ThreatQuotient

A Securonix Company

Lansweeper CDF

Version 1.0.0

January 26, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	>= 5.12.0
Support Tier	ThreatQ Supported

Introduction

The Lansweeper CDF integration ingests Lansweeper asset and vulnerability data into ThreatQ to support asset-centric analysis and risk visibility. Assets are mapped to Asset objects with related network identifiers as attributes, while vulnerabilities are ingested as Vulnerability objects and linked back to their associated assets.

The integration provides the following feeds:

- **Lansweeper Assets** - ingests asset data and related indicators.
- **Lansweeper Vulnerabilities** - ingests vulnerability data and links it to assets.

The integration ingests the following object types:

- Assets
- Asset Attributes
- Indicators
- Vulnerabilities
- Vulnerability Attributes

Prerequisites

The integration requires the following:

- A Lansweeper API Token.
- A Lansweeper Site ID

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
6. Select the individual feeds to install, when prompted and click **Install**.

   > 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 C**ommercial** option from the *Category* dropdown (optional).

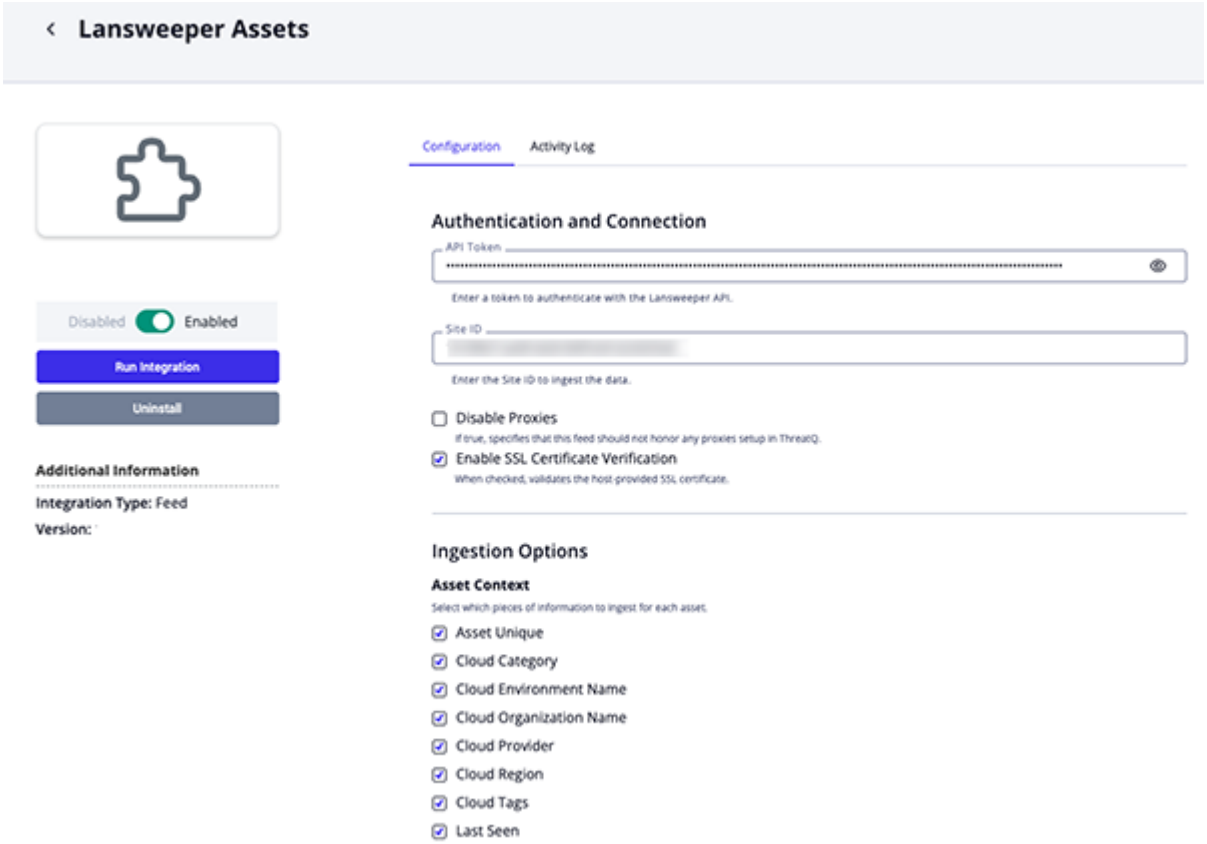
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

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

Lansweeper Assets Parameters

PARAMETER	DESCRIPTION
API Token	Enter your token used to authenticate with the Lansweeper API.
Site ID	Enter the Lansweeper Site ID to ingest data.
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.
Asset Context	Select which pieces of information to ingest for each asset. Options include: ◦ Asset Unique (*default*) ◦ Cloud Category ◦ Scan Server (*default*) ◦ SCCM Server ◦ Sub Type ◦ Type (*default*)

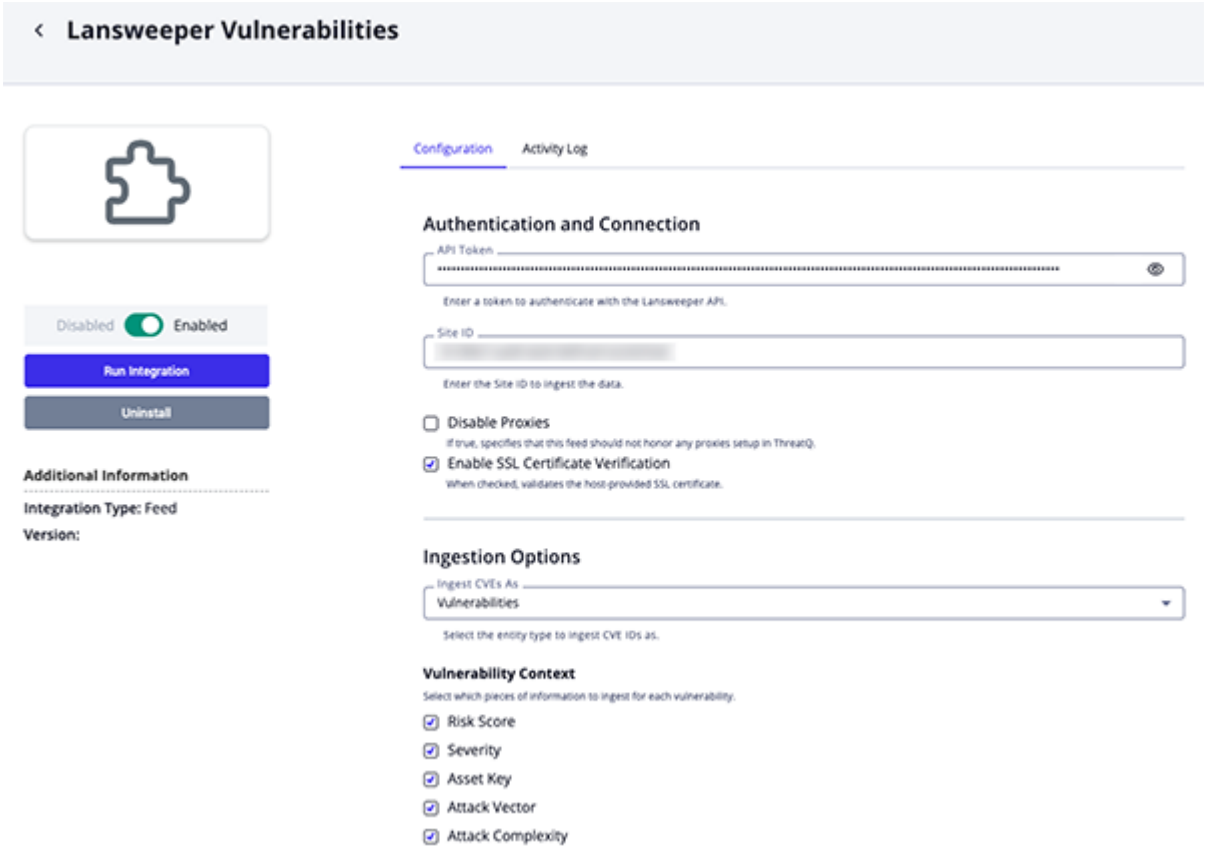
PARAMETER	DESCRIPTION
	◦ Cloud Environment Name ◦ Cloud Organization Name ◦ Cloud Provider ◦ Cloud Region ◦ Last Seen (*default*) ◦ Domain (*default*) ◦ First Seen (*default*) ◦ FQDN (*default*) ◦ IP Address (*default*) ◦ MAC Address (*default*) ◦ Scanner Type (*default*) ◦ Type Group ◦ Type Key (*default*) ◦ Uptime ◦ User SID ◦ Location (*default*) ◦ URL (*default*) ◦ Serial Number ◦ Department (*default*) ◦ CVE/Vulnerability (*default*)
Ingest CVEs As	Select which entity type to ingest CVE IDs as in ThreatQ. Options include: ◦ Vulnerabilities (*default*) ◦ Indicators (Type: CVE)



Lansweeper Vulnerabilities Parameters

PARAMETER	DESCRIPTION
API Token	Enter your token used to authenticate with the Lansweeper API.
Site ID	Enter the Lansweeper Site ID to ingest data.
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.
Ingest CVEs As	Select which entity type to ingest CVE IDs as in ThreatQ. Options include:

PARAMETER	DESCRIPTION
	◦ Vulnerabilities (*default*) ◦ Indicators (Type: CVE)
Vulnerability Context	Select which pieces of information to ingest for each vulnerability. Options include: ◦ Risk Score (*default*) ◦ Severity (*default*) ◦ Asset Key ◦ Attack Vector (*default*) ◦ Attack Complexity (*default*) ◦ Source (*default*) ◦ Updated On ◦ Availability Impact (*default*) ◦ Base Score (*default*) ◦ Confidentiality Impact ◦ Integrity Impact ◦ Privilege Required ◦ Scope ◦ User Interaction ◦ Weakness Enumeration (*default*) ◦ URL (*default*) ◦ Is Active ◦ Cause Category (*default*) ◦ Affected Product (*default*) ◦ Vendor (*default*)



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

Lansweeper Assets

The Lansweeper Assets feed ingests asset information from Lansweeper and filters records based on the `lastChanged` timestamp using the feed start and end dates. Pagination is controlled through the `limit` parameter, with a maximum supported value of `500`. If you encounter HTTP 400 errors, reduce the limit value accordingly. The default limit is `500`.

`POST https://api.lansweeper.com/api/v2/graphql`

Sample Curl:

```
query assetResources($siteID: ID!, $pagination: AssetsPaginationInputValidated,
$conjunction: AssetsFilterConjunction, $condition: [AssetsFiltersCondition!]){
      site(id: $siteID){
        assetResources(
          assetPagination: $pagination,
          fields: [
            "assetBasicInfo.name",
            "assetBasicInfo.assetUnique",
            "assetBasicInfo.cloudCategory",
            "assetBasicInfo.cloudEnvName",
            "assetBasicInfo.cloudOrgName",
            "assetBasicInfo.cloudProvider",
            "assetBasicInfo.cloudRegion",
            "assetBasicInfo.lastSeen",
            "assetBasicInfo.lastChanged",
            "assetBasicInfo.cloudTags",
            "assetBasicInfo.description",
            "assetBasicInfo.domain",
            "assetBasicInfo.firstSeen",
            "assetBasicInfo.fqdn",
            "assetBasicInfo.ipAddress",
            "assetBasicInfo.mac",
            "assetBasicInfo.scannerTypes",
            "assetBasicInfo.scanServer",
            "assetBasicInfo.sccmServer",
            "assetBasicInfo.subType",
            "assetBasicInfo.type",
            "assetBasicInfo.typeGroup",
            "assetBasicInfo.typeKey",
            "assetBasicInfo.upTime",
            "assetBasicInfo.userSid",
            "assetCustom.serialNumber",
            "assetCustom.location",
            "assetCustom.department",
            "url",
```

```
          "vulnerabilities.cve"
        ],
        filters: {
          conjunction: $conjunction,
          conditions: $condition
        }
      ) {
        total
        pagination {
          limit
          current
          next
          page
        }
        items
      }
    }
  }
```

Graph Variables:

```
{
  "siteID": "1610fb57-ea49-4a54-9ef9-e61e2c6253a5",
  "pagination": {
    "limit": 500,
    "page": "FIRST",
    "cursor": "f138eafb-637e-4c25-99ae-de2196655c48"
  },
  "conjunction": "AND",
  "condition": [
    {
      "operator": "GREATER_THAN",
      "path": "assetBasicInfo.lastSeen",
      "value": "2020-01-19T00:00:00Z"
    },
    {
      "operator": "SMALLER_THAN_OR_EQUAL",
      "path": "assetBasicInfo.lastSeen",
      "value": "2026-01-25T00:00:00Z"
    }
  ]
}
```

Sample Response:

```
{
    "data": {
        "site": {
            "assetResources": {
                "total": null,
                "pagination": {
```

```
                    "limit": 3,
                    "current":
"MjY3LUFzc2V0LTVmYmZjN2FlLTllODktNDYxOS05MmQ1LTlhOWI4MDc5ZjY3ZQ==",
                    "next":
"MjY4LUFzc2V0LTVmYmZjN2FlLTllODktNDYxOS05MmQ1LTlhOWI4MDc5ZjY3ZQ==",
                    "page": "NEXT"
                },
                "items": [
                    {
                        "key":
"MjY3LUFzc2V0LTVmYmZjN2FlLTllODktNDYxOS05MmQ1LTlhOWI4MDc5ZjY3ZQ==",
                        "assetBasicInfo": {
                            "scanServer": "uvmjaviprzprod",
                            "domain": "dmz",
                            "name": "UVMPoeWin19Svr",
                            "typeKey":
"LTEtQXNzZXRUeXBlLTE2MTBmYjU3LWVhNDktNGE1NC05ZWY5LWU2MWUyYzYyNTNhNQ==",
                            "type": "Windows",
                            "assetUnique": "dmz\\UVMPoeWin19Svr\\1",
                            "firstSeen": "2022-10-24T16:22:09.000Z",
                            "ipAddress": "10.37.1.37",
                            "lastChanged": "2022-10-24T16:22:15.000Z",
                            "mac": "00:50:56:87:C3:88",
                            "scannerTypes": [
                                "LS",
                                "ActiveDirectory"
                            ],
                            "fqdn": "uvmpoewin19svr.dmz.lab.local"
                        },
                        "assetCustom": {
                            "location": "Belgium",
                            "department": " Delivery"
                        },
                        "url": "https://eu.lansweeper.com/api-demo-data-site/
asset/MjY3LUFzc2V0LTVmYmZjN2FlLTllODktNDYxOS05MmQ1LTlhOWI4MDc5ZjY3ZQ==/summary"
                    },
                    {
                        "key":
"MjY3LUFzc2V0LWQ1NTcyMDRhLWRhMWUtNGQ1Yy1hOWYwLWEzMDFiOWE4MGVmZQ==",
                        "assetBasicInfo": {
                            "domain": "Lansweeper",
                            "name": "Dell Inc. LAN267",
                            "typeKey":
"MjA4LUFzc2V0VHlwZS0xNjEwZmI1Ny1lYTQ5LTRhNTQtOWVmOS1lNjFlMmM2MjUzYTU=",
                            "type": "Monitor",
                            "assetUnique": "Mon:DEL:G332H8AK0NBC",
                            "description": "Demo description",
                            "firstSeen": "2018-02-12T12:59:22.000Z",
                            "lastChanged": "2018-02-12T12:59:22.000Z",
                            "scannerTypes": [
```

```
                                "LS",
                                "ActiveDirectory"
                            ]
                        },
                        "assetCustom": {
                            "location": "Italy",
                            "serialNumber": "LAN267",
                            "department": "Engineering"
                        },
                        "url": "https://eu.lansweeper.com/api-demo-data-site/
asset/MjY3LUFzc2V0LWQ1NTcyMDRhLWRhMWUtNGQ1Yy1hOWYwLWEzMDFiOWE4MGVmZQ==/summary"
                    },
                    {
                        "key":
"MjY4LUFzc2V0LTVmYmZjN2FlLTllODktNDYxOS05MmQ1LTlhOWI4MDc5ZjY3ZQ==",
                        "assetBasicInfo": {
                            "scanServer": "uvmjaviprzprod",
                            "domain": "dmz",
                            "name": "UVMcloudmattc",
                            "typeKey":
"LTEtQXNzZXRUeXBlLTE2MTBmYjU3LWVhNDktNGE1NC05ZWY5LWU2MWUyYzYyNTNhNQ==",
                            "type": "Windows",
                            "assetUnique": "dmz\\UVMcloudmattc\\1",
                            "firstSeen": "2022-10-24T16:22:10.000Z",
                            "ipAddress": "10.37.1.39",
                            "lastChanged": "2022-10-24T16:22:17.000Z",
                            "mac": "00:50:56:87:F6:57",
                            "scannerTypes": [
                                "LS",
                                "ActiveDirectory"
                            ],
                            "fqdn": "uvmcloudmattc.dmz.lab.local"
                        },
                        "assetCustom": {
                            "location": "Belgium",
                            "department": " FInance"
                        },
                        "url": "https://eu.lansweeper.com/api-demo-data-site/
asset/MjY4LUFzc2V0LTVmYmZjN2FlLTllODktNDYxOS05MmQ1LTlhOWI4MDc5ZjY3ZQ==/
summary",
                        "vulnerabilities": [
                            {
                                "cve": "CVE-2022-37994"
                            },
                            {
                                "cve": "CVE-2023-36564"
                            }
                        ]
                    }
                ]
```

```
                }
            }
        }
}
```

ThreatQuotient provides the following default mapping for this feed based on fields within each `.data.site.assetResources.items[]`:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`assetBasicInfo.name`	Asset.Name	N/A	assetBasicInfo.firstSeen	`Desktop-101-EstatesManagement`	N/A
`assetBasicInfo.assetUnique`	Asset.Attribute	Asset Unique	assetBasicInfo.firstSeen	`Mon:DEL:G332H8AK0NBC`	User-configurable
`assetBasicInfo.cloudCategory`	Asset.Attribute	Cloud Category	assetBasicInfo.firstSeen	`N/A`	User-configurable
`assetBasicInfo.cloudEnvName`	Asset.Attribute	Cloud Environment Name	assetBasicInfo.firstSeen	`N/A`	User-configurable
`assetBasicInfo.cloudOrgName`	Asset.Attribute	Cloud Organization Name	assetBasicInfo.firstSeen	`N/A`	User-configurable
`assetBasicInfo.cloudProvider`	Asset.Attribute	Cloud Provider	assetBasicInfo.firstSeen	`N/A`	User-configurable
`assetBasicInfo.cloudRegion`	Asset.Attribute	Cloud Region	assetBasicInfo.firstSeen	`N/A`	User-configurable
`assetBasicInfo.lastSeen`	Asset.Attribute	Last Seen	assetBasicInfo.lastSeen	`2022-08-17T09:14:37.000Z`	User-configurable
`assetBasicInfo.cloudTags`	Asset.Attribute	Cloud Tags	assetBasicInfo.firstSeen	`N/A`	Each value becomes an attribute; User-configurable
`assetBasicInfo.description`	Asset.Description	N/A	assetBasicInfo.firstSeen	`My edited description.`	Mapped to Asset description
`assetBasicInfo.domain`	Asset.Attribute	Domain	assetBasicInfo.firstSeen	`mycorpdomain`	User-configurable
`assetBasicInfo.firstSeen`	Asset.Attribute	First Seen	assetBasicInfo.firstSeen	`2024-05-28T11:18:07.000Z`	Updatable. User-configurable
`assetBasicInfo.fqdn`	Asset.Attribute	FQDN	assetBasicInfo.firstSeen	`TOKLAP188.ESI-INTERNAL.esi-group.com`	Linked to Asset; User-configurable
`assetBasicInfo.ipAddress`	Asset.Attribute	IP Address	assetBasicInfo.firstSeen	`192.168.203.255`	Linked to Asset; User-configurable
`assetBasicInfo.mac`	Asset.Attribute	MAC Address	assetBasicInfo.firstSeen	`d1:01:12:78:b1:49`	Linked to Asset; User-configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`assetBasicInfo.scannerTypes[]`	Asset.Attribute	Scanner Type	assetBasicInfo.firstSeen	`LS`	List of values; User-configurable
`assetBasicInfo.scanServer`	Asset.Attribute	Scan Server	assetBasicInfo.firstSeen	`uvmjaviprzprod`	User-configurable
`assetBasicInfo.sccmServer`	Asset.Attribute	SCCM Server	assetBasicInfo.firstSeen	`N/A`	User-configurable
`assetBasicInfo.subType`	Asset.Attribute	Sub Type	assetBasicInfo.firstSeen	`Undefined`	User-configurable
`assetBasicInfo.type`	Asset.Attribute	Type	assetBasicInfo.firstSeen	`Alarm system`	User-configurable
`assetBasicInfo.typeGroup`	Asset.Attribute	Type Group	assetBasicInfo.firstSeen	`Generic`	User-configurable
`assetBasicInfo.typeKey`	Asset.Attribute	Type Key	assetBasicInfo.firstSeen	`MzMtQXNzZXRUeXBlLTE2MTBmYjU3LWVhNDktNGE1NC05ZWY5LWU2MWUyYzYyNTNhNQ==`	User-configurable
`assetBasicInfo.upTime`	Asset.Attribute	Uptime	assetBasicInfo.firstSeen	`0`	Updatable. User-configurable
`assetBasicInfo.userSid`	Asset.Attribute	User SID	assetBasicInfo.firstSeen	`N/A`	User-configurable
`assetCustom.location`	Asset.Attribute	Location	assetBasicInfo.firstSeen	`USA`	User-configurable
`vulnerabilities[].cve`	Related Indicator/ Vulnerability.Value	CVE/Vulnerability	assetBasicInfo.firstSeen	`CVE-2022-37994`	Ingested according to Ingest CVEs As; User-configurable
`url`	Asset.Attribute	URL	assetBasicInfo.firstSeen	`https://eu.lansweeper.com/api-demo-data-site/asset/23322206-b196-4953-b8ac-0b189dad7062/summary`	User-configurable
`assetCustom.serialNumber`	Asset.Attribute	Serial Number	assetBasicInfo.firstSeen	`DEMOSERIAL1`	User-configurable
`assetCustom.department`	Asset.Attribute	Department	assetBasicInfo.firstSeen	`Sales/Finance`	User-configurable

Lansweeper Vulnerabilities

The Lansweeper Vulnerabilities feed ingests vulnerability data and links it to assets.

`POST https://api.lansweeper.com/api/v2/graphql`

Example Request (vulnerabilities):

```
query getSiteVulnerabilities($siteID: ID!, $pagination:
AssetsPaginationInputValidated, $since: String!, $until: String!) {
  site(id: $siteID) {
    vulnerabilities(
        filters: {
            conjunction: AND
            conditions: [
                {
                    operator: GREATER_THAN,
                    path: "updatedOn",
                    value: $since
                },
                {
                    operator: SMALLER_THAN_OR_EQUAL,
                    path: "updatedOn",
                    value: $until
                }
            ]
        },
        pagination: $pagination ) {
      total
      pagination {
        limit
        current
        next
        page
      }
      items {
        cve
        riskScore
        severity
        assetKeys
        attackVector
        attackComplexity
        source
        updatedOn
        availabilityImpact
        baseScore
        confidentiality
        integrity
        privilegeRequired
        publishedOn
```

```
        scope
        userInteraction
        weaknessEnumeration
        references {
          url
          tags
        }
        isActive
        cause {
          category
          affectedProduct
          vendor
        }
      }
    }
  }
}
```

Graph Variables Sample Curl:

```
{
  "siteID": "1610fb57-ea49-4a54-9ef9-e61e2c6253a5",
  "pagination": {
    "limit": 500,
    "cursor": "eyJvZmZzZXQiOjYwMH0=",
    "page": "FIRST"
  },
  "since": "2026-01-01T00:00:00Z",
  "until": "2026-01-10T00:00:00Z"
}
```

Sample Response:

```
{
    "data": {
        "site": {
            "vulnerabilities": {
                "total": null,
                "pagination": {
                    "limit": 5,
                    "current": "eyJvZmZzZXQiOjEwNX0=",
                    "next": "eyJvZmZzZXQiOjEwNX0=",
                    "page": "NEXT"
                },
                "items": [
                    {
                        "cve": "CVE-2022-2617",
                        "riskScore": 8.8,
                        "severity": "High",
                        "assetKeys": [
```

```
"My1Bc3NldC01ZmJmYzdhZS05ZTg5LTQ2MTktOTJkNS05YTliODA3OWY2N2U="
                        ],
                        "attackVector": "Network",
                        "attackComplexity": "Low",
                        "source": "Google",
                        "updatedOn": "2026-01-08 00:05:11.213",
                        "availabilityImpact": "HIGH",
                        "baseScore": 8.8,
                        "confidentiality": "HIGH",
                        "integrity": "HIGH",
                        "privilegeRequired": "NONE",
                        "publishedOn": "2022-08-12 20:15:09.197",
                        "scope": "UNCHANGED",
                        "userInteraction": "REQUIRED",
                        "weaknessEnumeration": [
                            "CWE-362"
                        ],
                        "references": [
                            {
                                "url": "https://bdu.fstec.ru/vul/2022-05429",
                                "tags": [
                                    "Government Advisory",
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.cert.ssi.gouv.fr/avis/
CERTFR-2022-AVI-702/",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://security-tracker.debian.org/
tracker/DSA-5201-1",
                                "tags": [
                                    "Vendor Advisory",
                                    "Operating Systems"
                                ]
                            },
                            {
                                "url": "https://crbug.com/1292451",
                                "tags": [
                                    "Issue Tracking",
                                    "Permissions Required",
                                    "Vendor Advisory"
                                ]
                            },
                            {
                                "url": "https://lists.fedoraproject.org/
archives/list/package-announce%40lists.fedoraproject.org/message/
```

```
T4NMJURTG5RO3TGD7ZMIQ6Z4ZZ3SAVYE/",
                                "tags": []
                            },
                            {
                                "url": "https://security.gentoo.org/glsa/
202208-35",
                                "tags": [
                                    "Third Party Advisory"
                                ]
                            },
                            {
                                "url": "https://vulnerabilities.ncsc.nl/csaf/
v2/2022/cve-2022-2617.json",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163724",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163725",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163766",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163893",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163913",
                                "tags": [
                                    "Signature"
                                ]
```

```
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
164107",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
164320",
                                "tags": [
                                    "Signature"
                                ]
                            }
                        ],
                        "exploitability": {
                            "exploitable": "Unknown",
                            "exploitedInTheWild": "Unknown",
                            "CISA": {
                                "dueDate": null,
                                "exploited": "Unknown",
                                "knownRansomwareCampaignUse": "Unknown"
                            },
                            "MSRC": {
                                "exploitability": "Unknown"
                            },
                            "NVD": {
                                "exploitability": "Low",
                                "impact": "Medium"
                            }
                        },
                        "isActive": true,
                        "cause": {
                            "category": [
                                "Software"
                            ],
                            "affectedProduct": [
                                "Chrome 103.0.5060.66"
                            ],
                            "vendor": [
                                "Google"
                            ]
                        }
                    },
                    {
                        "cve": "CVE-2022-2614",
                        "riskScore": 8.8,
                        "severity": "High",
                        "assetKeys": [
```

```
"My1Bc3NldC01ZmJmYzdhZS05ZTg5LTQ2MTktOTJkNS05YTliODA3OWY2N2U="
                        ],
                        "attackVector": "Network",
                        "attackComplexity": "Low",
                        "source": "Google",
                        "updatedOn": "2026-01-08 00:05:11.213",
                        "availabilityImpact": "HIGH",
                        "baseScore": 8.8,
                        "confidentiality": "HIGH",
                        "integrity": "HIGH",
                        "privilegeRequired": "NONE",
                        "publishedOn": "2022-08-12 20:15:09.073",
                        "scope": "UNCHANGED",
                        "userInteraction": "REQUIRED",
                        "weaknessEnumeration": [
                            "CWE-416"
                        ],
                        "references": [
                            {
                                "url": "https://bdu.fstec.ru/vul/2022-05361",
                                "tags": [
                                    "Government Advisory",
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.cert.ssi.gouv.fr/avis/
CERTFR-2022-AVI-702/",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "http://www.cnnvd.org.cn/web/xxk/
ldxqById.tag?CNNVD=CNNVD-202208-2082",
                                "tags": [
                                    "Government Advisory",
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://security-tracker.debian.org/
tracker/DSA-5201-1",
                                "tags": [
                                    "Vendor Advisory",
                                    "Operating Systems"
                                ]
                            },
                            {
```

```
                                "url": "https://github.com/github/advisory-
database/blob/main/advisories/unreviewed/2022/08/GHSA-7ggx-3w8m-q494/
GHSA-7ggx-3w8m-q494.json",
                                "tags": [
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.hkcert.org/security-
bulletin/google-chrome-multiple-vulnerabilities_20220803",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://jvndb.jvn.jp/ja/contents/2022/
JVNDB-2022-016700.html",
                                "tags": [
                                    "Government Advisory",
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://api.msrc.microsoft.com/cvrf/
v3.0/cvrf/2022-Aug",
                                "tags": [
                                    "Vendor Advisory"
                                ]
                            },
                            {
                                "url": "https://crbug.com/1341907",
                                "tags": [
                                    "Issue Tracking",
                                    "Permissions Required",
                                    "Vendor Advisory"
                                ]
                            },
                            {
                                "url": "https://www.rapid7.com/db/
vulnerabilities/ubuntu-cve-2022-2614/",
                                "tags": [
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.csa.gov.sg/alerts-
advisories/security-bulletins/2022/sb-2022-045",
                                "tags": [
                                    "Government Advisory"
                                ]
```

```
                            },
                            {
                                "url": "https://ubuntu.com/security/
CVE-2022-2614",
                                "tags": [
                                    "Vendor Advisory",
                                    "Operating Systems"
                                ]
                            },
                            {
                                "url": "https://www.usom.gov.tr/bildirim/
tr-22-0535",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://www.usom.gov.tr/bildirim/
tr-22-0538",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://www.usom.gov.tr/bildirim/
tr-22-0551",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://www.cve.org/CVERecord?
id=CVE-2022-2614",
                                "tags": [
                                    "VDB Entry"
                                ]
                            }
                        ],
                        "exploitability": {
                            "exploitable": "Unknown",
                            "exploitedInTheWild": "Unknown",
                            "CISA": {
                                "dueDate": null,
                                "exploited": "Unknown",
                                "knownRansomwareCampaignUse": "Unknown"
                            },
                            "MSRC": {
                                "exploitability": "Unknown"
                            },
                            "NVD": {
```

```
                            "exploitability": "Low",
                            "impact": "Medium"
                        }
                    },
                    "isActive": true,
                    "cause": {
                        "category": [
                            "Software"
                        ],
                        "affectedProduct": [
                            "Chrome 103.0.5060.66"
                        ],
                        "vendor": [
                            "Google"
                        ]
                    }
                },
                {
                    "cve": "CVE-2022-2613",
                    "riskScore": 8.8,
                    "severity": "High",
                    "assetKeys": [
"My1Bc3NldC01ZmJmYzdhZS05ZTg5LTQ2MTktOTJkNS05YTliODA3OWY2N2U="
                    ],
                    "attackVector": "Network",
                    "attackComplexity": "Low",
                    "source": "Google",
                    "updatedOn": "2026-01-08 00:05:11.213",
                    "availabilityImpact": "HIGH",
                    "baseScore": 8.8,
                    "confidentiality": "HIGH",
                    "integrity": "HIGH",
                    "privilegeRequired": "NONE",
                    "publishedOn": "2022-08-12 20:15:09.030",
                    "scope": "UNCHANGED",
                    "userInteraction": "REQUIRED",
                    "weaknessEnumeration": [
                        "CWE-416"
                    ],
                    "references": [
                        {
                            "url": "https://bdu.fstec.ru/vul/2022-05747",
                            "tags": [
                                "Government Advisory",
                                "VDB Entry"
                            ]
                        },
                        {
                            "url": "https://www.cert.ssi.gouv.fr/avis/
```

```
CERTFR-2022-AVI-702/",
                                    "tags": [
                                        "Government Advisory"
                                    ]
                                },
                                {
                                    "url": "https://chromereleases.googleblog.com/
2022/08/stable-channel-update-for-desktop.html",
                                    "tags": [
                                        "Vendor Advisory"
                                    ]
                                },
                                {
                                    "url": "https://chromereleases.googleblog.com/
2022/08/stable-channel-promotion-for-chromeos.html",
                                    "tags": [
                                        "Vendor Advisory"
                                    ]
                                },
                                {
                                    "url": "https://chromereleases.googleblog.com/
2022/10/long-term-support-channel-update-for.html",
                                    "tags": [
                                        "Vendor Advisory"
                                    ]
                                },
                                {
                                    "url": "http://www.cnnvd.org.cn/web/xxk/
ldxqById.tag?CNNVD=CNNVD-202208-2087",
                                    "tags": [
                                        "Government Advisory",
                                        "VDB Entry"
                                    ]
                                },
                                {
                                    "url": "https://security-tracker.debian.org/
tracker/DSA-5201-1",
                                    "tags": [
                                        "Vendor Advisory",
                                        "Operating Systems"
                                    ]
                                },
                                {
                                    "url": "https://github.com/github/advisory-
database/blob/main/advisories/unreviewed/2022/08/GHSA-m3ww-86w6-hqwq/GHSA-
m3ww-86w6-hqwq.json",
                                    "tags": [
                                        "VDB Entry"
                                    ]
                                },
                                {
```

```
                                "url": "https://www.hkcert.org/security-
bulletin/google-chrome-multiple-vulnerabilities_20220803",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://www.hkcert.org/security-
bulletin/chromeos-multiple-vulnerabilities_20221005",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://jvndb.jvn.jp/ja/contents/2022/
JVNDB-2022-016701.html",
                                "tags": [
                                    "Government Advisory",
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://crbug.com/1325256",
                                "tags": [
                                    "Issue Tracking",
                                    "Permissions Required",
                                    "Vendor Advisory"
                                ]
                            },
                            {
                                "url": "https://lists.fedoraproject.org/
archives/list/package-announce%40lists.fedoraproject.org/message/
T4NMJURTG5RO3TGD7ZMIQ6Z4ZZ3SAVYE/",
                                "tags": []
                            },
                            {
                                "url": "https://security.gentoo.org/glsa/
202208-35",
                                "tags": [
                                    "Third Party Advisory"
                                ]
                            },
                            {
                                "url": "https://vulnerabilities.ncsc.nl/csaf/
v2/2022/cve-2022-2613.json",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
```

```
                                "url": "https://www.tenable.com/plugins/nessus/
163724",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163725",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163766",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163913",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
164107",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
164320",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
169098",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
```

```
169151",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
211177",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.rapid7.com/db/
vulnerabilities/google-chrome-cve-2022-2613/",
                                "tags": [
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.rapid7.com/db/
vulnerabilities/gentoo-linux-cve-2022-2613/",
                                "tags": [
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.rapid7.com/db/
vulnerabilities/suse-cve-2022-2613/",
                                "tags": [
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.rapid7.com/db/
vulnerabilities/debian-cve-2022-2613/",
                                "tags": [
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.rapid7.com/db/
vulnerabilities/freebsd-cve-2022-2613/",
                                "tags": [
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.rapid7.com/db/
vulnerabilities/ubuntu-cve-2022-2613/",
                                "tags": [
```

```
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.csa.gov.sg/alerts-
advisories/security-bulletins/2022/sb-2022-045",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://ubuntu.com/security/
CVE-2022-2613",
                                "tags": [
                                    "Vendor Advisory",
                                    "Operating Systems"
                                ]
                            },
                            {
                                "url": "https://www.usom.gov.tr/bildirim/
tr-22-0535",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://www.usom.gov.tr/bildirim/
tr-22-0551",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://www.cve.org/CVERecord?
id=CVE-2022-2613",
                                "tags": [
                                    "VDB Entry"
                                ]
                            }
                        ],
                        "exploitability": {
                            "exploitable": "Unknown",
                            "exploitedInTheWild": "Unknown",
                            "CISA": {
                                "dueDate": null,
                                "exploited": "Unknown",
                                "knownRansomwareCampaignUse": "Unknown"
                            },
                            "MSRC": {
                                "exploitability": "Unknown"
```

```
                            },
                            "NVD": {
                                "exploitability": "Low",
                                "impact": "Medium"
                            }
                        },
                        "isActive": true,
                        "cause": {
                            "category": [
                                "Software"
                            ],
                            "affectedProduct": [
                                "Chrome 103.0.5060.66"
                            ],
                            "vendor": [
                                "Google"
                            ]
                        }
                    },
                    {
                        "cve": "CVE-2022-2609",
                        "riskScore": 8.8,
                        "severity": "High",
                        "assetKeys": [

"My1Bc3NldC01ZmJmYzdhZS05ZTg5LTQ2MTktOTJkNS05YTliODA3OWY2N2U="
                        ],
                        "attackVector": "Network",
                        "attackComplexity": "Low",
                        "source": "Google",
                        "updatedOn": "2026-01-09 00:05:18.434",
                        "availabilityImpact": "HIGH",
                        "baseScore": 8.8,
                        "confidentiality": "HIGH",
                        "integrity": "HIGH",
                        "privilegeRequired": "NONE",
                        "publishedOn": "2022-08-12 20:15:08.863",
                        "scope": "UNCHANGED",
                        "userInteraction": "REQUIRED",
                        "weaknessEnumeration": [
                            "CWE-362"
                        ],
                        "references": [
                            {
                                "url": "https://bdu.fstec.ru/vul/2022-05665",
                                "tags": [
                                    "Government Advisory",
                                    "VDB Entry"
                                ]
                            },
```

```
                            {
                                "url": "https://www.cert.ssi.gouv.fr/avis/
CERTFR-2022-AVI-702/",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://chromereleases.googleblog.com/
2022/08/stable-channel-update-for-desktop.html",
                                "tags": [
                                    "Vendor Advisory"
                                ]
                            },
                            {
                                "url": "https://chromereleases.googleblog.com/
2022/08/stable-channel-promotion-for-chromeos.html",
                                "tags": [
                                    "Vendor Advisory"
                                ]
                            },
                            {
                                "url": "https://chromereleases.googleblog.com/
2022/09/long-term-support-candidate-channel-for.html",
                                "tags": [
                                    "Vendor Advisory"
                                ]
                            },
                            {
                                "url": "http://www.cnnvd.org.cn/web/xxk/
ldxqById.tag?CNNVD=CNNVD-202208-2089",
                                "tags": [
                                    "Government Advisory",
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://security-tracker.debian.org/
tracker/DSA-5201-1",
                                "tags": [
                                    "Vendor Advisory",
                                    "Operating Systems"
                                ]
                            },
                            {
                                "url": "https://github.com/github/advisory-
database/blob/main/advisories/unreviewed/2022/08/GHSA-95q6-7mr2-cvjh/
GHSA-95q6-7mr2-cvjh.json",
                                "tags": [
                                    "VDB Entry"
```

```
                                ]
                            },
                            {
                                "url": "https://www.hkcert.org/security-
bulletin/google-chrome-multiple-vulnerabilities_20220803",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://jvndb.jvn.jp/ja/contents/2022/
JVNDB-2022-016705.html",
                                "tags": [
                                    "Government Advisory",
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://crbug.com/1338560",
                                "tags": [
                                    "Issue Tracking",
                                    "Permissions Required",
                                    "Vendor Advisory"
                                ]
                            },
                            {
                                "url": "https://lists.fedoraproject.org/
archives/list/package-announce%40lists.fedoraproject.org/message/
T4NMJURTG5RO3TGD7ZMIQ6Z4ZZ3SAVYE/",
                                "tags": []
                            },
                            {
                                "url": "https://security.gentoo.org/glsa/
202208-35",
                                "tags": [
                                    "Third Party Advisory"
                                ]
                            },
                            {
                                "url": "https://vulnerabilities.ncsc.nl/csaf/
v2/2022/cve-2022-2609.json",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163724",
                                "tags": [
                                    "Signature"
```

```
                            ]
                        },
                        {
                            "url": "https://www.tenable.com/plugins/nessus/
163725",
                            "tags": [
                                "Signature"
                            ]
                        },
                        {
                            "url": "https://www.tenable.com/plugins/nessus/
163766",
                            "tags": [
                                "Signature"
                            ]
                        },
                        {
                            "url": "https://www.tenable.com/plugins/nessus/
163913",
                            "tags": [
                                "Signature"
                            ]
                        },
                        {
                            "url": "https://www.tenable.com/plugins/nessus/
164107",
                            "tags": [
                                "Signature"
                            ]
                        },
                        {
                            "url": "https://ubuntu.com/security/
CVE-2022-2609",
                            "tags": [
                                "Vendor Advisory",
                                "Operating Systems"
                            ]
                        },
                        {
                            "url": "https://www.usom.gov.tr/bildirim/
tr-22-0535",
                            "tags": [
                                "Government Advisory"
                            ]
                        },
                        {
                            "url": "https://www.usom.gov.tr/bildirim/
tr-22-0551",
                            "tags": [
                                "Government Advisory"
```

```
                                ]
                            },
                            {
                                "url": "https://www.cve.org/CVERecord?
id=CVE-2022-2609",
                                "tags": [
                                    "VDB Entry"
                                ]
                            }
                        ],
                        "exploitability": {
                            "exploitable": "Unknown",
                            "exploitedInTheWild": "Unknown",
                            "CISA": {
                                "dueDate": null,
                                "exploited": "Unknown",
                                "knownRansomwareCampaignUse": "Unknown"
                            },
                            "MSRC": {
                                "exploitability": "Unknown"
                            },
                            "NVD": {
                                "exploitability": "Low",
                                "impact": "Medium"
                            }
                        },
                        "isActive": true,
                        "cause": {
                            "category": [
                                "Software"
                            ],
                            "affectedProduct": [
                                "Chrome 103.0.5060.66"
                            ],
                            "vendor": [
                                "Google"
                            ]
                        }
                    },
                    {
                        "cve": "CVE-2022-2608",
                        "riskScore": 8.8,
                        "severity": "High",
                        "assetKeys": [

"My1Bc3NldC01ZmJmYzdhZS05ZTg5LTQ2MTktOTJkNS05YTliODA3OWY2N2U="
                        ],
                        "attackVector": "Network",
                        "attackComplexity": "Low",
                        "source": "Google",
```

```
                        "updatedOn": "2026-01-08 00:05:11.213",
                        "availabilityImpact": "HIGH",
                        "baseScore": 8.8,
                        "confidentiality": "HIGH",
                        "integrity": "HIGH",
                        "privilegeRequired": "NONE",
                        "publishedOn": "2022-08-12 20:15:08.823",
                        "scope": "UNCHANGED",
                        "userInteraction": "REQUIRED",
                        "weaknessEnumeration": [
                            "CWE-362"
                        ],
                        "references": [
                            {
                                "url": "https://bdu.fstec.ru/vul/2022-05746",
                                "tags": [
                                    "Government Advisory",
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.cert.ssi.gouv.fr/avis/
CERTFR-2022-AVI-702/",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://chromereleases.googleblog.com/
2022/08/stable-channel-update-for-desktop.html",
                                "tags": [
                                    "Vendor Advisory"
                                ]
                            },
                            {
                                "url": "https://jvndb.jvn.jp/ja/contents/2022/
JVNDB-2022-016707.html",
                                "tags": [
                                    "Government Advisory",
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://crbug.com/1330775",
                                "tags": [
                                    "Issue Tracking",
                                    "Permissions Required",
                                    "Vendor Advisory"
                                ]
                            },
```

```
                            {
                                "url": "https://lists.fedoraproject.org/
archives/list/package-announce%40lists.fedoraproject.org/message/
T4NMJURTG5RO3TGD7ZMIQ6Z4ZZ3SAVYE/",
                                "tags": []
                            },
                            {
                                "url": "https://security.gentoo.org/glsa/
202208-35",
                                "tags": [
                                    "Third Party Advisory"
                                ]
                            },
                            {
                                "url": "https://vulnerabilities.ncsc.nl/csaf/
v2/2022/cve-2022-2608.json",
                                "tags": [
                                    "Government Advisory"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163724",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163725",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163766",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
163913",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
```

```
164107",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
164320",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
169098",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
169151",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.tenable.com/plugins/nessus/
211177",
                                "tags": [
                                    "Signature"
                                ]
                            },
                            {
                                "url": "https://www.rapid7.com/db/
vulnerabilities/google-chrome-cve-2022-2608/",
                                "tags": [
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.rapid7.com/db/
vulnerabilities/gentoo-linux-cve-2022-2608/",
                                "tags": [
                                    "VDB Entry"
                                ]
                            },
                            {
                                "url": "https://www.cve.org/CVERecord?
id=CVE-2022-2608",
                                "tags": [
```

```
                                "VDB Entry"
                            ]
                        }
                    ],
                    "exploitability": {
                        "exploitable": "Unknown",
                        "exploitedInTheWild": "Unknown",
                        "CISA": {
                            "dueDate": null,
                            "exploited": "Unknown",
                            "knownRansomwareCampaignUse": "Unknown"
                        },
                        "MSRC": {
                            "exploitability": "Unknown"
                        },
                        "NVD": {
                            "exploitability": "Low",
                            "impact": "Medium"
                        }
                    },
                    "isActive": true,
                    "cause": {
                        "category": [
                            "Software"
                        ],
                        "affectedProduct": [
                            "Chrome 103.0.5060.66"
                        ],
                        "vendor": [
                            "Google"
                        ]
                    }
                }
            ]
        }
    }
}
```

ThreatQuotient provides the following default mapping for this feed based on fields within each `.data.site.vulnerabilities.items[]`:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`cve`	Vulnerability.Value	N/A	publishedOn	`CVE-2022-38034`	N/A
`riskScore`	Vulnerability.Attribute	Risk Score	publishedOn	`8.8`	User-configurable
`severity`	Vulnerability.Attribute	Severity	publishedOn	`High`	User-configurable
`assetKeys[]`	Vulnerability.Attribute	Asset Key	N/A	`MTA5LUFzc2V0LTVmYmZjN2FlLTllODktNDYxOS05MmQ1LTlhOWI4MDc5ZjY3ZQ==`	Used to relate vulnerability to assets; User-configurable
`attackVector`	Vulnerability.Attribute	Attack Vector	publishedOn	`Network`	User-configurable
`attackComplexity`	Vulnerability.Attribute	Attack Complexity	publishedOn	`Low`	User-configurable
`source`	Vulnerability.Attribute	Source	publishedOn	`Microsoft`	User-configurable
`updatedOn`	Vulnerability.Attribute	Updated On	updatedOn	`2026-01-07 0:05:20`	User-configurable
`availabilityImpact`	Vulnerability.Attribute	Availability Impact	publishedOn	`HIGH`	User-configurable
`baseScore`	Vulnerability.Attribute	Base Score	publishedOn	`8.8`	User-configurable
`confidentiality`	Vulnerability.Attribute	Confidentiality Impact	publishedOn	`HIGH`	User-configurable
`integrity`	Vulnerability.Attribute	Integrity Impact	publishedOn	`HIGH`	User-configurable
`privilegeRequired`	Vulnerability.Attribute	Privilege Required	publishedOn	`LOW`	User-configurable
`scope`	Vulnerability.Attribute	Scope	publishedOn	`UNCHANGED`	User-configurable
`userInteraction`	Vulnerability.Attribute	User Interaction	publishedOn	`NONE`	User-configurable
`weaknessEnumeration[]`	Vulnerability.Attribute	Weakness	publishedOn	`N/A`	Array of values; User-configurable
`references[].url`	Vulnerability.Attribute	URL	publishedOn	`https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-38034`	Linked to Vulnerability; User-configurable
`references[].tags[]`	Vulnerability.Attribute	N/A	N/A	`Vendor Advisory`	Applied to the related reference URL; User-configurable
`isActive`	Vulnerability.Attribute	Is Active	publishedOn	`TRUE`	User-configurable
`cause.category[]`	Vulnerability.Attribute	Cause Category	publishedOn	`OS`	User-configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`cause.affectedProduct[]`	Vulnerability.Attribute	Affected Product	publishedOn	`Windows 11 21h2`	User-configurable
`cause.vendor[]`	Vulnerability.Attribute	Vendor	publishedOn	`Microsoft`	User-configurable

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.

Lansweeper Assets

METRIC	RESULT
Run Time	1 minute
Assets	29
Asset Attributes	474
Indicators	1,574

Lansweeper Vulnerabilities

METRIC	RESULT
Run Time	1 minute
Vulnerabilities	8
Vulnerability Attributes	87

Known Issues / Limitations

- **Lansweeper Assets** - pagination is controlled through the `limit` parameter, with a maximum supported value of `500`. If you encounter HTTP 400 errors, reduce the limit value accordingly. The default limit is `500`.

Change Log

- **Version 1.0.0**
  - Initial release