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:

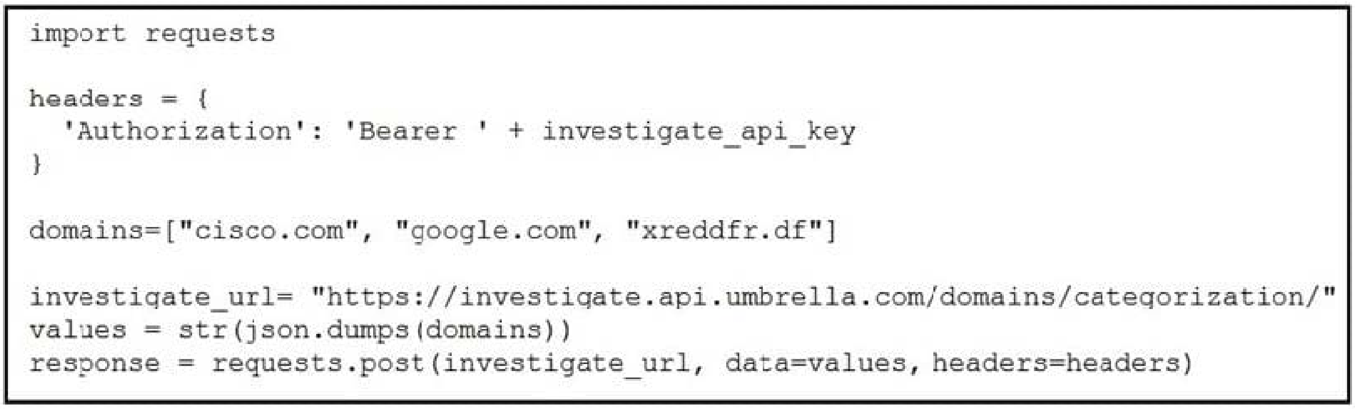
https://www.leads4pass.com/300-735.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibit.



```
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)
```

What does the response from the API contain when this code is executed?

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

Correct Answer: D

QUESTION 2

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

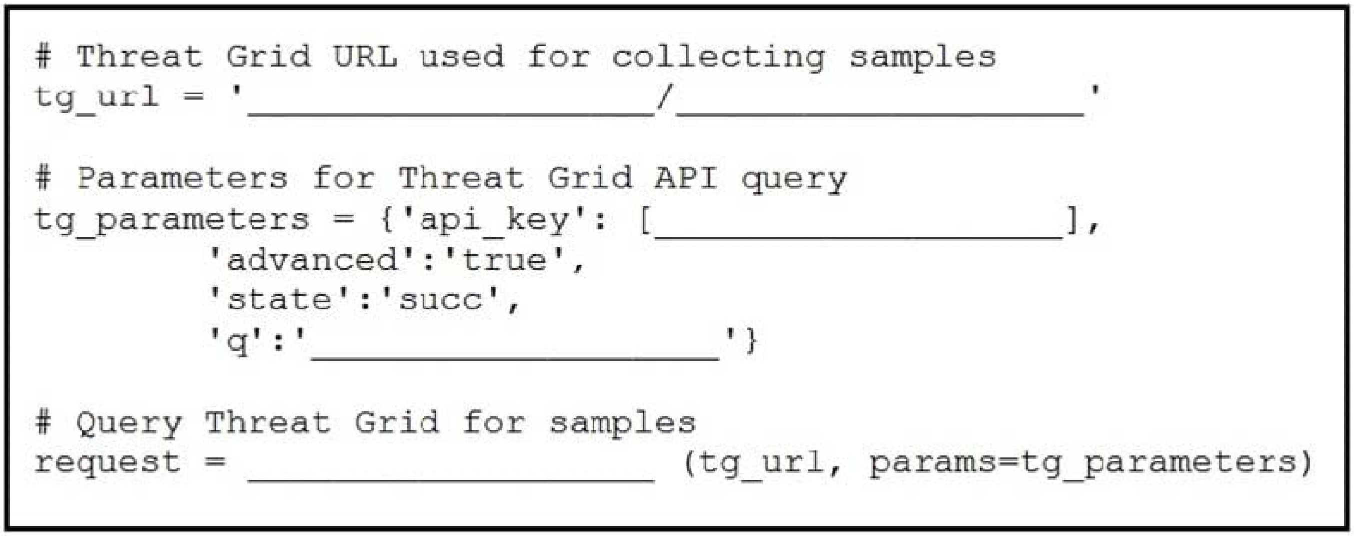
D. intrusion event extra data

E. malware events

Correct Answer: BD

QUESTION 3

DRAG DROP

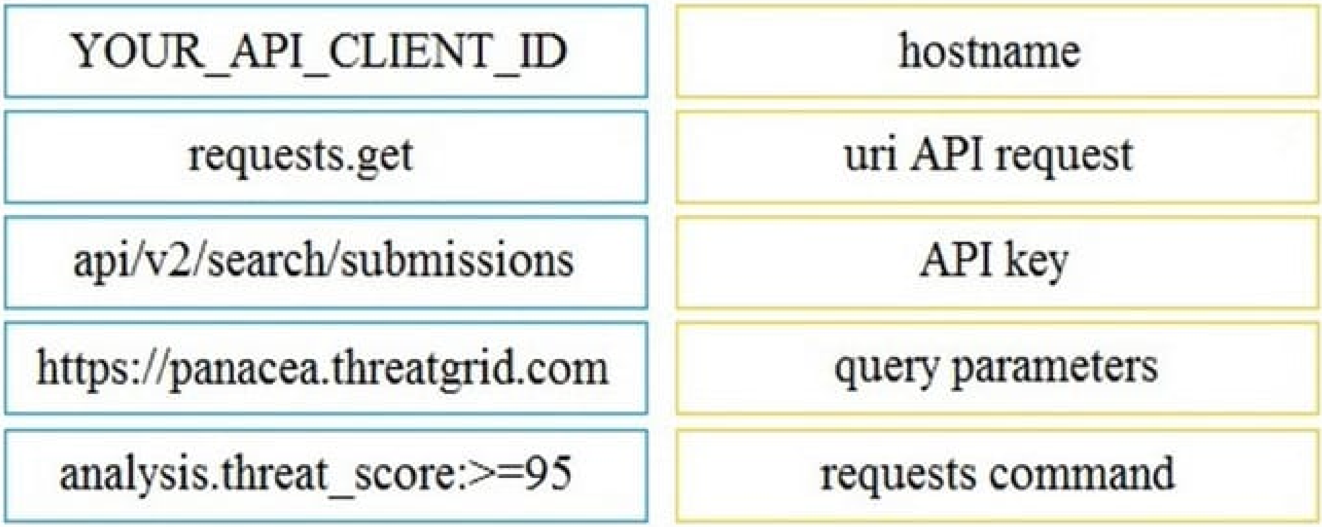


```
# Threat Grid URL used for collecting samples
tg_url = '____________________/____________________'

# 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.

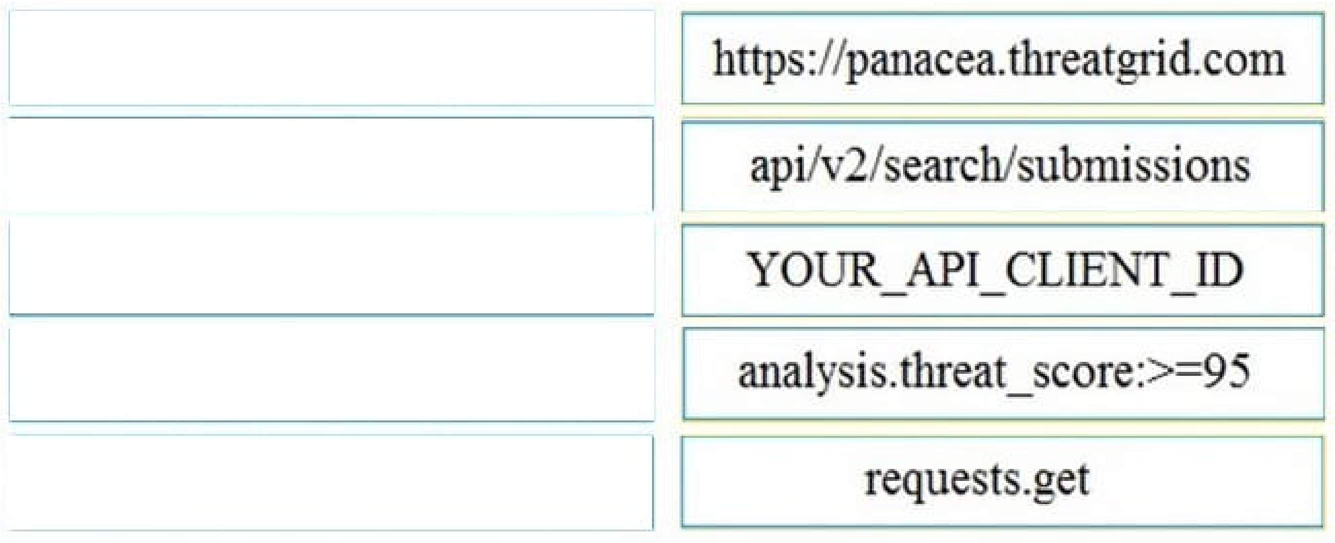
Drag and drop the elements from the left onto the script on the right that queries Cisco ThreatGRID for indications of compromise.

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

Correct Answer:



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

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

QUESTION 4

Which query parameter is required when using the reporting API of Cisco Security Management Appliances?

A. device_type

B. query_type

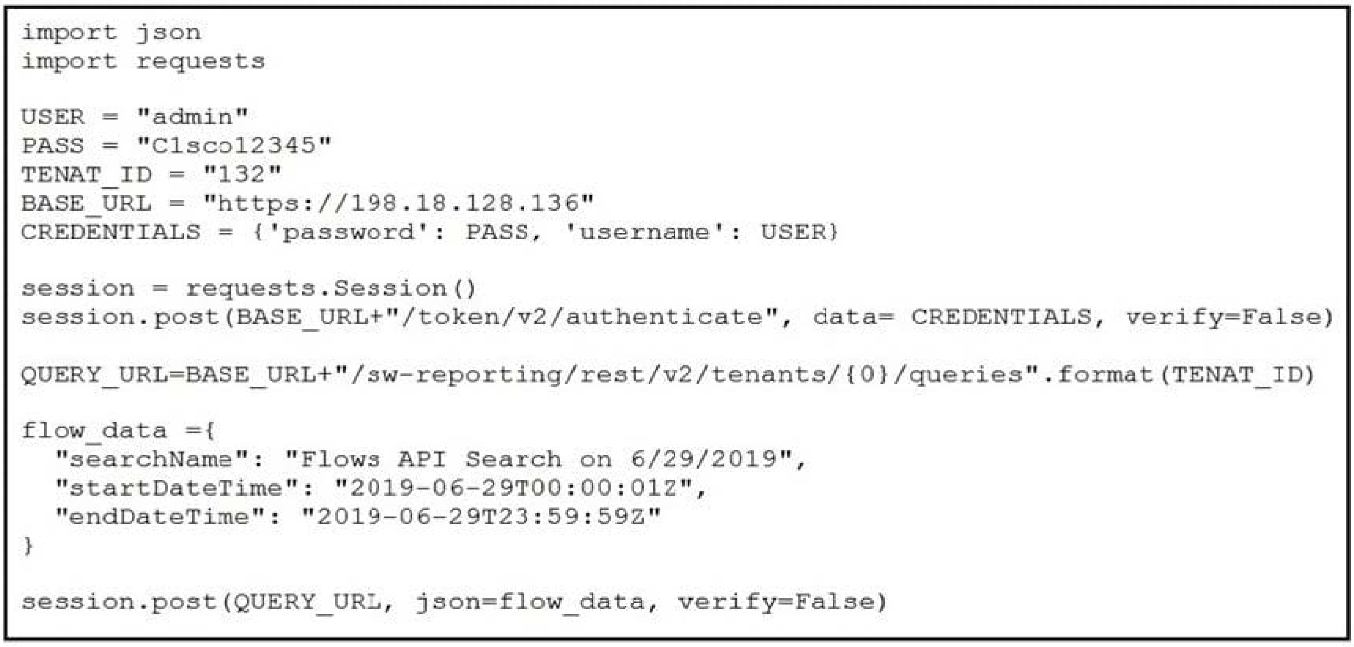
C. filterValue

D. startDate + endDate

Correct Answer: D

QUESTION 5

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