# Implementierung von DLP in Secure Access zur Beschränkung der Verwendung von Open Al ChatGPT für die Programmierung

### Inhalt

 Einleitung

 Voraussetzungen

 Anforderungen

 Verwendete Komponenten

 Konfigurieren

 1.Erstellen einer Datenklassifizierung zur Verwendung der Quellcodedaten-ID

 2. Erstellen Sie eine SvD-Policy, und rufen Sie die Datenklassifizierung als "Quellcode" auf.

 3. Stellen Sie sicher, dass Sie über eine Internet-Zugangsrichtlinie für den Datenverkehr in Richtung Chat-GPT mit aktivierter Entschlüsselung verfügen.

 i.Using Open AI ChatGPT versuchen, jedes Programm herunterzuladen oder hochzuladen.

 Überprüfung

 Eehlerbehebung

 Zugehörige Informationen

## Einleitung

In diesem Dokument wird beschrieben, wie Data Loss Prevention (DLP) in Secure Access implementiert wird, um die Verwendung von Open AI ChatGPT für Programmierung und Codierung einzuschränken.

### Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sicherer Zugriff
- SvD
- AI-ChatGPT öffnen

#### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

• Sicherer Zugriff

- SvD
- AI-ChatGPT öffnen

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

### Konfigurieren

### 1. Erstellen einer Datenklassifizierung zur Verwendung der Quellcodedaten-ID

Navigieren Sie zum Dashboard für sicheren Zugriff.

• Klicken Sie auf Secure > Data Classification > Add

	Overview	Data Classification		
	Experience Insights	For more information about data cla	ssification, see Help 🗗	
**	Connect	Data Classifications Exact D	ata Matches Indexed Document Matche	es
<b>i</b>	Resources			
U	Secure	Policy	Profiles	Settings
	Monitor	Access Policy Create rules to control and secure access to private and internet	Endpoint Posture Profiles Configure requirements for end- user devices connecting to private	Threat Categories Choose types of harmful destinations to restrict access to
<b>2</b> 0	Admin Workflows	destinations Data Loss Prevention Policy Prevent data loss/leakage with policy rules	resources IPS Profiles Configure settings for intrusion prevention	Notification Pages Configure notifications to present to end users who try to access blocked or warned destinations.
			Web Profiles Configure web security settings for use in internet access rules	Do Not Decrypt Lists Specify destinations for traffic that must never be decrypted
				Certificates Provide certificates needed to decrypt traffic, present end-user notifications, and authenticate VPN clients
				Data Classification Manage rules to prevent sensitive data loss

Geben Sie Data Classification Name > Select Built-in Data Identifiers > Search for Source Code ein, und wählen Sie es aus.

1	For more information about data classification, see Help 다	ADD CUSTOM IDENTIFIE
	Add New Data Classification	
-	Data Classification Name     Description (Optional)       Source Code	
-	Select Boolean Operator          Image: Organ select Boolean Operator         Image: Organ select Boolean Operator	
-	Built-in Data Identifiers      Q Source Code	
	Built-in Identifiers	
-	Source Code	>
	Custom Identifiers	

Data Classificati	ons Exact Data Matches Indexed Document Matches		
	For more information about data classification, see Help 🕜		ADD CUSTOM IDENTIFIER
	Add New Data Classification		
	Data Classification Name         Source Code         Select Boolean Operator         Image: OR       AND	Description (Optional)	
	Selected Data Identifiers		>
	Built-in Data Identifiers Q. Source Code No Data Identifiers found. Custom Identifiers		
		C/	

2. Erstellen Sie eine SvD-Policy, und rufen Sie die Datenklassifizierung als "Quellcode" auf.

Klicken Sie auf Secure > Data Loss Prevention Policy

U	Secure	Policy	Profiles	Settings
	Monitor	Access Policy Create rules to control and secure	Endpoint Posture Profiles Configure requirements for end- user devices connection to private	Threat Categories Choose types of harmful destinations to restrict access to
<b>2</b> 0 X	Admin Workflows	destinations  Data Loss Prevention Policy Prevent data loss/leakage with policy rules	IPS Profiles Configure settings for intrusion prevention	Notification Pages Configure notifications to present to end users who try to access blocked or warned destinations.
			Web Profiles Configure web security settings for use in internet access rules	Do Not Decrypt Lists Specify destinations for traffic that must never be decrypted
				Certificates Provide certificates needed to decrypt traffic, present end-user notifications, and authenticate VPN clients
				Data Classification Manage rules to prevent sensitive data loss

• Klicken Sie auf Add Rule > Real Time Rule

	Overview	Data Loss Prevention Policy When eaching the rate, the Data Loss Prevention policy are provided as the data being unleaded to the web. As well, it can discover and protect the sensitive data stored and shared in your
+  ©	Experience Insights	vinier enabled introgen is rules, the bala Loss Prevention policy can monitor or block the data being optioaded to the web, As weil, it can discover and protect the sensitive data stored and shared in your cloud sanctioned applications. Help 🕈
s.v	Connect	
<b>i</b>	Resources	1 DLP Rule SaaS API Rule

• Geben Sie ein Rule Name > Festlegen der entsprechenden Severity

53	Overview	Data Loss Prevention Policy	ACK TO DLP RULES						
+  Ø	Experience Insights	When enabled through its rules, the Data Loss Prevention policy can monitor or block the data being uploaded to the web. As well, it can discover and protect the sensitive data stored and shared in your cloud sanctioned applications. Help 🕜							
**	Connect								
iı.	Resources	Edit Real Time Rule							
U	Secure	Configure this rule to set the criteria as to what triggers its enforcement. The Realtime DLP inspects the content of outbound web requests that match this rule's identities and destinations. If a data violation is detected, this rule's Action setting is automatically enforced. Help ổ	1						
Ŀ	Monitor	Rule Name Description (Optional) Chat GPT DLP block							
20	Admin	Severity							
A	Workflows	High							

• Wählen Data Classifications Sie unter Content und Source Code

## Data Classifications

Select where to search for the selected data classifications.

Ontent

O File Name

O Content and File Name

#### Select data classifications to add them to this rule.

Q 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

• Wählen Sie bei Bedarf die gewünschten Identitäten Identitiesaus

Identities Select identities to add them to this rule.	
Search Identities	5 Selected REMOVE ALL
All Identities	Roaming Computers
AD Groups	1 Point onmicrosoft.com)
AD Users 4>	
C = Network Tunnel Groups 6>	
h Networks	
Roaming Computers 4>	

• Wählen Sie unter Ziele Select Destination Lists and Applications for Inclusion

• Auswählen Application Categories> Auswählen Generative AI > Auswählen OpenAI API (Vetted) und OpenAI ChatGPT (Vetted) in Outbound and InboundDirection

#### Destinations

Manage destination lists and vetted applications for this rule.

	<ul> <li>All Destinations Selecting All Destinations will scan the traffic to any app</li> <li>Select Destinations Lists and Applications for Inclusion Scans selected destination lists and vetted applications</li> </ul>	plication or website the user n	is b	rowsing to.	
	Destinations			2 Selected for Inclusion	REMOVE ALL
	Destination Lists	1>		Applications Categories	
	Application Categories	4802 (2 SELECTED) >		OpenAl API / Generative Al, Outbound & Inbound	×
ı				OpenAl ChatGPT / Generative Al, Outbound & Inbound	×

Unter ActionAuswählen Block

• Unter User Notifications können Sie E-Mail-Benachrichtigungen an Endbenutzer einrichten, wenn die Regel ausgelöst wird (optional)

### Action

Choose to monitor or block content for this rule.



### User Notifications

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



#### Email Message

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

Default Email
 Preview Default Email >
 Custom Email

Select template

Klicken Sie Save



3. Stellen Sie sicher, dass Sie über eine Internet-Zugangsrichtlinie für den Datenverkehr in Richtung Chat-GPT mit aktivierter Entschlüsselung verfügen.

**Beispiel:** 

Chat GPT	$\times$
Internet	
General	
Action	Allow
Last modified	
Rule order	1
Logging	Enabled
Hits	216
Sources Any	
<b>Destinations</b> 2 destinations	^
Application Settings	(2)
OpenALAPI Open	AI ChatGPT

• Fragen Sie nach einem Python-Beispielprogramm, und diese Anfrage wird blockiert.



Fragen Sie, ob das Programm korrekt ist und diese Anfrage blockiert wird.

### 25 chatgpt.com CC, ChatGPT ~ Is this program correct? # Python program to swap two variables x = 5 y = 10 # To take inputs from the user #x = input('Enter value of x: ') #y = input('Enter value of y: ') # create a temporary variable and swap the values temp = xx = y y = temp print('The value of x after swapping: {}'.format(x)) print('The value of y after swapping: {}'.format(y)) \$ (i) An error occurred. Either the engine you requested does not exist or there was another issue processing your request. If this issue persists please contact us through our help center at help.openai.com. < 2/2 > 凸 C ワ ~

Überprüfung

Wenn ein Benutzer versucht, ChatGPT nach einem Python-Beispielprogramm zu fragen, wird die Anfrage blockiert. Wir können bestätigen, dass in den Protokollen zum Schutz vor Datenverlust für sicheren Zugriff ein SvD-Ereignis ausgelöst wurde.

• Gehe zu Monitor> Data Loss Prevention

uludu cisco	Secure Access							
	Overview	Activity Se	earch					
1   0	Experience Insights							
*	Connect	FILTERS	Q Search by	domain, ide	ntity, or URL			
<b>i</b>	Resources	Q Search filter	'S		1,965 Tota	Ó	Vie	
0	Secure	Response	Advanced	Select All	Request	Source		
2	Monitor	Reports		Manage	ement			
		Remote Access Lo	gs	Export	ed Reports			
20	Admin	Activity Search		Scheduled Reports Saved Searches				
		Traffic logs						
		Security Activity Security events and to	p threats	Admin	Audit Log			
		Total Requests						
		Activity Volume						
		App Discovery Discover and analyze applications	network					
		Top Destinations Top domains visited by	y DNS					
		Top Categories Top security and conte categories by DNS	ent					
		Third-Party Apps						
		Cloud Malware View and manage determalware events	acted					
		Data Loss Prevent Data violations detect the Real Time and Saa	on ed through S API rules					

• Das SvD-Ereignis wird angezeigt.

Data Loss Prevention								Schedu	(±) LAST 24	HOURS ¥		
Events Discovery												
FILTERS	Salact All	Q Search			Advanced	<b>~</b>						
Real Time	Surger Mil	6 Total Events	Viewing activit	ty from Aug 6, 2024 at 9:53 AM to	Aug 7, 2024 at 9:	53 AM						۵
SaaS API		Event Type	Severity	Identity	File Owner	Event Actor	File Name 🔻	Destination	Rule	Action	Detected V	
Action		Real Time	• High	L Windows11-ZTNA	N/A	N/A	Form	OpenAl ChatGPT	Chat GPT DLP	Blocked	Aug 7, 2024 at 9:52 AM	

Klicken Sie auf die drei Punkte am Ende des Ereignisprotokolls, um weitere Details zum Ereignis anzuzeigen.

Data Loss Prevent	ion									Sched	)	24 HOURS ¥
Events Discovery												
FILTERS		Q Search			Advanced	~						
Event Type	Select All											
Real Time		6 Total Events	Viewing activi	ty from Aug 6, 2024 at 9:53 AM to	Aug 7, 2024 at 9:	53 AM						\$
SaaS API		Event Type	Severity	Identity	File Owner	Event Actor	File Name 🔻	Destination	Rule	Action	Detected V	
Action		Real Time	• High	L Windows11-ZTNA	N/A	N/A	Form	OpenAl ChatGPT	Chat GPT DLP	Blocked	Aug 7, 2024 at 9:52 AM	

• Klicken Sie View details.

٠

Event Type	Severity	Identity	File Owner	Event Actor	File Name 🔻	Destination	Rule	Action	Detected <b>V</b>	
Real Time	• High	L Windows11-ZTNA	N/A	N/A	Form	OpenAl ChatGPT	Chat GPT DLP	Blocked	View details	

• Jetzt werden alle Ereignisdetails angezeigt.

## **Event Details**

## Detected

Aug 7, 2024 at 9:52 AM

# Action



## File Name

Form

# Identity

Windows11-ZTNA

# Application

## **OpenAl ChatGPT**

**Application Category** 

Generative AI

# Destination URL

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

<sup>•</sup> Erweitern Sie die Klassifizierung, um festzustellen, welcher Inhalt mit der Klassifizierung übereinstimmt.

	$\overline{\mathbf{X}}$
Rule	$\sim$
Chat GPT DLP	
Severity	
<ul> <li>High</li> </ul>	
Direction	
Inbound	
Classification	
Source Code	1
8 Matches Source Code	
def calculate_year_of_century(age):, def main():	$\bigcirc$

• Es werden alle Details der Inhalte angezeigt, die mit der Klassifizierung/Klassifizierung der SvD-Richtlinie übereinstimmen.

## 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\ndef 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\ndef m ain():\n # Ask the user for their name and age\n name

Fehlerbehebung

• Stellen Sie sicher, dass für die Zugriffsrichtlinie, die Webanfragen für Open AI ChatGPT entspricht, die Entschlüsselung aktiviert ist.

Um schnell zu überprüfen, ob SSE den Datenverkehr für Open AI ChatGPT entschlüsselt, überprüfen Sie das Zertifikat der • Website, das den gebräuchlichen Namen zeigt und die Schlüsselwörter "Cisco Secure Access" enthält.

## Certificate Viewer: chatgpt.com

General

Details

#### Issued To

Common Name (CN)
Organization (O)
Organizational Unit (OU)

chatgpt.com Cisco Systems, Inc. <Not Part Of Certificate>

#### Issued By

Common Name (CN)	Cisco Secure Access Secondary SubCA p-apse210-SG
Organization (O)	Cisco
Organizational Unit (OU)	<not certificate="" of="" part=""></not>

#### 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 Viewe	r: chatgpt.com	×
General Details		
Issued To Common Name (CN Organization (O) Organizational Unit	N) chatgpt.com Cisco Systems, Inc. (OU) <not certificate="" of="" part=""></not>	
Issued By		
Common Name (CN	<ul> <li>Cisco Secure Access Secondary SubCA p-apse210-SG</li> </ul>	
Organization (O)	Cisco	
Organizational Unit	(OU) <not certificate="" of="" part=""></not>	
Validity Period	Monday, August 12, 2024 at 10:52:16 PM	
Expires On	Saturday, August 17, 2024 at 10:52:16 PM	
SHA-256 Fingerprints		
Certificate	4572b5f7a356b5a3c4292a587a130936a3e01990453c22cfdde138e 57647	236c
Public Key	650324e564bdddcf3b09426edfa866449e81c6c79d5d406b23a44e 13bd62	458b

• Beachten Sie, dass die Anforderung zu einer Blockierung führt. Unter Domäne wird Folgendes angezeigt: "block.sse.cisco.com

← → C 🔩 chatgp	Lcom		* 0 :	
(T)	re.	ChatGPT ~	📻 🖟 🖬 Dements Console Sources Network Performance Memory >> 🛛 🛛 2 🛦 34 🛤 3 🛞 1	¢
ω	0	childen	🖤 🛞 🖉 🍸 🔍 🗌 Preserve log 🗌 Disable cache. No throttling 💌 🖘 🏦 🛓	ġ.
			Y Filter Invert I Hide data URLs I Hide extension URLs	
ChatGPT			sample nuthon program All [feth/0HR] Doc CSS //S [fort img Media Manifest WS Wasm Other D Blocked response cookies	
			Sample python program	
88 Explore GPTs			2000 ms 4000 ms 6000 ms 1000 ms 10000 ms 10000 ms 10000 ms 10000 ms 10000 ms 20000 ms 20000 ms	1
		60		
		0		
			Name Status Domain Size Tit	ne
			there was another issue processing your request. If this issue persists	Ĵ
			please contact us through our help center at help.openai.com.	
			Conversation 302 chatgpt.com 8198 16	_
			© C C 00 t 200 dhtppt.com 980 8 27	
			Or D Or F         OD Open         Ab chatgetcom         13 kB         15	1
			dlp/1serverxmps-578677049d-dth/p.sigproxy.prod_awsTC CORS error blocksse.cisco.com 0.8 45.	-
			dlp/tserverxmps-57867749d-dtMp.sigproxy.prod_avsTC 200 blocksse.cisco.com 0.8 44	
			60 rgstr 202 ab.chutggt.com 1.3 kB 36	i.
			O rum?ddsource=browser8uddtags=sdk_version%3A5.20.0% 202 browser-intake_datadogh 145 B 43.	-

- Fragen Sie ChatGPT, ob der Programmcode korrekt ist.
- Beachten Sie, dass die Anfrage zu einem Block führt und unter "domain" "block.sse.cisco.com" angezeigt wird.

chatgpt.com					☆	8	:
chatgpt.com	Is this program correct? # Python program to swap two variables x = 5 y = 10 # To take inputs from the user #x = input(Enter value of x: ) #y = input(Enter value of y: )		Performance         N           No throttling         *           ata URLs         Hide en           450 me         30           200         302           200 sereor         300	temory >> • • 18 4 tension URIs • Other - Blocked respon- blocked response 00 ms - 3500 ms - 40 Domain chatgpt.com chatgpt.com chatgpt.com blockes.sciencom blockes.sciencom	41  5 se cookies to m 4 Size	5 500 ms 7.3 k8 s 1.0 k8 s 819 s 0 8 4 0 8 4	: × € Time 83 25 29
<ul> <li>An error occurred. Eithere was another is please contact us the</li> <li>4 2/2 &gt; D C Q </li> </ul>	<pre># create a temporary variable and swap the values temp = x x = y y = temp print("The value of x after swapping: ()'.format(x)) print("The value of y after swapping: ()'.format(y)) ther the engine you requested does not exist or sue processing your request. If this issue persists rough our help center at help.openai.com.</pre>	☐ dip/Terver imps-578677696-69768.4gproxy.prod_avizT G rgstr C rgstr	200 202 (pending)	blocksse.cisco.com ab.chatgpt.com ab.chatgpt.com		08 4	11 16 1e

#### Zugehörige Informationen

- <u>Cisco Secure Access Benutzerhandbuch</u>
- <u>Technischer Support und Downloads von Cisco</u>

#### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.