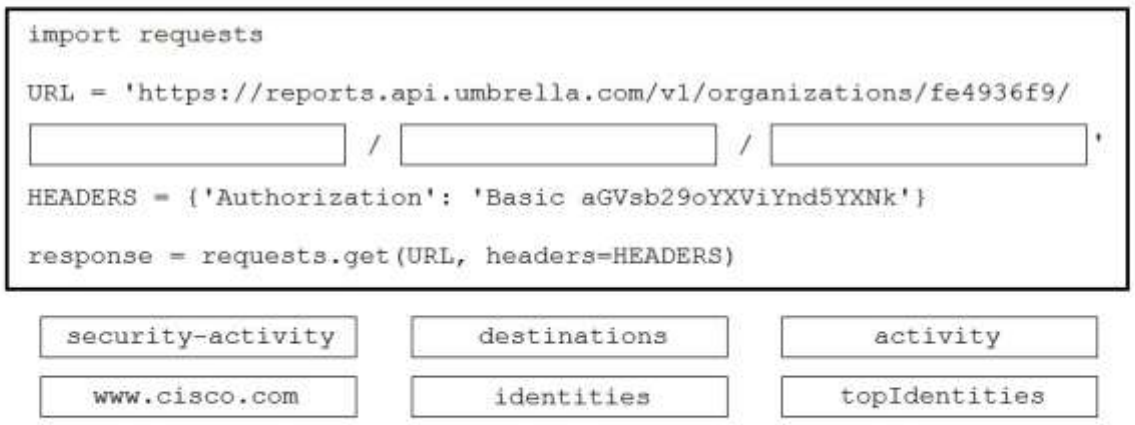
- **Vendor:** Cisco
- **Exam Code:** 300-735
- **Exam Name:** Automating and Programming Cisco Security Solutions
- **New Updated Questions from Braindump2go (Updated in December/2020)**

Visit Braindump2go and Download Full Version 300-735 Exam Dumps

QUESTION 29
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.
Answer: Umbrella

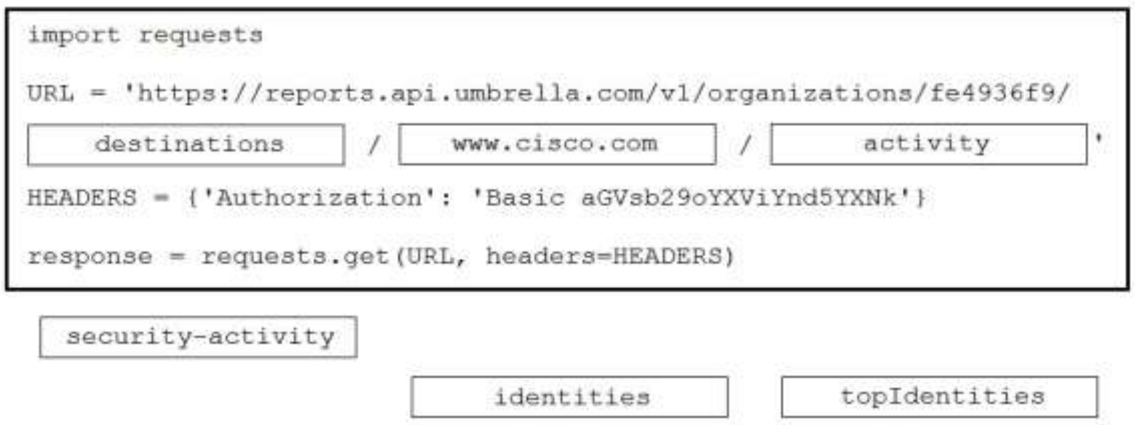
QUESTION 30
Drag and Drop Question
A Python script is being developed to return the top 10 identities in an organization that have made a DNS request to "www.cisco.com".
Drag and drop the code to complete the Cisco Umbrella Reporting API query to return the top identities. Not all options are used.



```
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
```

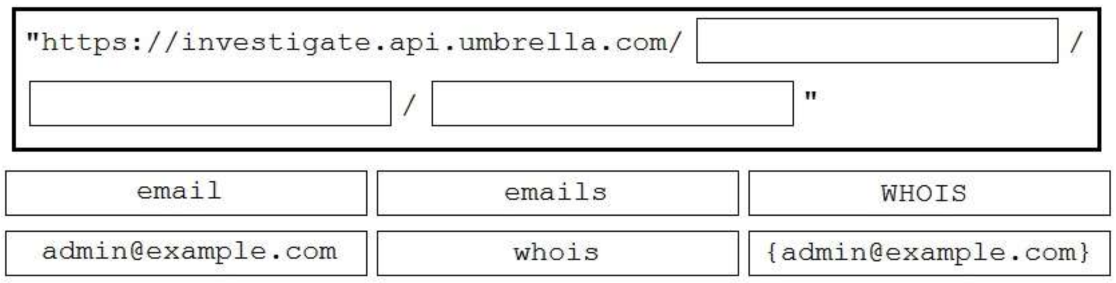
Answer:



```
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

                     identities      topIdentities
```

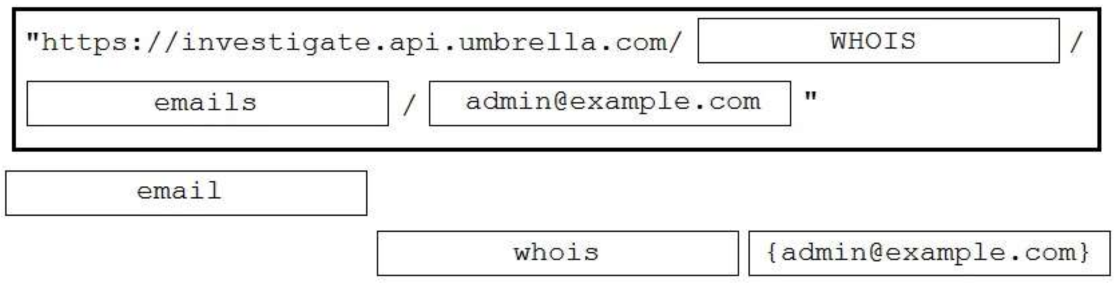
QUESTION 31
Drag and Drop Question
Drag and drop the code to complete the Cisco Umbrella Investigate WHOIS query that returns a list of domains that are associated with the email address "admin@example.com". Not all options are used.



```
"https://investigate.api.umbrella.com/ □ /
□ / □ "
```

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

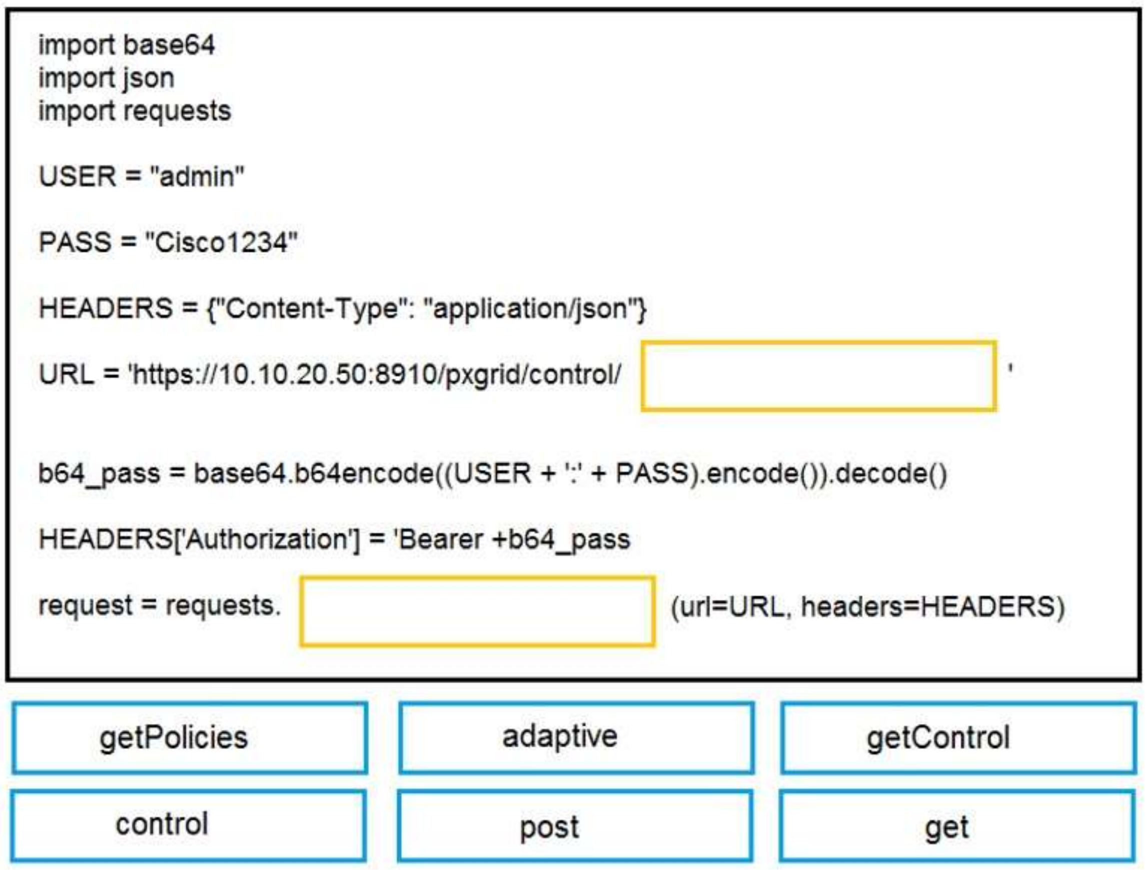
Answer:



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

```
email

                     whois     {admin@example.com}
```

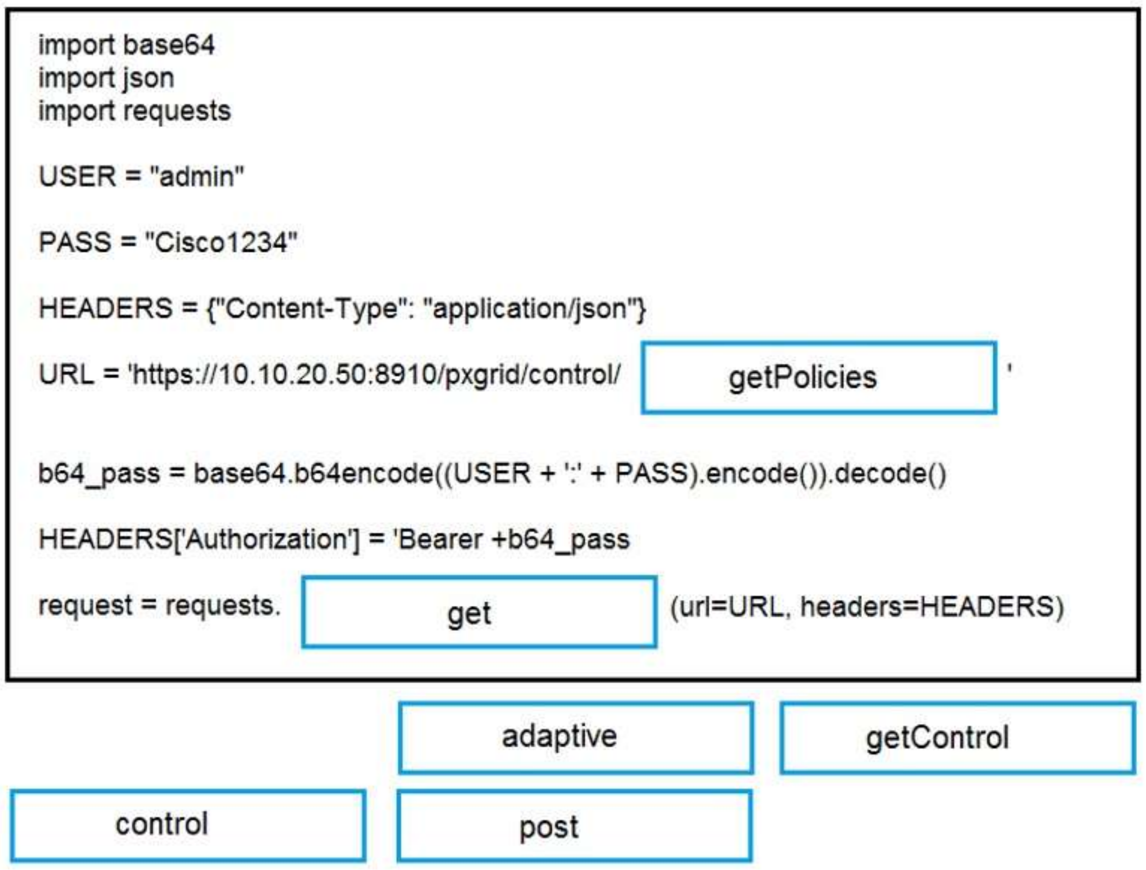
QUESTION 32
Drag and Drop Question
Drag and drop the items to complete the pxGrid script to retrieve all Adaptive Network Control policies. Assume that username, password, and base URL are correct. Not all options are used.



```
import base64
import json
import requests

USER = "admin"

PASS = "Cisco1234"

HEADERS = {"Content-Type": "application/json"}

URL = 'https://10.10.20.50:8910/pxgrid/control/ [          ] '

b64_pass = base64.b64encode((USER + ':' + PASS).encode()).decode()

HEADERS['Authorization'] = 'Bearer +b64_pass

request = requests. [          ] (url=URL, headers=HEADERS)
```

getPolicies | adaptive | getControl
control | post | get

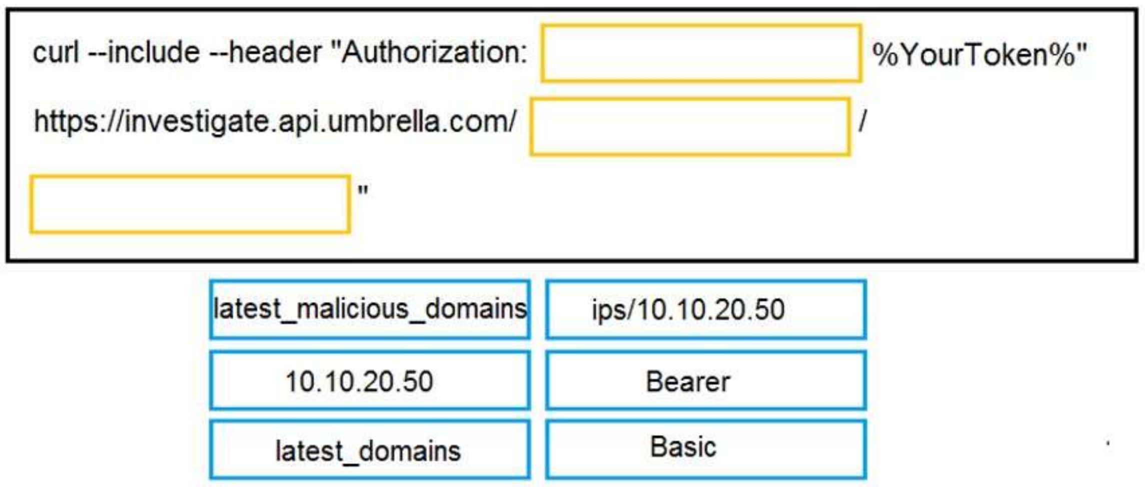
Answer:



```
import base64
import json
import requests

USER = "admin"

PASS = "Cisco1234"

HEADERS = {"Content-Type": "application/json"}

URL = 'https://10.10.20.50:8910/pxgrid/control/ getPolicies '

b64_pass = base64.b64encode((USER + ':' + PASS).encode()).decode()

HEADERS['Authorization'] = 'Bearer +b64_pass

request = requests. get (url=URL, headers=HEADERS)
```

adaptive | getControl
control | post

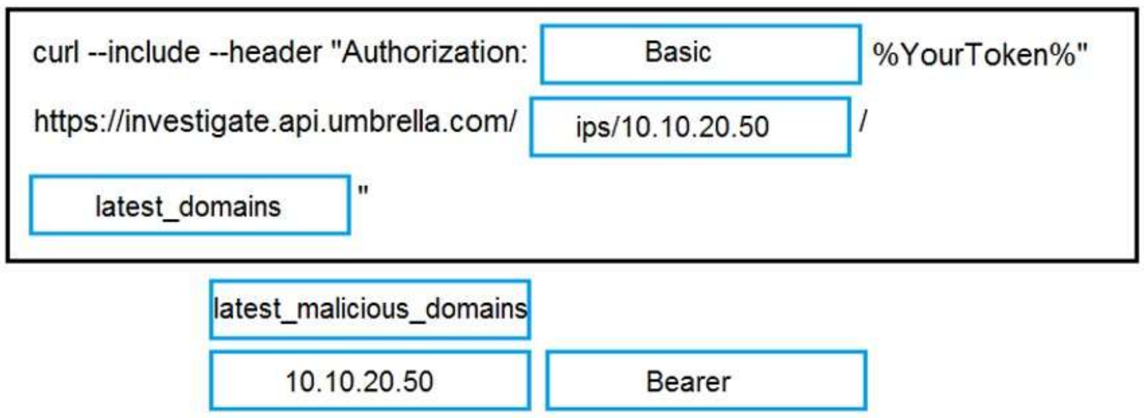
QUESTION 33
Drag and Drop Question
Drag and drop the code to complete the curl query to the Cisco Umbrella Investigate API for the Latest Malicious Domains for the IP address 10.10.20.50. Not all options are used.



```
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

Answer:



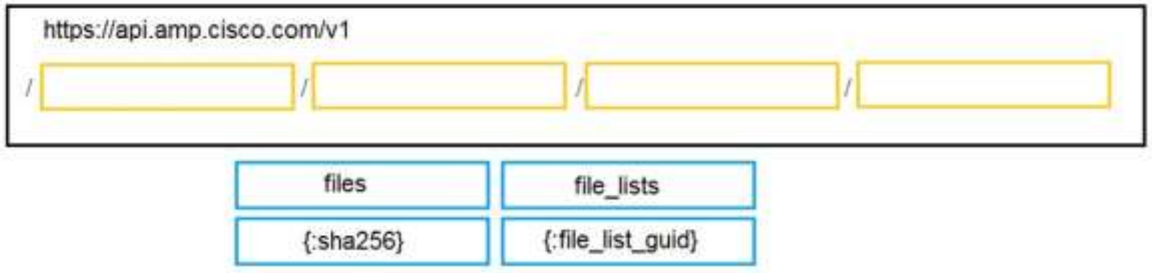
curl --include --header "Authorization: Basic %YourToken%"
https://investigate.api.umbrella.com/ ips/10.10.20.50 /
latest_domains "

latest_malicious_domains

10.10.20.50

Bearer

QUESTION 34
Drag and Drop Question
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.



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

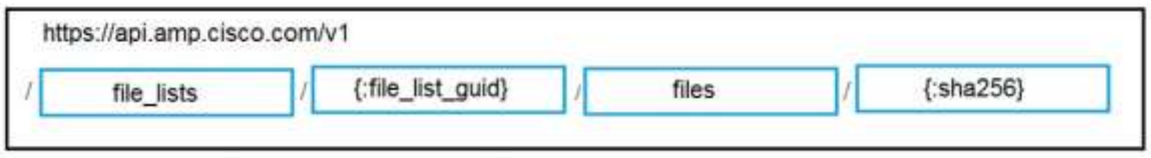
files

file_lists

{:sha256}

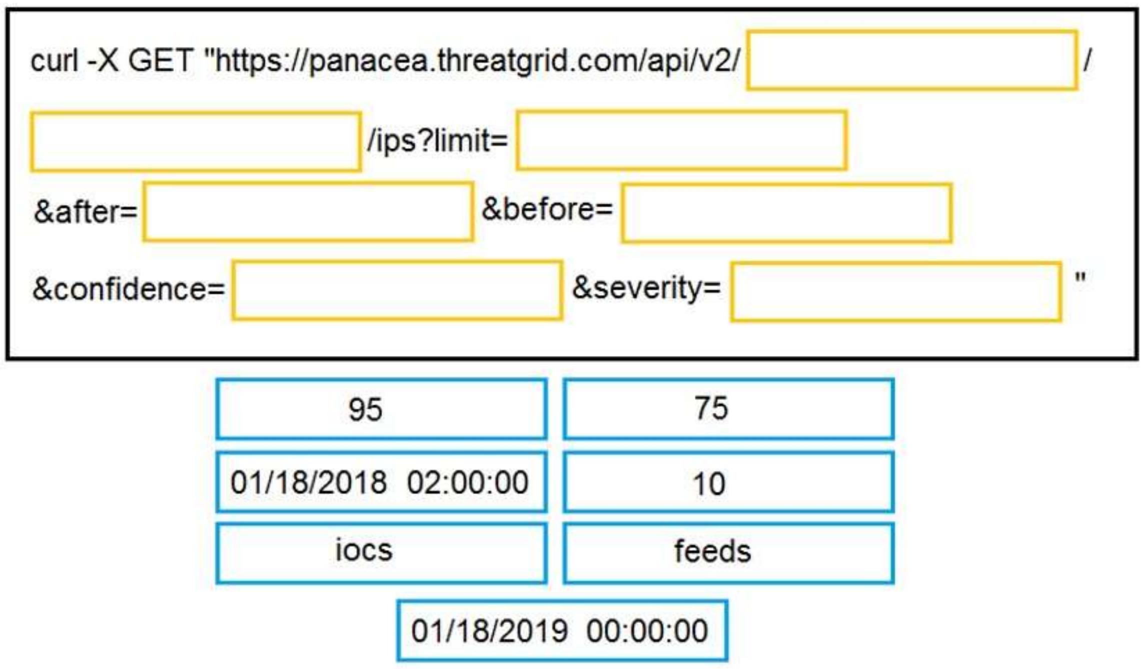
{:file_list_guid}

Answer:



https://api.amp.cisco.com/v1
/ file_lists / {:file_list_guid} / files / {:sha256}

QUESTION 35
Drag and Drop Question
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.



curl -X GET "https://panacea.threatgrid.com/api/v2/ /
/ips?limit=
&after= &before=
&confidence= &severity= "

95

75

01/18/2018 02:00:00

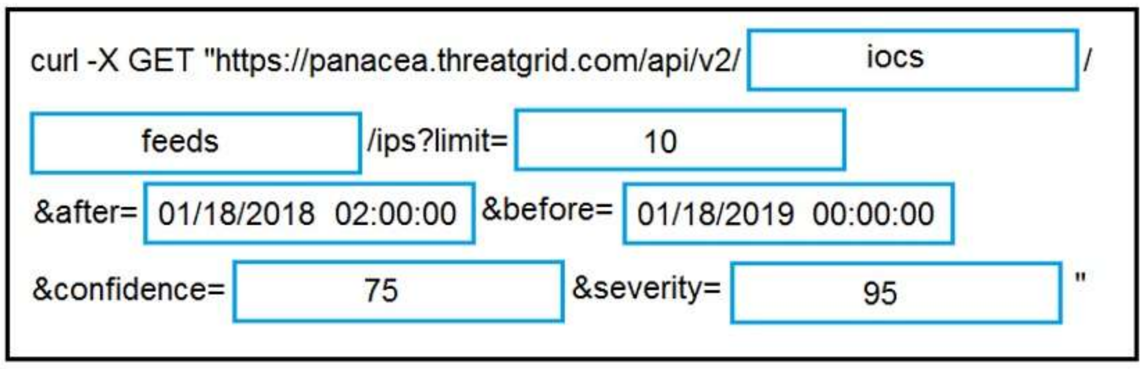
10

iocs

feeds

01/18/2019 00:00:00

Answer:



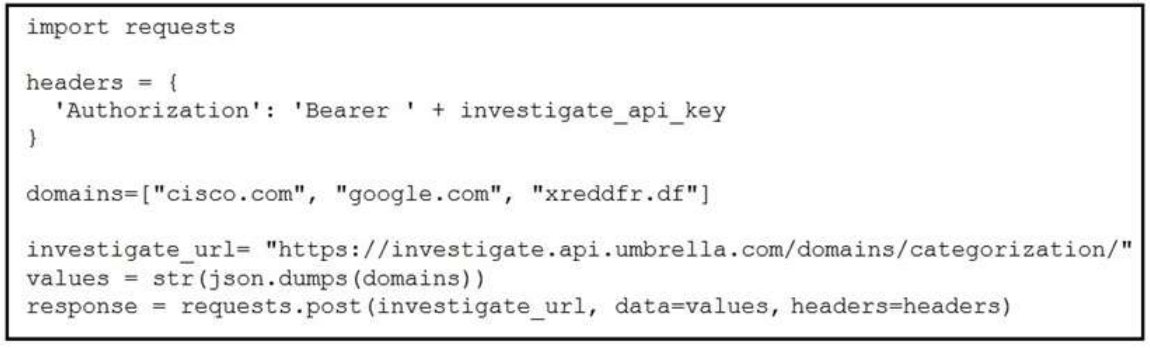
```
curl -X GET "https://panacea.threatgrid.com/api/v2/ iocs /
feeds /ips?limit= 10
&after= 01/18/2018 02:00:00 &before= 01/18/2019 00:00:00
&confidence= 75 &severity= 95 "
```

QUESTION 36
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.

Answer: B

QUESTION 37
Refer to the exhibit. What does the response from the API contain when this code is executed?

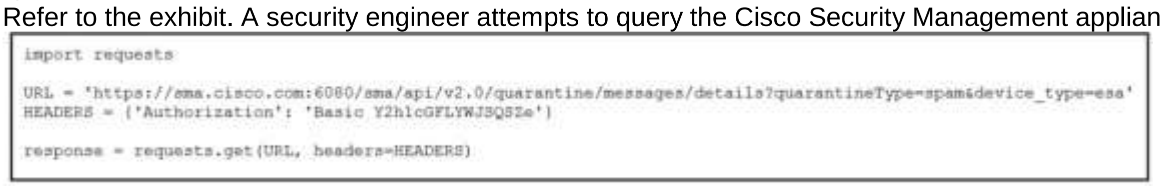


```
import requests

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)
```

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

Answer: D

QUESTION 38
Refer to the exhibit. A security engineer attempts to query the Cisco Security Management appliance to retrieve details of a specific message.



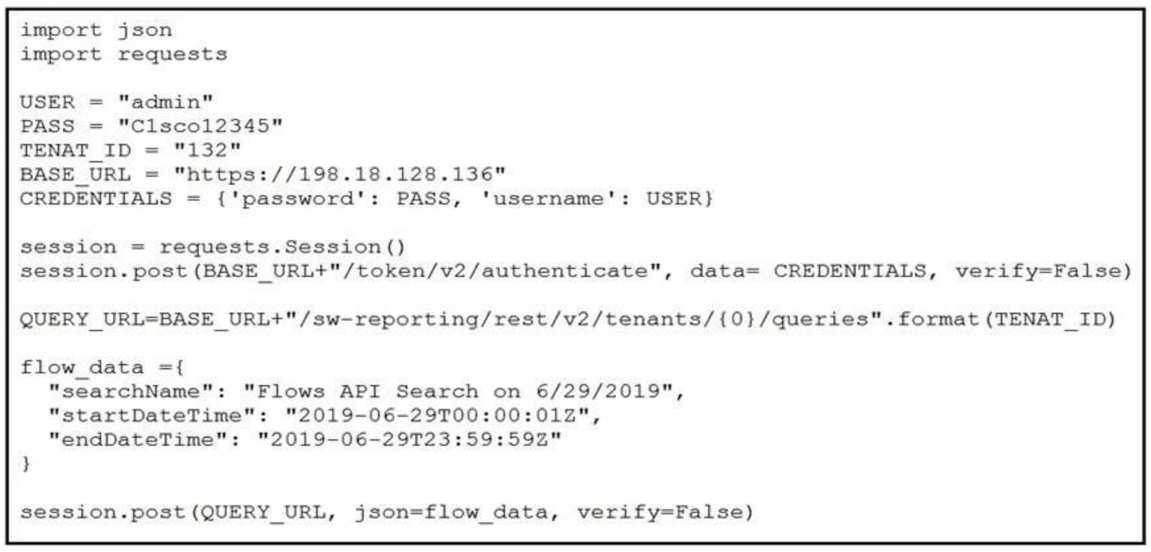
```
import requests

URL = 'https://sma.cisco.com:6080/sma/api/v2.0/quarantine/messages/details?quarantineType=spam&device_type=esa'
HEADERS = {'Authorization': 'Basic Y2hlcGFLYWJ3Q5Ze'}

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

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.

Answer: C

QUESTION 39
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.



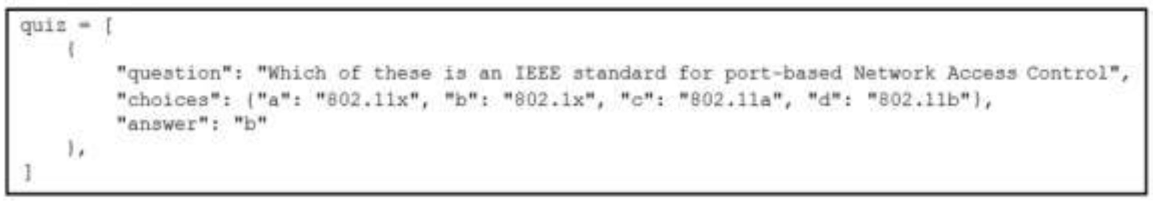
```
import json
import requests

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)
```

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.

Answer: AB

QUESTION 40
Refer to the exhibit. Which expression prints the text "802.1x"?



```
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"
    },
]
```

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'])

Answer: A