ThreatQuotient

S2W Quaxar CDF

Version 1.0.0

September 17, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

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

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 **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.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	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

S2W Quaxar is a multi-domain cyber threat intelligence platform specializing in hidden channels and dark web intelligence. S2W provides a wide range of intelligence services, including dark web monitoring, threat intelligence, and cyber risk management. The Quaxar platform provides tailored intelligence to help organizations identify and mitigate threats to their business.

The S2W Quaxar CDF for ThreatQ enables the automatic ingestion of customized threat intelligence from Quaxar into ThreatQ. This may include leaked credentials, threat actor profiles, vulnerability reports, indicators, and much more. Ultimately, this integration allows organizations to better understand their attack surface and proactively defend against threats, by providing analysts the information they need to make informed decisions.

The integration provides the following feeds:

- **S2W Quaxar - Threat Reports** - ingests Threat Reports from S2W Quaxar, into ThreatQ
- **S2W Quaxar - Vulnerability Reports** - ingests Vulnerability Reports from S2W Quaxar, into ThreatQ
- **S2W Quaxar - Indicator Reports** - ingests Indicator Reports from S2W Quaxar, into ThreatQ
- **S2W Quaxar - Talon Reports** - ingests Talon Reports from S2W Quaxar, into ThreatQ
- **S2W Quaxar - Threat Actors** - ingests Actor Profiles from S2W Quaxar, into ThreatQ
- **S2W Quaxar - Ransomware Activity** - ingests organizations (identities) that have been affected by ransomware, from S2W Quaxar, into ThreatQ
- **S2W Quaxar - Brand Impersonation Sites** - ingests indicators associated with brand impersonation sites, from S2W Quaxar, into ThreatQ
- **S2W Quaxar - Leaked Credit Cards** - ingests Leaked Credit Cards as Indicators (type: String), from S2W Quaxar, into ThreatQ
- **S2W Quaxar - Leaked Accounts** - ingests leaked accounts (identities), from S2W Quaxar, into ThreatQ
- **S2W Quaxar - Exposed Assets** - ingests exposed asset alerts from the S2W Quaxar Attack Surface Management module, into ThreatQ
- **S2W Quaxar - Signature Vault** - ingests Snort & YARA signatures from the S2W Quaxar Signature Vault module, into ThreatQ
- **S2W Quaxar - Indicators** - ingests indicators from S2W Quaxar, into ThreatQ

The integration ingests the following system objects:

- Adversaries
- Assets
- Attack Patterns
- Campaigns
- Compromised Accounts
- Compromised Cards
- Identities
- Indicators
- Intrusion Sets
- Malware
- Reports
- Signatures
- Tools
- TTPs
- Vulnerabilities

Prerequisites

The following is required to install and run the integration:

- A S2W Quaxar License and API Credentials.

  > Depending on your license, you may not have access to all of the feeds included in the integration.

- ThreatQ Custom Objects:
  - Compromised Account
  - Compromised Card

Installing the Custom Objects

The integration requires the Compromised Account and Compromised Card custom objects. These custom objects must be installed prior to installing the CDF. ThreatQuotient provides an install script to simplify the custom object installation process.

Use the steps provided to install the required custom objects.

> 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 objects 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 following location:

   ```
   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

Use the following steps to install the custom objects in ThreatQ v5:

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 s2w_cdf
```

5. Upload the **s2w.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the s2w_cdf directory.

```
mkdir images
```

7. Upload the svg files.
8. Navigate to the **/tmp/s2w_cdf**.

   The directory should resemble the following:

   - tmp
     - **s2w_cdf**
       - **s2w.json**
       - **install.sh**
       - **images**
         - **account.svg**
         - **CompromisedCard.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 s2w_cdf
```

Installation

The integration requires two custom objects: Compromised Card and Compromised Account. These customs objects must be installed prior to attempting to install the integration. The required files for these custom objects have been bundled with the marketplace download for the integration and the steps to install these objects are provided in the Prerequistes section of this guide.

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 zip file and extract its contents.
3. Install the required Compromised Card and Compromised Acccount custom objects.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the integration file using one of the following methods:
   - Drag and drop the yaml file into the dialog box
   - Select **Click to Browse** to locate the yaml file on your local machine
7. Select the feeds to install, when prompted, and click **Install**. The feed(s) will be added to the integrations page.

   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.

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.

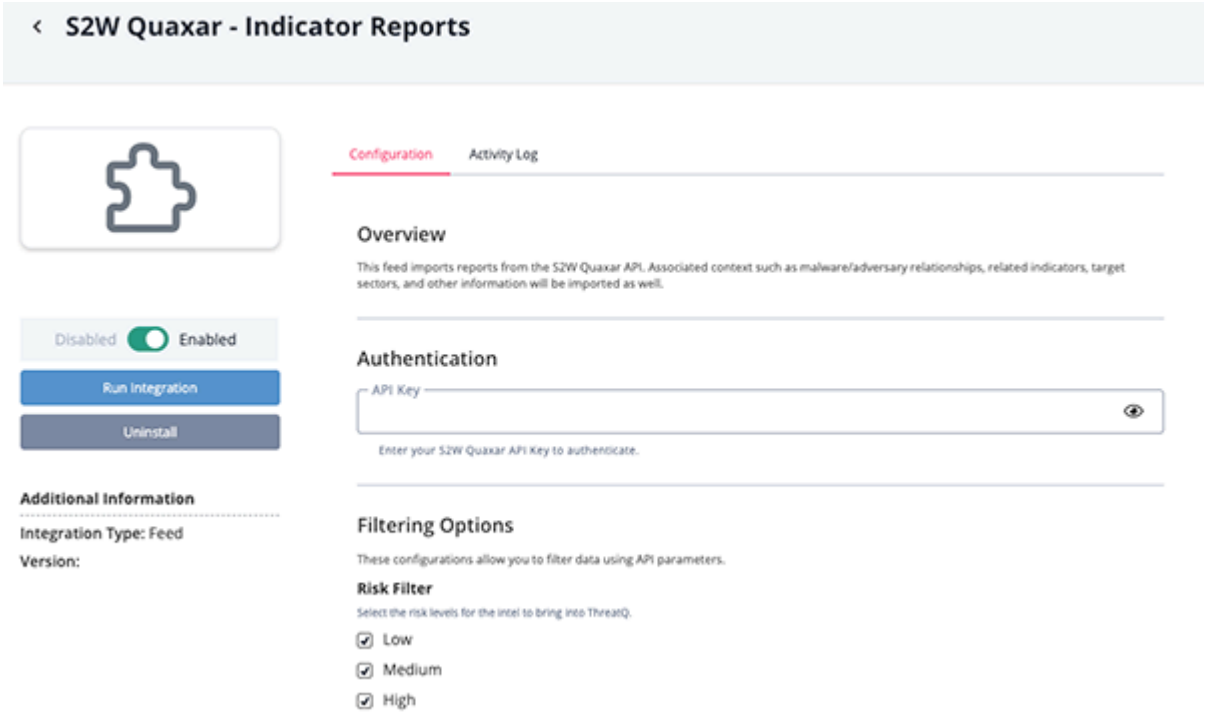
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

S2W Quaxar Reports Feeds

The parameters in the table below are for the following feeds: S2W Quaxar - Threat Reports, S2W Quaxar - Vulnerability Reports, S2W Quaxar - Indicator Reports, and S2W Quaxar - Talon Reports.

PARAMETER	DESCRIPTION
API Key	Enter your S2W Quaxar API Key.
Risk Filter	Select the risk levels for the intel to ingest into ThreatQ. Options include: ◦ Low ◦ Medium (default) ◦ High (default)
Context Filter	Select the pieces of context to bring into ThreatQ. This allows you to filter out context that your organization may not utilize. Options include: ◦ Report Type (default) ◦ Risk Score (default) ◦ Target Countries (default) ◦ Target Sectors (default) ◦ Target Regions (default) ◦ Affected Products (default)

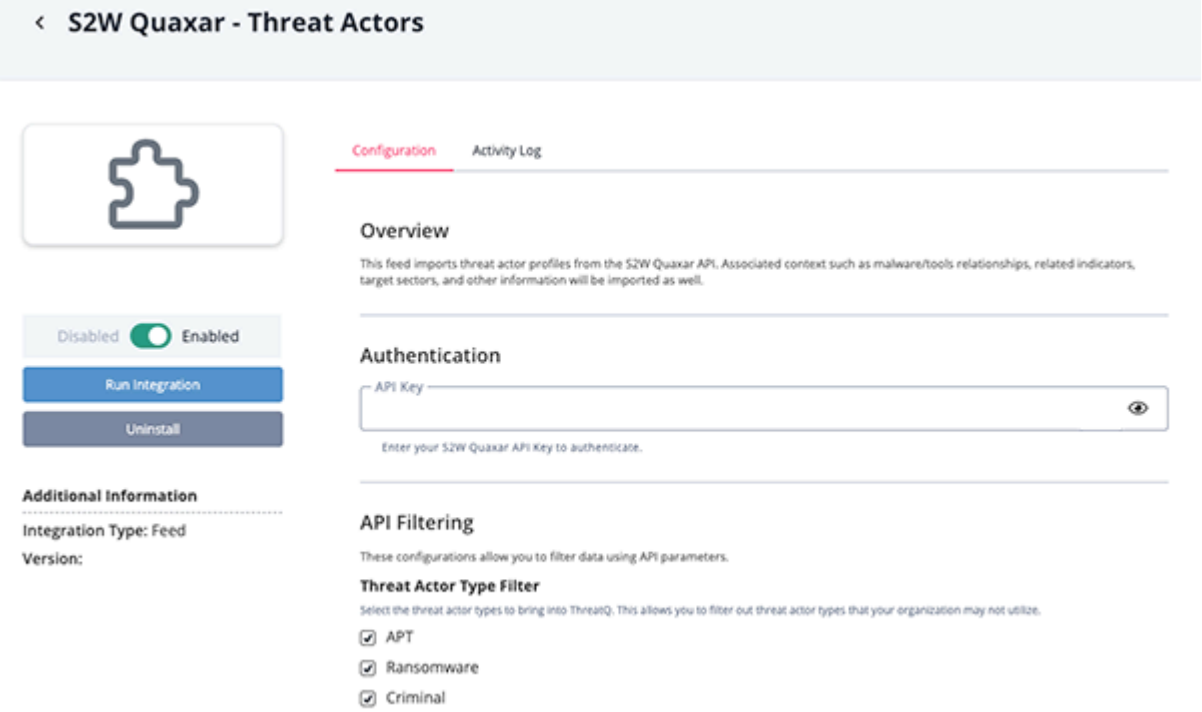
PARAMETER	DESCRIPTION
Relationship Context Filter	Select the relationships to bring into ThreatQ. This allows you to filter out context that your organization may not utilize. Options include: ◦ Indicators (default) ◦ Adversaries (default) ◦ Attack Patterns (default) ◦ Campaigns ◦ Incidents ◦ Identities ◦ Organizations (Identities) ◦ Intrusion Sets ◦ Malware (default) ◦ Tools (default) ◦ TTPs (default) ◦ Vulnerabilities (default)
Indicator Type Filter	Select the indicator types to bring into ThreatQ. This allows you to filter out indicator types that your organization may not utilize. This field will only display if the `Indicators` option is selected within the **Relationship Context Filter** field. Options include: ◦ IPv4 Address (default) ◦ IPv6 Address (default) ◦ FQDN (default) ◦ URL (default) ◦ Email Address (default) ◦ MD5 (default) ◦ SHA-1 (default) ◦ SHA-256 (default) ◦ HA-512 (default)



S2W Quaxar - Threat Actors

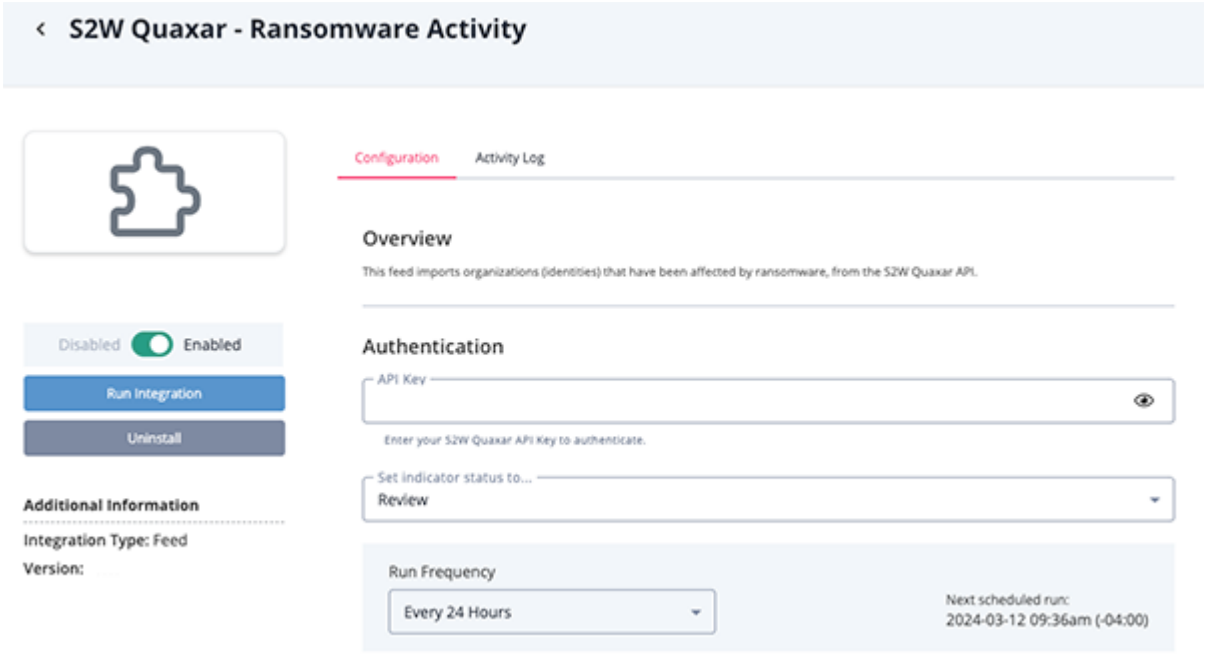
PARAMETER	DESCRIPTION
API Key	Enter your S2W Quaxar API Key.
Threat Actor Type Filter	Select the threat actor types to bring into ThreatQ. This allows you to filter out threat actor types that your organization may not utilize. Options include: ◦ APT (default) ◦ Ransomware (default) ◦ Criminal (default)
Context Filter	Select the pieces of context to bring into ThreatQ. This allows you to filter out context that your organization may not utilize. Options include: ◦ Threat Actor Types (default) ◦ Aliases (default) ◦ Target Countries (default) ◦ Target Sectors (default) ◦ Origins (default)

PARAMETER	DESCRIPTION
Relationship Context Filter	Select the relationships to bring into ThreatQ. This allows you to filter out context that your organization may not utilize. Options include: ◦ Indicators (default) ◦ Attack Patterns (default) ◦ Malware (default) ◦ Tools (default) ◦ Vulnerabilities (default)



S2W Quaxar - Ransomware Activity

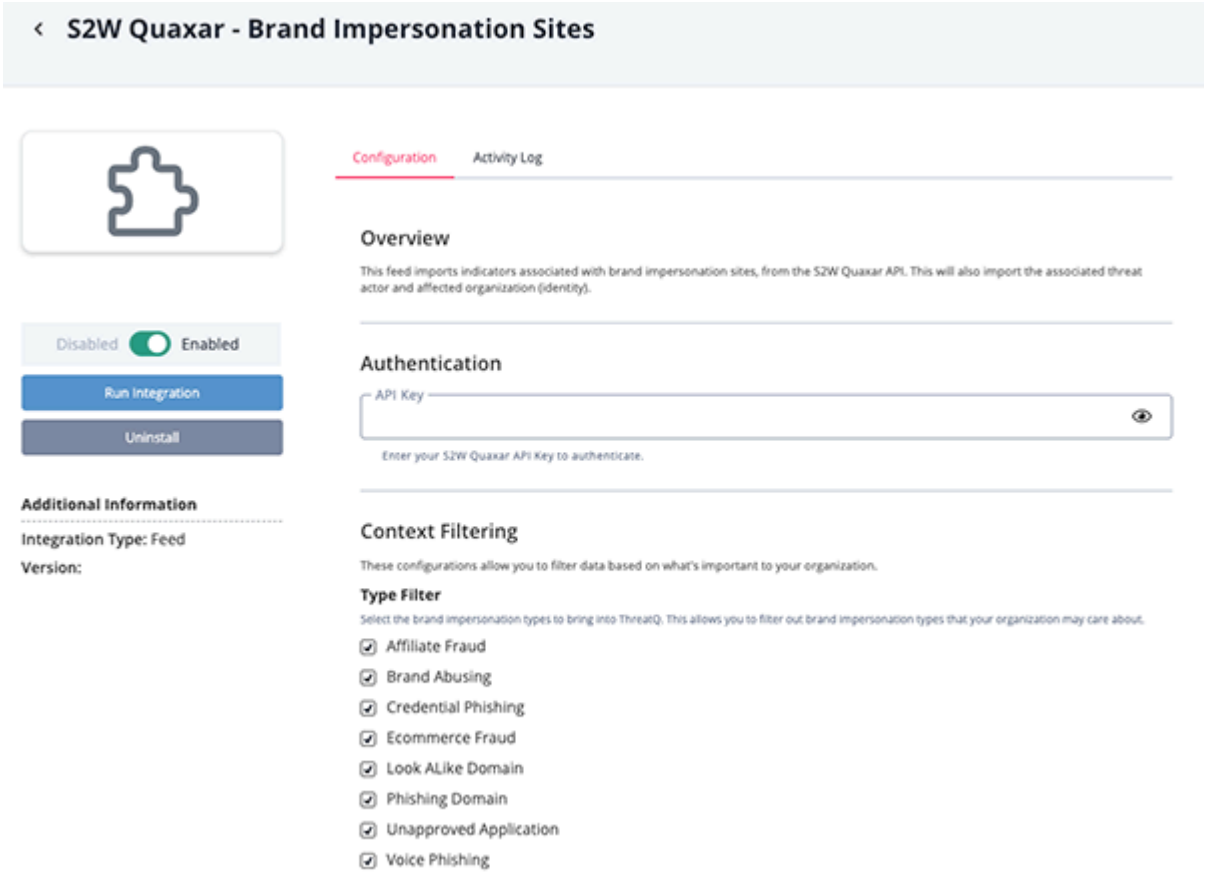
PARAMETER	DESCRIPTION
API Key	Enter your S2W Quaxar API Key.



S2W Quaxar - Brand Impersonation Sites

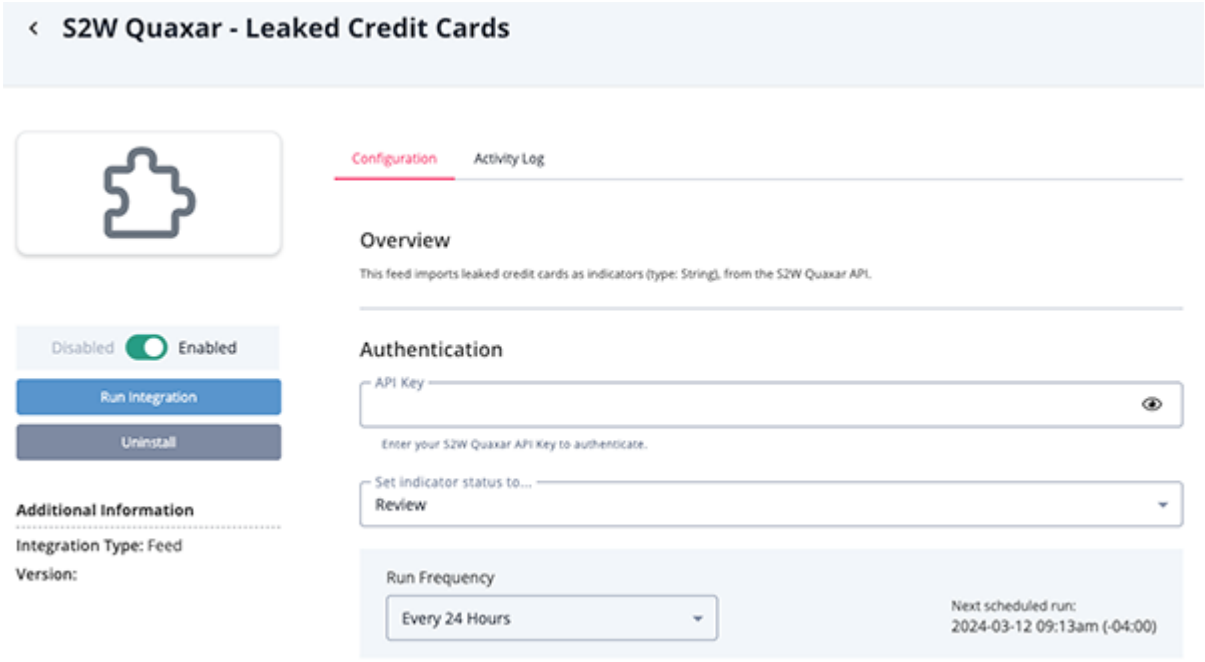
PARAMETER	DESCRIPTION
API Key	Enter your S2W Quaxar API Key.
Type Filter	Select the brand impersonation types to bring into ThreatQ. This allows you to filter out brand impersonation types that your organization is concerned about. Options include: ◦ Affiliate Fraud (default) ◦ Brand Abusing (default) ◦ Credential Phishing (default) Ecommerce ◦ Fraud (default) ◦ Look ALike Domain (default) ◦ Phishing Domain (default) ◦ Unapproved Application (default) ◦ Voice Phishing (default)
Risk Filter	Select the risk levels for the alerts to bring into ThreatQ. Options include: ◦ Unknown

PARAMETER	DESCRIPTION
	◦ Parking ◦ Suspicious ◦ Low ◦ Medium (default) ◦ High (default)
Executable Hash Types	Select the hash types to ingest for the related executables. Selecting none will not ingest any hashes for the executables. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256
Ingest Domain of Brand Impersonation URLs	Select whether or not to ingest the domains associated with the brand impersonation URLs. This parameter is enabled by default.
Default Domain Status	Select the default status for the domain. This defaults to Review because the domain may be legitimate.  This option only displays if the `Ingest Domain of Brand Impersonation URLs` option is enabled. Option include: ◦ Review (default) ◦ Active ◦ Indirect



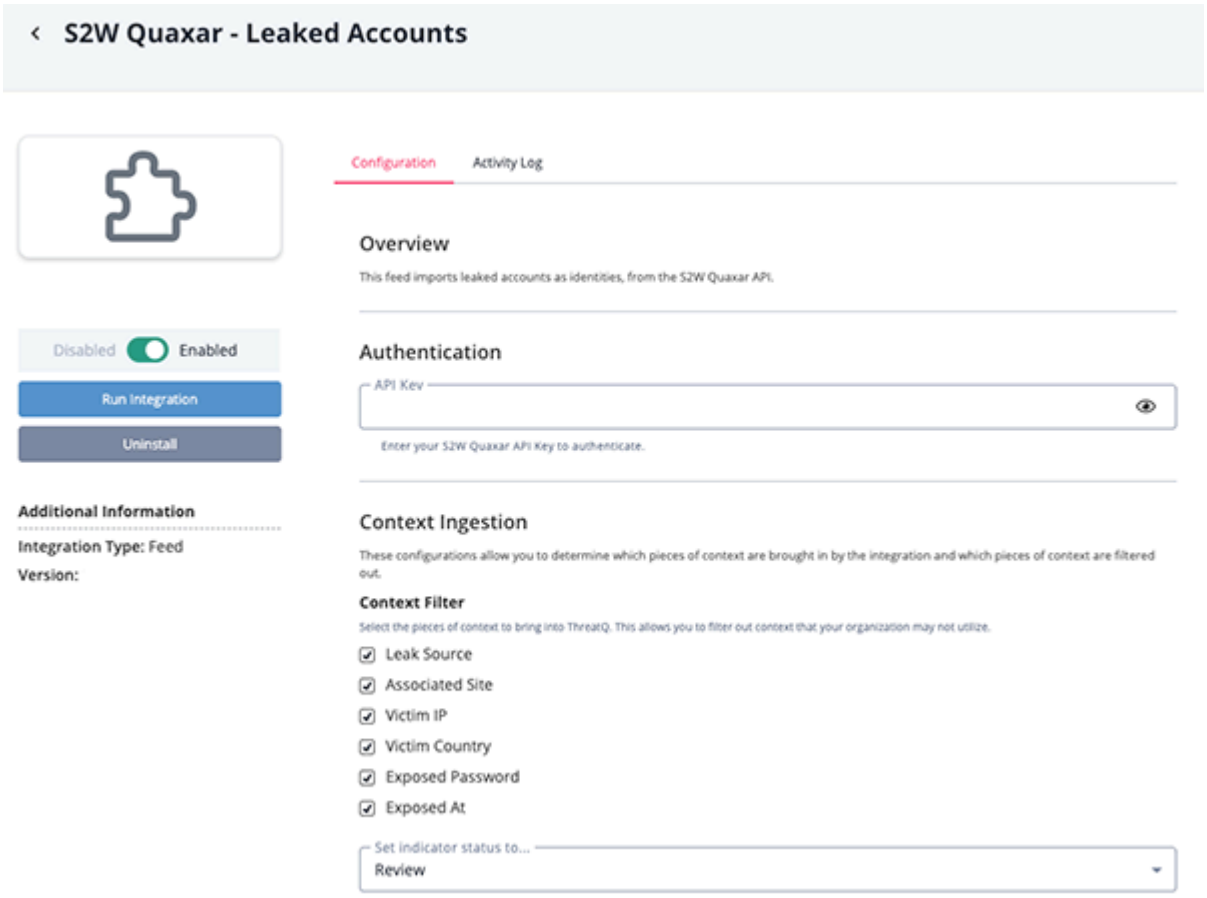
S2W Quaxar - Leaked Credit Cards

PARAMETER	DESCRIPTION
API Key	Enter your S2W Quaxar API Key.



S2W Quaxar - Leaked Accounts

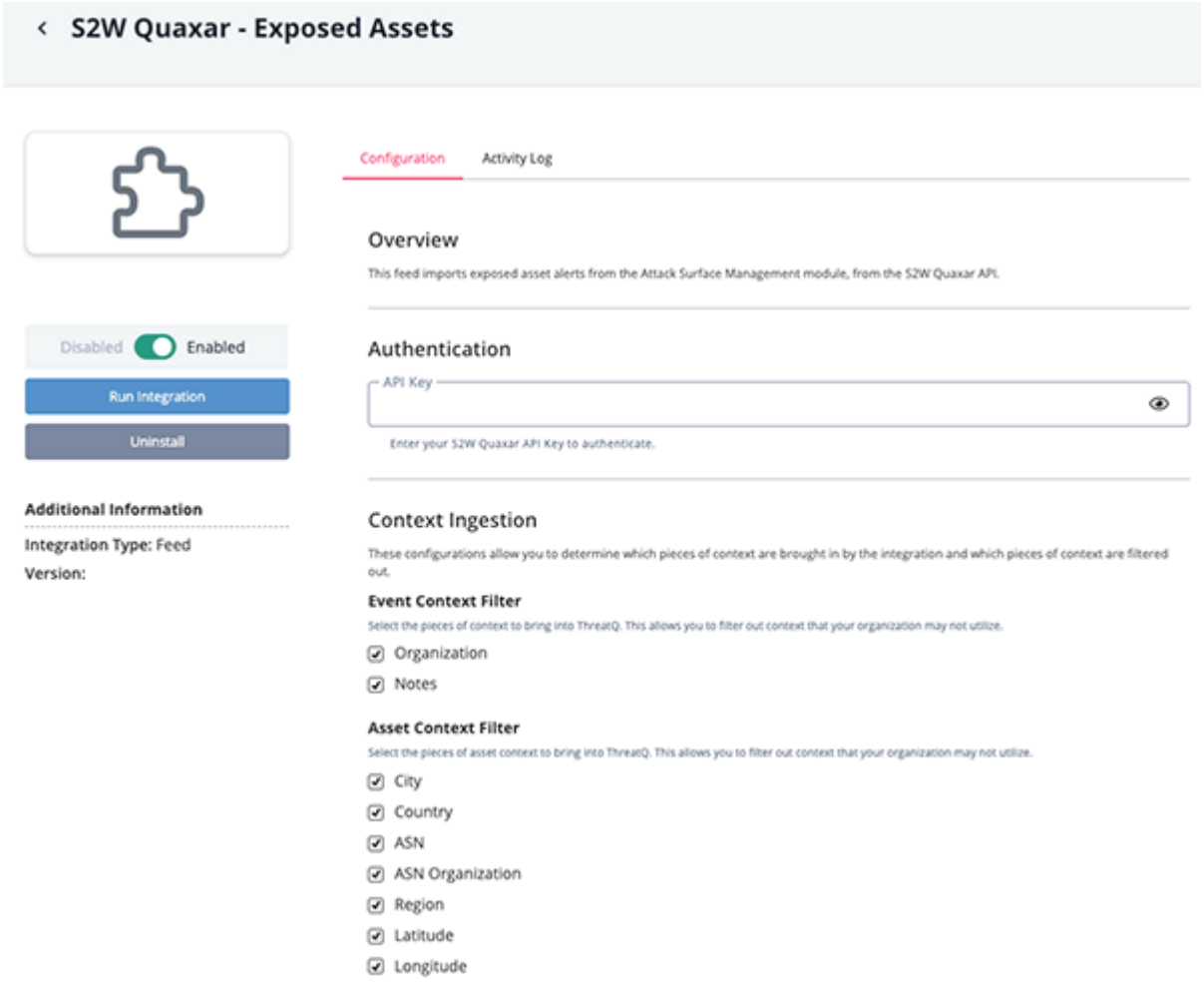
PARAMETER	DESCRIPTION
API Key	Enter your S2W Quaxar API Key.
Context Filter	Select the pieces of context to bring into ThreatQ. This allows you to filter out context that your organization may not utilize. Options include: ◦ Leak Source (default) ◦ Associated Site (default) ◦ Victim IP ◦ Victim Country (default) ◦ Exposed Password ◦ Exposed At (default)



S2W Quaxar - Exposed Assets

PARAMETER	DESCRIPTION
API Key	Enter your S2W Quaxar API Key.
Event Context Filter	Select the pieces of context to bring into ThreatQ. This allows you to filter out context that your organization may not utilize. Options include: ◦ Organization (default) ◦ Notes (default)
Asset Context Filter	Select the pieces of asset context to bring into ThreatQ. This allows you to filter out context that your organization may not utilize. Options include:

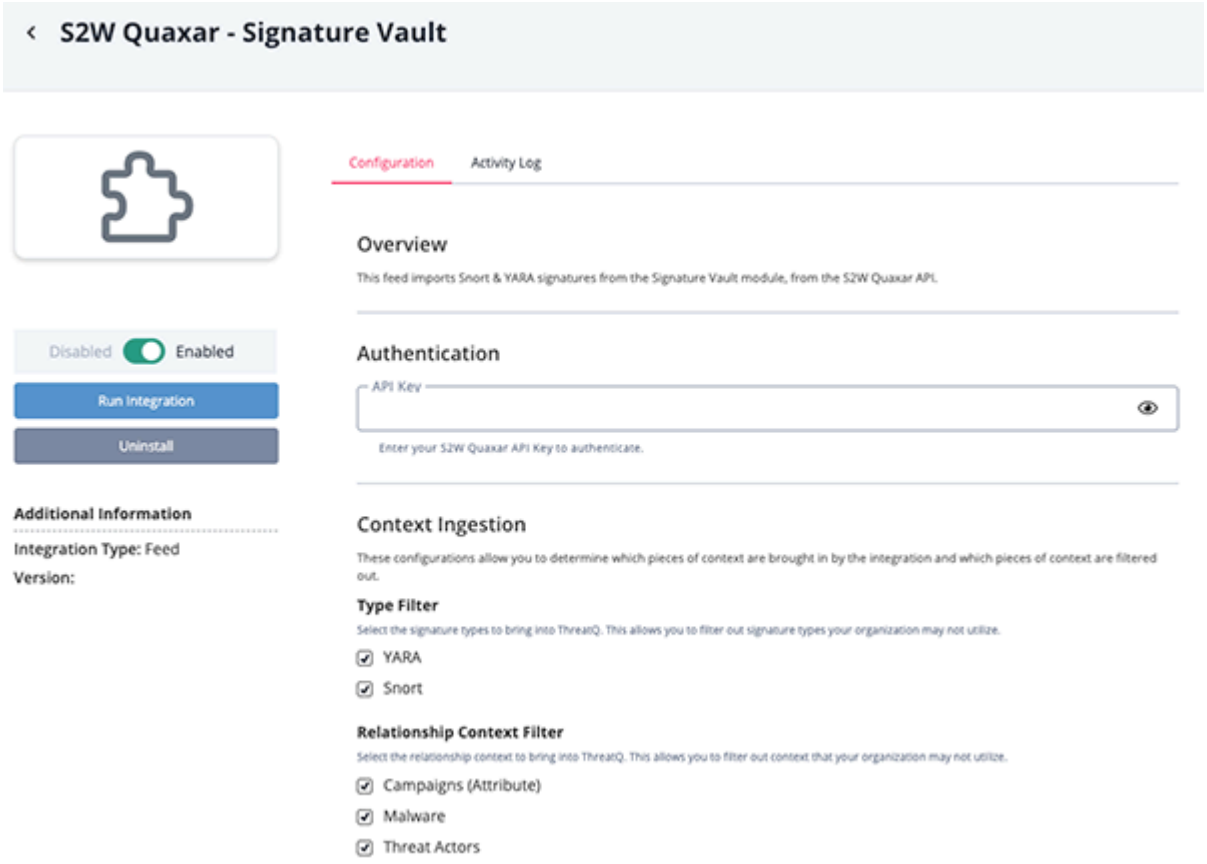
PARAMETER	DESCRIPTION
	◦ City (default) ◦ Country (default) ◦ ASN ◦ ASN Organization ◦ Region ◦ Latitude ◦ Longitude



S2W Quaxar - Signature Vault

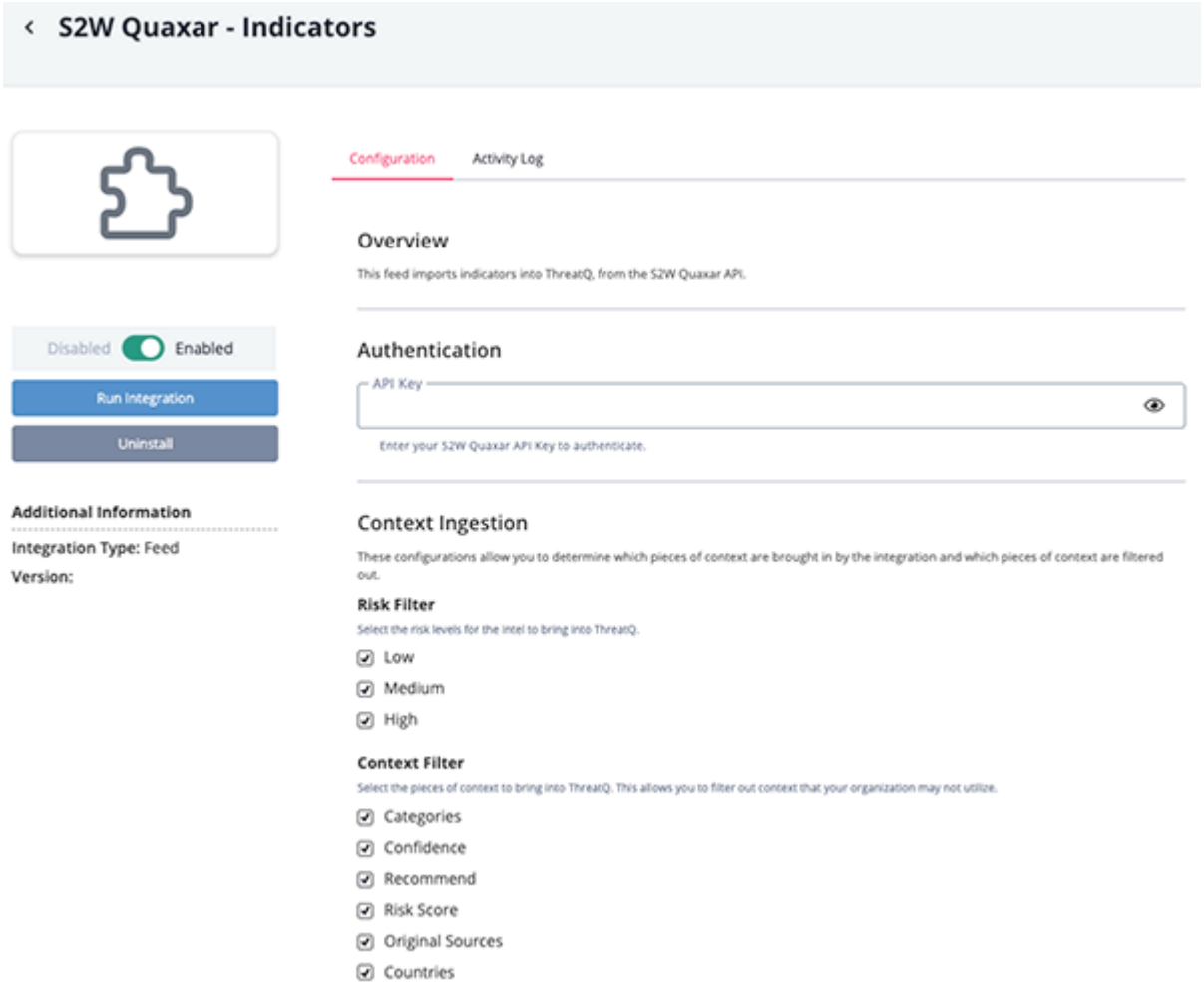
PARAMETER	DESCRIPTION
API Key	Enter your S2W Quaxar API Key.

PARAMETER	DESCRIPTION
Type Filter	Select the signature types to bring into ThreatQ. This allows you to filter out signature types your organization may not utilize. Options include: ◦ YARA (default) ◦ Snort (default)
Relationship Context Filter	Select the relationship context to bring into ThreatQ. This allows you to filter out context that your organization may not utilize. Options include: ◦ Campaigns (Attribute) (default) ◦ Malware (default) T ◦ hreat Actors (default)



S2W Quaxar - Indicators

PARAMETER	DESCRIPTION
API Key	Enter your S2W Quaxar API Key.
Risk Filter	Select the risk levels for the intel to bring into ThreatQ. Options include: ◦ Low ◦ Medium (default) ◦ High (default)
Context Filter	Select the pieces of context to bring into ThreatQ. This allows you to filter out context that your organization may not utilize. Options include: ◦ Categories (default) ◦ Confidence (default) ◦ Recommend ◦ Risk Score (default) ◦ Original Sources ◦ Countries (default)
Relationship Context Filter	Select the relationship context to bring into ThreatQ. This allows you to filter out context that your organization may not utilize. Options include: ◦ Campaigns (Attribute) ◦ Malware (default) ◦ Threat Actors (default) ◦ Tools (default) ◦ Attack Patterns (default) ◦ Vulnerabilities (default)
Indicator Type Filter	Select the indicator types to bring into ThreatQ. This allows you to filter out indicator types that your organization may not utilize. Options include: ◦ IPv4 Address (default) ◦ IPv6 Address (default) ◦ FQDN (default) ◦ URL (default) ◦ Email Address (default) ◦ MD5 (default) ◦ SHA-1 (default) ◦ SHA-256 (default) ◦ SHA-512 (default)



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

S2W Quaxar Report Feeds

The following feeds are included in the Reports feeds:

- S2W Quaxar - Threat Reports
- S2W Quaxar - Vulnerability Reports
- S2W Quaxar - Indicator Reports
- S2W Quaxar - Talon Reports

The Report feed periodically pulls reports from S2W Quaxar, into ThreatQ. The intelligence is ingested as Report objects, along with all of the related contextual data such as Indicators, Adversaries, Malware, as well as other objects within the STIX 2 data model.

`GET https://api.quaxar.io/report/list`

Sample Response:


```
{
  "total": 86,
  "data": [
    {
      "doclink": "https://portal.quaxar.io/knowledgebase/document/
report--155435f8-f4e3-43ae-bea5-1c787f81400b",
      "id": "report--155435f8-f4e3-43ae-bea5-1c787f81400b",
      "type": "vulnerability",
      "published": 1700499284000,
      "title": "Kinsing malware exploits Apache ActiveMQ RCE to plant
rootkits",
      "body": "The Kinsing malware operator is actively exploiting the
CVE-2023-46604 critical vulnerability in the Apache ActiveMQ open-source
message broker to compromise Linux systems.\nThe flaw allowsremote code
execution and was fixed in late October. Apacheâ€™s disclosure explains that
the issue allows running arbitrary shell commands leveraging serialized
cla...",
      "riskscore": 1,
      "tags": [
        {
          "id": "malware--85ee128f-6bb5-11eb-b195-b02628e2a7a1",
          "type": "malware",
          "name": "HELLOKITTY",
          "description": "[HELLOKITTY](https://attack.mitre.org/software/S0617)
is a ransomware written in C++  that shares similar code structure and
functionality with [DEATHRANSOM](https://attack.mitre.org/software/S0616) and
[FIVEHANDS](https://attack.mitre.org/software/S0618). [HELLOKITTY](https://
attack.mitre.org/software/S0617) has been used since at least 2020, targets
have included a Polish video game developer and a Brazilian electric power
company.(Citation: FireEye FiveHands April 2021)"
```

```
        },
        {
          "id": "vulnerability--163ed800-74f0-11ee-96a4-b02628e2a7a1",
          "type": "vulnerability",
          "name": "CVE-2023-46604",
          "description": "The Java OpenWire protocol marshaller is vulnerable
to Remote Code \nExecution. This vulnerability may allow a remote attacker with
network \naccess to either a Java-based OpenWire broker or client to run
arbitrary\n shell commands by manipulating serialized class types in the
OpenWire \nprotocol to cause either the client or the broker (respectively) to
\ninstantiate any class on the classpath.\n\nUsers are recommended to upgrade\n
both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 \nwhich
fixes this issue.\n\n"
        }
      ],
      "reference": "https://www.bleepingcomputer.com/news/security/kinsing-
malware-exploits-apache-activemq-rce-to-plant-rootkits/",
      "indicators": []
    },
    {
      "doclink": "https://portal.quaxar.io/knowledgebase/document/
report--659162d4-8794-11ee-96a4-b02628e2a7a1",
      "id": "report--659162d4-8794-11ee-96a4-b02628e2a7a1",
      "type": "indicator",
      "published": 1700477782467,
      "title": "Suspected Rattlesnake organization uses Nim backdoor to spy on
intelligence from many countries in South Asia",
      "body": "Sidewinder, also known as Sidewinder, QiAnXin internal tracking
number APT-Q-39. This organization is generally believed to have a background
in South Asia and was disclosed by domestic and foreign security vendors in
2018. Its earliest attack activities can be traced back to 2012. The
organization's attack targets are generally government and mili...",
      "riskscore": 1,
      "tags": [
        {
          "id": "attack-pattern--65fbff07-5f97-11eb-b195-b02628e2a7a1",
          "type": "attack-pattern",
          "name": "Mshta",
          "label": "T1170"
        }
      ],
      "reference": "https://mp.weixin.qq.com/s?
__biz=MzI2MDc2MDA4OA==&mid=2247508655&idx=1&sn=b808c9a435b473e5dc957d1b34a79432
&chksm=ea6655d8dd11dcce5db489b200b67463f251c5900402b9a1cb18c9e1d9d1c56adee066eb
165e&scene=178&cur_album_id=1539799351089283075#rd",
      "indicators": [
        {
          "id": "file--6757dfb6-2049-582e-a75c-0432ae34ec67",
          "type": "SHA-256",
          "name":
```

```
"1409f9d855c06f66fb7d7c7bf9f821b5d1631da926b07dcdb260606e09763ad3"
        },
        {
          "id": "file--06a9ffbb-3fb7-556d-b648-73defd4f50f5",
          "type": "MD5",
          "name": "92612dc223e8f0656512cd882d66f78b"
        }
      ]
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

> Mapping is based on each item within the `.data[]` list in the JSON response.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Report Value	N/A	`.published`	N/A	N/A
`.body`	Report Description	N/A	N/A	N/A	Description includes some report metadata as well; HTML formatted
`.indicators[].name`	Related Indicator Value	`.indicators[].type`	`.published`	`142.50.15.123`	Indicator type mapped to ThreatQ types
`.tags[].name`	Related Adversary Name	N/A	`.published`	`WIZARD SPIDER`	Where `.type` == `threat-actor`
`.tags[].label`, `.tags[].name`	Related Attack Pattern Value	N/A	`.published`	`T1001 - Some technique`	Where `.type` == `attack-pattern`
`.tags[].name`	Attribute	Campaign	`.published`	`OpIsrael`	Where `.type` == `campaign`
`.tags[].name`	Related Identity Value	N/A	`.published`	`Tim Cook`	Where `.type` == `identity`
`.tags[].name`	Related Tool Value	N/A	`.published`	`psexec`	Where `.type` == `tool`
`.tags[].name`	Related Intrusion Set Value	N/A	`.published`	`APT1`	Where `.type` == `intrusion-set`
`.tags[].name`	Related Malware Value	N/A	`.published`	`Lockbit 2.0`	Where `.type` == `malware`
`.tags[].name`	Related TTP Value	N/A	`.published`	N/A	Where `.type` == `ttp`
`.tags[].name`	Related Vulnerability Value	N/A	`.published`	`CVE-2024-12345`	Where `.type` == `vulnerability`; May be a CVE or other Vulnerability description
`.tags[].name`	Attribute	Target Country	`.published`	`USA`	Where `.type` == `country`
`.tags[].name`	Attribute	Target Sector	`.published`	`Energy`	Where `.type` == `sector`
`.tags[].name`	Attribute	Target Region	`.published`	`Middle East`	Where `.type` == `region`
`.tags[].name`	Attribute	Affected Product	`.published`	`Apache`	Where `.type` == `software`
`.tags[].name`	Related Identity Value	N/A	`.published`	`Acme Corp`	Where `.type` == `organization`
N/A	Attribute	Report Type	`.published`	`threat-report`	Static based on feed

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.riskscore`	Attribute	Risk Score	`.published`	`1`	N/A

S2W Quaxar - Threat Actors

The Threat Actors feed periodically pulls Threat Actor profiles from S2W Quaxar. Using this feed, you can stay up-to-date with APTs, Ransomware Groups, and other Criminal Actors. You'll be able to identify their aliases, target countries/sectors, and other relevant information such as relationships to Indicators, Tools, and more.

`GET https://api.quaxar.io/tap/list`

Sample Response:


```
{
  "total": 84,
  "data": [
    {
      "id": "group-threat-actor--f9a8d088-b8fb-410a-b7ae-39ca04479e42",
      "name": "SecretCrow",
      "types": [],
      "origins": [],
      "countries": ["South Korea"],
      "sectors": [],
      "aliases": [],
      "last_updated": 1700457942000
    },
    {
      "id": "group-threat-actor--7bc634a9-852b-11ee-96a4-b02628e2a7a1",
      "name": "spider",
      "types": [],
      "origins": [],
      "countries": [],
      "sectors": [],
      "aliases": [],
      "last_updated": 1700409277641
    }
  ]
}
```


See the Get Actor by ID supplemental feed for mapping information.

S2W Quaxar - Get Actor by ID (Supplemental)

This supplemental feed will pull an individual actor's full details from the Quaxar API by ID.

`GET https://api.quaxar.io/tap/{{ id }}`

Sample Response:


```
{
  "id": "group-threat-actor--a1f64882-7dd3-423c-b191-f44a5ee6eddf",
  "name": "LockBit",
  "types": ["ransomware"],
  "origins": [],
  "countries": [
    "Brazil",
    "Venezuela",
    "Canada",
    "Japan",
    "Poland",
    "Taiwan",
    "Thailand"
  ],
  "sectors": [
    "Defense",
    "BFSI",
    "software",
    "Government",
    "Research",
    "Healthcare",
    "Automotive"
  ],
  "aliases": [
    {
      "name": "LockbitSupp",
      "id": "threat-actor--8e549f69-3700-458c-934c-20c791a574a6"
    }
  ],
  "malwares": [
    {
      "name": "aukill",
      "id": "malware--f751f1cf-dea6-11ed-96a4-b02628e2a7a1"
    },
    {
      "name": "LockBit",
      "id": "malware--43d726db-0f53-44a2-a170-a696d9cbe359"
    }
  ],
  "tools": [
    {
      "name": "AdFind",
      "id": "tool--f59508a6-3615-47c3-b493-6676e1a39a87"
```

```
    },
    {
      "name": "PCHunter",
      "id": "tool--f7e5be1e-d4ea-495b-81b7-87dcc9c3b38e"
    },
    {
      "name": "Mimikatz",
      "id": "tool--afc079f3-c0ea-4096-b75d-3f05338b7f60"
    }
  ],
  "vulnerabilities": [
    {
      "name": "CVE-2023-20269",
      "id": "vulnerability--a4763cd1-4cf2-11ee-96a4-b02628e2a7a1"
    },
    {
      "name": "CVE-2018-13379",
      "id": "vulnerability--57019d58-9ca8-46ba-b261-ef85cdeee215"
    }
  ],
  "attackpatterns": [
    {
      "name": "PowerShell",
      "mitre_id": "T1059.001",
      "id": "attack-pattern--970a3432-3237-47ad-bcca-7d8cbb217736"
    },
    {
      "name": "Windows Command Shell",
      "mitre_id": "T1059.003",
      "id": "attack-pattern--d1fcf083-a721-4223-aedf-bf8960798d62"
    }
  ],
  "indicators": [
    {
      "id": "url--32c3b723-3469-58c2-91ae-c1d70b3062db",
      "type": "url",
      "value": "http://
lockbit7z55tuwaflw2c7torcryobdvhkcgvivhflyndyvcrexafssad.onion"
    },
    {
      "id": "file--eadd8705-0548-5f22-a308-fc62ce13ceb8",
      "type": "SHA-256",
      "value":
"0f9677642599cf23aafe225ee2dbe403f305dc5801298b83ba19f6b939a8f914"
    }
  ],
  "reports": [
    {
      "name": "Canadian government discloses data breach after contractor
hacks",
```

```
      "published": 1700500988000,
      "qxrlink": "https://portal.quaxar.io/knowledgebase/document/
report--7b68c65a-3ae9-4dd3-85a1-746e7d559d06"
    },
    {
      "name": "20th November â€“ Threat Intelligence Report",
      "published": 1700438400000,
      "qxrlink": "https://portal.quaxar.io/knowledgebase/document/
report--7290e021-b4e7-41ea-9d91-70704405cd92"
    }
  ],
  "last_updated": 1700500988000
}
```


ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
`.name`	Adversary Name	N/A	`.last_updated`	`CommentCrew`	N/A
`.attackpatterns[].mitre_id`, `.attackpatterns[].name`	Related Attack Pattern Value	N/A	`.last_updated`	`T1001 - Some technique`	N/A
`.vulnerabilities[].name`	Related Vulnerability Value	N/A	`.last_updated`	`CVE-2024-12345`	N/A
`.tools[].name`	Related Tool Value	N/A	`.last_updated`	`psexec`	N/A
`.malwares[].name`	Related Malware Value	N/A	`.last_updated`	`WannaCry`	N/A
`.aliases[].name`	Attribute	Alias	`.last_updated`	`WIZARD SPIDER`	N/A
`.aliases[].types`	Attribute	Threat Actor Type	`.last_updated`	`ransomware`	N/A
`.indicators[].value`	Related Indicator Value	`.indicators[].type`	`.last_updated`	`54.123.76.90`	N/A
`.countries[]`	Attribute	Target Country	`.last_updated`	`USA`	N/A
`.origins[]`	Attribute	Origin	`.last_updated`	`North Korea`	N/A
`.sectors[]`	Attribute	Target Sector	`.last_updated`	`Government`	N/A

S2W Quaxar - Ransomware Activity

The Ransomware Actitivty feed periodically pulls a list of Organizations that have been impacted by Ransomware, from S2W Quaxar. Using this feed, you can stay up-to-date with the latest Ransomware activity to better understand your organization's attack surface. Affected organizations will be ingested as Identity objects, with an attribute of `Detection: Ransomware Activity`

`GET https://api.quaxar.io/ram/list`

Sample Response:


```
{
  "total": 230,
  "data": [
    {
      "id": "73c82e70635c21ebdadfb8c60c0c1ed02fd8c47c3e7ad25788c3176be5a398e1",
      "organization": {
        "type": "organization",
        "name": "British Library"
      },
      "threatactor": {
        "type": "threat-actor",
        "name": "Rhysida"
      },
      "timestamp": 1700492437494
    },
    {
      "id": "40efb4c7bab7a466d448c888020abbcfdb44a67febe0f32717b7e20be0245592",
      "organization": {
        "type": "organization",
        "name": "Brown Integrated Logistics"
      },
      "threatactor": {
        "type": "threat-actor",
        "name": "LockBit"
      },
      "country": "USA",
      "sector": "Transportation",
      "timestamp": 1700479980000
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.organization.name`	Identity	N/A	`.timestamp`	`Acme Corp`	N/A
`.country`	Attribute	Country	`.timestamp`	USA	N/A
`.sector`	Attribute	Sector	`.timestamp`	`Energy`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
N/A	Attribute	Detection	`.timestamp`	`Ransomware Activity`	Added to all ingested Identities
`.threatactor.name`	Related Adversary Name	N/A	`.timestamp`	`CommentCrew`	N/A

S2W Quaxar - Brand Impersonation Sites

The Brand Impersonation Sites feed periodically pulls a list of Brand Impersonation indicators as well as the affected organizations from S2W Quaxar. Using this feed, you can stay up-to-date with the latest Brand Impersonation activity to better understand your organization's attack surface. S2W Quaxar also provides a risk level with each impersonation URL to provide analysts with the information they need to make quick information decisions. Affected organizations will be ingested as Identity objects, with an attribute of `Detection: Brand Impersonation`

`GET https://api.quaxar.io/basm/list`

Sample Response:


```
{
  "total": 21,
  "data": [
    {
      "id": "21b378375c0e759627059c65cad485573241a49ae026a9013d568338a2929c8b",
      "type": "Voice Phishing",
      "url": "http://111.246.140.167:80",
      "domain": "111.246.140.167:80",
      "detected": 1668075843000,
      "risklevel": "HIGH",
      "organization": {
        "type": "organization",
        "name": "Shinhanbank"
      },
      "ipinfos": [
        {
          "ip": "111.246.140.167",
          "country": "Taiwan",
          "coordinate": {
            "latitudes": 24.1469,
            "longitudes": 120.6839
          },
          "asn": 3462,
          "organization": "Data Communication Business Group"
        }
      ],
      "domaininfos": [{}],
      "executables": [
        {
          "name": "shinhan.apk",
          "sha256":
"ef9f4ba0e6c97c526ebc88d1e00817186394d441abf29ad2abaaf70426294ff9",
          "sha1": "1f59532d4b38acebd10124cef78a6b3d18cae422",
          "md5": "38c4a8a4559927e3277e7e254ca5b4f7"
        }
      ]
    }
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.domain`	Indicator Value	FQDN	`.detected`	N/A	URL paths are removed from this value; Optional
`.url`	Indicator Value	URL	`.detected`	N/A	N/A
`.executables[].md5`	Indicator Value	MD5	`.detected`	N/A	N/A
`.executables[].sha1`	Indicator Value	SHA-1	`.detected`	N/A	N/A
`.executables[].sha256`	Indicator Value	SHA-256	`.detected`	N/A	N/A
`.executables[].name`	Attribute	Filename	`.detected`	N/A	Applied to hash indicators (if available)
`.ipinfos[].ip`	Indicator Value	IP Address	`.detected`	N/A	N/A
`.ipinfos[].asn`	Attribute	ASN	`.detected`	N/A	Applied to IP indicators (if available)
`.ipinfos[].country`	Attribute	Country	`.detected`	`France`	Applied to IP indicators (if available)
`.ipinfos[].organization`	Attribute	ASN Organization	`.detected`	N/A	Applied to IP indicators (if available)
`.type`	Attribute	Impersonation Type	`.detected`	N/A	N/A
`.risklevel`	Attribute	Risk Level	`.detected`	`1`	N/A
N/A	Attribute	Detection	`.detected`	`Brand Impersonation`	Applied to the Related Identity (Organization)
`.organization.name`	Identity Value	N/A	`.detected`	`Acme Corp`	N/A
`.threatactor`	Adversary Value	N/A	`.detected`	`Kimsuky`	N/A

S2W Quaxar - Leaked Credit Cards

The Leaked Credit Cards feed periodically pulls leaked credit card numbers discovered on the dark web. Included with each credit card number is the country of origin, issuer, expiration, and where it was leaked. Credit Card numbers will be ingested as Compromised Card objects.

`GET https://api.quaxar.io/clm/list`

Sample Response:


```
{
  "total": 226,
  "data": [
    {
      "id": "3ffdf35cb6e735c83a2b7e661e3128da21c419b9",
      "number": "4355460164424370",
      "issuer": "visa",
      "expiry": 1846022400000,
      "country": "USA",
      "sitename": "livecc|livecreditcard",
      "timestamp": 1700475281000
    },
    {
      "id": "cdce1e3c924b49eed2f72cd8231c32eb947732c3",
      "number": "4355460288424310",
      "issuer": "visa",
      "expiry": 1846022400000,
      "country": "USA",
      "sitename": "ð–Ÿð–œð–©ð–˜ð–•ð–œð–¡ð–¦ð––ðŸ˜Ž",
      "timestamp": 1700450224000
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.number`	Compromised Card Value	N/A	`.timestamp`	N/A	N/A
`.issuer`	Attribute	Issuer	`.timestamp`	`Visa`	N/A
`.expiry`	Attribute	Expiration	`.timestamp`	N/A	Converted to ISO format
`.country`	Attribute	Country	`.timestamp`	`USA`	N/A
`.sitename`	Attribute	Leak Site	`.timestamp`	`livecc|livecreditcard`	Unicode characters are removed

S2W Quaxar - Leaked Accounts

The Leaked Accounts feed periodically pulls leaked account credentials obtained via Malware, Phishing, and other methods. These credentials will be ingested using the Compromised Account custom object. Included with each compromised account is the username, password, and the source of the leak.

```
GET https://api.quaxar.io/atom/list
```

Sample Response:


```
{
  "total": 11261,
  "data": [
    {
      "id": "ac33cf59f41774eb92ae5edd592a68dc289c9e22",
      "source": "Vidar",
      "site": "acme.com",
      "ip": "124.50.152.124",
      "country": "Japan",
      "exposedAt": 1671684162363,
      "username": "deathju",
      "password": "hunter2"
    },
    {
      "id": "977b629705426c85bd14c641a554b926b5bef03d",
      "source": "Redline",
      "site": "acme.org",
      "ip": "125.185.210.11",
      "country": "Korea",
      "exposedAt": 1658379726454,
      "loggedAt": 1654844643000,
      "username": "jangyee",
      "password": "example-password$$$"
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.username`	Compromised Account Value	N/A	`.exposedAt` or `.loggedAt`	N/A	N/A
`.source`	Attribute	Leak Source	`.exposedAt` or `.loggedAt`	`Vidar`	N/A
`.site`	Attribute	Associated Site	`.exposedAt` or `.loggedAt`	`acme.com`	N/A
`.ip`	Attribute	Victim IP	`.exposedAt` or `.loggedAt`	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.country`	Attribute	Victim Country	`.exposedAt` or `.loggedAt`	`Japan`	N/A
`.password`	Attribute	Exposed Password	`.exposedAt` or `.loggedAt`	N/A	N/A
`.exposedAt`	Attribute	Exposed At	`.exposedAt` or `.loggedAt`	N/A	Converted to ISO format

S2W Quaxar - Exposed Assets

The Exposed Assets feed periodically pulls private assets that have been exposed to the public internet. This can help organizations find and detect servers and services that may have accidentally been exposed to the internet. Discovering exposed assets can help organizations reduce their attack surface and prevent future breaches.

```
GET https://api.quaxar.io/asm/list
```

Sample Response:


```
{
  "total": 81,
  "data": [
    {
      "id": "e244bfbf-d32a-5fa6-a280-feaf234b8389",
      "asmId": "ASM-3009",
      "organization": "Acme",
      "ip": "41.230.110.115",
      "detected": 1667799832676,
      "ipinfo": {
        "ip": "41.230.110.115",
        "city": "Ulan Bator",
        "country": "Mongolia",
        "region": "Ulaanbaatar",
        "timezone": "Asia/Ulaanbaatar",
        "coordinate": {
          "latitudes": 47.9077,
          "longitudes": 106.8832
        },
        "asn": 63962,
        "organization": "iTools JSC"
      },
      "labels": [],
      "notes": [],
      "updated": 1668220610647,
      "details": [
        {
          "id":
"19f80e1afc5cd78a310080dd7550fbf167b349520e4408a648d505618962e84c",
          "ip": "41.230.110.115",
          "detected": 1668220610647,
          "port": 33060,
          "service": "unknown"
        },
        {
          "id":
"19fea3c439b9b04186c141c9496eb714eaeb9a153e47e3340734477b995ac48e",
          "ip": "41.230.110.115",
          "detected": 1668220610647,
```

```
          "port": 3306,
          "service": "mysql"
        }
      ],
      "title": "Private services at 41.230.110.115 have been exposed in public"
    },
    {
      "id": "7d7eb11e-45d5-55c1-8845-4e19ccc8f700",
      "asmId": "ASM-17237",
      "organization": "Acme Corp",
      "ip": "212.45.24.98",
      "detected": 1667268740399,
      "ipinfo": {
        "ip": "212.45.24.98",
        "city": "Moscow",
        "country": "Russian Federation",
        "region": "Moscow",
        "timezone": "Europe/Moscow",
        "coordinate": {
          "latitudes": 55.7522,
          "longitudes": 37.6156
        },
        "asn": 8732,
        "organization": "JSC Comcor"
      },
      "labels": [],
      "notes": [],
      "updated": 1674490154149,
      "details": [
        {
          "id":
"592044fa17028d26fc0777744aa3c25ecf1d2d34c14e4a65a1644d72371104fa",
          "ip": "211.45.24.98",
          "detected": 1675440733239,
          "port": 33894,
          "service": "rdp"
        }
      ],
      "title": "Private services at 211.45.24.98 have been exposed in public"
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title`	Event Title	Alert	`.detected` or `.updated`	`Private services at 41.230.110.115 have been exposed in public`	N/A
`.ip`	Asset Value	IP Address	`.detected` or `.updated`	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.ip`	Attribute	IP Address	`.detected` or `.updated`	N/A	Applied to Asset
`.ipinfo.city`	Attribute	City	`.detected` or `.updated`	N/A	Applied to Asset
`.ipinfo.country`	Attribute	Country	`.detected` or `.updated`	`China`	Applied to Asset
`.ipinfo.asn`	Attribute	ASN	`.detected` or `.updated`	N/A	Applied to Asset
`.ipinfo.organization`	Attribute	ASN Organization	`.detected` or `.updated`	N/A	Applied to Asset
`.ipinfo.region`	Attribute	Region	`.detected` or `.updated`	`Tokyo`	Applied to Asset
`.ipinfo.latitudes`	Attribute	Latitude	`.detected` or `.updated`	N/A	Applied to Asset
`.ipinfo.longitudes`	Attribute	Longitude	`.detected` or `.updated`	N/A	Applied to Asset
`.organization`	Attribute	Organization	`.detected` or `.updated`	N/A	Applied to Event
`.notes`	Attribute	Note	`.detected` or `.updated`	N/A	Applied to Event
`.labels[]`	Tag	N/A	`.detected` or `.updated`	N/A	Applied to Event

S2W Quaxar - Signature Vault

The Signature Vault feed periodically pulls Snort & YARA signatures from S2W Quaxar. Signatures will be parsed and ingested, bringing in related hashes, threat actors, malware, etc.

```
GET https://api.quaxar.io/sigv/list
```

Sample Response:


```
{
  "total": 42,
  "data": [
    {
      "id": "indicator--32ad1cb8-8241-11ed-96a4-b02628e2a7a1--1",
      "type": "yara",
      "name": "MAL_Win_Ransomware_ViceSociety",
      "description": "Detect a custom branded version of Vice Society
ransomware",
      "created": 1669593600000,
      "modified": 1671745205355,
      "author": "Antonio Cocomazzi @ SentinelOne",
      "pattern": "rule MAL_Win_Ransomware_ViceSociety {\n\nmeta:   \n
author = \"Antonio Cocomazzi @ SentinelOne\"   \n       description = \"Detect
a custom branded version of Vice Society ransomware\"   \n       date =
\"2022-11-28\"   \n       reference = \"https://www.sentinelone.com/labs/
custom-branded-ransomware-the-vice-society-group-and-the-threat-of-outsourced-
development\"   \n       hash = \"c8e7ecbbe78a26bea813eeed6801a0ac9d1eacac\"
\n      \n     \nstrings:   \n       $code1 = {4? 8B ?? 28 00 02 00 }   \n
$code2 = {4? C7 ?? 18 03 02 00 A3 00 00 00}   \n       $code3 = {(48|49) 8D 8?
58 00 02 00}   \n       $code4 = {(48|49) 8D 9? E8 02 02 00}   \n       $code5
= {(48|4C) 89 ?? 24 38}   \n       $code6 = {4? 8B ?? F8 02 02 00}   \n
$code7 = {C7 44 24 48 01 00 00 00}   \n       $string1 = \"vsociet\" nocase
wide ascii   \n      \n     \ncondition:   \n       uint16(0) == 0x5A4D and all
of them   \n   \n}",
      "references": [
        {
          "url": "https://www.sentinelone.com/labs/custom-branded-ransomware-
the-vice-society-group-and-the-threat-of-outsourced-development",
          "source": "www.sentinelone.com"
        }
      ],
      "campaigns": [
        {
          "id": "campaign--32ad1c92-8241-11ed-96a4-b02628e2a7a1",
          "type": "campaign",
          "name": "Custom-Branded Ransomware: The Vice Society Group and the
Threat of Outsourced Development"
        }
      ],
      "malwares": [
```

```
        {
          "id": "malware--90153a76-fcff-11ec-96a4-b02628e2a7a1",
          "type": "malware",
          "name": "redalert"
        }
      ],
      "threatactors": [
        {
          "id": "threat-actor--6fa8d901-a1e7-4681-9bbe-2152c0e69d45",
          "type": "threat-actor",
          "name": "Vice Society"
        }
      ],
      "qxrlinks": [
        "https://portal.quaxar.io/knowledgebase/document/
report--32ad1cba-8241-11ed-96a4-b02628e2a7a1"
      ]
    },
    {
      "id": "indicator--f3ae27cb-08b2-4fca-932c-f15b6efa9c16--1",
      "type": "snort",
      "name": "malware disguised as My PC Care in DNS Lookup (kisa-down.com)",
      "created": 1666342296940,
      "modified": 1666342296940,
      "author": "S2W Inc.",
      "pattern": "alert udp $HOME_NET any -> any 53 (msg:\"S2W malware
disguised as My PC Care in DNS Lookup (kisa-down.com)\"; content:\"|09|kisa-
down|03|com|00|\"; fast_pattern;
reference:md5,04007f9ec1b74dc0167b3d657d206e54; classtype:trojan-activity;
sid:22102101; rev:2; metadata:created_at 2022_10_21, threat_actor Kimsuky,
category malware, malware_name N/A, severity Mid, author sebin@s2w.inc;)",
      "references": [
        {
          "url": "https://portal.quaxar.io/dashboard",
          "source": "[MAL] Analysis of phishing emails disguised as contents of
the monthly national security strategy"
        }
      ],
      "threatactors": [
        {
          "id": "threat-actor--5c71ad21-84db-4c6b-8b8d-4d0e5010d226",
          "type": "threat-actor",
          "name": "Kimsuky"
        }
      ],
      "qxrlinks": [
        "https://portal.quaxar.io/knowledgebase/document/report--1d55f993-
b465-4173-9bef-e778bf5f071f"
      ]
    }
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.name`	Signature Name	`Snort` or `YARA`	`.created` or `.modified`	N/A	N/A
`.pattern`	Signature Value	`Snort` or `YARA`	`.created` or `.modified`	N/A	N/A
`.campaigns[].name`	Attribute	Campaign	`.created` or `.modified`	N/A	N/A
`.malwares[].name`	Malware	N/A	`.created` or `.modified`	N/A	Related to Signature; Optional
`.threatactors[].name`	Adversary	N/A	`.created` or `.modified`	N/A	Related to Signature; Optional
`.qxrlinks[]`	Attribute	Quaxar Link	`.created` or `.modified`	N/A	N/A
N/A	Tags	N/A	`.created` or `.modified`	N/A	Parsed from signature; Applied to signature
N/A	Indicator Value	Various Types (i.e. Hashes)	`.created` or `.modified`	N/A	Parsed from signature; Applied to signature

S2W Quaxar - Indicators

The Indicators feed periodically pulls indicators and their relationships from S2W Quaxar. This feed provides information on the categories, confidence, risk score, and more, for each indicator.

`GET https://api.quaxar.io/invi/list`

Sample Response:


```
{
  "total": 6730,
  "data": [
    {
      "id": "ipv4-addr--c6bdb358-2b08-5bc3-87c3-2b539d1d9600",
      "description": "",
      "value": "108.62.118.136",
      "type": "ipv4-addr",
      "confidence": 15,
      "recommend": 1,
      "riskscore": 1,
      "revoked": false,
      "categories": ["hosting-malware", "malware"],
      "references": [
        "https://portal.quaxar.io/knowledgebase/document/grouping--0a1aeea6-
e641-44f3-9dd1-eac298e7d033",
        "https://tip.kaspersky.com/",
        "https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a",
        "https://otx.alienvault.com/pulse/655537ff05840a2a8d7b3d3d"
      ],
      "sources": ["tip.kaspersky.com", "S2W Inc.", "www.cisa.gov"],
      "countries": ["North Korea"],
      "targets": [
        {
          "id": "threat-actor--46e6f7c5-cd32-49b1-a5d7-d42ccbf145e6",
          "type": "threat-actor",
          "name": "Lazarus"
        },
        {
          "id": "tool--a6346c09-4f18-4f5f-9c67-130a6d2dbf12",
          "type": "tool",
          "name": "Cobalt Strike"
        },
        {
          "id": "malware--248bb279-ff63-11ed-96a4-b02628e2a7a1",
          "type": "malware",
          "name": "rhysida"
        }
      ],
      "graph": {
        "nodes": [
```

```
          {
            "threat_actor_types": ["APT"],
            "name": "Lazarus",
            "id": "threat-actor--46e6f7c5-cd32-49b1-a5d7-d42ccbf145e6",
            "type": "threat-actor"
          },
          {
            "name": "Cobalt Strike",
            "id": "tool--a6346c09-4f18-4f5f-9c67-130a6d2dbf12",
            "type": "tool"
          }
        ],
        "links": [
          {
            "source": "campaign--7753a65a-8401-11ee-96a4-b02628e2a7a1",
            "type": "uses",
            "target": "attack-pattern--22905430-4901-4c2a-84f6-98243cb173f8"
          },
          {
            "source": "campaign--7753a65a-8401-11ee-96a4-b02628e2a7a1",
            "type": "uses",
            "target": "attack-pattern--b4d4e6c1-5ac1-419e-b45d-3676bfc55839"
          }
        ]
      },
      "created": 1611619200000,
      "modified": 1700083768563,
      "created_at": 1634713855844,
      "modified_at": 1700086211980
    },
    {
      "id": "ipv4-addr--f47ab7e2-1409-53bb-97c9-30407542e65f",
      "description": "CC=NL ASN=AS60404 The Infrastructure Group B.V.",
      "value": "5.255.99.59",
      "type": "ipv4-addr",
      "confidence": 15,
      "recommend": 1,
      "riskscore": 1,
      "revoked": false,
      "categories": ["malware"],
      "references": [
        "https://www.microsoft.com/en-us/security/blog/2022/10/25/dev-0832-
vice-society-opportunistic-ransomware-campaigns-impacting-us-education-
sector/",
        "https://www.cisa.gov/uscert/ncas/alerts/aa22-249a",
        "https://portal.quaxar.io/knowledgebase/document/report--
f8b940a7-09e1-423c-92b1-2a9c8972da0e"
      ],
      "sources": [
        "S2W Inc.",
```

```
      "blog.sekoia.io",
      "www.cisa.gov",
      "www.microsoft.com",
      "portal.quaxar.io",
      "blog.talosintelligence.com"
    ],
    "countries": [],
    "targets": [
      {
        "id": "threat-actor--6fa8d901-a1e7-4681-9bbe-2152c0e69d45",
        "type": "threat-actor",
        "name": "Vice Society"
      },
      {
        "id": "malware--248bb279-ff63-11ed-96a4-b02628e2a7a1",
        "type": "malware",
        "name": "rhysida"
      }
    ],
    "graph": {
      "nodes": [
        {
          "name": "Vice Society",
          "id": "threat-actor--6fa8d901-a1e7-4681-9bbe-2152c0e69d45",
          "type": "threat-actor"
        },
        {
          "name": "#StopRansomware: Rhysida Ransomware",
          "id": "campaign--7753a65a-8401-11ee-96a4-b02628e2a7a1",
          "type": "campaign"
        }
      ],
      "links": [
        {
          "source": "campaign--7753a65a-8401-11ee-96a4-b02628e2a7a1",
          "type": "uses",
          "target": "attack-pattern--22905430-4901-4c2a-84f6-98243cb173f8"
        },
        {
          "source": "campaign--7753a65a-8401-11ee-96a4-b02628e2a7a1",
          "type": "uses",
          "target": "attack-pattern--b4d4e6c1-5ac1-419e-b45d-3676bfc55839"
        }
      ]
    },
    "created": 1662553591572,
    "modified": 1700083768563,
    "created_at": 1662574205401,
    "modified_at": 1700086205013
  }
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.value`	Indicator Value	Mapped via `.type`	`.created` or `.created_at`	N/A	N/A
`.targets[]`	Tool Value	N/A	`.created` or `.created_at`	`Cobalt Strike`	If `.targets[].type` == `tool`; Related to Indicator
`.targets[]`	Vulnerability Value	N/A	`.created` or `.created_at`	`CVE-2021-26855`	If `.targets[].type` == `vulnerability`; Related to Indicator
`.targets[].mitre_id`, `.attack_patterns[].name`	Attack Pattern Value	N/A	`.created` or `.created_at`	N/A	If `.targets[].type` == `attack-pattern`; Related to Indicator; MITRE ID & Label concatenated
`.targets[]`	Malware Value	N/A	`.created` or `.created_at`	`rhysida`	If `.targets[].type` == `malware`; Related to Indicator
`.targets[]`	Adversary Name	N/A	`.created` or `.created_at`	`Lazarus`	If `.targets[].type` == `threat-actor`; Related to Indicator
`.targets[]`	Attribute	Campaign	`.created` or `.created_at`	`Sponsor with batch-filed whiskers: Ballistic Bobcat's scan and strike backdoor`	If `.targets[].type` == `campaign`
`.categories[]`	Attribute	Category	`.created` or `.created_at`	`malware`	Optional
`.confidence`	Attribute	Confidence	`.created` or `.created_at`	`15`	Optional
`.riskscore`	Attribute	Risk	`.created` or `.created_at`	`3`	Optional
`.recommend`	Attribute	Recommend	`.created` or `.created_at`	`3`	Optional
`.sources[]`	Attribute	Original Source	`.created` or `.created_at`	`otx.alienvault.com`	Optional
`.countries[]`	Attribute	Country	`.created` or `.created_at`	`North Korea`	Optional

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.

S2W Quaxar Repots

This includes the following feeds: S2W Quaxar - Threat Reports, S2W Quaxar - Vulnerability Reports, S2W Quaxar - Indicator Reports, and S2W Quaxar - Talon Reports.

METRIC	RESULT
Run Time	5 minutes
Reports	6
Report Attributes	24
Adversaries	4
Attack Patterns	1
Identities	4
Vulnerabilities	2

S2W Quaxar - Threat Actors

METRIC	RESULT
Run Time	15 minutes
Adversaries	58

METRIC	RESULT
Adversary Attributes	3,056
Attack Patterns	410
Indicators	39,634
Indicator Attributes	5,010
Malware	398
Tools	67
Vulnerabilities	82

S2W Quaxar - Ransomware Activity

METRIC	RESULT
Run Time	1 minute
Adversaries	3
Identities	4
Identity Attributes	6

S2W Quaxar - Brand Impersonation Sites

METRIC	RESULT
Run Time	1 minute
Identities	9
Indicators	45
Indicator Attributes	97

S2W Quaxar - Leaked Credit Cards

METRIC	RESULT
Run Time	1 minute
Compromised Cards	198
Compromised Card Attributes	990

S2W Quaxar - Leaked Accounts

METRIC	RESULT
Run Time	5 minutes
Compromised Accounts	9,976
Compromised Account Attributes	40,454

S2W Quaxar - Exposed Assets

METRIC	RESULT
Run Time	1 minute
Assets	43
Asset Attributes	129
Events	46
Event Attributes	46

S2W Quaxar - Signature Vault

METRIC	RESULT
Run Time	1 minute
Adversaries	6
Indicators	17
Malware	15
Signatures	42
Signature Attributes	216

S2W Quaxar - Indicators

METRIC	RESULT
Run Time	1 minute
Indicators	344
Indicator Attributes	3,513
Adversaries	30

Change Log

- **Version 1.0.0**
  - Initial release