

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.pass4itsure.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

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:

| tps | s://reports.api.umbrella.com/ | v1/ | |
|-----|-------------------------------|-------------------|--|
| | / | | |
| | 12345678 | security-activity | |
| | | | |
| | security-activity-events | organizations | |

Correct Answer:

| //reports.api.umbrella.co | m/v1/ organizations |
|---------------------------|---------------------|
| organizationId / | security-activity |
| 12345678 | |
| | 1 0 |

Reference: https://docs.umbrella.com/umbrella-api/docs/security-activity-report

QUESTION 2

The Cisco Security Management Appliance API is used to make a GET call using the URI /sma/api/v2.0/reporting/mail_i ncoming_traffic_summary/detected_amp?startDate=2016-09-10T19:00:00.000ZandendDate=2018-0924T23:00:00.000Zandevice_type=esaanddevice_name=esa01.

What does this GET call return?

A. values of all counters of a counter group, with the device group name and device type for web



- B. value of a specific counter from a counter group, with the device name and type for email
- C. value of a specific counter from a counter group, with the device name and type for web
- D. values of all counters of a counter group, with the device group name and device type for email

Correct Answer: D

QUESTION 3

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



| Α. | curl –X POSTheader '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' |
| В. | curl –X POSTheader '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 POSTheader 'Content-Type: application/json' \ |
| | header 'Authorization: Bearer \$Token' \ |
| | header 'Accept: application/json' -d '{ \ |
| | "name": "google_url", \ |
| | |
| | "description": "Google URL", \ |
| | "description": "Google URL", \ "url": "https://www.google.com", \ |
| | |
| | "url": "https://www.google.com", \ |
| D. | "url": "https://www.google.com", \ "type": "networkobject" \ }' 'https://198.18.133.8/api/fdm/v1/object/urls' |
| D. | "url": "https://www.google.com", \ "type": "networkobject" \ }' 'https://198.18.133.8/api/fdm/v1/object/urls' |
| D. | "url": "https://www.google.com", \ "type": "networkobject" \ }' 'https://198.18.133.8/api/fdm/v1/object/urls' curl –X POSTheader 'Content-Type: application/json' \ |
| D. | <pre>"url": "https://www.google.com", \ "type": "networkobject" \ }' 'https://198.18.133.8/api/fdm/v1/object/urls' curl _X POSTheader 'Content-Type: application/json' \header 'Authorization: Bearer \$Token' \</pre> |
| D. | <pre>"url": "https://www.google.com", \ "type": "networkobject" \ }' 'https://198.18.133.8/api/fdm/v1/object/urls' curl -X POSTheader 'Content-Type: application/json' \header 'Authorization: Bearer \$Token' \header 'Accept: application/json' -d '{ \</pre> |
| D. | <pre>"url": "https://www.google.com", \ "type": "networkobject" \ }' 'https://198.18.133.8/api/fdm/v1/object/urls' curl -X POSTheader 'Content-Type: application/json' \header 'Authorization: Bearer \$Token' \header 'Accept: application/json' -d '{ \ "id": "bfc6j984-9dcf-11e9-a6b5-617eea9159d3", \</pre> |
| D. | <pre>"url": "https://www.google.com", \ "type": "networkobject" \ }' 'https://198.18.133.8/api/fdm/v1/object/urls' curl -X POSTheader 'Content-Type: application/json' \header 'Authorization: Bearer \$Token' \header 'Accept: application/json' -d '{ \ "id": "bfc6j984-9dcf-11e9-a6b5-617eea9159d3", \ "description": "Google URL", \</pre> |



- A. Option A
- B. Option B
- C. Option C
- D. Option D
- Correct Answer: B

QUESTION 4

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
- Correct Answer: BD

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

Correct Answer: B

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.

```
Correct Answer: A
```

QUESTION 7

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.

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

```
Correct Answer: D
```

QUESTION 8

DRAG DROP

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 |

Correct Answer:



Reference: https://community.cisco.com/t5/endpoint-security/amp-threat-grid-api/m-p/3538319

QUESTION 9

Refer to the exhibit.

```
import requests
URL = 'https://reports.api.umbrella.com/v1/organizations/fe4936f9/destinations/www.cisco.com/activity'
HEADERS = {'Authorization': 'Basic aGVsb29oYXViYnd5YXNk'}
response = requests.get(URL, headers=HEADERS)
```

The script outputs too many results when it is queried against the Cisco Umbrella Reporting API.

Which two configurations restrict the returned result to only 10 entries? (Choose two.)

- A. Add params parameter in the get and assign in the {"return": "10"} value.
- B. Add ?limit=10 to the end of the URL string.
- C. Add params parameter in the get and assign in the {"limit": "10"} value.
- D. Add ?find=10 to the end of the URL string.
- E. Add ?return=10 to the end of the URL string.

Correct Answer: BC

QUESTION 10

Which header set should be sent with all API calls to the Cisco Stealthwatch Cloud API?

- Content-Type: application/json
 Accept: application/json
 Authorization: Bearer <api_key>
- B. Content-Type: application/json
 Accept: application/json
 Authorization: ApiKey <username>:<api_key>
- Content-Type: application/json
 Accept: application/json
 Authorization: Basic <api_key>
- D. Content-Type: application/json
 Accept: application/json
 Authorization: <username>:<api_key>
- A. Option A
- B. Option B
- C. Option C
- D. Option D
- Correct Answer: B

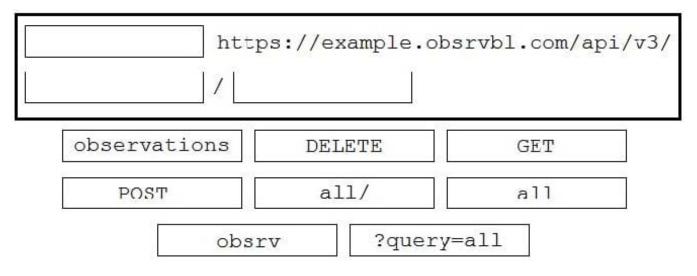
QUESTION 11



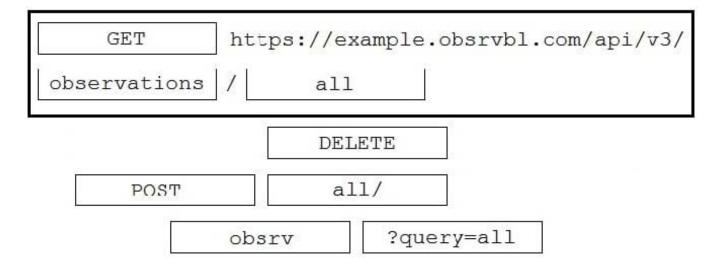
DRAG DROP

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:



Correct Answer:



QUESTION 12

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 13

For which two programming languages does Cisco offer an SDK for Cisco pxGrid 1.0? (Choose two.)

- A. Python
- B. Perl
- C. Java
- D. C
- E. JavaScript
- Correct Answer: CD

<u>300-735 PDF Dumps</u>

300-735 VCE Dumps

300-735 Practice Test