threatworx

GENERATE AN SBOM USING TWIGS

1 INSTALL TWIGS

twigs is a python based, open source CLI supported by ThreatWorx for discovering your attack surface. It can also create SBOMs for any part of the attack surface it discovers. This SBOM is ingestible by the ThreatWorx platform for continuous threat assessment.

The simplest way to install twigs on any modern linux system using python pip is:

```
$ pip install twigs
```

A comprehensive guide on twigs and all its features to discover code, containers, cloud, servers and more is available here

2 USE --SBOM OPTION TO GENERATE A THREATWORX STANDARD JSON SBOM

Simply include the "--sbom <filename>" option to have twigs generate an SBOM for any discovery run. For e.g.

```
# for a local code repository
twigs --sbom mycode.json repo --repo /my/code/repo

# for remote git  repository
twigs --sbom mycode.json repo --repo
https://github.com/myorg/myrepo

# for a local docker image
twigs --sbom mycontainer.json docker --image
mycontainerapp:v1.0.0

# for this linux server
twigs --sbom myserver.json host
```

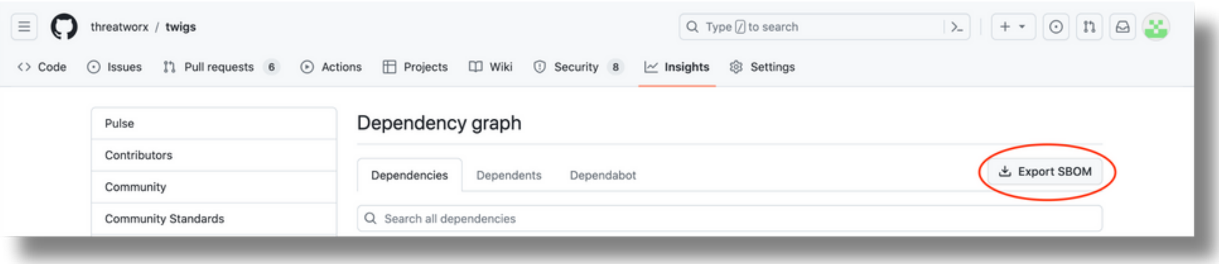
threatworx

GENERATE AN SBOM FOR A GITHUB PROJECT

1 NAVIGATE TO YOUR GITHUB PROJECT

GitHub now supports creation of SPDX SBOMs. If your project is on github.com, you should be able to pull an SBOM by navigating to your project -> Insights -> Dependency Graph.

If you have on-premise enterprise GitHub installation, please check your official documentation on how to enable this feature. These SBOMs are ingestible into the ThreatWorx console for continuous threat assessments.



GENERATE A CYCLONEDX OR SPDX SBOM

1

CHOOSE A TOOL AND GENERATE THE SBOM

There are several open source tools available for generating SBOMs.

The CycloneDX tools center has a big list of such tools. We recommend looking at the requirements of these tools as some of them may have dependencies on proprietary solutions.

One such tool for is an open source CLI called CDXGen. It as fewer dependencies and can be used to generate SBOMs for any code repository.

Microsoft is a big proponent of the SPDX standard and have also open sourced their SBOM generator which is available here.

The major difference in the two standards is that while the SPDX SBOMs cater mostly to open source software and license information while CycloneDX standard is evolving to include information about other software components such as operating systems, services etc.

These standards while they are evolving still do not cover many areas of the attack surface such as network devices, cloud misconfigurations, static code issues etc. which are covered quite effectively by the ThreatWorx SBOM standard.

threatworx

WHY USE THREATWORX SBOM

1 BETTER COVERAGE OF YOUR ATTACK SURFACE

Unlike other SBOM standards like Cyclone DX and SPDX, the ThreatWorx SBOM cover a lot areas of the attack surface including: VMware, Windows systems (including patch information), web applications, cloud and server misconfigurations, SAST, DAST, IaC issues, code secrets and more.

2 MULTIPLE ASSETS IN A SINGLE SBOM

The ThreatWorx SBOM specification allows for recording multiple assets in a single SBOM. This means that information on many servers, cloud instances, container images etc. can be captured in a single SBOM using twigs, eliminating the need for managing several SBOM files.

3 AUTOMATION USING TWIGS

Automate the generation and uploading of SBOMs to your secure ThreatWorx instance for assessment using twigs. For e.g.

```
$ twigs --sbom mycontainer.json docker --image
mycontainerapp:v1.0.0
```

```
$ twigs sbom --input mycontainer.json --standard
threatworx --format json
```

threatworx

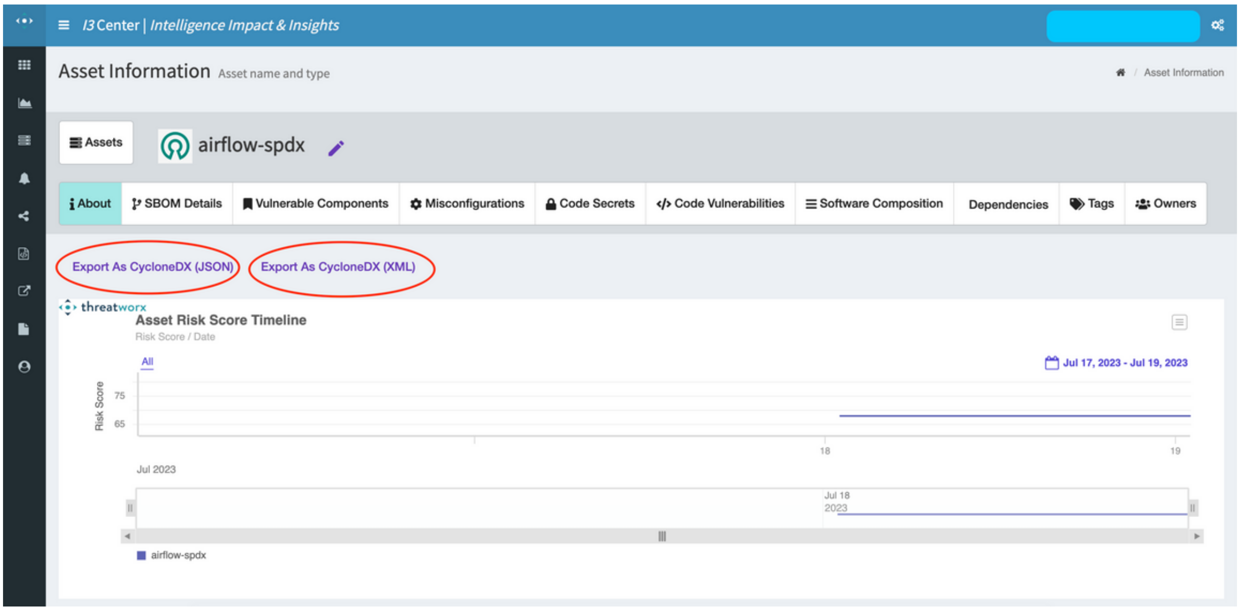
EXPORT SBOM FROM CONSOLE

1 CHOOSE AN ASSET

From the main menu navigate to the Asset -> Manage page and click on an asset in the table. Currently SBOM export is only supported for assets of type "Source Repository".

2 EXPORT THE SBOM

Click on the options to export a CycloneDX SBOM in either a JSON or XML format. The generated SBOM complies with the v1.4 CycloneDX standard. However it will not include information on SAST, IaC, code secrets which is currently supported only by the ThreatWorx SBOM standard.



UPLOAD SBOM TO CONSOLE

1

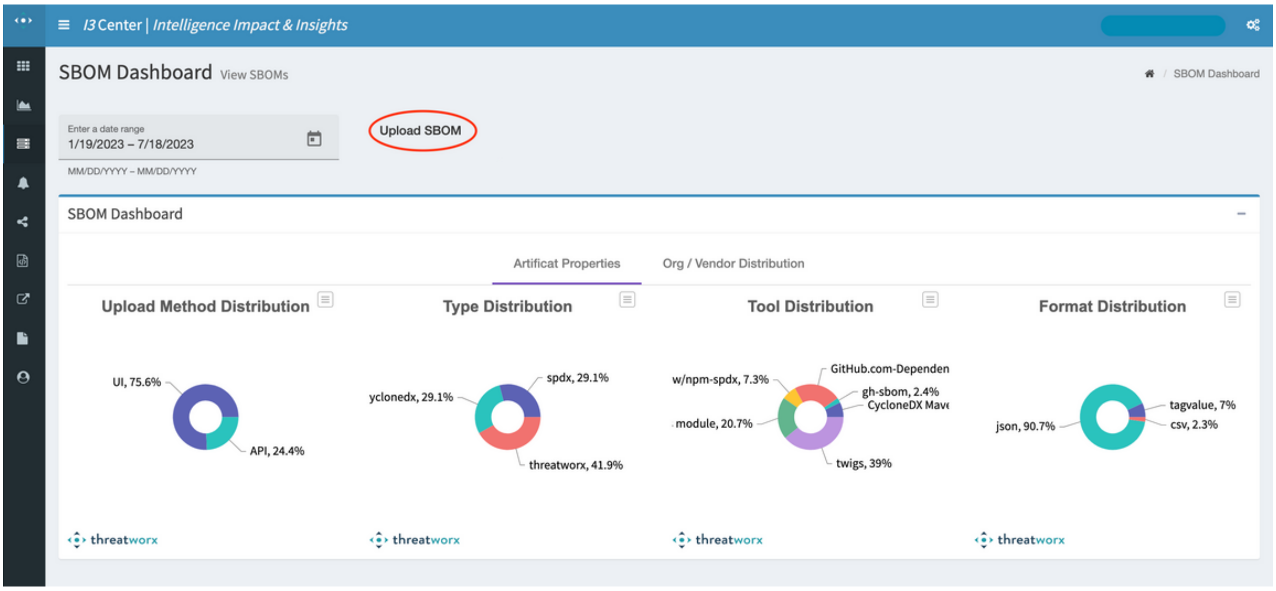
GET AN SBOM

Procure an SBOM from your partners, vendors, or business units within your organization. ThreatWorx currently supports SPDX (json, tagvalue) and CycloneDX (json) in addition to our own standard SBOM in json and csv formats.

2

NAVIGATE TO SBOM DASHBOARD

Go to Assets->SBOM Dashboard in the ThreatWorx console and click on the Upload SBOM button.



Enter a date range
1/19/2023 – 7/18/2023
MM/DD/YYYY – MM/DD/YYYY

UPLOAD SBOM TO CONSOLE

3 UPLOAD THE SBOM

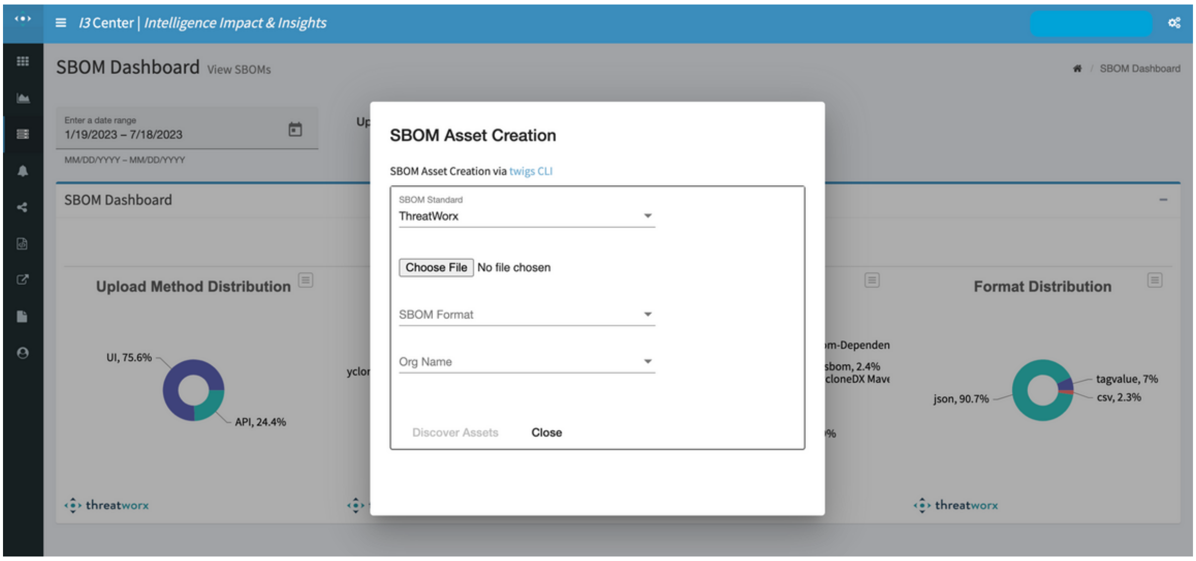
Select the SBOM file and the correct standard and format and upload the SBOM.

A unique asset id is required while uploading non-ThreatWorx SBOMs.

You could also optionally associate this SBOM to a vendor (i.e. Org) created in the ThreatWorx console. Select the right one from the available Orgs.

Once the SBOM is uploaded the platform will represent it as one (or more) assets, do a full threat and risk assessment on it and continue to track any new vulnerabilities reported against the SBOM components.

You can also track the SBOM artifact itself using the Assets->SBOM Dashboard.



I3 Center | *Intelligence Impact & Insights*

SBOM Dashboard View SBOMs

Enter a date range: 1/19/2023 – 7/18/2023

SBOM Asset Creation

SBOM Asset Creation via twigs CLI

SBOM Standard: ThreatWorx

Choose File No file chosen

SBOM Format

Org Name

Discover Assets Close

threatworx

UPLOAD SBOM USING TWIGS

1

GET AN SBOM

Procure an SBOM from your partners, vendors, or business units within your organization. ThreatWorx currently supports SPDX (json, tagvalue) andCycloneDX (json) in addition to our own standard SBOM in json and csv formats.

2

UPLOAD THE SBOM USING TWIGS

Point twigs to your dedicated ThreatWorx instance as explained the the guide here and then upload the SBOM using the right standard and format switches:

```
twigs sbom --input vendorsbom1 --standard spdx --
format json --assetid vendorasset1
```

A unique asset id is required while uploading non-ThreatWorx SBOMs.

You could also optionally associate this SBOM to a vendor i.e. Org created in the ThreatWorx console by using the --org switch e.g.

```
twigs sbom --input vendorsbom1 --standard spdx --
format json --assetid vendorasset1 --org Acme
```

Once the SBOM is uploaded the platform will represent it as one (or more) assets, do a full threat and risk assessment on it and continue to track any new vulnerabilities reported against the SBOM components.

You can also track the SBOM artifact itself using the Assets->SBOM Dashboard.