ThreatQuotient

A Securonix Company

Luminar Cognyte Threat Intelligence CDF User Guide

Version 1.0.0

September 30, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Developer Supported

Support
Email: luminar@cognyte.com
Web: N/A
Phone: N/A

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **Developer Supported**.

Support Email: luminar@cognyte.com
Support Web: N/A
Support Phone: N/A

Integrations designated as **Developer Supported** are supported and maintained by the developer who submitted the integration to the ThreatQ Marketplace. The developer's contact information can be found on the integration's download page within the Marketplace as well as in this guide.

You are responsible for engaging directly with the developer of Developer Supported integrations/ apps/add-ons to ensure proper functionality and version compatibility with the applicable ThreatQuotient Software.

If functional or compatibility issues that may arise are not resolved, you may be required to uninstall the app or add-on from their ThreatQuotient environment in order for ThreatQuotient to fulfill support obligations.

For ThreatQuotient Hosted instance customers, the Service Level Commitment and Service Level Credit in the ThreatQuotient Service Level Schedule will not apply for any issues caused by Developer Supported integrations/apps/add-ons.

ThreatQuotient reserves the right to remove the Developer-Supported designation of third-party apps and add-ons if the developer is not, in ThreatQuotient's determination, fulfilling reasonable obligations for support and maintenance.

> EX Failure by the developer to update compatibility of an app or add-on within 90 days of the release of a new version of applicable ThreatQuotient Software will result in reclassification to Not Actively Supported.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 6.4.0
Support Tier	Developer Supported
Developer Support Contact	luminar@cognyte.com

Introduction

The Luminar Cognyte Threat Intelligence CDF integration enables the automated ingestion of threat intelligence from Cognyte Luminar into the ThreatQ platform.

Cognyte, a global leader in security analytics software, delivers solutions that transform diverse data sources into actionable intelligence. Its asset-based cyber intelligence platform, Luminar, equips organizations to proactively monitor, anticipate, and mitigate threats across the web.

The integration provides the following feeds:

- **Luminar Cognyte IOCs** – ingests Indicators of Compromise (IOCs) including file hashes, IPs, domains, URLs, and email addresses.
- **Luminar Cognyte Leaked Records** – ingests compromised account credentials with related incident context.
- **Luminar Cognyte Cyberfeeds** – provides curated threat intelligence reports, malware, vulnerabilities, campaigns, and threat actors.

The integration ingests the following object types:

- Adversary
- Campaign
- Compromised Account (custom object)
- Identity
- Incident
- Indicators
- Malware
- Report
- Signatures
- Vulnerability

Prerequisites

The following is required in order to install and run the integration:

- Installation of the **Compromised Account** custom object.
- Cognyte Luminar credentials:
  - Luminar API Account ID
  - Luminar API Client ID
  - Luminar API Client Secret

Compromised Account Custom Object

The integration requires the Compromised Account custom object.

Use the steps provided to install the Compromised Account custom object.

> When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

ThreatQ V6 Steps

Use the following steps to install the custom object in ThreatQ v6:

1. Download the integration bundle from the ThreatQ Marketplace.
2. Unzip the bundle and locate the custom object files.

   > The custom object files will typically consist of a JSON definition file, install.sh script, and a images folder containing the svg icons.

3. SSH into your ThreatQ instance.
4. Navigate to the tmp folder:

   ```
   cd /var/lib/threatq/misc/
   ```

5. Upload the custom object files, including the images folder.

   The directory structure should be as the following:

   - misc
     - install.sh
     - <custom_object_name>.json
     - images (directory)
       - <custom_object_name>.svg

6. Run the following command:

```
kubectl exec -it deployment/api-schedule-run -n threatq -- sh /var/
lib/threatq/misc/install.sh /var/lib/threatq/misc
```

> The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

7. Delete the install.sh, definition json file, and images directory from the `misc` directory after the object has been installed as these files are no longer needed.

ThreatQ v5 Steps

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   cd /tmp/
   ```

4. Create a new directory:

   ```
   mkdir luminar_cdf
   ```

5. Upload the **account.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the luminar_cdf directory.

   ```
   mkdir images
   ```

7. Upload the account.svg.
8. Navigate to the **/tmp/luminar_CDF**.

   The directory should resemble the following:

   - tmp
     - **luminar_cdf**
       - **account.json**
       - **install.sh**
       - **images**
         - **account.svg**

9. Run the following command to ensure that you have the proper permissions to install the custom object:

```
chmod +x install.sh
```

10. Run the following command:

```
sudo ./install.sh
```

> You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf luminar_cdf
```

Installation

> The CDF requires the installation of the Compromised Account custom object before installing the actual CDF. See the Compromised Account section of this guide for more details. The custom object must be installed prior to installing the CDF. Attempting to install the CDF without the custom object will cause the CDF install process to fail.

Perform the following steps to install the integration:

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration zip file.
3. Extract the integration files and install the Compromised Account custom object if you have not done so already.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the file on your local machine
7. Select the individual feeds to install, when prompted, and click **Install**.

> ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

The feed(s) will be added to the integrations page. You will still need to configure and then enable the feed(s).

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

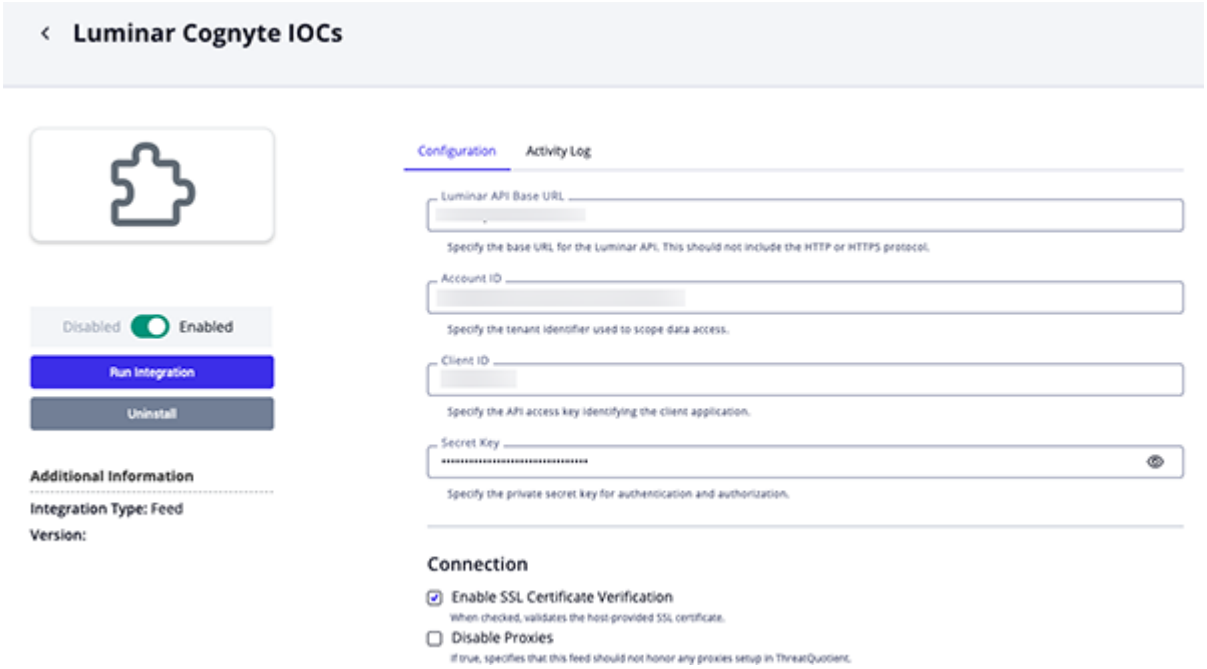
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Luminar API Base URL	Enter the base URL for the Luminar API. The default value is `www.cyberluminar.com`. > This should not include the HTTP or HTTPS protocol.
Luminar Account ID	The Tenant identifier used to scope data access.
Luminar Client ID	The API key identifying the client application.
Luminar Secret Key	The Private secret key for authentication.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Shared Mapping

The mappings for all the feeds are handled by the native ThreatQ STIX 2 parser. The value of the attributes `Modified At`, `Valid From`, `Valid Until`, `Is Family`, `Luminar Threat Score`, and `Confidence` is updated at ingestion.

For some object types there are some additional attributes to the ones parsed by STIX 2 parser. They are detailed below.

> These additional mappings are based on the data pulled from the objects list from the API response.

Indicators


```
{
  "objects": [
    {
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator--aa97252d-b910-50e0-8a8e-cbf3aad90bab",
      "created": "2024-12-24T00:00:00.000Z",
      "modified": "2025-05-03T16:01:12.833Z",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "score": 69,
          "asn": 202520,
          "protocols": ["ssh"],
          "extension_type": "property-extension",
          "luminar_tenant_id": "89b7646d-8b81-4529-b573-8229bdb6949f",
          "resolving_domains": [
            "api-quick.flextv.cc",
            "901bet.com",
            "3rr.xyz",
            "api-quicks.flextv.cc",
            "236bet7.com"
          ],
          "conviction_reasons": ["bad_reputation"]
        }
      },
      "labels": ["apt", "worm", "malware"],
      "confidence": 85,
      "pattern": "[ipv4-addr:value = '45.61.187.7']",
      "created_by_ref": "identity--ed9b8dce-7aab-42bd-8171-a8d1599fc849",
      "external_references": [
```

```
        {
          "source_name": "mitre-attack",
          "external_id": "T1643"
        }
      ],
      "pattern_type": "stix",
      "indicator_types": ["malicious-activity"],
      "valid_from": "2025-04-18T00:00:00.000Z",
      "valid_until": "2025-04-25T00:00:00.000Z"
    }
  ]
}
```

The following mapping table applies to the Luminar Cognyte IOCs feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.extensions.*.score`	Indicator.Attribute	Luminar Threat Score	N/A	`69`	Updatable.
`.extensions.*.asn`	Indicator.Attribute	ASN	N/A	`202520`	N/A
`.extensions.*.country`	Indicator.Attribute	Country	N/A	N/A	N/A
`.extensions.*.protocols[]`	Indicator.Attribute	Protocols	N/A	`ssh`	Values are concatenated.
`.extensions.*.resolving_domains[]`	Indicator.Attribute	Resolving Domains	N/A	N/A	Values are concatenated.
`.extensions.*.conviction_reasons[]`	Indicator.Attribute	Conviction Reasons	N/A	`bad_reputation`	Values are concatenated.
`.indicator_types[]`	Indicator.Attribute	Indicator Types	N/A	`malicious-activity`	Values are concatenated.
`.external_references[].*`	Indicator.Attribute	External References	N/A	`mitre-attack(T1643)`	Values `.source_name` and `.external_id` are concatenated.

Malware


```
{
  "objects": [
    {
      "aliases": [],
      "created": "2023-03-28T00:00:00.000Z",
      "created_by_ref": "identity--5bf1ac35-8d08-509e-b31a-044cb09b4199",
      "description": "The following credentials were obtained using REDLINE, a
stealer malware, and shared on 1652109402 on 2023-03-28T07:32:01.",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "collection_date": "2024-01-11T03:00:42.223Z",
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff",
          "luminar_threat_score": 71
        }
      },
      "id": "malware--0cc479c5-6d01-5e53-8fee-1cc28eaa6af0",
      "modified": "2025-09-21T23:48:13.130Z",
      "name": "REDLINE",
      "spec_version": "2.1",
      "type": "malware",
      "malware_types": ["spyware"],
      "capabilities": ["steals-authentication-credentials"],
      "is_family": true
    }
  ]
}
```


The following mapping table applies to the Luminar Cognyte IOCs, Luminar Cognyte Leaked Records, and Luminar Cognyte Cyberfeeds feeds.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.extensions.*.luminar_threat_score`	Malware.Attribute	Luminar Threat Score	N/A	`71`	Updatable.
`.malware_types[]`	Malware.Attribute	Malware Types	N/A	`spyware`	Values are concatenated.
`.is_family[]`	Malware.Attribute	Is Family	N/A	`true`	Converted to string.
`.capabilities[]`	Malware.Attribute	Capabilities	N/A	`steals-authentication-credentials`	Values are concatenated.
`.aliases[]`	Malware.Attribute	Aliases	N/A	N/A	Values are concatenated.

Incident


```
{
  "objects": [
    {
      "created": "2025-08-10T00:00:00.000Z",
      "created_by_ref": "identity--5bf1ac35-8d08-509e-b31a-044cb09b4199",
      "description": "The following credentials were shared on Telegram,
channel id: 1560764284, on 2025-08-10. They were extracted from a file named
\"Logs_10 August (1).rar\" with a size of 3.1 GB.",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "collection_date": "2025-08-11T19:09:12.467Z",
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff",
          "luminar_threat_score": 71,
          "computer_name": "nickn"
        }
      },
      "id": "incident--51df2159-98c6-5d5a-9686-7326163c4303",
      "modified": "2025-09-21T23:48:13.132Z",
      "name": "Logs_10_August_(1).rar",
      "spec_version": "2.1",
      "type": "incident"
    }
  ]
}
```


The following mapping table applies to the Luminar Cognyte Leaked Records feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.extensions.*.luminar_threat_score`	Incident.Attribute	Luminar Threat Score	N/A	`71`	Updatable.
`.extensions.*.collection_date`	Incident.Attribute	Collection Date	N/A	`2025-08-11T19:09:12.467Z`	N/A
`.extensions.*.computer_name`	Incident.Attribute	Computer Name	N/A	`nickn`	N/A

Compromised Account


```
{
  "objects": [
    {
      "account_login": "dumarchiti@loginsoft.com",
      "credential": "u@raja123!",
      "display_name": "dumarchiti@loginsoft.com",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "credential_is_fresh": true,
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff",
          "monitoring_plan_terms": ["@loginsoft.com"],
          "source": "telegram",
          "url": "www.7-eleven.com/login"
        }
      },
      "id": "user-account--fff1261f-a2fa-507b-8b1c-d8e53b0656ac",
      "spec_version": "2.1",
      "type": "user-account"
    }
  ]
}
```


The following mapping table applies to the Luminar Cognyte Leaked Records feed.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.extensions.*.monitoring_plan_terms`	Compromised Account.Attribute	Monitoring Plan Term	N/A	`@loginsoft.com`	Values are concatenated.
`.extensions.*.source`	Compromised Account.Attribute	Leak Source	N/A	`Telegram`	N/A
`.extensions.*.url`	Compromised Account.Attribute	Originating URL	N/A	`www.7-eleven.com/login`	N/A
`.extensions.*.credential_is_fresh`	Compromised Account.Attribute	Is Fresh	N/A	`true`	Converted to string.
`.credential`	Compromised Account.Attribute	Leaked Credential	N/A	`u@raja123!`	N/A

Adversary


```
{
  "objects": [
    {
      "type": "threat-actor",
      "spec_version": "2.1",
      "id": "threat-actor--b23c9f00-d4b6-52ed-9c3c-bd0254b6fb35",
      "created": "2024-12-24T00:00:00.000Z",
      "modified": "2025-05-03T16:01:12.833Z",
      "aliases": ["APT35"],
      "capabilities": ["steals-authentication-credentials"],
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
        }
      },
      "threat_actor_types": ["nation-state"],
      "name": "CoderSharp"
    }
  ]
}
```


The following mapping table applies to the Luminar Cognyte Cyberfeeds feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.threat_actor_types[]`	Adversary.Attribute	Threat Actor Types	N/A	`nation-state`	Values are concatenated.
`.aliases[]`	Adversary.Attribute	Aliases	N/A	APT35	Values are concatenated.
`.capabilities[]`	Adversary.Attribute	Capabilities	N/A	`steals-authentication-credentials`	Values are concatenated.

Luminar Cognyte IOCs

The Luminar Cognyte IOCs feed ingests Indicators of Compromise and associated context from the Cognyte API.

`GET https://www.cyberluminar.com/externalApi/taxii/collections/{IOC_collection_id}/objects/?added_after=2025-04-28T21:02:35.000000Z`

Sample Response:


```
{
  "more": true,
  "next":
"p9S1AwU2Y3RpX3N0aXhfMjAyNDEyMDNfMDBiZWQ5NTQtNGIxYS0==@1746327756111@1746288073
450@8590220163",
  "objects": [
    {
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator--aa97252d-b910-50e0-8a8e-cbf3aad90bab",
      "created": "2024-12-24T00:00:00.000Z",
      "modified": "2025-05-03T16:01:12.833Z",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "score": 69,
          "asn": 202520,
          "protocols": ["ssh"],
          "extension_type": "property-extension",
          "luminar_tenant_id": "89b7646d-8b81-4529-b573-8229bdb6949f",
          "resolving_domains": [
            "api-quick.flextv.cc",
            "901bet.com",
            "3rr.xyz",
            "api-quicks.flextv.cc",
            "236bet7.com"
          ],
          "conviction_reasons": ["bad_reputation"]
        }
      },
      "labels": ["apt", "worm", "malware"],
      "confidence": 85,
      "pattern": "[ipv4-addr:value = '45.61.187.7']",
      "created_by_ref": "identity--ed9b8dce-7aab-42bd-8171-a8d1599fc849",
      "external_references": [
        {
          "source_name": "mitre-attack",
          "external_id": "T1643"
        }
      ],
      "pattern_type": "stix",
```

```
    "indicator_types": ["malicious-activity"],
    "valid_from": "2025-04-18T00:00:00.000Z",
    "valid_until": "2025-04-25T00:00:00.000Z"
  },
  {
    "type": "threat-actor",
    "spec_version": "2.1",
    "id": "threat-actor--b23c9f00-d4b6-52ed-9c3c-bd0254b6fb35",
    "created": "2024-12-24T00:00:00.000Z",
    "modified": "2025-05-03T16:01:12.833Z",
    "extensions": {
      "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
        "extension_type": "property-extension",
        "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
      }
    },
    "name": "CoderSharp"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--cf6ab008-4781-50f7-aefe-7cc162b34b5b",
    "created": "2024-12-24T00:00:00.000Z",
    "modified": "2025-05-03T16:01:12.833Z",
    "extensions": {
      "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
        "extension_type": "property-extension",
        "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
      }
    },
    "relationship_type": "indicates",
    "source_ref": "indicator--aa97252d-b910-50e0-8a8e-cbf3aad90bab",
    "target_ref": "threat-actor--b23c9f00-d4b6-52ed-9c3c-bd0254b6fb35"
  },
  {
    "type": "relationship",
    "spec_version": "2.1",
    "id": "relationship--07918236-1430-51ca-9a5d-2c7f08876220",
    "created": "2024-12-24T00:00:00.000Z",
    "modified": "2025-05-03T16:01:12.833Z",
    "extensions": {
      "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
        "extension_type": "property-extension",
        "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
      }
    },
    "relationship_type": "indicates",
    "source_ref": "indicator--aa97252d-b910-50e0-8a8e-cbf3aad90bab",
    "target_ref": "malware--df643c50-568f-5a0b-861c-3354be0c290a"
  },
```

```
    {
      "type": "malware",
      "spec_version": "2.1",
      "id": "malware--df643c50-568f-5a0b-861c-3354be0c290a",
      "created": "2024-12-24T00:00:00.000Z",
      "modified": "2025-05-03T16:01:12.833Z",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff",
          "luminar_threat_score": 60
        }
      },
      "name": "Hannibal Stealer",
      "malware_types": ["spyware"],
      "is_family": false
    }
  ]
}
```

Luminar Cognyte Leaked Records

The Luminar Cognyte Leaked Records feed ingests Leaked records which consists of Compromised accounts details and its respective linked incidents and malware's from the Cognyte API.

```
GET https://www.cyberluminar.com/externalApi/taxii/collections/
{{leaked_records_collection_id}}/objects/?
added_after=2025-06-16T23:43:16.854307Z&limit=9999
```

Sample Response:


```
{
  "more": true,
  "next":
"p9S1AwU2Y3RpX3N0aXhfMjAyNDEyMDNfMDBiZWQ5NTQt==@1747796800499@1747767936933@859
0279076",
  "objects": [
    {
      "type": "user-account",
      "spec_version": "2.1",
      "id": "user-account--d10e0104-f10e-535e-b572-65894843605f",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "url": "www.7-eleven.com/login",
          "source": "telegram",
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff",
          "monitoring_plan_terms": ["7-eleven.com"],
          "credential_is_fresh": true
        }
      },
      "credential": "Alexandria11",
      "account_login": "mfuray81185@gmail.com",
      "display_name": "mfuray81185@gmail.com"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--9d7a5258-2bcb-573d-82be-7f39bf028e4f",
      "created": "2025-06-16T00:00:00.000Z",
      "modified": "2025-06-17T02:02:50.876Z",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
        }
      },
      "relationship_type": "related-to",
      "source_ref": "user-account--d10e0104-f10e-535e-b572-65894843605f",
      "target_ref": "incident--9940dbc8-facd-5e08-8326-7af7875e961c"
```

```
    },
    {
      "type": "incident",
      "spec_version": "2.1",
      "id": "incident--9940dbc8-facd-5e08-8326-7af7875e961c",
      "created": "2025-06-16T00:00:00.000Z",
      "modified": "2025-06-17T02:02:50.876Z",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff",
          "luminar_threat_score": 121,
          "collection_date": "2025-06-16T19:00:28.832Z",
          "computer_name": "CHRISSUPERSERVE"
        }
      },
      "name": "@RATCLOUDS_-_775626_LINES_06.16.2025.txt",
      "description": "The following credentials were shared on Telegram,
channel id: 2188311851, on 2025-06-16. They were extracted from a file named
\"@RATCLOUDS - 775626 LINES 06.16.2025.txt\" with a size of 37.5 MB.",
      "created_by_ref": "identity--5bf1ac35-8d08-509e-b31a-044cb09b4199"
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--81704de9-2218-513d-9221-5727a70129da",
      "created": "2025-05-11T00:00:00.000Z",
      "modified": "2025-06-17T02:02:51.271Z",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
        }
      },
      "relationship_type": "related-to",
      "source_ref": "malware--811a96f8-ffe2-53f6-9839-e7a3825b29f3",
      "target_ref": "incident--9940dbc8-facd-5e08-8326-7af7875e961c"
    },
    {
      "type": "malware",
      "spec_version": "2.1",
      "id": "malware--811a96f8-ffe2-53f6-9839-e7a3825b29f3",
      "created": "2025-05-11T00:00:00.000Z",
      "modified": "2025-06-17T02:02:51.271Z",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
        }
      },
```

```
      "name": "REDLINE",
      "capabilities": ["steals-authentication-credentials"],
      "malware_types": ["spyware"],
      "is_family": false
    }
  ]
}
```

Luminar Cognyte Cyberfeeds

The Luminar Cognyte Cyberfeeds feed fetches cyberfeed data consisting of structured threat intelligence entities such as reports, indicators, malware, vulnerabilities, and threat actors. The data is formatted using the STIX 2.1 standard and includes relationships between entities to provide rich context for threat analysis and incident response.

```
GET https://www.cyberluminar.com/externalApi/taxii/collections/
{{cyberfeeds_collection_id}}/objects/?
limit=9999&added_after=2025-06-09T03:43:16.854307Z
```

Sample Response:


```
{
  "more": true,
  "next": "p9S1AwU2Y3RpX3N0aXhfMjAyNDEyMDNfMDBiZWQ5NTQtNGIxY......",
  "objects": [
    {
      "type": "report",
      "spec_version": "2.1",
      "id": "report--dd40e0f0-50f8-5ef0-bc1d-7f4b95fb9601",
      "created": "2025-06-08T08:03:33.000Z",
      "modified": "2025-06-09T19:01:13.317Z",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
        }
      },
      "name": "From open-source to open threat: Tracking Chaos RAT\u2019s
evolution",
      "description": "Chaos RAT is an open-source, cross-platform remote access
trojan written in Golang and primarily used in real-world Linux and Windows
attacks since November 2022, with continuing updates and activity as of 2025.
Originally a legitimate remote management tool, it is now exploited by threat
actors for purposes such as espionage, data exfiltration, persistence, and
aiding post-compromise operations including ransomware deployment, often
reaching victims through phishing campaigns or malicious scripts modifying
the /etc/crontab file for persistence. Advanced persistent threat (APT) groups
use open-source RATs to evade attribution and blend into typical cybercrime
noise; Chaos RAT\u2019s low detection rates facilitate stealthy operations.
Chaos RAT\u2019s administrative panel allows payload generation, direct command
execution, and full remote control over compromised Windows and Linux systems,
with configurations and communications often protected and obfuscated using
randomized, base64-encoded fields and JSON Web Tokens for authorization.
Technical analysis revealed a critical remote code execution vulnerability in
the malware\u2019s web panel, as well as a prior cross-site scripting
vulnerability (CVE-2024-31839), both of which can be exploited for further
compromise. Recent attacks leveraged a Linux tar.gz payload disguised as a
legitimate network utility, with the malware primarily used for reconnaissance
```

```
and cryptocurrency mining, and confirmed uploads of new variants to VirusTotal
indicating ongoing threat activity.",
      "published": "2025-06-08T08:03:33.000Z",
      "report_types": ["indicator", "malware", "threat-actor",
"vulnerability"],
      "object_refs": ["indicator--8338cd68-30a2-5467-a124-391016c17d58"]
    },
    {
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator--8338cd68-30a2-5467-a124-391016c17d58",
      "created": "2025-06-18T09:41:37.000Z",
      "modified": "2025-06-18T20:31:43.676Z",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
        }
      },
      "pattern": "[file:hashes.'SHA-256' =
'a364ec51aa9314f831bc498ddaf82738766ca83b51401f77dbd857ba4e32a53b']",
      "pattern_type": "stix",
      "indicator_types": ["malicious-activity"],
      "valid_from": "2025-06-18T09:41:37.000Z"
    },
    {
      "type": "indicator",
      "spec_version": "2.1",
      "id": "indicator--3039d5d3-d1a2-5fda-b5e9-5acba9f69d33",
      "created": "2025-06-18T09:41:37.000Z",
      "modified": "2025-06-18T20:31:43.676Z",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
        }
      },
      "pattern": "[file:hashes.'SHA-256' =
'a6307aad70195369e7ca5575f1ab81c2fd82de2fe561179e38933f9da28c4850']",
      "pattern_type": "stix",
      "indicator_types": ["malicious-activity"],
      "valid_from": "2025-06-18T09:41:37.000Z"
    },
    {
      "type": "malware",
      "spec_version": "2.1",
      "id": "malware--5f7f7fff-d697-52ee-a398-7181711fb7b4",
      "created": "2025-06-17T08:10:27.000Z",
      "modified": "2025-06-17T19:00:15.347Z",
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
```

```
        "extension_type": "property-extension",
        "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
      }
    },
    "name": "AsyncRAT",
    "aliases": [],
    "malware_types": ["remote-access-trojan"],
    "is_family": false
  },
  {
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--27dec6e3-bfc8-50b8-86b7-7d11477efe79",
    "created": "2025-06-18T09:41:37.000Z",
    "modified": "2025-06-18T20:31:43.676Z",
    "extensions": {
      "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
        "extension_type": "property-extension",
        "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
      }
    },
    "name": "Chaos RAT",
    "aliases": [],
    "capabilities": ["captures-input-peripherals"],
    "malware_types": ["remote-access-trojan"],
    "is_family": false
  },
  {
    "type": "malware",
    "spec_version": "2.1",
    "id": "malware--415c6efe-2857-5179-98dc-fbe0acc140c1",
    "created": "2025-06-08T08:03:33.000Z",
    "modified": "2025-06-09T19:01:13.317Z",
    "extensions": {
      "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
        "extension_type": "property-extension",
        "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
      }
    },
    "name": "QuasarRAT",
    "aliases": [],
    "malware_types": ["remote-access-trojan"],
    "is_family": false
  },
  {
    "type": "threat-actor",
    "spec_version": "2.1",
    "id": "threat-actor--3cd8f4f3-72a4-51b0-9e4e-a7848c210e3b",
    "created": "2025-06-08T08:03:33.000Z",
    "modified": "2025-06-09T19:01:13.317Z",
```

```
      "extensions": {
        "extension-definition--ddd2bf71-3c91-5f4d-8251-10cd685737c3": {
          "extension_type": "property-extension",
          "luminar_tenant_id": "00bed954-4b1a-4d52-97f7-2a2c51b824ff"
        }
      },
      "name": "Charming Kitten",
      "description": "from Iran",
      "aliases": ["APT35"],
      "threat_actor_types": ["nation-state"]
    }
  ]
}
```

Average Feed Run

> Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Luminar Cognyte IOCs

METRIC	RESULT
Run Time	35 minutes
Adversaries	76
Adversary Attributes	135
Identity	79
Identity Attributes	158
Indicators	33,909
Indicator Attributes	328,105
Malware	34
Malware Attributes	87
Signatures	33,909

Luminar Cognyte Leaked Records

METRIC	RESULT
Run Time	2 minutes
Compromised Account	7
Account Attributes	36
Incidents	1,639
Incident Attributes	1,639
Malware	18
Malware Attributes	269

Luminar Cognyte Cyberfeeds

METRIC	RESULT
Run Time	1 minute
Adversaries	15
Adversary Attributes	32
Campaign	1
Campaign Attributes	1
Identity	29
Identity Attributes	58
Indicators	71
Indicator Attributes	142
Malware	7
Malware Attributes	25
Report	7
Report Attributes	7
Signatures	71
Signature Attributes	142

METRIC	RESULT
Vulnerabilities	1
Vulnerability Attributes	2

Known Issues / Limitations

- ThreatQ does not currently support `location` and `software` STIX 2.1 objects. These object types are skipped during ingestion. Only supported STIX objects and attributes are processed. Unsupported types are omitted without error. See the About STIX topic for more information on ThreatQ supported STIX types.
- Relationships involving unsupported objects are not ingested.

Change Log

- **Version 1.0.0**
  - Initial release