ThreatQuotient

Bolster.ai CDF

Version 1.0.0

April 01, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The Bolster.ai CDF integration allows users to ingest intelligence aggregated through Bolster.ai's playbooks. Intelligence provided includes:

- **Web intelligence** - phishing, scam, and other suspicious websites.
- **Social media intelligence** - links to fraudulent social media pages/accounts.
- **App store intelligence** - potentially fraudulent apps.
- **Dark web intelligence** - leaked/compromised credentials, as well as leaked credit cards or PII.

All data is subject to how you have configured the playbooks within Bolster.ai.

The integration provides the following feed:

- **Bolster.ai Playbooks** - ingests intelligence from configured Bolster.ai Playbooks.

The feed provided ingests the following object types:

- Adversaries
- Compromised Accounts (Custom Object)
- Compromised Cards (Custom Object)
- Events
- Indicators
    - FQDNs
    - IP Addresses
    - URLs

Prerequisites

The following is required to install and run the integration:

- A Bolster.ai API Key.
- Bolster.ai Playbooks configured to output JSON data.
- The Compromised Account and Compromised Card custom objects installed on the ThreatQ instance.

Custom Objects

The integration requires the Compromised Account and Compromised Card custom objects.

Use the steps provided to install the custom objects.

> When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

ThreatQ V6 Steps

Use the following steps to install the custom object in ThreatQ v6:

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.

   > The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Navigate to the tmp folder:

   ```
   cd /var/lib/threatq/misc/
   ```

5. Upload the custom object files, including the images folder.

   The directory structure should be as the following:

   - misc
     - install.sh
     - <custom_object_name>.json
     - images (directory)
       - <custom_object_name>.svg

6. Run the following command:

   ```
   kubectl exec -it deployment/api-schedule-run -n threatq -- sh /var/
   lib/threatq/misc/install.sh /var/lib/threatq/misc
   ```

> The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

7. Delete the install.sh, definition json file, and images directory from the `misc` directory after the object has been installed as these files are no longer needed.

ThreatQ v5 Steps

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   cd /tmp/
   ```

4. Create a new directory:

   ```
   mkdir bolster_cdf
   ```

5. Upload the **json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the bolster_cdf directory.

   ```
   mkdir images
   ```

7. Upload the svgs.
8. Navigate to the **/tmp/bolster_cdf**.

   The directory should resemble the following:

   - tmp
     - **bolster_cdf**
       - **bolster.json**
       - **install.sh**
       - **images**
         - **account.svg**
         - **compromised_card.svg**

9. Run the following command to ensure that you have the proper permissions to install the custom objects:

```
chmod +x install.sh
```

10. Run the following command:

```
sudo ./install.sh
```

> You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf bolster_cdf
```

Installation

> The integration requires that the Compromised Account and Compromised Card custom objects be installed on your ThreatQ instance prior to installing the CDF. Failure to install the custom objects will result in the CDF installation process failing.

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration zip file.
3. Extract and install the required custom objects if you have not done so already.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the file on your local machine

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

The feed will be added to the integrations page. You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

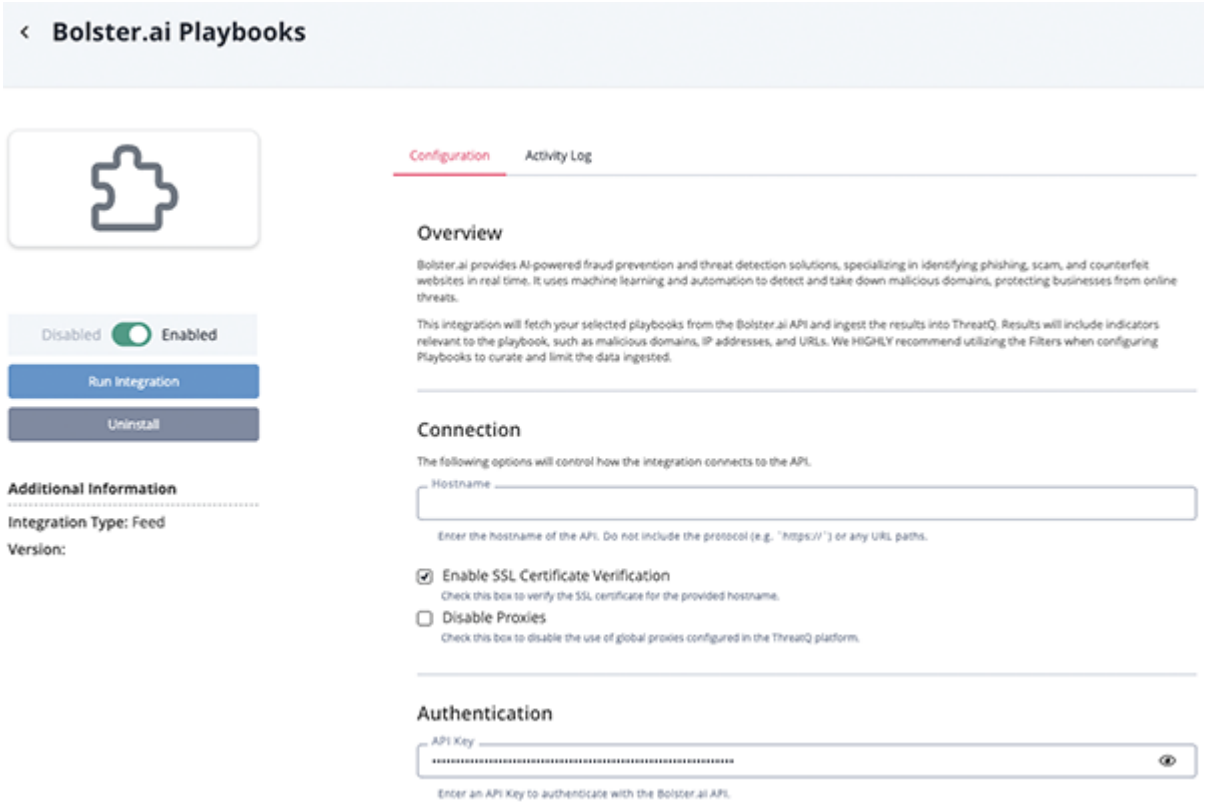
PARAMETER	DESCRIPTION
Hostname	Enter the hostname of the API. Do not include the protocol (e.g. `https://`) or any URL paths. The default setting is developers.bolster.ai.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
API Key	Enter your API Key used to authenticate with the Bolster.ai API.
Selected Playbooks	Enter a line-separated list of Playbook IDs or names to fetch from the Bolster.ai API.
Ingest Associated IP Address	Enable this parameter to ingest the IP Address associated with the source URL. This parameter is enabled by default.

PARAMETER	DESCRIPTION
Ingest Associated Domain Name	Enable this parameter to ingest the Domain Name associated with the source URL. This parameter is enabled by default.
Web Playbook Context Selection	Select which pieces of context to ingest with each result from Web Playbooks. Options include: ◦ Disposition *(default)* ◦ Risk Score *(default)* ◦ Category *(default)* ◦ Affected Brand *(default)* ◦ Country Code *(default)* ◦ Hosting Provider ◦ External Reference (Bolster.ai Insights URL) ◦ Registered At ◦ Registrant ◦ Registrar ◦ Logo Detected ◦ Takedown Requested At *(default)* ◦ Takedown Requested By *(default)* ◦ Taken Down At *(default)*
Ingest Privacy-Protected Registrant Names	Enable this parameter to ingest privacy-protected registrant names as attributes. When disabled, registrant names that are privacy-protected will not be ingested. This parameter requires that the `Registrant` option is enabled for the **Web Playbook Context Selection** parameter.
Phish Status	Assign a ThreatQ status to Web playbook objects with the Phish disposition value when the data is ingested into the ThreatQ platform. Example: selecting Active from the dropdown will result in objects with the deposition value of Phish being ingested with a status of Active in ThreatQ. The status selected here will be allied to Source URL, Domain Name, and IP Address. Options include: ◦ Active (default) ◦ Indirect ◦ Review

PARAMETER	DESCRIPTION
Scam Status	Assign a ThreatQ status to Web playbook objects with the Scam disposition value when the data is ingested into the ThreatQ platform. Example: selecting Active from the dropdown will result in objects with the deposition value of Scam being ingested with a status of Active in ThreatQ. The status selected here will be allied to Source URL, Domain Name, and IP Address. Options include: ◦ Review (default) ◦ Active ◦ Indirect
Suspicious Status	Assign a ThreatQ status to Web playbook objects with the Suspicious disposition value when the data is ingested into the ThreatQ platform. Example: selecting Active from the dropdown will result in objects with the deposition value of Suspicious being ingested with a status of Active in ThreatQ. The status selected here will be allied to Source URL, Domain Name, and IP Address. Options include: ◦ Review (default) ◦ Active ◦ Indirect
Clean Status	Assign a ThreatQ status to Web playbook objects with the Clean disposition value when the data is ingested into the ThreatQ platform. Example: selecting Active from the dropdown will result in objects with the deposition value of Clean being ingested with a status of Active in ThreatQ. The status selected here will be allied to Source URL, Domain Name, and IP Address. Options include: ◦ Review (default) ◦ Active ◦ Indirect
Dark Web Context Selection	Select which pieces of context to ingest with each result from Dark Web Playbooks. This data will be ingested as either Compromised Account or Compromised Card objects in ThreatQ. Options include: ◦ Associated Threat Actor *(default)* ◦ Data Leak Source *(default)* ◦ Risk *(default)* ◦ Status *(default)* ◦ Category *(default)* ◦ Compromised Card CVV *(default)* ◦ Expires At *(default)* ◦ Matched Search Term *(default)* ◦ Discovered At

PARAMETER	DESCRIPTION
	◦ Compromised Account Password (Plan Text) ◦ Compromised Account Password (Hash) ◦ Compromised Account Password Type ◦ Is Sensitive ◦ Victim IP Address ◦ Cryptocurrency Address ◦ Social Security Number Some fields may not be present in results depending on the type of compromised data.
Skip Entries with Down Status	Enable this parameter to skip entries with a status of DOWN. Unselect the parameter if you want to know when a social media page/group was taken down. This parameter is enabled by default.
Social Media URL Status	Select the status to apply to URLs from Social Media Playbooks. These URLs are typically links to social media platforms/profiles, and are not inherently malicious. Options include: ◦ Indirect *(default)* ◦ Review ◦ Active ◦ Whitelisted ◦ Custom
Social Media Context Selection	Select which pieces of context to ingest with each result from Social Media Playbooks. Options include: ◦ Category *(default)* ◦ Matched Search Term *(default)* ◦ Origin ◦ Platform *(default)* ◦ Status *(default)* ◦ Taken Down At *(default)* ◦ Logo Detected
App Store Context Selection	Select which pieces of context to ingest with each result from App Store Playbooks. Options include: ◦ Category *(default)* ◦ Status *(default)* ◦ Country Code *(default)* ◦ Search Term *(default)*

PARAMETER	DESCRIPTION
	◦ Listing URL *(default)* ◦ Taken Down At *(default)* ◦ App Store IP Address



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Bolster.ai Playbooks

The Bolster.ai Playbooks feed ingests intelligence from configured Bolster.ai Playbooks. Based on the selected Playbooks, ThreatQ will reach out to the Bolster.ai API and pull back the latest completed Playbook run data. The data is then mapped to ThreatQ entities and objects based on the feed configuration.

To curate and limit the amount of data being ingested into ThreatQ, make sure you configure your Bolster.ai Playbooks with the appropriate filters to only output the data that is relevant to your organization.

The initial request to the Bolster.ai API will return all of the available playbooks and their associated run history. The feed will find the selected Playbooks based on the user's configuration.

`POST https://{{ hostname }}/api/neo/v1/playbook`

Sample Response:


```
{
  "schedules": [
    {
      "id": 4453,
      "name": "Brand Impersonation - Phishing",
      "history": [
        {
          "id": 1121122,
          "resultCount": 289,
          "status": "COMPLETE",
          "createdTs": "2025-03-05T09:00:00.456Z",
          "updatedTs": "2025-03-05T09:00:07.238Z"
        },
        {
          "id": 1108511,
          "resultCount": 291,
          "status": "COMPLETE",
          "createdTs": "2025-02-26T09:00:00.624Z",
          "updatedTs": "2025-02-26T09:00:15.840Z"
        }
      ]
    }
  ]
}
```


When a Playbook match is found, the feed will then request the data for that Playbook:

`POST https://{{ hostname }}/api/neo/v1/playbook/download?historyId={{ history_id }}`

Potentially malicious indicators have been defanged in the following examples.

Web Playbook Sample


```
[
  {
    "Original Disposition": "suspicious",
    "Brand ID": "apple",
    "Last Scanned": "2025-02-25T05:05:26.320Z",
    "First Seen": "2025-02-25T05:05:26.320Z",
    "Hosting Provider": "Amazon.com, Inc.",
    "Scan Source": "Bolster",
    "TLD": "com",
    "Country": "US",
    "Logo Detected": false,
    "# Customer Scans": 0,
    "# Bolster Scans": 1,
    "Takedown Time": "",
    "IP Address": "75.2.18.233",
    "Past Phish on IP": "",
    "Past Phish on Host": "",
    "Current Disposition": "suspicious",
    "Disposition Change": "2025-02-25T05:05:26.320Z",
    "Registration Date": "2024-01-23T18:21:07.000Z",
    "Registrar": "Dynadot Inc",
    "Category": "domain_parking",
    "Insights URL": "https://platform.bolster.ai/web/insights/
1740459926320/61efcc7f60302c53b770c156703d80dd1997c2dc49a295aa9e086bf90cd0c84f"
,
    "Domain Name": "icloud-uk-map[.]com",
    "Last Updated": "2025-02-25T05:05:26.320Z",
    "Source URL": "http[://]www[.]wwww[.]icloud-uk-map[.]com/",
    "Risk": 5,
    "Registrant": "Privacy Protect, LLC (PrivacyProtect.org)",
    "MX Records": false,
    "Nameservers": "NS1.DYNA-NS.NET; NS2.DYNA-NS.NET",
    "SFB Detected": false,
    "Takedown Request Date": "",
    "Takedown Requester Email": "",
    "Tags": ""
  },
  {
    "Original Disposition": "suspicious",
    "Brand ID": "apple",
    "Last Scanned": "2025-02-25T06:27:45.039Z",
    "First Seen": "2025-02-25T06:27:45.039Z",
    "Hosting Provider": "",
    "Scan Source": "Bolster",
    "TLD": "com",
```

```
    "Country": "",
    "Logo Detected": false,
    "# Customer Scans": 0,
    "# Bolster Scans": 1,
    "Takedown Time": "",
    "IP Address": "0.0.0.0",
    "Past Phish on IP": "",
    "Past Phish on Host": "",
    "Current Disposition": "suspicious",
    "Disposition Change": "2025-02-25T06:27:45.039Z",
    "Registration Date": "",
    "Registrar": "",
    "Category": "unknown",
    "Insights URL": "https://platform.bolster.ai/web/insights/
1740464865039/738f4edfc5982e4917d85ad5b2f8e94252635832f0ef84ebd339a57ee68ac780"
,
    "Domain Name": "icloud-menager[.]com",
    "Last Updated": "2025-02-25T06:27:45.039Z",
    "Source URL": "http[://]icloud-menager[.]com/",
    "Risk": 3,
    "Registrant": "Netlify",
    "MX Records": false,
    "Nameservers": "",
    "SFB Detected": false,
    "Takedown Request Date": "",
    "Takedown Requester Email": "",
    "Tags": ""
  }
]
```


The following mapping is based on each item within the API response's array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.['Source URL']`	Indicator.Value	URL	`.['First Seen']`	N/A	URLs are normalized. Due to the normalization they can be ingested as FQDNs or IP Addresses.
`.['IP Address']`	Indicator.Value	IP Address	`.['First Seen']`	N/A	User-configurable
`.['Domain Name']`	Indicator.Value	FQDN	`.['First Seen']`	N/A	User-configurable
`.['Current Disposition']` or `.['Original Disposition']`	Attribute	Disposition	`.['First Seen']`	`Phish`	Updatable. User-configurable. `Original Disposition` is ingested only if `Current Disposition` is missing or it is empty.
`.['Brand ID']`	Attribute	Affected Brand	`.['First Seen']`	`apple`	User-configurable
`.['Hosting Provider']`	Attribute	Hosting Provider	`.['First Seen']`	`Amazon.com, Inc.`	User-configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.['Risk']`	Attribute	Risk Score	`.['First Seen']`	`3`	Updatable. User-configurable
`.['Insights URL']`	Attribute	External Reference	`.['First Seen']`	N/A	User-configurable
`.['Registration Date']`	Attribute	Registered At	`.['First Seen']`	`2024-01-23T18:21:07.000Z`	User-configurable
`.['Registrar']`	Attribute	Registrar	`.['First Seen']`	`Dynadot Inc`	User-configurable
`.['Registrant']`	Attribute	Registrant	`.['First Seen']`	Privacy Protect, LLC (PrivacyProtect.org)	User-configurable and ingested if `Ingest Privacy-Protected Registrant Names` is enabled because it contains the string `privacy`
`.['Registrant']`	Attribute	Registrant	`.['First Seen']`	Netlify	User-configurable.
`.['Takedown Request Date']`	Attribute	Takedown Requested At	`.['First Seen']`	`2025-02-25T05:05:26.320Z`	User-configurable
`.['Takedown Requester Email']`	Attribute	Takedown Requested By	`.['First Seen']`	`john.doe@gmail.com`	User-configurable
`.['Takedown Time']`	Attribute	Taken Down At	`.['First Seen']`	`2025-02-25T05:05:26.320Z`	User-configurable
`.['Logo Detected']`	Attribute	Logo Detected	`.['First Seen']`	`false`	User-configurable
`.['Category']`	Attribute	Category	`.['First Seen']`	`domain_parking`	User-configurable
`.['Country']`	Attribute	Country Code	`.['First Seen']`	`RU`	User-configurable
N/A	Attribute	Playbook Type	`.['First Seen']`	`Web`	Based on available fields
`.['Tags']`	Indicator.Tag	N/A	N/A	N/A	N/A

Social Media Sample


```
[
  {
    "URL": "https://www.facebook.com/Trainvloger/",
    "Source": "Bolster",
    "Origin": "Profile",
    "Platform": "Facebook",
    "First Seen": "2024-05-02T08:13:52.019105",
    "Logo Detection": false,
    "Category": ["Fake Advertisements"],
    "Matched Search Terms": ["apple"],
    "Tags": null,
    "Status": "SAFELIST",
    "TakeDownTime": null
  },
  {
    "URL": "https://www.facebook.com/profile.php/?id=100091727064053",
    "Source": "Bolster",
    "Origin": "Advertisement",
    "Platform": "Facebook",
    "First Seen": "2024-05-17T05:16:28.795553",
    "Logo Detection": false,
    "Category": ["Fake Advertisements"],
    "Matched Search Terms": ["jared"],
    "Tags": null,
    "Status": "LIVE",
    "TakeDownTime": null
  }
]
```


The following mapping is based on each item within the API response's array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.['URL']`	Indicator.Value	URL	`.['First Seen']`	N/A	URLs are normalized. Due to the normalization they can be ingested as FQDNs or IP Addresses.
`.['Origin']`	Attribute	Origin	`.['First Seen']`	`Profile`	User-configurable
`.['Platform']`	Attribute	Platform	`.['First Seen']`	`Facebook`	User-configurable
`.['TakeDownTime']`	Attribute	Taken Down At	`.['First Seen']`	N/A	User-configurable
`.['Logo Detection']`	Attribute	Logo Detected	`.['First Seen']`	`false`	User-configurable
`.['Status']`	Attribute	Status	`.['First Seen']`	`LIVE`	Updatable. User-configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.['Category']`	Attribute	Category	`.['First Seen']`	`Fake Advertisements`	User-configurable
`.['Tags']`	Tag	N/A	N/A	N/A	N/A
`.['Matched Search Term']`	Attribute	Matched Search Term	`.['First Seen']`	`apple`	User-configurable
N/A	Attribute	Playbook Type	`.['First Seen']`	`Social Media`	Based on available fields

APP Store Sample


```
[
  {
    "App Store": "Google Play",
    "App Name": "Sonic Forces - Running Battle - Apps on Google Play",
    "Category": "Brand Stores",
    "Status": "SAFELIST",
    "Last Scanned": "2022-09-06T21:31:10.354Z",
    "First Seen": "2022-09-06T21:31:10.354Z",
    "Scan Source": "Bolster",
    "Country": "CA",
    "Logo Detected": false,
    "Takedown Time": "",
    "IP Address": "142.251.215.238",
    "Source URL": "https://play.google.com/store/apps/details?
id=com.sega.sprint",
    "Search Term": "",
    "Tags": ["Top Priority", "Watchlist"]
  },
  {
    "App Store": "Google Play",
    "App Name": "Critical Ops: Multiplayer FPS - Apps on Google Play",
    "Category": "Brand Stores",
    "Status": "LIVE",
    "Last Scanned": "2022-09-06T22:14:43.544Z",
    "First Seen": "2022-09-06T22:14:43.544Z",
    "Scan Source": "Bolster",
    "Country": "US",
    "Logo Detected": false,
    "Takedown Time": "",
    "IP Address": "142.251.33.110",
    "Source URL": "https://play.google.com/store/apps/details?
id=com.criticalforceentertainment.criticalops",
    "Search Term": "",
    "Tags": ["Follow-Up Needed", "IP Legal Team"]
  }
]
```


The following mapping is based on each item within the API response's array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.['App Name'],.['App Store']`	Event.Title	App Store Monitoring	`.['First Seen']`	`App Alert: {{ app name }} | {{ app store }}`	N/A
`.['App Name']`	Attribute	App Name	`.['First Seen']`	`DRAGON BALL LEGENDS - Apps on Google Play`	N/A
`.['App Store']`	Attribute	App Store	`.['First Seen']`	`Google Play`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.['Search Term']`	Attribute	Search Term	`.['First Seen']`	`iCloud`	User-configurable
`.['Takedown Time']`	Attribute	Taken Down At	`.['First Seen']`	N/A	User-configurable
`.['IP Address']`	Attribute	App Store IP Address	`.['First Seen']`	N/A	User-configurable
`.['Source URL']`	Attribute	Listing URL	`.['First Seen']`	`https://play.google.com/store/apps/details?id=com.bandainamcoent.dblegends_ww`	User-configurable
`.['Status']`	Attribute	Status	`.['First Seen']`	`LIVE`	Updatable. User-configurable
`.['Country']`	Attribute	Country Code	`.['First Seen']`	`US`	User-configurable
`.['Category']`	Attribute	Category	`.['First Seen']`	Brand Stores	User-configurable
`.['Tags']`	Tag	N/A	N/A	N/A	N/A
N/A	Attribute	Playbook Type	`.['First Seen']`	`App Store`	Based on available fields

Dark Web Sample


```
[
  {
    "Last Scanned": "2025-03-04T01:39:19.860950",
    "Tags": "",
    "Email": "john.doe@outlook.com",
    "Password": "hunter2",
    "Password Type": "plain",
    "Credit Card Number": "",
    "CVV": "",
    "Expiry Date": "",
    "Title": "john.doe@outlook.com",
    "Risk": "HIGH",
    "Category": "Breach Data for Sale",
    "Status": "ACTIVE",
    "Matched Search Terms": ["intel.com"],
    "Threat Actor": "",
    "Discovery Date": "2025-03-02T02:36:04Z",
    "Sensitive Data": false,
    "Social Security Numbers": "",
    "Cryptocurrency Addresses": "",
    "IP Addresses": "",
    "Data Leak Source": "telegram"
  },
  {
    "Last Scanned": "2025-03-04T01:39:19.861226",
    "Tags": "",
    "Email": "jane.doe",
    "Password": "CHANGEME",
    "Password Type": "plain",
    "Credit Card Number": "",
    "CVV": "",
    "Expiry Date": "",
    "Title": "jane.doe",
    "Risk": "HIGH",
    "Category": "Breach Data for Sale",
    "Status": "ACTIVE",
    "Matched Search Terms": ["intel.com"],
    "Threat Actor": "",
    "Discovery Date": "2025-03-02T02:36:04Z",
    "Sensitive Data": false,
    "Social Security Numbers": "",
    "Cryptocurrency Addresses": "",
    "IP Addresses": "",
    "Data Leak Source": "telegram"
  }
]
```


The following mapping is based on each item within the API response's array.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.['Email']`	Compromised Account Value	Compromised Account	`.['Discovery Date']`	`john.doe@gmail.com`	N/A
`.['Credit Card Number']`	Compromised Card Value	Compromised Card	`.['Discovery Date']`	N/A	N/A
`.['CVV']`	Compromised Card Attribute	CVV	`.['Discovery Date']`	N/A	User-configurable
`.['Password']`	Compromised Account Attribute	Password	`.['Discovery Date']`	`hunter2`	User-configurable. If `['Password Type']` equals `plain`
`.['Password Type']`	Compromised Account Attribute	Password Type	`.['Discovery Date']`	`plain`	User-configurable
`.['Password']`	Compromised Account Attribute	Password Hash	`.['Discovery Date']`	N/A	User-configurable. If `['Password Type']` not equals `plain`
`.['Expiry Date']`	Compromised Card Attribute	Expires At	`.['Discovery Date']`	`03/24`	User-configurable
`.['Risk']`	Compromised Card/ Compromised Account Attribute	Risk	`.['Discovery Date']`	`High`	Updatable. User-configurable
`.['Category']`	Compromised Card/ Compromised Account Attribute	Category	`.['Discovery Date']`	`Breach Data for Sale`	User-configurable
`.['Status']`	Compromised Card/ Compromised Account Attribute	Status	`.['Discovery Date']`	`Active`	Updatable. User-configurable
`.['Matched Search Term']`	Compromised Card/ Compromised Account Attribute	Matched Search Term	`.['Discovery Date']`	`intel.com`	User-configurable
`.['Threat Actor']`	Related Adversary Name	Adversary	`.['Discovery Date']`	N/A	User-configurable
`.['Sensitive Data']`	Compromised Card/ Compromised Account Attribute	Is Sensitive	`.['Discovery Date']`	`false`	Updatable. User-configurable
`.['Social Security Numbers']`	Compromised Card/ Compromised Account Attribute	Social Security Number	`.['Discovery Date']`	N/A	User-configurable
`.['Cryptocurrency Addresses']`	Compromised Card/ Compromised Account Attribute	Cryptocurrency Address	`.['Discovery Date']`	N/A	User-configurable
`.['Data Leak Source']`	Compromised Card/ Compromised Account Attribute	Data Leak Source	`.['Discovery Date']`	`telegram`	User-configurable
`.['Discovery Date']`	Compromised Card/ Compromised Account Attribute	Discovered At	`.['Discovery Date']`	`telegram`	User-configurable
`.['IP Addresses']`	Compromised Card/ Compromised Account Attribute	Victim IP Address	`.['Discovery Date']`	N/A	User-configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.['Tags']`	Tag	N/A	N/A	N/A	N/A
N/A	Compromised Card/ Compromised Account Attribute	Playbook Type	`.['Discovery Date']`	`Dark Web`	Based on available fields

Average Feed Run

Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	18 minutes
Compromised Accounts	28,094
Compromised Account Attributes	195,549
Events	3
Event Attributes	21
Indicators	2,995
Indicator Attributes	17,329

Known Issues / Limitations

- For each selected Playbook, only the data from the latest completed Playbook run will be ingested. The Playbook's last updated timestamp must be within the feed's polling interval for a Playbook run to be ingested.
- To ingest historical Playbook data, use the manual feed run button to set the feed run timeframe to a date range that includes the historical data you'd like to ingest. Completed Playbooks are only held in Bolster.ai for a limited time (7 days), so not all Playbook runs may be available.
- New Indicator Custom statuses are not displayed immediately on the indicators pages and may take some time for the status to become visible.

Change Log

- **Version 1.0.0**
  - Initial release