ThreatQuotient

Elastic Operation User Guide

Version 1.0.0

January 02, 2024

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	>= 5.20.0
Compatible with Elastic Security Versions	>=8.x
Support Tier	ThreatQ Supported

Introduction

The Elastic Operation enriches submitted system objects with information found in Elastic Security.

Elastic Security unifies SIEM, endpoint security, and cloud security on an open platform, arming SecOps teams to protect, detect, and respond at scale. These analytical and protection capabilities, leveraged by the speed and extensibility of Elasticsearch, enable analysts to defend their organization from threats before damage and loss occur.

The operation provides the following action:

- **Query** - Executes an Elastic search query and gets back the hits that match the query.

The operation is compatible with the following system objects:

- Indicator
- Asset

Prerequisites

The following requirements are needed to use the operation:

- Elastic Security v8.x and newer.
- Credentials for the Elasticsearch API

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 operation .whl file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the .whl file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the 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
API Host	Enter your API host for your Elastic instance.
API Port	Enter your API port for your Elastic instance.
Username	Enter a username to authenticate with your Elastic instance.
Password	Enter the password associated with the entered username.
Verify SSL	Enable this to verify the host's SSL certificate.
IP Address Search Query	Enter a search query to use when searching for IP Addresses. Use `%s` as a placeholder for the IP Address.
FQDN Search Query	Enter a search query to use when searching for FQDNs. Use `%s` as a placeholder for the FQDN.
URL Search Query	Enter a search query to use when searching for URLs. Use `%s` as a placeholder for the URL.
Asset Search Query	Enter a search query to use when searching for assets. Use `%s` as a placeholder for the asset value.

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 operation provides the following action:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Query	Executes an Elastic search query and gets back the hits that match the query.	Indicator, Asset	(Indicator) IP Address, FQDN, URL

Query

The Query action executes an Elastic search query and gets back the hits that match the query. The query contains the value of the indicator/asset.

`GET {{API_HOST}}:{{API_PORT}}/_search?q=client.ip:10.114.0.243&sort=@timestamp:desc`

Sample Response:


```
{
  "took": 113,
  "timed_out": false,
  "_shards": {
    "total": 36,
    "successful": 36,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 1,
      "relation": "eq"
    },
    "max_score": null,
    "hits": [
      {
        "_index": ".ds-auditbeat-8.10.2-2023.11.30-000001",
        "_id": "3UIDfYwB7RuHjy-IBr4h",
        "_score": null,
        "_source": {
          "@timestamp": "2023-12-18T12:59:58.207Z",
          "agent": {
            "ephemeral_id": "4757edc4-7ec4-4954-93f6-10cda0905ad0",
            "id": "d9f71a78-927a-4583-8aca-cc727d3bc933",
            "name": "elk.tis.threatq.local",
            "type": "auditbeat",
            "version": "8.10.2"
          },
          "event": {
            "start": "2023-12-18T12:59:28.004Z",
            "end": "2023-12-18T12:59:28.004Z",
            "module": "system",
            "kind": "event",
            "action": "network_flow",
            "category": [
              "network"
            ],
            "dataset": "socket",
            "type": [
```

```
        "info",
        "connection"
      ],
      "duration": 20467
    },
    "flow": {
      "final": true,
      "complete": false
    },
    "client": {
      "port": 57200,
      "packets": 1,
      "bytes": 32,
      "ip": "10.114.0.243"
    },
    "related": {
      "ip": [
        "10.114.1.145",
        "10.114.0.243"
      ]
    },
    "service": {
      "type": "system"
    },
    "ecs": {
      "version": "8.0.0"
    },
    "host": {
      "id": "86b8f15024004e2cb5c8746ff57dcfc5",
      "containerized": false,
      "ip": [
        "10.114.1.145",
        "fe80::f816:3eff:fea6:dc6f"
      ],
      "mac": [
        "FA-16-3E-A6-DC-6F"
      ],
      "hostname": "elk.tis.threatq.local",
      "architecture": "x86_64",
      "os": {
        "platform": "ubuntu",
        "version": "22.04.3 LTS (Jammy Jellyfish)",
        "family": "debian",
        "name": "Ubuntu",
        "kernel": "5.15.0-84-generic",
        "codename": "jammy",
        "type": "linux"
      },
      "name": "elk.tis.threatq.local"
    },
```

```
      "network": {
        "direction": "unknown",
        "type": "ipv4",
        "transport": "tcp",
        "packets": 2,
        "bytes": 84,
        "community_id": "1:ybaELx9TIlP1rHQ/mbqlc/4uw+w="
      },
      "destination": {
        "ip": "10.114.1.145",
        "port": 9200,
        "packets": 1,
        "bytes": 52
      },
      "server": {
        "ip": "10.114.1.145",
        "port": 9200,
        "packets": 1,
        "bytes": 52
      },
      "system": {
        "audit": {
          "socket": {
            "kernel_sock_address": "0xffff9b19f21fe880"
          }
        }
      },
      "cloud": {
        "instance": {
          "id": "i-00000bb4",
          "name": "ladams-ubuntu"
        },
        "machine": {
          "type": "support.m4"
        },
        "availability_zone": "nova",
        "service": {
          "name": "Nova"
        },
        "provider": "openstack"
      },
      "source": {
        "ip": "10.114.0.243",
        "port": 57200,
        "packets": 1,
        "bytes": 32
      }
    },
    "sort": [
      1702904398207
```

```
          ]
        }
      ]
    }
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.@timestamp`	Indicator/ Asset.Attribute	Timestamp	N/A	`2023-12-18T12:59:58.207Z`	N/A
`.event.dataset`	Indicator/ Asset.Attribute	Dataset	N/A	`socket`	N/A
`.message`	Indicator/ Asset.Attribute	Message	N/A	N/A	N/A
`.message`	Indicator/ Asset.Attribute	Message	N/A	N/A	N/A
`.agent.name`	Indicator/ Asset.Attribute	Agent Name	N/A	elk.tis.threatq.local	N/A
`.agent.type`	Indicator/ Asset.Attribute	Agent Type	N/A	auditbeat	N/A
`.event.module`	Indicator/ Asset.Attribute	Event Module	N/A	system	N/A
`.event.action`	Indicator/ Asset.Attribute	Event Action	N/A	network_flow	N/A
`.event.category[]`	Indicator/ Asset.Attribute	Event Category	N/A	network	N/A
`.event.type[]`	Indicator/ Asset.Attribute	Event Type	N/A	info	N/A
`.host.id`	Indicator/ Asset.Attribute	Elastic Host ID	N/A	86b8f15024004e2cb5c8746ff57dcfc5	N/A
`.host.name`	Indicator/ Asset.Attribute	Elastic Host	N/A	elk.tis.threatq.local	N/A
`.host.mac[]`	Indicator/ Asset.Attribute	MAC Address	N/A	FA-16-3E-A6-DC-6F	N/A
`.host,architecture`	Indicator/ Asset.Attribute	Architecture	N/A	x86_64	N/A
`.host.os.name`	Indicator/ Asset.Attribute	Operating System	N/A	Ubuntu	N/A
`.network.direction`	Indicator/ Asset.Attribute	Network Direction	N/A	unknown	N/A
`.network.type`	Indicator/ Asset.Attribute	Network Type	N/A	ipv4	N/A
`.cloud.instance.name`	Indicator/ Asset.Attribute	Cloud Instance Name	N/A	ladams-ubuntu	N/A
`.cloud.machine.type`	Indicator/ Asset.Attribute	Cloud Machine Type	N/A	support.m4	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.cloud.service.name`	Indicator/ Asset.Attribute	Cloud Service Name	N/A	Nova	N/A
`.cloud.availability_zone`	Indicator/ Asset.Attribute	Cloud Availability Zone	N/A	nova	N/A
`.cloud.provider`	Indicator/ Asset.Attribute	Cloud provider	N/A	openstack	N/A

Run Parameters

The following run parameters are available after selecting the operation to run against an object:

PARAMETER	DESCRIPTION
Search Query Override	Enter a custom query to override the default query.
Search Query Start Date	Optional - Search only for entries added after a specific date. The format should be: **YYYY-MM-DD HH:MM:SS**.
Search Query End Date	Optional - Search only for entries added before a specific date. The format should be: **YYYY-MM-DD HH:MM:SS**.

Change Log

- **Version 1.0.0**
  - Initial release