ThreatQuotient

Elastic Action

Version 1.0.0

April 15, 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	>= 5.25.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Elastic Action integration enriches indicators with information found in Elastic Security.

Elastic Security unifies SIEM, endpoint security, and cloud security on an open platform. This allows 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 integration provides the following action:

- **Elastic Enrich Indicators** - executes an Elastic search query and retrieves the hits that match the query.

The action is compatible with the following object types:

- Assets
- Indicators

The action returns the following enriched system objects:

- Assets
- Indicators

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the the following object types:
  - Asset
  - Indicator

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

    > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

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:

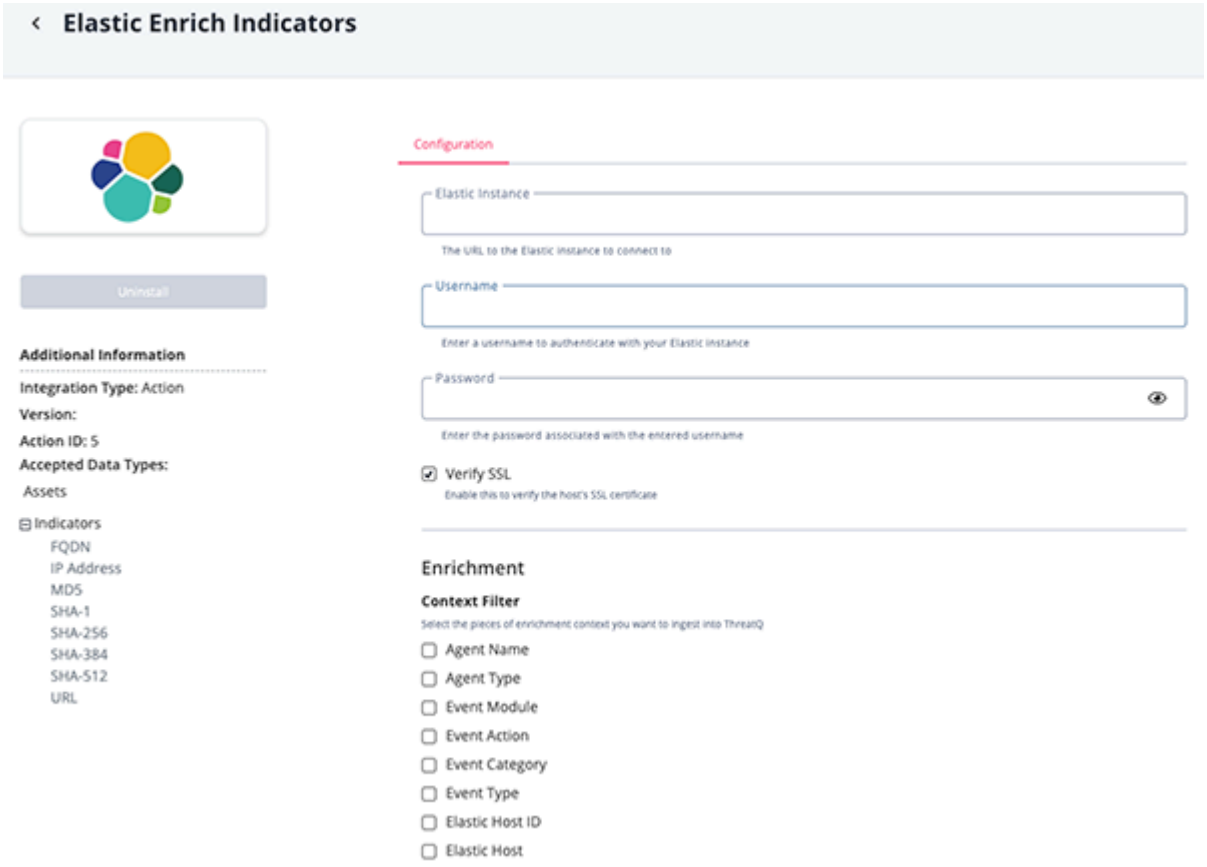
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Elastic Instance	The URL to the Elastic instance to connect to (http<s>://<hostname>:<port>).
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.
Context Filter	Select the pieces of enrichment context you want to ingest into ThreatQ. Options include: ◦ Agent Name ◦ Agent Type ◦ Event Module ◦ Event Action ◦ Event Category ◦ Event Type ◦ Elastic Host ID ◦ Architecture ◦ Operating System ◦ Network Direction ◦ Network Type ◦ Cloud Instance Name ◦ Cloud Machine Type ◦ Cloud Service Name

PARAMETER	DESCRIPTION
	◦ Elastic Host ◦ MAC Address ◦ Cloud Availability Zone ◦ Cloud Provide
Custom Attributes	Enter a comma-separated list of Elastic fields to ingested as attributes if they exist. (e.g process.name, host.os.platform)
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.
MD5 Search Query	Enter a search query to use when searching for MD5. Use %s as a placeholder for the MD5.
SHA-1 Search Query	Enter a search query to use when searching for SHA-1. Use %s as a placeholder for the SHA-1.
SHA-256 Search Query	Enter a search query to use when searching for SHA-256. Use %s as a placeholder for the SHA-256.
SHA-384 Search Query	Enter a search query to use when searching for SHA-384. Use %s as a placeholder for the SHA-384.
SHA-512 Search Query	Enter a search query to use when searching for SHA-512. Use %s as a placeholder for the SHA-512.
Search Query Start Date (YYYY-MM-DD HH:MM:SS)	Optional - Search only for entries added after a specific date. Use the format YYYY-MM-DD HH:MM:SS (e.g. 2023-07-17 00:00:00)

PARAMETER	DESCRIPTION
Search Query End Date (YYYY-MM-DD HH:MM:SS)	Optional - Search only for entries added before a specific date. Use the format YYYY-MM-DD HH:MM:SS (e.g. 2023-07-18 00:00:00)



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Elastic Enrich Indicators	Executes an Elastic search query and retrieves the hits that match the query.	Indicators, Assets	Indicator Types: IP Address, URL, FQDN, MD5, SHA-256, SHA-1, SHA-512, SHA-385

Elastic Enrich Indicators

The Elastic Enrich Indicators action executes an Elastic search query and retrieves the hits that match the query. The query contains the value of the indicator/asset.

```
GET "{{ELASTIC_INSTANCE}}/_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, .event.dataset, .message`	Indicator/ Asset.Description	N/A	N/A	N/A	Fields displayed in a table.
`.agent.name`	Indicator/ Asset.Attribute	Agent Name	N/A	elk.tis.threatq.local	If checked in `Context Filter`
`.agent.type`	Indicator/ Asset.Attribute	Agent Type	N/A	auditbeat	If checked in `Context Filter`
`.event.module`	Indicator/ Asset.Attribute	Event Module	N/A	system	If checked in `Context Filter`
`.event.action`	Indicator/ Asset.Attribute	Event Action	N/A	network_flow	If checked in `Context Filter`
`.event.category[]`	Indicator/ Asset.Attribute	Event Category	N/A	network	If checked in `Context Filter`
`.event.type[]`	Indicator/ Asset.Attribute	Event Type	N/A	info	If checked in `Context Filter`
`.host.id`	Indicator/ Asset.Attribute	Elastic Host ID	N/A	86b8f15024004e2cb5c8746ff57dcfc5	If checked in `Context Filter`
`.host.name`	Indicator/ Asset.Attribute	Elastic Host	N/A	elk.tis.threatq.local	If checked in `Context Filter`
`.host.mac[]`	Indicator/ Asset.Attribute	MAC Address	N/A	FA-16-3E-A6-DC-6F	If checked in `Context Filter`
`.host,architecture`	Indicator/ Asset.Attribute	Architecture	N/A	x86_64	If checked in `Context Filter`
`.host.os.name`	Indicator/ Asset.Attribute	Operating System	N/A	Ubuntu	If checked in `Context Filter`
`.network.direction`	Indicator/ Asset.Attribute	Network Direction	N/A	unknown	If checked in `Context Filter`
`.network.type`	Indicator/ Asset.Attribute	Network Type	N/A	ipv4	If checked in `Context Filter`
`.cloud.instance.name`	Indicator/ Asset.Attribute	Cloud Instance Name	N/A	ladams-ubuntu	If checked in `Context Filter`
`.cloud.machine.type`	Indicator/ Asset.Attribute	Cloud Machine Type	N/A	support.m4	If checked in `Context Filter`
`.cloud.service.name`	Indicator/ Asset.Attribute	Cloud Service Name	N/A	Nova	If checked in `Context Filter`
`.cloud.availability_zone`	Indicator/ Asset.Attribute	Cloud Availability Zone	N/A	nova	If checked in `Context Filter`
`.cloud.provider`	Indicator/ Asset.Attribute	Cloud provider	N/A	openstack	If checked in `Context Filter`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
Values specified in `Custom Attributes`	Indicator/ Asset.Attribute	Values specified in `Custom Attributes`	N/A	N/A	N/A

Change Log

- **Version 1.0.0**
  - Initial release