

Exam Questions 300-735

Automating and Programming Cisco Security Solutions (SAUTO)

<https://www.2passeasy.com/dumps/300-735/>



NEW QUESTION 1

DRAG DROP

Drag and drop the code to complete the script to search Cisco ThreatGRID and return all public submission records associated with cisco.com. Not all options are used.

Select and Place:

```
import requests

API_KEY = 'asdf1234asdf1234asdf1234'

QUERY = ' ',

URL = 'https://panacea.threatgrid.com/api/v2/ ' / ' ',

PARAMS={"q":QUERY,"api_key":API_KEY}

request = requests.get(url=URL, params=PARAMS)

print(request.json)
```

submissions

public

query

cisco

search

cisco.com

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

```
import requests

API_KEY = 'asdf1234asdf1234asdf1234'

QUERY = ' cisco.com ',

URL = 'https://panacea.threatgrid.com/api/v2/ search ' / ' submissions ',

PARAMS={"q":QUERY,"api_key":API_KEY}

request = requests.get(url=URL, params=PARAMS)

print(request.json)
```

submissions

public

query

cisco

search

cisco.com

NEW QUESTION 2

Refer to the exhibit. A security engineer attempts to query the Cisco Security Management appliance to retrieve details of a specific message. What must be added to the script to achieve the desired result?

- A. Add message ID information to the URL string as a URI.
B. Run the script and parse through the returned data to find the desired message.
C. Add message ID information to the URL string as a parameter.
D. Add message ID information to the headers.

Answer: C

NEW QUESTION 3

Refer to the exhibit. 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
B. followed by an integer (key:value) to the flow_data.
C. Add a for loop at the end of the script, and print each key value pair separately.
D. Add flowLimit, followed by an integer (key:value) to the flow_data.
E. Change the startDateTime and endDateTime values to include smaller time intervals.
F. Change the startDate and endDate values to include smaller date intervals.

Answer: AB

NEW QUESTION 4

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 5

DRAG DROP

Drag and drop the code to complete the curl query to the Umbrella Reporting API that provides a detailed report of blocked security activity events from the organization with an organizationId of "12345678" for the last 24 hours. Not all options are used.

Select and Place:

```
curl --include --header "Authorization: Basic %base64string%"
https://reports.api.umbrella.com/v1/ [ ] /
[ ] / [ ]
```

12345678	security-activity
security-activity-events	organizations
organizationId	security-events

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

```
curl --include --header "Authorization: Basic %base64string%"
https://reports.api.umbrella.com/v1/ organizations /
organizationId / security-activity
```

12345678	security-activity
security-activity-events	organizations
organizationId	security-events

NEW QUESTION 6

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 7

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 8

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
- D. <https://api.amp.cisco.com/v1/endpoints?group-6c3c2005-4c74-4ba7-8dbb-c4d5b6baf03>

Answer: B

NEW QUESTION 9

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 10

DRAG DROP

```
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())
```

Refer to the exhibit. A Python function named "query" has been developed, and will be used to query the service "com.cisco.ise.session" via Cisco pxGrid 2.0 APIs. Drag and drop the code to construct a Python call to the "query" function to identify the user groups that are associated with the user "fred". Not all options are used. Select and Place:

query (, ,
 ,)

"getUserGroupByUserName", "fred"

url

'{ "userName": "fred" }'

secret

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

query (, ,
 ,)

"getUserGroupByUserName", "fred"

url

'{ "userName": "fred" }'

secret

NEW QUESTION 10

Which curl command lists all tags (host groups) that are associated with a tenant using the Cisco Stealthwatch Enterprise API?

- A. curl -X PUT "Cookie:{Cookie Data}"https://{stealthwatch_host}/smc-configuration/rest/v1/tenants/{tenant_id}/tags
B. curl -X POST -H"Cookie:{Cookie Data}"https://{stealthwatch_host}/smc-configuration/rest/v1/tenants/tags
C. curl -X GET -H"Cookie:{Cookie Data}"https://{stealthwatch_host}/smc-configuration/rest/v1/tenants/{tenant_id}/tags
D. curl -X GET -H"Cookie:{Cookie Data}"https://{stealthwatch_host}/smc-configuration/rest/v1/tenants/tags

Answer: C

NEW QUESTION 12

```
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 missin
- 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 15

DRAG DROP

A Python script is being developed to return the top 10 identities in an organization that have made a DNS request to "www.cisco.com". Drag and drop the code to complete the Cisco Umbrella Reporting API query to return the top identities. Not all options are used. Select and Place:

```
import requests

URL = 'https://reports.api.umbrella.com/v1/organizations/fe4936f9/
[ ] / [ ] / [ ]'

HEADERS = {'Authorization': 'Basic aGVsb29oYXViYnd5YXNk'}

response = requests.get(URL, headers=HEADERS)
```

security-activity

destinations

activity

www.cisco.com

identities

topIdentities

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```
import requests

URL = 'https://reports.api.umbrella.com/v1/organizations/fe4936f9/
[ ] / [ ] / [ ]'

HEADERS = {'Authorization': 'Basic aGVsb29oYXViYnd5YXNk'}

response = requests.get(URL, headers=HEADERS)
```

security-activity

destinations

activity

www.cisco.com

identities

topIdentities

NEW QUESTION 16

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.

Answer: CE

NEW QUESTION 21

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 26

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

Which URI string is used to create a policy that takes precedence over other applicable policies that are configured on Cisco Stealthwatch?

A. /tenants/{tenantId}/policy/system/host-policy

B. /tenants/{tenantId}/policy/system/role-policy

C. /tenants/{tenantId}/policy/system

D. /tenants/{tenantId}/policy/system/{policyId}

Answer: A

NEW QUESTION 32

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-735 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-735 Product From:

<https://www.2passeasy.com/dumps/300-735/>

Money Back Guarantee

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 FirstTry
- * 300-735 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year