ThreatQuotient

A Securonix Company

Joe Sandbox CDF

Version 2.0.0

June 23, 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	2.0.0
Compatible with ThreatQ Versions	>= 6.0.0
Support Tier	ThreatQ Supported

Introduction

The Joe Sandbox CDF for ThreatQ enables analysts to automatically ingest analysis reports for samples submitted to Joe Sandbox.

The integration provides the following feed:

- **Joe Sandbox Analyses** - retrieves analyses available to the configured Joe Sandbox account and ingests detailed information for each analysis.
- **Joe Sandbox Submissions** - pulls analysis reports for samples submitted to Joe Sandbox.

The integration ingests the following system objects:

- Reports
- Indicators
- Malware

Prerequisites

The Joe Sandbox CDF integration for ThreatQ requires the following:

- A Joe Sandbox API Key which can be located under User Settings for your Joe Sandbox account.

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
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:

Joe Sandbox Analyses Parameters

PARAMETER	DESCRIPTION
Joe Sandbox API Host	Select the Joe Sandbox API endpoint to use for connectivity and data retrieval. If your account utilizes a legacy API key, select the **Legacy** option. Otherwise, use the **Current** endpoint. Options include: ◦ Current (`joesandbox.com/api`) *(Default)* ◦ Legacy (`jbxcloud.joesecurity.org/api`) ◦ Custom (Specify a custom API endpoint)
Custom API URL	Enter the URL of the custom Joe Sandbox API endpoint to use. Include the protocol (for example, `https://`) and the `/api` path unless your custom deployment uses a different endpoint structure or does not require the `/api` path. This parameter is only accessible if you have selected `Custom` in the **Joe Sandbox API Host** parameter.

PARAMETER	DESCRIPTION
Joe Sandbox API Key	Your Joe Sandbox API Key. This can be found under your User Settings in Joe Sandbox site.
Create Report for Each Analysis	Enable this parameter to create a report for each analysis that is ingested. Each report will contain details about the sandbox execution environment, detected YARA rule matches, and other analysis findings. The report will also be automatically related to any indicators extracted from the analysis, providing additional context for investigation and threat analysis.
Disposition Filter	Select the dispositions to ingest analysis for in ThreatQ. Options include: ◦ Unknown ◦ Clean ◦ Malicious *(Default)* ◦ Suspicious *(Default)*
Context Filter	Select the pieces of context you would like to be brought in with the sandbox reports. Options include: ◦ Joe Sandbox Link *(Default)* ◦ Disposition *(Default)* ◦ Classification *(Default)* ◦ Threat Score *(Default)* ◦ Related Malware *(Default)* ◦ Tags *(Default)* ◦ Sample SHA-1 Hash *(Default)* ◦ Sample SHA-256 Hash *(Default)* ◦ Sample Filename / URL *(Default)* ◦ Sandbox Environment *(Default)* ◦ Sandbox Script ◦ Triggered YARA Rule

PARAMETER	DESCRIPTION
	◦ Comments ◦ Sample MD5 Hash *(Default)* ◦ Triggered Sigma Rule

Joe Sandbox Submissions Parameters

PARAMETER	DESCRIPTION
Joe Sandbox API Host	Select the Joe Sandbox API endpoint to use for connectivity and data retrieval. If your account utilizes a legacy API key, select the **Legacy** option. Otherwise, use the **Current** endpoint. Options include: ◦ Current (`joesandbox.com/api`) *(Default)* ◦ Legacy (`jbxcloud.joesecurity.org/api`) ◦ Custom (Specify a custom API endpoint)
Custom API URL	Enter the URL of the custom Joe Sandbox API endpoint to use. Include the protocol (for example, `https://`) and the `/api` path unless your custom deployment uses a different endpoint structure or does not require the `/api` path. This parameter is only accessible if you have selected `Custom` in the **Joe Sandbox API Host** parameter.
Joe Sandbox API Key	Your Joe Sandbox API Key. This can be found under your User Settings in Joe Sandbox site.
Include Shared Submissions	Enable this parameter to include submissions that have been shared with you.

PARAMETER	DESCRIPTION
Create Report for Each Analysis	Enable this parameter to create a report for each analysis that is ingested. Each report will contain details about the sandbox execution environment, detected YARA rule matches, and other analysis findings. The report will also be automatically related to any indicators extracted from the analysis, providing additional context for investigation and threat analysis.
Disposition Filter	Select the dispositions to ingest analysis for in ThreatQ. Options include: ◦ Unknown ◦ Clean ◦ Malicious *(Default)* ◦ Suspicious *(Default)*
Context Filter	Select the pieces of context you would like to be brought in with the sandbox reports. Options include: ◦ Joe Sandbox Link *(Default)* ◦ Disposition *(Default)* ◦ Classification *(Default)* ◦ Threat Score *(Default)* ◦ Related Malware *(Default)* ◦ Tags *(Default)* ◦ Comments ◦ Sample MD5 Hash *(Default)* ◦ Sample SHA-1 Hash *(Default)* ◦ Sample SHA-256 Hash *(Default)* ◦ Sample Filename / URL *(Default)* ◦ Sandbox Environment *(Default)* ◦ Sandbox Script ◦ Triggered YARA Rule ◦ Triggered Sigma Rule

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

Joe Sandbox Analyses

The Joe Sandbox Analyses feed retrieves analysis submissions available to the configured account and ingests detailed information for each analysis into ThreatQ

`POST https://www.joesandbox.com/api/v2/analysis/list`

Sample Response:

```
{
  "data": [
    {
      "webid": "2530138"
    },
    {
      "webid": "2530129"
    },
    {
      "webid": "2530128"
    }
  ],
  "pagination": {}
}
```

The mappings for this feed are based on the data returned by the **Get Analysis Details** Supplemental Feed.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES	
`.analysisid`	`Report`	`N/A`	`URL query is stripped from title`	`.time`	`Joe Sandbox Analysis: http://begadi.ga/clue/gate.php`	`If report creation is enabled`
`.classification`	`Report.Attribute, Indicator.Attribute`	`Classification`	`N/A`	`N/A`	`spyw.evad`	`If enabled and non-empty`
`.comments`	`Report.Attribute`	`Comment`	`N/A`	`N/A`	`N/A`	`If enabled and non-empty`
`.detection`	`Report.Attribute, Indicator.Attribute`	`Disposition`	`N/A`	`N/A`	`malicious`	`If enabled and non-empty`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES	
.runs[0].sigma	Report.Attribute	Triggered Sigma Rule	Boolean rendered as True/False	N/A	False	If enabled and present
.runs[0].yara	Report.Attribute	Triggered YARA Rule	Boolean rendered as True/False	N/A	True	If enabled and present
.runs[0].system	Report.Attribute	Sandbox Environment	N/A	N/A	w10x64_office	If enabled and non-empty
.score	Report.Attribute, Indicator.Attribute	Threat Score	String	N/A	88	If enabled and present, including 0
.scriptname	Report.Attribute	Sandbox Script	N/A	N/A	urldownload.jbs	If enabled and non-empty
.threatname	Related Malware.Value	N/A	N/A	.time	Amadey	If enabled and not Unknown
.tags[]	Report.Tag	N/A	N/A	N/A	N/A	If enabled and present
.analysisid	Report.Attribute	Joe Sandbox Link	Derived from the selected API host	N/A	https://www.joesandbox.com/analysis/1824743/0/html	If enabled
.filename	Related Indicator.Value	URL or Filename	Type depends on value	.time	http://begadi.ga/clue/gate.php	If enabled
.md5	Related Indicator.Value	MD5	N/A	.time	N/A	If enabled and non-empty
.sha1	Related Indicator.Value	SHA-1	N/A	.time	N/A	If enabled and non-empty
.sha256	Related Indicator.Value	SHA-256	N/A	.time	N/A	If enabled and non-empty

Joe Sandbox Submissions

The Joe Sandbox Submissions feed retrieves submissions from the configured Joe Sandbox account, with the option to include shared submissions. For each submission, the feed retrieves detailed analysis results and ingests the associated intelligence into ThreatQ, providing visibility into analyzed samples and related threat data.

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

Sample Response:

```
{
  "data": [
    {
```

```
      "submission_id": "1158330"
    }
  ],
  "pagination": {}
}
```

The mappings for this feed are based on the data returned by the **Get Analysis Details** Supplemental Feed.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES	
.analysisid	Report	N/A	URL query is stripped from title	.time	Joe Sandbox Analysis: http://links.notification.intuit.com/ls/click	If report creation is enabled
.classification	Report.Attribute, Indicator.Attribute	Classification	N/A	N/A	spyw.evad	If enabled and non-empty
.comments	Report.Attribute	Comment	N/A	N/A	N/A	If enabled and non-empty
.detection	Report.Attribute, Indicator.Attribute	Disposition	N/A	N/A	clean	If enabled and non-empty
.runs[0].sigma	Report.Attribute	Triggered Sigma Rule	Boolean rendered as True/False	N/A	False	If enabled and present
.runs[0].yara	Report.Attribute	Triggered YARA Rule	Boolean rendered as True/False	N/A	False	If enabled and present
.runs[0].system	Report.Attribute	Sandbox Environment	N/A	N/A	w7x64	If enabled and non-empty
.score	Report.Attribute, Indicator.Attribute	Threat Score	String	N/A	0	If enabled and present, including 0
.scriptname	Report.Attribute	Sandbox Script	N/A	N/A	browseurl.jbs	If enabled and non-empty
.threatname	Related Malware.Value	N/A	N/A	.time	Amadey	If enabled and not Unknown
.tags[]	Report.Tag	N/A	N/A	N/A	N/A	If enabled and present
.analysisid	Report.Attribute	Joe Sandbox Link	Derived from the selected API host	N/A	https://www.joesandbox.com/analysis/846946/0/html	If enabled

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES	
.filename	Related Indicator.Value	URL or Filename	Type depends on value	.time	http://links.notification.intuit.com/ls/click?...	If enabled
.md5	Related Indicator.Value	MD5	N/A	.time	N/A	If enabled and non-empty
.sha1	Related Indicator.Value	SHA-1	N/A	.time	N/A	If enabled and non-empty
.sha256	Related Indicator.Value	SHA-256	N/A	.time	N/A	If enabled and non-empty

Get Analysis Details (Supplemental)

The Get Analysis Details supplemental feed fetches the details for a given submission ID.

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

Sample Response:


```
{
  "data": {
    "webid": "2530138",
    "time": "2022-04-19T15:28:17+02:00",
    "runs": [
      {
        "detection": "malicious",
        "error": null,
        "system": "w10x64_office",
        "yara": true,
        "sigma": false,
        "score": 88
      }
    ],
    "tags": [],
    "encrypted": false,
    "analysisid": "1824743",
    "duration": 491,
    "md5": "",
    "sha1": "",
    "sha256": "",
```

Get Submission Info (Supplemental)

The Get Submission Info supplemental feed fetches the details for a given submission ID.

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

Sample Response (truncated):


```
{
  "data": {
    "submission_id": "1158330",
    "name": "http://links.notification.intuit.com/ls/click?
upn=n1D1vNUf2DDfuFJ7P-2Bs2FOjggKQQ40"

"p0FkC-2Bz2D1trTjUxBswHbIwXnSGdD95YX6-2B4N1701lJdBFYH3-2BiUm8cg-3
(...)",
    "time": "2023-04-14T17:32:52+02:00",
    "status": "finished",
    "analyses": [
      {
        "webid": "1214018",
        "time": "2023-04-14T17:32:53+02:00",
        "runs": [
          {
            "detection": "clean",
            "error": null,
            "system": "w7x64",
            "yara": false,
            "sigma": false,
            "snort": false,
            "score": 0
          }
        ],
        "tags": [],
        "encrypted": false,
        "analysisid": "846946",
        "duration": 267,
        "md5": "",
        "sha1": "",
        "sha256": "",
        "filename": "http://links.notification.intuit.com/ls/
click?...",
        "scriptname": "browseurl.jbs",
```

```
        "status": "finished",
        "comments": "",
        "classification": "",
        "threatname": "",
        "score": 0,
        "detection": "clean"
      }
    ],
    "most_relevant_analysis": {
      "webid": "1214018",
      "detection": "clean",
      "score": 0
    }
  }
}
```

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.

Joe Sandbox Analyses

METRIC	RESULT
Run Time	1 minute
Reports	4
Report Attributes	25
Indicators	4
Indicator Attributes	8
Malware	1

Joe Sandbox Submissions

METRIC	RESULT
Run Time	1 minute
Reports	4
Report Attributes	25
Indicators	4

METRIC	RESULT
Indicator Attributes	8
Malware	1

Change Log

- **Version 2.0.0**
  - Added support for the latest API endpoints while maintaining backward compatibility with legacy API implementations, ensuring continued functionality across both current and existing deployments.
  - Added a new feed, **Joe Sandbox Analyses**, enabling ingestion of analysis results generated from submissions associated with the configured Joe Sandbox account. This feed focuses exclusively on analyses submitted by the authenticated user.
  - Add the following new configuration parameters to the **Joe Sandbox Submissions** feed:
    - Joe Sandbox API Host
    - Custom API URL
    - Include Shared Permissions
    - Create Report for Each Analysis
  - Updated the minimum ThreatQ version to 6.0.0.
- **Version 1.0.0**
  - Initial release