

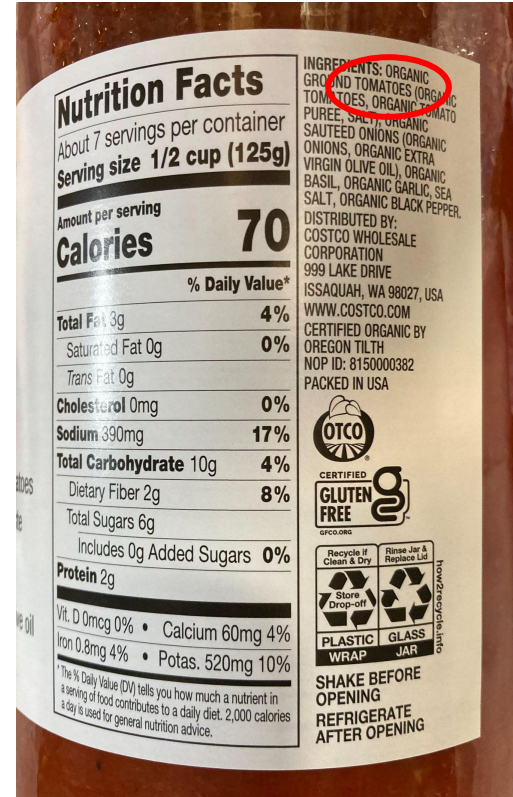
Intro to SBOM



Josh Bressers
Vice President, Security
Anchore

What is an SBOM?

Ingredients!



What is an SBOM?



What is an SBOM?



What is an SBOM?



What is an SBOM?

Actually it's software!
(not food)

```
16  "dependencies": {  
17    "@quasar/extras": "^1.0.0",  
18    "axios": "^0.21.1",  
19    "babel-plugin-prismjs": "^2.1.0",  
20    "cookie-parser": "^1.4.6",  
21    "cookie-session": "^2.0.0",  
22    "core-js": "^3.6.5",  
23    "csurf": "^1.11.0",  
24    "dompurify": "^3.0.1",  
25    "marked": "^4.3.0",  
26    "octokit": "^1.7.1",  
27    "prismjs": "^1.25.0",  
28    "quasar": "^2.0.0",  
29    "vue": "^3.0.0",  
30    "vue-router": "^4.0.0"  
31  },
```

First, a little history

Detect and avoid open source licenses

Open source was scary



open source
initiative
Approved License®



First, a little history

Now it's about understanding
open source

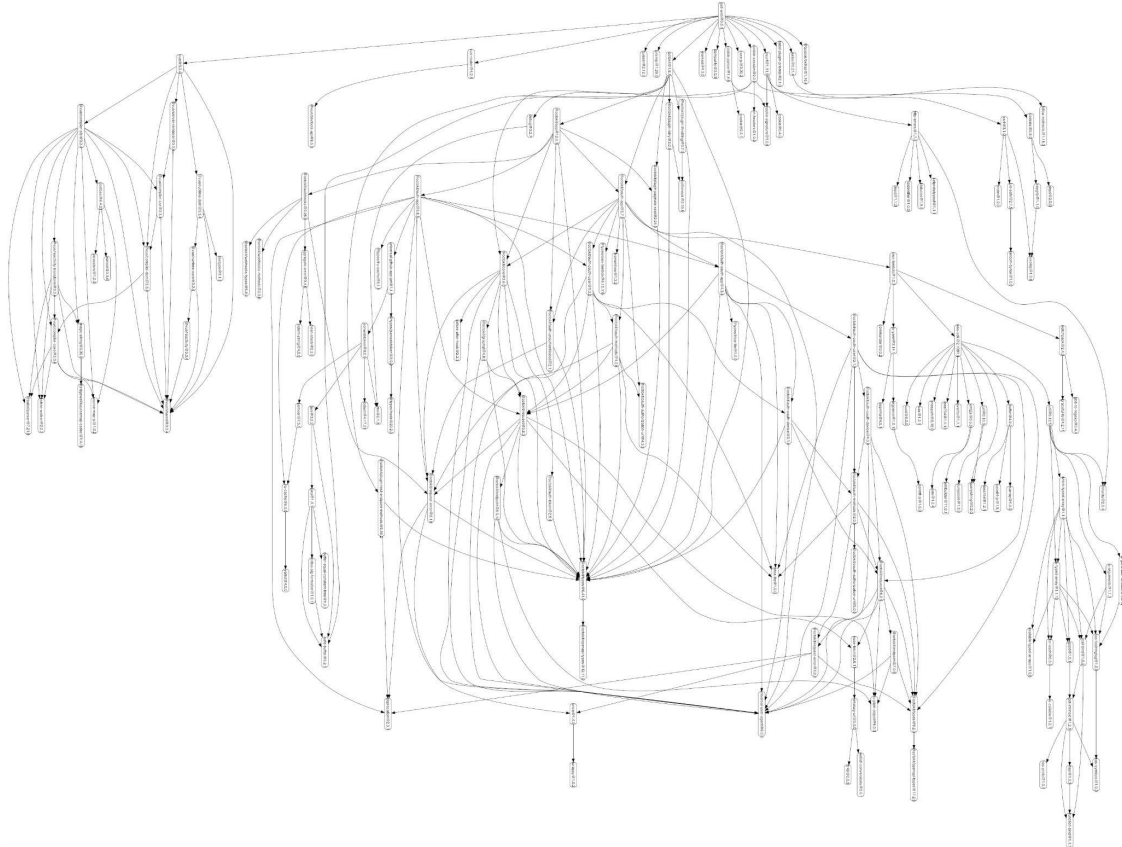


What is an SBOM?

Actually it's software!
(not food)

```
16  "dependencies": {
17    "@quasar/extras": "^1.0.0",
18    "axios": "^0.21.1",
19    "babel-plugin-prismjs": "^2.1.0",
20    "cookie-parser": "^1.4.6",
21    "cookie-session": "^2.0.0",
22    "core-js": "^3.6.5",
23    "csurf": "^1.11.0",
24    "dompurify": "^3.0.1",
25    "marked": "^4.3.0",
26    "octokit": "^1.7.1",
27    "prismjs": "^1.25.0",
28    "quasar": "^2.0.0",
29    "vue": "^3.0.0",
30    "vue-router": "^4.0.0"
31  },
```

What is an SBOM?



What is an SBOM?

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

SBOM data standards



SPDX



CycloneDX



SBOM data outputs

NAME	VERSION	TYPE
alpine-baselayout	3.4.3-r1	apk
alpine-baselayout-data	3.4.3-r1	apk
alpine-keys	2.4-r1	apk
apk-tools	2.14.0-r0	apk
busybox	1.36.0	binary
busybox	1.36.0-r9	apk
busybox-binsh	1.36.0-r9	apk
ca-certificates-bundle	20230506-r0	apk
libcrypt	0.7.3-r5	apk

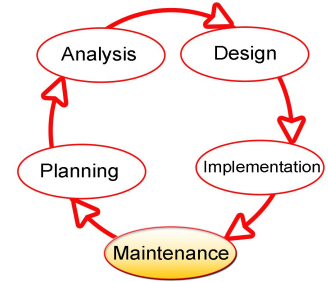
```
{  
  "spdxVersion": "SPDX-2.3",  
  "dataLicense": "CC0-1.0",  
  "SPDXID": "SPDXRef-DOCUMENT",  
  "name": "alpine:latest",  
}
```

```
SPDXVersion: SPDX-2.3  
DataLicense: CC0-1.0  
SPDXID: SPDXRef-DOCUMENT  
DocumentName: alpine:latest  
DocumentNamespace: https://anchore.com  
LicenseListVersion: 3.20  
Creator: Organization: Anchore, Inc  
Creator: Tool: syft-0.79.0  
Created: 2023-05-22T18:22:18Z
```

```
<?xml version="1.0" encoding="UTF-8"?>  
<bom xmlns="http://cyclonedx.org/schema/bom/1.4" serialNumber="urn:uuid:af298  
ac5-b161-4a5d-ab97-19efec73e1e6" version="1">  
  <metadata>  
    <timestamp>2023-05-22T13:20:53-05:00</timestamp>  
    <tools>  
      <tool>
```

Types of SBOMs

- **Design, Source, Build, Analyzed, Deployed, Runtime**
- Why different types matter
- What source am I using?
 - Testing could use things you don't ship
- What happened during the build?
- What happened when I put it in a container?
- What's changed since I started this application?

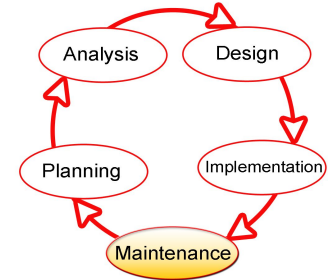


Types of SBOMs

- Design, Source,
- Why different types
- What source and
- Testing could
- What happened
- What happened
- What's changed

```
16   "dependencies": {  
17     "@quasar/extras": "^1.0.0",  
18     "axios": "^0.21.1",  
19     "babel-plugin-prismjs": "^2.1.0",  
20     "cookie-parser": "^1.4.6",  
21     "cookie-session": "^2.0.0",  
22     "core-js": "^3.6.5",  
23     "csurf": "^1.11.0",  
24     "dompurify": "^3.0.1",  
25     "marked": "^4.3.0",  
26     "octokit": "^1.7.1",  
27     "prismjs": "^1.25.0",  
28     "quasar": "^2.0.0",  
29     "vue": "^3.0.0",  
30     "vue-router": "^4.0.0"  
31   },
```

d, Runtime



er?

cation?

Recap: What is an SBOM

- List of software in our project
 - Dependencies of dependencies
- Minimum fields
- SPDX and CycloneDX standards
 - JSON, XML, and more
- Different types of SBOMs
 - Source, Build, Runtime, ...



How to create an SBOM

Manually

(don't do this)

```
16     "dependencies": {
17       "@quasar/extras": "^1.0.0",
18       "axios": "^0.21.1",
19       "babel-plugin-prismjs": "^2.1.0",
20       "cookie-parser": "^1.4.6",
21       "cookie-session": "^2.0.0",
22       "core-js": "^3.6.5",
23       "csurf": "^1.11.0",
24       "dompurify": "^3.0.1",
25       "marked": "^4.3.0",
26       "octokit": "^1.7.1",
27       "prismjs": "^1.25.0",
28       "quasar": "^2.0.0",
29       "vue": "^3.0.0",
30       "vue-router": "^4.0.0"
31     },
```

How to create an SBOM

Run a scanner

Syft

Trivy

Tern

And many more!

```
bress@anchore → ~ syft alpine:latest
✓ Parsed image
✓ Cataloged packages [16 packages]
NAME                VERSION      TYPE
alpine-baselayout    3.4.3-r1     apk
alpine-baselayout-data 3.4.3-r1     apk
alpine-keys          2.4-r1       apk
apk-tools            2.14.0-r0    apk
busybox              1.36.0       binary
busybox              1.36.0-r9    apk
busybox-binsh        1.36.0-r9    apk
ca-certificates-bundle 20230506-r0  apk
libc-utils           0.7.2-r5     apk
libcrypto3           3.1.0-r4     apk
libssl3              3.1.0-r4     apk
musl                 1.2.4-r0     apk
musl-utils           1.2.4-r0     apk
scanelf              1.3.7-r1     apk
ssl_client           1.36.0-r9    apk
zlib                 1.2.13-r1    apk
bress@anchore → ~
```

How to create an SBOM

Output SPDX

or CycloneDX

XML or JSON

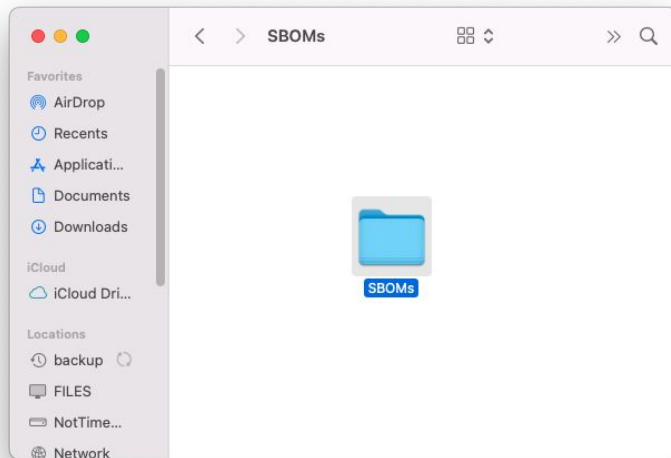
```
bress@anchore → ~ syft -o spdx-json alpine:latest
✓ Parsed image
✓ Cataloged packages      [16 packages]
{
  "spdxVersion": "SPDX-2.3",
  "dataLicense": "CC0-1.0",
  "SPDXID": "SPDXRef-DOCUMENT",
  "name": "alpine:latest",
  "documentNamespace": "https://anchore.com/syft/image/alpine-latest-a7f3c686-c2e2-4694-a503-7cd9645a2d05",
  "creationInfo": {
    "licenseListVersion": "3.20",
    "creators": [
      "Organization: Anchore, Inc",
      "Tool: syft-0.79.0"
    ],
    "created": "2023-05-22T14:46:45Z"
  },
  "packages": [
    {
      "name": "alpine-baselayout",
      "SPDXID": "SPDXRef-Package-apk-alpine-baselayout-206b74577cfae6ce",
      "versionInfo": "3.4.3-r1",
      "originator": "Person: Natanael Copa \u003cncopa@alpinelinux.org\u003e",
      "downloadLocation": "https://git.alpinelinux.org/cgit/aports/tree/main/alpine-baselayout",
      "sourceInfo": "acquired package info from APK DB: /lib/apk/db/installed",
      "licenseConcluded": "GPL-2.0-only",
      "licenseDeclared": "GPL-2.0-only",
      "copyrightText": "NOASSERTION",
      "checksums": {
        "sha256": "a7f3c686c2e24694a5037cd9645a2d05",
        "sha512": "a7f3c686c2e24694a5037cd9645a2d05"
      }
    }
  ]
}
```

I built an SBOM, now what?

This could be its own talk

There are tools available

Just put it in a folder to start



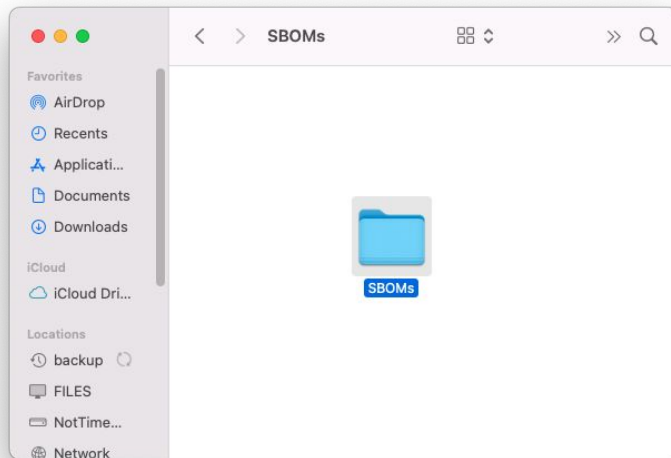
I built an SBOM, now what?

This could be its own talk

There are tools available

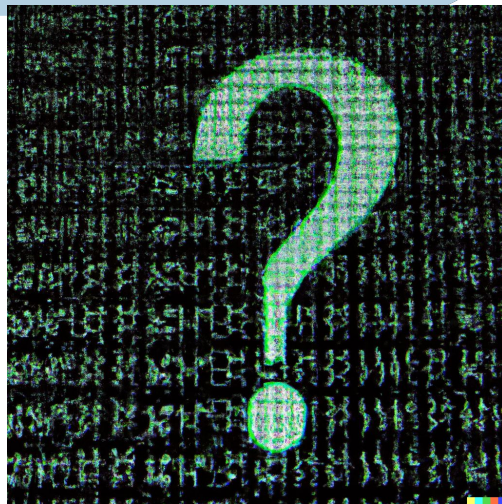
Just put it in a folder to start

But what does it actually do???



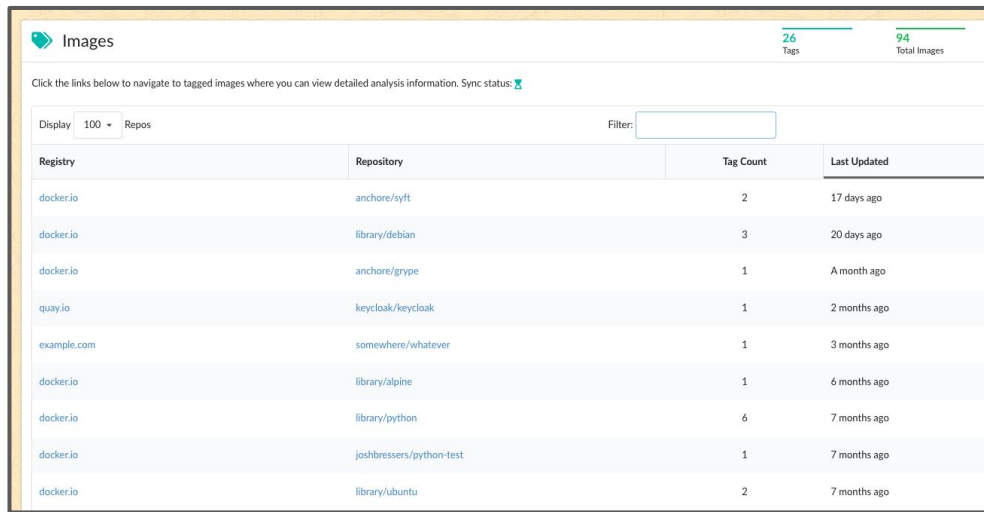
What does SBOM actually do


- Vulnerability scanning / management
 - Look back in time
- License compliance
- I need an SBOM for unknown reasons
 - My customers are demanding it
 - Regulation says I need it



The future of SBOM

Management systems



The screenshot displays the 'Images' management page in the Anchore system. At the top right, it shows '26 Tags' and '94 Total Images'. Below this is a navigation instruction: 'Click the links below to navigate to tagged images where you can view detailed analysis information. Sync status: '. The interface includes a 'Display' dropdown set to '100' and a 'Filter' input field. The main content is a table with the following data:

Registry	Repository	Tag Count	Last Updated
docker.io	anchore/syft	2	17 days ago
docker.io	library/debian	3	20 days ago
docker.io	anchore/grype	1	A month ago
quay.io	keycloak/keycloak	1	2 months ago
example.com	somewhere/whatever	1	3 months ago
docker.io	library/alpine	1	6 months ago
docker.io	library/python	6	7 months ago
docker.io	joshbressers/python-test	1	7 months ago
docker.io	library/ubuntu	2	7 months ago

The future of SBOM

Artifact discovery

Remember Log4Shell?



The future of SBOM

Distribution:
Create and receive SBOMs



The future of SBOM

Regulation and compliance



NIST Search NIST Menu

Information Technology Laboratory

EXECUTIVE ORDER 14028, IMPROVING THE NATION'S CYBERSECURITY

Software Supply Chain Security Guidance

Software Security in Supply Chains

Guidance, Purpose, Scope, and Audience

EO-Critical Software and Security Measures for EO-Critical Software

Software Cybersecurity

Software Security in Supply Chains: Software Bill of Materials (SBOM)

Section 10(j) of EO 14028 defines an SBOM as a "formal record containing the details and supply chain relationships of various components used in building software," similar to food ingredient labels on packaging. SBOMs hold the potential to provide increased transparency, provenance, and speed at which vulnerabilities can be identified and remediated by federal departments and agencies. SBOMs can also be indicative of a developer or suppliers' application of secure software development practices across the SDLC. Figure F-1 illustrates an example of how an SBOM may be assembled across the SDLC.

Center of Excellence / Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)

Cybersecurity in Medical Devices Frequently Asked Questions (FAQs)

Share Tweet LinkedIn Email Print

Digital Health Center of Excellence

This page provides answers to frequently asked questions (FAQs) related to cybersecurity in medical devices.

One last note ...

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



AMERICA'S CYBER DEFENSE AGENCY

Search

Topics ▾

Spotlight

Resources & Tools ▾

News & Events ▾

Careers ▾

About ▾

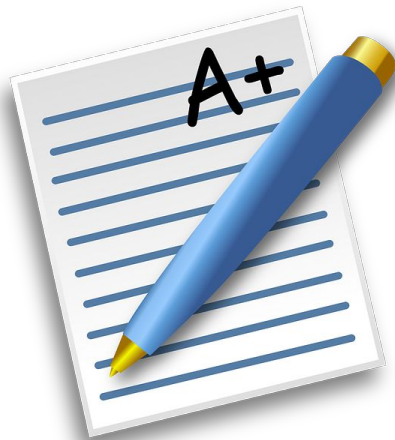
[Home](#) / [Resources & Tools](#) / [Resources](#)

PUBLICATION

Minimum Requirements for Vulnerability Exploitability eXchange (VEX)

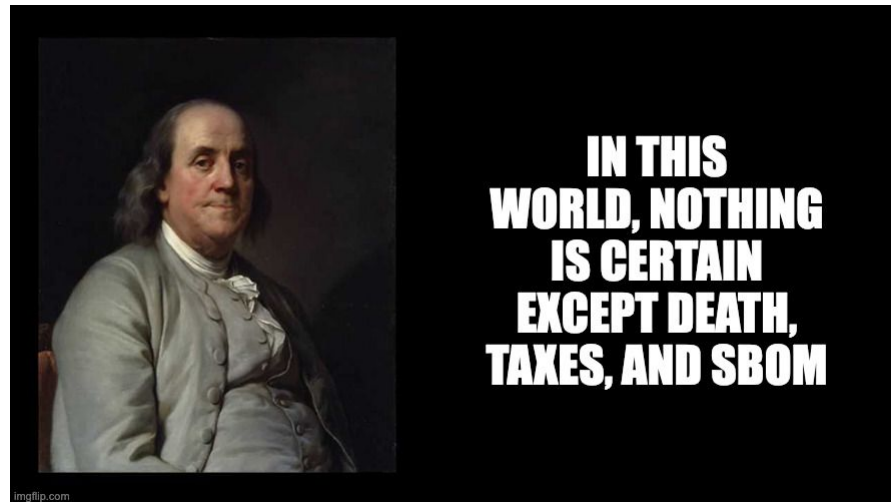
What SBOMs don't do

- **Tell you risk of your open source**
 - Risk assessment is an opinion
 - Every environment is different
 - SBOM is a factual objective document
 - The things you care about will change, the SBOM won't
- **Give you vulnerability details**
 - New vulnerabilities come out every day
 - SBOMs are static documents



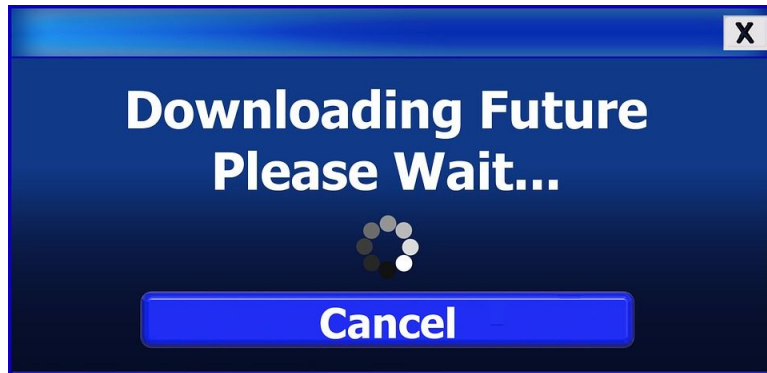
I'll never need an SBOM!

- You probably will
- Regulation is coming
 - FDA
 - EO, NDAA
 - CISA/NIST
- Insurance is coming
 - (but not just yet)
- Customers will ask
 - If they're not already



What can you do today!

- **Create your own SBOMs**
 - For internal use to start
 - Run an automated scanner
 - They're good enough
- **Ask your vendors for SBOMs**
 - It's a sign of vendor maturity
 - Put them in a folder for now
- **Expect to distribute and receive SBOMs for everything**
- **Get ready for the next major security event**



Questions?