ThreatQuotient

A Securonix Company

Allure Security Operation

Version 1.0.0

September 22, 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	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The Allure Security Operation lets an analyst report the active ThreatQ indicator directly from its object page.

Allure Security provides an AI-native brand protection platform that detects and dismantles digital impersonation threats, phishing websites, and disinformation across the web, social media, mobile apps, and the dark web. Backed by a 24/7 managed Security Operations Center (SOC), the service blocks and takes down malicious infrastructure.

The integration provides the following operation actions:

- **Report Threats** - reports a URL or FQDN as an existing website, app, or profile impersonating a protected brand.
- **Report Parked Domains** - reports an FQDN for monitoring in case it hosts impersonating content in the future.

The integration is compatible with URL and FQDN indicator types.

Prerequisites

The following is required to run the integration:

- An Allure Security API key with the `Reporter` role.
- At least one protected brand configured in Allure Security

API keys are available in the Allure Security portal under **Settings > API Keys**. Protected brand names are listed under **Settings > Entitlements**.

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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the integration file on your local machine

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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Allure Security API key used for bearer authentication. The API key must have the Allure `Reporter` role.

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.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Report Threats	Reports a website, app, or profile as a current brand threat.	Indicator	URL, FQDN
Report Parked Domains	Reports a parked domain for future impersonation monitoring.	Indicator	FQDN

Report Threats

The Report Threats action submits the active URL or FQDN to Allure Security using the following endpoint:

```
POST https://api.alluresecurity.com/api/v4/report-threat/current-threat
```

The action uses bearer authentication and sends `originalUrl`, `brand`, `type`, and `comment` as `text/plain` parts within a `multipart/form-data` request. This format ensures that supported ThreatQ versions generate the required multipart boundary even when no file is attached. If no comment is provided, the action sends an empty `comment` part.

Sample New Record Response:

```
{
  "alertId": 977101,
  "createdTime": "2026-07-15T16:15:10.734073918Z",
  "status": "Needs Customer Review",
  "risk": "Suspicious",
  "type": "Web",
  "url": "https://maliciousdomain.com",
  "brand": "acme.com",
  "reporter": "customer"
}
```

Sample Existing-Record Response:

```
{
  "createDetection": false,
  "reason": "Detection already exists for this URL"
}
```

The action displays a report summary and the raw API response. A response containing `alertId` is classified as new; a response containing `createDetection` is classified as `existing`.

Run Configuration Options

These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration option is provided when using the action on an object:

PARAMETER	DESCRIPTION
Brand	Enter the protected brand associated with the threat report.
Threat Type	Select the type of threat to report. Available options are **Web**, **Mobile**, **Social**, **Executive**, and **Ad**. The default value is **Web**.
Scheme to Prepend	Select the HTTP scheme to prepend when neither the submitted indicator nor its `Scheme` attribute specifies one. The default value is **HTTPS**.
Comment (Optional)	Enter any additional context to provide to the Allure Security SOC analyst.
Strip 'www' Prefix	Enable this parameter to remove a leading `www.` prefix from the submitted domain or URL hostname. This parameter is disabled by default.
Apply Attribute for Net New Records	Enable this parameter to add or update the `Report Threat Result = new` attribute when Allure Security creates a new alert for the submitted threat. This parameter is disabled by default.
Apply Attribute for Existing Records	Enable this parameter to add or update the `Report Threat Result = existing` attribute when the submitted threat is already known to Allure Security. This parameter is disabled by default.

If the indicator does not include a scheme, the action first uses the indicator's `Scheme` attribute when it is set to `http` or `https`. If no valid `Scheme` attribute is available, the action uses the configured **Scheme to Prepend** value. For

scheme-less indicators ending in port 443 or 80, the action applies HTTPS or HTTP, respectively, and removes the standard port suffix before submission.

Before submitting the indicator, the action verifies that it is a valid HTTP or HTTPS URL with a valid hostname. URLs containing embedded credentials, invalid ports, whitespace, control characters, or unsupported URI schemes are rejected.

Report Parked Domains

The Report Parked Domains action submits the active FQDN to Allure Security using the following endpoint:

```
POST https://api.alluresecurity.com/api/v4/report-threat/parked-domain
```

The action uses bearer authentication and sends the `domain` and `brand` values as text parts within a `multipart/form-data` request. Before submitting the request, the action verifies that the domain is a valid multi-label FQDN. Values containing URL syntax, IP addresses, or malformed DNS labels are rejected.

Sample Response:

```
{
  "id": 78725497,
  "brandName": "acme.com",
  "createDomain": true,
  "domain": "m1cros0ftserv1ces.com",
  "tags": [],
  "status": "Parked",
  "createTimestamp": "2026-07-15T16:15:54.509288084Z",
  "hasMxRecord": false
}
```

The action displays a report summary and the raw API response. `createDomain: true` is classified as new and `createDomain: false` is classified as existing.

Run Configuration Options

> These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following configuration option is provided when using the action on an object:

PARAMETER	DESCRIPTION
Brand	Enter the protected brand associated with the parked domain report.
Strip 'www' Prefix	Enable this parameter to remove a leading `www.` prefix from the submitted domain. This parameter is disabled by default.
Apply Attribute for Net New Records	Enable this parameter to add or update the `Report Parked Domain Result = new` attribute when Allure Security creates a new record for the submitted domain. This parameter is disabled by default.
Apply Attribute for Existing Records	Enable this parameter to add or update the `Report Parked Domain Result = existing` attribute when the submitted domain is already known to Allure Security. This parameter is disabled by default.

Known Issues / Limitations

- The operation does not attach files to threat reports.

Change Log

- **Version 1.0.0**
  - Initial release