ThreatQuotient

Lastline Operation Guide

Version 2.1.0

March 08, 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: `2.1.0`
- Compatible with ThreatQ versions >= `4.57.2`

Introduction

The Lastline operation provides users with the ability to query tasks, query network reputations, submit files, URLs, domains, and retrieve task reports from Lastline.

The operation provides the following actions:

- **Submit** - submits a file or indicator to Lastline.
- **Get Report** - retrieves a report for a task from Lastline.
- **Get Reputation** - retrieves a reputation query for a FQDN or IP Address.
- **Query Tasks** - submits a sample to Lastline for analysis.

See the Actions chapter for more details on the actions listed above.

The operation is compatible with the following system objects:

- Files
- Indicators
  - FQDN
  - IP Address

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.

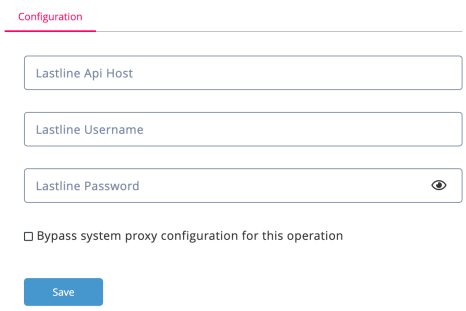
To configure the integration:

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 parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Lastline API Host	The API Host of your Lastline instance (including /papi).
Lastline Username	Your Lastline username for the API.
Lastline Password	Your Lastline password for the API.



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

Actions

The Lastline operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUB-TYPE
Submit	Submits a file or indicator to Lastline.	Indicators, Files	FQDN, Files
Get Report	Retrieve a report for a task from Lastline.	Indicators, Files	FQDN, Files
Get Reputation	Retrieves a reputation for an FQDN or IP Address.	Indicators	FQDN, IP Address
Query Tasks	Queries tasks from Lastline.	Indicators, Files	FQDN, IP Address, Files

Submit

The Submit action submits a sample to Lastline for analysis.

```
POST https://<Lastline Host>/analysis/submit_url/<Indicator>
```

```
POST https://<Lastline Host>/analysis/submit_file/<File>
```

Sample Response:

```
{
    "success": 1,
    "data": {
        "submission_timestamp": "2022-02-17 15:39:13",
        "task_uuid": "c6d6aa7a7d050010278daaeef0db406e",
        "expires": "2022-02-19 15:39:13"
    }
}
```

Get Report

The Get Report action will retrieve all the reports for the sample, with the only condition being that the sample (in ThreatQ) has an attribute with the name "Lastline Task ID" and the value will be the task ID. For each of these attributes, it will fetch a report correlating to the submission ID. If submission results are found, results will be shown and the full JSON report will be uploaded and related to the sample in ThreatQ

```
GET https://<Lastline Host>/analysis/get_result
```

Sample Response:


```
[
    {
        "success": 1,
        "data": {
            "progress": 100,
            "completed": 1
        }
    },
    {
        "success": 1,
        "data": {
            "analysis_subject": {
                "url": "http://sesverffvar.co.vu"
            },
            "expires": "2022-01-20 20:34:33",
            "last_submission_timestamp": "2022-01-18 20:34:34",
            "task_uuid": "14fe86401e9300100937fb7bf3811e81",
            "report": {
                "uuid": "f4fbdc680e75f1c4dTcI5OCx09w8llULqLhHydVO0nYIz5dEdMozlA",
                "format": {
                    "major_version": 1,
                    "build_version": 0,
                    "minor_version": 2,
                    "name": "ll-web"
                },
                "analysis": {
                    "new_functions": [],
                    "result": {
                        "analysis_ended": "2022-01-18 20:34:42+0000",
                        "detector": "1.0.0"
                    },
                    "urls_from_documents": [],
                    "evals": [],
                    "dropped_files": [],
                    "writes": [],
                    "plugins": [],
                    "applets": {},
                    "shellcodes": [],
                    "text_from_documents": [],
                    "hidden_elements": [],
                    "artifacts": [],
                    "network": {
```

```
            "requests": [
                {
                    "parent_url": "USER_URL",
                    "task_uuid": null,
                    "status": 403,
                    "url": "http://sesverffvar.co.vu/",
                    "content_sha1": "68e01dd3ef2fe8707210d79a9943d4f26bcbfec3",
                    "activities": [
                        {
                            "version": 4,
                            "threat_labels": [],
                            "score": 0,
                            "is_test": false,
                            "name": "llweb:errored-request",
                            "desc": "Info: The initial request failed"
                        },
                        {
                            "version": 1,
                            "threat_labels": [],
                            "score": 0,
                            "is_test": true,
                            "name": "llweb:screenshot-whitelist-match-phashwl-7-access-forbidden",
                            "desc": "Info: Page looks similar to Access Forbidden"
                        }
                    ],
                    "content_length": 555,
                    "content_md5": "6ce256529982abdafffa5d0e84890873",
                    "end": 464,
                    "filename": null,
                    "relation_type": 6,
                    "content_type": "text/html",
                    "start": 1,
                    "relation_type_str": "USER",
                    "error": null,
                    "ip": "92.242.40.175"
                }
            ]
        },
        "processes": [],
        "resources": [],
        "statics": [],
        "exploits": [],
        "strings": [],
        "subject": {}
    },
    "score": 0,
    "activities": [
        "Info: The initial request failed"
    ],
    "prefilter_score": 0,
    "prefilter_scanners": [],
    "analysis_engine_version": 16777216,
    "analysis_metadata": [
        {
            "retention_date": "2022-04-18 20:34:43",
            "name": "screenshot_capture.png",
            "metadata_type": "screenshot",
            "timestamp": 0
        },
        {
            "metadata_type": "traffic_capture",
```

```
                    "name": "traffic.pcap"
                },
                {
                    "retention_date": "2022-02-18 20:34:43",
                    "name": "trace.json",
                    "metadata_type": "llurl_framework_trace"
                }
            ]
        },
        "score": 30,
        "malicious_activity": [
            "Info: The initial request failed"
        ],
        "child_tasks": [
            {
                "score": 0,
                "tag": "network traffic analysis",
                "task_uuid": "41779647a0f3001002cb1e02a0d8865c",
                "parent_report_uuid": "f4fbdc680e75f1c4dTcI5OCx09w8llULqLhHydVO0nYIz5dEdMozlA"
            }
        ],
        "submission": "2022-01-18 20:34:34",
        "reports": [
            {
                "description": "Pcap analysis",
                "relevance": 0.0,
                "report_versions": [
                    "ll-pcap"
                ],
                "report_uuid": "a7c2f5d64f0687abcgMf8xWAR5tkKSIMDESQAVdzzF8mM56AotGkjA"
            },
            {
                "description": "Dynamic analysis in instrumented Chrome browser",
                "relevance": 0.0,
                "report_versions": [
                    "ll-web"
                ],
                "report_uuid": "f4fbdc680e75f1c4dTcI5OCx09w8llULqLhHydVO0nYIz5dEdMozlA"
            }
        ]
    }
}
]
```


ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
response.score	attribute	attribute.name.Resource Data	NA	30
response.malicious_activity	attribute	attribute.name.Resource Data	NA	Info: The initial request failed
response.submission_date	attribute	attribute.name.Resource Data	NA	2022-01-18 20:34:34

Get Reputation

The Get Reputation action will allow you get a reputation query for a FQDN or IP Address.

`GET https://<Lastline Host>//knowledgebase/intel_network_reputation`,

Sample Response:


```
{
    "data": {
        "reputations": [
            {
                "blacklist": [
                    {
                        "threat_class": "Malware Distribution",
                        "threat": "URLhaus blacklisted host",
                        "first_seen": "2019-05-23 18:55:00",
                        "comment": "The domain name of the contacted host is known to be involved in suspicious
redirection chains. Typically, threat actors inject a JavaScript script on a compromised website, starting the
redirection chain and leading its visitors to different threats, such as exploitation attempts, online scams, or
cookie stealers. Some of the intermediate steps may collect information on the victim and decide the next step
accordingly.",
                        "last_seen": "2019-06-03 05:32:34",
                        "threat_impact": 25,
                        "threat_severity": 80,
                        "compromised": false
                    }
                ],
                "entry": "treesguru.com"
            }
        ]
    },
    "success": 1
}
```


ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
response.threat_name	attribute	attribute.name.Resource Data	NA	URLhaus blacklisted host
response.last_seen	attribute	attribute.name.Resource Data	NA	2019-06-03 05:32:34
response.threat_class	attribute	attribute.name.Resource Data	NA	Malware Distribution
response.threat_severity	attribute	attribute.name.Resource Data	NA	80
response.comment	attribute	attribute.name.Resource Data	NA	No malicious activity found
response.threat_impact	attribute	attribute.name.Resource Data	NA	25
response.compromised	attribute	attribute.name.Resource Data	NA	false
response.first_seen	attribute	attribute.name.Resource Data	NA	2019-05-23 18:55:00

Query Tasks

The Query Tasks action submits a sample to Lastline for analysis.

```
POST https://<Lastline Host>//knowledgebase/<Indicator>
```

Sample Response:

```
{
    "success": 1,
    "data": {
        "list_domains": []
    }
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
response.threat_name	attribute	attribute.name.Resource Data	NA	Locky
response.threat_class	attribute	attribute.name.Resource Data	NA	command&control
response.threat_severity	attribute	attribute.name.Resource Data	NA	warning
response.compromised	attribute	attribute.name.Resource Data	NA	false
response.tag	attribute	attribute.name.Resource Data	NA	compromised:quant loader

Query Tasks Configuration Options

The Query Tasks action provides the following configuration options:

PARAMETER	DESCRIPTION
AV Filter	Allows you to filter your results by detecting the AV.
File Type Filter	Allows you to filter your results by detected file type.

Change Log

- **Version 2.1.0**
  - Added `Risk Estimate` to reports.
- **Version 2.0.0**
  - Added the ability to:
    - Query for Domains and SHA-1 hashes
    - Submit Files and URLs
    - Get Network Reputation for UPs and Domains.
- **Version 1.0.0**
  - Initial Release