ThreatQuotient

A Securonix Company



Securonix OSINT CDF

Version 2.1.0

October 13, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
Securonix Blog Parameters 9
Securonix Autonomous Threat Sweeper IOCs Parameters 11
Securonix Connect Parameters 12
ThreatQ Mapping **13**
Securonix Blog 13
Securonix Autonomous Threat Sweeper IOCs 14
Commit Details 17
IOC / README Change 21
Securonix Connect 21
Average Feed Run **23**
Securonix Blog 23
Securonix Autonomous Threat Sweeper IOCs 23
Securonix Connect 24
Known Issues / Limitations **25**
Change Log **26**

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.

Copyright © 2026 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

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

Support Email: tq-support@securonix.com
Support Web: https://ts.securonix.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	2.1.0
Compatible with ThreatQ Versions	>= 5.5.0
Support Tier	ThreatQ Supported

Introduction

The Securonix OSINT CDF integration is a collection of open-source intelligence, consisting of blog posts and curated tactical indicators, published by Securonix. The integration enables analysts to stay on top of emerging threats and other TTPs used by threat actors based on the latest research from Securonix as well as provide curated intelligence from OSINT sources for infrastructure sweeps.

The integration includes the following feeds:

- **Securonix Blog** - fetches, parses, and ingests posts from Securonix's blog: www.securonix.com/blog.
- **Securonix Autonomous Threat Sweeper IOCs** - fetches curated tactical indicators from Securonix's Autonomous Threat Sweeper GitHub repository.
- **Securonix Connect** - fetches, parses, and ingests Threat Research and Intelligence posts from the Securonix Connect Community page.

The integration ingests the following object types:

- Attack Patterns
- Indicators
- Reports
    - Report Attributes
- Vulnerabilities

Prerequisites

The following is recommended to optimize integration performance:

- Optional - a GitHub API Token (Personal Access Token) to increase the rate limit. This will allow you to pull data from the API without running into rate limits. Authenticated users have a 5000 requests per hour limit.
- MITRE ATT&CK Patterns - attack patterns must have already been ingested by a previous run of the **MITRE ATT&CK CDF** feeds to be correctly related to the attack patterns ingested by the Securonix Blog feed. The feeds within the MITRE ATT&CK CDF include:
  - MITRE Enterprise ATT&CK
  - MITRE Mobile ATT&CK
  - MITRE ICS ATT&CK

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. 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
6. 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 **OSINT** 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:

Securonix Blog Parameters

PARAMETER	DESCRIPTION
Topics	**Topics**: Select the categories of blog posts to pull from The Record. Options include: ◦ All Topics ◦ Threat Research *(default)* ◦ Cloud Security ◦ Company Insights ◦ Cybersecurity Basics ◦ Cybersecurity Policies and Regulations ◦ Incident Response and Forensics ◦ Information Security ◦ Insider Threat ◦ Network Security ◦ Partner

PARAMETER	DESCRIPTION
	◦ Security Analytics ◦ SIEM ◦ SOAR ◦ UEBA Selecting **All Topics** includes every category and overrides individual selections.
Parse for MITRE ATT&CK Techniques	Enable this parameter to parse the content for each post for MITRE ATT&CK Techniques (Attack Patterns). This parameter is enabled by default.
Parsed IOC Types	Select which IOC types to automatically parse from the content of each post. Options include: ◦ CIDR Blocks ◦ CVEs *(default)* ◦ Email Addresses ◦ Filenames ◦ File Paths ◦ FQDNs ◦ IP Addresses ◦ MD5 *(default)* ◦ SHA-1 *(default)* ◦ SHA-256 *(default)* ◦ SHA-384 ◦ SHA-512 *(default)* ◦ URLs
Ingest CVEs As	Select which entity type to ingest CVE IDs as in ThreatQ. Options include:

PARAMETER	DESCRIPTION
	◦ Vulnerabilities *(default)* ◦ Indicators (Type: CVE)
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.

Securonix Autonomous Threat Sweeper IOCs Parameters

PARAMETER	DESCRIPTION
GitHub API Token	Optional - enter your GitHub API Token (Personal Access Token) to increase the rate limit. This will allow the integration to pull data from the API without running into rate limits.  Authenticated users have a 5000 requests per hour limit.
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.

Securonix Connect Parameters

PARAMETER	DESCRIPTION
Parse for MITRE ATT&CK Techniques	Enable this parameter to parse the content of each blog for MITRE ATTCK Techniques (Attack Patterns).
Parsed IOC Types	Select which IOC types to automatically parse from the content from each blog. Options include: ◦ CIDR Blocks ◦ CVEs *(default)* ◦ Email Addresses ◦ Filenames ◦ File Paths ◦ FQDNs ◦ IP Addresses ◦ MD5 *(default)* ◦ SHA-1 *(default)* ◦ SHA-256 *(default)* ◦ SHA-384 ◦ SHA-512 *(default)* ◦ URLs
Ingest CVEs As	Select which entity type to ingest CVE IDs as in ThreatQ. Options include: ◦ Vulnerabilities *(default)* ◦ Indicators (Type: CVE)
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

Securonix Blog

The Securonix Blog feed pulls posts from Securonix's blog which contains information on the latest threats, vulnerabilities, and security research. You can subscribe to different topics within the blog to filter the content you want to ingest - see the **Topics** configuration parameter for a list of available topics. .

```
GET https://www.securonix.com/blog/
```

This request returns HTML, which is parsed for links to the blog posts. The full blog post content is then fetched.

```
GET https://www.securonix.com/{{ uri }}
```

This request returns HTML, which is parsed for the following fields:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Report.Title	Report	.published_at	Hunting Kerbrute: Analysis, Detection and Mitigation of Kerberos Attacks in Active Directory	Parsed from the HTML
N/A	Report.Description	N/A	N/A	N/A	Parsed from the HTML
N/A	Report.Attribute	Published At	.published_at	April 5, 2025	N/A
N/A	Report.Attribute	Category	.published_at	Threat Research	Parsed from the HTML
N/A	Report.Attribute	Author	.published_at	Kumaramanivel Ramanathan	Parsed from the article byline when present
N/A	Report.Attribute	External Reference	.published_at	https://www.securonix.com/blog/.../	Original blog post URL
N/A	Report.Tags	N/A	N/A	Threat Research	Parsed from the HTML
N/A	Related Indicator.Value	Various Types	N/A	N/A	User-configurable. Indicators parsed from HTML content based on user-field selection
N/A	Related Attack-Pattern.Value	Attack Pattern	N/A	T1087 - <technique name>	User-configurable. Techniques parsed from HTML content based on user-field selection

Securonix Autonomous Threat Sweeper IOCs

The Securonix Autonomous Threat Sweeper IOCs feed pulls posts from indicators of compromise from Securonix's Autonomous Threat Sweeper GitHub repository. The feed fetches the latest indicators and parses them for various types of IOCs, including, but not limited to, IP addresses, domain names, and file hashes.

```
GET https://api.github.com/repos/Securonix/AutonomousThreatSweeper/commits
```

Sample Response:


```
[
  {
    "sha": "64a34290afb744343ec991d68ceec5efefab6bad",
    "node_id":
"C_kwDOFXTfFdoAKDY0YTM0MjkwYWZiNzQ0MzQzZWM5OTFkNjhjZWVjNWVmZWZhYjZiYWQ",
    "commit": {
      "author": {
        "name": "artemis",
        "email": "artemis@securonix.com",
        "date": "2025-07-02T16:16:34Z"
      },
      "committer": {
        "name": "artemis",
        "email": "artemis@securonix.com",
        "date": "2025-07-02T16:16:34Z"
      },
      "message": "Committing Spotter Queries for:
Janela_RAT_with_Chromium_Stealer_Extension",
      "tree": {
        "sha": "8df337b7a64b6b2ce96a45e67e2cc984f4af1282",
        "url": "https://api.github.com/repos/Securonix/
AutonomousThreatSweeper/git/trees/
8df337b7a64b6b2ce96a45e67e2cc984f4af1282"
      },
      "url": "https://api.github.com/repos/Securonix/
AutonomousThreatSweeper/git/commits/
64a34290afb744343ec991d68ceec5efefab6bad",
      "comment_count": 0,
      "verification": {
        "verified": false,
```

```
        "reason": "unsigned",
        "signature": null,
        "payload": null,
        "verified_at": null
      }
    },
    "url": "https://api.github.com/repos/Securonix/
AutonomousThreatSweeper/commits/
64a34290afb744343ec991d68ceec5efefab6bad",
    "html_url": "https://github.com/Securonix/
AutonomousThreatSweeper/commit/
64a34290afb744343ec991d68ceec5efefab6bad",
    "comments_url": "https://api.github.com/repos/Securonix/
AutonomousThreatSweeper/commits/
64a34290afb744343ec991d68ceec5efefab6bad/comments",
    "author": {
      "login": "artemissnx",
      "id": 82166862,
      "node_id": "MDQ6VXNlcjgyMTY2ODYy",
      "avatar_url": "https://avatars.githubusercontent.com/u/
82166862?v=4",
      "gravatar_id": "",
      "url": "https://api.github.com/users/artemissnx",
      "html_url": "https://github.com/artemissnx",
      "followers_url": "https://api.github.com/users/artemissnx/
followers",
      "following_url": "https://api.github.com/users/artemissnx/
following{/other_user}",
      "gists_url": "https://api.github.com/users/artemissnx/gists{/
gist_id}",
      "starred_url": "https://api.github.com/users/artemissnx/
starred{/owner}{/repo}",
      "subscriptions_url": "https://api.github.com/users/artemissnx/
subscriptions",
      "organizations_url": "https://api.github.com/users/artemissnx/
orgs",
      "repos_url": "https://api.github.com/users/artemissnx/repos",
      "events_url": "https://api.github.com/users/artemissnx/events{/
privacy}",
      "received_events_url": "https://api.github.com/users/
artemissnx/received_events",
      "type": "User",
```

```
      "user_view_type": "public",
      "site_admin": false
    },
    "committer": {
      "login": "artemissnx",
      "id": 82166862,
      "node_id": "MDQ6VXNlcjgyMTY2ODYy",
      "avatar_url": "https://avatars.githubusercontent.com/u/
82166862?v=4",
      "gravatar_id": "",
      "url": "https://api.github.com/users/artemissnx",
      "html_url": "https://github.com/artemissnx",
      "followers_url": "https://api.github.com/users/artemissnx/
followers",
      "following_url": "https://api.github.com/users/artemissnx/
following{/other_user}",
      "gists_url": "https://api.github.com/users/artemissnx/gists{/
gist_id}",
      "starred_url": "https://api.github.com/users/artemissnx/
starred{/owner}{/repo}",
      "subscriptions_url": "https://api.github.com/users/artemissnx/
subscriptions",
      "organizations_url": "https://api.github.com/users/artemissnx/
orgs",
      "repos_url": "https://api.github.com/users/artemissnx/repos",
      "events_url": "https://api.github.com/users/artemissnx/events{/
privacy}",
      "received_events_url": "https://api.github.com/users/
artemissnx/received_events",
      "type": "User",
      "user_view_type": "public",
      "site_admin": false
    },
    "parents": [
      {
        "sha": "f0018bccfa9fb6e52acd29cb98ce42bb56a835b1",
        "url": "https://api.github.com/repos/Securonix/
AutonomousThreatSweeper/commits/
f0018bccfa9fb6e52acd29cb98ce42bb56a835b1",
        "html_url": "https://github.com/Securonix/
AutonomousThreatSweeper/commit/
f0018bccfa9fb6e52acd29cb98ce42bb56a835b1"
```

```
      }
    ]
  }
]
```

Commit Details

The feed fetches the commit details for each acceptable commit.

`GET https://api.github.com/repos/Securonix/AutonomousThreatSweeper/commits/{{ sha }}`

Sample Response:

```
{
  "sha": "64a34290afb744343ec991d68ceec5efefab6bad",
  "node_id":
"C_kwDOFXTfFdoAKDY0YTM0MjkwYWZiNzQ0MzQzZWM5OTFkNjhjZWVjNWVmZWZhYjZiYWQ",
  "commit": {
    "author": {
      "name": "artemis",
      "email": "artemis@securonix.com",
      "date": "2025-07-02T16:16:34Z"
    },
    "committer": {
      "name": "artemis",
      "email": "artemis@securonix.com",
      "date": "2025-07-02T16:16:34Z"
    },
    "message": "Committing Spotter Queries for:
Janela_RAT_with_Chromium_Stealer_Extension",
    "tree": {
      "sha": "8df337b7a64b6b2ce96a45e67e2cc984f4af1282",
      "url": "https://api.github.com/repos/Securonix/
AutonomousThreatSweeper/git/trees/
8df337b7a64b6b2ce96a45e67e2cc984f4af1282"
    },
    "url": "https://api.github.com/repos/Securonix/
AutonomousThreatSweeper/git/commits/
64a34290afb744343ec991d68ceec5efefab6bad",
    "comment_count": 0,
    "verification": {
```

```
      "verified": false,
      "reason": "unsigned",
      "signature": null,
      "payload": null,
      "verified_at": null
    }
  },
  "url": "https://api.github.com/repos/Securonix/
AutonomousThreatSweeper/commits/
64a34290afb744343ec991d68ceec5efefab6bad",
  "html_url": "https://github.com/Securonix/AutonomousThreatSweeper/
commit/64a34290afb744343ec991d68ceec5efefab6bad",
  "comments_url": "https://api.github.com/repos/Securonix/
AutonomousThreatSweeper/commits/
64a34290afb744343ec991d68ceec5efefab6bad/comments",
  "author": {
    "login": "artemissnx",
    "id": 82166862,
    "node_id": "MDQ6VXNlcjgyMTY2ODYy",
    "avatar_url": "https://avatars.githubusercontent.com/u/82166862?
v=4",
    "gravatar_id": "",
    "url": "https://api.github.com/users/artemissnx",
    "html_url": "https://github.com/artemissnx",
    "followers_url": "https://api.github.com/users/artemissnx/
followers",
    "following_url": "https://api.github.com/users/artemissnx/
following{/other_user}",
    "gists_url": "https://api.github.com/users/artemissnx/gists{/
gist_id}",
    "starred_url": "https://api.github.com/users/artemissnx/starred{/
owner}{/repo}",
    "subscriptions_url": "https://api.github.com/users/artemissnx/
subscriptions",
    "organizations_url": "https://api.github.com/users/artemissnx/
orgs",
    "repos_url": "https://api.github.com/users/artemissnx/repos",
    "events_url": "https://api.github.com/users/artemissnx/events{/
privacy}",
    "received_events_url": "https://api.github.com/users/artemissnx/
received_events",
    "type": "User",
```

```
    "user_view_type": "public",
    "site_admin": false
  },
  "committer": {
    "login": "artemissnx",
    "id": 82166862,
    "node_id": "MDQ6VXNlcjgyMTY2ODYy",
    "avatar_url": "https://avatars.githubusercontent.com/u/82166862?
v=4",
    "gravatar_id": "",
    "url": "https://api.github.com/users/artemissnx",
    "html_url": "https://github.com/artemissnx",
    "followers_url": "https://api.github.com/users/artemissnx/
followers",
    "following_url": "https://api.github.com/users/artemissnx/
following{/other_user}",
    "gists_url": "https://api.github.com/users/artemissnx/gists{/
gist_id}",
    "starred_url": "https://api.github.com/users/artemissnx/starred{/
owner}{/repo}",
    "subscriptions_url": "https://api.github.com/users/artemissnx/
subscriptions",
    "organizations_url": "https://api.github.com/users/artemissnx/
orgs",
    "repos_url": "https://api.github.com/users/artemissnx/repos",
    "events_url": "https://api.github.com/users/artemissnx/events{/
privacy}",
    "received_events_url": "https://api.github.com/users/artemissnx/
received_events",
    "type": "User",
    "user_view_type": "public",
    "site_admin": false
  },
  "parents": [
    {
      "sha": "f0018bccfa9fb6e52acd29cb98ce42bb56a835b1",
      "url": "https://api.github.com/repos/Securonix/
AutonomousThreatSweeper/commits/
f0018bccfa9fb6e52acd29cb98ce42bb56a835b1",
      "html_url": "https://github.com/Securonix/
AutonomousThreatSweeper/commit/
f0018bccfa9fb6e52acd29cb98ce42bb56a835b1"
```

```
    }
  ],
  "stats": {
    "total": 4026,
    "additions": 2128,
    "deletions": 1898
  },
  "files": [
    {
      "sha": "91098037005d20ee0fa4ba19589499d8c0c31353",
      "filename": "Janela_RAT_with_Chromium_Stealer_Extension/
README.md",
      "status": "added",
      "additions": 21,
      "deletions": 0,
      "changes": 21,
      "blob_url": "https://github.com/Securonix/
AutonomousThreatSweeper/blob/
64a34290afb744343ec991d68ceec5efefab6bad/
Janela_RAT_with_Chromium_Stealer_Extension%2FREADME.md",
      "raw_url": "https://github.com/Securonix/
AutonomousThreatSweeper/raw/64a34290afb744343ec991d68ceec5efefab6bad/
Janela_RAT_with_Chromium_Stealer_Extension%2FREADME.md",
      "contents_url": "https://api.github.com/repos/Securonix/
AutonomousThreatSweeper/contents/
Janela_RAT_with_Chromium_Stealer_Extension%2FREADME.md?
ref=64a34290afb744343ec991d68ceec5efefab6bad",
      "patch": "@@ -0,0 +1,21 @@\n+\n+## IOCs\n+\n+__domain__:\n+
\n+```text\n+team000analytics.safepurelink.com\n+w51w.worldassitencia
.com\n+bulder.wordsuporttsk.com\n+```\n+__hash__:\n+
\n+```text\n+da6b97b245c65193eb231de0314508759a69db35a8f76afc66b47577
02a231d0\n+248ee6233a85daaa3ddc2d9aaf6f24a26969a1f46981aa2a13af0c661f
e006d8\n+666ba2708be3fc6a208d1e961af343a8105959fa87bfd3322a36d6c4e57d
1122\n+6ed7ec9d0c366310d647f44830a6b9bc353a0d8b9e3345253c770bb23a90bd
d3\n+97364179ab942af483b973653b89c0dfb8ed5c7d56ed62dbbf7a62933c473fa6
\n+e2a86247b7089a5ffb4d0a3c421cedc044c744d37852ebac17291855c54713cf\n
+e200158dcca9b28c65d297cc2ff44a2183d8228568c2ebf98ac888d494e18649\n+`
``\n\\ No newline at end of file"
    }
  ]
}
```

IOC / README Change

The file content is fetched for each change to an IOC or README file.

```
GET https://github.com/Securonix/AutonomousThreatSweeper/raw/
{{ sha }}/{{ path }}%2FREADME.md
```

Sample Response:

````
## IOCs
**domain**:
```text
team000analytics.safepurelink.com
w51w.worldassitencia.com
bulder.wordsuporttsk.com
```
````

hash:

```
da6b97b245c65193eb231de0314508759a69db35a8f76afc66b4757702a231d0
248ee6233a85daaa3ddc2d9aaf6f24a26969a1f46981aa2a13af0c661fe006d8
666ba2708be3fc6a208d1e961af343a8105959fa87bfd3322a36d6c4e57d1122
6ed7ec9d0c366310d647f44830a6b9bc353a0d8b9e3345253c770bb23a90bdd3
97364179ab942af483b973653b89c0dfb8ed5c7d56ed62dbbf7a62933c473fa6
e2a86247b7089a5ffb4d0a3c421cedc044c744d37852ebac17291855c54713cf
e200158dcca9b28c65d297cc2ff44a2183d8228568c2ebf98ac888d494e18649
```

The `README.md` file contains the IOCs, which are parsed and ingested into ThreatQ using the mapping provided below.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Indicator.Value	MD5, SHA-1, SHA-256, SHA-512, FQDN, IP Address, URL	N/A	N/A	Parsed from the content
N/A	Indicator.Attribute	Threat Summary	Janela RAT with Chromium Stealer Extension	N/A	GitHub repository parent path

Securonix Connect

The Securonix Connect feed pulls posts from Securonix's Connect Community page, which contains information on the latest threats, vulnerabilities, and security research.

```
GET https://connect.securonix.com/threat-research-intelligence-62
```

This request returns HTML, which is parsed for links to the posts. The full post content is then fetched.

```
GET https://connect.securonix.com/threat-research-intelligence-62/{{ uri }}
```

This request returns HTML, which is parsed for the following fields:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Report.Title	Report	.published_at	Securonix Threat Research (STR) Monthly Newsletter - November 2025 Edition -	Parsed from the HTML
N/A	Report.Description	N/A	N/A	Welcome back to another newsletter by the Securonix Threat Research Team!	Parsed from the HTML
N/A	Report.Attribute	Published At	.published_at	December 03, 2025	N/A
N/A	Report.Attribute	Author	.published_at	Aaron Beardslee	Parsed from the HTML
N/A	Report.Attribute	External Reference	.published_at	https://connect.securonix.com/threat-research-intelligence-62/{uri}	Parsed from the HTML
N/A	Related Indicator.Value	Various Types	N/A	abd73e21cabebdfecfff7294a6f8e4abf9de08cd	User-configurable. Indicators parsed from HTML content based on user-field selection
N/A	Related Vulnerability.Value	Vulnerability	N/A	CVE-2025-24893	User-configurable. Indicators parsed from HTML content based on user-field selection
N/A	Related Attack-Pattern.Value	Attack Pattern	N/A	T1496	User-configurable. Techniques parsed from HTML content based on user-field selection

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.

Securonix Blog

METRIC	RESULT
Run Time	1 minute
Reports	10
Report Attributes	20
Attack Patterns	33
Indicators	217
Vulnerabilities	41

Securonix Autonomous Threat Sweeper IOCs

METRIC	RESULT
Run Time	1 minute
Indicators	60
Indicator Attributes	60

Securonix Connect

METRIC	RESULT
Run Time	1 minute
Reports	2
Report Attributes	6
Attack Patterns	43
Indicators	13
Vulnerabilities	1

Known Issues / Limitations

- Securonix Blog feed:
  - The feed will fetch, at maximum, the last 3 pages of blog posts.
  - The feed utilizes **since** and **until** dates to make sure entries are not re-ingested if they haven't been updated.
  - Run the feed manually by setting the **since** date back if you need to ingest historical blog posts.
  - Select **All Topics** to ingest reports from all current and future Securonix Blog categories. If you select individual topics, the connector ingests reports only from those selected categories.

Change Log

- **Version 2.1.0**
  - Enhanced data retrieval and topic filtering for Securonix Blog feed. Categories are now added as individual tags.
    - Added an **All Topics** option to the **Topics** parameter. When selected, it ingests all categories and overrides individual topic selections.
  - Improved IOC and MITRE ATT&CK parsing and added **Author** and **External Reference** report attributes.
- **Version 2.0.2**
  - Resolved an issue that caused the **Securonix Connect** feed to fail when a response contained missing or empty `div` content.
- **Version 2.0.1**
  - Improved the parsing logic for attack patterns used by the Securonix Blog feed.
- **Version 2.0.0**
  - Added a new feed: **Securonix Connect.**
- **Version 1.0.1**
  - Added improved error handling.
- **Version 1.0.0**
  - Initial release