

Cisco

Exam Questions 300-735

Automating and Programming Cisco Security Solutions (SAUTO)



NEW QUESTION 1

Which description of synchronous calls to an API is true?

- A. They can be used only within single-threaded processes.
- B. They pause execution and wait for the response.
- C. They always successfully return within a fixed time.
- D. They can be used only for small requests.

Answer: B

NEW QUESTION 2

DRAG DROP

Drag and drop the code to complete the script to search Cisco ThreatGRID and return all public submission records associated with cisco.com. Not all options are used.

Select and Place:

```
import requests

API_KEY = 'asdf1234asdf1234asdf1234'

QUERY = ' ',

URL = 'https://panacea.threatgrid.com/api/v2/ ' / ' ',

PARAMS={"q":QUERY,"api_key":API_KEY}

request = requests.get(url=URL, params=PARAMS)

print(request.json)
```

submissions

public

query

cisco

search

cisco.com

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```
import requests

API_KEY = 'asdf1234asdf1234asdf1234'

QUERY = ' cisco.com ',

URL = 'https://panacea.threatgrid.com/api/v2/ search / submissions ',

PARAMS={"q":QUERY,"api_key":API_KEY}

request = requests.get(url=URL, params=PARAMS)

print(request.json)
```

submissions

public

query

cisco

search

cisco.com

NEW QUESTION 3

Refer to the exhibit. A network operator must generate a daily flow report and learn how to act on or manipulate returned data. When the operator runs the script, it returns an enormous amount of information. Which two actions enable the operator to limit returned data? (Choose two.)

- A. Add recordLimit
- B. followed by an integer (key:value) to the flow_data.
- C. Add a for loop at the end of the script, and print each key value pair separately.
- D. Add flowLimit, followed by an integer (key:value) to the flow_data.
- E. Change the startDateTime and endDateTime values to include smaller time intervals.
- F. Change the startDate and endDate values to include smaller date intervals.

Answer: AB

NEW QUESTION 4

Refer to the exhibit.

Which expression prints the text "802.1x"?

- A. print(quiz[0]['choices']['b'])

- B. print(quiz['choices']['b'])
C. print(quiz[0]['choices']['b']['802.1x'])
D. print(quiz[0]['question']['choices']['b'])

Answer: A

NEW QUESTION 5

DRAG DROP

Drag and drop the code to complete the curl query to the Umbrella Reporting API that provides a detailed report of blocked security activity events from the organization with an organizationId of "12345678" for the last 24 hours. Not all options are used.

Select and Place:

```
curl --include --header "Authorization: Basic %base64string%"  
https://reports.api.umbrella.com/v1/ [ ] /  
[ ] / [ ]
```

12345678	security-activity
security-activity-events	organizations
organizationId	security-events

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

```
curl --include --header "Authorization: Basic %base64string%"  
https://reports.api.umbrella.com/v1/ [ organizations ] /  
[ organizationId ] / [ security-activity ]
```

12345678	security-activity
security-activity-events	organizations
organizationId	security-events

NEW QUESTION 6

DRAG DROP

Drag and drop the code to complete the curl command to query the Cisco Umbrella Investigate API for the umbrella popularity list. Not all options are used.

Select and Place:

```
curl -H "Authorization: [ ] %YourToken%"  
"https://investigate.api.umbrella.com/[ ]"
```

tophundred	Basic	topmillion
Bearer	topthousand	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

```
curl -H "Authorization: [ Bearer ] %YourToken%"  
"https://investigate.api.umbrella.com/[ topmillion ]"
```

tophundred	Basic	topmillion
Bearer	topthousand	

NEW QUESTION 7

DRAG DROP

Drag and drop the items to complete the ThreatGRID API call to return a curated feed of sinkholed-ip-dns in stix format. Not all options are used.
Select and Place:

https://panacea.threatgrid.com/api/v3/

/

?api_key=[API_KEY]

PUT

sinkholed-ip-dns

feeds

search

sinkholed-ip-dns.stix

GET

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

GET

https://panacea.threatgrid.com/api/v3/

feeds

/

sinkholed-ip-dns.stix

?api_key=[API_KEY]

PUT

sinkholed-ip-dns

feeds

search

sinkholed-ip-dns.stix

GET

NEW QUESTION 8

For which two programming languages does Cisco offer an SDK for Cisco pxGrid 1.0? (Choose two.)

- A. Python
B. Perl
C. Java
D. C
E. JavaScript

Answer: CD

NEW QUESTION 9

Which two URI parameters are needed for the Cisco Stealthwatch Top Alarm Host v1 API? (Choose two.)

- A. startAbsolute
B. externalGeos
C. tenantId
D. intervalLength
E. tagID

Answer: CE

NEW QUESTION 10

After changes are made to the Cisco Firepower Threat Defense configuration using the Cisco Firepower Device Manager API, what must be done to ensure that the new policy is activated?

- A. Submit a POST to the /api/fdm/latest/operational/deploy URI.
B. Submit a GET to the /api/fdm/latest/operational/deploy URI.
C. Submit a PUT to the /api/fdm/latest/devicesettings/pushpolicy URI.
D. Submit a POST to the /api/fdm/latest/devicesettings/pushpolicy URI.

Answer: A

NEW QUESTION 10

DRAG DROP

```
def query(config, secret, url, payload):
    print('query url=' + url)
    print(' request=' + payload)
    handler = urllib.request.HTTPSHandler(context=config.get_ssl_context())
    opener = urllib.request.build_opener(handler)
    rest_request = urllib.request.Request(url=url, data=str.encode(payload))
    rest_request.add_header('Content-Type', 'application/json')
    rest_request.add_header('Accept', 'application/json')
    b64 = base64.b64encode((config.get_node_name() + ':' + secret).encode()).decode()
    rest_request.add_header('Authorization', 'Basic ' + b64)
    rest_response = opener.open(rest_request)
    print(' response status=' + str(rest_response.getcode()))
    print(' response content=' + rest_response.read().decode())
```

Refer to the exhibit. A Python function named "query" has been developed, and will be used to query the service "com.cisco.ise.session" via Cisco pxGrid 2.0 APIs. Drag and drop the code to construct a Python call to the "query" function to identify the user groups that are associated with the user "fred". Not all options are used. Select and Place:

query (

 ,

 ,

 ,

)

"getUserGroupByUserName", "fred"	url
'{ "userName": "fred" }'	secret

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

query (

 ,

 ,

 ,

)

"getUserGroupByUserName", "fred"	url
'{ "userName": "fred" }'	secret

NEW QUESTION 14

Which two event types can the eStreamer server transmit to the requesting client from a managed device and a management center? (Choose two.)

- A. user activity events
 B. intrusion events
 C. file events
 D. intrusion event extra data
 E. malware events

Answer: BD

NEW QUESTION 17

Refer to the exhibit. The script outputs too many results when it is queried against the Cisco Umbrella Reporting API. Which two configurations restrict the returned result to only 10 entries? (Choose two.)

- A. Add params parameter in the get and assign in the {"return": "10"} value.
 B. Add ?limit=10 to the end of the URL string.
 C. Add params parameter in the get and assign in the {"limit": "10"} value.
 D. Add ?find=10 to the end of the URL string.
 E. Add ?return=10 to the end of the URL string.

Answer: BC

NEW QUESTION 22

Which two destinations are supported by the Cisco Security Management Appliance reporting APIs? (Choose two.)

- A. email
- B. Microsoft Word file
- C. FTP
- D. web
- E. csv file

Answer: AD

NEW QUESTION 27

```
import json
import requests

BASE_URL = "https://investigate.api.umbrella.com"
HEADERS = {"Authorization": "Bearer %YourToken%"}

---MISSING CODE---

request= requests.get(URL, parmas= PARAMS,
verify=False)
```

Refer to the exhibit. A network operator must create a Python script that makes an API request to Cisco Umbrella to do a pattern search and return all matched URLs with category information.
Which code completes the script?

- A. URL = BASE_URL + "/find/exa[a-z]ple.com" PARAMS = { "categoryinclude" : "true"}
- B. URL = BASE_URL + "/find/exa[a-z]ple.com" PARAMS = { "returncategory" : "true"}
- C. URL = BASE_URL + "/find/exa[a-z]ple.com" PARAMS = { "includeCategory" : "true"}
- D. URL = BASE_URL + "/find/exa[a-z]ple.com" PARAMS = { "returnCategory" : "true"}

Answer: D

NEW QUESTION 31

```
import requests

URL =
'https://sma.cisco.com:6080/sma/api/v2.0/reporting/web_malware_category_malware_name_user_detail/
blocked_malware?startDate=2019-03-14T02:00+00:00&endDate=2019-04-14T01:00+00:00&
filterValue=23&filterBy=na&filterOperator=is&device_type=wsa'

HEADERS = {'Authorization': "Basic Y2hlcGFLYWJSQSZe'"}

response = requests.get(URL, headers=HEADERS)
```

Refer to the exhibit.
What must be present in a Cisco Web Security Appliance before the script is run?

- A. reporting group with the name web_malware_category_malware_name_user_detail
- B. data for specified dates
- C. reporting group with the name blocked_malware
- D. data in the queried category

Answer: A

NEW QUESTION 36

The Cisco Security Management Appliance API is used to make a GET call using the URI
/sma/api/v2.0/reporting/mail_incoming_traffic_summary/detected_amp?startDate=2016-09-10T19:00:00.000Z&endDate=2018-0924T23:00:00.000Z&device_type=esa&device_name=esa01.
What does this GET call return?

- A. values of all counters of a counter group, with the device group name and device type for web
- B. value of a specific counter from a counter group, with the device name and type for email
- C. value of a specific counter from a counter group, with the device name and type for web
- D. values of all counters of a counter group, with the device group name and device type for email

Answer: D

NEW QUESTION 40

DRAG DROP

Drag and drop the code to complete the Cisco Umbrella Investigate WHOIS query that returns a list of domains that are associated with the email address "admin@example.com". Not all options are used.
Select and Place:

<code>"https://investigate.api.umbrella.com/ [] /</code>		
<code>[] / [] "</code>		
email	emails	WHOIS
admin@example.com	whois	{admin@example.com}

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

<code>"https://investigate.api.umbrella.com/ [WHOIS] /</code>		
<code>[emails] / [admin@example.com] "</code>		
email	emails	WHOIS
admin@example.com	whois	{admin@example.com}

NEW QUESTION 42

Which two commands create a new local source code branch? (Choose two.)

- A. git checkout -b new_branch
B. git branch -b new_branch
C. git checkout -f new_branch
D. git branch new_branch
E. git branch -m new_branch

Answer: AD

NEW QUESTION 44

Refer to the exhibit. A network operator wrote a Python script to retrieve events from Cisco AMP.

```
import requests
CLIENT_ID = 'a1b2c3d4e5f6g7h8i9j0'
API_KEY = 'a1b2c3d4-e5f6-g7h8-i9j0-k112m3n4o5p6'
----MISSING CODE----
URL = BASE_URL+'v1/events'
request = requests.get(url, auth=(amp_client_id, amp_api_key))
```

Against which API gateway must the operator make the request?

- A. BASE_URL = "https://api.amp.cisco.com"
B. BASE_URL = "https://amp.cisco.com/api"
C. BASE_URL = "https://amp.cisco.com/api/"
D. BASE_URL = "https://api.amp.cisco.com/"

Answer: A

NEW QUESTION 48

What is the purpose of the snapshot APIs exposed by Cisco Stealthwatch Cloud?

- A. Report on flow data during a customizable time period.
B. Operate and return alerts discovered from infrastructure observations.
C. Return current configuration data of Cisco Stealthwatch Cloud infrastructure.
D. Create snapshots of supported Cisco Stealthwatch Cloud infrastructure.

Answer: B

NEW QUESTION 51

Which query parameter is required when using the reporting API of Cisco Security Management Appliances?

- A. device_type
B. query_type
C. filterValue
D. startDate + endDate

Answer: D

NEW QUESTION 56

Which step is required by Cisco pxGrid providers to expose functionality to consumer applications that are written in Python? A. Look up the existing service using the /pxgrid/control/ServiceLookup endpoint.

- A. Register the service using the /pxgrid/control/ServiceRegister endpoint.
- B. Configure the service using the /pxgrid/ise/config/profiler endpoint.
- C. Expose the service using the /pxgrid/ise/pubsub endpoint.

Answer: D

NEW QUESTION 60

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

300-735 Practice Exam Features:

- * 300-735 Questions and Answers Updated Frequently
- * 300-735 Practice Questions Verified by Expert Senior Certified Staff
- * 300-735 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 300-735 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 300-735 Practice Test Here](#)