User Guide v 1.0

Group IB Threat Intelligence guide for ThreatConnet Platform.

Table of Content:

INTRODUCTION

This document outlines the process to integrate Group IB Threat Intelligence feeds into the ThreatConnect Platform and provides details on how to efficiently use the integrated Threat Intelligence to get a specific list of Indicators of Compromise (IoCs).

Group IB Threat Intelligence is offered in the following types of feeds:

- **Compromised Data :: Accounts (ind*)**
  The Accounts section contains information on logins intercepted by malicious programs.

- **Compromised Data :: IMEI**
  This section contains information on compromised mobile devices working under the Android operating system. Like in cases of ordinary botnets, Group IB research mobile botnets and provide our clients with mobile device lists of their customers and employees' devices infected with malicious programs.

- **Human Intelligence :: Threat**

- **APT :: Threat**
  From the participation in investigations and incident response, Group IB is among the first to learn about new threats. Over the last years, analysts have received access to the most closed hacker communities, which enables team to monitor their activity and inform clients about the results of monitoring.

- **Human Intelligence :: Threat Actor**

- **APT :: Threat Actor**
  Over the years, Group IB have been accumulating various data about large APT groups, small hacker groups, and hacktivists.

- **Attacks :: DDoS**
  To detect DDoS attacks, Group IB uses sensors set up in various countries. These sensors are servers adjusted in a similar way as those used by criminals to conduct attacks via amplification, such as NTP Amplification, DNS Amplification, or incorrectly adjusted SMS systems, such as WordPress Pingback. When screening the malicious network traffic through the sensors, we can see attack targets and inform on them in real-time.
  Also, Group IB monitor botnets and control commands received by malicious programs from their control servers, and decode them, which enables Group IB to accurately detect both attack targets and the malicious program used to conduct the attack and its control server.

- **Attacks :: Deface**
  This collection contains information about the attacker, the time of the attack, and the victim.

- **Attacks :: Phishing**
  The Phishing section contains information about phishing resources detected when analyzing the network traffic through the Bot-Trek TDS sensors and notifications received by CERT-GIB, monitoring SPAM messages, malicious contextual advertising, new domain names, open sources, and partner information resources.

- **Brand Abuse :: Phishing (ind*)**
  Brand Abuse Phishing is the data that can be obtained through the Attacks :: Phishing collection filtered for the user’s company.

- **Attacks :: Phishing Kit**
  A phishing kit is a collection of pages, scripts, and graphics that allows criminals to launch and manage a phishing resource. In fact, it is a ready-to-use phishing website with a configuration file that can contain phishing page display parameters and settings

to save/send data entered by a victim on phishing resources. The attacker can configure the website to record collected information to a local file or database, or send it to an email address. The last-mentioned method is the most popular technique among hackers.
This section contains archives of phishing kits detected while reacting to incidents. Group IB automatically analyze configuration files of phishing kits to identify addresses where compromised data is sent to by the attacker.

- **Brand Abuse :: Phishing Kit (ind*)**
  Brand Abuse Phishing Kit is the data that can be obtained through the Attacks :: Phishing Kit collection filtered for the user's company.

- **Malware :: Targeted malware(ind*)**
  Every day Group IB research thousands of malicious files and participate in incidents investigations that enable us to obtain information on malicious programs targeting your company and clients. If we notice that malware has the setting file where your systems, IP addresses, domains, or external phone numbers are mentioned, you will be immediately informed by Group-IB specialists.

- **Malware :: C2**
  The collection allows you to get information about the C&C servers extracted from malicious files in the "Malware:: Targeted Malware" collection.

- **Malware :: Malware**
  It is also possible to obtain more detailed data about new Malwares.

- **OSI :: Vulnerability**
  We collect and store data about all known vulnerabilities. Within the TI&A Servers this data will help to associate threats and APTs that use the same vulnerabilities as part of their attacks.

- **Suspicious IP :: Tor Node**
  The last Tor server in a proxy chain is called an exit node. The exit node serves as an intermediate link between a client of the Tor network and the public Internet.

- **Suspicious IP :: Open Proxy**
  Group-IB analysts constantly monitor the Web to detect servers configured as an open proxy. These lists are widely distributed on various resources devoted to browsing the Internet anonymously. There are public access proxy servers on the Internet that are intentionally open to the general public as well as those that are unintentionally left open because of misconfiguration or infection with malware. We collect lists of such servers by analyzing numerous resources that are popular among hackers.

- **Suspicious IP :: Socks Proxy**
  This section contains addresses where a malicious program was installed to run a SOCKS proxy on the computer. Such machines are leased and used in various attacks to provide the hacker with the highest level of anonymity.

Using this integration, this data becomes usable within the ThreatConnect Platform as part of security activities.

> **Note:** Individual collections depend on the data provided by the customer. For example, clients provide a list of their domains. The list of specified domains is used to search logins, passwords, and malicious programs related to your company. If hackers get a password from the account in a domain that is not included in this list, you will not be notified of this incident.

2. Configuration

The following section provides details on how to configure Group IB Threat Intelligence app developed for the ThreatConnect Platform, as a job to download and ingest IoCs from Group IB threat feeds into the platform.

2.1. Requirement

This integration supports the ThreatConnect Feed Deployer that can perform these tasks for you. These steps are only required if you are not using Feed Deployer.

To deploy integration in your ThreatConnect Platform instance, the following are required:

1. Group IB Threat Intelligence account.
2. At least one ThreatConnect Platform API user.
3. ThreatConnect Platform instance IP addresses whitelisted by Group IB.

> **Note:** system access through Web or API interface is allowed only for the IPs that have been whitelisted. All IP addresses of your company, indicated in the system access form, will be added to the Allow list and can be seen in Group IB account settings.

4. **Group IB Threat Intelligence** API Key to authenticate requests to Group IB Threat Intelligence platform.
5. **Group IB Threat Intelligence** app installed in ThreatConnect Platform.

6. **Group IB Threat Intelligence** attributes properly configured in your ThreatConnect Platform.

2.2. ThreatConnect Platform Job configuration

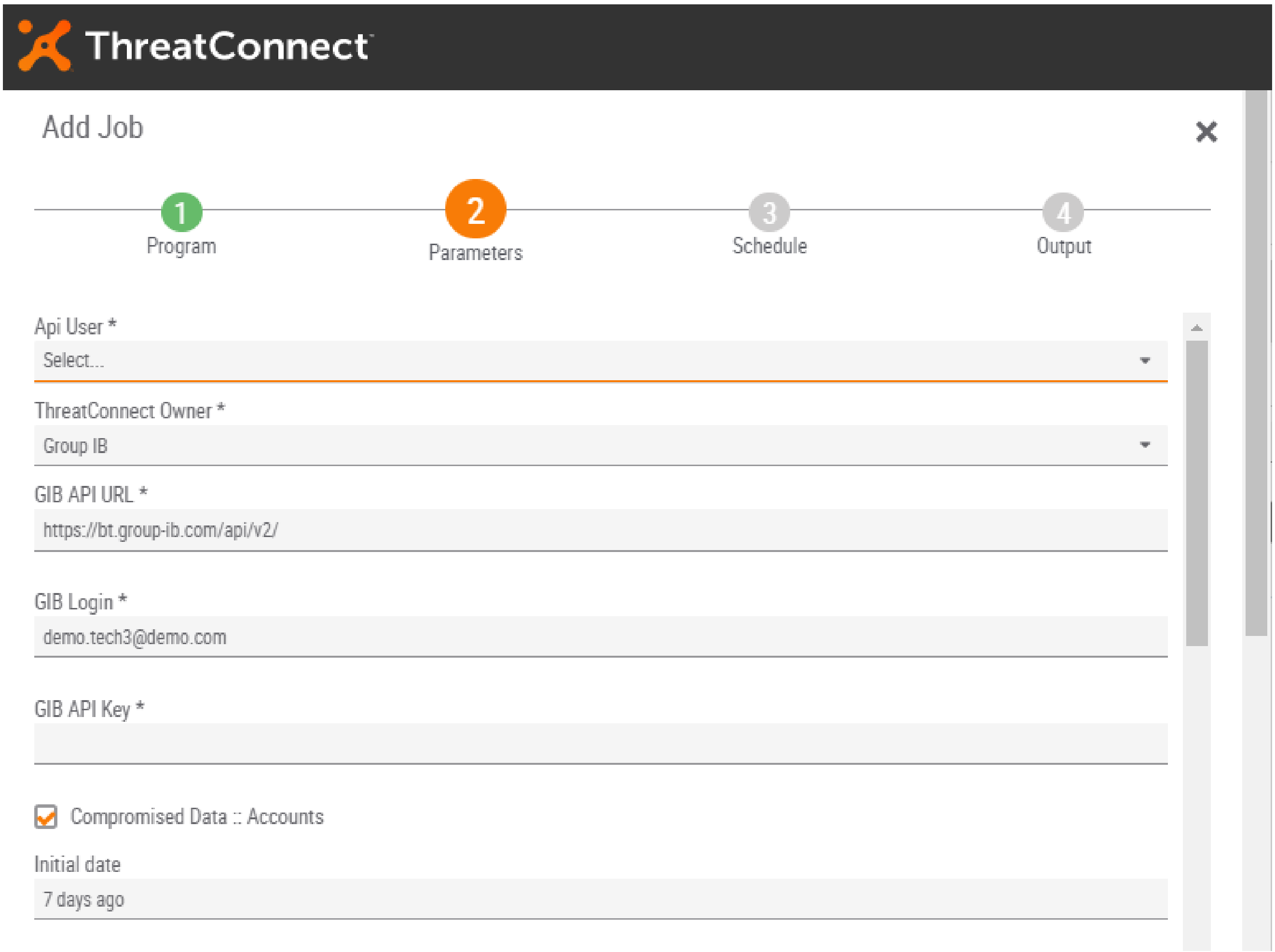
The ThreatConnect Platform provides the ability for customers to schedule applications as jobs, specifically known as Job apps, that can be run at configured intervals.
Job configuration can be found in the **Apps** tab in the **Org Setting**.

- **Program**
  In the Add Job panel, choose a suitable name for your Job in the Job Name option. Also, select **Group IB Threat Intelligence** from the Run Program drop-down list and click **Next**.

- **Parameters**

  - GIB API URL (https://bt.group-ib.com/api/v2/)
  - GIB Login - Login, which is used to enter the portal.
  - GIB API Key - API Key generated in your account
  - Collection:: collection - set to true to obtain feeds from this collection.
  - Initial date - date to get data from, used only in the first run. So, specifying “2020-01-01” or “7 days ago”, all compromised accounts starting from this date will be uploaded to the system. Further launches will upload data that has appeared in the Group IB TI since the last launch of the TC Job.

> **NOTE:** Do not use the too big interval between **initial date** and current date for some collections, especially for the “Suspicious IPs” section, uploading will take a very long time, and data that is too old may be out of date. We recommend setting the value to no more than 7 days ago, but for the “APT:: Threat Actor” and “HI:: Threat Actor” collections it is better to set this value for about 3-6 years ago. If it is necessary to get as much **threat** data from **threat** collections as possible, set this parameter to **7 years ago**. The description of the collections in the introduction will help to understand what value to assign to this parameter.



Api User *
Select...

ThreatConnect Owner *
Group IB

GIB API URL *
https://bt.group-ib.com/api/v2/

GIB Login *
demo.tech3@demo.com

GIB API Key *

☑ Compromised Data :: Accounts

Initial date
7 days ago

- **Schedule**
  We recommend executing a job every hour daily, for best syncing with the latest feed.

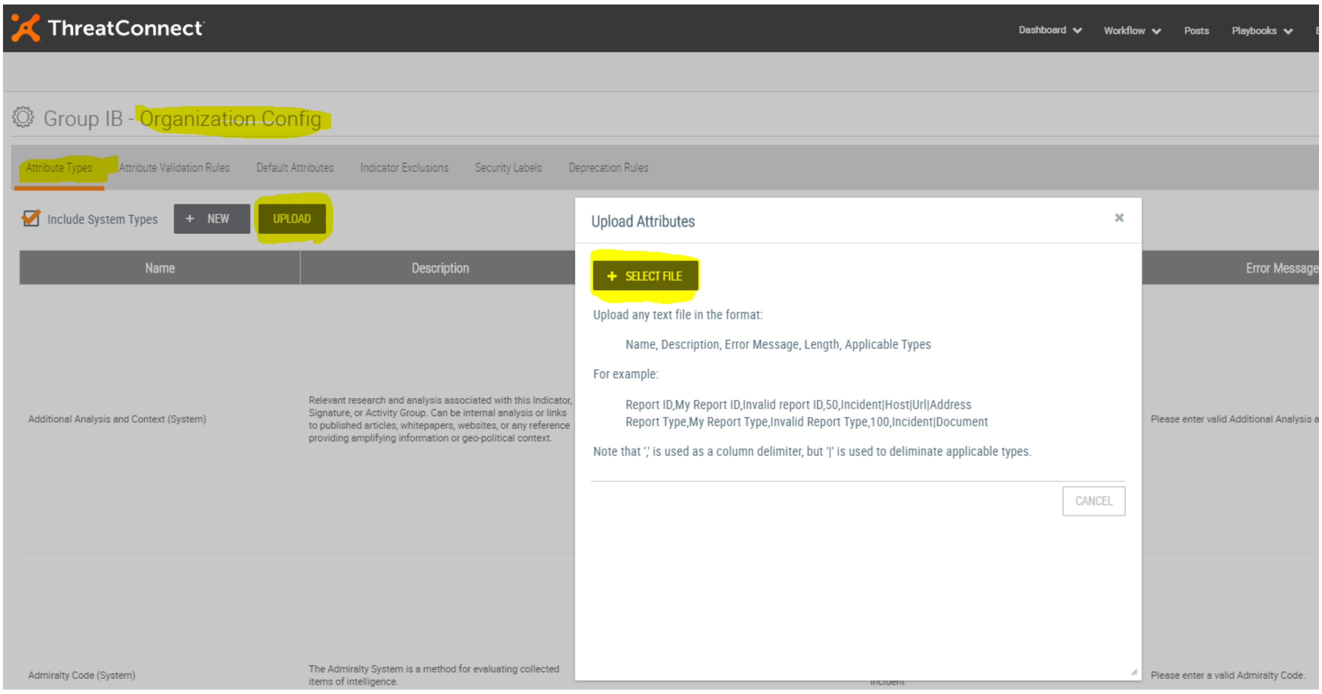
- **Output**
  Optionally, you can check the Enable Notifications checkbox to enable email notifications upon completion of the Job and provide the receiving Email Address. Under the Notify on Job Result option, check all the required scenarios at which email notifications are desired to be received. Also, click on Include Log Files checkbox under the Attachments option to receive job execution logs as attachments in the email notifications.

2.3. Attributes configuration

> **NOTE:** Note This step is not required for customers who use Feed Deployer as it is automatically performed by the Feed Deployer Wizard.

Since not all the integration attributes are presented in the system, it is necessary to configure custom attributes.

Go to **Org Config** -> **Attribute Types**, and upload the file attributes.json (present in the Github Repository), that contains the configuration metadata of the required attributes.



Upload Attributes

Upload any text file in the format:

Name, Description, Error Message, Length, Applicable Types

For example:

Report ID,My Report ID,Invalid report ID,50,Incident|Host|Url|Address
Report Type,My Report Type,Invalid Report Type,100,Incident|Document

Note that ',' is used as a column delimiter, but '|' is used to deliminate applicable types.

Name	Description	Error Message
Additional Analysis and Context (System)	Relevant research and analysis associated with this Indicator, Signature, or Activity Group. Can be internal analysis or links to published articles, whitepapers, websites, or any reference providing amplifying information or geo-political context.	Please enter valid Additional Analysis a
Admiralty Code (System)	The Admiralty System is a method for evaluating collected items of intelligence.	Please enter a valid Admiralty Code.

3. Indicator Deprecation configuration

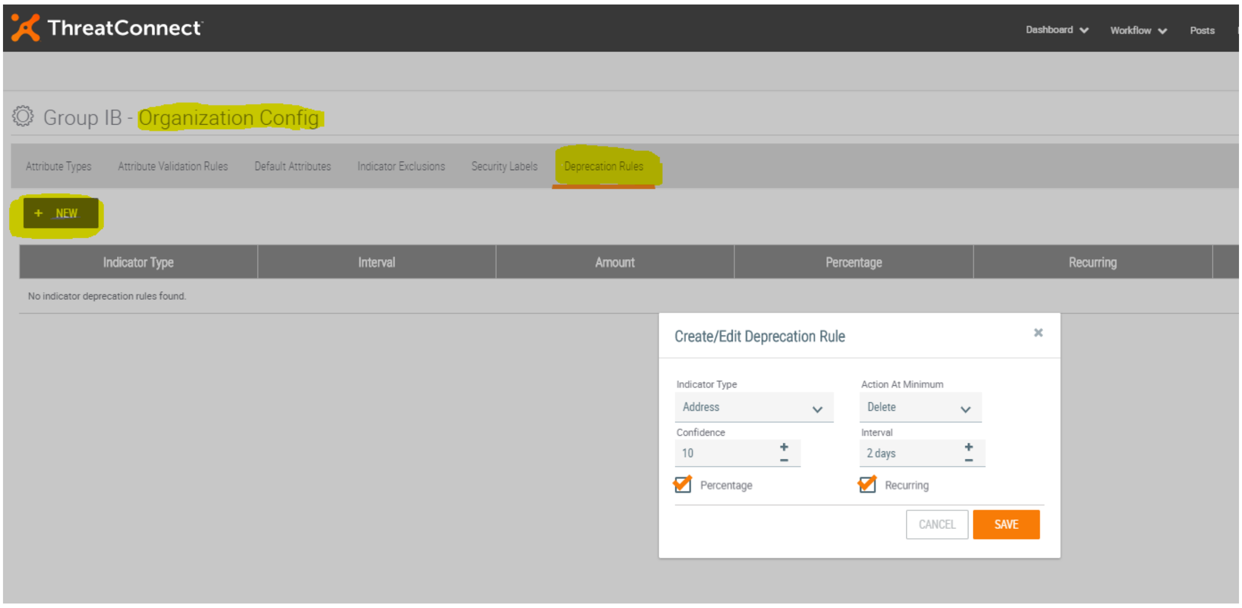
From time to time, Group IB Threat Intelligence retires indicators in its threat feed that it estimates are, no longer malicious and pose any significant threat.

These indicators previously ingested into the ThreatConnect Platform should also be deleted accordingly to avoid false-positives. ThreatConnect Platform provides the ability for users to configure an indicator deprecation policy to allow ThreatConnect Platform indicators to drop in confidence rating if their confidence rating is not being maintained and updated. Once the indicator rating reaches a minimum value (i.e. 0%), it can either be set to inactive or delete. To configure an indicator deprecation policy depending upon the type of your ThreatConnect Platform, please refer to the detailed knowledge-base article from ThreatConnect Platform: CONFIGURING INDICATOR CONFIDENCE DEPRECATION (See section Configuring Indicator Confidence Deprecation for an Organization and Configuring Indicator Confidence Deprecation for a Community or Source)

The recommended indicator deprecation rule settings for Group IB feeds:

- **Action at Minimum** selected to be Delete so that indicators are deleted as soon as they reach minimum confidence.
- **Percentage** checkbox unchecked which means that indicator confidence won't be dropped as a percent of its previous value.

- **Confidence** amount set to 33 so that 33 points of an indicator's confidence will be dropped.
- **Interval** value set to 2 days which is the period after which the confidence will be dropped.
- **Recurring** check this box for the deprecation rule to be applied on a recurring basis.



Indicator Type	Interval	Amount	Percentage	Recurring

No indicator deprecation rules found.

Create/Edit Deprecation Rule

Indicator Type: Address

Action At Minimum: Delete

Confidence: 10

Interval: 2 days

☑ Percentage

☑ Recurring

However, these are just recommendations.

4. Data filtering

All data received from a particular collection is marked with special tags. The table below displays the mapping of Group IB collections into Groups and Indicators presented in ThreatConnect Platform.

GIB Collection	TC Data type	Tag
Compromised Data :: Accounts	Report, URL, Address	compromised data/account
Compromised Data :: IMEI	Report, URL, Address, IMEI	compromised data/imei
Human Intelligence :: Threat	Campaign, File, Host, Address, URL	hi/threat
Human Intelligence :: Threat Actor	Threat	hi/threat actor
Attacks :: DDoS	Incident, Host	attacks/ddos

GIB Collection	TC Data type	Tag
Attacks :: Deface	Report	attacks/phishing
Attacks :: Phishing	Incident, Address, URL, Host	attacks/phishing kit
Attacks :: Phishing Kit	Incident, URL, E-mail	attacks/deface
OSI :: Vulnerability	Report	osi/vulnerability
Suspicious IP :: Tor Node	Address	tor node
Suspicious IP :: Open Proxy	Address	open proxy
Suspicious IP :: Socks Proxy	Address	socks proxy
Malware :: Targeted malware	Incident, File, Address	targted malware
Malware :: Malware	Report	malware
Malware :: C2	URL, Address, Host	malware/cnc
APT :: Threat	Campaign, File, Host, Address, URL	apt/threat actor
APT :: Threat Actor	Threat	apt/threat
Brand Abuse :: Phishing	Incident, Address, Host	bp/phishing
Brand Abuse :: Phishing Kit	Incident, Address, Host	bp/phishing kit

All C&C servers are marked with the CNC tag.
All the tags can be used in data filtering.

5. Support

Development, updating and support of this integration is carried out by the Group IB Team.
In case of any problems, contact the developer: i.ovchinnikov@group-ib.com