DLP in Secure Access to Restricted Open AI ChatGPT-gebruik voor programmeren implementeren

Inhoud

Inleiding

Dit document beschrijft hoe u DLP (Data Loss Prevention) in Secure Access kunt implementeren om het gebruik van Open AI ChatGPT voor programmering en codering te beperken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Beveiligde toegang
- DLP
- AI-chatGPT openen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Beveiligde toegang
- DLP
- AI-chatGPT openen

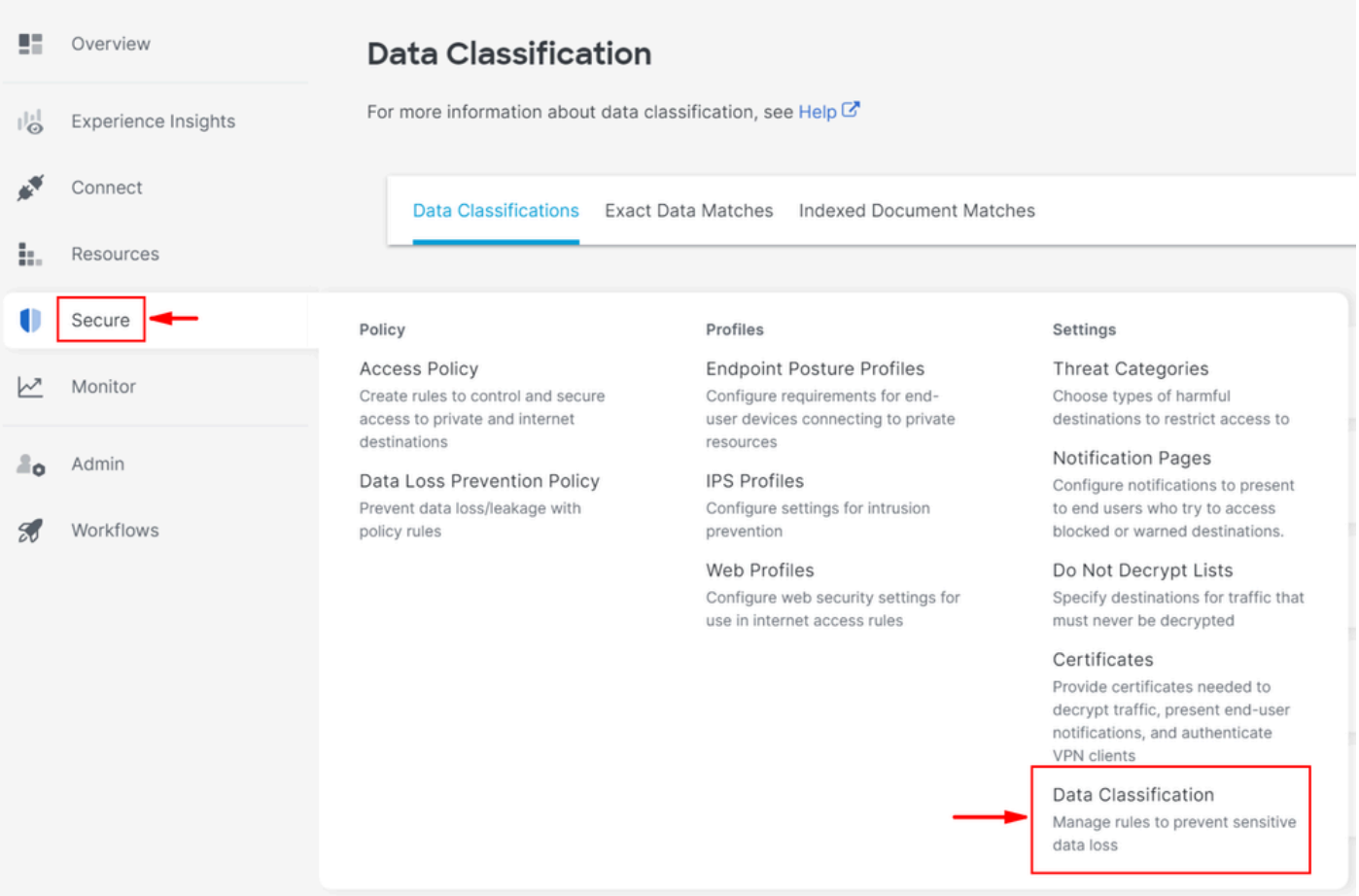
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

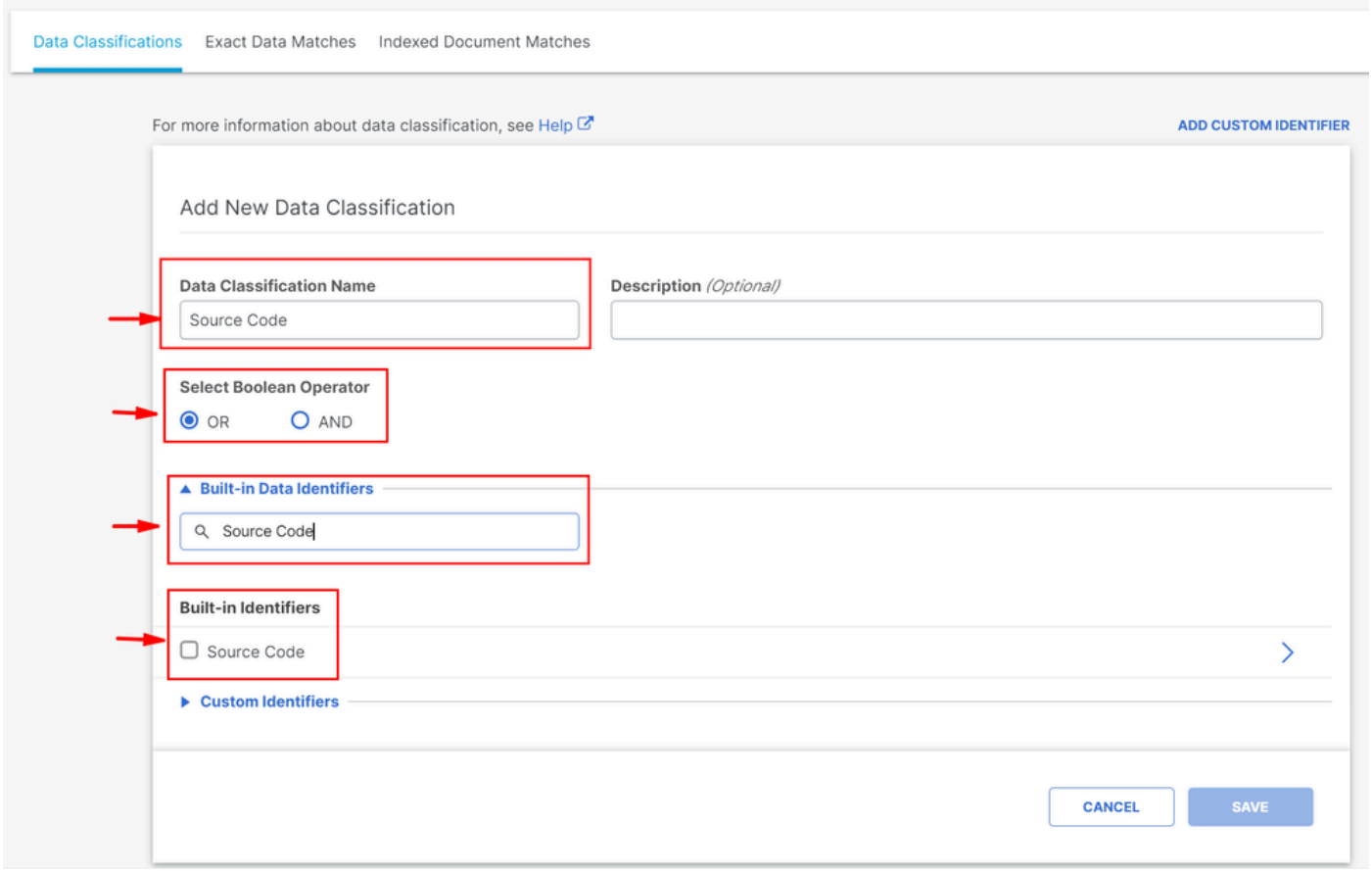
1.Maak een gegevensclassificatie om het Identificatiecode van de broncode te gebruiken

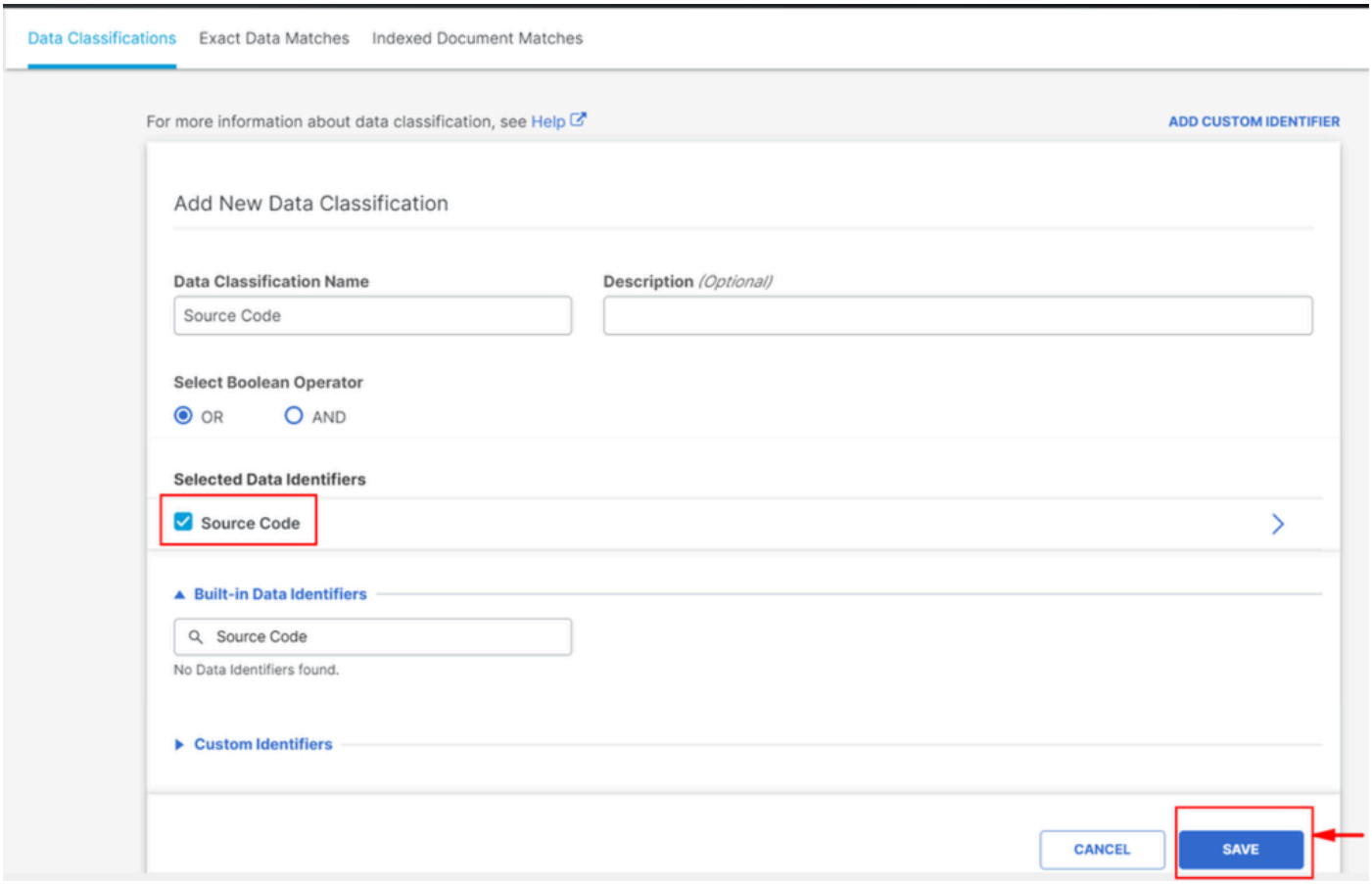
Navigeer naar [het Secure Access Dashboard.]

- Klik op Secure > Data Classification > Add



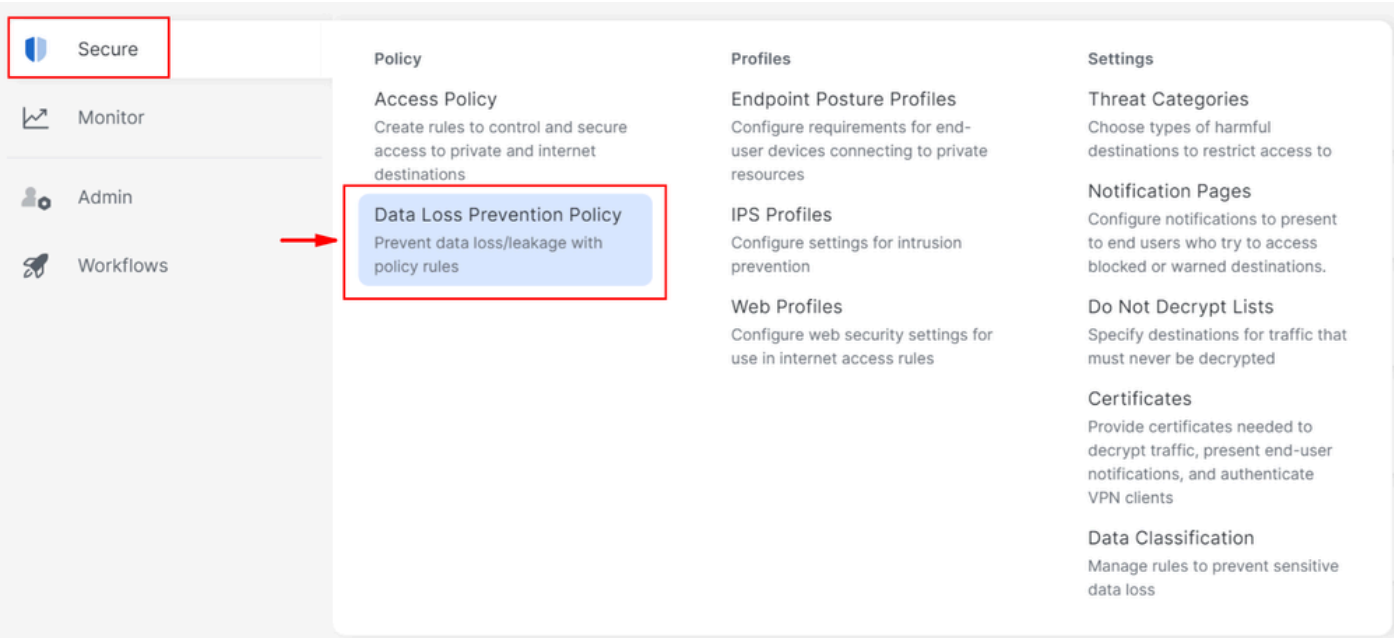
- Voer het veld Data Classification Name > **Selecteren** Built-in Data Identifiers > Zoeken naar Source Code in en selecteer het



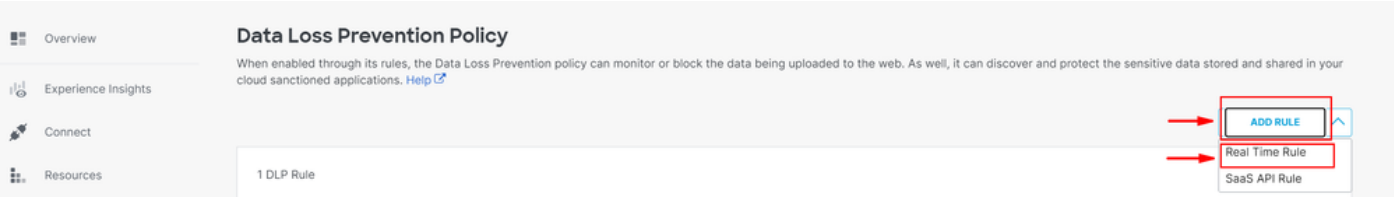


2. Maak een DLP-beleid en noem de gegevensclassificatie "broncode" erin.

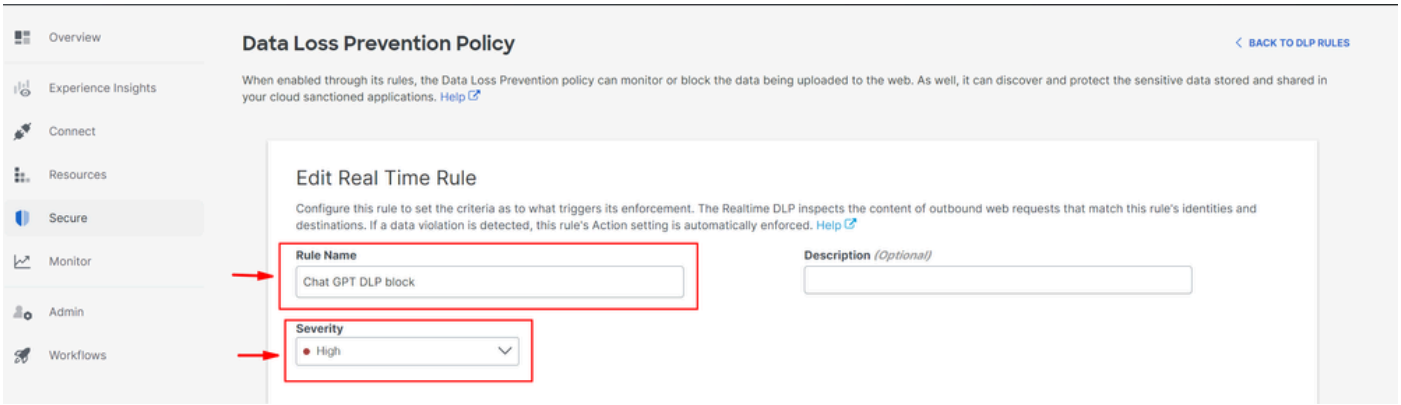
- Klik op Secure > Data Loss Prevention Policy



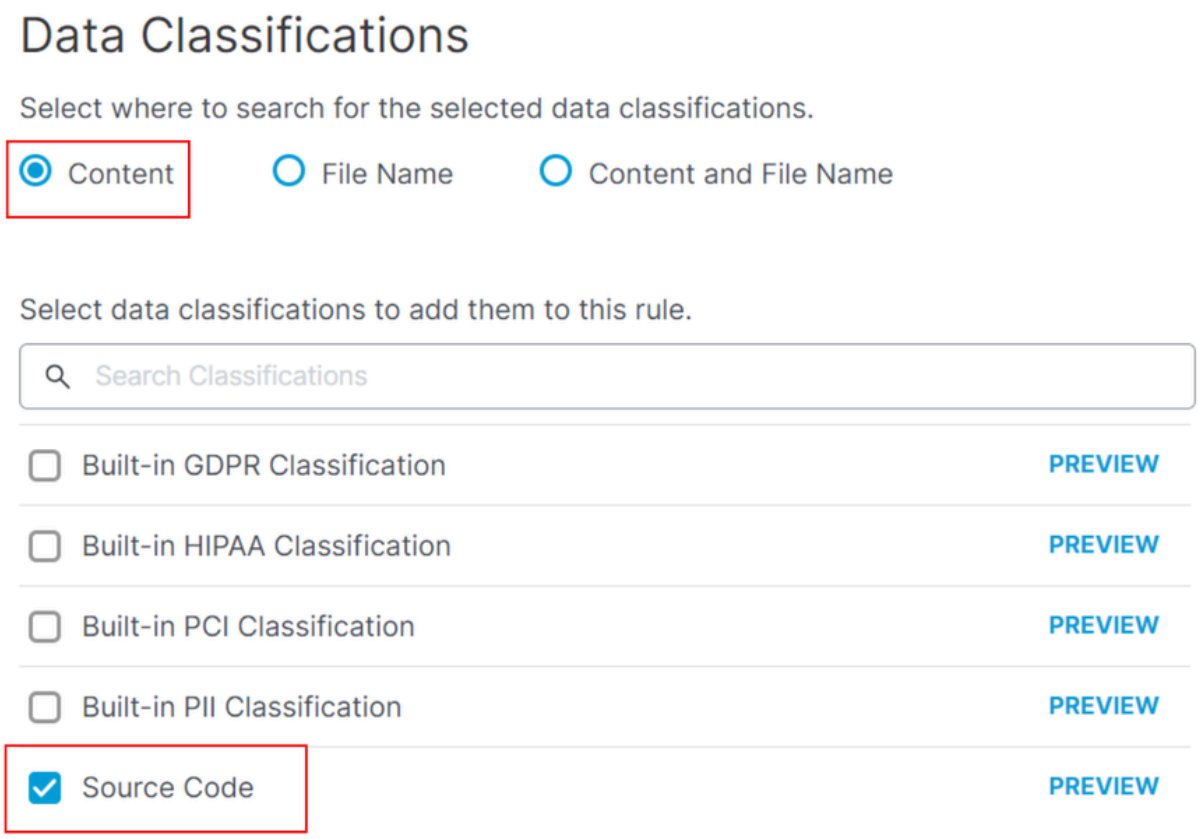
- Klik op Add Rule > Real Time Rule



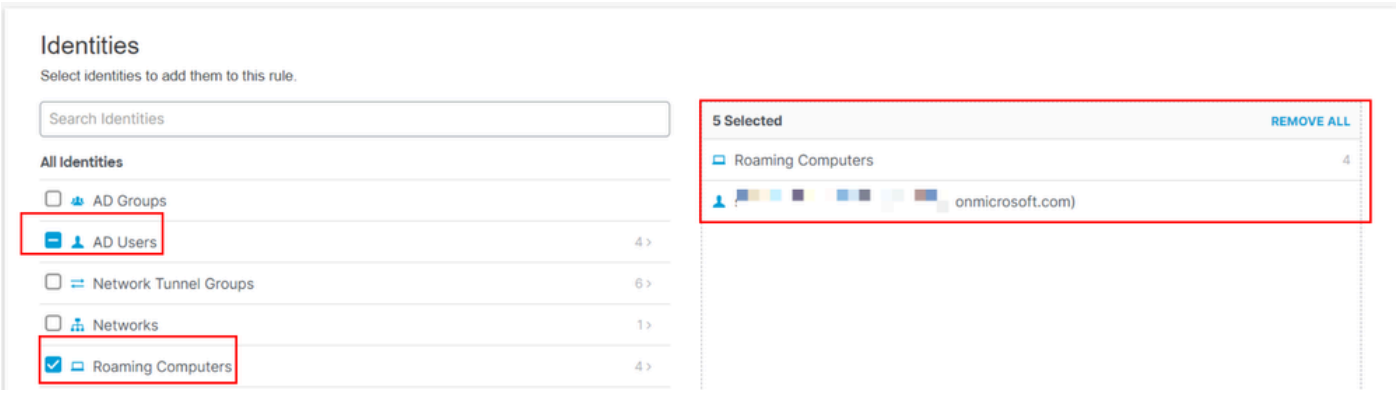
- Geef een Rule Name > Stel de juiste waarde in Severity



- Selecteer onder Data Classifications ContentSelecteer Source Code

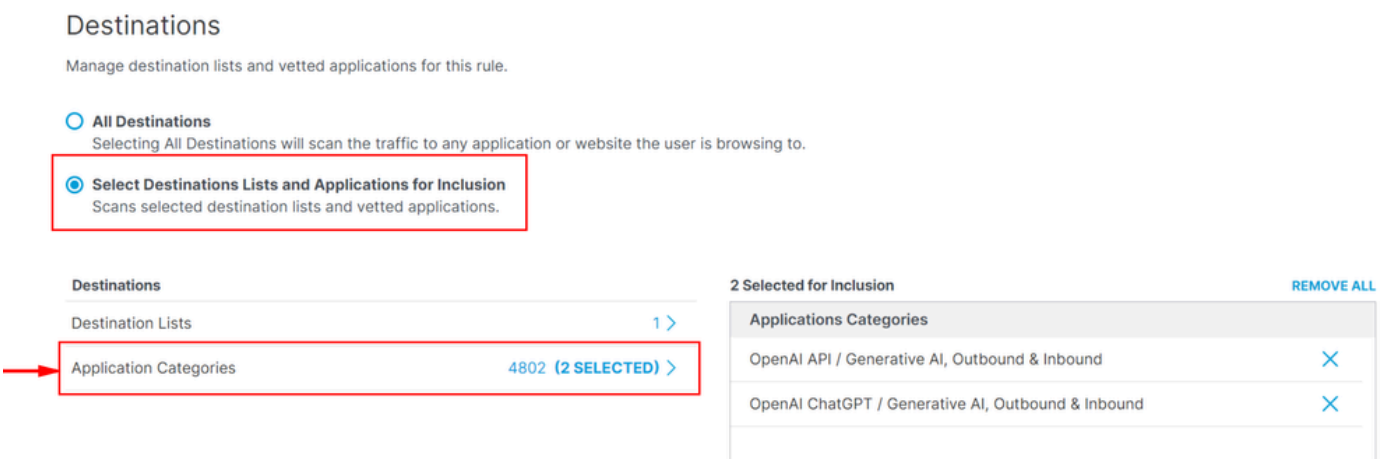


- Selecteer desgewenst de gewenste Identitiesidentiteiten



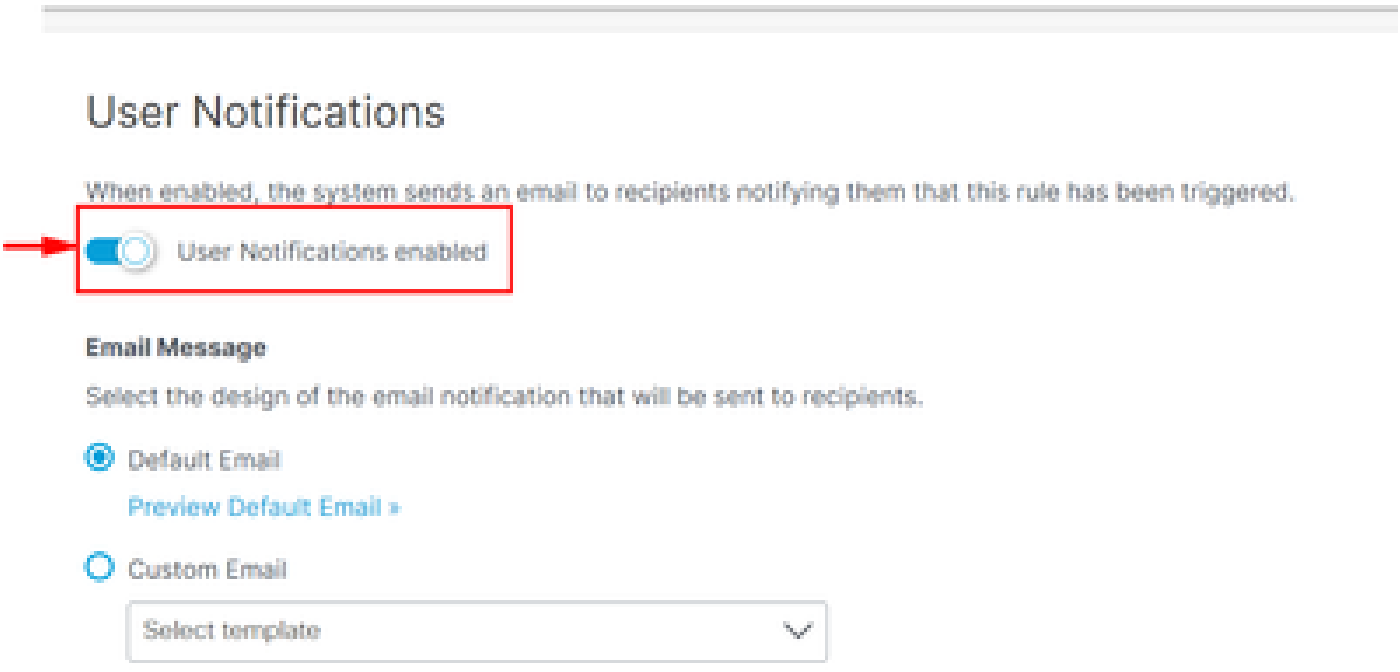
- Selecteer onder Bestemmingen Select Destination Lists and Applications for Inclusion

- Selecteer Application Categories> Selecteren Generative AI > Selecteren OpenAI API (Vetted) en OpenAI ChatGPT (Vetted) in Outbound and InboundDirection

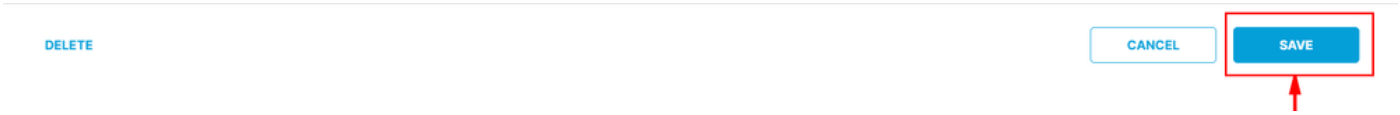


- Onder Actionselecteren Block

- Onder User Notifications, kunt u e-mailberichten aan eind - gebruikers opstellen, wanneer de regel wordt teweeggebracht (facultatief)



- Klik op Save



3. Zorg ervoor dat u een internettoegangsbeleid hebt voor verkeer naar Chat GPT met decryptie ingeschakeld.

Voorbeeld:

Chat GPT

Internet

General

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

Sources

Any

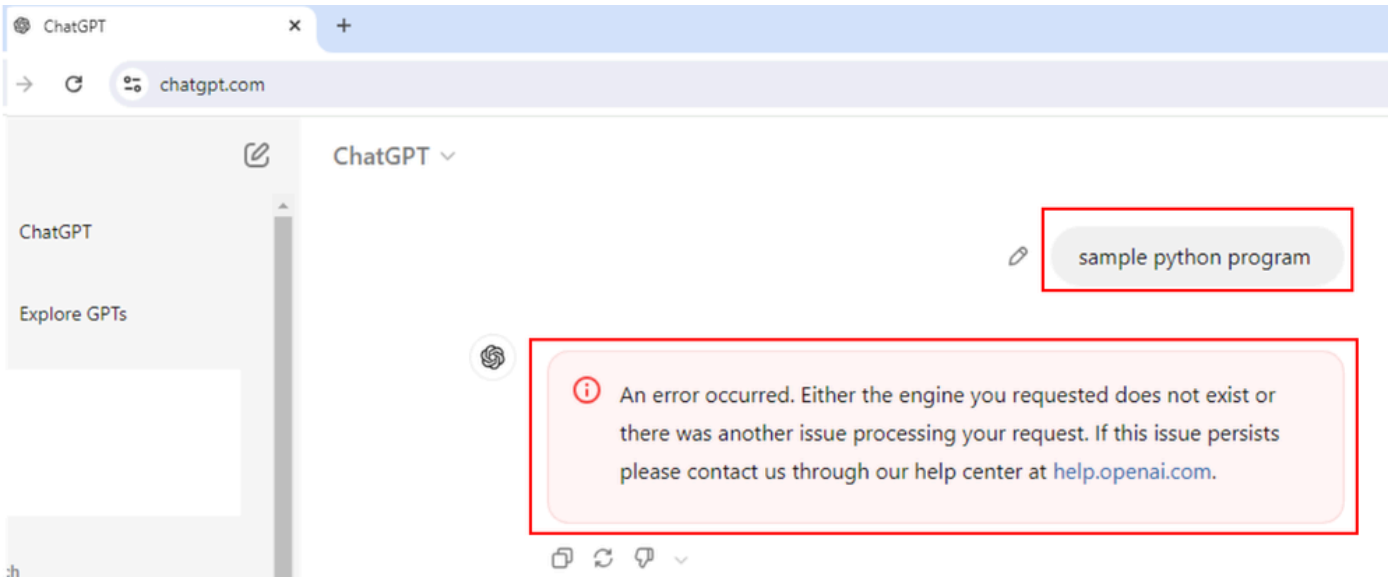
Destinations

2 destinations

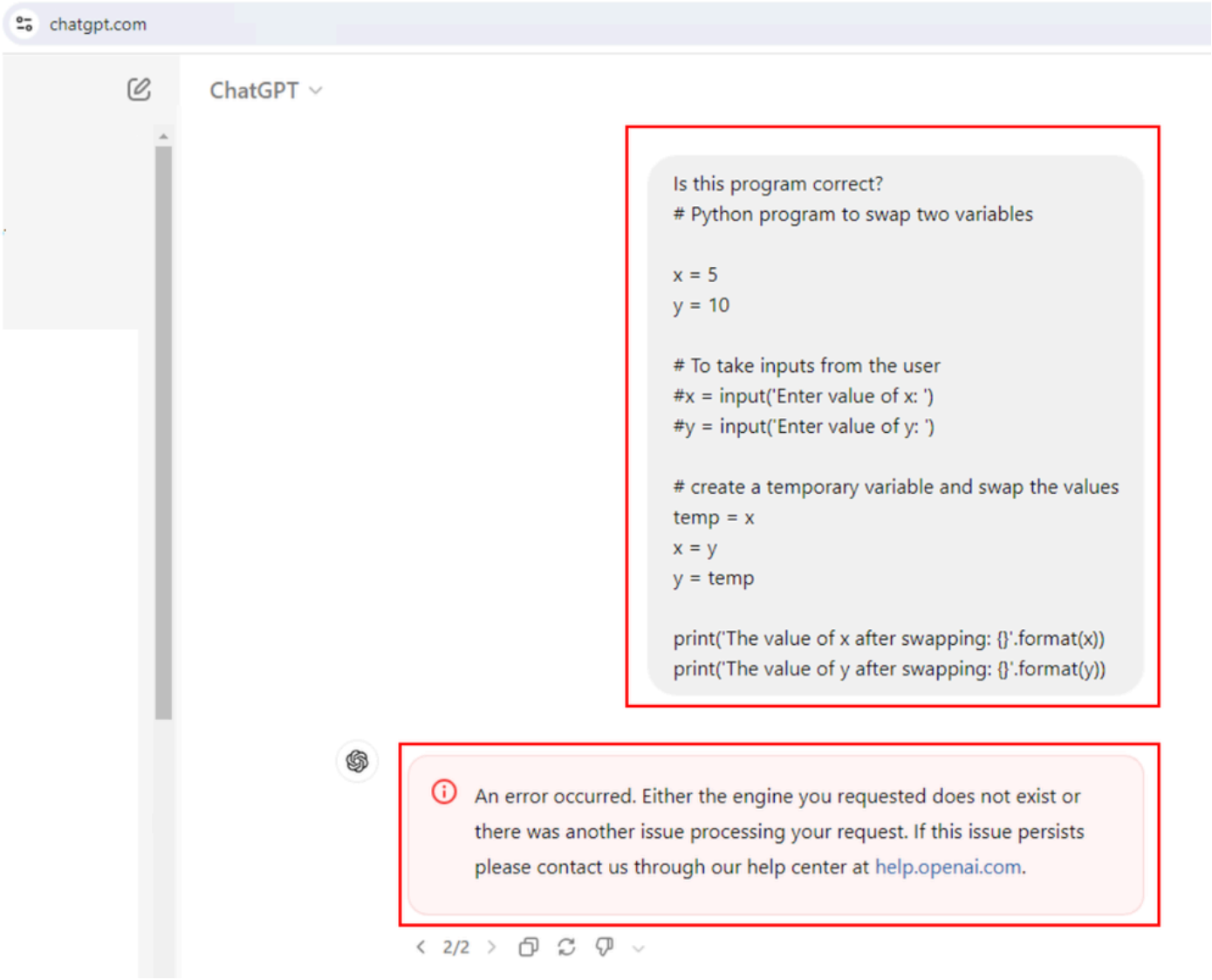
Application Settings (2)

OpenAI API OpenAI ChatGPT

- Vraag om een voorbeeldpython programma en dit verzoek wordt geblokkeerd.



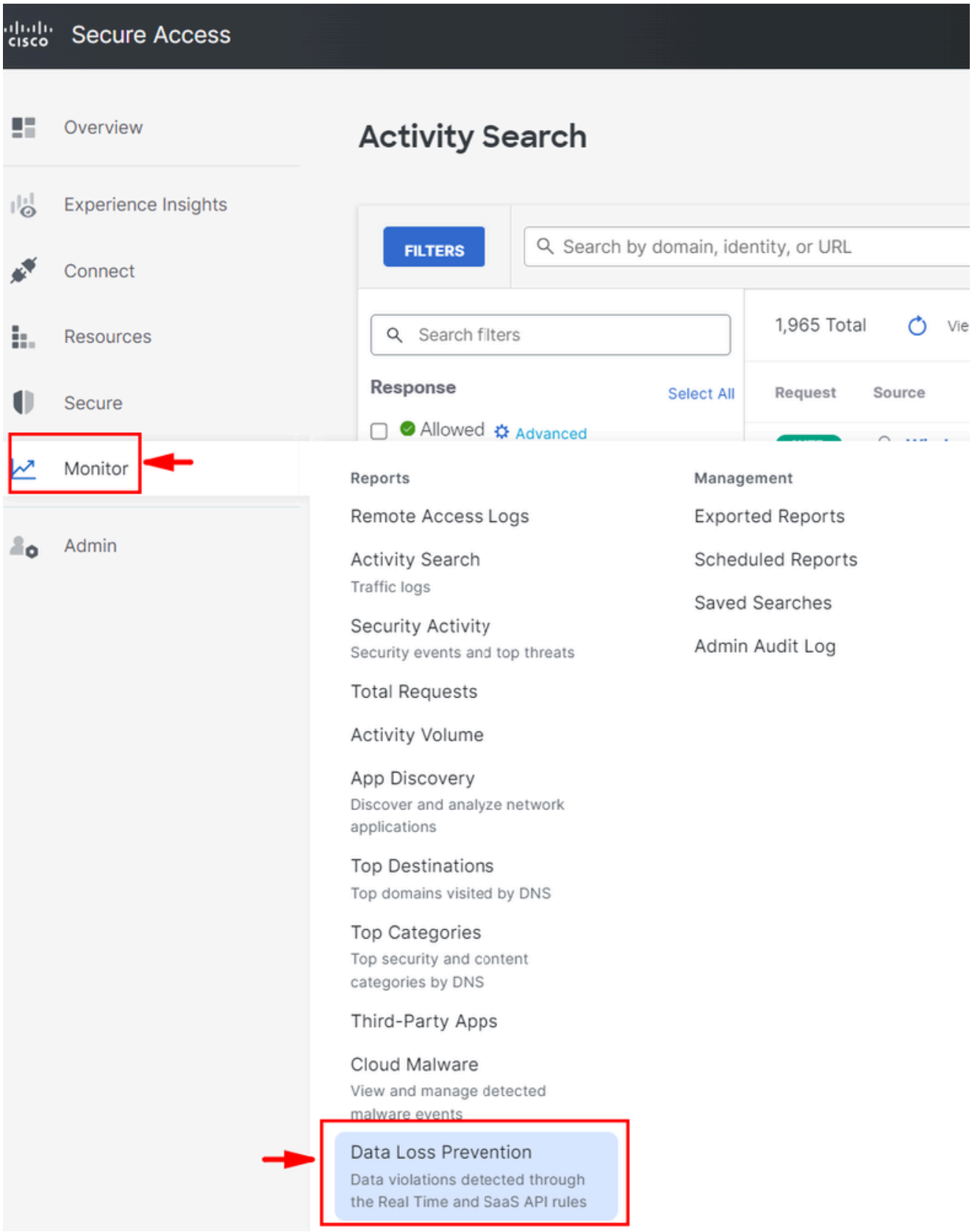
- Vraag of het programma juist is of niet en deze aanvraag wordt geblokkeerd.



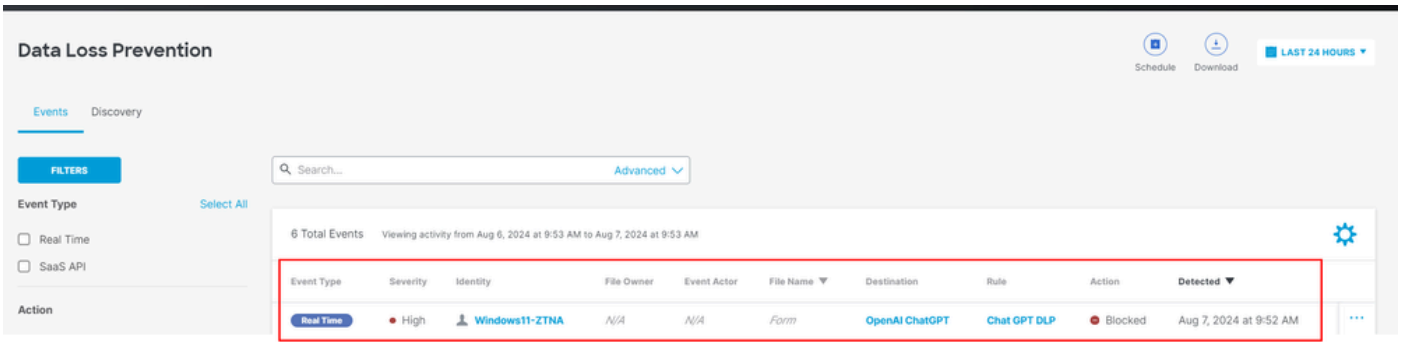
Verifiëren

We kunnen zien wanneer de gebruiker probeert om ChatGPT te vragen voor een voorbeeldpython-programma, het verzoek wordt geblokkeerd. We kunnen bevestigen dat een DLP-gebeurtenis is geactiveerd in Secure Access Data Loss Prevention-logboeken.

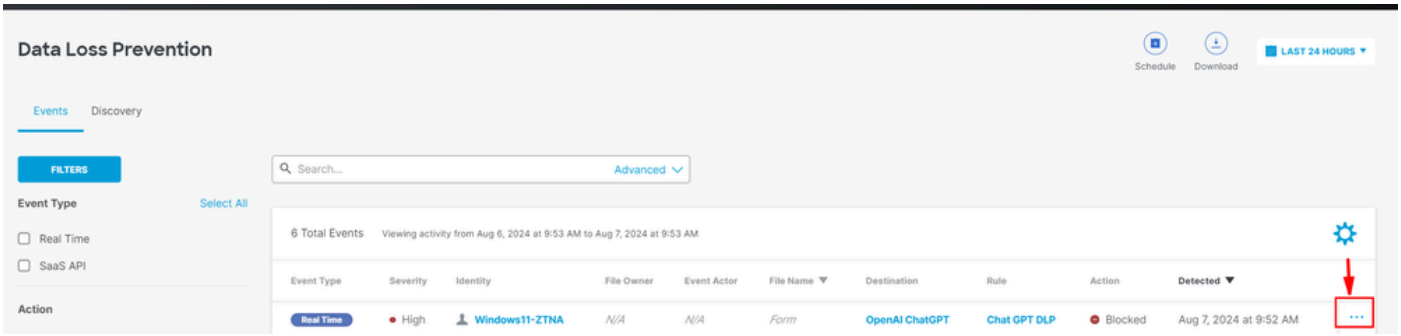
- Ga naar Monitor> Data Loss Prevention



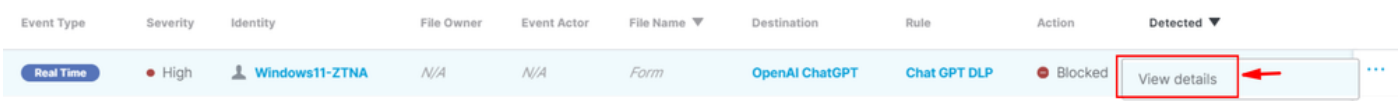
- We kunnen het DLP-evenement zien.



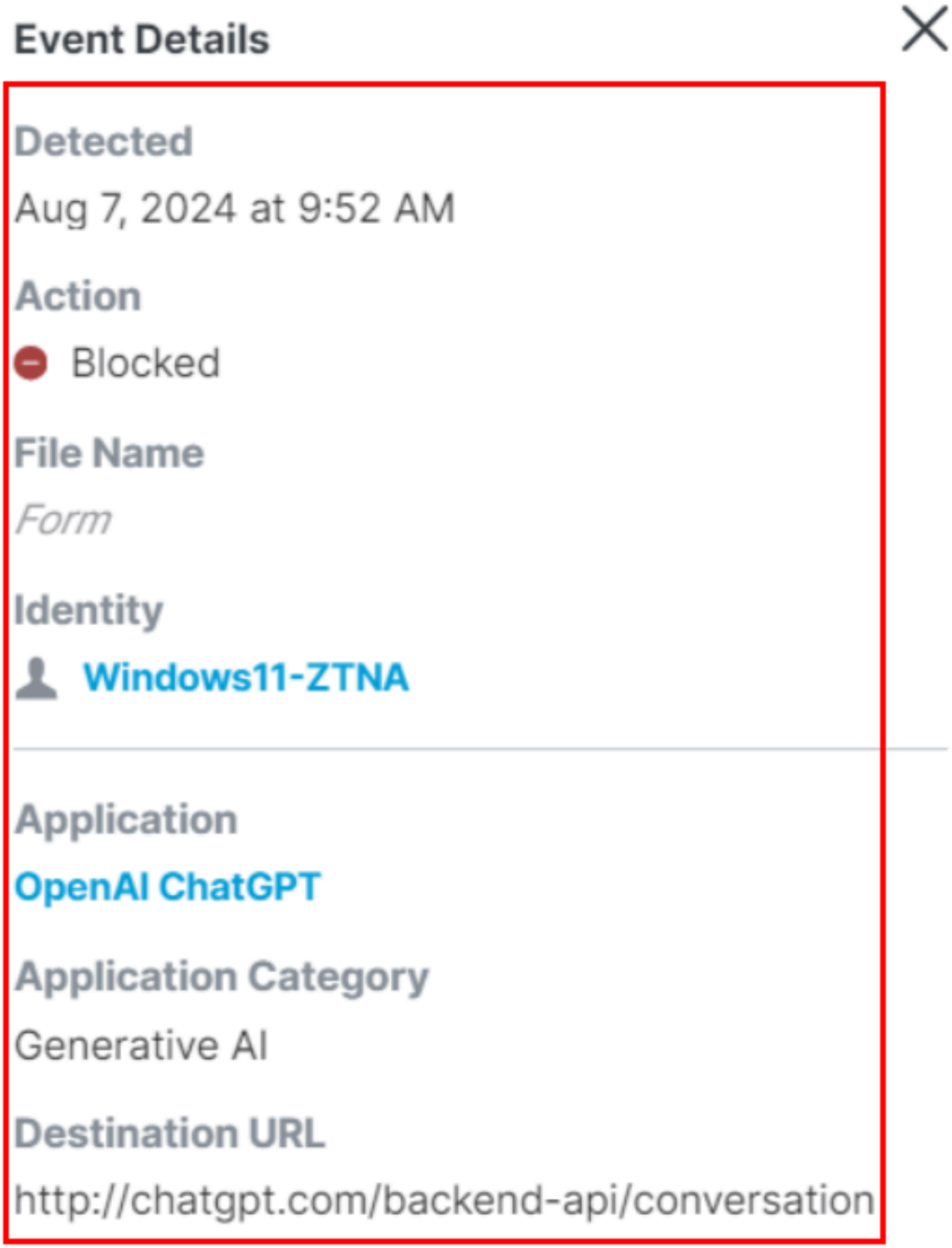
- Klik op de drie punten aan het einde van het gebeurtenissenlogboek om meer details over de gebeurtenis te controleren.



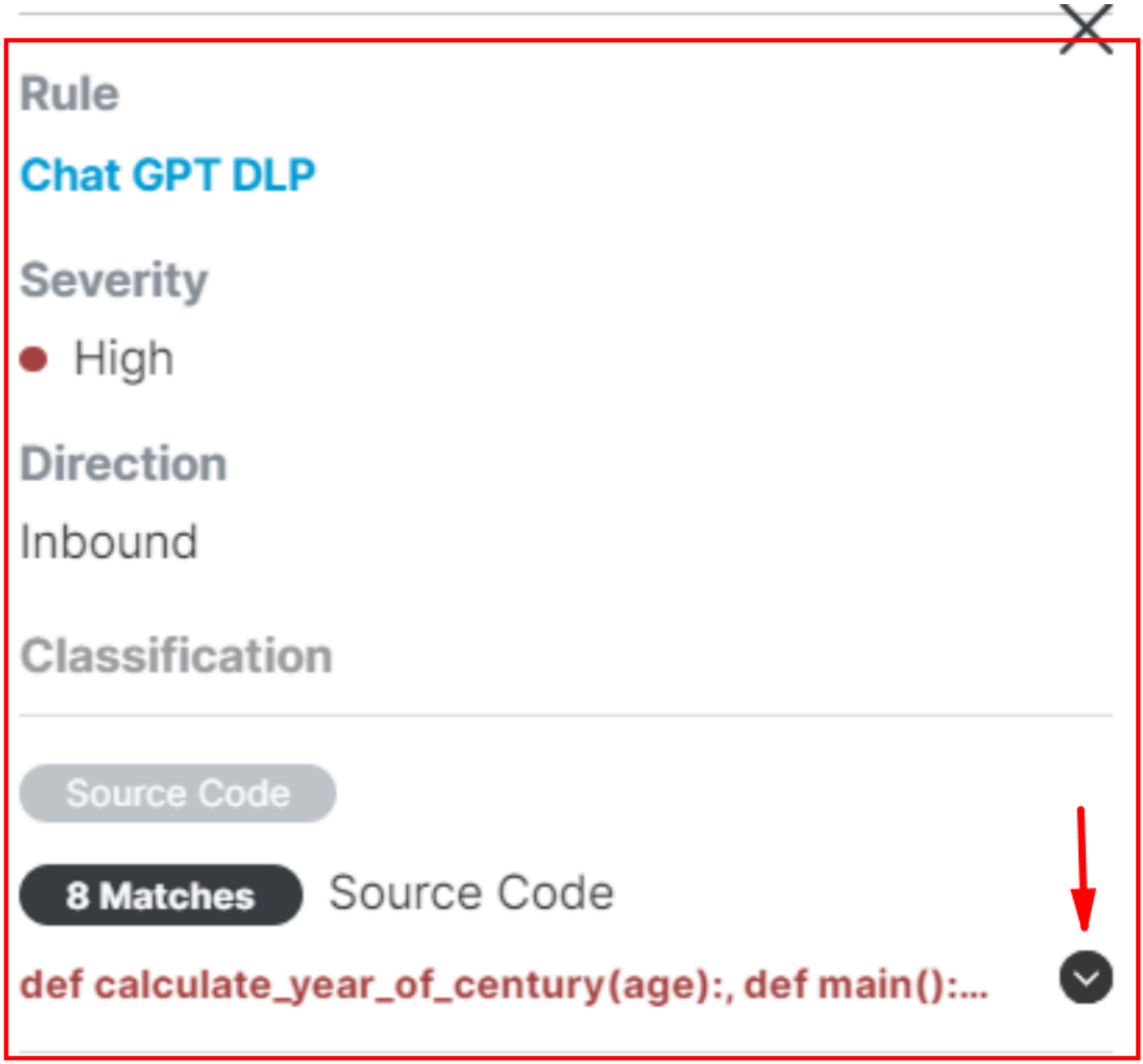
- Klik op View details.



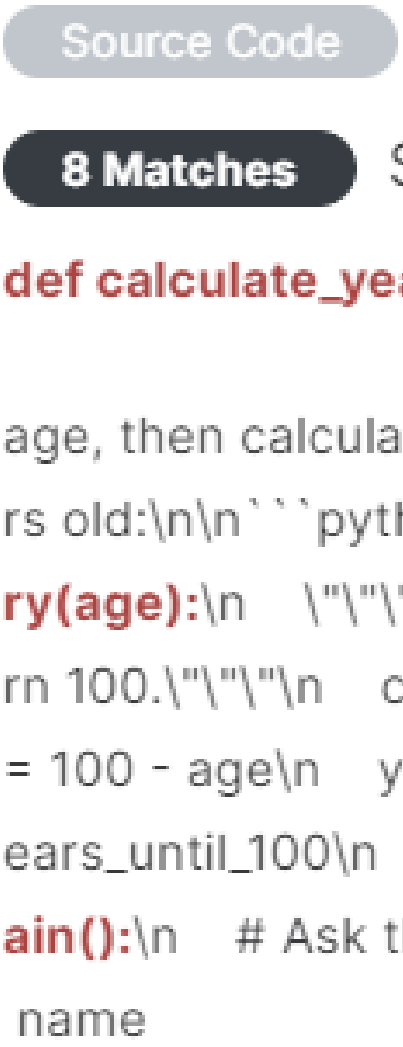
- Nu zien we de volledige eventdetails.



- Breid de classificatie uit om te zien welke inhoud overeenkomt met de classificator.

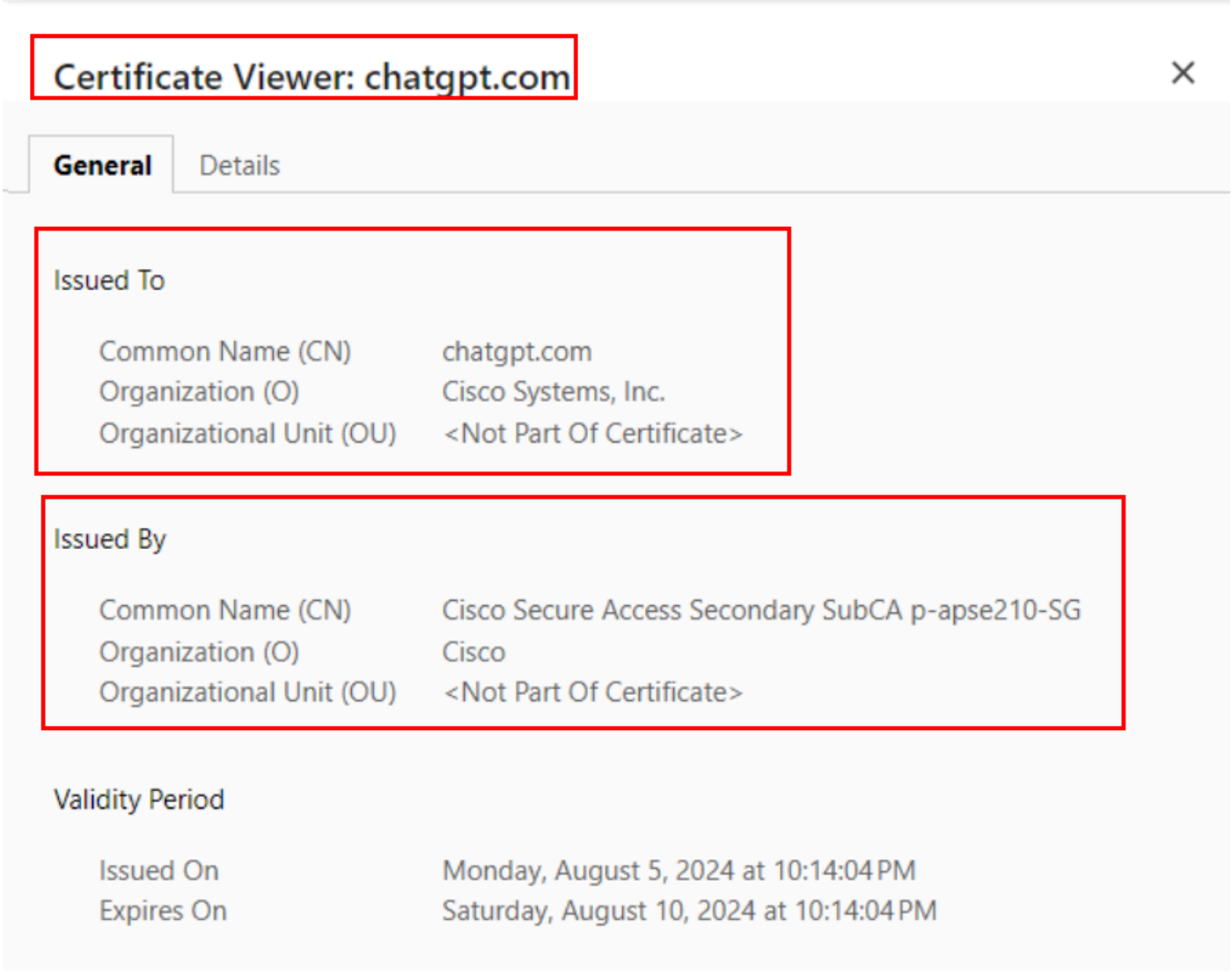


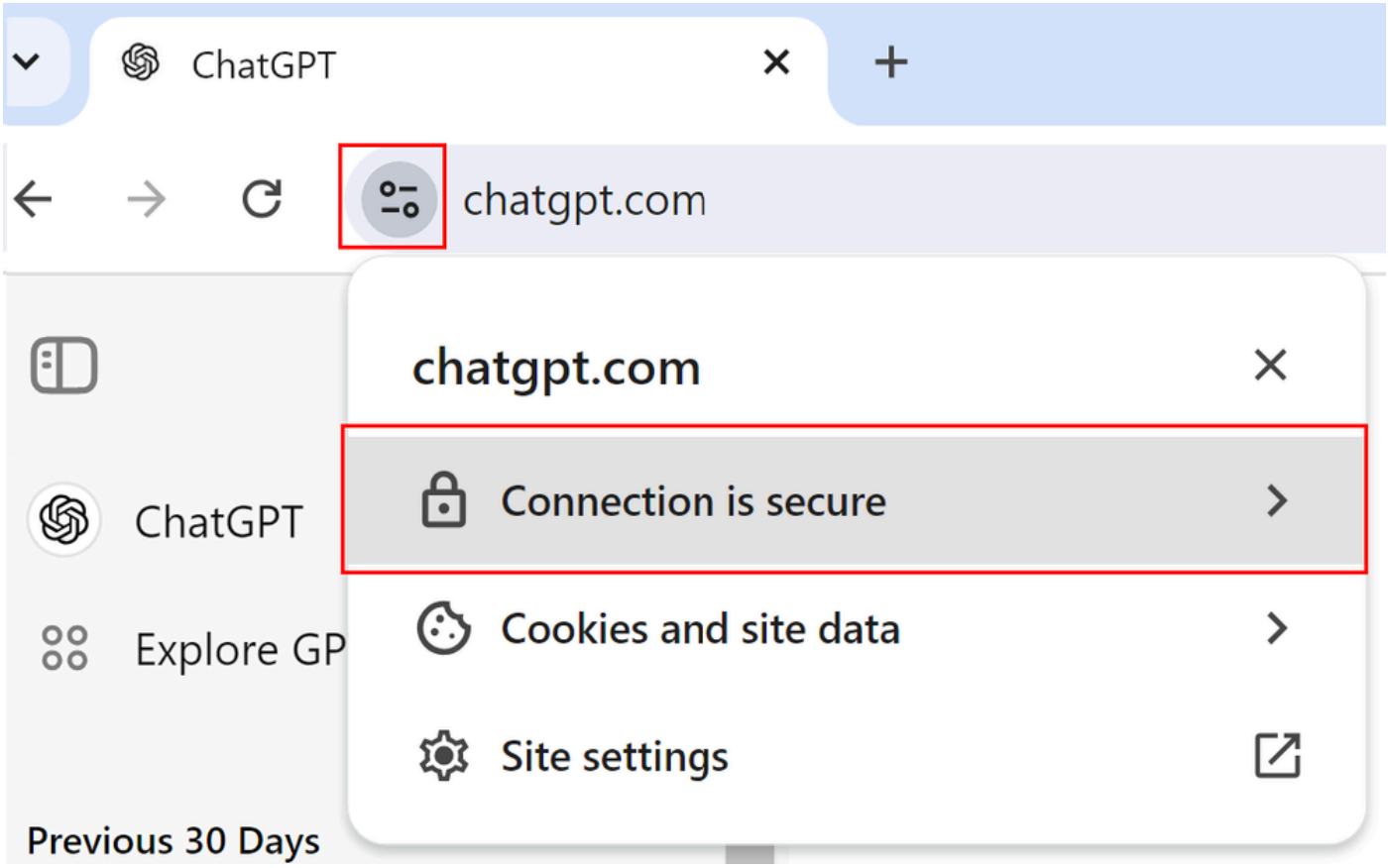
- We zien alle details van de inhoud die overeenkwam met de classificator / classificatie van het DLP-beleid.

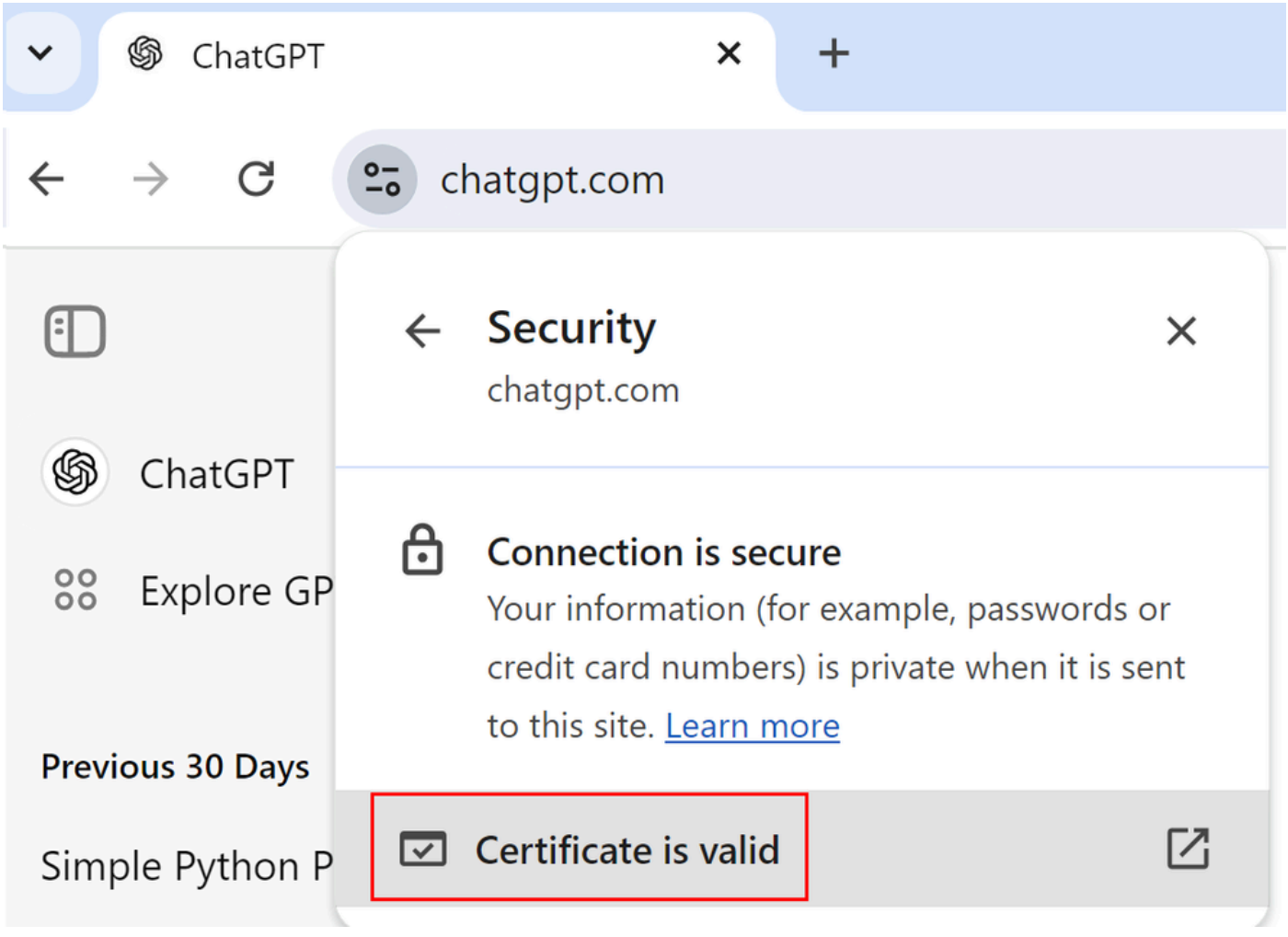


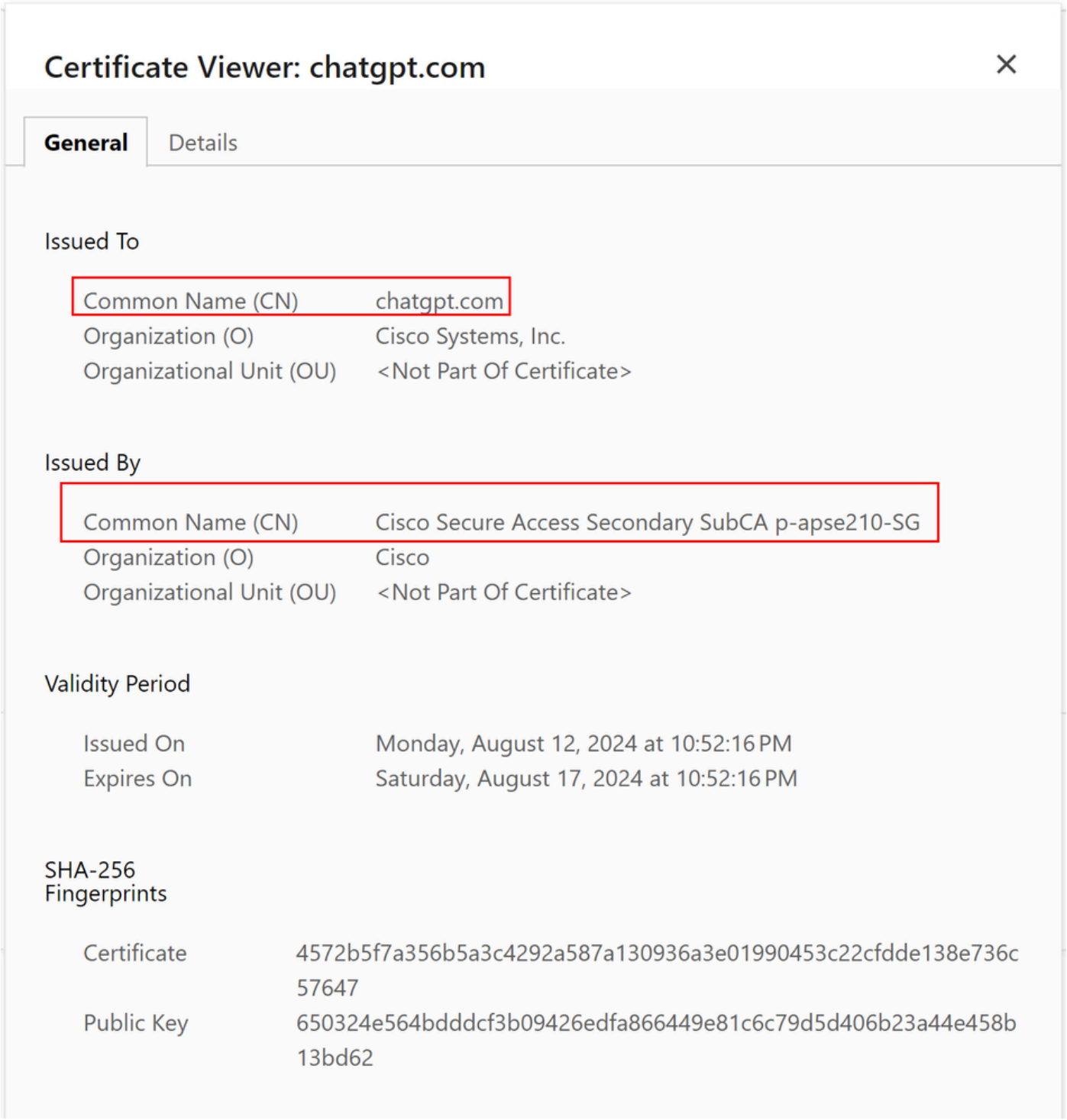
Problemen oplossen

- Zorg ervoor dat het toegangsbeleid dat overeenkomt met webaanvragen voor Open AI ChatGPT heeft decryptie ingeschakeld.
- Als u snel wilt controleren of SSE verkeer decodeert voor Open AI ChatGPT, controleert u het certificaat van de website waarop de veelvoorkomende naam "Cisco Secure Access" bevat.


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

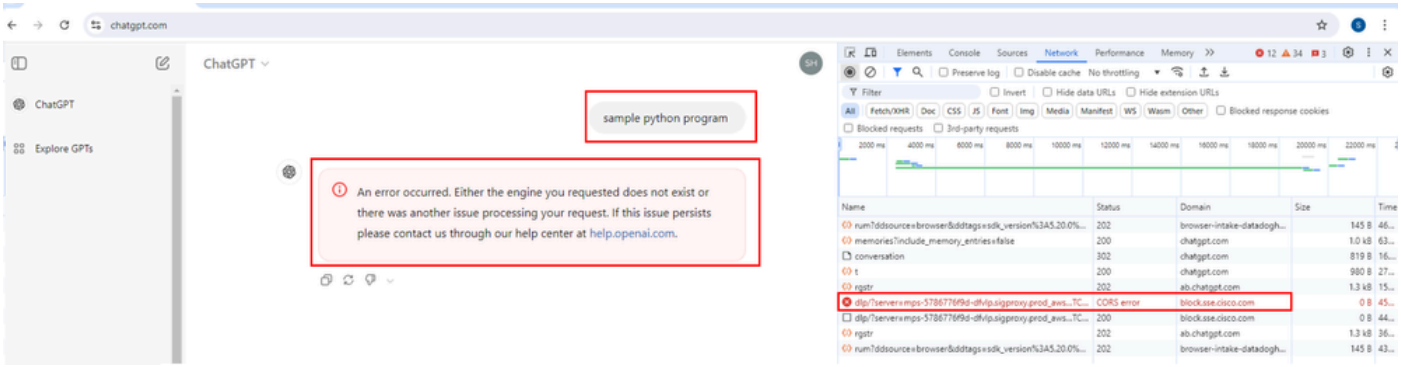

ChatGPT
chatgpt.com
chatgpt.com
Connection is secure
Cookies and site data
Site settings
ChatGPT
Explore GP
Previous 30 Days


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

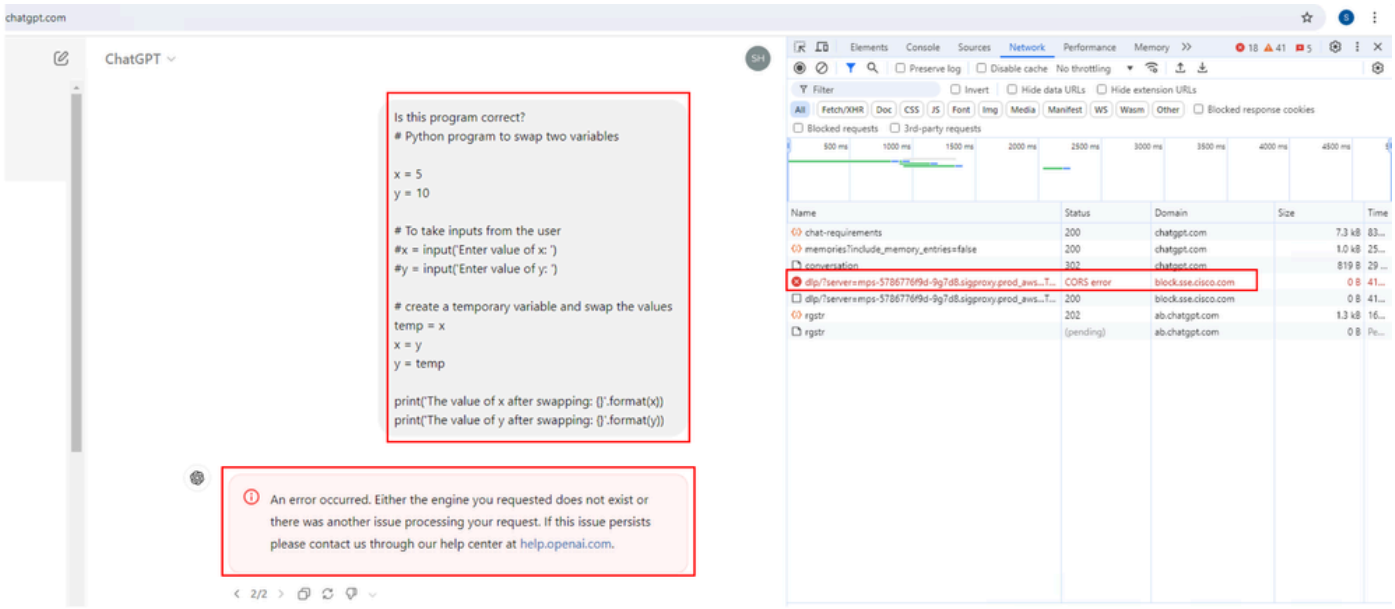


- Open ChatGPT > Open developer tools > Selecteer Netwerk > Volgende poging om ChatGPT te vragen voor een voorbeeldpython programma

- Merk op dat het verzoek resulteert in een blokkering. Onder het domein zie je "block.sse.cisco.com



- Vraag ChatGPT of de programmacode correct is.
- Merk op dat het verzoek resulteert in een blok en onder "domein" zie je "block.sse.cisco.com".



Gerelateerde informatie

- Gebruikershandleiding voor Cisco Secure Access
- Cisco technische ondersteuning en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.