ThreatQuotient

A Securonix Company

DomainTools Real Time Threat CDF

Version 1.0.0

May 11, 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

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: 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	1.0.0
Compatible with ThreatQ Versions	>= 5.24.1
Support Tier	ThreatQ Supported

Introduction

The DomainTools Real-Time Threat CDF integration enables ThreatQ users to ingest and operationalize high-value domain and hostname intelligence from DomainTools. By integrating multiple DomainTools intelligence feeds directly into the ThreatQ platform, this integration supports continuous enrichment of the Threat Library with newly observed, newly active, and high-risk domain indicators.

The integration provides the following feeds:

- **DomainTools Domain Hotlist** - ingests a list of active, high-risk domains with observed activity measured by DomainTools' global passive DNS sensor network.
- **DomainTools Domain Risk** - delivers domain-centric risk intelligence designed to identify and assess potentially malicious or suspicious domains.
- **DomainTools Newly Observed Domains** - ingests domains detected for the first time, enabling early identification of emerging online infrastructure.
- **DomainTools Newly Active Domains** - ingests data on domains that have recently begun resolving or exhibiting signs of activity.
- **DomainTools Newly Observed Hostnames** - ingests data on newly detected hostnames that may indicate emerging or evolving attacker infrastructure.
- **DomainTools Domain Discovery** - ingests data on domains that have recently begun resolving or exhibiting signs of activity.

The integration ingests indicators and indicator attributes into ThreatQ.

Prerequisites

The following is required to run the integration:

- A DomainTools Username.
- A DomainTools API Key.

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.

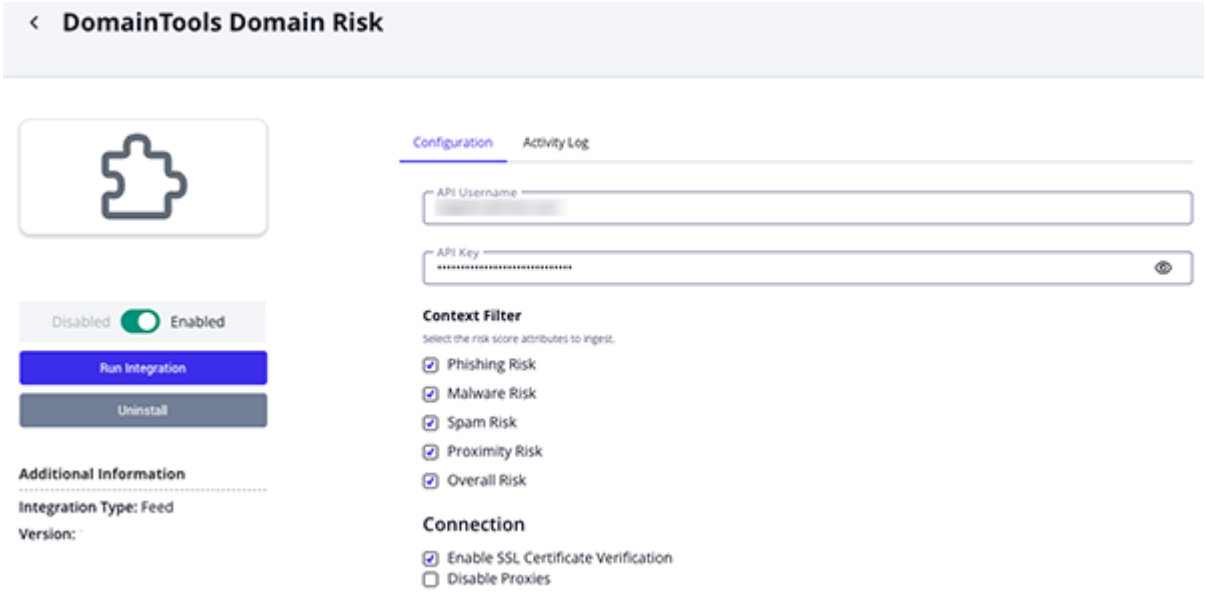
To configure the integration:

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

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

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

PARAMETER	DESCRIPTION
API Username	Enter your DomainTools username.
API Key	Enter you DomainTools API Key.
Context Filter *(**Domain Hotlist** and **Domain Risk** feeds only)*	Select the risk score attributes to ingest into ThreatQ. Options include: ◦ Phishing Risk ◦ Malware Risk ◦ pam Risk ◦ Proximity Risk ◦ Overall Risk
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

DomainTools Domain Hotlist

The DomainTools Domain Risk feed ingests a list of active, high-risk domains with observed activity measured by DomainTools' global passive DNS sensor network.

```
GET https://api.domaintools.com/v1/feed/domainhotlist?
api_username={username}&api_key={api_key}
```

Sample Response:


```
{
  "status": 206,
  "reason": "Partial Content",
  "host": "api.domaintools.com",
  "headers": {
    "Content-Type": "application/x-ndjson"
  },
  "text": "{\"timestamp\":\"2026-04-24T10:25:31Z\",\"domain\":
\"ora1i5.info\",
\"phishing_risk\":32,\"malware_risk\":20,\"spam_risk\":84,\"proximity
_risk\":100,\"overall_risk\":100,\"expires\":
\"2026-04-25T08:34:31Z\"}\n{\"timestamp\":\"2026-04-24T10:25:31Z\",
\"domain\":\"nbdmxxco.sbs\",
\"phishing_risk\":1,\"malware_risk\":97,\"spam_risk\":2,\"proximity_r
isk\":49,\"overall_risk\":97,\"expires\":\"2026-04-25T10:22:13Z\"}"
}
```


ThreatQuotient provides the following default mapping for this feed:

> The CDF will use response `url` to download data.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`domain`	`Indicator Value`	`FQDN`	`N/A`	`ora1i5.info`	`Domain value from the /feed/ domainhotlist response.`
`phishing_risk`	`Indicator Attribute`	`Phishing Risk`	`N/A`	`32`	`User-configurable. Updatable.`
`malware_risk`	`Indicator Attribute`	`Malware Risk`	`N/A`	`20`	`User-configurable. Updatable.`
`spam_risk`	`Indicator Attribute`	`Spam Risk`	`N/A`	`84`	`User-configurable. Updatable.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
proximity_risk	Indicator Attribute	Proximity Risk	N/A	100	User-configurable. Updatable.
overall_risk	Indicator Attribute	Overall Risk	N/A	100	User-configurable. Updatable.
expires	Indicator Attribute	Expiration	N/A	2026-04-25T08:34:31Z	Expiration timestamp from the /feed/domainhotlist response. Updatable.
request.url	Indicator Attribute	Feed Name	N/A	domainhotlist	Feed name derived from /feed/domainhotlist.
static	Indicator Tag	High Risk	N/A	High Risk	Tag observed in posted indicator payloads for this feed.

DomainTools Domain Risk

The DomainTools Newly Observed Domains feed delivers domain-centric risk intelligence designed to identify and assess potentially malicious or suspicious domains.

```
GET https://api.domaintools.com/v1/feed/domainrisk?
api_username={username}&api_key={api_key}
```

Sample Response:


```
{
  "status": 206,
  "reason": "Partial Content",
  "host": "api.domaintools.com",
  "headers": {
    "Content-Type": "application/x-ndjson"
  },
  "text": "{\"timestamp\":\"2026-04-24T08:39:41Z\",\"domain\":
\"lions-wwcazlegt.xyz\",
\"phishing_risk\":17,\"malware_risk\":73,\"spam_risk\":1,\"proximity_
risk\":50,\"overall_risk\":73}\n{\"timestamp\":
\"2026-04-24T08:50:12Z\",\"domain\":
\"adsfdgpeliangdancokers23.my.id\",
\"phishing_risk\":18,\"malware_risk\":31,\"spam_risk\":74,\"proximity
_risk\":37,\"overall_risk\":74}"
}
```


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	N/A	lions-wwcazlegt.xyz	Domain value from the /feed/domainrisk response.
phishing_risk	Indicator Attribute	Phishing Risk	N/A	17	User-configurable. Updatable.
malware_risk	Indicator Attribute	Malware Risk	N/A	73	User-configurable. Updatable.
spam_risk	Indicator Attribute	Spam Risk	N/A	1	User-configurable. Updatable.
proximity_risk	Indicator Attribute	Proximity Risk	N/A	50	User-configurable. Updatable.
overall_risk	Indicator Attribute	Overall Risk	N/A	73	User-configurable. Updatable.
request.url	Indicator Attribute	Feed Name	N/A	domainrisk	Feed name derived from /feed/domainrisk.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
static	Indicator Tag	High Risk	N/A	High Risk	Tag observed in posted indicator payloads for this feed.

DomainTools Newly Observed Domains

The DomainTools Newly Observed Domains feed ingests domains detected for the first time, enabling early identification of emerging online infrastructure.

```
GET https://api.domaintools.com/v1/feed/nad?api_username={username}
&api_key={api_key}
```

Sample Response:


```
{
  "status": 206,
  "reason": "Partial Content",
  "host": "api.domaintools.com",
  "headers": {
    "Content-Type": "application/x-ndjson"
  },
  "text": "{\"timestamp\":\"2026-04-27T17:01:36Z\",\"domain\":\"dcm-
invest.com\"}\n{\"timestamp\":\"2026-04-27T17:01:36Z\",\"domain\":
\"sek-trans.de\"}"
}
```


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`	`N/A`	`dcm-invest.com`	`Domain value from the /feed/nad response.`
`request.url`	`Indicator Attribute`	`Feed Name`	`N/A`	`nad`	`Feed name derived from /feed/nad.`

DomainTools Newly Active Domains

The DomainTools Newly Active Domains feed ingests data on domains that have recently begun resolving or exhibiting signs of activity.

```
GET https://api.domaintools.com/v1/feed/nad?api_username={username}
&api_key={api_key}
```

Sample Response:


```
{
  "status": 206,
  "reason": "Partial Content",
  "host": "api.domaintools.com",
  "headers": {
    "Content-Type": "application/x-ndjson"
  },
  "text": "{\"timestamp\":\"2026-04-27T17:01:36Z\",\"domain\":\"dcm-
invest.com\"}\n{\"timestamp\":\"2026-04-27T17:01:36Z\",\"domain\":
\"sek-trans.de\"}"
}
```


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`	`N/A`	`dcm-invest.com`	`Domain value from the /feed/nad response.`
`request.url`	`Indicator Attribute`	`Feed Name`	`N/A`	`nad`	`Feed name derived from /feed/nad.`

DomainTools Newly Observed Hostnames

The DomainTools Newly Observed Hostnames feed ingests data on newly detected hostnames that may indicate emerging or evolving attacker infrastructure.

```
GET https://api.domaintools.com/v1/feed/noh?api_username={username}
&api_key={api_key}
```

Sample Response:


```
{
  "status": 206,
  "reason": "Partial Content",
  "host": "api.domaintools.com",
  "headers": {
    "Content-Type": "application/x-ndjson"
  },
  "text": "{\"timestamp\":\"2026-04-24T08:34:49Z\",\"domain\":
\"www.mentoringinst.connection-trust.com\"}\n{\"timestamp\":
\"2026-04-24T08:34:49Z\",\"domain\":\"art-in-
caesarea.casino03.com\"}"
}
```


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	N/A	www.mentoringinst.connection-trust.com	Domain value from the /feed/noh response.
request.url	Indicator Attribute	Feed Name	N/A	noh	Feed name derived from /feed/noh.

DomainTools Domain Discovery

The DomainTools Domain Discovery feed ingests data on domains associated with a given starting set, providing visibility into infrastructure expansion and related domain clusters.

```
GET https://api.domaintools.com/v1/feed/domaindiscovery?
api_username={username}&api_key={api_key}
```

Sample Response:


```
{
  "status": 206,
  "reason": "Partial Content",
  "host": "api.domaintools.com",
  "headers": {
    "Content-Type": "application/x-ndjson"
  },
  "text": "{\"timestamp\":\"2026-04-27T14:58:32Z\",\"domain\":
\"ninecasinos-ita.com\"}\n{\"timestamp\":\"2026-04-27T14:58:33Z\",
\"domain\":\"dadscustom.ca\"}"
}
```


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	N/A	ninecasinos-ita.com	Domain value from the / feed/ domaindiscovery response.
request.url	Indicator Attribute	Feed Name	N/A	domaindiscovery	Feed name derived from / feed/domaindiscovery.

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.

DomainTools Domain Hotlist

METRIC	RESULT
Run Time	43 min
Indicators	99,998
Indicator Attributes	699,986

DomainTools Domain Risk

METRIC	RESULT
Run Time	34 min
Indicators	44,552
Indicator Attributes	267,312

DomainTools Newly Observed Domains

METRIC	RESULT
Run Time	30 min

METRIC	RESULT
Indicators	40,190
Indicator Attributes	40,190

DomainTools Newly Active Domains

METRIC	RESULT
Run Time	32 min
Indicators	144,937
Indicator Attributes	144,937

DomainTools Newly Observed Hostnames

METRIC	RESULT
Run Time	25 min
Indicators	5,128,551
Indicator Attributes	5,128,551

DomainTools Domain Discovery

METRIC	RESULT
Run Time	21 min

METRIC	RESULT
Indicators	16,517
Indicator Attributes	16,517

Change Log

- **Version 1.0.0**
  - Initial release