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

## Table des matières



## 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

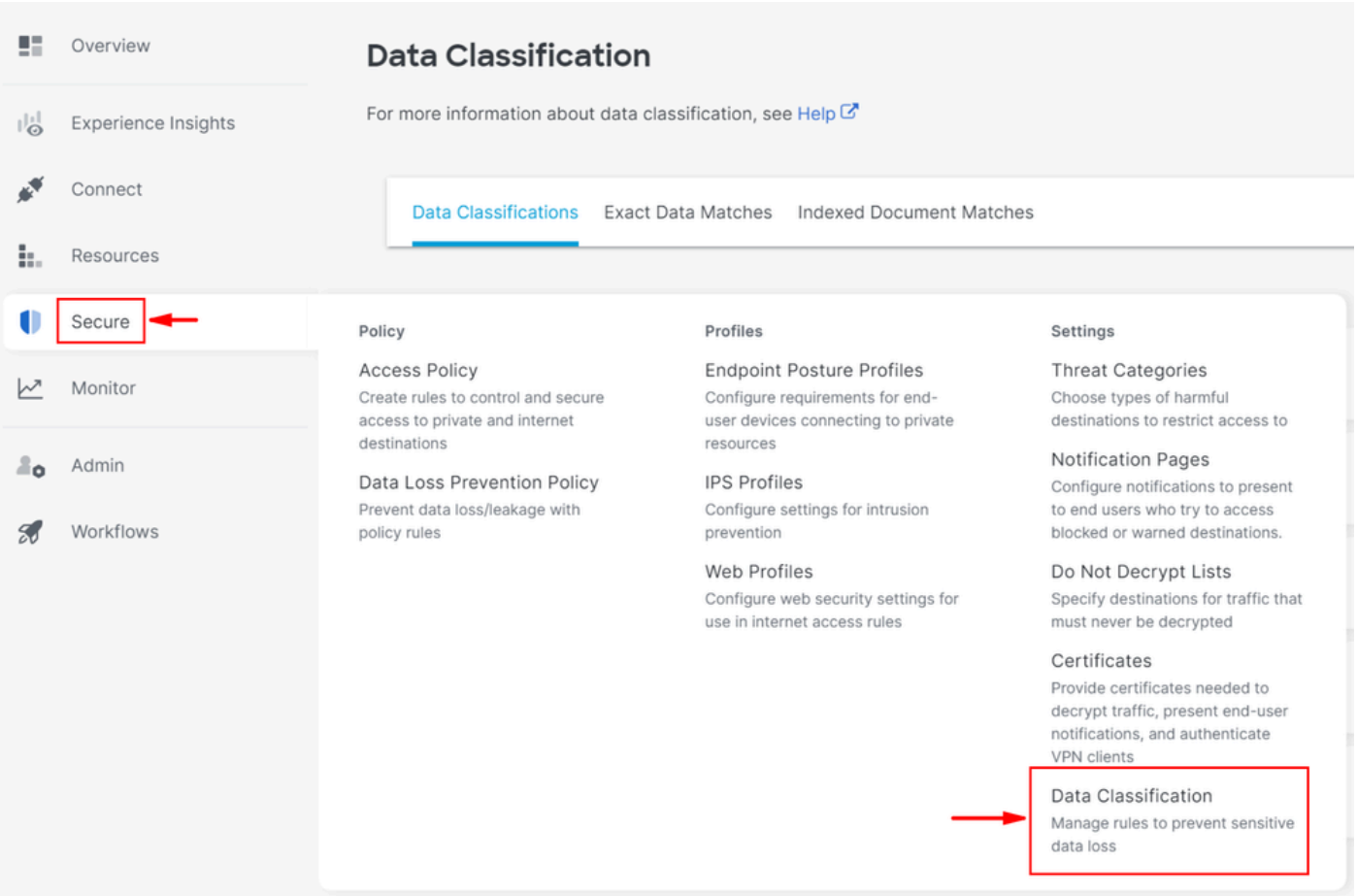
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

# Configurer

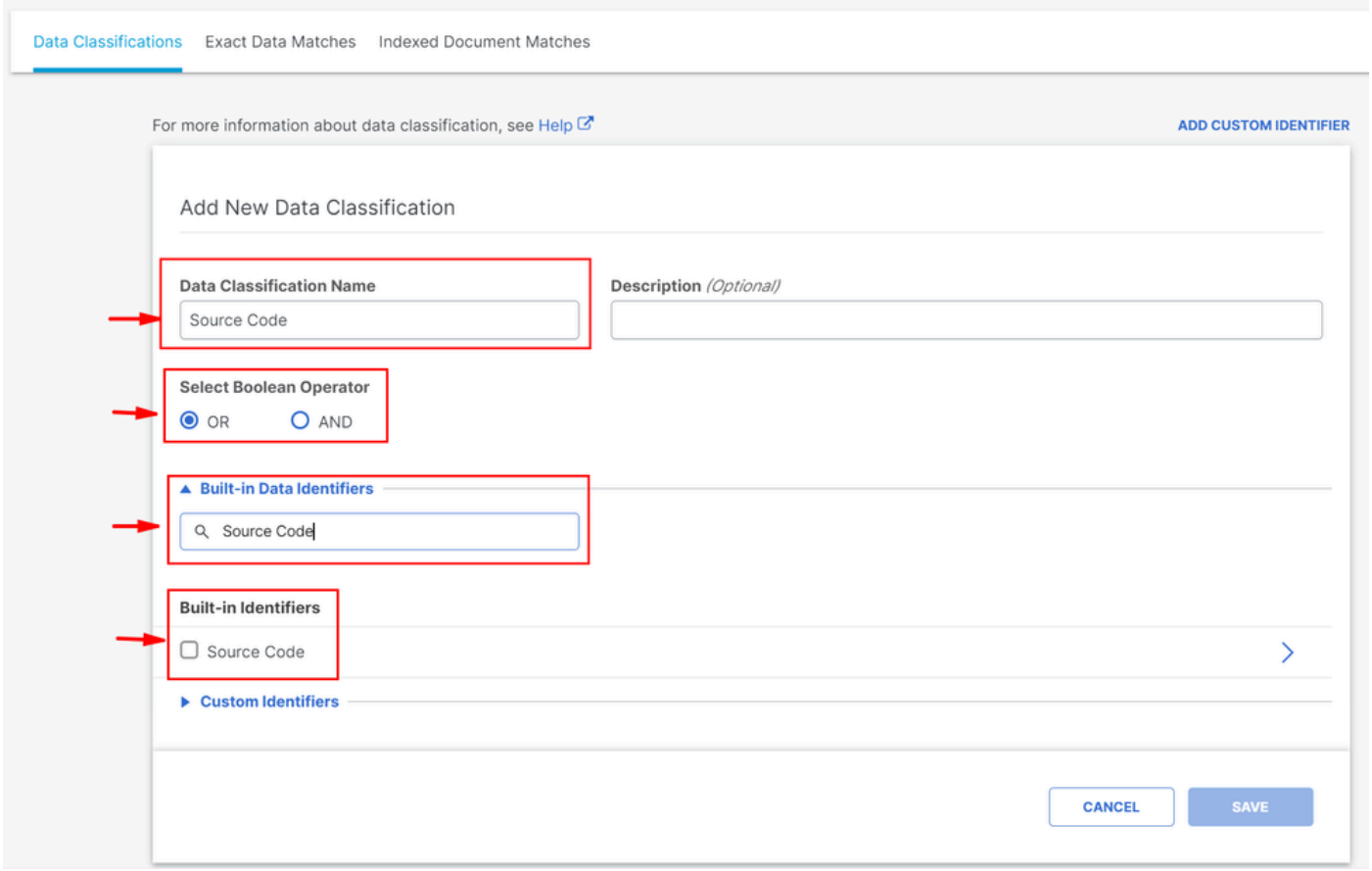
## 1.Créer une classification de données pour utiliser l'identificateur de données de code source

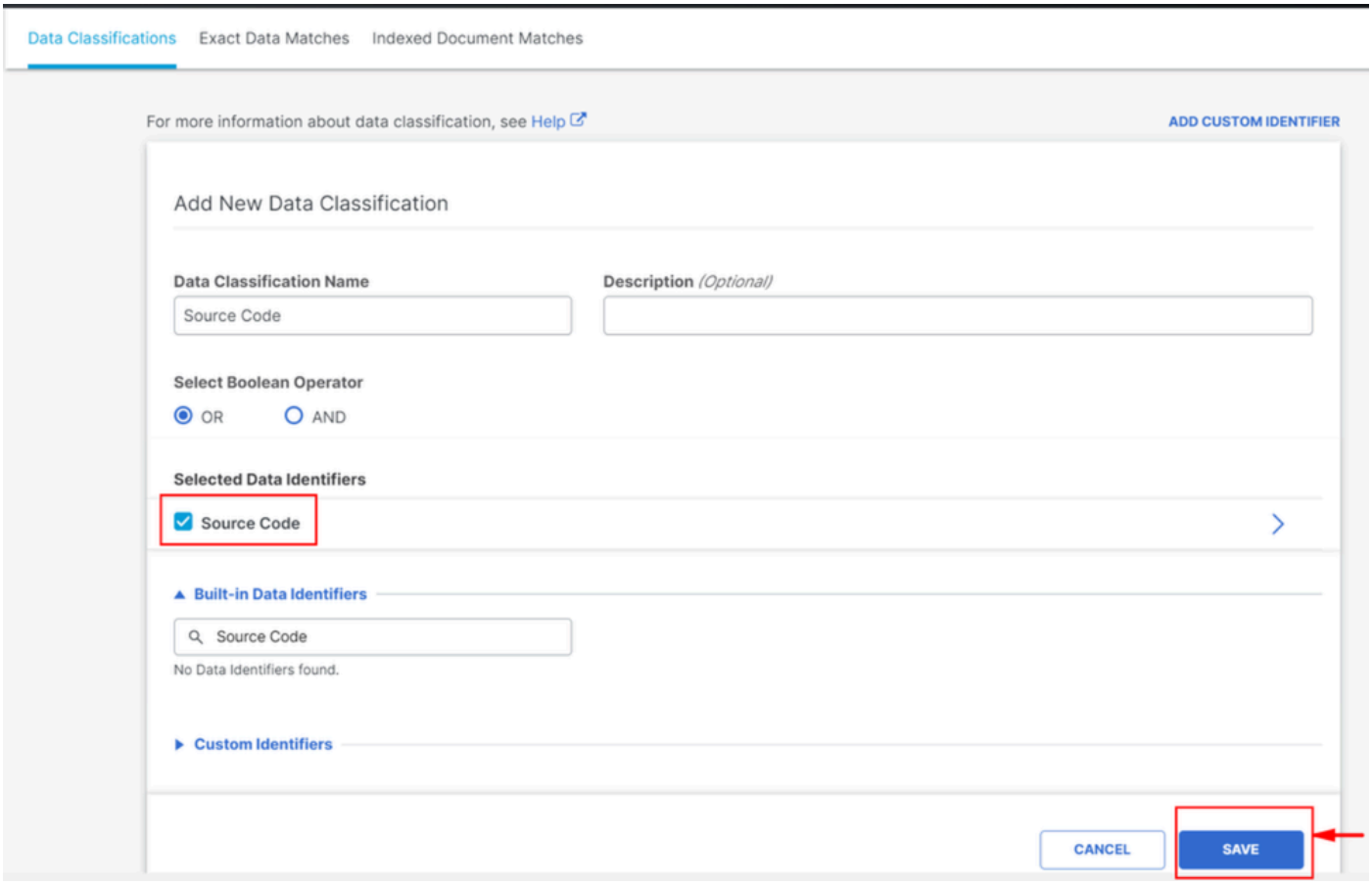
Accédez à Secure Access Dashboard.

- Cliquez sur Secure > Data Classification > Add



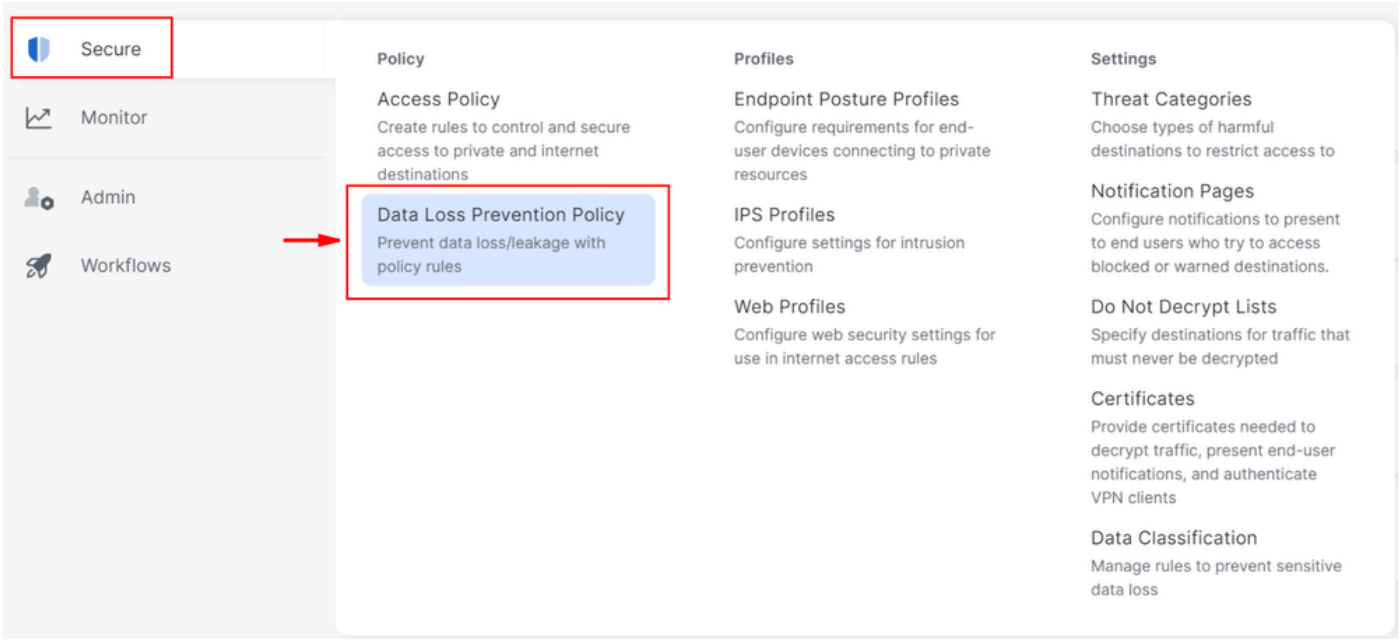

- Entrez la commande Data Classification Name > **Select** Built-in Data Identifiers > Search for Source Code et sélectionnez-la



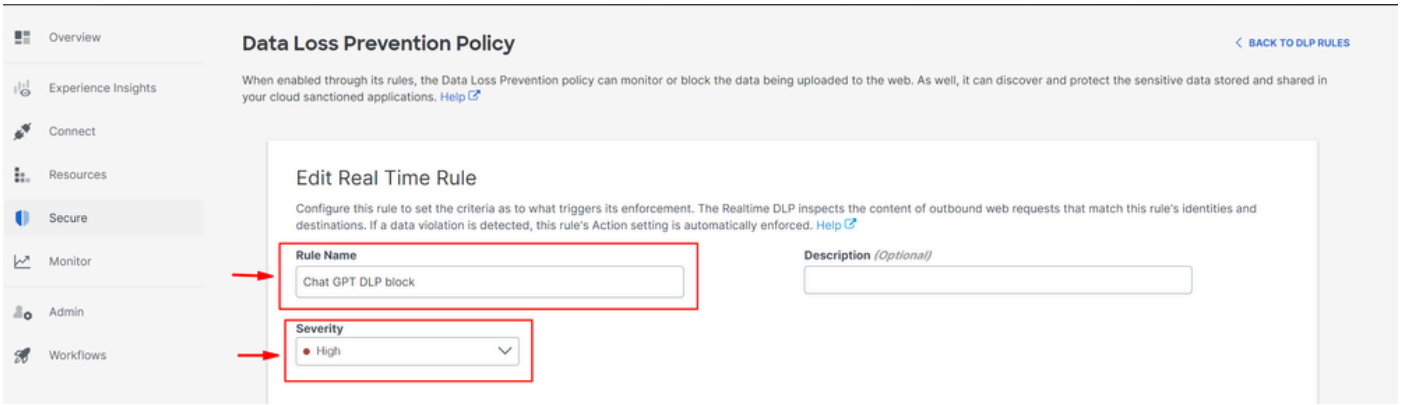

2. Créez une stratégie DLP et appelez-y la classification des données « Code source ».

- Cliquez sur Secure > Data Loss Prevention Policy

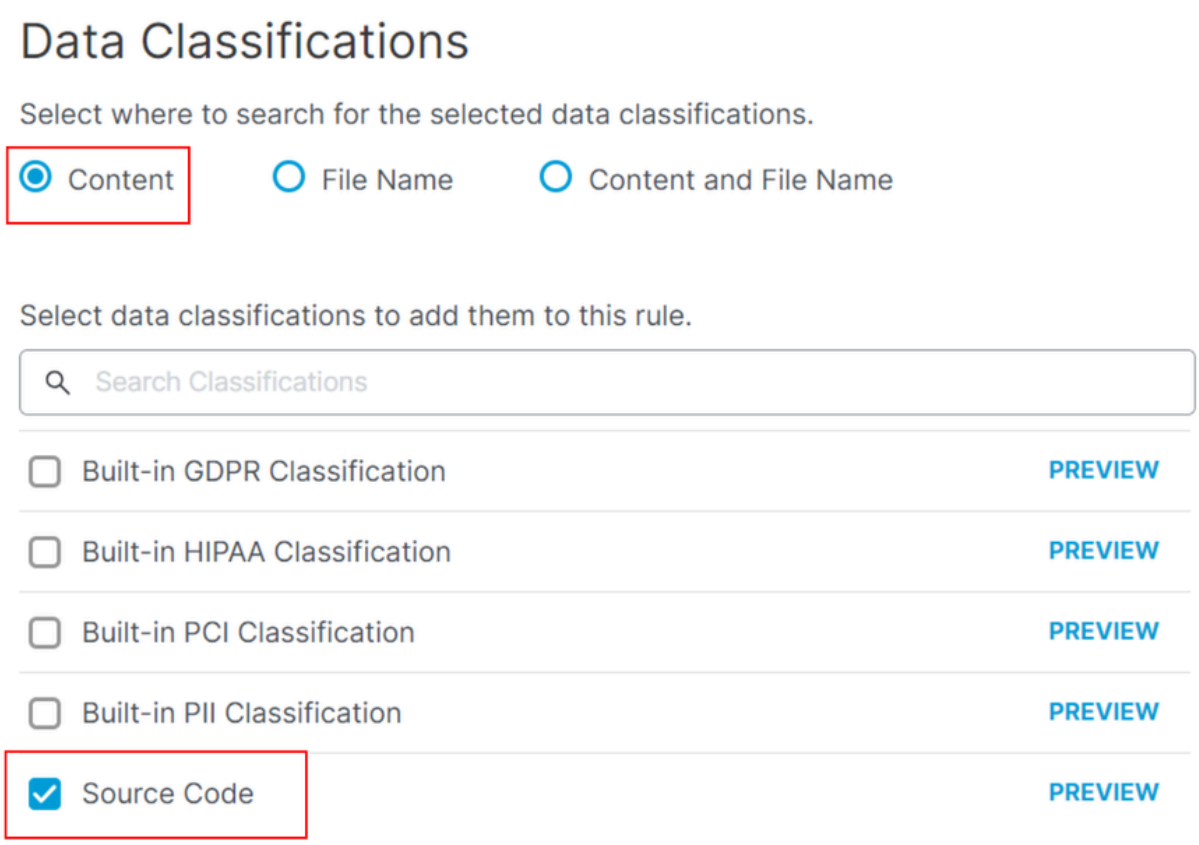



- Cliquez sur Add Rule > Real Time Rule

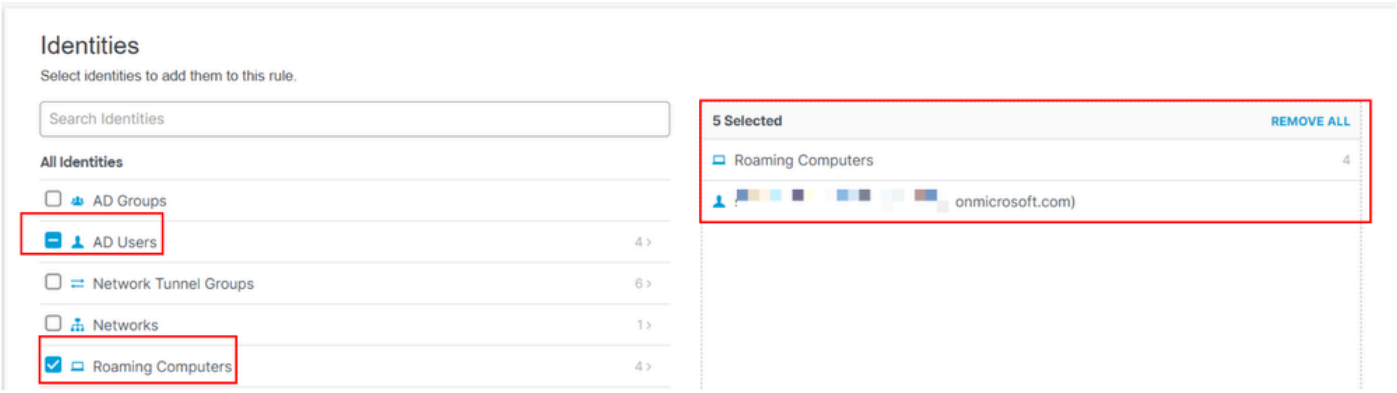

- Indiquez un Rule Name > Définir approprié Severity




- Sous Data Classifications sélectionner Content et sélectionner Source Code

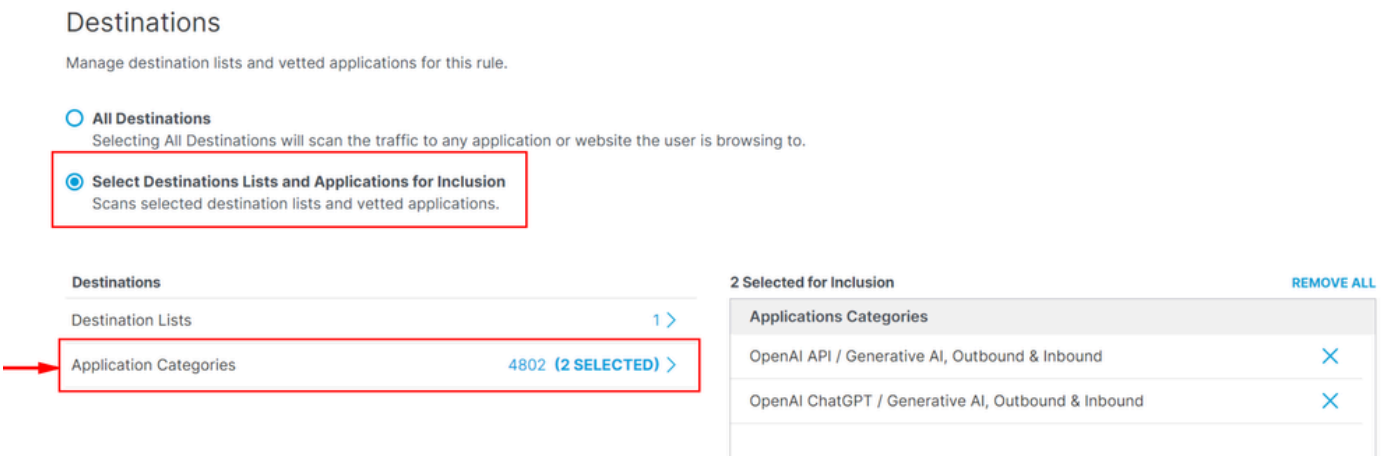



- Sous Identitiessélectionnez les identités souhaitées, le cas échéant



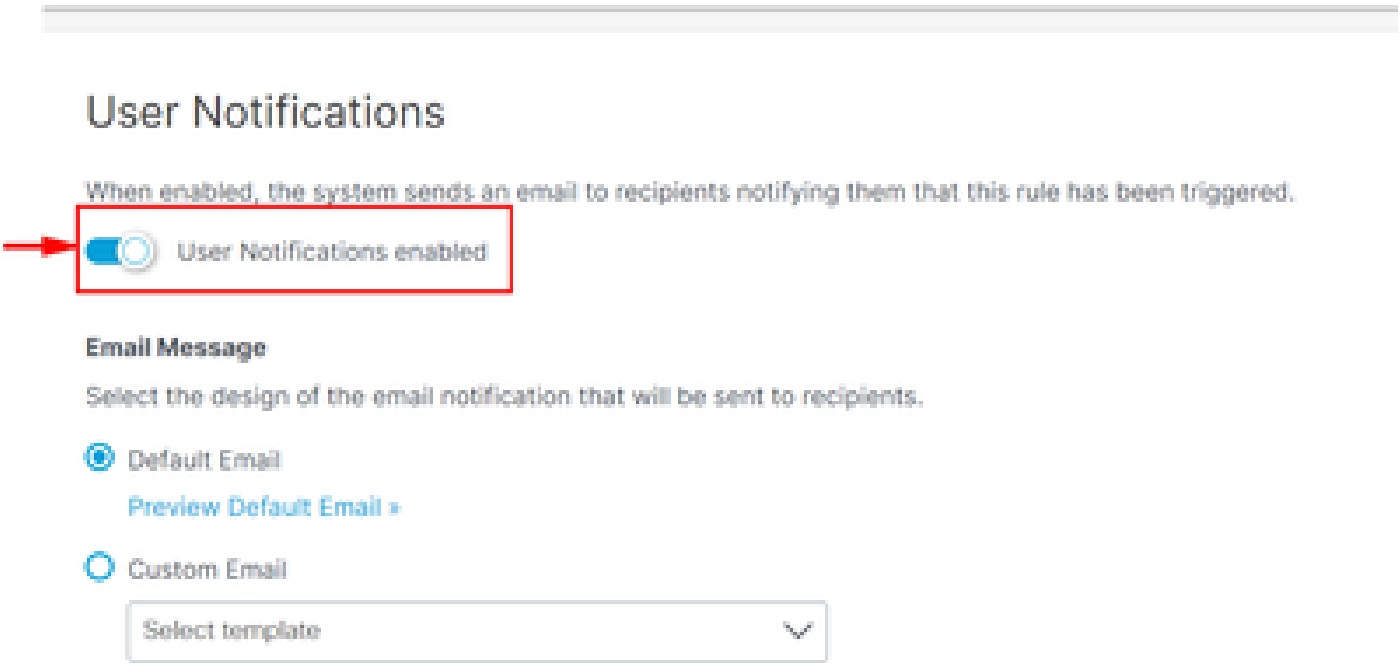

- Sous Destinations, sélectionnez Select Destination Lists and Applications for Inclusion

- Sélectionnez Application Categories> Sélectionner Generative AI> Sélectionner OpenAI API (Vetted) et OpenAI ChatGPT (Vetted) dans Outbound and InboundDirection

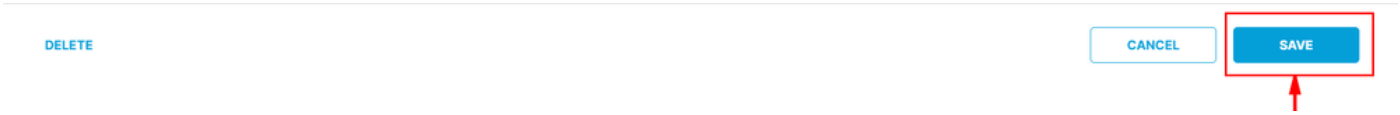



- Sous Actionsélectionner Block

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

- Cliquez sur 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 | [redacted] |
| Rule order | 1 |
| Logging | Enabled |
| Hits | 216 |

## Sources

Any

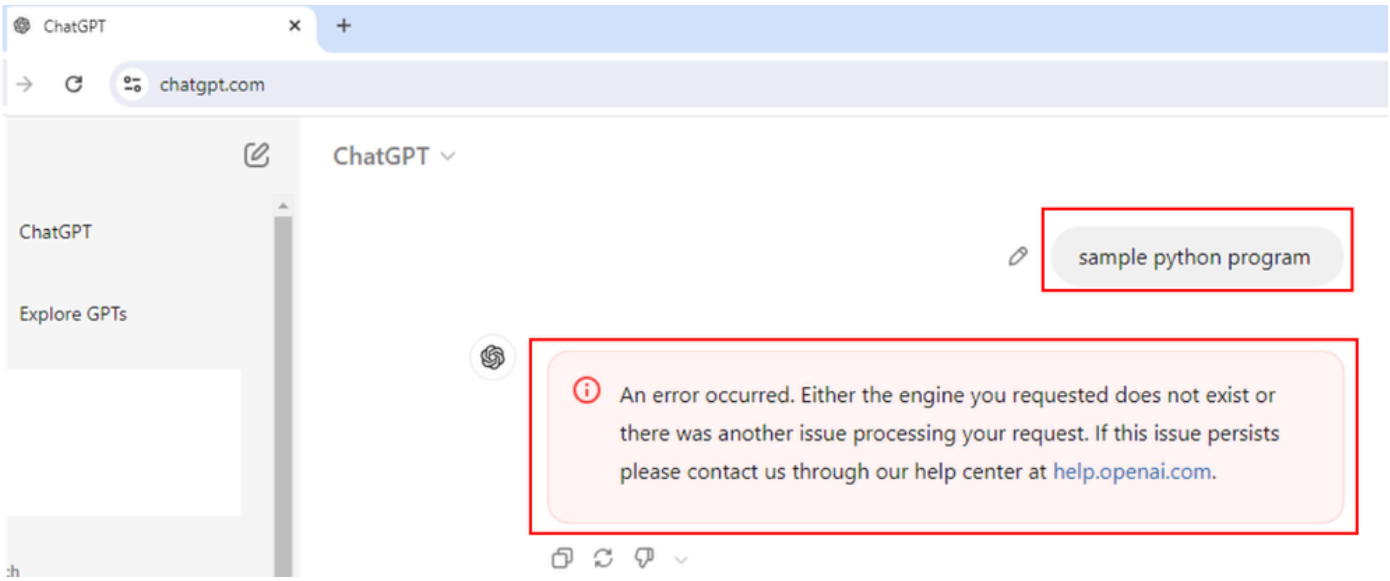
## Destinations

2 destinations

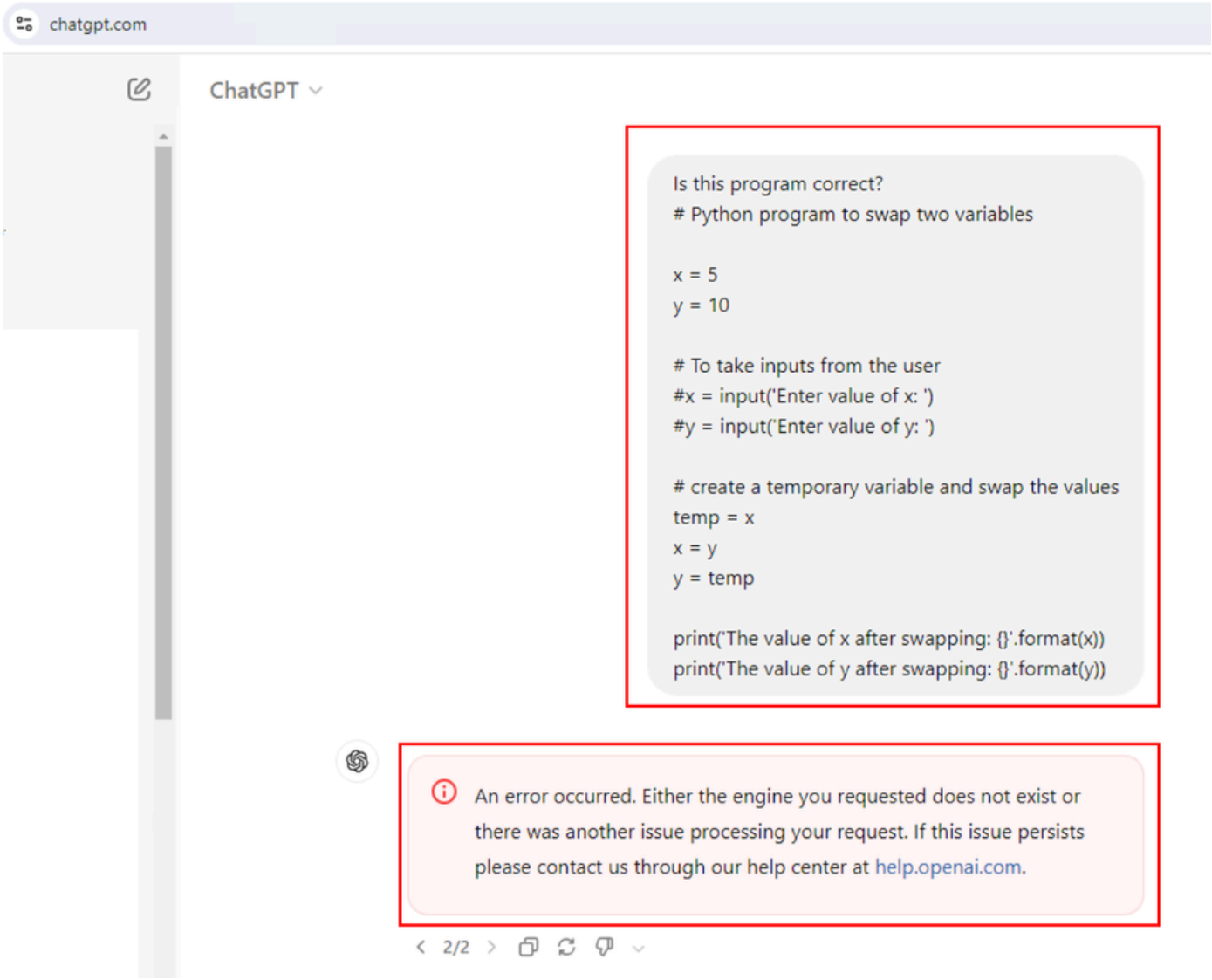
### Application Settings (2)

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.

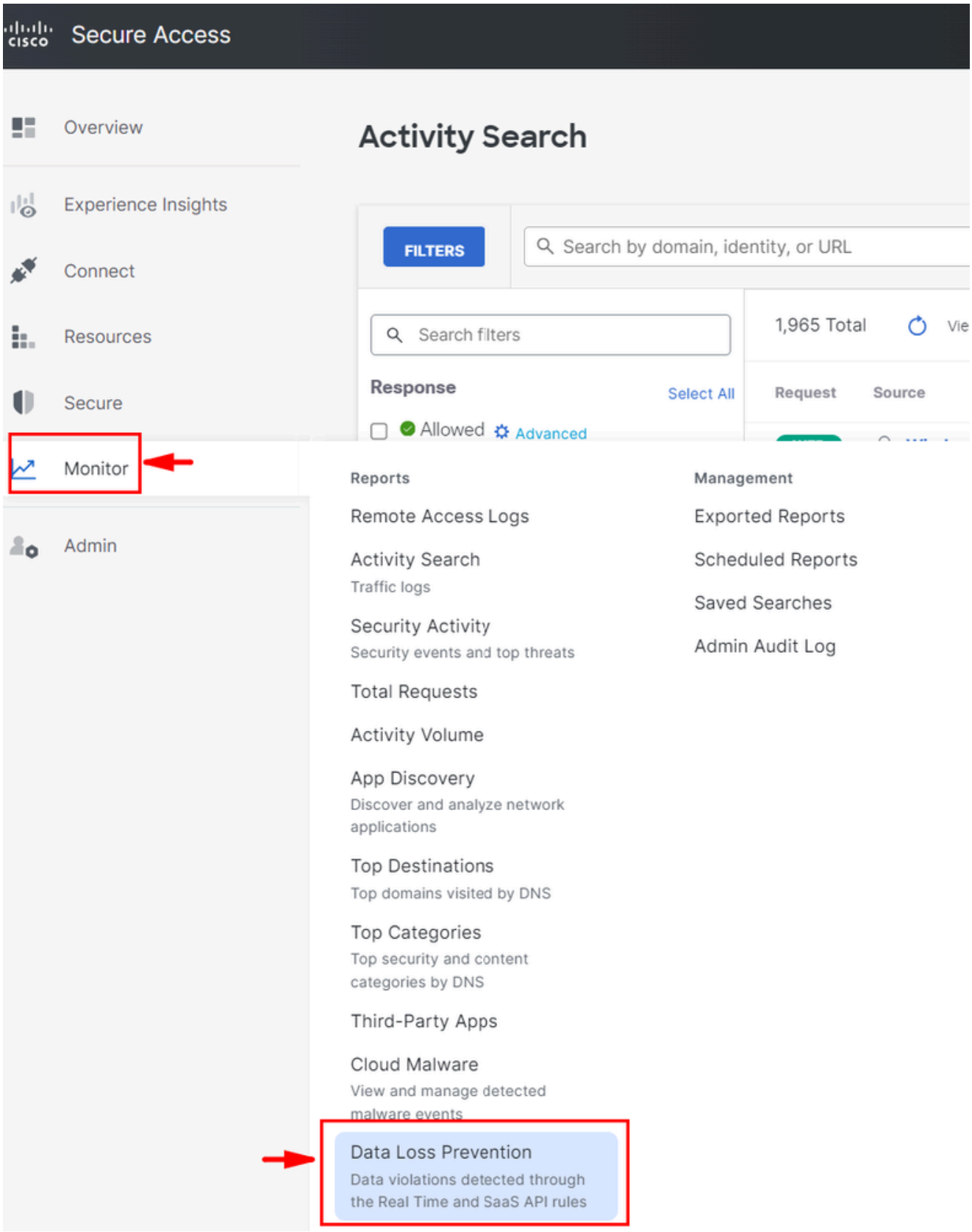



Vérifier

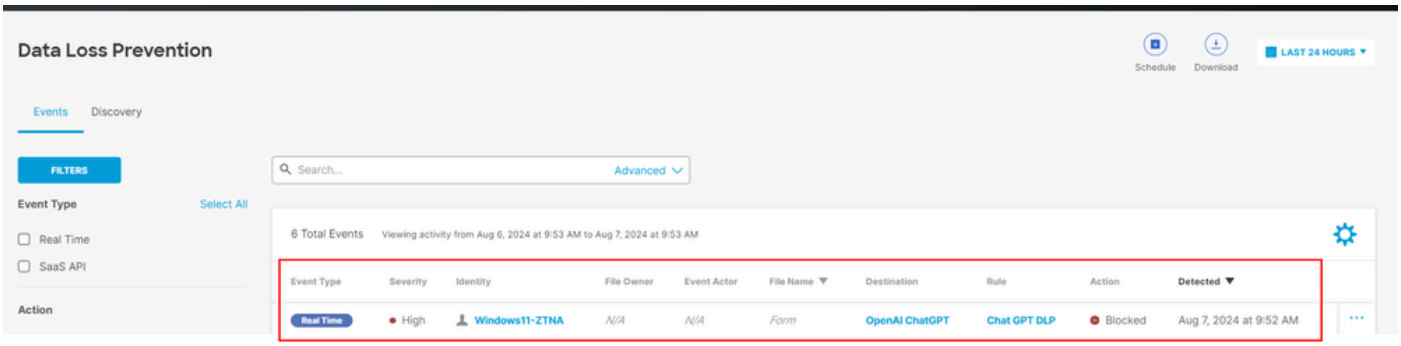
Nous pouvons voir quand l'utilisateur essaie de demander à ChatGPT un exemple de programme python, la requête est bloquée.

Nous pouvons confirmer qu'un événement DLP a été déclenché dans les journaux Secure Access Data Loss Prevention.

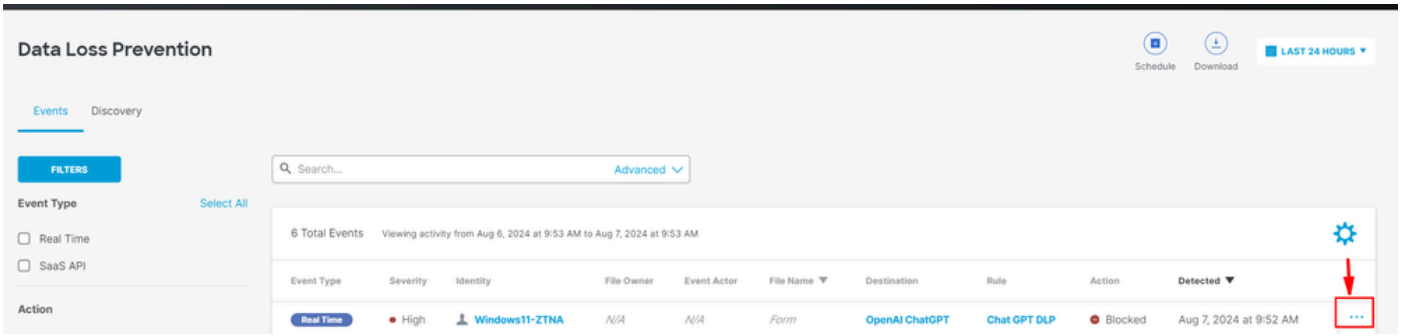
- Accéder à Monitor> Data Loss Prevention



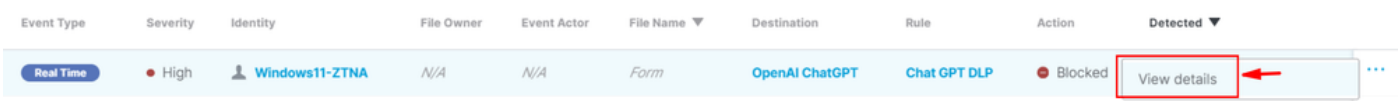

- Nous pouvons voir l'événement DLP.



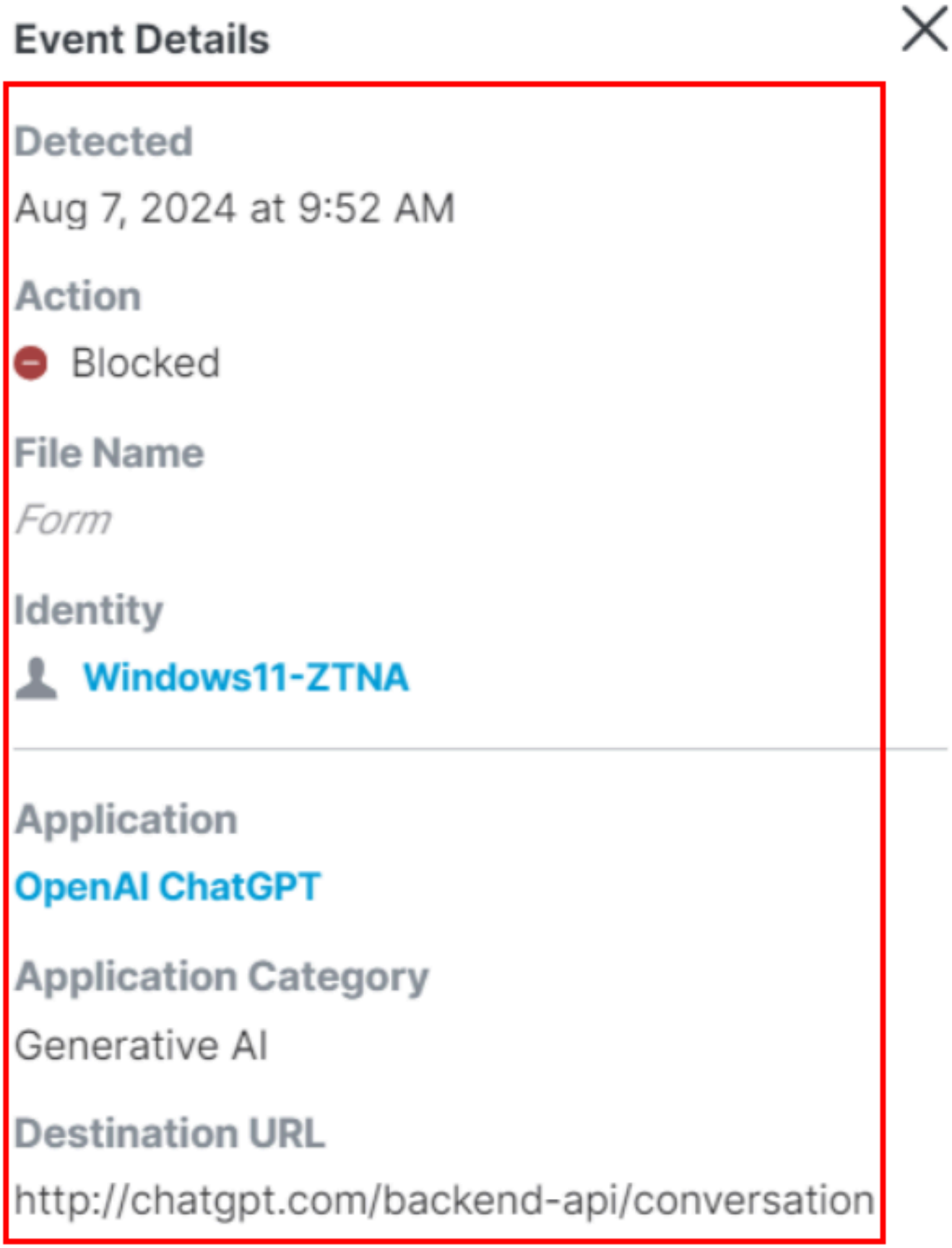

- Cliquez sur les trois points à la fin du journal des événements pour vérifier plus de détails sur l'événement.



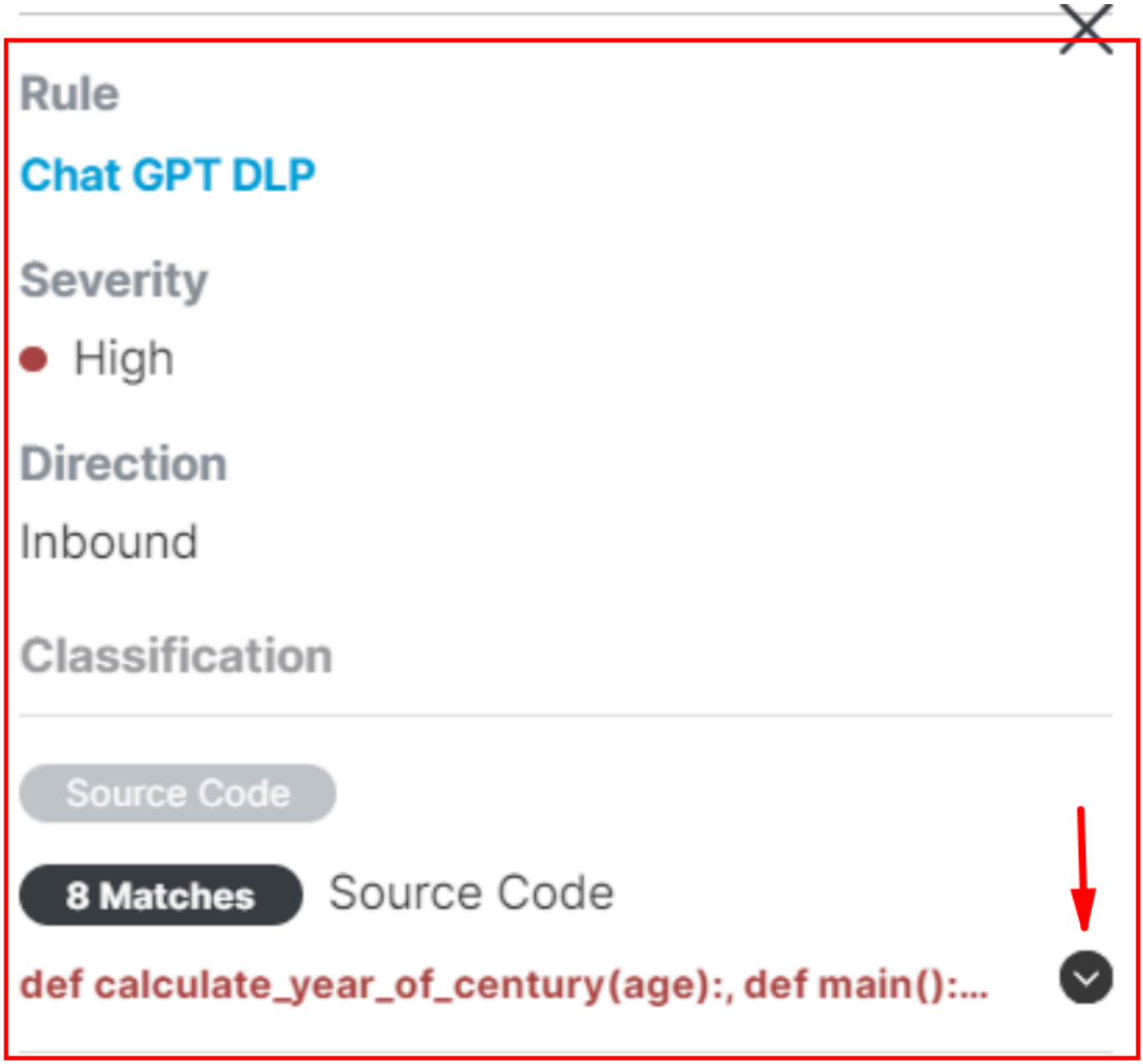

- Cliquez sur View details.



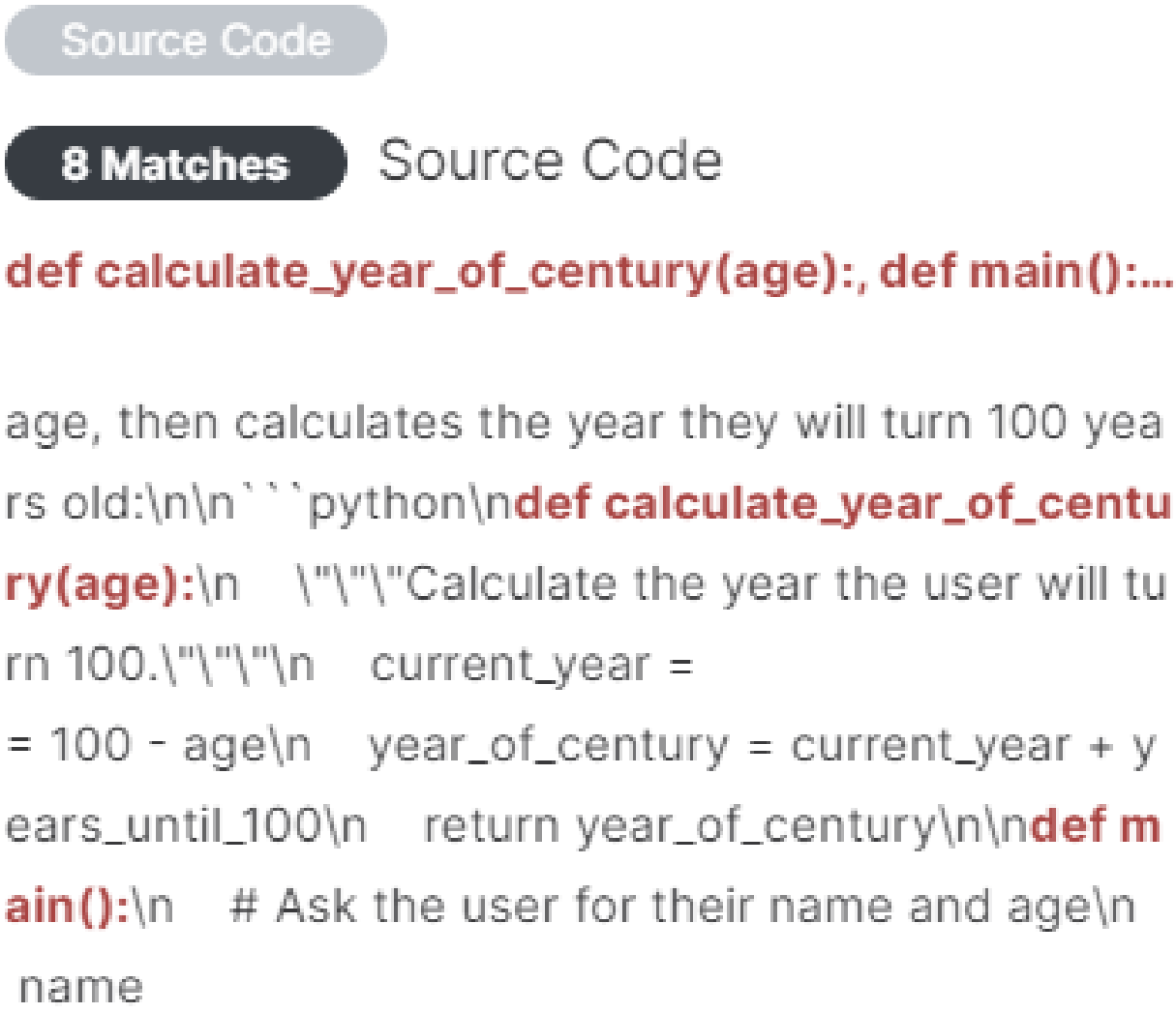

- Nous voyons maintenant l'intégralité des détails de l'événement.




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

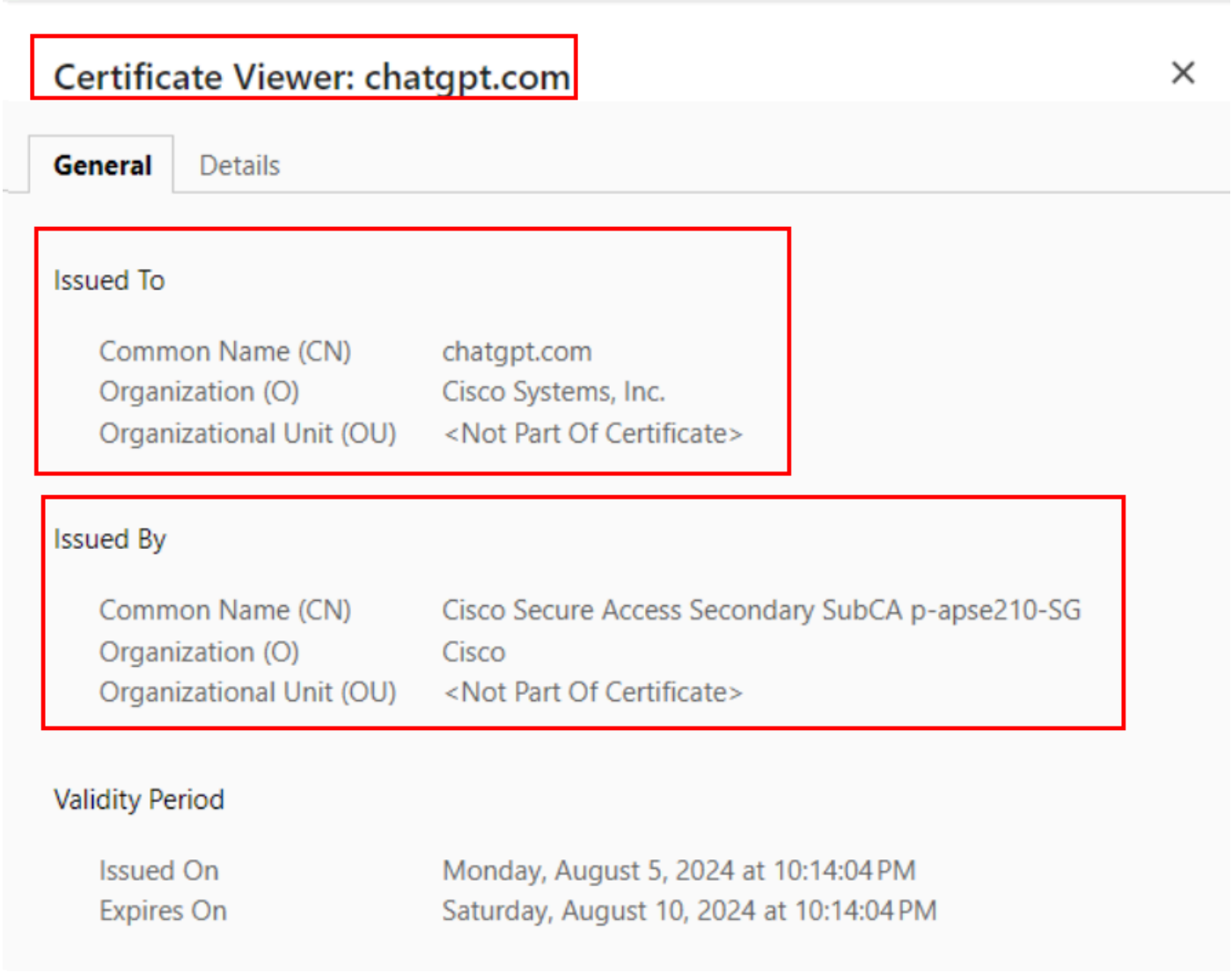


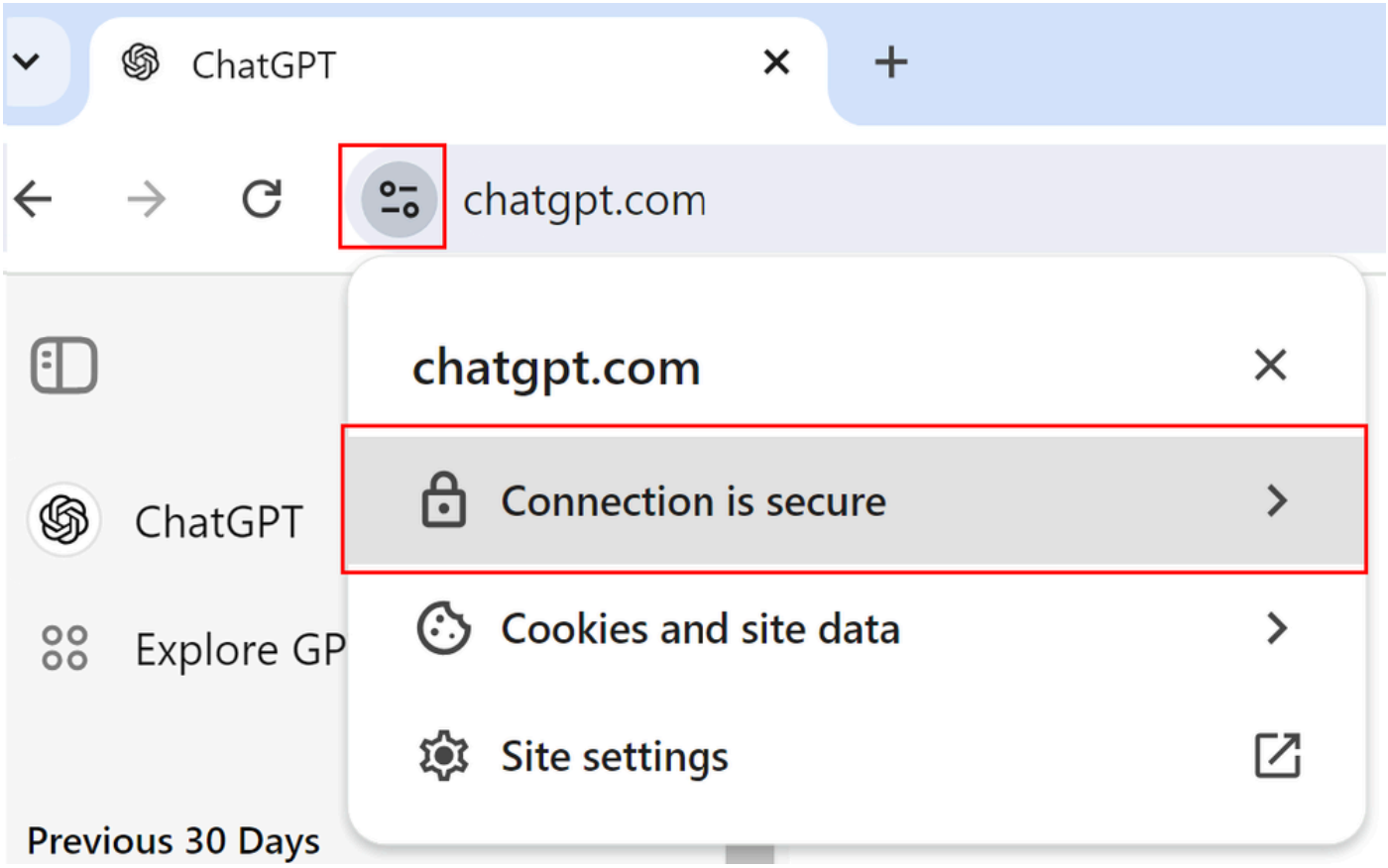

- Nous voyons tous les détails du contenu qui correspondait au classifieur / Classification de la politique DLP.

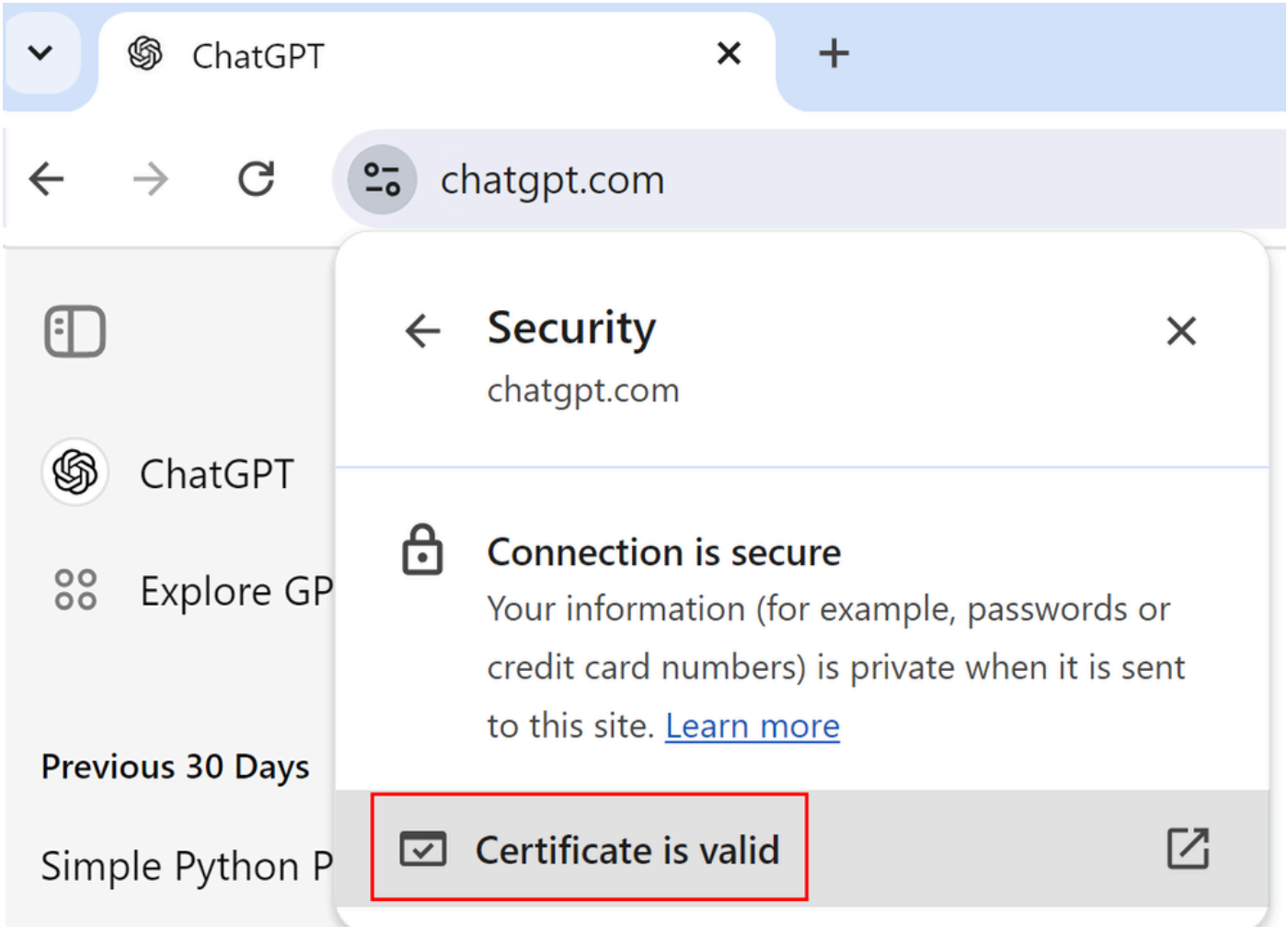


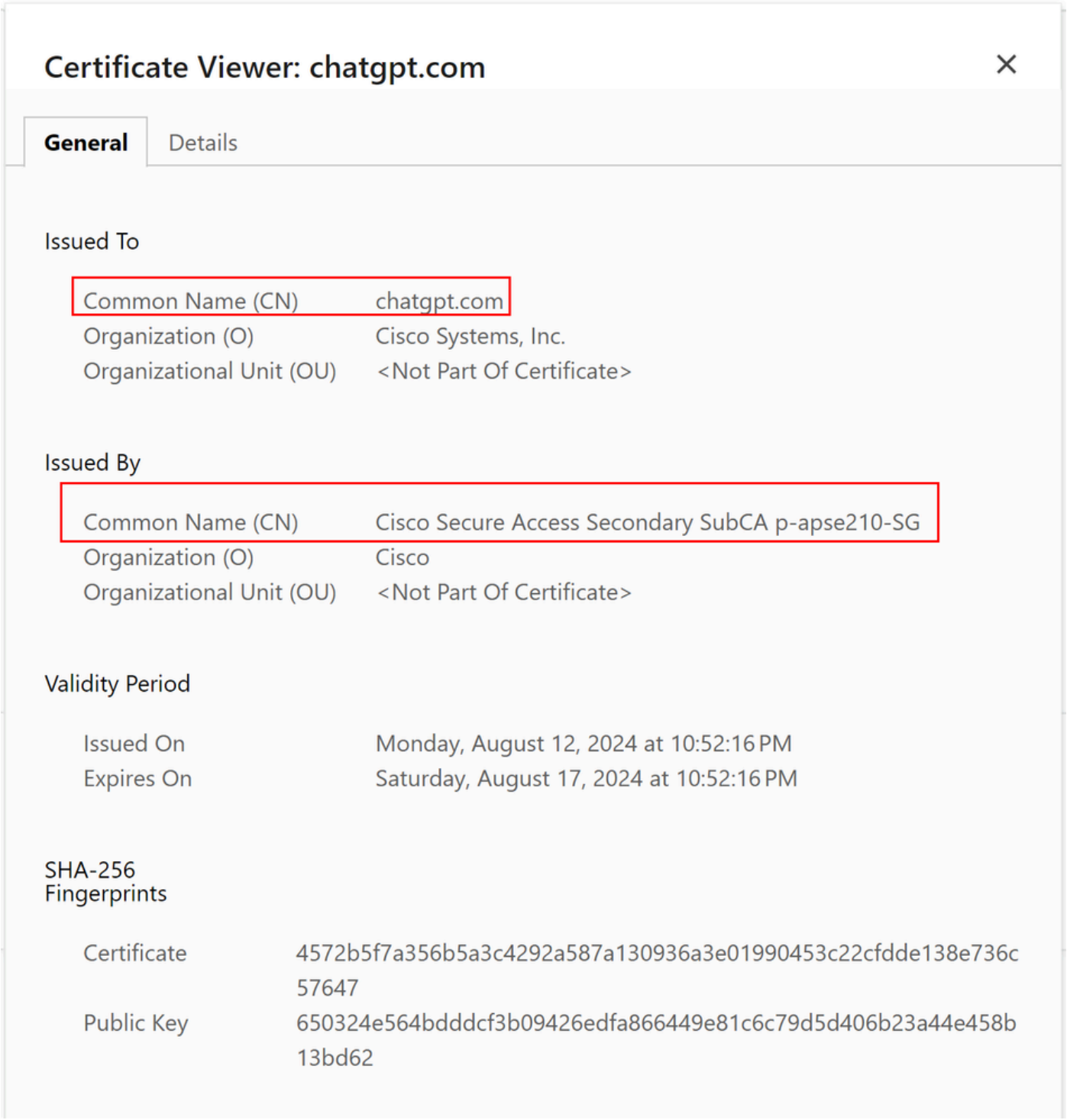

Dépannage

- 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

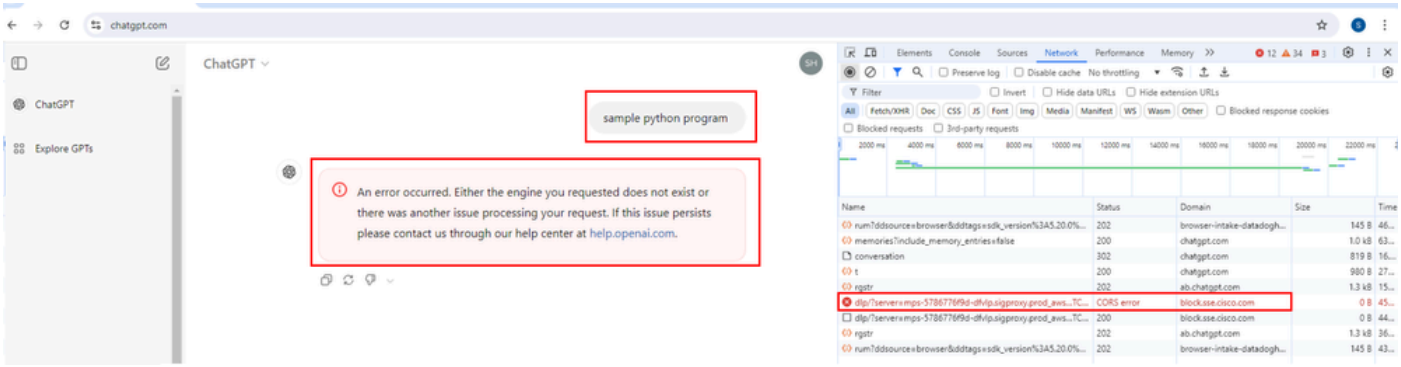

ChatGPT
chatgpt.com
chatgpt.com
Connection is secure
Cookies and site data
Site settings
ChatGPT
Explore GP
Previous 30 Days


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

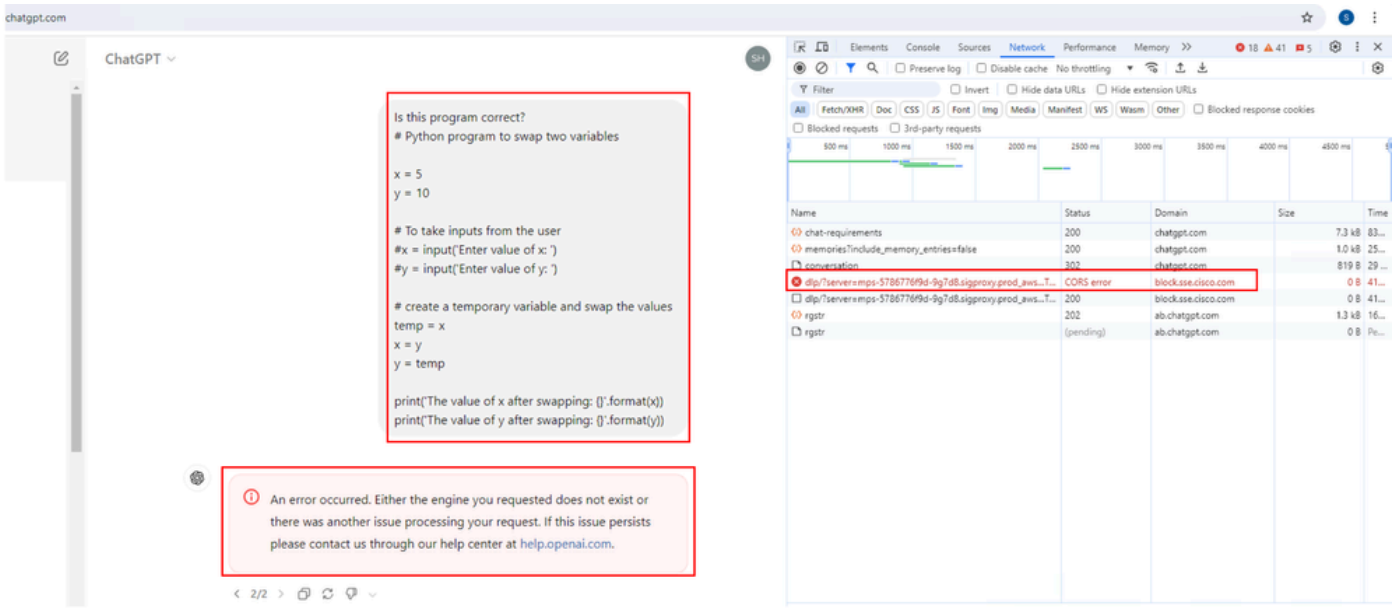



- Ouvrez ChatGPT > Ouvrez les outils de développement > Sélectionnez Réseau > Ensuite essayez de demander à ChatGPT un exemple de programme python

- 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.