300-735Q&As

Automating and Programming Cisco Security Solutions (SAUTO)

QUESTION 1

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

QUESTION 2

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

QUESTION 3

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

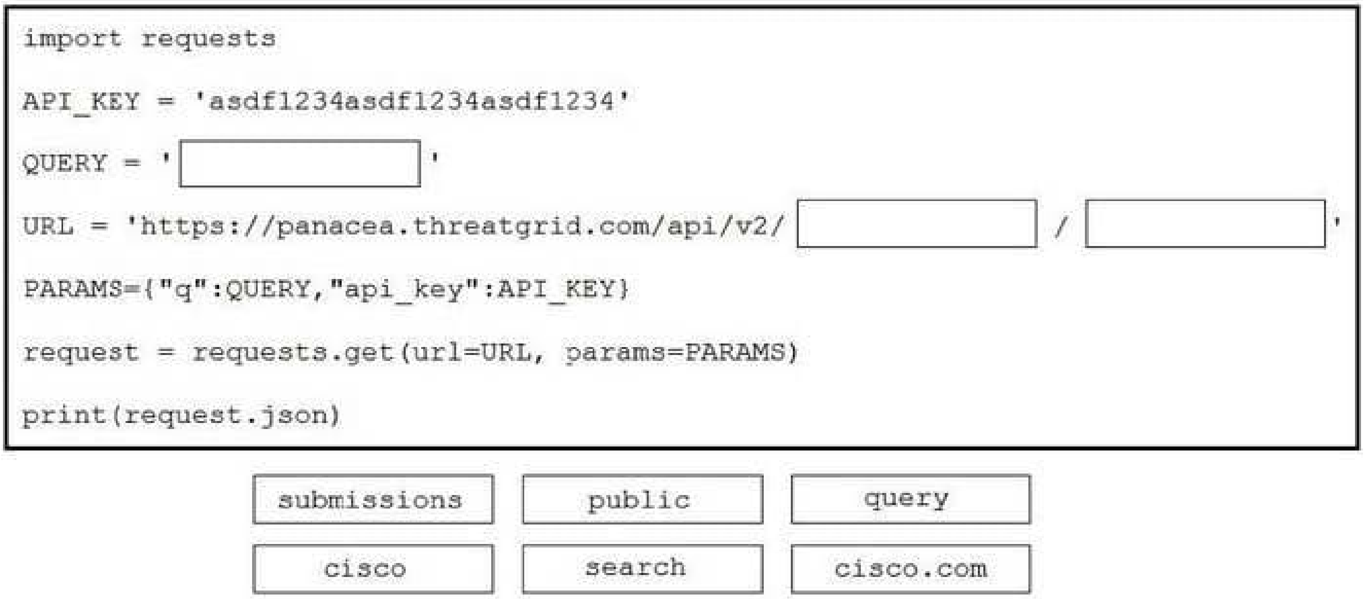
Correct Answer: BD

QUESTION 4

DRAG DROP

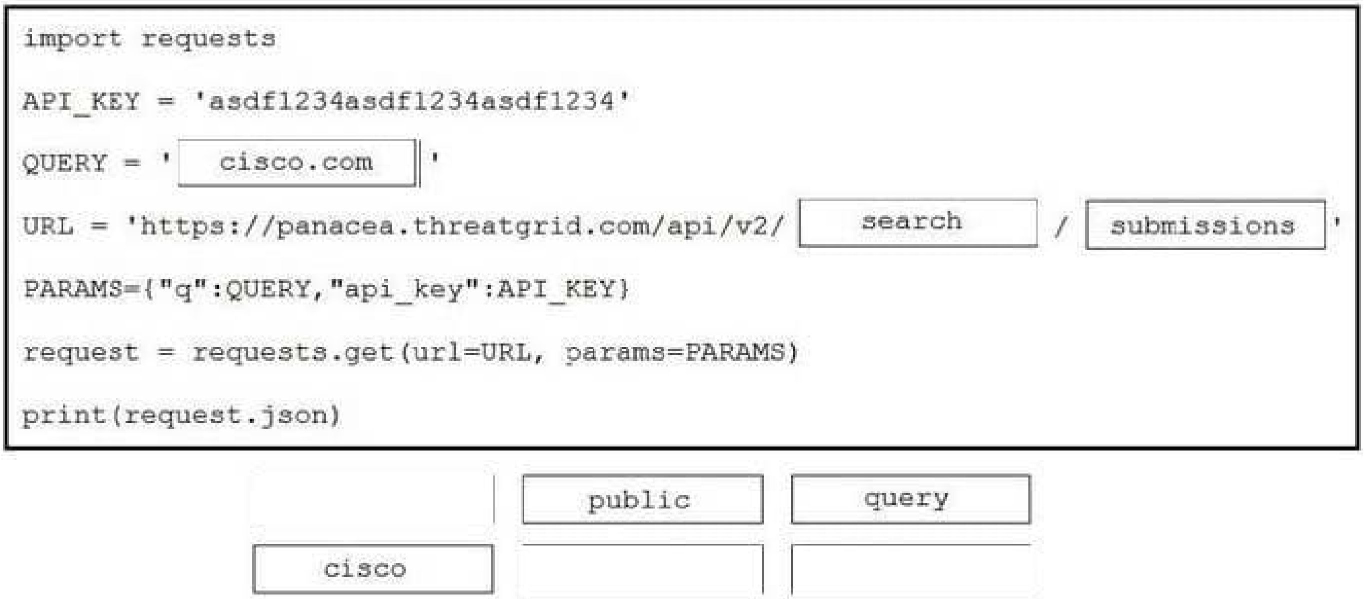
Drag and drop the code to complete the script to search Cisco ThreatGRID and return all public submission records associated with cisco.com. Not all options are used.

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)
```

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)
```

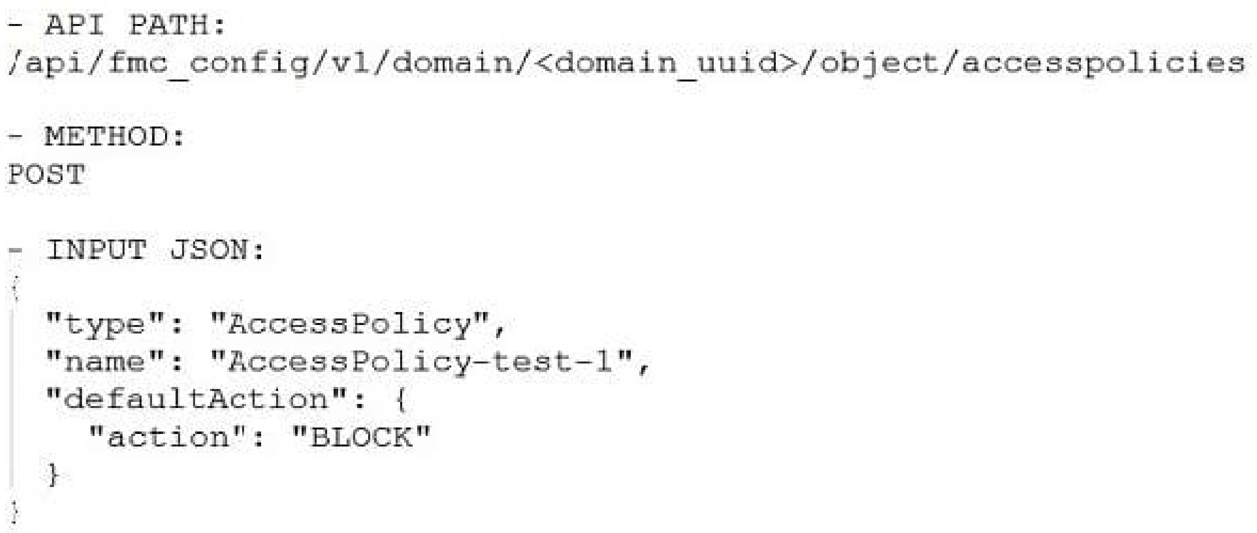
Reference: https://community.cisco.com/t5/endpoint-security/amp-threat-grid-api/m-p/3538319

QUESTION 5

If the goal is to create an access policy with the default action of blocking traffic, using Cisco Firepower Management

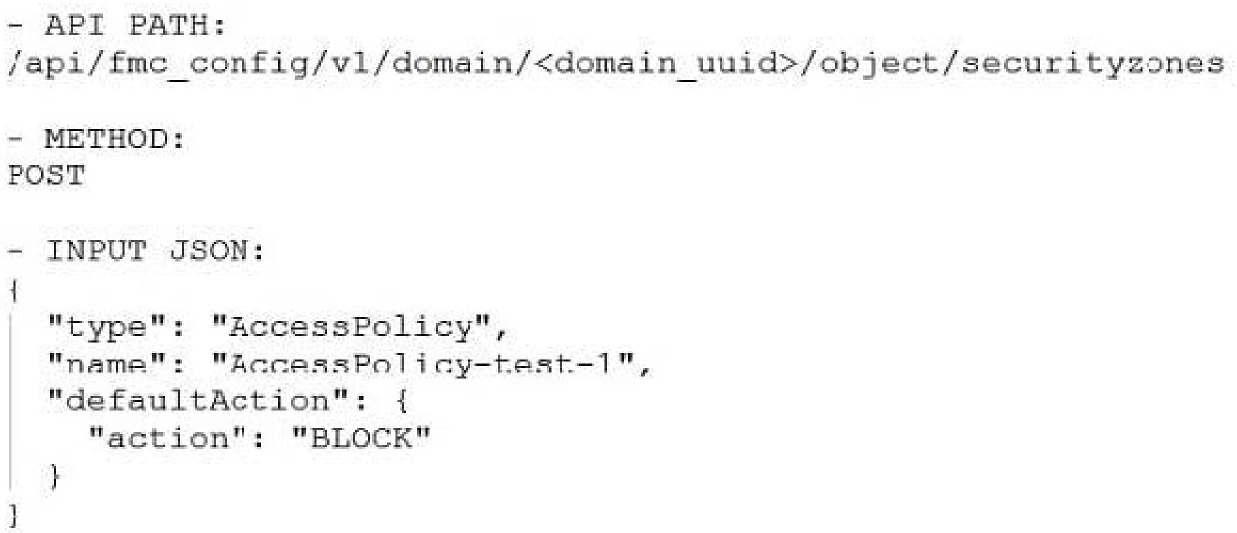
Center REST APIs, which snippet is used?

A.



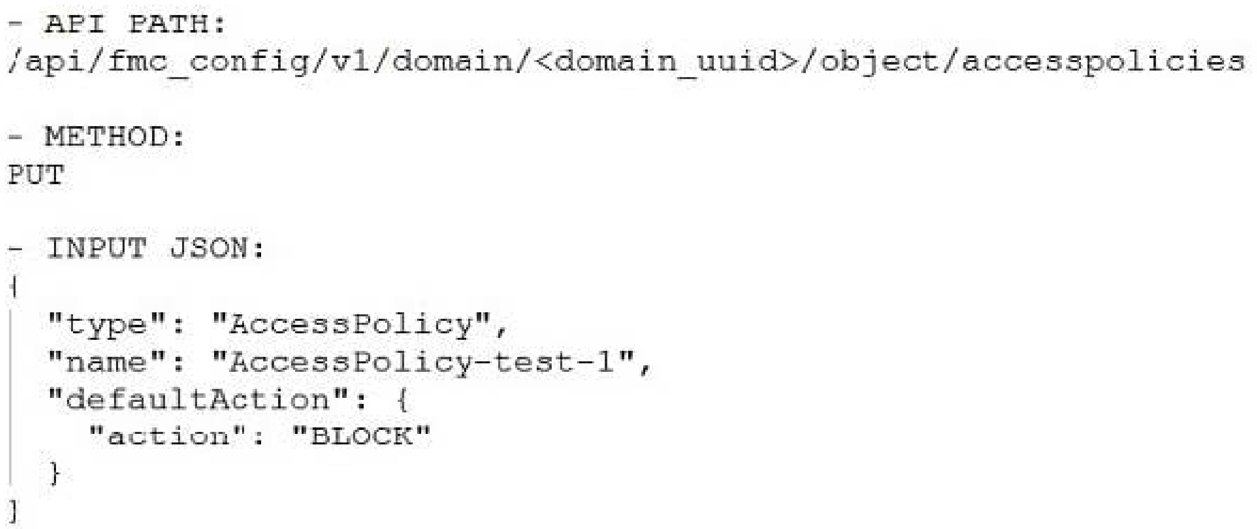
```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/accesspolicies

- METHOD:
POST

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

B.

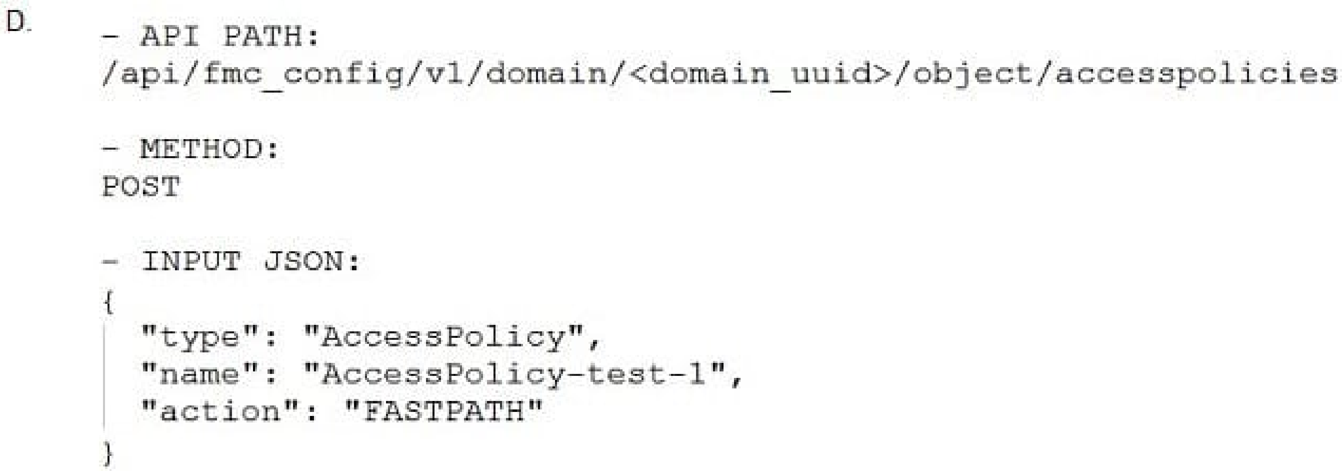


```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/securityzones

- 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"
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

Latest 300-735 Dumps 300-735 VCE Dumps 300-735 Exam Questions