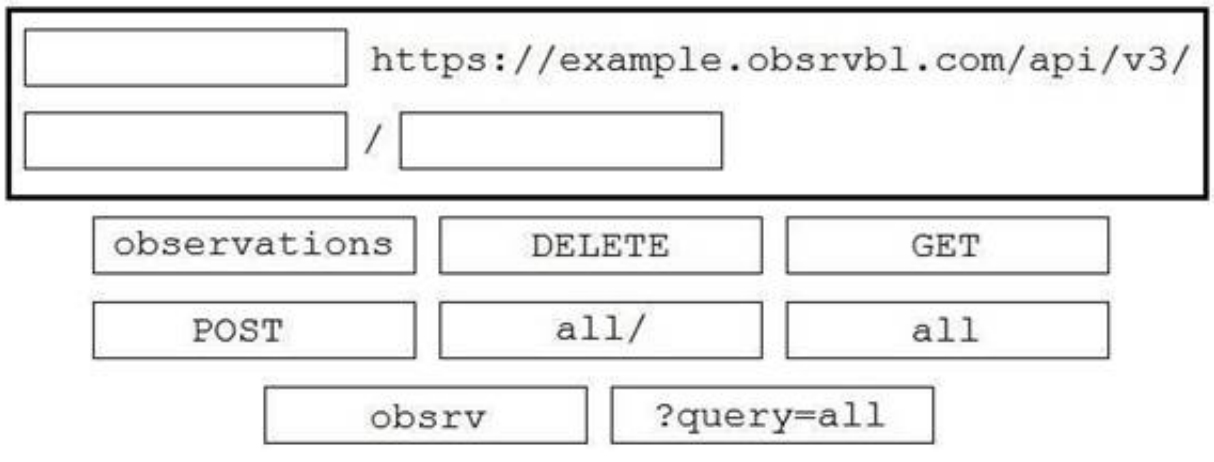
Exam Questions 300-735

Automating and Programming Cisco Security Solutions (SAUTO)

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

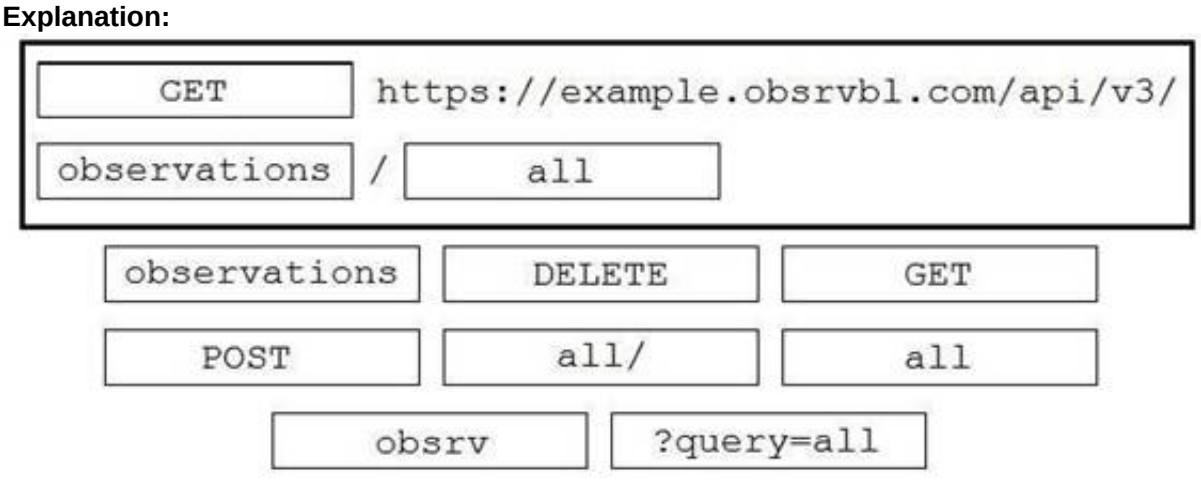
NEW QUESTION 1
DRAG DROP
Drag and drop the code to complete the API call to query all Cisco Stealthwatch Cloud observations. Not all options are used.
Select and Place:



A. Mastered
B. Not Mastered

Answer: A

Explanation:

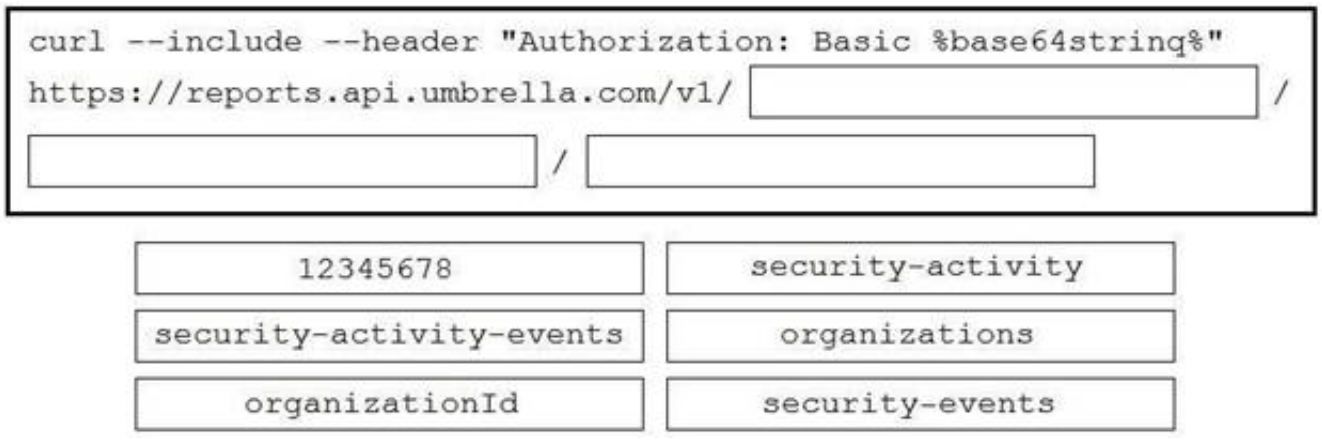


NEW QUESTION 2
Refer to the exhibit. A network operator must generate a daily flow report and learn how to act on or manipulate returned data. When the operator runs the script, it returns an enormous amount of information. Which two actions enable the operator to limit returned data? (Choose two.)

A. Add recordLimi
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

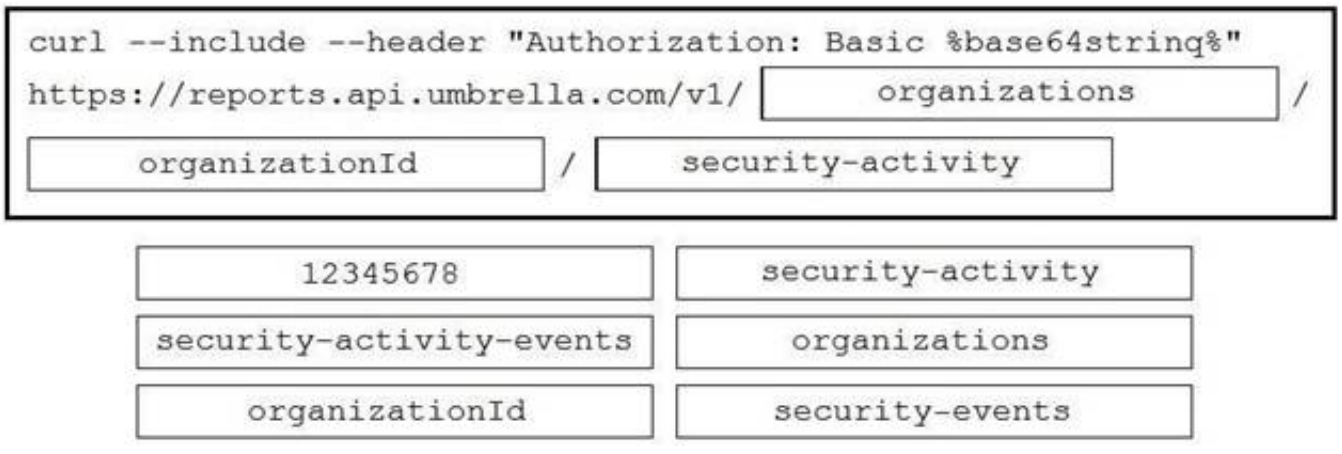
NEW QUESTION 3
DRAG DROP
Drag and drop the code to complete the curl query to the Umbrella Reporting API that provides a detailed report of blocked security activity events from the organization with an organizationId of "12345678" for the last 24 hours. Not all options are used.
Select and Place:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 4
When the URI "/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies" is used to make a POST request, what does "e276abec-e0f2-11e3-8169- 6d9ed49b625f" represent?

A. API token
B. domain UUID
C. access policy UUID
D. object UUID

Answer: B

NEW QUESTION 5
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-c4d5b6bafe03?

A. https://api.amp.cisco.com/v1/endpoints?group[]=6c3c2005-4c74-4ba7-8dbb-c4d5b6bafe03
B. https://api.amp.cisco.com/v1/computers?group_guid[]=6c3c2005-4c74-4ba7-8dbb-c4d5b6bafe03
C. https://api.amp.cisco.com/v1/computers?group_guid-6c3c2005-4c74-4ba7-8dbb-c4d5b6bafe03
D. https://api.amp.cisco.com/v1/endpoints?group-6c3c2005-4c74-4ba7-8dbb-c4d5b6bafe03

Answer: B

NEW QUESTION 6
Which two API capabilities are available on Cisco Identity Services Engine? (Choose two.)

A. Platform Configuration APIs
B. Monitoring REST APIs
C. Performance Management REST APIs
D. External RESTful Services APIs
E. Internal RESTful Services APIs

Answer: BD

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
Which two event types can the eStreamer server transmit to the requesting client from a managed device and a management center? (Choose two.)

A. user activity events
B. intrusion events
C. file events
D. intrusion event extra data
E. malware events

Answer: BD

NEW QUESTION 9
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.

Answer: C

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 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 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 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 15
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 23

```
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 24
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 27
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 29

```
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 32
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

.....

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