ThreatQuotient

Darktrace CDF

Version 1.0.0

August 20, 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
Support Tier	ThreatQ Supported

Introduction

The Darktrace CDF ingests alerts from Darktrace as AI Analyst and Model Breach Events with devices as related indicators and assets.

The integration provides the following feeds:

- **Darktrace AIAnalyst Incident Events -** ingests Darktrace alerts related to a group of anomalies or network activity investigated by Cyber AI Analyst.
- **Darktrace Model Breaches** - ingests Darktrace alerts related to model breaches.

The integration ingests the following object types:

- Assets
- Events
- Indicators

Prerequisites

The following is required to run the integration:

- A Darktrace Instance
- A Public and Private Darktrace token.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml 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
6. Select the individual feeds to install, when prompted and click **Install**.

    > ThreatQ will inform you if the feed 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 feed and will require user confirmation before proceeding.

The feed(s) will be added to the integrations page. You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

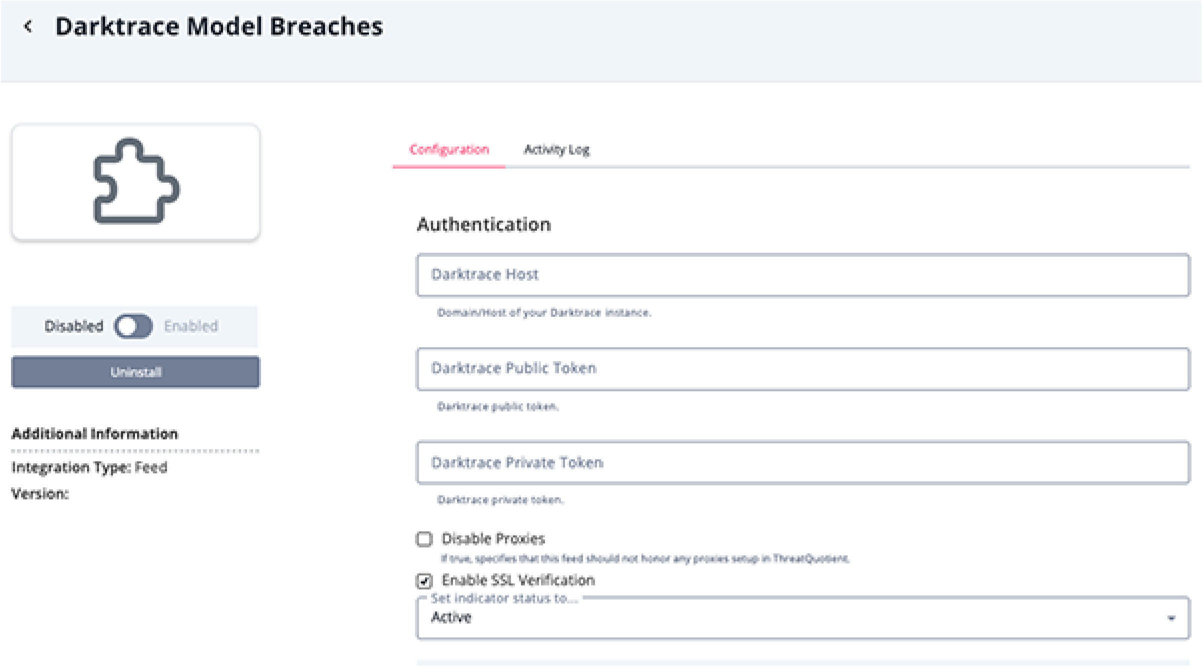
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* 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 entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Darktrace Host	The Domain/Host of your Darktrace instance.
Darktrace Public Token	Your Darktrace public token.
Darktrace Private Token	Your Darktrace private token.
Enable SSL Verification	When checked, validates the host-provided SSL certificate. This option is enabled by default.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.



Additional Information

Integration Type: Feed

Version:

Authentication

Darktrace Host

Domain/Host of your Darktrace instance.

Darktrace Public Token

Darktrace public token.

Darktrace Private Token

Darktrace private token.

☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

☑ Enable SSL Verification

Set indicator status to...: Active

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.

ThreatQ Mapping

Darktrace AIAnalyst Incident Events

The Darktrace AIAnalyst Incident Events feed ingests Darktrace alerts related to a group of anomalies or network activity investigated by Cyber AI Analyst. The threat data is ingested into ThreatQ as AI Analyst Events with devices as related indicators and assets.

`GET https://{host}/aianalyst/incidentevents`

Sample Response:

```
[
    {
        "summariser": "HttpAgentSummary",
        "acknowledged": false,
        "pinned": true,
        "createdAt": 1646162137536,
        "attackPhases": [
            2
        ],
        "mitreTactics": [
            "command-and-control"
        ],
        "title": "Possible HTTP Command and Control",
        "id": "58b1c336-01b2-4418-86f8-3a53b0856aaa",
        "incidentEventUrl": "https://usw1-54655-01.cloud.darktrace.com/
#aiaincidentevent/58b1c336-01b2-4418-86f8-3a53b0856aaa",
        "children": [
            "58b1c336-01b2-4418-86f8-3a53b0856aaa"
        ],
        "category": null,
        "currentGroup": null,
        "groupCategory": null,
        "groupScore": null,
        "groupPreviousGroups": null,
        "activityId": "da39a3ee",
        "groupingIds": [
            "9e6a55b6"
        ],
        "groupByActivity": false,
        "userTriggered": false,
        "externalTriggered": false,
        "aiaScore": 41.915465465599745,
        "summary": "The device wef.windomain.local was observed making an HTTP
connection to the rare external endpoint 35.178.78.199, without a user agent
header.\n\nThe lack of this header suggests that this activity was initiated by
a standalone software process as opposed to a web browser.\n\nIf such behaviour
is unexpected, further investigation may be required to determine if this
activity represents malicious command and control as opposed to legitimate
telemetry of some form.",
        "periods": [
            {
                "start": 1646155303577,
                "end": 1646155303577
            }
        ],
        "sender": null,
        "breachDevices": [
            {
                "identifier": "wef.windomain.local",
                "hostname": "wef.windomain.local",
                "ip": "192.168.1.3",
                "mac": "06:7b:81:5d:4b:5c",
                "subnet": null,
                "did": 18,
                "sid": 3
            }
        ],
        "relatedBreaches": [
            {
                "modelName": "Device / Suspicious Domain",
                "pbid": 1777,
                "threatScore": 33.0,
                "timestamp": 1646158351000
            }
        ],
        "details": [
            [
                {
                    "header": "Suspicious Endpoints Contacted by Application",
                    "contents": [
                        {
                            "key": "Time",
                            "type": "timestampRange",
                            "values": [
                                {
                                    "start": 1646155303577,
                                    "end": 1646155303577
                                }
                            ]
                        }
                    ]
                }
            ]
        ]
    }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.title` (Event UUID:`.id`)	Event.Title	AI Analyst	`.createdAt`	`Possible HTTP Command and Control (Event UUID:58b1c336-01b2-4418-86f8-3a53b0856aaa)`	N/A
`.summary`	Event.Description	N/A	`.createdAt`	`The device wef.windomain.local was observed making an HTTP connection ...`	N/A
`.acknowledged`, `.userTriggered`, `.externalTriggered`	Event.Tags	N/A	`.createdAt`	N/A	`.acknowledged`, `.userTriggered`, `.externalTriggered` key is set as tag if the value is True
`.breachDevices.mac`	Related Indicator	Mac Address	`.createdAt`	`06:7b:81:5d:4b:5c`	N/A
`.breachDevices.ip`	Related Indicator/ Related Asset	IP Address	`.createdAt`	`192.168.1.3`	If `ip` is private Asset is ingested, if not Indicator
`.breachDevices.hostname`	Related Indicator/ Related Asset	FQDN	`.createdAt`	`wef.windomain.local`	If `hostname` is not a valid domain Asset will be ingested, if not Indicator
`.incidentEventUrl`	Event.Attribute	Incident Event URL	`.createdAt`	`https://usw1-54655-01.cloud.darktrace.com/#aiaincidentevent/58b1c336-01b2-4418-86f8-3a53b0856aaa`	N/A
`.attackPhases`	Event.Attribute	Attack Phases	`.createdAt`	2	N/A
`.category`	Event.Attribute	Category	`.createdAt`	N/A	N/A
`.aiaScore`	Event.Attribute	AI Analyst Score	`.createdAt`	`41.915465465599745`	N/A

Darktrace Model Breaches

The Darktrace Model Breaches feed ingests Darktrace alerts related to model breaches. The threat data is ingested into ThreatQ as Model Breach Events with devices as related indicators and assets.

`GET https://{host}/modelbreaches`

Sample Response:

```
[
    {
        "breachUrl": "https://usw1-54655-01.cloud.darktrace.com/#modelbreach/
53001",
        "commentCount": 0,
        "pbid": 53001,
        "time": 1723070608000,
        "creationTime": 1723070607000,
        "model": {
            "then": {
                "name": "System::System",
                "pid": 530,
                "phid": 4861,
                "uuid": "1c3f429b-ccb9-46a2-b864-868653bc780a",
                "logic": {
                    "data": [
                        9686
                    ],
                    "type": "componentList",
                    "version": 1
                },
                "throttle": 10,
                "sharedEndpoints": false,
                "actions": {
                    "alert": true,
                    "antigena": {},
                    "breach": true,
                    "model": true,
                    "setPriority": false,
                    "setTag": false,
                    "setType": false
                },
                "tags": [],
                "interval": 0,
                "delay": 0,
                "sequenced": true,
                "active": true,
                "modified": "2021-11-24 18:04:19",
                "activeTimes": {
                    "devices": {},
                    "tags": {},
                    "type": "exclusions",
                    "version": 2
                },
                "autoUpdatable": true,
                "autoUpdate": true,
                "autoSuppress": true,
                "description": "An issue with the system has been detected.
This system alert is generated for system information that may merit further
investigation. This may be due to things like probes failing to connect.
\n\nAction: Review the system message. Use the status page to see additional
system information that may help with diagnostics.",
                "behaviour": "decreasing",
                "defeats": [],
                "created": {
                    "by": "System"
                },
                "edited": {
                    "by": "System"
                },
                "version": 16,
                "priority": 3,
                "category": "Informational",
                "compliance": false
            },
            "now": {
                "name": "System::System",
                "pid": 530,
                "phid": 4861,
                "uuid": "1c3f429b-ccb9-46a2-b864-868653bc780a",
                "logic": {
                    "data": [
                        9686
                    ],
                    "type": "componentList",
                    "version": 1
                },
                "throttle": 10,
                "sharedEndpoints": false,
                "actions": {
                    "alert": true,
                    "antigena": {},
                    "breach": true,
                    "model": true,
                    "setPriority": false,
                    "setTag": false,
                    "setType": false
                },
                "tags": [],
                "interval": 0,
                "delay": 0,
                "sequenced": true,
                "active": true,
                "modified": "2021-11-24 18:04:19",
                "activeTimes": {
                    "devices": {},
                    "tags": {},
                    "type": "exclusions",
                    "version": 2
                },
                "autoUpdatable": true,
                "autoUpdate": true,
                "autoSuppress": true,
                "description": "An issue with the system has been detected.
This system alert is generated for system information that may merit further
investigation. This may be due to things like probes failing to connect.
\n\nAction: Review the system message. Use the status page to see additional
system information that may help with diagnostics.",
                "behaviour": "decreasing",
                "defeats": [],
                "created": {
                    "by": "System"
                },
                "edited": {
                    "by": "System"
                },
                "message": "Updated model filters and logic",
                "version": 16,
                "priority": 3,
                "category": "Informational",
                "compliance": false
            }
        },
        "triggeredComponents": [
            {
                "time": 1723070607000,
                "cbid": 54607,
                "cid": 9686,
                "chid": 15251,
                "size": 1,
                "threshold": 0,
                "interval": 3600,
                "logic": {
                    "data": {
                        "left": {
                            "left": "A",
                            "operator": "AND",
                            "right": "B"
                        },
                        "operator": "OR",
                        "right": {
                            "left": {
                                "left": "A",
                                "operator": "AND",
                                "right": "C"
                            },
                            "operator": "OR",
                            "right": {
                                "left": {
                                    "left": "A",
                                    "operator": "AND",
                                    "right": "D"
                                },
                                "operator": "OR",
                                "right": {
                                    "left": {
                                        "left": "A",
                                        "operator": "AND",
                                        "right": "E"
                                    },
                                    "operator": "OR",
                                    "right": {
                                        "left": "A",
                                        "operator": "AND",
                                        "right": "F"
                                    }
                                }
                            }
                        }
                    },
                    "version": "v0.1"
                },
                "metric": {
                    "mlid": 206,
                    "name": "dtsystem",
                    "label": "System"
                },
                "triggeredFilters": [
                    {
                        "cfid": 111299,
                        "id": "A",
                        "filterType": "Event details",
                        "arguments": {
                            "value": "analyze credential ignore list"
                        },
                        "comparatorType": "does not contain",
                        "trigger": {
                            "value": "Probe erebus-pull-mode-vsensor
(54.155.33.146) last contact was 67 hours ago"
                        }
                    }
                ]
            }
        ],
        "percentscore": 73,
        "score": 0.728,
        "device": {
            "did": -1
        },
        "did": -1
    }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.model.now.name` on `.device.ip` (Policy Breach ID: `.pbid`)	Event.Title	Model Breach	`.creationTime`	`System::System on -1 (Policy Breach ID: 53001)`	N/A
`.description`	Event.Description	N/A	`.creationTime`	`An issue with the system has been detected. ...`	N/A
`.sharedEndpoints`, `.sequenced`,`.active`, `.compliance`, `.autoUpdatable`, `.autoUpdate`, `.autoSuppress`	Event.Tags	N/A	`.creationTime`	N/A	Key is set as tag if the value for that key is True
`.model.now.tags`	Event.Tags	N/A	`.creationTime`	N/A	N/A
`.device.mac`	Related Indicator	Mac Address	`.creationTime`	N/A	N/A
`.device.ip`	Related Indicator/ Related Asset	IP Address	`.creationTime`	N/A	If `ip` is private Asset is ingested, if not Indicator
`.device.ips[].ip`	Related Indicator/ Related Asset	IP Address	`.creationTime`	N/A	If `ip` is private Asset is ingested, if not Indicator
N/A	Related Indicator Tag/ Related Asset Tag	N/A	`.creationTime`	`Current`	If `ip` is from the path `.device.ip`
N/A	Related Indicator Tag/ Related Asset Tag	N/A	`.creationTime`	`Historic`	If `ip` is from the path `.device.ips[].ip`
`.device.hostname`	Related Indicator/ Related Asset	FQDN	`.creationTime`	N/A	If `hostname` is not a valid domain Asset will be ingested, if not Indicator
`.pbid`	Event.Attribute	Policy Breach ID	`.creationTime`	`53001`	N/A
`.score`	Event.Attribute	Score	`.creationTime`	`0.728`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.breachUrl`	Event.Attribute	Breach URL	`.creationTime`	`https://usw1-54655-01.cloud.darktrace.com/#modelbreach/53001`	N/A
`.model.now.pid`	Event.Attribute	Policy ID	`.creationTime`	`530`	N/A
`.model.now.throttle`	Event.Attribute	Throttle	`.creationTime`	`10`	N/A
`.model.now.interval`	Event.Attribute	Interval	`.creationTime`	`3600`	N/A
`.model.now.priority`	Event.Attribute	Priority	`.creationTime`	`3`	Updated at ingestion
`.model.now.category`	Event.Attribute	Category d	`.creationTime`	`Informational`	Updated at ingestion
`.model.now.behaviour`	Event.Attribute	Behaviour	`.creationTime`	`decreasing`	Updated at ingestion
`.model.now.version`	Event.Attribute	Version	`.creationTime`	`16`	Updated at ingestion

Average Feed Run

Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

Darktrace AI Analyst Incident Events

METRIC	RESULT
Run Time	1 minute
Events	5
Event Attributes	18
Indicators	2
Assets	3

Darktrace Model Breaches

METRIC	RESULT
Run Time	2 minutes
Events	1,183
Event Attributes	9,464
Indicators	4
Assets	39

Change Log

- **Version 1.0.0**
  - Initial release