program is correct or not and this request gets blocked.



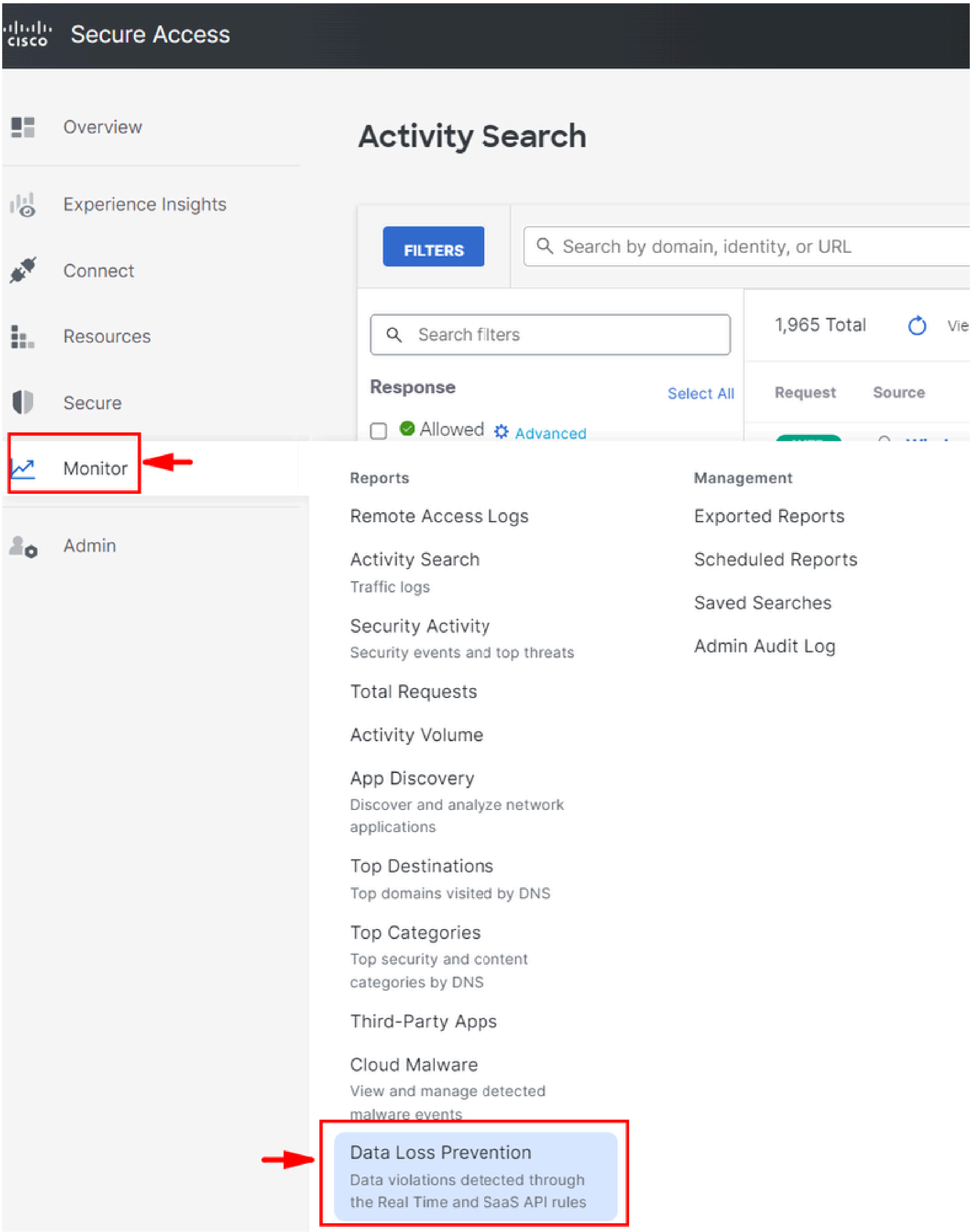
```
Is this program correct?
# Python program to swap two variables

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.

Verify

We can see when user tries to ask ChatGPT for a sample python program, the request gets blocked. We can confirm that a DLP event was triggered in Secure Access Data Loss Prevention logs.

- Go to Monitor> Data Loss Prevention



Secure Access

Overview

Experience Insights

Connect

Resources

Secure

Monitor

Admin

Activity Search

FILTERS

Search by domain, identity, or URL

Search filters

Response

Select All

□ Allowed Advanced

1,965 Total

Request Source

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

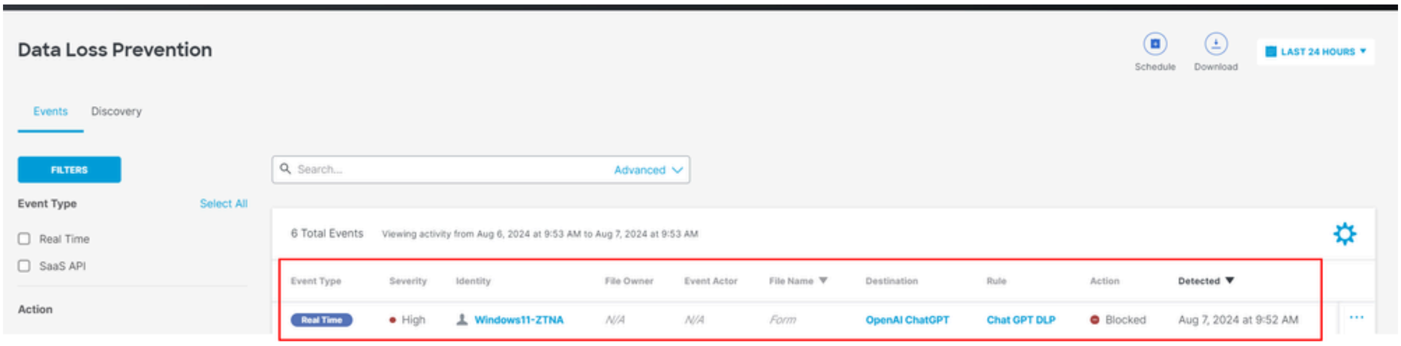
Exported Reports

Scheduled Reports

Saved Searches

Admin Audit Log

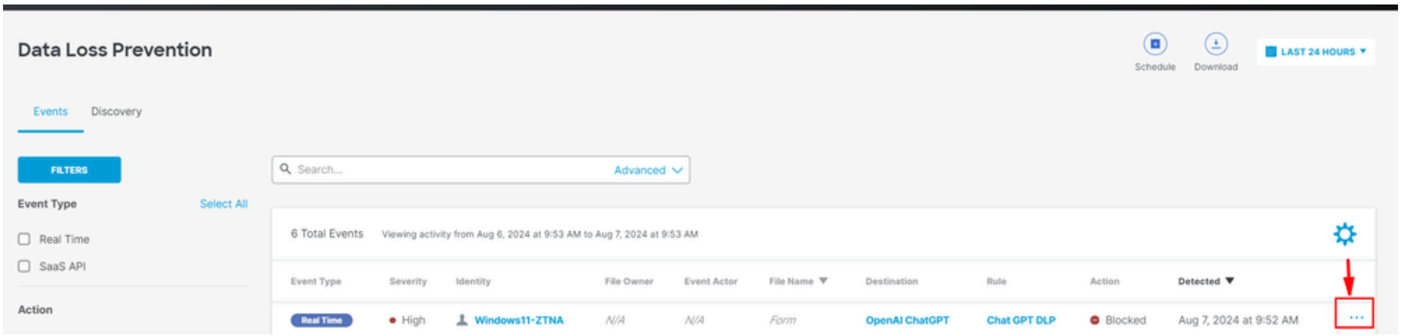
- We are able to see the DLP event.



6 Total Events Viewing activity from Aug 6, 2024 at 9:53 AM to Aug 7, 2024 at 9:53 AM

Event Type	Severity	Identity	File Owner	Event Actor	File Name ▼	Destination	Rule	Action	Detected ▼
Real Time	● High	Windows11-ZTNA	N/A	N/A	Form	OpenAI ChatGPT	Chat GPT DLP	● Blocked	Aug 7, 2024 at 9:52 AM

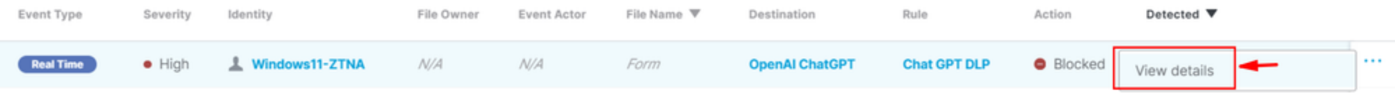
- Click on the three dots at the end of the event log to check for more details about the event.



6 Total Events Viewing activity from Aug 6, 2024 at 9:53 AM to Aug 7, 2024 at 9:53 AM

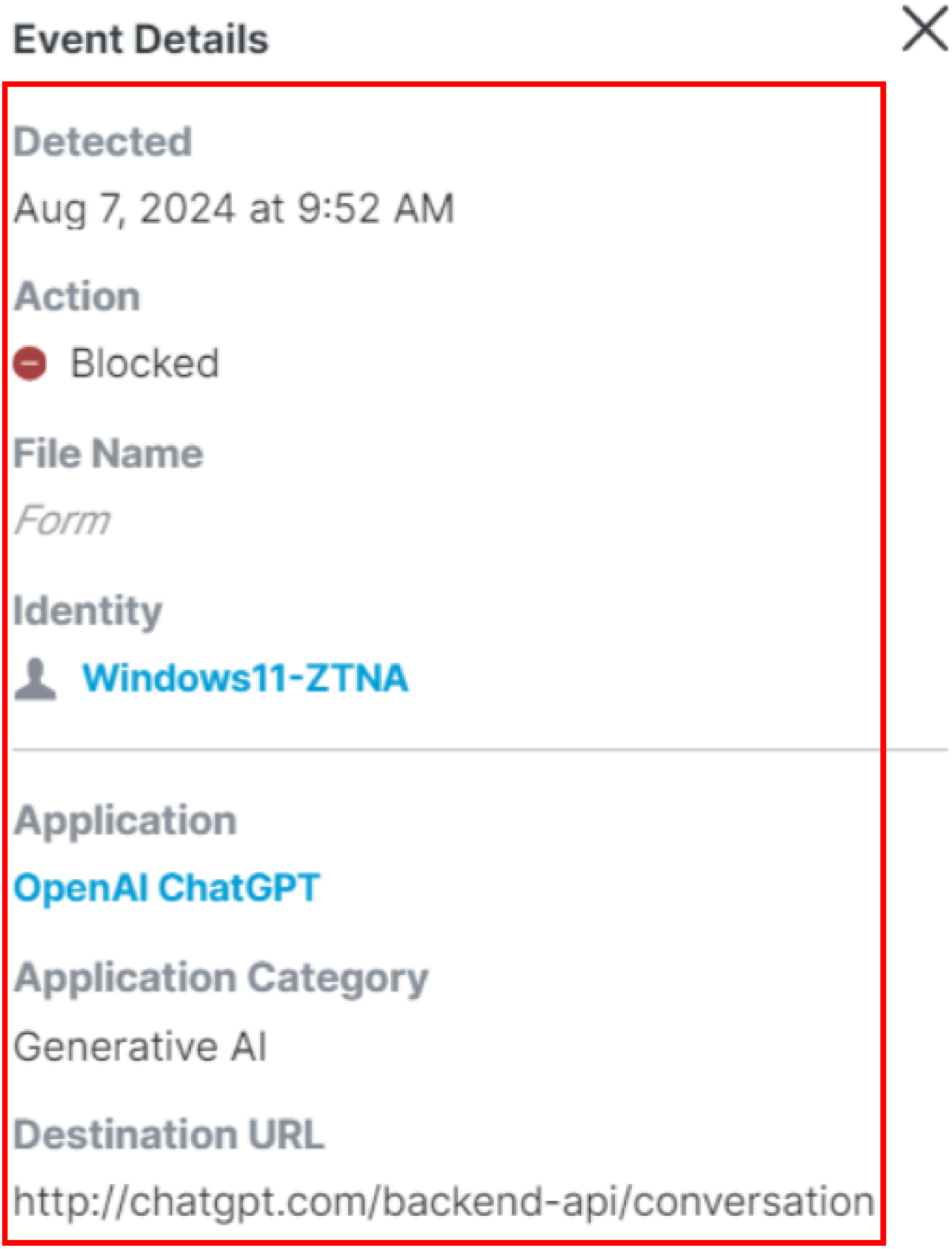
Event Type	Severity	Identity	File Owner	Event Actor	File Name ▼	Destination	Rule	Action	Detected ▼
Real Time	● High	Windows11-ZTNA	N/A	N/A	Form	OpenAI ChatGPT	Chat GPT DLP	● Blocked	Aug 7, 2024 at 9:52 AM

- Click on View details.



Event Type	Severity	Identity	File Owner	Event Actor	File Name ▼	Destination	Rule	Action	Detected ▼
Real Time	● High	Windows11-ZTNA	N/A	N/A	Form	OpenAI ChatGPT	Chat GPT DLP	● Blocked	

- Now we see the entire Event Details.



Event Details

Detected

Aug 7, 2024 at 9:52 AM

Action

Blocked

File Name

Form

Identity

Windows11-ZTNA

Application

OpenAI ChatGPT

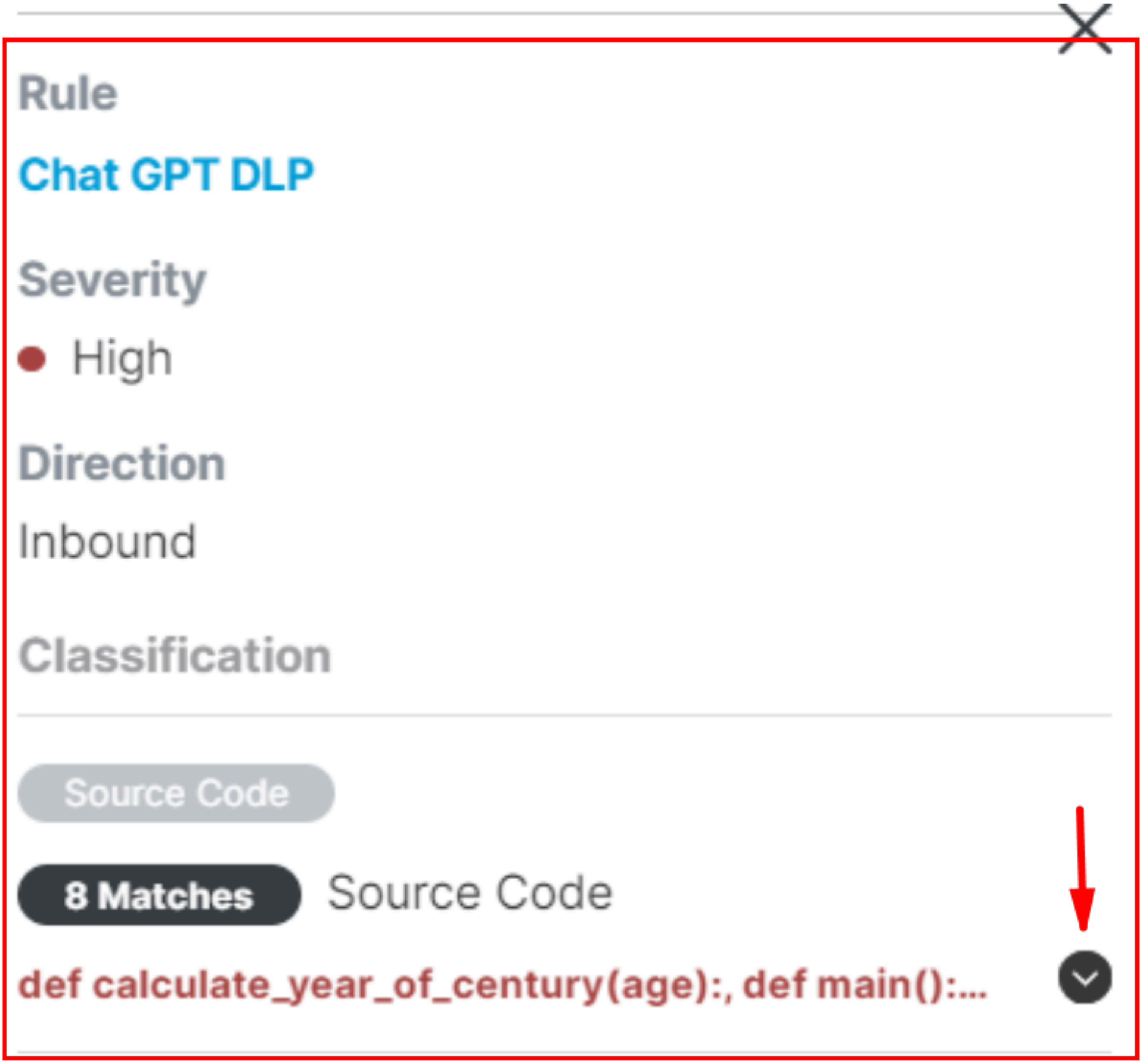
Application Category

Generative AI

Destination URL

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

- Expand the classificaton to see what content matched with the classifier.



Rule

Chat GPT DLP

Severity

● High

Direction

Inbound

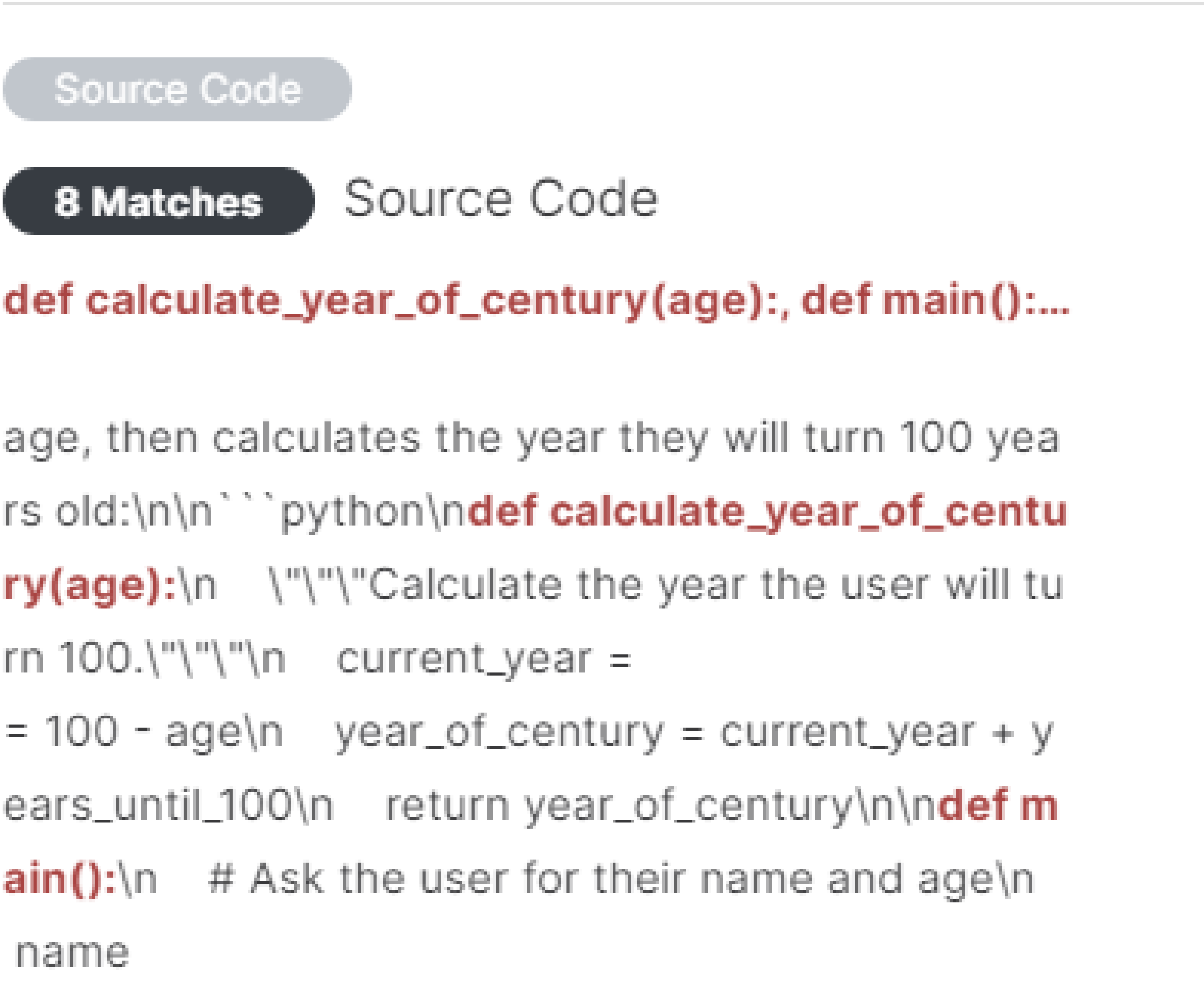
Classification

Source Code

8 Matches Source Code

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

- We see all the details of the content which matched the classifier / Classification of the DLP policy.



Source Code

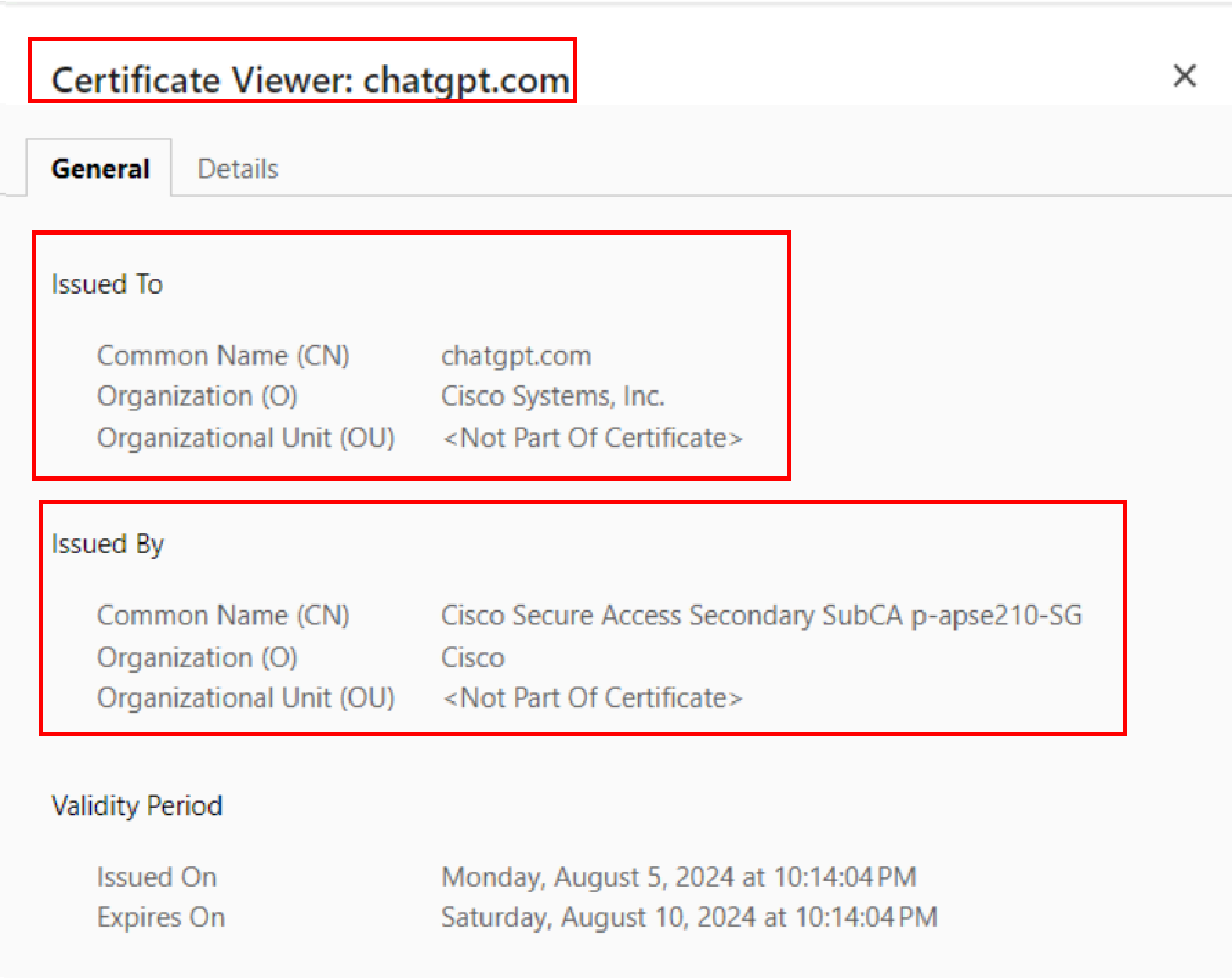
8 Matches Source Code

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

~~~~
age, then calculates the year they will turn 100 yea
rs old:\n\n```python\ndef calculate_year_of_centu
ry(age):\n    \"\"\"Calculate the year the user will tu
rn 100.\"\"\"\n    current_year =
= 100 - age\n    year_of_century = current_year + y
ears_until_100\n    return year_of_century\n\ndef m
ain():\n    # Ask the user for their name and age\n
 name
~~~~

Troubleshoot

- Ensure the access policy which matches web requests for Open AI ChatGPT has decryption enabled.
- To quickly check if SSE is decrypting traffic for Open AI ChatGPT, check the certificate of the website which shows common name includes keywords "Cisco Secure Access" in it.



Certificate Viewer: chatgpt.com

Issued To

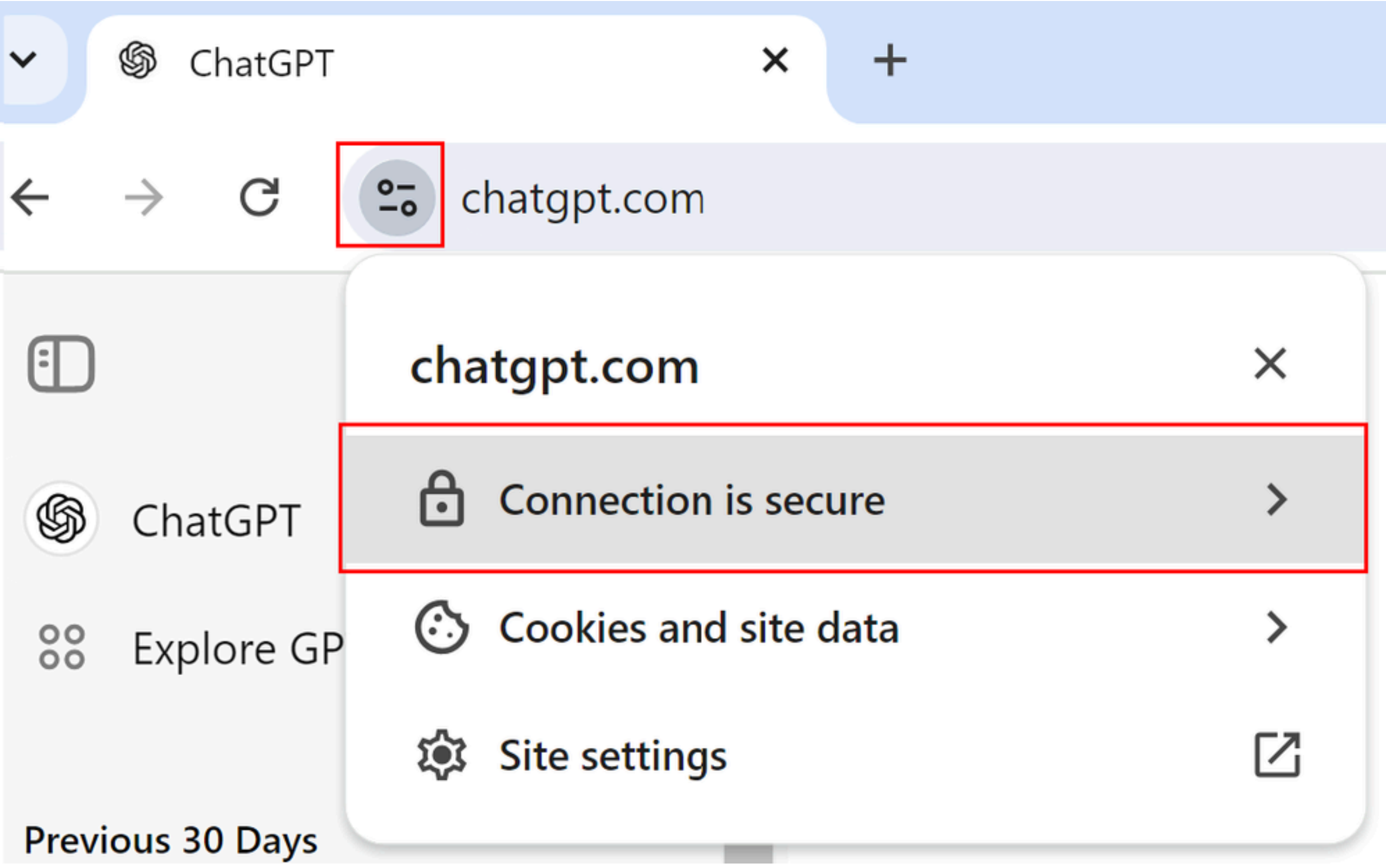
Common Name (CN)	chatgpt.com
Organization (O)	Cisco Systems, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

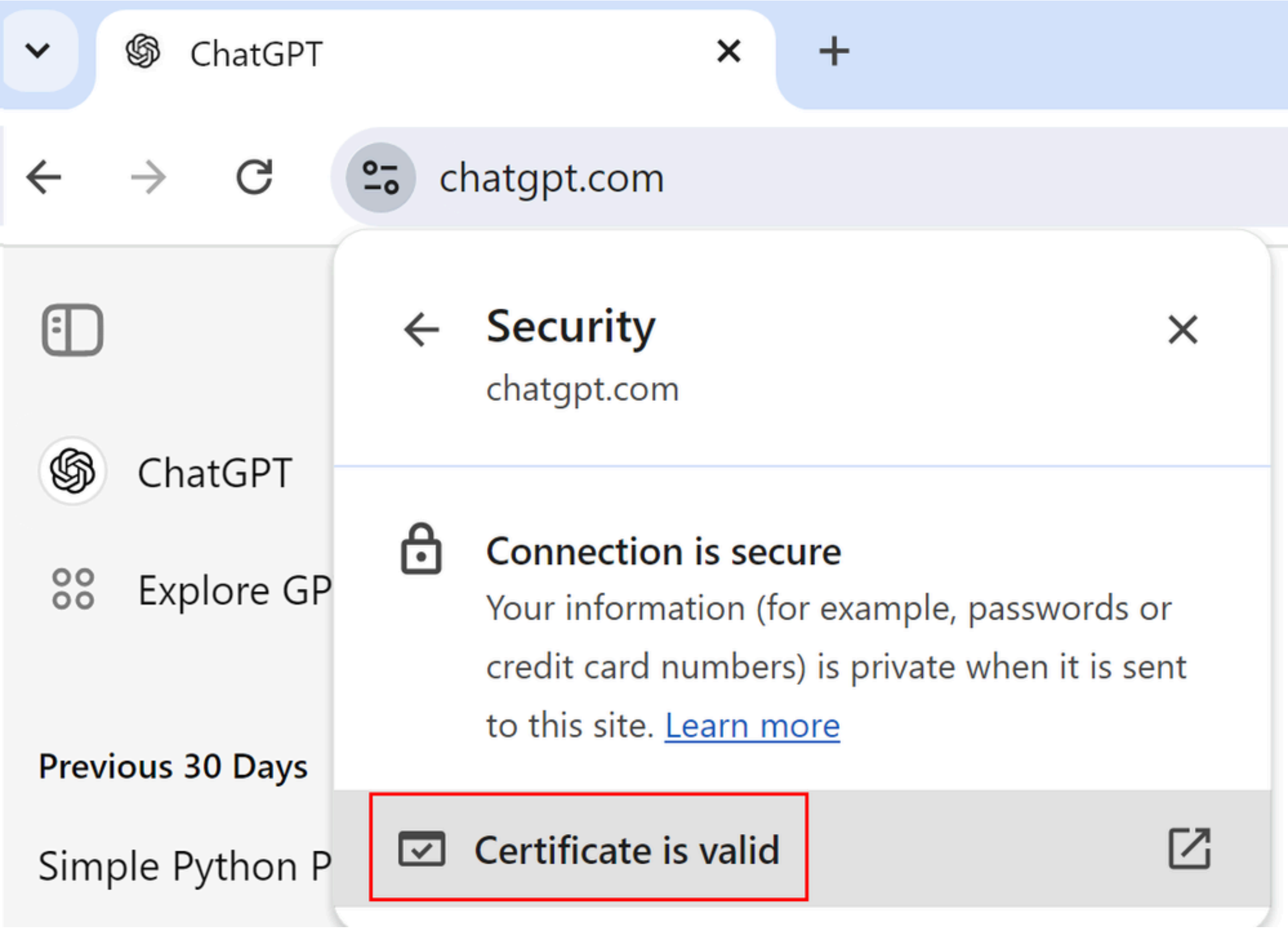
Issued By

Common Name (CN)	Cisco Secure Access Secondary SubCA p-apse210-SG
Organization (O)	Cisco
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

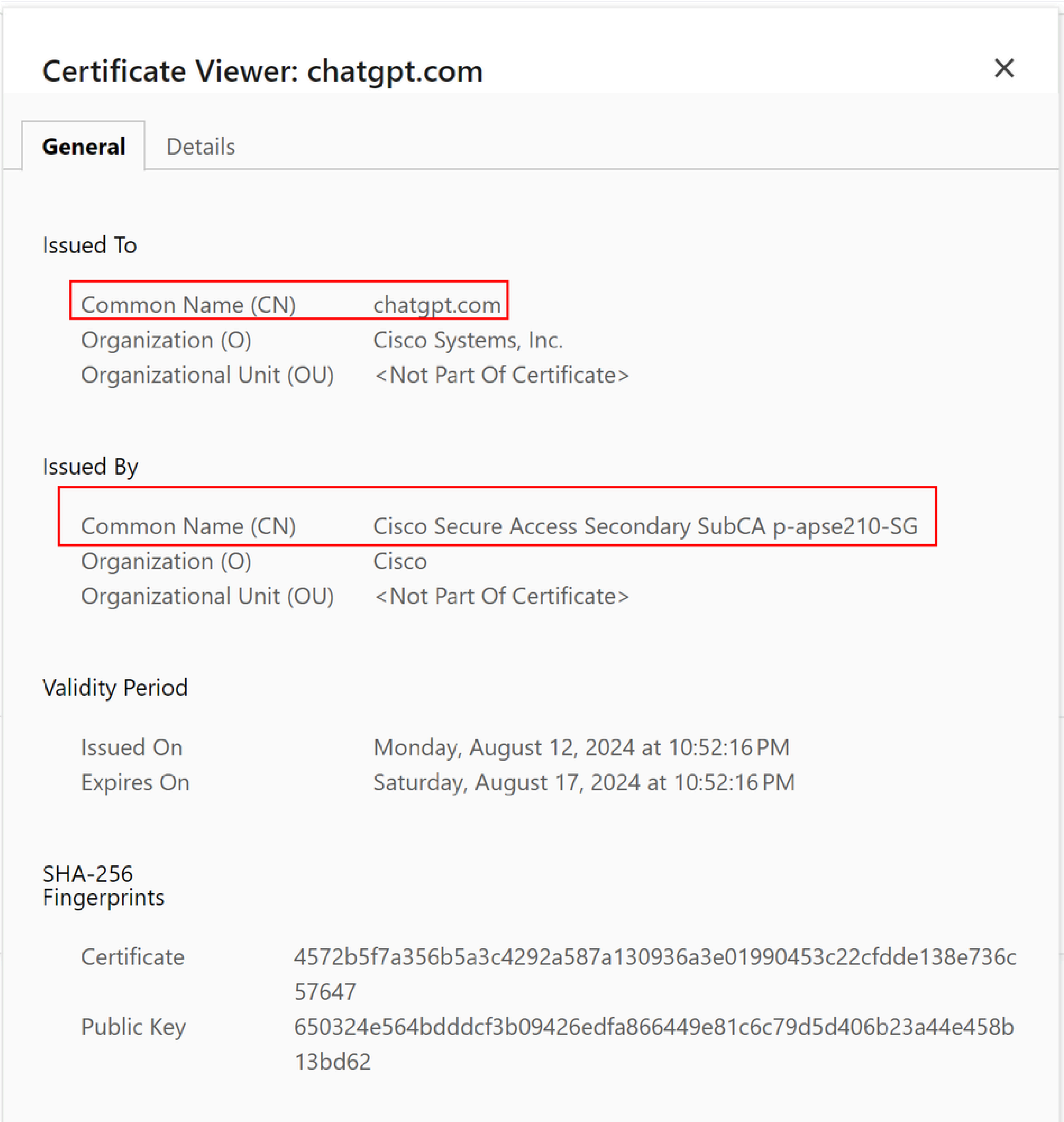
Issued On	Monday, August 5, 2024 at 10:14:04 PM
Expires On	Saturday, August 10, 2024 at 10:14:04 PM





Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more



Certificate Viewer: chatgpt.com

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>

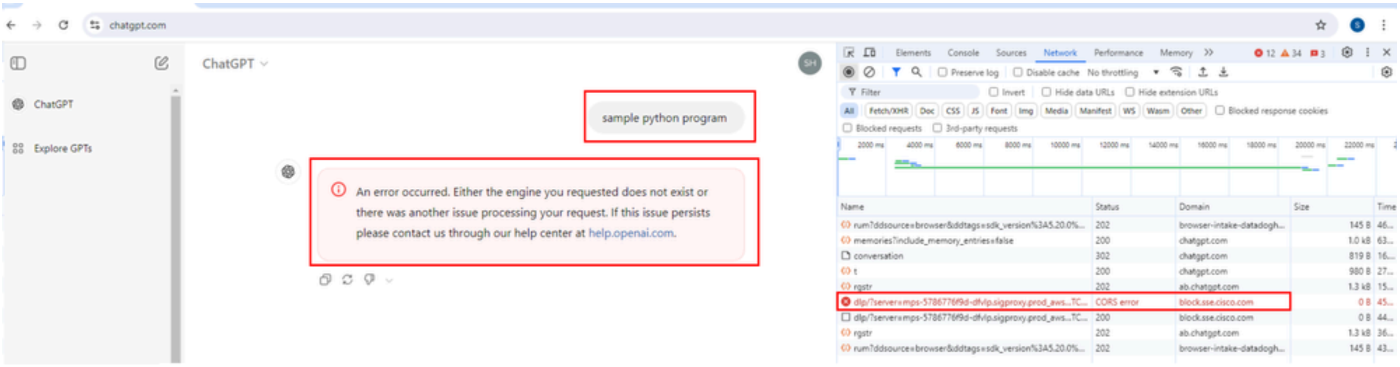
Validity Period

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

- Open ChatGPT > Open developer tools > Select Network > Next try to ask ChatGPT for a sample python program
- Observe that the request results in a block. Under domain you see "block.sse.cisco.com

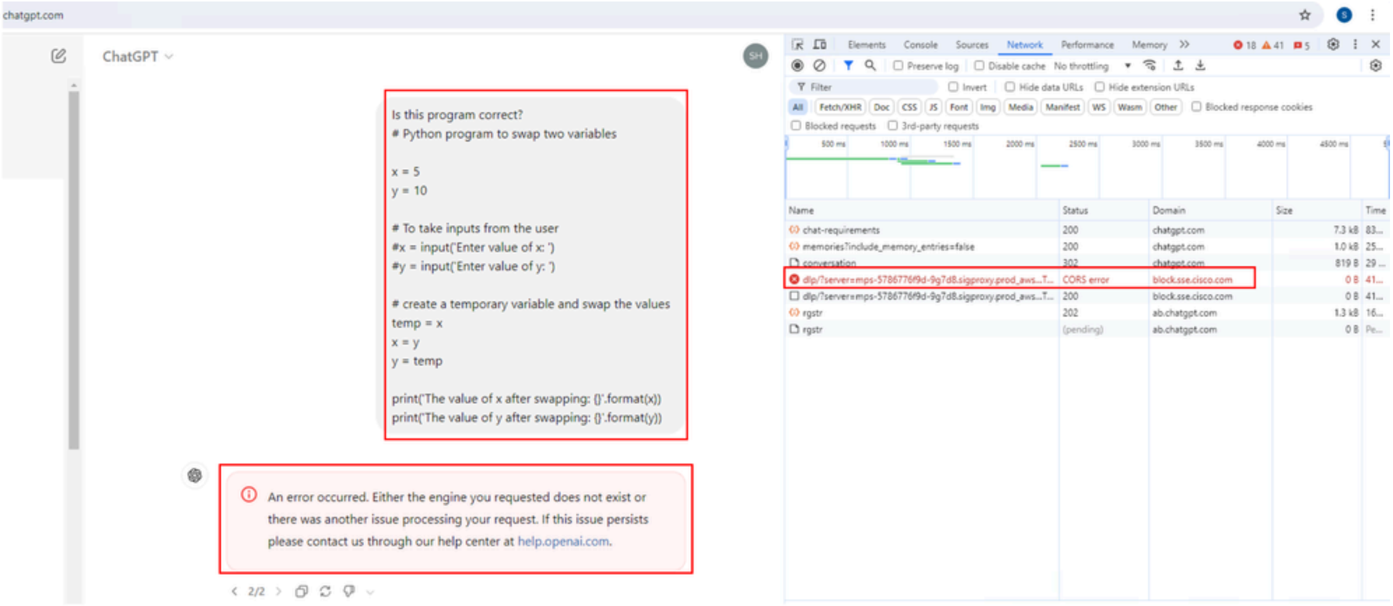


sample python program

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.

Name	Status	Domain	Size	Time
rum?ddsource=browser&ddtags=sdk_version%3A5.20.0%...	202	browser-intake-datadogh...	145 B	46...
memories?include_memory_entries=false	200	chatgpt.com	1.0 kB	63...
conversation	302	chatgpt.com	819 B	16...
t	200	chatgpt.com	980 B	27...
rgstr	202	ab.chatgpt.com	1.3 kB	15...
dlp/?server=mps-5786776f9d-dfvlp.sigproxy.prod_aws...TC...	CORS error	block.sse.cisco.com	0 B	45...
dlp/?server=mps-5786776f9d-dfvlp.sigproxy.prod_aws...TC...	200	block.sse.cisco.com	0 B	44...
rgstr	202	ab.chatgpt.com	1.3 kB	36...
rum?ddsource=browser&ddtags=sdk_version%3A5.20.0%...	202	browser-intake-datadogh...	145 B	43...

- Ask ChatGPT whether the program code is correct.
- Observe that the request results in a block and under "domain" you see "block.sse.cisco.com".



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.

Name	Status	Domain	Size	Time
chat-requirements	200	chatgpt.com	7.3 kB	83...
memories?include_memory_entries=false	200	chatgpt.com	1.0 kB	25...
conversation	302	chatgpt.com	819 B	29 ...
dlp/?server=mps-5786776f9d-9g7d8.sigproxy.prod_aws...T...	CORS error	block.sse.cisco.com	0 B	41...
dlp/?server=mps-5786776f9d-9g7d8.sigproxy.prod_aws...T...	200	block.sse.cisco.com	0 B	41...
rgstr	202	ab.chatgpt.com	1.3 kB	16...
rgstr	(pending)	ab.chatgpt.com	0 B	Pe...

Related Information

- Cisco Secure Access User Guide
- Cisco Technical Support and Downloads