تطبيق DLP في الوصول الآمن لتقييد إستخدام ChatGPT المفتوح للبرمجة

المحتويات

المقدمة

يوضح هذا المستند كيفية تنفيذ ميزة عن "منع فقدان البيانات (DLP)" في "الوصول الآمن" لتقييد إستخدام برنامج ChatGPT المفتوح للدردشة عبر برتوكول الإنترنت (AI) للبرمجة والترميز.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الوصول الآمن
- DLP
- فتح AI ChatGPT

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الوصول الآمن
- DLP
- فتح AI ChatGPT

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

1.إنشاء تصنيف بيانات للاستخدام معرف بيانات كود المصدر

انتقل إلى <u>لوحة معلومات الوصول الآمن.</u>

- انقر فوق Secure > Data Classification > Add

- أدخل Data Classification Name > تحديد Built-in Data Identifiers > البحث عن Source Code وحدده

For more information about data classification, see Help ↗   ADD CUSTOM IDENTIFIER

Add New Data Classification

Data Classification Name   **Description** *(Optional)*

Source Code

Select Boolean Operator

⊙ OR   ○ AND

▲ **Built-in Data Identifiers**

🔍 Source Code

Built-in Identifiers

☐ Source Code   ⟩

▶ **Custom Identifiers**

CANCEL   SAVE

Selected Data Identifiers

☑ Source Code   ⟩

▲ **Built-in Data Identifiers**

🔍 Source Code

No Data Identifiers found.

▶ **Custom Identifiers**

CANCEL   SAVE

2.إنشاء سياسة DLP واستدعاء تصنيف البيانات "كود المصدر" فيها.

- انقر فوق Secure > Data Loss Prevention Policy
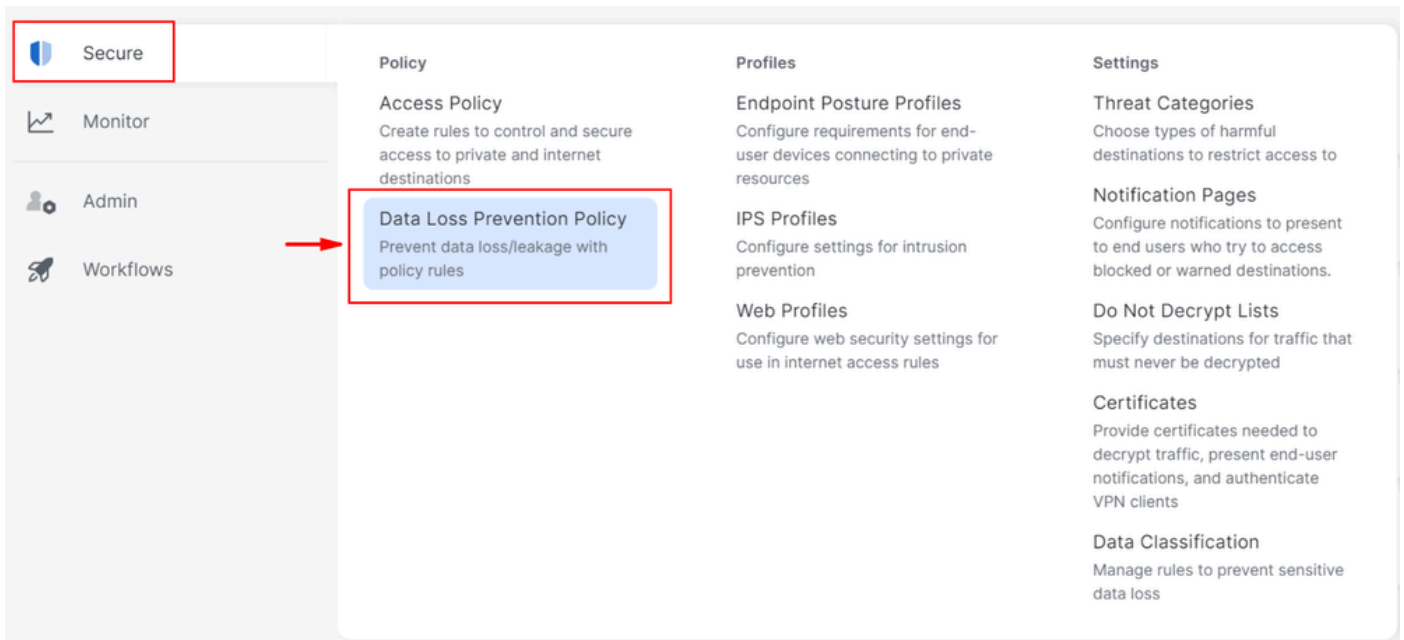
- انقر فوق Add Rule > Real Time Rule
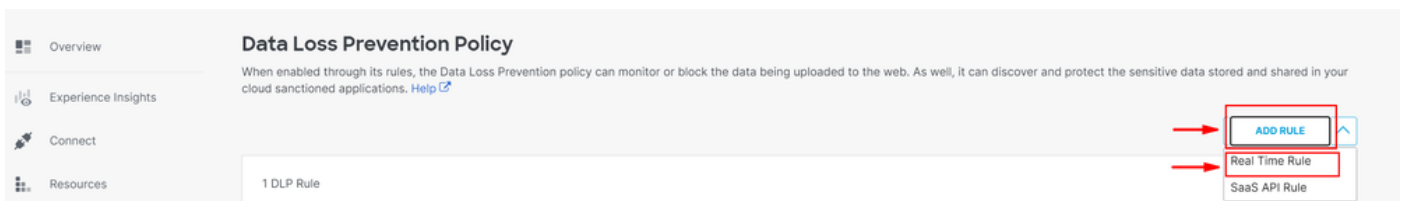
- توفير Severity تعيين مناسب > Rule Name
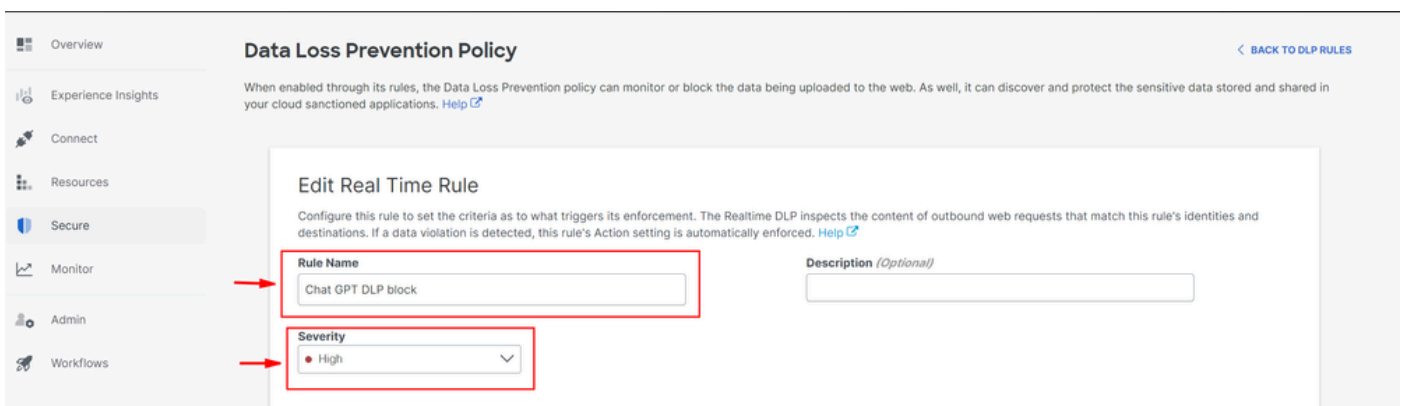
- تحت تحديدData Classifications Content وتحديد Source Code

Data Classifications

Select where to search for the selected data classifications.

- ⦿ Content   ◯ File Name   ◯ Content and File Name

Select data classifications to add them to this rule.

🔍 Search Classifications

☐ Built-in GDPR Classification	PREVIEW
☐ Built-in HIPAA Classification	PREVIEW
☐ Built-in PCI Classification	PREVIEW
☐ Built-in PII Classification	PREVIEW
☑ Source Code	PREVIEW

- تحت Identitiesتحديد الهويات المطلوبة حسب الطلب

Identities

Select identities to add them to this rule.

Search Identities

All Identities

			5 Selected	REMOVE ALL
☐ 👥 AD Groups			🖥 Roaming Computers	4
⊟ 👤 AD Users	4 ›		👤 ▮▮▮▮ ▮▮ ▮▮ ▮▮ onmicrosoft.com)	
☐ ⇄ Network Tunnel Groups	6 ›			
☐ 🔗 Networks	1 ›			
☑ 🖥 Roaming Computers	4 ›			

- تحت الوجهات حدد Select Destination Lists and Applications for Inclusion

- حدد Application Categories> حدد Generative AI > تحديد OpenAI API (Vetted) وفيOpenAI ChatGPT (Vetted) Outbound and InboundDirection

Destinations

Manage destination lists and vetted applications for this rule.

○ **All Destinations**
Selecting All Destinations will scan the traffic to any application or website the user is browsing to.

◉ **Select Destinations Lists and Applications for Inclusion**
Scans selected destination lists and vetted applications.

Destinations		2 Selected for Inclusion	REMOVE ALL
Destination Lists	1 >	**Applications Categories**	
Application Categories	4802 **(2 SELECTED)** >	OpenAI API / Generative AI, Outbound & Inbound	✕
		OpenAI ChatGPT / Generative AI, Outbound & Inbound	✕

- • تحت Action تحديد Block

- • تحت User Notifications، يمكنك إعداد إعلامات البريد الإلكتروني للمستخدمين النهائيين، عند تشغيل القاعدة (اختياري)

Action

Choose to monitor or block content for this rule.

⬤ Block ⌄

The Default Block Page Applied

User Notifications

When enabled, the system sends an email to recipients notifying them that this rule has been triggered.

[◉] User Notifications enabled

Email Message

Select the design of the email notification that will be sent to recipients.

◉ Default Email

Preview Default Email »

○ Custom Email

Select template ⌄

- انقر فوق Save

3.تأكد من وجود منهج وصول إلى الإنترنت لحركة المرور نحو Chat GPT مع تمكين فك التشفير.

مثال:

Chat GPT

×

`Internet`

General

Action	✓ Allow
Last modified	▮ ▬ ▮ ▮ ▬ ▮ ▬
Rule order	1
Logging	Enabled
Hits	216

Sources

Any

Destinations

2 destinations

∧

Application Settings (2)

`OpenAI API`　`OpenAI ChatGPT`

- اطلب برنامج معين بلغة بايثون وهذا الطلب يتم حظره.

- أسأل إذا كان البرنامج صحيحا أم لا، ويتم حظر هذا الطلب.

التحقق من الصحة

يمكننا ملاحظة أنه عندما يحاول المستخدم طلب ChatGPT لعينة من برنامج python، يتم حظر الطلب. يمكننا تأكيد تشغيل حدث DLP في سجلات منع فقدان بيانات الوصول الآمن.

- الانتقال إلى Monitor> Data Loss Prevention

- يمكننا رؤية حدث DLP.

- انقر فوق النقاط الثلاث في نهاية سجل الأحداث للتحقق من الحصول على مزيد من التفاصيل حول الحدث.

- انقر فوق View details.

- الآن نشاهد تفاصيل الحدث بأكمله.

Event Details

✕

Detected

Aug 7, 2024 at 9:52 AM

Action

🔴 Blocked

File Name

Form

Identity

👤 **Windows11-ZTNA**

Application

OpenAI ChatGPT

Application Category

Generative AI

Destination URL

http://chatgpt.com/backend-api/conversation

- قم بتوسيع التصنيف لمعرفة المحتوى الذي يتطابق مع المصنف.

Rule

Chat GPT DLP

Severity

● High

Direction

Inbound

Classification

Source Code

8 Matches   Source Code

def calculate_year_of_century(age):, def main():...

- إننا نرى جميع تفاصيل المحتوى التي تتطابق مع مصنف / تصنيف سياسة DLP.

8 Matches Source Code

def calculate_year_of_century(age):, def main():...

age, then calculates the year they will turn 100 yea
rs old:\n\n```python\n**def calculate_year_of_centu**
ry(age):\n   \"\"\"Calculate the year the user will tu
rn 100.\"\"\"\n   current_year =
= 100 - age\n   year_of_century = current_year + y
ears_until_100\n   return year_of_century\n\n**def m**
ain():\n   # Ask the user for their name and age\n
 name

اكتشاف الأخطاء وإصلاحها

- تأكد من تمكين فك التشفير لنهج الوصول الذي يطابق طلبات الويب ل Open AI ChatGPT.

- للتحقق بسرعة مما إذا كان SSE موقع فك تشفير حركة مرور البيانات ل Open AI ChatGPT، تحقق من شهادة موقع الويب الذي يظهر الاسم الشائع يتضمن كلمات أساسية "Cisco Secure Access" في.

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

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

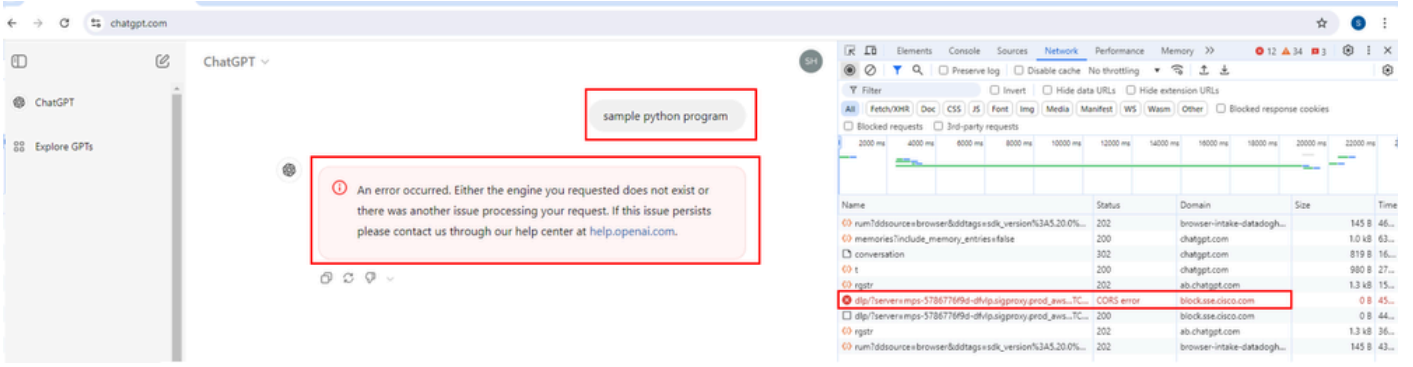|	
Common Name (CN)	Cisco Secure Access Secondary SubCA p-apse210-SG
Organization (O)	Cisco
Organizational Unit (OU)	\<Not Part Of Certificate\>

Validity Period

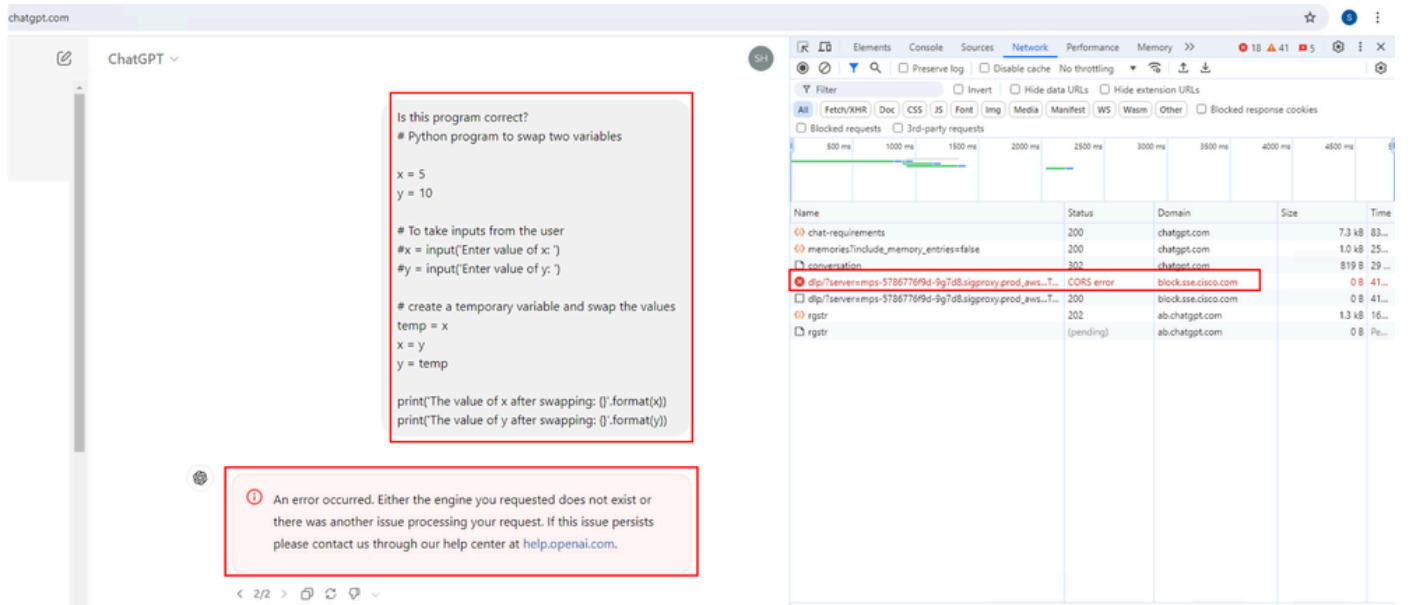|	
Issued On	Monday, August 12, 2024 at 10:52:16 PM
Expires On	Saturday, August 17, 2024 at 10:52:16 PM

SHA-256 Fingerprints

Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e736c 57647
Public Key	650324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e458b 13bd62

- افتح ChatGPT > افتح أدوات المطور > تحديد الشبكة > التالي محاولة طلب ChatGPT لعينة من برنامج python

- لاحظ أن الطلب ينتج عنه كتلة. تحت المجال مشاهدة block.sse.cisco.com

- أسأل ChatGPT ما اذا كان رمز البرنامج صحيحا.

- لاحظ أن الطلب ينتج عنه كتلة وتحت "domain"، يمكنك الاطلاع على "block.sse.cisco.com".

معلومات ذات صلة

- [دليل مستخدم Cisco Secure Access](#)

- [الدعم الفني والتنزيلات من Cisco](#)

حول هذه الترجمة

ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية
والبشرية لتقديم دعم للمستخدمين في جميع أنحاء العالم
بغلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما
هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco
Systems مسؤوليتها عن دقة هذه الترجمات وتوصي بالرجوع دائمًا إلى
المستند الإنجليزي الأصلي (الرابط متوفر).