

Cisco

Exam Questions 300-735

Automating and Programming Cisco Security Solutions (SAUTO)



NEW QUESTION 1

Refer to the exhibit.
Which expression prints the text "802.1x"?

- A. print(quiz[0]['choices']['b'])
- B. print(quiz['choices']['b'])
- C. print(quiz[0]['choices']['b']['802.1x'])
- D. print(quiz[0]['question']['choices']['b'])

Answer: A

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

Which snippet is used to create an object for network 10.0.69.0/24 using Cisco Firepower Management Center REST APIs?

- A.

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

- METHOD:
POST

- INPUT JSON:
{
  "type": "Network",
  "value": "10.0.69.0/24",
  "overridable": false,
  "description": " ",
  "name": "Branch_1_net"
}
```

- B.
- ```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/networkgroups

- METHOD:
PUT

- INPUT JSON:
{
 "type": "Network",
 "value": "10.0.69.0/24",
 "overridable": false,
 "description": " ",
 "name": "Branch_1_net"
}
```
- C.
- ```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/networkgroups

- METHOD:
POST

- INPUT JSON:
{
  "type": "Network",
  "value": "10.0.69.0/24",
  "overridable": false,
  "description": " "
}
```
- D.
- ```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/networks

- METHOD:
POST

- INPUT JSON:
{
 "type": "Network",
 "value": "10.0.69.0/24",
 "overridable": false,
 "description": " "
}
```

**Answer:** A

#### NEW QUESTION 4

In Cisco AMP for Endpoints, which API queues to find the list of endpoints in the group "Finance Hosts," which has a GUID of 6c3c2005-4c74-4ba7-8dbb-c4d5b6baf03?

- A. [https://api.amp.cisco.com/v1/endpoints?group\[\]=6c3c2005-4c74-4ba7-8dbb-c4d5b6baf03](https://api.amp.cisco.com/v1/endpoints?group[]=6c3c2005-4c74-4ba7-8dbb-c4d5b6baf03)  
B. [https://api.amp.cisco.com/v1/computers?group\\_guid\[\]=6c3c2005-4c74-4ba7-8dbb-c4d5b6baf03](https://api.amp.cisco.com/v1/computers?group_guid[]=6c3c2005-4c74-4ba7-8dbb-c4d5b6baf03)  
C. [https://api.amp.cisco.com/v1/computers?group\\_guid-6c3c2005-4c74-4ba7-8dbb-c4d5b6baf03](https://api.amp.cisco.com/v1/computers?group_guid-6c3c2005-4c74-4ba7-8dbb-c4d5b6baf03)  
D. <https://api.amp.cisco.com/v1/endpoints?group-6c3c2005-4c74-4ba7-8dbb-c4d5b6baf03>

**Answer:** B

#### NEW QUESTION 5

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:** CD

#### NEW QUESTION 6

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:** CE

#### NEW QUESTION 7

Which API is designed to give technology partners the ability to send security events from their platform/service/appliance within a mutual customer's environment to the Umbrella cloud for enforcement?

- A. Cisco Umbrella Management API
- B. Cisco Umbrella Security Events API
- C. Cisco Umbrella Enforcement API
- D. Cisco Umbrella Reporting API

**Answer:** C

#### NEW QUESTION 8

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 9

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:** BE

#### NEW QUESTION 10

```
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 12**

```
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 17**

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=2016-09-10T19:00:00.000Z&endDate=2018-0924T23:00:00.000Z&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**

**NEW QUESTION 19**

Which two commands create a new local source code branch? (Choose two.)

- A. git checkout -b new\_branch
- B. git branch -b new\_branch
- C. git checkout -f new\_branch
- D. git branch new\_branch
- E. git branch -m new\_branch

**Answer: AD**

**NEW QUESTION 20**

Which header set should be sent with all API calls to the Cisco Stealthwatch Cloud API?

- A. Content-Type: application/json  
Accept: application/json  
Authorization: Bearer <api\_key>
- B. Content-Type: application/json  
Accept: application/json  
Authorization: ApiKey <username>:<api\_key>
- C. Content-Type: application/json  
Accept: application/json  
Authorization: Basic <api\_key>
- D. Content-Type: application/json  
Accept: application/json  
Authorization: <username>:<api\_key>

**Answer:** B

#### **NEW QUESTION 25**

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

#### **NEW QUESTION 29**

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 32**

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

**Answer:** D

#### **NEW QUESTION 35**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 300-735 Practice Exam Features:

- \* 300-735 Questions and Answers Updated Frequently
- \* 300-735 Practice Questions Verified by Expert Senior Certified Staff
- \* 300-735 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* 300-735 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The 300-735 Practice Test Here](#)**