Vendor: Cisco

Exam Code: 300-735

Exam Name: Automating and Programming Cisco Security Solutions (SAUTO)

Version: Demo

Exam A

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

Correct 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

Section: (none)

Explanation

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

QUESTION 3

```
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)
```

Refer to the exhibit.

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4

```
import requests

URL = 'https://sma.cisco.com:6080/sma/api/v2.0/quarantine/messages/details?quarantineType=spam&device_type=esa'
HEADERS = {'Authorization': 'Basic Y2h1cGFLYWJSQSZe'}

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

Refer to the exhibit. 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.

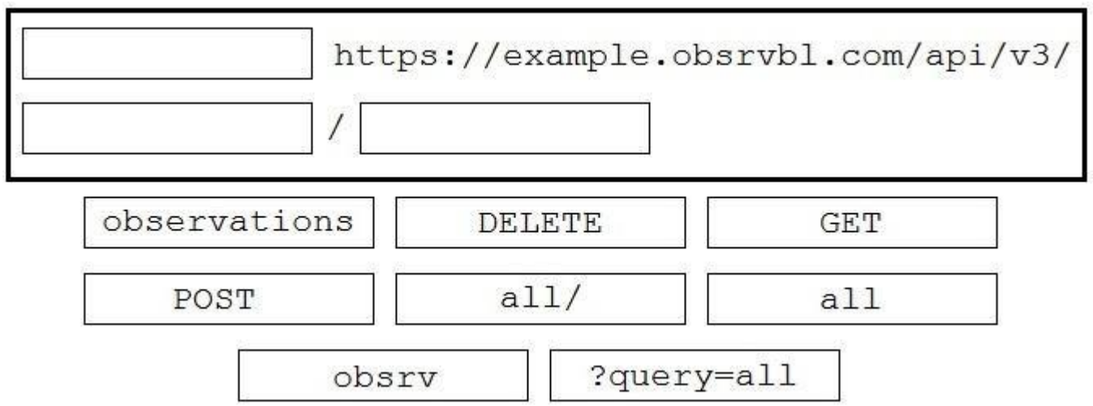
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

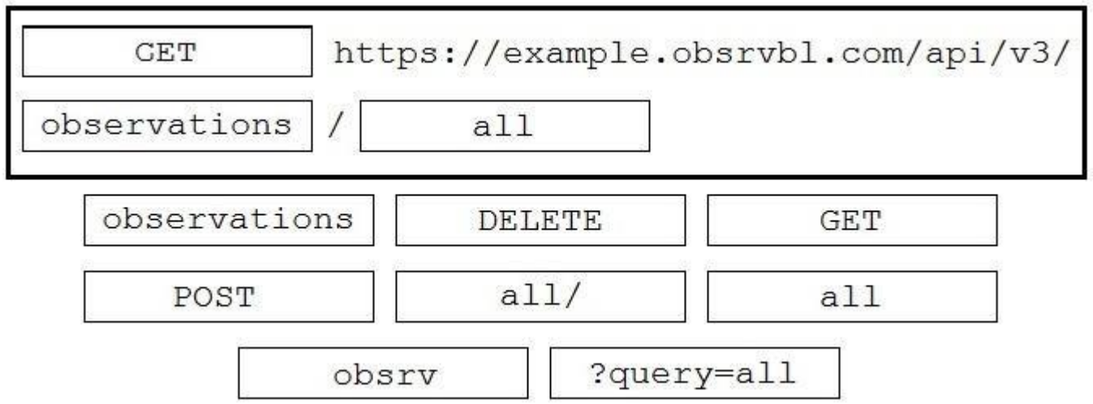
QUESTION 5
DRAG DROP

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:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:

QUESTION 6

```
import json
import requests

USER = "admin"
PASS = "C1sco12345"
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)
```

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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

```
quiz = [
    {
        "question": "Which of these is an IEEE standard for port-based Network Access Control",
        "choices": {"a": "802.11x", "b": "802.1x", "c": "802.11a", "d": "802.11b"},
        "answer": "b"
    },
]
```

Refer to the exhibit.

Which expression prints the text "802.1x"?

A. print(quiz[0]['choices']['b'])
B. print(quiz['choices']['b'])
C. print(quiz[0]['choices']['b']['802.1x'])
D. print(quiz[0]['question']['choices']['b'])

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
DRAG DROP

```
# Threat Grid URL used for collecting samples
tg_url = '____________________/____________________'

# Parameters for Threat Grid API query
tg_parameters = {'api_key': [____________________],
        'advanced':'true',
        'state':'succ',
        'q':'____________________'}

# Query Threat Grid for samples
request = ____________________ (tg_url, params=tg_parameters)
```

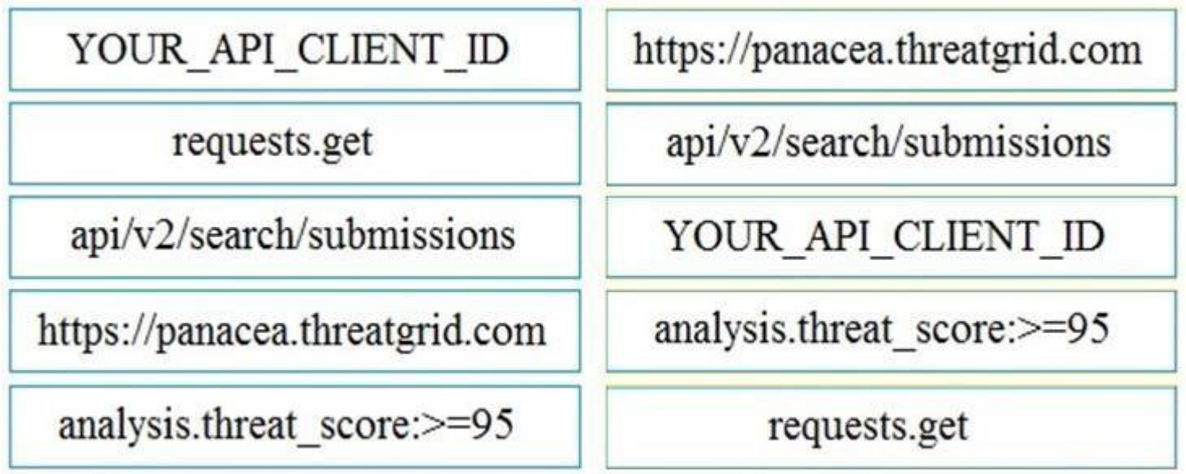
Refer to the exhibit.

Drag and drop the elements from the left onto the script on the right that queries Cisco ThreatGRID for indications of compromise.

Select and Place:

YOUR_API_CLIENT_ID	hostname
requests.get	uri API request
api/v2/search/submissions	API key
https://panacea.threatgrid.com	query parameters
analysis.threat_score:>=95	requests command

Correct Answer:



Section: (none)
Explanation

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

QUESTION 9 What are two advantages of Python virtual environments?
(Choose two.)

A. Virtual environments can move compiled modules between different platforms.
B. Virtual environments permit non-administrative users to install packages.
C. The application code is run in an environment that is destroyed upon exit.
D. Virtual environments allow for stateful high availability.
E. Virtual environments prevent packaging conflicts between multiple Python projects.

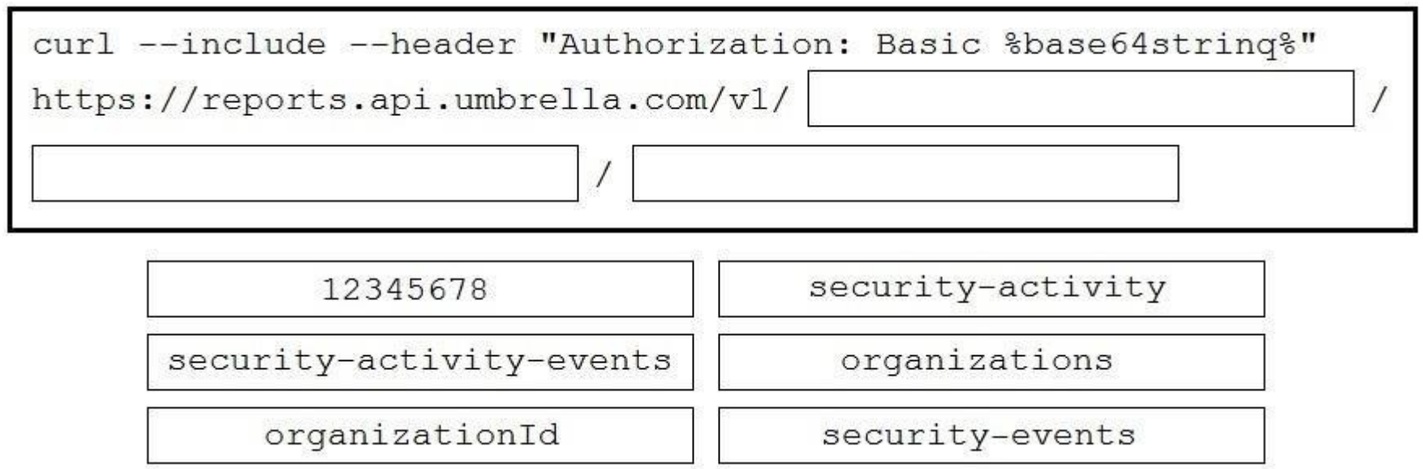
Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

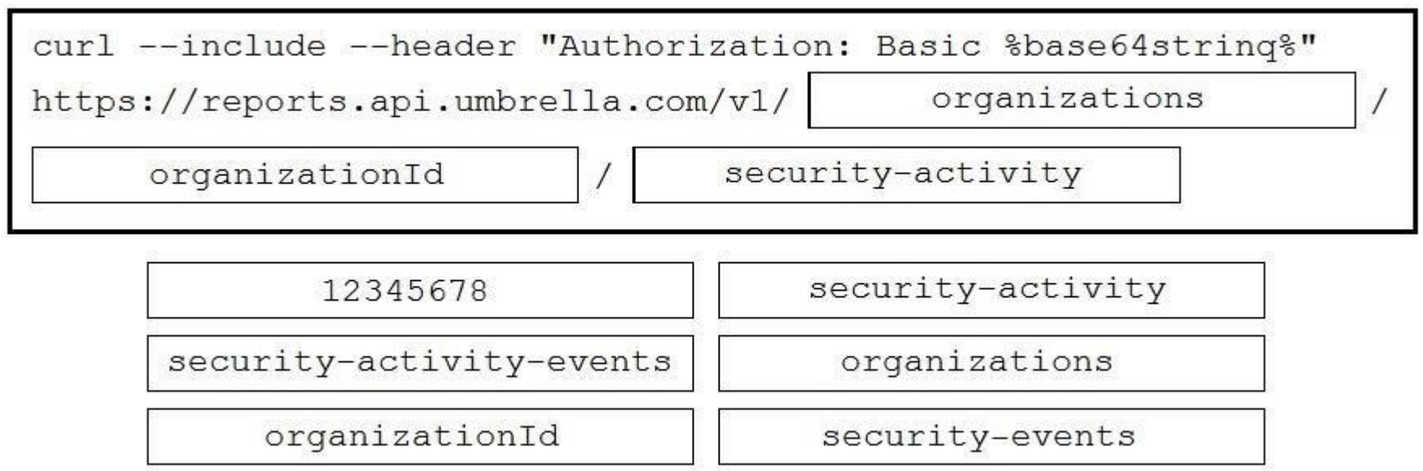
QUESTION 10
DRAG DROP

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:



Section: (none)
Explanation

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

QUESTION 11 When the URI "/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies" is used to make a POST request, what does "e276abec-e0f2-11e3-8169-6d9ed49b625f" represent?

A. API token
B. domain UUID
C. access policy UUID
D. object UUID

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 12 Which snippet is used to create an object for network 10.0.69.0/24 using Cisco Firepower Management Center REST APIs?

```
- 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"
}
```

```
- 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"
}
```

```
- 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": " "
}
```

```
- 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": " "
}
```

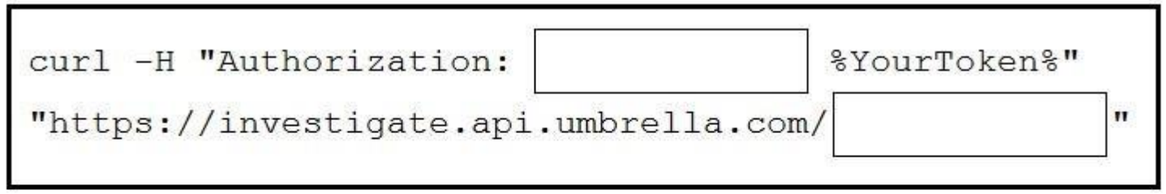
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

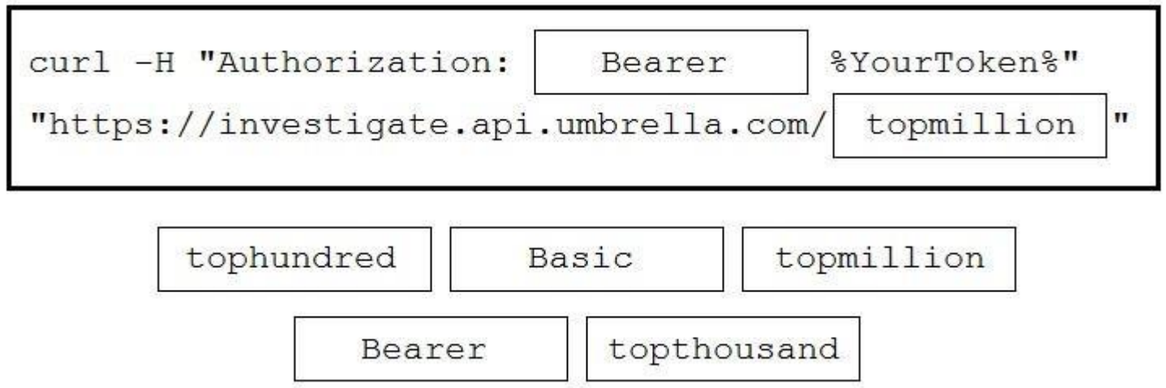
QUESTION 13
DRAG DROP

Drag and drop the code to complete the curl command to query the Cisco Umbrella Investigate API for the umbrella popularity list. Not all options are used.

Select and Place:



Correct Answer:



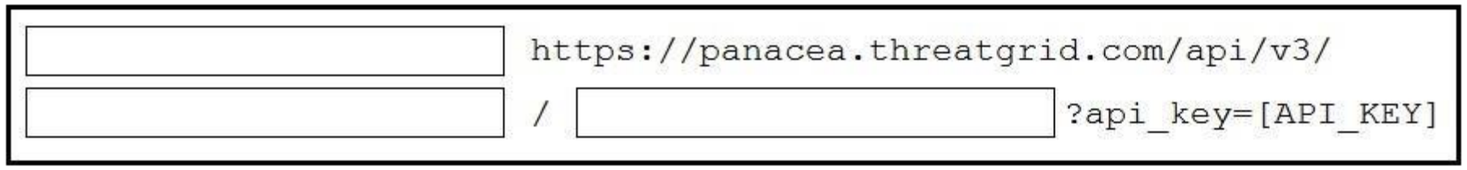
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.umbrella.com/investigate-api/reference

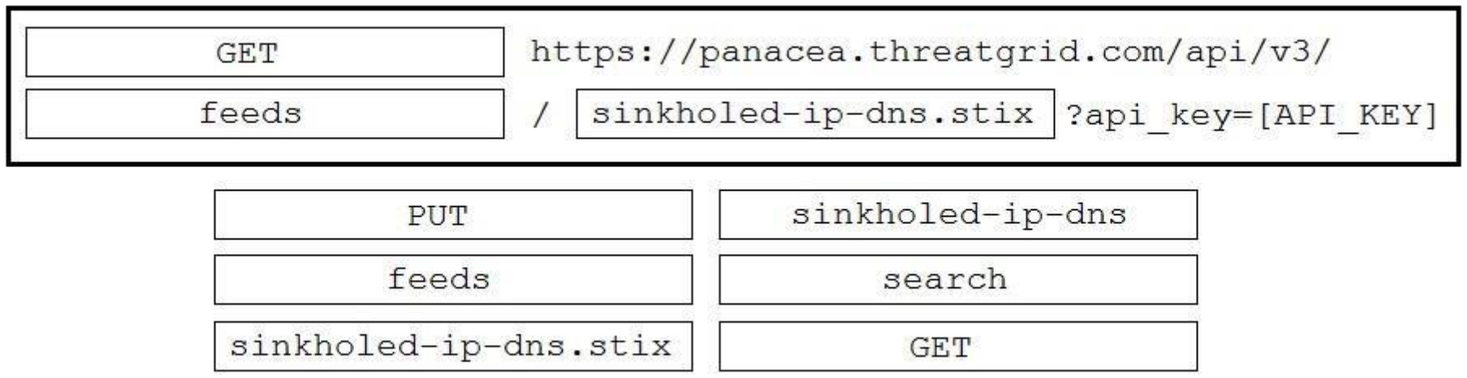
QUESTION 14
DRAG DROP

Drag and drop the items to complete the ThreatGRID API call to return a curated feed of sinkholed-ip-dns in stix format. Not all options are used.

Select and Place:



Correct Answer:



Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/DEVNET-2164.pdf

QUESTION 15
In Cisco AMP for Endpoints, which API queues to find the list of endpoints in the group "Finance Hosts," which has a GUID of **6c3c2005-4c74-4ba7-8dbb-c4d5b6bafe03**?

A. `https://api.amp.cisco.com/v1/endpoints?group[]=6c3c2005-4c74-4ba7-8dbb-c4d5b6bafe03`
B. `https://api.amp.cisco.com/v1/computers?group_guid[]=6c3c2005-4c74-4ba7-8dbb-c4d5b6bafe03`
C. `https://api.amp.cisco.com/v1/computers?group_guid-6c3c2005-4c74-4ba7-8dbb-c4d5b6bafe03`
D. `https://api.amp.cisco.com/v1/endpoints?group-6c3c2005-4c74-4ba7-8dbb-c4d5b6bafe03`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17 Which two URI parameters are needed for the Cisco Stealthwatch Top Alarm Host v1 API? (Choose two.)

A. startAbsolute

B. externalGeos
C. tenantId
D. intervalLength
E. tagID

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18


```
{
  "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"
      }
    ]
}
```


Refer to the exhibit.

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
After changes are made to the Cisco Firepower Threat Defense configuration using the Cisco Firepower Device Manager API, what must be done to ensure that the new policy is activated?

A. Submit a POST to the **/api/fdm/latest/operational/deploy** URI.
B. Submit a GET to the **/api/fdm/latest/operational/deploy** URI.
C. Submit a PUT to the **/api/fdm/latest/devicesettings/pushpolicy** URI.
D. Submit a POST to the **/api/fdm/latest/devicesettings/pushpolicy** URI.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20

```
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"}')**

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Thank You for Trying Our Product

EnsurePass Certification Exam Features:

♀ **More than 99,900 Satisfied Customers Worldwide.**

♀ **Average 99.9% Success Rate.**

♀ **Free Update to match latest and real exam scenarios**

♀ **Instant Download Access! No Setup required**

♀ **Questions & Answers are downloadable in PDF format and VCE test engine format.**

♀ **100% Guaranteed Success or 100% Money Back Guarantee**

♀ **Fast, helpful support 24x7.**

View list of all certification exams:

https://www.ensurepass.com

2023 Coupon Code 20% OFF : PASS20