ThreatQuotient

Cybereason Operation User Guide

Version 1.0.0

October 25, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	ThreatQ Supported

Introduction

The Cybereason Operation for ThreatQ enables you to blocklist or allowlist an indicator. It also provides a way to query an indicator for any sightings.

The operation provides the following actions:

- **blocklist** - blocklists a given indicator.
- **allowlist** - allowlists a given indicator.
- **query** - queries Cybereason for any sightings of an indicator.

The operation is compatible with the following indicators types:

- FQDN
- IP Address
- MD5
- SHA-1

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 parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Cybereason Host and Port	Your Cybereason host and port (if required).
Username	Your Cybereason Username.
Password	Your Cybereason Password.

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 Cybereason operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
blocklist	Blocklists a given indicator.	Indicator	FQDN, IP Address, MD5, SHA-1
allowlist	Allowlists a given indicator.	Indicator	FQDN, IP Address, MD5, SHA-1
query	Queries Cybereason for any sightings of an indicator.	Indicator	IP Address, MD5, SHA-1

Blocklist

This action blocklists an Indicator in Cybereason. You can choose to prevent the execution (indicates whether to prevent the file's execution with Application Control) You can also choose to add or remove the reputation.

`POST {Host:Port}/rest/classification/update`

Sample Response:

```
{
  "comment": "Added by ThreatQ",
  "prevent": false,
  "keys": [
      "emag.ro"
  ],
  "maliciousType": "blacklist",
  "remove": true
}
```

Allowlist

This action allowlists an Indicator in Cybereason. You can choose to add or remove the reputation.

`POST {Host:Port}/rest/classification/update`

Sample Response:

```
{
  "keys": [
      "emag.ro"
  ],
  "comment": "Added by ThreatQ",
  "prevent": false,
  "remove": true,
  "maliciousType": "whitelist"
}
```

Query

Enrich the submitted Indicator

`POST {Host:Port}/rest/visualsearch/query/simple`

Sample Response:


```
{
    "failures": 0,
    "message": "",
    "data": {
        "evidenceMap": {
            "blackListClassificationEvidence": 10,
            "reportedByAntiMalwareEvidence": 10
        },
        "queryLimits": {
            "perGroupLimit": 100,
            "perFeatureLimit": 100,
            "totalResultLimit": 1000,
            "groupingFeature": {
                "elementInstanceType": "File",
                "featureName": "fileHash"
            },
            "sortInGroupFeature": null
        },
        "resultIdToElementDataMap": {
            "-371603117.-4881354770789208719": {
                "suspicions": {
                    "reportedByAntiMalwareSuspicion": 1615982754135,
                    "blackListedFileSuspicion": 1625041043432
                },
                "malopPriority": null,
                "guidString": "-371603117.-4881354770789208719",
                "suspicionCount": 2,
                "isMalicious": false,
                "elementValues": {
                    "localAddress": {},
                    "domainName": {
                      "totalSuspicious": 1,
                        "totalMalicious": 0,
                        "totalValues": 1,
                        "elementValues": [
                            {
                                "hasMalops": false,
                                "elementType": {},
                                "name": "cenas.org",
                                "guid": {},
                                "hasSuspicions": true
                            }
```

```
                ],
              "guessedTotal": 0
            },
            "self": {
                "totalSuspicious": 1,
                "totalMalicious": 0,
                "totalValues": 1,
                "elementValues": [
                    {
                        "hasMalops": false,
                        "elementType": "File",
                        "name": "undetectable_mimikatz_agent.py",
                        "guid": "-371603117.-4881354770789208719",
                        "hasSuspicions": true
                    }
                ],
                "guessedTotal": 0
            },
            "ownerMachine": {
                "totalSuspicious": 0,
                "totalMalicious": 0,
                "totalValues": 1,
                "elementValues": [
                    {
                        "hasMalops": false,
                        "elementType": "Machine",
                        "name": "ec2amaz-2utfkt5",
                        "guid": "-371603117.1198775089551518743",
                        "hasSuspicions": false
                    }
                ],
                "guessedTotal": 0
            }
        },
        "suspect": true,
        "labelsIds": null,
        "filterData": {
            "sortInGroupValue": "-371603117.-4881354770789208719",
            "groupByValue": "FileHashRuntime:0.4498703058583044935 "
        },
        "simpleValues": {
            "md5String": {
                "values": [
                    "e0180a291f1b6f05ebd16a96f05c00a5"
                ],
                "totalValues": 1
            },
            "correctedPath": {
                "values": [
                    "c:\\undetectable_mimikatz_agent.py"
```

```
            ],
            "totalValues": 1
        },
        "isSuspicious": {
            "values": [
                "true"
            ],
            "totalValues": 1
        },
        "classificationDetectionName": {
            "values": [
                "Heur.BZC.PZQ.Boxter.81.4A61989F"
            ],
            "totalValues": 1
        },
        "relatedToMalop": {
            "values": [
                "true"
            ],
            "totalValues": 1
        },
        "blackListClassificationEvidence": {
            "values": [
                "av_detected"
            ],
            "totalValues": 1
        },
        "maliciousClassificationType": {
            "values": [
                "av_detected"
            ],
            "totalValues": 1
        },
        "lastDetectEventDetectionStatus": {
            "values": [
                "DDS_USER_DETECT_ONLY"
            ],
            "totalValues": 1
        },
        "elementDisplayName": {
            "values": [
                "undetectable_mimikatz_agent.py"
            ],
            "totalValues": 1
        },
        "ownerMachine.isActiveProbeConnected": {
            "values": [
                "false"
            ],
            "totalValues": 1
```

```
                },
                "productType": {
                    "values": [
                        "NONE"
                    ],
                    "totalValues": 1
                },
                "sha1String": {
                    "values": [
                        "bd3961fe67753b29d4af68fa64c7fc5244352479"
                    ],
                    "totalValues": 1
                },
                "serverAddress": {
                    "values": [
                        "192.158.1.38"
                    ],
                    "totalValues": 1
                },
                "dualExtensionEvidence": {
                    "values": [
                        "WooowFile"
                    ],
                    "totalValues": 1
                },
                "originalFileName": {
                    "values": [
                        "TerraNostra"
                    ],
                    "totalValues": 1
                },
                "extensionType": {
                    "values": [
                        "EXECUTABLE_SCRIPT"
                    ],
                    "totalValues": 1
                },
                "canonizedPath": {
                    "values": [
                        "c:\\home\\dir"
                    ],
                    "totalValues": 1
                },
                "direction": {
                    "values": [
                        "Nort"
                    ],
                    "totalValues": 1
                },
                "remoteAddressCountryName": {
```

```
                    "values": [
                        "India"
                    ],
                    "totalValues": 1
                },
                "reportedByAntiMalwareEvidence": {
                    "values": [
                        "av_detected"
                    ],
                    "totalValues": 1
                },
                "remoteAddress.maliciousClassificationType": {},
                "signedInternalOrExternal": {},
                "size": {},
                "productName": {},
                "signatureVerifiedInternalOrExternal": {},
                "aggregatedReceivedBytesCount": {
                    "values": [
                        "128"
                    ],
                    "totalValues": 1
                },
                "aggregatedTransmittedBytesCount": {
                    "values": [
                        "3"
                    ],
                    "totalValues": 1
                },
                "ownerMachine.osVersionType": {
                    "values": [
                        "Windows_Server_2019"
                    ],
                    "totalValues": 1
                }
            },
            "malicious": false
        }
    },
    "totalPossibleResults": 10,
    "pathResultCounts": [
        {
            "count": 10,
            "featureDescriptor": {
                "elementInstanceType": "File",
                "featureName": null
            }
        }
    ],
    "guessedPossibleResults": 0,
    "suspicionsMap": {
```

```
            "reportedByAntiMalwareSuspicion": {
                "totalSuspicions": 10,
                "firstTimestamp": 1612570103071,
                "potentialEvidence": [
                    "reportedByAntiMalwareEvidence"
                ]
            },
            "blackListedFileSuspicion": {
                "totalSuspicions": 10,
                "firstTimestamp": 1625041043432,
                "potentialEvidence": [
                    "blackListClassificationEvidence"
                ]
            }
        },
        "queryTerminated": false,
        "guids": []
    },
    "status": "SUCCESS",
    "hidePartialSuccess": false,
    "expectedResults": 1
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
.data.simpleValues.correctedPath.values[]	Indicator.Value	File Path	c:\undetectable_mimikatz_agent.py
.data.simpleValues.sha1String.values[]	Indicator.Value	SHA-1	bd3961fe67753b29d4af68fa64c7fc5244352479
.data.simpleValues.serverAddress.values[]	Indicator.Value	IP Address	192.158. 1.38
.data.simpleValues.dualExtensionEvidence.values[]	Indicator.Value	Filename	WooowFile
.data.simpleValues.originalFileName.values[]	Indicator.Value	Filename	TerraNostra
.data.simpleValues.canonizedPath.values[]	Indicator.Value	File Path	c:\home\dir.py
.data.simpleValues.maliciousClassificationType.values[]	Indicator.Attribute	Malicious Classification	av_detected
.data.simpleValues.elementDisplayName.values[]	Indicator.Attribute	Display Name	undetectable_mimikatz_agent.py
.data.simpleValues.ownerMachine.osVersionType.values[]	Indicator.Attribute	Host Operating System	Windows_Server_2019
.data.simpleValues.relatedToMalop.values[]	Indicator.Attribute	Is Related to MalOp	true
.data.simpleValues.isSuspicious.values[]	Indicator.Attribute	Is Suspicious	true
.data.simpleValues.lastDetectEventDetectionStatus.values[]	Indicator.Attribute	Detected Event	DDS_USER_DETECT_ONLY
.data.simpleValues.ownerMachine.isActiveProbeConnected.values[]	Indicator.Attribute	Is Active Probe Conntected	false
.data.simpleValues.extensionType.values[]	Indicator.Attribute	Extension Type	EXECUTABLE_SCRIPT
.data.simpleValues.direction.values[]	Indicator.Attribute	Connection Direction	Nort
.data.simpleValues.remoteAddressCountryName.values[]	Indicator.Attribute	Remote Country	India
.data.simpleValues.aggregatedReceivedBytesCount.values[]	Indicator.Attribute	Received Bytes	128
.data.simpleValues.aggregatedTransmittedBytesCount.values[]	Indicator.Attribute	Transmitted Bytes	3
.data.simpleValues.remoteAddress.maliciousClassificationType.values[]	Indicator.Attribute	Malicious Classification	N/A
.data.simpleValues.signedInternalOrExternal.values[]	Indicator.Attribute	Signed Internal/ External	N/A
.data.simpleValues.size.values[]	Indicator.Attribute	File Size	N/A
.data.simpleValues.productName.values[]	Indicator.Attribute	Product Name	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
.data.simpleValues.signatureVerifiedInternalOrExternal.values[]	Indicator.Attribute	Signature Verified	N/A
.data.elementValues.domainName.elementValues[].name	Indicator.Value	FQDN	cenas.org
.data.elementValues.ownerMachine.elementValues[].name	Indicator.Attribute	Host Machine	ec2amaz-2utfkt5
.data.elementValues.ownerMachine.totalSuspicious	Indicator.Attribute	Total Suspicious	0
.data.elementValues.ownerMachine.totalMalicious	Indicator.Attribute	Total Malicious	0
.data.elementValues.ownerMachine.guessedTotal	Indicator.Attribute	Total Guessed	0
.data.elementValues.localAddress.elementValues[].name	Indicator.Attribute	Local Address	N/A

Change Log

- **Version 1.0.0**
  - Initial release