Flashpoint Phantom Integration Technical Design 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

Table of Contents

Revision History

Document Version	Date	Owner	Description
1.0	14-Feb-2020	Crest Data Systems	Initial Draft
1.1	28-Feb-2020	Crest Data Systems	● Added the components of the custom output view for actions ● 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 ● Added the output data-paths for multiple base types in the action “Run Query” ● Added the “General Notes” section
1.2	17-Mar-2020	Crest Data Systems	● Added more examples in functional use cases for “Run Query” and “Get Compromised Credentials” actions
1.3	20-Mar-2020	Crest Data Systems	● Added Known Issues in the General Notes section

1. Flashpoint Platform

Flashpoint Intelligence Platform grants access to the archive of finished intelligence reports, data from illicit forums, marketplaces, chat services, blogs, paste sites, technical data, card shops, login credentials, and vulnerabilities, in a single, finished intelligence experience. Flashpoint provides scalable results by broadening the scope of intelligence beyond traditional threat detection, and gain scalable, contextual, rich results that help teams make better decisions and protect their ability to operate across the enterprise.

2. Flashpoint Phantom Integration

This integration implements the investigative actions for the Flashpoint on the Phantom Platform. It will allow the end-users to implement any use cases on Flashpoint Platform that are possible using a combination of the below-mentioned actions.

1. **Test Connectivity -** This action tests the connectivity of the Phantom server to the Flashpoint instance by making an initial API call to the Indicators API.
2. **List Indicators -** Fetch a list of Indicator of Compromises (IoCs) that occur in the context of an event from the Flashpoint Platform. The user can filter the IoCs (while fetching) based on the query or the attribute types. The user can also limit the output results by providing a limit value in the action parameters.
3. **Search Indicators -** Fetch an IoC value of a specific attribute type from the list of available IoCs on the Flashpoint Platform. The user can also limit the output results by providing a limit value in the action parameters.
4. **List Reports -** Fetch a list of all the intelligence reports from the Flashpoint Platform. The user can also limit the output results by providing a limit value in the action parameters.
5. **Get Report -** Fetch a specific intelligence report from the Flashpoint Platform for the provided report ID.

6. **Get Related Reports -** Fetch a list of all the related intelligence reports from the Flashpoint Platform for the provided report ID. The user can also limit the output results by providing a limit value in the action parameters.
7. **Get Compromised Credentials -** Fetch a list of all the Credential Sightings from the Flashpoint Platform. The user can narrow down the fetched data by providing a filter value. The user can also limit the output results by providing a limit value in the action parameters.
8. **Run Query -** Fetch the data by performing an all search from the Flashpoint Platform. The user can limit the searches by providing the criteria in the query parameter. The user can also limit the output results by providing a limit value in the action parameters.

3. Flashpoint API Analysis

Flashpoint API grants access to the intelligence reports, technical data, and uniquely sourced conversations from illicit threat actor communities, enabling users to enrich and enhance internal data with our targeted data acquired from highly curated sources.

After analysis of the provided requirements for the Flashpoint Phantom integration, these requirements are translated into a set of actions for the Phantom app. For each action, the Flashpoint APIs are analyzed and a set of API calls to the Flashpoint Platform is prepared. The inputs to the API calls are translated to the action parameters and the outcome of the API calls is translated to the app output and output data paths.

Flashpoint APIs used in the Phantom integration.

- Indicators API
- Reports API
- Search API
- Scrolling Session API

The API analysis document for the Flashpoint Phantom Integration is mentioned below.

API Analysis Document Link

- https://docs.google.com/document/d/1ftN1UqAPtp6oMx8-kArS_lw_2PEr8RN17BS5Sg9DMTo/edit

4. Business Goals

Phantom is a Security Orchestration, Automation, and Response (SOAR) Platform and it combines security infrastructure orchestration, playbook automation, and case management capabilities to integrate the team, processes, and tools. The majority of the companies use the SOAR tools for the below-mentioned objectives.

- To automate repetitive tasks to increase effective team efforts and provide attention to mission-critical decisions.
- To perform automated investigations and reduce the turnaround time to such critical decision-making situations using extensive playbooks designed on the Phantom Platform.
- To integrate the existing security infrastructure to ensure the active participation of each part in the security defense workflow.

The goal of building the Flashpoint Phantom Integration is to allow the SOC team to leverage the Flashpoint intelligence capabilities and allow it to be automated via the Phantom Platform. This will help the customers to get the below-mentioned capabilities.

1. **Indicator Lookups**

   Provide the functionality for indicator lookup to see if something in the end user’s environment matches an indicator in the Flashpoint Platform to further determine whether it is malicious or not.

2. **Report Lookups**

   Provide the functionality for reports lookup to fetch and see all or a specific report based on the report ID from the Flashpoint Platform. The integration will also facilitate the customer to fetch the daily latest reports from the Flashpoint Platform to use them further discuss in their meetings.

3. **All Search**
   Provide the functionality for a universal search across all the available datasets on the Flashpoint Platform.

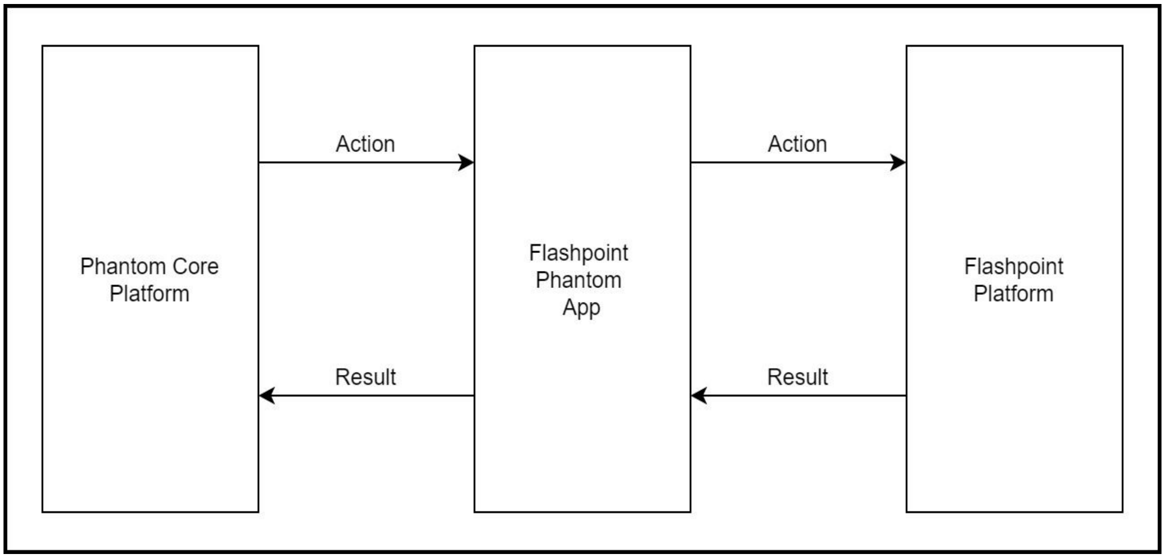
5. Compatibility Matrix

For deployment and usage of the integration, below compatibility matrix is required.

- Flashpoint Platform Version - 4.5.19
- Flashpoint API Version - 4 (/api/v4)
- Minimum Phantom Platform Version - 4.6.19142
- OS Platforms - Linux (for Phantom Platform deployment)

6. Flashpoint Phantom App Architecture

Flashpoint Phantom integration is designed in Python to create a bridge between the Phantom Platform and the Flashpoint Platform. It can be considered as having two strict edges. On the left edge, an app is given an action to be carried out on behalf of the Phantom Platform and the right edge, an app converts this 'action' into commands specific to the device/service or tool that it is talking to. The result of these actions is then read by the app and passed on to the Phantom Platform. This design approach helps facilitate automated actions that are carried out by the Phantom Platform on behalf of the user.



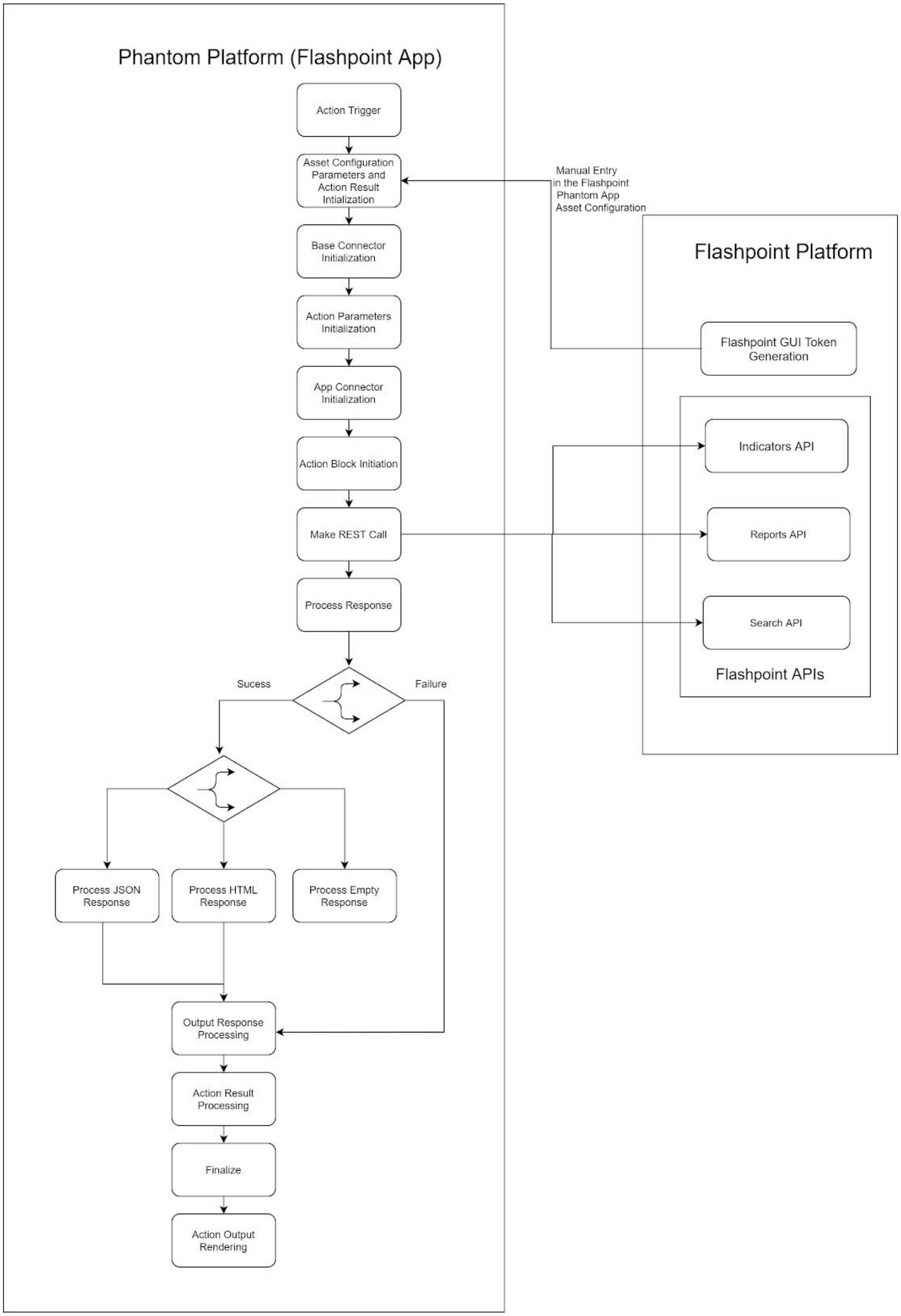
6.1. Flashpoint Phantom App Components

The Flashpoint Phantom app consists of several components. The high-level functional description of these components is mentioned below.

__init__.py	Required to initialize and define a Python package. An empty file should suffice.
flashpoint.json	JSON meta-data that describes the app and functionality that the app provides
flashpoint_connector.py	The app main Connector module (Python script) that implements the actions that are provided by the app. This module is a class that is derived from the BaseConnector class.
flashpoint_consts.py	All the constants which are used in the app connector
readme.html	Additional documentation for the app
logo_flashpoint.svg	The Flashpoint Phantom app logo for the light theme
logo_flashpoint_dark.svg	The Flashpoint Phantom app logo for the dark theme

flashpoint_view.py	The app view module that implements the view function declared/specified in the app JSON and returns Django template HTML file used to render the results' context.
flashpoint_iocs_view.html	The Django HTML template to render the output results of IoCs
flashpoint_reports_view.html	The Django HTML template to render the output results of reports

6.2. Architecture Diagram


Phantom Platform (Flashpoint App)
Action Trigger
Asset Configuration Parameters and Action Result Intialization
Manual Entry in the Flashpoint Phantom App Asset Configuration
Base Connector Initialization
Action Parameters Initialization
App Connector Initialization
Action Block Initiation
Make REST Call
Process Response
Sucess
Failure
Process JSON Response
Process HTML Response
Process Empty Response
Output Response Processing
Action Result Processing
Finalize
Action Output Rendering
Flashpoint Platform
Flashpoint GUI Token Generation
Indicators API
Reports API
Search API
Flashpoint APIs

7. Integrated Actions

In any Phantom integration for a tool or service, the actions are the most modular components. They are designed consisting of a set of API endpoints (of that tool or service) that are integrated with the phantom app with a provision of the input action parameters to retrieve the required results using those APIs.

In the Flashpoint Phantom integration, we support a single Test Connectivity action and 7 investigative actions by using the Indicators, Reports, and All Search APIs of the Flashpoint Platform. The actions are listed in the following sections.

7.1. Test Connectivity

7.1.1. Action Goal

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

7.1.2. Action Parameters

To run the test connectivity successfully below-mentioned are the required asset configuration parameters.

Parameter	Data type	Required	Default
Base URL	String	Yes	https://fp.tools/api/v4
API Token	Password	Yes	None
Retry Wait Period (in seconds)	Numeric	No	5
Number Of Retries	Numeric	No	1

7.1.3. Action Workflow

This action will test connectivity to the Flashpoint instance using the provided asset configuration parameters. This action will use simplified indicators API to test the Base URL and API Token. Based on the API call response, the appropriate success and failure message will be displayed when the test connectivity gets executed with the configured asset configuration parameters.

7.1.4. Functional Use Cases

The only functional use case of the connectivity action is to validate the provided asset configuration parameters. An API call to the Indicators endpoint is executed as mentioned below.

GET <base_url><endpoint>?<params>

- **Method -** GET
- **Base URL -** https://fp.tools/api/v4
- **Endpoint -** /indicators/simple
- **Params -** limit=1
- **API token -** xxxABcXyz12345njIkXXXXXXX

The API call for the test connectivity with the above attributes is mentioned below.

GET https://fp.tools/api/v4/indicatos/simple?limit=1

Headers

- Authorization: Bearer xxxABcXyz12345njIkXXXXXXX
- 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')

7.1.5. Action Output

The action displays the success or failure message based on the output response of the connectivity API call to the Indicators API. For a successful run, it displays 'Test Connectivity Passed' output message and in case of failure scenarios, it displays the message 'Test Connectivity Failed' with an appropriate output error response. There are no output data paths in the Phantom for the Test Connectivity action.

7.2. List Indicators

7.2.1. Action Goal

Fetch a list of IoCs that occur in the context of an event from the Flashpoint Platform. The user can filter the IoCs (while fetching) based on the query or the attribute types. The user can also limit the output results by providing a limit value in the action parameters.

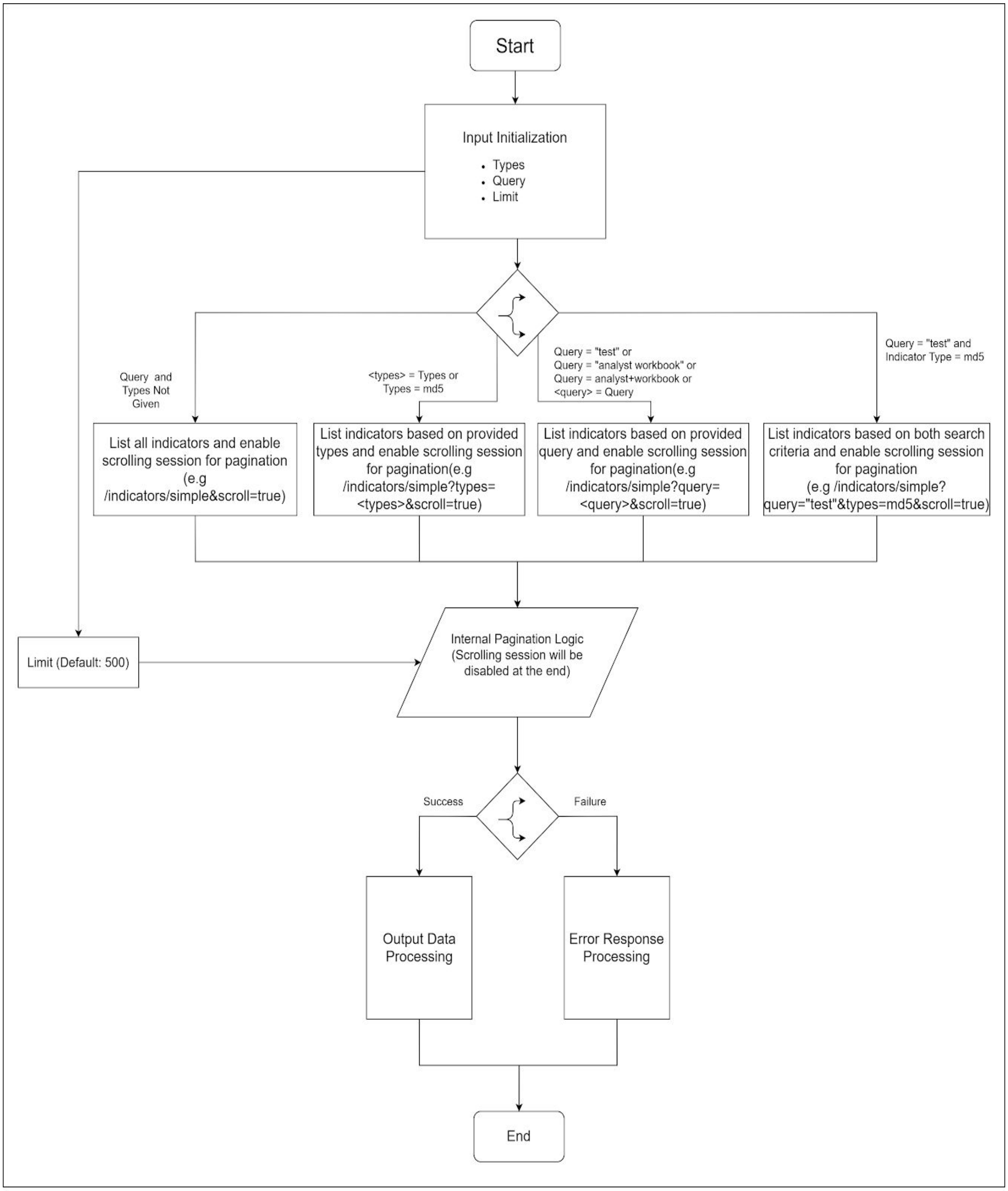
7.2.2. Action Parameters

The action parameters are listed below.

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

7.2.3. Action Workflow

The action will fetch a simplified list of IoCs from the Flashpoint instance. The results are retrieved based on the provided action parameters. The internal action workflow diagram is demonstrated below.


Start
Input Initialization
Types
Query
Limit
Query and Types Not Given
<types> = Types or Types = md5
Query = "test" or Query = "analyst workbook" or Query = analyst+workbook or <query> = Query
Query = "test" and Indicator Type = md5
List all indicators and enable scrolling session for pagination (e.g /indicators/simple&scroll=true)
List indicators based on provided types and enable scrolling session for pagination(e.g /indicators/simple?types=<types>&scroll=true)
List indicators based on provided query and enable scrolling session for pagination(e.g /indicators/simple?query=<query>&scroll=true)
List indicators based on both search criteria and enable scrolling session for pagination (e.g /indicators/simple?query="test"&types=md5&scroll=true)
Limit (Default: 500)
Internal Pagination Logic (Scrolling session will be disabled at the end)
Success
Failure
Output Data Processing
Error Response Processing
End

7.2.4. Functional Use Cases

The action provides a provision to fetch the IoCs and technical data across the Flashpoint datasets which consist of IPs, Domains, URLs, YARA Rules, MD5 and other hashes. Based on the values provided in the action parameters, multiple use cases for the IoC search can be achieved. The use cases are listed below.

Action Parameter - Attribute Types

This parameter enables search by attribute types. It is an optional action parameter. It supports the comma-separated values list of attribute types. Each value from the provided comma-separated list must correspond to one of the MISP types, a list of which can be found here (https://www.circl.lu/doc/misp/categories-and-types/).

Examples

a) Get recent md5, sha1, or source IP indicators.

Action parameters value:

- Attribute Types = md5,sha1,ip-src

Internal API call:

- https://fp.tools/api/v4/indicators/simple?types=md5,sha1,ip-src (GET)

Action Parameter - Query

This parameter will be used for free text searching. It is an optional parameter. You can also provide different queries to filter out indicators results.

Examples

a) Filtering results based on the field value.

Action parameters value:

- Query = category:”Payload Delivery”

Internal API call:

- https://fp.tools/api/v4/indicators/simple?query=category:”Payload Delivery” (GET)

Note - When using multiple words, use a + instead of space and for specific word search use “test text” (inverted double quotes) in the query action parameter.

Action parameters value:

- Query = gandcrab+ransomware
- Query = “test text”

Internal API call:

- https://fp.tools/api/v4/indicators/simple?limit=10&query="gandcrab+ransomware" (GET)
- https://fp.tools/api/v4/indicators/simple?limit=10&query="test text" (GET)

Limit

This parameter is used to limit the number of indicator results. The default value is 500. If the limit is not provided, it will fetch by default 500 indicator results. The internal pagination logic for fetching a large number of indicator results implements the scrolling session-based indicator APIs.

7.2.5. Action Output Data Paths

The Flashpoint Phantom integration data paths for this action are listed below.

- action_result.status
- action_result.data.*.Attribute.category
- action_result.data.*.Attribute.href
- action_result.data.*.Attribute.uuid
- action_result.data.*.Attribute.timestamp
- action_result.data.*.Attribute.to_ids
- action_result.data.*.Attribute.type
- action_result.data.*.Attribute.Event.info
- action_result.data.*.Attribute.Event.href
- action_result.data.*.Attribute.Event.attack_ids
- action_result.data.*.Attribute.Event.Tags
- action_result.data.*.Attribute.Event.timestamp
- action_result.data.*.Attribute.Event.fpid

- action_result.data.*.Attribute.Event.RelatedEvent.*.Event.info
- action_result.data.*.Attribute.Event.RelatedEvent.*.Event.fpid
- action_result.data.*.Attribute.value.comment
- action_result.data.*.Attribute.value.domain
- action_result.data.*.Attribute.fpid
- action_result.message
- action_result.parameter.attribute_types
- action_result.parameter.limit
- action_result.parameter.query
- action_result.summary
- summary.total_objects
- summary.total_objects_successful

7.3. Search Indicators

7.3.1. Action Goal

Fetch an IoC value of a specific attribute type from the list of available IoCs on the Flashpoint Platform. The user can also limit the output results by providing a limit value in the action parameters.

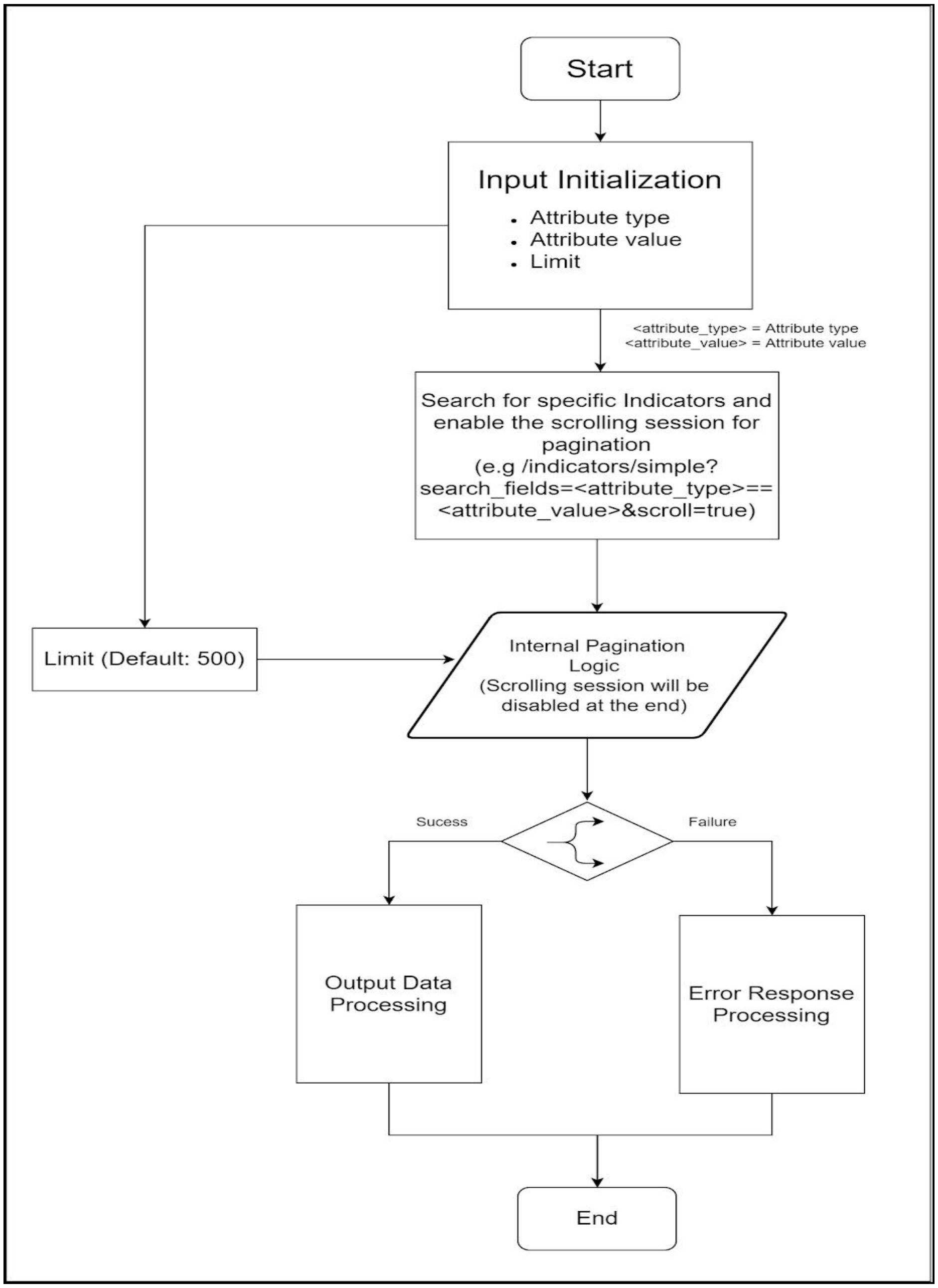
7.3.2. Action Parameters

The action parameters are listed below.

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

7.3.3. Action Workflow

The action will fetch a simplified list of IoCs having provided attribute type and attribute value. The attribute type must correspond to one of the MISP types, a list of which can be found here (https://www.circl.lu/doc/misp/categories-and-types/). The internal action workflow diagram is demonstrated below.


Start
Input Initialization
Attribute type
Attribute value
Limit
<attribute_type> = Attribute type
<attribute_value> = Attribute value
Search for specific Indicators and enable the scrolling session for pagination (e.g /indicators/simple?search_fields=<attribute_type>==<attribute_value>&scroll=true)
Limit (Default: 500)
Internal Pagination Logic (Scrolling session will be disabled at the end)
Sucess
Failure
Output Data Processing
Error Response Processing
End

7.3.4. Functional Use Cases

The action will fetch a simplified list of IoCs having provided attribute type and attribute value. Based on the values provided in the action parameters, multiple use cases for fetching specific IoCs can be achieved. The use cases are listed below.

Action Parameters - Attribute Type and Attribute Value

These parameters are required parameters. They will be used to retrieve specific indicator results based on the provided values.

Examples

a) Get indicator matching specific hash value.

Action parameters values:

- Attribute Type = md5 (any of md5,sha1,sha256, etc.)
- Attribute Value= 16139ce9025274a388a4281fef65049e

Internal API call:

- https://fp.tools/api/v4/indicators/simple?search_fields=md5==16139ce9025274a388a4281fef65049e (GET)

b) Get indicator matching specific filename.

Action parameters values:

- Attribute Type = filename
- Attribute Value= "PLEASE-CHECK”

Internal API call:

- https://fp.tools/api/v4/indicators/simple?search_fields=filename=="PLEASE-CHECK" (GET)

Note - In the above example, without the double quotes around the filename, it will search for every filename that matches 'PLEASE'. The hyphen/space will be considered as the end of search value and it will search for indicators matching the value until the first encountered hyphen/space.

c) Get indicator matching a specific source IP Address.

Action parameters values:

- Attribute Type = ip-src
- Attribute Value= 111.255.198.92

Internal API call:

- https://fp.tools/api/v4/indicators/simple?search_fields=ip-src=="111.255.198.92" (GET)

d) Get indicator matching a specific destination IP Address.

Action parameters values:

- Attribute Type = ip-dst
- Attribute Value= 111.255.198.92

Internal API call:

- https://fp.tools/api/v4/indicators/simple?search_fields=ip-dst=="111.255.198.92" (GET)

Limit

This parameter is used to limit the number of indicator results. The default value is 500. If the limit is not provided, it will fetch by default 500 indicator results. The internal pagination logic for fetching a large number of indicator results implements the scrolling session-based indicator APIs.

7.3.5. Action Output Data Paths

The Flashpoint Phantom integration data paths for this action are listed below.

- action_result.status
- action_result.data.*.Attribute.category
- action_result.data.*.Attribute.href
- action_result.data.*.Attribute.uuid
- action_result.data.*.Attribute.timestamp
- action_result.data.*.Attribute.to_ids
- action_result.data.*.Attribute.type
- action_result.data.*.Attribute.Event.info
- action_result.data.*.Attribute.Event.href
- action_result.data.*.Attribute.Event.attack_ids
- action_result.data.*.Attribute.Event.Tags
- action_result.data.*.Attribute.Event.timestamp
- action_result.data.*.Attribute.Event.fpid
- action_result.data.*.Attribute.Event.RelatedEvent.*.Event.info
- action_result.data.*.Attribute.Event.RelatedEvent.*.Event.fpid
- action_result.data.*.Attribute.value.comment

- action_result.data.*.Attribute.value.domain
- action_result.data.*.Attribute.fpid
- action_result.message
- action_result.parameter.attribute_type
- action_result.parameter.attribute_value
- action_result.parameter.limit
- action_result.summary
- summary.total_objects
- summary.total_objects_successful

7.4. List Reports

7.4.1. Action Goal

Fetch a list of all the intelligence reports from the Flashpoint Platform. The user can also limit the output results by providing a limit value in the action parameters.

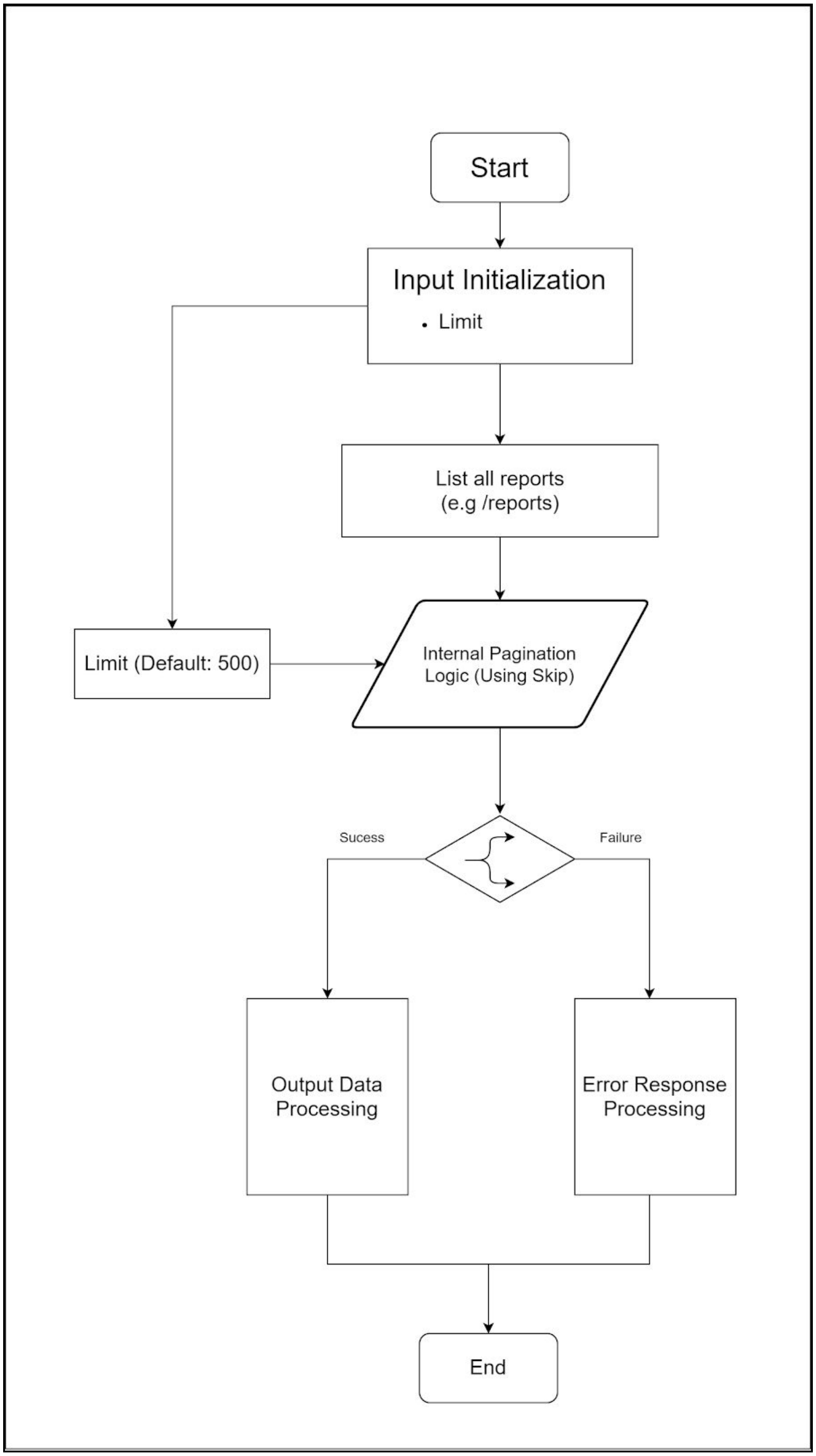
7.4.2. Action Parameters

The action parameters are listed below.

Parameter	Data type	Required	Default
Limit	Numeric	No	500

7.4.3. Action Workflow

The action will fetch a list of all the intelligence reports from the Flashpoint instance using the pagination mechanism. The internal action workflow diagram is demonstrated below.


Start
Input Initialization
Limit
List all reports
(e.g /reports)
Limit (Default: 500)
Internal Pagination
Logic (Using Skip)
Sucess
Failure
Output Data
Processing
Error Response
Processing
End

7.4.4. Functional Use Cases

This action will fetch all the analytical reports generated by the Flashpoint subject matter experts (SMEs). These reports cover a wide spectrum of illicit underground activity, from crimeware to fraud, emergent malware, violent extremism, physical threats, and many more. The use cases are listed below.

Action Parameter - Limit

This is an optional parameter. It is used to limit the number of fetched intelligence reports. The default value is 500. If the limit is not provided, it will fetch by default 500 intelligence reports.

Examples

a) Fetch 2000 intelligence reports.

NOTE - Here, we fetch only 500 intelligence reports in a single API call and then, followed by internal pagination logic using ‘skip’ API attribute to keep on fetching more intelligence reports until the list of available reports on the Flashpoint instance gets exhausted or the reports equal to the provided ‘limit’ value are already fetched whichever is earlier.

Action parameters values:

- Limit = 2000

Internal API calls: (4 API calls to fetch 500 reports in each API call)

- https://fp.tools/api/v4/reports?limit=500&skip=0 (GET)
- https://fp.tools/api/v4/reports?limit=500&skip=500 (GET)
- https://fp.tools/api/v4/reports?limit=500&skip=1000 (GET)
- https://fp.tools/api/v4/reports?limit=500&skip=1500 (GET)

b) Fetch 500 intelligence reports.

Action parameters values:

- Limit = Keep it empty

Internal API calls: (1 API call to fetch 500 reports in the first API call)

- https://fp.tools/api/v4/reports?limit=500&skip=0 (GET)

7.4.5. Action Output Data Paths

The Flashpoint Phantom integration data paths for this action are listed below.

- action_result.status
- action_result.data.*.body
- action_result.data.*.notified_at
- action_result.data.*.ingested_at
- action_result.data.*.title
- action_result.data.*.updated_at
- action_result.data.*.posted_at
- action_result.data.*.tags
- action_result.data.*.title_asset_id
- action_result.data.*.summary
- action_result.data.*.sources.*.title
- action_result.data.*.sources.*.source
- action_result.data.*.sources.*.source_id
- action_result.data.*.sources.*.platform_url
- action_result.data.*.sources.*.type
- action_result.data.*.sources.*.original
- action_result.data.*.published_status
- action_result.data.*.title_asset
- action_result.data.*.version_posted_at
- action_result.data.*.is_featured
- action_result.data.*.platform_url
- action_result.data.*.id
- action_result.message
- action_result.parameter.limit
- action_result.summary
- summary.total_objects
- summary.total_objects_successful

7.5. Get Report

7.5.1. Action Goal

Fetch a specific intelligence report from the Flashpoint Platform for the provided report ID.

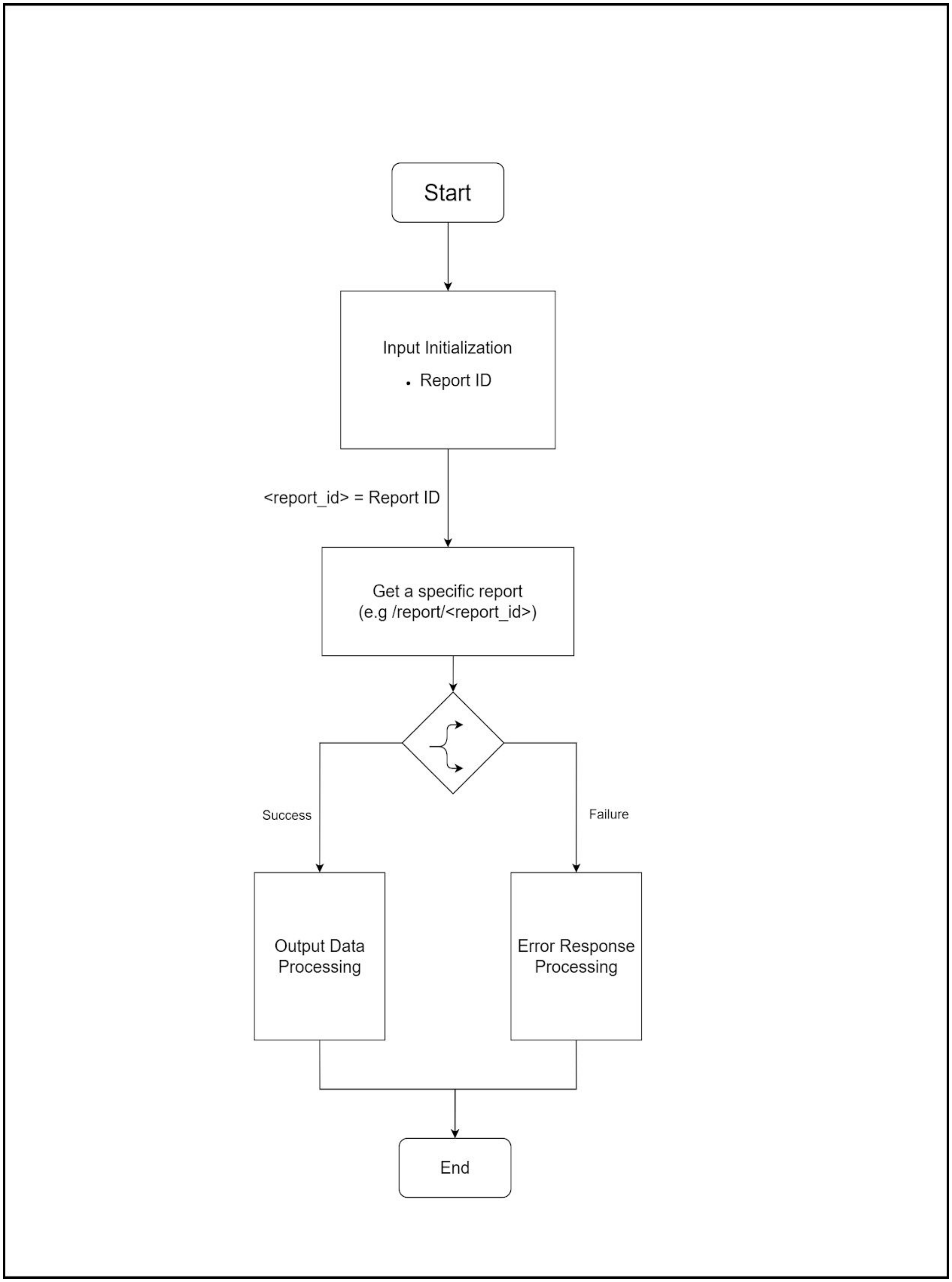
7.5.2. Action Parameters

The action parameters are listed below.

Parameter	Data type	Required	Default
Report ID	String	Yes	None

7.5.3. Action Workflow

The action will fetch a specific intelligence report for the provided report ID. The internal action workflow diagram is demonstrated below.


Start
Input Initialization
• Report ID
<report_id> = Report ID
Get a specific report
(e.g /report/<report_id>)
Success
Failure
Output Data Processing
Error Response Processing
End

7.5.4. Functional Use Cases

This action will fetch a specific intelligence report for the provided report ID. The report ID can correspond to any of the reports that cover a wide spectrum of illicit underground activity, from crimeware to fraud, emergent malware, violent extremism, physical threats, and many more. The use cases are listed below.

Action Parameter - Report ID

This parameter is a required parameter.

Examples

a) Fetch an intelligence report having the provided report ID value.

   NOTE - There is no need for implementing an internal pagination logic here as we are fetching a specific report based on the report ID.

   Action parameter value:

   - Report ID = wrh9BCZETzu3AO3CUopOlw

   Internal API call:

   - https://fp.tools/api/v4/reports/wrh9BCZETzu3AO3CUopOlw (GET)

7.5.5. Action Output Data Paths

The Flashpoint Phantom integration data paths for this action are listed below.

- action_result.status
- action_result.data.*.body
- action_result.data.*.notified_at
- action_result.data.*.ingested_at
- action_result.data.*.title
- action_result.data.*.updated_at
- action_result.data.*.posted_at
- action_result.data.*.tags
- action_result.data.*.title_asset_id
- action_result.data.*.summary
- action_result.data.*.sources.*.title

- action_result.data.*.sources.*.source
- action_result.data.*.sources.*.source_id
- action_result.data.*.sources.*.platform_url
- action_result.data.*.sources.*.type
- action_result.data.*.sources.*.original
- action_result.data.*.published_status
- action_result.data.*.title_asset
- action_result.data.*.version_posted_at
- action_result.data.*.is_featured
- action_result.data.*.platform_url
- action_result.data.*.id
- action_result.message
- action_result.parameter.report_id
- action_result.summary
- summary.total_objects
- summary.total_objects_successful

7.6. List Related Reports

7.6.1. Action Goal

Fetch a list of all the related intelligence reports from the Flashpoint Platform for the provided report ID. The user can also limit the output results by providing a limit value in the action parameters.

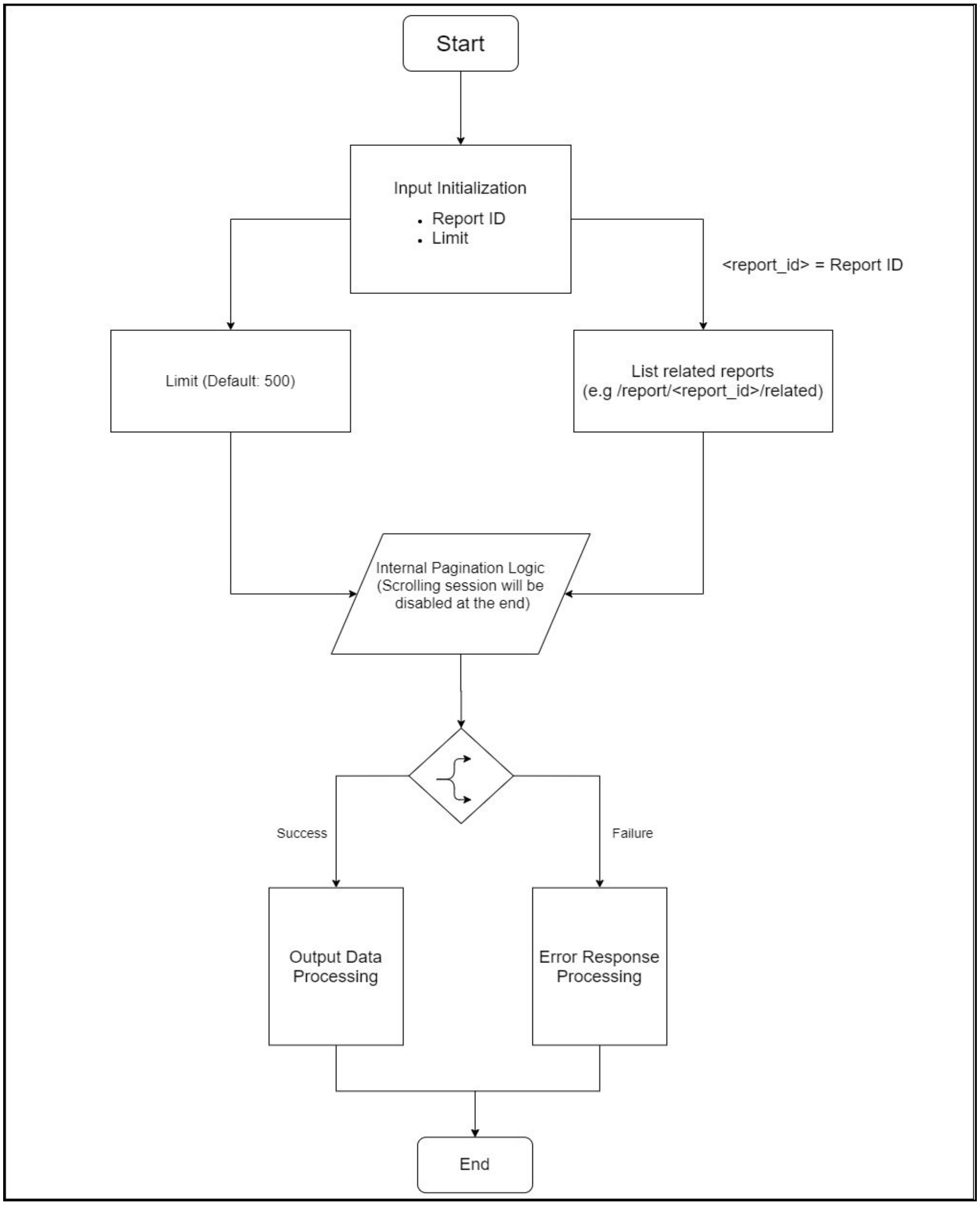
7.6.2. Action Parameters

The action parameters are listed below.

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

7.6.3. Action Workflow

The action will fetch all the related intelligence reports for the provided report ID using the paginated mechanism. The internal action workflow diagram is demonstrated below.



7.6.4. Functional Use Cases

This action will fetch all the related intelligence reports for the provided report ID. The report ID can correspond to any of the reports that cover a wide spectrum of illicit underground activity, from crimeware to fraud, emergent malware, violent extremism, physical threats, and many more. The use cases are listed below.

Action Parameters - Report ID and Limit

The 'Report ID' parameter is a required parameter and the 'Limit' parameter is optional.

Examples

a) Fetch default 500 related intelligence reports for the provided report ID.

   Action parameters values:
   - Report ID = wrh9BCZETzu3AO3CUopOlw
   - Limit = Keep it empty

   Internal API call:
   - https://fp.tools/api/v4/reports/wrh9BCZETzu3AO3CUopOlw/related (GET)

b) Fetch 2000 related intelligence reports for the provided report ID.

   NOTE - Here, we fetch only 500 related intelligence reports in a single API call and then, followed by internal pagination logic using 'skip' API attribute to keep on fetching more related intelligence reports until the list of available related reports on the Flashpoint instance for the provided 'Report ID' gets exhausted or the related reports equal to the provided 'Limit' value is already fetched whichever is earlier.

   Action parameters values:
   - Report ID = wrh9BCZETzu3AO3CUopOlw
   - Limit = 2000

   Internal API calls: (4 API calls to fetch 500 related reports in each API call)
   - https://fp.tools/api/v4/reports/wrh9BCZETzu3AO3CUopOlw/related?limit=500&skip=0 (GET)

- https://fp.tools/api/v4/reports/wrh9BCZETzu3AO3CUopOlw/related?limit=500&skip=500 (GET)
- https://fp.tools/api/v4/reports/wrh9BCZETzu3AO3CUopOlw/related?limit=500&skip=1000 (GET)
- https://fp.tools/api/v4/reports/wrh9BCZETzu3AO3CUopOlw/related?limit=500&skip=1500 (GET)

7.6.5. Action Output Data Paths

The Flashpoint Phantom integration data paths for this action are listed below.

- action_result.status
- action_result.data.*.body
- action_result.data.*.notified_at
- action_result.data.*.ingested_at
- action_result.data.*.title
- action_result.data.*.updated_at
- action_result.data.*.posted_at
- action_result.data.*.tags
- action_result.data.*.title_asset_id
- action_result.data.*.summary
- action_result.data.*.sources.*.title
- action_result.data.*.sources.*.source
- action_result.data.*.sources.*.source_id
- action_result.data.*.sources.*.platform_url
- action_result.data.*.sources.*.type
- action_result.data.*.sources.*.original
- action_result.data.*.published_status
- action_result.data.*.title_asset
- action_result.data.*.version_posted_at
- action_result.data.*.is_featured
- action_result.data.*.platform_url
- action_result.data.*.id
- action_result.message
- action_result.parameter.report_id
- action_result.parameter.limit
- action_result.summary
- summary.total_objects

- summary.total_objects_successful

7.7. Get Compromised Credentials

7.7.1. Action Goal

Fetch a list of all the Credential Sightings from the Flashpoint Platform. The user can narrow down the fetched data by providing a filter value. The user can also limit the output results by providing a limit value in the action parameters.

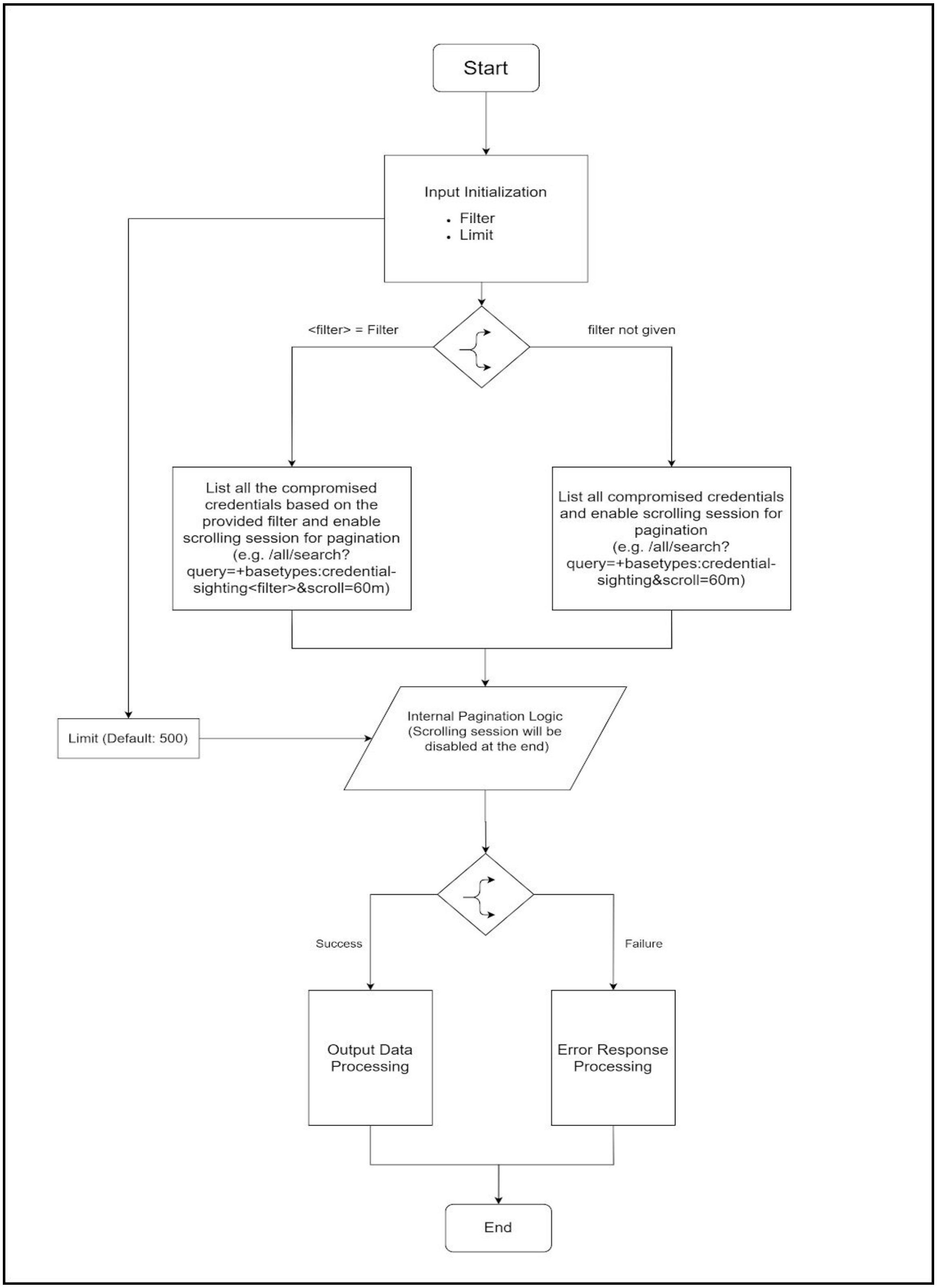
7.7.2. Action Parameters

The action parameters are listed below.

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

7.7.3. Action Workflow

The action will search for all compromised credentials based on the provided credential sighting filter. The internal action workflow diagram is demonstrated below.


Start
Input Initialization
• Filter
• Limit
<filter> = Filter
filter not given
List all the compromised credentials based on the provided filter and enable scrolling session for pagination (e.g. /all/search?query=+basetypes:credential-sighting<filter>&scroll=60m)
List all compromised credentials and enable scrolling session for pagination (e.g. /all/search?query=+basetypes:credential-sighting&scroll=60m)
Limit (Default: 500)
Internal Pagination Logic (Scrolling session will be disabled at the end)
Success
Failure
Output Data Processing
Error Response Processing
End

7.7.4. Functional Use Cases

This action will search for all compromised credentials based on the provided credential sighting filter. A Credential Sighting is a single occurrence of a username/password pair. The use cases are listed below.

Action Parameter - Filter

This parameter will be used for filtering the data of credentials sightings on the Flashpoint instance. It is an optional parameter. If not given, it will get all the compromised credentials. A few sample values of the filter action parameter are listed below.

- +is_fresh:true (search for only new credential sightings)
- +breach.first_observed_at.date-time:[now-30d TO now] (search for credential sightings which are discovered in the last month)
- +breach.fpid:nIbeDs_VXyKedBmuhFEaGQ (search for all credential sightings in a Breach)
- +email:username (search for a username)
- +email.keyword:username@domain.com (search for an email address)
- +domain.keyword:domain.com (search for credentials sightings data pertaining to a particular domain)

Examples

a) Search for credential sightings pertaining to the given domain and that are discovered in the last month based on the date provided from the source of this credential sightings data.

   Action parameters values:
   - Filter = +domain.keyword:domain.com+breach.first_observed_at.date-time:[now-30d TO now]

   Internal API call:
   - https://fp.tools/api/v4/all/search?query=+basetypes:credential-sighting+domain.keyword:domain.com+breach.first_observed_at.date-time:[now-30d TO now] (GET)

b) Search for credential sightings pertaining to the given domain and that are discovered in the last month based on the date of indexing of the data into the Flashpoint server

   Action parameters values:
   - Filter = +domain.keyword:domain.com+header_.indexed_at:[now-30d TO now]

   Internal API call:
   - https://fp.tools/api/v4/all/search?query=+basetypes:credential-sighting+domain.keyword:domain.com+header_.indexed_at:[now-30d TO now] (GET)

c) Search for credential sightings which are discovered in the last month based on the date of indexing of the data into the Flashpoint server

   Action parameters values:
   - Filter = +header_.indexed_at:[now-30d TO now]

   Internal API call:
   - https://fp.tools/api/v4/all/search?query=+basetypes:credential-sighting+header_.indexed_at:[now-30d TO now] (GET)

d) Search for credential sightings which are discovered in between the provided timestamps based on the date provided from the source of this credential sightings data

   Action parameters values:
   - Filter = +breach.first_observed_at.timestamp:[1234567890 TO 1234567890]

   Internal API call:
   - https://fp.tools/api/v4/all/search?query=+breach.first_observed_at.timestamp:[1234567890 TO 1234567890](GET)

Limit

This parameter is used to limit the number of fetched compromised credentials. The default value is 500. If the limit is not provided, it will fetch by default 500 compromised credentials. The internal pagination logic for fetching a large number of compromised credentials implements the scrolling session-based Credentials All Search APIs.

7.7.5. Action Output Data Paths

The Flashpoint Phantom integration data paths for this action are listed below.

- action_result.status
- action_result.data.*._type
- action_result.data.*._id
- action_result.data.*._source.body.raw
- action_result.data.*._source.extraction_id
- action_result.data.*._source.domain
- action_result.data.*._source.password
- action_result.data.*._source.header_.indexed_at
- action_result.data.*._source.times_seen
- action_result.data.*._source.extraction_record_id
- action_result.data.*._source.fpid
- action_result.data.*._source.last_observed_at.timestamp
- action_result.data.*._source.last_observed_at.date-time
- action_result.data.*._source.credential_record_fpid
- action_result.data.*._source.is_fresh
- action_result.data.*._source.basetypes
- action_result.data.*._source.breach.fpid
- action_result.data.*._source.breach.source_type
- action_result.data.*._source.breach.source
- action_result.data.*._source.breach.victim
- action_result.data.*._source.breach.basetypes
- action_result.data.*._source.breach.breach_type
- action_result.data.*._source.breach.created_at.timestamp
- action_result.data.*._source.breach.created_at.date-time
- action_result.data.*._source.breach.title
- action_result.data.*._source.breach.first_observed_at.timestamp
- action_result.data.*._source.breach.first_observed_at.date-time
- action_result.data.*._source.customer_id
- action_result.data.*._source.password_complexity.has_symbol
- action_result.data.*._source.password_complexity.has_number
- action_result.data.*._source.password_complexity.has_uppercase

- action_result.data.*._source.password_complexity.length
- action_result.data.*._source.password_complexity.has_lowercase
- action_result.data.*._source.email
- action_result.message
- action_result.parameter.filter
- action_result.parameter.limit
- action_result.summary
- summary.total_objects
- summary.total_objects_successful

7.8. Run Query

7.8.1. Action Goal

Fetch the data by performing an all search from the Flashpoint Platform. The user can limit the searches by providing the criteria in the query parameter. The user can also limit the output results by providing a limit value in the action parameters.

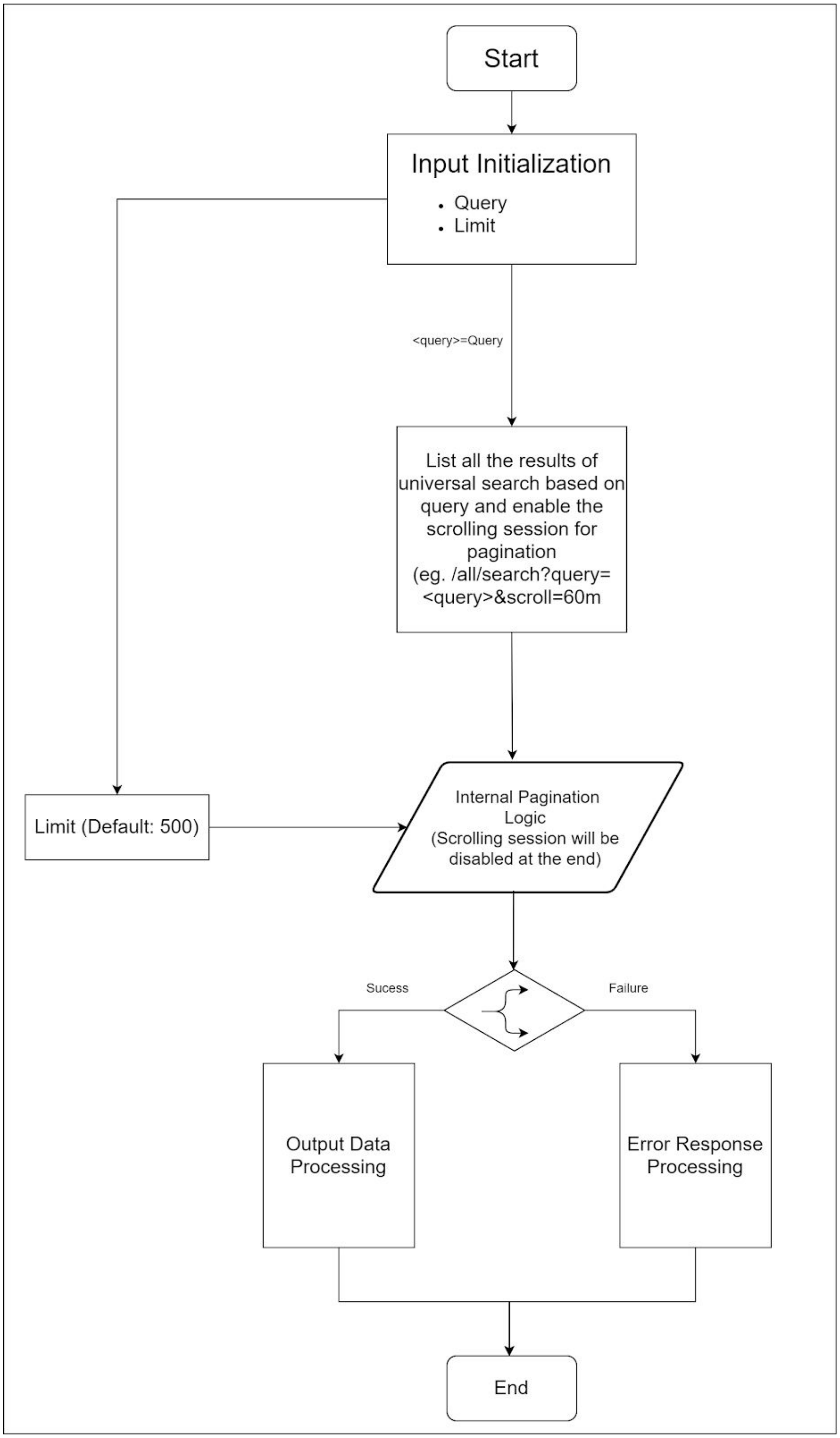
7.8.2. Action Parameters

The action parameters are listed below.

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

7.8.3. Action Workflow

The action performs an all search on the Flashpoint Platform. The internal action workflow diagram is demonstrated below.


Start
Input Initialization
Query
Limit
<query>=Query
List all the results of universal search based on query and enable the scrolling session for pagination (eg. /all/search?query=<query>&scroll=60m
Limit (Default: 500)
Internal Pagination Logic (Scrolling session will be disabled at the end)
Sucess
Failure
Output Data Processing
Error Response Processing
End

7.8.4. Functional Use Cases

This action will perform an all search based on the provided criteria in the ‘Query’ parameter. The use cases are listed below.

Action Parameter - Query

This parameter will be used to search across all fields in the marketplace data by appending terms to it or limit searches to individual fields by appending <field name>:<value> to the ‘Query’ parameter. The queries supported by

- All credential breach queries (+basetypes:breach)
  (For more information https://docs.fp.tools/#search-api-creds)
- All CVE queries (+basetypes:cve)
  (For more https://docs.fp.tools/#search-api-cves)
- All card queries (+basetypes:card)
  (For more https://docs.fp.tools/#search-api-cards)
- All paste queries (+basetypes:paste)
  (For more https://docs.fp.tools/#search-api-paste)
- All chat queries (+basetypes:generic-product)
  (For more https://docs.fp.tools/#search-api-marketplaces)

Examples

a) Search for “Analyst Research” breaches.

Action parameters values:

- Query= +basetypes:breach+source_type:Analyst Research

Internal API call:

- https://fp.tools/api/v4/all/search?query=+basetypes:breach+source_type:Analyst Research (GET)

b) Search for "testing" across all free-form fields (message body, channel profile, channel name, and user name)

Action parameters values:

- Query = +basetypes:card+testing

Internal API call:

- https://fp.tools/api/v4/all/search?query=+basetypes:card+testing (GET)

c) Search for credential sightings pertaining to the given domain and that are discovered in the last month based on the date provided from the source of this credential sightings data

Action parameters values:

- Query = +basetypes:credential-sighting+domain.keyword:domain.com+breach.first_observed_at.date-time:[now-30d TO now]

Internal API call:

- https://fp.tools/api/v4/all/search?query=+basetypes:credential-sighting+domain.keyword:domain.com+breach.first_observed_at.date-time:[now-30d TO now] (GET)

d) Filter all search results by ISO date/time range based on the date provided from the source of this search data.

Action parameters values:

- Query = +basetypes:paste+testing+created_at.date-time:["2018-10-24T10:05:10+00:00" TO "2018-10-26T10:05:10+00:00"]

Internal API call:

- https://fp.tools/api/v4/all/search?query=+basetypes:card+created_at.date-time:["2018-10-24T10:05:10+00:00" TO "2018-10-26T10:05:10+00:00"] (GET)

e) Filter results by Unix time for all paste results based on the date provided from the source of this paste search data

Action parameters values:

- Query = +basetypes:paste+created_at.timestamp:[1234567890 TO 1234567890]

Internal API call:

- https://fp.tools/api/v4/all/search?query=+basetypes:paste+created_at.timestamp:[1234567890 TO 1234567890] (GET)

Limit

This parameter is used to limit the number of fetched all search data. The default value is 500. If the limit is not provided, it will fetch by default 500 search items. The internal pagination logic for fetching a large number of search items implements the scrolling session-based All Search APIs.

7.8.5. Action Output Data Paths

The Flashpoint Phantom integration data paths for this action are listed below.

- action_result.data.*._id
- action_result.data.*._source.Event.Org.id
- action_result.data.*._source.Event.Org.name
- action_result.data.*._source.Event.Org.uuid
- action_result.data.*._source.Event.Orgc.id
- action_result.data.*._source.Event.Orgc.name
- action_result.data.*._source.Event.Orgc.uuid
- action_result.data.*._source.Event.Tag.*.colour
- action_result.data.*._source.Event.Tag.*.exportable
- action_result.data.*._source.Event.Tag.*.hide_tag
- action_result.data.*._source.Event.Tag.*.id
- action_result.data.*._source.Event.Tag.*.name
- action_result.data.*._source.Event.Tag.*.user_id
- action_result.data.*._source.Event.analysis
- action_result.data.*._source.Event.attribute_count
- action_result.data.*._source.Event.date
- action_result.data.*._source.Event.disable_correlation
- action_result.data.*._source.Event.distribution
- action_result.data.*._source.Event.event_creator_email
- action_result.data.*._source.Event.extends_uuid
- action_result.data.*._source.Event.fpid
- action_result.data.*._source.Event.id
- action_result.data.*._source.Event.info
- action_result.data.*._source.Event.locked
- action_result.data.*._source.Event.org_id
- action_result.data.*._source.Event.orgc_id
- action_result.data.*._source.Event.proposal_email_lock
- action_result.data.*._source.Event.publish_timestamp

- action_result.data.*._source.Event.published
- action_result.data.*._source.Event.sharing_group_id
- action_result.data.*._source.Event.threat_level_id
- action_result.data.*._source.Event.timestamp
- action_result.data.*._source.Event.uuid
- action_result.data.*._source.bank_name
- action_result.data.*._source.base.basetypes
- action_result.data.*._source.base.fpid
- action_result.data.*._source.base.native_id
- action_result.data.*._source.base.raw
- action_result.data.*._source.base.release_date.date-time
- action_result.data.*._source.base.release_date.raw
- action_result.data.*._source.base.release_date.timestamp
- action_result.data.*._source.base.title
- action_result.data.*._source.basetypes
- action_result.data.*._source.bin
- action_result.data.*._source.body.enrichments.cves
- action_result.data.*._source.body.enrichments.language
- action_result.data.*._source.body.enrichments.links.*.href
- action_result.data.*._source.body.raw
- action_result.data.*._source.body.text/html+sanitized
- action_result.data.*._source.body.text/html-sanitized
- action_result.data.*._source.body.text/plain
- action_result.data.*._source.breach.basetypes
- action_result.data.*._source.breach.breach_type
- action_result.data.*._source.breach.created_at.date-time
- action_result.data.*._source.breach.created_at.timestamp
- action_result.data.*._source.breach.first_observed_at.date-time
- action_result.data.*._source.breach.first_observed_at.timestamp
- action_result.data.*._source.breach.fpid
- action_result.data.*._source.breach.source
- action_result.data.*._source.breach.source_type
- action_result.data.*._source.breach.title
- action_result.data.*._source.breach.victim
- action_result.data.*._source.card_type
- action_result.data.*._source.cardholder_information.email
- action_result.data.*._source.cardholder_information.first

- action_result.data.*._source.cardholder_information.is_date_of_birth_available
- action_result.data.*._source.cardholder_information.is_email_available
- action_result.data.*._source.cardholder_information.is_phone_number_available
- action_result.data.*._source.cardholder_information.is_social_security_number_available
- action_result.data.*._source.cardholder_information.location.address
- action_result.data.*._source.cardholder_information.location.city
- action_result.data.*._source.cardholder_information.location.country.abbreviation
- action_result.data.*._source.cardholder_information.location.country.raw
- action_result.data.*._source.cardholder_information.location.region.raw
- action_result.data.*._source.cardholder_information.location.zip_code
- action_result.data.*._source.cardholder_information.phone_number
- action_result.data.*._source.cardholder_information.social_security_number.full
- action_result.data.*._source.category
- action_result.data.*._source.container.admins_count
- action_result.data.*._source.container.basetypes
- action_result.data.*._source.container.body.enrichments.domains
- action_result.data.*._source.container.body.enrichments.language
- action_result.data.*._source.container.body.enrichments.links.*.href
- action_result.data.*._source.container.body.raw
- action_result.data.*._source.container.body.text/html+sanitized
- action_result.data.*._source.container.body.text/plain
- action_result.data.*._source.container.category
- action_result.data.*._source.container.container.basetypes
- action_result.data.*._source.container.container.body.enrichments.domains
- action_result.data.*._source.container.container.body.enrichments.hashtags
- action_result.data.*._source.container.container.body.enrichments.language
- action_result.data.*._source.container.container.body.enrichments.links.*.href
- action_result.data.*._source.container.container.body.raw
- action_result.data.*._source.container.container.body.text/plain

- action_result.data.*._source.container.container.created_at.date-time
- action_result.data.*._source.container.container.created_at.raw
- action_result.data.*._source.container.container.created_at.timestamp
- action_result.data.*._source.container.container.fpid
- action_result.data.*._source.container.container.last_observed_at.date-time
- action_result.data.*._source.container.container.last_observed_at.raw
- action_result.data.*._source.container.container.last_observed_at.timestamp
- action_result.data.*._source.container.container.name
- action_result.data.*._source.container.container.native_id
- action_result.data.*._source.container.container.num_subscribers
- action_result.data.*._source.container.container.source_uri
- action_result.data.*._source.container.container.url
- action_result.data.*._source.container.created_at.date-time
- action_result.data.*._source.container.created_at.raw
- action_result.data.*._source.container.created_at.timestamp
- action_result.data.*._source.container.description
- action_result.data.*._source.container.enrichments.language
- action_result.data.*._source.container.fpid
- action_result.data.*._source.container.is_deleted
- action_result.data.*._source.container.kicked_count
- action_result.data.*._source.container.last_observed_at.date-time
- action_result.data.*._source.container.last_observed_at.raw
- action_result.data.*._source.container.last_observed_at.timestamp
- action_result.data.*._source.container.name
- action_result.data.*._source.container.native_id
- action_result.data.*._source.container.participants_count
- action_result.data.*._source.container.raw_href
- action_result.data.*._source.container.reputation.number_of_downvotes
- action_result.data.*._source.container.reputation.number_of_upvotes
- action_result.data.*._source.container.site_actor.basetypes
- action_result.data.*._source.container.site_actor.fpid
- action_result.data.*._source.container.site_actor.last_observed_at.date-time
- action_result.data.*._source.container.site_actor.last_observed_at.raw
- action_result.data.*._source.container.site_actor.last_observed_at.timestamp

- action_result.data.*._source.container.site_actor.names.aliases
- action_result.data.*._source.container.site_actor.names.handle
- action_result.data.*._source.container.site_actor.native_id
- action_result.data.*._source.container.site_actor.site.base_uris
- action_result.data.*._source.container.site_actor.site.basetypes
- action_result.data.*._source.container.site_actor.site.created_at.date-time
- action_result.data.*._source.container.site_actor.site.description.raw
- action_result.data.*._source.container.site_actor.site.fpid
- action_result.data.*._source.container.site_actor.site.site_type
- action_result.data.*._source.container.site_actor.site.source_uri
- action_result.data.*._source.container.site_actor.site.tags.*.name
- action_result.data.*._source.container.site_actor.site.tags.*.parent_tag.name
- action_result.data.*._source.container.site_actor.site.title
- action_result.data.*._source.container.site_actor.site.updated_at.date-time
- action_result.data.*._source.container.site_actor.source_uri
- action_result.data.*._source.container.site_actor.url
- action_result.data.*._source.container.source_uri
- action_result.data.*._source.container.title
- action_result.data.*._source.container.type
- action_result.data.*._source.container.url
- action_result.data.*._source.container.username
- action_result.data.*._source.created_at.date-time
- action_result.data.*._source.created_at.raw
- action_result.data.*._source.created_at.timestamp
- action_result.data.*._source.credential_record_fpid
- action_result.data.*._source.customer_id
- action_result.data.*._source.cve.basetypes
- action_result.data.*._source.cve.fpid
- action_result.data.*._source.cve.last_observed_at.date-time
- action_result.data.*._source.cve.last_observed_at.raw
- action_result.data.*._source.cve.last_observed_at.timestamp
- action_result.data.*._source.cve.mitre.basetypes
- action_result.data.*._source.cve.mitre.body.enrichments.cves
- action_result.data.*._source.cve.mitre.body.enrichments.links.*.href
- action_result.data.*._source.cve.mitre.body.raw
- action_result.data.*._source.cve.mitre.body.text/html-sanitized
- action_result.data.*._source.cve.mitre.body.text/plain

- action_result.data.*._source.cve.mitre.created_at.date-time
- action_result.data.*._source.cve.mitre.created_at.raw
- action_result.data.*._source.cve.mitre.created_at.timestamp
- action_result.data.*._source.cve.mitre.fpid
- action_result.data.*._source.cve.mitre.last_observed_at.date-time
- action_result.data.*._source.cve.mitre.last_observed_at.raw
- action_result.data.*._source.cve.mitre.last_observed_at.timestamp
- action_result.data.*._source.cve.mitre.native_id
- action_result.data.*._source.cve.mitre.phase
- action_result.data.*._source.cve.mitre.site.base_uris
- action_result.data.*._source.cve.mitre.site.basetypes
- action_result.data.*._source.cve.mitre.site.created_at.date-time
- action_result.data.*._source.cve.mitre.site.description.raw
- action_result.data.*._source.cve.mitre.site.fpid
- action_result.data.*._source.cve.mitre.site.site_type
- action_result.data.*._source.cve.mitre.site.source_uri
- action_result.data.*._source.cve.mitre.site.tags.*.name
- action_result.data.*._source.cve.mitre.site.tags.*.parent_tag.name
- action_result.data.*._source.cve.mitre.site.title
- action_result.data.*._source.cve.mitre.site.updated_at.date-time
- action_result.data.*._source.cve.mitre.status
- action_result.data.*._source.cve.mitre.title
- action_result.data.*._source.cve.native_id
- action_result.data.*._source.cve.nist.assigner
- action_result.data.*._source.cve.nist.basetypes
- action_result.data.*._source.cve.nist.body.enrichments.cves
- action_result.data.*._source.cve.nist.body.enrichments.links.*.href
- action_result.data.*._source.cve.nist.body.raw
- action_result.data.*._source.cve.nist.body.text/html-sanitized
- action_result.data.*._source.cve.nist.body.text/plain
- action_result.data.*._source.cve.nist.configurations.*.cpe23_uri
- action_result.data.*._source.cve.nist.configurations.*.version_end_including
- action_result.data.*._source.cve.nist.created_at.date-time
- action_result.data.*._source.cve.nist.created_at.raw
- action_result.data.*._source.cve.nist.created_at.timestamp
- action_result.data.*._source.cve.nist.cvssv2.access_complexity
- action_result.data.*._source.cve.nist.cvssv2.access_vector

- action_result.data.*._source.cve.nist.cvssv2.authentication
- action_result.data.*._source.cve.nist.cvssv2.availability_impact
- action_result.data.*._source.cve.nist.cvssv2.base_score
- action_result.data.*._source.cve.nist.cvssv2.confidentiality_impact
- action_result.data.*._source.cve.nist.cvssv2.exploitability_score
- action_result.data.*._source.cve.nist.cvssv2.impact_score
- action_result.data.*._source.cve.nist.cvssv2.integrity_impact
- action_result.data.*._source.cve.nist.cvssv2.severity
- action_result.data.*._source.cve.nist.cvssv2.vector_string
- action_result.data.*._source.cve.nist.cvssv3.attack_complexity
- action_result.data.*._source.cve.nist.cvssv3.attack_vector
- action_result.data.*._source.cve.nist.cvssv3.availability_impact
- action_result.data.*._source.cve.nist.cvssv3.base_score
- action_result.data.*._source.cve.nist.cvssv3.confidentiality_impact
- action_result.data.*._source.cve.nist.cvssv3.exploitability_score
- action_result.data.*._source.cve.nist.cvssv3.impact_score
- action_result.data.*._source.cve.nist.cvssv3.integrity_impact
- action_result.data.*._source.cve.nist.cvssv3.privileges_required
- action_result.data.*._source.cve.nist.cvssv3.scope
- action_result.data.*._source.cve.nist.cvssv3.severity
- action_result.data.*._source.cve.nist.cvssv3.user_interaction
- action_result.data.*._source.cve.nist.cvssv3.vector_string
- action_result.data.*._source.cve.nist.fpid
- action_result.data.*._source.cve.nist.last_observed_at.date-time
- action_result.data.*._source.cve.nist.last_observed_at.raw
- action_result.data.*._source.cve.nist.last_observed_at.timestamp
- action_result.data.*._source.cve.nist.native_id
- action_result.data.*._source.cve.nist.products.*.product_name
- action_result.data.*._source.cve.nist.products.*.vendor_name
- action_result.data.*._source.cve.nist.references.*.name
- action_result.data.*._source.cve.nist.references.*.refsource
- action_result.data.*._source.cve.nist.references.*.tags
- action_result.data.*._source.cve.nist.references.*.url
- action_result.data.*._source.cve.nist.site.base_uris
- action_result.data.*._source.cve.nist.site.basetypes
- action_result.data.*._source.cve.nist.site.created_at.date-time
- action_result.data.*._source.cve.nist.site.description.raw
- action_result.data.*._source.cve.nist.site.fpid

- action_result.data.*._source.cve.nist.site.site_type
- action_result.data.*._source.cve.nist.site.source_uri
- action_result.data.*._source.cve.nist.site.tags.*.name
- action_result.data.*._source.cve.nist.site.title
- action_result.data.*._source.cve.nist.site.updated_at.date-time
- action_result.data.*._source.cve.nist.title
- action_result.data.*._source.cve.nist.updated_at.date-time
- action_result.data.*._source.cve.nist.updated_at.raw
- action_result.data.*._source.cve.nist.updated_at.timestamp
- action_result.data.*._source.cve.nist.vulnerability_types
- action_result.data.*._source.cve.title
- action_result.data.*._source.deleted
- action_result.data.*._source.disable_correlation
- action_result.data.*._source.distribution
- action_result.data.*._source.domain
- action_result.data.*._source.email
- action_result.data.*._source.enrichments.language
- action_result.data.*._source.extraction_id
- action_result.data.*._source.extraction_record_id
- action_result.data.*._source.first_observed_at.date-time
- action_result.data.*._source.first_observed_at.timestamp
- action_result.data.*._source.fpid
- action_result.data.*._source.header_.indexed_at
- action_result.data.*._source.header_.ingested_at
- action_result.data.*._source.header_.observed_at
- action_result.data.*._source.header_.source
- action_result.data.*._source.header_.source_fpid
- action_result.data.*._source.header_.source_keyword
- action_result.data.*._source.id
- action_result.data.*._source.is_deleted
- action_result.data.*._source.is_fresh
- action_result.data.*._source.is_media
- action_result.data.*._source.last_observed_at.date-time
- action_result.data.*._source.last_observed_at.raw
- action_result.data.*._source.last_observed_at.timestamp
- action_result.data.*._source.level
- action_result.data.*._source.message_count.count
- action_result.data.*._source.mitre.basetypes

- action_result.data.*._source.mitre.body.enrichments.cves
- action_result.data.*._source.mitre.body.enrichments.links.*.href
- action_result.data.*._source.mitre.body.raw
- action_result.data.*._source.mitre.body.text/html-sanitized
- action_result.data.*._source.mitre.body.text/plain
- action_result.data.*._source.mitre.created_at.date-time
- action_result.data.*._source.mitre.created_at.raw
- action_result.data.*._source.mitre.created_at.timestamp
- action_result.data.*._source.mitre.fpid
- action_result.data.*._source.mitre.last_observed_at.date-time
- action_result.data.*._source.mitre.last_observed_at.raw
- action_result.data.*._source.mitre.last_observed_at.timestamp
- action_result.data.*._source.mitre.native_id
- action_result.data.*._source.mitre.phase
- action_result.data.*._source.mitre.site.base_uris
- action_result.data.*._source.mitre.site.basetypes
- action_result.data.*._source.mitre.site.created_at.date-time
- action_result.data.*._source.mitre.site.description.raw
- action_result.data.*._source.mitre.site.fpid
- action_result.data.*._source.mitre.site.site_type
- action_result.data.*._source.mitre.site.source_uri
- action_result.data.*._source.mitre.site.tags.*.name
- action_result.data.*._source.mitre.site.tags.*.parent_tag.name
- action_result.data.*._source.mitre.site.title
- action_result.data.*._source.mitre.site.updated_at.date-time
- action_result.data.*._source.mitre.status
- action_result.data.*._source.mitre.title
- action_result.data.*._source.native_id
- action_result.data.*._source.new_records
- action_result.data.*._source.num_replies
- action_result.data.*._source.object_id
- action_result.data.*._source.object_relation
- action_result.data.*._source.old_records
- action_result.data.*._source.parent_message.basetypes
- action_result.data.*._source.parent_message.fpid
- action_result.data.*._source.parent_message.native_id
- action_result.data.*._source.password
- action_result.data.*._source.password_complexity.has_lowercase

- action_result.data.*._source.password_complexity.has_number
- action_result.data.*._source.password_complexity.has_symbol
- action_result.data.*._source.password_complexity.has_uppercase
- action_result.data.*._source.password_complexity.length
- action_result.data.*._source.payment_method
- action_result.data.*._source.previous_message
- action_result.data.*._source.prices.*.currency.abbreviation
- action_result.data.*._source.prices.*.currency.raw
- action_result.data.*._source.prices.*.raw
- action_result.data.*._source.prices.*.value
- action_result.data.*._source.quantity.available.raw
- action_result.data.*._source.raw_href
- action_result.data.*._source.reputation.number_of_downvotes
- action_result.data.*._source.reputation.number_of_upvotes
- action_result.data.*._source.resource_fpid
- action_result.data.*._source.room_count.count
- action_result.data.*._source.sharing_group_id
- action_result.data.*._source.shipping.*.raw
- action_result.data.*._source.ships_from
- action_result.data.*._source.ships_to
- action_result.data.*._source.site.base_uris
- action_result.data.*._source.site.basetypes
- action_result.data.*._source.site.created_at.date-time
- action_result.data.*._source.site.description.raw
- action_result.data.*._source.site.fpid
- action_result.data.*._source.site.is_deleted
- action_result.data.*._source.site.site_type
- action_result.data.*._source.site.source_uri
- action_result.data.*._source.site.tags.*.name
- action_result.data.*._source.site.tags.*.parent_tag.name
- action_result.data.*._source.site.title
- action_result.data.*._source.site.type
- action_result.data.*._source.site.updated_at.date-time
- action_result.data.*._source.site_actor.basetypes
- action_result.data.*._source.site_actor.flair.flair_text
- action_result.data.*._source.site_actor.fpid
- action_result.data.*._source.site_actor.is_deleted
- action_result.data.*._source.site_actor.name

- action_result.data.*._source.site_actor.names.aliases
- action_result.data.*._source.site_actor.names.handle
- action_result.data.*._source.site_actor.native_id
- action_result.data.*._source.site_actor.reputation.positive_feedback
- action_result.data.*._source.site_actor.source_uri
- action_result.data.*._source.site_actor.url
- action_result.data.*._source.site_actor_count.count
- action_result.data.*._source.size.number_of_bytes
- action_result.data.*._source.size.raw
- action_result.data.*._source.source
- action_result.data.*._source.source_type
- action_result.data.*._source.source_uri
- action_result.data.*._source.syntax
- action_result.data.*._source.thread_count.count
- action_result.data.*._source.times_seen
- action_result.data.*._source.timestamp
- action_result.data.*._source.title
- action_result.data.*._source.to_ids
- action_result.data.*._source.top_domains.*.count
- action_result.data.*._source.top_domains.*.value
- action_result.data.*._source.top_passwords.*.count
- action_result.data.*._source.top_passwords.*.value
- action_result.data.*._source.total_records
- action_result.data.*._source.type
- action_result.data.*._source.unique_records
- action_result.data.*._source.unique_visits
- action_result.data.*._source.uuid
- action_result.data.*._source.value.comment
- action_result.data.*._source.value.md5
- action_result.data.*._type
- action_result.message
- action_result.parameter.limit
- action_result.parameter.query
- action_result.status
- action_result.summary
- summary.total_object_successful
- summary.total_object_successfulaction_result.status
- summary.total_objects

8. General Notes

8.1.1. Handling for 500 Internal Server Error from the Flashpoint API

Flashpoint APIs intermittently throws “500 Internal Server Error” due to some internal reasons associated with the Flashpoint server load. Hence, while executing the actions of the Flashpoint Phantom integration, there were situations where the actions failed due to the above-mentioned API error. To handle this scenario, we have implemented the below-mentioned logic.

- The action will execute as per the normal action flow.
- If the Flashpoint APIs return “500 Internal Server Error”, then, the retry API calls workflow will be executed. The retry workflow is governed by the 2 asset configuration parameters named “Retry Wait Period(in seconds)” and “Number Of Retries”. The explanation of both the parameters is provided below.

    - **Retry Wait Period(in seconds) -** The value of this parameter defines the waiting period in seconds for which to hold the current execution of the action on receiving the “500 Internal Server Error” and then, retry the same API call after the waiting period is exhausted. This ensures that the integration provides a mechanism of attempting to overcome the intermittent “500 Internal Server Error”.
    - **Number Of Retries -** The value of this parameter defines the number of attempts for which the action will keep on retrying if the Flashpoint API continuously returns the “500 Internal Server Error”. If the intermittent error gets eliminated before the number of retries gets exhausted, then, the action execution will continue along its workflow with the next set of API calls and if the intermittent error is still persistent and all the number of retries are exhausted, then, the action will fail with the latest error message being displayed.

8.1.2. Known Issues

- **Search Indicators Action**

  This action is not working with the valid value of IoC type which consists of pipe symbol(|) in its name. In case of searching the IoC of that type, you can use [run query] or [list indicators] actions by providing appropriate query in the "Query" action parameter. Below are the examples:

  I. **For “Run Query” action**
  Search for IoC value which consists of pipe symbol(|) in the IoC attribute type.

  Usage
  - Query=+basetypes:indicator_attribute+type:"<ioc_type>"+value.*:<ioc_value>

  Example
  - Query=+basetypes:indicator_attribute+type:"ip-dst|port"+value.*:5.79.68.110|80

  II. **For “List Indicators” action**
  Search for IoC value which consists of pipe symbol(|) in the IoC attribute type.

  Usage
  - Attribute Types = <ioc_type>
  - Query = +value.*:<ioc_value>

  Example
  - Attribute Types = ip-dst|port
  - Query = +value.*:"5.79.68.110|80"

- **List Indicators Action**

  I. The user will have to provide URL value in the "Attribute Types" action parameter and the URL value enclosed in double-quotes in the "Query" parameter if they want to search for an IoC having specific URL value. This does not work correctly if the user provides the URL value without double-quotes in the "Query" parameter. This is based on current API behavior of the Flashpoint.

  II. The scenario of pairing multiple IoC types (e.g. md5,url) in the action is possible. But, supporting that requires a change in the existing approved APIs that have been used in the action. Hence, the support for that scenario is not provided as a part of this project delivery.

9. Glossary

- ISO - International Organization for Standardization
- IoC - Indicator of Compromise
- IoCs - Indicator of Compromises
- SOAR - Security Orchestration, Automation, and Response
- Credential Sighting - A Credential Sighting is a single occurrence of a username/password pair.
- MISP - Malware Information Sharing Platform