

Cisco

Exam Questions 300-735

Automating and Programming Cisco Security Solutions (SAUTO)



NEW QUESTION 1

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 2

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 3

When the URI "/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/policy/accesspolicies" is used to make a POST request, what does "e276abec-e0f2-11e3-8169- 6d9ed49b625f" represent?

- A. API token
- B. domain UUID
- C. access policy UUID

D. object UUID

Answer: B

NEW QUESTION 4

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 5

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 6

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 7

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 8

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 9

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 10

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 10

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

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:

<code>"https://investigate.api.umbrella.com/ [] /</code>		
<code>[]</code>	<code>/ []</code>	<code>"</code>
<code>email</code>	<code>emails</code>	<code>WHOIS</code>
<code>admin@example.com</code>	<code>whois</code>	<code>{admin@example.com}</code>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<code>"https://investigate.api.umbrella.com/ [WHOIS] /</code>		
<code>[emails]</code>	<code>/ [admin@example.com]</code>	<code>"</code>
<code>email</code>	<code>emails</code>	<code>WHOIS</code>
<code>admin@example.com</code>	<code>whois</code>	<code>{admin@example.com}</code>

NEW QUESTION 16

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 19

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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 First Try
- * 300-735 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 300-735 Practice Test Here](#)