Exam Questions 300-735

Automating and Programming Cisco Security Solutions (SAUTO)

https://www.2passeasy.com/dumps/300-735/

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
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 4
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 5
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 6
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 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

```
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 9
Which API capability is available on Cisco Firepower devices?

A. Firepower Management Center - Sockets API
B. Firepower Management Center - eStreamer API
C. Firepower Management Center - Camera API
D. Firepower Management Center - Host Output API

Answer: B

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 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 13

```
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
Refer to the exhibit. The script outputs too many results when it is queried against the Cisco Umbrella Reporting API. Which two configurations restrict the returned result to only 10 entries? (Choose two.)

A. Add params parameter in the get and assign in the {"return": "10"} value.
B. Add ?limit=10 to the end of the URL string.
C. Add params parameter in the get and assign in the {"limit": "10"} value.
D. Add ?find=10 to the end of the URL string.
E. Add ?return=10 to the end of the URL string.

Answer: BC

NEW QUESTION 21
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 26
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 29
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

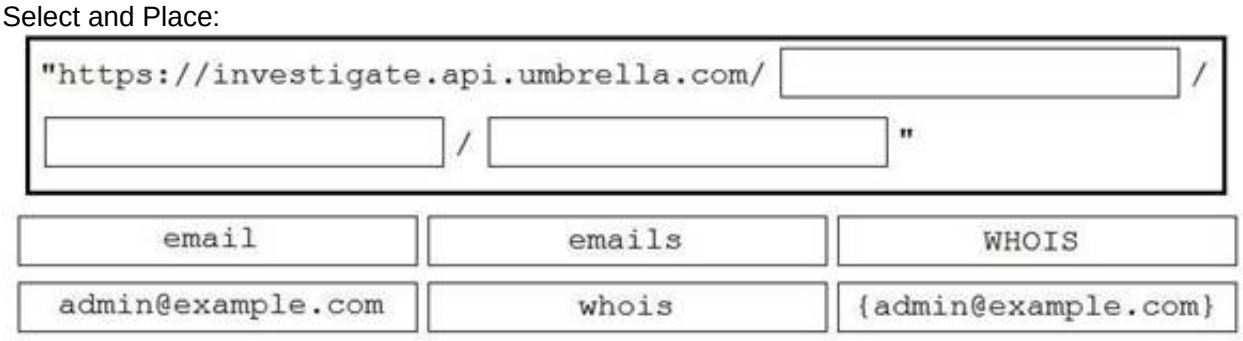
Answer: D

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

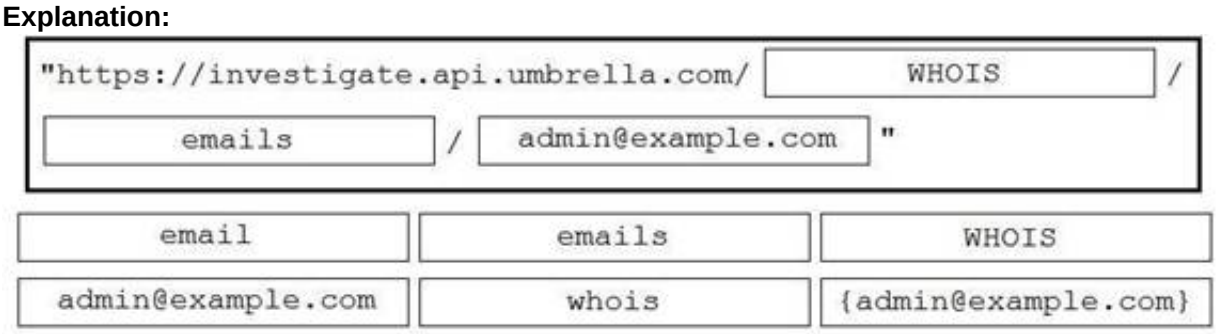
NEW QUESTION 37
DRAG DROP
Drag and drop the code to complete the Cisco Umbrella Investigate WHOIS query that returns a list of domains that are associated with the email address "admin@example.com". Not all options are used.
Select and Place:



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 39
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 41
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 46
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 47
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 52
Which step is required by Cisco pxGrid providers to expose functionality to consumer applications that are written in Python? A. Look up the existing service using the /pxgrid/control/ServiceLookup endpoint.

A. Register the service using the /pxgrid/control/ServiceRegister endpoint.
B. Configure the service using the /pxgrid/ise/config/profiler endpoint.
C. Expose the service using the /pxgrid/ise/pubsub endpoint.

Answer: D

NEW QUESTION 53
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-735 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-735 Product From:

https://www.2passeasy.com/dumps/300-735/

Money Back Guarantee

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