Vendor: Cisco

Exam Code:300-735

Exam Name: Automating and Programming Cisco Security Solutions (SAUTO)

Version: Demo

QUESTION 1

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

Correct Answer: D

QUESTION 2

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

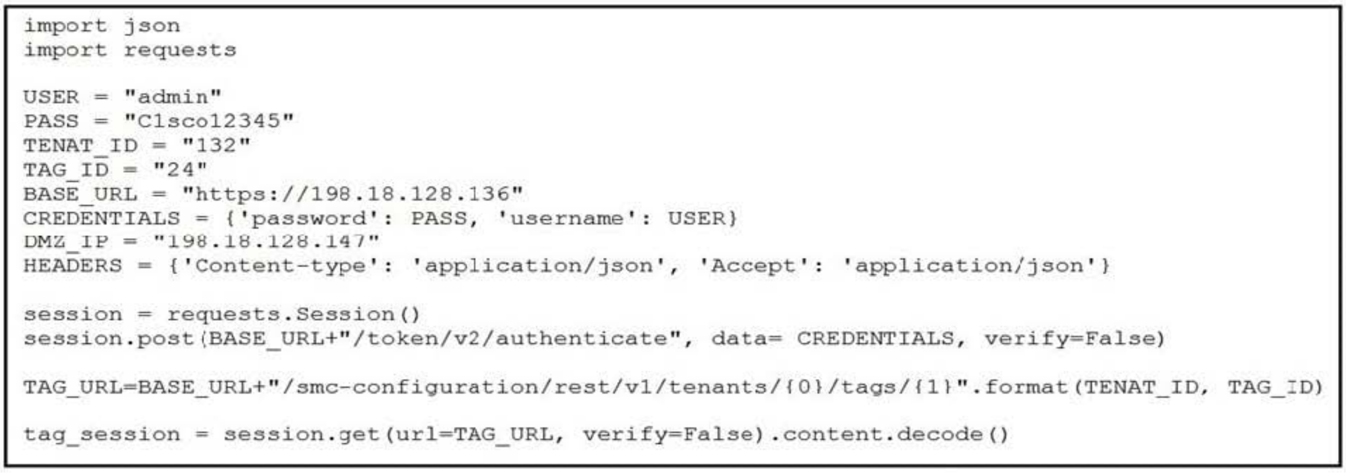
C. access policy UUID

D. object UUID

Correct Answer: B

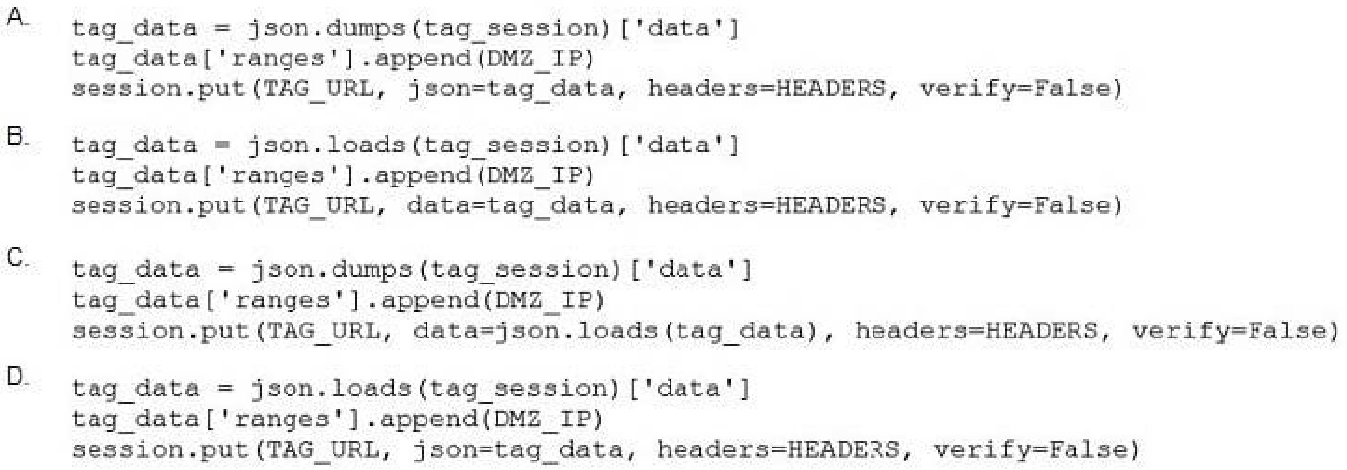
QUESTION 3

Refer to the exhibit.



```
import json
import requests

USER = "admin"
PASS = "C1sco12345"
TENAT_ID = "132"
TAG_ID = "24"
BASE_URL = "https://198.18.128.136"
CREDENTIALS = {'password': PASS, 'username': USER}
DMZ_IP = "198.18.128.147"
HEADERS = {'Content-type': 'application/json', 'Accept': 'application/json'}

session = requests.Session()
session.post(BASE_URL+"/token/v2/authenticate", data= CREDENTIALS, verify=False)

TAG_URL=BASE_URL+"/smc-configuration/rest/v1/tenants/{0}/tags/{1}".format(TENAT_ID, TAG_ID)

tag_session = session.get(url=TAG_URL, verify=False).content.decode()
```

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)
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 4

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.

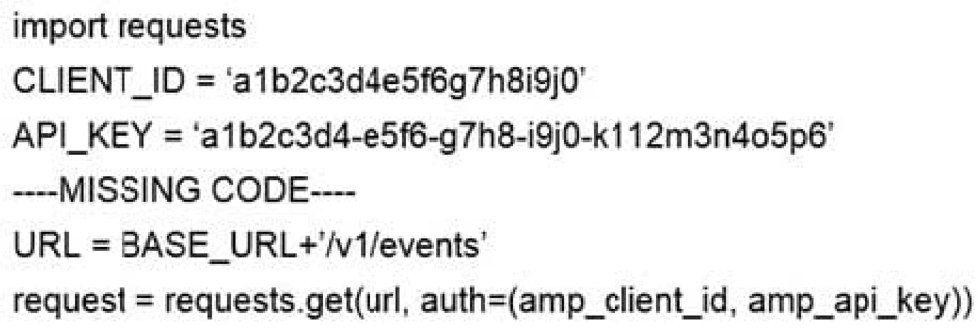
D. Anomalous network traffic can be detected and correlated.

E. The time that is needed to deploy a change is reduced, compared to manually applying the change.

Correct Answer: CE

QUESTION 5

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/"

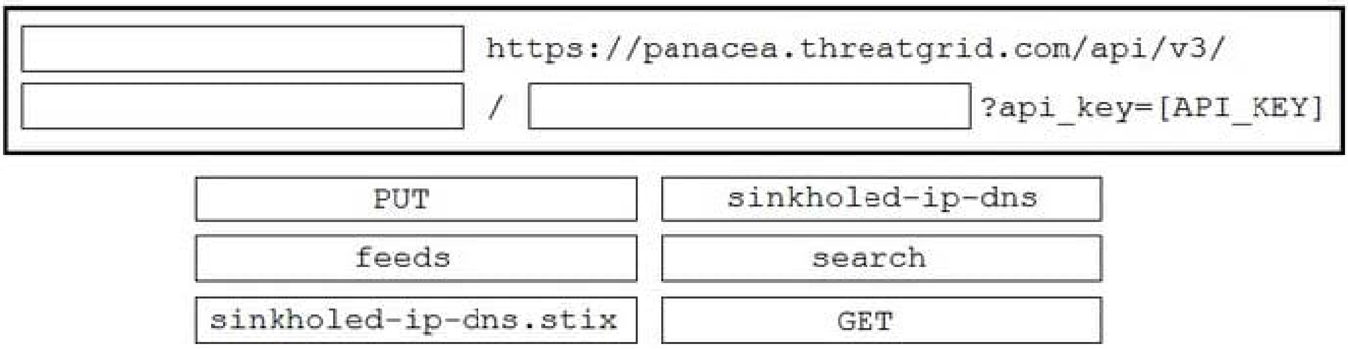
Correct Answer: A

QUESTION 6

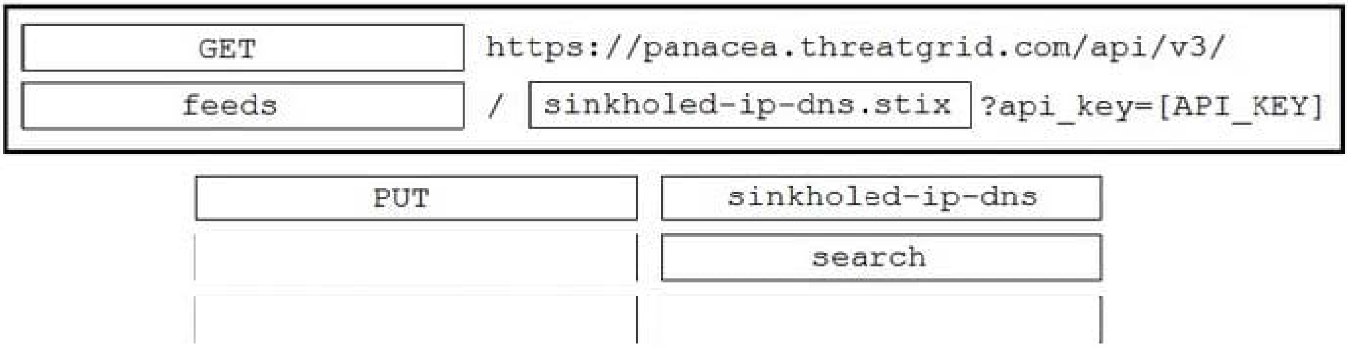
DRAG DROP

Drag and drop the items to complete the ThreatGRID API call to return a curated feed of sinkholed-ip-dns in stix format. Not all options are used.

Select and Place:



Correct Answer:



GET https://panacea.threatgrid.com/api/v3/

feeds / sinkholed-ip-dns.stix ?api_key=[API_KEY]

PUT

sinkholed-ip-dns

search

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/DEVNET-2164.pdf

---

QUESTION 7

A developer has just completed the configuration of an API that connects sensitive internal systems. Based on company policies, the security of the data is a high priority.

Which approach must be taken to secure API keys and passwords?

A. Embed them directly in the code.

B. Store them in a hidden file.

C. Store them inside the source tree of the application.

D. Change them periodically.

Correct Answer: D

QUESTION 8

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

Correct Answer: CE

QUESTION 9

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.

Correct Answer: C

QUESTION 10

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

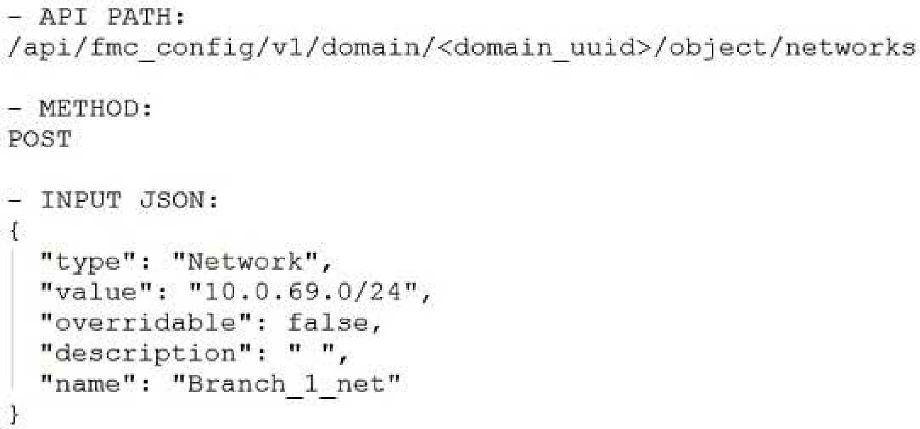
D. https://s-platform.api.opendns.com/1.0/domains?example.com

Correct Answer: B

QUESTION 11

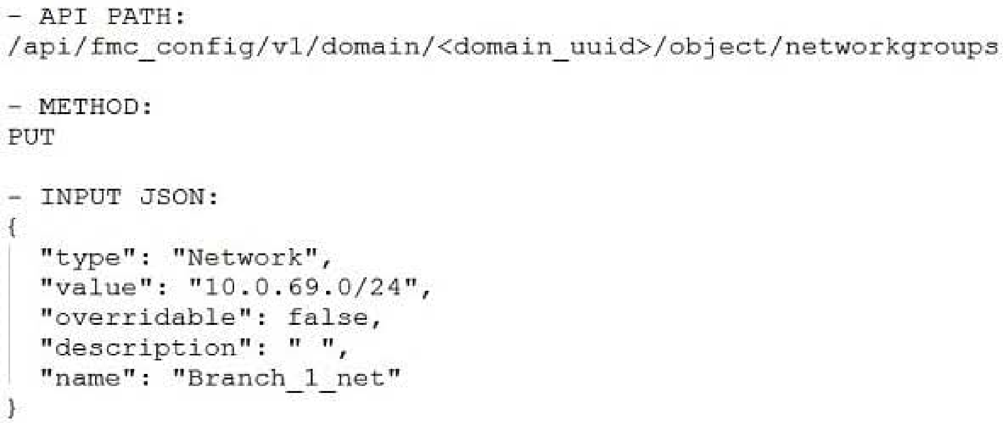
Which snippet is used to create an object for network 10.0.69.0/24 using Cisco Firepower Management Center REST APIs?

A.



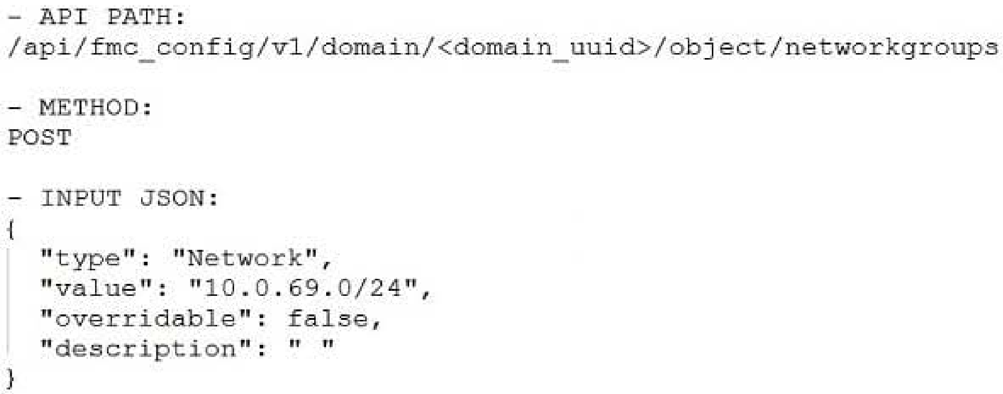
```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/networks

- METHOD:
POST

- INPUT JSON:
{
  "type": "Network",
  "value": "10.0.69.0/24",
  "overridable": false,
  "description": " ",
  "name": "Branch_1_net"
}
```

B.



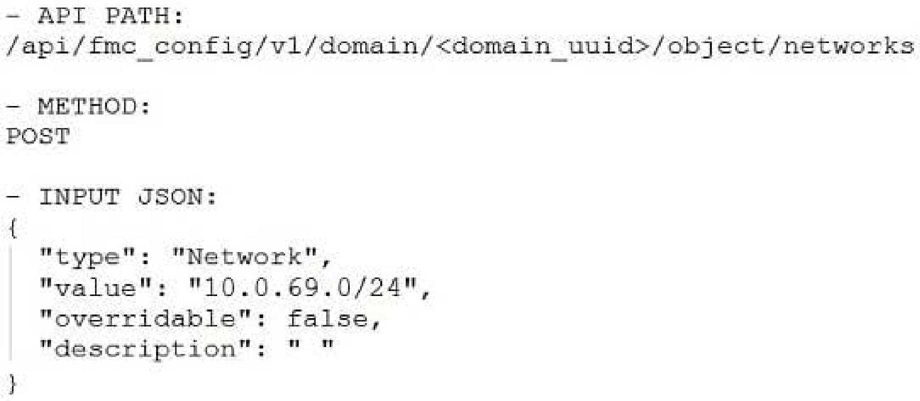
```
- API PATH:
/api/fmc_config/v1/domain/<domain_uuid>/object/networkgroups

- 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": " "
}
```

A. Option A

B. Option B

C. Option C

D. Option D

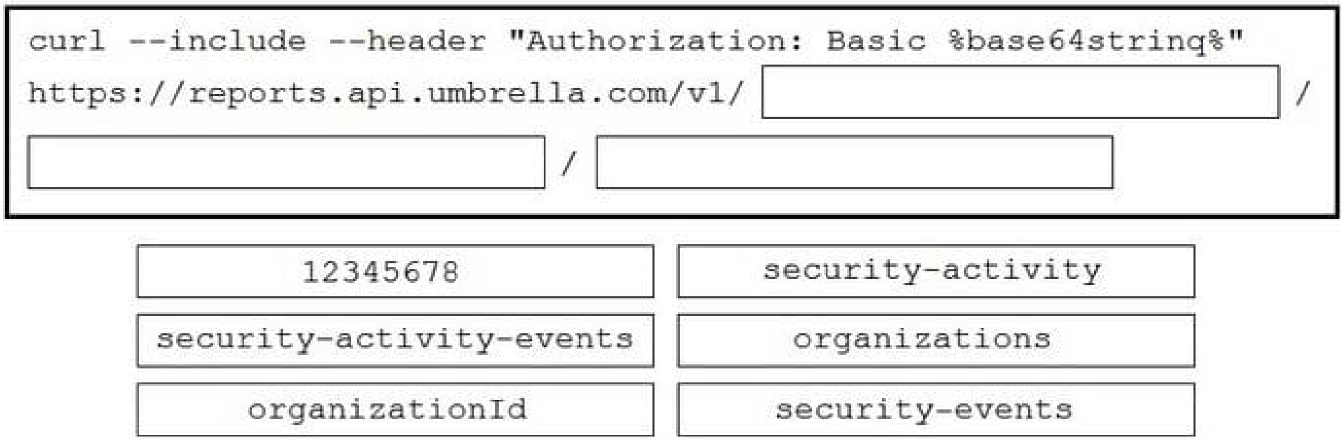
Correct Answer: A

QUESTION 12

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 %base64strinq%"
https://reports.api.umbrella.com/v1/ [          ] /
[          ] / [          ]
```

12345678

security-activity

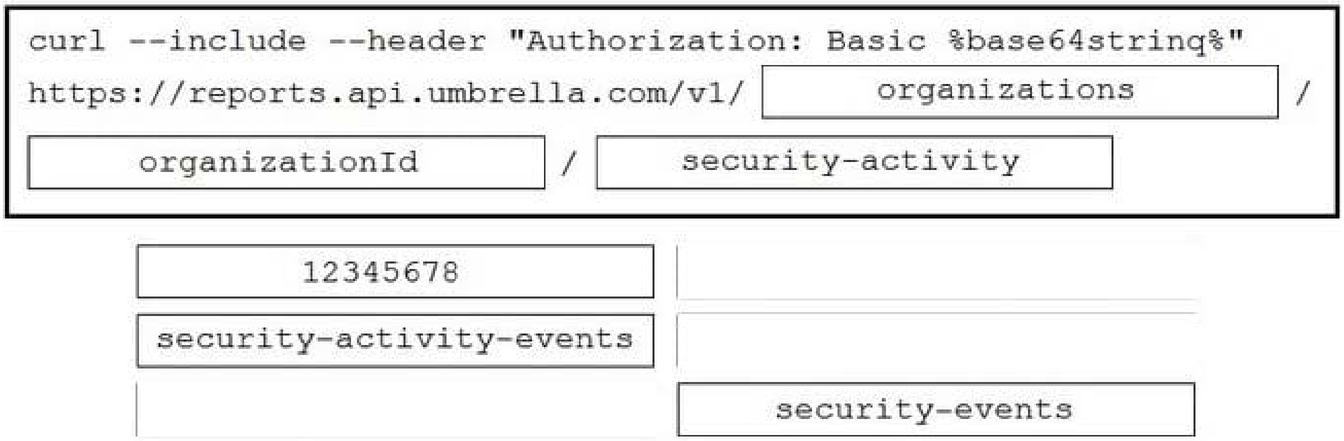
security-activity-events

organizations

organizationId

security-events

Correct Answer:



```
curl --include --header "Authorization: Basic %base64strinq%"
https://reports.api.umbrella.com/v1/ organizations /
organizationId / security-activity
```

12345678

security-activity-events

security-events

Reference: https://docs.umbrella.com/umbrella-api/docs/security-activity-report