A blue and white logo

AI-generated content may be incorrect.

**ThreatConnect – Cognyte Luminar User Guide**

**Version 1.0.0**

**Contents**

[**Introduction** 2](#_Toc194674206)

[**Release Notes** 3](#_Toc194674207)

[**Data Mapping** 4](#_Toc194674208)

[**Configuration Requirements** 4](#_Toc194674209)

[**Job App Installation** 4](#_Toc194674210)

[**ThreatConnect Job Configuration** 4](#_Toc194674211)

[**Browsing Luminar Intelligence Feed** 10](#_Toc194674212)

[**Luminar IOC Feed** 10](#_Toc194674213)

[**Luminar Leaked Credentials Feed** 12](#_Toc194674214)

[**Luminar Cyber Feeds** 13](#_Toc194674215)

[**Support** 14](#_Toc194674216)

# 

# **Introduction**

**Cognyte** is a global leader in security analytics software that empowers governments and enterprises with Actionable Intelligence for a safer world. Our open software fuses, analyzes and visualizes disparate data sets at scale to help security organizations find the needles in the haystacks. Over 1,000 government and enterprise customers in more than 100 countries rely on Cognyte’s solutions to accelerate security investigations and connect the dots to successfully identify, neutralize, and prevent threats to national security, business continuity and cyber security.

Luminar is an asset-based cybersecurity intelligence platform that empowers enterprise organizations to build and maintain a proactive threat intelligence operation that enables to anticipate and mitigate cyber threats, reduce risk, and enhance security resilience. Luminar enables security teams to define a customized, dynamic monitoring plan to uncover malicious activity in its earliest stages on all layers of the Web.

“Luminar Threat Intelligence” App allows integration of intelligence-based IOC data, customer-related leaked records and Threat Intelligence Data identified by Luminar. A high-level run of the Luminar Threat Intelligence feed is shown below.

A diagram of a process flow

AI-generated content may be incorrect.

# **Release Notes**

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

# **Data Mapping**

The table below documents the data mapping that takes place between the Luminar Threat Intelligence data and the ThreatConnect Platform.

|  |  |  |
| --- | --- | --- |
| **Luminar Intelligence** | **ThreatConnect Object** | **ThreatConnect Object Type** |
| MD5 | File | Indicator |
| SHA256 | File | Indicator |
| SHA512 | File | Indicator |
| Domain | Host | Indicator |
| IP | Address | Indicator |
| URL | URL | Indicator |
| Email | Email Address | Indicator |
| Mutex | Mutex | Indicator |
| Windows\_Registry\_Key | Registry Key | Indicator |
| User Account | Victim | Victim |
| Malware | malware | Group |
| Incident | Incident | Group |
| Vulnerability | Vulnerability | Group |
| Campaign | Campaign | Group |
| Threat Actor | Threat | Group |
| Report | Report | Group |
| Attack Pattern | Attack Pattern | Group |
| Tool | Tool | Group |

# **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 Luminar Threat Intelligence feed as frequently as they desire. By default, the App will run daily.

**Note:** 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: Luminar Intelligence Feed).
* Select the Run program as a "Luminar Threat Intelligence" from the dropdown.
* Click NEXT.

A screenshot of a computer

AI-generated content may be incorrect.

**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 Luminar API Account ID, please provide credentials received from Cognyte.
* For Luminar API Client ID, please provide credentials received from Cognyte.
* For Luminar API Client Secret, please provide credentials received from Cognyte.
* For Initial Fetch Date, please select date from which you want to pull the data from Luminar, ideally 3 months back date.
* For Log Level, select it from dropdown default log level set to warning.
* Click NEXT

A screenshot of a computer

AI-generated content may be incorrect.

**Schedule Screen:**

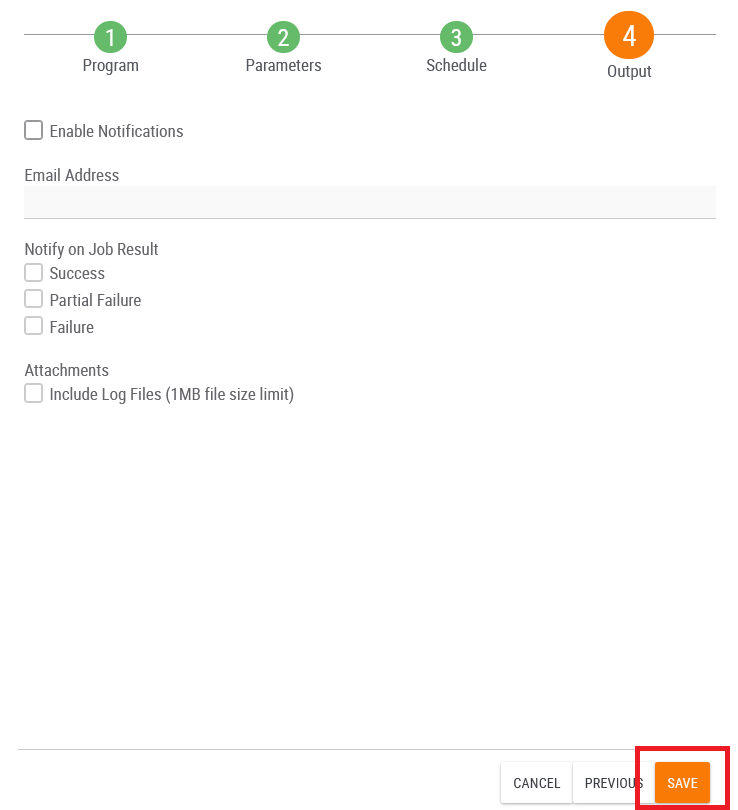
* Depending on your environment, you can schedule the feed at daily hours, weekly etc., select the appropriate values from the dropdown menu.
* Click NEXT

Graphical user interface, text, application, email

Description automatically generated

**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.

A screenshot of a computer

AI-generated content may be incorrect.

# **Browsing Luminar Intelligence 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>

Navigate to the browse page and check to make sure that the Luminar Source Feed is checked.

## **Luminar IOC Feed**

“Luminar Intelligence” integration fetches the Luminar IOC’s and ingests into ThreatConnect “File”, “Host”, “Address”, “URL”, “Email Address”, “Mutex” and “Registry Key” indicator types accordingly, you can browse to the indicator type and see the data accordingly.

For example, to browse **IP Address Feed**, select Address Indicator.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

For example, to browse **Hosts Feed** from Luminar Intelligence, select Host Indicator.

A screenshot of a computer

AI-generated content may be incorrect.

## **Luminar Leaked Credentials Feed**

“Luminar Intelligence” integration fetches the leaked credentials information from Luminar and saves it to ThreatConnect Victims object.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

# 

## **Luminar Cyber Feeds**

“Luminar Intelligence” integration fetches the Cyber Feeds data from Luminar and ingests into ThreatConnect group type’s “Vulnerability”, “Campaign”, “Threat”, “Indicator”, “Report”, “Attack Pattern” and “Tool” accordingly, you can browse to the group type and see the data accordingly.

For example, to browse **Report Feed**, select Report group.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

For example, to browse **Threat Feed**, select Threat group.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

# **Support**

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

|  |  |
| --- | --- |
| **Email** | [luminar@cognyte.com](mailto:luminar@cognyte.com) |