ThreatQuotient

CTM360 - CYNA CDF

Version 1.0.0

February 18, 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	>= 6.5.0
Support Tier	ThreatQ Supported

Introduction

The CTM360 CYNA CDF integration ingests threat intelligence from CTM360 CYNA.

The integration provides the following feed:

- **CTM360 - CYNA** - ingests Reports from CTM360 CYNA.

The integration ingests Reports and Report Attributes into the ThreatQ platform.

Prerequisites

The following is required to utilize the integration:

- A CTM360 API Key.

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

   > 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.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

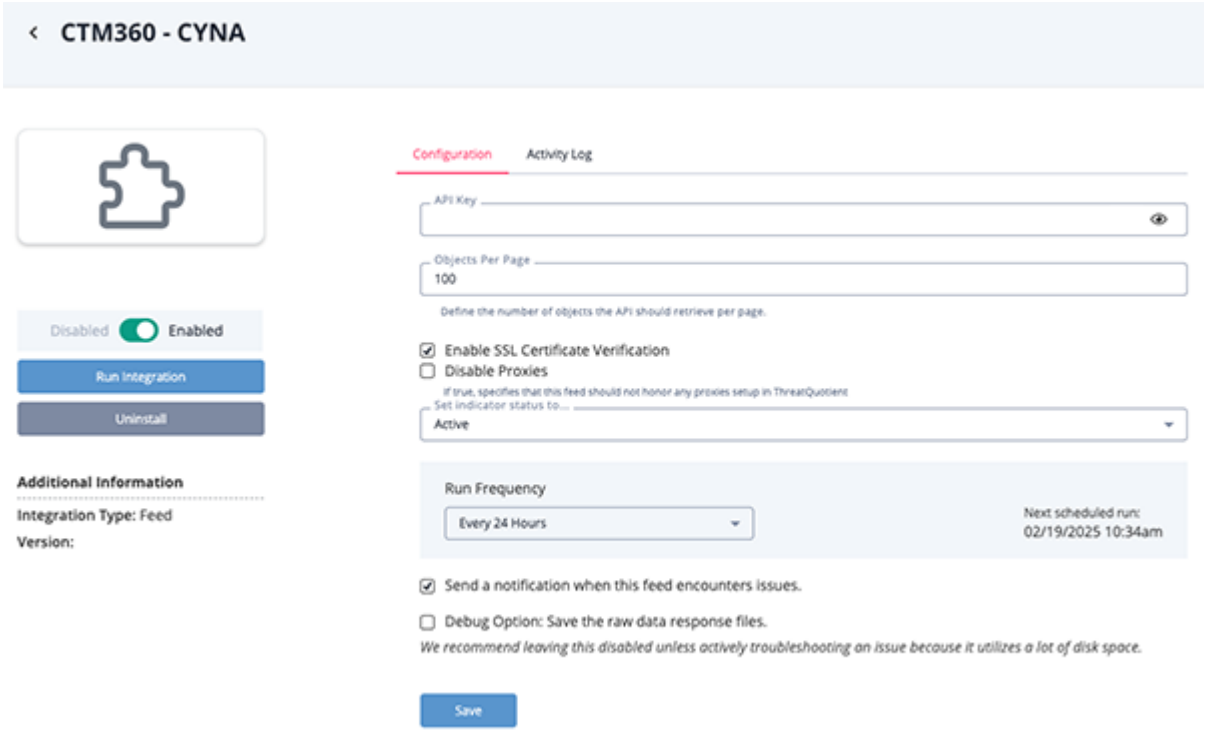
To configure the integration:

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 Key	Your CTM360 API Key.
Objects per Page	Enter the number of objects the API should retrieve per page.
Enable SSL Certificate Verification	Enable this parameter if the feed should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the feed should not honor proxies set in the ThreatQ UI.



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

CTM360 - CYNA

The CTM360 - CYNA feed retrieves a list of reports links and uses each link to fetch report content.

```
GET https://cyna.ctm360.com/api/v1/news
```

Sample Response:


```
{
  "statusCode": 200,
  "success": true,
  "data": [
    {
      "image": "https://apicms.thestar.com.my/uploads/images/
2025/02/10/3160289.jpg",
      "link": "https://www.thestar.com.my/news/nation/2025/02/10/company-
director-claims-trial-in-rm51mil-fraud-money-laundering-case",
      "description": "KUALA LUMPUR: A 60-year-old company director claimed
trial at the Sessions Court here to eight counts of cheating and money
laundering amounting to RM5.1mil linked to the purchase of gloves.",
      "title": "Company director claims trial in RM5.1mil fraud, money
laundering case",
      "published_date": "2025-02-10 07:25:00",
      "_id": "https://www.thestar.com.my/news/nation/2025/02/10/company-
director-claims-trial-in-rm51mil-fraud-money-laundering-case"
    },
    {
      "image": "https://blogger.googleusercontent.com/img/b/R29vZ2xl/
AVvXsEg68jko7KEBKAcKU_1Bp4k3JBw-OuDwvdHBzpLuOBtOVjjMC4RQt-
kfcRHKTNHMVtgElZ6kys6shIKXwtOZ6XZz2c8Gk1dibh8eGHZoAtyQQZATEGD1dwRC1ATda_B_4cJXJ
73kiWNb2UEO9gXeKF1dYMRZiXSULXuV3lex_qemTJSotpUPzfl0FRUPtCuw/s728-rw-e365/
ransomware.png",
      "link": "https://thehackernews.com/2025/02/8base-ransomware-data-leak-
sites-seized.html",
      "description": "Law enforcement seizes 8Base ransomware's dark web sites,
arresting four suspects linked to Phobos ransomware and $16M in global cyber
extortion.",
      "title": "8Base Ransomware Data Leak Sites Seized in International Law
Enforcement Operation",
      "published_date": "2025-02-11 07:03:00",
      "_id": "https://thehackernews.com/2025/02/8base-ransomware-data-leak-
sites-seized"
    }
  ],
  "total": {
    "value": 2464,
    "relation": "eq"
```

```
  },
  "size": 20,
  "nextSearchAfter":
"WzE3MzkxMTc4ODYwMDAsImh0dHBzOi8vd3d3LmRhd24uY29tL25ld3MvMTg5MDg1My90cnVtcC1zYXlzLW11c2std2lsbC1oZWxwLXVuY292ZXItaHVuZHJlZHMtb2YtYmlsbGlvbnMtaW4tdXMtZ292dC1mcmF1ZCJd",
  "hasMore": true
}
```


Fetch Report Content

The integration uses the `link` to fetch the report content

`GET https://www.thestar.com.my/news/nation/2025/02/10/company-director-claims-trial-in-rm51mil-fraud-money-laundering-case`

Sample Response:


```
{
    "BS4_Doctype": [
        "html"
    ],
    "html": [
        {
            "ATTR_dir": "ltr",
            "ATTR_lang": "en",
            "BS4_Comment": [
                "<head>\n<link href='https://www.blogger.com/dyn-css/
authorization.css?targetBlogID=4802841478634147276&amp;zx=b9ba197a-fb5b-4460-
ac0b-b18f2f734cc4' media='none' onload='if(media!
=&#39;all&#39;)media=&#39;all&#39;' rel='stylesheet'/><noscript><link
href='https://www.blogger.com/dyn-css/authorization.css?
targetBlogID=4802841478634147276&amp;zx=b9ba197a-fb5b-4460-ac0b-b18f2f734cc4'
rel='stylesheet'/></noscript>\n<meta name='google-adsense-platform-account'
content='ca-host-pub-1556223355139109'/>\n<meta name='google-adsense-platform-
domain' content='blogspot.com'/>\n\n<!-- data-ad-client=ca-
pub-7983783048239650"
            ],
            "body": (...),
            "content": "8Base Ransomware Data Leak Sites Seized in
International Law Enforcement Operation #1 Trusted Cybersecurity News Platform
Followed by 5.20+ million \uf099 \uf0e1 \uf09a \uf0c9 \ue800 \uf0e0 Subscribe
\u2013 Get Latest News \ue801 Home \uf0e0 Newsletter \ue805 Webinars Home Data
Breaches Cyber Attacks Vulnerabilities Webinars Expert Insights Contact \uf0c9
\ue800 \ue80a Resources Webinars Free eBooks About Site About THN Jobs
Advertise with us Contact/Tip Us \uf0e0 Reach out to get featured\u2014contact
us to send your exclusive story idea, research, hacks, or ask us a question or
leave a comment/feedback! Follow Us On Social Media \uf09a \uf099 \uf0e1 \uf167
\uf16d \uf09e RSS Feeds \uf0f3 Email Alerts \uf2c6 Telegram Channel 8Base
Ransomware Data Leak Sites Seized in International Law Enforcement Operation
\ue802 Feb 11, 2025 \ue804 Ravie Lakshmanan Cybercrime / Ransomware Source: The
```

Nation A coordinated law enforcement operation has taken down the dark web data leak and negotiation sites associated with the 8Base ransomware gang. Visitors to the data leak site are now greeted with a seizure banner that says: \"This hidden site and the criminal content have been seized by the Bavarian State Criminal Police Office on behalf of the Office of the Public Prosecutor General in Bamberg.\" The takedown involved the U.K. National Crime Agency (NCA), the U.S. Federal Bureau of Investigation (FBI), Europol, as well as agencies from Bavaria, Belgium, Czechia, France, Germany, Japan, Romania, Spain, Switzerland, and Thailand. Thai media reports have revealed that four European nationals \u2013 two men and two women \u2013 were arrested across four different locations on Monday as part of an effort codenamed Operation Phobos Aetor. The identities of the suspects were not disclosed. Authorities are said to have seized more than 40 pieces of evidence, including mobile phones, laptops, and digital wallets. They are alleged to be linked to the deployment of Phobos ransomware against 17 companies located in Switzerland between April 2023 and October 2024. Furthermore, the group has been accused of earning $16 million through attacks that claimed over 1,000 victims across the world. 8Base, which emerged as a major double extortion player in 2023, has been previously found incorporating Phobos ransomware artifacts into their financially motivated cyber attacks, with research from VMware uncovering a Phobos sample using a \".8base\" file extension on encrypted files. Overlaps have also been identified between 8Base and RansomHouse, particularly when it comes to their ransom notes and dark web infrastructure. The latest development comes in the aftermath of a series of high-profile disruptions associated with Hive , LockBit , and BlackCat in recent years. Late last year, Evgenii Ptitsyn, a 42-year-old Russian national believed to be the administrator of the Phobos ransomware, was extradited to the U.S. Found this article interesting? Follow us on Twitter \uf099 and LinkedIn to read more exclusive content we post. SHARE \uf09a \uf099 \uf0e1 \uf1e0 \uf099 Tweet \uf0e1 Share \uf09a Share \uf1e0 Share \ue80a \uf09a Share on Facebook \uf099 Share on Twitter \uf0e1 Share on Linkedin \uf281 Share on Reddit \uf1d4 Share on Hacker News \uf0e0 Share on Email \uf232 Share on WhatsApp Share on Facebook Messenger \uf2c6 Share on Telegram SHARE \uf1e0 Cyber Threat Cybercrime cybersecurity dark web data breach encryption law enforcement Phishing ransomware Trending News \u26a1 THN Weekly Recap: Top Cybersecurity Threats, Tools and Tips [3 February] Top 5 AI-Powered Social Engineering Attacks Malicious ML Models on Hugging Face Leverage Broken Pickle Format to Evade Detection DeepSeek App Transmits Sensitive User and Device Data Without Encryption Microsoft Identifies 3,000 Leaked ASP.NET Keys Enabling Code Injection Attacks Fake Google Chrome Sites Distribute ValleyRAT Malware via DLL Hijacking AI-Powered Social Engineering: Reinvented Threats AsyncRAT Campaign Uses Python Payloads and TryCloudflare Tunnels for Stealth Attacks Cisco Patches Critical ISE Vulnerabilities Enabling Root CmdExec and PrivEsc Hackers Exploiting SimpleHelp RMM Flaws for Persistent Access and Ransomware Russian Cybercrime Groups Exploiting 7-Zip Flaw to Bypass Windows MotW Protections Popular Resources Automate Your Vulnerability Scans and Reduce Risk \u2013 See VulScan in Action Symphony 2025: Transform Your Cyber Defense in Just 60 Minutes Spot Hidden Vulnerabilities \u2013 Uncover Exposures Before They Become Threats Struggling with Your SOC? Discover Trends & Tactics from Top Security Leaders Cybersecurity Webinars ASPM \u2013 Ultimate Cyber Shield Learn How ASPM Transforms AppSec to Outpace Evolving Threats Discover how ASPM revolutionizes AppSec by unifying code and runtime insights

```
to proactively outpace evolving threats. Register Eliminate Identity Debt
Transform Your Identity Security: A Simple, Actionable Roadmap Join Okta
experts to uncover a clear roadmap for closing identity gaps, reducing
technical debt, and building a resilient security posture. Register Breaking
News Cybersecurity Resources Data Security Go-To Best Practices Get the
straightforward guide that makes protecting your data feel effortless and
simplified. Strengthen your cloud data security with these essential best
practices. 81% of Organizations Choose Zero Trust for Cyber Defense State of
Cyberthreats and Protection Report: Results of a ViB survey commissioned by
Zscaler The Definitive Guide to SaaS Security Proactive strategies to protect
your critical data, strengthen your SaaS security and equip your security team
for success. Earn a Master's in Cybersecurity Risk Management Lead the future
of cybersecurity risk management with an online Master's from Georgetown.
Expert Insights / Articles Videos Solving Identity Challenges with an
Extensible CIAM Solution \ue802 February 10, 2025 Read \u279d Hacking in the
name of \ue802 February 3, 2024 Read \u279d Eliminate Your Attack Surface by
Becoming Invisible: Hackers Can't Attack What They Can't See \ue802 February 3,
2024 Read \u279d Using Roles and Attributes to Protect Identities \ue802
February 3, 2024 Read \u279d Get Latest News in Your Inbox Get the latest news,
expert insights, exclusive resources, and strategies from industry leaders
\u2013 all for free. Email Connect with us! \uf099 922,500 Followers \uf0e1
625,000 Followers \uf167 23,100 Subscribers \uf16d 145,000 Followers \uf09a
1,890,500 Followers \uf2c6 143,200 Subscribers Company About THN Advertise with
us Contact Pages Webinars Privacy Policy \uf09e RSS Feeds \uf0e0 Contact Us
\u00a9 The Hacker News, 2024. All Rights Reserved.",
            "head": (...)
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].title`	Report.Title	N/A	`data[].published_date`	`8Base Ransomware Data Leak Sites Seized in International Law Enforcement Operation`	N/A
`.html.content`	Report.Description	N/A	`data[].published_date`	`8Base Ransomware Data Leak Sites Seized...`	N/A
`.data[].link`	Report.Attribute	Report Link	`data[].published_date`	`https://www.blogger.com/dyn-css/authorization.css?targetBlogID=4802841478634147276`	N/A

Average Feed Run

Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 minute
Reports	20
Report Attributes	20

Known Issues / Limitations

- The integration successfully parses articles from the following websites:
  - The Hacker News
  - Bleeping Computer
  - ZDNet
  - Security Affairs
  - Security Boulevard
  - HackRead
  - Inquirer
  - The Register

  For all other sources, the full HTML content is included in the description.

- Some news websites may return a 4xx error. In such cases, you should contact the vendor for more information.

Change Log

- **Version 1.0.0**
  - Initial release