So, SBOMs matter... Now what?

Frankie Gallina-Jones

@fg-j

Sophie Wigmore

@sophiewigmore

paketo buildpacks

Software Bill of Materials 101

From the United States Cybersecurity & Infrastructure Security Agency (CISA):

> *“A ‘software bill of materials’ (SBOM) has emerged as a key building block in software security and software supply chain risk management.* ***A SBOM is a nested inventory, a list of ingredients that make up software components.****”*

Software Bills of Materials (SBOMs) matter. Why?

They are essential for supply chain risk management.

Software Bills of Materials (SBOMs) matter. Now what?

25%

of the respondents to the 2021 Anchore Software Supply Chain Report produce an SBOM for the containerized apps they build.

How can you meet consumers' SBOM expectations?

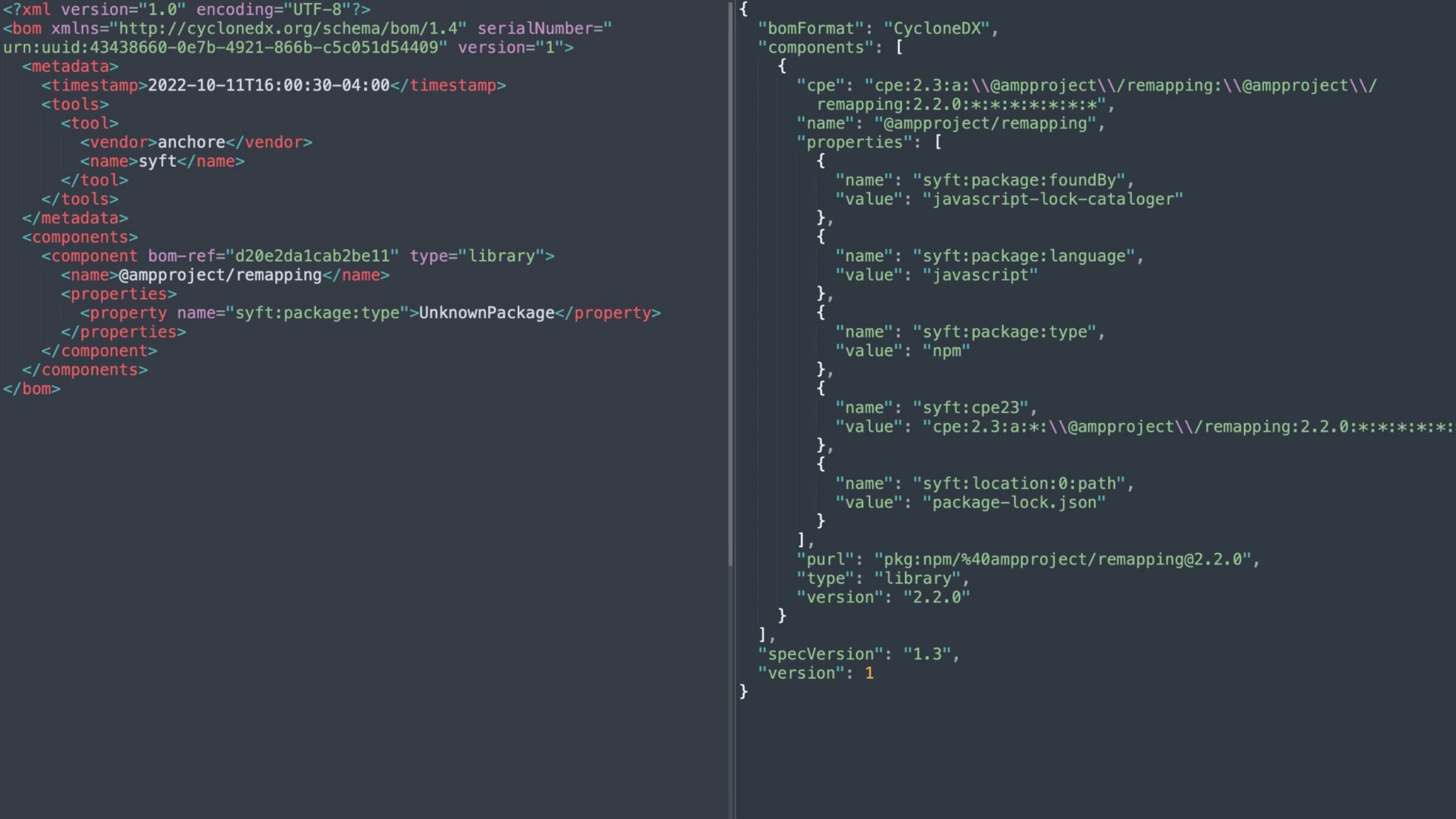
The best way to to this is to devise a solution that addresses these five questions:

1. **Why** do SBOMs matter? ✅
2. **What** constitutes a useful SBOM?
3. **Who** wants SBOMs?
4. **Where** should SBOMs be stored?
5. **When** should SBOMs be generated?

What constitutes a useful SBOM?

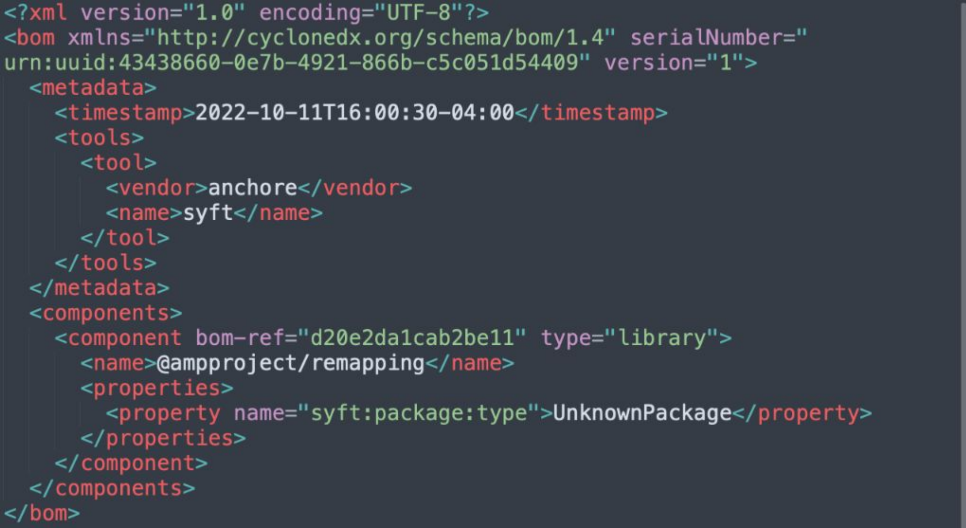
PRESERVATISED
THIS FOOD CONTAINS NOT MORE THAN
2 GRAINS SULPHUR DIOXIDE PER PINT.

An SBOM is ***not*** *a list of vulnerabilities. It’s a list of ingredients.*



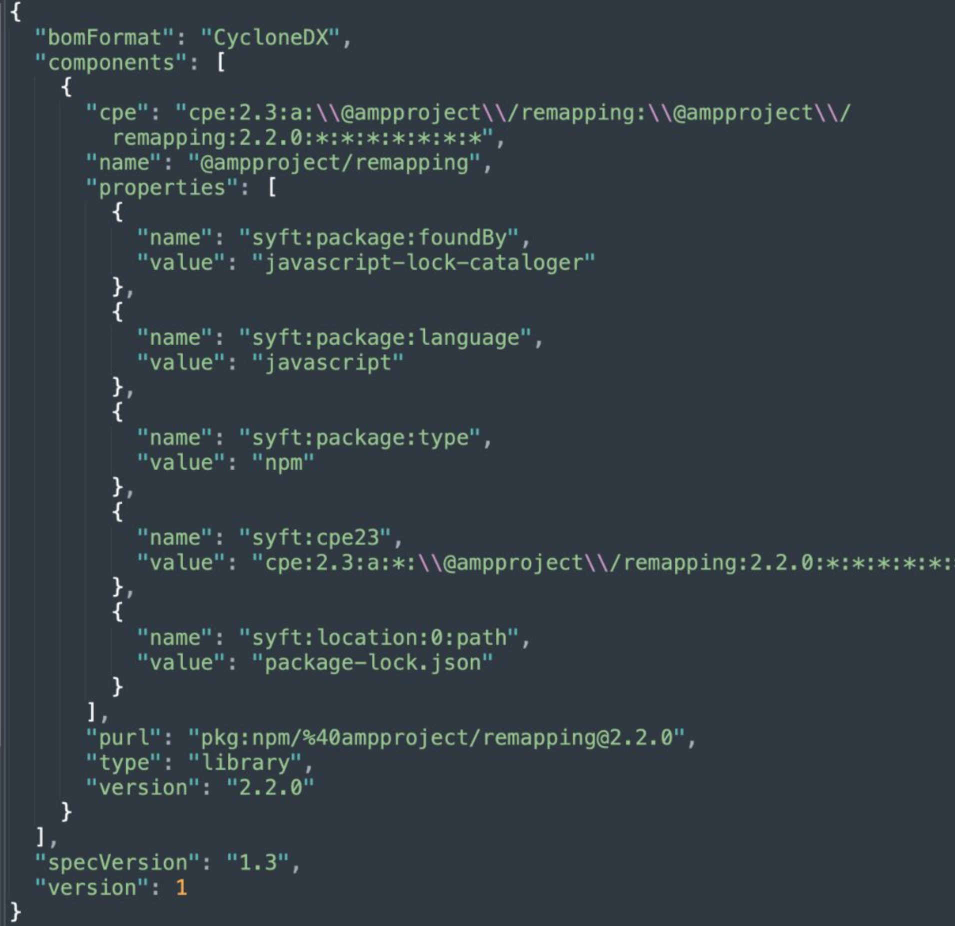
```xml
<?xml version="1.0" encoding="UTF-8"?>
<bom xmlns="http://cyclonedx.org/schema/bom/1.4" serialNumber="
urn:uuid:43438660-0e7b-4921-866b-c5c051d54409" version="1">
  <metadata>
    <timestamp>2022-10-11T16:00:30-04:00</timestamp>
    <tools>
      <tool>
        <vendor>anchore</vendor>
        <name>syft</name>
      </tool>
    </tools>
  </metadata>
  <components>
    <component bom-ref="d20e2da1cab2be11" type="library">
      <name>@ampproject/remapping</name>
      <properties>
        <property name="syft:package:type">UnknownPackage</property>
      </properties>
    </component>
  </components>
</bom>
```

```json
{
  "bomFormat": "CycloneDX",
  "components": [
    {
      "cpe": "cpe:2.3:a:\\@ampproject\\/remapping:\\@ampproject\\/
        remapping:2.2.0:*:*:*:*:*:*:*",
      "name": "@ampproject/remapping",
      "properties": [
        {
          "name": "syft:package:foundBy",
          "value": "javascript-lock-cataloger"
        },
        {
          "name": "syft:package:language",
          "value": "javascript"
        },
        {
          "name": "syft:package:type",
          "value": "npm"
        },
        {
          "name": "syft:cpe23",
          "value": "cpe:2.3:a:*:\\@ampproject\\/remapping:2.2.0:*:*:*:*:*:
        },
        {
          "name": "syft:location:0:path",
          "value": "package-lock.json"
        }
      ],
      "purl": "pkg:npm/%40ampproject/remapping@2.2.0",
      "type": "library",
      "version": "2.2.0"
    }
  ],
  "specVersion": "1.3",
  "version": 1
}
```



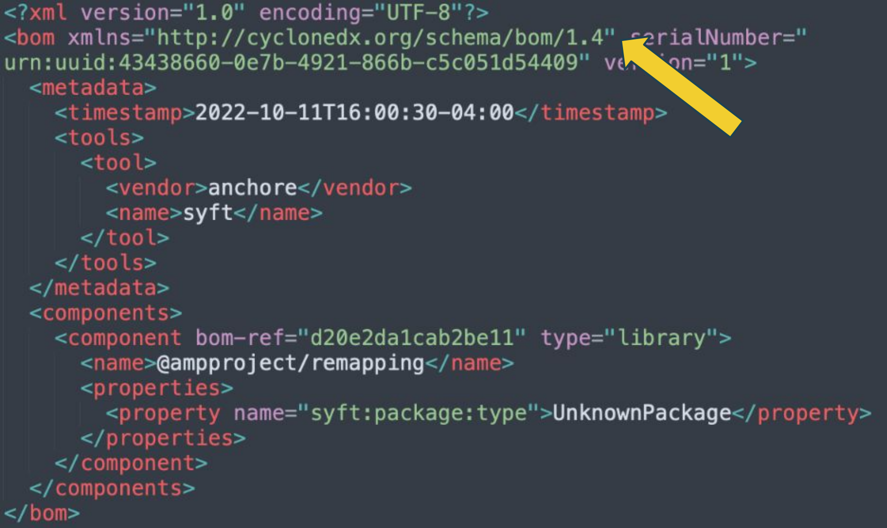
```xml
<?xml version="1.0" encoding="UTF-8"?>
<bom xmlns="http://cyclonedx.org/schema/bom/1.4" serialNumber="
urn:uuid:43438660-0e7b-4921-866b-c5c051d54409" version="1">
  <metadata>
    <timestamp>2022-10-11T16:00:30-04:00</timestamp>
    <tools>
      <tool>
        <vendor>anchore</vendor>
        <name>syft</name>
      </tool>
    </tools>
  </metadata>
  <components>
    <component bom-ref="d20e2da1cab2be11" type="library">
      <name>@ampproject/remapping</name>
      <properties>
        <property name="syft:package:type">UnknownPackage</property>
      </properties>
    </component>
  </components>
</bom>
```

XML

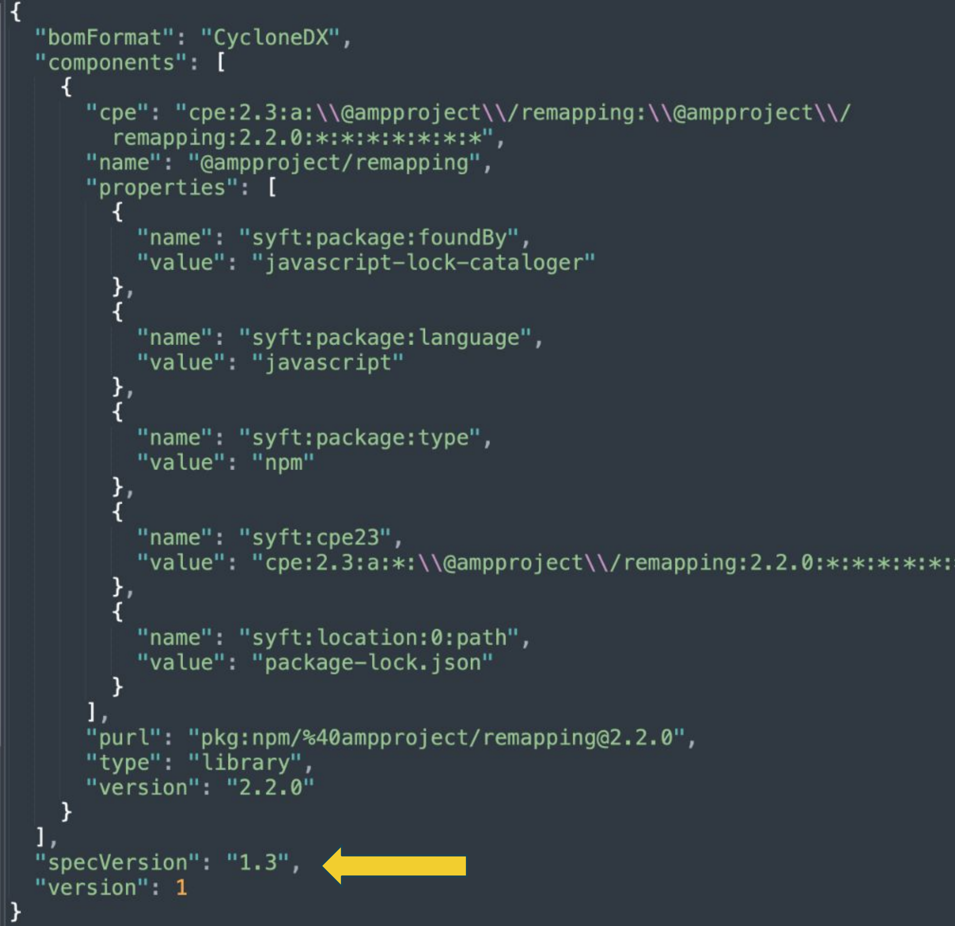


```json
{
  "bomFormat": "CycloneDX",
  "components": [
    {
      "cpe": "cpe:2.3:a:\\@ampproject\\/remapping:\\@ampproject\\/
        remapping:2.2.0:*:*:*:*:*:*:*",
      "name": "@ampproject/remapping",
      "properties": [
        {
          "name": "syft:package:foundBy",
          "value": "javascript-lock-cataloger"
        },
        {
          "name": "syft:package:language",
          "value": "javascript"
        },
        {
          "name": "syft:package:type",
          "value": "npm"
        },
        {
          "name": "syft:cpe23",
          "value": "cpe:2.3:a:*:\\@ampproject\\/remapping:2.2.0:*:*:*:*:*:
        },
        {
          "name": "syft:location:0:path",
          "value": "package-lock.json"
        }
      ],
      "purl": "pkg:npm/%40ampproject/remapping@2.2.0",
      "type": "library",
      "version": "2.2.0"
    }
  ],
  "specVersion": "1.3",
  "version": 1
}
```

JSON



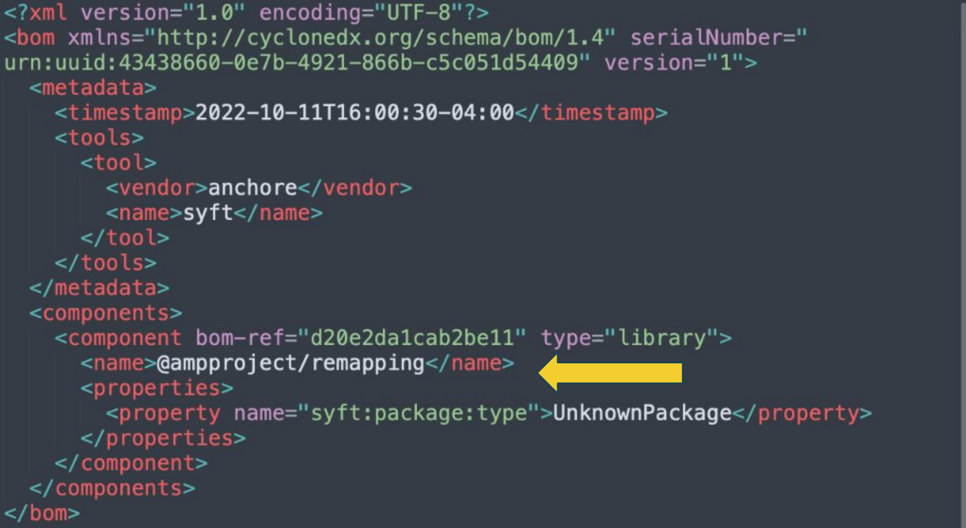
```xml
<?xml version="1.0" encoding="UTF-8"?>
<bom xmlns="http://cyclonedx.org/schema/bom/1.4" serialNumber="
urn:uuid:43438660-0e7b-4921-866b-c5c051d54409" version="1">
  <metadata>
    <timestamp>2022-10-11T16:00:30-04:00</timestamp>
    <tools>
      <tool>
        <vendor>anchore</vendor>
        <name>syft</name>
      </tool>
    </tools>
  </metadata>
  <components>
    <component bom-ref="d20e2da1cab2be11" type="library">
      <name>@ampproject/remapping</name>
      <properties>
        <property name="syft:package:type">UnknownPackage</property>
      </properties>
    </component>
  </components>
</bom>
```



```json
{
  "bomFormat": "CycloneDX",
  "components": [
    {
      "cpe": "cpe:2.3:a:\\@ampproject\\/remapping:\\@ampproject\\/
        remapping:2.2.0:*:*:*:*:*:*:*",
      "name": "@ampproject/remapping",
      "properties": [
        {
          "name": "syft:package:foundBy",
          "value": "javascript-lock-cataloger"
        },
        {
          "name": "syft:package:language",
          "value": "javascript"
        },
        {
          "name": "syft:package:type",
          "value": "npm"
        },
        {
          "name": "syft:cpe23",
          "value": "cpe:2.3:a:*:\\@ampproject\\/remapping:2.2.0:*:*:*:*:*:
        },
        {
          "name": "syft:location:0:path",
          "value": "package-lock.json"
        }
      ],
      "purl": "pkg:npm/%40ampproject/remapping@2.2.0",
      "type": "library",
      "version": "2.2.0"
    }
  ],
  "specVersion": "1.3",
  "version": 1
}
```

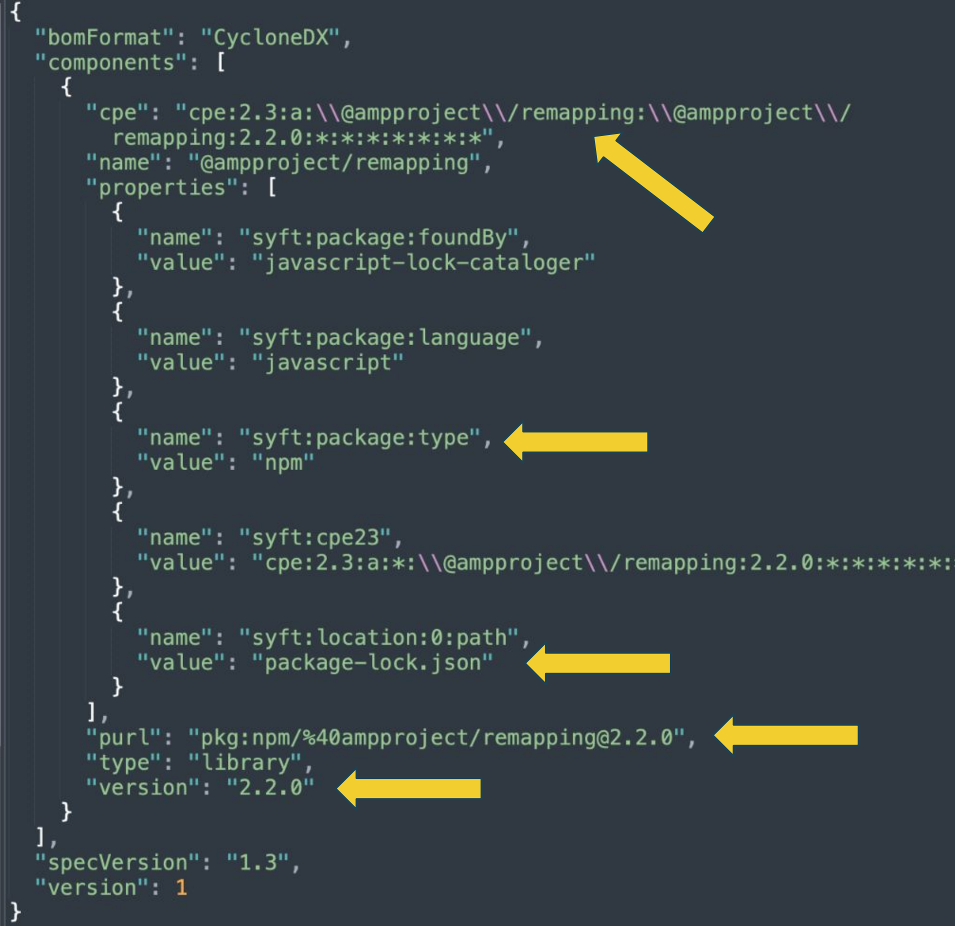
CycloneDX 1.4

CycloneDX 1.3



```xml
<?xml version="1.0" encoding="UTF-8"?>
<bom xmlns="http://cyclonedx.org/schema/bom/1.4" serialNumber="
urn:uuid:43438660-0e7b-4921-866b-c5c051d54409" version="1">
  <metadata>
    <timestamp>2022-10-11T16:00:30-04:00</timestamp>
    <tools>
      <tool>
        <vendor>anchore</vendor>
        <name>syft</name>
      </tool>
    </tools>
  </metadata>
  <components>
    <component bom-ref="d20e2da1cab2be11" type="library">
      <name>@ampproject/remapping</name>
      <properties>
        <property name="syft:package:type">UnknownPackage</property>
      </properties>
    </component>
  </components>
</bom>
```

Minimal package info



```json
{
  "bomFormat": "CycloneDX",
  "components": [
    {
      "cpe": "cpe:2.3:a:\\@ampproject\\/remapping:\\@ampproject\\/
        remapping:2.2.0:*:*:*:*:*:*:*",
      "name": "@ampproject/remapping",
      "properties": [
        {
          "name": "syft:package:foundBy",
          "value": "javascript-lock-cataloger"
        },
        {
          "name": "syft:package:language",
          "value": "javascript"
        },
        {
          "name": "syft:package:type",
          "value": "npm"
        },
        {
          "name": "syft:cpe23",
          "value": "cpe:2.3:a:*:\\@ampproject\\/remapping:2.2.0:*:*:*:*:*:
        },
        {
          "name": "syft:location:0:path",
          "value": "package-lock.json"
        }
      ],
      "purl": "pkg:npm/%40ampproject/remapping@2.2.0",
      "type": "library",
      "version": "2.2.0"
    }
  ],
  "specVersion": "1.3",
  "version": 1
}
```

Detailed package info

Who wants SBOMs?

Who wants SBOMs? (And what kinds do they want?)

(Versioned) Schema

Data Values

Formats

Who wants SBOMs? (And what kinds do they want?)

(Versioned) Schema

- SPDX
- CycloneDX
- SWID
- Syft
- & more

Data Values

- PURL
- CPE
- SWID
- Checksum
- License
- & more

Formats

- XML
- JSON
- YAML
- Human-readable
- & more

Who wants SBOMs? (And what kinds do they want?)

(Versioned) Schema

- SPDX 2.2
- CycloneDX 1.3, 1.4
- Syft 2.0.2, 3.0.1

Data Values

- PURL
- CPE
- Checksum
- License

Formats

- JSON

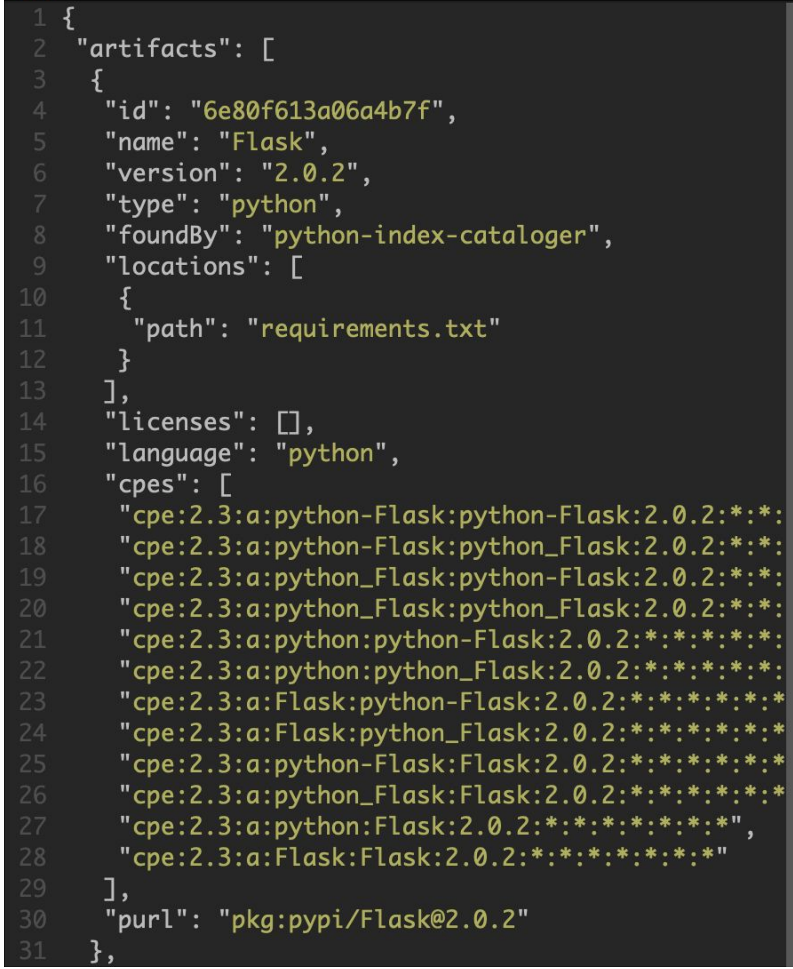
How do you generate SBOMs that are useful for *all* of your stakeholders?

Case Study #1

A React front end application built into static assets and served with NGINX

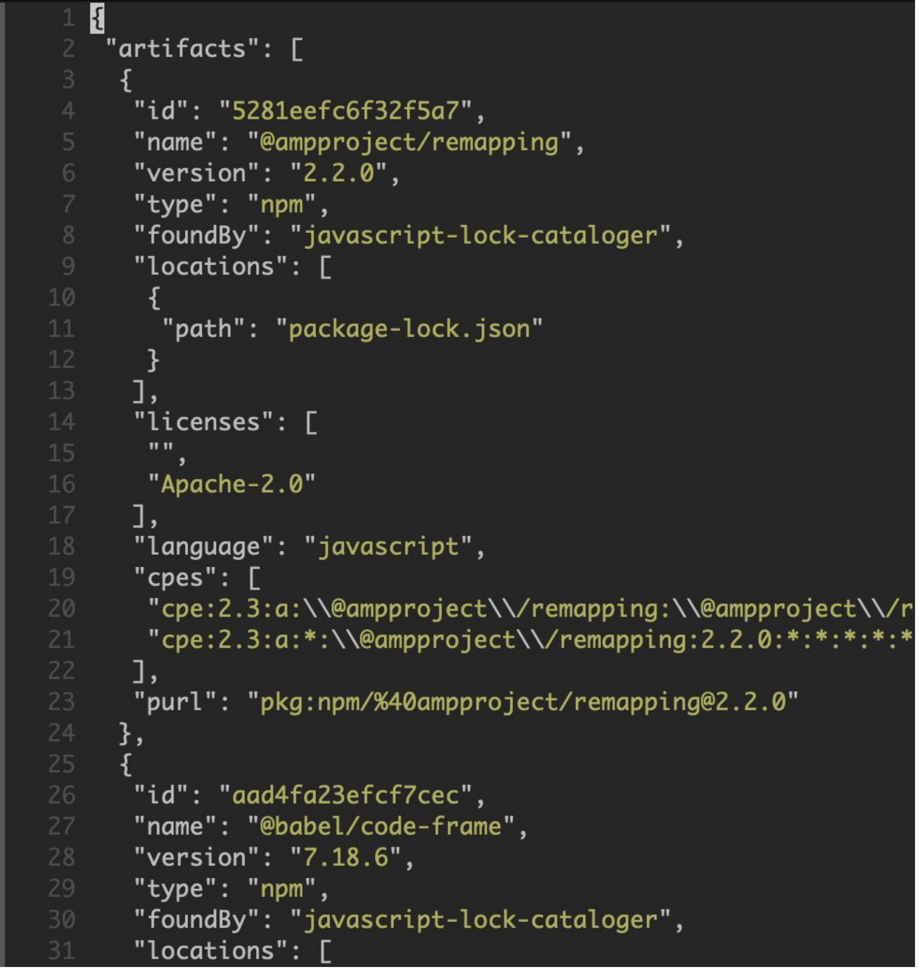
Case Study #2

A Flask server app that uses pip for package management



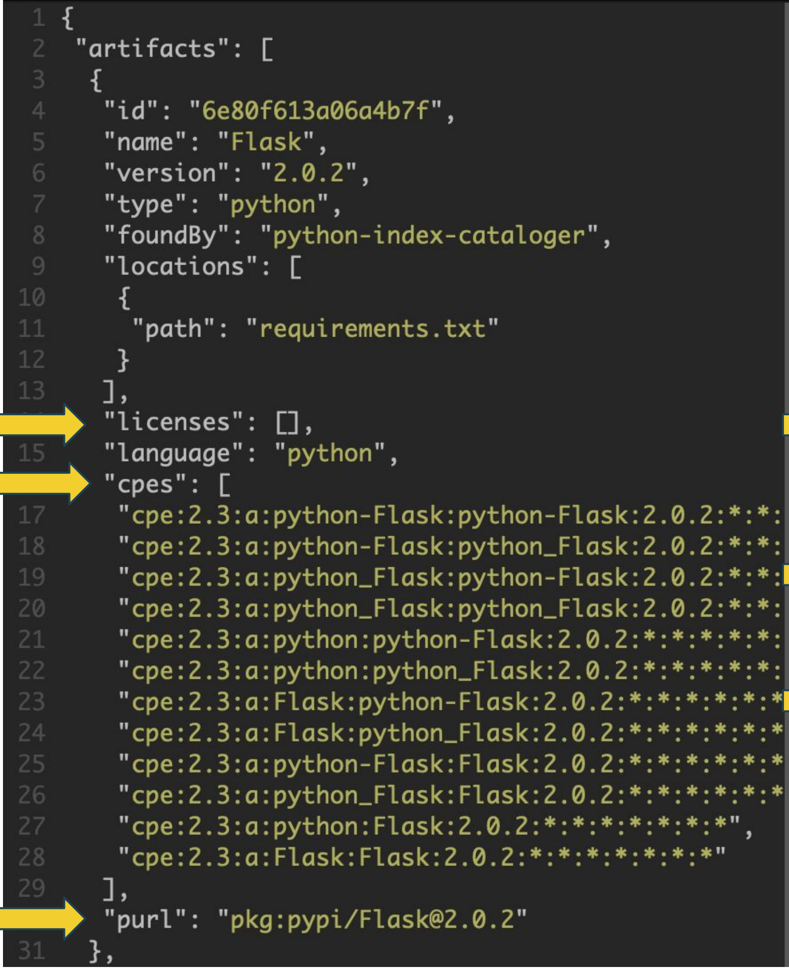
```
{
 "artifacts": [
  {
   "id": "6e80f613a06a4b7f",
   "name": "Flask",
   "version": "2.0.2",
   "type": "python",
   "foundBy": "python-index-cataloger",
   "locations": [
    {
     "path": "requirements.txt"
    }
   ],
   "licenses": [],
   "language": "python",
   "cpes": [
    "cpe:2.3:a:python-Flask:python-Flask:2.0.2:*:*:
    "cpe:2.3:a:python-Flask:python_Flask:2.0.2:*:*:
    "cpe:2.3:a:python_Flask:python-Flask:2.0.2:*:*:
    "cpe:2.3:a:python_Flask:python_Flask:2.0.2:*:*:
    "cpe:2.3:a:python:python-Flask:2.0.2:*:*:*:*:*:
    "cpe:2.3:a:python:python_Flask:2.0.2:*:*:*:*:*:
    "cpe:2.3:a:Flask:python-Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:Flask:python_Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:python-Flask:Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:python_Flask:Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:python:Flask:2.0.2:*:*:*:*:*:*:*",
    "cpe:2.3:a:Flask:Flask:2.0.2:*:*:*:*:*:*:*"
   ],
   "purl": "pkg:pypi/Flask@2.0.2"
  },
```

Python App



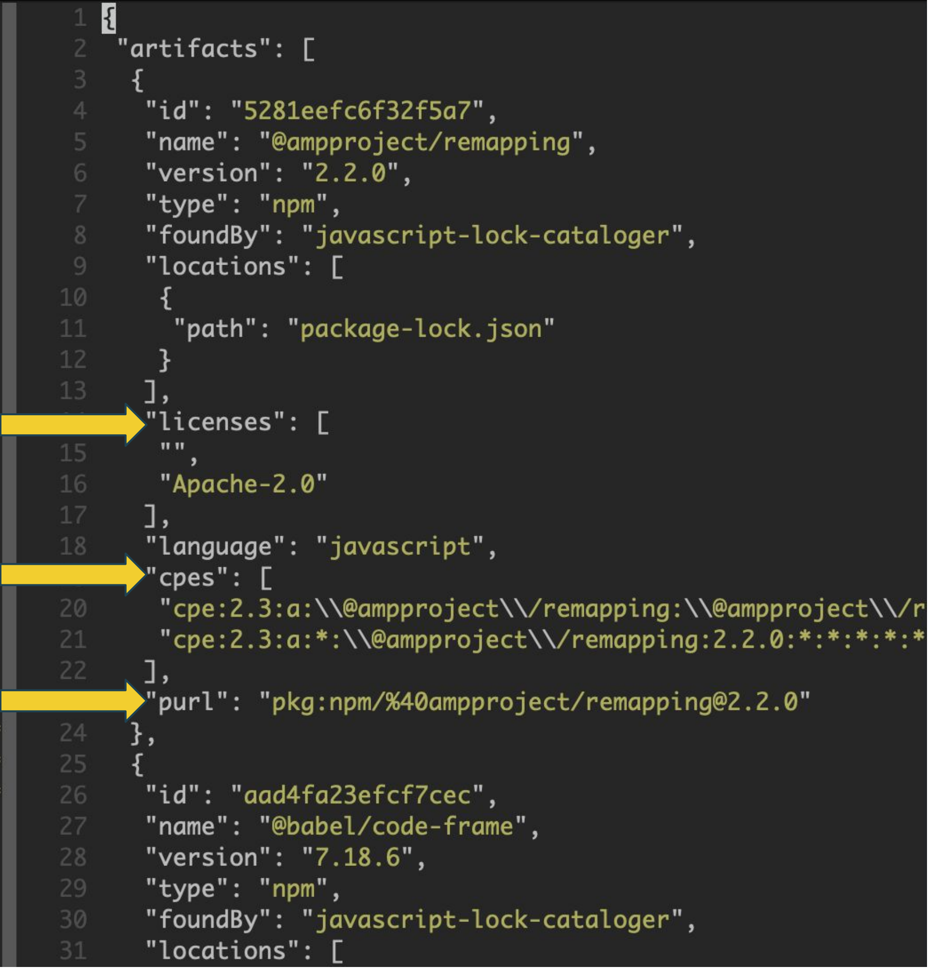
```
{
 "artifacts": [
  {
   "id": "5281eefc6f32f5a7",
   "name": "@ampproject/remapping",
   "version": "2.2.0",
   "type": "npm",
   "foundBy": "javascript-lock-cataloger",
   "locations": [
    {
     "path": "package-lock.json"
    }
   ],
   "licenses": [
    "",
    "Apache-2.0"
   ],
   "language": "javascript",
   "cpes": [
    "cpe:2.3:a:\\@ampproject\\/remapping:\\@ampproject\\/r
    "cpe:2.3:a:*:\\@ampproject\\/remapping:2.2.0:*:*:*:*:*
   ],
   "purl": "pkg:npm/%40ampproject/remapping@2.2.0"
  },
  {
   "id": "aad4fa23efcf7cec",
   "name": "@babel/code-frame",
   "version": "7.18.6",
   "type": "npm",
   "foundBy": "javascript-lock-cataloger",
   "locations": [
```

React App



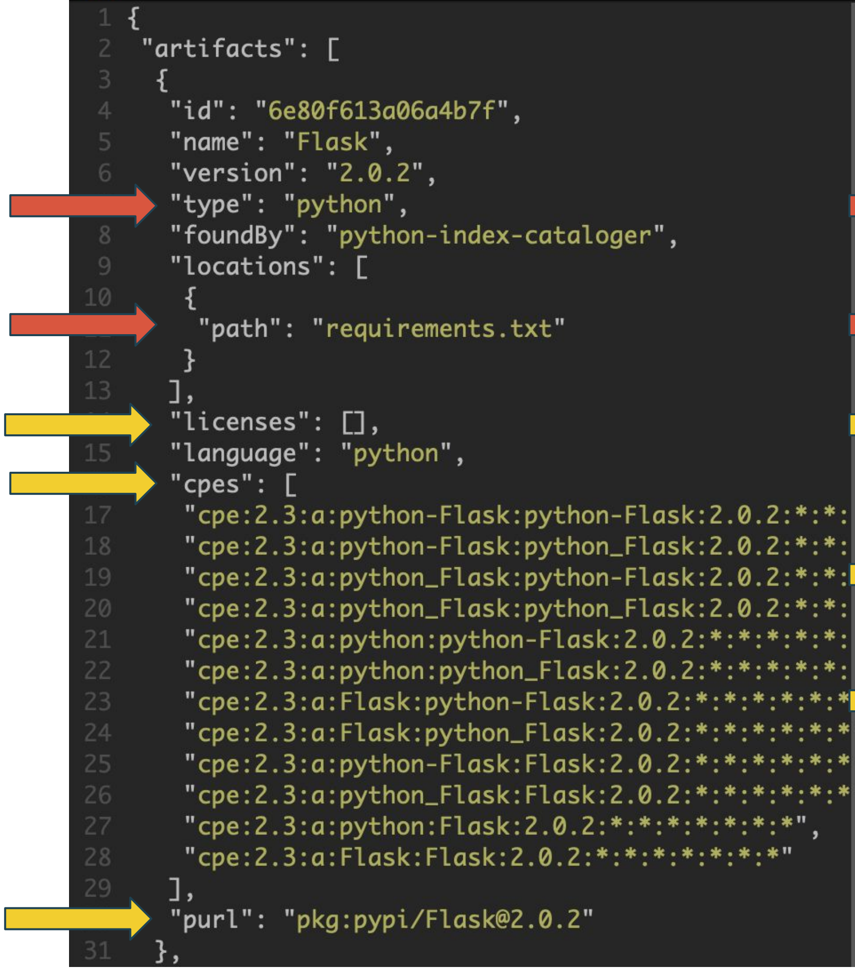
```
{
 "artifacts": [
  {
   "id": "6e80f613a06a4b7f",
   "name": "Flask",
   "version": "2.0.2",
   "type": "python",
   "foundBy": "python-index-cataloger",
   "locations": [
    {
     "path": "requirements.txt"
    }
   ],
   "licenses": [],
   "language": "python",
   "cpes": [
    "cpe:2.3:a:python-Flask:python-Flask:2.0.2:*:*:
    "cpe:2.3:a:python-Flask:python_Flask:2.0.2:*:*:
    "cpe:2.3:a:python_Flask:python-Flask:2.0.2:*:*:
    "cpe:2.3:a:python_Flask:python_Flask:2.0.2:*:*:
    "cpe:2.3:a:python:python-Flask:2.0.2:*:*:*:*:*:
    "cpe:2.3:a:python:python_Flask:2.0.2:*:*:*:*:*:
    "cpe:2.3:a:Flask:python-Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:Flask:python_Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:python-Flask:Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:python_Flask:Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:python:Flask:2.0.2:*:*:*:*:*:*:*",
    "cpe:2.3:a:Flask:Flask:2.0.2:*:*:*:*:*:*:*"
   ],
   "purl": "pkg:pypi/Flask@2.0.2"
  },
```

Python App



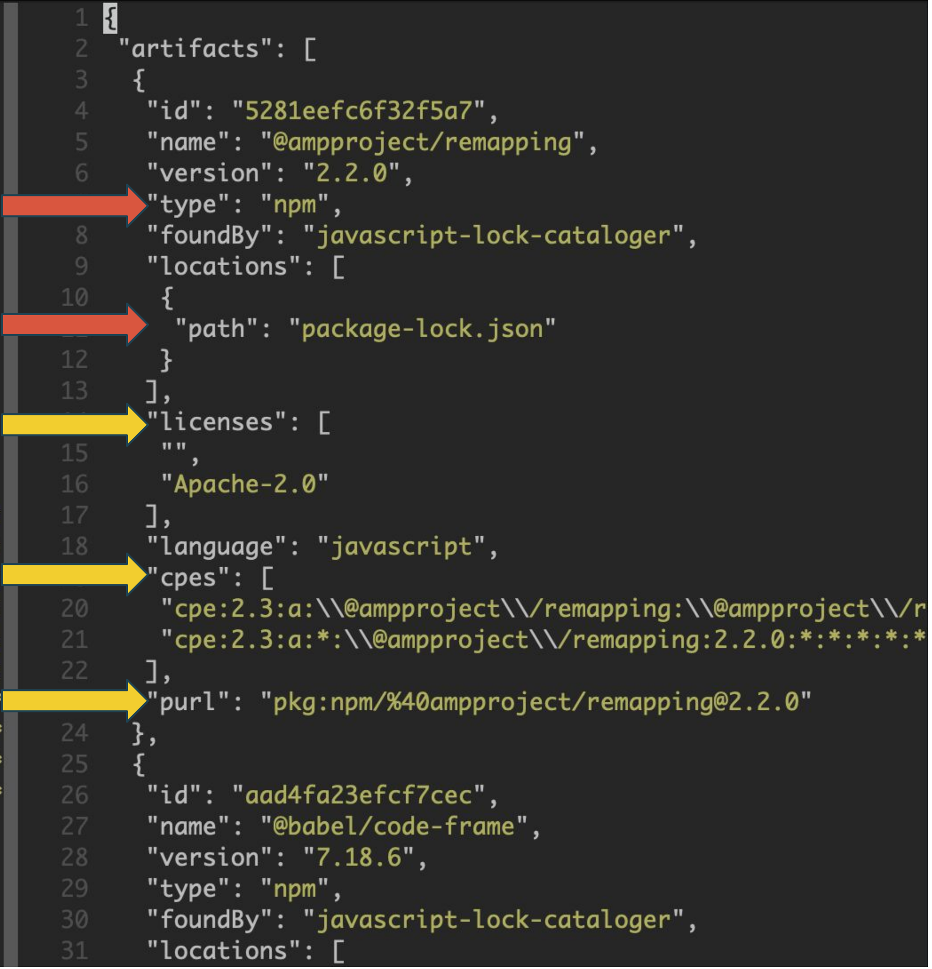
```
{
 "artifacts": [
  {
   "id": "5281eefc6f32f5a7",
   "name": "@ampproject/remapping",
   "version": "2.2.0",
   "type": "npm",
   "foundBy": "javascript-lock-cataloger",
   "locations": [
    {
     "path": "package-lock.json"
    }
   ],
   "licenses": [
    "",
    "Apache-2.0"
   ],
   "language": "javascript",
   "cpes": [
    "cpe:2.3:a:\\@ampproject\\/remapping:\\@ampproject\\/r
    "cpe:2.3:a:*:\\@ampproject\\/remapping:2.2.0:*:*:*:*:*
   ],
   "purl": "pkg:npm/%40ampproject/remapping@2.2.0"
  },
  {
   "id": "aad4fa23efcf7cec",
   "name": "@babel/code-frame",
   "version": "7.18.6",
   "type": "npm",
   "foundBy": "javascript-lock-cataloger",
   "locations": [
```

React App



```
{
 "artifacts": [
  {
   "id": "6e80f613a06a4b7f",
   "name": "Flask",
   "version": "2.0.2",
   "type": "python",
   "foundBy": "python-index-cataloger",
   "locations": [
    {
     "path": "requirements.txt"
    }
   ],
   "licenses": [],
   "language": "python",
   "cpes": [
    "cpe:2.3:a:python-Flask:python-Flask:2.0.2:*:*:
    "cpe:2.3:a:python-Flask:python_Flask:2.0.2:*:*:
    "cpe:2.3:a:python_Flask:python-Flask:2.0.2:*:*:
    "cpe:2.3:a:python_Flask:python_Flask:2.0.2:*:*:
    "cpe:2.3:a:python:python-Flask:2.0.2:*:*:*:*:*:
    "cpe:2.3:a:python:python_Flask:2.0.2:*:*:*:*:*:
    "cpe:2.3:a:Flask:python-Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:Flask:python_Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:python-Flask:Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:python_Flask:Flask:2.0.2:*:*:*:*:*:*
    "cpe:2.3:a:python:Flask:2.0.2:*:*:*:*:*:*:*",
    "cpe:2.3:a:Flask:Flask:2.0.2:*:*:*:*:*:*:*"
   ],
   "purl": "pkg:pypi/Flask@2.0.2"
  },
```

Python App



```
{
 "artifacts": [
  {
   "id": "5281eefc6f32f5a7",
   "name": "@ampproject/remapping",
   "version": "2.2.0",
   "type": "npm",
   "foundBy": "javascript-lock-cataloger",
   "locations": [
    {
     "path": "package-lock.json"
    }
   ],
   "licenses": [
    "",
    "Apache-2.0"
   ],
   "language": "javascript",
   "cpes": [
    "cpe:2.3:a:\\@ampproject\\/remapping:\\@ampproject\\/r
    "cpe:2.3:a:*:\\@ampproject\\/remapping:2.2.0:*:*:*:*:*
   ],
   "purl": "pkg:npm/%40ampproject/remapping@2.2.0"
  },
  {
   "id": "aad4fa23efcf7cec",
   "name": "@babel/code-frame",
   "version": "7.18.6",
   "type": "npm",
   "foundBy": "javascript-lock-cataloger",
   "locations": [
```

React App

So, you’ve generated SBOMs… now what?

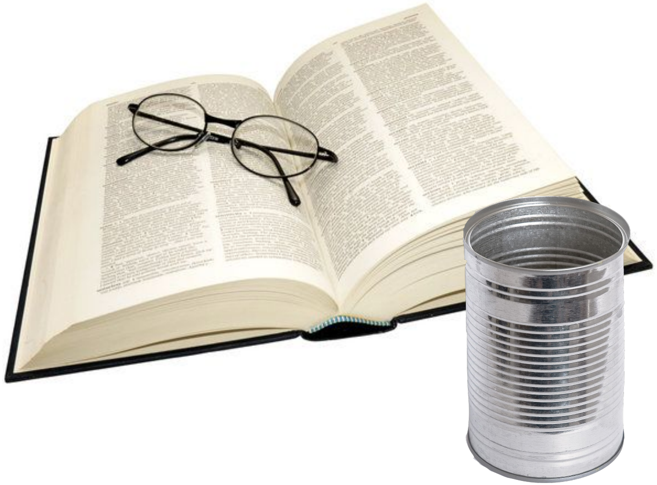
How can you meet consumers’ SBOM expectations?

The best way to to this is to devise a solution that addresses these five questions:

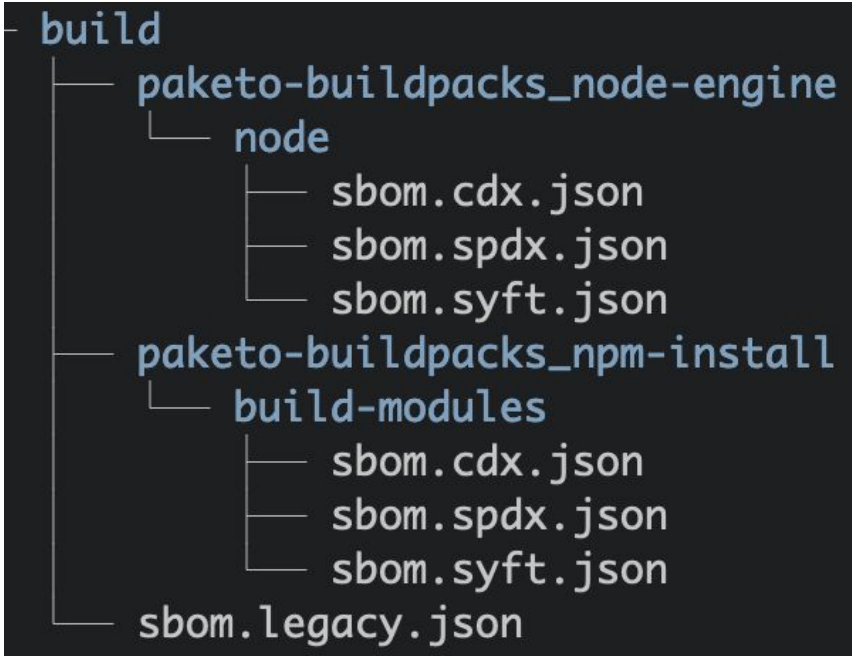
1. **Why** do SBOMs matter? ✅
2. **What** constitutes a useful SBOM? ✅
3. **Who** wants SBOMs? ✅
4. **Where** should SBOMs be stored?
5. **When** should SBOMs be generated?

Where should SBOMs be stored?

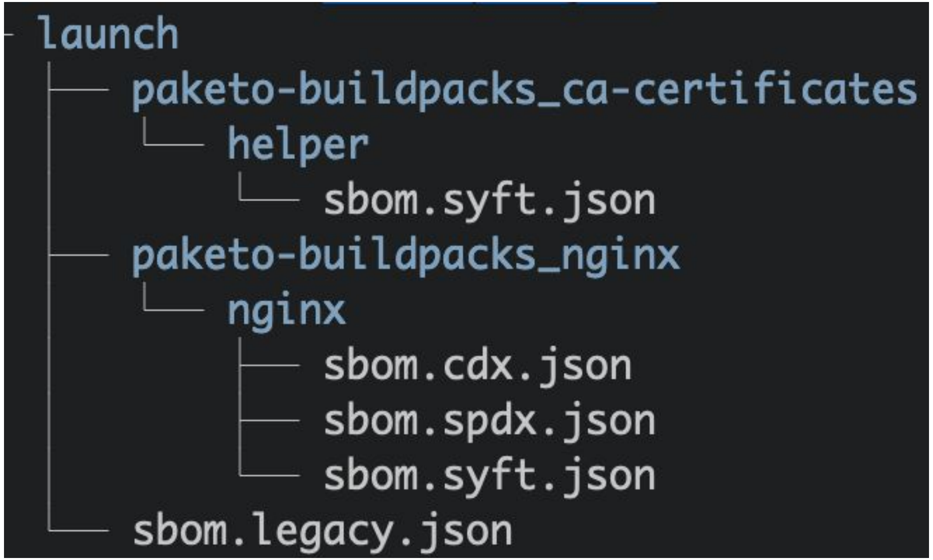
Market Pantry canned pasta combine
value in a rich and hearty home-style
Nutrition Facts
Serving Size 1 cup (252g)
Servings Per Container about 2
Amount Per Serving
Calories 270 Calories from Fat 70
% Daily Value*
Total Fat 7g 11%
Saturated Fat 2.5g 13%
Trans Fat 0g
Cholesterol 15mg 5%
Sodium 1310mg 54%
Total Carbohydrate 43g 14%
Dietary Fiber 2g 6%
Sugars 9g
Protein 9g
Vitamin A 10% • Vitamin C 0%
Calcium 2% • Iron 10%
*Percent Daily Values are based on a 2,000 calorie diet.



Where should SBOMs be stored?



```
- build
  ├── paketo-buildpacks_node-engine
  │   └── node
  │       ├── sbom.cdx.json
  │       ├── sbom.spdx.json
  │       └── sbom.syft.json
  ├── paketo-buildpacks_npm-install
  │   └── build-modules
  │       ├── sbom.cdx.json
  │       ├── sbom.spdx.json
  │       └── sbom.syft.json
  └── sbom.legacy.json
```



```
- launch
  ├── paketo-buildpacks_ca-certificates
  │   └── helper
  │       └── sbom.syft.json
  ├── paketo-buildpacks_nginx
  │   └── nginx
  │       ├── sbom.cdx.json
  │       ├── sbom.spdx.json
  │       └── sbom.syft.json
  └── sbom.legacy.json
```

Are you done?

How can you meet consumers’ SBOM expectations?

The best way to to this is to devise a solution that addresses these five questions:

1. **Why** do SBOMs matter? ✅
2. **What** constitutes a useful SBOM? ✅
3. **Who** wants SBOMs? ✅
4. **Where** should SBOMs be stored? ✅
5. **When** should SBOMs be generated?

When should SBOMs be generated?

Why does it matter **when** you generate your SBOM?

Anchore says:

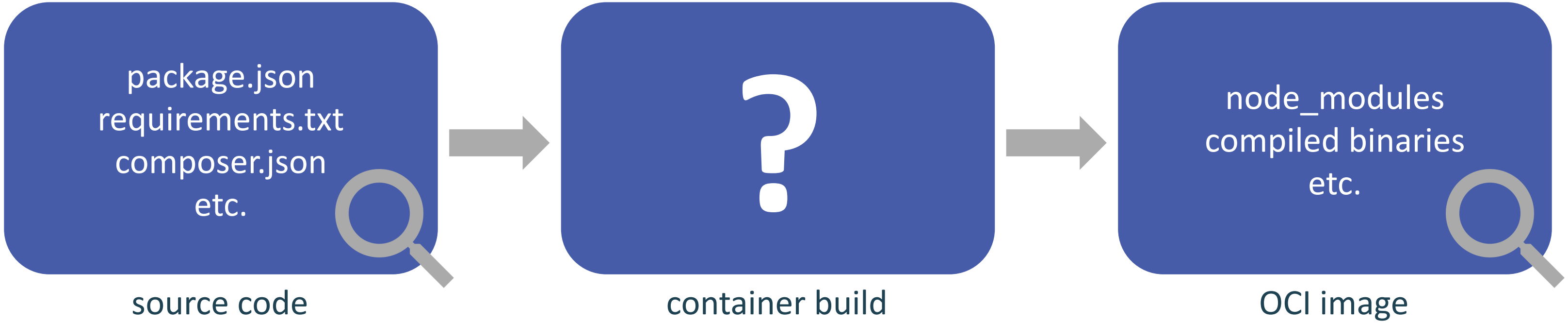
> *"The use of SBOMs for containerized applications provides a unique opportunity to watch for **SBOM drift**—unexpected changes in the contents of a software application—which can indicate potential tampering, new versions, or changes in dependencies..*
>
> *Generating an SBOM creates a snapshot of the components of your container at a specific time during the development process. **By generating an SBOM for each build and at each step in the development process, you can look for differences over time.** Some of those differences might be expected, but any changes should be investigated to determine if they introduce new risk."*

Why does it matter **when** you generate your SBOM?

Minimal images are better for security posture… but are worse for SBOM scans.

Wow, such empty

Why does it matter **when** you generate your SBOM?



package.json
requirements.txt
composer.json
etc.

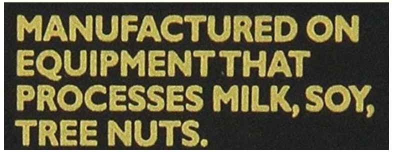
source code

?

container build

node_modules
compiled binaries
etc.

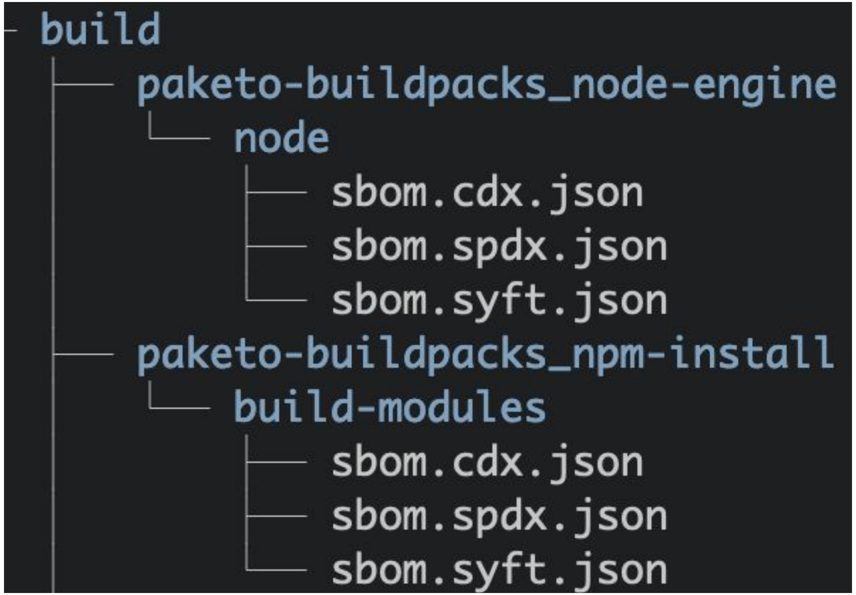
OCI image



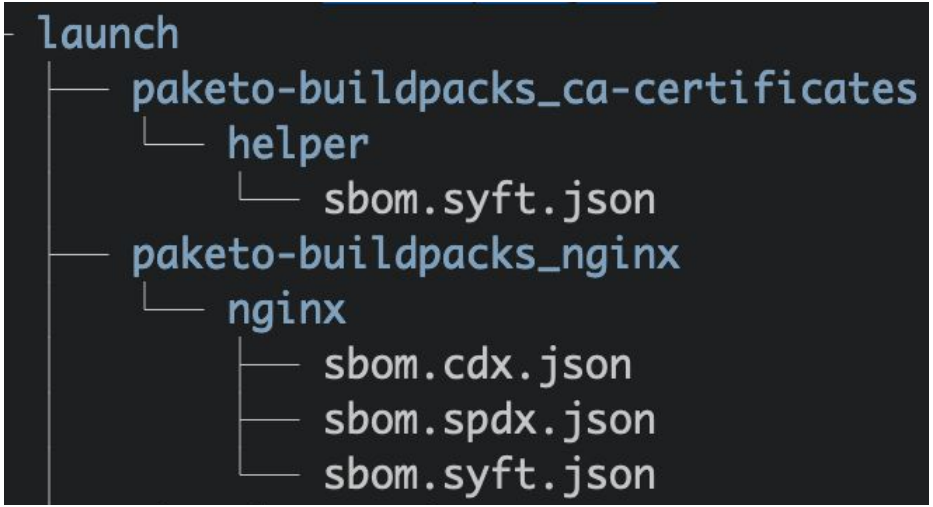
MANUFACTURED ON EQUIPMENT THAT PROCESSES MILK, SOY, TREE NUTS.

"...at each step in the development process…"

Why does it matter **when** you generate your SBOM?

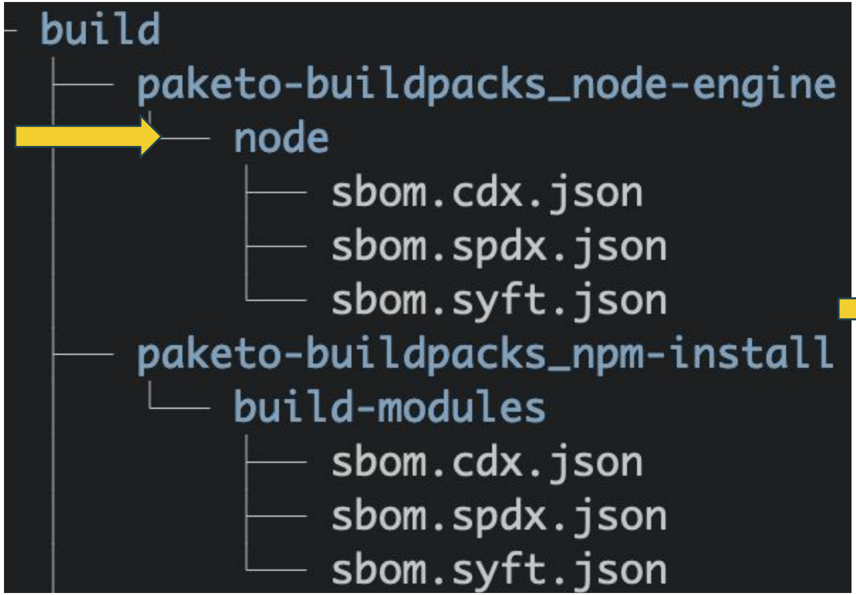


```
- build
  │── paketo-buildpacks_node-engine
  │   └── node
  │       ├── sbom.cdx.json
  │       ├── sbom.spdx.json
  │       └── sbom.syft.json
  ├── paketo-buildpacks_npm-install
  │   └── build-modules
  │       ├── sbom.cdx.json
  │       ├── sbom.spdx.json
  │       └── sbom.syft.json
```

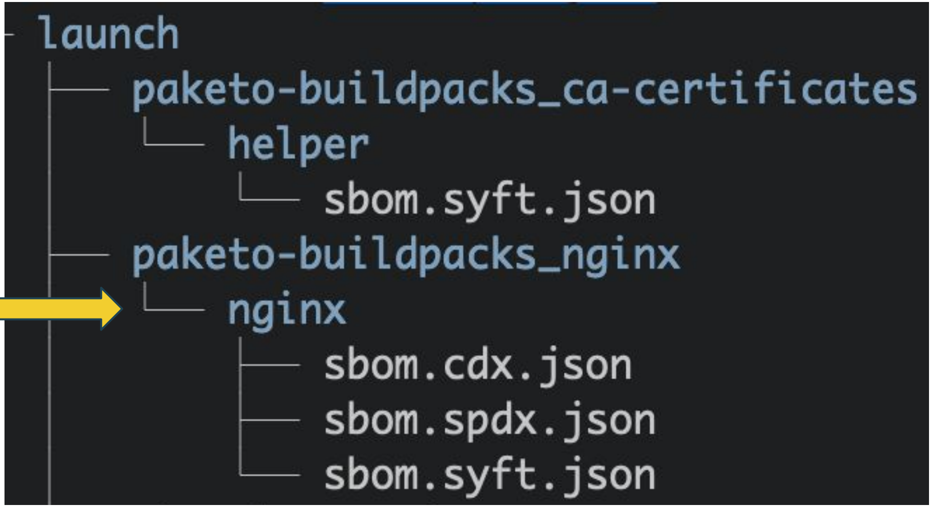


```
- launch
  │── paketo-buildpacks_ca-certificates
  │   └── helper
  │       └── sbom.syft.json
  ├── paketo-buildpacks_nginx
  │   └── nginx
  │       ├── sbom.cdx.json
  │       ├── sbom.spdx.json
  │       └── sbom.syft.json
```

Why does it matter **when** you generate your SBOM?

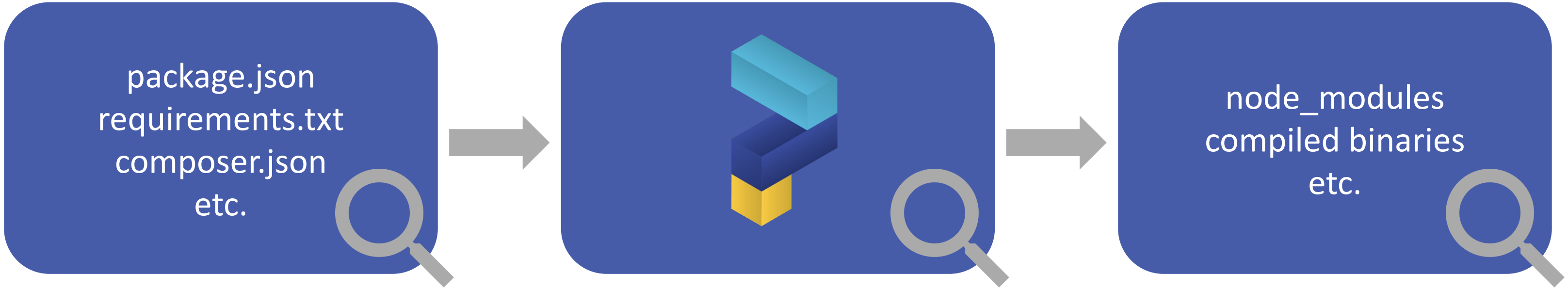


```
- build
  ├── paketo-buildpacks_node-engine
  │   └── node
  │       ├── sbom.cdx.json
  │       ├── sbom.spdx.json
  │       └── sbom.syft.json
  ├── paketo-buildpacks_npm-install
  │   └── build-modules
  │       ├── sbom.cdx.json
  │       ├── sbom.spdx.json
  │       └── sbom.syft.json
```



```
- launch
  ├── paketo-buildpacks_ca-certificates
  │   └── helper
  │       └── sbom.syft.json
  ├── paketo-buildpacks_nginx
  │   └── nginx
  │       ├── sbom.cdx.json
  │       ├── sbom.spdx.json
  │       └── sbom.syft.json
```

SBOMs at each step in development



package.json
requirements.txt
composer.json
etc.

source code

container build

node_modules
compiled binaries
etc.

OCI image

How can you meet consumers’ SBOM expectations?

The best way to to this is to devise a solution that addresses these five questions:

1. **Why** do SBOMs matter? ✅
2. **What** constitutes a useful SBOM? ✅
3. **Who** wants SBOMs? ✅
4. **Where** should SBOMs be stored? ✅
5. **When** should SBOMs be generated? ✅

paketo
buildpacks

Thanks! Questions?

Thanks! Questions?

Visit us at paketo.io

Feedback? Provide it here