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

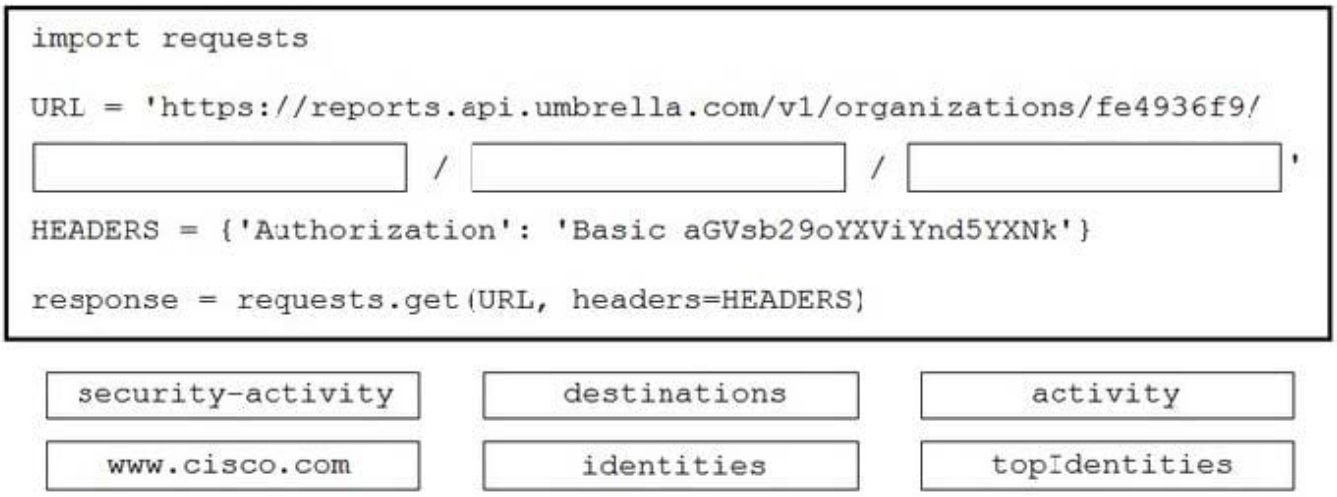
QUESTION 1

DRAG DROP

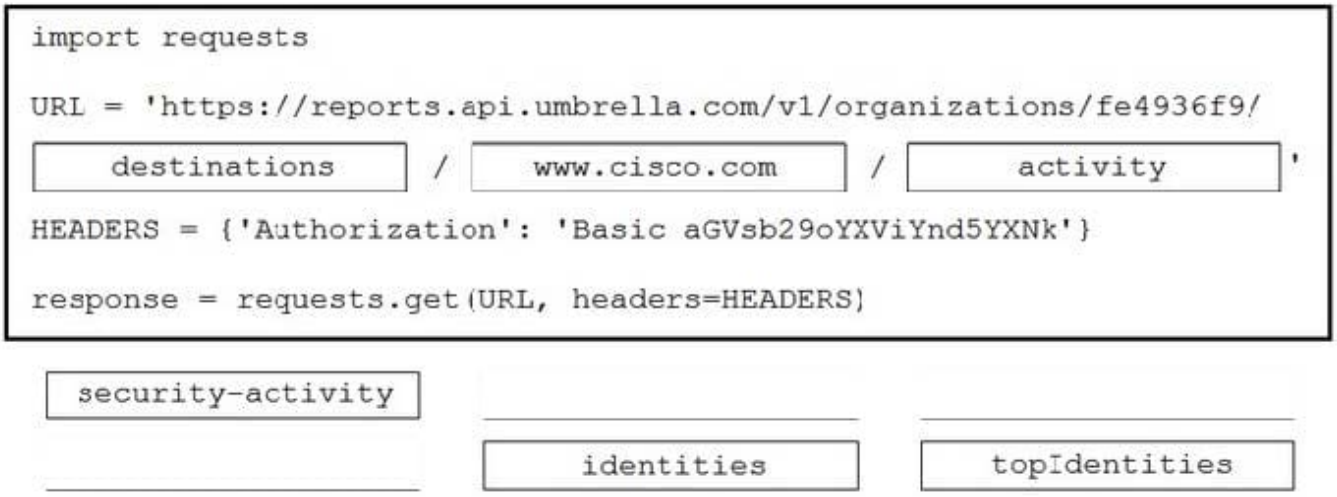
A Python script is being developed to return the top 10 identities in an organization that have made a DNS request to "www.cisco.com".

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:



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

QUESTION 2

Which API is used to query if the domain "example.com" has been flagged as malicious by the Cisco Security Labs team?

A. https://s-platform.api.opendns.com/1.0/events?example.com

B. https://investigate.api.umbrella.com/domains/categorization/example.com

C. https://investigate.api.umbrella.com/domains/volume/example.com

D. https://s-platform.api.opendns.com/1.0/domains?example.com

Correct Answer: B

QUESTION 3

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

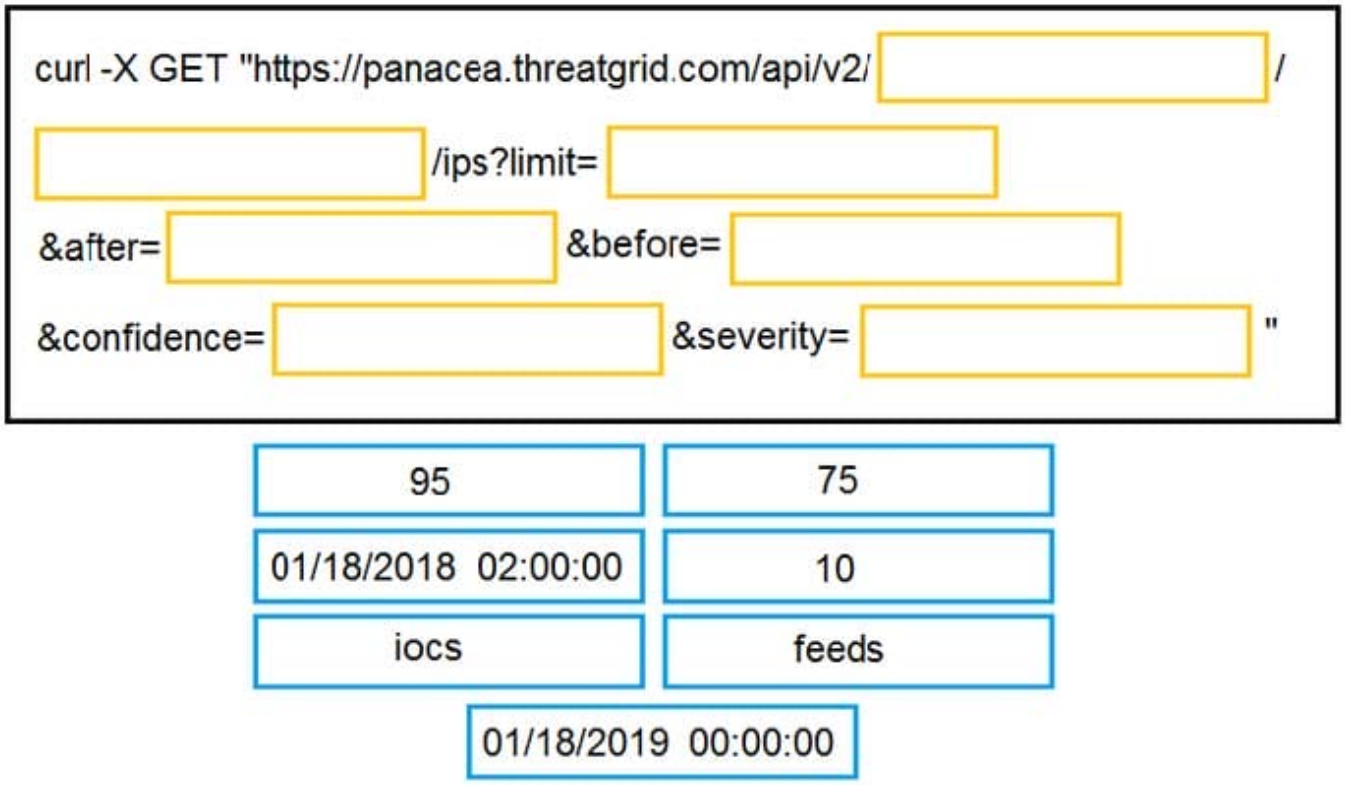
E. JavaScript

Correct Answer: CD

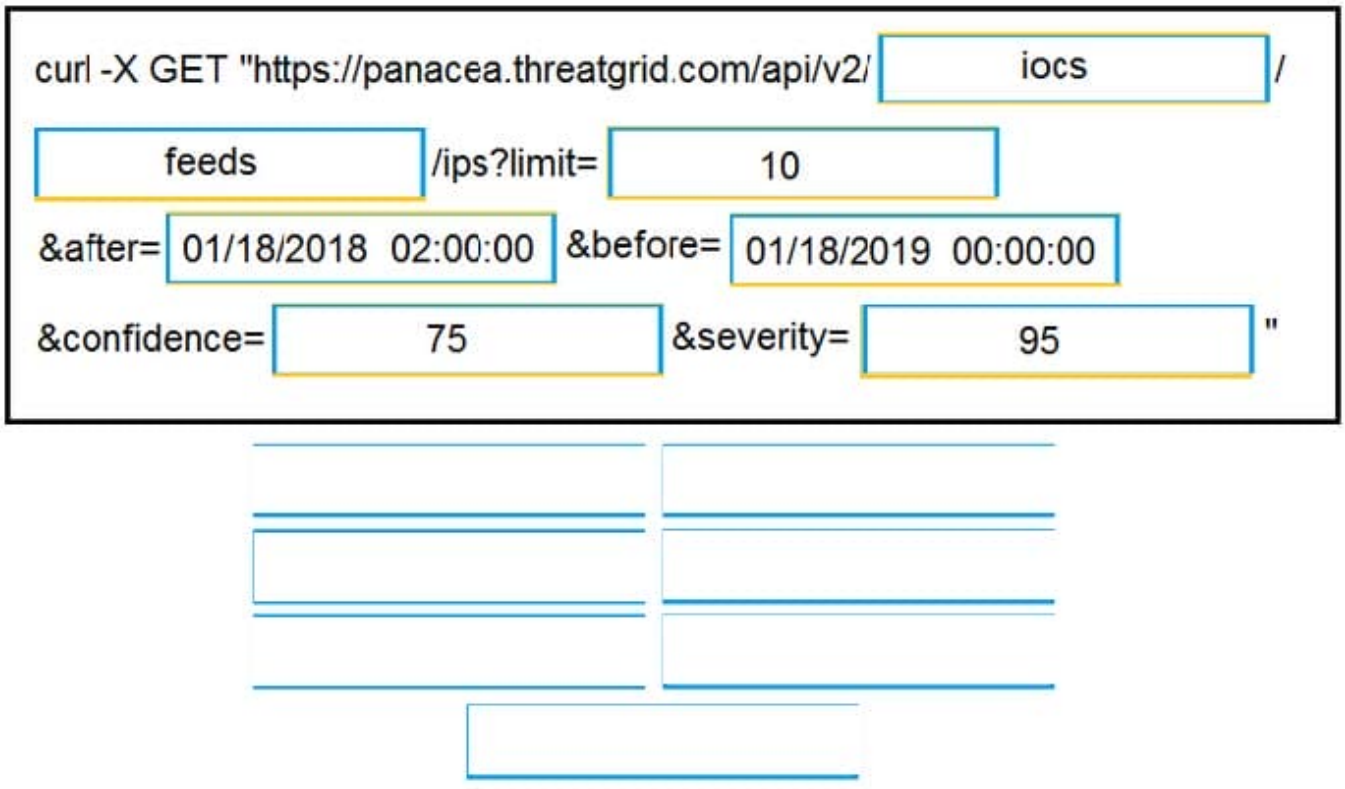
QUESTION 4

DRAG DROP Drag and drop the items to complete the curl request to the ThreatGRID API. The API call should request the first 10 IP addresses that ThreatGRID saw samples communicate with during analysis, in the first two hours of January 18th (UTC time), where those communications triggered a Behavior Indicator that had a confidence equal to or higher than 75 and a severity equal to or higher than 95.

Select and Place:



Correct Answer:



Reference: https://support.umbrella.com/hc/en-us/articles/231248768-Cisco-Umbrella-Cisco-AMP-Threat-Grid-Cloud-Integration-Setup-Guide

QUESTION 5

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
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

QUESTION 6

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 7

Which snippet is used to create an object for network 10.0.69.0/24 using Cisco Firepower Management Center REST APIs?

A.

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

- METHOD:
POST

- INPUT JSON:
{
  "type": "Network",
  "value": "10.0.69.0/24",
  "overridable": false,
  "description": " ",
  "name": "Branch_1_net"
}
```

B.

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

- METHOD:
PUT

- INPUT JSON:
{
  "type": "Network",
  "value": "10.0.69.0/24",
  "overridable": false,
  "description": " ",
  "name": "Branch_1_net"
}
```

C.

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

- METHOD:
POST

- INPUT JSON:
{
  "type": "Network",
  "value": "10.0.69.0/24",
  "overridable": false,
  "description": " "
}
```

D.

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

- METHOD:
POST

- INPUT JSON:
{
  "type": "Network",
  "value": "10.0.69.0/24",
  "overridable": false,
  "description": " "
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 8

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 9

Refer to the exhibit.

```
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)
```

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 10

Which two methods are API security best practices? (Choose two.)

A. Use tokens after the identity of a client has been established.

B. Use the same operating system throughout the infrastructure.

C. Use encryption and signatures to secure data.

D. Use basic auth credentials over all internal API interactions.

E. Use cloud hosting services to manage security configuration.

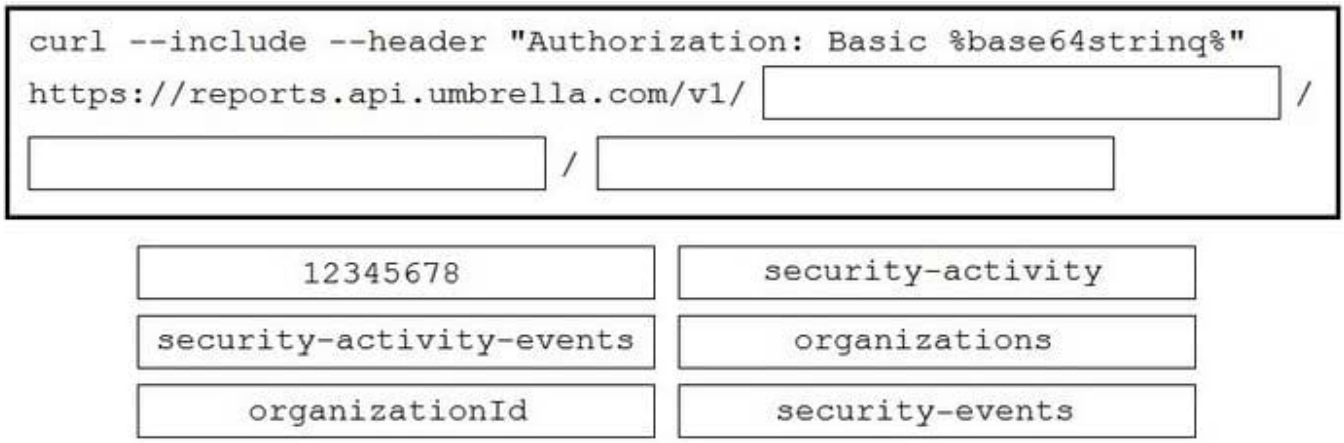
Correct Answer: AC

QUESTION 11

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:



Correct Answer:

Reference: https://docs.umbrella.com/umbrella-api/docs/security-activity-report

QUESTION 12

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/"

Correct Answer: A

QUESTION 13

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>
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

QUESTION 14

Which two statements describe the characteristics of API styles for REST and RPC? (Choose two.)

A. REST-based APIs function in a similar way to procedures.

B. REST-based APIs are used primarily for CRUD operations.

C. REST and RPC API styles are the same.

D. RPC-based APIs function in a similar way to procedures.

E. RPC-based APIs are used primarily for CRUD operations.

Correct Answer: BD

QUESTION 15

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