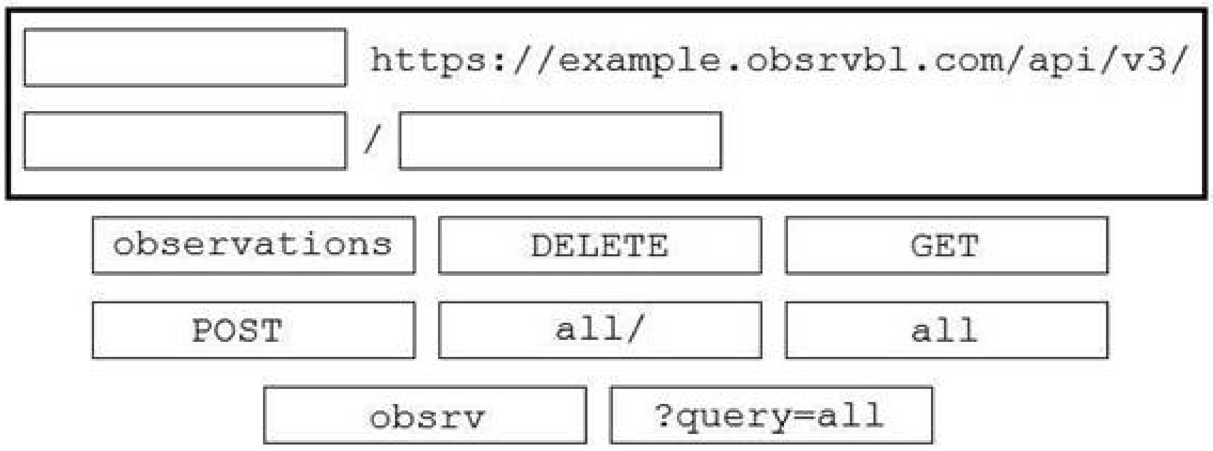
Exam Questions 300-735

Automating and Programming Cisco Security Solutions (SAUTO)

https://www.2passeasy.com/dumps/300-735/

NEW QUESTION 1
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:



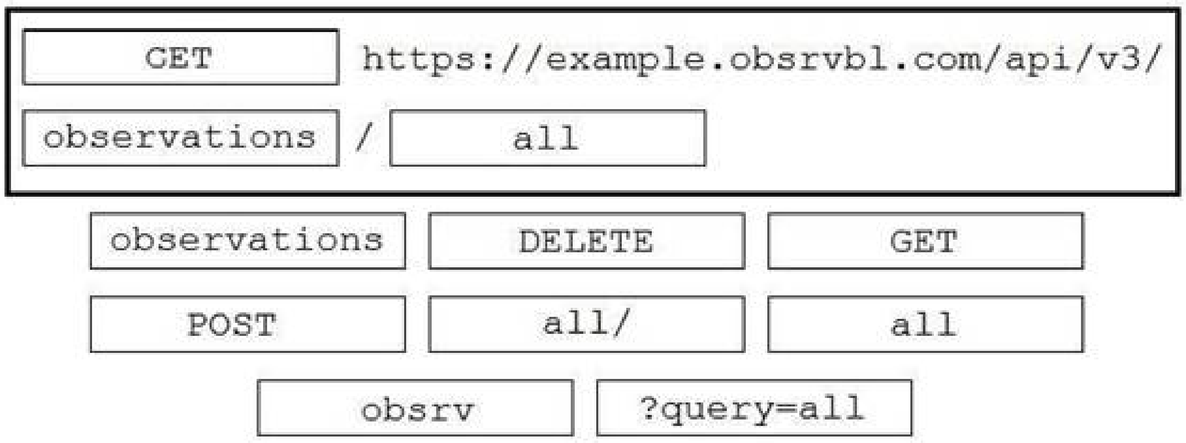
```
[              ] https://example.obsrvbl.com/api/v3/
[              ] / [              ]
```

observations	DELETE	GET
POST	all/	all
obsrv	?query=all	

A. Mastered
B. Not Mastered

Answer: A

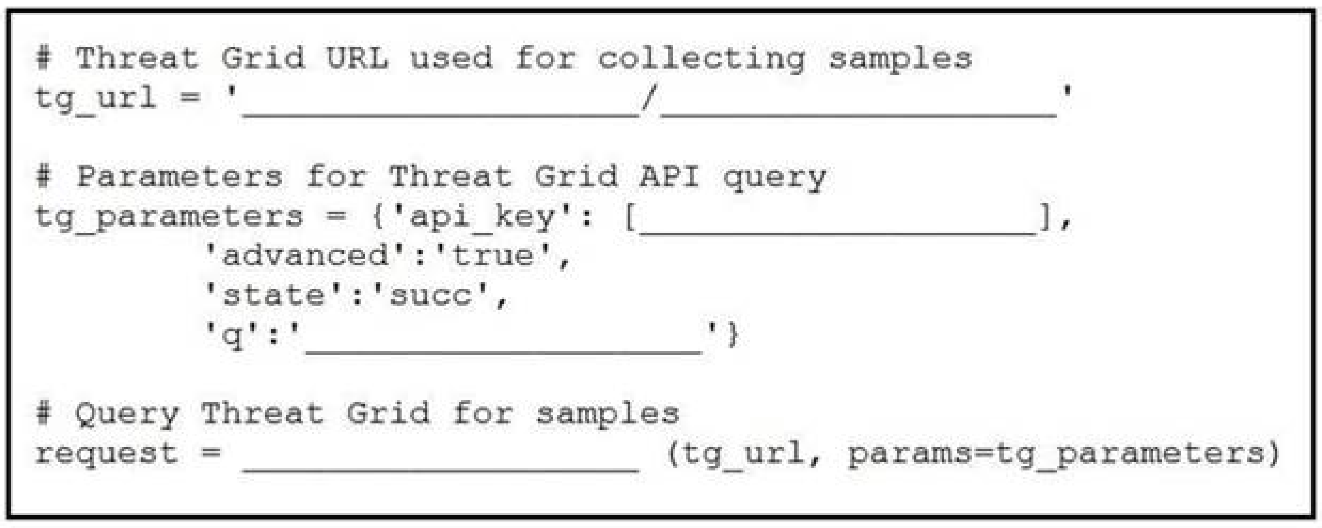
Explanation:



```
[GET] https://example.obsrvbl.com/api/v3/
[observations] / [all]
```

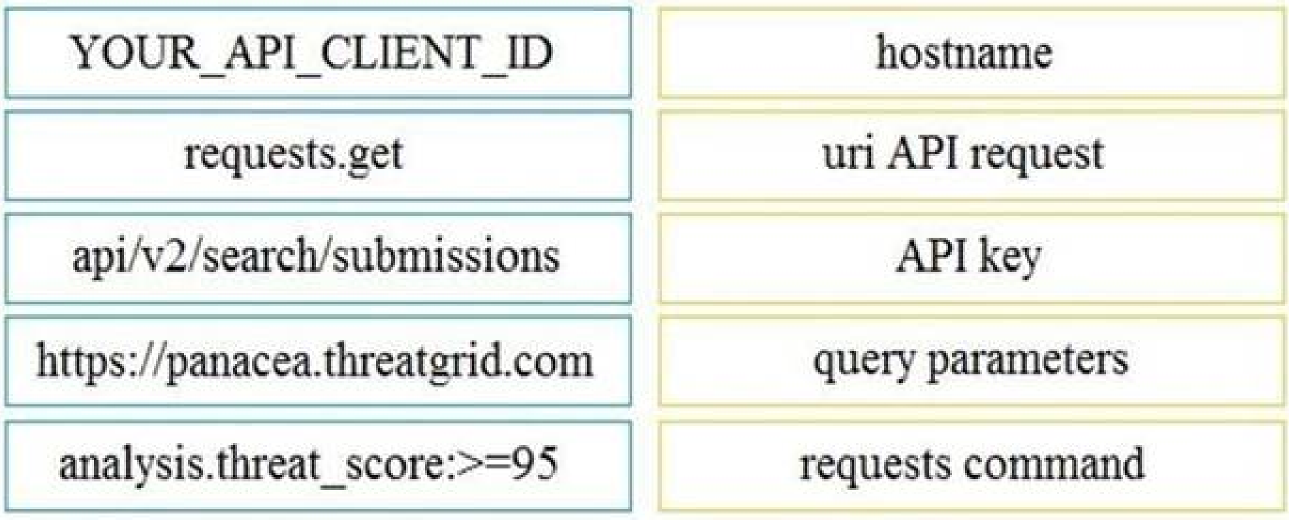
observations	DELETE	GET
POST	all/	all
obsrv	?query=all	

NEW QUESTION 2
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:

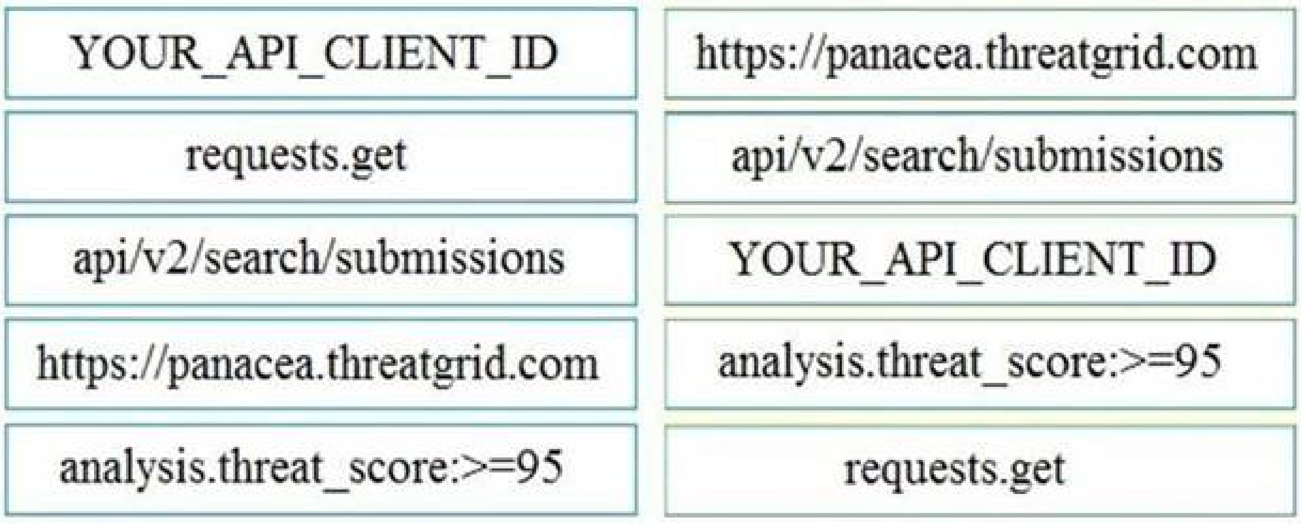


YOUR_API_CLIENT_ID	hostname
requests.get	uri API request
api/v2/search/submissions	API key
https://panacea.threatgrid.com	query parameters
analysis.threat_score:>=95	requests command

A. Mastered
B. Not Mastered

Answer: A

Explanation:



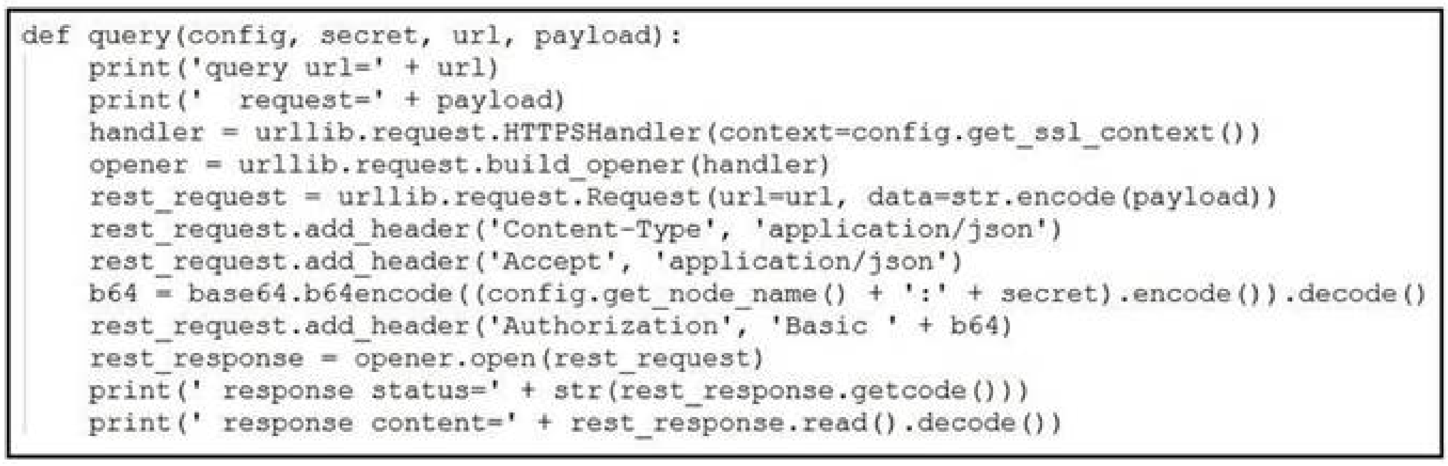
YOUR_API_CLIENT_ID	https://panacea.threatgrid.com
requests.get	api/v2/search/submissions
api/v2/search/submissions	YOUR_API_CLIENT_ID
https://panacea.threatgrid.com	analysis.threat_score:>=95
analysis.threat_score:>=95	requests.get

NEW QUESTION 3
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

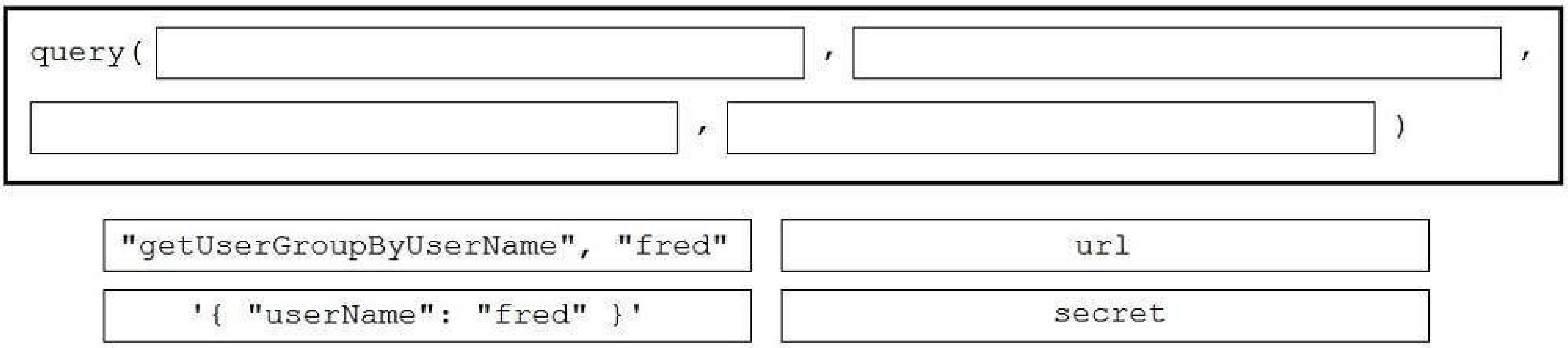
Answer: B

NEW QUESTION 4
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:



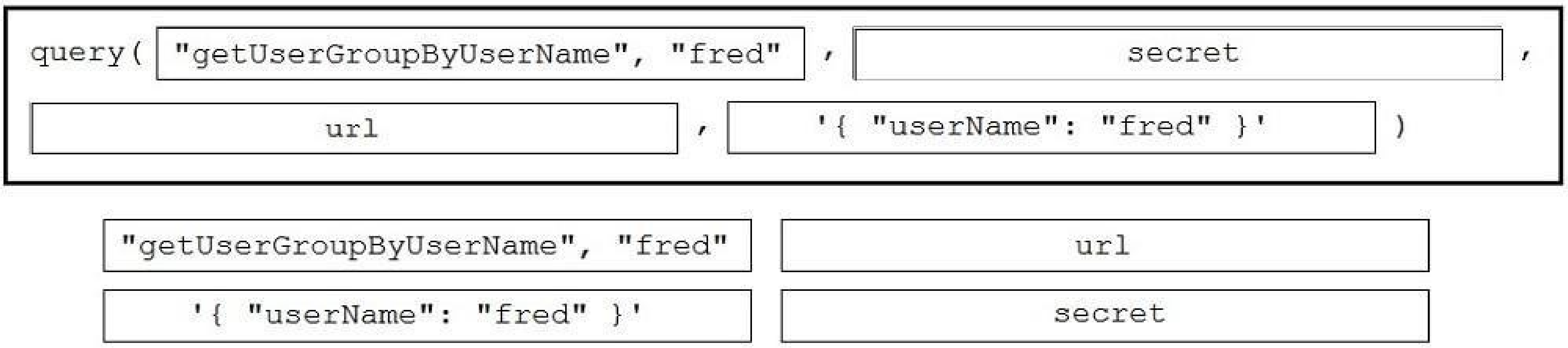
```
query( [                    ] , [                    ] ,
[                    ] , [                    ] )
```

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



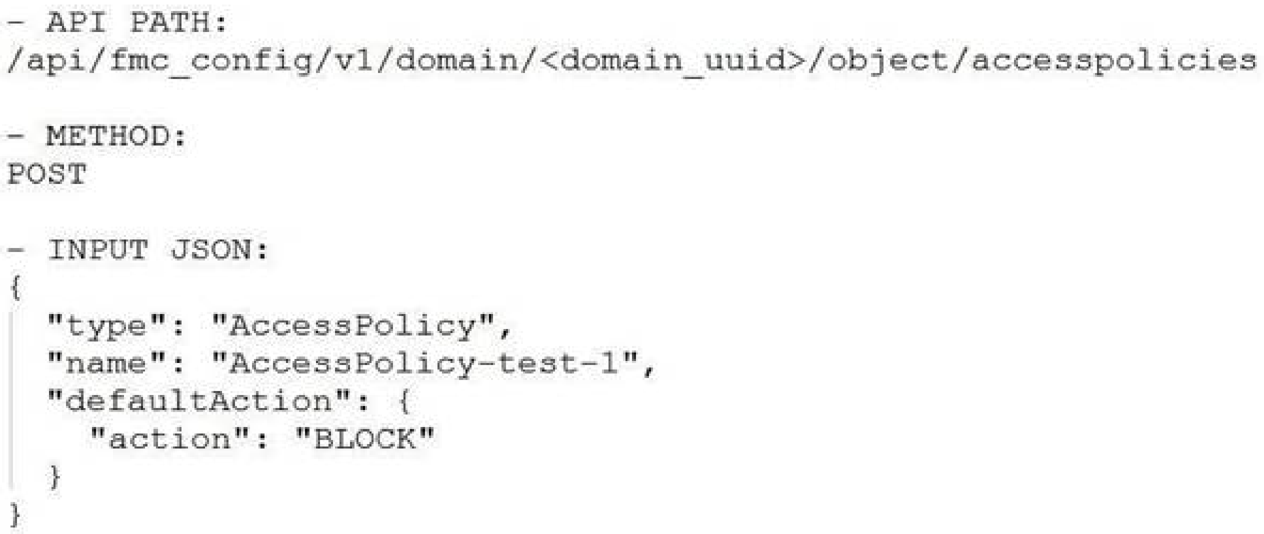
```
query( "getUserGroupByUserName", "fred" , secret ,
url , '{ "userName": "fred" }' )
```

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

NEW QUESTION 5

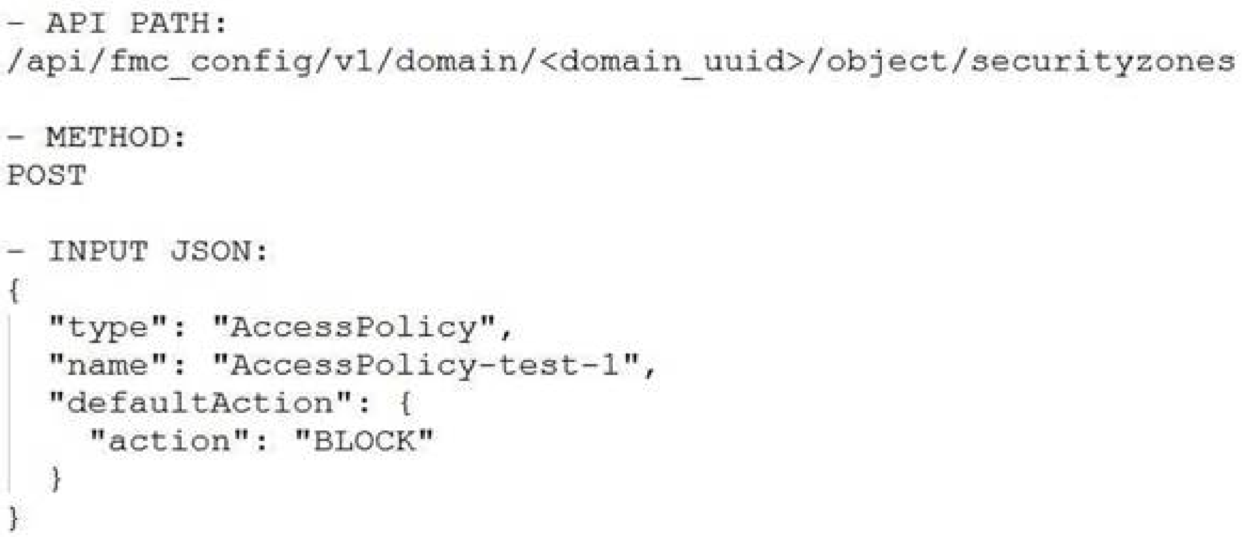
If the goal is to create an access policy with the default action of blocking traffic, using Cisco Firepower Management Center REST APIs, which snippet is used?

A.



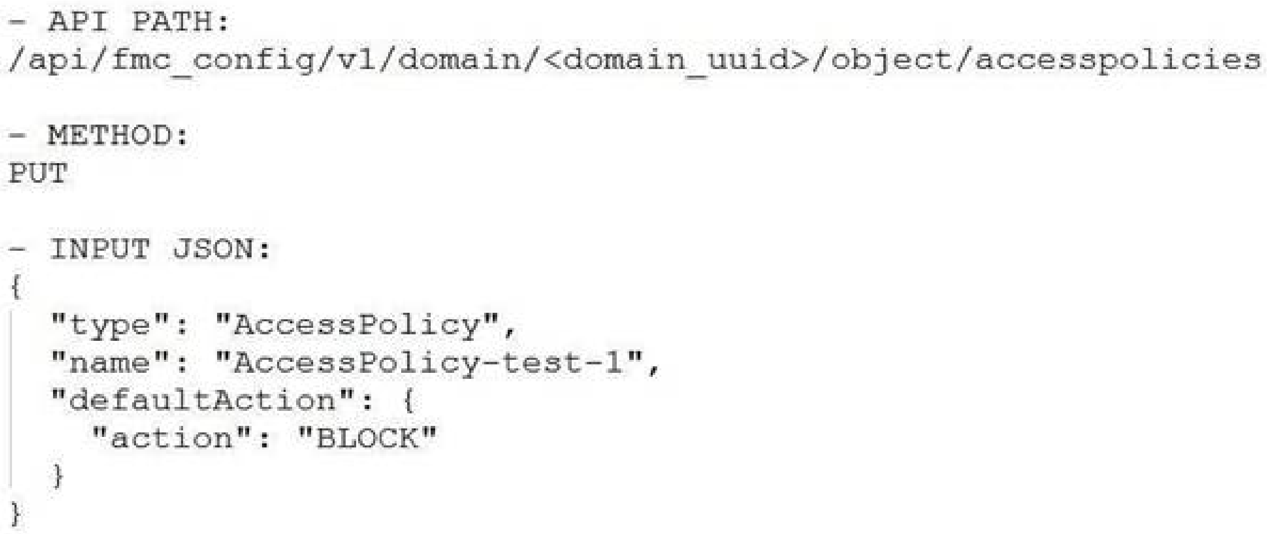
```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/accesspolicies

- METHOD:
POST

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

B.



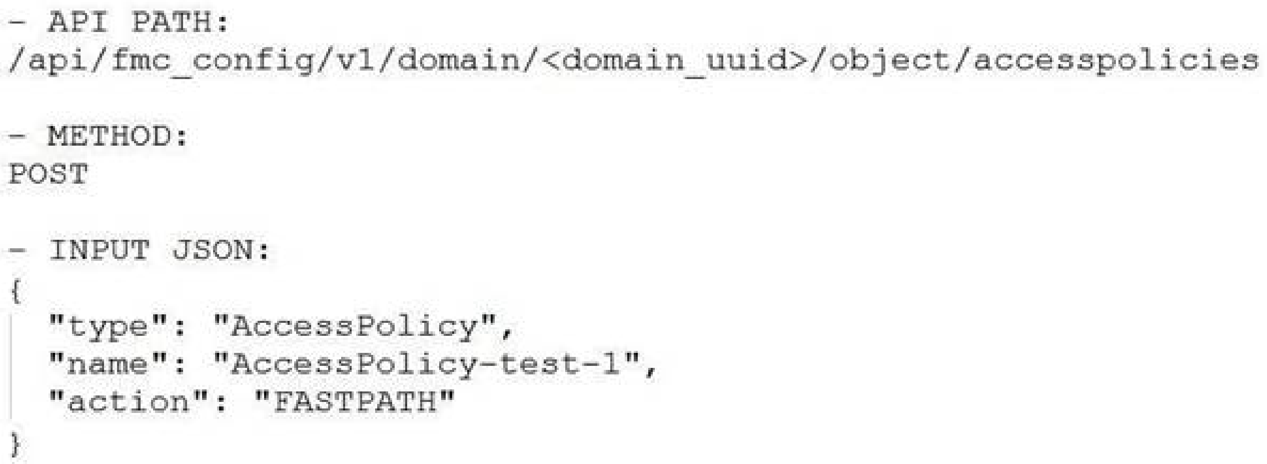
```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/securityzones

- 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"
}
```

Answer: D

NEW 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.

Answer: C

NEW QUESTION 7
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.

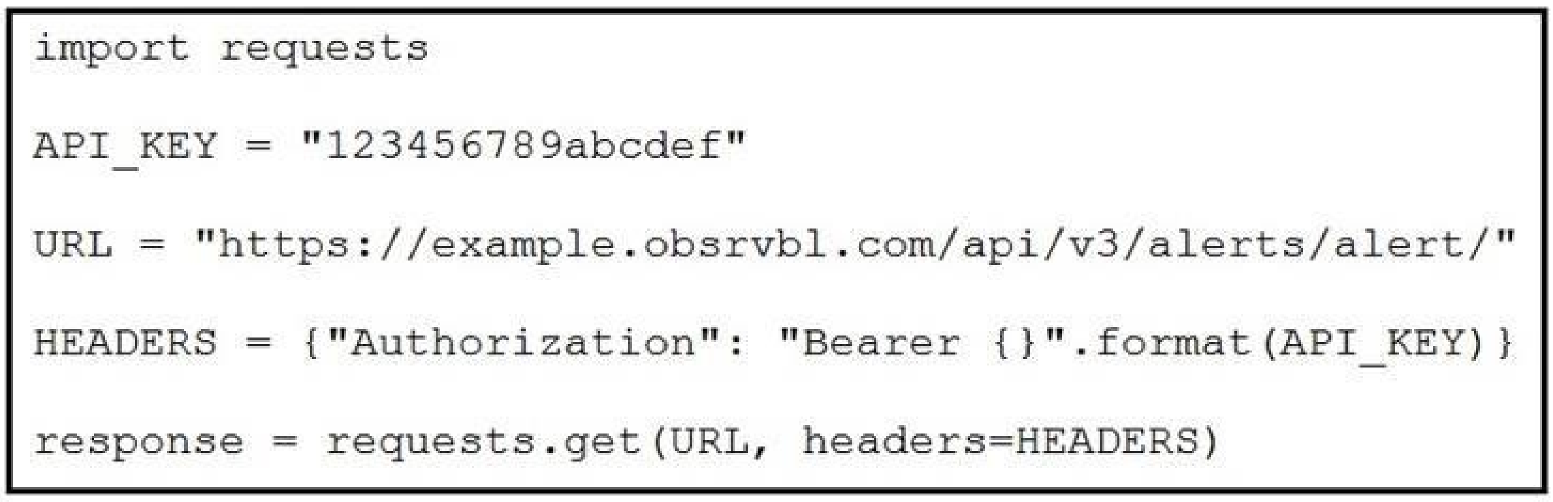
Answer: BC

NEW QUESTION 8
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

Answer: AD

NEW QUESTION 9



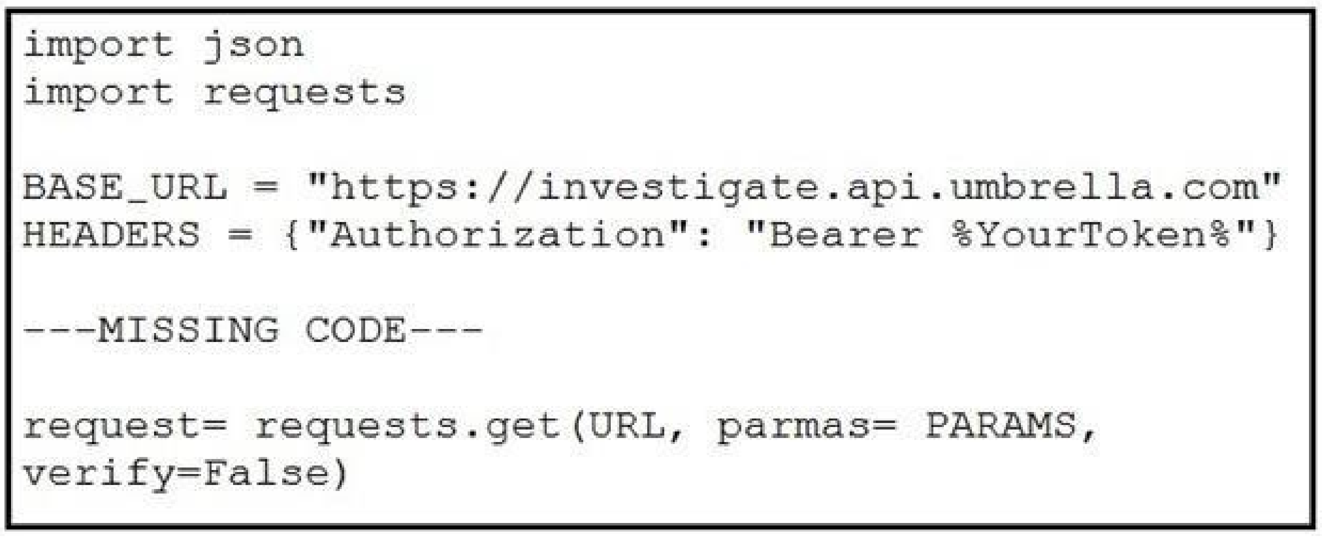
```
import requests

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])

Answer: A

NEW QUESTION 10



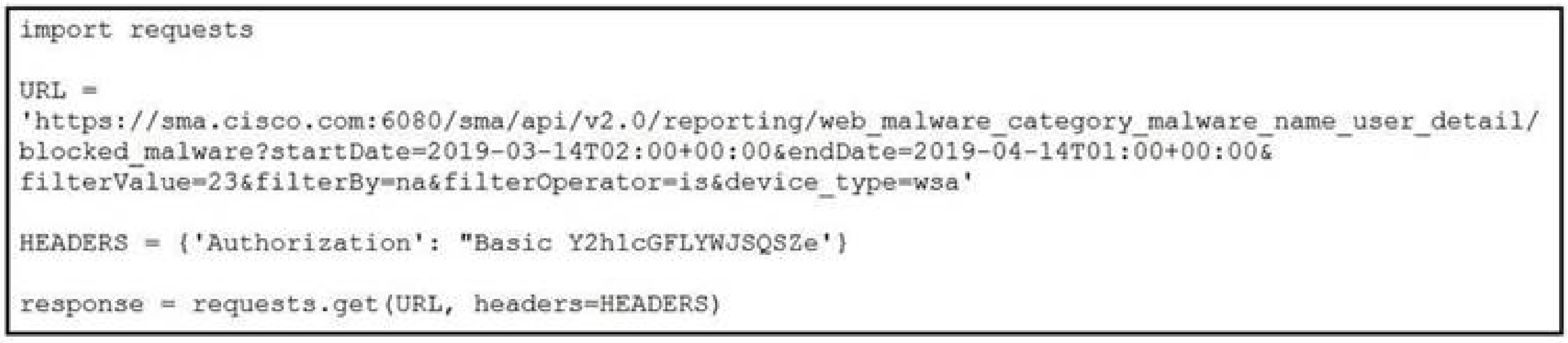
```
import json
import requests

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"}

Answer: D

NEW QUESTION 10



```
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 Y2hlcGFLYWJSQSZe'}

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

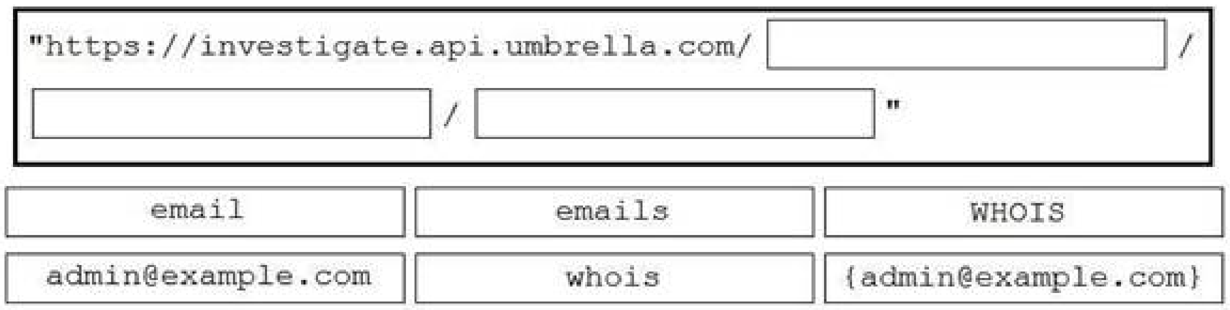
Answer: A

NEW QUESTION 11
Which two APIs are available from Cisco ThreatGRID? (Choose two.)

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

Answer: CE

NEW QUESTION 15
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:



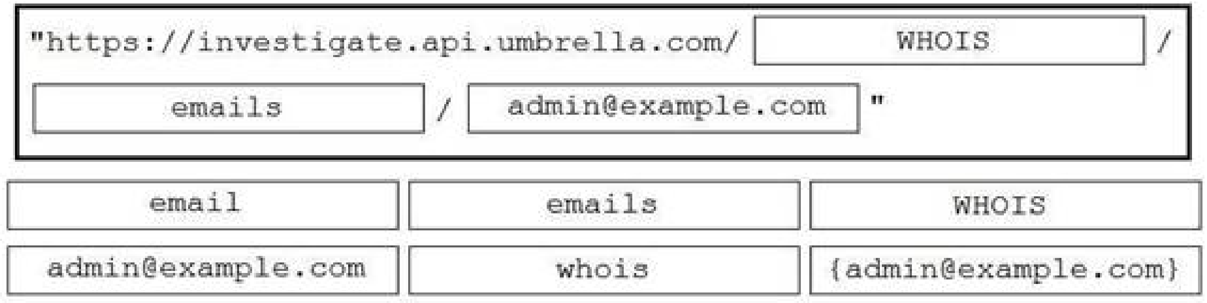
```
"https://investigate.api.umbrella.com/ [          ] /
[          ] / [          ] "
```

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

A. Mastered
B. Not Mastered

Answer: A

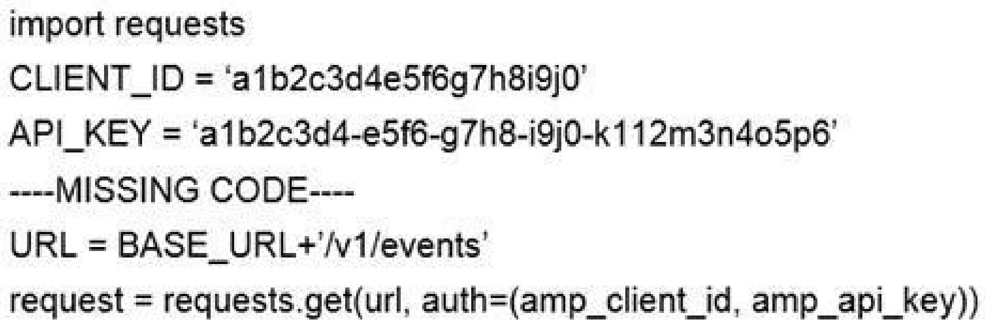
Explanation:



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

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

NEW QUESTION 16
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/”

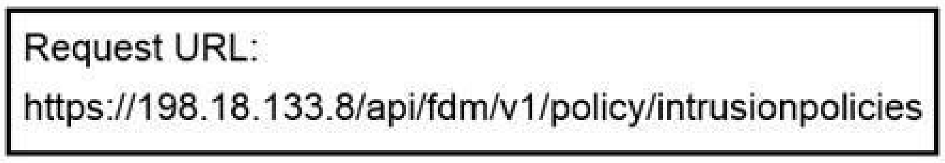
Answer: A

NEW QUESTION 17
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.

Answer: B

NEW QUESTION 19



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

Answer: D

NEW QUESTION 24
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.

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

Answer: D

NEW QUESTION 26
......