ThreatQuotient

A Securonix Company

Bolster AI Action Bundle

Version 1.0.0

July 14, 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	>= 5.29.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Bolster AI Action Bundle enables ThreatQ users to enrich FQDN and URL type indicators with threat intelligence from the Bolster AI platform. By querying the Bolster AI DomainTest and Scan APIs, the bundle retrieves domain dispositions and scan results, adding valuable context to indicators to support investigation and threat analysis within ThreatQ.

The integration provides the following actions:

- **Bolster AI - DomainTest** - submits an FQDN or URL indicator to Bolster AI and adds the returned disposition to the indicator.
- **Bolster AI - Scan Results** - maps completed Scan API-style results for an FQDN or URL indicator and adds richer scan context.

The integration is compatible with the following indicator types:

- FQDN
- URL

The integration returns enriched indicators and indicator attributes.

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

The following is required to run the integration:

- An active ThreatQ TDR Orchestrator (TQO) license.
- A valid Bolster AI API Key.
- Your Bolster AI API URL.
- A data collection containing at least one of the following indicator types:
  - FQDN
  - URL

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine
6. Select the actions to install, when prompted, and click on **Install.**

    > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

The action(s) will now be installed on your ThreatQ instance. You will still need to configure the action(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 **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

   The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Bolster AI Key	Enter your Bolster API Key.
Bolster API URL	Enter your Bolster API URL.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Bolster AI - DomainTest	Checks a domain or URL against Bolster's DomainTest API.	Indicator	FQDN, URL
Bolster AI - Scan Results	Enriches a domain or URL from Bolster Scan API results.	Indicator	FQDN, URL

Bolster AI - DomainTest

The Bolster AI - DomainTest action submits the selected indicator value to the Bolster AI DomainTest endpoint and adds the returned disposition to the indicator.

```
GET https://developers.bolster.ai/api/neo/v1/domainTest
```

Sample Response (If URL does exist in Bolster):

```
false
```

Sample Response (If URL exists in Bolster):

```
"suspicious"
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.disposition	Indicator.Attribute	Disposition	N/A	suspicious	Added only when the API returns a value.

Bolster AI - Scan Results

Bolster AI - Scan Results action retrieves and maps detailed scan results from the Bolster AI Scan API, enriching FQDN and URL indicators with additional analysis and contextual intelligence.

```
POST https://developers.bolster.ai/api/neo/scan/status
```

Sample Response:


```
{
  "job_id": "7f786af7-f9c8-4d4c-9df5-014b46c7b241",
  "status": "DONE",
  "url": "http://suspicious-login.com/admin",
  "url_sha256":
"2e90e4c1df7e45c772ff92418dc1b77c21f474b36d3d7a3f397ea580f6582505",
  "disposition": "phish",
  "brand": "example-bank",
  "categories": ["zero-day phishing"],
  "tags": ["Watchlist"],
  "insights": {
    "insights_path": "https://checkphish.ai/insights/url/
1654129884891/2e90e4c1df7e45c772ff92418dc1b77c21f474b36d3d7a3f397ea58
0f6582505",
    "resolved": true,
    "past_phish": 4
  }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.disposition	Indicator.Attribute	Scan Disposition	N/A	phish	N/A
.brand	Indicator.Attribute	Targeted Brand	N/A	example-bank	N/A
.categories[]	Indicator.Attribute	Categories	N/A	zero-day phishing	N/A
.url_sha256	Indicator.Attribute	URL SHA256	N/A	2e90e4c1df7e45c772ff92418dc1b77c21f474b36d3d7a3f397ea580f6582505	N/A
.insights.insights_path	Indicator.Attribute	Insights URL	N/A	https://checkphish.ai/insights/...	N/A
.insights.resolved	Indicator.Attribute	Resolved	N/A	true	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.insights.past_phish`	`Indicator.Attribute`	`Past Phish Count`	`N/A`	`4`	`N/A`

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

Bolster AI - DomainTest

METRIC	RESULT
Run Time	1 minute
Indicators	1
Indicator Attributes	1

Bolster AI - Scan Results

METRIC	RESULT
Run Time	1 minute
Indicators	1
Indicator Attributes	7

Change Log

- **Version 1.0.0**
  - Initial release