

Cisco

Exam Questions 300-735

Automating and Programming Cisco Security Solutions (SAUTO)



NEW QUESTION 1

DRAG DROP

Drag and drop the code to complete the API call to query all Cisco Stealthwatch Cloud observations. Not all options are used.
Select and Place:

<input type="text"/>	<code>https://example.observbl.com/api/v3/</code>
<input type="text"/>	<code>/</code> <input type="text"/>

observations	DELETE	GET
POST	all/	all
obsrv	?query=all	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

GET	<code>https://example.observbl.com/api/v3/</code>
observations	<code>/</code> <input type="text" value="all"/>

observations	DELETE	GET
POST	all/	all
obsrv	?query=all	

NEW QUESTION 2

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 3

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:

<code>curl --include --header "Authorization: Basic %base64string%"</code>
<code>https://reports.api.umbrella.com/v1/</code> <input type="text"/>
<input type="text"/> <code>/</code> <input type="text"/>

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 4

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 5

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/
```

tophundred

Basic

topmillion

Bearer

topthousand

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

tophundred

Basic

topmillion

Bearer

topthousand

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

```
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 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"}')

Answer: D

NEW QUESTION 8

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 9

```
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 10

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 10

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 13

```
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 17

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 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 21

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 25

Which snippet describes the way to create an URL object in Cisco FDM using FDM REST APIs with curl?

- A.

```
curl -X POST --header 'Content-Type: application/json' \
--header 'Authorization: Bearer $Token' \
--header 'Accept: application/json' -d '{ \
    "id": "bfc6j984-9dcf-11e9-a6b5-617eea9159d3", \
    "description": "Google URL", \
    "url": "https://www.google.com", \
    "type": "urlobject" \
}' 'https://198.18.133.8/api/fdm/v1/object/url'
```
- B.

```
curl -X POST --header 'Content-Type: application/json' \
--header 'Authorization: Bearer $Token' \
--header 'Accept: application/json' -d '{ \
    "name": "google_url", \
    "description": "Google URL", \
    "url": "https://www.google.com", \
    "type": "urlobject" \
}' 'https://198.18.133.8/api/fdm/v1/object/urls'
```
- C.

```
curl -X POST --header 'Content-Type: application/json' \
--header 'Authorization: Bearer $Token' \
--header 'Accept: application/json' -d '{ \
    "name": "google_url", \
    "description": "Google URL", \
    "url": "https://www.google.com", \
    "type": "networkobject" \
}' 'https://198.18.133.8/api/fdm/v1/object/urls'
```
- D.

```
curl -X POST --header 'Content-Type: application/json' \
--header 'Authorization: Bearer $Token' \
--header 'Accept: application/json' -d '{ \
    "id": "bfc6j984-9dcf-11e9-a6b5-617eea9159d3", \
    "description": "Google URL", \
    "url": "https://www.google.com", \
    "type": "urlobject" \
}' 'https://198.18.133.8/api/fdm/v1/object/urlcategories'
```

Answer: B

NEW QUESTION 26

Refer to the exhibit. A network operator wrote a Python script to retrieve events from Cisco AMP.

```
import requests
CLIENT_ID = 'a1b2c3d4e5f6g7h8i9j0'
API_KEY = 'a1b2c3d4-e5f6-g7h8-i9j0-k112m3n4o5p6'
----MISSING CODE----
URL = BASE_URL+'v1/events'
request = requests.get(url, auth=(amp_client_id, amp_api_key))
```

Against which API gateway must the operator make the request?

- A. BASE_URL = "https://api.amp.cisco.com"
- B. BASE_URL = "https://amp.cisco.com/api"
- C. BASE_URL = "https://amp.cisco.com/api/"
- D. BASE_URL = "https://api.amp.cisco.com/"

Answer: A

NEW QUESTION 31

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 33

Which step is required by Cisco pxGrid providers to expose functionality to consumer applications that are written in Python? A. Look up the existing service using the /pxgrid/control/ServiceLookup endpoint.

- A. Register the service using the /pxgrid/control/ServiceRegister endpoint.
- B. Configure the service using the /pxgrid/ise/config/profiler endpoint.
- C. Expose the service using the /pxgrid/ise/pubsub endpoint.

Answer: D

NEW QUESTION 34

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 38
.....

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](#)