**Logo

Description automatically generated**

ThreatConnect – Loginsoft PursuitX User Guide

**Version 1.0.0**

Contents

[**Introduction** 2](#_Toc78463910)

[**Release Notes** 3](#_Toc78463911)

[**Data Mapping** 4](#_Toc78463912)

[**Configuration Requirements** 5](#_Toc78463913)

[**App Installation via Feed Deployer** 5](#_Toc78463914)

[**ThreatConnect Job Configuration** 5](#_Toc78463915)

[**Browsing Loginsoft PursuitX Feed** 10](#_Toc78463916)

[**Signature Feed:** 11](#_Toc78463917)

[**Threat Feed:** 12](#_Toc78463918)

[**Support** 13](#_Toc78463919)

# **Introduction**

**Loginsoft PursuitX** provides intelligence-driven threat detections of malware families and threat actors and their tactics, techniques, and procedures which help an organization to integrate with their current SIEM solutions. PursuitX consistently monitors various adversaries by tracking the attack behavior comprising TTPs and collect relevant log events to generate detection rules specific to a malware family or a threat actor.

* With context driven signatures that help to improve existing security controls, the detection feed comes in a prominent and revolutionary format "SIGMA" which is a human-readable and effective format that can describe relevant log events from various telemetry and convert rules to queries of the respective SIEM solution of their choice.
* The PursuitX team continuously research and update the detections to automatically prioritize the events for actionable response.

**Sigma Rules as De facto:**

* Describes detection and includes metadata which is helpful for investigations
* Can easily be integrated with several SIEM solutions
* Community endorsed
* Can easily be shared with threat intelligence platforms

This integration consists of consuming the Loginsoft PursuitX Threat Intelligence feed and importing the data as signature and threat groups into the ThreatConnect Platform as a Threat Intelligence feed. A high-level run of the Loginsoft PursuitX Threat Intelligence feed is shown below.

Diagram

Description automatically generated

# **Release Notes**

|  |  |  |
| --- | --- | --- |
| **App Version** | **Release Date** | **Details** |
| 1.0.0 |  | Initial Release. |

# **Data Mapping**

The following table documents the data mapping that takes place between the Loginsoft PursuitX Threat Intelligence feed data and the ThreatConnect Platform.

|  |  |  |  |
| --- | --- | --- | --- |
| **Malware Threat Intelligence Feed** | **ThreatConnect Field/Object** | **Possible Values** | **Notes** |
| title | name – Signature Group | String | The title data point from the Loginsoft feed will be mapped to the name attribute of the signature object. |
| description | Attribute – Description – Signature Group | String | The description data point from the Loginsoft feed will be mapped to the Description Attribute. |
| malware\_family | name – Threat Group | String | The malware\_family data point from the Loginsoft feed will be mapped to the name of the Threat Object. |
| malware\_type | Attribute - Malware Family Variety – Threat Group | String | The malware\_type data point from the Loginsoft feed will be mapped to the Malware Family Variety Attribute of Threat Object.  And also, we will adding the Threat Type Attribute to Malware Family |
| mitre\_techniques | Tags – Signature Group | String Array | The mitre\_techniques data point from the feed will be added as tags. |
| reference | Attribute – Source – Signature Group | String Array | The reference data point from the feed will be mapped to the Source Attribute. |
| rule\_source | Signature File Content – Signature Group | String | The rule\_source data point from the Loginsoft feed will be mapped to the Signature File Content of the Signature Object. |
| rule\_id | xid – Signature Group | String | The rule\_id data point from the Loginsoft feed will be mapped to xid attribute of the Signature object |

# **Configuration Requirements**

1. Access to a ThreatConnect Platform Instance
2. ThreatConnect API user

# **Job App Installation**

For download and installation instructions, please refer to the ThreatConnect System Administration Guide(Install an App). For more information, contact your ThreatConnect Customer Success representatives.

# **ThreatConnect Job Configuration**

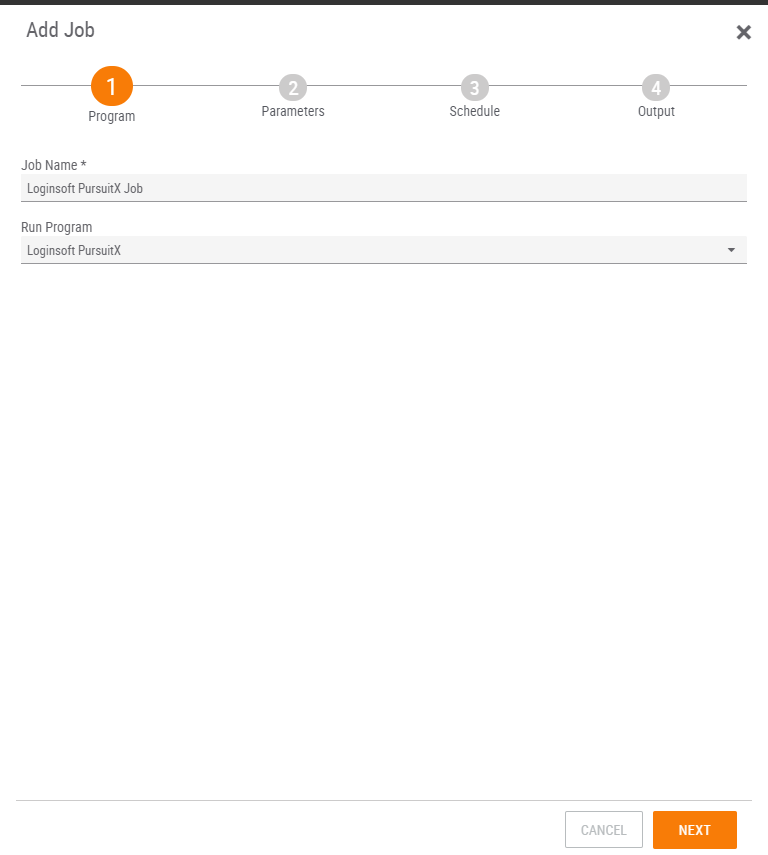
The ThreatConnect Platform allows customers to run jobs on a scheduled basis. Once the package has been installed, the customer can run the Loginsoft PursuitX Threat Intelligence feed as frequently as they desire. The Loginsoft PursuitX feed is quite small and so running the feed very frequently does not affect the performance of the ThreatConnect Platform.

\*\*Note that these steps are not necessary if the app was deployed using Feed Deployer as the job would have already been configured.

* Go to the gear in the top right corner in the ThreatConnect platform then **Org Settings > Apps.**
* Click on the + to create a new job

**Program Screen:**

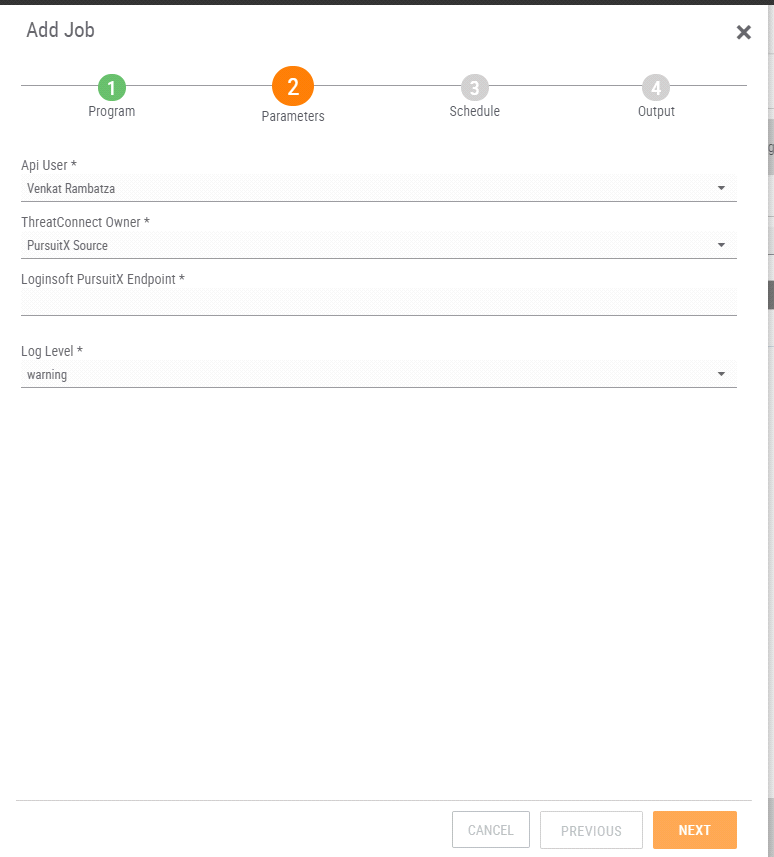
* Enter the Job Name (Ex: Loginsoft PursuitX Feed).
* Select the Run program as a Loginsoft PursuitX from the dropdown.



* Click NEXT.

**Parameter Screen:**

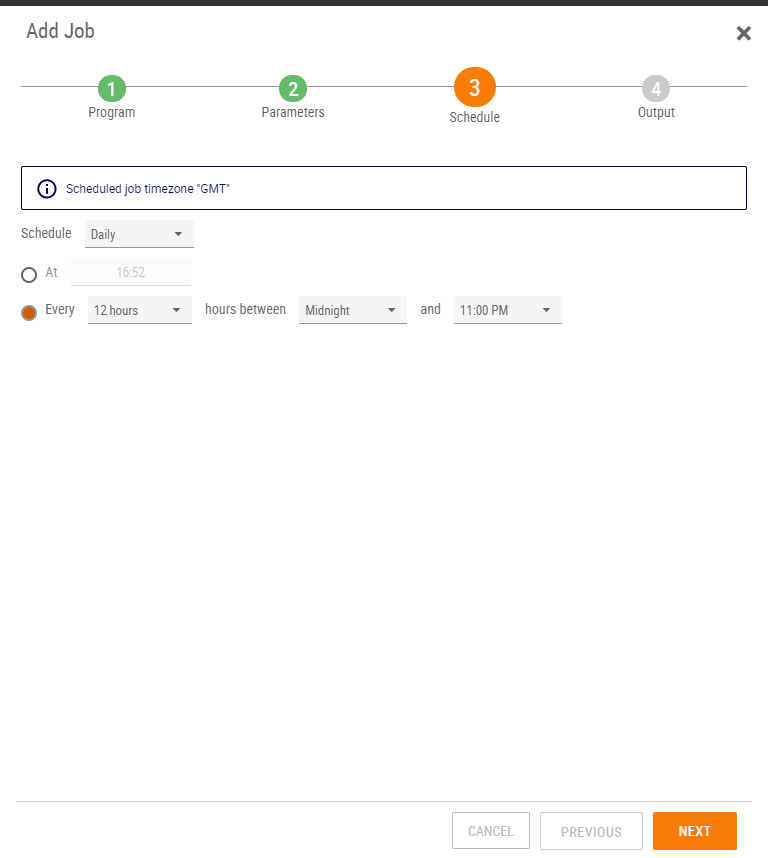
* For API User, click on the down arrow and select your organization
* For ThreatConnect Owner, click on the down arrow and select the source created by the Feed Deployer
* For Log Level, select it from dropdown default log level set to warning.



* Click NEXT

**Schedule Screen:**

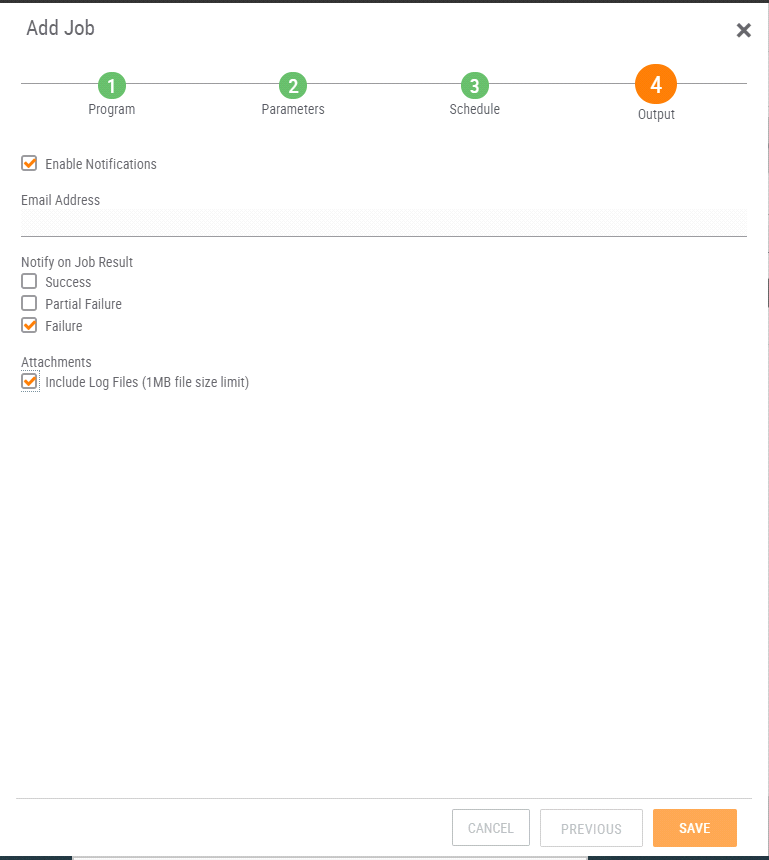
* Depending on your environment, you can schedule the feed at daily hours, weekly etc., select the appropriate values from the dropdown menu.



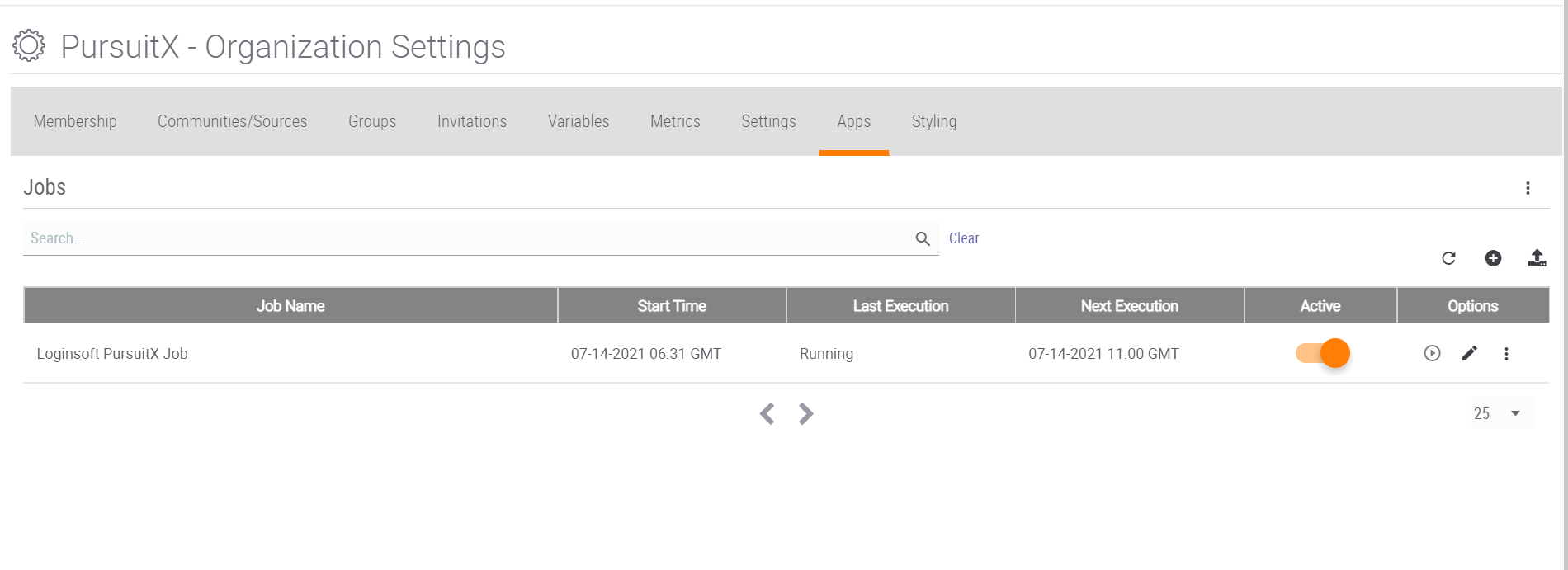
* Click NEXT

**Output Screen:**

* If you want to be notified on job results, click the box next to Enable Notifications, enter an email address for the notifications to be sent, and which notifications that you want and if you want a log file attached.



* Click SAVE
* Once the Job has been saved, we can find our job on Jobs under Apps
* Click on the slider under Active to activate the job.



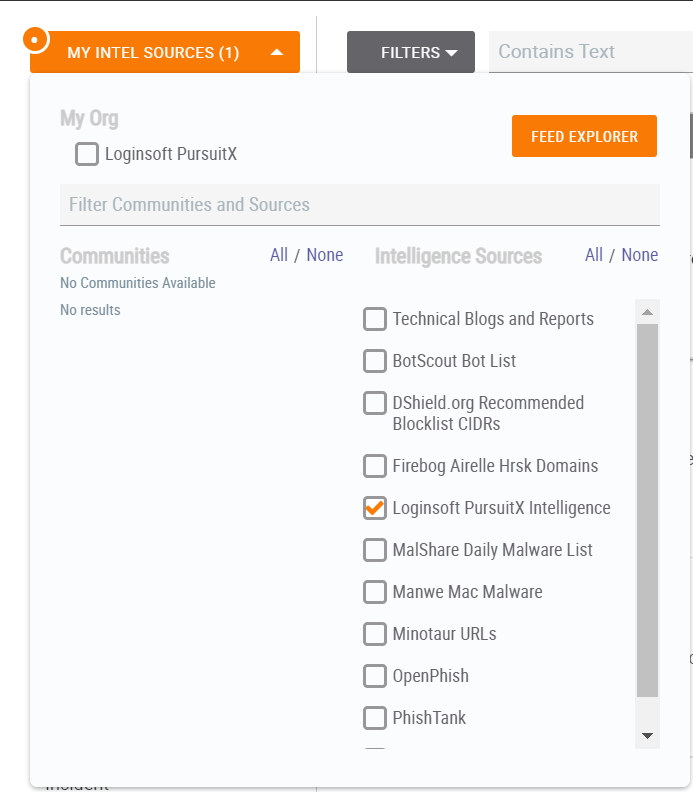
* Here we can observe the Start Time and Next Execution time and Last Execution Status as well if you want to run the job at this time click on the play button in options tab.

# **Browsing Loginsoft PursuitX Feed**

For guidance on general browsing of indicators and groups in the ThreatConnect Platform, please refer to the article below:

<https://training.threatconnect.com/learn/article/browse-kb-article>

1. Navigate to the browse page and check to make sure that the Loginsoft PursuitX Threat Intelligence Feed is checked.



## **Signature Feed:**

To browse **Signature Feed** from Loginsoft PursuitX, select signature group.

A screenshot of a computer

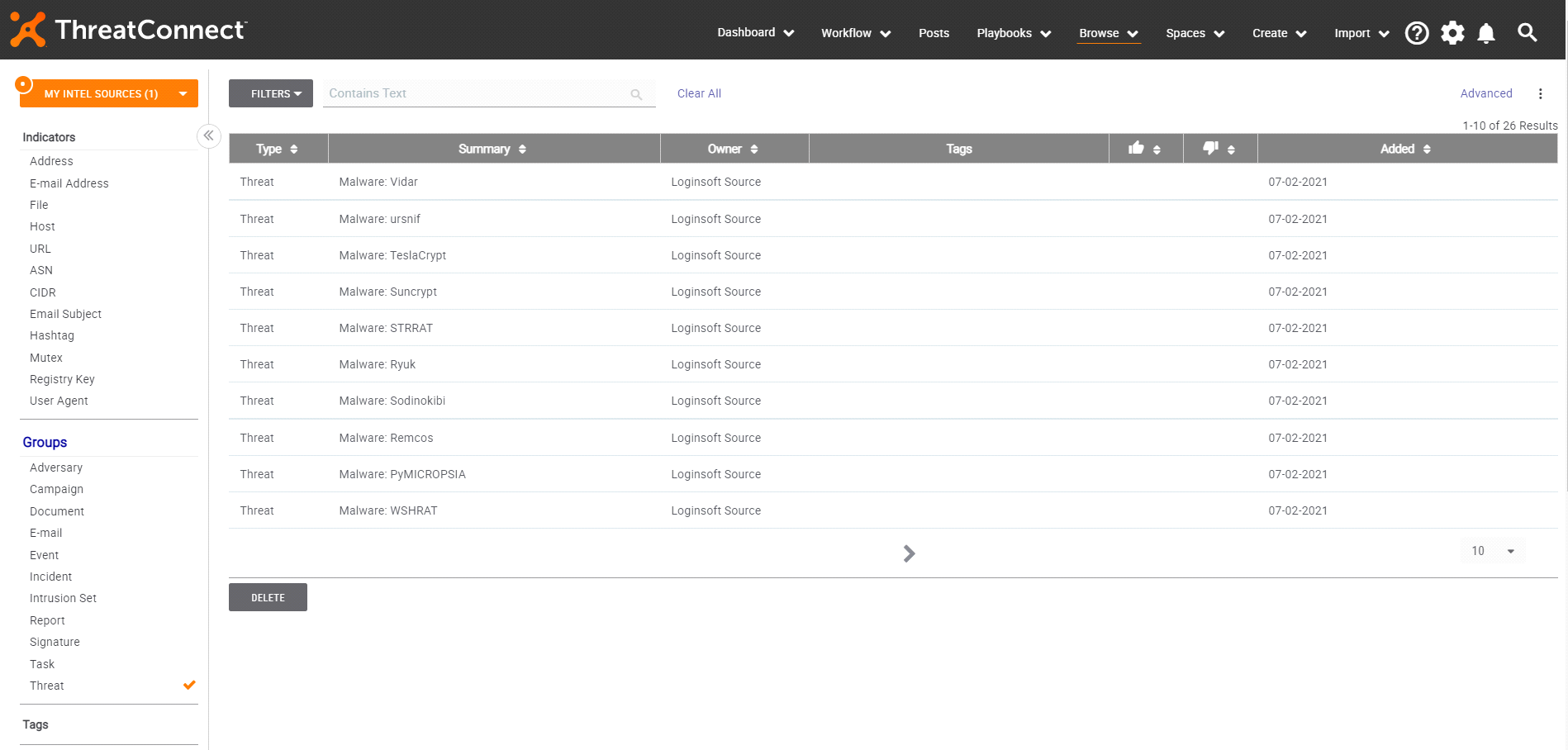
Description automatically generated

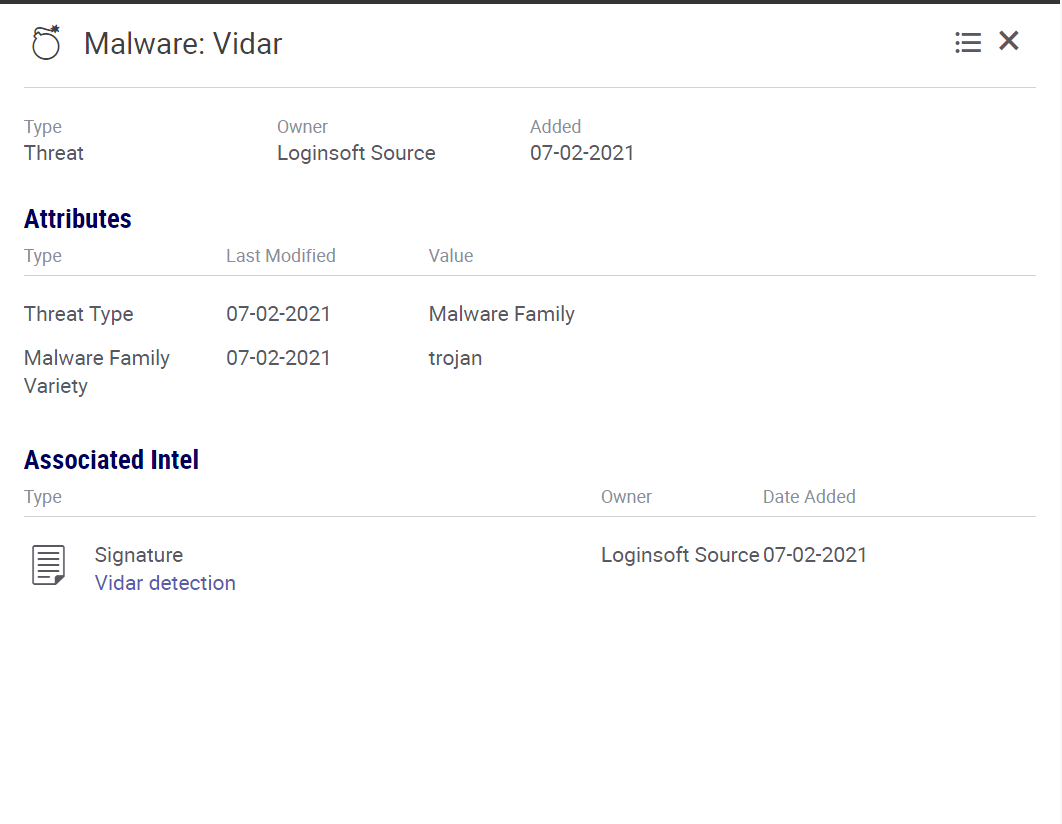
Graphical user interface, text, application, email

Description automatically generated

## **Threat Feed:**

To browse **Threat Feed** from Loginsoft PursuitX, select threat group





# **Support**

For assistance with this App, to report a bug, or feature requests please contact us via the following.

|  |  |
| --- | --- |
| **Support Portal** | <https://www.loginsoft.com/contact/> |
| **Email** | [pursuitX-Intel@loginsoft.com](mailto:pursuitX-Intel@loginsoft.com) |
| **Phone** | +1 7039567410 |