Cisco

Exam Questions 300-735

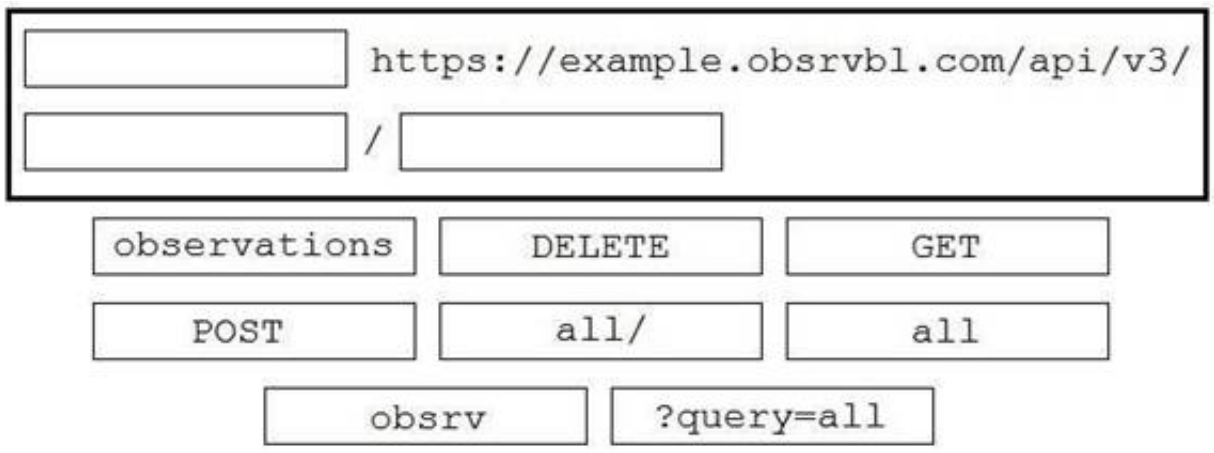
Automating and Programming Cisco Security Solutions (SAUTO)

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

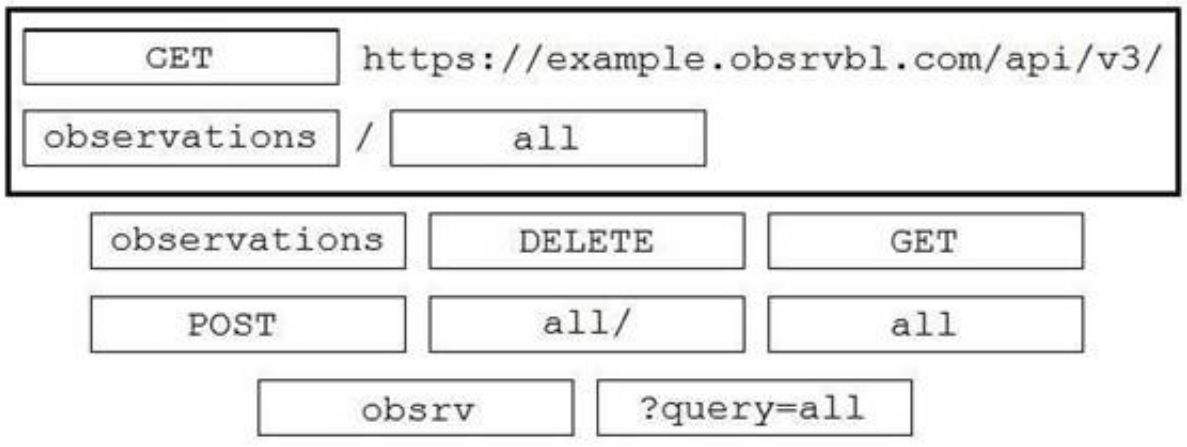
NEW QUESTION 2
DRAG DROP
Drag and drop the code to complete the API call to query all Cisco Stealthwatch Cloud observations. Not all options are used.
Select and Place:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 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
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
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 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:

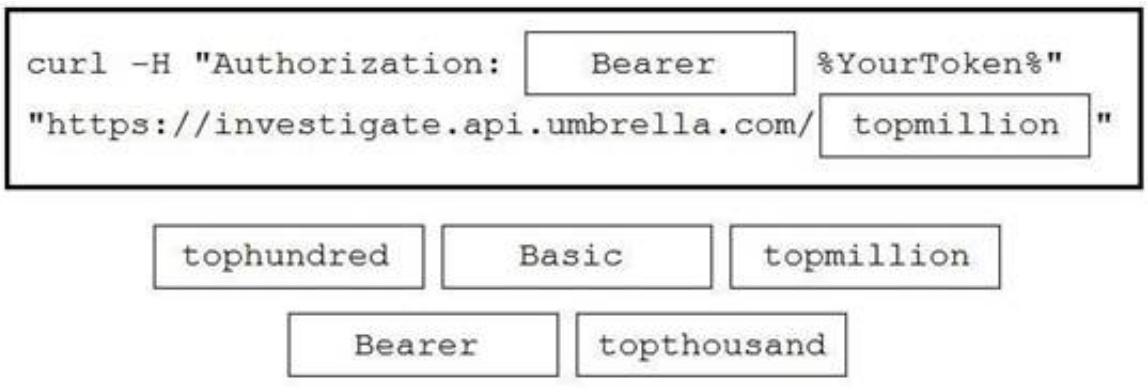
```
curl -H "Authorization: [          ] %YourToken%"
"https://investigate.api.umbrella.com/[          ]"
```

tophundred | Basic | topmillion | Bearer | topthousand

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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.
Which URL returned the data?

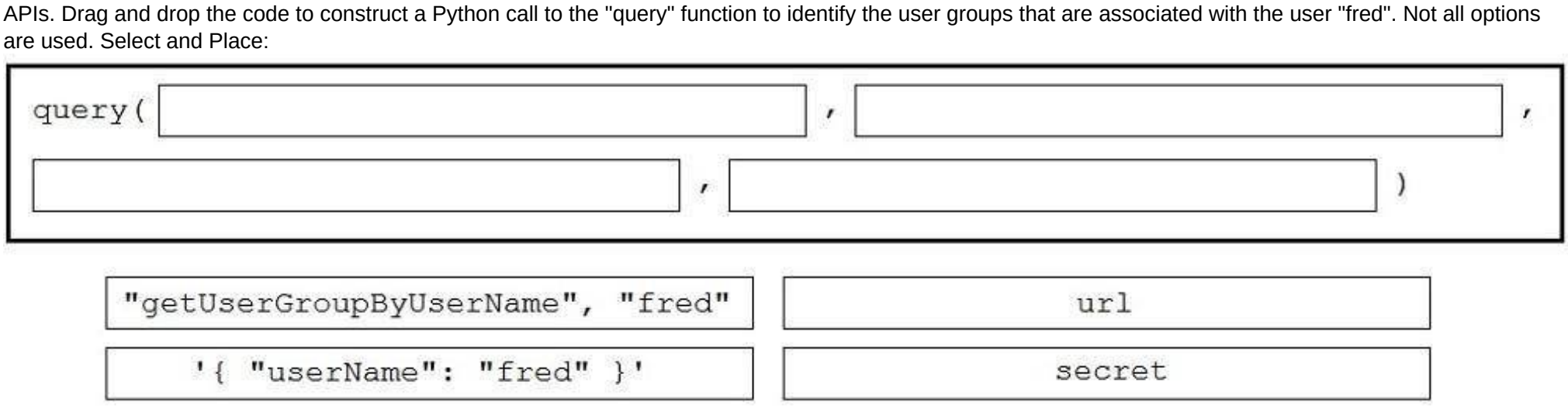
A. https://api.amp.cisco.com/v1/computers
B. https://api.amp.cisco.com/v0/computers
C. https://amp.cisco.com/api/v0/computers
D. https://amp.cisco.com/api/v1/computers

Answer: A

NEW QUESTION 9
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())
```

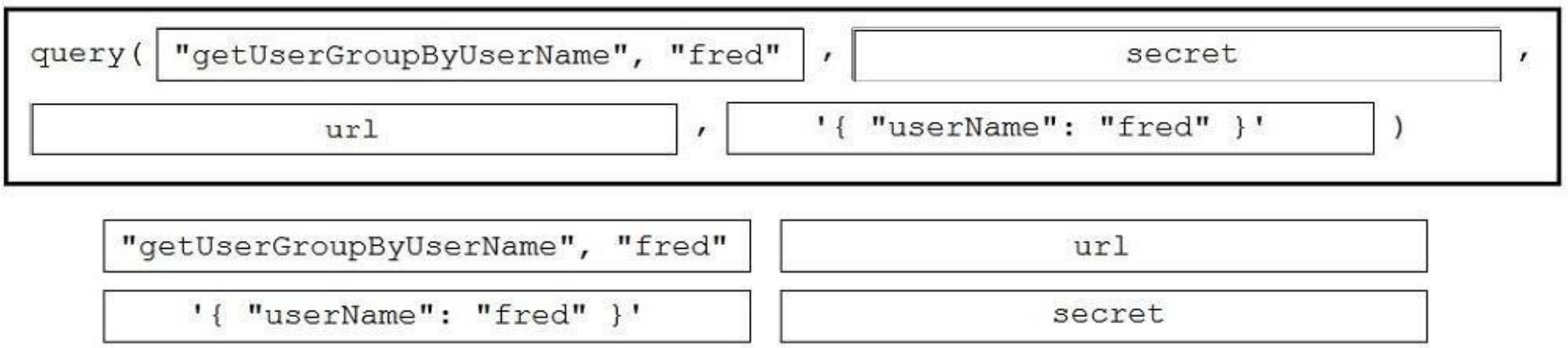
Refer to the exhibit. A Python function named "query" has been developed, and will be used to query the service "com.cisco.ise.session" via Cisco pxGrid 2.0 APIs. Drag and drop the code to construct a Python call to the "query" function to identify the user groups that are associated with the user "fred".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



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 10
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 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 12

```
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 17
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 19
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 22
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 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 25
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 29
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 31
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 32
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 37

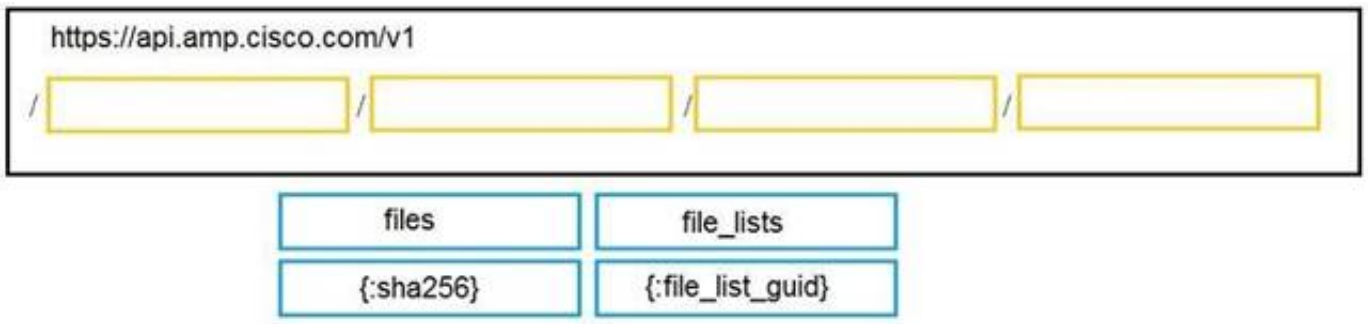
```
Request URL:
https://198.18.133.8/api/fdm/v1/policy/intrusionpolicies
```

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

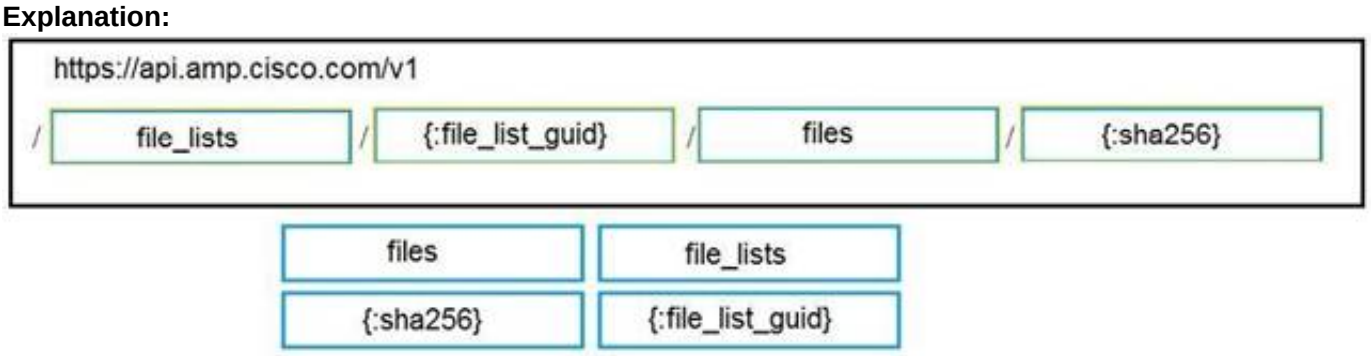
NEW QUESTION 39
DRAG DROP
Drag and drop the code to complete the URL for the Cisco AMP for Endpoints API POST request so that it will add a sha256 to a given file_list using file_list_guid.
Select and Place:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 42
.....

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