ThreatQuotient

VulnCheck CDF

Version 1.0.0

June 23, 2025

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	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The VulnCheck CDF integration provides the ability to ingest vulnerability intelligence from VulnCheck's API into the ThreatQ platform. The integration allows users to receive timely updates on known exploited vulnerabilities, potential attack vectors, and threat actor activities, enabling them to proactively manage their security risks and prioritize remediation efforts.

The integration provides the following feeds:

- **VulnCheck Exploits** - ingests exploited vulnerability data from VulnCheck's `exploits` index.
- **VulnCheck Threat Actors** - ingests vulnerability data associated with threat actors from VulnCheck's `threat-actors` index.
- **VulnCheck Vulnerabilities** - ingests vulnerability data from VulnCheck's `vulncheck-nvd2` index.

The integration ingests the following object types:

- Adversaries
- Attack Patterns
- Indicators
- Vulnerabilities

Prerequisites

The following is required to run the integration:

- A VulnCheck API Key.
- For the VulnCheck Vulnerabilities feed, ThreatQuotient recommends installing the following integrations if you enable these parameters:

ENABLED CONFIGURATION PARAMETER	RECOMMENDED ADDITIONAL THREATQ FEED
Ingest MITRE ATT&CK CWEs	MITRE ATT&CK CWE CDF - https://marketplace.threatq.com/details/mitre-att-ck-cwe-cdf
Ingest MITRE ATT&CK CAPECs	MITRE ATT&CK CAPEC CDF - https://marketplace.threatq.com/details/mitre-att-ck-capec-cdf
Ingest MITER ATT&CK Techniques	MITRE ATT&CK CDF - https://marketplace.threatq.com/details/mitre-att-ck-cdf

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(s).

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).

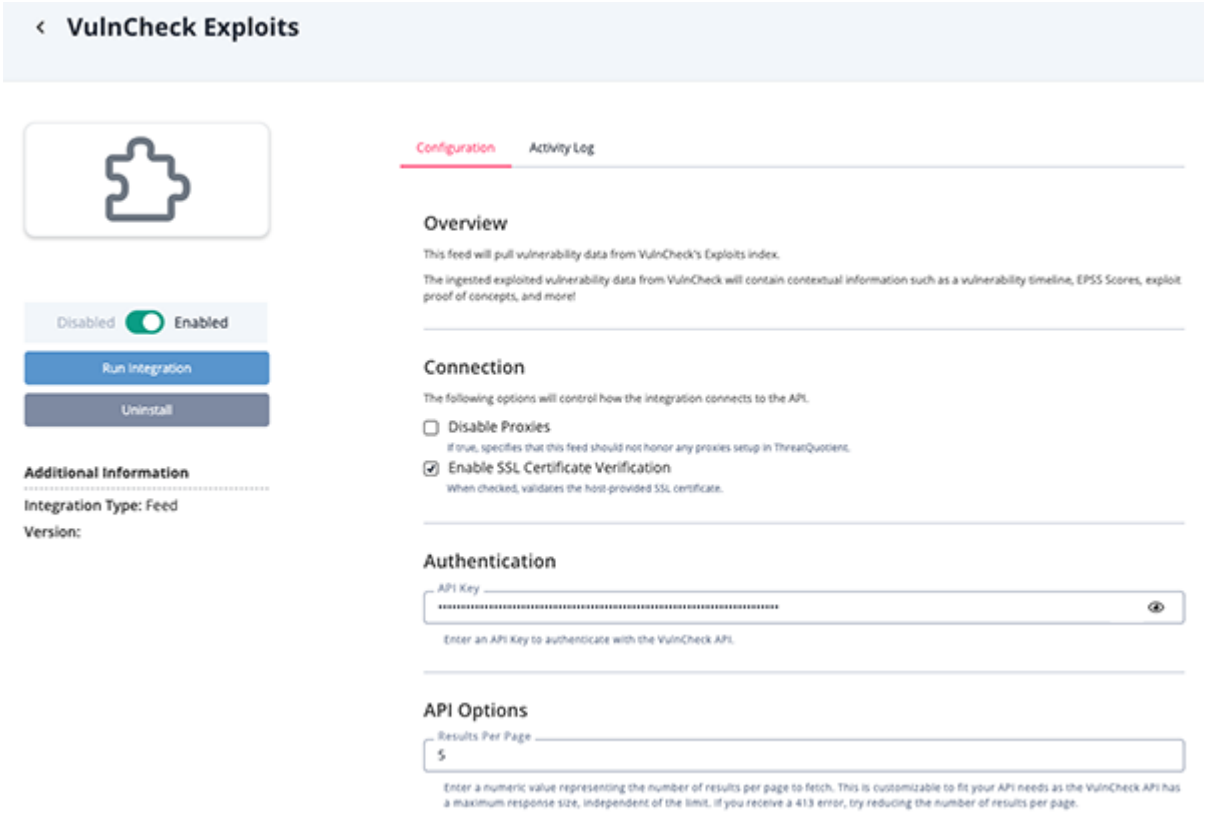
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

VulnCheck Exploits Parameters

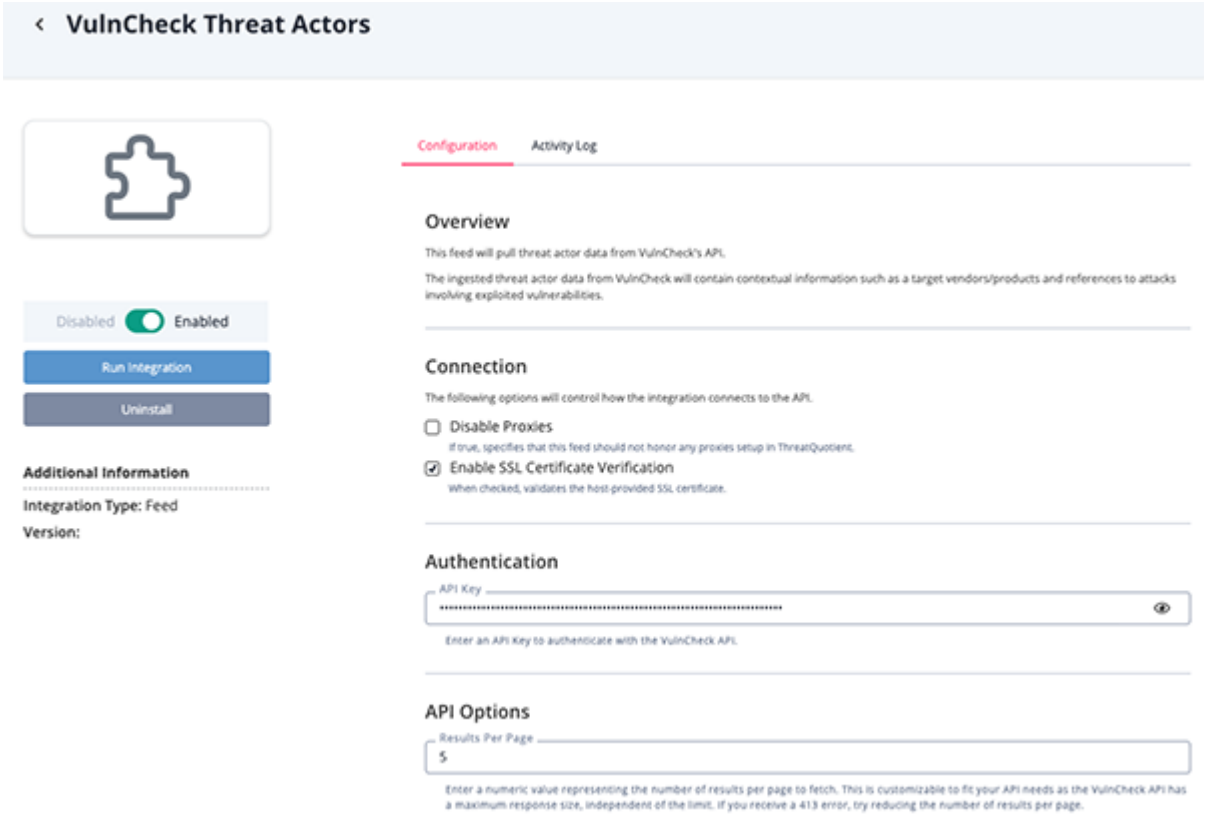
PARAMETER	DESCRIPTION
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
API Key	Enter your VulnCheck API key.
Results per Page	Enter a numeric value representing the number of results per page to fetch. This allows you to customize results to fit your API needs as the VulnCheck API has a maximum response size, independent of the limit. The default value for this parameter is 5. > If you receive a 413 error, reduce the number of results per page.

PARAMETER	DESCRIPTION
Ingest CVEs As	Select which entity type to ingest CVEs as into the ThreatQ platform. Options include: ◦ Indicators (Type: CVE) ◦ Vulnerabilities *(default)*
Relationship Options	Select the relationships to ingest into ThreatQ with each CVE. Options include: ◦ Threat Actor *(default)* ◦ Ransomware *(default)* ◦ Botnet *(default)*



VulnCheck Threat Actors Parameters

PARAMETER	DESCRIPTION
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
API Key	Enter your VulnCheck API key.
Results per Page	Enter a numeric value representing the number of results per page to fetch. This allows you to customize results to fit your API needs as the VulnCheck API has a maximum response size, independent of the limit. The default value for this parameter is 5. If you receive a 413 error, reduce the number of results per page.
Ingest CVEs As	Select which entity type to ingest CVEs as into the ThreatQ platform. Options include: ◦ Indicators (Type: CVE) ◦ Vulnerabilities *(default)*

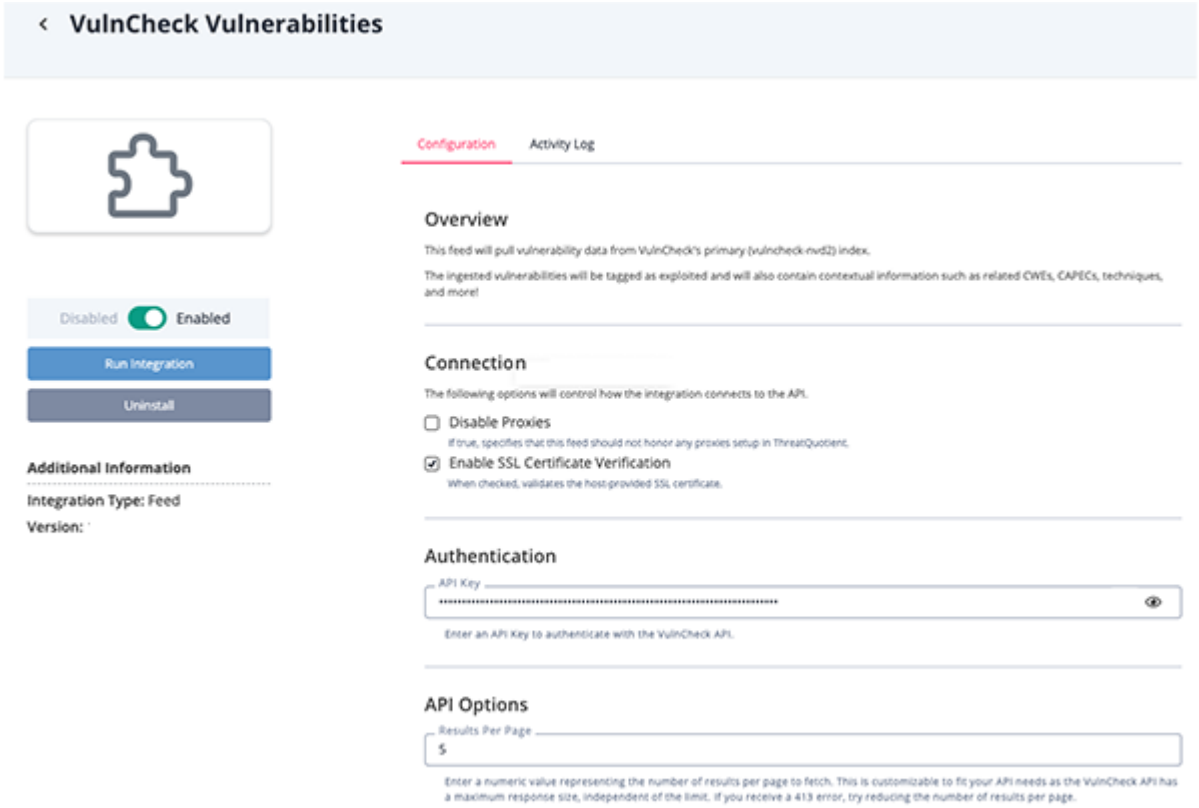


VulnCheck Vulnerabilities Parameters

PARAMETER	DESCRIPTION
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
API Key	Enter your VulnCheck API key.
Results per Page	Enter a numeric value representing the number of results per page to fetch. This allows you to customize results to fit your API needs as the VulnCheck API has a maximum response size, independent of the limit. The default value for this parameter is 5.

PARAMETER	DESCRIPTION
	If you receive a 413 error, reduce the number of results per page.
Ingested CVSS Metrics	Select which CVSS Metrics to ingest as attributes. All CVSS metrics will be ingested to the vulnerability's description for viewing. Options include: ◦ CVSS v4.0 ◦ CVSS v3.1 (default) ◦ CVSS v2.0
CVSS Context Selection	Select which CVSS Context to ingest as attributes. Attributes will be prefixed by the version number based on the selected metrics. For example, CVSS v4.0 will bring in attributes like `CVSSv40 Base Score` while CVSS v3.1 will bring in attributes like `CVSSv31 Base Score` and CVSSv2 will bring in attributes like `CVSSv2 Base Score`. Parameters options include: ◦ Vector String ◦ Base Score (default) ◦ Temporal Score ◦ Base Severity (default) ◦ Base Threat Score (default) ◦ Base Threat Severity (default) ◦ Exploitability Score ◦ Impact Score ◦ Attack Vector ◦ Access Vector ◦ Attack Complexity ◦ Access Complexity ◦ Exploit Code Maturity ◦ Report Confidence ◦ Remediation Level ◦ Privileges Required ◦ User Interaction ◦ Scope ◦ Confidentiality Impact ◦ Integrity Impact ◦ Availability Impact ◦ Environmental Score Not all fields will be available for all CVSS metric versions. When multiple metrics are found for the same version. The `Primary` metric will be used when available.
Ingest MITRE ATT&CK CWEs	Enable this parameter to ingest Common Weakness Enumerations (CWEs) associated with the CVEs. If enabled, ThreatQuotient highly recommend installing the MITRE ATT&CK CWE feed from the ThreatQ

PARAMETER	DESCRIPTION
	Marketplace: https://marketplace.threatq.com/details/mitre-att-ck-cwe-cdf.
Ingest MITRE ATT&CK CAPECs	Enable this parameter to ingest Common Attack Pattern Enumeration and Classifications (CAPECs) associated with the CVEs. If enabled, ThreatQuotient highly recommend installing the MITRE ATT&CK CAPEC feed from the ThreatQ Marketplace: https://marketplace.threatq.com/details/mitre-att-ck-capec-cdf.
Ingest MITRE ATT&CK Techniques	Enable this parameter to ingest MITRE ATT&CK Techniques associated with the CVEs. If enabled, ThreatQuotient highly recommend installing the MITRE ATT&CK feed from the ThreatQ Marketplace: https://marketplace.threatq.com/details/mitre-att-ck-cdf.
Ingest CVEs As	Select which entity type to ingest CVEs as into the ThreatQ platform. Options include: ◦ Indicators (Type: CVE) ◦ Vulnerabilities *(default)*
Description Language	Enter the language code to use when extracting the CVE descriptions. This will be used to localize the feed data. For example, `en` for English, `es` for Spanish, `fr` for French, etc. If the selected language is not available, the feed will default to English.



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

VulnCheck Exploits

The VulnCheck Exploits feed ingests exploited vulnerability data from VulnCheck' `exploits` index. The endpoint provides aggregated data from VulnCheck's team as well as data from NVD and CISA KEV.

`GET https://api.vulncheck.com/v3/index/exploits`

Sample Response:


```
{
  "_benchmark": 0.071894,
  "_meta": {
    "timestamp": "2025-02-11T20:37:36.835026371Z",
    "index": "exploits",
    "limit": 10,
    "total_documents": 2,
    "sort": "_id",
    "order": "asc",
    "cursor": "",
    "next_cursor": ""
  },
  "data": [
    {
      "id": "CVE-2021-43163",
      "public_exploit_found": false,
      "commercial_exploit_found": false,
      "weaponized_exploit_found": true,
      "max_exploit_maturity": "weaponized",
      "reported_exploited": true,
      "reported_exploited_by_threat_actors": false,
      "reported_exploited_by_ransomware": false,
      "reported_exploited_by_botnets": false,
      "inKEV": false,
      "inVCKEV": true,
      "timeline": {
        "nvd_published": "2022-05-04T01:15:00Z",
        "nvd_last_modified": "2024-11-21T06:28:00Z",
        "vulncheck_kev_date_added": "2024-12-05T00:00:00Z"
      },
      "trending": {
        "github": false
      },
      "epss": {
        "epss_score": 0.00397,
        "epss_percentile": 0.7348,
```

```
        "last_modified": "2025-02-11T10:00:44.062273Z"
      },
      "counts": {
        "exploits": 0,
        "threat_actors": 0,
        "botnets": 0,
        "ransomware_families": 0
      },
      "reported_exploitation": [
        {
          "url": "https://dashboard.shadowserver.org/statistics/honeypot/
vulnerability/map/?day=2024-12-05host_type=srcvulnerability=cve-2021-43163",
          "name": "Ruijie RG-EW Series Routers (CVE-2021-43163)",
          "refsource": "shadowserver-exploited",
          "date_added": "2024-12-05T00:00:00Z"
        },
        {
          "date_added": "2023-03-10T00:00:00Z",
          "name": "LemonDuck",
          "refsource": "vulncheck-botnets",
          "url": "https://www.antiy.cn/research/noticereport/research_report/
20230310.html"
        },
        {
          "date_added": "2022-06-29T00:00:00Z",
          "name": "Conti",
          "refsource": "vulncheck-ransomware",
          "url": "https://www.securin.io/articles/all-about-conti-ransomware/"
        },
        {
          "date_added": "2023-02-14T00:00:00Z",
          "name": "Razor Tiger",
          "refsource": "vulncheck-threat-actors",
          "url": "https://www.group-ib.com/resources/research-hub/sidewinder-
apt/"
        }
      ],
      "date_added": "2024-12-05T00:00:00Z",
      "_timestamp": "2025-02-10T09:27:37.772678659Z"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed based on each item within the API's response `.data` array.

> The following fields are added to the description for each CVE: `.timeline[].first_exploit_published, .timeline[].most_recent_exploit_published, .counts.exploits, .counts.threat_actors, .counts.ransomware_families, .counts.botnets, .reported_exploitation[].name, .reported_exploitation[].url, .reported_exploitation[].date_added, .exploits[].name, .exploits[].exploit_maturity, .exploits[].exploit_availability, .exploits[].exploit_type, exploits[].date_added`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.id`	Indicator/ Vulnerability.Value	CVE/Vulnerability	`.date_added`	`CVE-2025-12345`	Ingested object type depends on user-field selection
`.reported_exploitation[]`	Malware.Value	Malware	`.date_added`	`LemonDuck Botnet`	Where `refsource` in [`botnets`, `vulncheck-botnets`]. `Botnet` appended to value if not already present. Not added if value ends with `Attribution`. User-configurable
`.reported_exploitation[]`	Malware.Value	Malware	`.date_added`	`Conti Ransomware`	Where `refsource` in [`ransomware`, `vulncheck-ransomware`]. `Ransomware` appended to value if not already present. Not added if value ends with `Attribution`. User-configurable
`.reported_exploitation[]`	Adversary.Name	Adversary	`.date_added`	`Razor Tiger`	Where `refsource` in [`threat-actors`, `vulncheck-threat-actors`]. Not added if value ends with `Attribution`. User-configurable
`.inKEV`, `.inVCKEV`	Indicator/ Vulnerability.Tag	N/A	N/A	`exploited`	Static tag added when either field is true
`.inKEV`, `.inVCKEV`	Indicator/ Vulnerability.Attribute	Is KEV	N/A	`true`	true if either field is true. Updatable
`.public_exploit_found`	Indicator/ Vulnerability.Attribute	Public Exploit Found	`.date_added`	`true`	Updatable
`.commercial_exploit_found`	Indicator/ Vulnerability.Attribute	Commercial Exploit Found	`.date_added`	`true`	Updatable
`.weaponized_exploit_found`	Indicator/ Vulnerability.Attribute	Weaponized Exploit Found	`.date_added`	`false`	Updatable
`.max_exploit_maturity`	Indicator/ Vulnerability.Attribute	Max Exploit Maturity	`.date_added`	`weaponized`	Updatable
`.reported_exploited_by_threat_actors`	Indicator/ Vulnerability.Attribute	Exploited by Threat Actors	`.date_added`	`true`	Updatable
`.reported_exploite`	Indicator/ Vulnerability.Attribute	Exploited by Ransomware	`.date_added`	`false`	Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`d_by_ransomware`					
`.reported_exploited_by_botnets`	Indicator/ Vulnerability.Attribute	Exploited by Botnets	`.date_added`	`false`	Updatable
`.epss.epss_score`	Indicator/ Vulnerability.Attribute	EPSS Score	`.date_added`	`0.97374`	Updatable
`.epss.epss_percentile`	Indicator /Vulnerability.Attribute	EPSS Percentile	`.date_added`	`0.99961`	Updatable

VulnCheck Threat Actors

The VulnCheck Threat Actors feed ingests vulnerability data associated with threat actors from VulnCheck's `threat-actors` index. This API provides information such as the linked threat actor, the targeted sectors/vendors/products, and recent attacks by the threat actor.

`GET https://api.vulncheck.com/v3/index/threat-actors`

Sample Response:


```
{
  "_benchmark": 0.135262,
  "_meta": {
    "timestamp": "2025-02-11T18:36:23.268737444Z",
    "index": "threat-actors",
    "limit": 100,
    "total_documents": 348,
    "sort": "_id",
    "order": "asc",
    "next_cursor": "NDhlNzc1M2I1NzBhM2FjMDBlYTViZDFiZTliZWU1YWU="
  },
  "data": [
    {
      "threat_actor_name": "Gold Southfield",
      "date_added": "2019-09-24",
      "mitre_id": "G0115",
      "misp_id": "262c8537-1cdb-4297-aa3e-1410164160bf",
      "malpedia_url": "https://malpedia.caad.fkie.fraunhofer.de/actor/
gold_southfield",
      "cve_references": [
        {
          "url": "https://www.secureworks.com/research/revil-sodinokibi-
ransomware",
          "date_added": "2019-09-24",
          "cve": [
            "CVE-2018-8453"
          ]
        },
        {
          "url": "https://www.secureworks.com/blog/revil-the-gandcrab-
connection",
          "date_added": "2019-09-24",
          "cve": [
            "CVE-2018-8453"
          ]
        }
      ],
      "country": "KP",
      "mitre_attack_group": {
        "name": "GOLD SOUTHFIELD",
```

```
        "aliases": [
          "GOLD SOUTHFIELD"
        ],
        "description": "GOLD SOUTHFIELD is a financially motivated threat group
active since at least 2019 that operates the REvil Ransomware-as-a Service
(RaaS). GOLD SOUTHFIELD provides backend infrastructure for affiliates
recruited on underground forums to perpetrate high value deployments.",
        "techniques": [
          {
            "technique_id": "T1133",
            "technique_name": "External Remote Services",
            "tactic": [
              "persistence",
              "initial-access"
            ]
          },
          {
            "technique_id": "T1190",
            "technique_name": "Exploit Public-Facing Application",
            "tactic": [
              "initial-access"
            ]
          },
          {
            "technique_id": "T1195",
            "technique_name": "Supply Chain Compromise",
            "sub_technique": "002",
            "sub_technique_name": "Compromise Software Supply Chain",
            "tactic": [
              "initial-access"
            ]
          },
          {
            "technique_id": "T1199",
            "technique_name": "Trusted Relationship",
            "tactic": [
              "initial-access"
            ]
          },
          {
            "technique_id": "T1566",
            "technique_name": "Phishing",
            "tactic": [
              "initial-access"
            ]
          }
        ]
      },
      "misp_threat_actor": {
        "description": "GOLD SOUTHFIELD is a financially motivated
```

```
cybercriminal threat group that authors and operates the REvil (aka Sodinokibi)
ransomware on behalf of various affiliated threat groups. Operational since
April 2019, the group obtained the GandCrab source code from GOLD GARDEN, the
operators of GandCrab that voluntarily withdrew their ransomware from
underground markets in May 2019. GOLD SOUTHFIELD is responsible for authoring
REvil and operating the backend infrastructure used by affiliates (also called
partners) to create malware builds and to collect ransom payments from victims.
CTU researchers assess with high confidence that GOLD SOUTHFIELD is a former
GandCrab affiliate and continues to work with other former GandCrab
affiliates.",
        "meta": {
          "cfr-suspected-state-sponsor": "North Korea",
          "cfr-suspected-victims": [
            "Ministry of Unification"
          ],
          "cfr-target-category": [
            "Government"
          ],
          "cfr-type-of-incident": [
            "Espionage"
          ],
          "country": "KP",
          "refs": [
            "http://www.secureworks.com/research/threat-profiles/gold-
southfield",
            "https://www.secureworks.com/research/revil-sodinokibi-ransomware",
            "https://www.secureworks.com/blog/how-cyber-adversaries-are-
adapting-to-exploit-the-global-pandemic",
            "https://www.secureworks.com/blog/revil-the-gandcrab-connection"
          ]
        },
        "value": "GOLD SOUTHFIELD"
      },
      "mitre_group_cti": {
        "id": "G0115",
        "aliases": [
          "GOLD SOUTHFIELD",
          "Pinchy Spider"
        ],
        "description": "[GOLD SOUTHFIELD](https://attack.mitre.org/groups/
G0115) is a financially motivated threat group active since at least 2018 that
operates the [REvil](https://attack.mitre.org/software/S0496) Ransomware-as-a
Service (RaaS). [GOLD SOUTHFIELD](https://attack.mitre.org/groups/G0115)
provides backend infrastructure for affiliates recruited on underground forums
to perpetrate high value deployments. By early 2020, [GOLD SOUTHFIELD](https://
attack.mitre.org/groups/G0115) started capitalizing on the new trend of
stealing data and further extorting the victim to pay for their data to not get
publicly leaked.(Citation: Secureworks REvil September 2019)(Citation:
Secureworks GandCrab and REvil September 2019)(Citation: Secureworks GOLD
SOUTHFIELD)(Citation: CrowdStrike Evolution of Pinchy Spider July 2021)",
        "references": [
```

```
          {
            "source_name": "mitre-attack",
            "url": "https://attack.mitre.org/groups/G0115",
            "external_id": "G0115"
          },
          {
            "source_name": "Pinchy Spider",
            "description": "(Citation: CrowdStrike Evolution of Pinchy Spider
July 2021)"
          },
          {
            "source_name": "Secureworks REvil September 2019",
            "url": "https://www.secureworks.com/research/revil-sodinokibi-
ransomware",
            "description": "Counter Threat Unit Research Team. (2019, September
24). REvil/Sodinokibi Ransomware. Retrieved August 4, 2020."
          }
        ]
      },
      "vendors_and_products_targeted": [
        {
          "vendor": "Microsoft",
          "product": "Win32k"
        },
        {
          "vendor": "Oracle",
          "product": "WebLogic Server"
        },
        {
          "vendor": "Citrix",
          "product": "Application Delivery Controller (ADC), Gateway, and SD-
WAN WANOP Appliance"
        },
        {
          "vendor": "Ivanti",
          "product": "Connect Secure and Policy Secure"
        }
      ],
      "_timestamp": "2025-02-10T20:57:24.310088Z"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed based on each item with the API's response `.data` array.

> The following fields are added to the description for each threat actor: `.misp_threat_actor.description or .mitre_attack_group.description or .mitre_group_cti.description, cve_references[].*, .vendor_names_for_threat_actors[].threat_actor_name, .vendor_names_for_threat_actors[].vendor_name, .mitre_group_cti.aliases[], .misp_threat_actor.meta.synonyms, .mitre_attack_group.aliases`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.threat_actor_name`	Adversary.Name	Adversary	`._timestamp`	`Gold Southfield`	N/A
`.misp_threat_actor.meta ['cfr-suspected-state-sponsor']`	Adversary.Attribute	State Sponsor	`._timestamp`	`North Korea`	N/A
`.misp_threat_actor.meta ['cfr-suspected-victims'][]`	Adversary.Attribute	Victim	`._timestamp`	`Ministry of Unification`	N/A
`.misp_threat_actor.meta ['cfr-target-category'][]`	Adversary.Attribute	Target Sector	`._timestamp`	`Government`	N/A
`.misp_threat_actor.meta ['cfr-type-of-incident'][]`	Adversary.Attribute	Tactic	`._timestamp`	`Espionage`	N/A
`.misp_threat_actor.meta.country`	Adversary.Attribute	Country Code	`._timestamp`	`KP`	N/A
`.country`	Adversary.Attribute	Country Code	`._timestamp`	`KP`	N/A
`.vendors_and_products_targeted[].vendor`	Adversary.Attribute	Target Vendor	`._timestamp`	`Microsoft`	N/A
`.vendors_and_products_targeted[].product`	Adversary.Attribute	Target Product	`._timestamp`	`Win32k`	N/A
`.mitre_attack_group.techniques[].technique_id, .mitre_attack_group.techniques[].technique_name`	Related Attack-Pattern.Value	Attack-Pattern	`._timestamp`	`T1195 - Supply Chain Compromise`	N/A
`.mitre_attack_group.techniques[].sub_technique, .mitre_attack_group.techniques[].sub_technique_name`	Related Attack-Pattern.Value	Attack-Pattern	`._timestamp`	`T1195.002 - Compromise Software Supply Chain`	N/A
`.cve_references[].cve`	Related Indicator/ Vulnerability.Value	CVE/Vulnerability	`._timestamp`	`CVE-2018-8453`	Ingested object

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					type depends on user-field selection

VulnCheck Vulnerabilities

The VulnCheck Vulnerabilities feed ingests vulnerability data from VulnCheck's `vulncheck-nvd2` index. This API provides aggregated data from VulnCheck's team, NVD, and other sources. The data includes information such as the vulnerability's CVSS metrics, relevant CWEs, references, and more.

`GET https://api.vulncheck.com/v3/index/vulncheck-nvd2`

Sample Response:


```
{
  "_benchmark": 0.084083,
  "_meta": {
    "timestamp": "2025-02-11T20:37:05.011728753Z",
    "index": "vulncheck-nvd2",
    "limit": 10,
    "total_documents": 18755,
    "sort": "_id",
    "order": "asc",
    "next_cursor": "Q1ZFLTIwMTYtMTA0MDg="
  },
  "data": [
    {
      "id": "CVE-2002-20002",
      "sourceIdentifier": "cve@mitre.org (MITRE)",
      "vulnStatus": "Awaiting Analysis",
      "published": "2025-01-02T05:15:06.43Z",
      "lastModified": "2025-01-02T05:15:06.43Z",
      "descriptions": [
        {
          "lang": "en",
          "value": "The Net::EasyTCP package before 0.15 for Perl always uses
Perl's builtin rand(), which is not a strong random number generator, for
cryptographic keys."
        },
        {
          "lang": "es",
          "value": "El paquete Net::EasyTCP anterior a la versión 0.15 para
Perl siempre utiliza el rand() integrado de Perl, que no es un generador de
números aleatorios potente, para las claves criptográficas."
        }
      ],
      "references": [
        {
          "status": "active",
          "lang": "cn",
          "name": "MetaCPAN Net::EasyTCP 安全漏洞
          "url": "http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?
CNNVD=CNNVD-202501-088",
          "refsource": "CNNVD",
```

```
          "tags": [
            "Government Advisory",
            "VDB Entry"
          ],
          "date_added": "2025-01-02T00:00:00Z"
        },
        {
          "status": "active",
          "lang": "en",
          "url": "https://github.com/github/advisory-database/blob/main/
advisories/unreviewed/2025/01/GHSA-pm3j-mqcc-rjqr/GHSA-pm3j-mqcc-rjqr.json",
          "refsource": "GHSA",
          "tags": [
            "VDB Entry"
          ],
          "date_added": "2025-01-02T06:30:47Z"
        },
        {
          "url": "https://github.com/briandfoy/cpan-security-advisory/issues/
184",
          "source": "cve@mitre.org (MITRE)",
          "refsource": "MISC",
          "date_added": "1970-01-01T00:00:00Z"
        },
        {
          "url": "https://metacpan.org/release/MNAGUIB/EasyTCP-0.15/view/
EasyTCP.pm",
          "source": "cve@mitre.org (MITRE)",
          "refsource": "MISC",
          "date_added": "1970-01-01T00:00:00Z"
        },
        {
          "url": "https://metacpan.org/release/MNAGUIB/EasyTCP-0.26/changes",
          "source": "cve@mitre.org (MITRE)",
          "refsource": "MISC",
          "date_added": "1970-01-01T00:00:00Z"
        },
        {
          "status": "active",
          "lang": "en",
          "name": "Security Bulletin 8 Jan 2025",
          "url": "https://www.csa.gov.sg/alerts-advisories/security-bulletins/
2025/sb-2025-002",
          "refsource": "SINGCERT",
          "tags": [
            "Government Advisory"
          ],
          "date_added": "2025-01-08T00:00:00Z"
        },
        {
```

```
          "status": "active",
          "lang": "en",
          "url": "https://www.cve.org/CVERecord?id=CVE-2002-20002",
          "refsource": "VULNCHECK-CVELIST-V5",
          "tags": [
            "VDB Entry"
          ],
          "date_added": "2025-01-02T00:00:00Z"
        },
        {
          "status": "active",
          "lang": "en",
          "url": "https://github.com/cisagov/vulnrichment/blob/develop/
2002/20xxx/CVE-2002-20002.json",
          "refsource": "VULNRICHMENT",
          "tags": [
            "Government Advisory"
          ],
          "date_added": "2025-01-02T00:00:00Z"
        }
      ],
      "metrics": {
        "cvssMetricV31": [
          {
            "source": "cve@mitre.org (MITRE)",
            "type": "Secondary",
            "cvssData": {
              "version": "3.1",
              "vectorString": "CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N",
              "attackVector": "NETWORK",
              "attackComplexity": "HIGH",
              "privilegesRequired": "NONE",
              "userInteraction": "NONE",
              "scope": "CHANGED",
              "confidentialityImpact": "LOW",
              "integrityImpact": "LOW",
              "availabilityImpact": "NONE",
              "baseScore": 5.4,
              "baseSeverity": "MEDIUM",
              "temporalScore": 0,
              "environmentalScore": 0
            },
            "exploitabilityScore": 2.2,
            "impactScore": 2.7
          }
        ],
        "temporalCVSSV31Secondary": [
          {
            "version": "3.1",
            "vectorString": "E:U/RL:X/RC:C",
```

```
          "exploitCodeMaturity": "UNPROVEN",
          "remediationLevel": "NOT_DEFINED",
          "reportConfidence": "CONFIRMED",
          "temporalScore": 4.9,
          "associatedBaseMetricV3": {
            "source": "cve@mitre.org (MITRE)",
            "type": "Secondary",
            "baseScore": 5.4
          }
        }
      ],
      "ssvc": [
        {
          "source": "CISA-ADP",
          "exploitation": "NONE",
          "automatable": "NO",
          "technicalImpact": "PARTIAL"
        }
      ],
      "epss": {
        "epss_score": 0.00045,
        "epss_percentile": 0.17779,
        "last_modified": "2025-02-11T09:40:52.212986Z"
      }
    },
    "mitreAttackTechniques": [
      {
        "domain": "Enterprise",
        "id": "T1190",
        "name": "Exploit Public-Facing Application",
        "subtechnique": false,
        "tactics": [
          "initial-access"
        ],
        "url": "https://attack.mitre.org/techniques/T1190"
      }
    ],
    "relatedAttackPatterns": [
      {
        "capec_id": "CAPEC-66",
        "capec_name": "SQL Injection",
        "capec_url": "https://capec.mitre.org/data/definitions/66.html",
        "lang": "en"
      }
    ],
    "weaknesses": [
      {
        "source": "cve@mitre.org (MITRE)",
        "type": "Secondary",
        "description": [
```

```
            {
              "lang": "en",
              "value": "CWE-338",
              "name": "Use of Cryptographically Weak Pseudo-Random Number
Generator (PRNG)",
              "url": "https://cwe.mitre.org/data/definitions/338.html"
            }
          ]
        }
      ],
      "vcVulnerableCPEs": [
        "cpe:2.3:a:mikexstudios:xcomic:0.8.0:*:*:*:*:*:*:*"
      ],
      "vulnerableCPEs": [
        "cpe:2.3:o:foscam:ip_camera_firmware:11.37.2.49:*:*:*:*:*:*:*"
      ],
      "STATUS": "Awaiting Analysis",
      "categorization": {
        "tags": [
          "Firmware"
        ]
      },
      "date_added": "2025-01-02T00:00:00Z",
      "_timestamp": "2025-01-28T03:55:46.66662198Z",
      "documentGenerationDate": "2025-02-11T11:46:29.277932111Z"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed based on each item within the API's response `.data` array.

> The following fields are added to the description for each CVE: `.descriptions[].value, .metrics.cvssMetricV40[].*` or `.metrics.cvssMetricV31[].*` or `.metrics.cvssMetricV2[].*, .references[].name, .references[].lang, .references[].url, .references[].tags, .references[].date_added, .vcVulnerableCPEs[]`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.id`	Indicator/ Vulnerability.Value	CVE/Vulnerability	`.published`	`CVE-2002-20002`	Ingested object type depends on user-field selection
`.categorization.tags[]`	Indicator/ Vulnerability.Tag	N/A	N/A	`Firmware`	N/A
`.mitreAttackTechniques[].id`, `.mitreAttackTechniques[].name`	Related Attack-Pattern.Value	Attack-Pattern	`.published`	`T1190 - Exploit Public-Facing Application`	User-configurable
`.mitreAttackTechniques[].url`	Related Attack-Pattern.Attribute	External Reference	`.published`	`https://attack.mitre.org/techniques/T1190`	N/A
`.relatedAttackPatterns[].capec_id`, `.relatedAttackPatterns[].capec_name`	Related Attack-Pattern.Value	Attack-Pattern	`.published`	`CAPEC-66 - SQL Injection`	User-configurable
`.relatedAttackPatterns[].url`	Related Attack-Pattern.Attribute	External Reference	`.published`	`https://capec.mitre.org/data/definitions/66.html`	N/A
`.weaknesses[].description[].value`	Related Vulnerability	Vulnerability	`.published`	`CWE-338`	User-configurable
`.weaknesses[].description[].url`	Related Vulnerability.Attribute	External Reference	`.published`	`https://cwe.mitre.org/data/definitions/338.html`	N/A
`.vcVulnerableCPEs[]`	Attribute	Affected Vendor	`.published`	`mikexstudios`	Parsed from the CPE string
`.vcVulnerableCPEs[]`	Attribute	Affected Product	`.published`	`xcomic`	Parsed from the CPE string
`.vulnerableCPEs[]`	Attribute	Affected Vendor	`.published`	`foscam`	Parsed from the CPE string
`.vulnerableCPEs[]`	Attribute	Affected Product	`.published`	`ip_camera_firmware`	Parsed from the CPE string
`.STATUS`	Attribute	VulnCheck Status	`.published`	`Awaiting Analysis`	Updatable
`.metrics.epss.epss_score`	Attribute	EPSS Score	`.published`	`0.97374`	Updatable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.metrics.epss.epss_percentile`	Attribute	EPSS Percentile	`.published`	`0.99961`	Updatable
`.metrics.{CVSS Metric Version}.vectorString`	Attribute	CVSSv{#} Vector String	N/A	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:N`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.attackVector`	Attribute	CVSSv{#} Attack Vector	N/A	`NETWORK`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.accessVector`	Attribute	CVSSv{#} Access Vector	N/A	N/A	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.attackComplexity`	Attribute	CVSSv{#} Attack Complexity	N/A	`HIGH`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.accessComplexity`	Attribute	CVSSv{#} Access Complexity	N/A	N/A	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.privilegesRequired`	Attribute	CVSSv{#} Privileges Required	N/A	`NONE`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.userInteraction`	Attribute	CVSSv{#} User Interaction	N/A	`NONE`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.scope`	Attribute	CVSSv{#} Scope	N/A	`CHANGED`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.confidentialityImpact`	Attribute	CVSSv{#} Confidentiality Impact	N/A	`LOW`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.integrityImpact`	Attribute	CVSSv{#} Integrity Impact	N/A	`LOW`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.availabilityImpact`	Attribute	CVSSv{#} Availability Impact	N/A	`NONE`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.baseSeverity`	Attribute	CVSSv{#} Base Severity	N/A	`MEDIUM`	Updatable. User-configurable
`.metrics.{CVSS Metric`	Attribute	CVSSv{#} Temporal Score	N/A	`0`	Updatable. User-configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`Version}.cvssData.temporalScore`					
`.metrics.{CVSS Metric Version}.cvssData.baseScore`	Attribute	CVSSv{#} Base Score	N/A	`5.4`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.cvssData.environmentalScore`	Attribute	CVSSv{#} Environmental Score	N/A	`0`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.exploitabilityScore`	Attribute	CVSSv{#} Exploitability Score	N/A	`2.2`	Updatable. User-configurable
`.metrics.{CVSS Metric Version}.impactScore`	Attribute	CVSSv{#} Impact Score	N/A	`2.7`	Updatable. User-configurable
`.metrics.{CVSS Temporal Metric Version}.exploitability`	Attribute	CVSSv{#} Exploit Code Maturity	N/A	`UNPROVEN`	Updatable. User-configurable
`.metrics.{CVSS Temporal Metric Version}.remediationLevel`	Attribute	CVSSv{#} Remediation Level	N/A	`NOT_DEFINED`	Updatable. User-configurable
`.metrics.{CVSS Temporal Metric Version}.reportConfidence`	Attribute	CVSSv{#} Report Confidence	N/A	`CONFIRMED`	Updatable. User-configurable
`.metrics.{temporalCVSSV40/temporalCVSSV40Secondary}.baseThreatScore`	Attribute	CVSSv40 Base Threat Score	N/A	N/A	Updatable. User-configurable
`.metrics.{temporalCVSSV40/temporalCVSSV40Secondary}.baseThreatSeverity`	Attribute	CVSSv40 Base Threat Severity	N/A	N/A	Updatable. User-configurable

The values for {CVSS Metric Version} can be: `cvssMetricV2, cvssMetricV31` or `cvssMetricV4`. The values for {CVSS Temporal Metric Version} can be: `temporalCVSSV2, temporalCVSSV2Secondary, temporalCVSSV31, temporalCVSSV31Secondary, temporalCVSSV40, temporalCVSSV40Secondary`. Secondary is used in case primary is not present.

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.

VulnCheck Exploits

METRIC	RESULT
Run Time	2 minutes
Indicators	464
Indicator Attributes	4,616
Adversaries	118
Malware	107

VulnCheck Threat Actors

METRIC	RESULT
Run Time	1 minute
Indicators	87
Adversaries	6
Adversary Attributes	131

VulnCheck Vulnerabilities

METRIC	RESULT
Run Time	22 minutes
Indicators	14,376
Indicator Attributes	145,930
Attack Patterns	78
Attack Pattern Attributes	78

Change Log

- **Version 1.0.0**
  - Initial release