ThreatQuotient

Sekoia Feed Guide

Version 1.1.1

January 25, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

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.

Contents

Versioning

- Current integration version: `1.1.1`
- Supported on ThreatQ versions >= `4.42.0`

Introduction

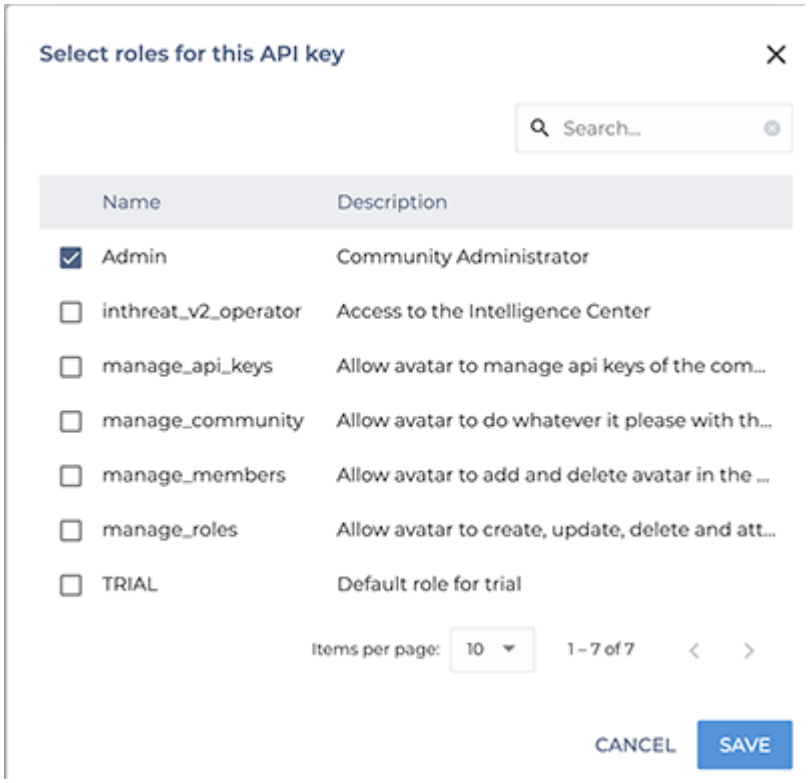
Sekoia is a French-based company that provides intelligence-driven cybersecurity. The Sekoia feed integrates with Sekoia's `InThreat` Intelligence Center API as described in Sekoia's Documentation.

Prerequisites

In order to pull data from Sekoia's Intelligence Center API, one must first generate an API key within Sekoia's UI. To do this:

1. Navigate to the User Center Communities page.
2. Click on a Community with Intelligence Center permissions to see more settings for that particular Community.
3. On the Community settings page, click the `API keys` tab and then the `+ API Key` button.
4. In the Add API Key modal, give the key an identifiable name and description.
5. On the next page, give the key the Admin role as shown below.

After clicking `Save`, copy the newly generated API key presented on the next screen and save it as it will only be displayed once. This API key should be used for the `Sekoia API Key` User Field in the ThreatQ UI.



Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the My Integrations page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

   > 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.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

Configuration

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

To configure the feed:

1. Navigate to the My Integrations 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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Sekoia Collection / Feed ID	Collection ID of the Sekoia Feed data should be pulled from. If not supplied, the default Feed will be used.
Sekoia API Key	Secret authorization key for Sekoia's API. See the **Prerequisites** section for information on generating a key within Sekoia.
Disable Proxies	Whether configured proxies should be ignored for requests made by this Feed. The default is `False`.
Enable SSL Verification	Whether the provider's SSL certificate should be verified on requests. The default is `True`.

5. Review the **Settings** configuration, 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

Sekoia

This feed targets Indicator Patterns within Sekoia Collections, pulling in each Indicator Pattern along with its accompanying context.

The first endpoint used is dynamic based on the specified `Sekoia Collection / Feed ID` User Field. If a `Sekoia Collection / Feed ID` is not specified, the default Sekoia Collection (`d6092c37-d8d7-45c3-8aff-c4dc26030608`) will be used.

```
GET https://app.sekoia.io/api/v2/inthreat/collections/{{ Sekoia Collection / Feed ID }}/patterns
```

The JSON data returned contains the object UUIDs needed to poll Sekoia's Indicator Context endpoint:

```
{
    "next_id": "indicator--c000c6f9-ef4e-4143-93e5-87c0e566e8e6",
    "items": [
        {
            "pattern": "[url:value = 'https://tny.de/Em9s?index.php?vywdbxwwquijbubkw']",
            "revoked": false,
            "modified": "2020-12-06T21:57:35.19529Z",
            "valid_from": "2020-12-06T00:00:00Z",
            "uuid": "indicator--daa711ef-9e7e-46d3-882c-d42ec6f2f0d4",
            "valid_until": "2021-06-05T00:00:00Z",
            "created": "2020-12-06T21:57:35.195307Z"
        },
        {
            "pattern": "[url:value = 'http://fb-iverifications.tk/']",
            "revoked": false,
            "modified": "2020-12-06T21:57:35.195327Z",
            "valid_from": "2020-12-06T00:00:00Z",
            "uuid": "indicator--b72c0244-58b9-413c-b034-5c4ea7fa950f",
            "valid_until": "2021-06-05T00:00:00Z",
            "created": "2020-12-06T21:57:35.195341Z"
        },
        ...
    ]
}
```

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.items[].uuid	N/A	N/A	N/A	indicator--b72c0244-58b9-413c-b034-5c4ea7fa950f	Used to poll Sekoia's Indicator Context endpoint

Sekoia Indicator Context

Supplemental feed to poll Sekoia's Indicator Context endpoint for each Indicator returned by the primary feed. For each Indicator, a STIX package is returned containing:

- The Indicator
- The Indicator's top-level relationships and related objects
- Potentially relevant Course-Of-Action objects
- Referenced Sources and Object Markings like TLP

```
GET https://app.sekoia.io/api/v2/inthreat/objects/{{ Indicator UUID }}/context
```

The JSON data returned is a qualified STIX bundle that is passed into ThreatQ's STIX Parser.


```
{
    "id": "bundle--6fb8fbe6-dff0-43a8-b838-e2723ca9df73",
    "type": "bundle",
    "objects": [
        {
            "kill_chain_phases": [
                {
                    "phase_name": "delivery",
                    "kill_chain_name": "lockheed-martin-cyber-kill-chain"
                },
                {
                    "phase_name": "initial-access",
                    "kill_chain_name": "mitre-attack"
                }
            ],
            "x_inthreat_sources_refs": [
                "identity--357447d7-9229-4ce1-b7fa-f1b83587048e"
            ],
            "created_by_ref": "identity--357447d7-9229-4ce1-b7fa-f1b83587048e",
            "object_marking_refs": [
                "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"
            ],
            "created": "2019-07-31T15:28:10.544209Z",
            "revoked": false,
            "pattern": "[file:hashes[*] = '3c8b026ca685673f5be574a837c4ae7e608e75a57e3eb4ebcc48f058005a8270' OR
file:hashes[*] = 'dde658eb388512ee9f4f31f0f027a7df' OR file:hashes[*] = '42782042bb64fa0b0daad35a6a4cf81ef313129f']",
            "x_ic_impacted_sectors": [],
            "valid_until": "2018-01-31T23:00:00.000Z",
            "id": "indicator--0b2dc54f-f920-4381-8e3f-492e7186d052",
            "description": "Договор намерения.chm",
            "lang": "en",
            "modified": "2019-08-01T10:49:46.360696Z",
            "indicator_types": [
                "malicious-activity"
            ],
            "x_ic_deprecated": false,
            "name": "Malicious CHM",
            "spec_version": "2.1",
            "type": "indicator",
            "x_ic_is_in_flint": false,
            "confidence": 79,
```

```
        "pattern_type": "stix",
        "valid_from": "2017-08-31T22:00:00.000Z",
        "x_ic_impacted_locations": []
    },
    {
        "external_references": [
            {
                "source_name": "SEKOIA website",
                "url": "https://www.sekoia.fr"
            }
        ],
        "object_marking_refs": [
            "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9"
        ],
        "created": "2008-01-01T00:00:00Z",
        "revoked": false,
        "x_ic_is_sector": false,
        "x_ic_impacted_sectors": [],
        "identity_class": "organization",
        "id": "identity--357447d7-9229-4ce1-b7fa-f1b83587048e",
        "x_ic_is_source": true,
        "description": "SEKOIA is a French company which applies intelligence-driven cybersecurity",
        "lang": "en",
        "modified": "2019-09-30T07:54:40.149166Z",
        "contact_information": "threatintel@sekoia.fr",
        "x_ic_deprecated": false,
        "name": "SEKOIA",
        "sectors": [
            "technology"
        ],
        "spec_version": "2.1",
        "type": "identity",
        "x_ic_is_in_flint": true,
        "confidence": 95,
        "x_ic_impacted_locations": []
    },
    {
        "id": "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da",
        "type": "marking-definition",
        "object_marking_refs": [
            "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"
        ],
        "created": "2019-10-09T16:10:07.239899Z",
        "spec_version": "2.1",
        "definition": {
            "tlp": "green"
        },
        "definition_type": "tlp",
        "name": "TLP:GREEN",
        "x_ic_deprecated": false
    },
    {
        "id": "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9",
        "type": "marking-definition",
        "object_marking_refs": [
            "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"
        ],
        "created": "2019-10-31T16:57:02.018068Z",
        "spec_version": "2.1",
        "definition": {
            "tlp": "white"
        },
        "definition_type": "tlp",
```

```
            "name": "TLP:WHITE",
            "x_ic_deprecated": false
        }
    ]
}
```

Average Feed Run

Average Feed Run results for an hourly scheduled run of Sekoia:

METRIC	RESULT
Run Time	4 minutes
Indicators	394
Indicator Attributes	2,377
Attack Patterns	1
Attack Pattern Attributes	20
Courses Of Action	6
Course Of Action Attributes	19
Identities	6
Identity Attributes	14
Malwares	11
Malware Attributes	73
Signatures	138
Signature Attributes	828

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.

Known Issues/Limitations

- Due to transient errors raised by Sekoia's server, ThreatQ recommends running this feed on an hourly period and avoiding Manual Runs longer than 2 months. Sekoia's server can sporadically throw the following errors when performing large manual runs:
  - `503 Service Unavailable`
  - `504 Gateway Time-out`
  - `[Errno 104] Connection reset by peer`
- ThreatQ's STIX Parser does not currently handle custom STIX 2 attributes beginning with `x_`, such as `x_ic_impacted_sectors`
- Sekoia uses an unconventional method of providing file hashes in their STIX Indicator Patterns that is not supported by the STIX spec. As a result, the ThreatQ STIX Parser may fail to parse out Indicator objects from these Pattern strings.

Change Log

- **Version 1.1.1**
  - Fixed a pagination issue that would cause Sekoia feed runs to fail to complete.
- **Version 1.1.0**
  - Feed revamp and initial release
- **Version 1.0.0**
  - Initial beta development