ThreatQuotient

Check Point SandBlast Operation Guide

Version 1.0.0 rev-a

February 14, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

ThreatQ Supported

Support

Email:	support@threatq.com
Web:	support.threatq.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: support@threatq.com
Support Web: https://support.threatq.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.

Versioning

- Current integration version: `1.0.0`
- Compatible with ThreatQ versions >= `4.34.0`

Introduction

The Check Point SandBlast operation enriches ThreatQ indicators with context obtained from the Check Point SandBlast API.

The operation provides the following actions:

- **Upload** - uploads ThreatQ attachments to Check Point SandBlast for analysis.
- **Query** - enriches ThreatQ objects using the returned JSON response.

See the Actions chapter for further information on these actions.

The operation is compatible with ThreatQ attachments and indicators.

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 feed 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.

6. 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).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your Check Point SandBlast API Key.

5. Click **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable the operation.

Actions

ACTION	DESCRIPTION	OBJECT TYPES
Upload	Uploads ThreatQ objects	Attachments
Query	Enriches ThreatQ objects	MD5, SHA-1, SHA-256 Indicators and Attachments

Upload

Uploads ThreatQ attachments to Check Point SandBlast for analysis.

`POST https://te.checkpoint.com/tecloud/api/v1/file/upload`

Sample Response:

```
{
    "response": {
        "status": {
            "code": 1002,
            "label": "UPLOAD_SUCCESS",
            "message": "The file was uploaded successfully."
        },
        "sha1": "86bb5ed57999602fc4540ace6086a891c996e3f3",
        "md5": "010cfb902cae00576e39556914eb7af5",
        "sha256": "c79ac8a613c7a25793b2a0167d48a6a5e8e7c811ccdaf01d0a47efc7dff99dbd",
        "file_type": "",
        "file_name": "0.exe.zip",
        "features": [
            "te",
            "av",
            "extraction"
        ],
        "te": {
            "trust": 0,
            "images": [
                {
                    "report": {
                        "verdict": "unknown"
                    },
                    "status": "not_found",
                    "id": "e50e99f3-5963-4573-af9e-e3f4750b55e2",
                    "revision": 1
                },
                {
                    "report": {
                        "verdict": "unknown"
                    },
                    "status": "not_found",
                    "id": "5e5de275-a103-4f67-b55b-47532918fa59",
                    "revision": 1
                }
            ],
            "score": -2147483648,
            "status": {
                "code": 1002,
                "label": "UPLOAD_SUCCESS",
                "message": "The file was uploaded successfully."
            }
        },
        "extraction": {
            "method": "pdf",
            "tex_product": false,
            "status": {
                "code": 1002,
                "label": "UPLOAD_SUCCESS",
                "message": "The file was uploaded successfully."
            }
        },
        "av": {
            "status": {
                "code": 1002,
                "label": "UPLOAD_SUCCESS",
                "message": "The file was uploaded successfully."
            }
        }
    }
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.response.sha1	Indicator.Value	SHA-1	86bb5ed57999602fc4540ace6086a891c996e3f3	N/A
.response.sha256	Indicator.Value	SHA-256	c79ac8a613c7a25793b2a0167d48a6a5e8e7c811ccdaf01d0a47efc7dff99dbd	N/A
.response.md5	Indicator.Value	MD5	010cfb902cae00576e39556914eb7af5	N/A

Query

The Query action enriches ThreatQ objects using the returned JSON response.

`POST https://te.checkpoint.com/tecloud/api/v1/file/query`

Sample Response:

```
{
    "response": [
        {
            "status": {
                "code": 1001,
                "label": "FOUND",
                "message": "The request has been fully answered."
            },
            "md5": "6573cd9789c3fe1be39c3cc595e64942",
            "file_type": "",
            "file_name": "",
            "features": [
                "te",
                "av",
                "extraction"
            ],
            "te": {
                "trust": 10,
                "images": [
                    {
                        "report": {
                            "verdict": "benign"
                        },
                        "status": "found",
                        "id": "e50e99f3-5963-4573-af9e-e3f4750b55e2",
                        "revision": 1
                    },
                    {
                        "report": {
                            "verdict": "benign"
                        },
                        "status": "found",
                        "id": "5e5de275-a103-4f67-b55b-47532918fa59",
                        "revision": 1
                    }
                ],
                "score": -2147483648,
                "combined_verdict": "benign",
                "status": {
                    "code": 1001,
                    "label": "FOUND",
                    "message": "The request has been fully answered."
                }
            },
            "av": {
                "malware_info": {
                    "signature_name": "",
                    "malware_family": 0,
                    "malware_type": 0,
                    "severity": 0,
                    "confidence": 0
                },
                "status": {
                    "code": 1001,
                    "label": "FOUND",
                    "message": "The request has been fully answered."
                }
            },
            "extraction": {
                "method": "pdf",
                "extract_result": "CP_EXTRACT_RESULT_SUCCESS",
                "extracted_file_download_id": "eb727562-eb55-40ae-abf2-5c489bb871a7",
                "output_file_name": "applsci-09-04764-v2.cleaned.pdf",
                "time": "60.426",
                "extract_content": "PDF URI Actions",
                "extraction_data": {
                    "input_extension": "pdf",
                    "input_real_extension": "pdf",
                    "message": "OK",
                    "output_file_name": "applsci-09-04764-v2.cleaned.pdf",
                    "protection_name": "Potential malicious content extracted",
                    "protection_type": "Conversion to PDF",
                    "protocol_version": "1.0",
                    "risk": 3.0,
                    "scrub_activity": "Active content was found - PDF file was converted to PDF",
                    "scrub_method": "Convert to PDF",
                    "scrub_result": 0.0,
                    "scrub_time": "60.426",
                    "scrubbed_content": "PDF URI Actions"
                },
                "tex_product": false,
                "status": {
                    "code": 1001,
                    "label": "FOUND",
                    "message": "The request has been fully answered."
                }
            }
        }
    ]
}
```

ThreatQ provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.response[].file_type	Indicator.Attribute	File Type	N/A	N/A
.response[].file_name	Indicator.Attribute	File Name	N/A	N/A
.response[].te.trust	Indicator.Attribute	Trust	10	N/A
.response[].te.combined_verdict	Indicator.Attribute	Verdict	Benign	Title cased
.response[].av.malware_info.signature_name	Indicator.Attribute	Signature Name	N/A	N/A
.response[].av.malware_info.malware_family	Indicator.Attribute	Malware Family	0	N/A
.response[].av.malware_info.malware_type	Indicator.Attribute	Malware Type	0	N/A
.response[].av.malware_info.severity	Indicator.Attribute	Severity	0	N/A
.response[].av.malware_info.confidence	Indicator.Attribute	Confidence	0	N/A
.response[].extraction.extraction_data.risk	Indicator.Attribute	Risk	3.0	N/A

Change Log

- **Version 1.0.0 rev-a**
    - Updated vendor name in this user guide.
- **Version 1.0.0**
    - Initial Release