



Cisco

300-735 Exam

**Automating and Programming Cisco Security Solutions (300-735 SAUTO) Exam
Questions & Answers
Demo**

Version: 8.0

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

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.

```
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

Answer:

```
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

Reference:

<https://community.cisco.com/t5/endpoint-security/amp-threat-grid-api/m-p/3538319>

Question: 3

Refer to the exhibit.

```
import requests

headers = {
    'Authorization': 'Bearer ' + investigate_api_key
}

domains=["cisco.com", "google.com", "xreddfr.df"]

investigate_url= "https://investigate.api.umbrella.com/domains/categorization/"
values = str(json.dumps(domains))
response = requests.post(investigate_url, data=values, headers=headers)
```

What does the response from the API contain when this code is executed?

- A. error message and status code of 403
- B. newly created domains in Cisco Umbrella Investigate
- C. updated domains in Cisco Umbrella Investigate
- D. status and security details for the domains

Answer: D

Question: 4

Refer to the exhibit.

```
import requests

URL = 'https://sma.cisco.com:6080/sma/api/v2.0/quarantine/messages/details?quarantineType=spam&device_type=esa'
HEADERS = {'Authorization': 'Basic Y2hlcGFLYWJSQSZe'}

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

A security engineer attempts to query the Cisco Security Management appliance to retrieve details of a

specific message.

What must be added to the script to achieve the desired result?

- A. Add message ID information to the URL string as a URI.
- B. Run the script and parse through the returned data to find the desired message.
- C. Add message ID information to the URL string as a parameter.
- D. Add message ID information to the headers.

Answer: C

Question: 5

Refer to the exhibit.

```
import json
import requests

USER = "admin"
PASS = "Cisco12345"
TENAT_ID = "132"
BASE_URL = "https://198.18.128.136"
CREDENTIALS = {'password': PASS, 'username': USER}

session = requests.Session()
session.post(BASE_URL+"/token/v2/authenticate", data= CREDENTIALS, verify=False)

QUERY_URL=BASE_URL+"/sw-reporting/rest/v2/tenants/{0}/queries".format(TENAT_ID)

flow_data ={
    "searchName": "Flows API Search on 6/29/2019",
    "startDateTime": "2019-06-29T00:00:01Z",
    "endDateTime": "2019-06-29T23:59:59Z"
}

session.post(QUERY_URL, json=flow_data, verify=False)
```

A network operator must generate a daily flow report and learn how to act on or manipulate returned data

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

Answer: AB
