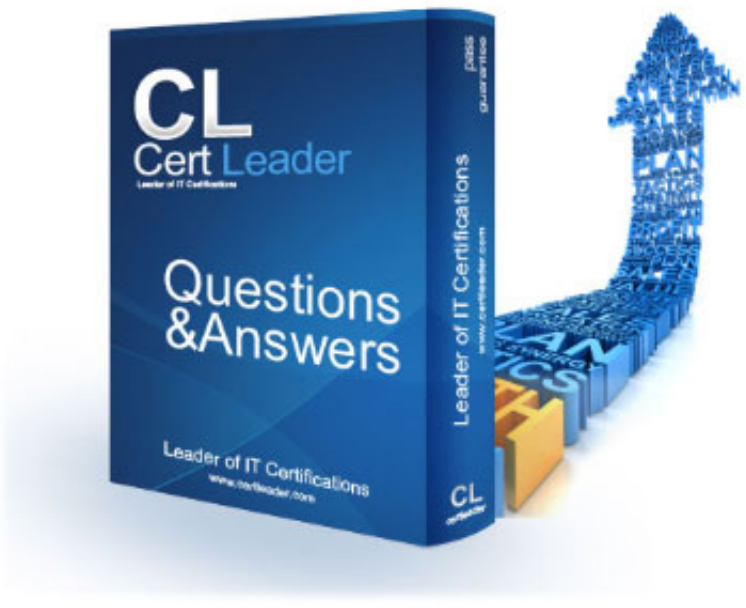
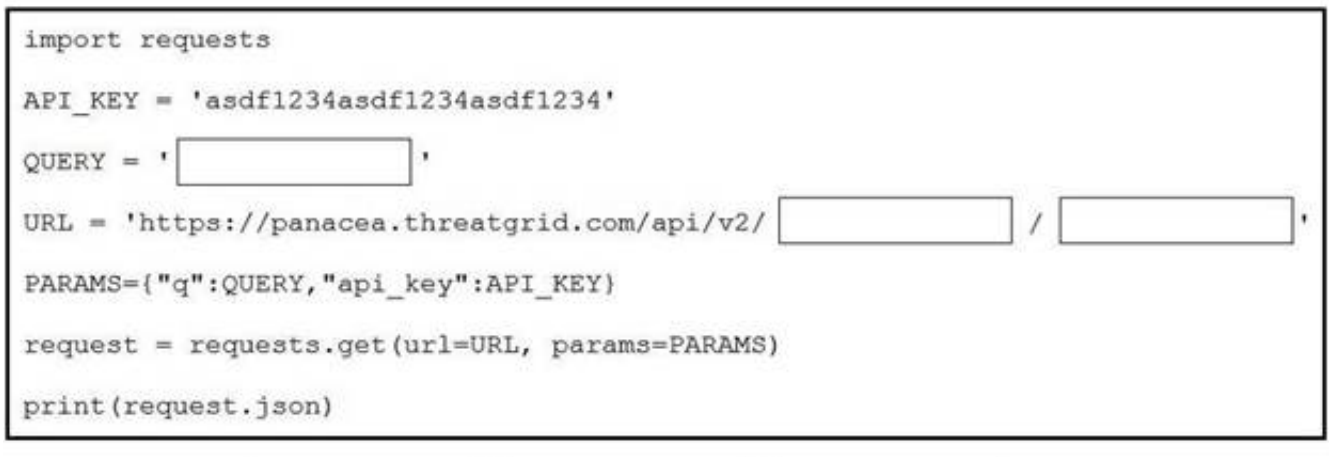
300-735 Dumps

Automating and Programming Cisco Security Solutions (SAUTO)

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



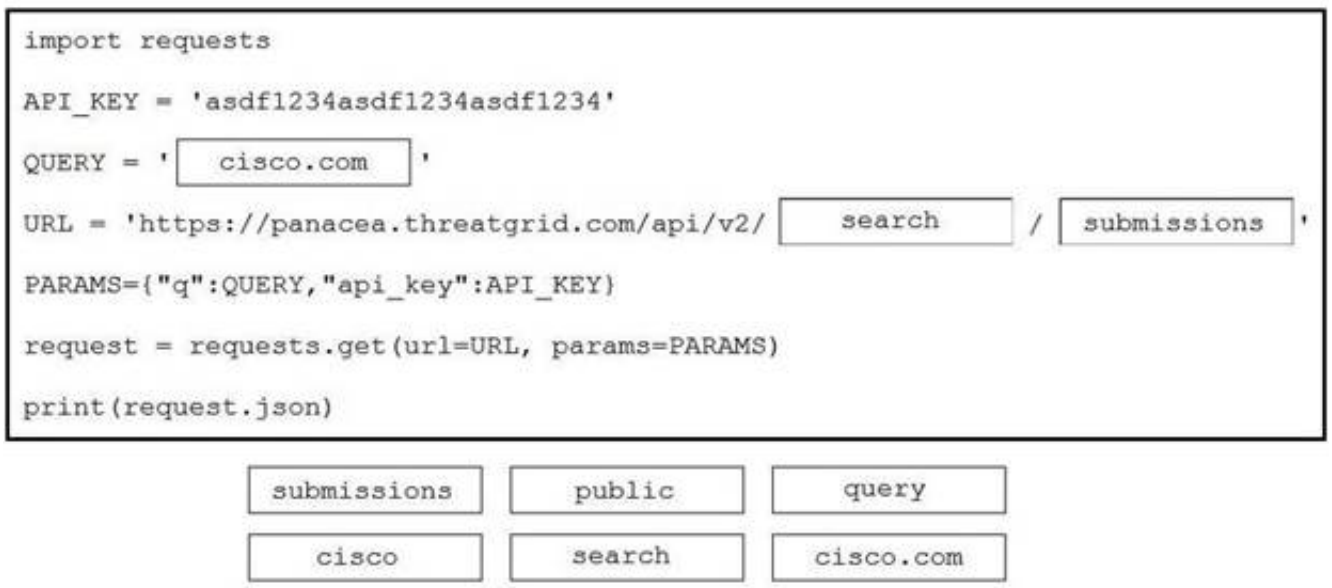
NEW QUESTION 1
DRAG DROP
Drag and drop the code to complete the script to search Cisco ThreatGRID and return all public submission records associated with cisco.com. Not all options are used.
Select and Place:



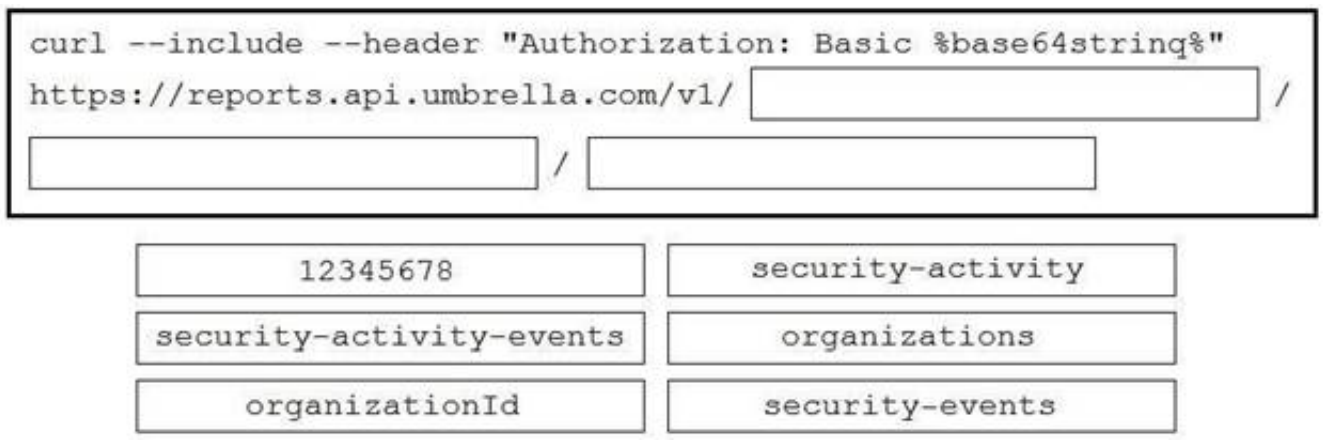
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 2
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:



A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

[12345678] [security-activity]
[security-activity-events] [organizations]
[organizationId] [security-events]

NEW QUESTION 3
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] [topthousand]

NEW QUESTION 4
Which two URI parameters are needed for the Cisco Stealthwatch Top Alarm Host v1 API? (Choose two.)
A. startAbsolute
B. externalGeos
C. tenantId
D. intervalLength
E. tagID

Answer: CE

NEW QUESTION 5

```
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")

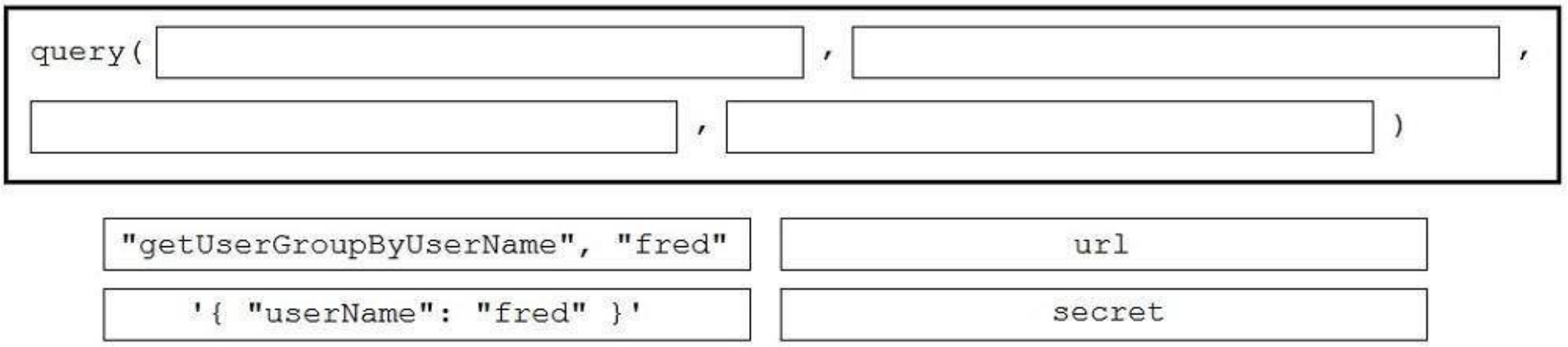
B. query(config, "10.0.0.50", url, payload)
C. query(config, secret, url, "10.0.0.50")
D. query(config, secret, url, '{"ipAddress": "10.0.0.50"}')

Answer: D

NEW QUESTION 6
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())
```

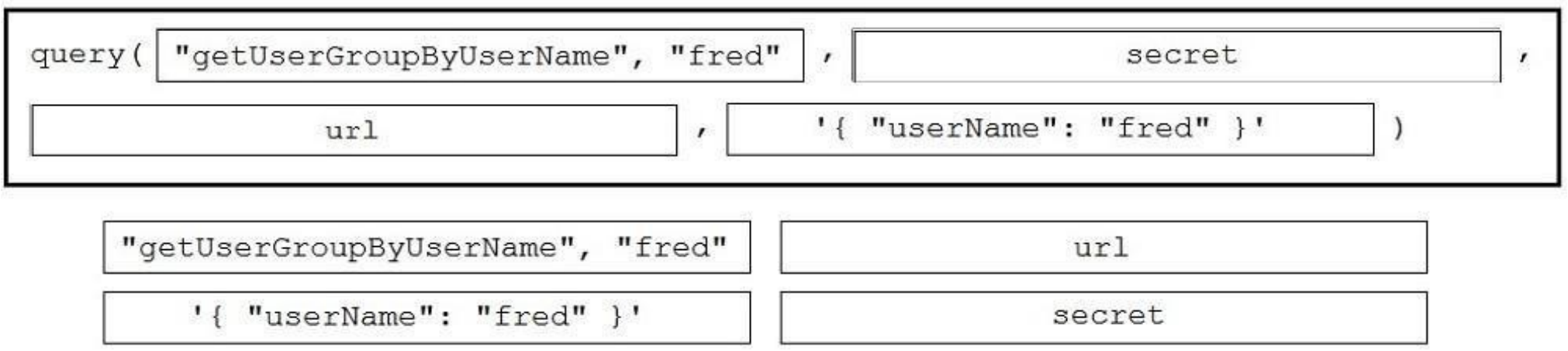
Refer to the exhibit. A Python function named "query" has been developed, and will be used to query the service "com.cisco.ise.session" via Cisco pxGrid 2.0 APIs. Drag and drop the code to construct a Python call to the "query" function to identify the user groups that are associated with the user "fred".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



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 7
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 8
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 9

```
import requests

API_KEY = "123456789abcdef"

URL = "https://example.obsrvbl.com/api/v3/alerts/alert/"

HEADERS = {"Authorization": "Bearer {}".format(API_KEY)}

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

Refer to the exhibit. A security engineer created a script and successfully executed it to retrieve all currently open alerts. Which print command shows the first returned alert?

A. print(response[data][0])
B. print(response[results][0])
C. print(response.json()[data][0])
D. print(response.json()[results][0])

Answer: A

NEW QUESTION 10

```
import json
import requests

BASE_URL = "https://investigate.api.umbrella.com"
HEADERS = {"Authorization": "Bearer %YourToken%"}

---MISSING CODE---

request= requests.get(URL, parmas= PARAMS,
verify=False)
```

Refer to the exhibit. A network operator must create a Python script that makes an API request to Cisco Umbrella to do a pattern search and return all matched URLs with category information.
Which code completes the script?

A. URL = BASE_URL + "/find/exa\[a-z\]ple.com" PARAMS = { "categoryinclude" : "true"}
B. URL = BASE_URL + "/find/exa\[a-z\]ple.com" PARAMS = { "returncategory" : "true"}
C. URL = BASE_URL + "/find/exa\[a-z\]ple.com" PARAMS = { "includeCategory" : "true"}
D. URL = BASE_URL + "/find/exa\[a-z\]ple.com" PARAMS = { "returnCategory" : "true"}

Answer: D

NEW QUESTION 10
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 11
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

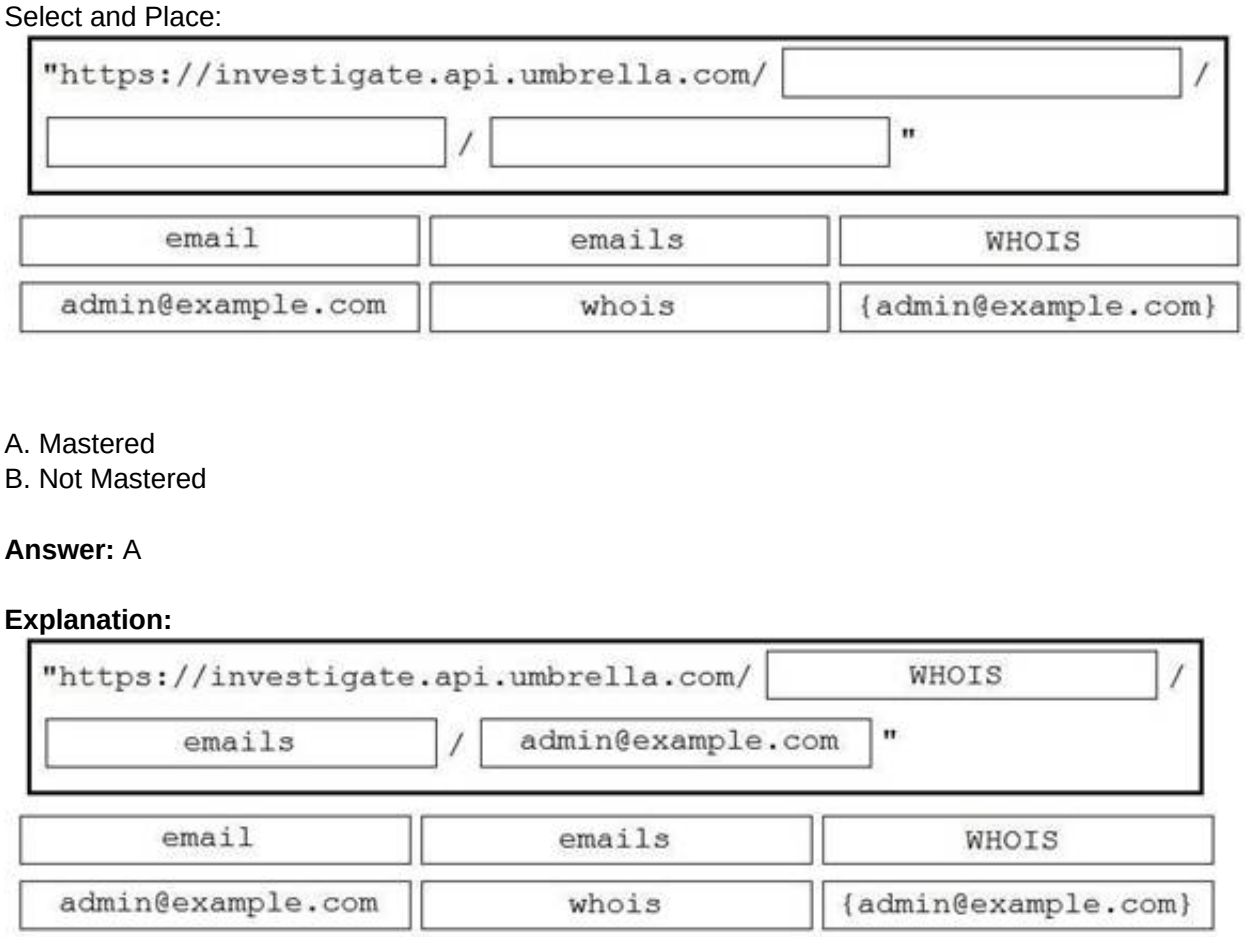
Answer: D

NEW QUESTION 15
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 18
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:



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 19
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 23
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 28
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 33

```
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

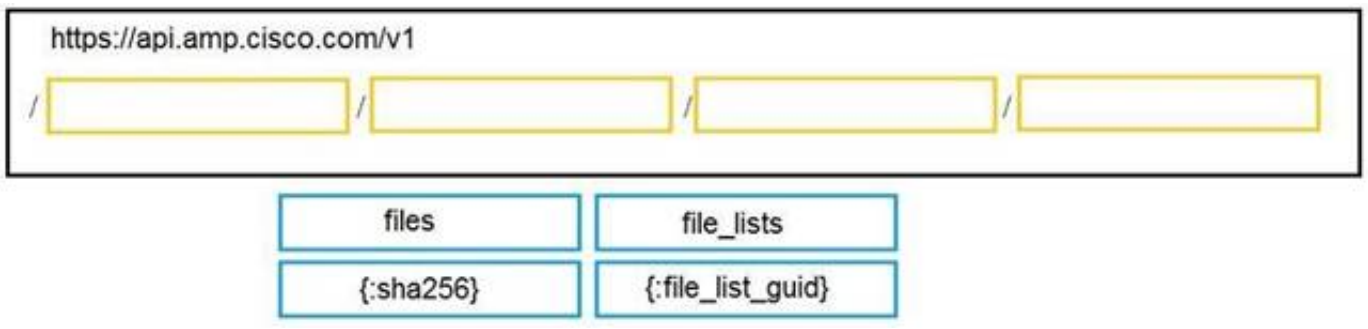
Answer: D

NEW QUESTION 37
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

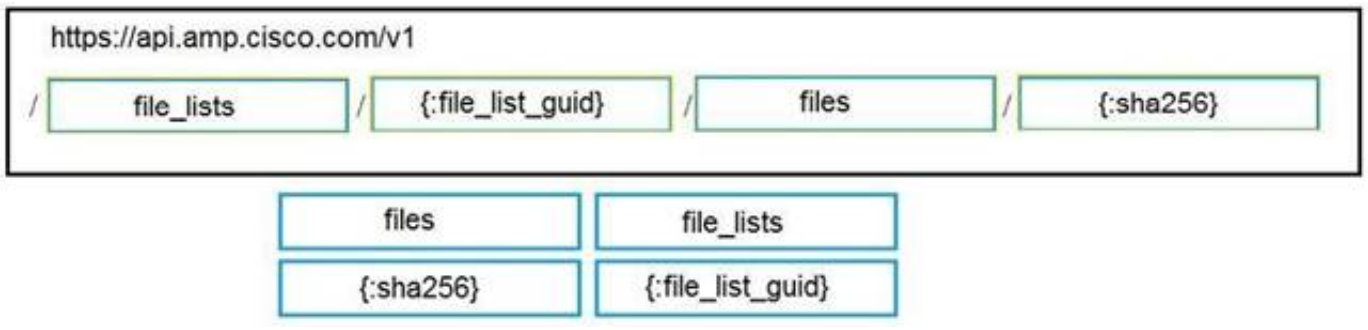
NEW QUESTION 38
DRAG DROP
Drag and drop the code to complete the URL for the Cisco AMP for Endpoints API POST request so that it will add a sha256 to a given file_list using file_list_guid.
Select and Place:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 39

.....

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