Cisco

Exam Questions 300-735

Automating and Programming Cisco Security Solutions (SAUTO)

NEW QUESTION 1

```
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 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 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 4
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:

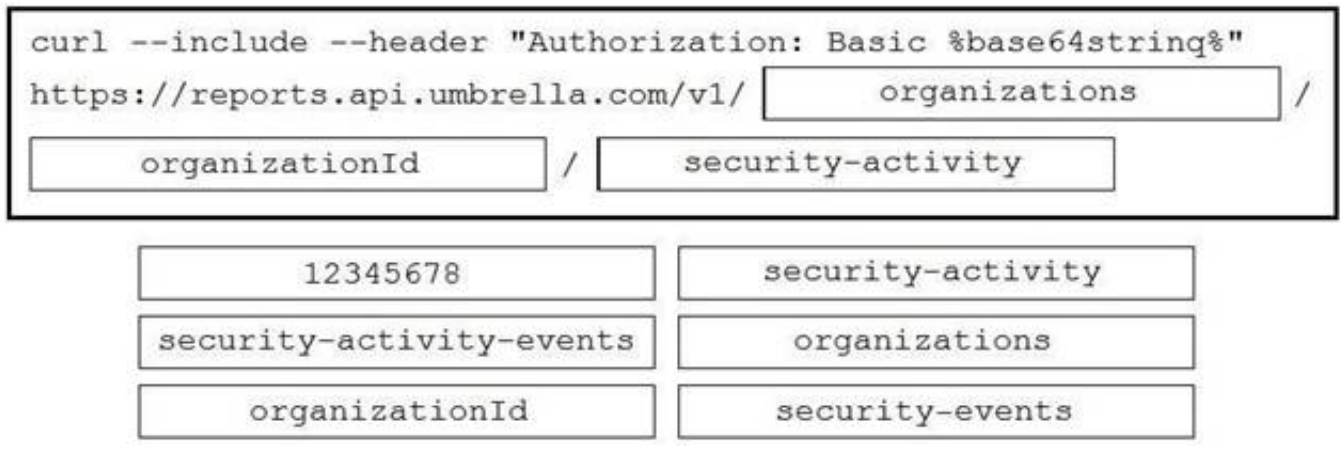
```
curl --include --header "Authorization: Basic %base64string%"
https://reports.api.umbrella.com/v1/ [          ] /
[          ] / [          ]
```

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 5
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 6
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 7
Refer to the exhibit.
Which URL returned the data?

A. https://api.amp.cisco.com/v1/computers
B. https://api.amp.cisco.com/v0/computers
C. https://amp.cisco.com/api/v0/computers
D. https://amp.cisco.com/api/v1/computers

Answer: A

NEW QUESTION 8
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.

Answer: A

NEW QUESTION 9

```
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 10
Which two API capabilities are available on Cisco Identity Services Engine? (Choose two.)

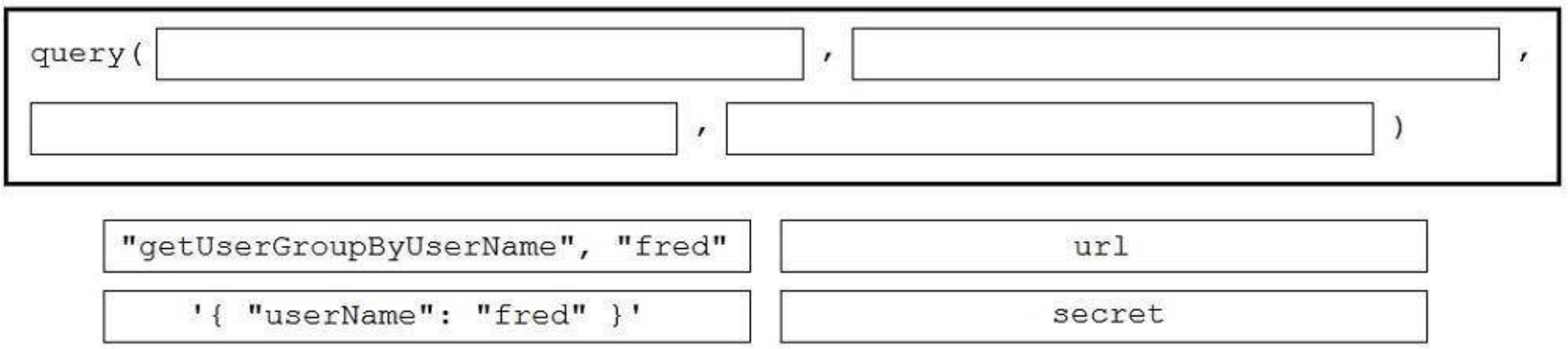
A. Platform Configuration APIs
B. Monitoring REST APIs
C. Performance Management REST APIs
D. External RESTful Services APIs
E. Internal RESTful Services APIs

Answer: BD

NEW QUESTION 10
DRAG DROP

```
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())
```

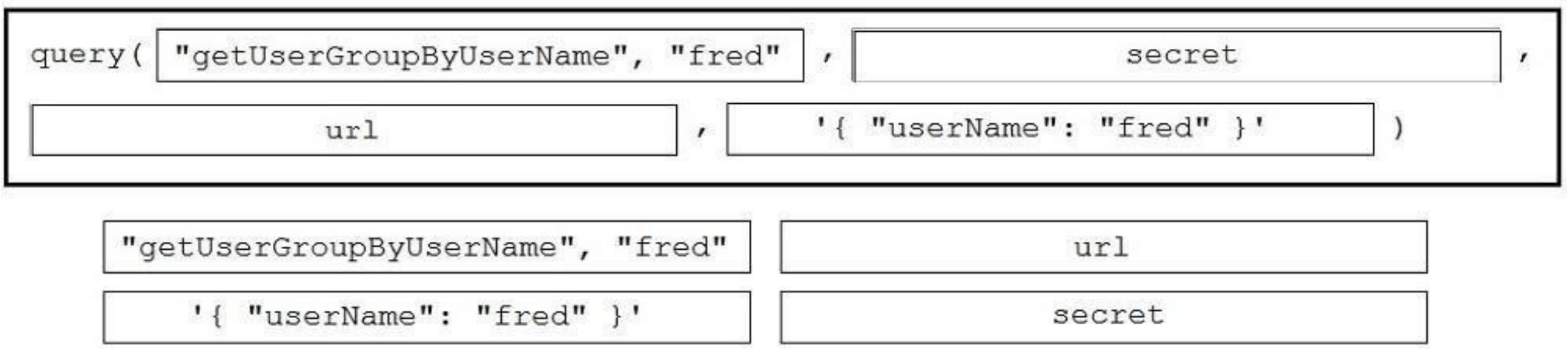
Refer to the exhibit. A Python function named "query" has been developed, and will be used to query the service "com.cisco.ise.session" via Cisco pxGrid 2.0 APIs. Drag and drop the code to construct a Python call to the "query" function to identify the user groups that are associated with the user "fred". Not all options are used. Select and Place:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 13
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 14
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 19
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 22
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 27
DRAG DROP
A Python script is being developed to return the top 10 identities in an organization that have made a DNS request to "www.cisco.com". Drag and drop the code to complete the Cisco Umbrella Reporting API query to return the top identities. Not all options are used. Select and Place:

```
import requests

URL = 'https://reports.api.umbrella.com/v1/organizations/fe4936f9/
[                    ] / [                    ] / [                    ]'

HEADERS = {'Authorization': 'Basic aGVsb29oYXViYnd5YXNk'}

response = requests.get(URL, headers=HEADERS)
```

security-activity	destinations	activity
www.cisco.com	identities	topIdentities

A. Mastered
B. Not Mastered

Answer: A

Explanation:

```
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)
```

security-activity	destinations	activity
www.cisco.com	identities	topIdentities

NEW QUESTION 31

```
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 32
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 34
Which two APIs are available from Cisco ThreatGRID? (Choose two.)

A. Access
B. User Scope
C. Data
D. Domains
E. Curated Feeds

Answer: CE

NEW QUESTION 38
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 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 46
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 51
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

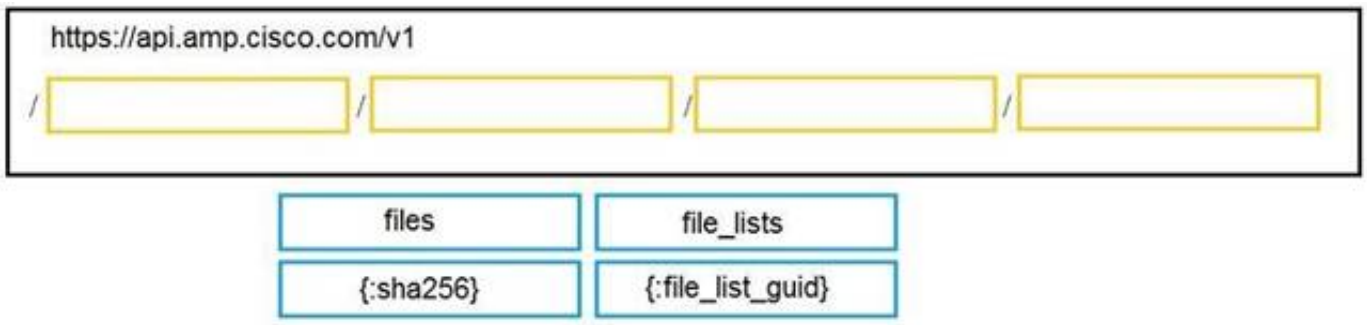
Answer: D

NEW QUESTION 53
Which URI string is used to create a policy that takes precedence over other applicable policies that are configured on Cisco Stealthwatch?

A. /tenants/{tenantId}/policy/system/host-policy
B. /tenants/{tenantId}/policy/system/role-policy
C. /tenants/{tenantId}/policy/system
D. /tenants/{tenantId}/policy/system/{policyId}

Answer: A

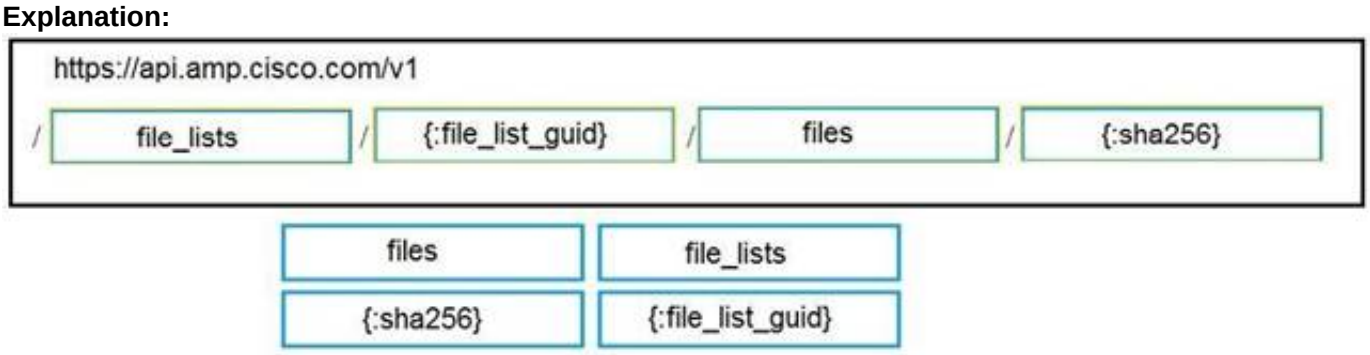
NEW QUESTION 56
DRAG DROP
Drag and drop the code to complete the URL for the Cisco AMP for Endpoints API POST request so that it will add a sha256 to a given file_list using file_list_guid.
Select and Place:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 58
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons 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 FirstTry

* 300-735 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year