



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

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.

Answer: CE

NEW QUESTION 4

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:

```
curl -H "Authorization:  %YourToken%"  
"https://investigate.api.umbrella.com/
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```
curl -H "Authorization:  %YourToken%"  
"https://investigate.api.umbrella.com/
```

NEW QUESTION 5

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 6

After changes are made to the Cisco Firepower Threat Defense configuration using the Cisco Firepower Device Manager API, what must be done to ensure that the new policy is activated?

- A. Submit a POST to the /api/fdm/latest/operational/deploy URI.
- B. Submit a GET to the /api/fdm/latest/operational/deploy URI.
- C. Submit a PUT to the /api/fdm/latest/devicesettings/pushpolicy URI.
- D. Submit a POST to the /api/fdm/latest/devicesettings/pushpolicy URI.

Answer: A

NEW QUESTION 7

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

Answer: B

NEW QUESTION 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"
}
```

Answer: D

NEW QUESTION 9

Refer to the exhibit. A network operator wants to add a certain IP to a DMZ tag.
Which code segment completes the script and achieves the goal?

- A.

```
tag_data = json.dumps(tag_session['data'])
tag_data['ranges'].append(DMZ_IP)
session.put(TAG_URL, json=tag_data, headers=HEADERS, verify=False)
```
- B.

```
tag_data = json.loads(tag_session['data'])
tag_data['ranges'].append(DMZ_IP)
session.put(TAG_URL, data=tag_data, headers=HEADERS, verify=False)
```
- C.

```
tag_data = json.dumps(tag_session['data'])
tag_data['ranges'].append(DMZ_IP)
session.put(TAG_URL, data=json.loads(tag_data), headers=HEADERS, verify=False)
```
- D.


```
tag_data = json.loads(tag_session)['data']
tag_data['ranges'].append(DMZ_IP)
session.put(TAG_URL, json=tag_data, headers=HEADERS, verify=False)
```

Answer: A

NEW QUESTION 10

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 10

```
curl -X PUT \
--header "Accept: application/json" \
--header "Authorization: Bearer ${ACCESS_TOKEN}" \
--header "Content-Type: application/json" \
-d '{
  "id": "XXXXXXXXXX",
  "ruleAction": "DENY",
  "eventLogAction": "LOG_FLOW_START",
  "type": "accessrule",
}' \
"https://${HOST}:${PORT}/api/fdm/v3/policy/accesspolicies
/{parentId}/accessrules/{objId}"
```

Refer to the exhibit. 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.

Answer: C

NEW QUESTION 13

FILL BLANK

Fill in the blank to complete the statement with the correct technology.

Cisco Investigate provides access to data that pertains to DNS security events and correlations collected by the Cisco security team.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Umbrella

NEW QUESTION 16

Which two destinations are supported by the Cisco Security Management Appliance reporting APIs? (Choose two.)

- A. email
- B. Microsoft Word file
- C. FTP
- D. web
- E. csv file

Answer: AD

NEW QUESTION 19

```
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 22

Which two APIs are available from Cisco ThreatGRID? (Choose two.)

- A. Access
- B. User Scope
- C. Data
- D. Domains
- E. Curated Feeds

Answer: CE

NEW QUESTION 26

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 28

Which API is used to query if the domain "example.com" has been flagged as malicious by the Cisco Security Labs team?

- A. `https://s-platform.api.opendns.com/1.0/events?example.com`
- B. `https://investigate.api.umbrella.com/domains/categorization/example.com`
- C. `https://investigate.api.umbrella.com/domains/volume/example.com`
- D. `https://s-platform.api.opendns.com/1.0/domains?example.com`

Answer: B

NEW QUESTION 31

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 35

Request URL:

https://198.18.133.8/api/fdm/v1/policy/intrusionpolicies

Refer to the exhibit.
What is the purpose of the API represented by this URL?

- A. Getting or setting intrusion policies in FMC
- B. Creating an intrusion policy in FDM
- C. Updating access policies
- D. Getting the list of intrusion policies configured in FDM

Answer: D

NEW QUESTION 36

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:

https://api.amp.cisco.com/v1

/

/

/

/

files

file_lists

{:sha256}

{:file_list_guid}

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

https://api.amp.cisco.com/v1

/

file_lists

/

{:file_list_guid}

/

files

/

{:sha256}

files

file_lists

{:sha256}

{:file_list_guid}

NEW QUESTION 39

.....

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](#)