# Implemente DLP en Secure Access para restringir el uso de Open AI ChatGPT para programación

## Contenido


Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Configurar

- 1.Cree una clasificación de datos para utilizar el identificador de datos de código fuente
- 2.Cree una política DLP y llame al "Código fuente" de clasificación de datos que contiene.
- 3. Asegúrese de que dispone de una política de acceso a Internet para el tráfico hacia Chat GPT con el descifrado habilitado.
- 4.Utilizando Open AI ChatGPT intenta descargar o cargar cualquier programa.

Verificación

Troubleshoot

Información Relacionada


## Introducción

Este documento describe cómo implementar Data Loss Prevention (DLP) en Secure Access para restringir el uso de Open AI ChatGPT para programación y codificación.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso seguro
- DLP
- Abrir AI ChatGPT

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Acceso seguro
- DLP

- Abrir AI ChatGPT

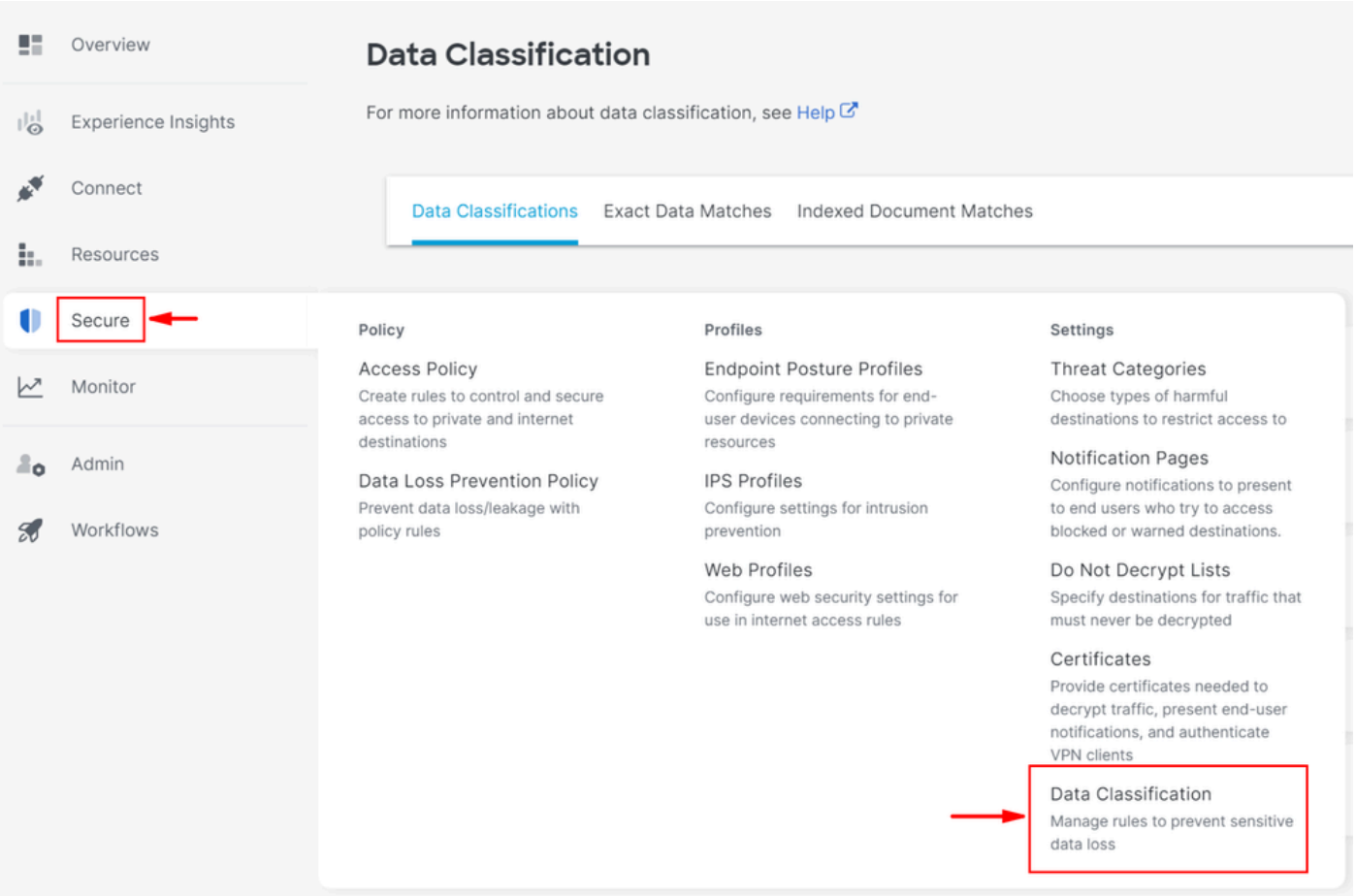
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

# Configurar

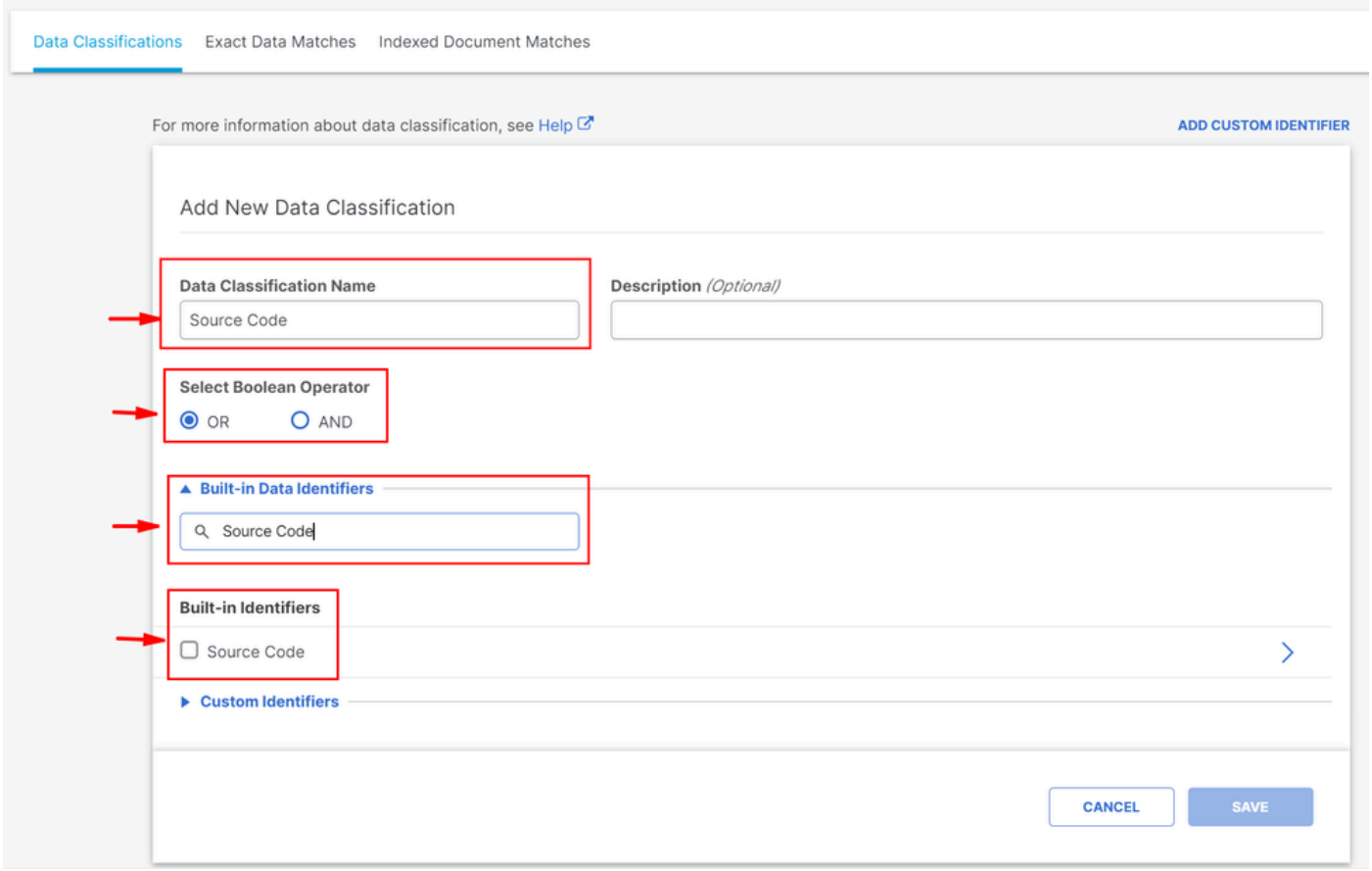
## 1.Cree una clasificación de datos para utilizar el identificador de datos de código fuente

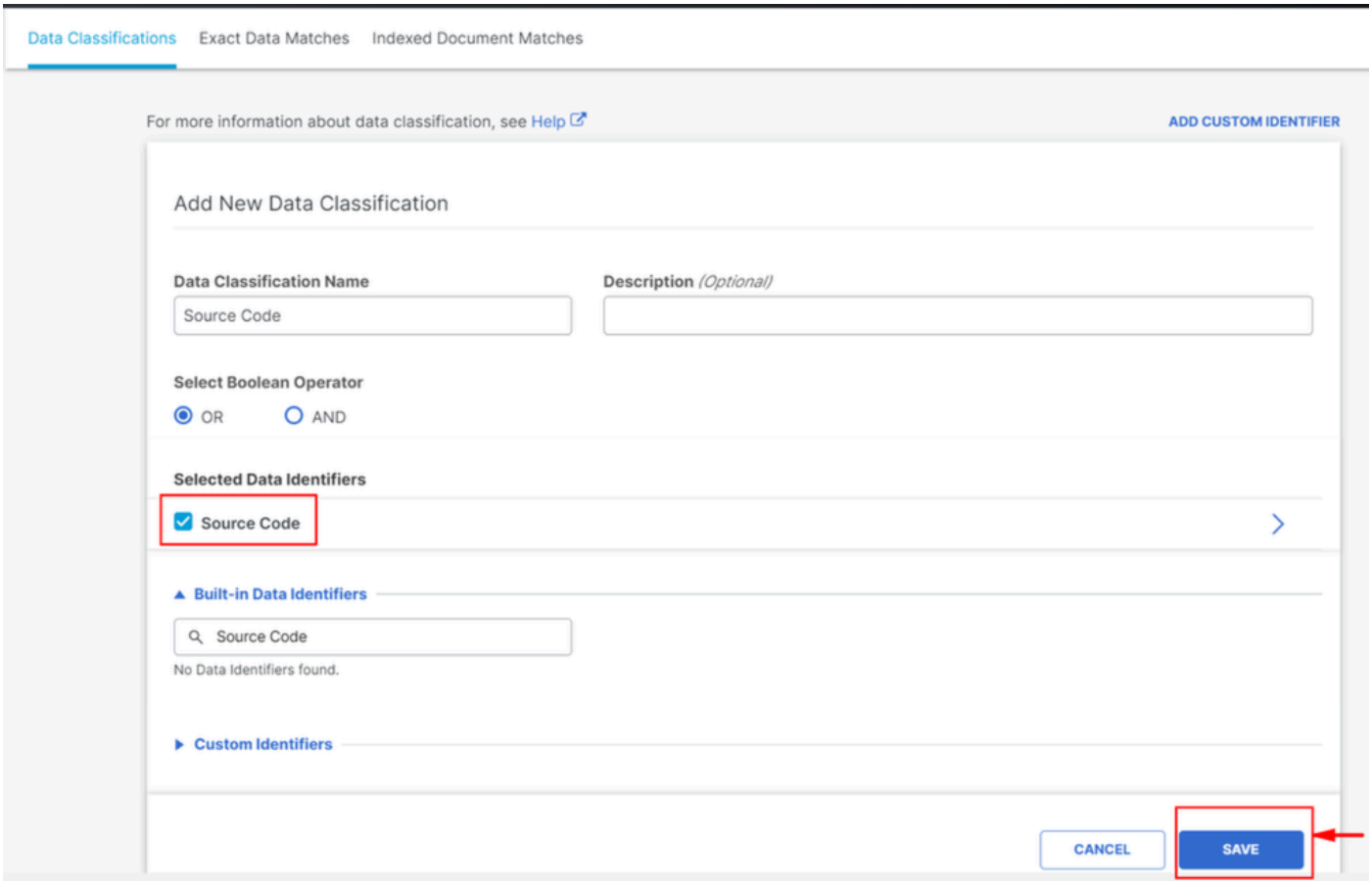
Vaya a [Panel de acceso seguro.]

- Haga clic en Secure > Data Classification > Add



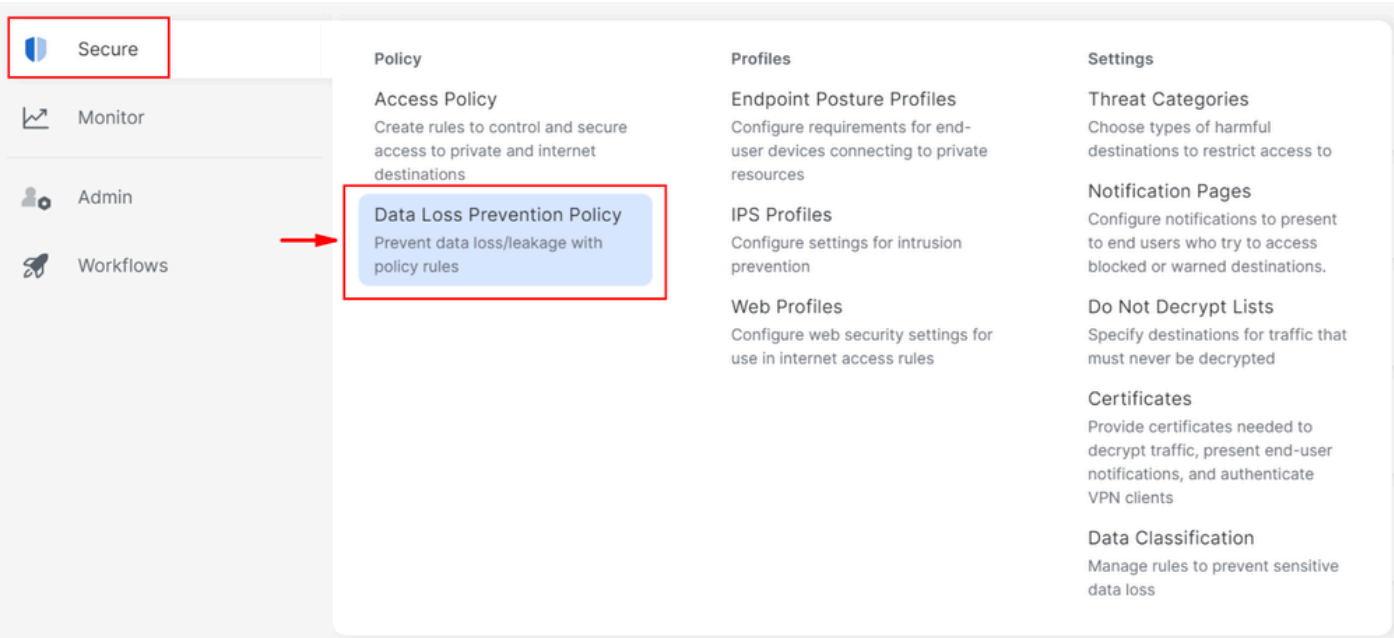

- Ingrese el Data Classification Name > **Select** Built-in Data Identifiers > Search for Source Code y selecciónelo



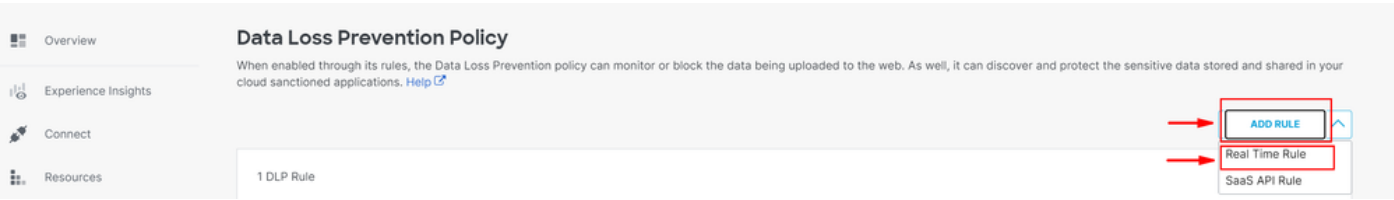




2.Cree una política DLP y llame al "Código fuente" de clasificación de datos que contiene.

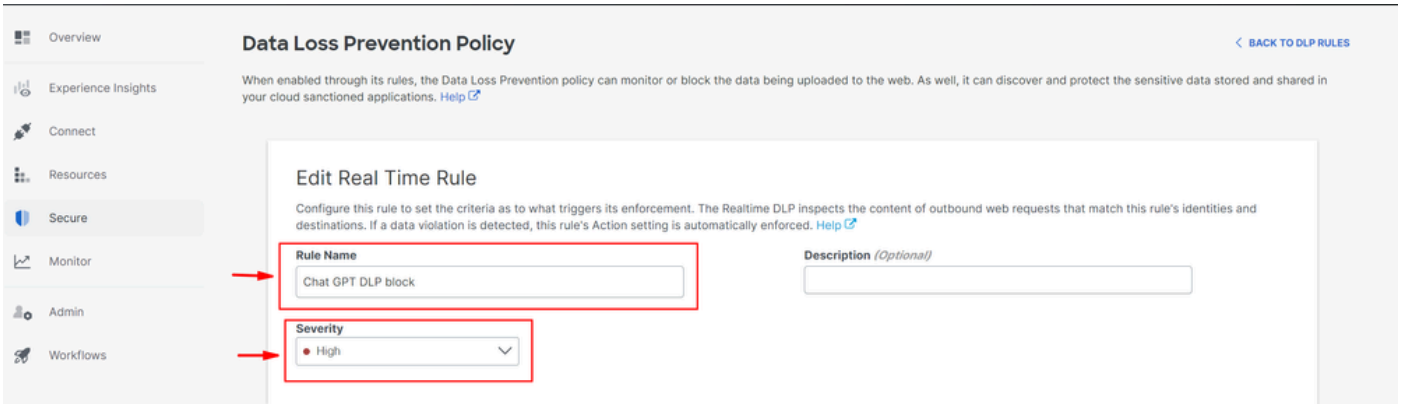
- Haga clic en Secure > Data Loss Prevention Policy



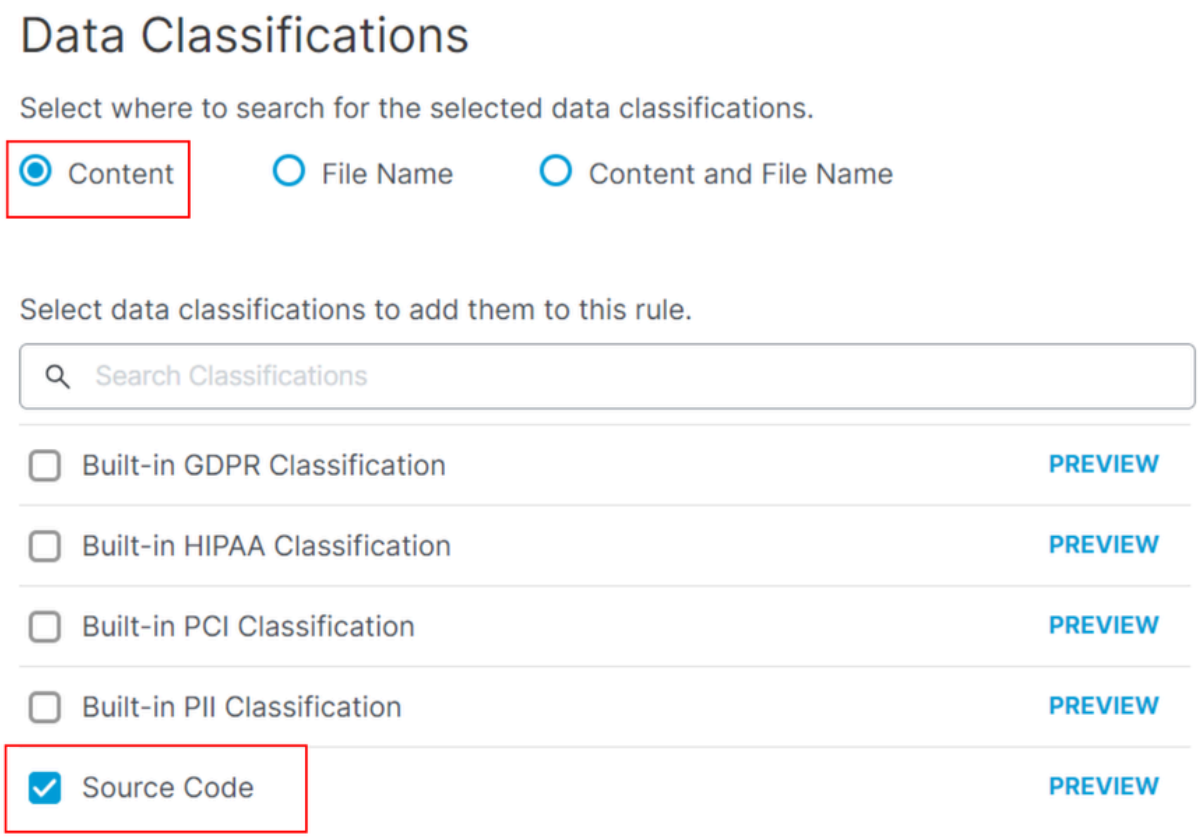

- Haga clic en Add Rule > Real Time Rule



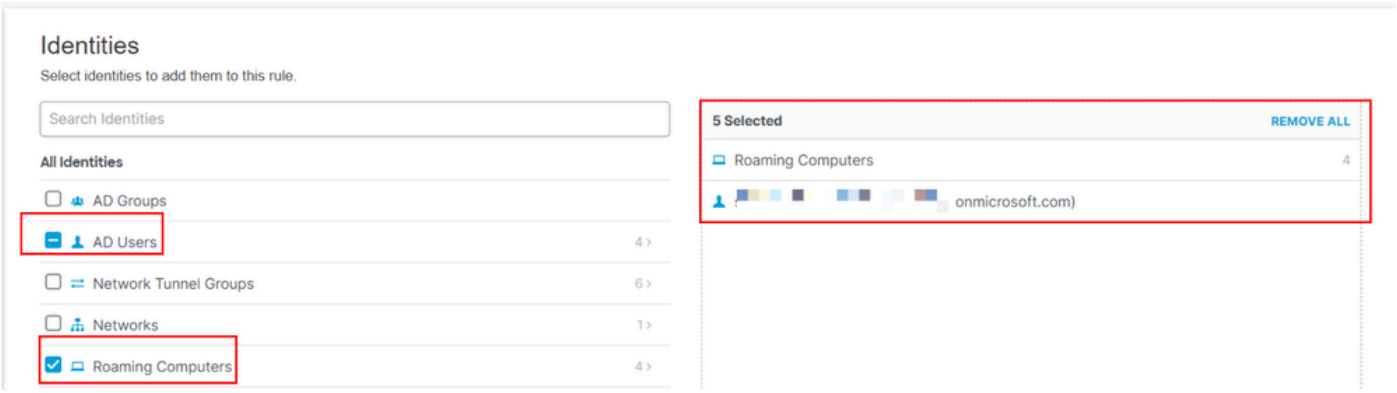

- Proporcione un Rule Name > Set apropiado Severity




- En Data Classifications seleccionar Content y seleccionar Source Code

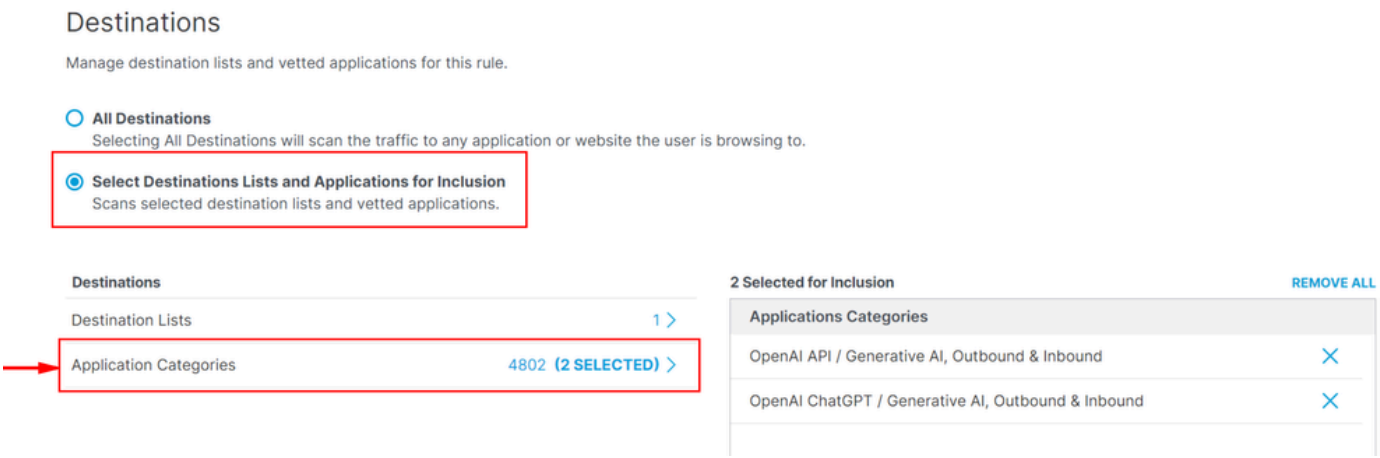



- En Identitiesseleccione las identidades deseadas según sea necesario



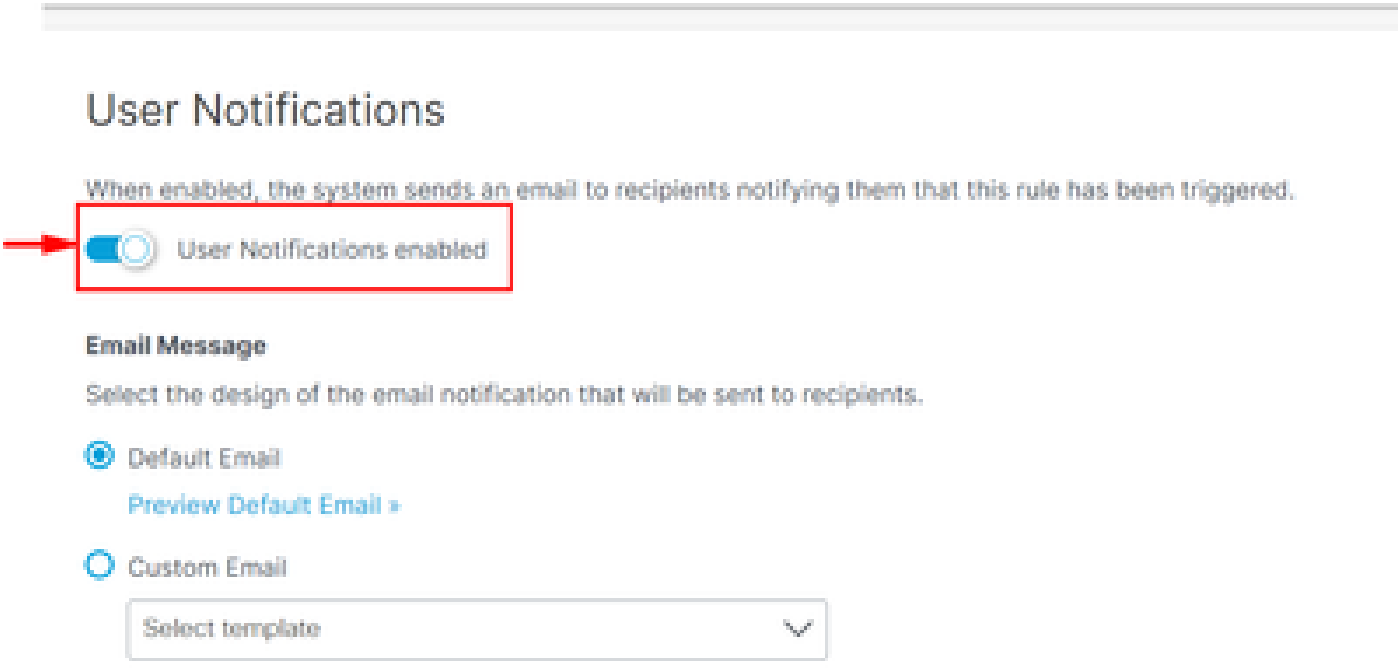

- En Destinos, seleccione Select Destination Lists and Applications for Inclusion

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

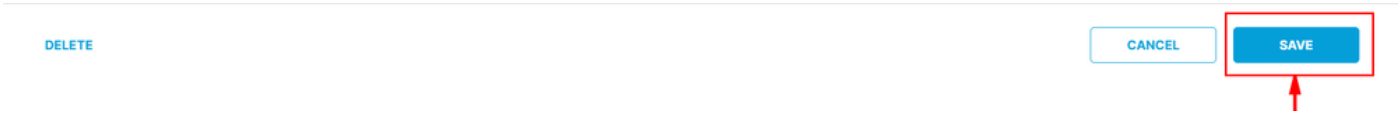



- En Actionseleccionar Block

- En User Notifications, puede configurar las notificaciones de correo electrónico para los usuarios finales, cuando se active la regla (opcional)

- Haga clic en Save




3. Asegúrese de que dispone de una política de acceso a Internet para el tráfico hacia Chat GPT con el descifrado habilitado.

**Ejemplo:**

# Chat GPT

Internet

## General

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

## Sources

Any

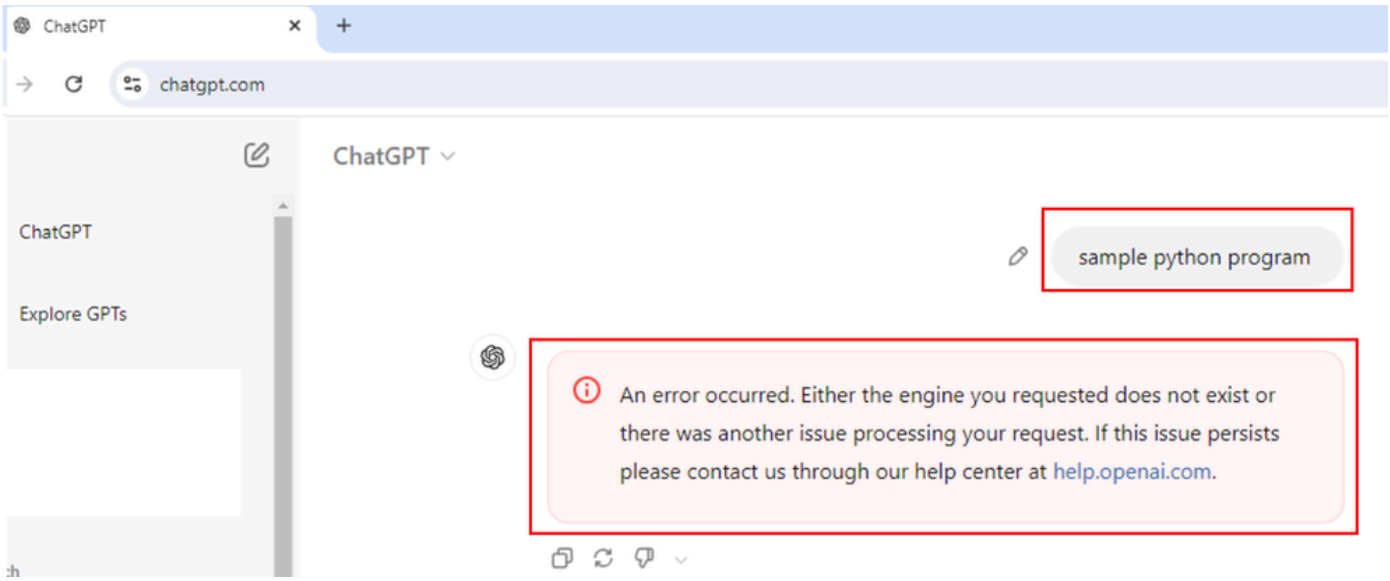
## Destinations

2 destinations

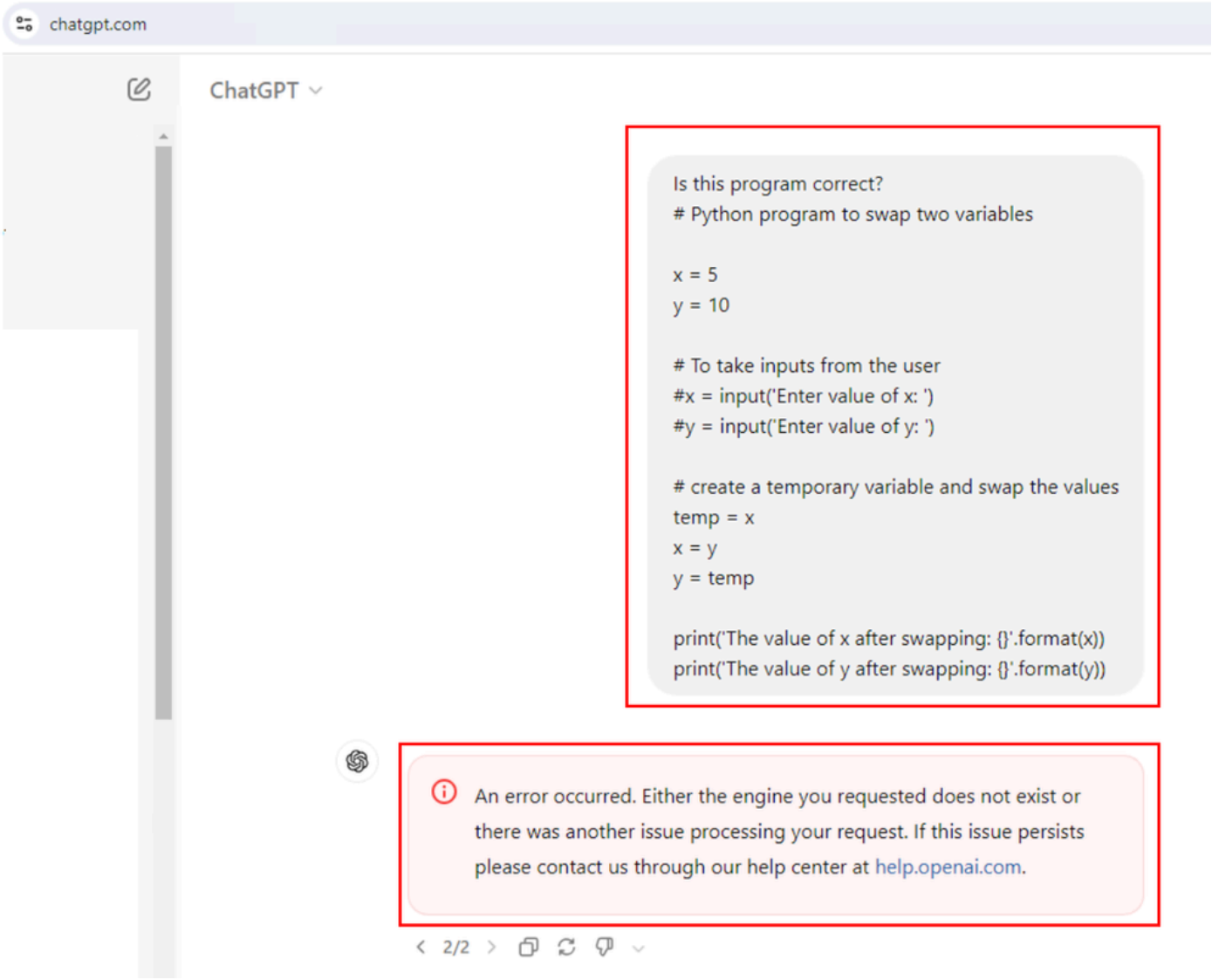
### Application Settings (2)

OpenAI API  OpenAI ChatGPT

- Solicite un programa python de muestra y esta solicitud se bloqueará.




- Pregunte si el programa es correcto o no y esta solicitud se bloqueará.

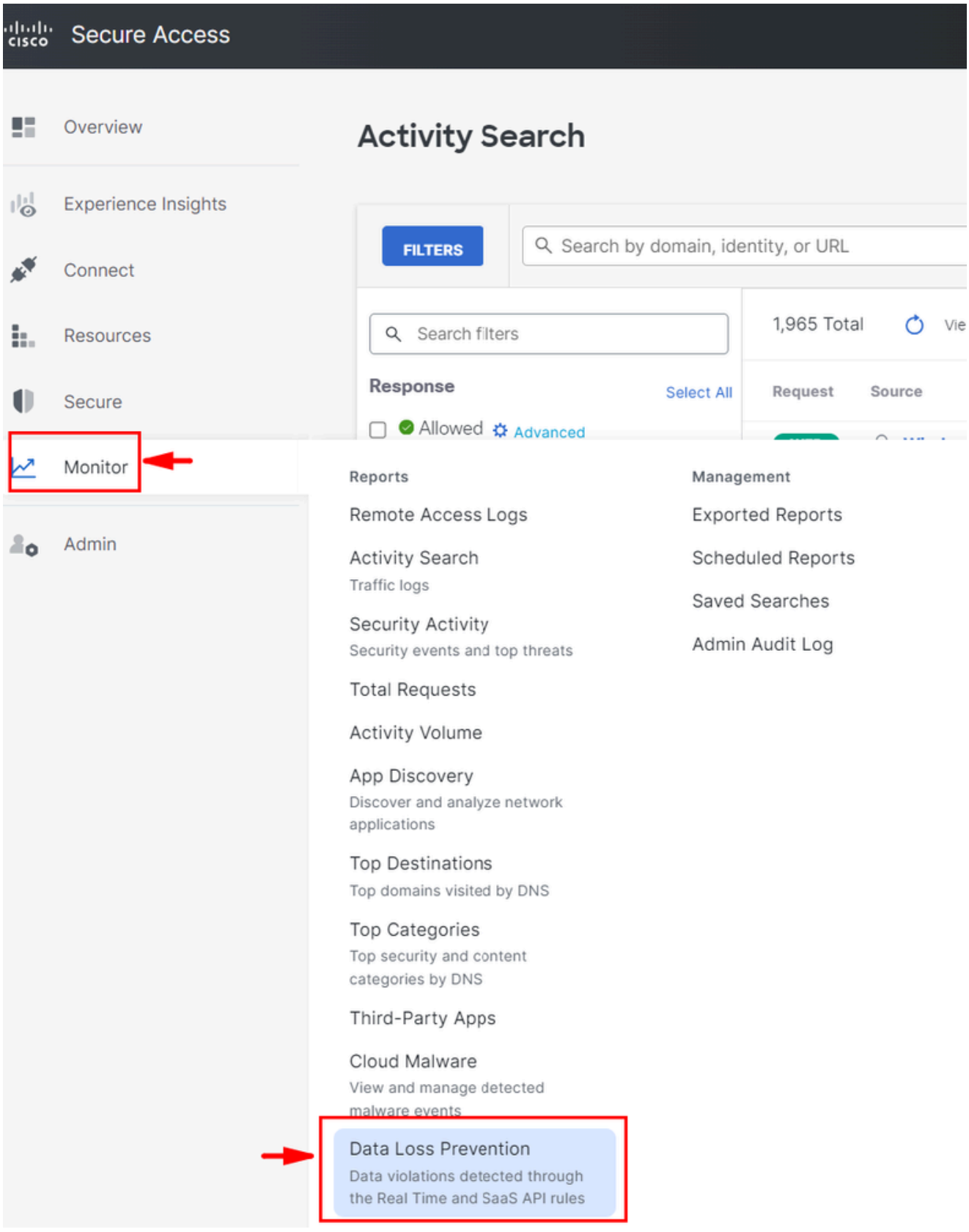



Verificación

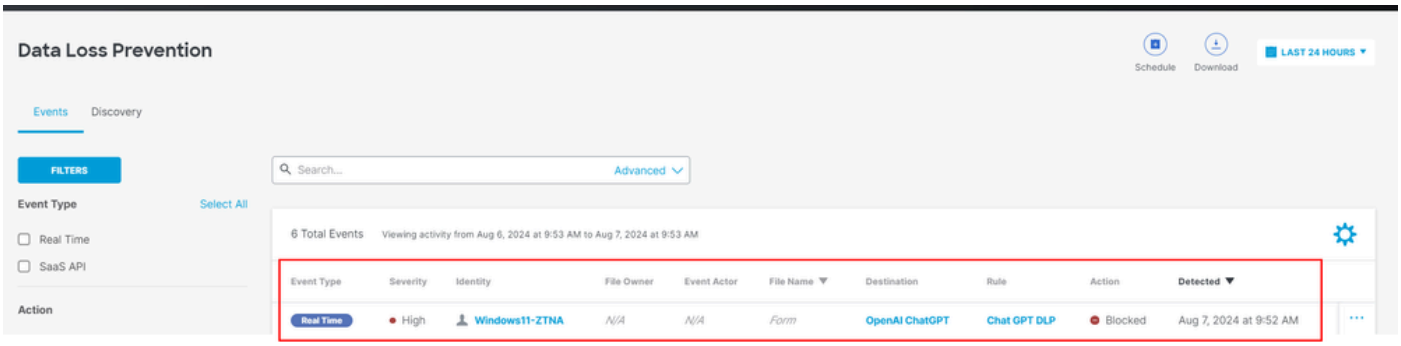
Podemos ver que cuando un usuario intenta pedir a ChatGPT un programa de Python de muestra, la solicitud se bloquea.

Podemos confirmar que se ha desencadenado un evento de DLP en los registros de prevención de pérdida de datos de acceso seguro.

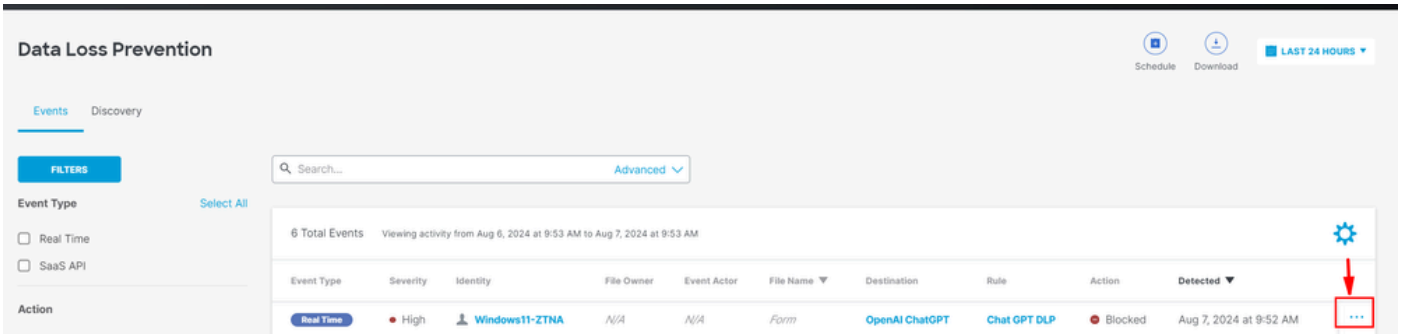
- Vaya a Monitor> Data Loss Prevention



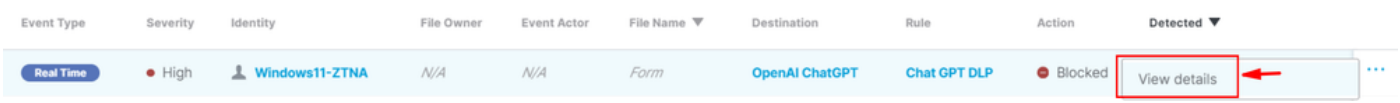

- Podemos ver el evento de DLP.



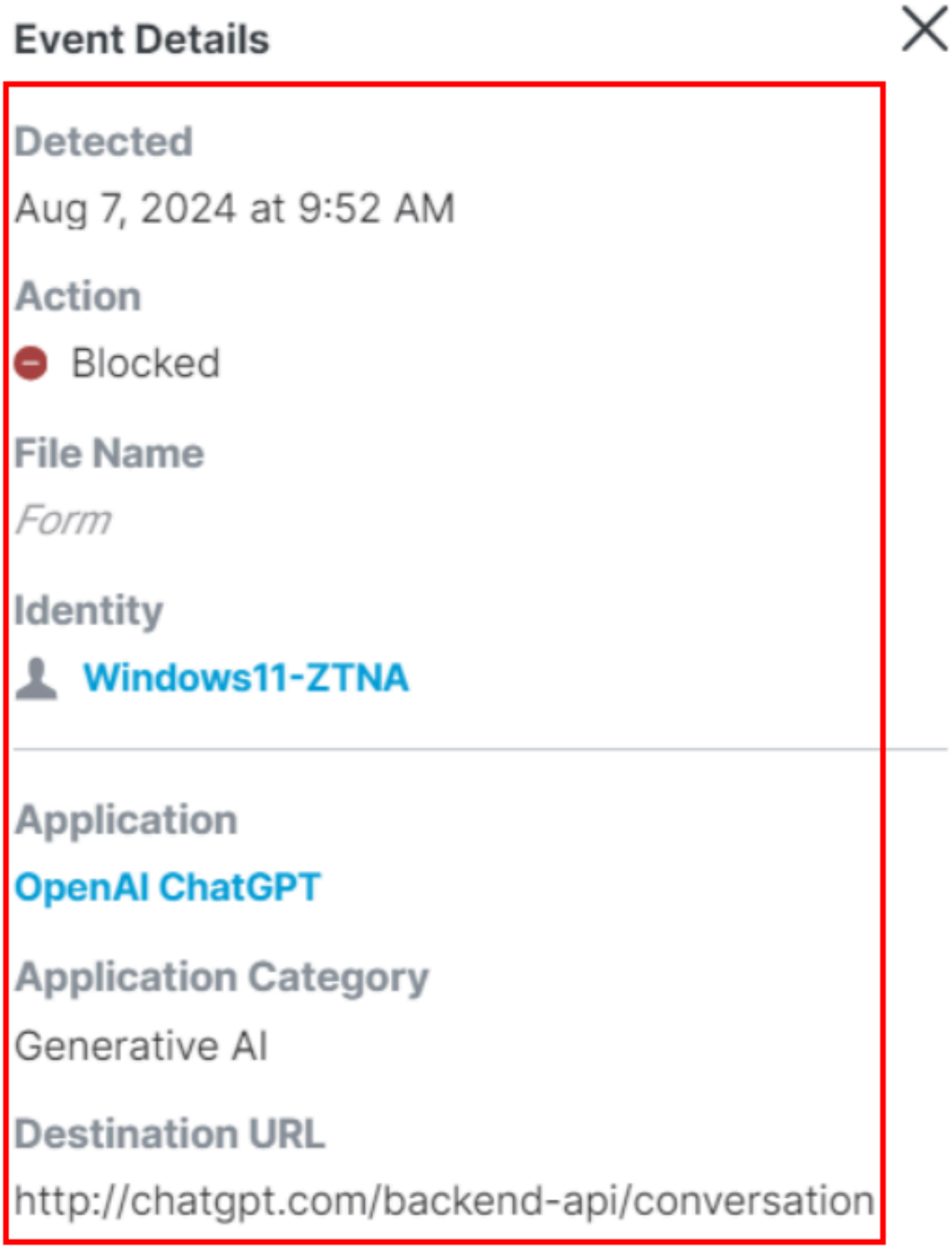

- Haga clic en los tres puntos situados al final del registro de eventos para comprobar si hay más detalles sobre el evento.



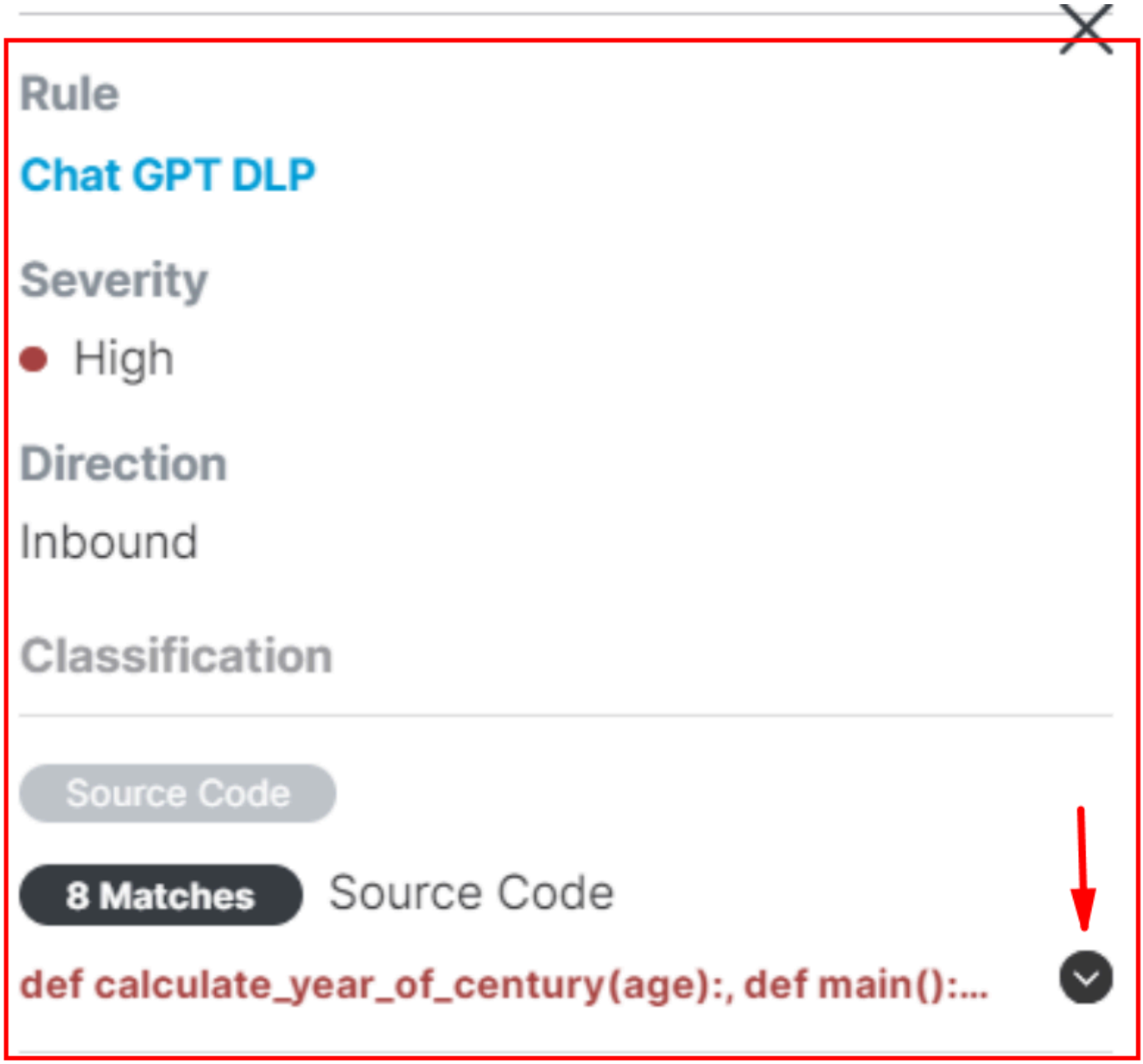

- Haga clic en View details.



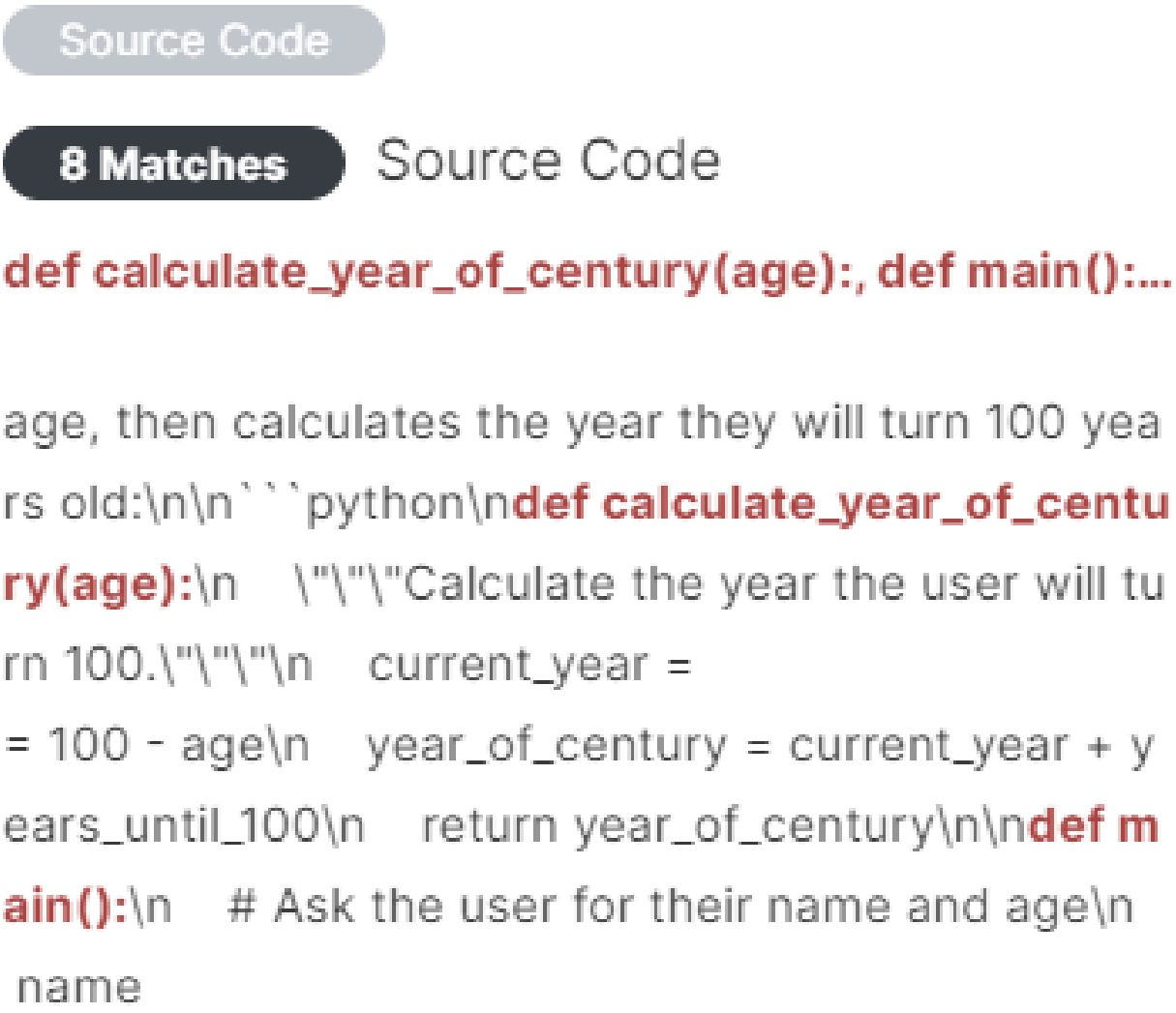

- Ahora vemos todos los detalles del evento.




- Expanda la clasificación para ver qué contenido coincide con el clasificador.

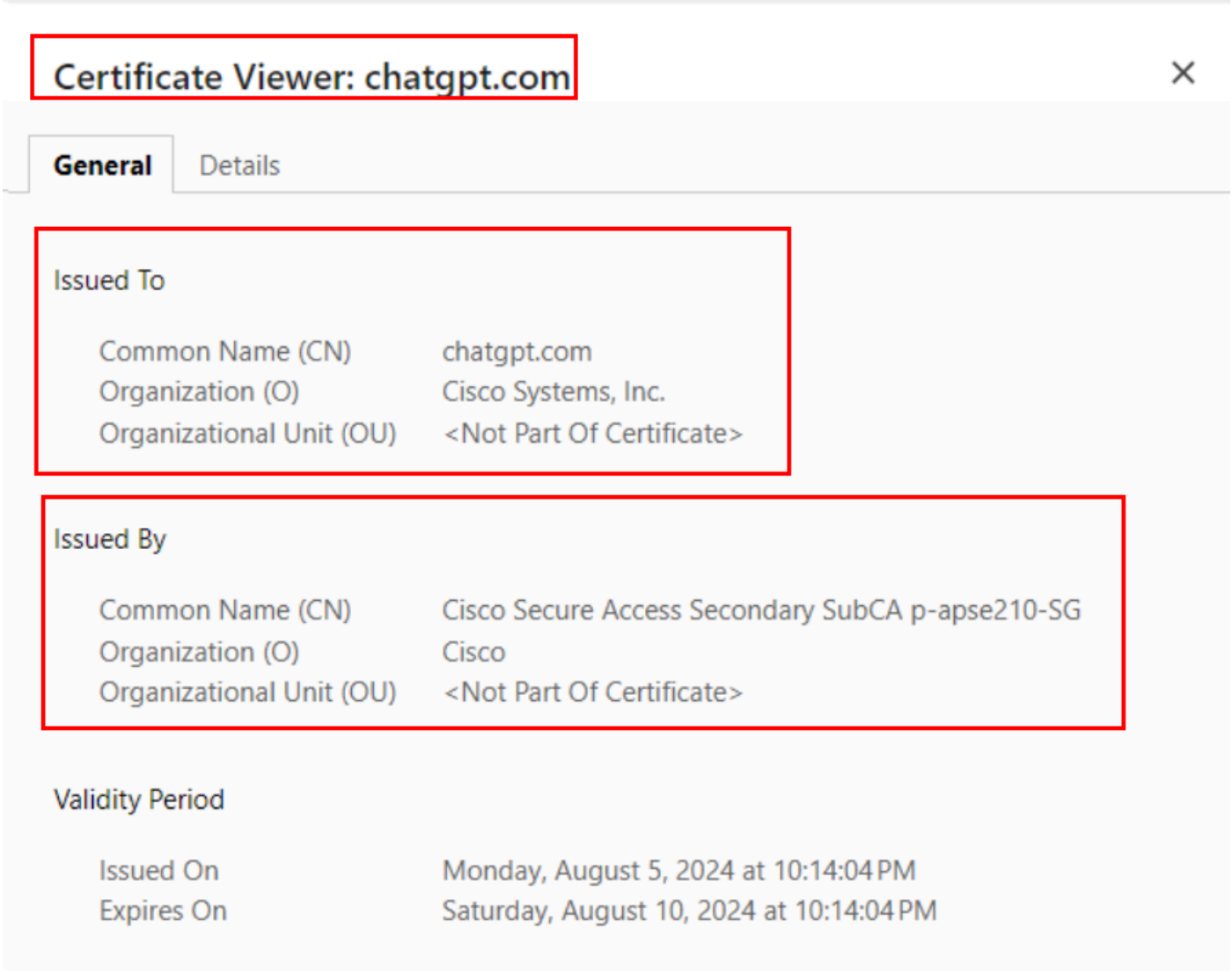


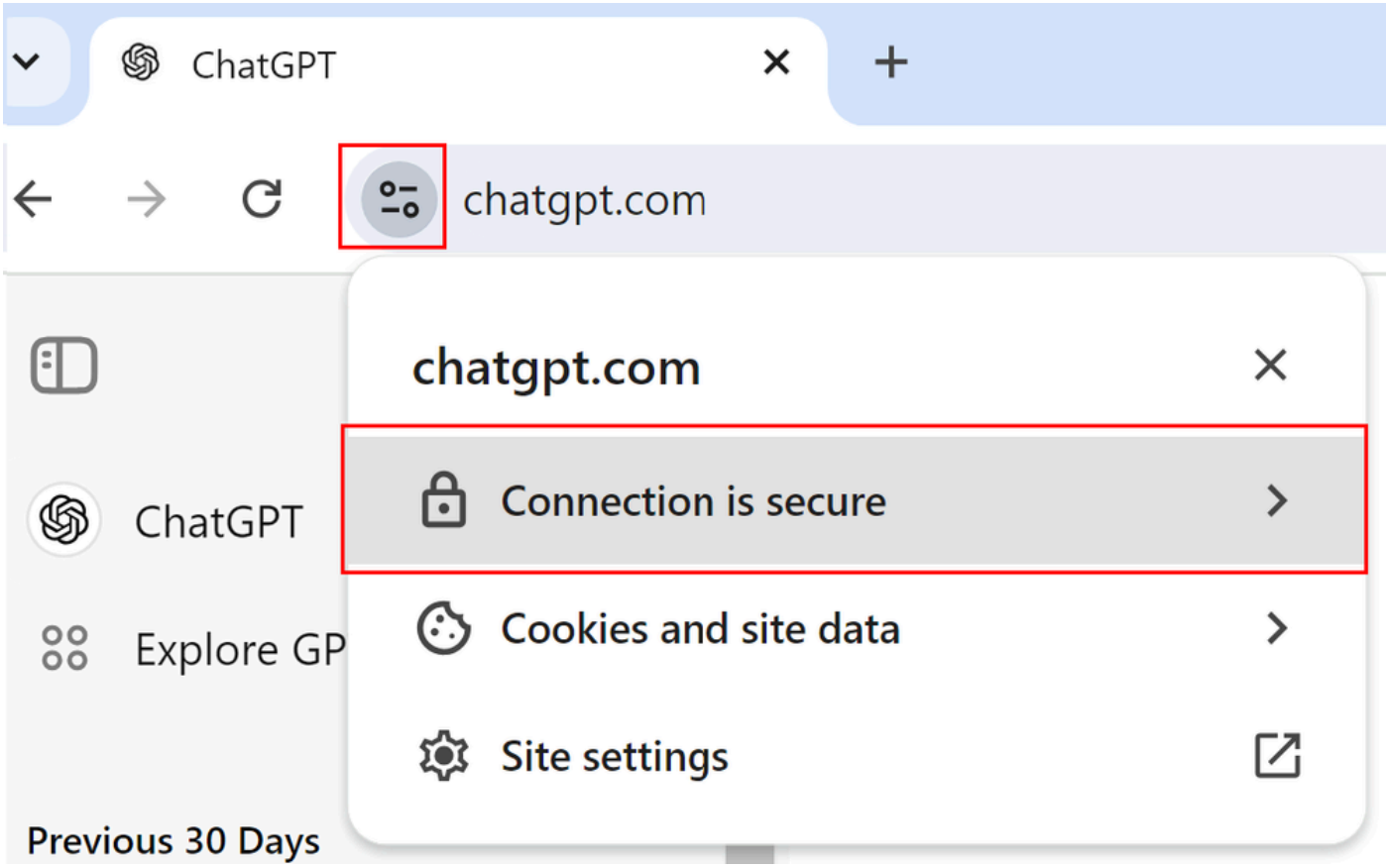

- Vemos todos los detalles del contenido que coinciden con el clasificador/clasificación de la política DLP.

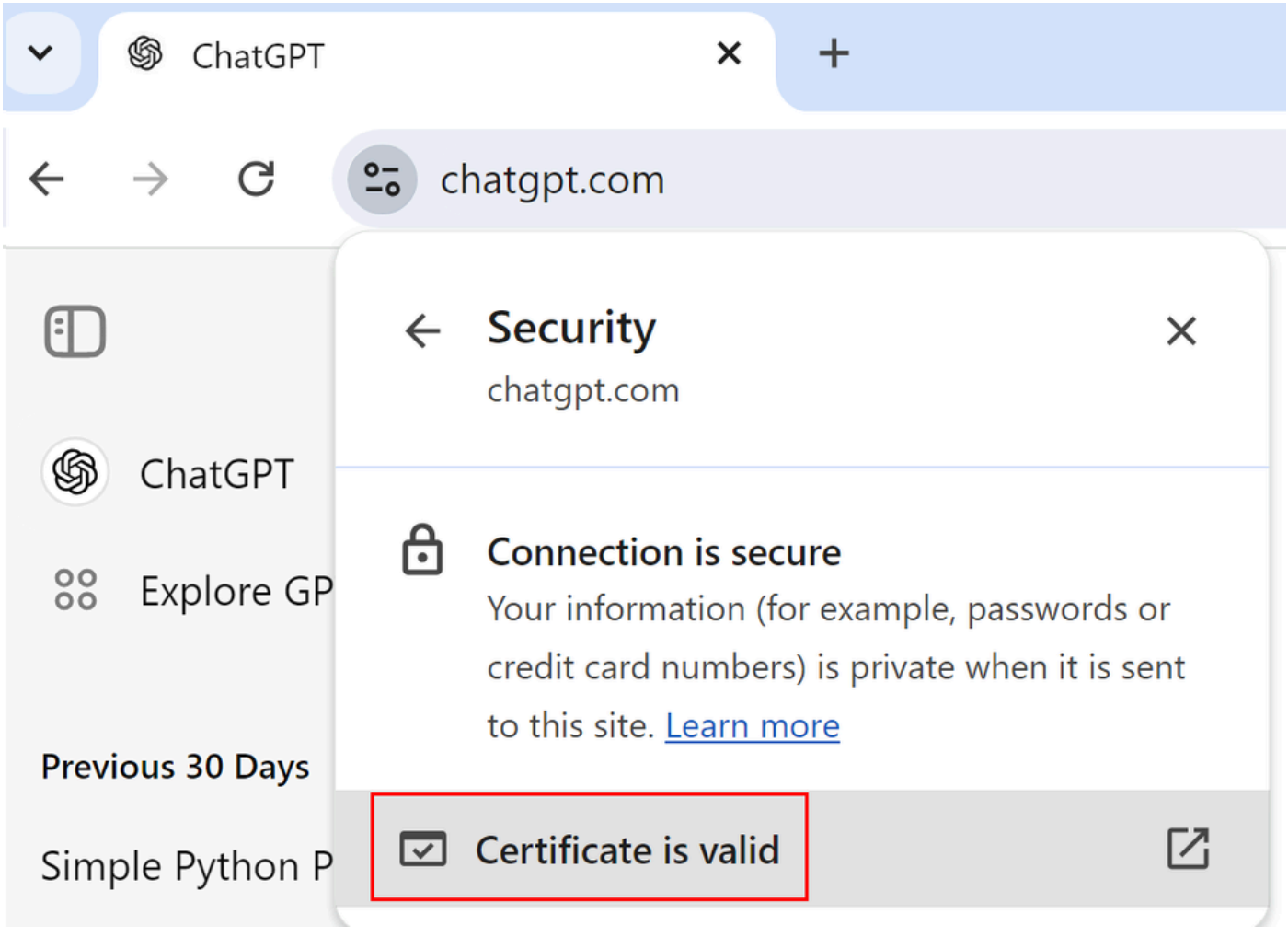


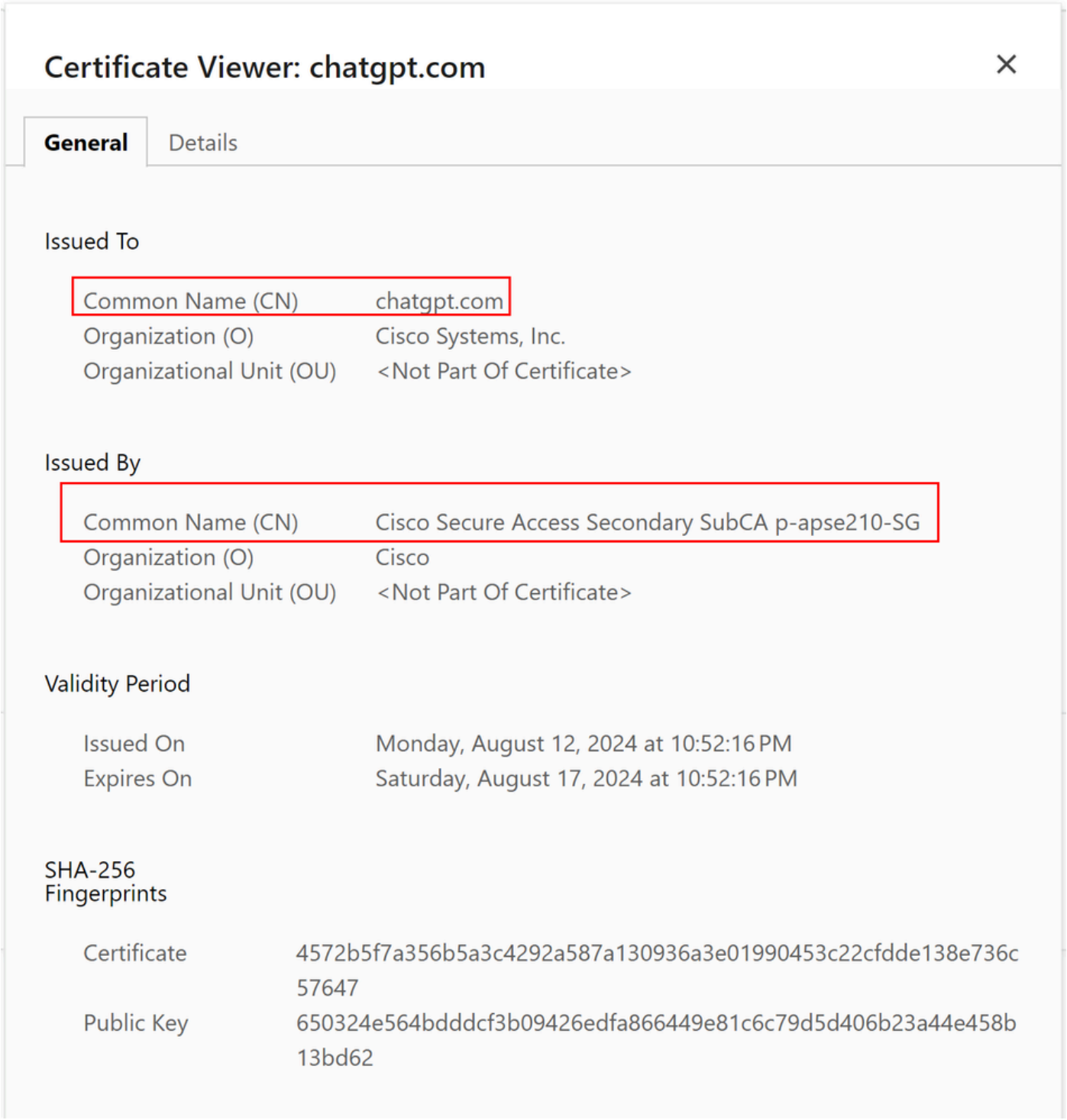

Troubleshoot

- Asegúrese de que la política de acceso que coincide con las solicitudes web para Open AI ChatGPT tenga el descifrado habilitado.
- Para verificar rápidamente si SSE está descifrando el tráfico para Open AI ChatGPT, verifique el certificado del sitio web que muestra que el nombre común incluye las palabras clave "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

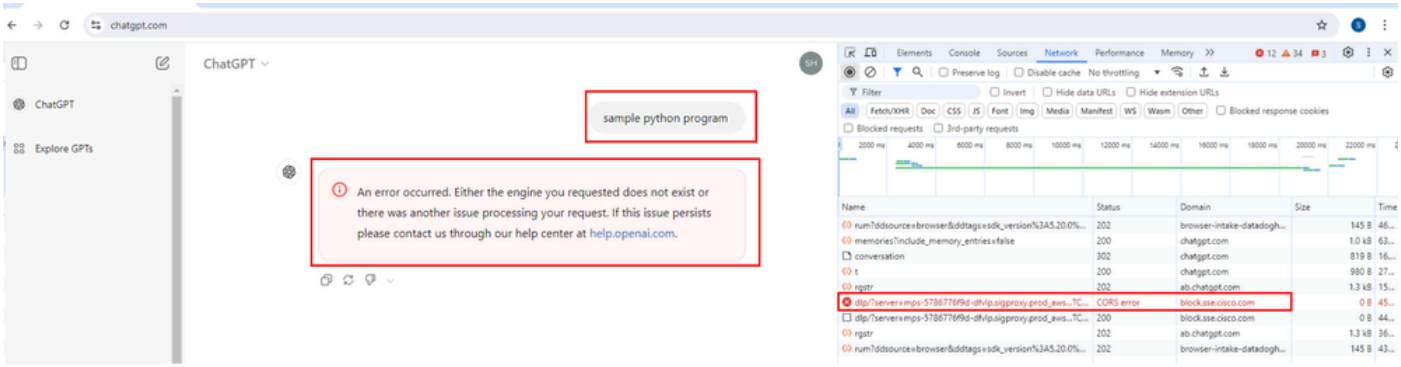

ChatGPT
chatgpt.com
chatgpt.com
Connection is secure
Cookies and site data
Site settings
ChatGPT
Explore GP
Previous 30 Days


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

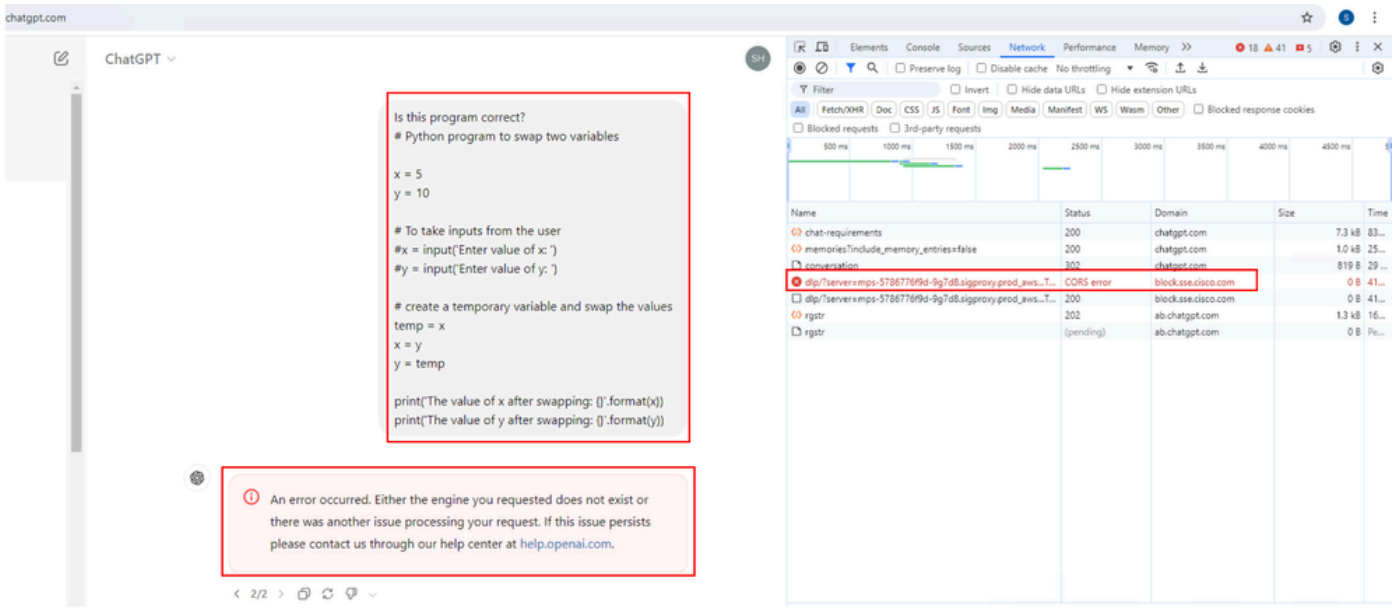



- Abra ChatGPT > Open developer tools > Select Network > A continuación, intente solicitar a ChatGPT un programa python de ejemplo

- Observe que la solicitud da como resultado un bloque. En domain (dominio), verá "block.sse.cisco.com




- Pregunte a ChatGPT si el código del programa es correcto.
- Observe que la solicitud da como resultado un bloque y bajo "domain" verá "block.sse.cisco.com".




Información Relacionada

- Guía del usuario de Cisco Secure Access
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).