

ThreatQuotient



Dataminr Pulse CDF

Version 1.0.2

November 19, 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 3

Support 4

Integration Details..... 5

Introduction 6

Prerequisites 7

Installation..... 8

Configuration 9

ThreatQ Mapping..... 12

 Dataminr Pulse Alerts..... 12

 Dataminr Supplemental Feeds 13

 Channel Mapping Table..... 20

Average Feed Run..... 21

Known Issues / Limitations 22

Change Log 23

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.

Copyright © 2024 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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	1.0.2
Compatible with ThreatQ Versions	>= 5.22.0
Support Tier	ThreatQ Supported

Introduction

The Dataminr Pulse CDF enables the automatic ingestion of alerts from Dataminr portal into ThreatQ. Dataminr Pulse contains alerts on activity across multiple publicly available sources. The alerts are ingested as ThreatQ events.

The integration provides the following feed:

- **Dataminr Pulse Alerts** - ingests Dataminr Pulse Alerts into ThreatQ as events.

The integration ingests the following system objects:

- Events
- Indicators
- Vulnerabilities

Prerequisites

The following is required to use the integration:

- A Dataminr Pulse Client ID and Secret.
- **At least one valid Alert List must be configured on the account before using this integration.**

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 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.

6. The feed 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.
 1. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Client ID	Your Client ID used to authenticate with the Dataminr Pulse API.
Client Secret	Your Client Secret used to authenticate with the Dataminr Pulse API.
Dataminr List	If specified, the feed ingests only alerts belonging to the specified list from Dataminr application.
Dataminr Query	If specified, the feed ingests only alerts that match the query provided. Example: (hurricane OR fire) AND "office building".
List Type	If specified, the feed ingests only alerts belonging to the lists having the selected type. Options include: ▪ Topics ▪ Company ▪ Custom ▪ Cyber
Alert Type	Filter data ingested into the platform by Alert Type. Options include: ▪ All

PARAMETER	DESCRIPTION
	▪ Flash ▪ Urgent ▪ Alert
Ingest related alerts	When enabled, the feed ingests all the related alerts even if they do not satisfy the previously configured filters.
Metadata Objects	When enabled, the feed will ingest the selected related objects. Options include: ▪ Addresses ▪ URLs ▪ Vulnerabilities ▪ Adversary ▪ Malware ▪ Hashes  Network Scans, Phishing, Malware and Domain Impersonation Categories - only Addresses and URLs will be ingested if selected.
ASN Metadata	When enabled, the feed will ingest the selected metadata as Address and URL attributes. Options include: ▪ ASN ▪ ASN Organization
Ingest CVEs As	Select the ThreatQ object type to ingest the CVEs into ThreatQ as. Options include: ▪ Vulnerabilities ▪ Indicators
Vulnerabilities Context	When enabled, the feed will ingest the selected metadata as Vulnerability attributes. Options include: ▪ CVSS Score ▪ Products affected ▪ Vendors ▪ Exploit POC links
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

PARAMETER

DESCRIPTION

Enable SSL
Verification

Enable this for the feed to validate the host-provided SSL certificate.

< Datamir Pulse Alerts



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

Authentication

Client ID

Enter your Client ID to authenticate with the Datamir Pulse API

Client Secret

Enter your Client Secret to authenticate with the Datamir Pulse API

Data Filtering

Only one of the filters Datamir List and Datamir Query can be used. If both are present the Datamir Query filter is ignored. If no filter is selected all the alerts will be ingested. The List Type filter is applied only if Datamir Query is not present.

Datamir List

If present the feed ingests only alerts belonging to the specified list from Datamir application

Datamir Query

If present the feed ingests only alerts that match this query e.g. (hurricane OR fire) AND "office building"

List Type

If present the feed ingests only alerts belonging to the lists having the selected type.

- ☒ Topic
- ☒ Company
- ☒ Custom
- ☒ Cyber

4. Review any additional settings, make any changes if needed, and click on **Save**.
5. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Dataminr Pulse Alerts

The Dataminr Pulse Alerts feed ingests Dataminr Pulse Alerts into the ThreatQ platform as events.

GET https://gateway.dataminr.com/account/2/get_lists



The feed retrieves all the IDs (`.watchlists.{{CATEGORY}}.id`) for the lists configured in Dataminr Portal. The IDs are sent to the supplemental feeds Dataminr Get Next Alerts, Dataminr Get Previous Alerts to get the needed alerts.

Sample Response:

```
{
  "watchlists": {
    "TOPIC": [
      {
        "id": 4153708,
        "properties": {
          "watchlistColor": "darkblue"
        },
        "name": "Government",
        "description": "",
        "type": "TOPIC"
      }
    ],
    "COMPANY": [
      {
        "name": "Top Companies",
        "companies": [
          {
            "id": "e7a463003d6229c750586f8a263ec4e0",
            "name": "YUM! Brands, Inc."
          }
        ],
        "description": "",
        "type": "COMPANY",
        "id": 4153722,
        "properties": {
          "watchlistColor": "darkblue"
        }
      }
    ],
    "CUSTOM": [
      {
        "id": 4177550,
```

```

    "properties": {
      "watchlistColor": "darkblue"
    },
    "name": "Exploits",
    "description": "",
    "type": "CUSTOM"
  }
]
}
}

```

Dataminr Supplemental Feeds

The integration utilizes three supplemental feeds: Dataminr Get Next Alerts, Dataminr Get Previous Alerts, Dataminr Get Related Alerts.

The Dataminr API has a cursor based implementation. Dataminr Get Next Alerts retrieves the alerts that Dataminr considers as new alerts for the user. Dataminr Get Previous Alerts retrieves the alerts that are considered old/read. If user config Ingest related alerts is enabled, the feed Dataminr Get Related Alerts ingested the related alerts for each entry.

Dataminr Get Next Alerts, Dataminr Get Previous Alerts - GET <https://gateway.dataminr.com/api/3/alerts>

Dataminr Get Related Alerts - GET https://gateway.dataminr.com/alerts/2/get_related?id={{ALERT_ID}}

Sample Response:

```

{
  "data": {
    "alerts": [
      {
        "alertId": "1407810963-1701783539058-3",
        "alertType": {
          "id": "urgent",
          "name": "Urgent",
          "color": "FFBB05"
        },
        "watchlistsMatchedByType": [
          {
            "id": "4177550",
            "type": "CUSTOM",
            "name": "Exploits",
            "externalTopicIds": [],
            "userProperties": {
              "omnिलist": "true"
            }
          }
        ],
        "availableRelatedAlerts": 0,

```

```

"eventTime": 1701783733823,
"eventVolume": 0,
"metadata": {
  "cyber": {
    "vulnerabilities": [
      {
        "id": "CVE-2023-49105",
        "cvss": 9.8,
        "products": [
          {
            "productName": "owncloud",
            "productVersion": " ",
            "productVendor": "owncloud"
          }
        ],
        "exploitPocLinks": []
      }
    ],
    "URLs": [
      "ambionics.io"
    ],
    "addresses": [
      {
        "ip": "148.72.164.186",
        "port": "80"
      }
    ],
    "asns": [],
    "orgs": [],
    "hashes": [],
    "products": [],
    "malwares": [],
    "threats": [],
    "asOrgs": [
      {
        "asn": "AS13335",
        "asOrg": "Cloudflare"
      }
    ],
    "hashValues": []
  }
},
"caption": "CVE-2023-49105 referenced on X (formerly Twitter)",
"subCaption": {
  "bullets": {
    "content": "Philip Morris mentioned in headline\nSampoerna and Philip Morris International mentioned in article",
    "source": "According to Capital Romanian"
  }
},

```

```

"companies": [
  {
    "name": "Apple Inc.",
    "topicType": "company",
    "id": "2adac6e9b077021a8c4e5de1a3aa057b",
    "idStr": "2adac6e9b077021a8c4e5de1a3aa057b",
    "ticker": "\"apple+\"",
    "retired": false
  }
],
"categories": [
  {
    "name": "Cybersecurity",
    "topicType": "category",
    "id": "124022",
    "idStr": "124022",
    "path": "/TOPIC/EXT/CS/124022",
    "retired": false
  }
],
"eventLocation": {
  "coordinates": [
    37.3318598,
    -122.0302485
  ],
  "name": "Apple Inc. HQ, Cupertino, CA, USA",
  "places": [
    "8e51ba12f754ae46a6ec7816d6e7a617",
    "f66b10a1b6d5d260b3ddb7e7518aa5ac",
    "2f7245ea29c7d5a90bfd48512f971ef0",
    "0a269a52d33a19cd680c4d33aef9a4af",
    "4e9ea3cb3310c59405b5cd3844856d12"
  ],
  "probability": 0.0,
  "radius": 0.1
},
"sectors": [],
"headerColor": "FFFFAD",
"publisherCategory": {
  "id": "chatter",
  "name": "Chatter",
  "color": "A24512",
  "shortName": "CTR"
},
"expandAlertURL": "https://app.dataminr.com/#alertDetail/5/1407810963-1701783539058-3",
"expandUserURL": "https://app.dataminr.com/#userDetail/@ambionics",
"relatedTerms": [
  {
    "text": "exploit",

```

```

        "url": "https://app.dataminr.com/app/core/corporate/search-
popup.html#search/
%7B%22history%22%3A%5B%7B%22displayTitle%22%3A%22exploit%22%2C%22elements%22%3A
%5B%7B%22topicName%22%3A%22exploit%22%2C%22type%22%3A%22string%22%2C%22topicId%
22%3A-1%2C%22equitySymbol%22%3A%22%22%7D%5D%2C%22target%22%3A%22searchinput%22%
2C%22type%22%3A%22complex%22%2C%22isEquity%22%3Afalse%2C%22topicId%22%3A-1%2C%2
2text%22%3A%22%22%7D%5D%7D/location/
%7B%22center%22%3A%7B%22lat%22%3A14.43468021529728%2C%22lng%22%3A-65.91796875%2
C%22zoom%22%3A2%7D%2C%22zoom%22%3A2%2C%22extent%22%3A%7B%22north%22%3A73.428423
64106818%2C%22east%22%3A48.1640625%2C%22south%22%3A-62.91523303947613%2C%22west
%22%3A-179.6484375%7D%7D"
    },
    {
      "text": "referenced",
      "url": "https://app.dataminr.com/app/core/corporate/search-
popup.html#search/
%7B%22history%22%3A%5B%7B%22displayTitle%22%3A%22referenced%22%2C%22elements%22
%3A%5B%7B%22topicName%22%3A%22referenced%22%2C%22type%22%3A%22string%22%2C%22to
picId%22%3A-1%2C%22equitySymbol%22%3A%22%22%7D%5D%2C%22target%22%3A%22searchinp
ut%22%2C%22type%22%3A%22complex%22%2C%22isEquity%22%3Afalse%2C%22topicId%22%3A-
1%2C%22text%22%3A%22%22%7D%5D%7D/location/
%7B%22center%22%3A%7B%22lat%22%3A14.43468021529728%2C%22lng%22%3A-65.91796875%2
C%22zoom%22%3A2%7D%2C%22zoom%22%3A2%2C%22extent%22%3A%7B%22north%22%3A73.428423
64106818%2C%22east%22%3A48.1640625%2C%22south%22%3A-62.91523303947613%2C%22west
%22%3A-179.6484375%7D%7D"
    }
  ],
  "relatedTermsQueryURL": "https://app.dataminr.com/#search-popup/search/
%7B%22history%22%3A%5B%7B%22displayTitle%22%3A%22blogpost,cve,cyber
exploits,exploit,referenced%22%2C%22elements%22%3A%5B%7B%22topicName%22%3A%22bl
ogpost,cve,cyber
exploits,exploit,referenced%22%2C%22type%22%3A%22string%22%2C%22topicId%22%3A-1
%2C%22equitySymbol%22%3A%22%22%7D%5D%2C%22target%22%3A%22searchinput%22%2C%22ty
pe%22%3A%22complex%22%2C%22isEquity%22%3Afalse%2C%22topicId%22%3A-1%2C%22text%2
2%3A%22%22%7D%5D%7D/location/
%7B%22center%22%3A%7B%22lat%22%3A14.43468021529728%2C%22lng%22%3A-65.91796875%2
C%22zoom%22%3A2%7D%2C%22zoom%22%3A2%2C%22extent%22%3A%7B%22north%22%3A73.428423
64106818%2C%22east%22%3A48.1640625%2C%22south%22%3A-62.91523303947613%2C%22west
%22%3A-179.6484375%7D%7D",
  "userRecentImages": [],
  "userTopHashtags": [],
  "post": {
    "timestamp": 1701788203472,
    "languages": [],
    "media": [],
    "link": "https://www.axios.com/2023/12/05/us-israeli-settler-west-
bank-visa-ban-plan"
  },
  "source": {
    "verified": false,

```

```

    "displayName": "Axios",
    "channels": [
      "news"
    ]
  }
}
}
}
}
}
}
}
}
}
}

```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.alerts[].caption	Event.Title	N/A	.data.alerts[].eventTime	Dataminr Alert: CVE-2023-49105 referenced on X (formerly Twitter)"	Prepended with Dataminr Alert:
.data.alerts[].subCaption.bullets + .data.alerts[].post.media[].url	Event.Description	N/A	N/A	According to Capital Romanian hilip Morris mentioned in headline...	N/A
.data.alerts[].availableRelatedAlerts	Event.Attribute	Available Related Alerts	.data.alerts[].eventTime	0	Updated if already exists
.data.alerts[].eventLocation.coordinates[0]	Event.Attribute	Latitude	.data.alerts[].eventTime	37.33	Rounded to 2 decimals
.data.alerts[].eventLocation.coordinates[1]	Event.Attribute	Longitude	.data.alerts[].eventTime	-122.0	Rounded to 2 decimals
.data.alerts[].eventLocation.name	Event.Attribute	Location	.data.alerts[].eventTime	Apple Inc. HQ, Cupertino, CA, USA	N/A
.data.alerts[].post.link	Event.Attribute	Post Link	.data.alerts[].eventTime	https://www.axios.com/2023/12/05/us-israeli-se ttler-west-bank-visa-ban-plan	N/A
.data.alerts[].source.verified	Event.Attribute	Is Source Verified	.data.alerts[].eventTime	False	Updated if already exists
.data.alerts[].source.displayName	Event.Attribute	Source	.data.alerts[].eventTime	Axios	N/A
.data.alerts[].source.channels	Event.Attribute	Source Channel	.data.alerts[].eventTime	Major News	See Channel Mapping Table
.data.alerts[].alertType.name	Event.Attribute	Alert Type	.data.alerts[].eventTime	Urgent	N/A
.data.alerts[].companies[].name	Event.Attribute	Company	.data.alerts[].eventTime	Apple Inc.	N/A
.data.alerts[].categories[].name	Event.Attribute	Category	.data.alerts[].eventTime	Cybersecurity	N/A
.data.alerts[].watchlistsMatchedByType[].name	Event.Attribute	Dataminr Watchlist Name	.data.alerts[].eventTime	Exploits	N/A
.data.alerts[].expandAlertURL	Event.Attribute	Dataminr Alert URL	.data.alerts[].eventTime	https://app.dataminr.com/#alertDetail/5/1407810963-1701783539058-3	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.alerts[].metadata.cyber.vulnerabilities[].id	Related Indicator/Vulnerability.Value	CVE/ N/A	.data.alerts[].eventTime	CVE-2023-49105	Ingested according to Ingest CVEs As... config
.data.alerts[].metadata.cyber.vulnerabilities[].cvss	Related Indicator/Vulnerability.Attribute	CVSS Score	.data.alerts[].eventTime	9.8	If "CVSS score" checked in "Vulnerabilities Context". Updated if already exists
.data.alerts[].metadata.cyber.vulnerabilities[].products[].productName	Related Indicator/Vulnerability.Attribute	Product	.data.alerts[].eventTime	owncloud	if "Products affected" checked in "Vulnerabilities Context"
.data.alerts[].metadata.cyber.vulnerabilities[].products[].productVendor	Related Indicator/Vulnerability.Attribute	Vendor	.data.alerts[].eventTime	owncloud	if "Vendors" checked in "Vulnerabilities Context"
.data.alerts[].metadata.cyber.vulnerabilities[].exploitPocLinks[]	Related Indicator/Vulnerability.Attribute	Exploit POC Link	.data.alerts[].eventTime	N/A	If "Exploit POC links" checked in "Vulnerabilities Context"
.data.alerts[].metadata.cyber.addresses[].ip	Related Indicator.Value	IP Addresss	.data.alerts[].eventTime	148.72.164.186	Ingests IP Address IOCs, if "Addresses" checked in "Metadata Objects", if category is one of: "Network Scans", "Phishing", "Malware", "Domain Impersonation"
.data.alerts[].metadata.cyber.addresses[].port	Related Indicator.Attribute	Port	.data.alerts[].eventTime	80	N/A
.data.alerts[].metadata.cyber.URLs[]	Related Indicator.Value	FQDN	.data.alerts[].eventTime	ambionics.io	Ingests URL IOCs, if "URLs" checked in "Metadata Objects", if category is one of: "Network Scans", "Phishing", "Malware", "Domain Impersonation"
.data.alerts[].metadata.cyber.asOrgs[].asn	Related Indicator.Attribute	ASN	.data.alerts[].eventTime	AS13335	For Addresses and URLs, if "ASN" checked

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					in ASN Metadata
.data.alerts[].metadata.cyber.asOrgs[].asOrg	Related Indicator.Attribute	ASN Organization	.data.alerts[].eventTime	Cloudflare	For Addresses and URLs, if "ASN Organization" checked in "ASN Metadata"
.data.alerts[].metadata.cyber.hashValues[].hash	Related Indicator.Value	.data.alerts[].metadata.cyber.hashValues[].type	.data.alerts[].eventTime	N/A	Ingests Hash IOCs, if "Hashes" checked in "Metadata Objects"
.data.alerts[].metadata.cyber.malwares[]	Related Malware.Value	N/A	.data.alerts[].eventTime	N/A	If "Malware" checked in "Metadata Objects"
.data.alerts[].metadata.cyber.threats[]	Related Adversary.Name	N/A	.data.alerts[].eventTime	N/A	If "Adversary" checked in "Metadata Objects"

Channel Mapping Table

ThreatQuotient provides the following Mapping table for Dataminr API and Portal values.

DATAMINR API VALUE	DATAMINR PORTAL VALUE
news	Major News
majorblog	Major Blog
chatter	Chatter
localnews	Local News
stock	Stock Talk
market	Market Commentary
reported	Reporter
blog	Blog
corp	Corporate
gov	Government
emergency	Emergency Responders
university	University
sensor	Sensor

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.

METRIC	RESULT
Run Time	1 minute
Events	46
Event Attributes	574
Indicators	57
Indicator Attributes	137
Vulnerabilities	154
Vulnerability Attributes	202

Known Issues / Limitations

- Due to API limitations, only one of the filters `Dataminr List` or `Dataminr Query` can be used. If both are present, the `Dataminr Query` filter is ignored. If no filter is selected all the alerts will be ingested. The `List Type` filter is applied only if `Dataminr Query` is not present.

Change Log

- **Version 1.0.2**
 - Added the following configuration parameters:
 - **Alert Type** - filter threat intelligence to ingest into the ThreatQ platform by alert type.
 - **Enable SSL Verification**
 - **Disable Proxies**
- **Version 1.0.1**
 - Added the following new configuration parameters:
 - **Metadata Objects** - ingests the selected related objects.
 - **ASN Metadata** - ingest the selected metadata as address and URL attributes.
 - **Vulnerabilities Context** - ingest the selected metadata as a vulnerability attribute.
- **Version 1.0.0**
 - Initial release