ThreatQuotient

A Securonix Company

Joe Sandbox Action Bundle

Version 1.0.0

July 07, 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 **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
Actions **11**
Joe Sandbox - Submit 12
Joe Sandbox - Get Report 14
Enriched Data **17**
Joe Sandbox - Submit 17
Joe Sandbox - Get Report 17
Change Log **18**

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 Joe Sandbox Action Bundle enables ThreatQ users to automate malware analysis by submitting supported URL indicators and ThreatQ files to Joe Sandbox Cloud and retrieving analysis results directly into ThreatQ. The bundle streamlines submission and enrichment workflows, allowing analysts to incorporate Joe Sandbox intelligence into their ThreatQ investigations.

The integration provides the following actions:

- **Joe Sandbox - Submit** - submits supported URL indicators and ThreatQ files to Joe Sandbox Cloud for analysis. URL indicators can be submitted either as browser URLs or as URL-hosted file samples, depending on the configured submission type.
- **Joe Sandbox - Get Report** - retrieves the analysis report for an existing Joe Sandbox submission and enriches the associated ThreatQ indicator with report details and related intelligence.

The integration is compatible with the following object types:

- Indicators
  - Filename
  - MD5
  - SHA-1
  - SHA-256
  - URL
- Files

The integration returns the following enriched object types:

- Indicators
  - Indicator Attributes
- Files
  - File Attributes
- Reports
  - Report Attributes

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.
- A Joe Sandbox API Key.
- A valid Joe Sandbox analysis system such as `w10x64`.
- A data collection containing at least one of the following object types:
  - Indicator
    - Filename
    - MD5
    - SHA-1
    - SHA-256
    - URL
  - File

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
API Key	Enter the API key used to authenticate requests to Joe Sandbox.
API URL	Enter the base URL for the Joe Sandbox API. The default value is `https://www.joesandbox.com/api`.
Default URL Scheme	Select the protocol to prepend to URL indicators that do not begin with `http://` or `https://`. The default value is `HTTPS`.
URL Submission Type	Select whether URL indicators are submitted using the Joe Sandbox `url` field or the `sample-url` field.
Analysis System	Specify the Joe Sandbox analysis system to use for submitted samples. Options include: ◦ Windows 10 x64: `w10x64` *(Default)*

PARAMETER	DESCRIPTION
	◦ Windows 10 x64 Remote Assistance: `w10x64_ra` ◦ Windows 10 x64 Native: `w10x64native` ◦ Windows 7 x64: `w7x64` ◦ Ubuntu Linux 20.04 x64: `lnxubuntu20` ◦ Ubuntu Linux 16.04 x64: `lnxubuntu1` ◦ macOS Monterey: `macvm-monterey` ◦ Windows 11 x64 Office: `w11x64_office`
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.
Objects Per Run	Specify the maximum number of objects to process during a single execution. The default value is `1000`.

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
Joe Sandbox - Submit	Submit a URL, URL-hosted sample, or ThreatQ file for analysis	Indicators, Files	Indicator type - URL
Joe Sandbox - Get Report	Retrieve a completed or in-progress Joe Sandbox submission report	Indicators, Files	Indicator type - URL, MD5, SHA-1, SHA-256, Filename

Joe Sandbox - Submit

The Joe Sandbox – Submit action submits supported URL indicators and ThreatQ files to Joe Sandbox for analysis using a common submission endpoint.

```
POST https://www.joesandbox.com/api/v2/submission/new
```

For URL indicators, the **URL Submission Type** parameter determines how the indicator is submitted:

- **`url`** – Opens and analyzes the URL in the selected Joe Sandbox analysis environment.

  Sample URL Request:

  ```
  {
    "accept-tac": "1",
    "systems[]": ["w10x64"],
    "url": "https://www.example.com"
  }
  ```

- **`sample-url`** – Downloads and analyzes the file hosted at the specified URL.

  Sample URL-Hosted File Request:

  ```
  {
    "accept-tac": "1",
    "systems[]": ["w10x64"],
    "sample-url": "https://github.com/ytisf/theZoo/raw/master/
  malware/Binaries/All.ElectroRAT/All.ElectroRAT.zip"
  }
  ```

For ThreatQ files, the action downloads the file from ThreatQ and submits it to Joe Sandbox as a multipart file sample.

Sample File Response:

```
{
  "accept-tac": "1",
  "systems[]": ["w10x64"],
  "sample": {
    "filename": "joe_test.txt",
    "content_type": "text/plain",
    "value": "This is a harmless test file."
```

```
  }
}
```

Sample Response:

```
{
  "data": {
    "submission_id": "1867086"
  }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.submission_id	Indicator.Attribute	Joe Sandbox Submission ID	N/A	1867086	N/A
.data.submission_id	File.Attribute	Joe Sandbox Submission ID	N/A	1870001	N/A

Joe Sandbox - Get Report

The Joe Sandbox – Get Report action retrieves the analysis report for an indicator that contains a valid Joe Sandbox `Submission ID` attribute. The action uses the stored Submission ID to query Joe Sandbox and return the corresponding report details to ThreatQ.

`POST https://www.joesandbox.com/api/v2/submission/info`

Sample Request:

```
{
  "submission_id": "1867086"
}
```

Sample Response:

```
{
  "data": {
    "submission_id": "1869360",
    "name": "https://www.google.com",
    "time": "2026-06-23T08:39:18+02:00",
    "status": "finished",
    "analyses": [
      {
        "webid": "1932342",
        "time": "2026-06-23T08:39:19+02:00",
        "runs": [
          {
            "detection": "clean",
            "error": null,
            "system": "w10x64",
            "yara": false,
            "sigma": false,
            "suricata": false,
            "score": 2
          }
        ],
        "tags": [
          "malware",
          "phishing"
        ],
        "encrypted": false,
        "analysisid": "1932342",
```

```
        "duration": 275,
        "md5": "44d88512fea8a8f36de82e1278abb0",
        "sha1": "3395856ce81f2b7382dee72062f798",
        "sha256": "275a021bbfb6489e54d471899f7db9",
        "filename": "sample_report.pdf",
        "scriptname": "browseurl.jbs",
        "status": "finished",
        "comments": "Analysis completed successfully without
structural errors.",
        "classification": "spyw.evad",
        "threatname": "Amadey",
        "score": 2,
        "detection": "clean",
        "has_malwareconfig": false
      }
    ],
    "most_relevant_analysis": {
      "webid": "1932342",
      "detection": "clean",
      "score": 2
    }
  }
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.analyses[].analysisid	Indicator.Attribute	Joe Sandbox Report ID	N/A	1930015	Added to the original indicator.
.data.analyses[].webid	Indicator.Attribute	Joe Sandbox Report Link	N/A	https://www.joesandbox.com/analysis/1930015	Built from the Joe Sandbox report base URL and the webid.
.data.analyses[].status	Indicator.Attribute	Joe Sandbox Status	N/A	finished	Analysis status.
.data.analyses[].detection	Indicator.Attribute	Joe Sandbox Detection	N/A	clean	Analysis detection verdict.
.data.analyses[].score	Indicator.Attribute	Joe Sandbox Score	N/A	1	Joe Sandbox score.
.data.analyses[].classification	Indicator.Attribute	Joe Sandbox Classification	N/A	spyw.evad	Only mapped when present.
.data.analyses[].threatname	Indicator.Attribute	Joe Sandbox Threat Name	N/A	Amadey	Only mapped when present.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.analyses[].runs[].system	Indicator.Attribute	System <system> Detection	N/A	System w10x64 Detection: clean	Added when the run has a detection and no run error.
.data.analyses[].md5	Related Indicator.value	MD5	N/A	44d88612fea8a8f36de82e1278abb02f	Created as related indicator when present.
.data.analyses[].sha1	Related Indicator.value	SHA-1	N/A	3395856ce81f2b7382dee72602f798b642f14140	Created as related indicator when present.
.data.analyses[].sha256	Related Indicator.value	SHA-256	N/A	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f	Created as related indicator when present.
.data.analyses[].filename	Related Indicator.value	Filename	N/A	https://www.example.com	Created as related indicator when present.
data.analyses[].analysisid	Report.Attribute	Joe Sandbox Report ID	N/A	1932342	N/A
data.analyses[].webid	Report.Attribute	Joe Sandbox Report Link	N/A	https://www.joesandbox.com/analysis/1932342	N/A
data.analyses[].threatname	Report.Attribute	Joe Sandbox Threat Name	N/A	``	N/A
text	Report	Description	N/A	Joe Sandbox Report Link: ...	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.

Joe Sandbox - Submit

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	1
Files	1
File Attributes	1

Joe Sandbox - Get Report

METRIC	RESULT
Run Time	2 minutes
Indicators	1
Indicator Attributes	8
Reports	1
Report Attributes	6

Change Log

- **Version 1.0.0**
  - Initial release