300-735.VCEplus.premium.exam.58q

Number: 300-735
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

300-735

Automating and Programming Cisco Security Solutions

Version 1.0

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.

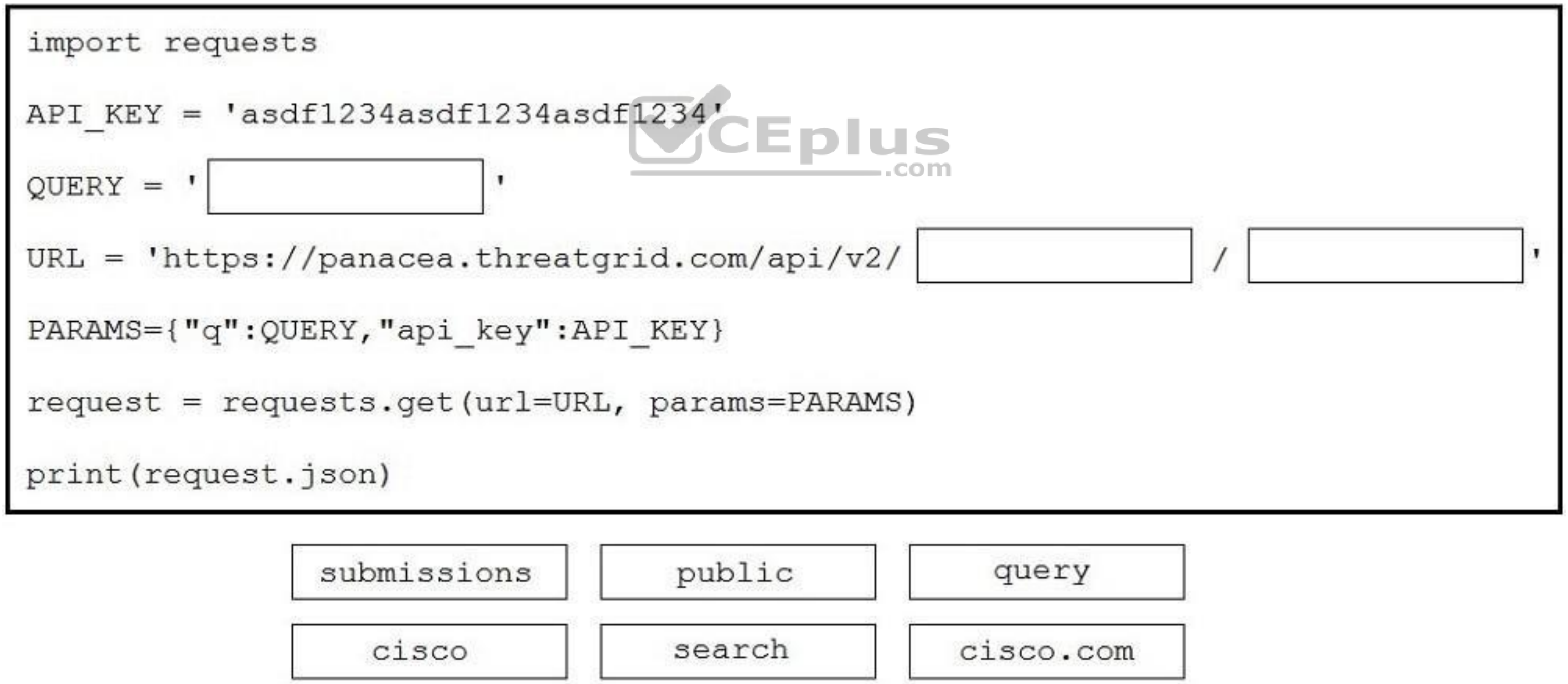
Correct Answer: B
Section: (none)
Explanation

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.

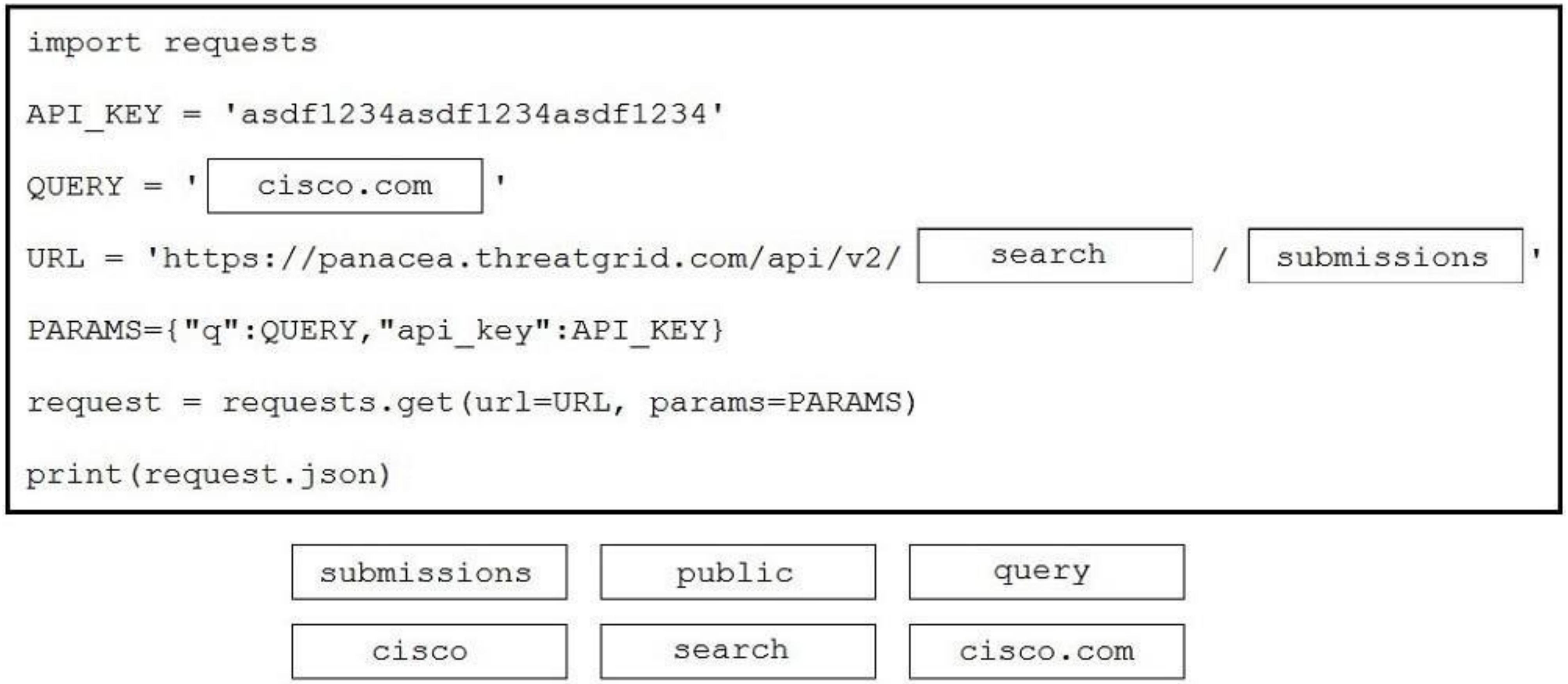
Select and Place:



```
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:

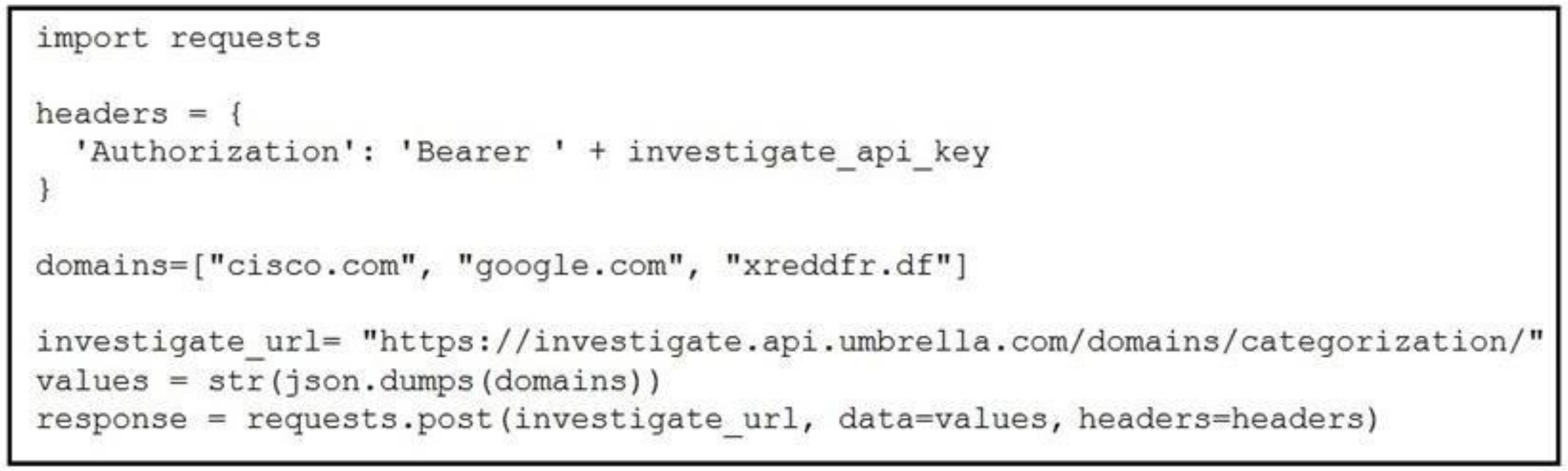


```
import requests

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)
```

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?

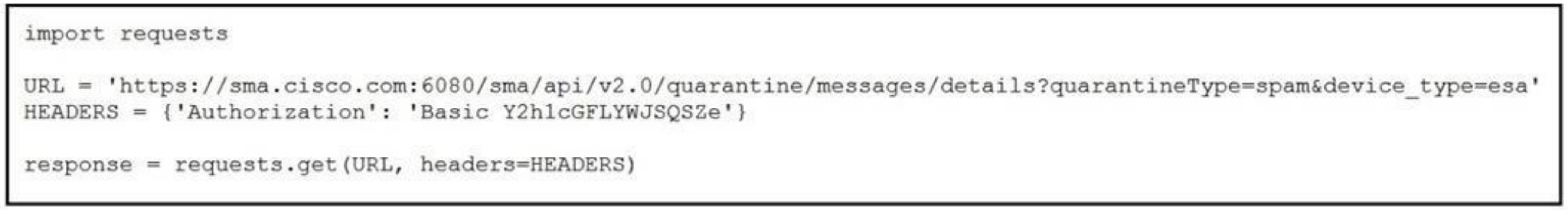
A. error message and status code of 403
B. newly created domains in Cisco Umbrella Investigate

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.

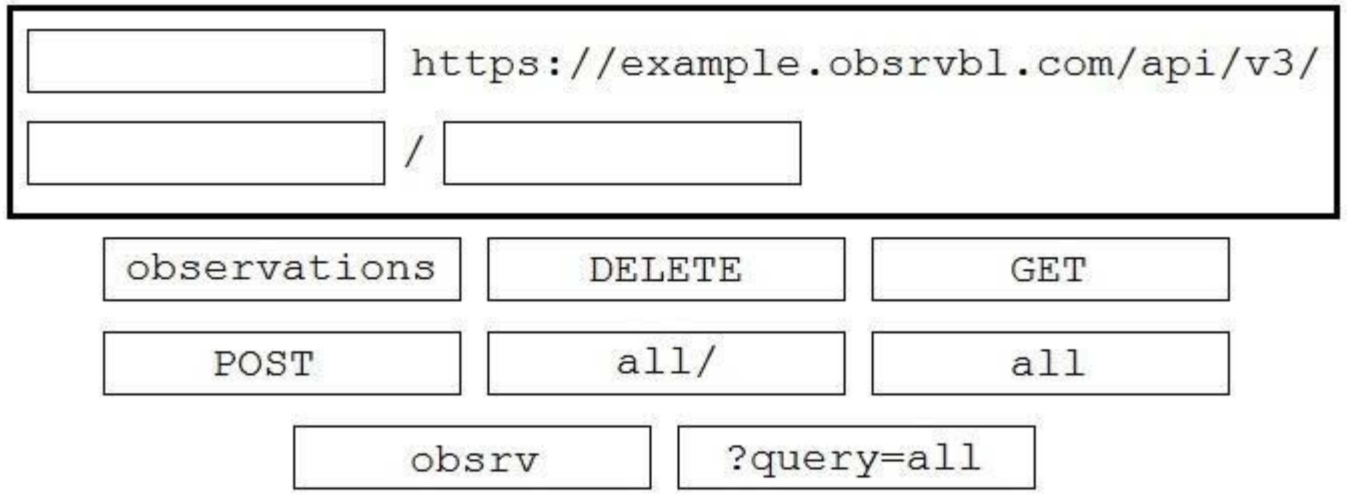
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

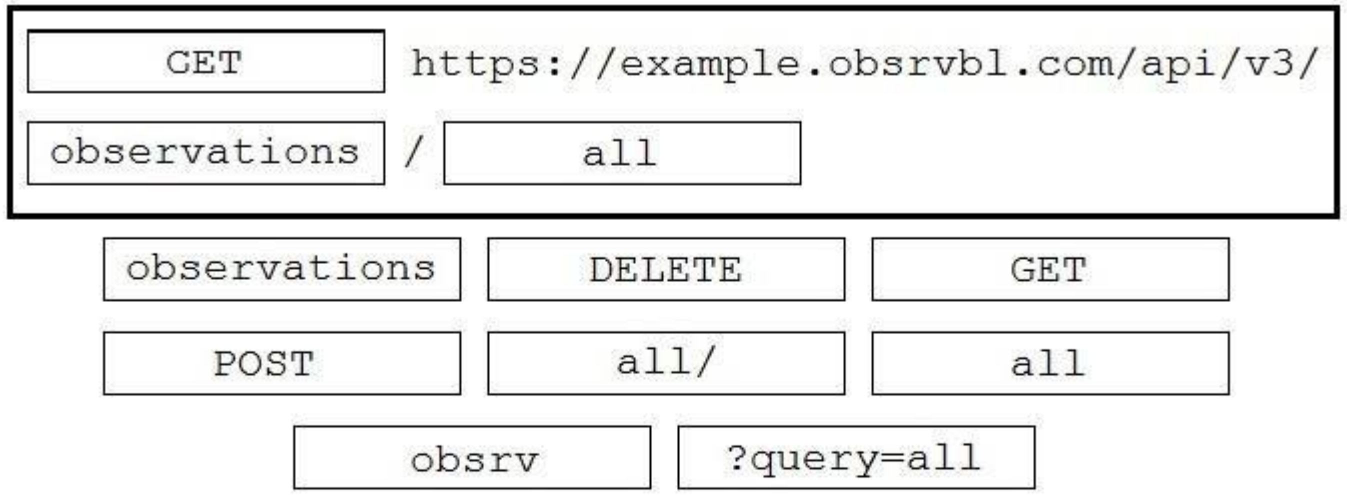
QUESTION 5
DRAG DROP

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:



GET https://example.obsrvbl.com/api/v3/

observations / all

observations DELETE GET

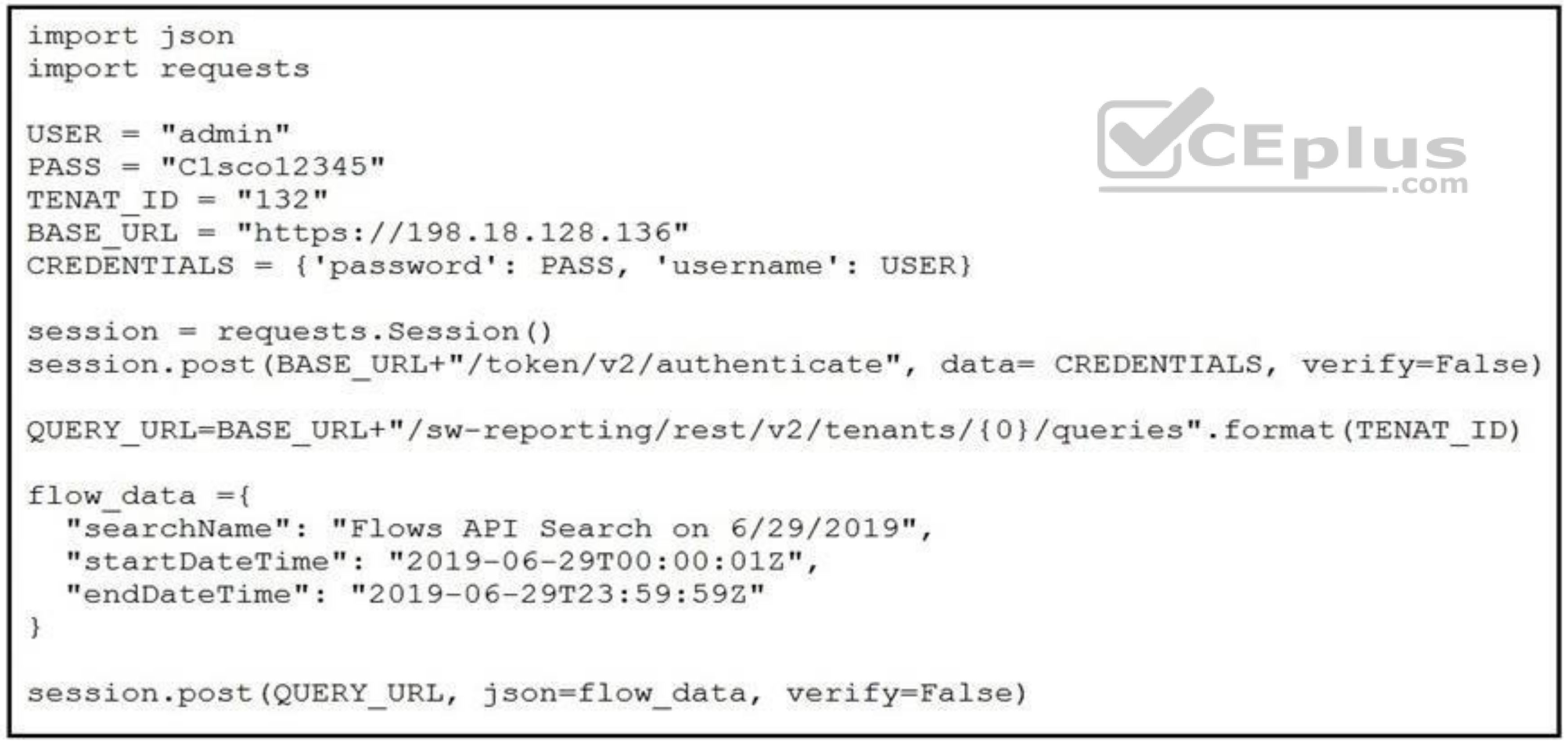
POST all/ all

obsrv ?query=all

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.)

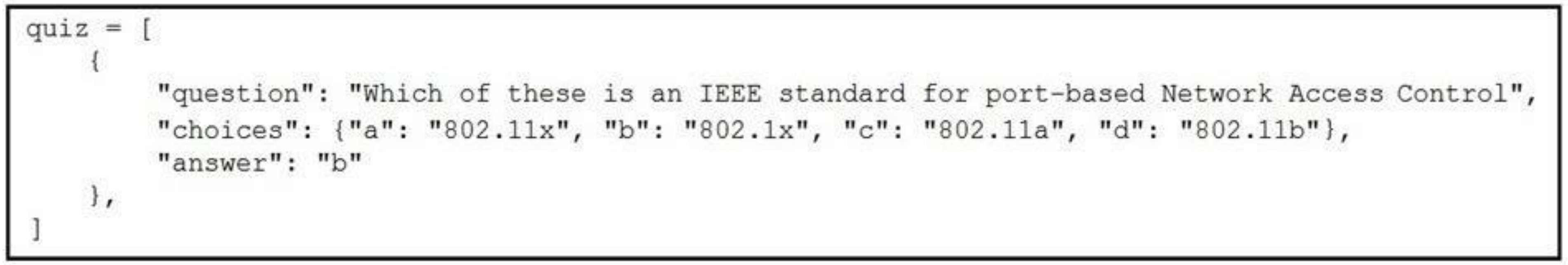
A. Add recordLimit. followed by an integer (key:value) to the flow_data.
B. Add a **for** loop at the end of the script, and print each key value pair separately.
C. Add flowLimit, followed by an integer (key:value) to the flow_data.

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.

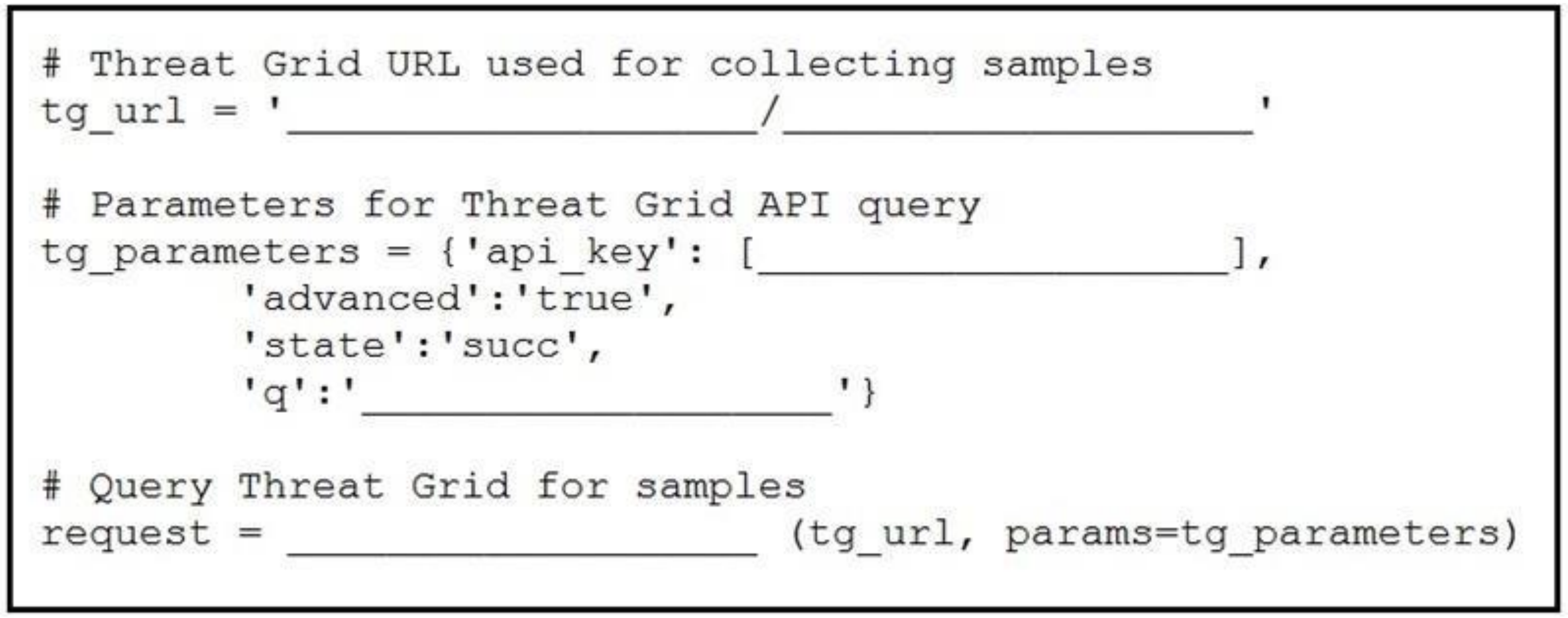
Which expression prints the text "802.1x"?

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

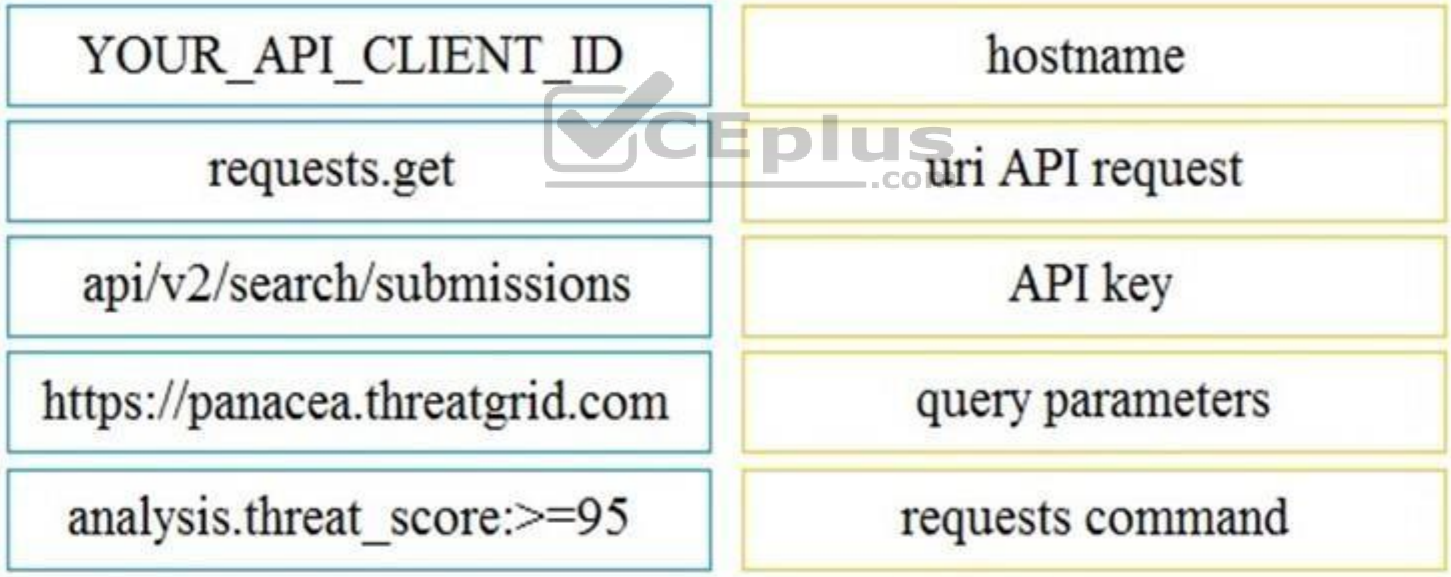


```
# Threat Grid URL used for collecting samples
tg_url = '____________________/____________________'

# 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.

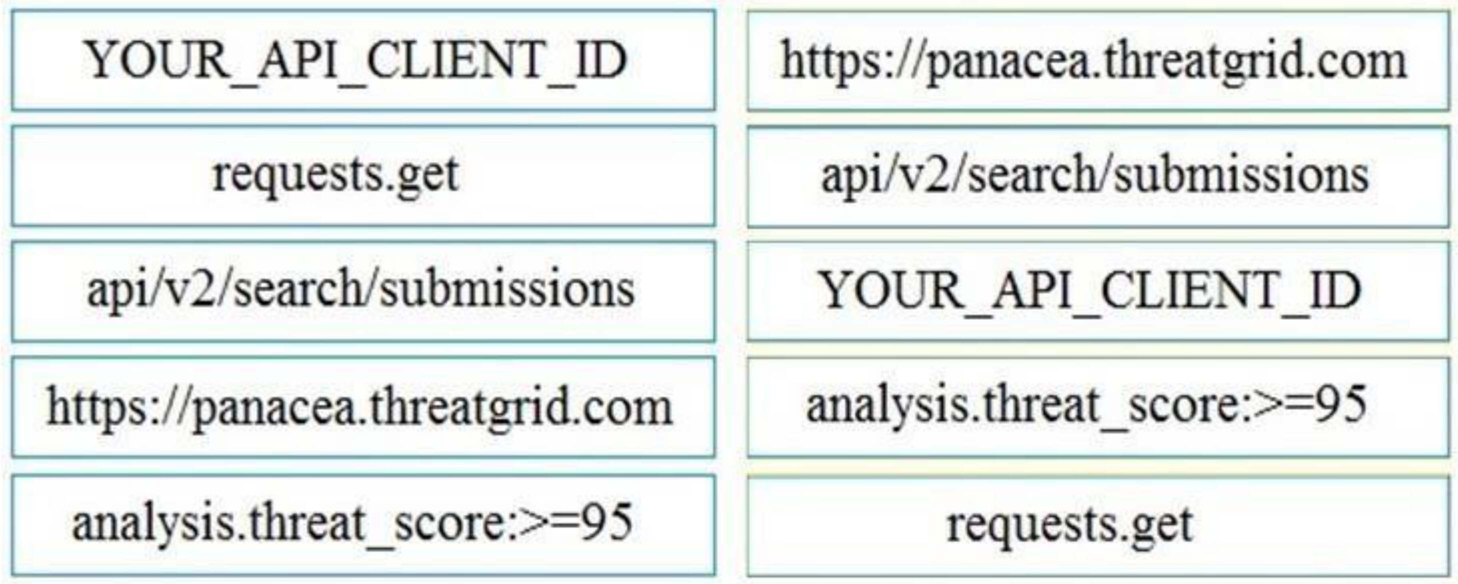
Drag and drop the elements from the left onto the script on the right that queries Cisco ThreatGRID for indications of compromise.

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:



YOUR_API_CLIENT_ID	https://panacea.threatgrid.com
requests.get	api/v2/search/submissions
api/v2/search/submissions	YOUR_API_CLIENT_ID
https://panacea.threatgrid.com	analysis.threat_score:>=95
analysis.threat_score:>=95	requests.get

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.

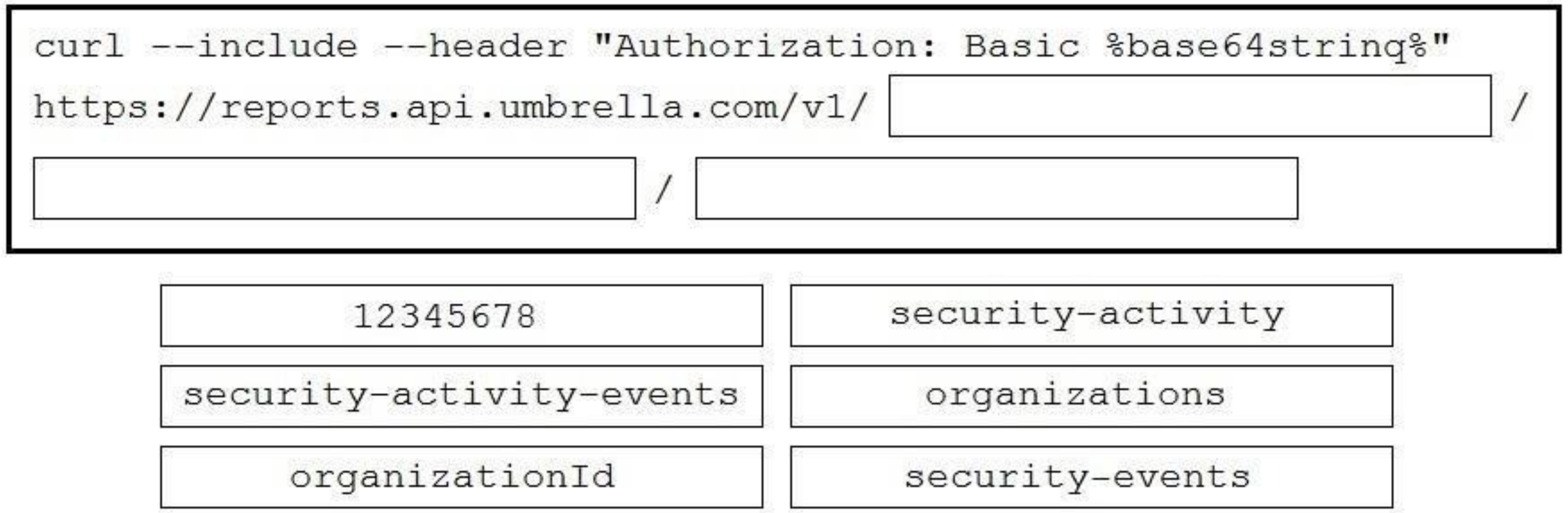
Correct Answer: CE
Section: (none)
Explanation

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.

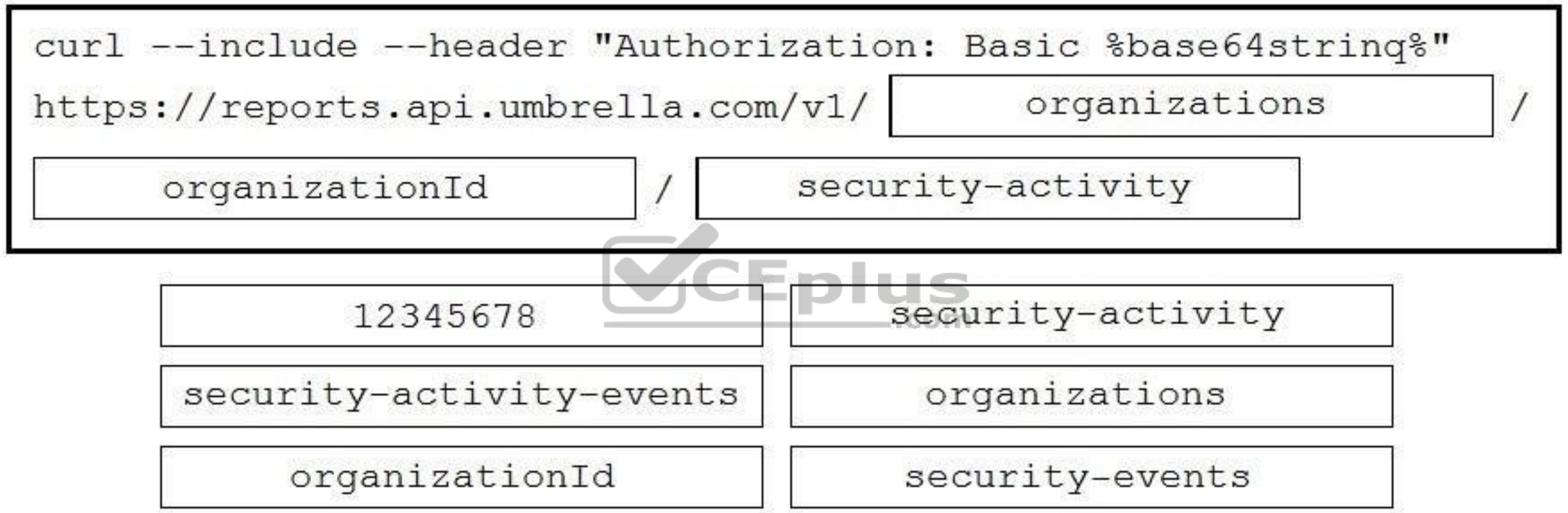
Select and Place:



```
curl --include --header "Authorization: Basic %base64string%"
https://reports.api.umbrella.com/v1/ [          ] /
[          ] / [          ]
```

12345678	security-activity
security-activity-events	organizations
organizationId	security-events

Correct Answer:



```
curl --include --header "Authorization: Basic %base64string%"
https://reports.api.umbrella.com/v1/ [organizations] /
[organizationId] / [security-activity]
```

12345678	security-activity
security-activity-events	organizations
organizationId	security-events

Section: (none)
Explanation

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

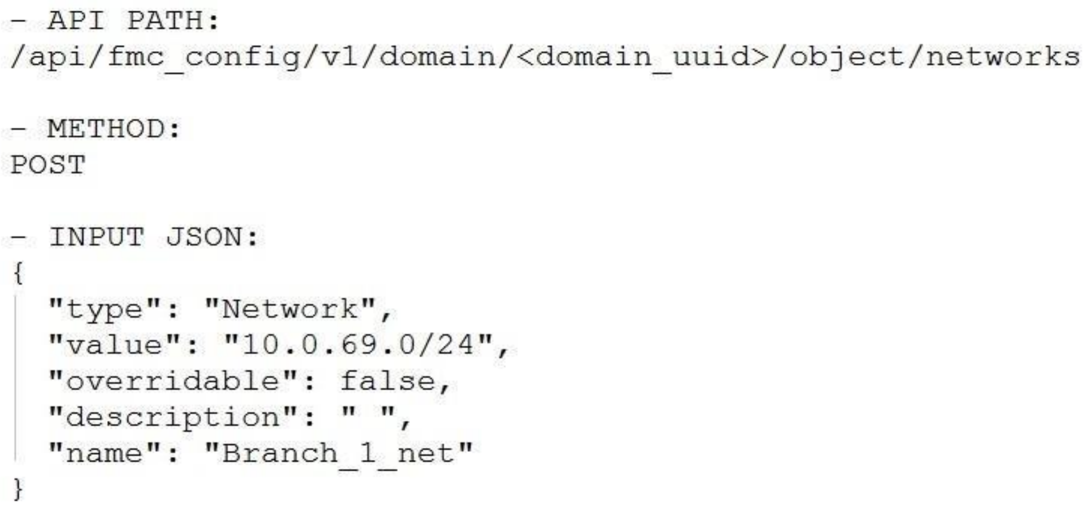
QUESTION 11 When the URI "/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies" is used to make a POST request, what does "e276abec-e0f2-11e3-8169-6d9ed49b625f" represent?

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

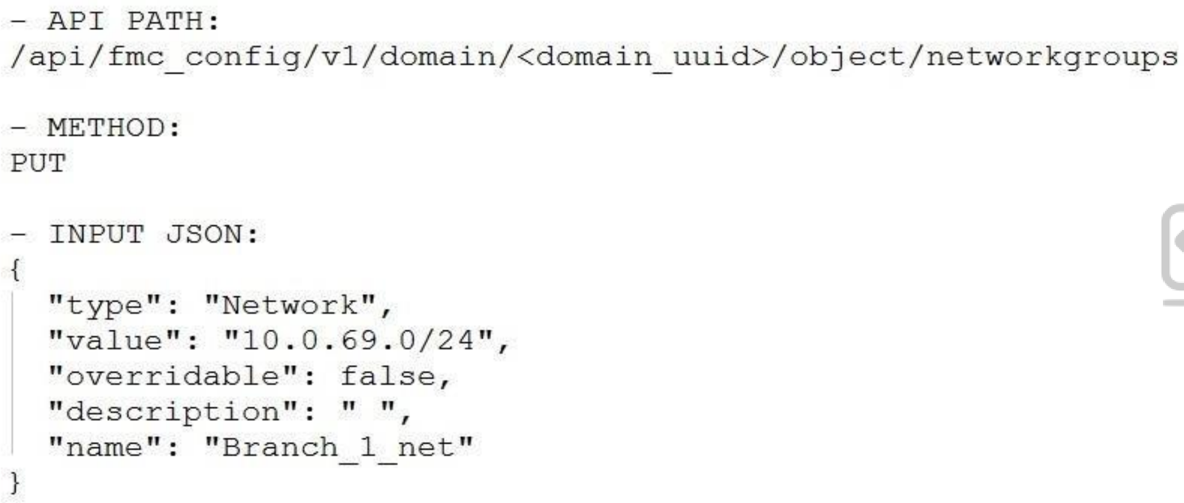
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

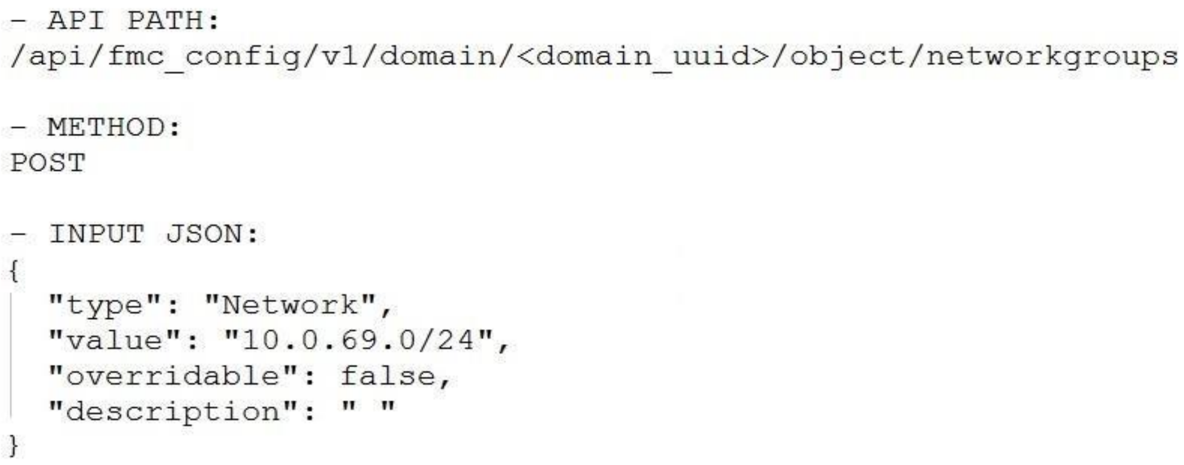
QUESTION 12 Which snippet is used to create an object for network 10.0.69.0/24 using Cisco Firepower Management Center REST APIs? A.



```
- 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"
}
```

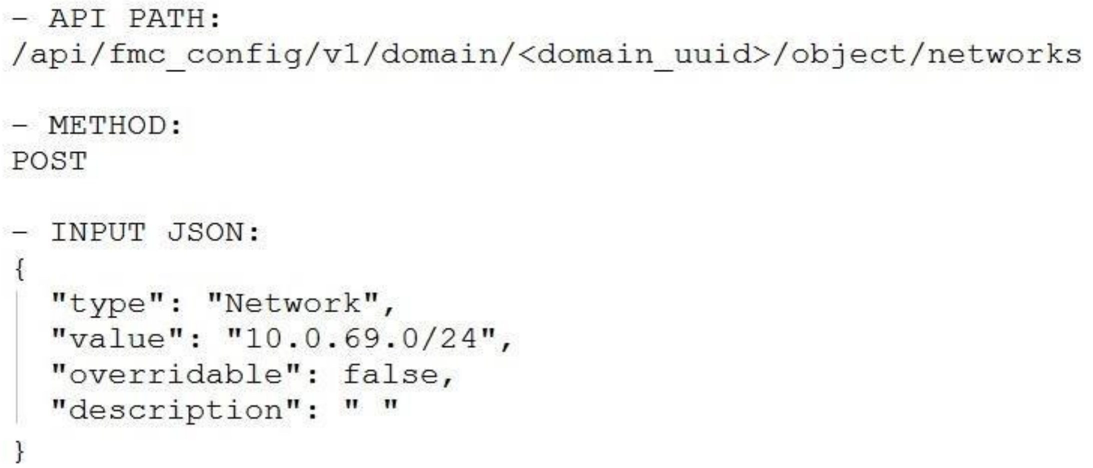


```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/networkgroups

- 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": " "
}
```

B. C.



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

D.

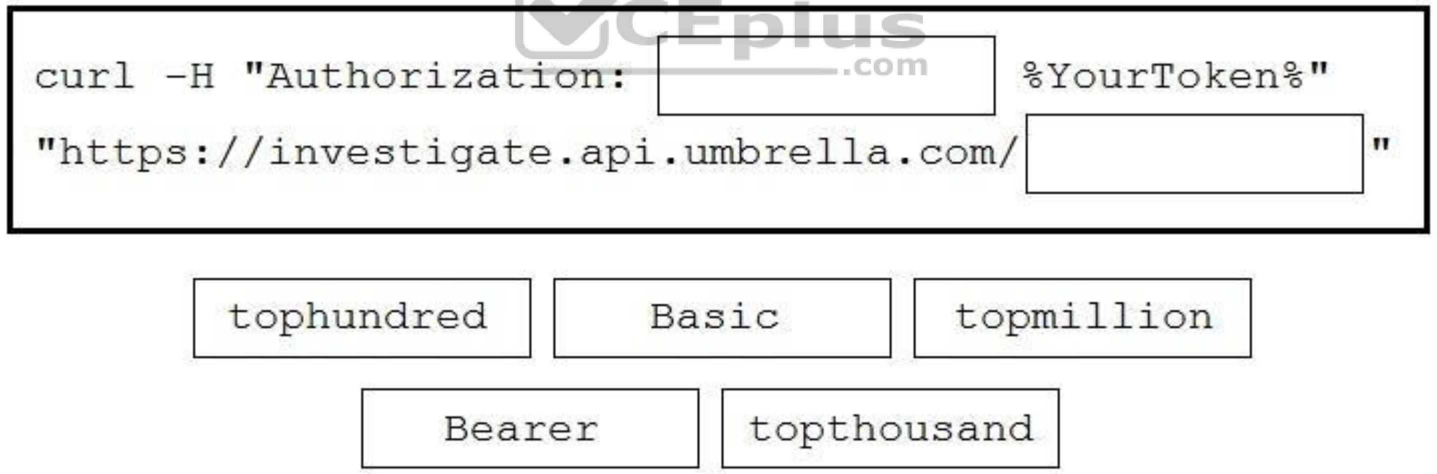
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
DRAG DROP

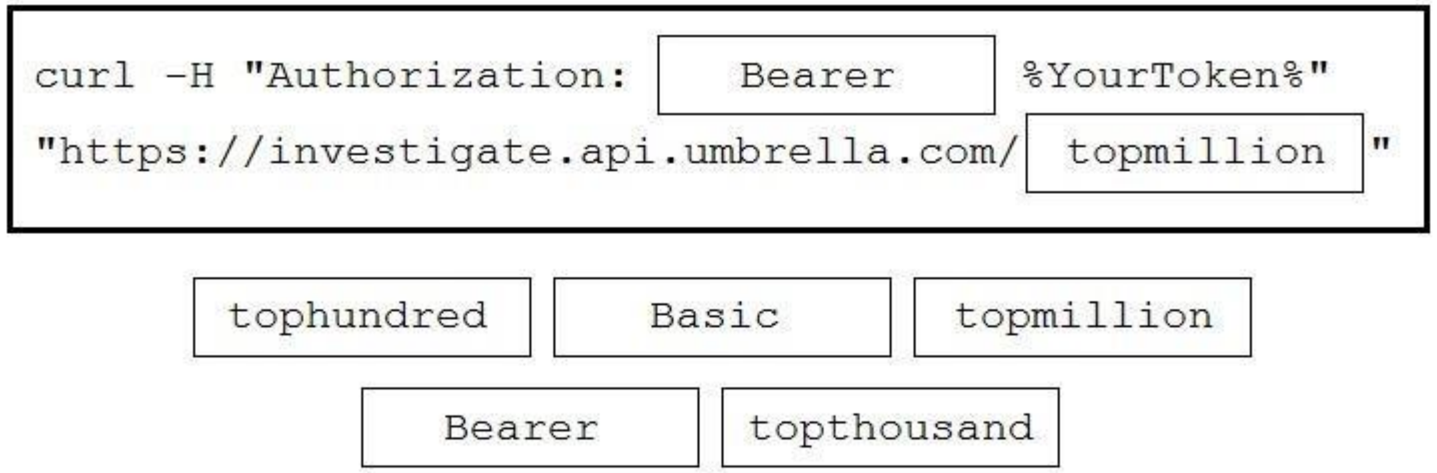
Drag and drop the code to complete the curl command to query the Cisco Umbrella Investigate API for the umbrella popularity list. Not all options are used.

Select and Place:



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

Correct Answer:



```
curl -H "Authorization: [Bearer] %YourToken%"
"https://investigate.api.umbrella.com/[topmillion]"
```

tophundred | Basic | topmillion

Bearer | topthousand

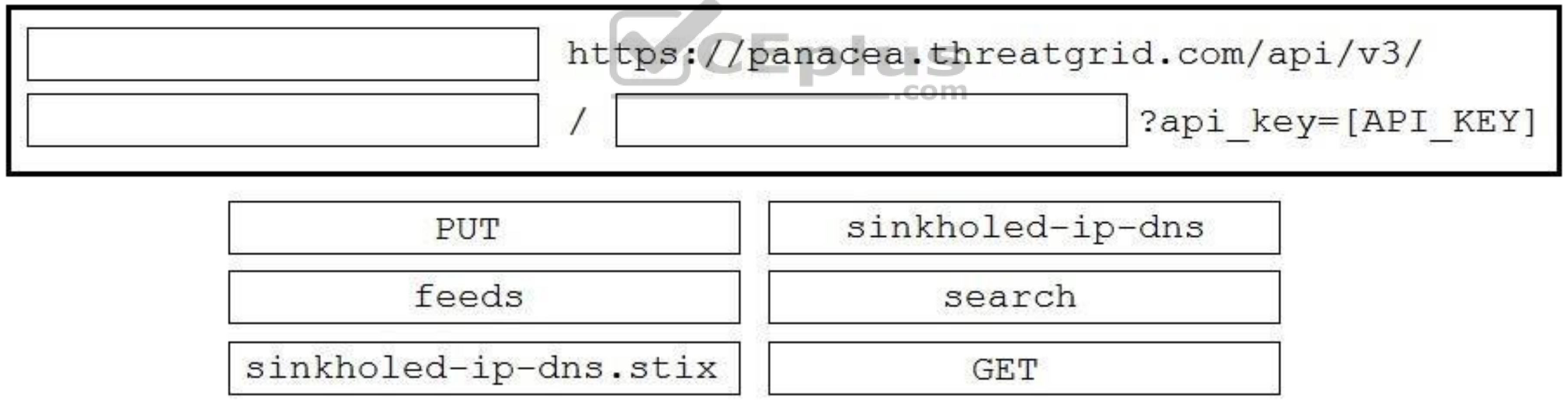
Section: (none)
Explanation

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:



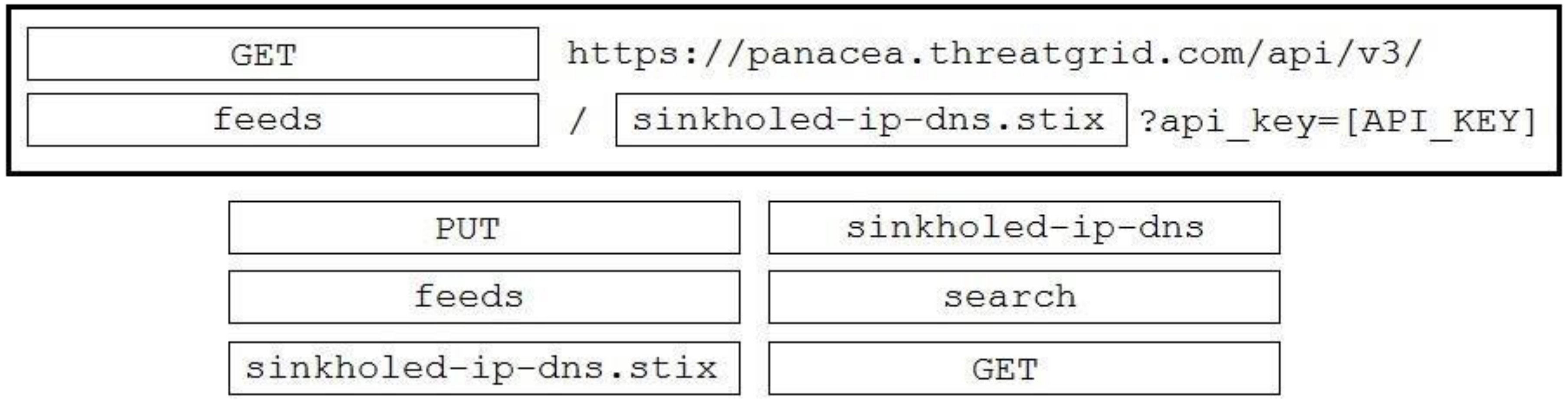
```
[          ] https://panacea.threatgrid.com/api/v3/
[          ] / [          ] ?api_key=[API_KEY]
```

PUT | sinkholed-ip-dns

feeds | search

sinkholed-ip-dns.stix | GET

Correct Answer:



GET https://panacea.threatgrid.com/api/v3/

feeds / sinkholed-ip-dns.stix ?api_key=[API_KEY]

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.)

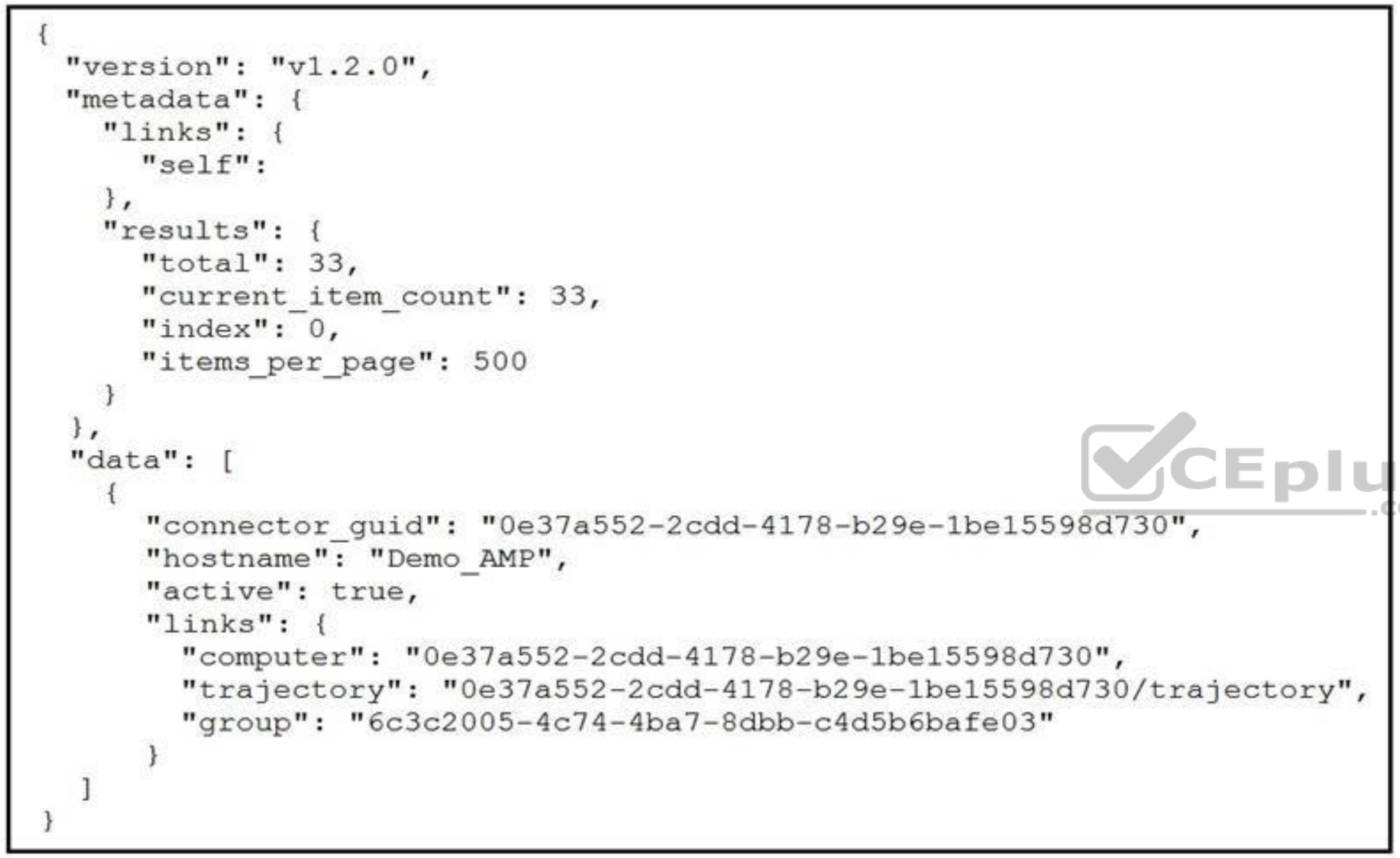
A. startAbsolute

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:

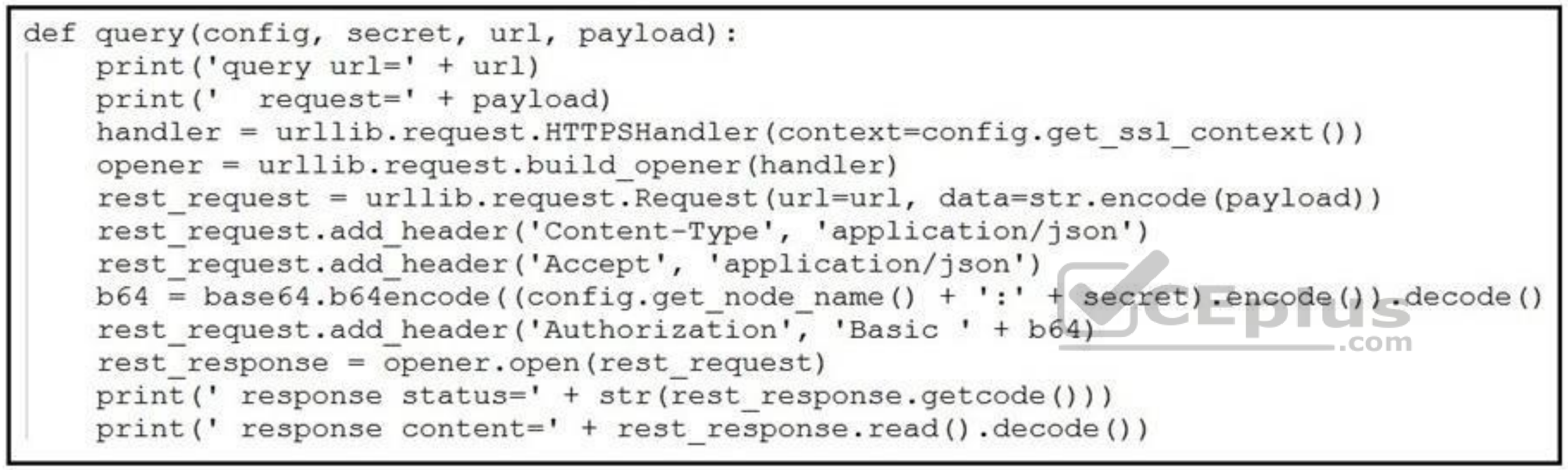
QUESTION 19
After changes are made to the Cisco Firepower Threat Defense configuration using the Cisco Firepower Device Manager API, what must be done to ensure that the new policy is activated?

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:

QUESTION 21 Which two API capabilities are available on Cisco Identity Services Engine?
(Choose two.)

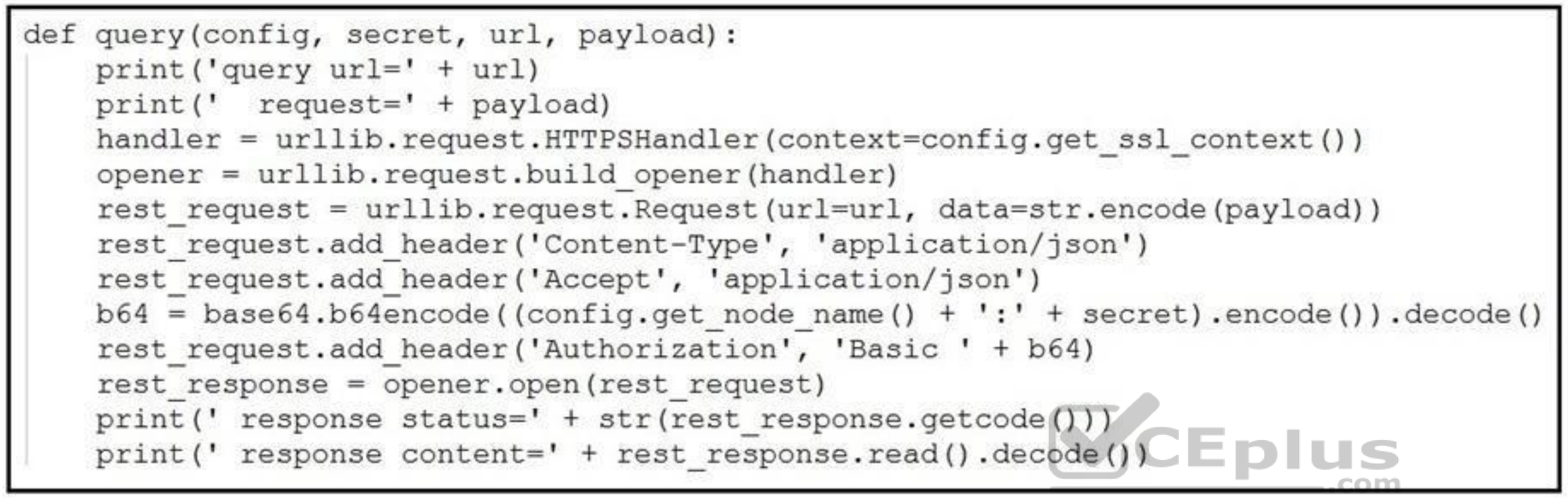
A. Platform Configuration APIs
B. Monitoring REST APIs

C. Performance Management REST APIs
D. External RESTful Services APIs
E. Internal RESTful Services APIs

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
DRAG DROP

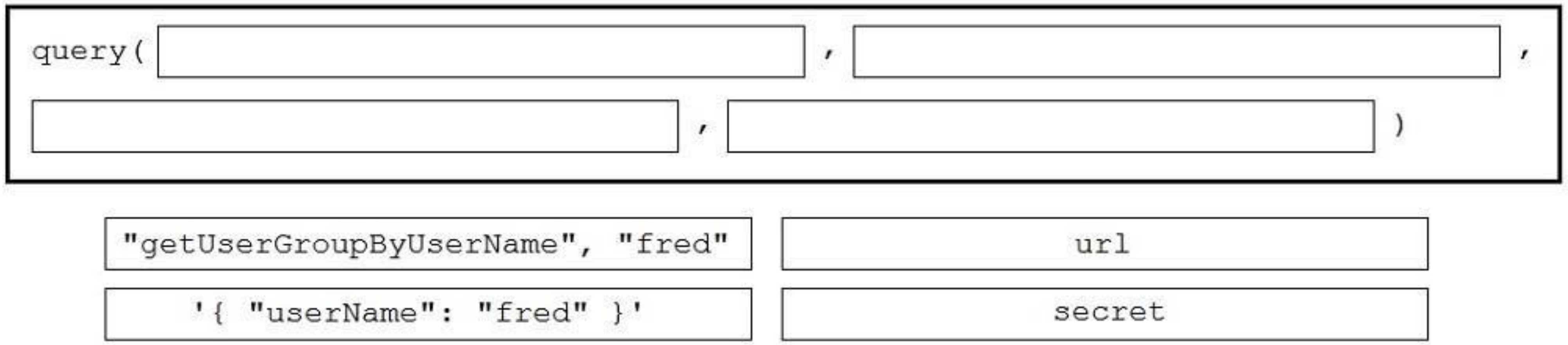


```
def query(config, secret, url, payload):
    print('query url=' + url)
    print('  request=' + payload)
    handler = urllib.request.HTTPSHandler(context=config.get_ssl_context())
    opener = urllib.request.build_opener(handler)
    rest_request = urllib.request.Request(url=url, data=str.encode(payload))
    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 will be used to query the service "com.cisco.ise.session" via Cisco pxGrid 2.0 APIs.

Drag and drop the code to construct a Python call to the "query" function to identify the user groups that are associated with the user "fred". Not all options are used.

Select and Place:



```
query( ______ , ______ ,
______ , ______ )
```

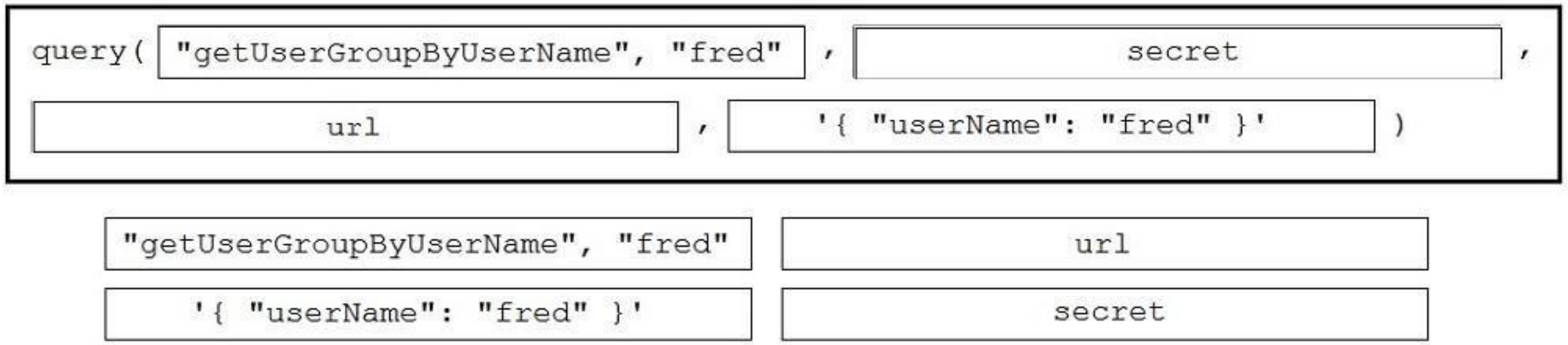
"getUserGroupByUserName", "fred"

url

'{ "userName": "fred" }'

secret

Correct Answer:



```
query( "getUserGroupByUserName", "fred" , secret ,
url , '{ "userName": "fred" }' )
```

```
"getUserGroupByUserName", "fred"      url
'{ "userName": "fred" }'              secret
```

Section: (none)
Explanation

Explanation/Reference:

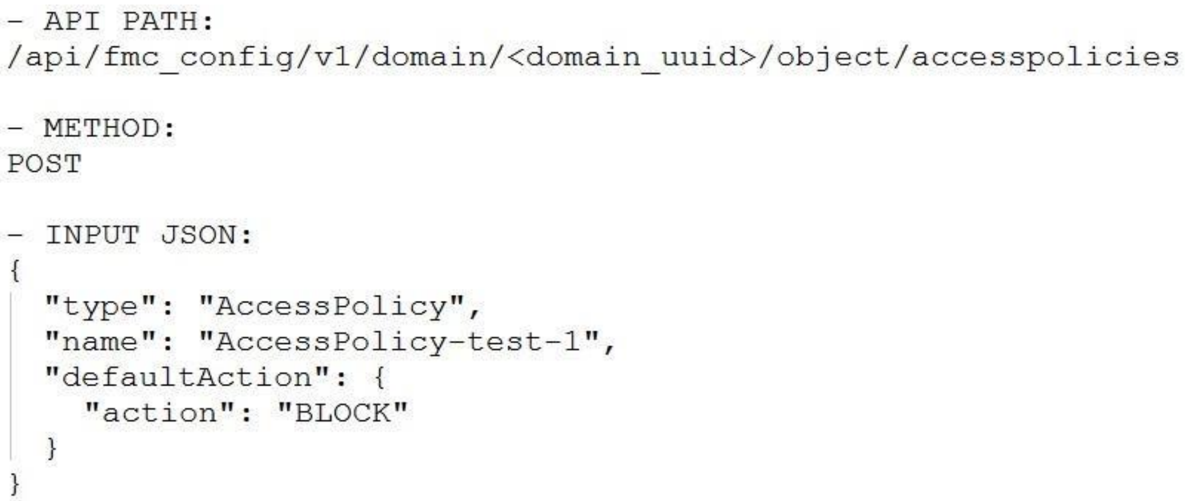
QUESTION 23 Which API capability is available on Cisco Firepower devices?

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

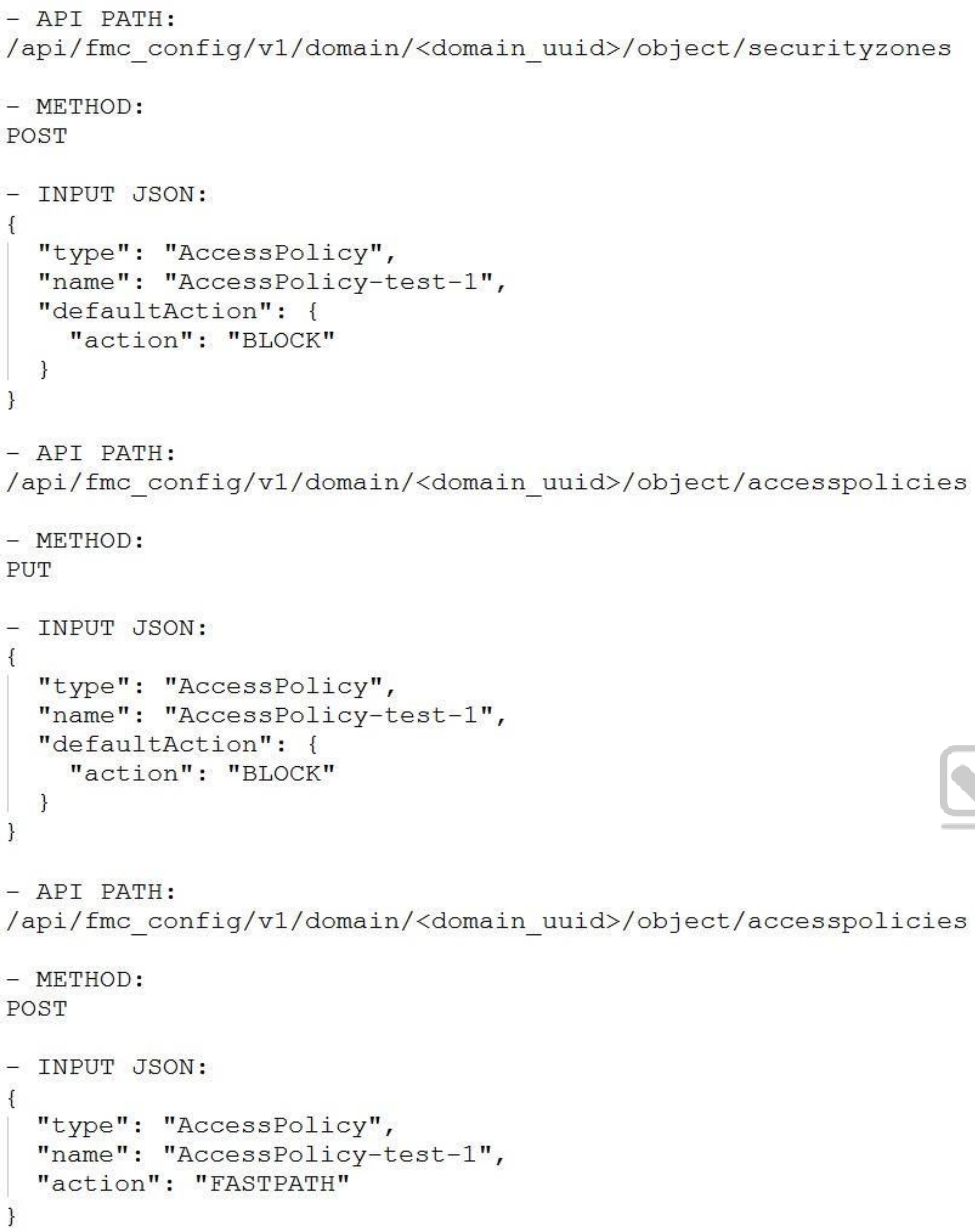
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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"
  }
}

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

- METHOD:
PUT

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

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

- METHOD:
POST

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

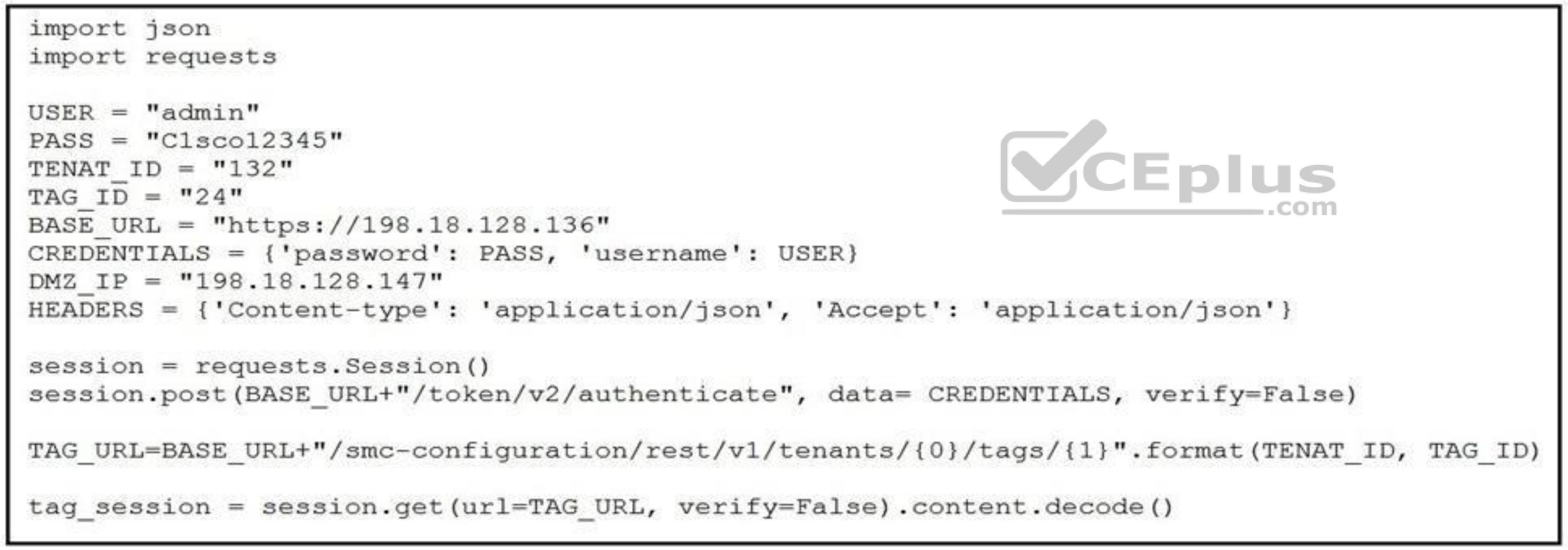
B. C.

D.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

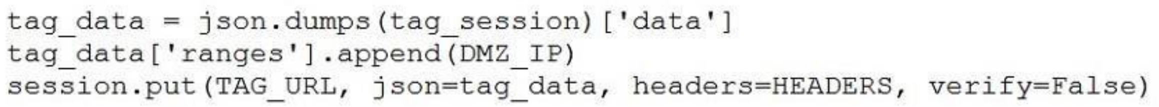
QUESTION 25



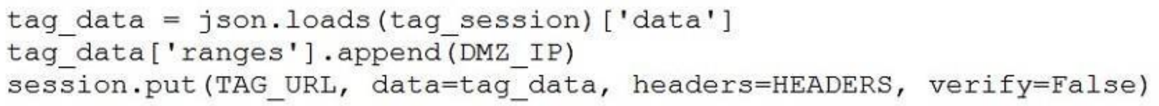
```
import json
import requests

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.

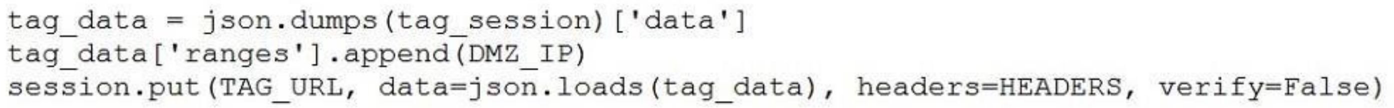
Which code segment completes the script and achieves the goal? A.



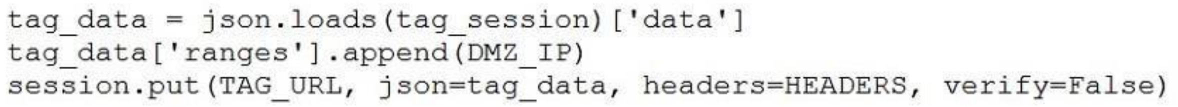
```
tag_data = json.dumps(tag_session)['data']
tag_data['ranges'].append(DMZ_IP)
session.put(TAG_URL, json=tag_data, headers=HEADERS, verify=False)
```



```
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)
```



```
tag_data = json.loads(tag_session)['data']
tag_data['ranges'].append(DMZ_IP)
session.put(TAG_URL, json=tag_data, headers=HEADERS, verify=False)
```

B.

C.

D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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
Section: (none)
Explanation

Explanation/Reference:

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
Section: (none)
Explanation

Explanation/Reference:

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
Section: (none)
Explanation

Explanation/Reference:

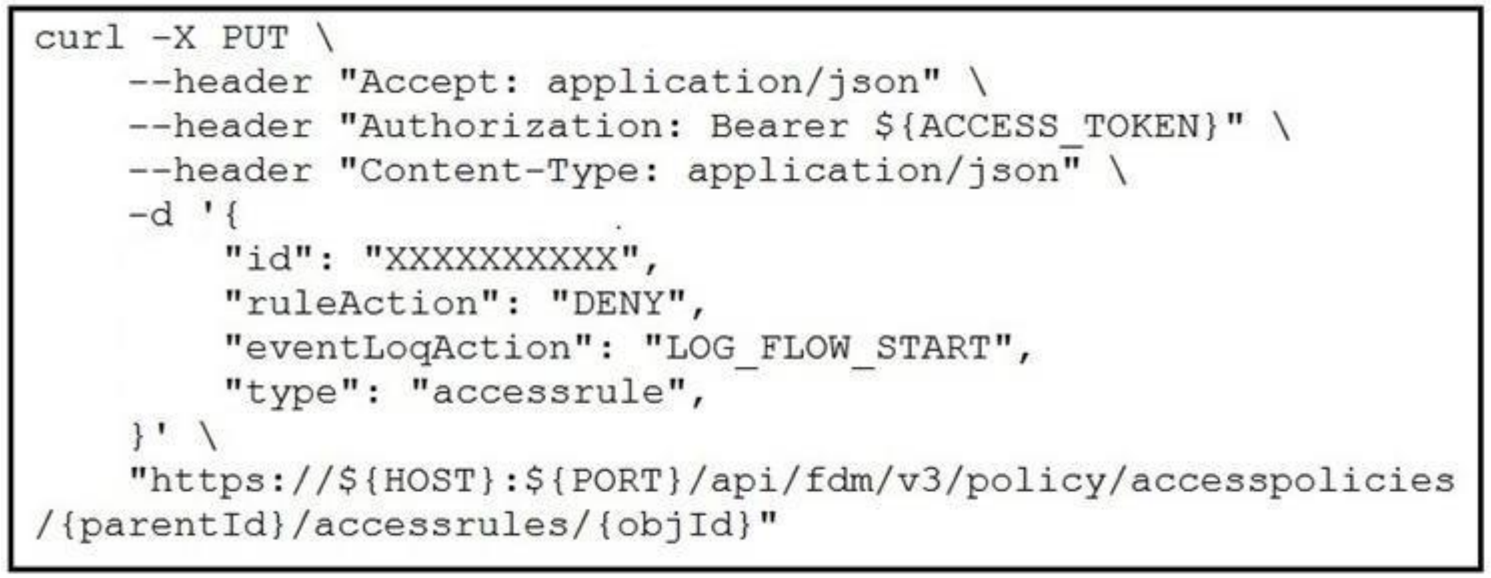
QUESTION 29 Which curl command lists all tags (host groups) that are associated with a tenant using the Cisco Stealthwatch Enterprise API?

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30



```
curl -X PUT \
    --header "Accept: application/json" \
    --header "Authorization: Bearer ${ACCESS_TOKEN}" \
    --header "Content-Type: application/json" \
    -d '{
        "id": "XXXXXXXXXX",
        "ruleAction": "DENY",
        "eventLoqAction": "LOG_FLOW_START",
        "type": "accessrule",
    }' \
    "https://${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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
FILL BLANK

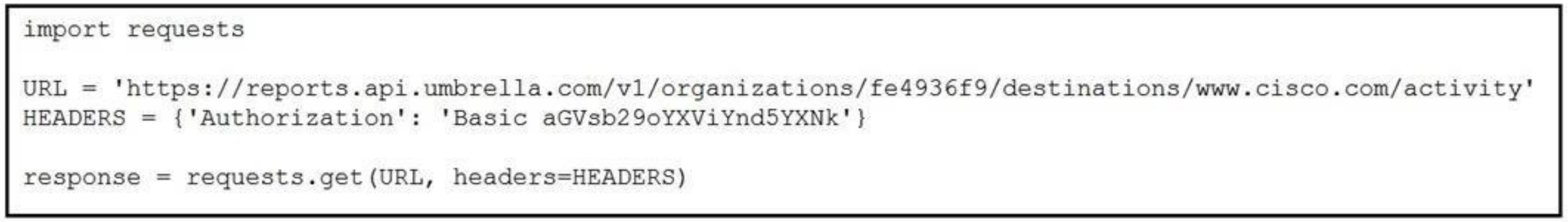
Fill in the blank to complete the statement with the correct technology.

Cisco __________ Investigate provides access to data that pertains to DNS security events and correlations collected by the Cisco security team.

Correct Answer: Umbrella
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32



```
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
Section: (none)
Explanation

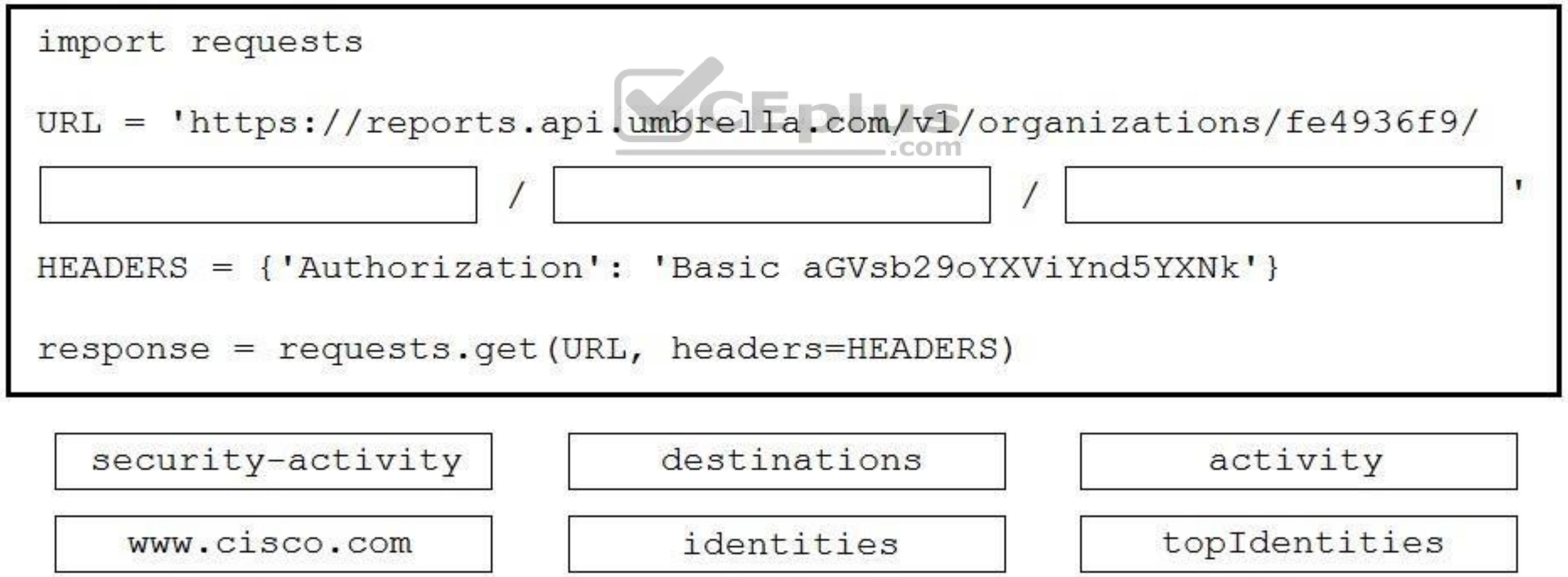
Explanation/Reference:

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:



```
import requests

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

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

security-activity

destinations

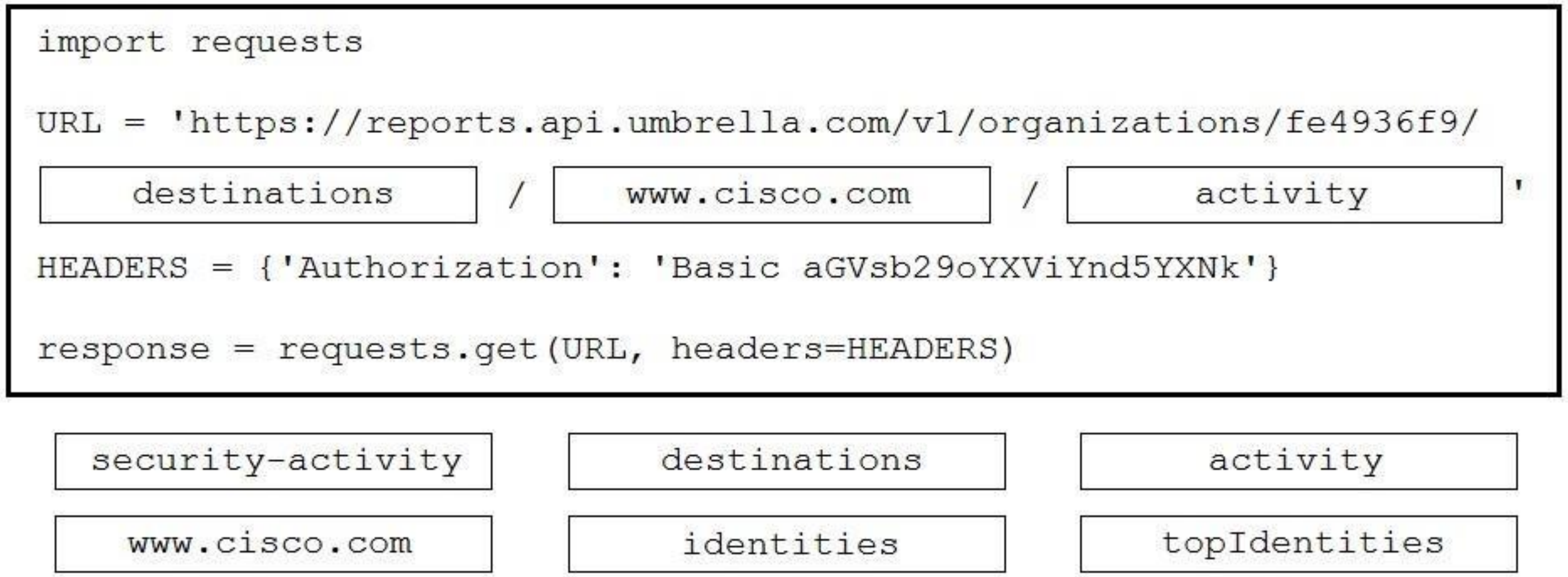
activity

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 aGVsb29oYXViYnd5YXNk'}

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

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

Section: (none)
Explanation

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

QUESTION 34 Which two destinations are supported by the Cisco Security Management Appliance reporting APIs? (Choose two.)

A. email
B. Microsoft Word file
C. FTP
D. web
E. csv file

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

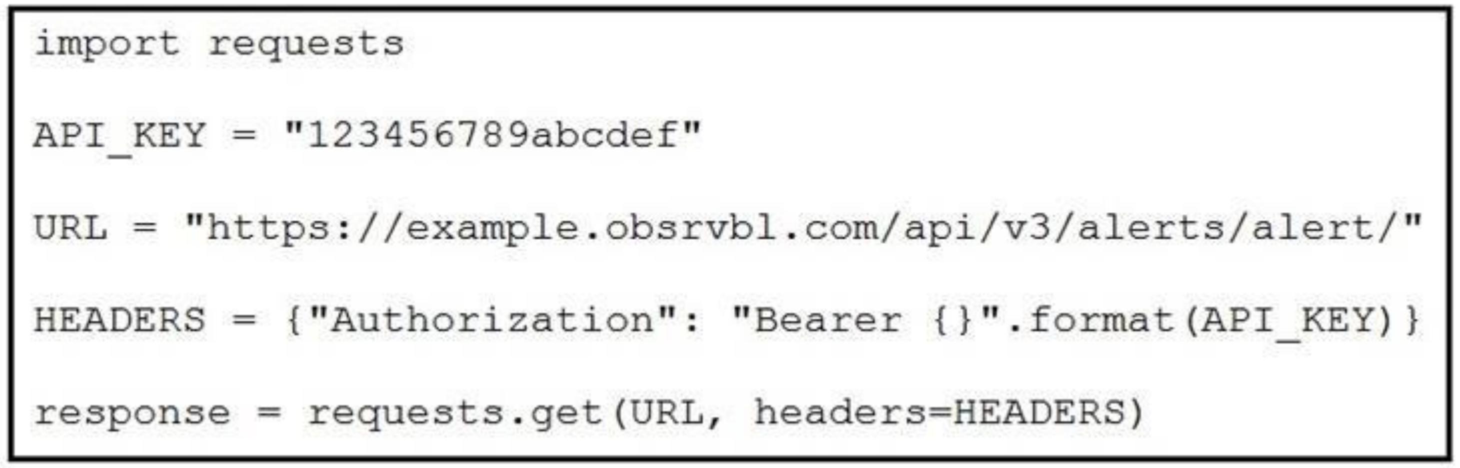
QUESTION 35 What are two capabilities of Cisco Firepower Management Center eStreamer? (Choose two.)

A. eStreamer is used to get sources for intelligence services.
B. eStreamer is used to send malware event data.
C. eStreamer is used to get a list of access control policies.
D. eStreamer is used to send policy data.
E. eStreamer is used to send intrusion event data.

Correct Answer: BE
Section: (none)

Explanation
Explanation/Reference:

QUESTION 36



```
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)
```

Refer to the exhibit. A security engineer created a script and successfully executed it to retrieve all currently open alerts.

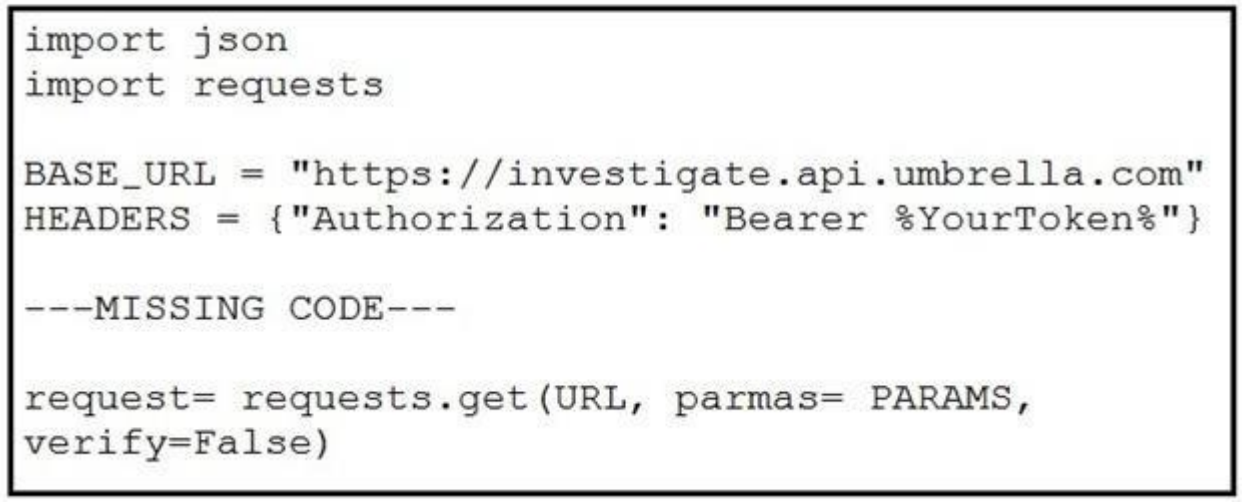
Which print command shows the first returned alert?

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37



```
import json
import requests

BASE_URL = "https://investigate.api.umbrella.com"
HEADERS = {"Authorization": "Bearer %YourToken%"}

---MISSING CODE---

request= requests.get(URL, parmas= PARAMS,
verify=False)
```

Refer to the exhibit. A network operator must create a Python script that makes an API request to Cisco Umbrella to do a pattern search and return all matched URLs with category information.

Which code completes the script?

A.
```
URL = BASE_URL + "/find/exa\[a-z\]ple.com"
PARAMS = { "categoryinclude" : "true"}
```

B.
```
URL = BASE_URL + "/find/exa\[a-z\]ple.com"
PARAMS = { "returncategory" : "true"}
```

C.
```
URL = BASE_URL + "/find/exa\[a-z\]ple.com"
PARAMS = { "includeCategory" : "true"}
```

D.
```
URL = BASE_URL + "/find/exa\[a-z\]ple.com"
PARAMS = { "returnCategory" : "true"}
```

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38 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
Section: (none)
Explanation

Explanation/Reference:

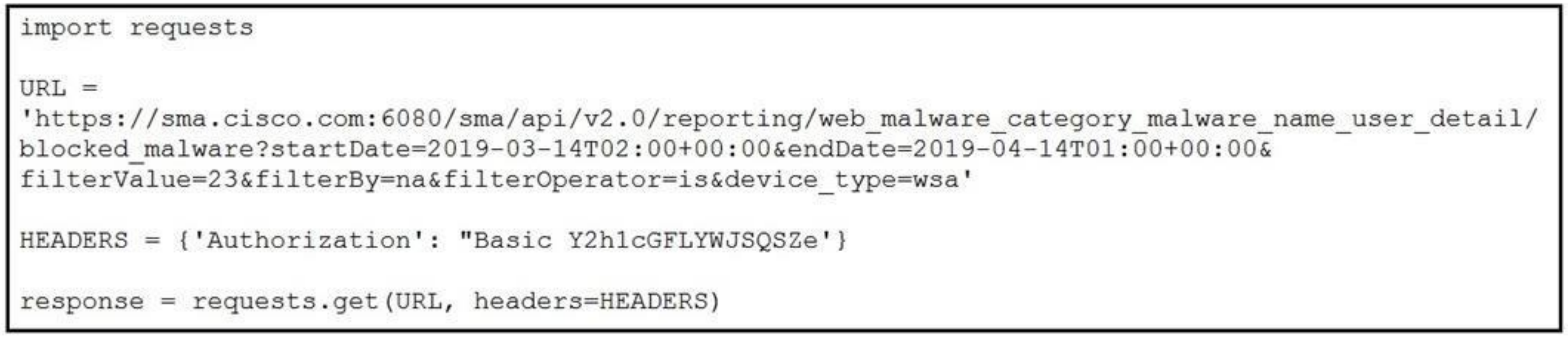
QUESTION 39 What are two benefits of Ansible when managing security platforms? (Choose two.)

A. End users can be identified and tracked across a network.
B. Network performance issues can be identified and automatically remediated.
C. Policies can be updated on multiple devices concurrently, which reduces outage windows.
D. Anomalous network traffic can be detected and correlated.
E. The time that is needed to deploy a change is reduced, compared to manually applying the change.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40



```
import requests

URL =
'https://sma.cisco.com:6080/sma/api/v2.0/reporting/web_malware_category_malware_name_user_detail/
blocked_malware?startDate=2019-03-14T02:00+00:00&endDate=2019-04-14T01:00+00:00&
filterValue=23&filterBy=na&filterOperator=is&device_type=wsa'

HEADERS = {'Authorization': "Basic Y2h1cGFLYWJSQSZe'}

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

Refer to the exhibit.

What must be present in a Cisco Web Security Appliance before the script is run?

A. reporting group with the name web_malware_category_malware_name_user_detail
B. data for specified dates
C. reporting group with the name blocked_malware
D. data in the queried category

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
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=2016-09-10T19:00:00.000Z&endDate=2018-0924T23:00:00.000Z&device_type=esa&device_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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42 Which two APIs are available from Cisco ThreatGRID? (Choose two.)

A. Access
B. User Scope
C. Data
D. Domains
E. Curated Feeds

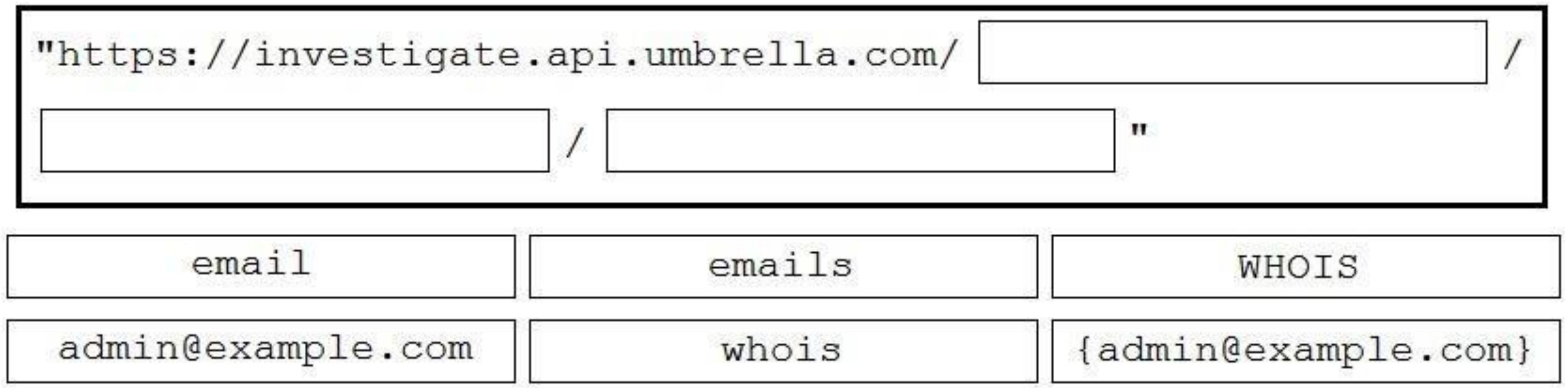
Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
DRAG DROP

Drag and drop the code to complete the Cisco Umbrella Investigate WHOIS query that returns a list of domains that are associated with the email address "admin@example.com". Not all options are used.

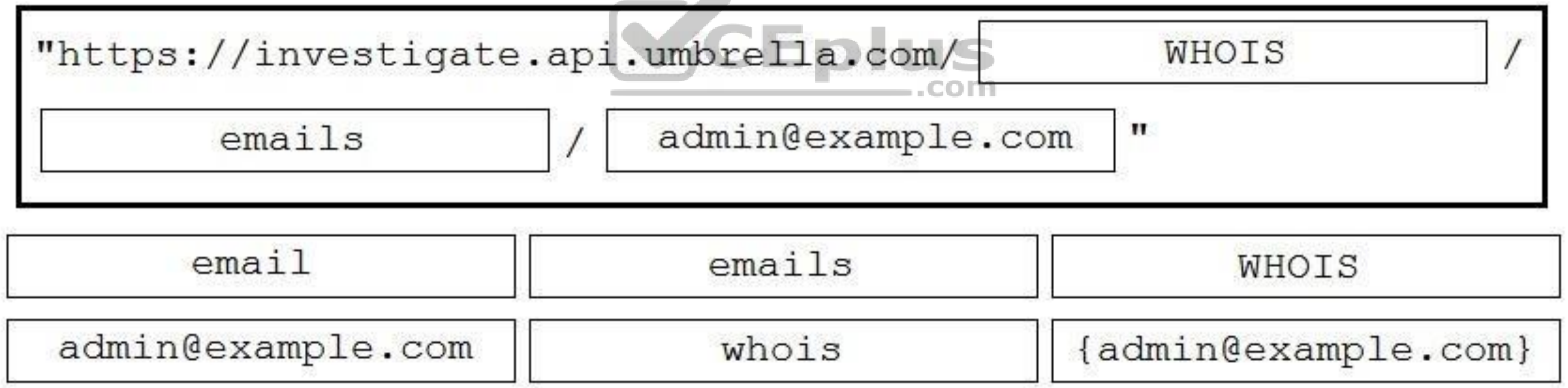
Select and Place:



```
"https://investigate.api.umbrella.com/ [            ] /
[            ] / [            ] "
```

email	emails	WHOIS
admin@example.com	whois	{admin@example.com}

Correct Answer:



```
"https://investigate.api.umbrella.com/ WHOIS /
emails / admin@example.com "
```

email	emails	WHOIS
admin@example.com	whois	{admin@example.com}

Section: (none)
Explanation

Explanation/Reference:
Explanation: https://docs.umbrella.com/investigate-api/docs/whois-information-for-a-domain-1

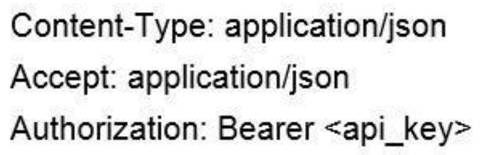
QUESTION 44 Which two commands create a new local source code branch? (Choose two.)

A. **git checkout -b new_branch**
B. **git branch -b new_branch**
C. **git checkout -f new_branch**
D. **git branch new_branch**
E. **git branch -m new_branch**
Correct Answer: AD

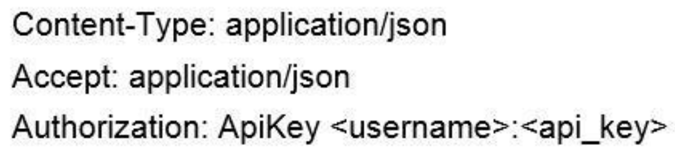
Section: (none)
Explanation

Explanation/Reference:

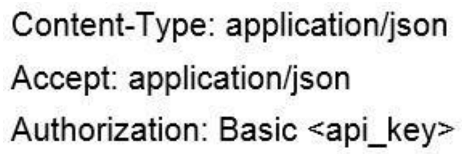
QUESTION 45 Which header set should be sent with all API calls to the Cisco Stealthwatch Cloud API? A.



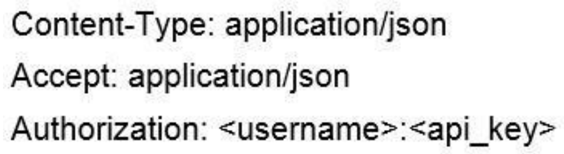
```
Content-Type: application/json
Accept: application/json
Authorization: Bearer <api_key>
```



```
Content-Type: application/json
Accept: application/json
Authorization: ApiKey <username>:<api_key>
```



```
Content-Type: application/json
Accept: application/json
Authorization: Basic <api_key>
```



```
Content-Type: application/json
Accept: application/json
Authorization: <username>:<api_key>
```

B. C.

D.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46 Which API is used to query if the domain “example.com” has been flagged as malicious by the Cisco Security Labs team?

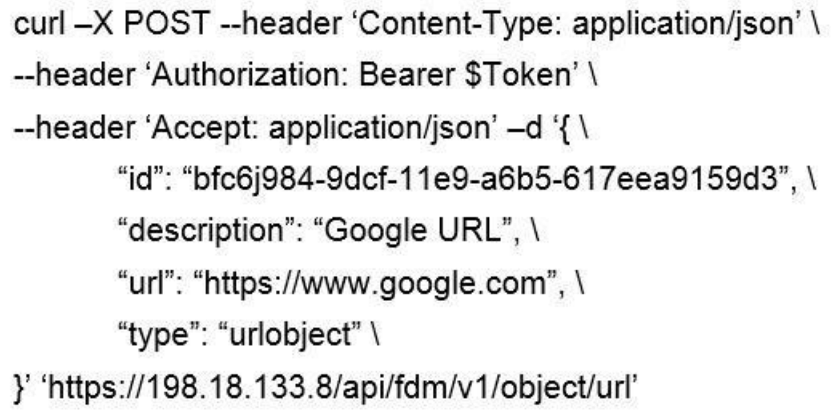
A. https://s-platform.api.opendns.com/1.0/events?example.com
B. https://investigate.api.umbrella.com/domains/categorization/example.com
C. https://investigate.api.umbrella.com/domains/volume/example.com
D. https://s-platform.api.opendns.com/1.0/domains?example.com

Correct Answer: B
Section: (none)
Explanation

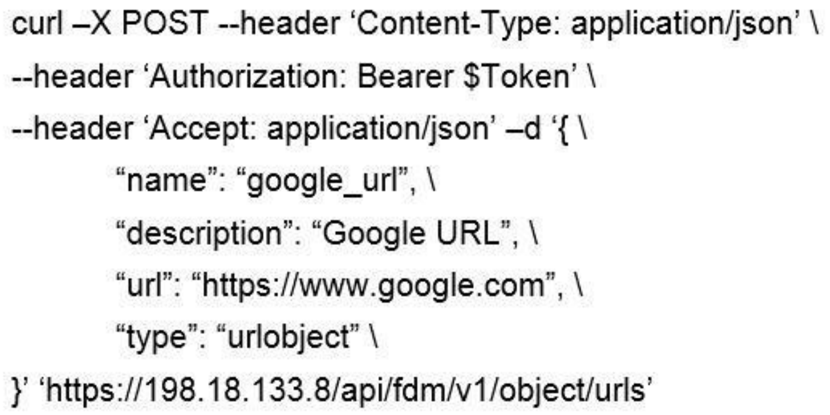
Explanation/Reference:

QUESTION 47

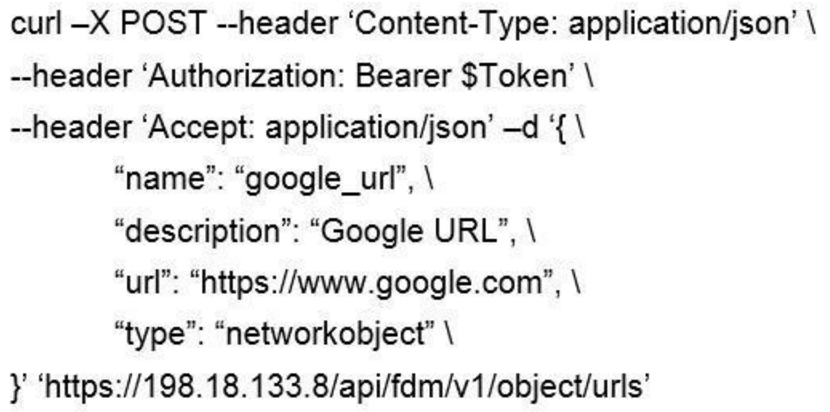
Which snippet describes the way to create an URL object in Cisco FDM using FDM REST APIs with curl?



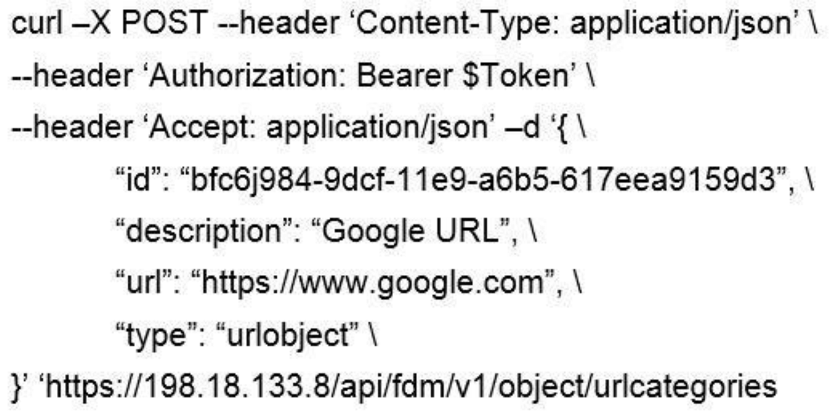
```
curl –X POST --header ‘Content-Type: application/json’ \
--header ‘Authorization: Bearer $Token’ \
--header ‘Accept: application/json’ –d ‘{ \
          “id”: “bfc6j984-9dcf-11e9-a6b5-617eea9159d3”, \
          “description”: “Google URL”, \
          “url”: “https://www.google.com”, \
          “type”: “urlobject” \
}’ ‘https://198.18.133.8/api/fdm/v1/object/url’
```



```
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’
```



```
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’
```



```
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.

B. C.

D.

Correct Answer: B
Section: (none)
Explanation

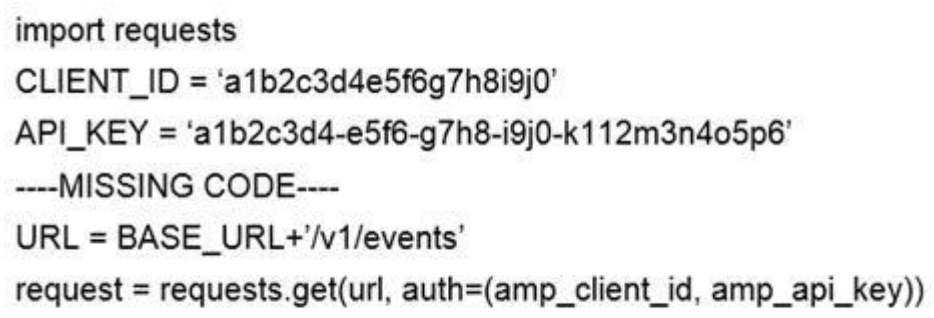
Explanation/Reference:
QUESTION 48 Which request searches for a process window in Cisco ThreatGRID that contains the word “secret”?

A. /api/v2/search/submissions?term=processwindow&title=secret
B. /api/v2/search/submissions?term=processwindow&q=secret
C. /api/v2/search/submissions?term=window&title=secret
D. /api/v2/search/submissions?term=process&q=secret

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50 What is the purpose of the snapshot APIs exposed by Cisco Stealthwatch Cloud?

A. Report on flow data during a customizable time period.
B. Operate and return alerts discovered from infrastructure observations.
C. Return current configuration data of Cisco Stealthwatch Cloud infrastructure.
D. Create snapshots of supported Cisco Stealthwatch Cloud infrastructure.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 51
DRAG DROP

Drag and drop the items to complete the pxGrid script to retrieve all Adaptive Network Control policies. Assume that username, password, and base URL are correct. Not all options are used.

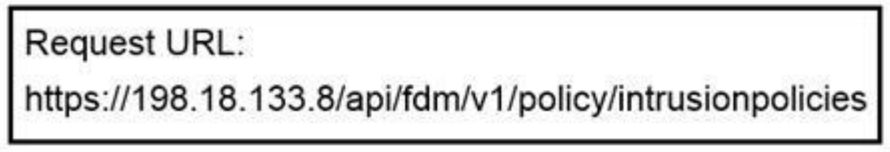
Select and Place:

Correct Answer:

Section: (none)
Explanation

Explanation/Reference:
Reference: https://developer.cisco.com/docs/pxgrid/#!retreiving-all-anc-polices/java-sample-code

QUESTION 52



Request URL:
https://198.18.133.8/api/fdm/v1/policy/intrusionpolicies

Refer to the exhibit.

What is the purpose of the API represented by this URL?

A. Getting or setting intrusion policies in FMC
B. Creating an intrusion policy in FDM
C. Updating access policies
D. Getting the list of intrusion policies configured in FDM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53 Which query parameter is required when using the reporting API of Cisco Security Management Appliances?

A. device_type
B. query_type
C. filterValue
D. startDate + endDate

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which step is required by Cisco pxGrid providers to expose functionality to consumer applications that are written in Python? A.

Look up the existing service using the /pxgrid/control/ServiceLookup endpoint.

B. Register the service using the /pxgrid/control/ServiceRegister endpoint.
C. Configure the service using the /pxgrid/ise/config/profiler endpoint.
D. Expose the service using the /pxgrid/ise/pubsub endpoint.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
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

Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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:

Correct Answer:

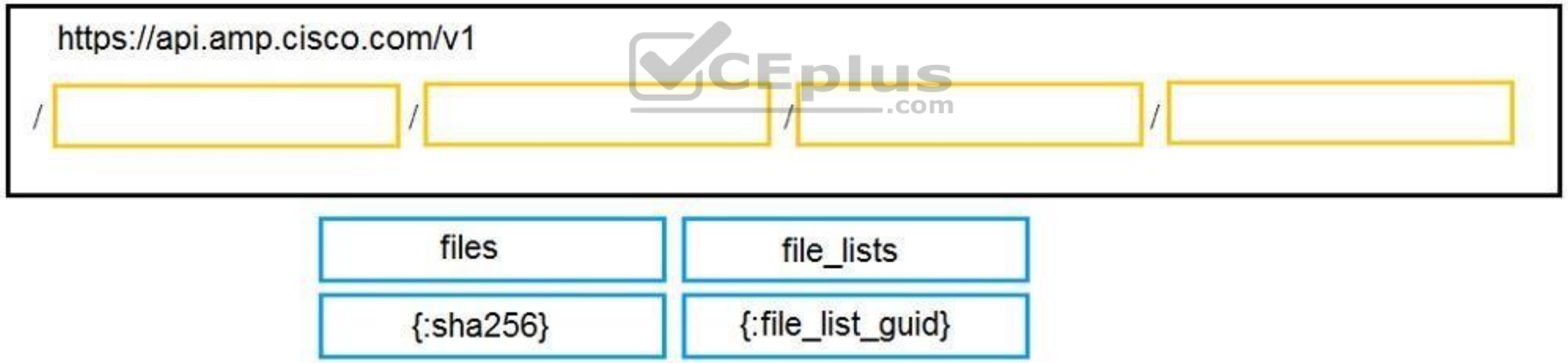
Section: (none)
Explanation

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

QUESTION 57
DRAG DROP

Drag and drop the code to complete the URL for the Cisco AMP for Endpoints API POST request so that it will add a sha256 to a given file_list using file_list_guid.

Select and Place:

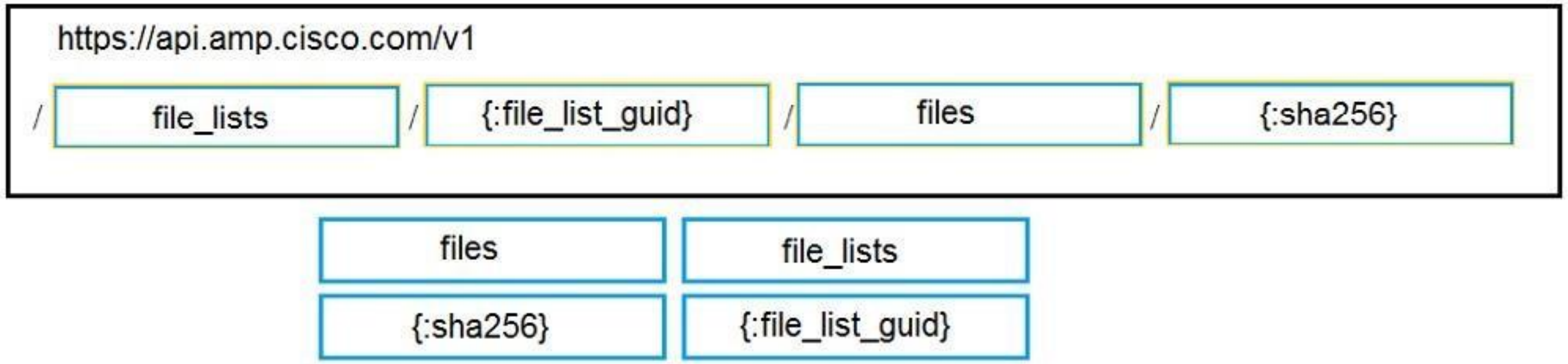


https://api.amp.cisco.com/v1

/ ____ / ____ / ____ / ____

files | file_lists
{:sha256} | {:file_list_guid}

Correct Answer:



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

/ file_lists / {:file_list_guid} / files / {:sha256}

files | file_lists
{:sha256} | {:file_list_guid}

Section: (none)
Explanation

Explanation/Reference:
Reference:
https://api-docs.amp.cisco.com/api_actions/details?api_action=POST+%2Fv1%2Ffile_lists%2F%7B%3Afile_list_guid%7D%2Ffiles%2F%7B%3Asha256%7D&api_host=api.eu.amp.cisco.com&api_resource=File+List+Item&api_version=v1

QUESTION 58
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:

Section: (none)
Explanation

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