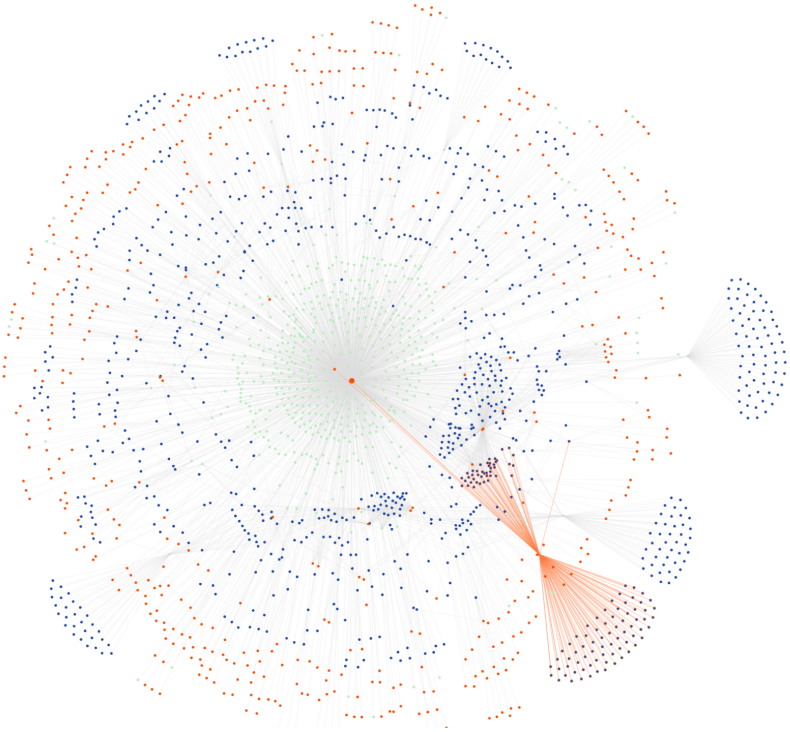
ThreatConnect – Bayse Early Alert Integration User Guide

v1.0.0



1. Introduction

This integration enables users to ingest, correlate, and cluster Bayse Intelligence's real-time phishing intelligence feed (known as Bayse Early Alert – additional details here) into ThreatConnect. The phishing intelligence is produced by performing a deep analysis of links (using Bayse's automated URL sandbox) we discover from a variety of individual and aggregated sources across the world. This integration is powerful for a number of user personas (from sophisticated CTI teams through brands with external customers) and provides considerable innovation backed by Bayse's Site Fingerprints functionality. Moreover, each individual indicator has a link back to Bayse's URL sandbox to view a screenshot and full human-readable explanation of why Bayse decided the link was phishing.

2. Changelog

App Version	Release Date	Details
1.0.0	11/15/2023	First version of app

3. Data Mapping

The table below documents the data mapping from fields associated with Bayse Intelligence's Bayse Early Alert intelligence feed (API docs here) and ThreatConnect's fields. Note that several of these fields are described in more detail later in this document.

Bayse Field	ThreatConnect Field	Possible Value	Notes
url	Indicator of type URL, tagged with **Submitted Link**	A valid URL	If the URL is too long or contains characters ThreatConnect does not support, the value **_TRUNCATED** is appended.
final_url	Indicator of type URL, tagged with **Phishing Portal**	A valid URL	If the URL is too long or contains characters ThreatConnect does not support, the value **_TRUNCATED** is appended.
following_activity	Indicator of type URL, tagged with **Credential**	A valid URL	If the URL is too long or contains characters

	Collection		ThreatConnect does not support, the value **_TRUNCATED** is appended.
ui_link	Additional Analysis and Context attribute added to potentially any URL indicators	Link within Markdown	Links back to Bayse Intelligence's UI for deeper investigation.
site_fingerprints	Tag values added to **Phishing Portal** Indicators	Specific type of Site Fingerprint followed by a hash value	Details about Site Fingerprints can be found in Bayse's introductory blog post.
identified_brands	Tag values added to **Phishing Portal** Indicators and **Campaign** Groups	Text string	Brands (as named within Bayse) associated with this attack
identified_verticals	Tag values added to **Phishing Portal** Indicators and **Campaign** Groups	Text string	Industry Sectors from STIX v2.1 (table here)
IOCs	Relevant **Campaign** Group (when IOC is a Bayse IOC)	Text string	Campaign Grouping is described in more detail later in this document.
TLS Info	Tag values added to **Phishing Portal**	TLS certificate field type followed by data as a text string	Most commonly-analyzed attributes are extracted.
IP Mappings	Tag values added to potentially any URL indicators	"Host IP:" followed by IPv4 or IPV6 address	IP lookup occurs when the site is identified as malicious.

4. Configuration Requirements

In order to successfully install and configure the Bayse app described in the following few sections, you will need:

1. Access to a ThreatConnect Platform Instance
2. At least one ThreatConnect API user
3. A free or paid account from Bayse Intelligence with a valid API key. If you do not have an account, please follow the *Creating an Account* instructions shown here to register.

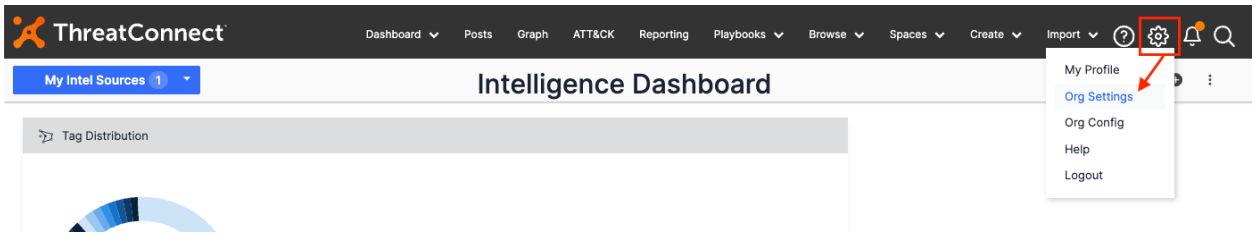
5. Job App Installation

For download and installation instructions, please refer to the ThreatConnect System Administration Guide (*Install an App*). The Bayse app is available on GitHub here. For more information, please contact your ThreatConnect Customer Success representative.

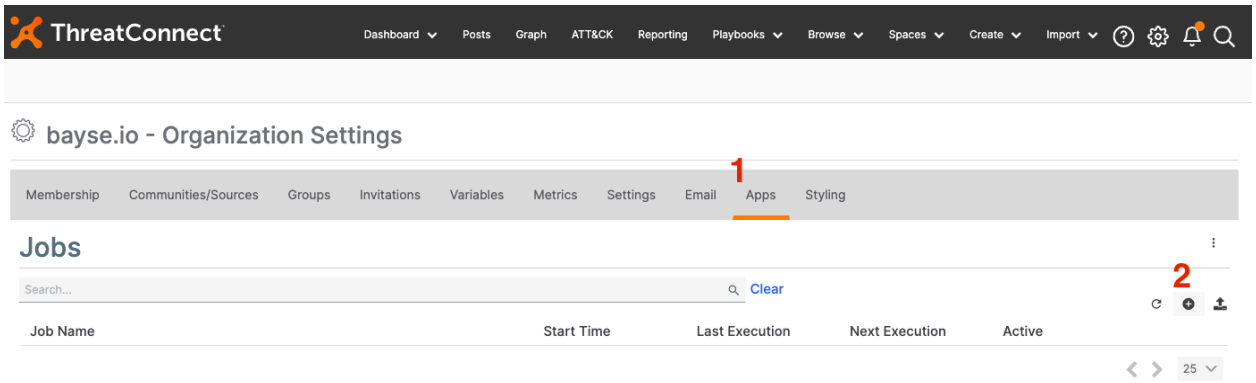
6. ThreatConnect Job Configuration

ThreatConnect allows customers to schedule applications as jobs (known as job apps) that can be run at configured intervals. Bayse has developed a Job app (referenced above) for ThreatConnect customers that is named *Bayse Early Alert Intelligence Feed*. This app handles the process of downloading, ingesting, and correlating Bayse's phishing intelligence feed in the ThreatConnect platform. In order to configure the Bayse job, follow the steps below.

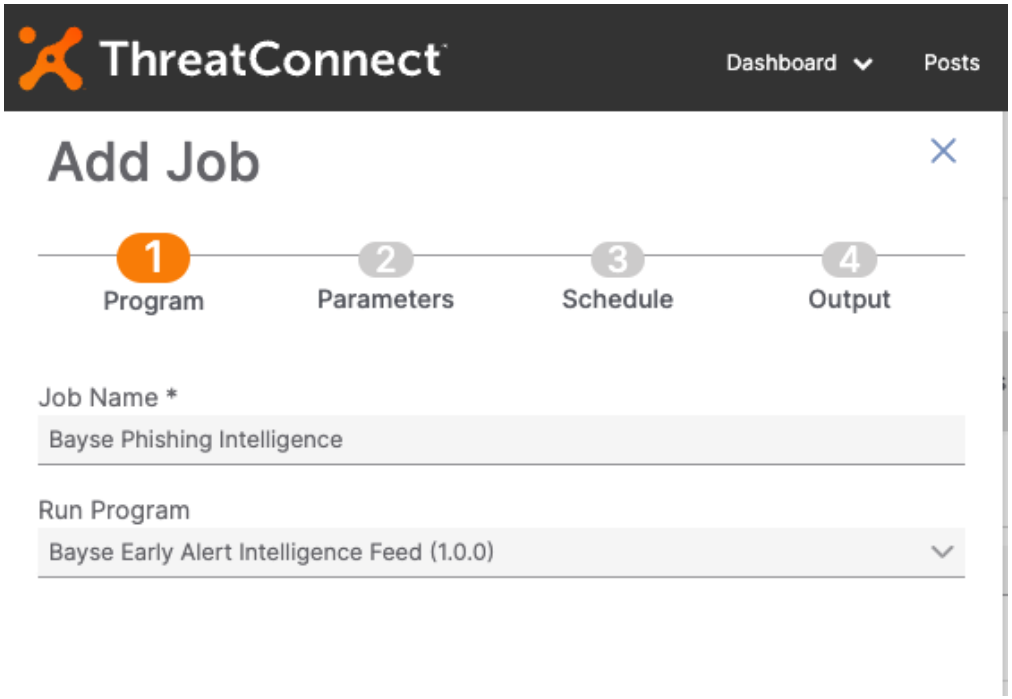
1. In the ThreatConnect console, click the gear icon on the top menu bar and select *Org Settings* from the dropdown list.



2. Select the *Apps* tab and click on ⊕ to add a new job.

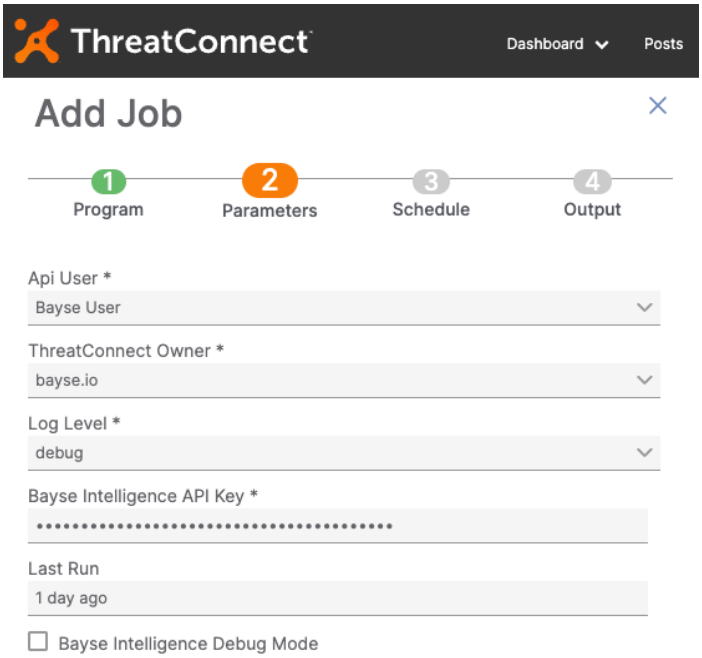


3. In the *Add Job* panel, create an identifiable name for your Job in the *Job Name* field. Select **Bayse Early Alert Intelligence Feed** from the *Run Program* drop-down list, then click *Next*.

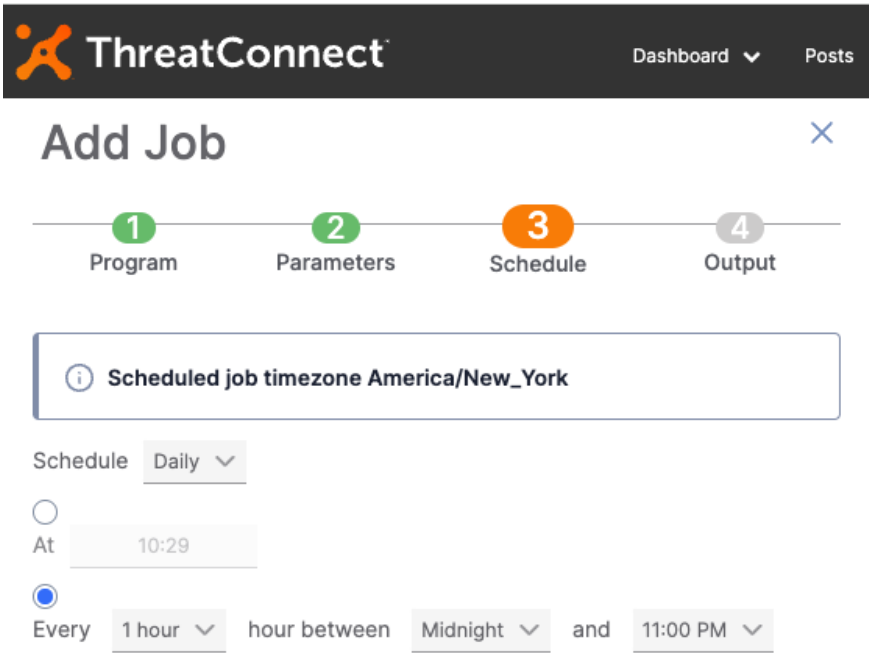


4. **NOTE:** If you already have an API Key for Bayse Intelligence, you can proceed at this point. If not, please follow the *Creating an Account* instructions shown here to request one.

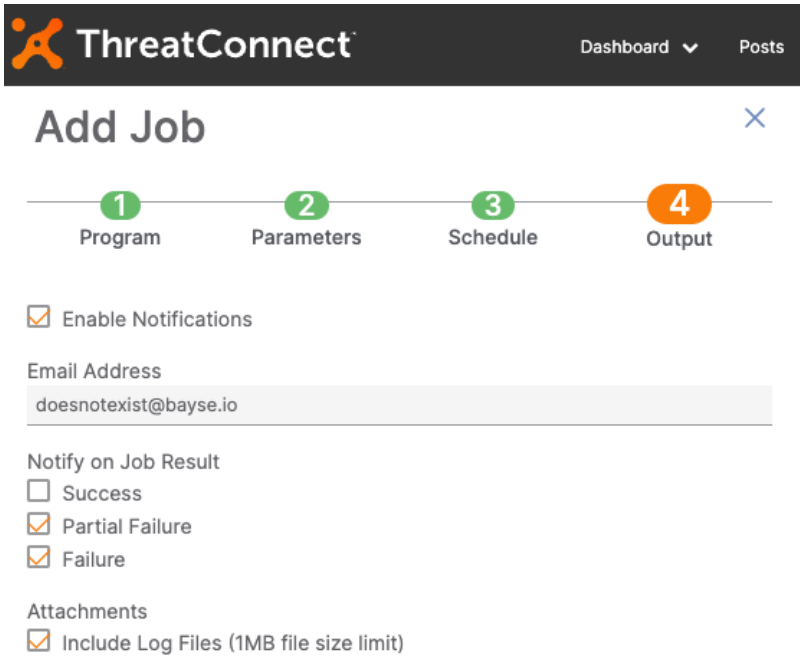
5. On the *Parameters* page, configure the Job as follows (replacing *ThreatConnect Owner* with your own organization's value). If you would like to debug any potential issues, please check the *Bayse Intelligence Debug Mode* box. Click *Next* to continue configuration.



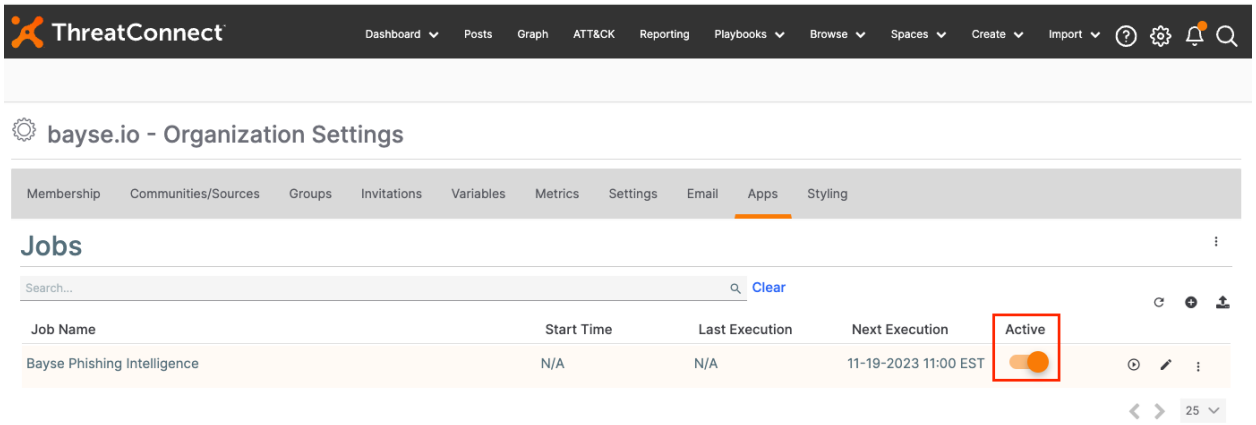
6. On the *Schedule* page, we recommend that you schedule your app to fetch new Indicators **every hour** in order to have the most up-to-date information from our real-time phishing feed. Click *Next* to continue.



7. Set up the *Output* you desire based on your internal processes and documentation requirements. Click on the *Save* button to finish configuration.



8. At this point, the job is configured but **not yet active**! In order to activate the job, toggle the *Active* slider on in order to complete your setup. Note that the first run (which will collect and correlate the last day's intelligence) may take 30 or more minutes to complete, depending on the volume of Indicators.

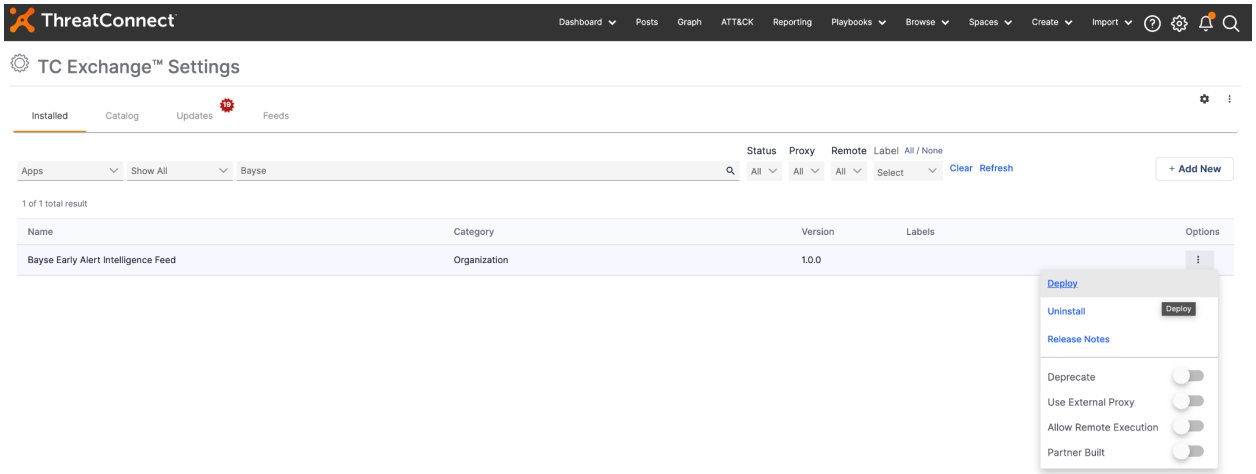


9. If you encounter any issues while running the app, please reach out to Bayse by emailing support@bayse.io.

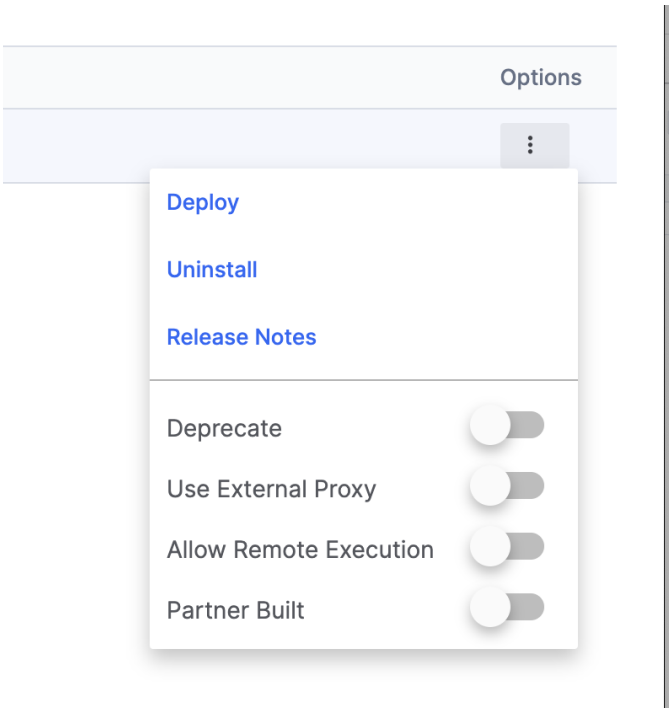
7. Feed Deployer Instructions

For users that want an easy experience with deploying the Bayse Early Alert Intelligence Feed, follow these steps below.

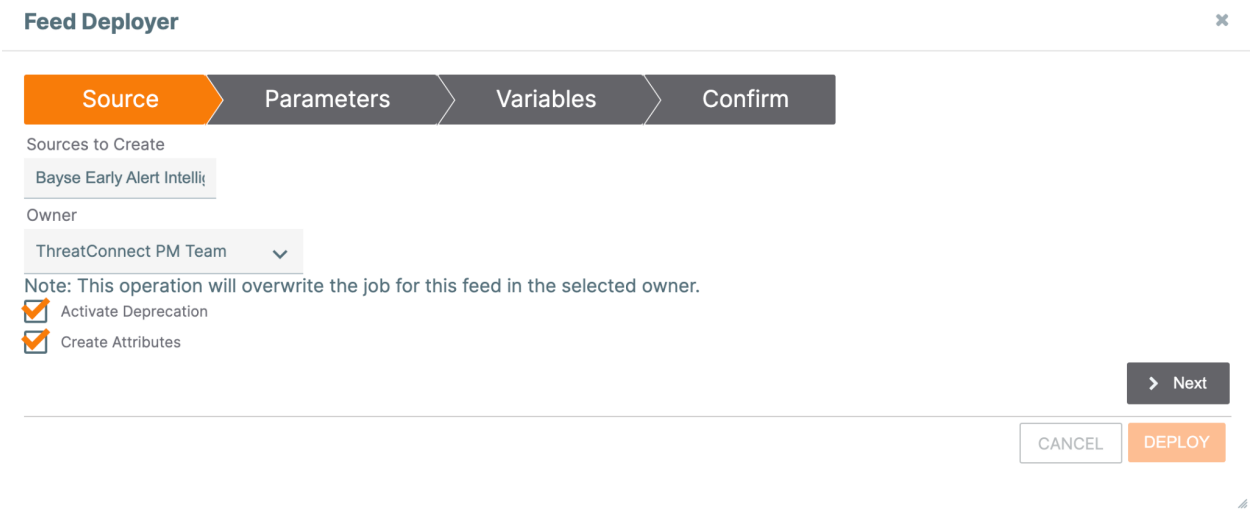
1. Navigate to the TC Exchange Settings area of the ThreatConnect Platform and go to the *Installed* tab. Filter by Apps and type in Bayse in the search bar.



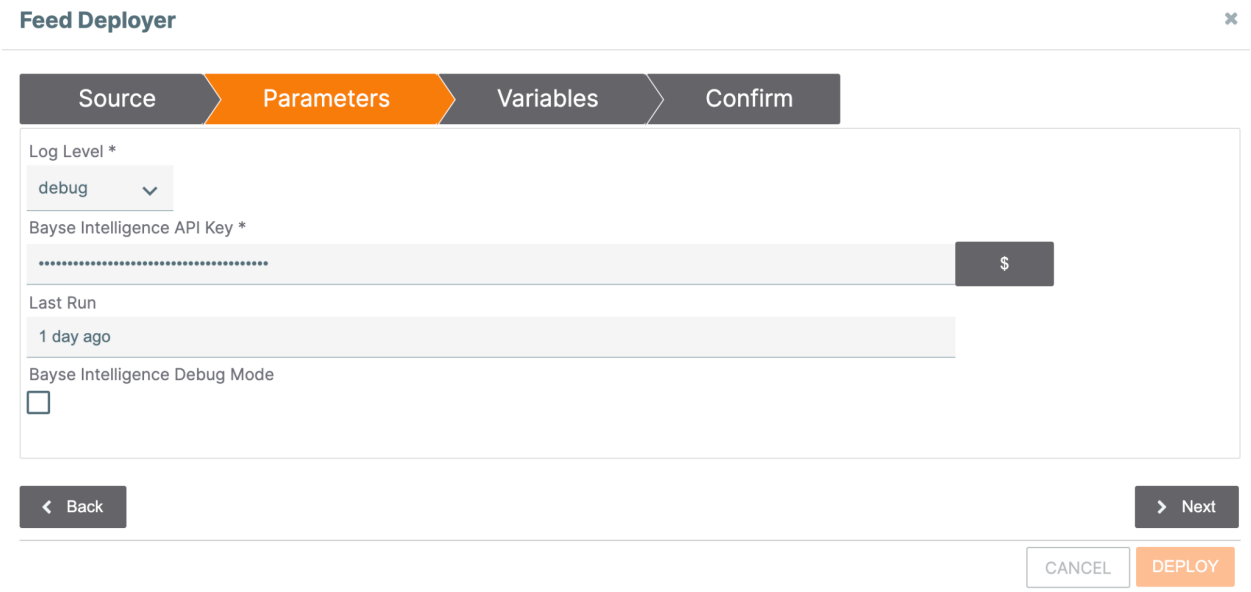
2. Click on the ⋮ under *Options* on the right side and select *Deploy*.



3. The first page of the feed deployer menu will show up. The *Sources to Create* section will populate automatically with **Bayse Early Alert Intelligence**. For the *Owner* section, choose the organization that the source will be created in.



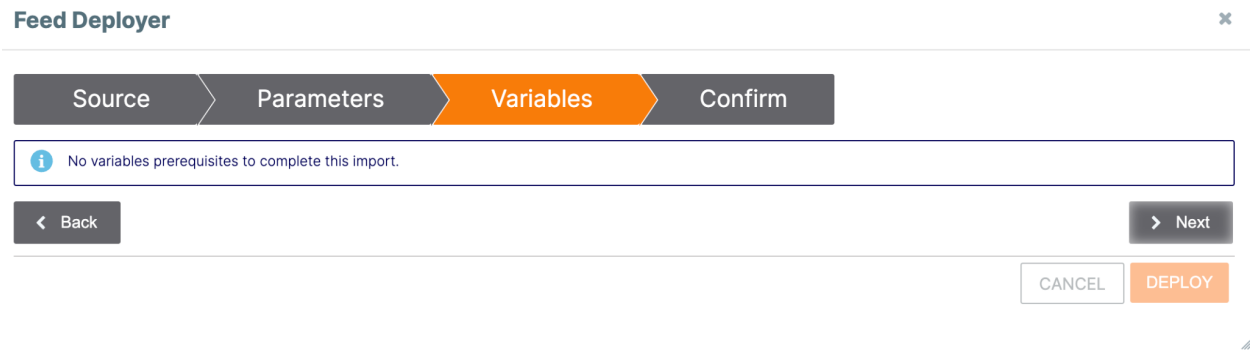
4. Click *Next* to advance to the Parameters Tab.



5. The following Parameters need to be filled in or selected:
    a. Log Level
        i. This determines what level and how much debug output will be presented in the app logs.
    b. Bayse Intelligence API Key
        i. This is the required API key that needs to be used to get data from the Bayse. If you do not already have an API key for Bayse, please follow the *Creating an Account* instructions shown here to request one.
    c. Last Run
        i. This is an auto-populated field and will always be set to **1 day ago** for now.
    d. Bayse Intelligence Debug Mode
        i. This is an optional mode that can be used if the feed does not complete and can be used to debug the feed.

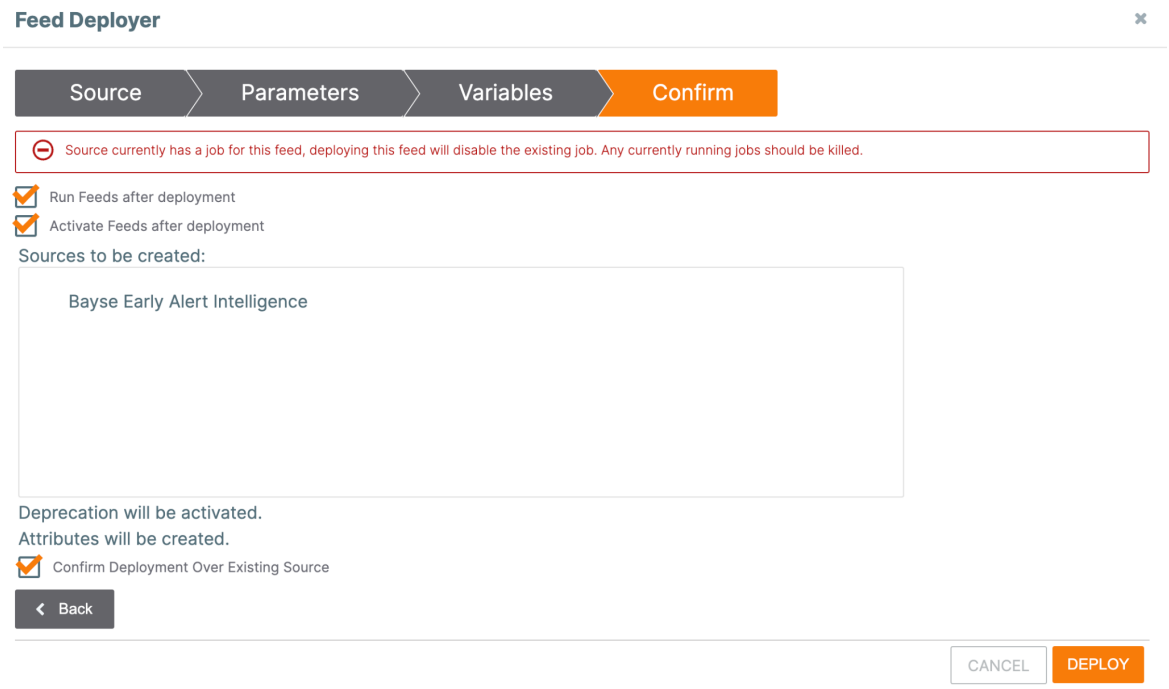
6. Click *Next* once the parameters have been filled in.

7. Click *Next* on the variable tab, as there are no variables to fill in.



8. Once on the *Confirm* tab, click the *Deploy* button to deploy the feed.

9. If the feed has already been deployed on the system in the same org, an error such as below will show up. Select the "**Confirm Deployment Over Existing Source**" checkbox to redeploy the job and deactivate the previous feed deployer job.



10. Once deployed, a job should show up by the name of "**Bayse Early Alert Intelligence**" under Organization Settings -> Apps.

11. Note that any feeds deactivated by the feed deployer will be shown as well.

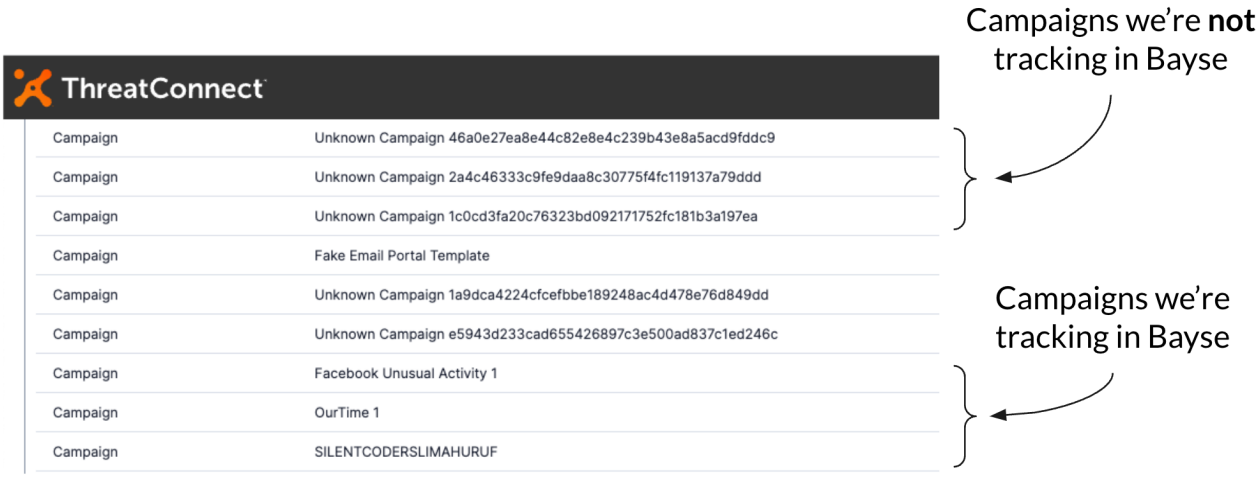
Bayse Early Alert Intelligence Feed v1
Bayse Early Alert Intelligence Feed v1 (Deactivated by Feed Deployer)

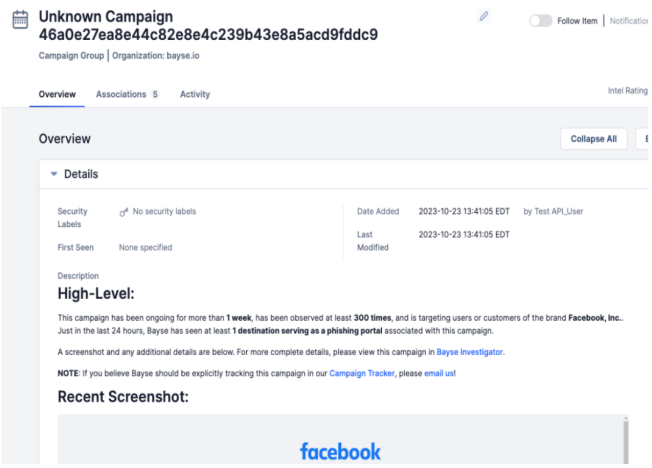
12. The created Job will start and run automatically.

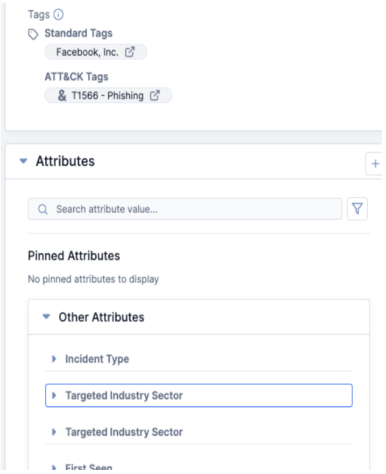
8. Understanding the Data

There are two important concepts to understand with Bayse. First – and most important – is that all individual indicators we create will automatically be grouped into ThreatConnect **Groups** of type **Campaign**. This is possible because Bayse automatically calculates the Site Fingerprints associated with each site we analyze. All sites that contain the same *structural_id* Site Fingerprint (please read the intro linked above for additional information) are extremely likely to be either a particular phishing campaign or leverage a phishing kit (whether or not the kit is known by the security community).

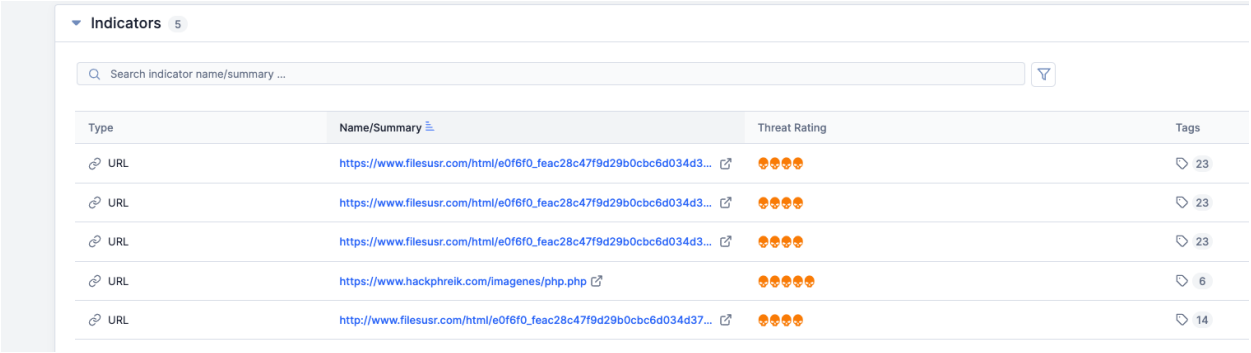
When Bayse Intelligence is tracking a campaign (currently-tracked campaigns can be found in Bayse's campaign tracker), the campaign will provide additional human-created intelligence added to the Group. When Bayse Intelligence is not officially tracking a campaign, the name will begin with *Unknown Campaign* followed by the *structural_id* Site Fingerprint value. Automatically-generated information (such as screenshot, duration of campaign, companies or industry sectors impacted, etc…) will be included in these Groups.





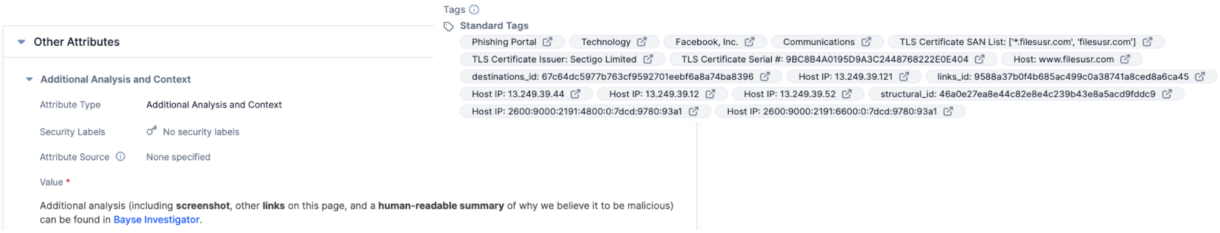


The **second important concept** for the Bayse integration is that individual indicators will all be of ThreatConnect's **URL** type. This allows us to share the full link (for deeper investigation) and also to identify when legitimate services are being abused.



These *URL* indicators are classified into **3 different types** (each of which will be indicated by a **Tag** value):

1. **Submitted Link**
    a. The Submitted Link was whatever URL Bayse originally encountered. This could be a link from an email, a link pointing to a newly-registered domain, or a URL-shortened link. Note that there are many times where the underlying destination (such as *tinyurl[.]com* for a link shortened using TinyURL's link shortener service) is not malicious, but the specific Submitted Link does point to a malicious site.
2. **Phishing Portal**
    a. Bayse follows redirects, which means we will ultimately end up on the site we believe to be the actual phishing portal. URLs tagged with Phishing Portal will usually contain the most context within both Tags and Other Attributes:



3. **Credential Collection**
    a. Whenever possible, Bayse automatically extracts the full link of the site where credentials (or other victim-supplied information) are being exfiltrated. Note that sites tagged with Credential Collection will often be compromised sites (that look benign from the main homepage) or legitimate services (such as Telegram's bot API endpoint or Google Docs). The full link provides the additional context to differentiate the malicious use of a benign website/legitimate service.

9. Support

If you encounter any issues while running the app or have technical questions, please reach out to Bayse by emailing *support@bayse.io*.