ThreatQuotient

VERIS Community Database CDF User Guide

Version 1.0.0

October 18, 2023

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	>= 4.33.0
Support Tier	ThreatQ Supported

Introduction

The VERIS Community Database is a valuable source of information about reported known data breaches. More information about this data source can be found at VERIS . Within ThreatQ it can provide context about the motivations, tools and vulnerabilities used by adversaries to breach real organizations.

> The data is licensed under the Create Commons Attribution-ShareAlike 4.0 Public license.

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. If prompted, select the individual feeds to install and click **Install**. 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 **OSINT** option from the *Category* dropdown (optional).

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

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

PARAMETER	DESCRIPTION
Save CVE Data As	A required multi-select field that can be configured to ingest VERIS CVE data as CVE Indicators, Vulnerabilities, or both. Ingest CVE Data as CVE Indicators is the default selection.

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

Veris VCDB

`GET https://raw.githubusercontent.com/vz-risk/VCDB/master/data/joined/vcdb.json.zip`

Sample Response:

```
{
        "incident_id": "36d6e590-9715-11e7-a11c-5542f7e3819f",
        "confidence": "High",
        "reference": "https://www.wired.co.uk/article/nhs-cyberattack-ransomware-security; https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/; https://www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/; http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/; http://www.wired.co.uk/article/nhs-trusts-affected-by-cyber-attack",
        "targeted": "Opportunistic",
        "attribute": {
            "integrity": {
                "variety": ["Modify data", "Software installation"]
            },
            "availability": {
                "duration": { "unit": "Unknown" },
                "notes": "Given the number of victims, this had a wide variety of values.",
                "variety": ["Obscuration"]
            },
            "confidentiality": {
                "data_victim": ["Patient"],
                "state": ["Stored"],
                "data": [{ "variety": "Medical" }],
                "data_disclosure": "Yes"
            }
        },
        "discovery_method": { "external": { "variety": ["Actor disclosure"] } },
        "actor": {
            "external": {
                "motive": ["Financial"],
                "country": ["Unknown"],
                "region": ["000000"],
                "variety": ["Unaffiliated"]
            }
        },
        "summary": "At least 16 hospitals in the United Kingdom are being
```

```
forced to divert emergency patients today after computer systems there were
infected with ransomware, a type of malicious software that encrypts a
victim\u2019s documents, images, music and other files unless the victim pays
for a key to unlock them.  The ransomware is using an NSA exploit leaked by The
Shadow Brokers, and has made tens of thousands of victims worldwide, including
the Russian Interior Ministry, Chinese universities, Hungarian telcos, FedEx
branches, and more.  Cybersecurity firm Avast said it had identified more than
75,000 ransomware attacks in 99 countries, making it one of the broadest and
most damaging cyberattacks in history. Avast said the majority of the attacks
targeted Russia, Ukraine and Taiwan. But U.K. hospitals, Chinese universities
and global firms like Fedex (FDX) also reported they had come under assault.",
        "source_id": "vcdb",
        "security_incident": "Confirmed",
        "plus": {
            "github": "9521",
            "dbir_year": 2018,
            "data_abuse": "Yes",
            "created": "2017-10-25T22:54:34.723Z",
            "sub_source": "phidbr",
            "modified": "2017-10-26T08:01:05.823Z",
            "asset_os": ["Windows"],
            "analysis_status": "Validated",
            "master_id": "efb0510a-365a-4db1-bcbe-c1b6315d6e39",
            "analyst": "swidup"
        },
        "asset": {
            "assets": [
                { "variety": "S - Web application" },
                { "variety": "S - Database" }
            ],
            "cloud": ["Unknown"]
        },
        "victim": {
            "victim_id": "Plymouth Hospitals NHS Trust",
            "country": ["GB"],
            "region": ["150154"],
            "locations_affected": 16,
            "employee_count": "Large",
            "industry": "622110",
            "secondary": {
                "victim_id": [
                    "Telefonica",
                    "Gas Natural",
                    "Iberdrola ",
                    "Santander bank",
                    "KPMG",
                    "Fedex",
                    "Russia's Interior Ministry",
                    "Megafon",
                    "Honda Motor Company",
                    "Mid Essex Clinical Commissioning Group",
                    "Wingate Medical Centre",
                    "NHS Liverpool Community Health NHS Trust",
                    "East Lancashire Hospitals NHS Trust",
                    "George Eliot Hospital NHS Trust in Nuneaton,
Warwickshire",
                    "Blackpool Teaching Hospitals NHS Trust",
                    "St Barts Health NHS Trust",
                    "Derbyshire Community Health Services",
                    "East and North Hertfordshire Clinical Commissioning
Group",
                    "East and North Hertfordshire Hospitals NHS Trust",
                    "Sherwood Forest NHS Trust",
                    "Nottinghamshire Healthcare",
                    "Burton Hospitals NHS Foundation Trust",
                    "United Lincolnshire Hospitals NHS Trust",
                    "Colchester General Hospital",
                    "Cheshire and Wirral Partnership NHS Foundation Trust",
                    "Northern Lincolnshire and Goole NHS Foundation Trust",
                    "North Staffordshire Combined Healthcare NHS Trust",
                    "Cumbria Partnership NHS Foundation Trust",
                    "Morecombe Bay NHS Trust",
                    "University Hospitals of North Midlands NHS Trust",
                    "NHS Hampshire Hospitals",
                    "Kent Community Health NHS Foundation Trust",
                    "The Royal Berkshire Hospital",
                    "University Hospital of Hartlepool",
                    "University Hospital of North Tees",
                    "Carlise's Cumberland Infirmary",
                    "West Cumberland Hospital in Whitehaven",
                    "Penrith Community Hospital",
                    "Hull Royal Infirmary",
                    "Castle Hill Hospital",
                    "Morecambe Bay NHS Trust",
                    "Broomfield Hospital",
                    "St Michael's Hospital",
                    "St Peter's Hospital",
                    "Braintree Community Hospital",
                    "Basingstoke and North Hampshire Hospital",
                    "Lister Hospital",
                    "Hertford County Hospital",
                    "Mount Vernon Cancer Centre ",
                    "QEII Hospita",
                    "Waterloo Medical Centre",
                    "Royal Preston Hospital",
                    "Chorley Hospital",
                    "Barts Hospital",
                    "Royal London Hospital",
                    "Whipps Cross University Hospital",
                    "Grantham Hospital",
                    "Lincoln County Hospital",
                    "Pilgrim Hospital"
                ]
            }
        },
        "timeline": {
            "incident": { "year": 2017, "month": 5 },
            "discovery": { "unit": "Hours" },
            "containment": { "unit": "Weeks" }
        },
        "action": {
            "malware": {
                "vector": ["Network propagation"],
                "variety": ["Ransomware"]
            }
        },
        "schema_version": "1.3.4"
    }
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.victim.victim_id	Event.Title	Incident	.timeline.incident	Ohio Department of Job and Family Services breach (a1e8f)	
.action.malware.cve	Indicator.Value	CVE	.timeline.incident	CVE-1234-2344	
.action.malware.cve	Vulnerability.Value	N/A	.timeline.incident	CVE-1234-2344	
.action.hacking.cve	Indicator.Value	CVE	.timeline.incident	CVE-1234-1223	
.action.hacking.cve	Vulnerability.Value	N/A	.timeline.incident	CVE-1234-1223	
.actor.external.name	Adversary.Name	N/A	.timeline.incident	EvilSparrow	
.action.malware.name	Malware.Value	N/A	.timeline.incident	Hydraq	
.summary	Event.Description	N/A	N/A	Hackers part of the Anonymous-affiliated k0detec collective havegained unauthorized access to the systems of MOAB Training International.	
.victim.country	Event.Attribute	Target Country Code	.timeline.incident	UK	
.victim.state	Event.Attribute	Target Country State	.timeline.incident	MD	
.actor.external.country	Event.Attribute	Source Country Code	.timeline.incident	FR	
.notes	Event.Attribute	Notes	.timeline.incident	497 Victim National Organization for Marriage collateral: Internal Revenue Service number of employees/volunteers: 7 naics 813990 Incident 2012-03-30 Notification 2012-03-30 (public brag) Discovery: Posted on the website Actor: Human Rights Campaign	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				Motive: ideological vector it could not be determined exactly how the IRS documents were accessed and provided to HRC Data confidential tax documents Names of donors Impact IRS Pays Nonprofit Group $50,000 Settlement for Leaking Documents	
.reference	Event.Attribute	Reference URL	.timeline.incident	http://news.softpedia.com/news/Syrian-Arab-News-Agency-Disrupted-by-Cyberattack-382945.shtml	
.victim.victim_id	Event.Attribute	Victim	.timeline.incident	Mackenzie Health	
.action.malware.name	Event.Attribute	Malware	.timeline.incident	Rocra	
.actor.external.motive	Event.Attribute	Motivation	.timeline.incident	Financial	
.actor.external.variety	Event.Attribute	Actor Variety	.timeline.incident	Activist	
.incident_id	Event.Attribute	VCDB Incident ID	.timeline.incident	0008DADB-E83D-4278-A19A-CEE01610CF43	
.action.hacking.vector	Event.Attribute	Hacking Vector	.timeline.incident	Web application	
.action.hacking.notes	Event.Attribute	Hacking Notes	.timeline.incident	it was as easy as using a commonly used password, that is often the default code that never gets changed	
.discovery_notes	Event.Attribute	Discovery Notes	.timeline.incident	a call from Pakistan was traced to the officer.	
.action.hacking.variety	Event.Attribute	Hacking Methods	.timeline.incident	Use of stolen creds	
.action.malware.notes	Malware.Attribute	Notes	.timeline.incident	They found out about the error a month ago, but no word on when they shared the data.	
.action.malware.variety	Malware.Attribute	Capability	.timeline.incident	Destroy data	
.incident_id	Malware.Attribute / Indicator.Attribute / Vulnerability.Attribute	Used in Breach ID	.timeline.incident	0CE4D1F7-FB16-43CE-8FE8-2D50B6C9C63C	
.actor.external.notes	Adversary.Attribute	Notes	.timeline.incident	asset.assets was empty and removed by script.	
.actor.external.motive	Adversary.Attribute	Motive	.timeline.incident	Financial	

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.

VERIS Community Database

Scheduled run ingesting CVE data as CVE Indicators (default configuration):

METRIC	RESULT
Run Time	17 minutes
Adversaries	128
Adversary Attributes	217
Events	8,512
Event Attributes	72,249
Indicators	22
Indicator Attributes	592
Malware	40
Malware Attributes	402

Scheduled run ingesting CVE data as CVE Indicators and Vulnerabilities:

METRIC	RESULT
Run Time	18 minutes

METRIC	RESULT
Adversaries	128
Adversary Attributes	217
Events	8,512
Event Attributes	72,249
Indicators	22
Indicator Attributes	592
Malware	40
Malware Attributes	402
Vulnerabilities	22
Vulnerability Attributes	592

Change Log

- **Version 1.0.0**
    - Initial release