# Implementazione di DLP in accesso sicuro per limitare l'utilizzo di GPT per la programmazione tramite chat API aperta

## Sommario



## Introduzione

In questo documento viene descritto come implementare Data Loss Prevention (DLP) in Secure Access per limitare l'utilizzo di Open AI ChatGPT per la programmazione e la codifica.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso sicuro
- DLP
- Apri API ChatGPT

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Accesso sicuro

- DLP
- Apri API ChatGPT

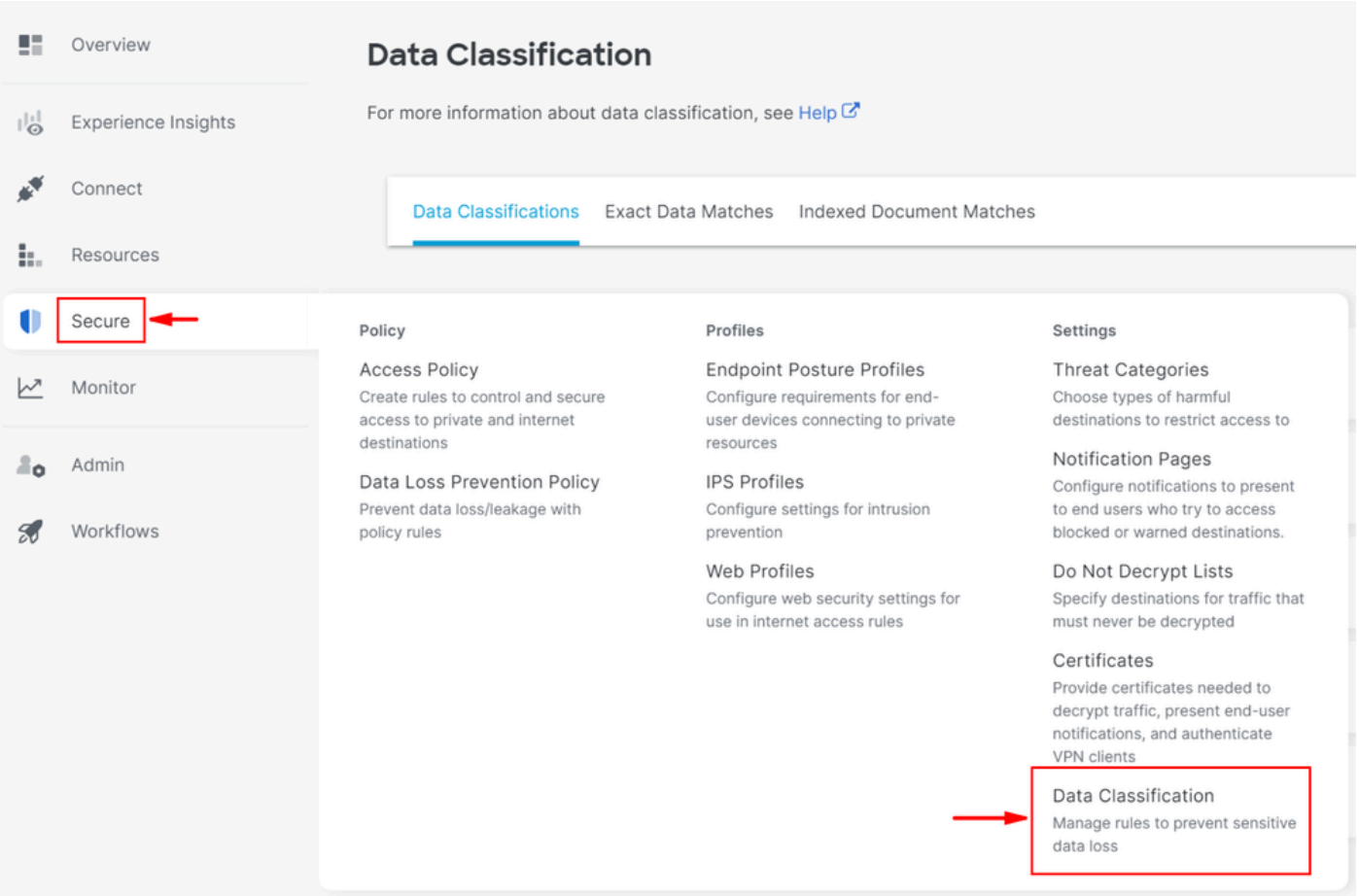
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Configurazione

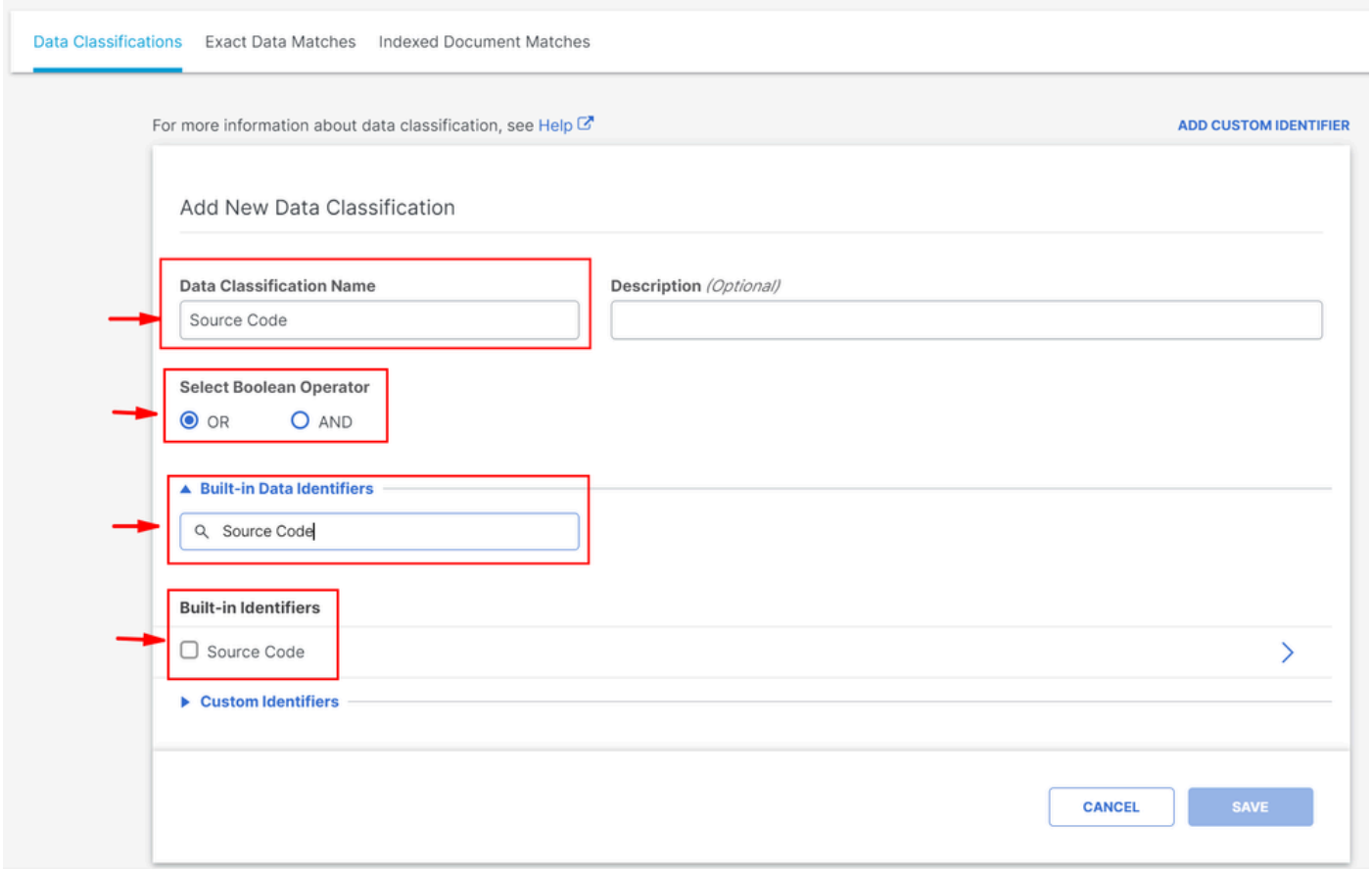
## 1.Creare una classificazione dei dati per utilizzare l'identificatore dei dati del codice sorgente

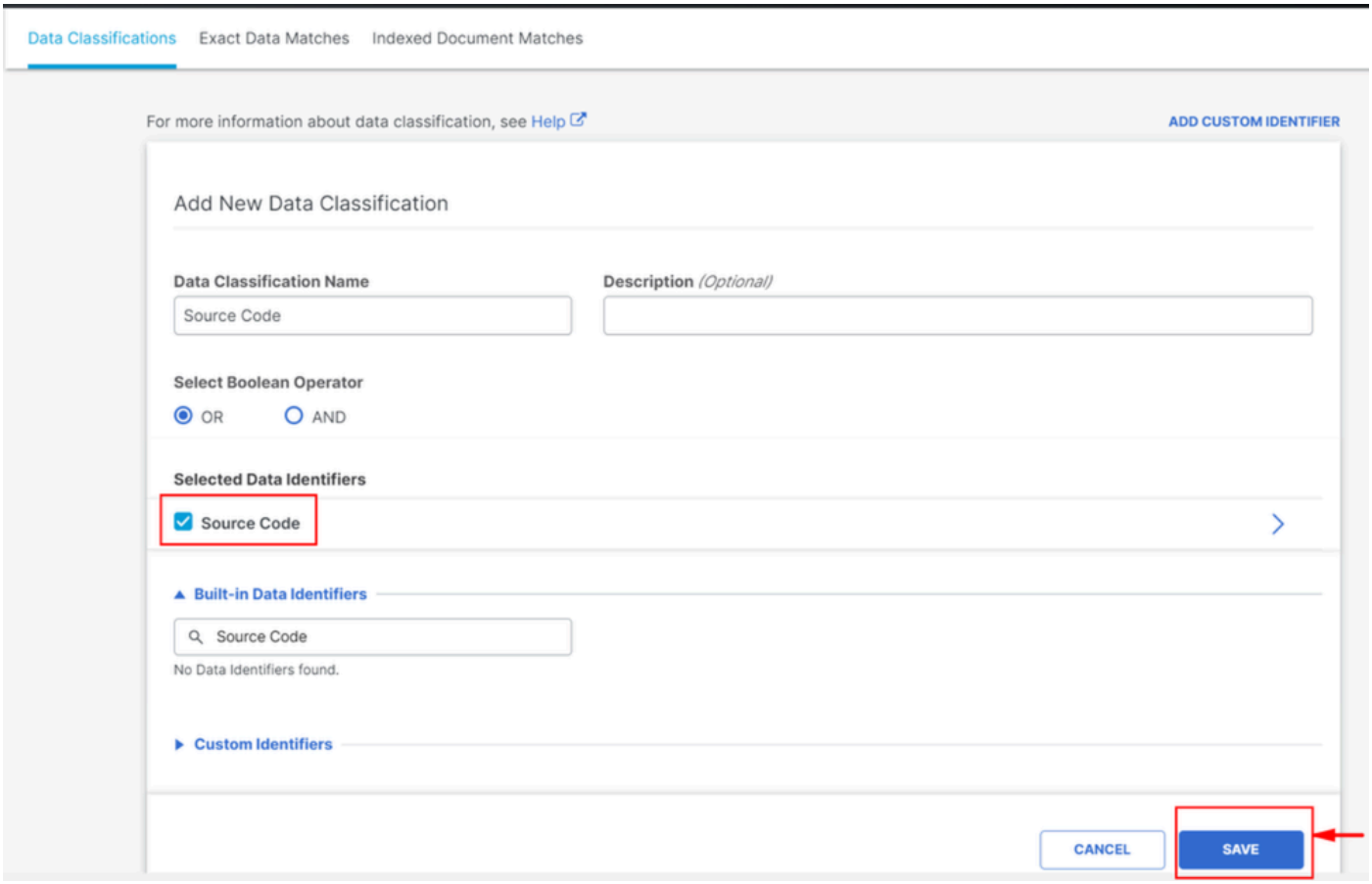
Passare a Dashboard di accesso protetto.

- Fare clic su Secure > Data Classification > Add



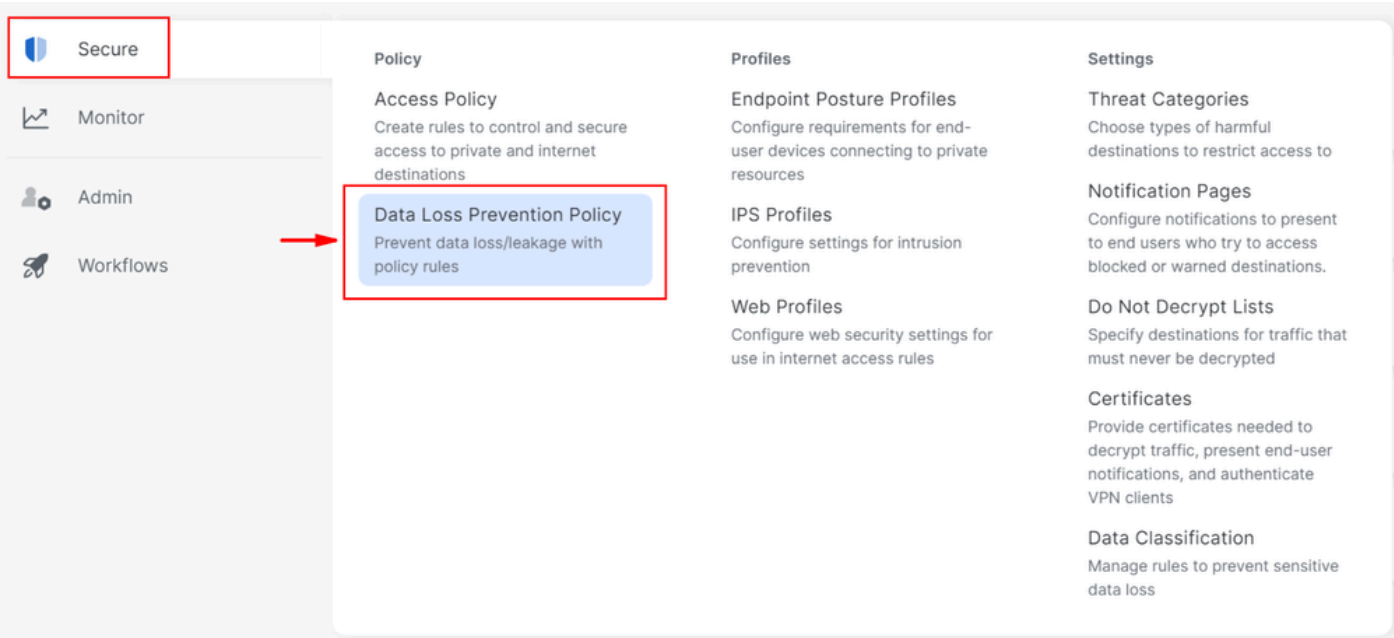

- Immettere il comando Data Classification Name > **Seleziona** Built-in Data Identifiers > Cerca Source Code e selezionarlo



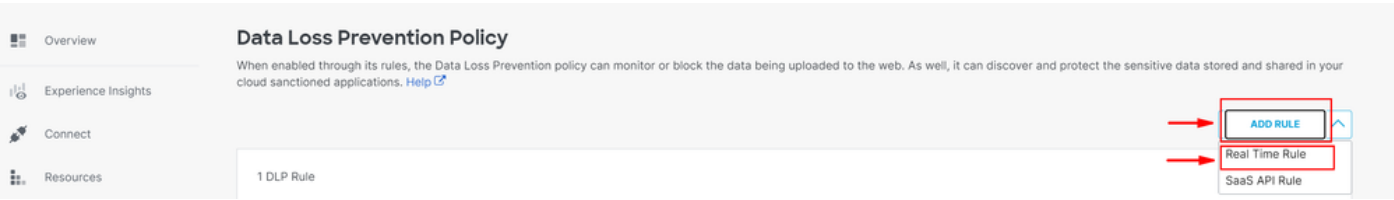




2. Creare i criteri di prevenzione della perdita dei dati e chiamarli "Codice sorgente" per la classificazione dei dati.

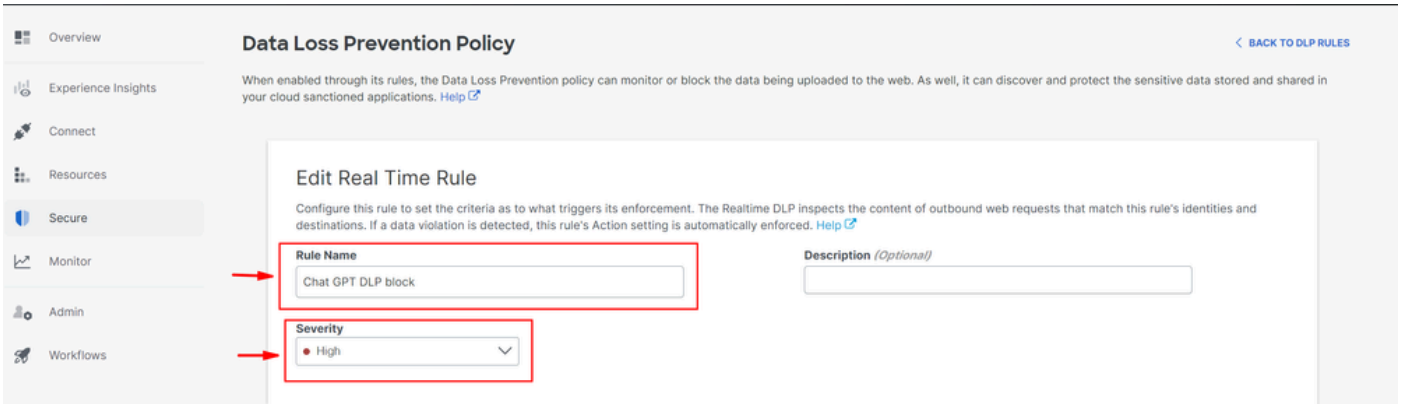
- Fare clic su Secure > Data Loss Prevention Policy



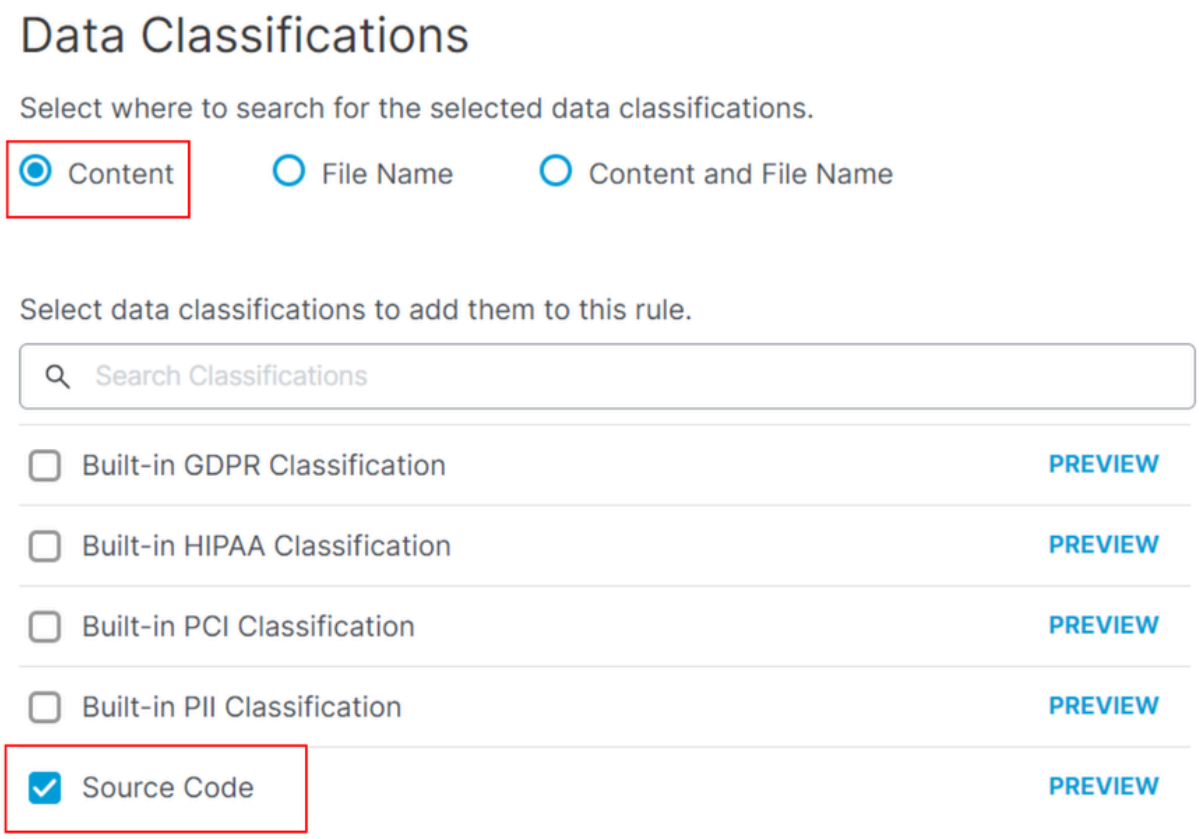

- Fare clic su Add Rule > Real Time Rule



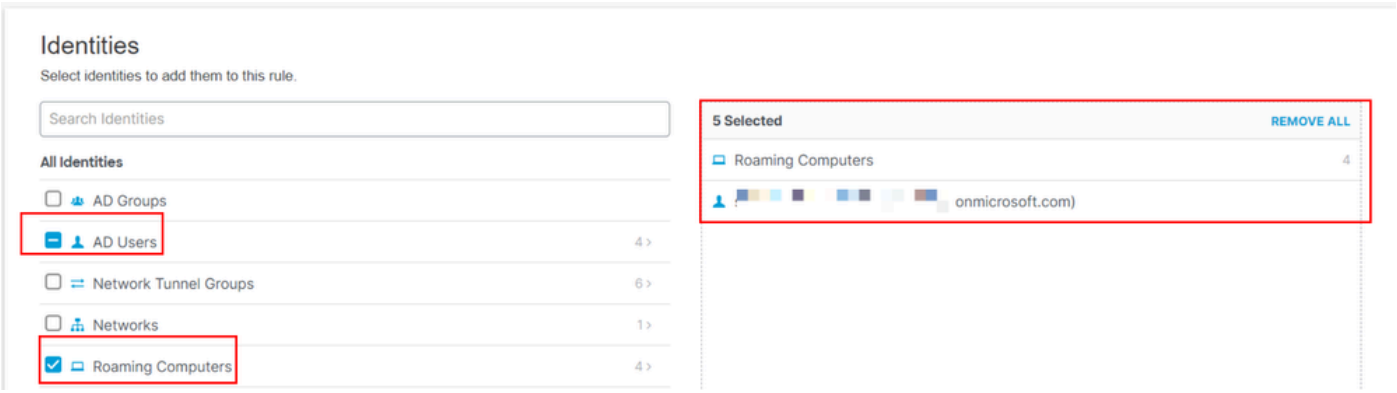

- Fornire un Rule Name > Imposta appropriato Severity




- In Seleziona (Select)Data Classifications Content e selezionate Source Code

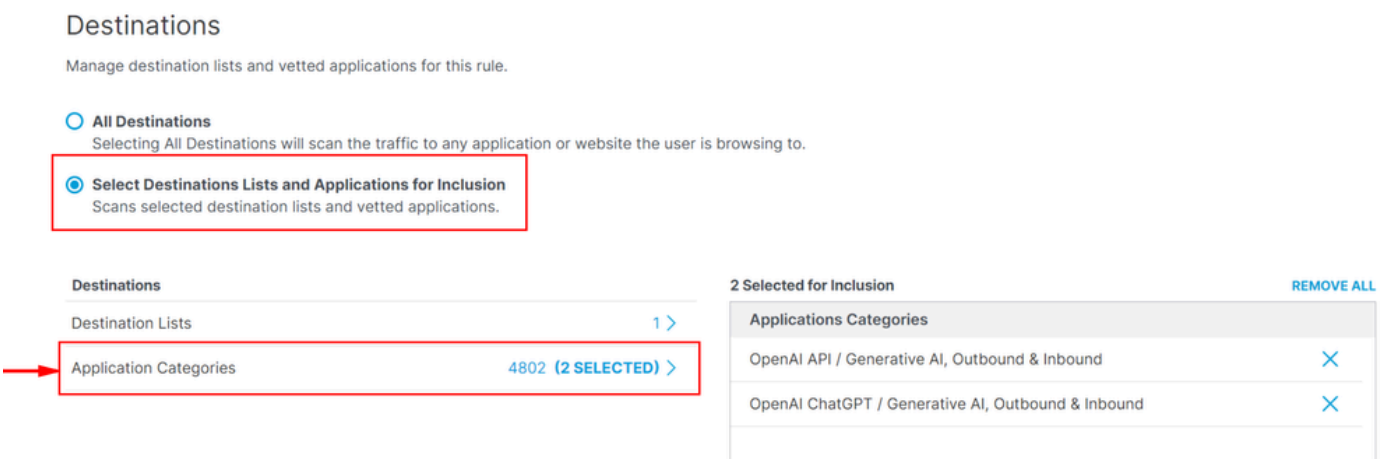



- In Identitiesselezionare le identità desiderate

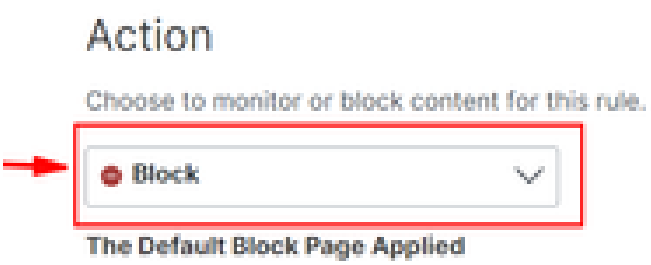


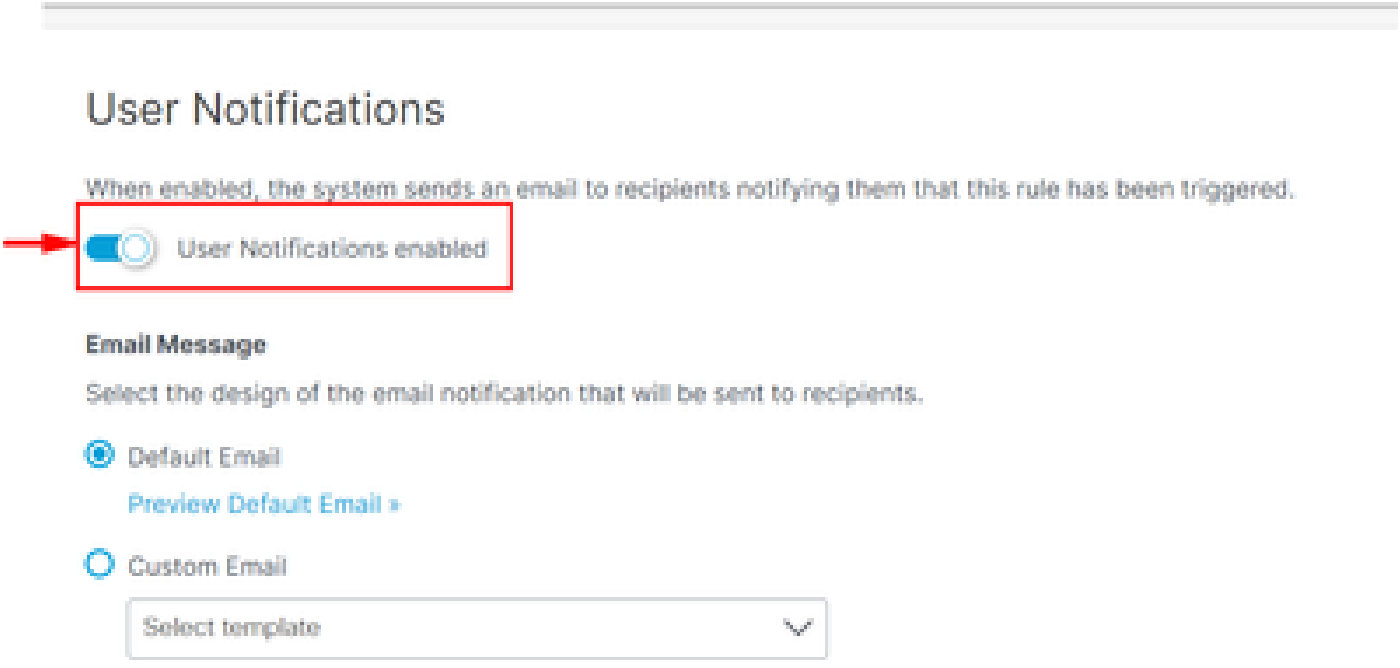

- In Destinazioni selezionare Select Destination Lists and Applications for Inclusion

- Seleziona Application Categories> Seleziona Generative AI > Seleziona OpenAI API (Vetted) e OpenAI ChatGPT (Vetted)in Outbound and InboundDirection

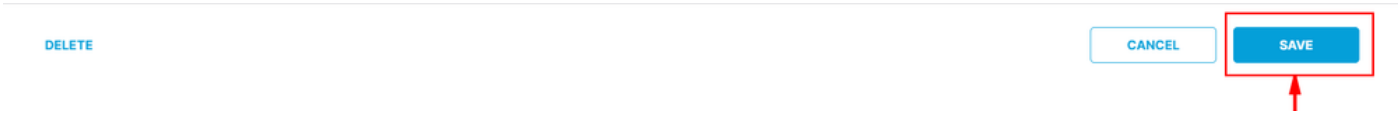



- In Actionseleziona Block
- In User Notifications, è possibile impostare notifiche e-mail per gli utenti finali quando la regola viene attivata (facoltativo)



- Fare clic su Save




3. Assicurarsi di disporre di criteri di accesso a Internet per il traffico verso Chat GPT con decrittografia abilitata.

**Esempio:**

# Chat GPT

Internet

## General

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

## Sources

Any

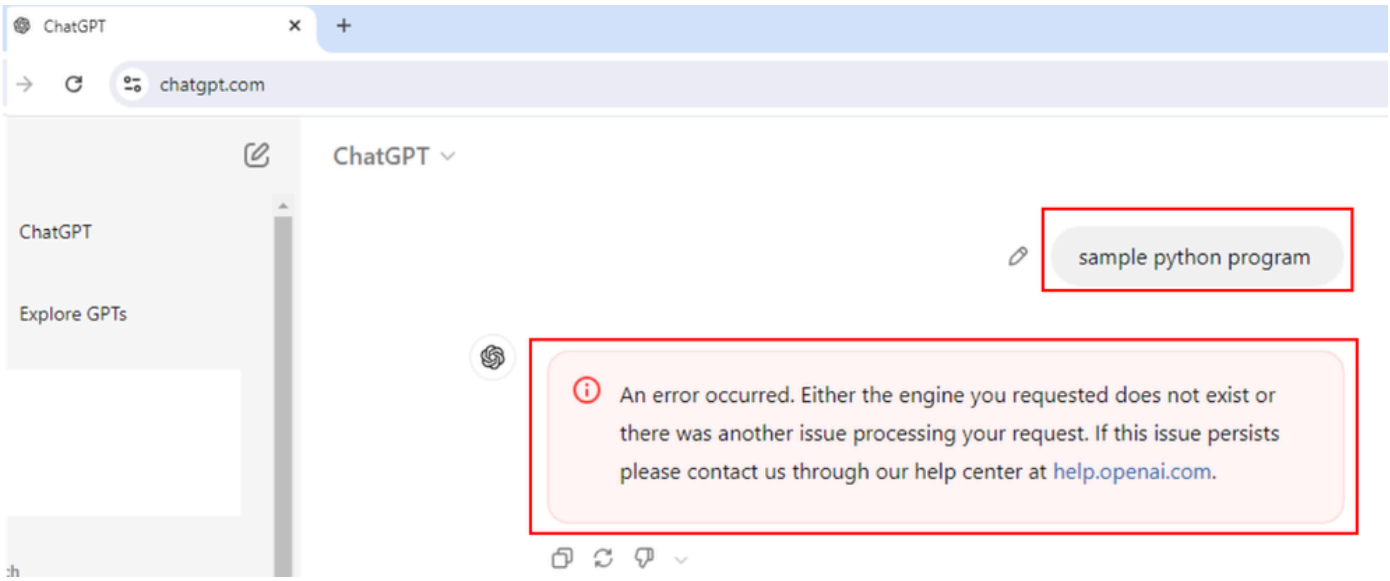
## Destinations

2 destinations

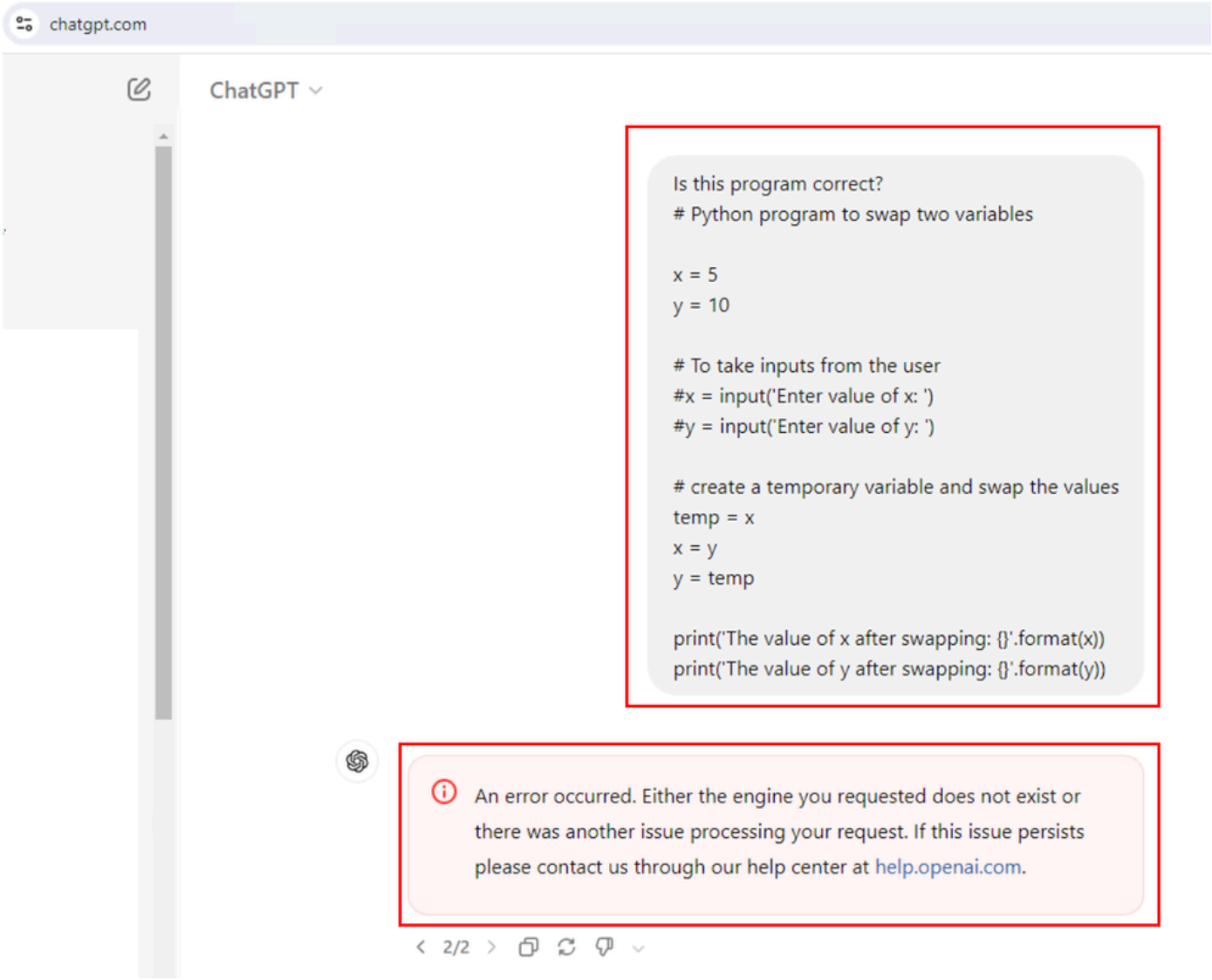
### Application Settings (2)

OpenAI API  OpenAI ChatGPT

- Chiedi un programma Python di esempio e questa richiesta viene bloccata.




- Chiedere se il programma è corretto o meno e questa richiesta viene bloccata.

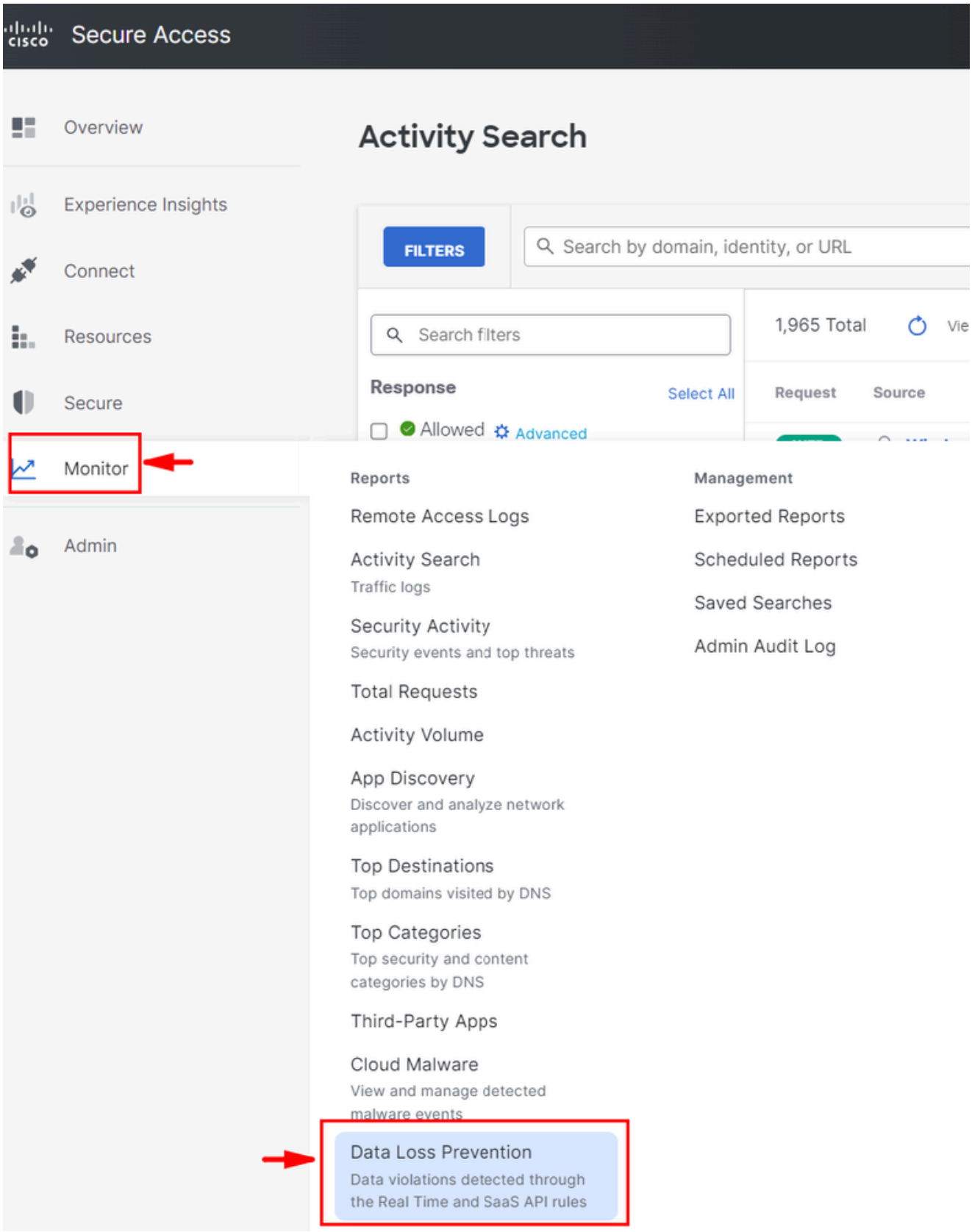



Verifica

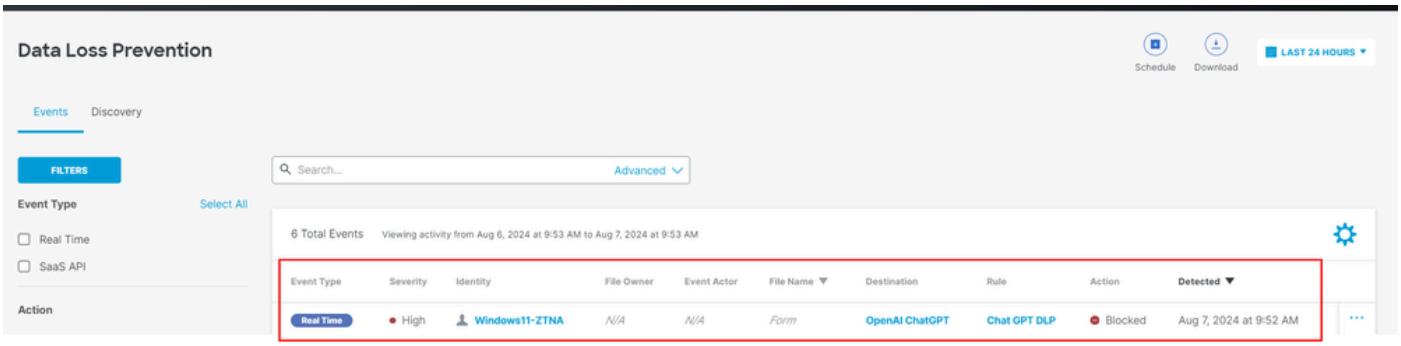
Possiamo vedere quando l'utente cerca di chiedere a ChatGPT un programma Python di esempio, la richiesta viene bloccata.

Possiamo confermare che un evento DLP è stato attivato nei log di Secure Access Data Loss Prevention.

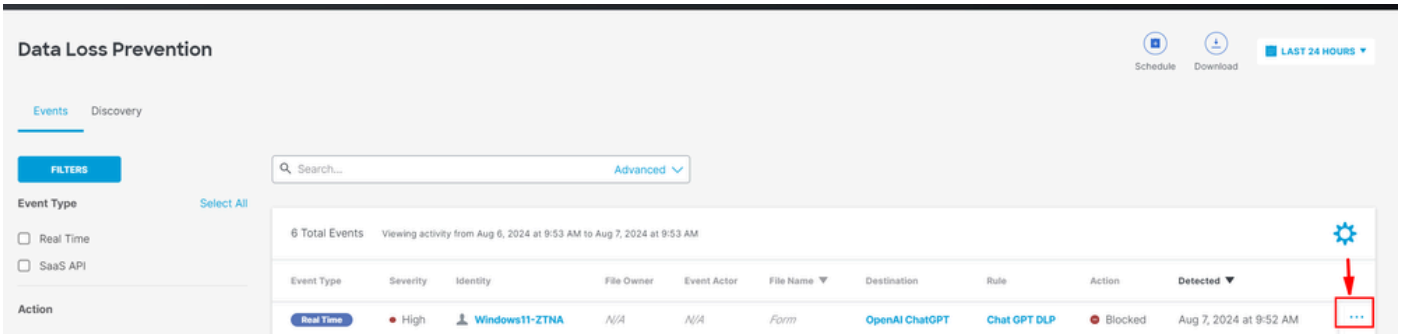
- Vai a Monitor> Data Loss Prevention



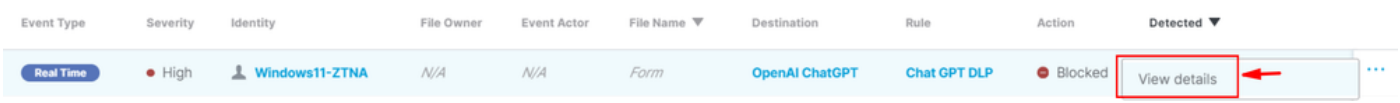

- Siamo in grado di vedere l'evento DLP.



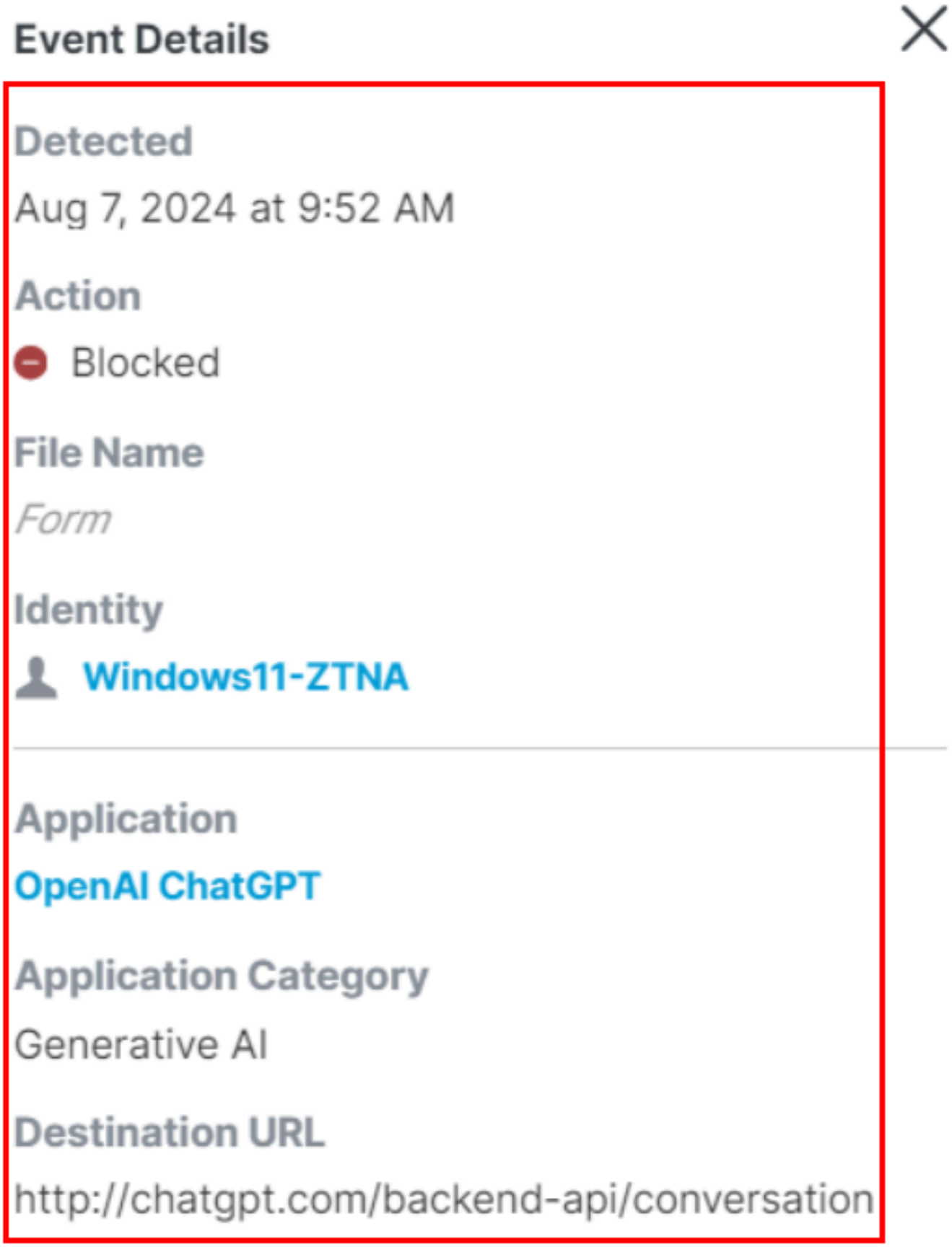

- Fare clic sui tre punti alla fine del registro eventi per verificare ulteriori dettagli sull'evento.



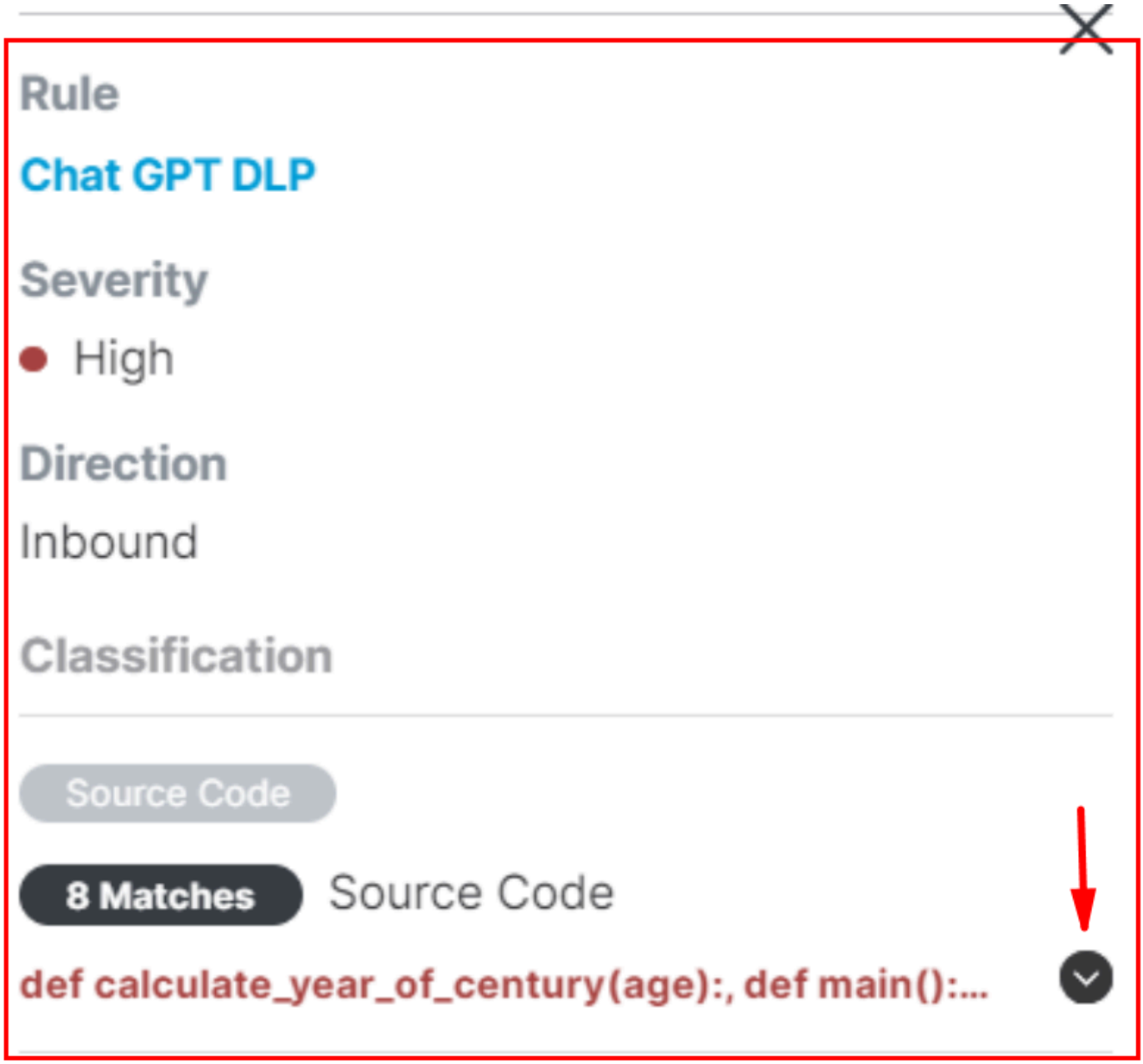

- Fare clic su View details.



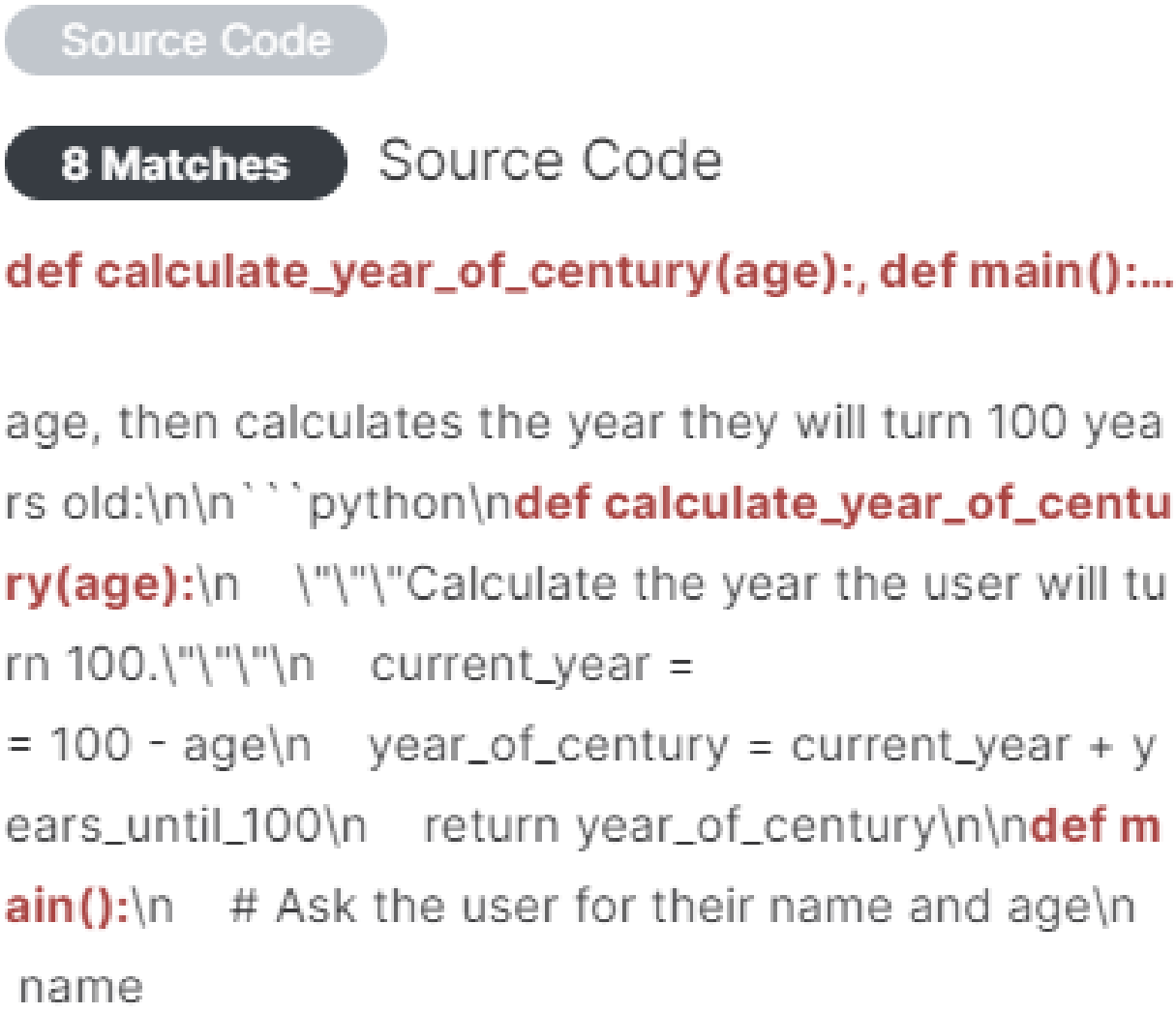

- A questo punto è possibile visualizzare tutti i dettagli dell'evento.




- Espandere la classificazione per visualizzare il contenuto corrispondente al classificatore.

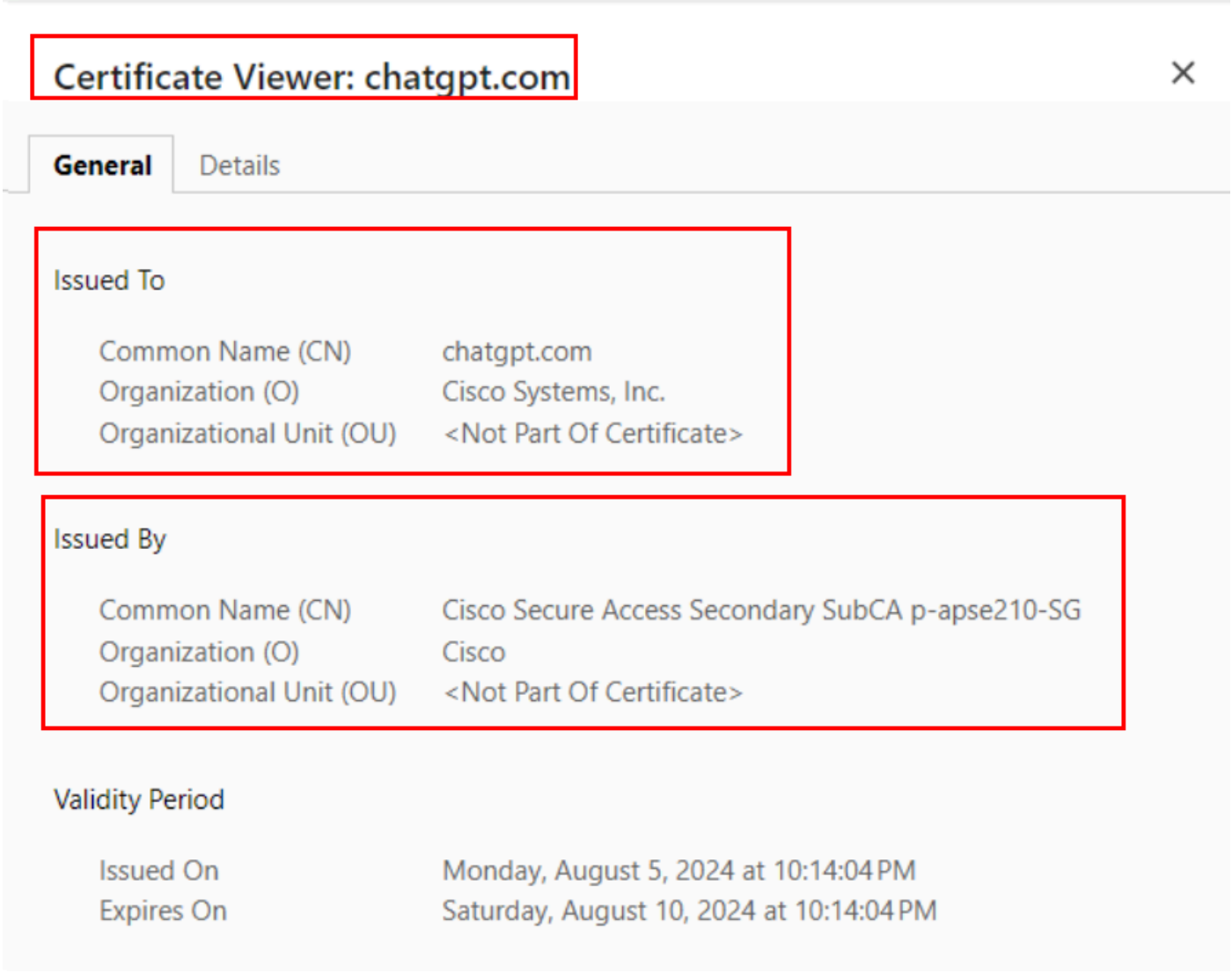


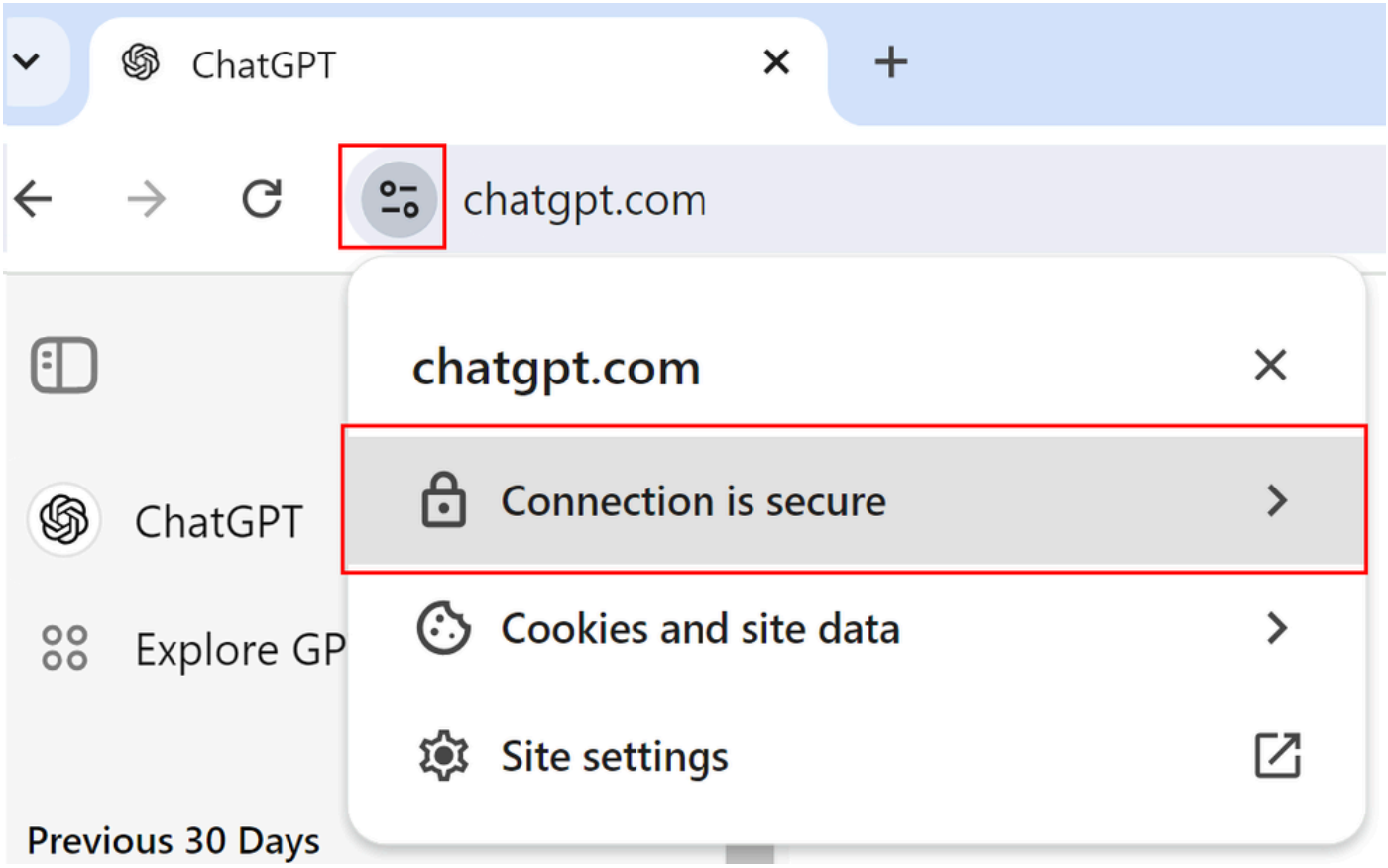

- Vediamo tutti i dettagli del contenuto che corrisponde al classificatore / classificazione dei criteri di prevenzione della perdita dei dati.

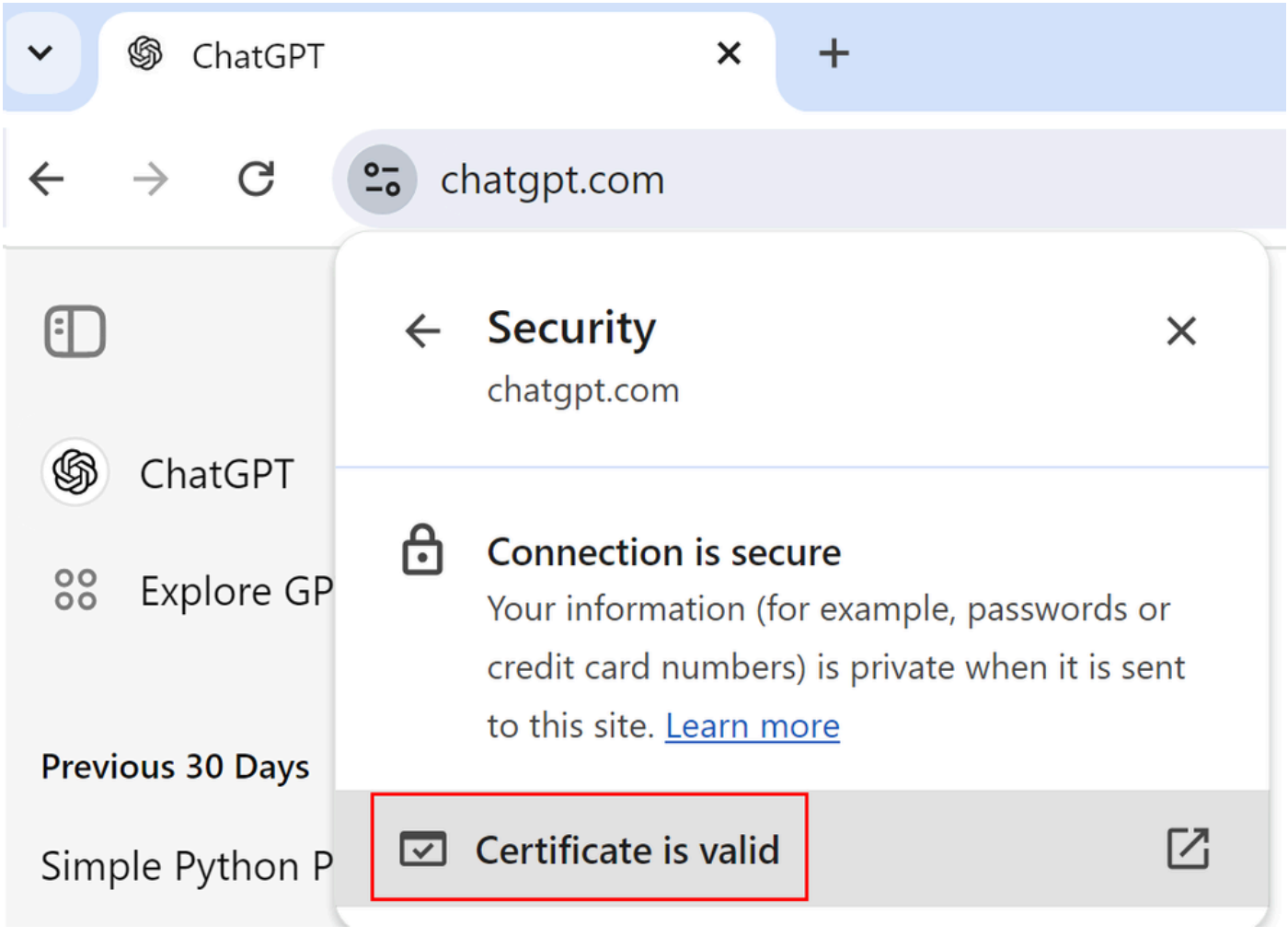


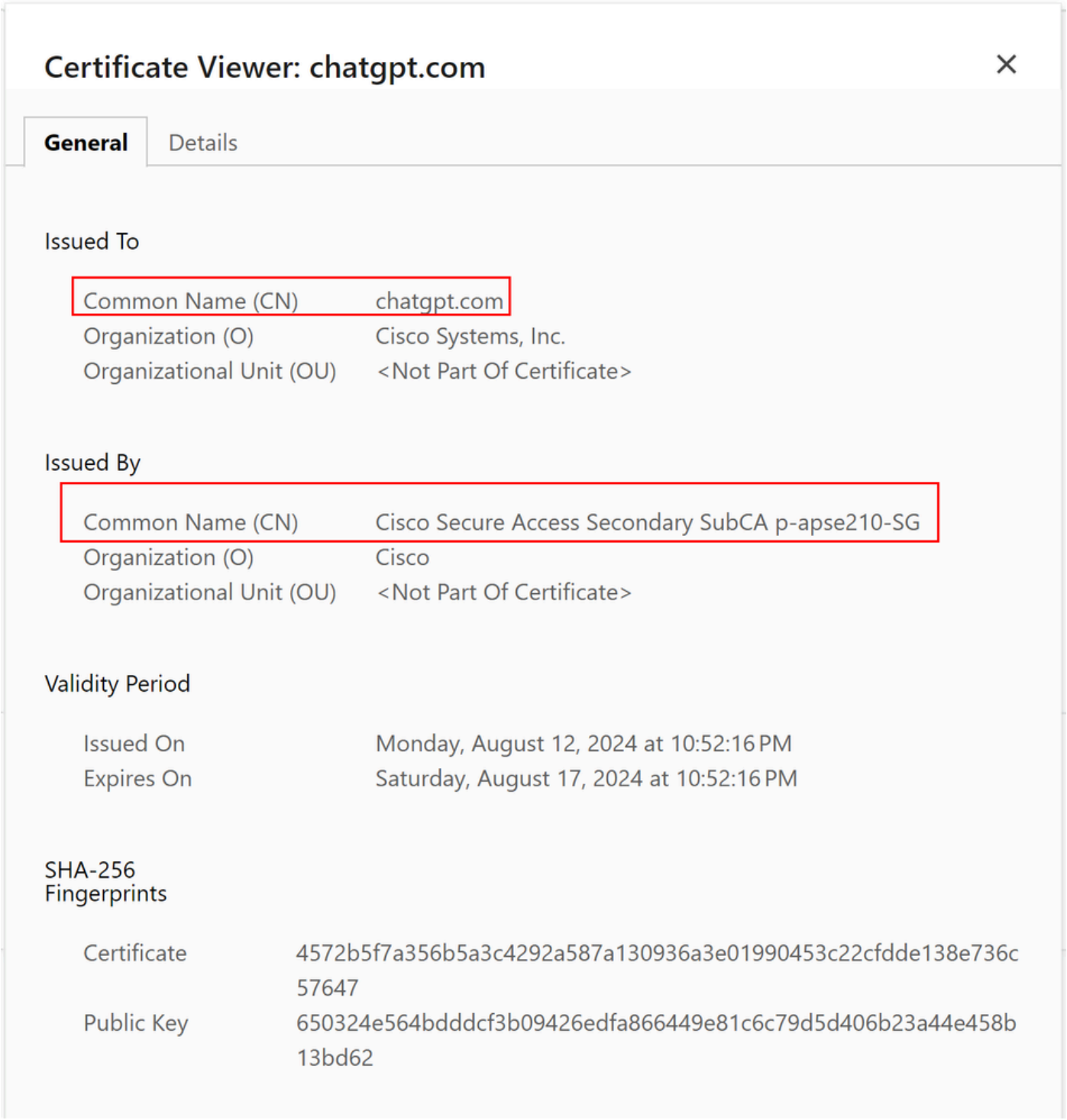

Risoluzione dei problemi

- Verificare che il criterio di accesso corrispondente alle richieste Web per Open API ChatGPT abbia la decrittografia abilitata.
- Per verificare rapidamente se SSE sta decrittografando il traffico per Open AI ChatGPT, controllare il certificato del sito web che mostra il nome comune che include le parole chiave "Cisco Secure Access" in esso.


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

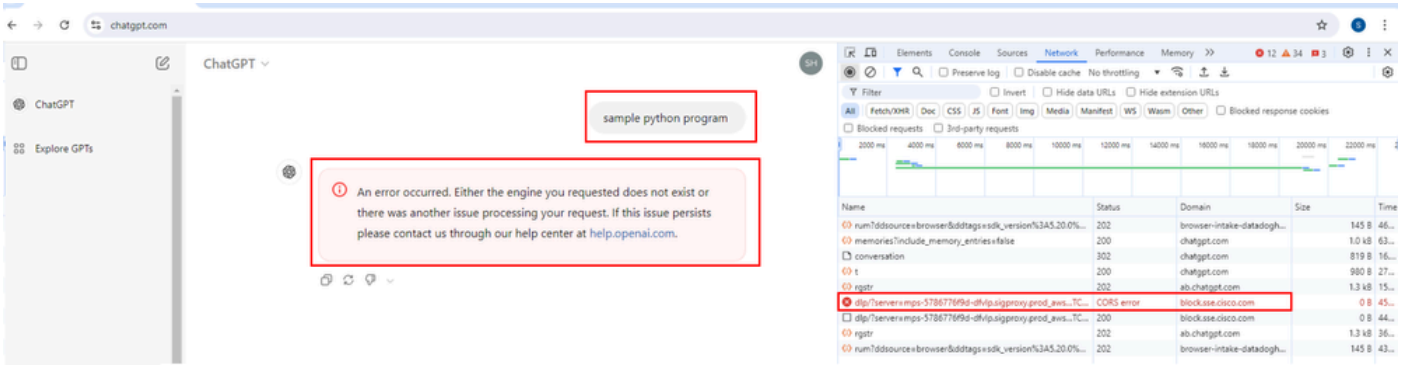

ChatGPT
chatgpt.com
chatgpt.com
Connection is secure
Cookies and site data
Site settings
ChatGPT
Explore GP
Previous 30 Days


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

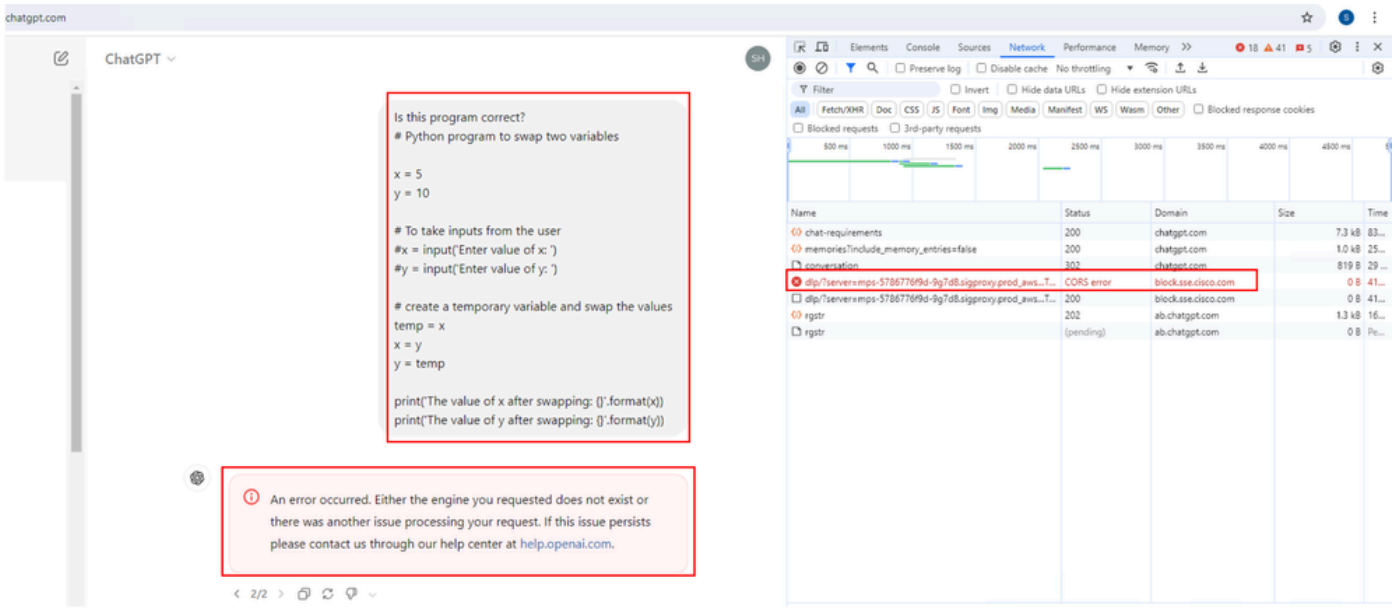



- Apri ChatGPT > Apri strumenti di sviluppo > Seleziona Rete > Avanti prova a chiedere a ChatGPT un programma Python di esempio

- La richiesta genera un blocco. Sotto dominio si vede "block.sse.cisco.com




- Chiedere a ChatGPT se il codice del programma è corretto.
- Si noti che la richiesta genera un blocco e sotto "dominio" viene visualizzato "block.sse.cisco.com".




Informazioni correlate

- Guida per l'utente di Cisco Secure Access
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).