300-735 ^{Q&As}

300-735^{Q&As}

Automating and Programming Cisco Security Solutions (SAUTO)

Pass Cisco 300-735 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/300-735.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

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

Correct Answer: B

QUESTION 2

Refer to the exhibit.

```
import json
import requests

USER = "admin"
PASS = "C1sco12345"
TENAT_ID = "132"
TAG_ID = "24"
BASE_URL = "https://198.18.128.136"
CREDENTIALS = {'password': PASS, 'username': USER}
DMZ_IP = "198.18.128.147"
HEADERS = {'Content-type': 'application/json', 'Accept': 'application/json'}

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

TAG_URL=BASE_URL+"/smc-configuration/rest/v1/tenants/{0}/tags/{1}".format(TENAT_ID, TAG_ID)

tag_session = session.get(url=TAG_URL, verify=False).content.decode()
```

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)
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 3

Refer to the exhibit.

```
import requests

URL = 'https://reports.api.umbrella.com/v1/organizations/fe4936f9/destinations/www.cisco.com/activity'
HEADERS = {'Authorization': 'Basic aGVsb29YXViYnd5YXNk'}

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

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.

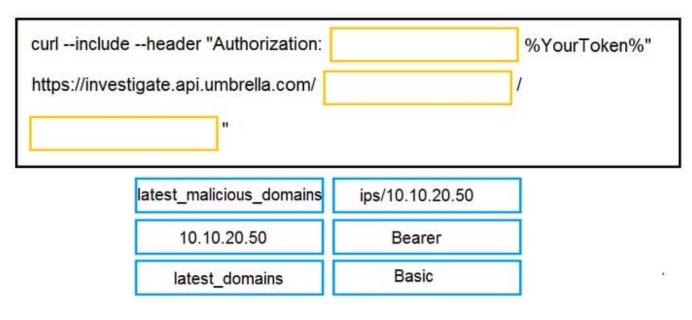E. Add ?return=10 to the end of the URL string.
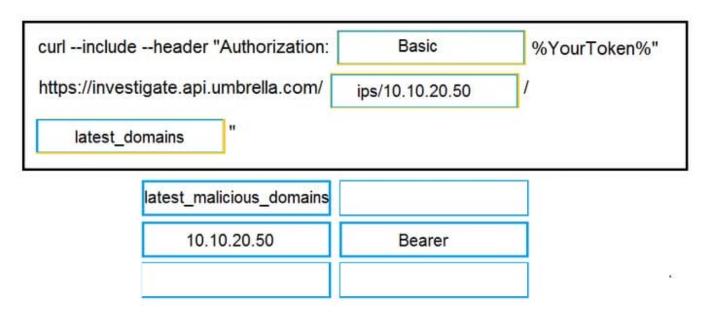
Correct Answer: BC

QUESTION 4

DRAG DROP

Drag and drop the code to complete the curl query to the Cisco Umbrella Investigate API for the Latest Malicious Domains for the IP address 10.10.20.50. Not all options are used.

Select and Place:

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

latest_malicious_domains	ips/10.10.20.50
10.10.20.50	Bearer
latest_domains	Basic

Correct Answer:

```
curl --include --header "Authorization:  Basic  %YourToken%"
https://investigate.api.umbrella.com/  ips/10.10.20.50  /
latest_domains  "
```

latest_malicious_domains	
10.10.20.50	Bearer

Reference: https://docs.umbrella.com/investigate-api/reference#about-the-api-and-authentication

QUESTION 5

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 Y2hlcGFYWJSQSZe'}

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.

Correct Answer: C

QUESTION 6

DRAG DROP

A Python script is being developed to return the top 10 identities in an organization that have made a DNS request to "www.cisco.com".

Drag and drop the code to complete the Cisco Umbrella Reporting API query to return the top identities. Not all options are used.

Select and Place:

```
import requests

URL = 'https://reports.api.umbrella.com/v1/organizations/fe4936f9/

       [          ]  /  [          ]  /  [          ]  '

HEADERS = {'Authorization': 'Basic aGVsb29oYXViYind5YXNk'}

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

security-activity	destinations	activity
www.cisco.com	identities	topIdentities

Correct Answer:

```
import requests

URL = 'https://reports.api.umbrella.com/v1/organizations/fe4936f9/

    destinations    /    www.cisco.com    /    activity    '

HEADERS = {'Authorization': 'Basic aGVsb29oYXViYYnd5YXNk'}

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

```
security-activity
```

```
identities
```

```
topIdentities
```

Reference: https://docs.umbrella.com/umbrella-api/docs/reporting-destinations-most-recent-requests

QUESTION 7

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

Correct Answer: BD

QUESTION 8

Refer to the exhibit.

```
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)
```

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])

Correct Answer: A

QUESTION 9

Which curl command lists all tags (host groups) that are associated with a tenant using the Cisco Stealthwatch Enterprise API?

A. curl -X PUT"Cookie:{Cookie Data}"https://{stealthwatch_host}/smc-configuration/rest/v1/tenants/{tenant_id}/tags

B. curl -X POST -H"Cookie:{Cookie Data}"https://{stealthwatch_host}/smc-configuration/rest/v1/tenants/tags

C. curl -X GET -H"Cookie:{Cookie Data}"https://{stealthwatch_host}/smc-configuration/rest/v1/tenants/{tenant_id}/tags

D. curl -X GET -H"Cookie:{Cookie Data}"https://{stealthwatch_host}/smc-configuration/rest/v1/tenants/tags

Correct Answer: C

QUESTION 10

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.

Correct Answer: B

QUESTION 11

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=2016-09-10T19:00:00.000ZandendDate=2018-0924T23:00:00.000Zanddevice_type=esaanddevice_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

Correct Answer: D

QUESTION 12

Refer to the exhibit.

```
{
  "version": "v1.2.0",
  "metadata": {
    "links": {
      "self":
    },
    "results": {
      "total": 33,
      "current_item_count": 33,
      "index": 0,
      "items_per_page": 500
    }
  },
  "data": [
    {
      "connector_guid": "0e37a552-2cdd-4178-b29e-1be15598d730",
      "hostname": "Demo_AMP",
      "active": true,
      "links": {
        "computer": "0e37a552-2cdd-4178-b29e-1be15598d730",
        "trajectory": "0e37a552-2cdd-4178-b29e-1be15598d730/trajectory",
        "group": "6c3c2005-4c74-4ba7-8dbb-c4d5b6bafe03"
      }
    }
  ]
}
```

Which URL returned the data?

A. https://api.amp.cisco.com/v1/computers

B. https://api.amp.cisco.com/v0/computers

C. https://amp.cisco.com/api/v0/computers

D. https://amp.cisco.com/api/v1/computers

Correct Answer: A

QUESTION 13

Which URI string is used to create a policy that takes precedence over other applicable policies that are configured on Cisco Stealthwatch?

A. /tenants/{tenantId}/policy/system/host-policy

B. /tenants/{tenantId}/policy/system/role-policy

C. /tenants/{tenantId}/policy/system

D. /tenants/{tenantId}/policy/system/{policyId}

Correct Answer: A

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

Correct Answer: BD

QUESTION 15

Refer to the exhibit.

```
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())
```

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"}\\')

Correct Answer: D

Latest 300-735 Dumps   300-735 Practice Test   300-735 Study Guide