IntelFinder

# IntelFinder Integration Guide with ThreatConnect Platform

User Guide v1.0

## Introduction

This document outlines the process of integrating IntelFinder with the ThreatConnect platform.

The document is intended for organizations with a ThreatConnect deployment, as well as access (via subscription or trial) to the IntelFinder (https://intelfinder.io) threat intelligence service.

The IntelFinder Integration playbook *IntelFinder – Receive Alerts* and *IntelFinder Alert Processing* ThreatConnect app enable users to receive IntelFinder alerts as ThreatConnect reports.

## 1. Configuration

### 1.1 Requirement

The following requirements must be met to integrate IntelFinder with ThreatConnect:

- Access to ThreatConnect Playbooks functionality
- ThreatConnect paid subscription
- IntelFinder paid subscription or trial

### 1.2 Integration Setup

The IntelFinder integration consists of two elements:

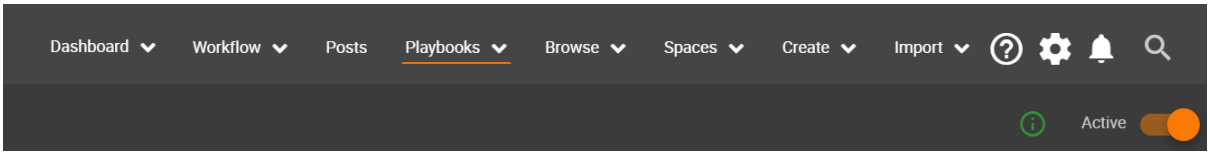
- **App** – IntelFinder Alert Processing

#### Playbook – *IntelFinder – Receive Alerts*

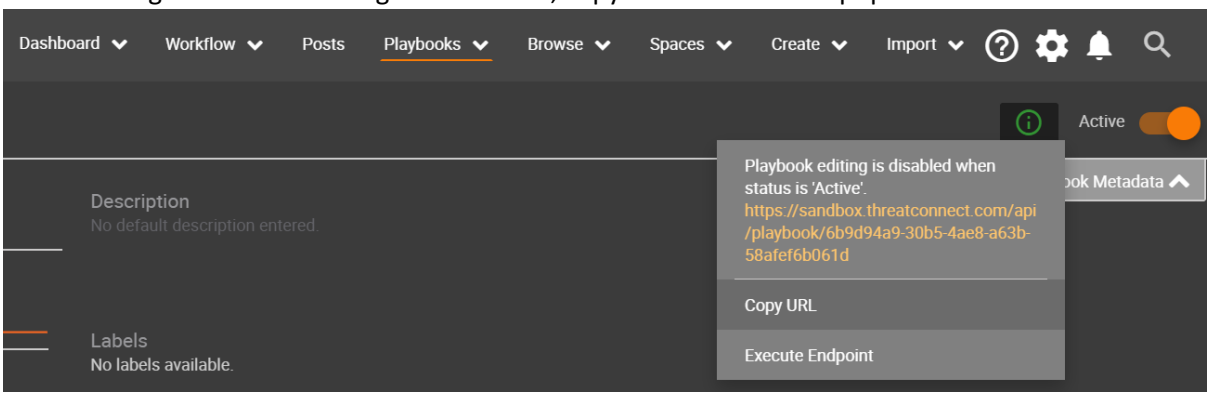
#### IntelFinder Integration Installation on ThreatConnect

In order to make use of this integration, you must install both a Playbooks App and the Playbook Template itself. Both of these elements are available on the ThreatConnect GitHub.

1. To install the IntelFinder Alert Processing Playbook app, download the TCX file from GitHub and refer to the ThreatConnect System Administration Guide (Install an App). For more information, contact your ThreatConnect Customer Success representatives.
2. To install the IntelFinder – Receive Alerts Playbook template, download the PBX file from GitHub, visit the Playbooks tab within the ThreatConnect Platform. Select New > Import and locate the PBX file you wish to add to your system. Follow the on-screen instructions to complete the import.
3. To activate the Playbook and obtain the webhook URL, click on the “IntelFinder – Receive Alerts” playbook. Click on the **Active** button to enable the playbook:




4. Click on the green icon to the right of “Active”, copy the URL from the pop-over



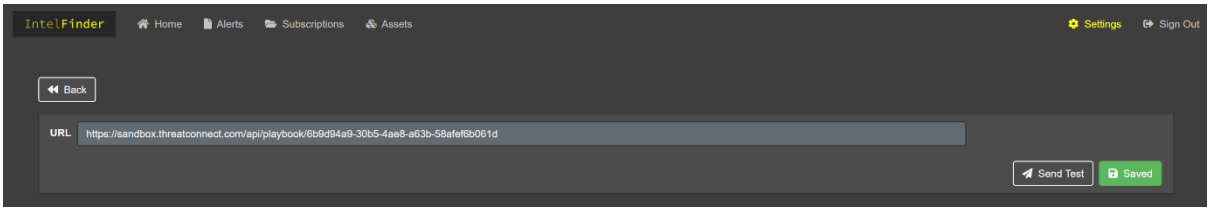

## IntelFinder Setup

To set up the integration on IntelFinder’s end:

1. Go to https://dash.intelfinder.io/
2. Log into the service
3. Click on **Settings** at the top right of the screen
4. Select **Integrations** in the pop-over

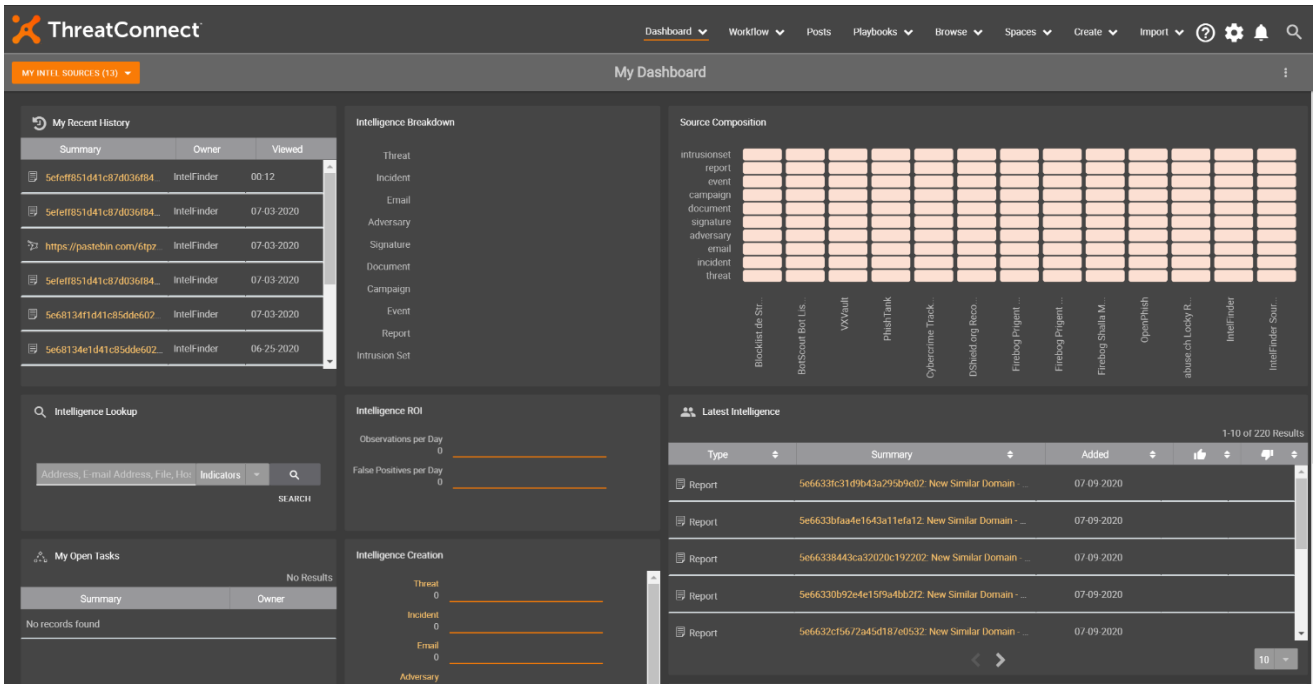

5. Click on **Webhooks**

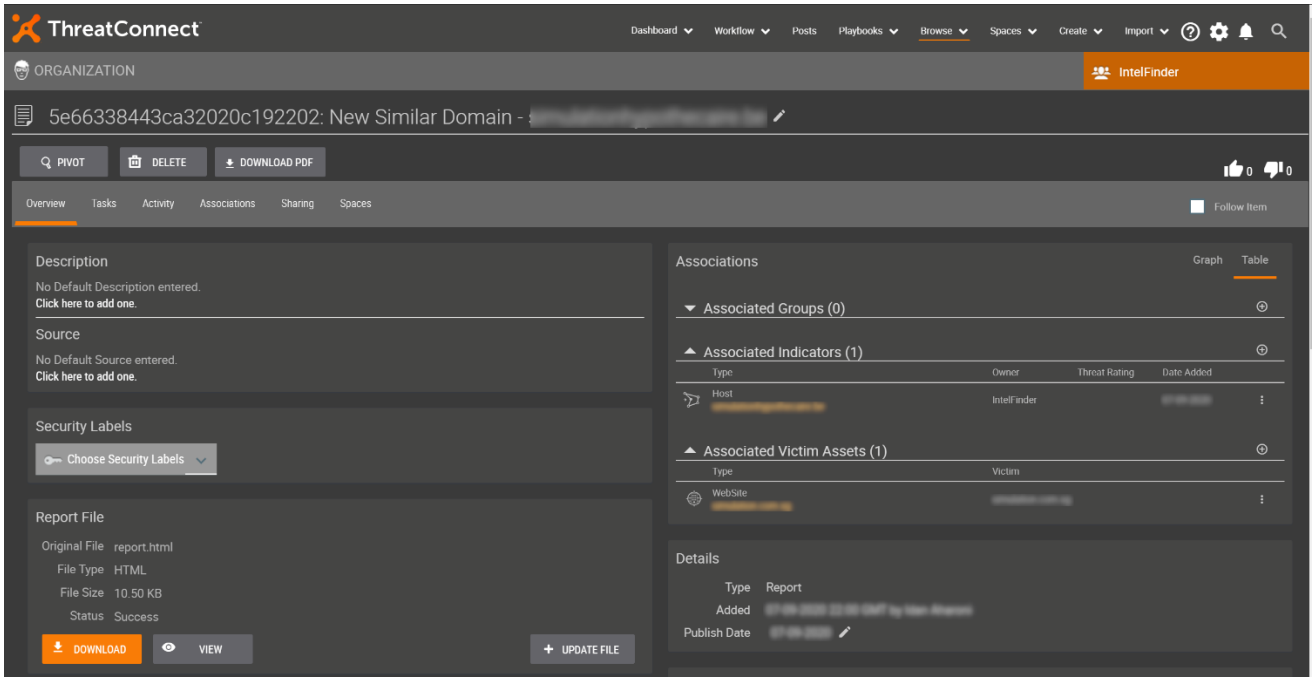

6. Paste the URL copied from the playbook on step 4 in the above instructions into the “URL” field
7. Click **Save**



## 1.3 Integration Notes

- Once the integration has been set up, IntelFinder will send all existing alerts to ThreatConnect for report generation, unless Webhooks have been previously configured for your account. In such a case, if you wish to receive all existing alerts, please contact IntelFinder support to reset the Webhooks.
- New alerts will be added as reports on ThreatConnect:




- IntelFinder alerts appearing on the ThreatConnect platform may receive a separate priority than the one set by IntelFinder.

- Failure to push information by IntelFinder to the ThreatConnect URL will result in retry attempts until successful.
- Technical differences between the ThreatConnect and IntelFinder platforms may limit certain alerts from being fully or successfully integrated. It is recommended to keep track of IntelFinder alert notifications from time to time in order to find any discrepancies.
- **NOTE:** The IntelFinder-provided Playbook should be set to **Low** priority and should not have the trigger looped-back to wait for a response. The IntelFinder service requires near-immediate acknowledgement for webhook requests.

## 2. Support

For assistance with the integration, to report a bug, or a feature request, please contact us at **contact@intelfinder.io**, or open a support ticket on the IntelFinder dashboard.