"SBOM 102"

SOFTWARE BILL OF MATERIALS

SBOM 101

Last time - We covered:

What is an SBOM?

What is the purpose?

How many formats are there?

How to create SBOM?

How to consume SBOM?

Where to learn more

SBOM 102

Today - We will Cover:

Key vendors in the SBOM space

OWASP initiatives

Thoughts on the Role of Artificial Intelligence

SONATYPE

- Sonatype is an SCA and source code review tools vendor.

- Best Practices: https://help.sonatype.com/iqserver/lifecycle-best-practices/software-bill-of-materials-best-practices

- Their software offers CycloneDX as a REST API

MICROSOFT

- Taking a “ check the box” approach to the Presidential directive
  - https://devblogs.microsoft.com/engineering-at-microsoft/tag/sbom/
- offers a free open source sbom-tool "a highly scalable and enterprise ready tool to create SPDX 2.2 compatible SBOMs for any variety of artifacts”
  - https://github.com/microsoft/sbom-tool
- Runs in a docker, weird invocation syntax: sbom-tool generate -b <drop path> -bc <build components path> -pn <package name> -pv <package version> -ps <package supplier> -nsb <namespace uri base>

GITHUB

- self-service SBOM on the level of repositories in GitHub enterprise
  - https://github.blog/2023-03-28-introducing-self-service-sboms/
- “To generate an SBOM, simply click the new Export SBOM button on a repository’s dependency graph “
  - foundation for SCA tooling (software component analytics)
- Feature seems mature and handles dependencies elegantly.

SNYK

So Now You Know

https://snyk.io/blog/building-sbom-open-source-supply-chain-security/

snyk2spdx which is an open source project that converts the Snyk CLI output to SPDX format

https://github.com/snyk-tech-services/snyk2spdx

CodeChecker lets you drag-drop spdx files for mapping to bulbs:

https://snyk.io/code-checker/sbom-security/

FLEXERA / REVENERA

Flexera Insights has SBOM creation in it

https://community.flexera.com/t5/Flexera-One-Blog/New-SBOM-Management-in-Flexera-One/bc-p/267624

Revenera has pivoted to visualization and “SBOM Management” software:

https://www.revenera.com/software-composition-analysis/products/sbom-insights

NOWSECURE

offer AppSecVulnScan (ASVS) for mobile apps

https://info.nowsecure.com/free-dynamic-SBOMs.html

“Get ten free SBOMs when you sign up” Likely using other tools, no indication of their own library or API for SBOM creation

ANCHORE
SOFT AND GRAPE

- open source - command line and a library written in Go
- Syft converts between SBOM formats: CycloneDX, SPDX, and Syft's own format
- Grype maps SBOM to CVE databases
- Entire approach is more focused on containers than on built software projects such as apps
-

FOUR PRIMARY SBOM FORMATS

- **Software package data exchange (SPDX)—**an open source machine-readable format with origins in Linux.
- **Software identification tags (SWID)—**an industry standard used by different commercial software publishers
- **CycloneDX (CDX)—**an open source machine-readable format with origins in the Open Web Application Security Project (OWASP) community
- **json** formatted SBOM and software inventories (.json)

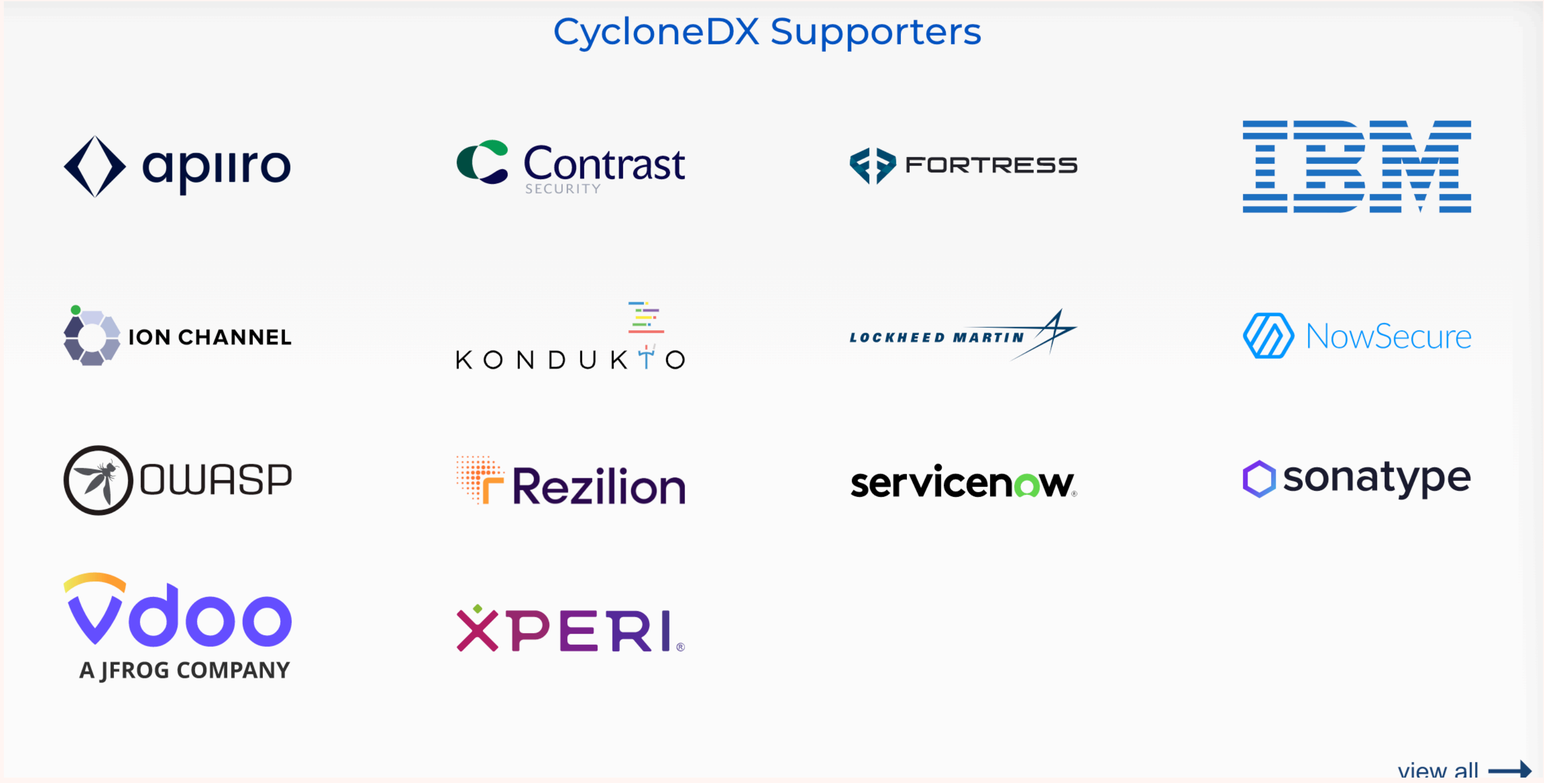
- Key observation: cloud integrations reduce the need to worry about SBOM formatting.

FOR PACKAGE AND CONTAINER LEVEL SBOM OPEN SOURCE STILL RULES THE DAY

- https://thenewstack.io/create-a-software-bill-of-materials-for-your-operating-system/
- dpkg --list
- rpm -qa --qf
- wmic \ output:C:\list.txt product get name, version
- pkgutil --pkgs

OWASP UPDATE

- **cycloneDX branching out:**
- **https://cyclonedx.org/**
- **Has many vendors on board,**



IBM AND CBOM

- IBM has been working on a specialized SBOM called the CBOM, or cryptography bill of materials:
- https://github.com/IBM/CBOM
- the goal of CBOM is to capture relevant crypto asset properties.
- track dependencies specific to cryptography, is an extension of CycloneDX to handle these

AI AND SBOM?

- security copilot by microsoft:
- https://www.cnbc.com/2023/03/28/microsoft-launches-security-copilot-in-private-preview.html

- SBOM can be an information source for generative AI software such as GPT-4
  - creative red-team attacking
  - enlightens where blue team can fix and remediate

QUESTIONS / ANSWERS

- **Mat Caughron CISSP CSSLP NSA-I[AE]M**
- **caughron@gmail.com**
- **(408) 910-1266**