300-735 Q&As

Automating and Programming Cisco Security Solutions (SAUTO)

Pass Cisco 300-735 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/300-735.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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

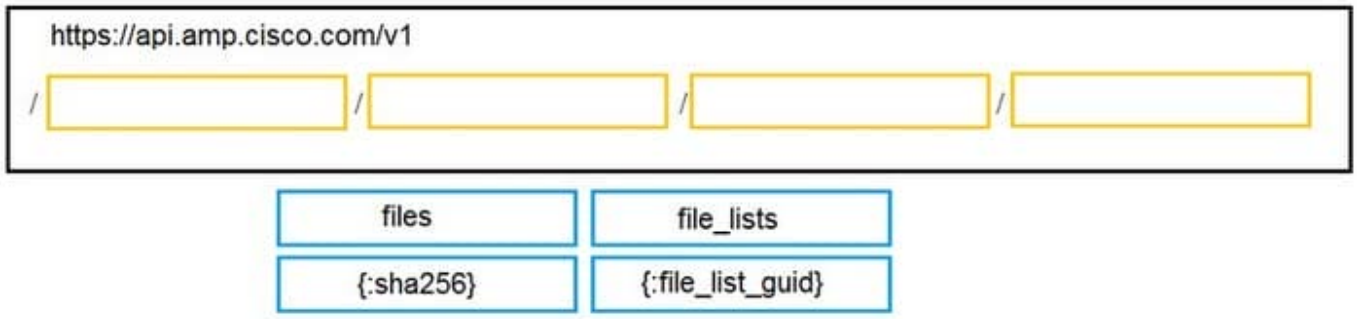
Correct Answer: BD

QUESTION 2

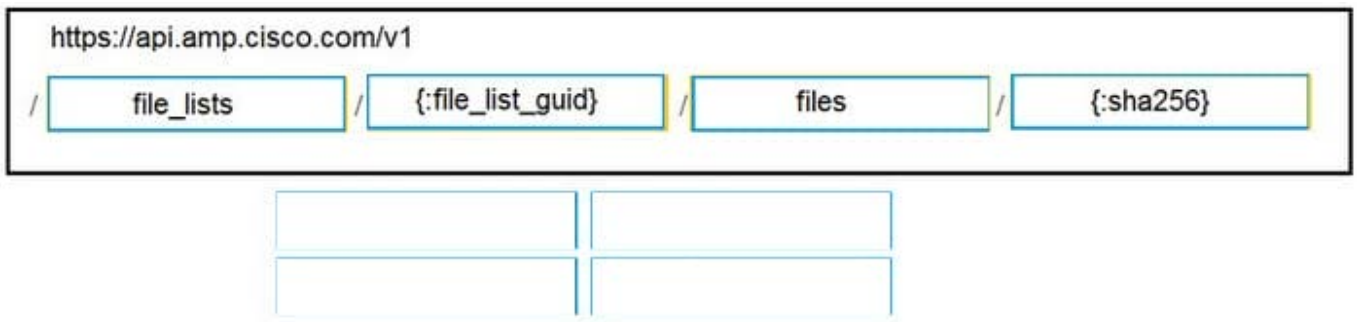
DRAG DROP

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:



Correct Answer:



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%7Dandapi_host=api.eu.amp.cisco.comandapi_resource=File+List+Iteman

dapi_version=v1

QUESTION 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

Correct Answer: CE

QUESTION 4

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.

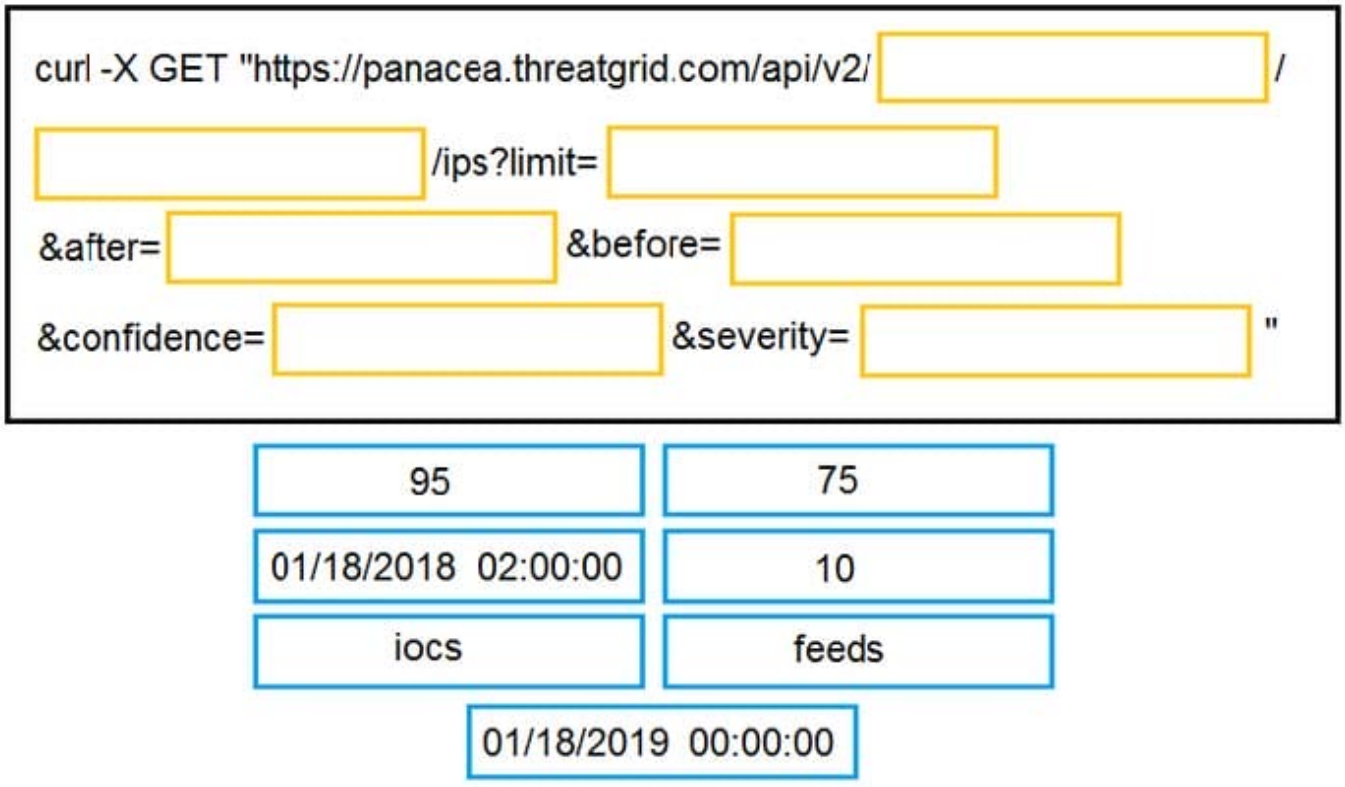
E. RPC-based APIs are used primarily for CRUD operations.

Correct Answer: BD

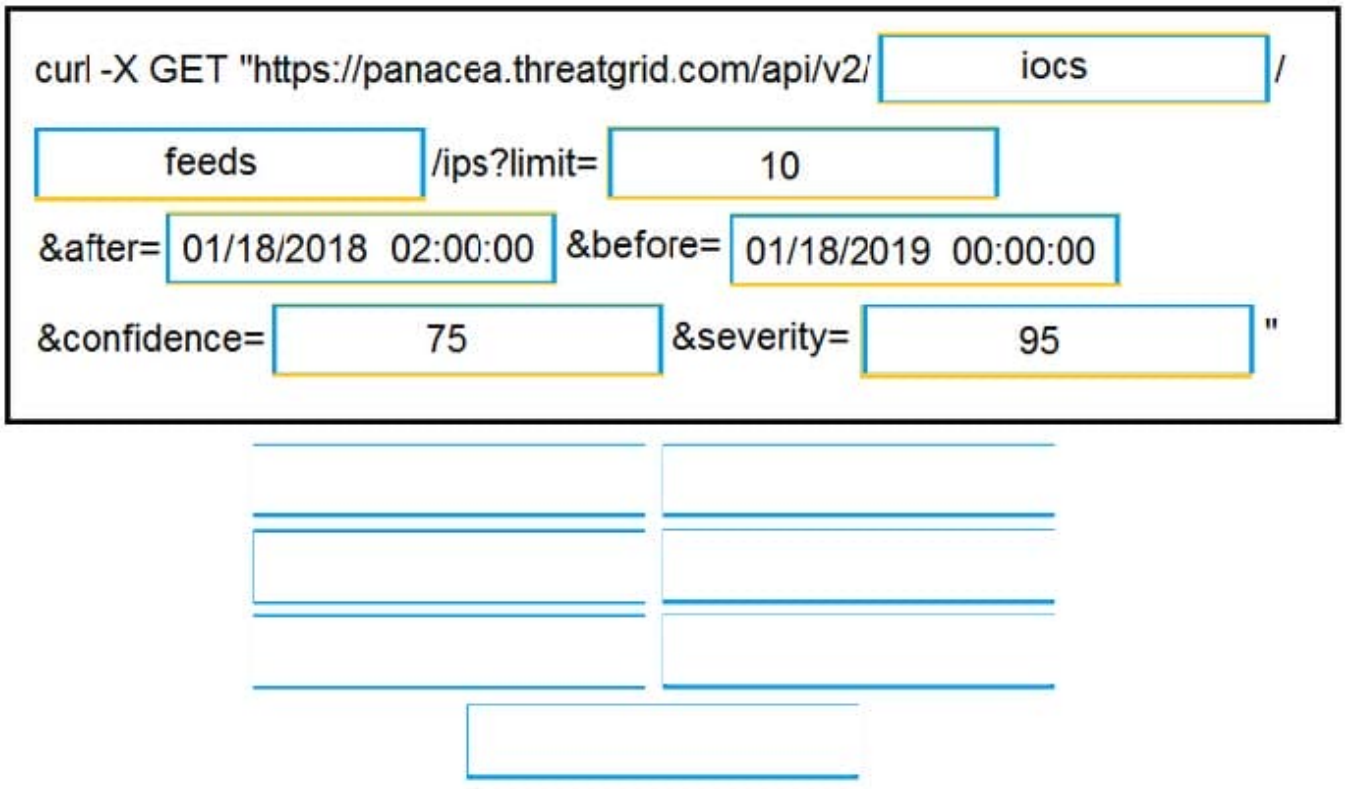
QUESTION 5

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:



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

QUESTION 6

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 7

Refer to the exhibit.

```
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}"
```

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

QUESTION 8

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

QUESTION 9

Refer to the exhibit.

```
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)
```

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

QUESTION 10

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