在安全访问中实施DLP以限制开放式AI ChatGPT用于编程

目录

简介

本文档介绍如何在安全访问中实施防数据丢失(DLP)，以限制Open AI ChatGPT用于编程和编码。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全访问
- DLP
- 打开AI ChatGPT

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全访问
- DLP
- 打开AI ChatGPT

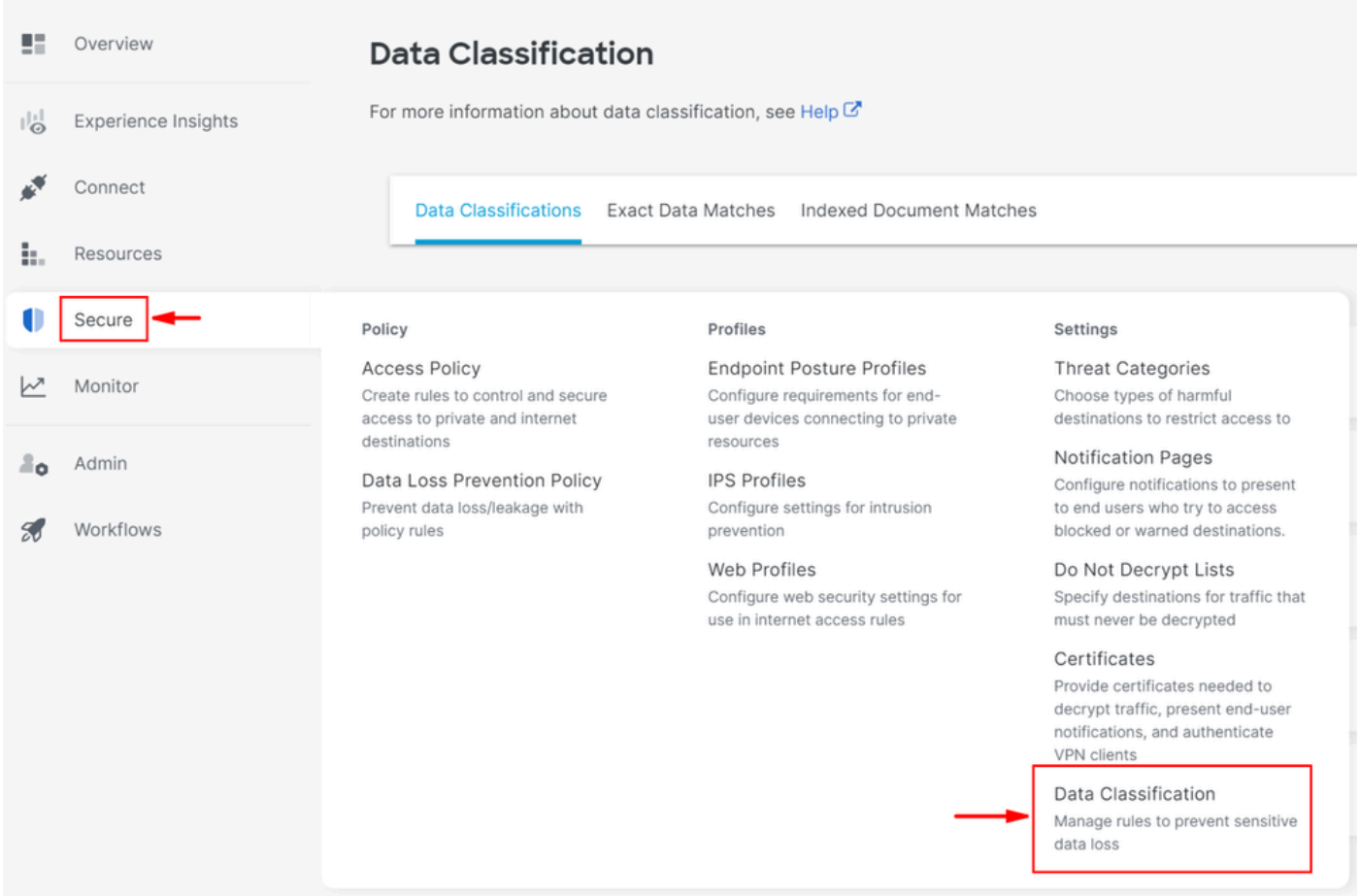
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

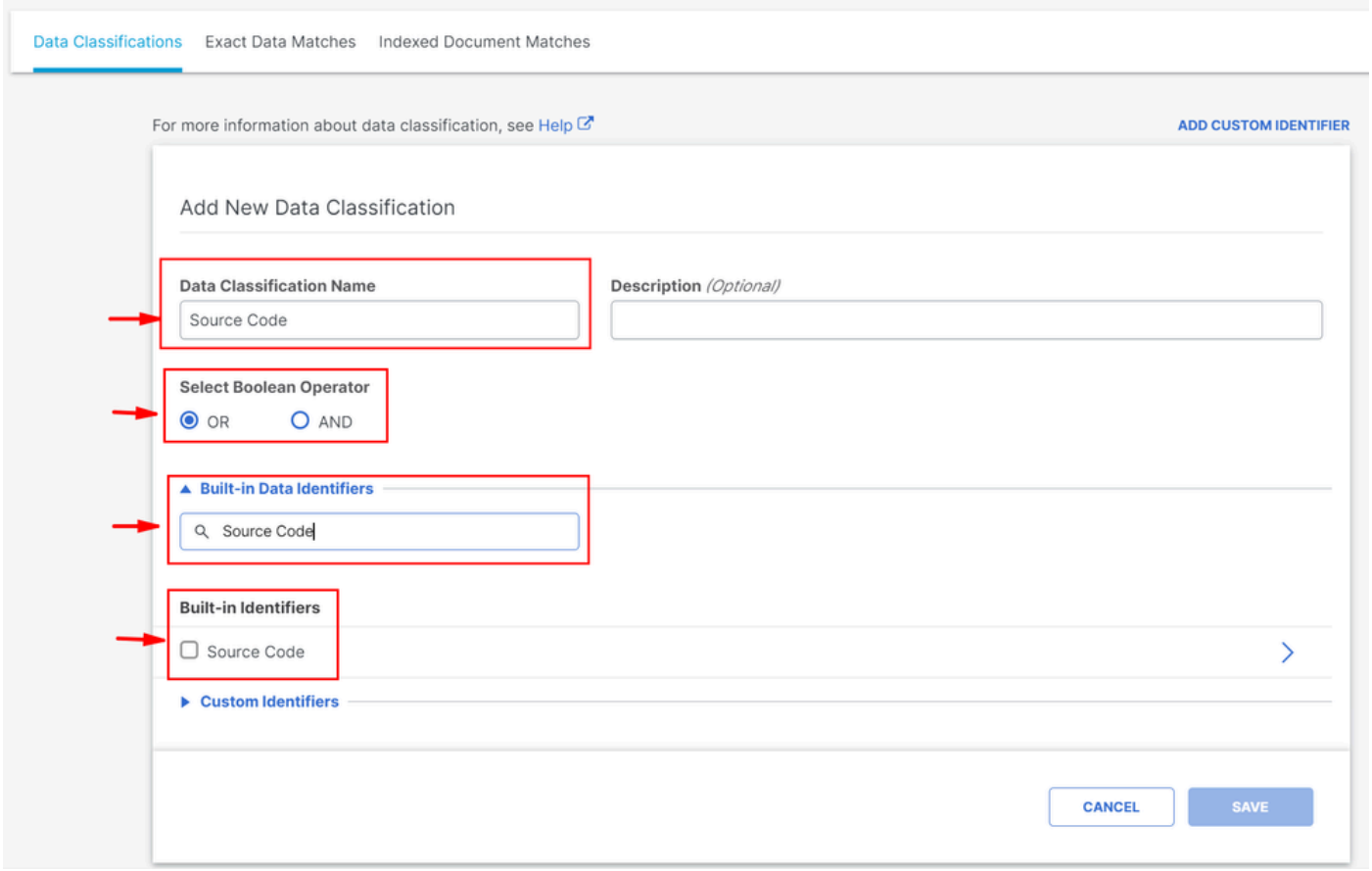
1. 创建数据分类以使用源代码数据标识符

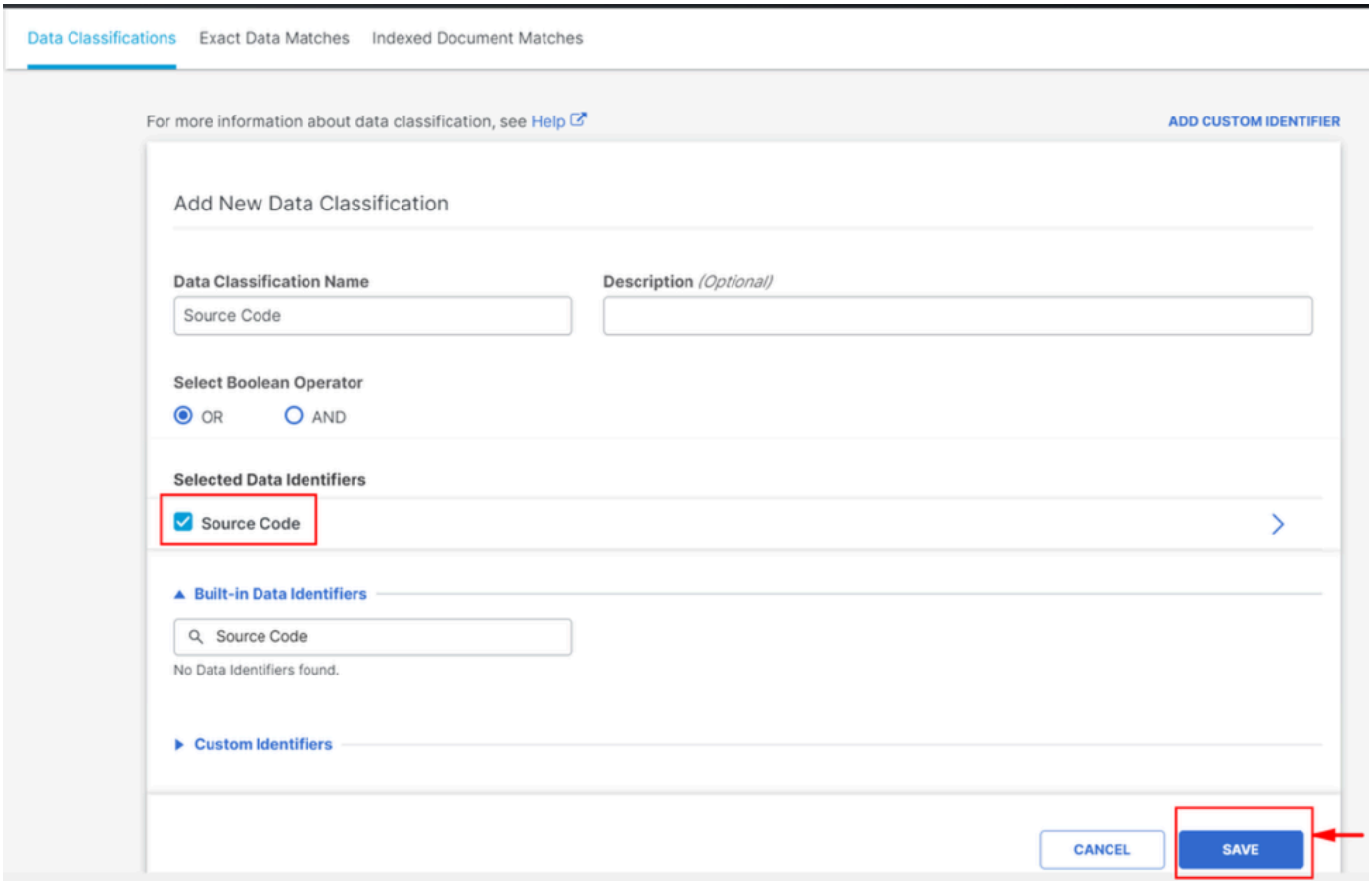
导航到[安全访问控制面板。]

- 点击Secure>>Data Classification> Add



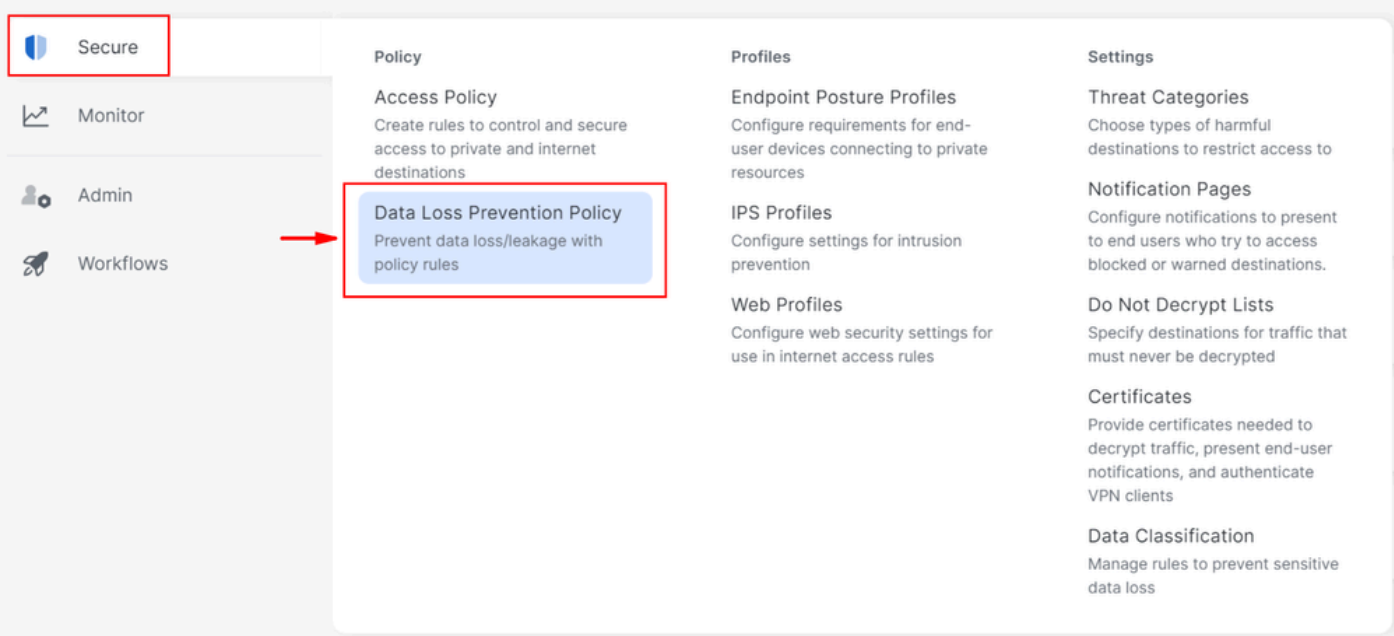
- 输入Data Classification Name>选择 Built-in Data Identifiers>搜索并选定Source Code



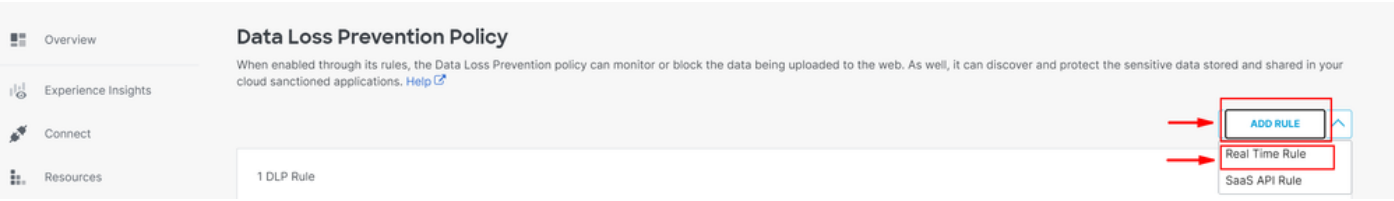


2. 创建DLP策略，并在其中调用数据分类“源代码”。

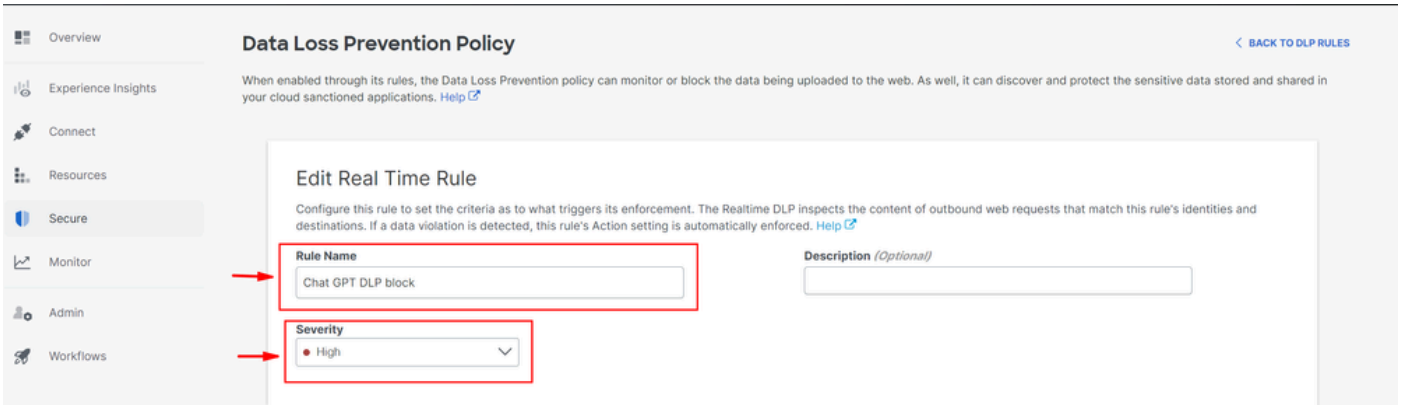
- 点击Secure> Data Loss Prevention Policy



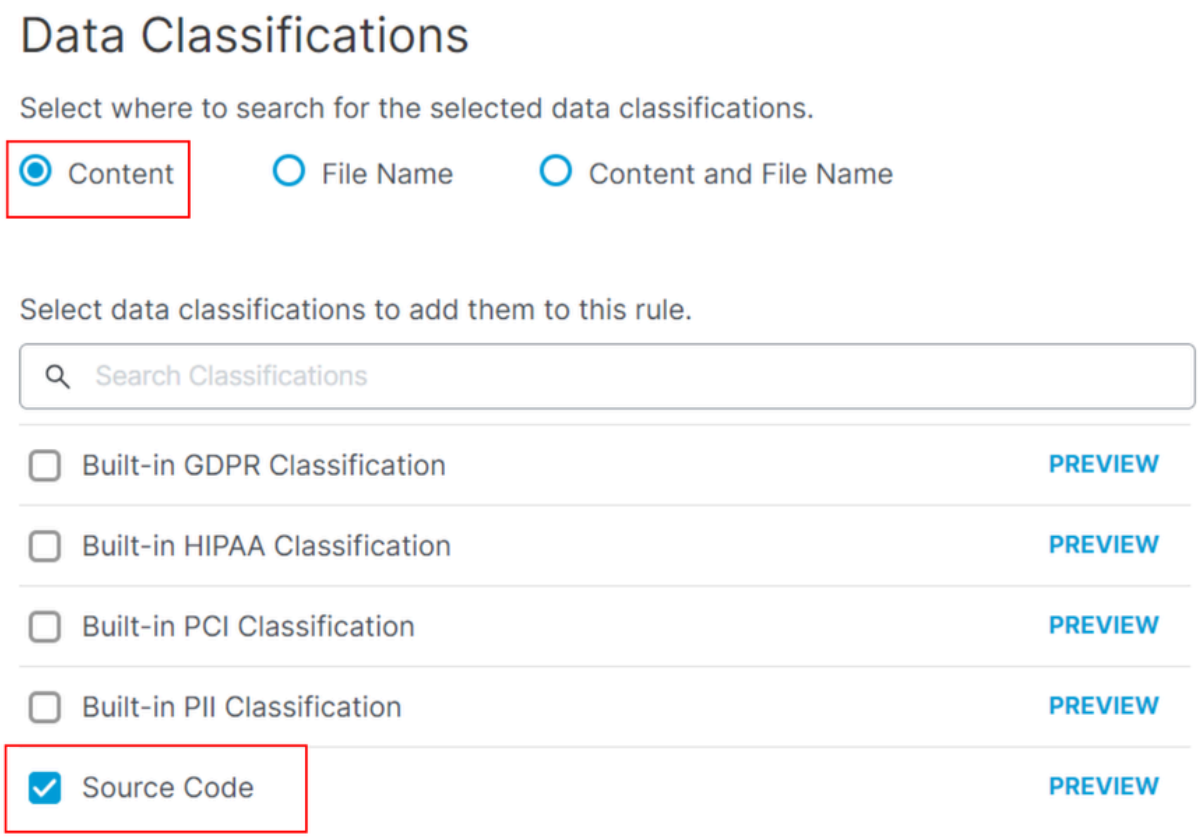
- 点击Add Rule> Real Time Rule



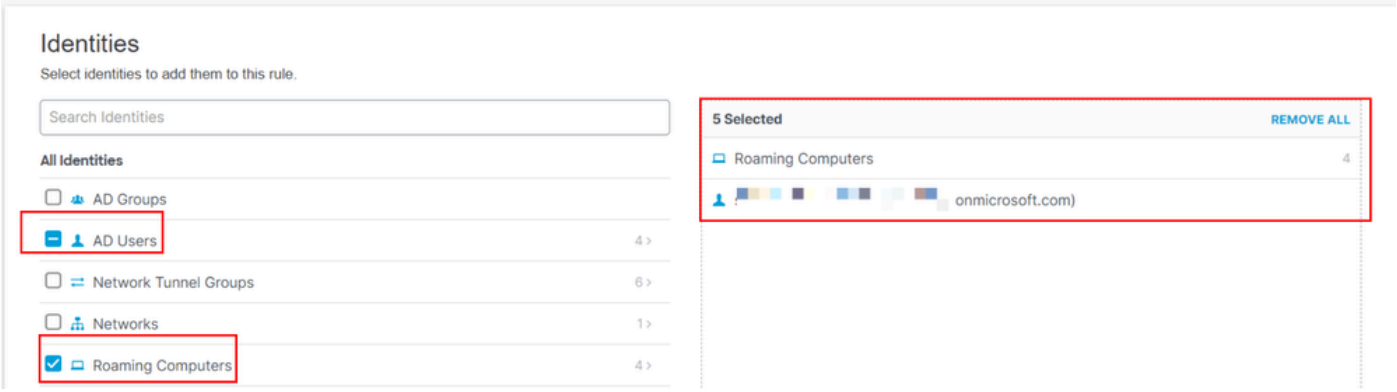
- 输入Rule Name>设置适当的 Severity



- 在Data Classifications下，选择Content Source Code

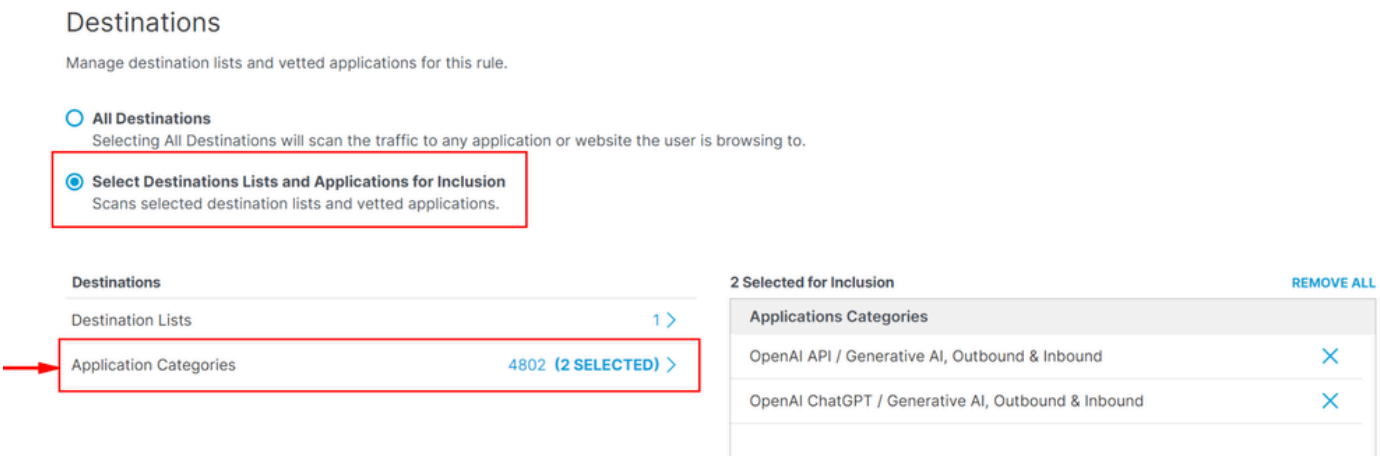


- 在Identities下，根据需要选择所需的身份

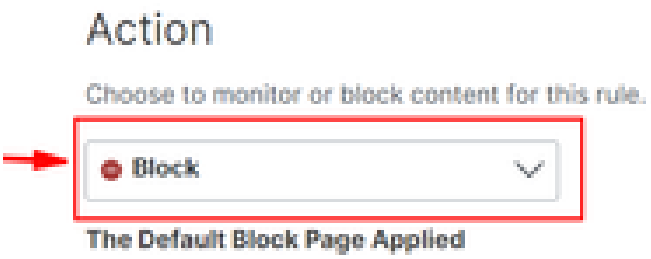


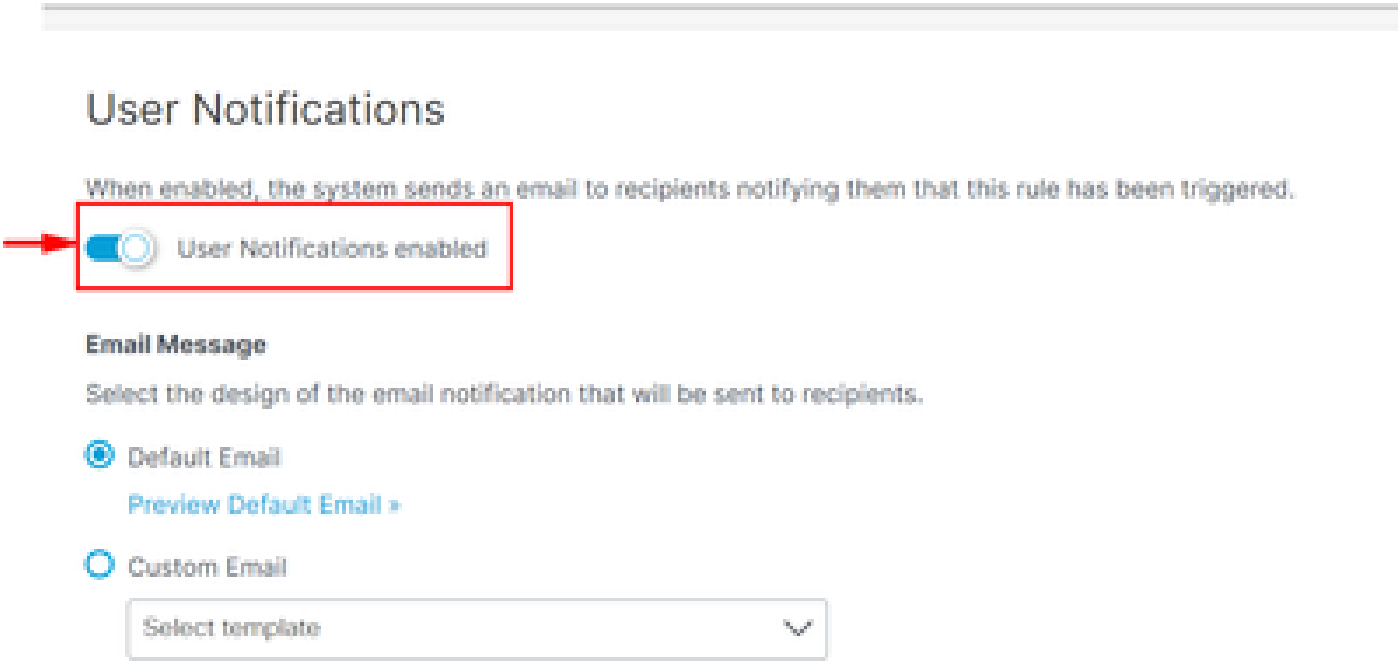
- 在Destinations下，选择 Select Destination Lists and Applications for Inclusion

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



- 在Actionselect下 Block
- 在User Notifications下，您可以在触发规则时设置发送给最终用户的邮件通知（可选）





- 点击 Save

3. 确保您对发往“聊天GPT”且已启用解密的流量拥有适当的互联网访问策略。

示例：

Chat GPT

Internet

General

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

Sources

Any

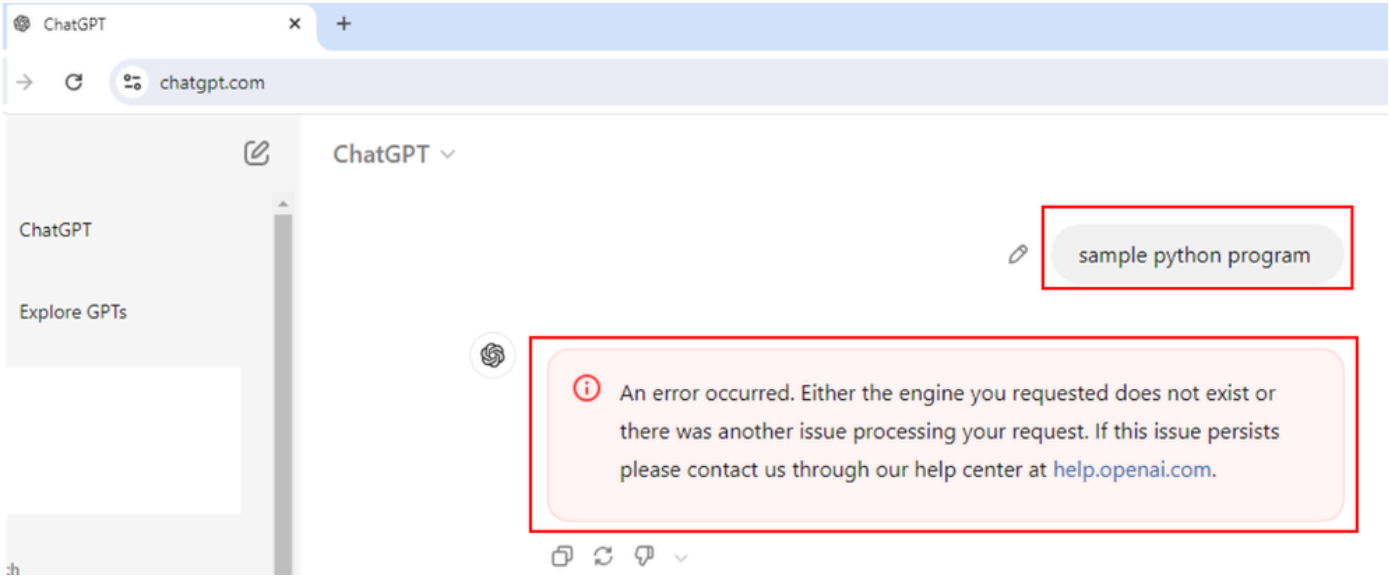
Destinations

2 destinations

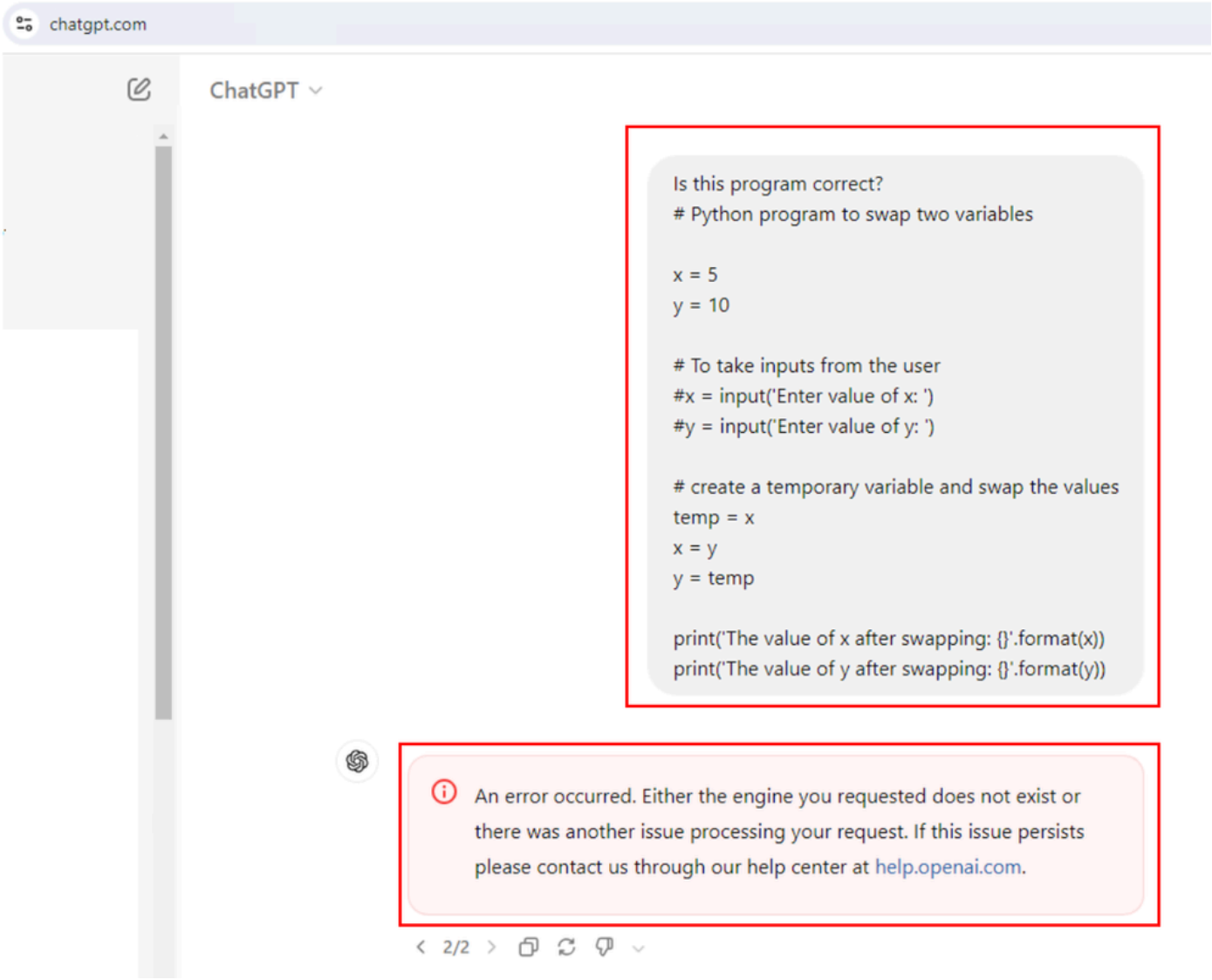
Application Settings (2)

OpenAI API OpenAI ChatGPT

- 请求一个示例python程序，此请求被阻止。



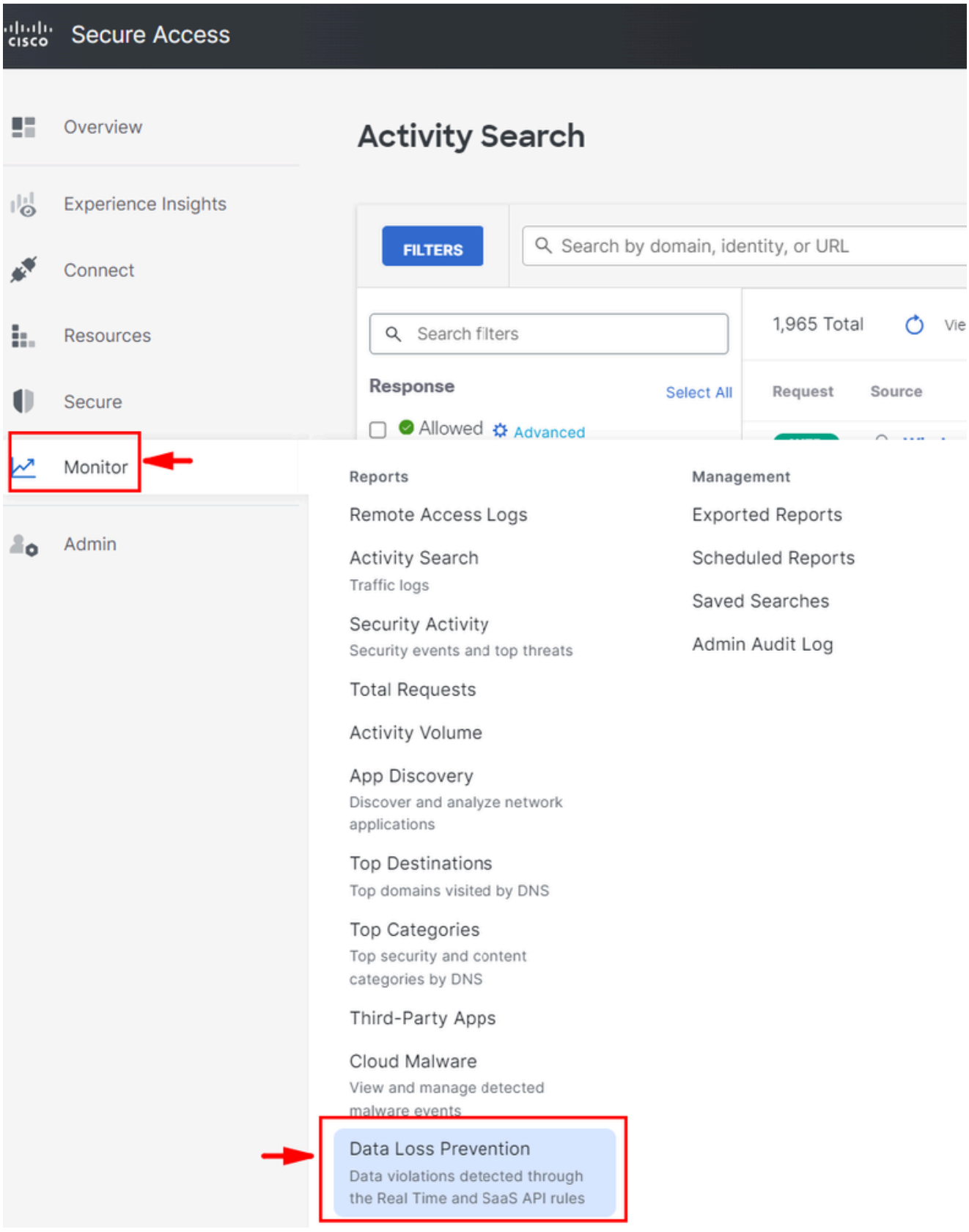
- 询问程序是否正确并阻止此请求。



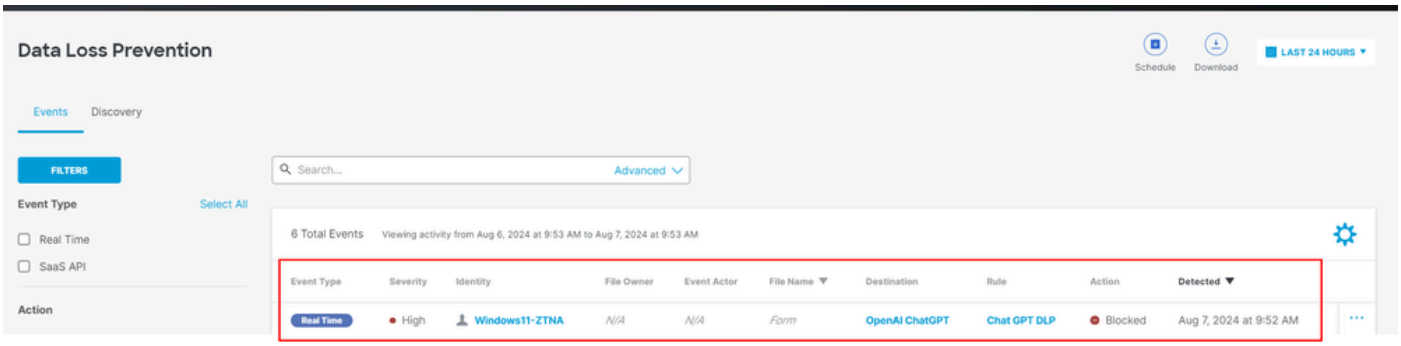
验证

我们可以看到，当用户尝试向ChatGPT请求示例python程序时，请求会被阻止。
我们可以确认安全访问防数据丢失日志中是否触发了DLP事件。

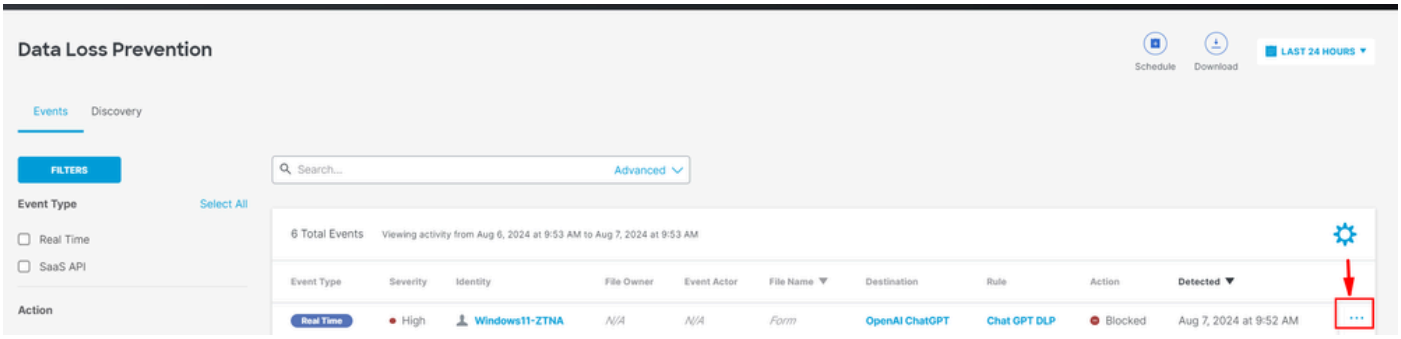
- 转至Monitor> Data Loss Prevention



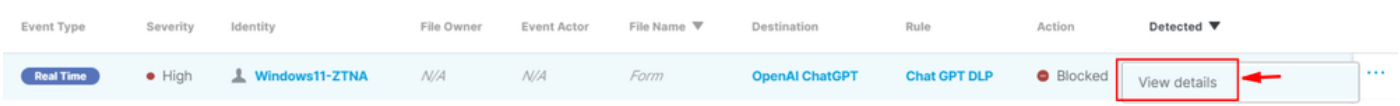
- 我们可以看到DLP事件。



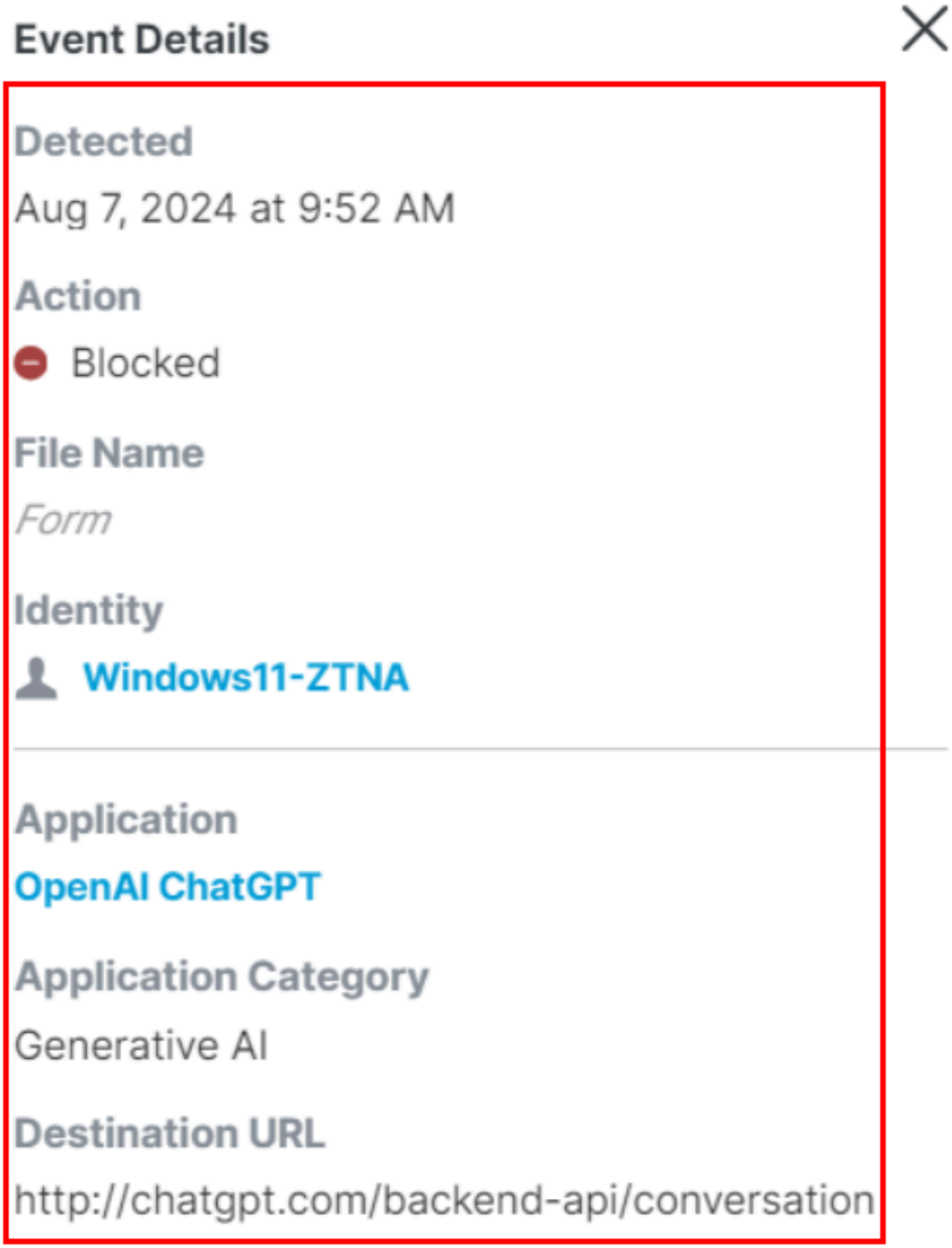
- 单击事件日志末尾的三个点，查看事件的详细信息。



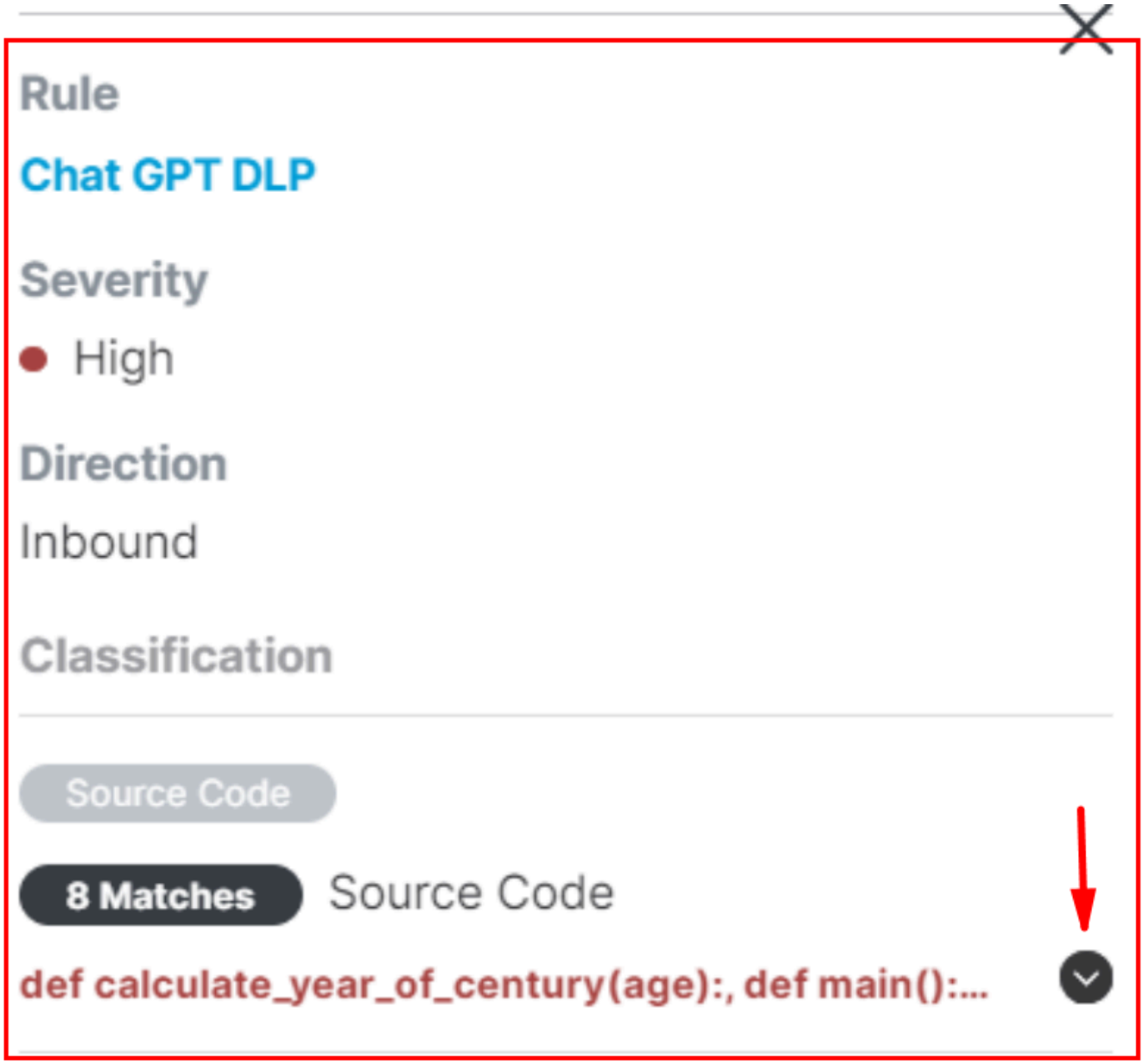
- 点击 View details.



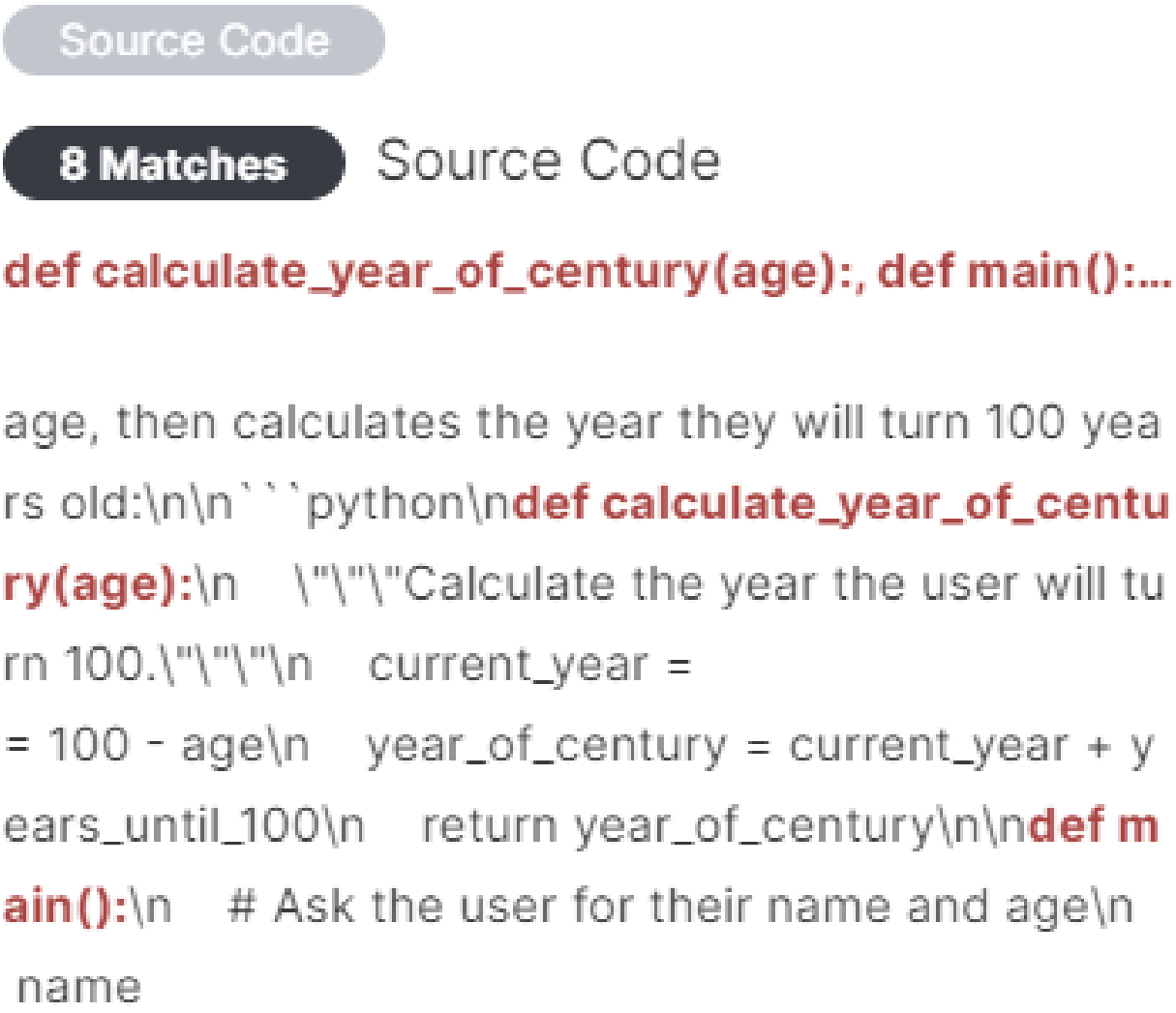
- 现在，我们可以看到整个活动详细信息。



- 展开分类以查看与分类器匹配的内容。

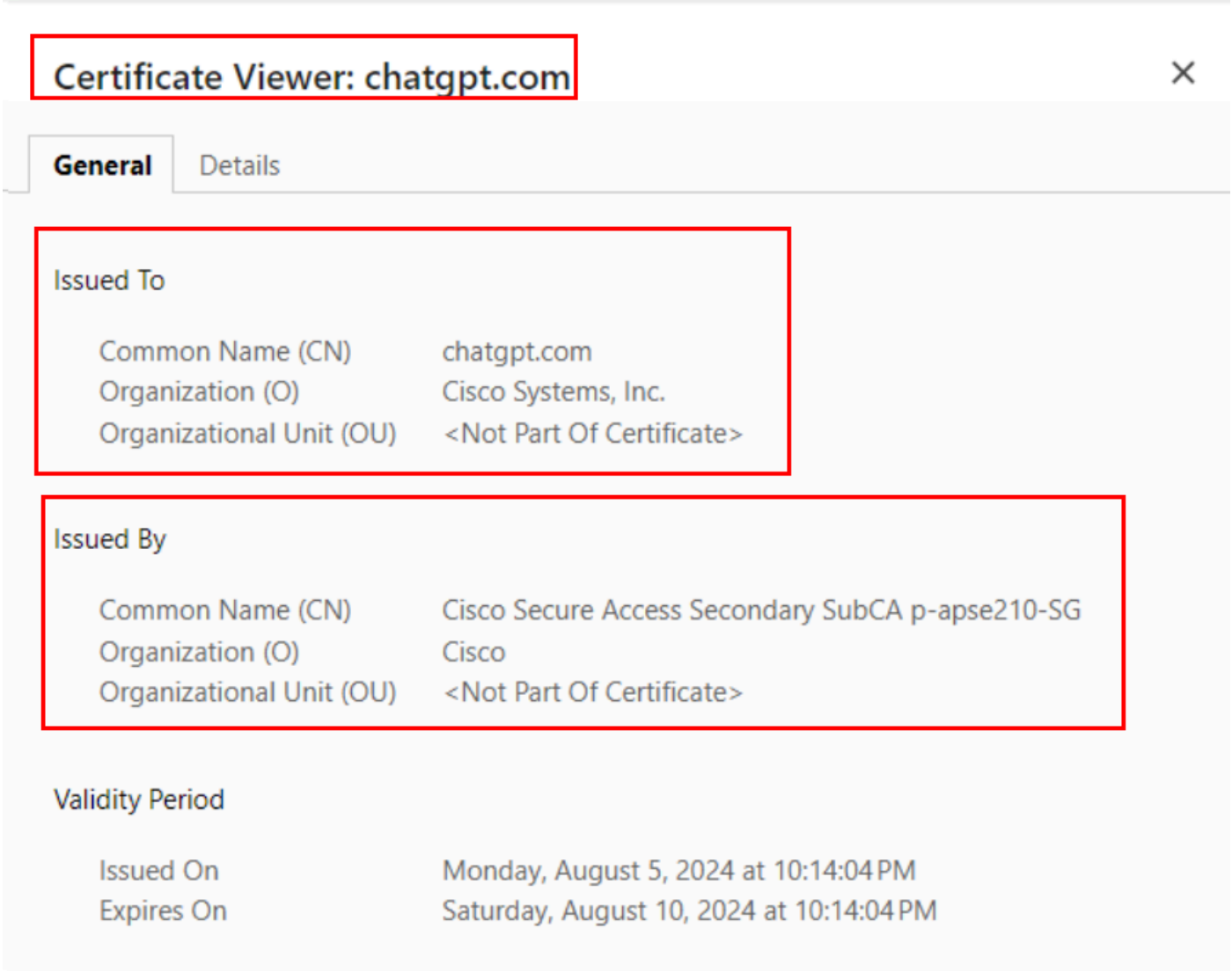


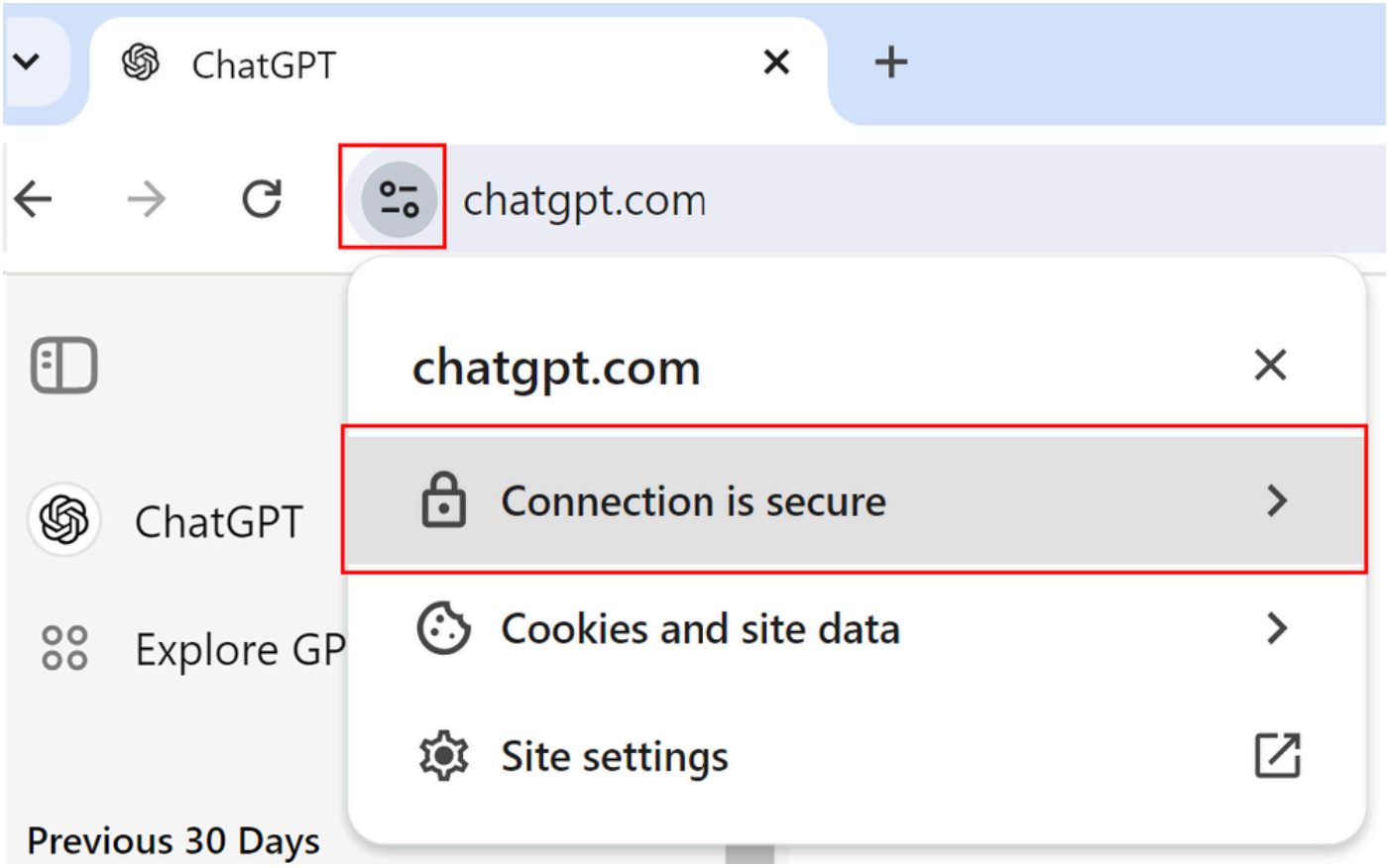
- 我们将看到匹配分类器/DLP策略分类的所有内容详细信息。

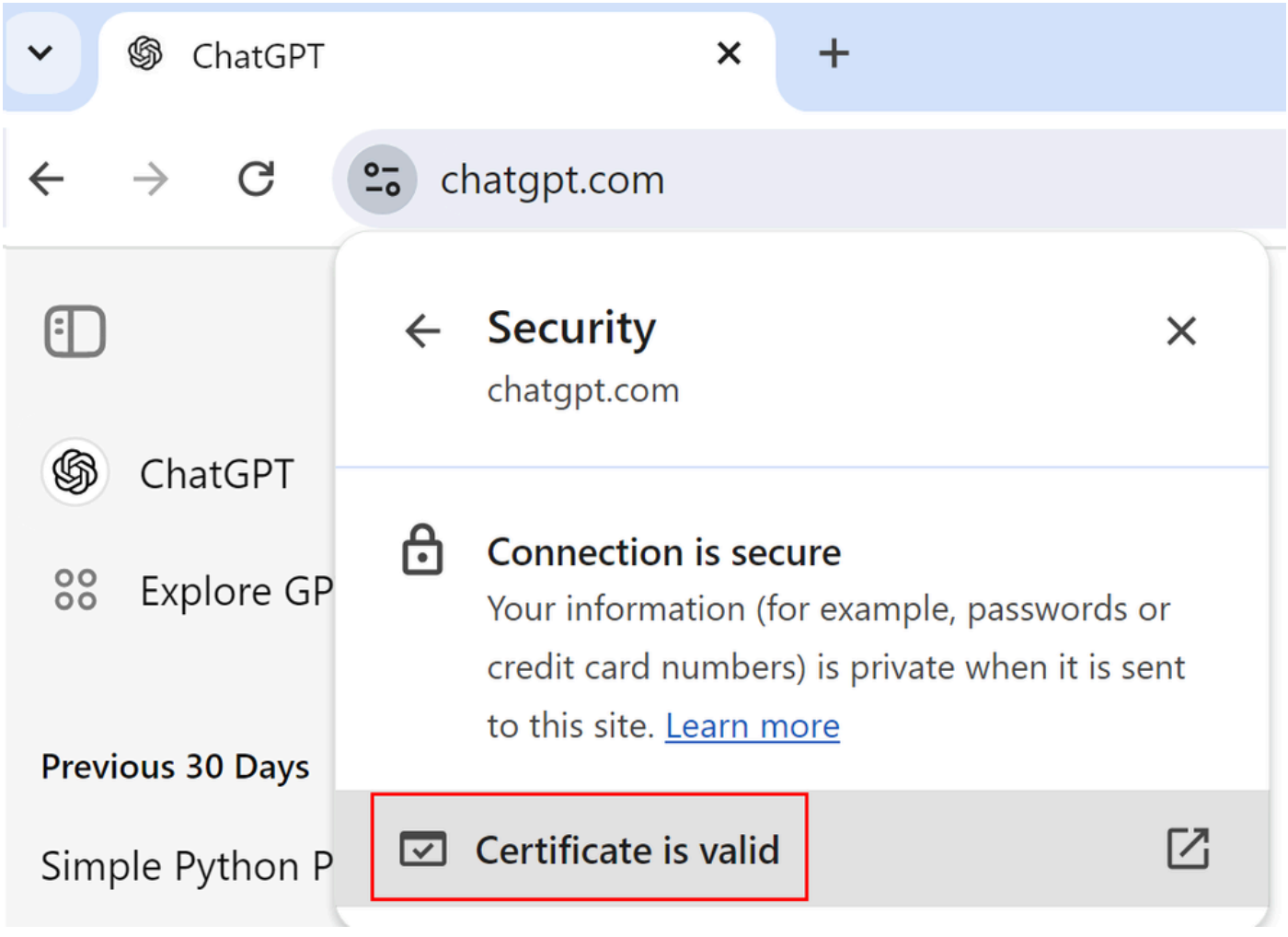


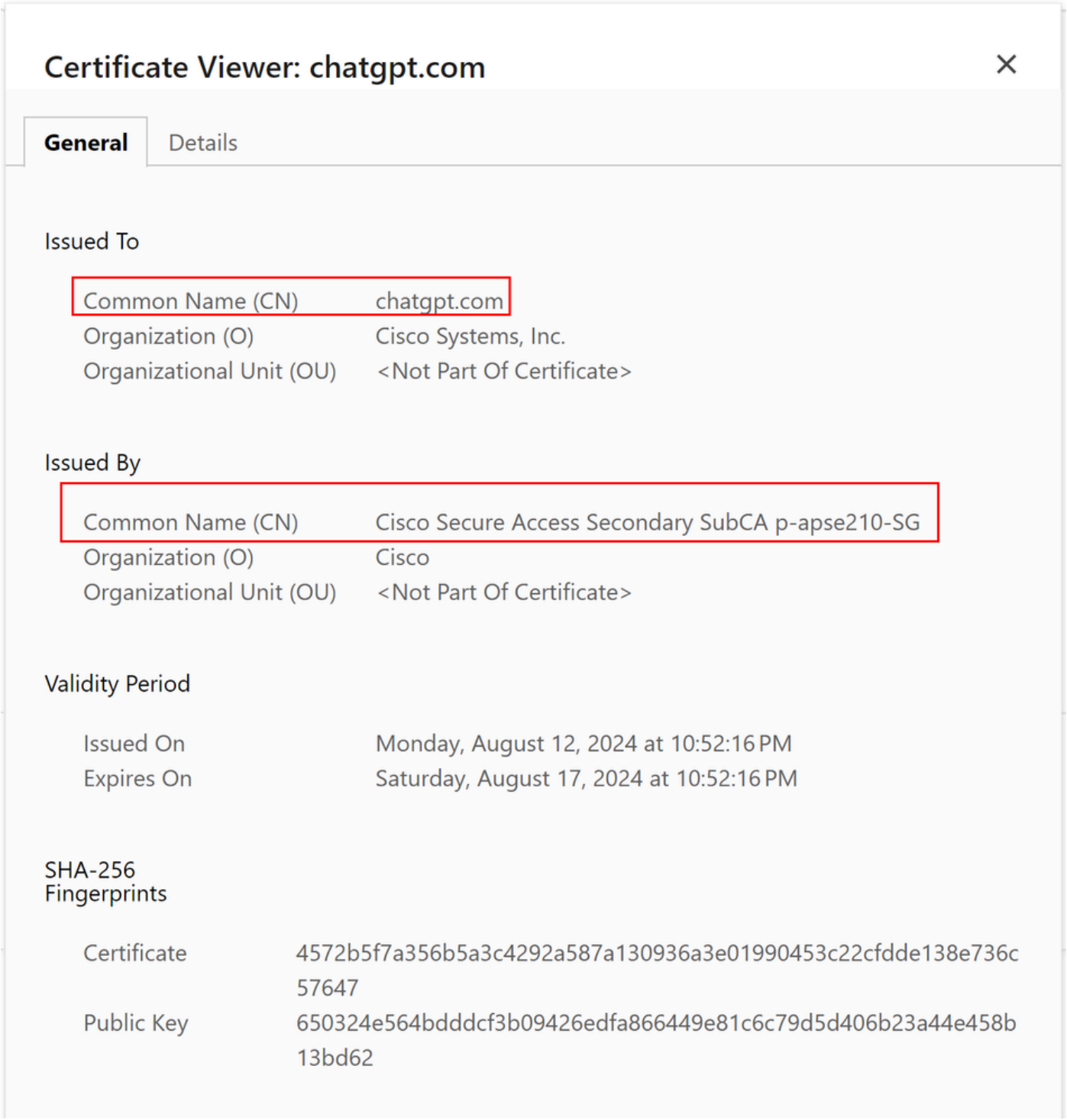
故障排除

- 确保与Open AI ChatGPT的Web请求匹配的访问策略已启用解密。
- 要快速检查SSE是否解密了Open AI ChatGPT的流量，请检查显示常用名称的网站证书，其中包含关键字“Cisco Secure Access”。

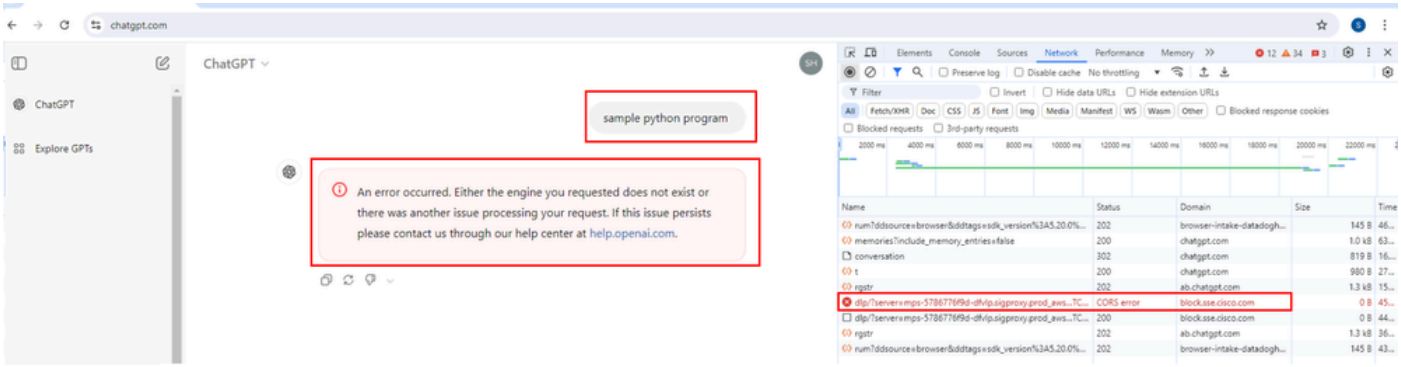

Certificate Viewer: chatgpt.com
General
Details
Issued To
Common Name (CN) chatgpt.com
Organization (O) Cisco Systems, Inc.
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) Cisco Secure Access Secondary SubCA p-apse210-SG
Organization (O) Cisco
Organizational Unit (OU) <Not 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

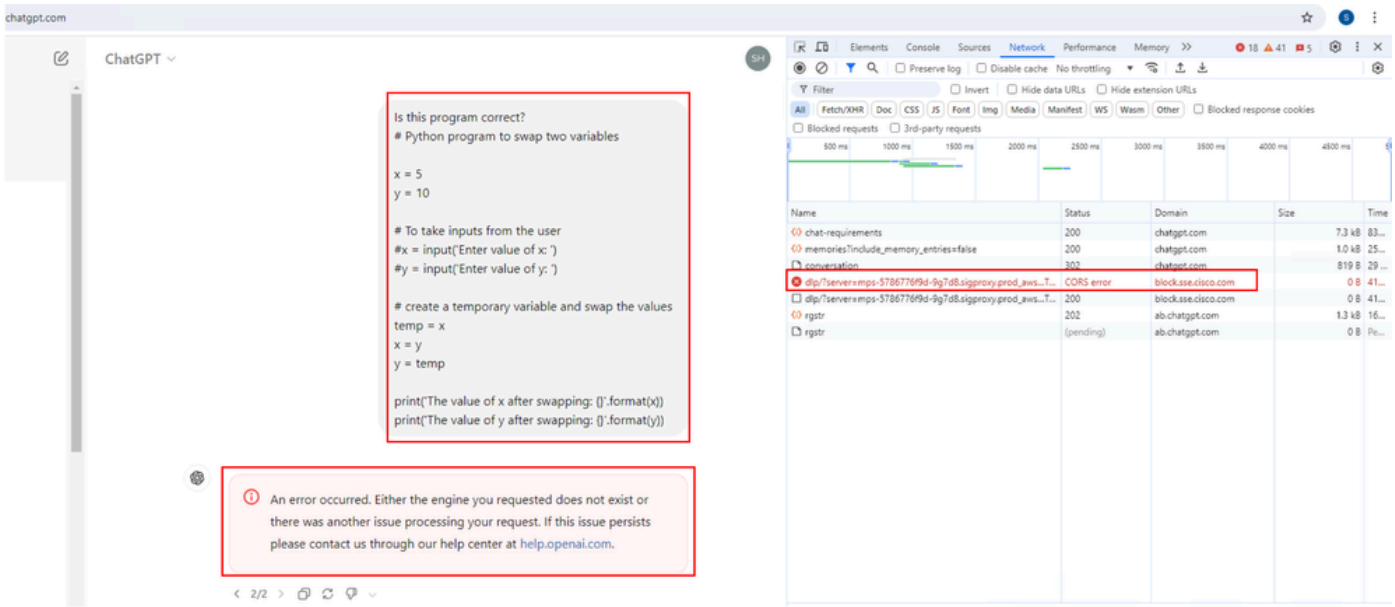

ChatGPT
chatgpt.com
Security
chatgpt.com
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more
Certificate is valid
ChatGPT
Explore GP
Previous 30 Days
Simple Python P



- 打开ChatGPT > Open developer tools > Select Network > Next to ask ChatGPT for a sample python program
- 请注意，请求会导致阻止。在域下，您可以看到“block.sse.cisco.com



- 询问ChatGPT程序代码是否正确。
- 请注意，请求会导致阻止，在“domain”下您会看到“block.sse.cisco.com”。



相关信息

- 思科安全访问用户指南
- Cisco技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。