ThreatQuotient

CTM360 HackerView CDF User Guide

Version 1.0.0

June 21, 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.

Copyright © 2023 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	1.0.0
Compatible with ThreatQ Versions	>= 4.58.1
Support Tier	ThreatQ Supported

Introduction

The CTM360 HackerView CDF provides a feed that ingests incidents and related indicators of compromise from CTM360 HackerView.

The integration provides the following feed:

- **CTM360 HackerView** - ingests incidents with related indicators of compromise.

The integration ingests the following system objects:

- Events - type Incident
- Indicators - IP Addresses and FQDNs

Prerequisites

An API Key for CTM360 HackerView is required by the 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. 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.

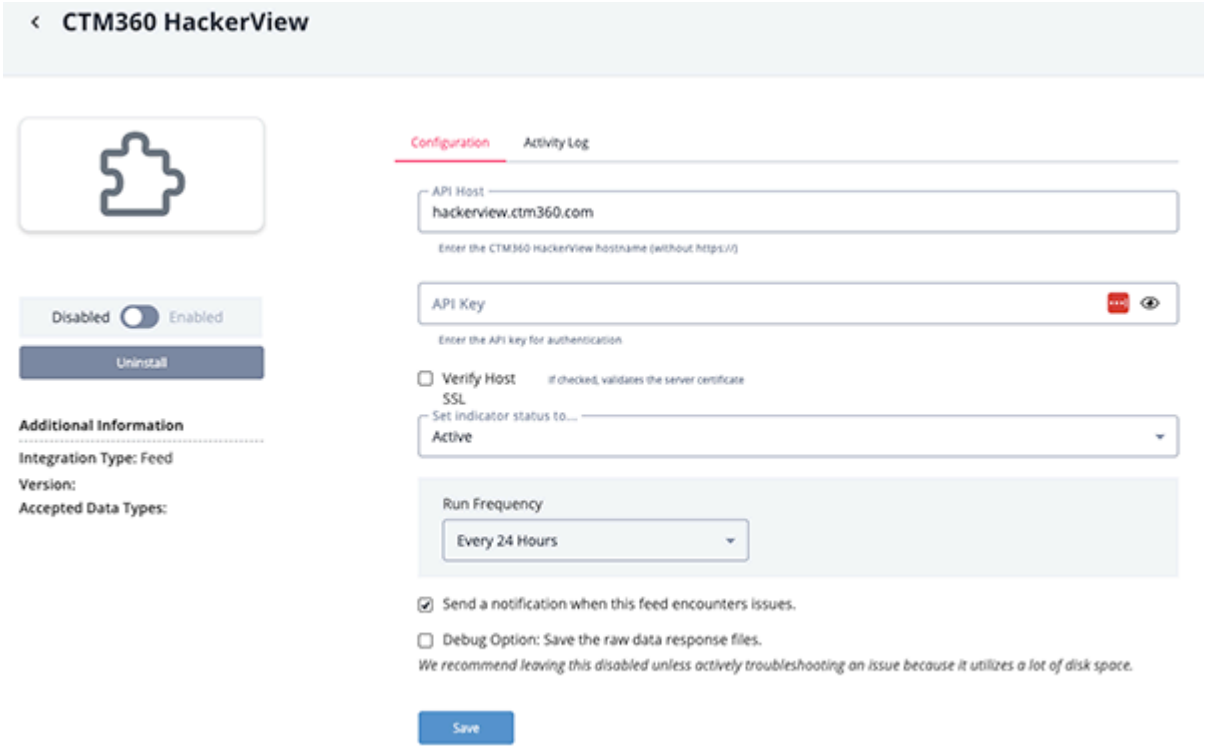
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

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

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

PARAMETER	DESCRIPTION
API Host	Enter the CTM360 hostname without `https://`. The default is **hackerview.ctm360.com**.
API Key	Enter your API Key for authentication.
Verify Host SSL	When enabled, the integration will validate the server certificate.



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

The CTM360 HackerView feed returns the incidents and related IOCs (FQDN and URL).

`GET https://hackerview.ctm360.com/api/v2/issues`

Sample Response:


```
{
  "success": true,
  "message": "Ok",
  "issues": [
    {
      "severity": "medium",
      "fixing_effort": "Moderate",
      "issue_type": [
        "IT Hygiene"
      ],
      "issue_category": [
        "IP Reputation"
      ],
      "potential_attack_type": [],
      "cwe": [],
      "issue_name": "IP Blacklisted",
      "meta": {
        "first_seen": "23-04-2023 23:41:54",
        "last_seen": "23-04-2023 23:41:54",
        "environments": [
          "Web servers"
        ],
        "hosts": [
          "gateway.example.com"
        ],
        "ip": "223.197.225.224",
        "ip_type": "dedicated",
        "ticket_id": "HVI-12887306",
        "business_unit": [],
        "technologies": [
          "Lighttpd"
        ],
        "discovery_source": [
          "ssl_certificate"
        ],
        "asset_type": "ip",
        "asset": "223.197.225.224",
        "brand": "ISS Enterprise"
      },
      "detail": "[\"224.225.197.223.b.barracudacentral.org\",
\"224.225.197.223.spam.dnsbl.sorbs.net\"]",
      "progress_status": "New",
```

```
      "status": "active",
      "assigned_to": "unassigned",
      "potential_impact": [],
      "hackerview_link": "https://hackerview.ctm360.com/issues/issues_found/
overview/e2d72bc443a977751eb5f2e474464672/46"
    },
    {
      "severity": "medium",
      "fixing_effort": "Moderate",
      "issue_type": [
        "Vulnerability"
      ],
      "issue_category": [
        "Common Vulnerabilities"
      ],
      "potential_attack_type": [],
      "cwe": [],
      "issue_name": "Medium Severity CVE Detected",
      "cve_id": "CVE-2022-22707",
      "meta": {
        "first_seen": "23-04-2023 23:41:54",
        "last_seen": "23-04-2023 23:41:54",
        "environments": [
          "Web servers"
        ],
        "hosts": [
          "gateway.example.com"
        ],
        "ip": "223.197.225.224",
        "ip_type": "dedicated",
        "ticket_id": "HVI-59434846",
        "business_unit": [],
        "technologies": [
          "Lighttpd"
        ],
        "discovery_source": [
          "ssl_certificate"
        ],
        "asset_type": "ip",
        "asset": "223.197.225.224",
        "brand": "ISS Enterprise"
      },
      "detail": null,
      "progress_status": "New",
      "status": "active",
      "assigned_to": "unassigned",
      "potential_impact": [],
      "hackerview_link": "https://hackerview.ctm360.com/issues/issues_found/
overview/995e6cfb7dc33282f04323aeabdeae37/202222707"
    }
```

```
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
issues[].issue_type[]	Event Attributes	Issue Type	["Vulnerability"]	N/A	
issues[].issue_category[]	Event Attributes	Issue Category	["Common Vulnerabilities"]	N/A	
issues[].potential_attack_type[]	Event Attributes	Potential Attack Type	["Brute Force Attack", "Data Leakage"]	N/A	
issues[].potential_impact[]	Event Attributes	Potential Impact	["Loss of Integrity","Loss of Confidentiality","Loss of Availability","Access Control Issues"]	N/A	
issues[].severity	Event Attributes	Severity	medium	N/A	
issues[].fixing_effort	Event Attributes	Fixing Effort	Moderate	N/A	
issues[].hackerview_link	Event Attributes	HackerView Link	https://hackerview.ctm360.com/issues/issues_found/overview/995e6cfb7dc33282f04323aeabdeae37/202222707	N/A	
issues[].progress_status	Event Attributes	Progress Status	New	N/A	
issues[].status	Event Attributes	Status	active	N/A	
issues[].assigned_to	Event Attributes	Assigned To	unassigned	N/A	
issues[].meta{}.environments[]	Indicator Attributes	Environments	["Web servers"]	N/A	
issues[].meta{}.technologies[]	Indicator Attributes	Technologies	["Lighttpd"]	N/A	
issues[].meta{}.discovery_source[]	Indicator Attributes	Discovery Source	["ssl_certificate"]	N/A	
issues[].meta{}.brand[]	Indicator Attributes	Brand	ISS Enterprise	N/A	
issues[].meta{}.ip_type[]	Indicator Attributes	IP Type	Dedicated	N/A	
issues[].meta{}.last_seen[]	Indicator Attributes	Last Seen	27-04-2023 23:27:18	N/A	
issues[].meta{}.first_seen[]	Indicator Attributes	First Seen	27-04-2023 23:27:18	N/A	
issues[].meta{}.asset	Indicator	IP Address/FQDN	49.12.128.248	N/A	
issues[].cve_id	Indicator	CVE	CVE-2023-28625	N/A	
issues[].issue_name (Ticket ID: issues[].meta{}.ticket_id)	Event	Event Name	SSH Uses Weak Cipher (Ticket ID: HVI-57067419)	N/A	

Change Log

- **Version 1.0.0**
  - Initial release