

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.pass2lead.com/300-735.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

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

Correct Answer: C

QUESTION 2

Refer to the exhibit.

```
def query(config, secret, url, payload):
    print('query url=' + url)
    print(' request=' + payload)
    handler = urllib.request.HTTPSHandler(context=config.get_ssl_context())
    opener = urllib.request.build_opener(handler)
    rest_request = urllib.request.Request(url=url, data=str.encode(payload))
    rest_request.add_header('Content-Type', 'application/json')
    rest_request.add_header('Accept', 'application/json')
    b64 = base64.b64encode((config.get_node_name() + ':' + secret).encode()).decode()
    rest_request.add_header('Authorization', 'Basic ' + b64)
    rest_response = opener.open(rest_request)
    print(' response status=' + str(rest_response.getcode()))
    print(' response content=' + rest_response.read().decode())
```

A Python function named "query" has been developed and the goal is to use it to query the service "com.cisco.ise.session" via Cisco pxGrid 2.0 APIs.

How is the function called, if the goal is to identify the sessions that are associated with the IP address 10.0.0.50?

- A. query(config, secret, "getSessionByIpAddress/10.0.0.50", "ipAddress")
- B. query(config, "10.0.0.50", url, payload)
- C. query(config, secret, url, "10.0.0.50")
- D. query(config, secret, url, \{"ipAddress": "10.0.0.50"\})

Correct Answer: D

QUESTION 3

Refer to the exhibit.

```
quiz = [
  {
    "question": "Which of these is an IEEE standard for port-based Network Access Control",
    "choices": {"a": "802.11x", "b": "802.1x", "c": "802.11a", "d": "802.11b"},
    "answer": "b"
  },
]
```

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\])`

Correct Answer: A

QUESTION 4

Refer to the exhibit.

```
import json
import requests

USER = "admin"
PASS = "Cisco12345"
TENAT_ID = "132"
TAG_ID = "24"
BASE_URL = "https://198.18.128.136"
CREDENTIALS = {'password': PASS, 'username': USER}
DMZ_IP = "198.18.128.147"
HEADERS = {'Content-type': 'application/json', 'Accept': 'application/json'}

session = requests.Session()
session.post(BASE_URL+"/token/v2/authenticate", data= CREDENTIALS, verify=False)

TAG_URL=BASE_URL+"/smc-configuration/rest/v1/tenants/{0}/tags/{1}".format(TENAT_ID, TAG_ID)

tag_session = session.get(url=TAG_URL, verify=False).content.decode()
```

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)
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Correct Answer: A

QUESTION 5

DRAG DROP

Drag and drop the code to complete the Cisco Umbrella Investigate WHOIS query that returns a list of domains that are associated with the email address "admin@example.com". Not all options are used.

Select and Place:

"https://investigate.api.umbrella.com/ [] /		
[] /	[]	"
email	emails	WHOIS
admin@example.com	whois	{admin@example.com}

Correct Answer:

```
"https://investigate.api.umbrella.com/ [WHOIS] /  
[emails] / [admin@example.com]"
```

email		
	whois	{admin@example.com}

Explanation: <https://docs.umbrella.com/investigate-api/docs/whois-information-for-a-domain-1>

QUESTION 6

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:

```
curl -X GET "https://panacea.threatgrid.com/api/v2/[ ] /  
[ ]/ips?limit=[ ]  
&after=[ ] &before=[ ]  
&confidence=[ ] &severity=[ ]"
```

95	75
01/18/2018 02:00:00	10
iocs	feeds
01/18/2019 00:00:00	

Correct Answer:

```
curl -X GET "https://panacea.threatgrid.com/api/v2/ iocs /  
feeds /ips?limit= 10  
&after= 01/18/2018 02:00:00 &before= 01/18/2019 00:00:00  
&confidence= 75 &severity= 95 "
```


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

QUESTION 7

A security network engineer must implement intrusion policies using the Cisco Firepower Management Center API.

Which action does the engineer take to achieve the goal?

- A. Make a PATCH request to the URI /api/fmc_config/v1/domain/{DOMAIN_UUID}/policy/intrusionpolicies.
- B. Make a POST request to the URI /api/fmc_config/v1/domain/{DOMAIN_UUID}/policy/intrusionpolicies.
- C. Intrusion policies can be read but not configured using the Cisco Firepower Management Center API.
- D. Make a PUT request to the URI /api/fmc_config/v1/domain/{DOMAIN_UUID}/policy/intrusionpolicies.

Correct Answer: C

QUESTION 8

DRAG DROP

Drag and drop the items to complete the pxGrid script to retrieve all Adaptive Network Control policies. Assume that username, password, and base URL are correct. Not all options are used.

Select and Place:


```
import base64
import json
import requests

USER = "admin"

PASS = "Cisco1234"

HEADERS = {"Content-Type": "application/json"}

URL = 'https://10.10.20.50:8910/pxgrid/control/  '

b64_pass = base64.b64encode((USER + ':' + PASS).encode()).decode()

HEADERS['Authorization'] = 'Bearer +b64_pass

request = requests.  (url=URL, headers=HEADERS)
```

getPolicies

adaptive

getControl

control

post

get

Correct Answer:

```
import base64
import json
import requests

USER = "admin"

PASS = "Cisco1234"

HEADERS = {"Content-Type": "application/json"}

URL = 'https://10.10.20.50:8910/pxgrid/control/ getPolicies '

b64_pass = base64.b64encode((USER + ':' + PASS).encode()).decode()

HEADERS['Authorization'] = 'Bearer +b64_pass

request = requests. get (url=URL, headers=HEADERS)
```

	adaptive	getControl
control	post	

Reference: <https://developer.cisco.com/docs/pxgrid/#!retrieving-all-anc-polices/java-sample-code>

QUESTION 9

A developer has just completed the configuration of an API that connects sensitive internal systems. Based on company policies, the security of the data is a high priority.

Which approach must be taken to secure API keys and passwords?

- A. Embed them directly in the code.
- B. Store them in a hidden file.
- C. Store them inside the source tree of the application.
- D. Change them periodically.

Correct Answer: D

QUESTION 10

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