ThreatQuotient

Secureworks CDF

Version 1.1.0

August 26, 2024

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	1.1.0
Compatible with ThreatQ Versions	>= 4.23.1
Support Tier	ThreatQ Supported

Introduction

The Secureworks CDF ingests threat intelligence data on events, indicators, reports, and vulnerabilities from the Secureworks provider.

The integration provides the following feeds:

- **Secureworks** - ingests Vulnerabilities, Indicators, and Reports from Secureworks.
- **Secureworks Alerts** - ingests Events objects from Secureworks

The integration ingests the following system object types:

- Events
- Indicators
- Reports
- Vulnerabilities

Prerequisites

The following is required to use the integration:

- Secureworks API Key
- Secureworks API Hostname
- Secureworks Client ID
- Secureworks Client Secret
- Sercureworks Client Tenant

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 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:

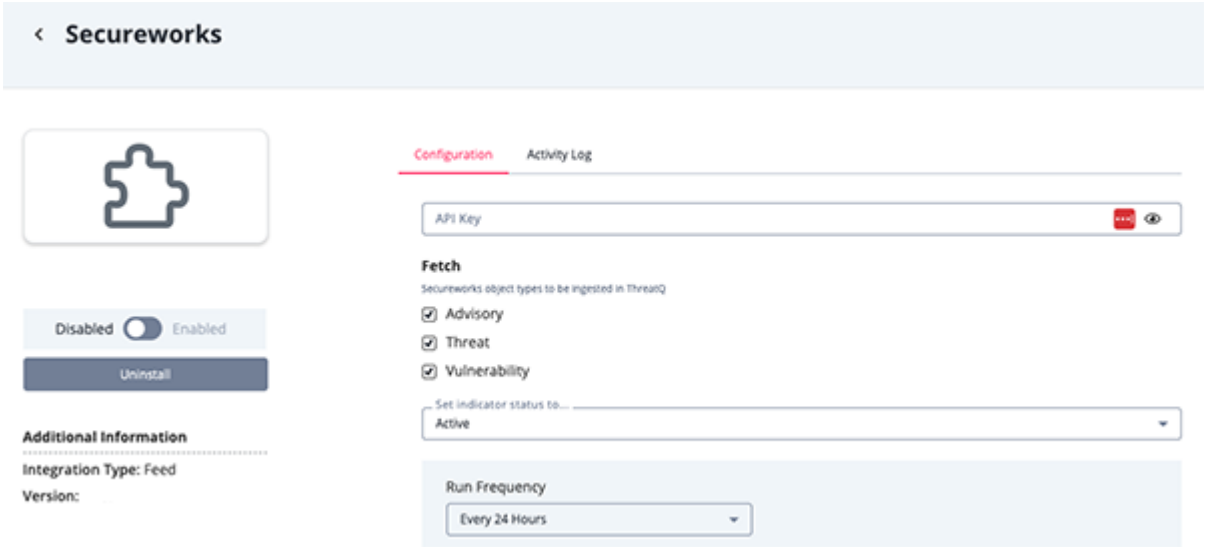
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > 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:

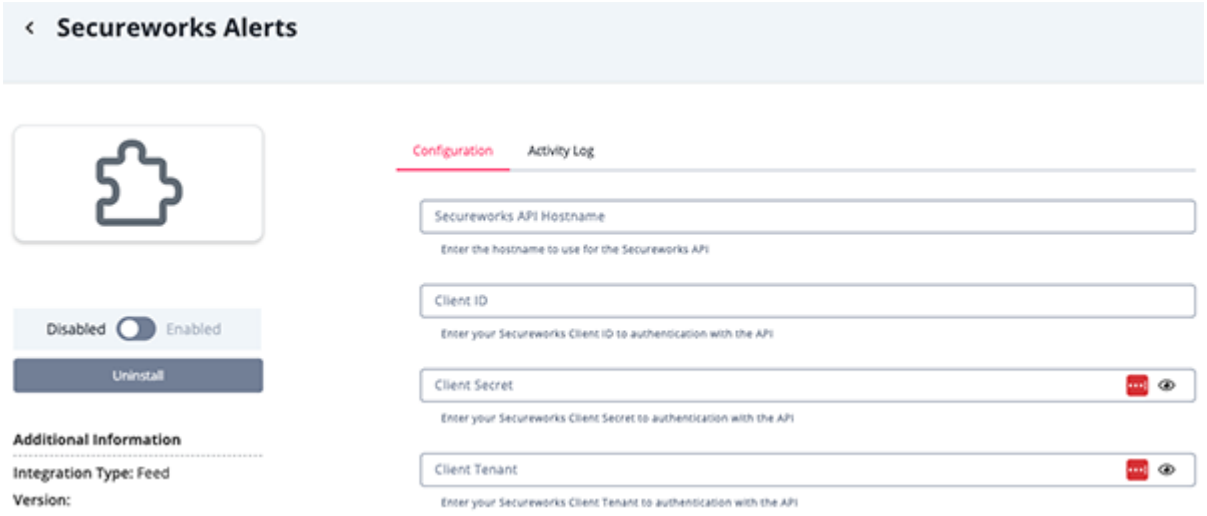
Secureworks Parameters

PARAMETER	DESCRIPTION
API Key	Your Secureworks API Key.
Fetch	Select the objects types to be ingested into the ThreatQ platform. Options include: ◦ Advisory (default) ◦ Threat (default) ◦ Vulnerability (default)



Secureworks Alerts Parameters

PARAMETER	DESCRIPTION
Secureworks API Hostname	Your Secureworks account API hostname.
Client ID	Your Secureworks Client ID.
Client Secret	Your Secureworks Client Secret.
Client Tenant	Your Securewors Client Tenant.



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

Secureworks

The Secureworks feed ingests ingests Vulnerabilities and Reports from Secureworks.

```
GET https://ws.secureworks.com/ti/feed-token/threatIntel
```

Sample Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<Intelligence time_t="1558467371598" from="1556668800000" to="1558396800000">
    <Threats>
        <Threat id="1251">
            <Created time_t="1555520403000">2019-04-17 17:00:03</Created>
            <Updated time_t="1557161402000">2019-05-06 16:50:02</Updated>
            <Impact value="1">Medium</Impact>
            <Title>Underground Insights Brief - February 2019</Title>
            <Summary>Dummy Summary</Summary>
            <Analysis>Dummy Analysis</Analysis>
            <Solution>Dummy Solution</Solution>
            <Type>Thread</Type>
            <ModificationHistory>2019-04-17 17:00:02 UTC - Initial revision</ModificationHistory>
            <Associations></Associations>
        </Threat>
        <Threat id="1257">
            <Created time_t="1556882402000">2019-05-03 11:20:02</Created>
            <Updated time_t="1556882402000">2019-05-03 11:20:02</Updated>
            <Impact value="1">Medium</Impact>
            <Title>Country Threat Assessment: People's Republic of China (2019)</Title>
            <Summary>Dummy Summary</Summary>
            <Analysis>Dummy Analysis</Analysis>
            <Solution>Dummy Solution</Solution>
            <Type>Thread</Type>
            <ModificationHistory>2019-05-03 11:20:02 UTC - Initial revision</ModificationHistory>
            <Associations>
                <Threat id="1089"></Threat>
                <Vulnerability id="229701"></Vulnerability>
                <Vulnerability id="229702"></Vulnerability>
            </Associations>
        </Threat>
        <Threat id="1258">
            <Created time_t="1556882402000">2019-05-03 11:20:02</Created>
            <Updated time_t="1556882402000">2019-05-03 11:20:02</Updated>
            <Impact value="1">Medium</Impact>
            <Title>Dummy</Title>
            <Summary>Dummy Summary</Summary>
            <Analysis>Dummy Analysis</Analysis>
            <Solution>Dummy Solution</Solution>
            <Type>Thread</Type>
            <ModificationHistory>2019-05-03 11:20:02 UTC - Initial revision</ModificationHistory>
            <Associations>
                <Threat id="1089"></Threat>
                <Threat id="1169"></Threat>
                <Threat id="1233"></Threat>
                <Threat id="1203"></Threat>
                <Threat id="1183"></Threat>
                <Advisory id="1111"></Advisory>
            </Associations>
```

```
        </Threat>
    </Threats>
    <Advisories>
        <Advisory id="275">
            <Created time_t="1560538802000">2019-06-14 19:00:02</Created>
            <Impact value="2">High</Impact>
            <Subject>Secureworks Security Advisory - Exploitation of EXIM Mail Transport Agent
vulnerability (CVE-2019-10149) - Action Recommended</Subject>
            <Type>Advisory</Type>
            <Detail>Dummy Detail</Detail>
            <Associations>
                <Vulnerability id="229701"></Vulnerability>
            </Associations>
        </Advisory>
    </Advisories>
    <Vulnerabilities>
        <Vulnerability id="232739">
            <Created time_t="1562765403000">2019-07-10 13:30:03</Created>
            <Updated time_t="1562765403000">2019-07-10 13:30:03</Updated>
            <Impact value="1">Medium</Impact>
            <ImpactV3 value="2">High</ImpactV3>
            <Type>Design Error</Type>
            <CVE>CVE-2019-13351</CVE>
            <Title>(CVE-2019-13351) JACK2 JackSocket.cpp Double File Descriptor Close Vulnerability</
Title>
            <References>
                <Reference>https://github.com/jackaudio/jack2/commit/
dad4b5702782eef3bd66e3c3f4fefaaae3571208</Reference>
                <Reference>https://github.com/jackaudio/jack2/pull/480</Reference>
                <Reference>https://github.com/xbmc/xbmc/issues/16258</Reference>
                <Reference>http://jackaudio.org</Reference>
            </References>
            <Summary>Dummy Summary</Summary>
            <Analysis>Dummy Analysis</Analysis>
            <Solution>Dummy Solution</Solution>
            <Version>1</Version>
            <ModificationHistory>Initial Revision (rev 0) Entered on July 10, 2019</
ModificationHistory>
            <Associations></Associations>
            <Affected_Vendors>
                <Vendor>
                    <Name id="113119">Kodi</Name>
                    <Product id="182859">Kodi</Product>
                    <Version id="0">0</Version>
                </Vendor>
                <Vendor>
                    <Name id="125553">jackaudio</Name>
                    <Product id="242795">JACK2</Product>
                    <Version id="0">0</Version>
                </Vendor>
            </Affected_Vendors>
            <AffectedCPEs>
                <Cpe>cpe:/a:kodi:kodi</Cpe>
                <Cpe>cpe:/a:jackaudio:jack2</Cpe>
            </AffectedCPEs>
            <CVSS>
                <CVSSv2>
                    <CVSSScore>5.5</CVSSScore>
                    <BaseMetrics>
                        <score>7.5</score>
                        <access_vector>network</access_vector>
                        <access_complexity>low</access_complexity>
                        <authentication_needed>none</authentication_needed>
                        <confidentiality_impact>partial</confidentiality_impact>
```

```
                        <integrity_impact>partial</integrity_impact>
                        <availability_impact>partial</availability_impact>
                    </BaseMetrics>
                    <TemporalMetrics>
                        <score>5.5</score>
                        <exploitability>unproven</exploitability>
                        <remediation_level>official_fix</remediation_level>
                        <report_confidence>confirmed</report_confidence>
                    </TemporalMetrics>
                </CVSSv2>
                <CVSSv3>
                    <CVSSScore>7.3</CVSSScore>
                    <BaseMetrics>
                        <score>8.4</score>
                        <attack_vector>local</attack_vector>
                        <attack_complexity>low</attack_complexity>
                        <privileges_required>none</privileges_required>
                        <user_interaction>none</user_interaction>
                        <scope>unchanged</scope>
                        <confidentiality>high</confidentiality>
                        <integrity>high</integrity>
                        <availability>high</availability>
                        <uri>CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</uri>
                    </BaseMetrics>
                    <TemporalMetrics>
                        <score>7.3</score>
                        <exploit_code_maturity>unproven</exploit_code_maturity>
                        <remediation_level>official_fix</remediation_level>
                        <report_confidence>confirmed</report_confidence>
                    </TemporalMetrics>
                </CVSSv3>
            </CVSS>
            <ChangeSummary>Initial Revision (rev 0) Entered on July 10, 2019</ChangeSummary>
            <CWEs>
                <CWE id="910">CWE-910 - Use of Expired File Descriptor</CWE>
            </CWEs>
        </Vulnerability>
        <Vulnerability id="232741">
            <Created time_t="1562767204000">2019-07-10 14:00:04</Created>
            <Updated time_t="1562767204000">2019-07-10 14:00:04</Updated>
            <Impact value="1">Medium</Impact>
            <ImpactV3 value="2">High</ImpactV3>
            <Type>File Upload</Type>
            <CVE>CVE-2019-12971</CVE>
            <Title>(CVE-2019-12971) BKS EBK Ethernet-Buskoppler Pro Arbitrary File Upload
Vulnerability</Title>
            <References>
                <Reference>https://www.g-u.com/en/service.html</Reference>
                <Reference>https://seclists.org/bugtraq/2019/Jul/6</Reference>
                <Reference>https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/
SYSS-2019-017.txt</Reference>
                <Reference>http://www.packetstormsecurity.com/files/153525/</Reference>
            </References>
            <Summary>Dummy Summary</Summary>
            <Analysis>Dummy Analysis</Analysis>
            <Solution>Dummy Solution</Solution>
            <Version>1</Version>
            <ModificationHistory>Initial Revision (rev 0) Entered on July 10, 2019</
ModificationHistory>
            <Associations></Associations>
            <Affected_Vendors>
                <Vendor>
                    <Name id="125555">BKS</Name>
                    <Product id="242797">EBK Ethernet-Buskoppler</Product>
```

```
                <Version id="0">0</Version>
            </Vendor>
            <Vendor>
                <Name id="125555">BKS</Name>
                <Product id="242799">EBK Ethernet-Buskoppler Firmware</Product>
                <Version id="0">0</Version>
            </Vendor>
        </Affected_Vendors>
        <AffectedCPEs>
            <Cpe>cpe:/h:bks:ebk_ethernet-buskoppler:::~~pro~~~</Cpe>
            <Cpe>cpe:/o:bks:ebk_ethernet-buskoppler_firmware:::~~pro~~~</Cpe>
        </AffectedCPEs>
        <CVSS>
            <CVSSv2>
                <CVSSScore>5.9</CVSSScore>
                <BaseMetrics>
                    <score>7.5</score>
                    <access_vector>network</access_vector>
                    <access_complexity>low</access_complexity>
                    <authentication_needed>none</authentication_needed>
                    <confidentiality_impact>partial</confidentiality_impact>
                    <integrity_impact>partial</integrity_impact>
                    <availability_impact>partial</availability_impact>
                </BaseMetrics>
                <TemporalMetrics>
                    <score>5.9</score>
                    <exploitability>poc</exploitability>
                    <remediation_level>official_fix</remediation_level>
                    <report_confidence>confirmed</report_confidence>
                </TemporalMetrics>
            </CVSSv2>
            <CVSSv3>
                <CVSSScore>8.8</CVSSScore>
                <BaseMetrics>
                    <score>9.8</score>
                    <attack_vector>network</attack_vector>
                    <attack_complexity>low</attack_complexity>
                    <privileges_required>none</privileges_required>
                    <user_interaction>none</user_interaction>
                    <scope>unchanged</scope>
                    <confidentiality>high</confidentiality>
                    <integrity>high</integrity>
                    <availability>high</availability>
                    <uri>CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C</uri>
                </BaseMetrics>
                <TemporalMetrics>
                    <score>8.8</score>
                    <exploit_code_maturity>proof_of_concept</exploit_code_maturity>
                    <remediation_level>official_fix</remediation_level>
                    <report_confidence>confirmed</report_confidence>
                </TemporalMetrics>
            </CVSSv3>
        </CVSS>
        <ChangeSummary>Initial Revision (rev 0) Entered on July 10, 2019</ChangeSummary>
        <CWEs>
            <CWE id="434">CWE-434 - Unrestricted Upload of File with Dangerous Type</CWE>
        </CWEs>
    </Vulnerability>
</Vulnerabilities>
</Intelligence>
```

ThreatQuotient provides the following default mapping for this feed:

Vulnerabilities Mapping Table

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
id	Vulnerability.Attribute	ID	<Vulnerability id="232739">	Note1
Created Time	Vulnerability.Attribute	Created Time	<Created time_t="xxx">2019-07-10 13:30:03	N/A
Updaed Time	Vulnerability.Attribute	Updated Time	<Updated time_t="xxx">2019-07-10 13:30:03	N/A
Impact Value	Vulnerability.Attribute	Impact Value	<Impact value="1">	N/A
ImpactV3 Value	Vulnerability.Attribute	ImpactV3 Value	<ImpactV3 value="2">	N/A
Type	Vulnerability.Attribute	Type	<Type>Design Error	N/A
CVE	Related.Indicator	CVE	<CVE>CVE-2019-13351	N/A
Title	Vulnerability.Name	N/A	`<Title>`(CVE-2019-13351) JACK2 Jack	N/A
References	Vulnerability.Attribute	Reference	<References>[<Reference>ref1</Reference>]	N/A
Summary	Vulnerability.Description	N/A	<Summary>Dummy Summary	N/A
Analysis	Vulnerability.Attribute	Analysis	<Analysis>Dummy Analysis	N/A
Solution	Vulnerability.Attribute	Solution	<Solution>Dummy Solution	N/A
Version	Vulnerability.Attribute	Version	<Version>1	N/A
Modification History	Vulnerability.Attribute	Comments	<ModificationHistory>Initial Revision...	N/A
Associations	Vulnerability.Attribute	Associations	List of associated objects (see sample)	See Note 2

Note 1: ID is constructed as `https://portal.secureworks.com/portal/intel/vulnerability/{Vulnerability_ID}`.

Note 2: Associations are constructed based on the parsed XML node type (Threat/Vulnerability/Advisory) as `https://portal.secureworks.com/portal/intel/{Object_Type}/{Parsed_ID}`.

Advisories Mapping Table

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
id	Report.Attribute	ID	<Advisory id="232739">	See Note 1
Created Time	Report.Attribute	Created Time	<Created time_t="xxx">2019-07-10 13:30:03	
Impact Value	Report.Attribute	Impact Value	<Impact value="1">	
Subject	Report.Title	N/A	<Subject>Secureworks Security Advisory...	
Type	Report.Attribute	Type	<Type>Advisory	
Summary	Report.Description	N/A	<Detail>Dummy Detail.	
CVE	Related.Indicator	CVE	Value extracted from <Subject>	See Note 2
Associations	Report.Attribute	Associations	List of associated objects (see sample)	See Note 3

Note 1: ID is constructed as `https://portal.secureworks.com/portal/intel/advisory/{Advisory_ID}`

Note 2: The related CVE Indicator value is extracted from the Subject xml node, example: `CVE-2019-10149` (Value between brackets)

Note 3: Associations are constructed based on the parsed XML node type (Threat/Vulnerability/Advisory) as `https://portal.secureworks.com/portal/intel/{Object_Type}/{Parsed_ID}`

Threats Mapping Table

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
id	Report.Attribute	ID	<Advisory id="232739">	See Note 1
Created Time	Report.Attribute	Created Time	<Created time_t="xxx">2019-07-10 13:30:03	
Updaed Time	Report.Attribute	Updated Time	<Updated time_t="xxx">2019-07-10 13:30:03	
Impact Value	Report.Attribute	Impact Value	<Impact value="1">	
Title	Report.Title	N/A	`<Title>`Secureworks Security Advisory...	
Summary	Report.Description	N/A	<Summary>Dummy Summary	
Analysis	Report.Attribute	Analysis	<Analysis>Dummy Analysis	
Solution	Report.Attribute	Solution	<Solution>Dummy Solution	
Associations	Report.Attribute	Associations	List of associated objects (see sample)	See Note 2

Note 1: ID is constructed as `https://portal.secureworks.com/portal/intel/threat/{Advisory_ID}`.

Note 2: Associations are constructed based on the parsed XML node type (Threat/Vulnerability/Advisory) as `https://portal.secureworks.com/portal/intel/{Object_Type}/{Parsed_ID}`.

Secureworks Alerts

The Secureworks Alerts feed ingests Events objects from Secureworks.

`POST https://{secureworks_host}/graphql`

Sample Response:


```
{
    "data": {
        "alertsServiceSearch": {
            "reason": "success",
            "search_id": null,
            "status": "OK",
            "alerts": {
                "previous_offset": 0,
                "total_results": 1,
                "first_offset": 0,
                "group_by": null,
                "last_offset": 0,
                "next_offset": 0,
                "total_parts": 1,
                "list": [
                    {
                        "resolution_reason": "",
                        "third_party_details": null,
                        "id": "alert://
priv:domain_blacklist:146063:1702484636095:b9186e8a-
a118-57bd-9ca6-257c919e19d6",
                        "parent_tenant_id": "",
                        "metadata": {
                            "confidence": 0.9,
                            "began_at": {
                                "seconds": 1702484487,
                                "nanos": 850866000
                            },
                            "full_title": null,
                            "title": "watchlist-test.ctpx.secureworks.com was
identified as malicious on 2 watchlists",
                            "severity_updated_at": {
                                "seconds": 1702484652,
                                "nanos": 508564718
                            },
                            "first_seen_at": null,
                            "created_at": {
                                "seconds": 1702484636,
                                "nanos": 95629378
                            },
                            "inserted_at": {
                                "seconds": 1702484656,
```

```
                                "nanos": 66277636
                            },
                            "first_investigated_at": null,
                            "description": "watchlist-test.ctpx.secureworks.com
was identified as malicious on the following watchlists:\nCTU Protection Domain
List:\nReason: Test - Dell SecureWorks AttackerDB Customer Test Event (non-
malicious)\nConfidence: 90\n\nCTU Malicious Domain Watchlist:\nReason: Test -
Dell SecureWorks AttackerDB Customer Test Event (non-malicious)\nConfidence:
90\n",
                            "updated_at": {
                                "seconds": 1702484671,
                                "nanos": 146287578
                            },
                            "engine": {
                                "version": "1.9.0",
                                "name": "app:detect:domain_blacklist"
                            },
                            "origin": "INTERNAL",
                            "first_resolved_at": null,
                            "creator": {
                                "rule": {
                                    "version": "1665757166",
                                    "rule_id":
"dff1c8f1-79ad-4349-85dc-66414009dd87"
                                },
                                "detector": {
                                    "detector_id":
"app:detect:domain_blacklist",
                                    "detector_name": "Domain Blocklist",
                                    "version": "1.9.0"
                                }
                            },
                            "ended_at": {
                                "seconds": 1702484538,
                                "nanos": 0
                            },
                            "severity": 0.75
                        },
                        "severity_history": [
                            {
                                "id": "17fefaf1-1c5f-5d3e-ad13-3e96b68a8db1",
                                "changed_at": {
                                    "seconds": 1702484652,
                                    "nanos": 508564718
                                },
                                "severity": 0.75
                            }
                        ],
                        "enrichment_details": null,
                        "priority": null,
```

```
                        "sensor_types": [
                            "ENDPOINT_TAEGIS"
                        ],
                        "events_metadata": {
                            "began_at": {
                                "seconds": 1702484487,
                                "nanos": 850866000
                            },
                            "first_event_id": "event://
priv:scwx.dnsquery:146063:1702484538000:1bea9e97-2658-58ed-a3dd-f7a5a408a75c",
                            "last_event_id": null,
                            "updated_at": {
                                "seconds": 1702484656,
                                "nanos": 84478550
                            },
                            "total_events": 1,
                            "ended_at": {
                                "seconds": 1702484538,
                                "nanos": 0
                            }
                        },
                        "reference_details": null,
                        "group_key": [

"2023-12-13:app:detect:domain_blacklist:146063:watchlist-
test.ctpx.secureworks.com"
                        ],
                        "entities": {
                            "relationships": [
                                {
                                    "to_entity":
"ipAddress:fe80::d424:9103:e253:54c2",
                                    "relationship": "is",
                                    "from_entity":
"hostName:aa3d5a88-9140-4fd4-8528-4ca28def18f1",
                                    "type": ""
                                },
                                {
                                    "to_entity":
"sensorHostId:4ba68135-42f5-50e8-bd63-c91eb4bfce2d",
                                    "relationship": "is",
                                    "from_entity":
"hostName:aa3d5a88-9140-4fd4-8528-4ca28def18f1",
                                    "type": ""
                                },
                                {
                                    "to_entity":
"ipAddress:::ffff:96.82.141.209",
                                    "relationship": "resolvedTo",
                                    "from_entity": "ipDomain:watchlist-
```

```
test.ctpx.secureworks.com",
                                    "type": ""
                                },
                                {
                                    "to_entity": "ipDomain:watchlist-
test.ctpx.secureworks.com",
                                    "relationship": "connectedTo",
                                    "from_entity":
"sensorHostId:4ba68135-42f5-50e8-bd63-c91eb4bfce2d",
                                    "type": ""
                                }
                            ],
                            "entities": [
                                "hostId:4ba68135-42f5-50e8-bd63-c91eb4bfce2d",

"hostName:aa3d5a88-9140-4fd4-8528-4ca28def18f1",

"hostNameAndHostId:aa3d5a88-9140-4fd4-8528-4ca28def18f1:4ba68135-42f5-50e8-
bd63-c91eb4bfce2d",

"hostNameAndHostIpAddress:aa3d5a88-9140-4fd4-8528-4ca28def18f1:fe80::d424:9103:
e253:54c2",
                                "ipAddress:::ffff:96.82.141.209",
                                "ipDomain:watchlist-test.ctpx.secureworks.com",
                                "sensorHostId:4ba68135-42f5-50e8-bd63-
c91eb4bfce2d",
                                "sensorId:4ba68135-42f5-50e8-bd63-
c91eb4bfce2d",
                                "sensorType:ENDPOINT_TAEGIS",
                                "topPrivateIpDomain:secureworks.com"
                            ]
                        },
                        "event_ids": [
                            {
                                "id": "event://
priv:scwx.dnsquery:146063:1702484538000:1bea9e97-2658-58ed-a3dd-f7a5a408a75c"
                            }
                        ],
                        "tags": [
                            "alertRule:dff1c8f1-79ad-4349-85dc-66414009dd87",
                            "compactor:handler"
                        ],
                        "suppressed": false,
                        "resolution_history": null,
                        "tenant_id": "146063",
                        "key_entities": null,
                        "observation_ids": [
                            {
                                "id": "observation://
priv:domain_blacklist:146063:1702484636095:21a583b0-b6ba-4b5c-
acec-39008fd46511"
```

```
                        }
                    ],
                    "visibility": "DEPLOYED",
                    "suppression_rules": null,
                    "alerting_rules": [
                        {
                            "id": "dff1c8f1-79ad-4349-85dc-66414009dd87",
                            "version": "1665757166"
                        }
                    ],
                    "collection_ids": null,
                    "status": "OPEN",
                    "attack_technique_ids": null,
                    "investigation_ids": null
                }
            ],
            "part": 1
        }
    }
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`data.alertsServiceSearch.alerts.list[].metadata.title`	Event.Title	N/A	`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	`watchlist-test.ctpx.secureworks.com was identified as malicious on 2 watchlists`	N/A
`data.alertsServiceSearch.alerts.list[].metadata.description`	Event.Description	N/A	`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	`watchlist-test.ctpx.secureworks.com was identified as malicious...`	N/A
`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	Event.Happened_At	N/A	`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	`2023-12-13 16:21:27`	N/A
`data.alertsServiceSearch.alerts.list[].tags`	Event.Tag	N/A	`N/A`	`compactor:handler`	N/A
`data.alertsServiceSearch.alerts.list[].metadata.confidence`	Event.Attribute	Confidence	`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	`0.9`	If the attribute already exists, the value will be updated.
`data.alertsServiceSearch.alerts.list[].metadata.engine.version`	Event.Attribute	Engine Version	`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	`1.9.0`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`data.alertsServiceSearch.alerts.list[].metadata.engine.name`	Event.Attribute	Engine Name	`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	`app:detect:domain_blacklist`	N/A
`data.alertsServiceSearch.alerts.list[].metadata.origin`	Event.Attribute	Origin	`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	`INTERNAL`	N/A
`data.alertsServiceSearch.alerts.list[].metadata.severity`	Event.Attribute	Severity	`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	`0.75`	If the attribute already exists, the value will be updated.
`data.alertsServiceSearch.alerts.list[].sensor_types`	Event.Attribute	Sensor Types	`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	`ENDPOINT_TAEGIS`	N/A
`data.alertsServiceSearch.alerts.list[].visibility`	Event.Attribute	Visibility	`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	`DEPLOYED`	N/A
`data.alertsServiceSearch.alerts.list[].status`	Event.Attribute	Status	`data.alertsServiceSearch.alerts.list[].metadata.created_at.seconds`	`OPEN`	If the attribute already exists, the value will be updated.

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.

Secureworks

METRIC	RESULT
Run Time	2 minutes
Indicators	3
Reports	9
Reports Attributes	36
Vulnerabilities	20
Vulnerabilities Attributes	47

Secureworks Alerts

METRIC	RESULT
Run Time	1 minute
Event	1
Event Attributes	8

Change Log

- **Version 1.1.0**
  - Added new feed: **Secureworks Alerts**.
- **Version 1.0.0**
  - Initial release