Seqrite Threat Feed

User Guide

Version 1.0

January 5, 2024

Contents

Introduction

Threat intelligence feeds provide automated streams of useful threat information that enterprises can ingest into their security tools and platforms to block threats or derive helpful insights. This information includes traditional indicators of compromise (IoCs) such as malicious Domains, URLs, IP addresses, Malware hashes, and more.

Seqrite Labs is processing and detecting millions of threats every day. Information related to threats are messaged and put together in STIX format and delivered to customers via TAXII server. The following page details how you can obtain Cyber Threat Intelligence (CTI) using the Trusted Automated Exchange of Intelligence Information (TAXII) services.

What is STIX?

- Structured Threat Information eXpression or **STIX**, is a language format used to exchange CTI (Cyber Threat Intelligence). The STIX format is used to show information related to **indicator objects**, **malware objects** and **relationship objects**. Relationship objects link a common association between indicator and malware objects.

- The STIX feed is in a standardized JSON format and conveys CTI data that can be easily understood. It represents the common language where both entities, client, and server, can use STIX for a common method of communication.

What is TAXII?

- Trusted Automated Exchange of Intelligence Information or **TAXII** , is a transport protocol used to exchange CTI data over Hyper Text Transfer Protocol Secure (HTTPS).

- TAXII enables companies like Seqrite, to share CTI with other users by defining an API that aligns with common sharing models.

- TAXII is specifically designed to support the exchange of CTI represented in **STIX** format.

The TAXII and STIX Relationship

- The open-source projects of TAXII and STIX standards were developed by the **OASIS CTI Technical Committee** for the prevention and mitigation of cyber-attacks. STIX indicates the cyber threat intelligence data and TAXII is the vehicle for the exchange of that information.

- TAXII is the mechanism for transport of CTI represented in STIX format. You can use TAXII services to share cyber threat information in a secure and automated manner.

Relationship between Feeds and Collections

- As mentioned, STIX provides CTI data Feeds in JSON format. Feeds contain CTI data from Collections.
- A TAXII Collection is an interface to a database of CTI objects provided by a TAXII Server. It is used by TAXII Clients to request information from the TAXII Server.
- It is common to use the term Feeds when referring to STIX CTI threat data with the understanding that what comprises a CTI Feed is information from a Collection of CTI objects.

Feeds and Collection available from Seqrite Threat Feed

Collection ID	**Collection Title**	**Description**
b5a0bc3a-aad6-11ee-807a-325096b39f47	Malicious File	This collection contains malwares hashes which are currently active in-field.
b5a0be38-aad6-11ee-b32a-325096b39f47	Malicious IP (India Specific)	This collection contains IPs being used for performing malicious activities primarily on Indian territory.
b5a0bea6-aad6-11ee-8215-325096b39f47	Malicious IP (Zero Day)	This collection contains IPs being used for malicious activities but seen by Seqrite Labs for the first time.
b5a0bfd2-aad6-11ee-b815-325096b39f47	Malicious IP (Global Threats)	This collection contains IPs being used for malicious activities across the globe.
b5a0c018-aad6-11ee-af09-325096b39f47	Malicious Domain (India Specific)	This collection contains Domains being used for performing malicious activities primarily on Indian territory.
b5a0c072-aad6-11ee-8131-325096b39f47	Malicious Domain (Zero Day)	This collection contains Domains being used for malicious activities but seen by Seqrite Labs for the first time.
b5a0c0e0-aad6-11ee-a233-325096b39f47	Malicious Domain (Global Threats)	This collection contains Domains being used for malicious activities across the globe.
b5a0c13a-aad6-11ee-8ca6-325096b39f47	Malicious URL (India Specific)	This collection contains URLs being used for performing malicious activities primarily on Indian territory.
b5a0c19e-aad6-11ee-93f8-325096b39f47	Malicious URL (Zero Day)	This collection contains URLs being used for malicious activities but seen by Seqrite Labs for the first time.
b5a0c202-aad6-11ee-b1e7-325096b39f47	Malicious URL (Global Threats)	This collection contains URLs being used for malicious activities across the globe.

Feed Format and Example

Seqrite Threat Intel Feeds are available for polling from a Seqrite TAXII Server. One feed file represents one STIX report which contains list of multiple IOCs such as IP, Domain, URL or File Hash generated within a time interval.

For example, the following STIX report consists of 5 malicious URLs.


```
{
    "type": "bundle",
    "id": "bundle--1d45b200-16a8-4b17-beb2-f1fd2011a196",
    "objects": [
        {
            "type": "identity",
            "spec_version": "2.1",
            "id": "identity--f360e704-0941-44fe-932c-1cc3ec1949ab",
            "created": "2023-12-17T16:28:24.226308Z",
            "modified": "2023-12-17T16:28:24.226308Z",
            "name": "Quick Heal Technologies Limited",
            "identity_class": "organization",
            "sectors": [
                "technology"
            ],
            "contact_information": "DA@quickheal.com"
        },
        {
            "type": "report",
            "spec_version": "2.1",
            "id": "report--eaf82737-f79a-426d-b15c-052cc9f80e5f",
            "created_by_ref": "identity--f360e704-0941-44fe-932c-1cc3ec1949ab",
            "created": "2023-12-17T16:28:24.244307Z",
            "modified": "2023-12-17T16:28:24.244307Z",
            "name": "Malicious_URL_report",
            "description": "Malicious URLs detected from Quick Heal Antivirus",
```

```
        "published": "2023-12-17T15:27:17.497225Z",
        "object_refs": [
                "indicator--4c5f24ab-8b79-4be7-9146-698a7eec15ea",
                "indicator--88280143-3858-4310-86d9-d1d22e45f793",
                "indicator--63e4af65-90c1-4931-8ad2-a43408cd67c2",
                "indicator--deeba6ba-cff7-492a-864a-e135e35e5d50",
                "indicator--0f5d5cfe-0a0d-463c-8974-a0d1cc3bfa3c"
        ]
},
{
        "type": "indicator",
        "spec_version": "2.1",
        "id": "indicator--4c5f24ab-8b79-4be7-9146-698a7eec15ea",
        "created": "2023-12-17T15:27:17.497225Z",
        "modified": "2023-12-17T15:27:17.497225Z",
        "name": "Malicious_URL0",
        "description": "This Domain is Malicious",
        "indicator_types": [
                "malicious-activity"
        ],
        "pattern": "[url:value = '95.211.187.170/upg/LAUNCHMGR.DLL.gz']",
        "pattern_type": "stix",
        "pattern_version": "2.1",
        "valid_from": "2023-12-17T16:28:24.226308Z"
},
{
        "type": "indicator",
        "spec_version": "2.1",
        "id": "indicator--88280143-3858-4310-86d9-d1d22e45f793",
        "created": "2023-12-17T15:27:17.497225Z",
        "modified": "2023-12-17T15:27:17.497225Z",
```

```
        "name": "Malicious_URL1",
        "description": "This Domain is Malicious",
        "indicator_types": [
                "malicious-activity"
        ],
        "pattern": "[url:value = 'besttenns.live/out_photo/1012_.jpg']",
        "pattern_type": "stix",
        "pattern_version": "2.1",
        "valid_from": "2023-12-17T16:28:24.228313Z"
},
{
        "type": "indicator",
        "spec_version": "2.1",
        "id": "indicator--63e4af65-90c1-4931-8ad2-a43408cd67c2",
        "created": "2023-12-17T15:27:17.497225Z",
        "modified": "2023-12-17T15:27:17.497225Z",
        "name": "Malicious_URL2",
        "description": "This Domain is Malicious",
        "indicator_types": [
                "malicious-activity"
        ],
        "pattern": "[url:value = 'adssa.banketas.com:8080/ny4']",
        "pattern_type": "stix",
        "pattern_version": "2.1",
        "valid_from": "2023-12-17T16:28:24.230312Z"
},
{
        "type": "indicator",
        "spec_version": "2.1",
        "id": "indicator--deeba6ba-cff7-492a-864a-e135e35e5d50",
        "created": "2023-12-17T15:27:17.497225Z",
```

```
            "modified": "2023-12-17T15:27:17.497225Z",
            "name": "Malicious_URL3",
            "description": "This Domain is Malicious",
            "indicator_types": [
                "malicious-activity"
            ],
            "pattern": "[url:value = '112.26.121.7:19139/3EBCE3A4.Png']",
            "pattern_type": "stix",
            "pattern_version": "2.1",
            "valid_from": "2023-12-17T16:28:24.23131Z"
        },
        {
            "type": "indicator",
            "spec_version": "2.1",
            "id": "indicator--0f5d5cfe-0a0d-463c-8974-a0d1cc3bfa3c",
            "created": "2023-12-17T15:27:17.497225Z",
            "modified": "2023-12-17T15:27:17.497225Z",
            "name": "Malicious_URL4",
            "description": "This Domain is Malicious",
            "indicator_types": [
                "malicious-activity"
            ],
            "pattern": "[url:value = 'www.discoverysaddles.com.au/wp-login.php']",
            "pattern_type": "stix",
            "pattern_version": "2.1",
            "valid_from": "2023-12-17T16:28:24.234308Z"
        }
    ]
}
```

How To Poll Feeds

Feeds from Seqrite TAXII server can be polled by calling a TAXII Rest API. Customer can use any rest API client of their choice.

To make a call to the polling API, the following parameters are required:

- API URL: https://threat-feed.seqrite.com/{api_root}/collections/{collection_id}/objects/
- api_root: API root of for the API endpoints.
- collection_id: Alphanumeric ID assigned for each collection.
- user_name & password: Credentials for polling collection from TAXII server.
- x-api-key: API key for polling collection from TAXII server.
- Additional mandatory header Accept: application/taxii+json;version=2.1

API Filters

URL Query Parameters	Description	Example
added_after	A single "T-Syntax" RFC3339 time stamp that filters objects to only include those objects added after the specified time stamp. If no added_after URL query parameter is provided, the server will return the oldest objects matching the request first. For example, if a server has 100 objects (0-99), the server will start at record 0 looking for a match and work its way up from oldest to newest finding 1000 (the default & maximum limit) of objects that matched the request.	2023-12-11T07:06:39.847694Z
Limit	A single integer value that indicates the maximum	5

	number of objects to receive in a single response. This must be a positive integer greater than 1 and less than 1000.	
Next	An alphanumeric UUID is generated by server and sent back as response whenever there is more data available for polling. Same UUID should be sent as query parameter (?next=uuid) in request to poll next batch.	{base_url}/?next=8d56e147-67a9-422b-be05-bed678d3aa6c

How to get credentials for polling feeds

- Send email to Support.Threatfeed@seqrite.com requesting for credentials for polling Seqrite threat Feed.
- Mention desired user name, email address, contact number, organization detail.
- Mention your organization's Public IP so that we can whitelist specified IP for accessing APIs.
- After internal verification you will receive user_name, password, and API Key for polling feeds.
- You can poll any of the above mentioned feed collections using your credentials.
- You can use API client of your choice like Postman, Python request module or simply CURL command line.

Example API call from CURL

curl --request GET \

--url https://threat-feed.seqrite.com/{api_root}/collections/{collection_id}/objects/ \

--header 'Accept: application/taxii+json;version=2.1' \

--header 'Authorization : Basic {base64 encoded string of username:password}' \

--header 'x-api-key: {x-api-key}'

Polling the feed using script

Seqrite has created a client script for polling threat feeds from all or any specific collection. All required parameters must be filled inside the script before starting the script.

Salient points of polling script:

- {script_dir} - This is any directory on a Linux PC where the customer can store the polling script.

- Starts polling all data if script is running for the first time or poll_start_time is not set.

- Once polling session finishes, last_poll_time is stored in a text file ({script_dir}/last_poll_time_stamp.txt) in the same directory where the client script is stored.

- last_poll_time_stamp.txt is used in subsequent polling as start point so that only new data is polled.

- Script polls data in batches, default batch size is 10 feeds, but user can reduce batch size if required.

- Data that is being polled in a session is stored inside folder. {script_dir}/objects/{current_time_stamp_epoch}/objects.json

- Apart from raw feeds (STIX Bundle), polling script also extracts important fields such as IP, Domain, URLs, MD5, etc from the feed and stores them in a CSV file at {script_dir}/objects/{current_time_stamp_epoch}/md5.csv. Customer can use this CSV file to feed into their threat platform.

Important Notes

- Feeds are published 24x7 so it is suggested to schedule polling on hourly basis.
- One feed bundle is a report of multiple IOCs (IP/Domain/URL/File Hash).
- Feeds are stored on server for limited period. For example, Files Hash feed is retained only for 3 days and for IP, Domain and URLs, feeds are retained for 30 days.