ThreatQuotient

Palo Alto Prisma 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	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The Palo Alto Prisma Cloud CDF integration provides the ability to ingest host CVE data into ThreatQ from Palo Alto Prisma Cloud.

The integration provides the following feed:

- **Palo Alto Prisma Cloud** - ingests vulnerability data from Palo Alto Prisma Cloud as Asset Objects with related CVE data.

The integration ingests the following system objects:

- Asset
  - Asset Attributes
- Indicators
  - Indicator Attributes
- Vulnerabilities
  - Vulnerability Attributes

Prerequisites

The following is required to install and run the integration:

- The Hostname or IP Address of your Prisma Cloud instance.

  > This can be found by navigating to Computer > Manage > System > Utilities and copying the Path to Console.

- A Palo Alto username and password.
- The API version of your Palo Alto Cloud instance.
- A defender deployed on a host VM in order for data to be ingested.

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:

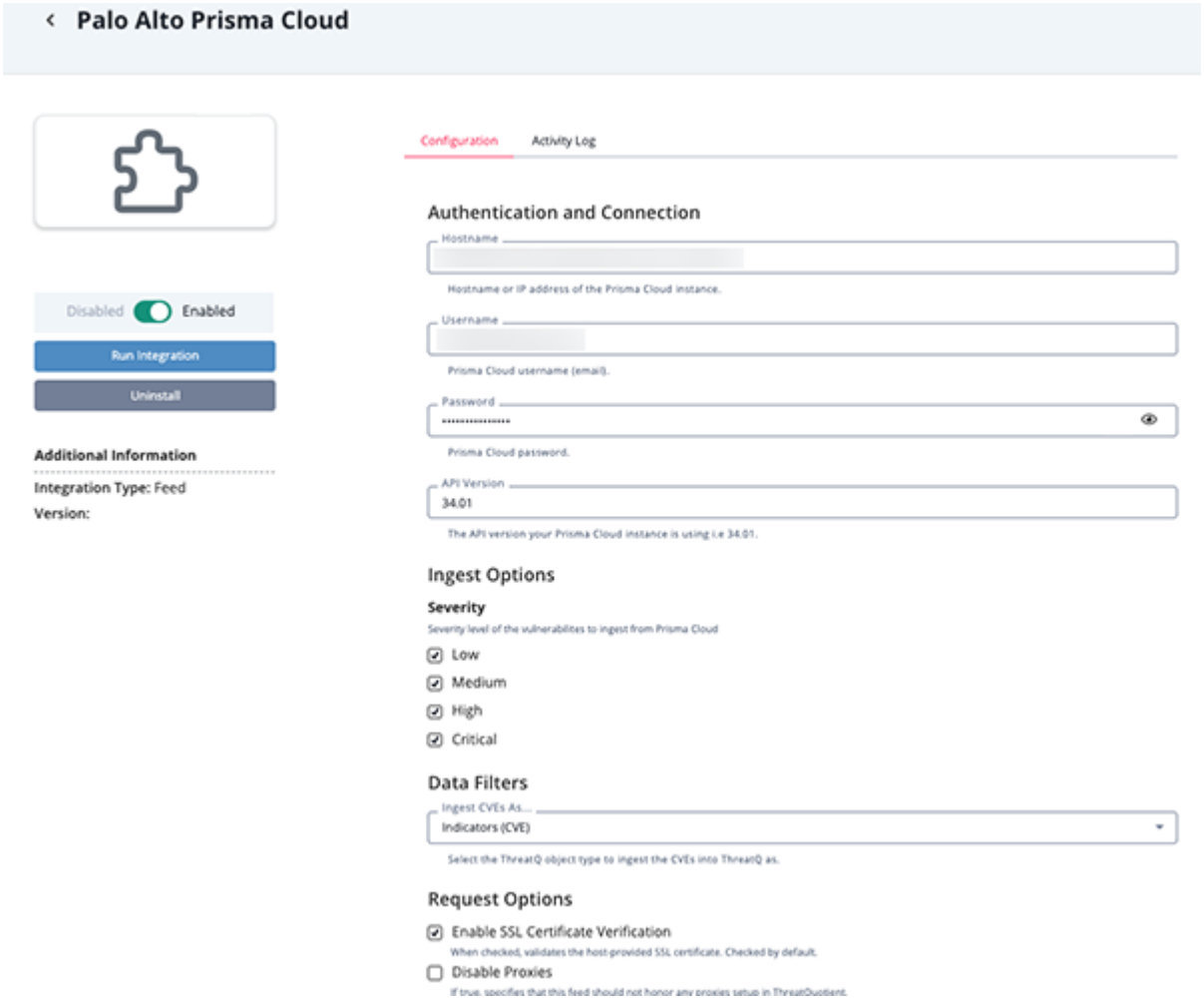
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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
Hostname	Enter your Prisma Cloud instance Hostname or IP Address.
Username	Enter your Prisma Cloud email.
Password	Enter the password associated with the username above.
API Version	Enter the API version of your Prisma Cloud instance. The default value is `34.01`.
Severity Level	Select which levels of severities to ingest. Options include: ◦ Low *(default)* ◦ Medium *(default)* ◦ High *(default)* ◦ Critical *(default)*
Ingest CVEs As	Select which data type to ingest CVEs as in the platform. Options include: ◦ Vulnerabilities *(default)* ◦ Indicators

PARAMETER	DESCRIPTION
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

Palo Alto Prisma Cloud

The Palo Alto Prisma Cloud feed ingests the vulnerabilities found by defenders deployed on systems and stores each defender as an Asset with related CVEs.

`GET {HOSTNAME}/api/v{VERSION}/hosts` `GET https://us-east1.cloud.twistlock.com/us-1-113062851/api/v34.01/hosts`

Sample Response:


```
[
  {
    "_id": "int-8465",
    "type": "host",
    "hostname": "int-8465",
    "scanTime": "2025-06-12T18:03:15.279Z",
    "binaries": [
      {
        "name": "systemd",
        "path": "/usr/lib/systemd/systemd",
        "md5": "",
        "cveCount": 0
      }
    ],
    "Secrets": [],
    "startupBinaries": [],
    "osDistro": "ubuntu",
    "osDistroVersion": "22.04",
    "osDistroRelease": "jammy",
    "distro": "Ubuntu 22.04.5 LTS",
    "packages": [
      {
        "pkgsType": "package",
        "pkgs": [
          {
            "version": "0.634-1build1",
            "name": "libproc-processtable-perl",
            "cveCount": 4,
            "license": "Artistic or GPL-1+",
            "layerTime": 0,
            "purl": "pkg:deb/ubuntu/libproc-processtable-perl@0.634-1build1",
            "author": "Ubuntu Developers <ubuntu-devel-
discuss@lists.ubuntu.com>"
          }
        ]
      }
```

```
    ],
    "files": null,
    "packageManager": true,
    "applications": [
      {
        "name": "kubernetes",
        "version": "1.32.5",
        "path": "",
        "layerTime": 0,
        "knownVulnerabilities": 52
      }
    ],
    "isARM64": false,
    "redHatNonRPMImage": false,
    "foundSecrets": null,
    "secretScanMetrics": {},
    "image": {
      "created": "0001-01-01T00:00:00Z"
    },
    "history": [],
    "complianceIssues": [
      {
        "text": "",
        "id": 16,
        "severity": "high",
        "cvss": 0,
        "status": "",
        "cve": "",
        "cause": "1 users in docker group: ubuntu",
        "description": "Docker allows you to share a directory between the
Docker host and a guest container\nwithout limiting the access rights of the
container. This means that you can start a\ncontainer and map the / directory
on your host to the container. The container will then be\nable to alter your
host file system without any restrictions. In simple terms, it means that\nyou
can attain elevated privileges with just being a member of the docker group and
then\nstarting a container with mapped / directory on the host",
        "title": "(CIS_Docker_v1.5.0 - 1.1.2) Only allow trusted users to
control Docker daemon",
        "vecStr": "",
        "exploit": "",
        "riskFactors": null,
        "link": "",
        "type": "host_config",
        "packageName": "",
        "packageVersion": "",
        "packageType": "",
        "layerTime": 0,
        "templates": ["GDPR"],
        "twistlock": false,
        "cri": false,
```

```
        "published": 0,
        "fixDate": 0,
        "discovered": "0001-01-01T00:00:00Z",
        "functionLayer": "",
        "wildfireMalware": {},
        "secret": {}
      }
    ],
    "allCompliance": {},
    "vulnerabilities": [
      {
        "text": "",
        "id": 46,
        "severity": "low",
        "cvss": 7.1,
        "status": "needed",
        "cve": "CVE-2023-30630",
        "cause": "",
        "description": "Dmidecode before 3.5 allows -dump-bin to overwrite a
local file. This has security relevance because, for example, execution of
Dmidecode via Sudo is plausible. NOTE: Some third parties have indicated the
fix in 3.5 does not adequately address the vulnerability. The argument is that
the proposed patch prevents dmidecode from writing to an existing file.
However, there are multiple attack vectors that would not require overwriting
an existing file that would provide the same level of unauthorized privilege
escalation (e.g. creating a new file in /etc/cron.hourly).",
        "title": "",
        "vecStr": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H",
        "exploit": "",
        "riskFactors": {
          "Attack complexity: low": {},
          "DoS - High": {}
        },
        "link": "https://ubuntu.com/security/CVE-2023-30630",
        "type": "image",
        "packageName": "dmidecode",
        "packageVersion": "3.3-3ubuntu0.2",
        "packageType": "package",
        "layerTime": 0,
        "templates": null,
        "twistlock": false,
        "cri": false,
        "published": 1681402507,
        "fixDate": 0,
        "applicableRules": ["*"],
        "discovered": "2025-06-10T18:03:16Z",
        "functionLayer": "",
        "wildfireMalware": {},
        "secret": {}
      }
```

```
  ],
  "repoTag": null,
  "tags": [],
  "repoDigests": [],
  "creationTime": "0001-01-01T00:00:00Z",
  "pushTime": "0001-01-01T00:00:00Z",
  "vulnerabilitiesCount": 4751,
  "complianceIssuesCount": 30,
  "vulnerabilityDistribution": {
    "critical": 0,
    "high": 123,
    "medium": 4441,
    "low": 187,
    "total": 4751
  },
  "complianceDistribution": {
    "critical": 1,
    "high": 29,
    "medium": 0,
    "low": 0,
    "total": 30
  },
  "vulnerabilityRiskScore": 1674287,
  "complianceRiskScore": 1290000,
  "k8sClusterAddr": "https://127.0.0.1:6443",
  "riskFactors": {
    "Attack complexity: low": {}
  },
  "labels": ["osDistro:ubuntu", "osVersion:22.04"],
  "installedProducts": {
    "docker": "28.2.2",
    "kubernetes": "1.32.5",
    "osDistro": "jammy",
    "k8sEtcd": true,
    "k8sKubelet": true,
    "k8sScheduler": true,
    "k8sApiServer": true,
    "k8sControllerManager": true,
    "k8sProxy": true,
    "hasPackageManager": true
  },
  "scanVersion": "34.01.126",
  "scanBuildDate": "20250514",
  "hostDevices": [
    {
      "name": "ens4",
      "ip": "10.113.1.232"
    }
  ],
  "firstScanTime": "2025-06-10T18:03:16.104Z",
```

```
    "cloudMetadata": {
      "accountID": "Non-onboarded cloud accounts"
    },
    "instances": [],
    "hosts": {},
    "err": "",
    "collections": ["All"],
    "scanID": 0,
    "trustStatus": "",
    "firewallProtection": {
      "enabled": false,
      "supported": true,
      "outOfBandMode": "",
      "unprotectedProcesses": [
        {
          "process": "rke2",
          "port": 9345,
          "tls": true
        }
      ]
    },
    "appEmbedded": false,
    "caasSpecReferencesTotal": 0,
    "wildFireUsage": null,
    "agentless": false,
    "csaWindows": false,
    "malwareAnalyzedTime": "0001-01-01T00:00:00Z"
  }
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`._id`	Asset.Value	Asset	`.firstScanTime`	`int-8465`	N/A
`.type`	Asset.Attribute	Type	`.firstScanTime`	`host`	N/A
`.vulnerabilities[].cve`	Vulnerability/ Indicator.Value	Vulnerability/CVE	`.vulnerabilites[].discovered`	`CVE-2022-48630`	User-configurable, Ingested according to `Ingest CVEs As...`
`.vulnerabilities[].description`	Vulnerability/ Indicator.Description	N/A	N/A	`In the Linux kernel...`	N/A
`.vulnerabilities[].severity`	Vulnerability/ Indicator.Attribute	Severity	`.vulnerabilites[].discovered`	`low`	User-configurable, Updatable
`.vulnerabilities[].status`	Vulnerability/ Indicator.Attribute	Status	`.vulnerabilites[].discovered`	`needed`	Updatable
`.vulnerabilities[].link`	Vulnerability/ Indicator.Attribute	Link	`.vulnerabilites[].discovered`	`https://ubuntu.com/security/CVE-2023-30630`	Updatable
`.vulnerabilities[].packageName`	Vulnerability/ Indicator.Attribute	Package Name	`.vulnerabilites[].discovered`	`dmidecode`	Updatable
`.vulnerabilities[].type`	Vulnerability/ Indicator.Attribute	Type	`.vulnerabilites[].discovered`	`image`	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	2 min 20 seconds
Assets	1
Asset Attributes	1
Vulnerability	3,876
Vulnerability Attributes	19,382

Known Issues / Limitations

- If a Vulnerability Value contains `PRISMA` in its name, it will be replaced with `CVE`.

Change Log

- **Version 1.0.0**
  - Initial release