# ThreatQuotient

**A Securonix Company**

## Allure Security Action Bundle

**Version 1.0.0**

July 27, 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** | >= 6.7.3 |
| **ThreatQ TQO License Required** | Yes |
| **Support Tier** | ThreatQ Supported |

# Introduction

The Allure Security Action Bundle integrates ThreatQ with the Allure Security AI-native brand protection platform, enabling organizations to automatically report potential phishing websites, malicious domains, and parked domains directly from ThreatQ. By incorporating these actions into ThreatQ Orchestration Workflows, security teams can streamline the reporting of curated intelligence to Allure Security, accelerating threat investigation, monitoring, and takedown efforts while reducing manual effort.

The integration provides the following actions:

- **Allure Security - Report Parked Domains** - reports FQDN indicators identified as parked domains from ThreatQ to Allure Security for monitoring and analysis.
- **Allure Security - Report Threats** - reports URL and FQDN indicators from ThreatQ to Allure Security as potential threats for investigation and response.

The integration is compatible with URL and FQDN indicator types.

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

# Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- An Allure Security API Key.
- A data collection containing 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

    > 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.

You will still need to configure the action.

# 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.

## Report Parked Domains Parameters

| PARAMETER | DESCRIPTION |
|---|---|
| **API Key** | Enter your Allure Security API key to authenticate requests to the Allure Security API. |
| **Brand** | Enter the brand name associated with the report. Brand names are available in the Allure Security portal under Settings > Entitlements. If your account includes multiple brands, create separate workflows for each brand. |
| **Strip 'www' Prefix** | Enable this parameter to remove the `www` prefix from domain names and URLs before submitting them to Allure Security. |
| **Apply Attribute for Net New Records** | Enable this parameter to add the Report Parked Domain Result attribute with a value of `new` when the API creates a new record. |

| PARAMETER | DESCRIPTION |
|---|---|
| **Apply Attribute for Existing Records** | Enable this parameter to add the Report Parked Domain Result attribute with a value of `existing` when the API updates an existing record. |
| **Objects Per Run** | The number of objects to process per run of the workflow. The default value is `100`. |

## Report Threats Parameters

| PARAMETER | DESCRIPTION |
|---|---|
| **API Key** | Enter your **Allure Security API key** to authenticate requests to the Allure Security API. |
| **Scheme to Prepend** | Select the scheme to prepend when a URL or domain value does not already include one. Options include:<br>◦ Prepend HTTPS *(default)*<br>◦ Prepend HTTP |
| **Threat Type** | Select the threat type to assign to reported threats. Options include:<br>◦ Web *(default)*<br>◦ Mobile<br>◦ Social<br>◦ Executive<br>◦ Ad |
| **Brand** | Enter the **brand name** associated with the report. Brand names are available in the Allure Security portal under **Settings > Entitlements**. If your account includes multiple brands, create separate workflows for each brand. |

| PARAMETER | DESCRIPTION |
|---|---|
| **Comment** | Optional - enter additional information about the reported threat for review by the Allure Security SOC analyst. |
| **Strip `www` Prefix** | Enable this parameter to remove the `www` prefix from domain names and URLs before submitting them to Allure Security. |
| **Apply Attribute for Net New Records** | Enable this parameter to add the **Report Threat Result** attribute with a value of `new` when the API creates a new record. |
| **Apply Attribute for Existing Records** | Enable this parameter to add the **Report Threat Result** attribute with a value of `existing` when the API updates an existing record. |
| **Objects Per Run** | Specify the maximum number of objects to process during each workflow execution. The default value is `100`. |

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 |
|---|---|---|---|
| Report Parked Domains | Submits domains to Allure Security, as parked domains. | Indicators | FQDN |
| Report Threats | Submits URLs to Allure Security, as threats. | Indicators | URL, FQDN |

# Allure Security - Report Parked Domains

The Allure Security - Report Parked Domains action enables you to report parked domains from ThreatQ to Allure Security for analysis and tracking. The action identifies FQDN indicators in the input data and submits them to the Allure Security platform.

```
POST https://api.alluresecurity.com/api/v4/report-threat/parked-domain?domain={{ ioc }}&brand={{ brand }}
```

**Sample Response:**

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

ThreatQuotient provides the following default mapping for this action:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| API response | Indicator.Attribute | Report Parked Domain Result | N/A | new, existing | Optional; controlled by the net new and existing record attribute toggles |

# Allure Security - Report Threats

The Allure Security - Report Threats action enables you to report suspected malicious websites to Allure Security for investigation. The action identifies URL and FQDN indicators in the input data and submits them to the Allure Security platform, along with any additional context configured for the workflow.

```
POST https://api.alluresecurity.com/api/v4/report-threat/current-threat?originalUrl={{ ioc }}&brand={{ brand }}&type={{ threat_type }}&comment={{ comment }}
```

**Sample Response:**


```
{
    "alertId": 977101,
    "createdTime": "2026-07-15T16:15:10.734073918Z",
    "status": "Needs Customer Review",
    "risk": "Suspicious",
    "type": "Web",
    "url": "https://maliciousdomain.com",
    "screenshot": null,
    "brand": "acme.com",
    "reporter": "customer",
    "description": null,
    "takedownInitiatedDate": null,
    "blockedDate": null,
    "takedownCompletedDate": null,
    "domainInfo": {
        "serverIp": null,
        "organization": null,
        "country": null,
        "dns": null,
        "sslCertificate": null,
        "whois": null,
        "registrar": null,
        "registrantContact": null,
        "redirectRequest": null
    },
    "message": null,
    "domainHistory": [],
    "tags": [],
    "pageContentCategories": [],
    "promotedFromMonitoredSites": false,
```

```
    "monitoredSiteMatch": null,
    "additionalAlerts": null
}
```

ThreatQuotient provides the following default mapping for this action:

| FEED DATA PATH | THREATQ ENTITY | THREATQ OBJECT TYPE OR ATTRIBUTE KEY | PUBLISHED DATE | EXAMPLES | NOTES |
|---|---|---|---|---|---|
| API response | Indicator.Attribute | Report Threat Result | N/A | new, existing | Optional; controlled by the net new and existing record attribute toggles |

# 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.

## Allure Security - Report Parked Domains

| METRIC | RESULT |
|---|---|
| **Run Time** | 2 minutes |
| **Indicators** | 52 |

## Allure Security - Report Threats

| METRIC | RESULT |
|---|---|
| **Run Time** | 5 minutes |
| **Indicators** | 1,254 |

# Use Case Example

Your security team maintains a curated list of **URL** and **FQDN** indicators associated with potential brand impersonation, phishing campaigns, and suspicious parked domains. To accelerate brand protection efforts, you configure a ThreatQ Orchestration Workflow that automatically submits newly identified indicators to Allure Security.

As new domains and URLs are added to ThreatQ through threat intelligence, analyst investigations, or internal detections, the workflow reports them to Allure Security using either the **Report Threats** or **Report Parked Domains** action. This automated integration eliminates manual reporting, ensures that potential threats are submitted for analysis as soon as they are identified, and enables Allure Security to begin monitoring, investigating, and taking appropriate action against malicious infrastructure more quickly.

# Change Log

- **Version 1.0.0**
  - Initial release