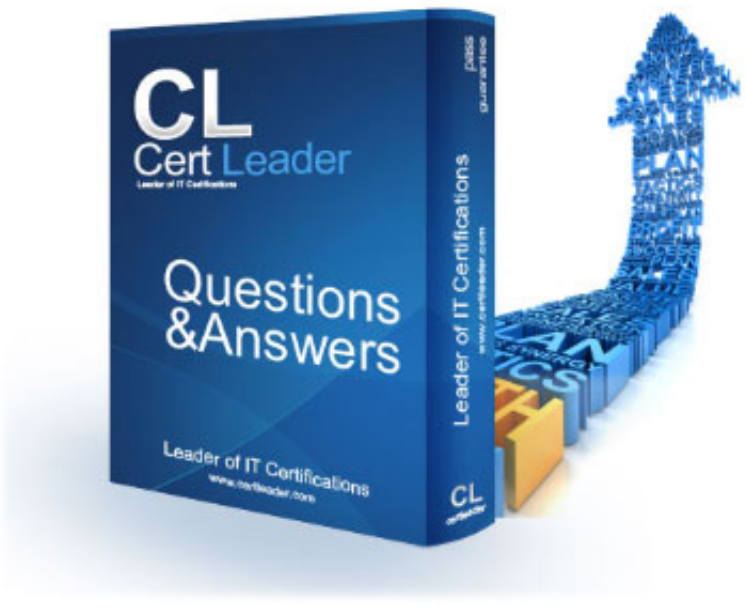
300-735 Dumps

Automating and Programming Cisco Security Solutions (SAUTO)

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



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

```
import requests

headers = {
  'Authorization': 'Bearer ' + investigate_api_key
}

domains=["cisco.com", "google.com", "xreddfr.df"]

investigate_url= "https://investigate.api.umbrella.com/domains/categorization/"
values = str(json.dumps(domains))
response = requests.post(investigate_url, data=values, headers=headers)
```

Refer to the exhibit.
What does the response from the API contain when this code is executed?

A. error message and status code of 403
B. newly created domains in Cisco Umbrella Investigate
C. updated domains in Cisco Umbrella Investigate
D. status and security details for the domains

Answer: D

NEW QUESTION 3
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 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:

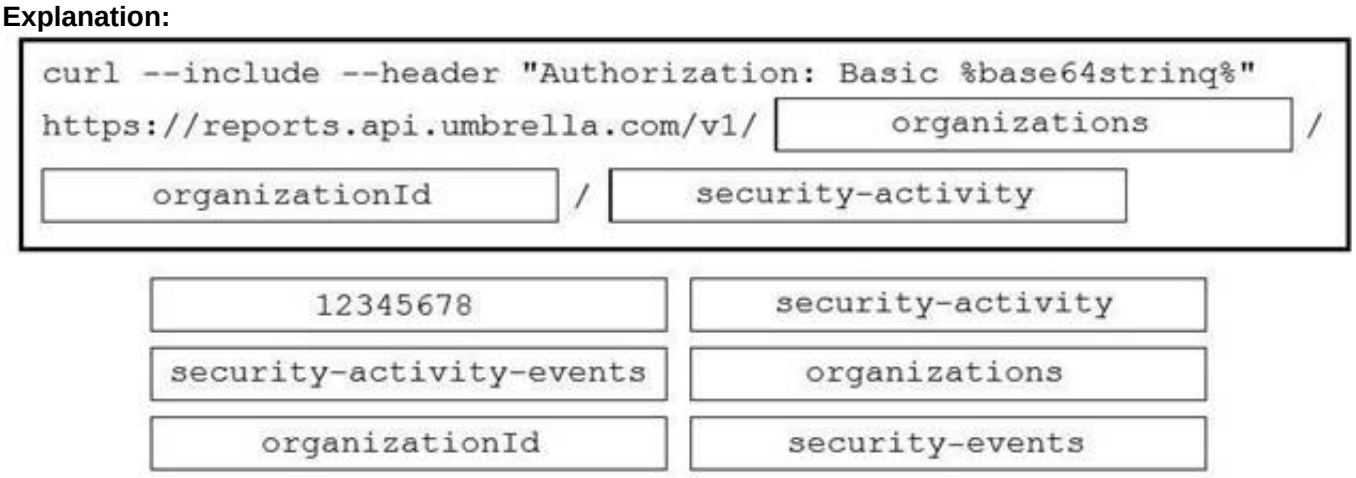
```
curl --include --header "Authorization: Basic %base64string%"
https://reports.api.umbrella.com/v1/ [          ] /
[          ] / [          ]
```

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

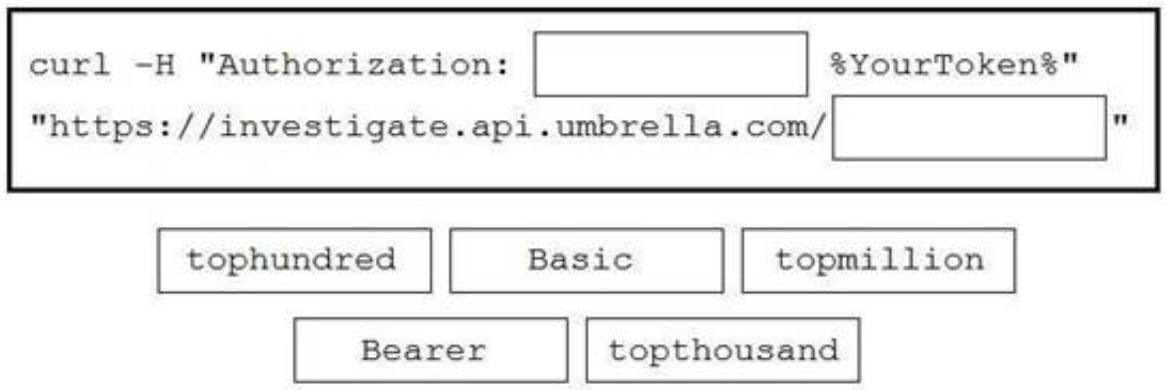
A. Mastered
B. Not Mastered

Answer: A

Explanation:



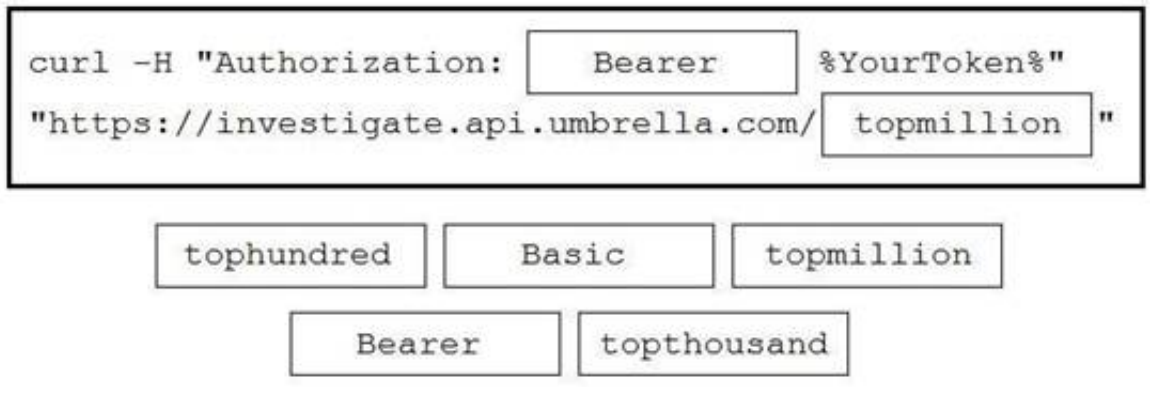
NEW QUESTION 6
DRAG DROP
Drag and drop the code to complete the curl command to query the Cisco Umbrella Investigate API for the umbrella popularity list. Not all options are used.
Select and Place:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 7
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 8
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 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
```
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 10
What are two capabilities of Cisco Firepower Management Center eStreamer? (Choose two.)

A. eStreamer is used to get sources for intelligence services.
B. eStreamer is used to send malware event data.
C. eStreamer is used to get a list of access control policies.
D. eStreamer is used to send policy data.
E. eStreamer is used to send intrusion event data.

Answer: BE

NEW QUESTION 12
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 14
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 17
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

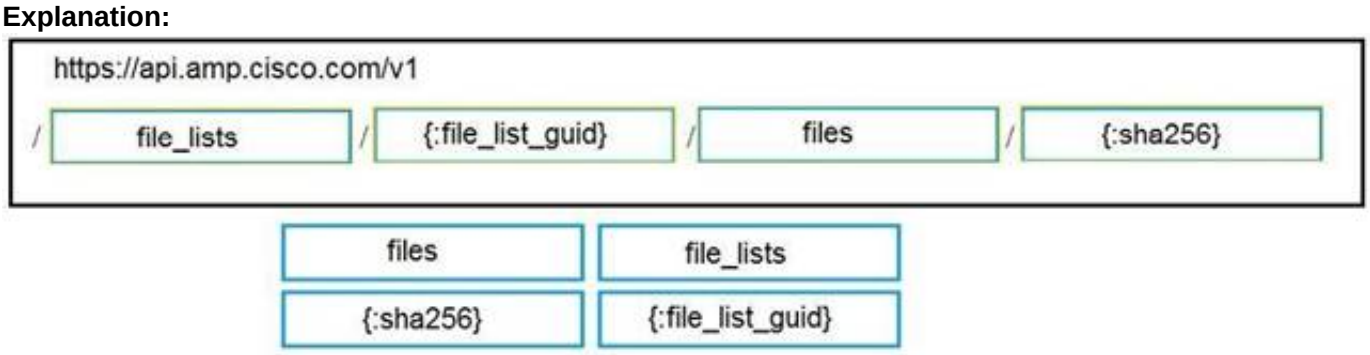
Answer: B

NEW QUESTION 20
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:

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 24
.....

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