

## 300-735 Dumps

# Automating and Programming Cisco Security Solutions (SAUTO)

<https://www.certleader.com/300-735-dumps.html>



#### NEW QUESTION 1

Which description of synchronous calls to an API is true?

- A. They can be used only within single-threaded processes.
- B. They pause execution and wait for the response.
- C. They always successfully return within a fixed time.
- D. They can be used only for small requests.

**Answer:** B

#### 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

Refer to the exhibit.

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'])

**Answer:** A

#### NEW QUESTION 5

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 6

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: Bearer %YourToken%"  
"https://investigate.api.umbrella.com/topmillion"
```

tophundred   Basic   topmillion

Bearer   tophousand

#### NEW QUESTION 7

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](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 8

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

**Answer:** CD

#### NEW QUESTION 9

Refer to the exhibit. 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)
```

**Answer:** A

#### 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 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 11

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 15

Which two statements describe the characteristics of API styles for REST and RPC? (Choose two.)

- A. REST-based APIs function in a similar way to procedures.
- B. REST-based APIs are used primarily for CRUD operations.
- C. REST and RPC API styles are the same.
- D. RPC-based APIs function in a similar way to procedures.
- E. RPC-based APIs are used primarily for CRUD operations.

**Answer: BD**

#### NEW QUESTION 20

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 25

```
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 28**

The Cisco Security Management Appliance API is used to make a GET call using the URI  
/sma/api/v2.0/reporting/mail\_incoming\_traffic\_summary/detected\_amp?startDate=2016-09-10T19:00:00.000Z&endDate=2018-0924T23:00:00.000Z&device\_type=esa&device\_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

**Answer: D**

**NEW QUESTION 33**

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}

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

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

email	emails	WHOIS
admin@example.com	whois	{admin@example.com}

**NEW QUESTION 37**

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 38**

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 42

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 47

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 48

Which query parameter is required when using the reporting API of Cisco Security Management Appliances?

- A. device\_type
- B. query\_type
- C. filterValue
- D. startDate + endDate

**Answer:** D

#### NEW QUESTION 49

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your 300-735 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/300-735-dumps.html>