

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

DRAG DROP

Drag and drop the code to complete the API call to query all Cisco Stealthwatch Cloud observations. Not all options are used.

Select and Place:

```
 https://example.obsrvbl.com/api/v3/

 / 
```

observations	DELETE	GET
POST	all/	all
obsrv	?query=all	

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

GET	https://example.observbl.com/api/v3/	
observations	/	all

observations	DELETE	GET
POST	all/	all

obsrv	?query=all
-------	------------

NEW QUESTION 4

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 5

```
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 the goal is to use it to query the service "com.cisco.ise.session" via Cisco pxGrid 2.0 APIs. How is the function called, if the goal is to identify the sessions that are associated with the IP address 10.0.0.50?

- A. query(config, secret, "getSessionByIpAddress/10.0.0.50", "ipAddress")
- B. query(config, "10.0.0.50", url, payload)
- C. query(config, secret, url, "10.0.0.50")
- D. query(config, secret, url, '{"ipAddress": "10.0.0.50"}')

Answer: D

NEW QUESTION 6

Which two API capabilities are available on Cisco Identity Services Engine? (Choose two.)

- A. Platform Configuration APIs
- B. Monitoring REST APIs
- C. Performance Management REST APIs
- D. External RESTful Services APIs
- E. Internal RESTful Services APIs

Answer: BD

NEW QUESTION 7

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

"getUserGroupByUserName", "fred"

url

'{ "userName": "fred" }'

secret

NEW QUESTION 8

Which API capability is available on Cisco Firepower devices?

- A. Firepower Management Center - Sockets API
- B. Firepower Management Center - eStreamer API
- C. Firepower Management Center - Camera API
- D. Firepower Management Center - Host Output API

Answer: B

NEW QUESTION 9

Refer to the exhibit. A network operator wants to add a certain IP to a DMZ tag. Which code segment completes the script and achieves the goal?

- A.

```
tag_data = json.dumps(tag_session)['data']
tag_data['ranges'].append(DMZ_IP)
session.put(TAG_URL, json=tag_data, headers=HEADERS, verify=False)
```
- B.

```
tag_data = json.loads(tag_session)['data']
tag_data['ranges'].append(DMZ_IP)
session.put(TAG_URL, data=tag_data, headers=HEADERS, verify=False)
```
- C.

```
tag_data = json.dumps(tag_session)['data']
tag_data['ranges'].append(DMZ_IP)
session.put(TAG_URL, data=json.loads(tag_data), headers=HEADERS, verify=False)
```
- D.

```
tag_data = json.loads(tag_session)['data']
tag_data['ranges'].append(DMZ_IP)
session.put(TAG_URL, json=tag_data, headers=HEADERS, verify=False)
```

Answer: A

NEW QUESTION 10

A security network engineer must implement intrusion policies using the Cisco Firepower Management Center API. Which action does the engineer take to achieve the goal?

- A. Make a PATCH request to the URI /api/fmc_config/v1/domain/{DOMAIN_UUID}/policy/intrusionpolicies.
- B. Make a POST request to the URI /api/fmc_config/v1/domain/{DOMAIN_UUID}/policy/intrusionpolicies.
- C. Intrusion policies can be read but not configured using the Cisco Firepower Management Center API.
- D. Make a PUT request to the URI /api/fmc_config/v1/domain/{DOMAIN_UUID}/policy/intrusionpolicies.

Answer: C

NEW QUESTION 10

FILL BLANK

Fill in the blank to complete the statement with the correct technology.

Cisco Investigate provides access to data that pertains to DNS security events and correlations collected by the Cisco security team.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Umbrella

NEW QUESTION 12

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 15

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 19

```
import requests

API_KEY = "123456789abcdef"

URL = "https://example.obsrvbl.com/api/v3/alerts/alert/"

HEADERS = {"Authorization": "Bearer {}".format(API_KEY)}

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

Refer to the exhibit. A security engineer created a script and successfully executed it to retrieve all currently open alerts. Which print command shows the first returned alert?

- A. `print(response[data][0])`
- B. `print(response[results][0])`
- C. `print(response.json()[data][0])`
- D. `print(response.json()[results][0])`

Answer: A

NEW QUESTION 24

What are two benefits of Ansible when managing security platforms? (Choose two.)

- A. End users can be identified and tracked across a network.
- B. Network performance issues can be identified and automatically remediated.
- C. Policies can be updated on multiple devices concurrently, which reduces outage windows.
- D. Anomalous network traffic can be detected and correlated.
- E. The time that is needed to deploy a change is reduced, compared to manually applying the change.

Answer: CE

NEW QUESTION 29

```
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 33

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 34

Which header set should be sent with all API calls to the Cisco Stealthwatch Cloud API?

- A. `Content-Type: application/json`
`Accept: application/json`
`Authorization: Bearer <api_key>`

- B. Content-Type: application/json
Accept: application/json
Authorization: ApiKey <username>:<api_key>
- C. Content-Type: application/json
Accept: application/json
Authorization: Basic <api_key>
- D. Content-Type: application/json
Accept: application/json
Authorization: <username>:<api_key>

Answer: B

NEW QUESTION 37

Which snippet describes the way to create an URL object in Cisco FDM using FDM REST APIs with curl?

- A.

```
curl -X POST --header 'Content-Type: application/json' \
--header 'Authorization: Bearer $Token' \
--header 'Accept: application/json' -d '{ \
  "id": "bfc6j984-9dcf-11e9-a6b5-617eea9159d3", \
  "description": "Google URL", \
  "url": "https://www.google.com", \
  "type": "urlobject" \
}' 'https://198.18.133.8/api/fdm/v1/object/url'
```
- B.

```
curl -X POST --header 'Content-Type: application/json' \
--header 'Authorization: Bearer $Token' \
--header 'Accept: application/json' -d '{ \
  "name": "google_url", \
  "description": "Google URL", \
  "url": "https://www.google.com", \
  "type": "urlobject" \
}' 'https://198.18.133.8/api/fdm/v1/object/urls'
```
- C.

```
curl -X POST --header 'Content-Type: application/json' \
--header 'Authorization: Bearer $Token' \
--header 'Accept: application/json' -d '{ \
  "name": "google_url", \
  "description": "Google URL", \
  "url": "https://www.google.com", \
  "type": "networkobject" \
}' 'https://198.18.133.8/api/fdm/v1/object/urls'
```
- D.

```
curl -X POST --header 'Content-Type: application/json' \
--header 'Authorization: Bearer $Token' \
--header 'Accept: application/json' -d '{ \
  "id": "bfc6j984-9dcf-11e9-a6b5-617eea9159d3", \
  "description": "Google URL", \
  "url": "https://www.google.com", \
  "type": "urlobject" \
}' 'https://198.18.133.8/api/fdm/v1/object/urlcategories'
```

Answer: B

NEW QUESTION 40

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 42

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 46

.....

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](#)