- **Vendor:** Cisco
- **Exam Code:** 300-735
- **Exam Name:** Automating and Programming Cisco Security Solutions
- **New Updated Questions from Braindump2go (Updated in May/2020)**

QUESTION 23
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 24
If the goal is to create an access policy with the default action of blocking traffic, using Cisco Firepower Management Center REST APIs, which snippet is used?

A.
```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/accesspolicies

- METHOD:
POST

- INPUT JSON:
{
  "type": "AccessPolicy",
  "name": "AccessPolicy-test-1",
  "defaultAction": {
    "action": "BLOCK"
  }
}
```

```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/securityzones

- METHOD:
POST

- INPUT JSON:
{
  "type": "AccessPolicy",
  "name": "AccessPolicy-test-1",
  "defaultAction": {
    "action": "BLOCK"
  }
}
```

C.

```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/accesspolicies

- METHOD:
PUT

- INPUT JSON:
{
  "type": "AccessPolicy",
  "name": "AccessPolicy-test-1",
  "defaultAction": {
    "action": "BLOCK"
  }
}
```

D.

```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/accesspolicies

- METHOD:
POST

- INPUT JSON:
{
  "type": "AccessPolicy",
  "name": "AccessPolicy-test-1",
  "action": "FASTPATH"
}
```

Correct Answer: D

QUESTION 25

```
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()
```

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)
```

```
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)
```

Correct Answer: A

QUESTION 26
Which API is designed to give technology partners the ability to send security events from their platform/service/appliance within a mutual customer's environment to the Umbrella cloud for enforcement?

A. Cisco Umbrella Management API
B. Cisco Umbrella Security Events API
C. Cisco Umbrella Enforcement API
D. Cisco Umbrella Reporting API

Correct Answer: C

QUESTION 27
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 28
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**.

Correct Answer: C

QUESTION 29
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 30

```
curl -X PUT \
    --header "Accept: application/json" \
    --header "Authorization: Bearer ${ACCESS_TOKEN}" \
    --header "Content-Type: application/json" \
    -d '{
        "id": "XXXXXXXXXX",
        "ruleAction": "DENY",
        "eventLogAction": "LOG_FLOW_START",
        "type": "accessrule",
    }' \
    "https://${HOST}:${PORT}/api/fdm/v3/policy/accesspolicies
/{parentId}/accessrules/{objId}"
```

Refer to the exhibit. The security administrator must temporarily disallow traffic that goes to a production web server using the Cisco FDM REST API. The administrator sends an API query as shown in the exhibit.

What is the outcome of that action?

A. The given code does not execute because the mandatory parameters, source, destination, and services are missing.
B. The given code does not execute because it uses the HTTP method "PUT". It should use the HTTP method "POST".
C. The appropriate rule is updated with the source, destination, services, and other fields set to "Any" and the action set to "DENY". Traffic to the production web server is disallowed, as expected.

D. A new rule is created with the source, destination, services, and other fields set to "Any" and the action set to "DENY". Traffic to the production web server is disallowed, as expected.

Correct Answer: C

QUESTION 31
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.

Correct Answer: Umbrella

```
import requests

URL = 'https://reports.api.umbrella.com/v1/organizations/fe4936f9/destinations/www.cisco.com/activity'
HEADERS = {'Authorization': 'Basic aGVsb29oYXViYnd5YXNk'}

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

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.

Correct Answer: BC

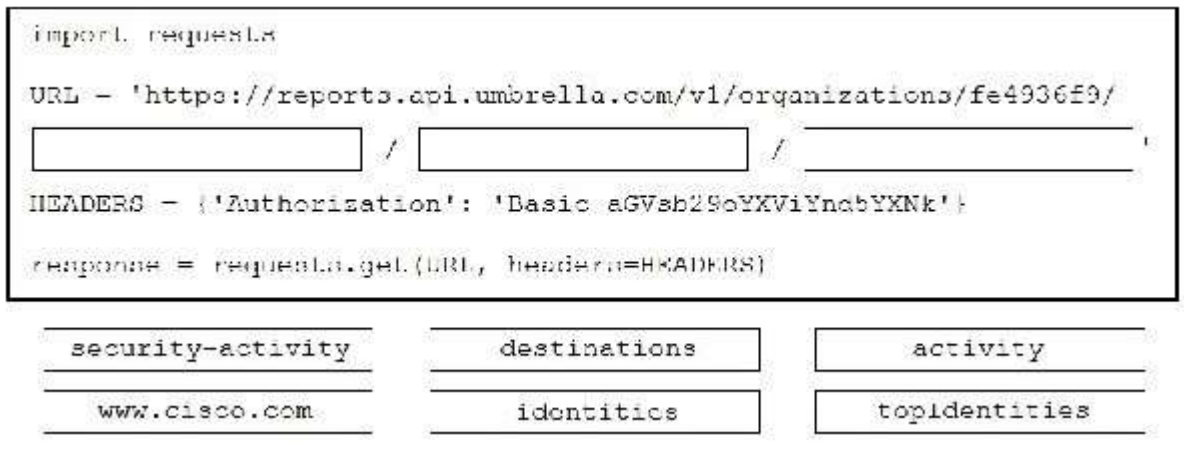
QUESTION 33
DRAG DROP

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:



Correct Answer: