ThreatQuotient

Cyberint Argos Edge CDF

Version 1.1.0

November 05, 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	1.1.0
Compatible with ThreatQ Versions	>= 6.5.0
Support Tier	ThreatQ Supported

Introduction

The Cyberint Argos Edge CDF for ThreatQ allows the automatic ingestion of intelligence from the Cyberint Argos Edge platform. Intelligence such as alerts and/or CVEs can be pulled into ThreatQ to drive incident response and prioritization.

The integration provides the following feeds:

- **Cyberint Argos Edge - Alerts -** pulls alerts from the Cyberint Argos Edge platform.
- **Cyberint Argos Edge - CVEs -** pulls relevant CVEs from the Cyberint Argos Edge platform.

The integration ingests the following system object types:

- Assets
- Adversaries
- Attack Patterns
- Events
- Indicators
- Tools
- Identities

Prerequisites

The following is required in order to use the integration:

- A Cyberint Argos Edge account with an API Access 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 feeds to install, when prompted, and click **Install**. The feed(s) will be added to the integrations page.

    > 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.

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:

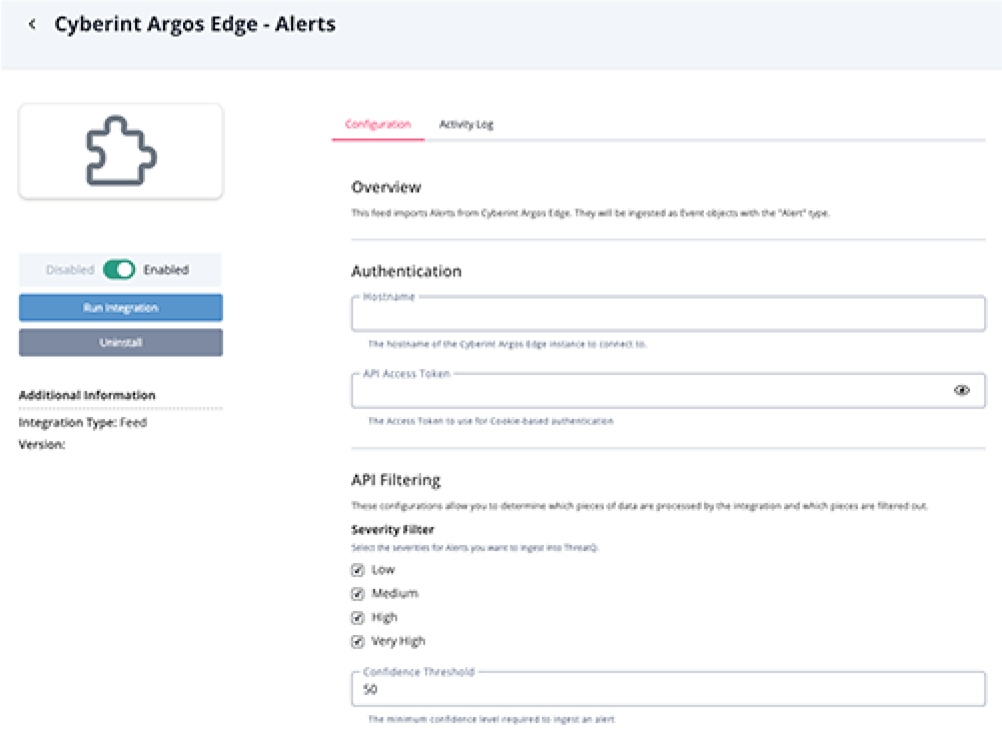
Alerts Configuration Parameters

PARAMETER	DESCRIPTION
Hostname	The hostname of your Cyberint Argos Edge instance.
API Access Token	Your Access Token to use for Cookie-based authentication.
Severity Filter	Select the severities for Alerts you want to ingest into ThreatQ. Options include: ◦ Low ◦ Medium ◦ High ◦ Very High
Confidence Threshold	Select the minimum confidence level required to ingest an alert. The default value is 50.
Alert Type Filter	Select the Alert Types you want to ingest into ThreatQ. Options include:

PARAMETER	DESCRIPTION
	◦ All (default) ◦ Refund Fraud ◦ Carding ◦ Coupon Fraud ◦ Money Laundering ◦ Victim Report ◦ Malicious Insider ◦ Extortion ◦ Phishing Email ◦ Phishing Kit ◦ Phishing Website ◦ Lookalike Domain ◦ Phishing Target List ◦ Malicious File ◦ Reconnaissance ◦ Automated Attack Tools ◦ Business Logic Bypass ◦ Target List ◦ Official Social Mediua Profile ◦ Impersonation ◦ Intellectual Property Infringement ◦ Unauthorized Trading ◦ Negative Sentiment ◦ Fake Job Posting ◦ Defacement ◦ Compromised PII ◦ Internal Information Disclosure ◦ Compromised Payment Cards ◦ Compromised Employee Credentials ◦ Compromised Customer Credentials ◦ Compromised Access Token ◦ Ransomware ◦ Exposed Web Interfaces ◦ Hijackable Subdomains ◦ Website Vulnerabilities ◦ Exposed Cloud Storage ◦ Exploitable Ports ◦ Mail Servers in Blacklist ◦ Server Connected to Botnet ◦ Email Security Issues ◦ Certificate Authority Issues ◦ SSL/TLS ◦ User Defined Saved Query ◦ Vendor Incident ◦ Other
Context Filter	Select the pieces context you want to ingest into ThreatQ with each alert. Options include: ◦ Environment (default) ◦ Tags (default) ◦ Confidence (default) ◦ Severity (default) ◦ Category (default) ◦ Alert Type (default) ◦ Impact (default) ◦ Source Category ◦ Target Vector (default) ◦ Target Brand (default)

PARAMETER	DESCRIPTION
Relationship Filter	Select the relationships you want to ingest into ThreatQ with each alert. Options include: ◦ IOCs (default) ◦ Threat Actors (default) ◦ MITRE ATT&CK Techniques (default) ◦ Assets (default) ◦ Related CVEs (default) ◦ Related Tools ◦ Leaked/Compromised Credentials (Identities)
Alert Context Filter	Select the pieces alert data context you want to ingest into ThreatQ with each alert. Options include: ◦ Detection Reasons (default) ◦ Detection Source (default) ◦ IP Reputation (default) ◦ Affected Products (default) ◦ Cyberint Score (default) ◦ Nameservers ◦ Registrar ◦ Site Title ◦ A Record ◦ Interface Type ◦ Mail Server ◦ Blacklist Repository ◦ Hosting Provider ◦ Vendor Name ◦ Exposed Code Link Not all pieces of context will be available for certain alert types.
Include Leaked Credentials Password	Enable this parameter to include the password for leaked credentials (Identities). This parameter is disabled by default.
Include Raw Alert Data in Description	Enable this to include the Raw Alert Data in the Event Description. ⚠ The integration will attempt to parse as much details out of the raw alert data as possible. However, new fields that have introduced after the release of this integration may not be parsed.

PARAMETER	DESCRIPTION
Ingest CVEs As	Select the ThreatQ object type to ingest the CVEs into ThreatQ as. Options include: Vulnerabilities (default) and Indicators (CVE).
Verify SSL	Enable this option if the feed should verify the SSL certificate.
Disable Proxies	Enable this option to have the feed ignore proxies set in the ThreatQ UI.



Additional Information

Integration Type: Feed

Version:

Overview

This feed imports Alerts from Cyberint Argos Edge. They will be ingested as Event objects with the "Alert" type.

Authentication

Hostname

The hostname of the Cyberint Argos Edge instance to connect to.

API Access Token

The Access Token to use for Cookie-based authentication.

API Filtering

These configurations allow you to determine which pieces of data are processed by the integration and which pieces are filtered out.

Severity Filter

Select the severities for Alerts you want to ingest into ThreatQ.

☑ Low
☑ Medium
☑ High
☑ Very High

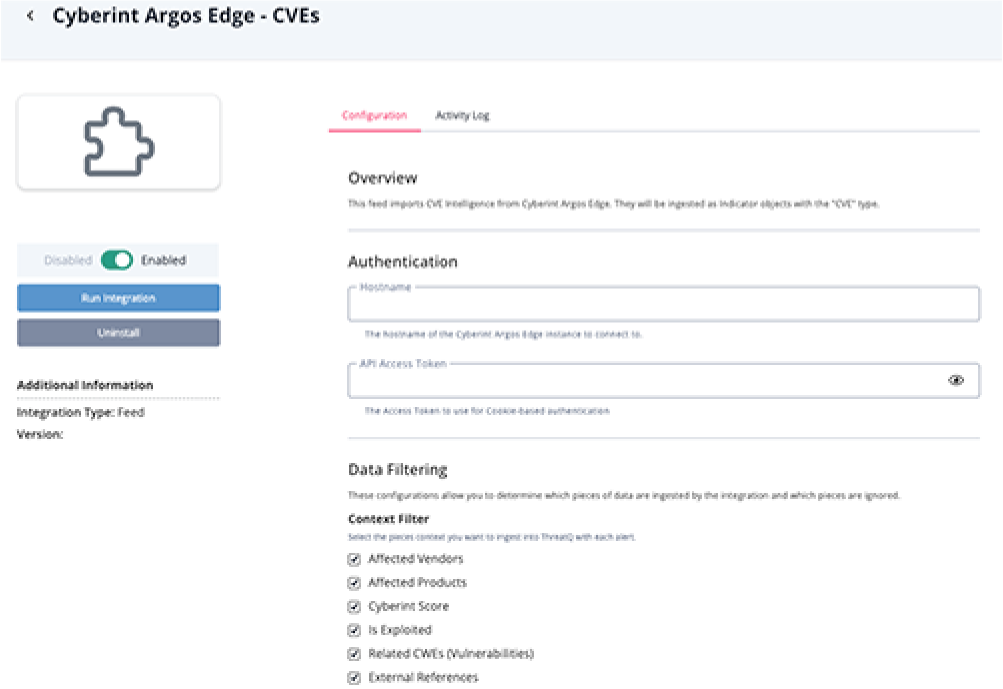
Confidence Threshold: 50

The minimum confidence level required to ingest an alert.

CVEs Configuration Parameters

PARAMETER	DESCRIPTION
Hostname	The hostname of your Cyberint Argos Edge instance.
API Access Token	Your Access Token to use for Cookie-based authentication.

PARAMETER	DESCRIPTION
Context Filter	Select the pieces context you want to ingest into ThreatQ. Options include: ◦ Affected Vendors (default) ◦ Affected Products (default) ◦ Cyberint Score (default) ◦ Is Exploited (default) ◦ Related CWEs (Vulnerabilities) (default) ◦ External References
CVSS Version	Select the CVSS version to use when parsing CVSS data. Options include: ◦ CVSS v2 ◦ CVSS v3 (default)
CVSS Context Filter	Select the CVSS context to ingest into ThreatQ. Options include: ◦ Impact Score (default) ◦ Exploitability Score (default) ◦ Vector String (default) ◦ Attack Vector ◦ Attack Complexity ◦ Privileges Required ◦ User Interaction ◦ Scope ◦ Confidentiality Impact ◦ Integrity Impact ◦ Availability Impact ◦ Base Score (default) ◦ Base Severity (default)
Ingest CVEs As	Select the ThreatQ object type to ingest the CVEs into ThreatQ as. Options include: Vulnerabilities (default) and Indicators (CVE).
Language	Enter the language (code) to choose when parsing contextual data. The default setting is `en`.
Verify SSL	Enable this option if the feed should verify the SSL certificate.
Disable Proxies	Enable this option to have the feed ignore proxies set in the ThreatQ UI.



Cyberint Argos Edge - CVEs

Additional Information

Integration Type: Feed

Version:

Overview

This feed imports CVE intelligence from Cyberint Argos Edge. They will be ingested as Indicator objects with the "CVE" type.

Authentication

Hostname

The hostname of the Cyberint Argos Edge instance to connect to.

API Access Token

The Access Token to use for Cookie-based authentication.

Data Filtering

These configurations allow you to determine which pieces of data are ingested by the integration and which pieces are ignored.

Context Filter

Select the pieces context you want to ingest into ThreatQ with each alert.

☑ Affected Vendors
☑ Affected Products
☑ Cyberint Score
☑ Is Exploited
☑ Related CWEs (Vulnerabilities)
☑ External References

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

Cyberint Argos Edge - Alerts

The Cyberint Argos Edge - Alerts feed automatically pulls alerts from Cyberint Argos Edge into ThreatQ. You can filter down the alerts by severity, confidence, and/or type. You can also customize which fields are pulled into ThreatQ with the goal of reducing noise and focusing on the most relevant alerts.

`POST https://{{ host }}/api/v1/alerts`

Sample Response:

```
{
  "total": 1,
  "alerts": [
    {
      "environment": "ThreatQ",
      "ref_id": "THR-623",
      "confidence": 90,
      "status": "open",
      "severity": "high",
      "created_date": "2023-09-07T11:15:17",
      "created_by": {
        "email": "system"
      },
      "category": "data",
      "type": "compromised_customer_credentials",
      "source_category": "malware_log",
      "source": "RedLine Malware Logs",
      "targeted_vectors": ["customer"],
      "targeted_brands": ["ThreatQ"],
      "related_entities": ["example.com"],
      "impacts": [
        "data_compromise",
        "unauthorized_access",
        "account_takeover",
        "revenue_loss",
        "brand_degradation",
        "customer_churn",
        "financial_penalties"
      ],
      "acknowledged_date": null,
      "acknowledged_by": null,
      "publish_date": "2021-09-05T10:44:44",
      "title": "Company Customer Credentials Exposed",
      "alert_data": {
        "csv": {
          "id": 1509034,
          "name": "company_customer_credentials_exposed.csv",
          "mimetype": "text/csv",
          "is_safe": true,
          "content": null
        },
        "application": null,
        "total_credentials": 2,
        "hashed_attachment_content_csv":
"d84a34a201fc9b34e401a8d06301bda30ef998502f95c4974b3933a224988b27"
      },
      "iocs": [],
      "ticket_id": null,
      "threat_actor": null,
      "modification_date": "2023-09-07T11:15:17",
      "closure_date": null,
      "closed_by": null,
      "closure_reason": null,
      "closure_reason_description": null,
      "description": "Compromised customer credentials for a company interface
have been detected. The credentials seem to have been obtained by credential
harvesting malware, which has infected the customer's machine and is sending
user input logs, including harvested credentials, to the Command & Control
(C&C) server operator. Therefore, the malware logs contain user credentials not
only for the company login interface, but for other site login interfaces as
well. Compromised customer credentials may be used by threat actors to perform
fraudulent account activity on the customer's behalf, including unauthorized
transactions, exposing the company to both financial impact and legal claims.",
      "recommendation": "Best practices include enforcing password reset for
the compromised account and analyzing for fraudulent activity. In addition,
consider implementing MFA in order to prevent account takeover with malware-
harvested credentials. Note that the victim might still be infected by malware,
so it is likely that new credentials will be harvested again. Therefore,
consider contacting the customer and recommending they clean the infected
machine. If fraudulent activity is found within the account's records, any IOCs
should be flagged within the company's systems.",
      "tags": [],
      "analysis_report": null,
      "attachments": [],
      "mitre": ["T1593", "T1594", "T1589"],
      "related_assets": [
        {
          "name": "example.com",
          "id": "domain/ThreatQ/example.com",
          "type": "domain"
        }
      ]
    }
  ]
```

```
}
```

Cyberint - Fetch Alert Details (Supplemental)

The Cyberint - Fetch Alert Details supplemental feed fetches an individual alert's details by its ID.

`GET https://{{ host }}/api/v1/alerts/{{ id }}`

Sample Response:

```
{
  "environment": "ThreatQ",
  "ref_id": "THR-623",
  "confidence": 90,
  "status": "open",
  "severity": "high",
  "created_date": "2023-09-07T11:15:17",
  "created_by": {
    "email": "system"
  },
  "category": "data",
  "type": "compromised_customer_credentials",
  "source_category": "malware_log",
  "source": "RedLine Malware Logs",
  "targeted_vectors": ["customer"],
  "targeted_brands": ["ThreatQ"],
  "related_entities": ["example.com"],
  "impacts": [
    "data_compromise",
    "unauthorized_access",
    "account_takeover",
    "revenue_loss",
    "brand_degradation",
    "customer_churn",
    "financial_penalties"
  ],
  "acknowledged_date": null,
  "acknowledged_by": null,
  "publish_date": "2021-09-05T10:44:44",
  "title": "Company Customer Credentials Exposed",
  "alert_data": {
    "csv": {
      "id": 1509034,
      "name": "company_customer_credentials_exposed.csv",
      "mimetype": "text/csv",
      "is_safe": true,
      "content": null
    },
    "application": null,
    "total_credentials": 2,
    "hashed_attachment_content_csv":
```

```
"d84a34a201fc9b34e401a8d06301bda30ef998502f95c4974b3933a224988b27"
  },
  "iocs": [],
  "ticket_id": null,
  "threat_actor": null,
  "modification_date": "2023-09-07T11:15:17",
  "closure_date": null,
  "closed_by": null,
  "closure_reason": null,
  "closure_reason_description": null,
  "description": "Compromised customer credentials for a company interface have
been detected. The credentials seem to have been obtained by credential
harvesting malware, which has infected the customer's machine and is sending
user input logs, including harvested credentials, to the Command & Control
(C&C) server operator. Therefore, the malware logs contain user credentials not
only for the company login interface, but for other site login interfaces as
well. Compromised customer credentials may be used by threat actors to perform
fraudulent account activity on the customer's behalf, including unauthorized
transactions, exposing the company to both financial impact and legal claims.",
  "recommendation": "Best practices include enforcing password reset for the
compromised account and analyzing for fraudulent activity. In addition,
consider implementing MFA in order to prevent account takeover with malware-
harvested credentials. Note that the victim might still be infected by malware,
so it is likely that new credentials will be harvested again. Therefore,
consider contacting the customer and recommending they clean the infected
machine. If fraudulent activity is found within the account's records, any IOCs
should be flagged within the company's systems.",
  "tags": [],
  "analysis_report": null,
  "attachments": [],
  "mitre": ["T1593", "T1594", "T1589"],
  "related_assets": [
    {
      "name": "example.com",
      "id": "domain/ThreatQ/example.com",
      "type": "domain"
    }
  ]
}
```

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`, `.severity`, `.confidence`	Event.Title	Alert	`.publish_date`	N/A	Additional fields are used in the title, when available
`.[multiple_fields]`	Event.Description	N/A	N/A	N/A	Available fields are concatenated together to form an HTML description
`.tags[]`	Event.Tag	N/A	N/A	`demo`	Ingested if it is enabled in `Context Filter`.
`.alert_data.domain`	Event.Attribute	Affected Domain	`.created_date`	N/A	N/A
`.alert_data.environment`	Event.Attribute	Environment	`.created_date`	ThreatQ	Ingested if it is enabled in `Context Filter`.
`.ref_id`	Event.Attribute	Alert ID	`.created_date`	N/A	N/A
`.confidence`	Event.Attribute	Confidence	`.created_date`	`90`	Ingested if it is enabled in `Context Filter`. Updated if it already exists.
`.severity`	Event.Attribute	Severity	`.created_date`	`High`	Ingested if it is enabled in `Context Filter`. Updated if it already exists.
`.category`	Event.Attribute	Category	`.created_date`	`Data`	Ingested if it is enabled in `Context Filter`.
`.type`	Event.Attribute	Alert Type	`.created_date`	`Compromised Customer Credentials`	Ingested if it is enabled in `Context Filter`.
`.source_category`	Event.Attribute	Source Category	`.created_date`	`malware_log`	Ingested if it is enabled in `Context Filter`.
`.source`	Event.Attribute	Source	`.created_date`	`RedLine Malware Logs`	Ingested if it is enabled in `Context Filter`.
`.targeted_vectors[]`	Event.Attribute	Target Vector	`.created_date`	`customer`	Ingested if it is enabled in `Context Filter`.
`.targeted_brands[]`	Event.Attribute	Target Brand	`.created_date`	`ThreatQ`	Ingested if it is enabled in `Context Filter`.
`.impacts[]`	Event.Attribute	Impact	`.created_date`	`data_compromise`	Ingested if it is enabled in `Context Filter`.
`.alert_data.detection_reasons[]`	Event.Attribute	Detection Reason	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.detection_source`	Event.Attribute	Detection Source	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.ip_reputation`	Event.Attribute	IP Reputation	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.nameservers[]`	Event.Attribute	Nameserver	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.alert_data.registrar`	Event.Attribute	Registrar	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.title`	Event.Attribute	Site Title	`.created_date`	`Welcome`	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.a_record[]`	Event.Attribute	A Record	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.interface_type`	Event.Attribute	Interface Type	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.affected_product`	Event.Attribute	Affected Product	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.mail_server`	Event.Attribute	Mail Server	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.blacklist_repository`	Event.Attribute	Blacklist Repository	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.hosting_provider`	Event.Attribute	Hosting Provider	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.vendor_name`	Event.Attribute	Vendor Name	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.exposed_code_link`	Event.Attribute	Exposed Code Link	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`.
`.mitre[]`	Event.AttackPattern	N/A	`.created_date`	N/A	Mapped to existing Attack Patterns
`.threat_actor`	Event.Adversary.Name	N/A	`.created_date`	N/A	Ingested if it is enabled in `Relationship Filter`.
`.related_assets[].name`	Event.Asset.Value	N/A	`.created_date`	`threatq.com`	Ingested if it is enabled in `Relationship Filter`.
`.related_assets[].type`	Event.Asset.Attribute	Asset Type	N/A	`domain`	N/A
`.iocs[].value`	Event.Indicator.Value	`.related_assets[].type`	`.created_date`	N/A	Ingested if it is enabled in `Relationship Filter`.
`.alert_data.csv.content[].username`	Event.Identity.Value	N/A	`.created_date`	N/A	N/A
`.alert_data.tool_name`	Event.Tool.Value	N/A	`.created_date`	N/A	Ingested if it is enabled in `Relationship Filter`.
`.alert_data.cves[].name`	Event.Vulnerability.Value, Event.Indicator.Value	CVE	`.created_date`	N/A	Ingested object type based on user-field selection
`.alert_data.cves[].cyberint_score`	Event.Attribute	Cyberint Score	`.created_date`	`7.9`	Ingested if it is enabled in `Alert Context Filter`. Rounded to 2 decimals. Updated if it already exists.
`.alert_data.techologies[].cves[].name`	Event.Vulnerability.Value, Event.Indicator.Value	CVE	`.created_date`	N/A	Ingested object type based on user-field selection

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.alert_data.technologies[].cves[].cyberint_score`	Event.Attribute	Cyberint Score	`.created_date`	N/A	Ingested if it is enabled in `Alert Context Filter`. Rounded to 2 decimals. Updated if it already exists.
`.alert_data.technologies[].service_product`	Event.Attribute	Affected Product	`.created_date`	`windows_server_2012`	Ingested if it is enabled in `Alert Context Filter`.
`.alert_data.additional_technologies_detected[].name`	Event.Vulnerability.Value, Event.Indicator.Value	CVE	`.created_date`	N/A	Ingested object type based on user-field selection
`.alert_data.additional_technologies_detected[].cyberint_score`	Event.Attribute	Cyberint Score	`.created_date`	`7.9`	Ingested if it is enabled in `Alert Context Filter`. Rounded to 2 decimals. Updated if it already exists.
`.alert_data.additional_technologies_detected[].package`	Event.Attribute	Affected Product	`.created_date`	`jquery`	Ingested if it is enabled in `Alert Context Filter`.

Cyberint Argos Edge - CVEs

The Cyberint Argos Edge - CVEs feed automatically pulls vulnerabilities affecting your organization's assets, tracked in Cyberint Argos Edge. You can customize the context that gets brought back from the API, including information such as Affected Vendors and CVSS Score. This will allow you to prioritize vulnerabilities based on your organization's assets and the context of the vulnerability.

`POST https://{{ host }}/cve-intel/get_cves`

Sample Response:

```
{
  "data": {
    "page_size": 20,
    "page_number": 1,
    "cves": [
      {
        "id": "CVE-2022-41073",
        "cve": {
          "data_type": "CVE",
          "data_format": "MITRE",
          "data_version": "4.0",
          "cve_data_meta": {
            "id": "CVE-2022-41073",
            "assigner": "secure@microsoft.com"
          },
          "problem_type": {
            "problem_type_data": [
              {
                "description": [
                  {
                    "lang": "en",
                    "value": "CWE-787"
                  }
                ]
              }
            ]
          },
          "references": {
            "reference_data": [
              {
                "url": "https://msrc.microsoft.com/update-guide/vulnerability/
CVE-2022-41073",
                "name": "https://msrc.microsoft.com/update-guide/vulnerability/
CVE-2022-41073",
                "reference_source": "MISC",
                "tags": []
              },
              {
                "url": "http://packetstormsecurity.com/files/174528/Microsoft-
Windows-Privilege-Escalation.html",
                "name": "http://packetstormsecurity.com/files/174528/Microsoft-
Windows-Privilege-Escalation.html",
                "reference_source": "MISC",
                "tags": []
              }
            ]
          },
          "description": {
            "description_data": [
              {
                "lang": "en",
                "value": "Windows Print Spooler Elevation of Privilege
Vulnerability"
              }
            ]
          }
        },
        "configurations": {
          "cve_data_version": "4.0",
          "nodes": [
            {
              "operator": "OR",
              "negate": null,
              "children": [],
              "cpe_match": [
                {
                  "version_start_excluding": null,
                  "version_start_including": null,
                  "version_end_excluding": null,
                  "version_end_including": null,
                  "vulnerable": true,
                  "cpe23_uri":
"cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:*",
                  "cpe_name": []
                },
                {
                  "version_start_excluding": null,
                  "version_start_including": null,
                  "version_end_excluding": null,
                  "version_end_including": null,
                  "vulnerable": true,
                  "cpe23_uri":
"cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*",
                  "cpe_name": []
                }
              ]
            }
          ]
        },
        "impact": {
          "base_metric_v3": {
            "cvss_v3": {
              "version": "3.1",
              "vector_string": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
              "attack_vector": "LOCAL",
              "attack_complexity": "LOW",
              "privileges_required": "LOW",
              "user_interaction": "NONE",
              "scope": "UNCHANGED",
              "confidentiality_impact": "HIGH",
              "integrity_impact": "HIGH",
              "availability_impact": "HIGH",
              "base_score": 7.8,
              "base_severity": "HIGH"
            },
            "exploitability_score": 1.8,
            "impact_score": 5.9
          },
          "base_metric_v2": null
        },
        "published_date": "2022-11-09T22:15:00+00:00",
        "last_modified_date": "2023-09-06T21:15:00+00:00",
        "cyberint_score": 9.80063,
        "research_content": {
          "analysis": "",
          "recommendation": "",
          "is_notable": true,
          "alias": [""],
          "updated_date": "2022-11-13T14:57:56.378035"
        },
        "known_exploited_vulnerability": true,
        "cpes": [
          {
            "vendor": "microsoft",
            "product": "windows_server_2008",
            "version": ["r2"],
            "version_start_excluding": null,
            "version_start_including": null,
            "version_end_excluding": null,
            "version_end_including": null,
            "vulnerable": null
          },
          {
            "vendor": "microsoft",
            "product": "windows_server_2012",
            "version": ["r2"],
            "version_start_excluding": null,
            "version_start_including": null,
            "version_end_excluding": null,
            "version_end_including": null,
            "vulnerable": null
          }
        ]
      }
    ]
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.id`	Indicator.Value, Vulnerability.Value	CVE	`.published_date`	`CVE-2023-0001`	ThreatQ Entity depends on user-field selection
`.cve.description.description_data[]`	Indicator.Description, Vulnerability.Description	N/A	N/A	N/A	Each item in list is joined together
`.cve.problem_type.problem_type_data[]`	Vulnerability.Vulnerability.Value	N/A	`.published_date`	`CWE-100`	Ingested if it is enabled in `Context Filter`
`.known_exploited_vulnerability`	Attribute	`Is Exploited`	`.published_date`	`true`	Ingested if it is enabled in `Context Filter`. Updated if it already exists.
`.cyberint_score`	Attribute	`Cyberint Score`	`.published_date`	`7.91`	Ingested if it is enabled in `Context Filter`. Rounded to 2 decimals. Updated if it already exists.
`.cpes[].vendor`	Attribute	`Affected Vendor`	`.published_date`	`jquery`	Ingested if it is enabled in `Context Filter`.
`.cpes[].product`	Attribute	`Affected Product`	`.published_date`	`windows_server`	Ingested if it is enabled in `Context Filter`.
`.cve.references.reference_data[].url`	Attribute	`External Reference`	`.published_date`	N/A	Ingested if it is enabled in `Context Filter`.
`.impact.base_metric.impact_score`	Attribute	`CVSS Impact Score`	`.published_date`	`5.9`	Ingested if it is enabled in `CVSS Context Filter`. Updated if it already exists.
`.impact.base_metric.exploitability_score`	Attribute	`CVSS Exploitability Score`	`.published_date`	`1.8`	Ingested if it is enabled in `CVSS Context Filter`. Updated if it already exists.
`.impact.base_metric.cvss.vector_string`	Attribute	`CVSS Vector String`	`.published_date`	N/A	Ingested if it is enabled in `CVSS Context Filter`.
`.impact.base_metric.cvss.attack_vector`	Attribute	`CVSS Attack Vector`	`.published_date`	`LOCAL`	Ingested if it is enabled in `CVSS Context Filter`.
`.impact.base_metric.cvss.attack_complexity`	Attribute	`CVSS Attack Complexity`	`.published_date`	`LOW`	Ingested if it is enabled in `CVSS Context Filter`. Updated if it already exists.
`.impact.base_metric.cvss.privileges_required`	Attribute	`CVSS Privileges Required`	`.published_date`	`LOW`	Ingested if it is enabled in `CVSS Context Filter`. Updated if it already exists.
`.impact.base_metric.cvss.user_interaction`	Attribute	`CVSS User Interaction`	`.published_date`	`NONE`	Ingested if it is enabled in `CVSS Context Filter`.
`.impact.base_metric.cvss.scope`	Attribute	`CVSS Scope`	`.published_date`	`UNCHANGED`	Ingested if it is enabled in `CVSS Context Filter`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.impact.base_metric.cvss.confidentiality_impact`	Attribute	`CVSS Confidentiality Impact`	`.published_date`	`HIGH`	Ingested if it is enabled in `CVSS Context Filter`. Updated if it already exists.
`.impact.base_metric.cvss.integrity_impact`	Attribute	`CVSS Integrity Impact`	`.published_date`	`HIGH`	Ingested if it is enabled in `CVSS Context Filter`. Updated if it already exists.
`.impact.base_metric.cvss.availability_impact`	Attribute	`CVSS Availability Impact`	`.published_date`	`HIGH`	Ingested if it is enabled in `CVSS Context Filter`. Updated if it already exists.
`.impact.base_metric.cvss.base_score`	Attribute	`CVSS Base Score`	`.published_date`	`7.8`	Ingested if it is enabled in `CVSS Context Filter`. Updated if it already exists.
`.impact.base_metric.cvss.base_severity`	Attribute	`CVSS Base Severity`	`.published_date`	`HIGH`	Ingested if it is enabled in `CVSS Context Filter`. Updated if it already exists.

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.

Alerts

METRIC	RESULT
Run Time	1 minute
Assets	2
Asset Attributes	2
Attack Patterns	4
Events	8
Event Attributes	115

CVEs

METRIC	RESULT
Run Time	1 minute
Indicators	50
Indicator Attributes	723
Vulnerabilities	19

Known Issues / Limitations

- Alert Data will be parsed, but due to the vast number of alert types, not all fields may be parsed. You can use the **Include Raw Alert Data in Description** option to include the raw alert data in the Event Description.

Change Log

- **Version 1.1.0**
  - Added a new MITRE Filter designed to streamline the handling of MITRE ATT&CK data and improve efficiency.
  - Updated minimum ThreatQ version to 6.5.0.
- **Version 1.0.1**
  - Resolved a Type Error that resulted in a `Cannot parse argument of type None` message.
  - All Cyberint Argos Edge feeds - added two new configuration parameters: **Enable SSL Verification** and **Disable Proxies**.
- **Version 1.0.0**
  - Initial release