DUMPSARENA

Automating and Programming Cisco Security Solutions (300-735 SAUTO)

Cisco 300-735

Version Demo

Total Demo Questions: 10

Total Premium Questions: 58

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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=2016-0910T19:00:00.000Z&endDate=2018-09-24T23:00:00.000Z&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

ANSWER: D

QUESTION NO: 2 - (DRAG DROP)

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:

ANSWER:

Explanation:

Reference:

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

QUESTION NO: 3

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

ANSWER: C E

QUESTION NO: 4

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.

ANSWER: B E

QUESTION NO: 5

```
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.

ANSWER: A B

QUESTION NO: 6

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

ANSWER: C D

QUESTION NO: 7

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

ANSWER: D

QUESTION NO: 8

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

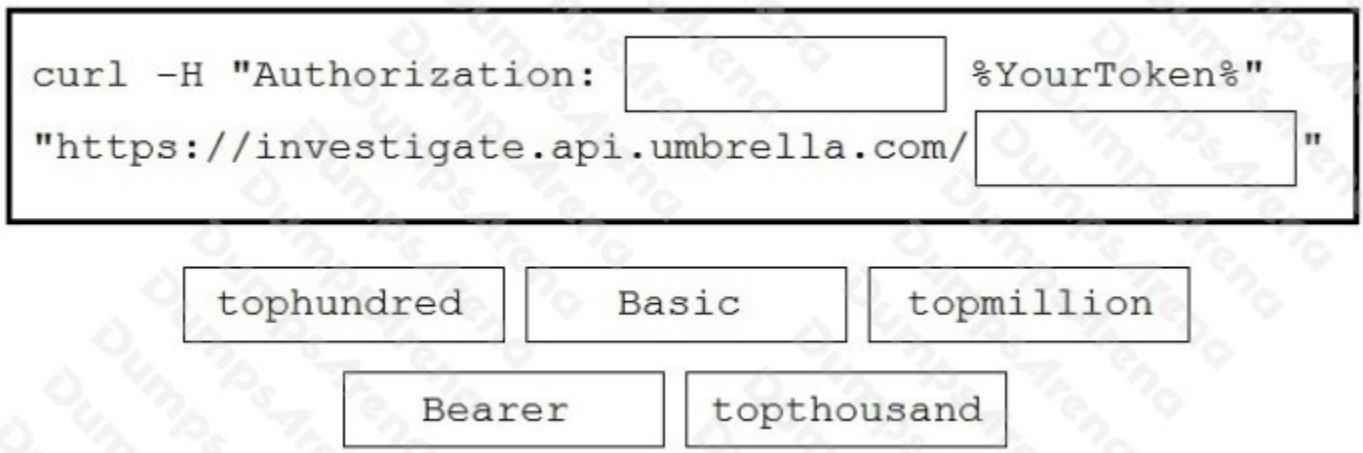
ANSWER: D

QUESTION NO: 9 - (DRAG DROP)

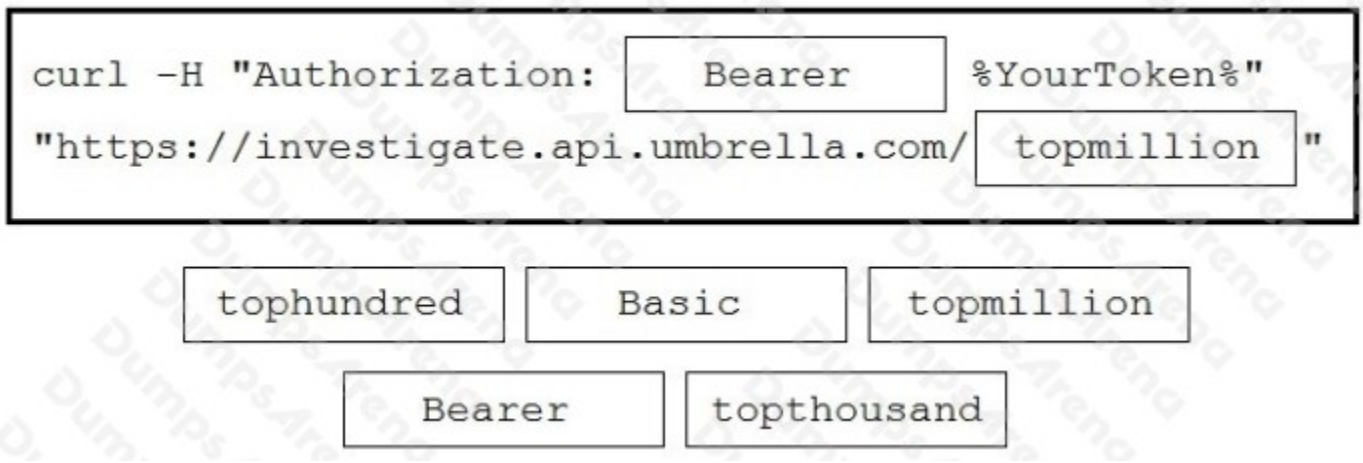
DRAG DROP

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:



ANSWER:



Explanation:

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

QUESTION NO: 10

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.

ANSWER: D