

ThreatQuotient



SecAlliance ThreatMatch CDF Guide

Version 1.1.0

May 22, 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

Integration Details	5
Introduction	6
Installation	7
Configuration	8
ThreatQ Mapping	11
ThreatMatch Alerts	11
ThreatMatch Alert Details (Supplemental)	12
ThreatMatch Intelligence	20
ThreatMatch Profile Details (Supplemental)	21
Universal Mapping Tables	26
Average Feed Run	30
ThreatMatch Alerts	30
ThreatMatch Intelligence	31
Change Log	32

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	1.1.0
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	ThreatQ Supported

Introduction

The SecAlliance ThreatMatch CDF enables analysts to automatically import alerts & profiles from ThreatMatch, along with related MITRE Attack Techniques, related threat actors, and other context.

The integration provides the following feeds:

- **ThreatMatch Alerts**- brings in alerts from ThreatMatch, along with any related context such as related profiles (malware, threat actors, campaigns, & incidents).
- **ThreatMatch Intelligence** - brings in intelligence from ThreatMatch's Profiles API. This will only bring in alerts if a profile has alerts related to it.
- **ThreatMatch Alert Details (supplemental)** - fetches details for a given Alert or ID.
- **ThreatMatch Profile Details (supplemental)** - fetches details for a given Alert or ID.

The feeds ingest the following system objects:

- Adversaries
 - Adversary Attributes
- Attack Patterns
- Campaigns
 - Campaign Attributes
- Events
 - Event Attributes
- Incidents
- Indicators
- Malware
 - Malware Attributes

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
ThreatMatch Hostname	Enter your ThreatMatch Hostname without https://.
ThreatMatch Client ID	Enter your ThreatMatch Client ID.
ThreatMatch Client Secret	Enter your ThreatMatch Client Secret.
Alert Type Filter (<i>ThreatMatch Alerts feed only</i>)	Select the type of alerts to ingest. Options include: ◦ Actor Campaigns ◦ Credential Breaches ◦ DDoS ◦ Exploit Alert ◦ General Notification ◦ New Malware ◦ Pastebin dumps ◦ Phishing Attempts ◦ PII exposure

PARAMETER	DESCRIPTION
	◦ High Impact Vulnerabilities ◦ Information leakages ◦ Malware Analysis ◦ Nefarious Domains ◦ Nefarious Forum mention ◦ Sensitive information disclosures ◦ Social Media Alerts ◦ Supply chain Event ◦ Technical exposure ◦ Threat Actor Updates ◦ Trigger events
Alert Priority Filter <i>(ThreatMatch Alerts feed only)</i>	Select the priority levels to filter alerts to ingest. Options include: ◦ Very Low ◦ Low ◦ Medium ◦ High ◦ Very High

< SecAlliance ThreatMatch Intelligence



Disabled ☐ Enabled

Uninstall

Additional Information

Integration Type: Feed

Version: 1.1.0

Accepted Data Types:

Configuration Activity Log

ThreatMatch Hostname

new.threatmatch.com

Enter your ThreatMatch hostname (without https://)

ThreatMatch Client ID

Enter your ThreatMatch Client ID API key

ThreatMatch Client Secret

Enter your ThreatMatch Client Secret API key

Set indicator status to...

Active

Run Frequency

Every 24 Hours

☒ Send a notification when this feed encounters issues.

☐ Debug Option: Save the raw data response files.

We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.

Save

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

ThreatMatch Alerts

The ThreatMatch Alerts feed brings in alerts from ThreatMatch, along with any related context such as related profiles (malware, threat actors, campaigns, & incidents)

GET <https://new.threatmatch.com/api/alerts/all>

Sample Response:

```
{
  "list": [
    1
  ],
  "date_applied": "2020-09-23 11:26"
}
```

ThreatMatch Alert Details (Supplemental)

The ThreatMatch Alert Details feed fetches details for a given Alert or ID.

GET https://new.threatmatch.com/api/alerts/{{alert_id}}/edit

Sample Response:

```
{
  "data": [
    {
      "id": 3122,
      "status_id": 2,
      "type_id": 9,
      "priority_id": 4,
      "title": "Chinese Group Targeting French National Cybersecurity Agency (ANSSI)",
      "known_as": "",
      "slug": "chinese-group-targeting-french-national-cybersecurity-agency-anssi",
      "image": null,
      "content": "{\n  \"overview_text\": \"<p>France's Agence nationale de la sécurité des systèmes d'information (ANSSI, French National Agency for the Security of Information Systems) has revealed it is now dealing with a \\\"massive\\\" hacking campaign being conducted by the China-linked advanced persistent threat (APT) group APT31 (Zirconium, Judgment Panda). While ANSSI did not disclose which sectors were being targeted, it stated that it is asking French organizations to investigate whether they have been compromised. According to ANSSI, APT31's activity in France is an ongoing, \\\"large intrusion campaign of compromise.\\\" According to Ben Koehl with Microsoft's Threat Intelligence Center, \\\"Zirconium appears to operate numerous router networks to facilitate these actions. They are layered together and strategically used. If investigating these IP addresses they should be used mostly as source IPs but on occasion they are pointing implant traffic into the network. Historically they did the classic I have a dnsname -&gt; ip approach for C2 communications. They've since moved that traffic into the router network. This allows them flexibility to manipulate the traffic destination at several layers while slowing the efforts of pursuit elements.\\\"</p>\",\n  \"overview_gallery\": [],\n  \"tags_connectors\": [{\n    \"id\": 478,\n    \"name\": \"France\",\n    \"type\": \"tag\",\n    \"text\": \"France (tag)\",\n    \"title\": \"France\"\n  }, {\n    \"id\": 2002,\n    \"name\": \"Europe\",\n    \"type\": \"tag\",\n    \"text\": \"Europe (tag)\",\n    \"title\": \"Europe\"\n  }, {\n    \"id\": 2040,\n    \"name\": \"Government & public services\",\n    \"type\": \"tag\",\n    \"text\": \"Government & public services (tag)\",\n    \"title\": \"Government & public services\"\n  }],\n  \"sector_relevance_sector_relevance\": \"<p>Government & public services</p>\",\n  \"mitre_tags_mitre_navigator_tags_selection_summary\": [{\n    \"id\": 794,\n    \"type\": \"tag\"\n  }]\n},\n  \"update_notes\": null,\n  \"are_numbered_headings_enabled\": false,\n  \"is_table_included_in_pdf\": false,\n  \"pdf_cover_enabled\": false,\n  \"notes\": null,\n  \"published\": 1,\n  \"publish_now\": 1,\n  \"publish_on\": null,\n  \"published_at\": \"2021-07-28 15:31:23\",\n  \"updated_at\": \"2021-08-05 13:35:37\",\n  \"additional_dates\": {\n    \"event_date\": \"2021-06-30T22:00:00.000Z\",\n    \"discovery_date\": \"2021-07-07T22:00:00.000Z\"\n  }\n},\n  \"t1p\": {\n    \"colour\": \"green\",\n    \"caveat\": null,\n    \"shortcode\": \"green\",\n    \"colour_code\": \"#3AAA35\",\n    \"label\": \"TLP: GREEN\",
```

```

        "description": "Limited disclosure, restricted to the community.",
        "classification_title": "",
        "classification_description": ""
    },
    "published_updated_at": null,
    "update_summary": "<p>France's national cybersecurity agency said on Wednesday that it is contending with
a massive campaign by Chinese state-backed hackers targeting French organizations through compromised routers.</p>",
    "is_linear_content_builder": true,
    "published_insignificant_updated_at": "2021-08-05 13:35:36",
    "is_simple_mode_enabled": false,
    "priorityName": "High",
    "is_flagged": false,
    "tag_tactics": {
        "794": [
            9
        ]
    },
    "tags": [
        478,
        794,
        2002,
        2040
    ],
    "tagsFull": [
        {
            "id": 478,
            "name": "France",
            "slug": "france",
            "sort_id": 0,
            "created_at": "2019-05-09 11:49:01",
            "updated_at": "2019-05-09 11:49:01",
            "stix_type": null,
            "misp_name": null,
            "mitre_technique_id": null,
            "parent_tag_id": null,
            "is_deprecated": false,
            "pivot": {
                "mapped_item_id": 2848,
                "tag_id": 478,
                "content_section_id": null
            }
        },
        {
            "id": 794,
            "name": "T1190 - Exploit public-facing application",
            "slug": "t1190-exploit-public-facing-application",
            "sort_id": 0,
            "created_at": "2019-05-09 11:49:02",
            "updated_at": "2021-06-22 07:13:35",
            "stix_type": null,
            "misp_name": null,
            "mitre_technique_id": 211,
            "parent_tag_id": null,
            "is_deprecated": false,
            "pivot": {
                "mapped_item_id": 2848,
                "tag_id": 794,
                "content_section_id": null
            }
        }
    ],
    {

```

```
    "id": 2002,
    "name": "Europe",
    "slug": "europe",
    "sort_id": 0,
    "created_at": "2019-05-09 11:49:05",
    "updated_at": "2019-05-09 11:49:05",
    "stix_type": null,
    "misp_name": null,
    "mitre_technique_id": null,
    "parent_tag_id": null,
    "is_deprecated": false,
    "pivot": {
      "mapped_item_id": 2848,
      "tag_id": 2002,
      "content_section_id": null
    }
  },
  {
    "id": 2040,
    "name": "Government & public services",
    "slug": "government-public-services",
    "sort_id": 0,
    "created_at": "2019-05-09 11:49:05",
    "updated_at": "2019-05-09 11:49:05",
    "stix_type": null,
    "misp_name": null,
    "mitre_technique_id": null,
    "parent_tag_id": null,
    "is_deprecated": false,
    "pivot": {
      "mapped_item_id": 2848,
      "tag_id": 2040,
      "content_section_id": null
    }
  }
],
"related": [
  2369,
  2384
],
"related_alerts": [],
"related_scenarios": [],
"author": "ThreatQuotient",
"author_id": 656,
"relevanceName": "Global",
"relevanceSlug": "global",
"text_relevance": "Government & public services",
"mitre_navigator_data": {
  "matrices": [
    {
      "id": 2,
      "sort_id": 0
    }
  ],
  "matricesNames": {
    "2": "Enterprise"
  },
  "tacticsIds": [
    9
  ],
  "techniques": {
```

```

        "211": {
          "9": {
            "colour_grade": 1
          }
        }
      },
      "tacticsNames": {
        "9": "Initial Access"
      },
      "techniquesNames": {
        "211": {
          "name": "T1190 - Exploit Public-Facing Application",
          "description": "<p>Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL)(Citation: NVD CVE-2016-6662), standard services (like SMB(Citation: CIS Multiple SMB Vulnerabilities) or SSH), network device administration and management protocols (like SNMP and Smart Install(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)), and any other applications with Internet accessible open sockets, such as web servers and related services.(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may include Exploitation for Defense Evasion. </p>\n<p>If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via Escape to Host, or take advantage of weak identity and access management policies.</p>\n<p>For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities.(Citation: OWASP Top 10)(Citation: CWE top 25)</p>",
          "is_detectable_by_common_defenses": null,
          "detectable_by_common_defenses_explanation": null,
          "difficulty_for_adversary": null,
          "difficulty_for_adversary_explanation": null,
          "detection": "<p>Monitor application logs for abnormal behavior that may indicate attempted or successful exploitation. Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection. Web Application Firewalls may detect improper inputs attempting exploitation.</p>",
          "tactics_ids": [
            9
          ],
          "matrix_id": 2
        }
      }
    },
    "linked_profiles": [
      {
        "id": 2369,
        "title": "APT31",
        "listing_description": null,
        "capability_id": 4,
        "type_id": 1,
        "misp_cluster_name": null,
        "created_at": "2021-07-28 15:32:51",
        "published_at": "2021-07-28 15:34:26",
        "published_updated_at": null,
        "published_insignificant_updated_at": null,
        "typeName": "Threat Actor",
        "typeSlug": "threat-actor",
        "capabilityName": "High"
      },
      {
        "id": 2384,
        "title": "Judgement Panda",
        "listing_description": null,
        "capability_id": 4,
        "type_id": 1,

```

```
        "misp_cluster_name": null,
        "created_at": "2021-08-05 13:26:42",
        "published_at": "2021-08-05 13:28:44",
        "published_updated_at": null,
        "published_insignificant_updated_at": "2021-08-05 13:30:39",
        "typeName": "Threat Actor",
        "typeSlug": "threat-actor",
        "capabilityName": "High"
    }
],
"linked_alerts": [],
"comments": [],
"total_comments_count": 0,
"profile_types": [
    {
        "id": 1,
        "name": "Threat Actor",
        "slug": "threat-actor",
        "created_at": "2019-04-05 13:28:46",
        "updated_at": "2020-07-07 07:14:01",
        "stix_type": "threat-actor",
        "acronym": "TA"
    },
    {
        "id": 2,
        "name": "Country",
        "slug": "country",
        "created_at": "2019-04-05 13:28:46",
        "updated_at": "2020-07-07 07:14:01",
        "stix_type": "threat-actor",
        "acronym": "C"
    },
    {
        "id": 3,
        "name": "Incident",
        "slug": "incident",
        "created_at": "2019-04-05 13:28:46",
        "updated_at": "2020-07-07 07:14:01",
        "stix_type": "campaign",
        "acronym": "I"
    },
    {
        "id": 4,
        "name": "Operation",
        "slug": "operation",
        "created_at": "2019-04-05 13:28:46",
        "updated_at": "2020-07-07 07:14:01",
        "stix_type": "campaign",
        "acronym": "O"
    },
    {
        "id": 5,
        "name": "Malware & Tools",
        "slug": "malware-tools",
        "created_at": "2019-04-05 13:28:46",
        "updated_at": "2020-07-07 07:14:01",
        "stix_type": "malware",
        "acronym": "MT"
    }
],
>alert_types": [
```

```
{
  "id": 9,
  "name": "Actor Campaigns",
  "slug": "actor-campaigns",
  "acronym": "AC"
},
{
  "id": 2,
  "name": "Credential Breaches",
  "slug": "credential-breaches",
  "acronym": "CB"
},
{
  "id": 12,
  "name": "DDoS",
  "slug": "ddos",
  "acronym": "D"
},
{
  "id": 17,
  "name": "Exploit Alert",
  "slug": "exploit-alert",
  "acronym": "EA"
},
{
  "id": 1,
  "name": "General Notification",
  "slug": "general-notification",
  "acronym": "GN"
},
{
  "id": 7,
  "name": "High Impact Vulnerabilities",
  "slug": "high-impact-vulnerabilities",
  "acronym": "HI"
},
{
  "id": 6,
  "name": "Information leakages",
  "slug": "information-leakages",
  "acronym": "IL"
},
{
  "id": 10,
  "name": "Malware Analysis",
  "slug": "malware-analysis",
  "acronym": "MA"
},
{
  "id": 13,
  "name": "Nefarious Domains",
  "slug": "nefarious-domains",
  "acronym": "ND"
},
{
  "id": 8,
  "name": "Nefarious Forum mention",
  "slug": "nefarious-forum-mention",
  "acronym": "NF"
},
{
```

```
        "id": 11,
        "name": "New Malware",
        "slug": "new-malware",
        "acronym": "NM"
    },
    {
        "id": 4,
        "name": "Pastebin dumps",
        "slug": "pastebin-dumps",
        "acronym": "PD"
    },
    {
        "id": 3,
        "name": "Phishing Attempts",
        "slug": "phishing-attempts",
        "acronym": "PA"
    },
    {
        "id": 16,
        "name": "PII exposure",
        "slug": "pii-exposure",
        "acronym": "PE"
    },
    {
        "id": 5,
        "name": "Sensitive information disclosures",
        "slug": "sensitive-information-disclosures",
        "acronym": "SI"
    },
    {
        "id": 20,
        "name": "Social Media Alerts",
        "slug": "social-media-alerts",
        "acronym": "SM"
    },
    {
        "id": 14,
        "name": "Supply chain Event",
        "slug": "supply-chain-event",
        "acronym": "SC"
    },
    {
        "id": 15,
        "name": "Technical exposure",
        "slug": "technical-exposure",
        "acronym": "TE"
    },
    {
        "id": 19,
        "name": "Threat Actor Updates",
        "slug": "threat-actor-updates",
        "acronym": "TA"
    },
    {
        "id": 18,
        "name": "Trigger events",
        "slug": "trigger-events",
        "acronym": "TE"
    }
  ]
}
```

```
} ]
```

ThreatMatch Intelligence

The ThreatMatch Intelligence feed brings in intelligence from ThreatMatch's Profiles API. This will only bring in alerts if a profile has alerts related to it.

GET <https://new.threatmatch.com/api/profiles/all>

Sample Response:

```
{
  "list": [
    1
  ],
  "date_applied": "2020-09-23 11:26"
}
```

ThreatMatch Profile Details (Supplemental)

The ThreatMatch Profile Details feed fetches details for a given Profile or ID.

GET https://new.threatmatch.com/api/profiles/{{profile_id}}/edit

Sample Response:

```
{
  "data": [
    {
      "additional_dates": null,
      "alert_types": [
        {
          "acronym": "AC",
          "id": 9,
          "name": "Actor Campaigns",
          "slug": "actor-campaigns"
        },
        {
          "acronym": "CB",
          "id": 2,
          "name": "Credential Breaches",
          "slug": "credential-breaches"
        },
        {
          "acronym": "D",
          "id": 12,
          "name": "DDoS",
          "slug": "ddos"
        },
        {
          "acronym": "EA",
          "id": 17,
          "name": "Exploit Alert",
          "slug": "exploit-alert"
        },
        {
          "acronym": "GN",
          "id": 1,
          "name": "General Notification",
          "slug": "general-notification"
        },
        {
          "acronym": "HI",
          "id": 7,
          "name": "High Impact Vulnerabilities",
          "slug": "high-impact-vulnerabilities"
        },
        {
          "acronym": "IL",
          "id": 6,
          "name": "Information leakages",
          "slug": "information-leakages"
        }
      ]
    }
  ]
}
```

```
    "acronym": "MA",
    "id": 10,
    "name": "Malware Analysis",
    "slug": "malware-analysis"
  },
  {
    "acronym": "ND",
    "id": 13,
    "name": "Nefarious Domains",
    "slug": "nefarious-domains"
  },
  {
    "acronym": "NF",
    "id": 8,
    "name": "Nefarious Forum mention",
    "slug": "nefarious-forum-mention"
  },
  {
    "acronym": "NM",
    "id": 11,
    "name": "New Malware",
    "slug": "new-malware"
  },
  {
    "acronym": "PD",
    "id": 4,
    "name": "Pastebin dumps",
    "slug": "pastebin-dumps"
  },
  {
    "acronym": "PA",
    "id": 3,
    "name": "Phishing Attempts",
    "slug": "phishing-attempts"
  },
  {
    "acronym": "PE",
    "id": 16,
    "name": "PII exposure",
    "slug": "pii-exposure"
  },
  {
    "acronym": "SI",
    "id": 5,
    "name": "Sensitive information disclosures",
    "slug": "sensitive-information-disclosures"
  },
  {
    "acronym": "SM",
    "id": 20,
    "name": "Social Media Alerts",
    "slug": "social-media-alerts"
  },
  {
    "acronym": "SC",
    "id": 14,
    "name": "Supply chain Event",
    "slug": "supply-chain-event"
  },
  {
    "acronym": "TE",
```

```
        "id": 15,
        "name": "Technical exposure",
        "slug": "technical-exposure"
    },
    {
        "acronym": "TA",
        "id": 19,
        "name": "Threat Actor Updates",
        "slug": "threat-actor-updates"
    },
    {
        "acronym": "TE",
        "id": 18,
        "name": "Trigger events",
        "slug": "trigger-events"
    }
],
"associated_alerts_ids": [
    3156
],
"associated_profiles_ids": [],
"author": "ThreatQuotient",
"author_id": 692,
"capabilityName": "Very High",
"capability_id": 5,
"comments": [],
"content": "{\"summary_gallery\": [], \"summary_text\": \"<p>This is a country :)</p>\"}",
"id": 2404,
"image": "",
"is_flagged": false,
"is_linear_content_builder": true,
"is_simple_mode_enabled": true,
"known_as": "USA",
"linked_alerts": [
    {
        "capabilityName": "Medium",
        "created_at": "2021-08-18T14:45:02.000000Z",
        "id": 3156,
        "priority_id": 3,
        "published_at": "2021-08-18T14:45:28.000000Z",
        "published_insignificant_updated_at": "2021-08-19T13:54:00.000000Z",
        "published_updated_at": null,
        "relevanceName": "Global",
        "relevanceSlug": "global",
        "title": "Malware Analysis of Nanocore RAT",
        "typeName": "Malware Analysis",
        "typeSlug": "malware-analysis",
        "type_id": 10
    }
],
"linked_profiles": [],
"listing_description": "The land of the \"free\"",
"misp_cluster_name": null,
"mitre_navigator_data": {
    "matrices": [],
    "matricesNames": [],
    "tacticsIds": [],
    "tacticsNames": [],
    "techniques": [],
    "techniquesNames": []
},
},
```

```
"notes": null,
"pdf_cover_enabled": false,
"profile_types": [
  {
    "acronym": "TA",
    "created_at": "2019-04-05T12:28:46.000000Z",
    "id": 1,
    "name": "Threat Actor",
    "slug": "threat-actor",
    "stix_type": "threat-actor",
    "updated_at": "2020-07-07T06:14:01.000000Z"
  },
  {
    "acronym": "C",
    "created_at": "2019-04-05T12:28:46.000000Z",
    "id": 2,
    "name": "Country",
    "slug": "country",
    "stix_type": "threat-actor",
    "updated_at": "2020-07-07T06:14:01.000000Z"
  },
  {
    "acronym": "I",
    "created_at": "2019-04-05T12:28:46.000000Z",
    "id": 3,
    "name": "Incident",
    "slug": "incident",
    "stix_type": "campaign",
    "updated_at": "2020-07-07T06:14:01.000000Z"
  },
  {
    "acronym": "O",
    "created_at": "2019-04-05T12:28:46.000000Z",
    "id": 4,
    "name": "Operation",
    "slug": "operation",
    "stix_type": "campaign",
    "updated_at": "2020-07-07T06:14:01.000000Z"
  },
  {
    "acronym": "MT",
    "created_at": "2019-04-05T12:28:46.000000Z",
    "id": 5,
    "name": "Malware & Tools",
    "slug": "malware-tools",
    "stix_type": "malware",
    "updated_at": "2020-07-07T06:14:01.000000Z"
  }
],
"publish_now": 1,
"publish_on": null,
"published": 1,
"published_at": "2021-08-19T13:52:39.000000Z",
"published_insignificant_updated_at": null,
"published_updated_at": null,
"related": [],
"related_alerts": [
  3156
],
"related_scenarios": [],
"relevanceName": "Global",
```

```
    "relevanceSlug": "global",
    "slug": "united-states-of-america-1",
    "status_id": 2,
    "tag_tactics": [],
    "tags": [],
    "tagsFull": [],
    "text_relevance": "",
    "title": "United States of America",
    "tlp": {
      "caveat": null,
      "classification_description": "",
      "classification_title": "",
      "colour": "green",
      "colour_code": "#3AAA35",
      "description": "Limited disclosure, restricted to the community.",
      "label": "TLP: GREEN",
      "shortcode": "green"
    },
    "total_comments_count": 0,
    "typeName": "Country",
    "typeSlug": "country",
    "type_id": 2,
    "update_summary": null,
    "updated_at": "2021-08-19T13:52:40.000000Z"
  }
]
```

Universal Mapping Tables

ThreatQuotient provides the following default mapping for the ThreatMatch Alert Details and ThreatMatch Profile Details supplemental feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
<code>data.title</code>	Event Title	Alert	N/A	<code>data.additional_dates.event_date</code>	Chinese Group Targeting French National Cybersecurity Agency (ANSSI)	N/A
<code>data.tlp.colour</code>	TLP	Event, Attribute	N/A	N/A	green	N/A
<code>data.priorityName</code>	Attribute	Priority	N/A	<code>data.published_at</code>	High	N/A
<code>data.additional_dates.discovery_date</code>	Attribute	Discovery Date	N/A	<code>data.published_at</code>	N/A	N/A
<code>data.alert_types[].name</code>	Attribute	Alert Type	N/A	<code>data.published_at</code>	Actor Campaigns	Only if the <code>data.type_id</code> matches the <code>id</code>
<code>data.profile_types[].name</code>	Attribute	Profile Type	N/A	<code>data.published_at</code>	Threat Actor	Only if an <code>id</code> from the <code>data.linked_profiles</code> matches the <code>id</code>
<code>data.is_flagged</code>	Attribute	Is Flagged	bool -> string	<code>data.published_at</code>	True	N/A
<code>data.relevanceName</code>	Attribute	Relevance	N/A	<code>data.published_at</code>	Global	N/A
<code>data.text_relevance</code>	Attribute	Sector Relevance	N/A	<code>data.published_at</code>	Government & public services	N/A
<code>data.mitre_navigator_data.tacticsNames</code>	Attribute	Tactic	N/A	<code>data.published_at</code>	Initial Access	We only want the values from this dict
<code>data.tagsFull</code>	Name	Tag	N/A	N/A	France	We ignore MITRE techniques & CVEs
<code>data.tagsFull</code>	Value	Attack Pattern	N/A	<code>data.published_at</code>	T1190 - Exploit Public-Facing Application	Parsed for MITRE Techniques (if the key is not null)
<code>data.tagsFull</code>	Indicator Value	CVE	N/A	<code>data.published_at</code>	CVE-2021-00001	Parsed for CVEs
<code>data.tagsFull</code>	Attribute	Target Geography	N/A	<code>data.published_at</code>	United States	If the <code>content_section_id == target-geography_connectors</code>
<code>data.tagsFull</code>	Attribute	Country of Origin	N/A	<code>data.published_at</code>	United States	If the <code>content_section_id == country-of-origin_connectors</code>
<code>data.tagsFull</code>	Attribute	Category	N/A	<code>data.published_at</code>	United States	If the <code>content_section_id == category_connectors</code>

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
data.tagsFull	Attribute	Motivation	N/A	data.published_at	United States	If the content_section_id == motivation_connectors
data.tagsFull	Attribute	Intended Effect	N/A	data.published_at	United States	If the content_section_id == intended-effect_connectors
data.id	Attribute	ThreatMatch Link	N/A	data.published_at	N/A	Concatenated with the portal URL
data.content.overview_text/assessment/dates_date_assessment	Indicator Value	CVE	N/A	data.published_at	N/A	Parsed for CVEs
data.content.overview_text/assessment/dates_date_assessment	Indicator Value	MD5	N/A	data.published_at	N/A	Parsed for MD5s
data.content.overview_text/assessment/dates_date_assessment	Indicator Value	SHA-1	N/A	data.published_at	N/A	Parsed for SHA-1s
data.content.overview_text/assessment/dates_date_assessment	Indicator Value	SHA-256	N/A	data.published_at	N/A	Parsed for SHA-256s
data.content.overview_text/assessment/dates_date_assessment	Indicator Value	SHA-512	N/A	data.published_at	N/A	Parsed for SHA-512s
data.capabilityName	Attribute	Capability	N/A	data.published_at	High	N/A
data.known_as	Attribute	Known As	N/A	data.published_at	Carbanak	N/A
data.notes	Attribute	Note	N/A	data.published_at	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
data.content.malware_malware_family	Attribute	Malware Family	N/A	data.published_at	Trojan	N/A
data.content.malware_malware_type	Attribute	Malware Type	N/A	data.published_at	Remote Administrative Trojan	N/A
data.linked_profiles[].title	Attribute	Country	N/A	data.published_at	United States	If the slugType == country
data.linked_profiles[].title	Value	Malware	N/A	data.published_at	Carbanak	If the slugType == malware-tools
data.linked_profiles[].title	Value	Campaign	N/A	data.published_at	Operation Sandstorm	If the slugType == operation
data.linked_profiles[].title	Name	Adversary	N/A	data.published_at	APT31	If the slugType == threat-actor
data.linked_profiles[].title	Value	Incident	N/A	data.published_at	N/A	If the slugType == incident
data.priorityName	Attribute	Priority	N/A	data.published_at	Very High	N/A
data.author	Attribute	Author	N/A	data.published_at	ThreatQuotient	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.

ThreatMatch Alerts

METRIC	RESULT
Run Time	1 minute
Events	6
Event Attributes	34
Adversaries	1
Adversary Attributes	22
Attack Patterns	9
Campaigns	1
Campaign Attributes	4
Indicators	16
Malware	1
Malware Attributes	14

ThreatMatch Intelligence

METRIC	RESULT
Run Time	1 minute
Events	3
Event Attributes	32
Adversaries	3
Adversary Attributes	39
Attack Patterns	9
Campaigns	1
Campaign Attributes	6
Incidents	1
Incident Attributes	6
Malware	1
Malware Attributes	16

Change Log

- **Version 1.1.0**
 - Added Hostname configuration option.
 - Rebranded CDF from ThreatMatch to **SecAlliance Threat Match**.
 - Updated Support Tier from **Not Actively Supported** to **ThreatQ Supported**.
- **Version 1.0.0**
 - Initial Release