Flashpoint Phantom Integration API Analysis Document

Crest Data Systems
First Floor, Bhaskar House, SG Road, Makaraba, Ahmedabad 380015
E: info@crestdatasys.com, P: +91 (79) 4004-4200, +1 (408) 909-9161

Revision History

Document Version	Date	Owner	Description
1.0	14-Feb-2020	Crest Data Systems	API Analysis Draft
1.1	28-Feb-2020	Crest Data Systems	• Added two new asset configuration parameters “Retry Wait Period(in seconds)” and “Number Of Retries” • Made query parameter mandatory in the “Run Query” action and updated the diagram of the action’s workflow
1.2	17-Mar-2020	Crest Data Systems	• Updated the scroll session timeout for ‘Run Query’ and ‘Get Compromised Credentials’ actions

Authentication

We will use token-based authentication. Here, the user will generate a new authentication token from the Flashpoint account and will provide the token in the asset configuration parameter. This token is used in the actions for authentication of request.

Base URL https://fp.tools/api/v4

Method - GET | POST
Request URL - <base_url>/<endpoint>
Request Headers -

- Authorization: Bearer <api_token>
- Content-Type: application/json
- X-FP-IntegrationPlatform: Phantom
- X-FP-IntegrationPlatformVersion: BaseConnector().get_product_version()
- X-FP-IntegrationVersion: BaseConnector().get_app_json().get('app_version')

Reference Link

- https://docs.fp.tools/

Configuration parameters

Parameter	Data type	Required	Default
API Token	Password	Yes	None
Base URL	String	Yes	https://fp.tools/api/v4

Retry wait period (in seconds)	Numeric	No	5
Number Of Retries	Numeric	No	1

Actions

For the actions, we are using Flashpoint API v4 endpoints.

1. Test connectivity

Test the connectivity of the Phantom server to the Flashpoint instance by making an initial API call to the indicators API

Endpoint

GET /indicators/simple?limit=1

2. List Indicators

Retrieve a simplified list of indicators of compromise, those occur in the context of an event. Either Indicator Type or Query is mandatory to be provided.

Endpoint

GET /indicators/simple

Endpoints for pagination

GET /indicators/simple?scroll=true
POST /indicators/scroll
DELETE /indicators/scroll

Parameters

Parameter	Data type	Required	Default
Attribute Types	String	No	None
Query	String	No	None
Limit	Numeric	No	500

Sample Requests

- https://fp.tools/api/v4/indicators/simple?types=<indicator_type(e.g md5,filename,ip-src)>
- https://fp.tools/api/v4/indicators/simple?query=<query(e.g. “text”)>

3. Search Indicators

Get indicators matching the specific search field value

Endpoint

GET /indicators/simple?search_fields=<search_field>==”<field_value>”

Endpoints for pagination

GET /indicators/simple?scroll=true
POST /indicators/scroll
DELETE /indicators/scroll

Parameters

Parameter	Data type	Required	Default
Attribute type	String	Yes	None
Attribute value	String	Yes	None
Limit	Numeric	No	500

Sample Requests

1. https://fp.tools/api/v4/indicators/simple?search_fields=md5==”<hash_value>

4. List Reports

Search Flashpoint Intelligence Reports

Endpoint

GET /reports

Parameters

Parameter	Data type	Required	Default
Limit	Numeric	No	500

5. Get Report

Retrieve a specific Intelligence Report

Endpoint

GET /reports/{report_id}

Parameters

Parameter	Data type	Required	Default
Report ID	String	Yes	None

6. Get Related Reports

Retrieve a list of related reports

Endpoint

GET /reports/{report_id}/related

Parameters

Parameter	Data type	Required	Default
Report ID	String	Yes	None
Limit	Numeric	No	500

7. Get Compromised Credentials

Get all compromised credentials

Endpoint

GET
/all/search?query=+basetypes:credential-sighting{filter}

Endpoints for pagination

GET /all/search?scroll=60m
POST /all/scroll?scroll=60m
DELETE /all/scroll

Here, the scroll session timeout for the paginator is 60 minutes(set to the maximum supported by the API endpoint).

Parameters

Parameter	Data type	Required	Default
Filter	String	No	None
Limit	Numeric	No	500

Sample Filter Values

1. +is_fresh:true
   (search for only new credential sightings)
2. +breach.first_observed_at.date-time:[now-30d TO now]

(search for credential sightings which are discovered in the last month)

3. +breach.fpid:nIbeDs_VXyKedBmuhFEaGQ
   (search for all credential sightings in a Breach)
4. +email:username
   (search for a username)
5. +email.keyword:username@domain.com
   (search for an email address)
6. +domain.keyword:domain.com
   (search for a domain)

8. Run Query

Get the results of Universal Search based on the provided query

Endpoint

GET /all/search?query=<query>

Endpoints for pagination

GET /all/search?scroll=60m
POST /all/scroll?scroll=60m
DELETE /all/scroll

Here, the scroll session timeout for the paginator is 60 minutes(set to the maximum supported by the API endpoint).

Parameters

Parameter	Data type	Required	Default
Query	String	Yes	None
Limit	Numeric	No	500

Sample Requests

1. https://fp.tools/api/v4/all/search?query=”free text”
2. https://fp.tools/api/v4/all/search?query=analyst+workbook

NOTES & QUERIES

- How many and which base types (e.g. indicator, chat, telegram, credential-sighting) to be included for their API response data-paths to be added in the Flashpoint app JSON?
    - indicator_attribute
    - chat
    - credential-sighting
    - card
    - paste
    - vulnerability
    - conversation
    - chan
    - generic-product
    - blog
    - reddit
    - forum
    - cve
    - breach