Source: Pierre Metivier (https://flic.kr/p/rdHr) CC BY-NC / Desaturated from the original

NTIA Software Component Transparency
October 22, 2020

Formats & Tooling Workgroup

JC Herz
Kate Stewart

Agenda

- Workgroup Goals
- Recap of Formats in Use
  - Populating Example repos, Ecosystem Documents
- Playbooks
  - Consumer playbook overview
  - Supplier playbook overview
- Future Directions
- Feedback Requests

Formats and Tooling Workgroup Goal

Wrapping up from phase I, we identified for the need for:

- Tooling
  - Documenting tooling
  - Identifying tooling gaps
  - Documenting processes ← Playbooks starting to address
  - Turnkey universal translation tools

Formats and Tooling workgroup is focusing on addressing these items.

Examples of Formats

SWID


```xml
<?xml version="1.0" encoding="utf-8"?>
<SoftwareIdentity xmlns="http://standards.iso.org/iso/19770/-2/2015/schema.xsd" xmlns:sha256="http:/
/www.w3.org/2001/04/xmlenc#sha256" xmlns:n8060="http://csrc.nist.gov/ns/swid/2015-extensions/1.0" xm
lns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://standards.iso.org/iso
/19770/-2/2015/schema.xsd http://standards.iso.org/iso/19770/-2/2015-current/schema.xsd     http://c
src.nist.gov/ns/swid/2015-extensions/1.0 https://csrc.nist.gov/schema/swid/2015-extensions/swid-2015
-extensions-1.0.xsd" xml:lang="en-US" name="zip" tagId="unavailable.invalid.zip-3.0-26.fc32.x86_64"
version="3.0-26.fc32.x86_64" versionScheme="rpm">
  <Entity name="" regid="invalid.unavailable" role="tagCreator"/>
  <Link rel="required" use="required" type="swid+xml" ownership="shared" href="swid:unavailable.inva
lid.bzip2-libs-1.0.8-2.fc32.x86_64-rpm-72c50b49853aa8ce60896262a85734085f7836d7553e18e68037f3e913724
25d.swidtag"/>
  <Link rel="required" use="required" type="swid+xml" ownership="shared" href="swid:unavailable.inva
lid.glibc-2.31-2.fc32.x86_64-rpm-e8641adf7969deaa30846bac77c7accf70f3588da3ee4668c73090bfa2e97507.sw
idtag"/>
  <Link rel="required" use="required" type="swid+xml" ownership="shared" href="swid:unavailable.inva
lid.unzip-6.0-47.fc32.x86_64-rpm-8a274fd9aafd2a6d435dd0f923b73be1870097e3bd8e989ad5809f59de14ba78.sw
idtag"/>
  <Meta product="zip" colloquialVersion="3.0" revision="26.fc32" arch="x86_64" summary="A file compr
ession and packaging utility companiestible with PKZIP"/>
  <Evidence date="2020-06-12T19:08:27Z" deviceId="localhost.localdomain" n8060:pathSeparator="/" n80
60:envVarPrefix="$" n8060:envVarSuffix="">
    <File size="213648" name="zip" location="/usr/bin" sha256:hash="8abb7885954cd7cd8a2f9dbecf96a965
c4a837329b9a9bf1eb4e586b8f7e22f5" key="true"/>
    <File size="106416" name="zipcloak" location="/usr/bin" sha256:hash="fa902ca689f188350642284ba56
306660d574755ddb63fcf27f9b333e8ec7f80" key="true"/>
    <File size="97816" name="zipnote" location="/usr/bin" sha256:hash="1418608f5d7675b39e681eec8cc6f
30e0bb418ffd92a73a28575514c38abbac2" key="true"/>
    <File size="97864" name="zipsplit" location="/usr/bin" sha256:hash="0d13183bb15a20ad76012b83b26b
a5b8def1e37195caf48c34a54e09557ef2f0" key="true"/>
    <Directory name=".build-id" location="/usr/lib">
      <Directory name="4c">
        <File size="28" name="224381b5ef923772bf5e1742f00af581b848da" key="true"/>
      </Directory>
      <Directory name="54">
        <File size="27" name="65529f3700a5309915077e5c55cf4db21ad84a" key="true"/>
      </Directory>
```


CycloneDX


```xml
<?xml version="1.0"?><bom serialNumber="9e253f92-4e1c-497e-8f87-50730d24f18a" xmlns="http://cyclonedx.org/schema/bom/1.1">
<components><component type="library"><description>Nerves System BR - Buildroot based build platform for Nerves
Systems</description><hashes><hash alg="SHA-256">e3fda6bc49f8e3662d37355aad88c0839296597c0b6f6653d21967db1890b038</hash></hashes>
<licenses><license><id>Apache-2.0</id></license><license><name>GPLv2</name></license></licenses><name>nerves_system_br</name>
<purl>pkg:hex/nerves_system_br@1.9.5</purl><version>1.9.5</version></component><component type="library"><description>Nerves -
Create firmware for embedded devices like Raspberry Pi, BeagleBone Black, and more</description><hashes><hash alg="SHA-
256">07079342db3a03d19694118a93f220359fbd94b6e174b98d1ea2709db9e81da9</hash></hashes><licenses><license><id>Apache-2.0</id>
</license></licenses><name>nerves</name><purl>pkg:hex/nerves@1.5.1</purl><version>1.5.1</version></component><component
type="library"><description>Socket handling library for Elixir</description><hashes><hash alg="SHA-
256">98a2ab20ce17f95fb512c5cadddba32b57273e0d2dba2d2e5f976c5969d0c632</hash></hashes><licenses><license><id>WTFPL</id></license>
</licenses><name>socket</name><purl>pkg:hex/socket@0.3.13</purl><version>0.3.13</version></component><component type="library">
<description>Read and write to U-Boot environment blocks</description><hashes><hash alg="SHA-
256">b01e3ec0973e99473234f27839e29e63b5b81eba6a136a18a78d049d4813d6c5</hash></hashes><licenses><license><id>Apache-2.0</id>
</license></licenses><name>uboot_env</name><purl>pkg:hex/uboot_env@0.1.1</purl><version>0.1.1</version></component><component
type="library"><description>Nerves Toolchain CTNG - Toolchain Platform</description><hashes><hash alg="SHA-
256">452f8589c1a58ac787477caab20a8cfc6671e345837ccc19beefe49ae35ba983</hash></hashes><licenses><license><id>Apache-2.0</id>
</license></licenses><name>nerves_toolchain_ctng</name><purl>pkg:hex/nerves_toolchain_ctng@1.6.0</purl><version>1.6.0</version>
</component><component type="library"><description>A ring buffer backend for Elixir Logger with IO streaming.</description><hashes>
<hash alg="SHA-256">b1baddc269099b2afe2ea3a87b8e2b71e57331c0000038ae55090068aac679db</hash></hashes><licenses><license><id>Apache-
2.0</id></license></licenses><name>ring_logger</name><purl>pkg:hex/ring_logger@0.8.0</purl><version>0.8.0</version></component>
<component type="library"><description>Nerves System Linter - Lint Nerves System Defconfigs.</description><hashes><hash alg="SHA-
256">84e0f63c8ac196b16b77608bbe7df66dcf352845c4e4fb394bffd2b572025413</hash></hashes><licenses><license><id>Apache-2.0</id>
</license></licenses><name>nerves_system_linter</name><purl>pkg:hex/nerves_system_linter@0.3.0</purl><version>0.3.0</version>
</component><component type="library"><description>DNS library for Elixir using `inet_dns` module.

Note: The `inet_dns` module is considered internal to Erlang and subject to
change. If this happened this library will be updated.</description><hashes><hash alg="SHA-
256">81c46d39f7934f0e73368355126e4266762cf227ba61d5889635d83b2d64a493</hash></hashes><licenses><license><name>BSD-3-Clauses</name>
</license></licenses><name>dns</name><purl>pkg:hex/dns@2.1.2</purl><version>2.1.2</version></component><component type="library">
<description>A simple mDNS (zeroconf, bonjour) server and client for device discovery on your local network.</description><hashes>
<hash alg="SHA-256">f08414daf5636bf5cd364611e838818e9250c91a3282a817ad9174b03e757401</hash></hashes><licenses><license><id>Apache-
2.0</id></license></licenses><name>mdns</name><purl>pkg:hex/mdns@1.0.3</purl><version>1.0.3</version></component><component
type="library"><description>Nerves Toolchain - arm-unknown-linux-gnueabihf</description><hashes><hash alg="SHA-
256">ba48ce7c846ee12dfca8148dc7240988d96a3f2eb9c234bf08bffe4f0f7a3c62</hash></hashes><licenses><license><id>Apache-2.0</id>
</license></licenses><name>nerves_toolchain_arm_unknown_linux_gnueabihf</name>
<purl>pkg:hex/nerves_toolchain_arm_unknown_linux_gnueabihf@1.2.0</purl><version>1.2.0</version></component><component
type="library"><description>Nerves System - Raspberry Pi 3 A+</description><hashes><hash alg="SHA-
256">c75c5a4c42a2aed5a4ed8116c143993500d1546edb5550978f528e980a7d5f03</hash></hashes><licenses><license><id>Apache-2.0</id>
</license></licenses><name>nerves_system_rpi3a</name><purl>pkg:hex/nerves_system_rpi3a@1.9.2</purl><version>1.9.2</version>
</component><component type="library"><description>Atomic nested term storage and dispatch registry</description><hashes><hash
alg="SHA-256">df791dc276652fcfb53be4dab823e05f8269b96ac57c26f86a67838dbc0eefe7</hash></hashes><licenses><license><id>Apache-
2.0</id></license></licenses><name>system_registry</name><purl>pkg:hex/system_registry@0.8.2</purl><version>0.8.2</version>
</component><component type="library"><description>Nerves Toolchain - armv6-rpi-linux-gnueabi</description><hashes><hash alg="SHA-
256">007668c7ad1f73bad8fd54ad1a27a3b0fb91bca51b4af6bb3bbdac968ccae0ba</hash></hashes><licenses><license><id>Apache-2.0</id>
</license></licenses><name>nerves_toolchain_armv6_rpi_linux_gnueabi</name>
<purl>pkg:hex/nerves_toolchain_armv6_rpi_linux_gnueabi@1.2.0</purl><version>1.2.0</version></component><component type="library">
<description>Nerves System - Raspberry Pi A+ / B+ / B</description><hashes><hash alg="SHA-
256">a9b68559cbb4585d7b050394f2e2395cc7517f9a0816d9ea9115f1164db731e9</hash></hashes><licenses><license><id>Apache-2.0</id>
</license></licenses><name>nerves_system_rpi</name><purl>pkg:hex/nerves_system_rpi@1.9.2</purl><version>1.9.2</version></component
<component type="library"><description>Get your boot on.</description><hashes><hash alg="SHA-
256">f9a1b7d6212cf18ba91c4f71c26076059df33cea4db2eb3c098bfa6673349412</hash></hashes><licenses><license><id>Apache-2.0</id>
</license></licenses><name>shoehorn</name><purl>pkg:hex/shoehorn@0.6.0</purl><version>0.6.0</version></component><component
type="library"><description>Nerves System - BeagleBone Black, BeagleBone Green, PocketBeagle and more</description><hashes><hash
alg="SHA-256">e7ac32898cc4fb259a308116df2745fff12ea360cdb91c74906baef49b223ada</hash></hashes><licenses><license><id>Apache-
2.0</id></license></licenses><name>nerves_system_bbb</name><purl>pkg:hex/nerves_system_bbb@2.4.2</purl><version>2.4.2</version>
</component><component type="library"><description>A Make compiler for Mix</description><hashes><hash alg="SHA-
256">38349f3e29aff4864352084fc736fa7fa0f2995a819a737554f7ebd28b85aaab</hash></hashes><licenses><license><id>Apache-2.0</id>
</license></licenses><name>elixir_make</name><purl>pkg:hex/elixir_make@0.6.0</purl><version>0.6.0</version></component><component
```


SPDX


```
SPDXVersion: SPDX-2.1
DataLicense: CC0-1.0
DocumentNamespace: http://www.spdx.org/spdxdocs/8f141b09-1138-4fc5-aecb-
fc10d9ac1eed
DocumentName: SpdxDoc for GNU Time
SPDXID: SPDXRef-DOCUMENT

## Creation Information
Creator: Person: Gary O'Neall
Creator: Tool: Source Auditor Open Source Console
Created: 2018-08-17T11:29:46Z
LicenseListVersion: 3.2
## Relationships
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-1

## Package Information
PackageName: GNU Time
SPDXID: SPDXRef-1
PackageVersion: 1.9
PackageFileName: time-1.9.tar.gz
PackageSupplier: Organization: GNU
PackageOriginator: Organization: GNU
PackageDownloadLocation: https://ftp.gnu.org/gnu/time/time-1.9.tar.gz
PackageVerificationCode: 4ee8abb8bc16eaa2a44446bb6354fef171bb5543
PackageChecksum: SHA1: 75068c26abbed3ad3980685bae21d7202d288317
PackageHomePage: https://www.gnu.org/software/time/
PackageLicenseConcluded: (GFDL-1.3 AND GPL-3.0-or-later AND LicenseRef-1)
## License information from files
PackageLicenseInfoFromFiles: X11
PackageLicenseInfoFromFiles: GPL-2.0-or-later WITH Libtool-exception
PackageLicenseInfoFromFiles: GPL-3.0-or-later
PackageLicenseInfoFromFiles: LicenseRef-1
PackageLicenseInfoFromFiles: GFDL-1.3
PackageLicenseDeclared: GPL-3.0-or-later
PackageLicenseComments: <text>Several files contained a GPL 2.0 or later
license.  Since they were linked to a GPL 3.0 package, GPL 3.0 was used.</
text>
PackageCopyrightText: <text>Copyright (C) 1990-2018 Free Software Foundation,
Inc.</text>
PackageSummary: <text>The `time' command runs another program, then displays
information about the resources used by that program.</text>
PackageDescription: <text>The `time' command runs another program, then
displays information about the resources used by that program.</text>

## File Information
FileName: ./tests/help-version.sh
SPDXID: SPDXRef-164
FileType: SOURCE
FileChecksum: SHA1: 30b3973b22ddbcd9e8982a06c5a2440fcb315013
LicenseConcluded: GPL-3.0-or-later
LicenseInfoInFile: GPL-3.0
LicenseComments: Seen licenses generated by Source Auditor Scanner.  Results
should be manually verified.
FileCopyrightText: <text>Copyright Free Software Foundation, Inc</text>
FileNotice: <text>NOASSERTION</text>
```


Phase II - Test Corpus

Are there examples that community needs?

How much rigor?

Tooling Surveys Collected to date:

SWID

SPDX

CycloneDX

Contact document curators if questions, follow up, etc. or add comments in documents

- SWID: Charles Schmidt <cmschmidt@mitre.org>
- SPDX: Kate Stewart <kstewart@linuxfoundation.org>
- Cyclone DX: Steve Springett <steve.springett@owasp.org>

Taxonomy used for Classifying Tools

Category	Type	Description
Author during Build	Build	Document is automatically created as part of building an artifact and contains information about the build.
Author after Creation	Manual	A person will manually fill in the information
	Audit Tool	A source code analysis or audit tool will generate the document by inspection of the artifact and any associated sources.
Consume	View	Be able to understand the contents in human readable form (picture, figures, tables, text.). Use to support decision making & business processes.
	Diff	Be able to compare two documents of a given formation and clearly see the differences. For instance, comparing between two versions of a piece of software.
	Analyze	Be able to import a document into your system
Transform	Translate	Change from one file type to another file type while preserving the same information.
	Merge	Multiple sources of documents can be merged together for analysis and audit puproses
	Tool integration	Support use in other tools by APIs, libraries.

SwiftBom – A web based tool to build Software Bill of Material (SBOM)

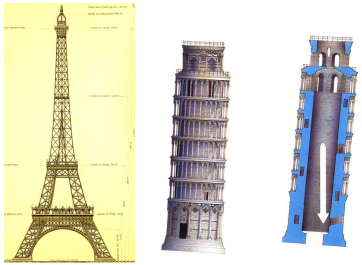
Vijay Sarvepalli CERT/CC

Copyright and license

Introduction and Background

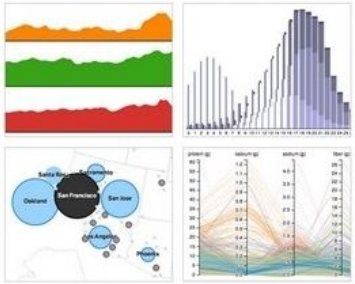
- Authors : Vijay Sarvepalli CERT/CC
- Sponsors : DHS CISA, NTIA
- Collaborators: Linux Foundation, Open C2
- Users: Health care PoC and others via NTIA outreach

Architecture
== put things together
For better or for worse



Automation
∝ workload

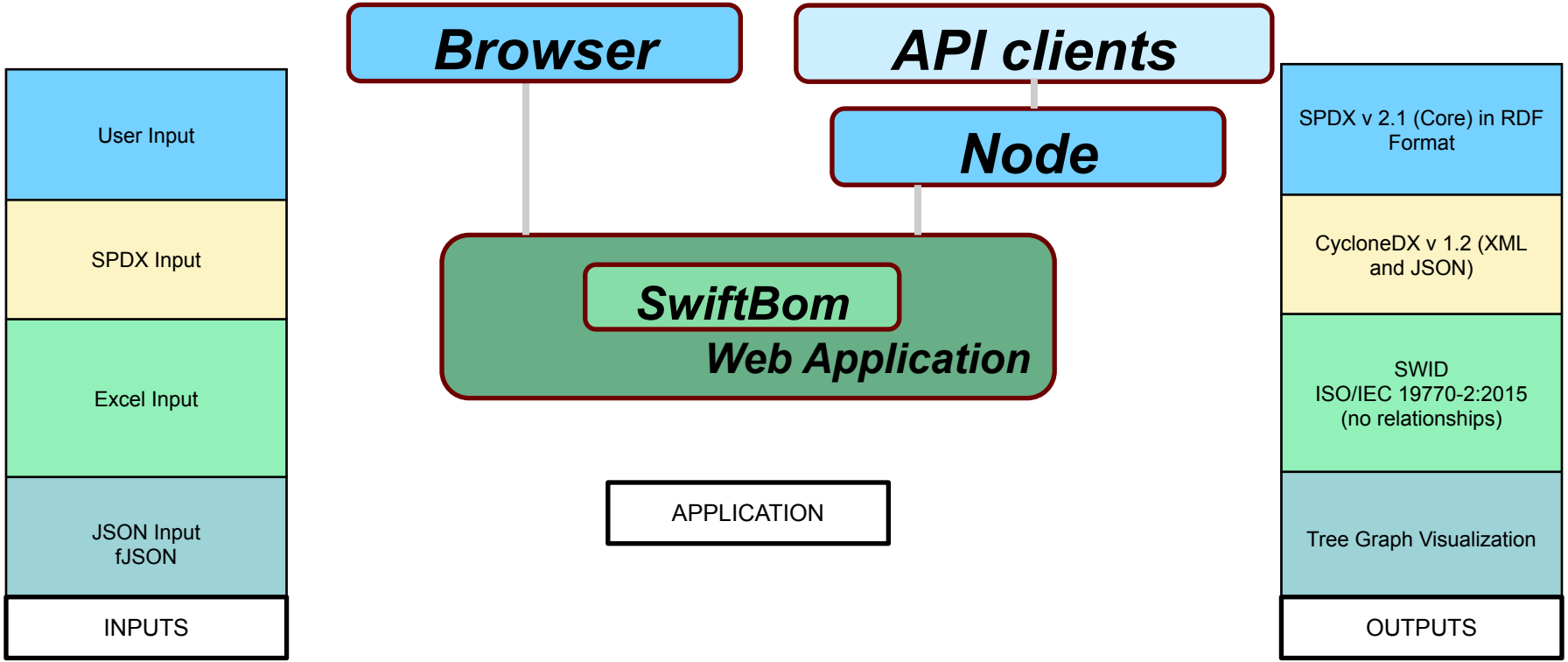
Visualization
== simplicity + clarity



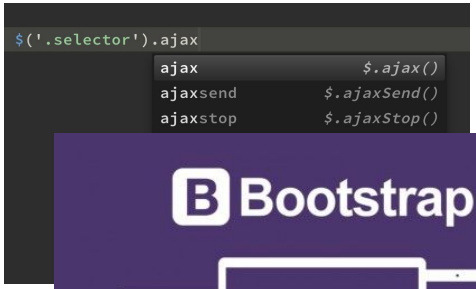
SwiftBom – why and what

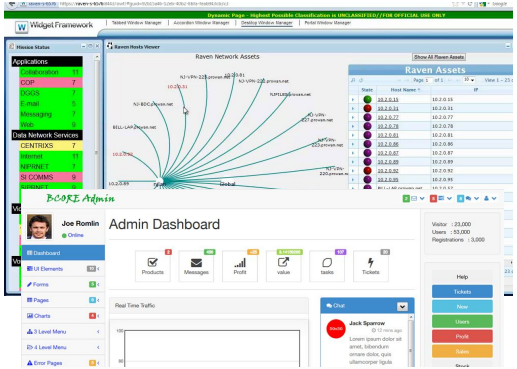
- *Healthcare PoC reveals practical needs for SBOM*
- In the principle of “See something , ~~say something~~ Do something” – SwiftBOM is born.
- SwiftBom will accept user input generate machine-friendly SBOM format and a simple user-friendly graphic to validate input
- Ease of use in mind to manage SBOMs, merge SBOMs and modify SBOMs
- Other use cases such as vulnerability analysis via UI is possible simple examples tried so far

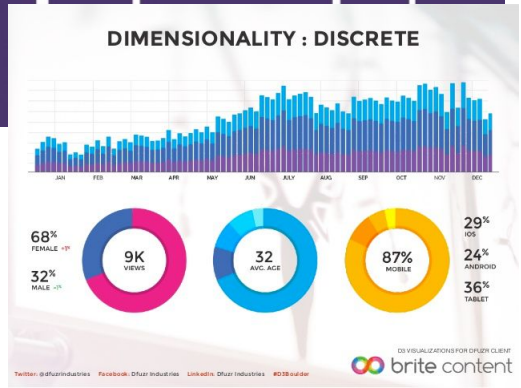
Components of SwiftBOM

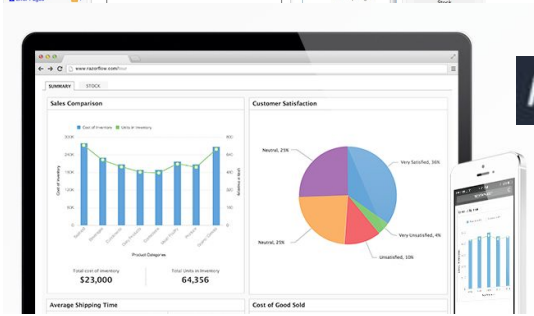


Public framework by design -reuse





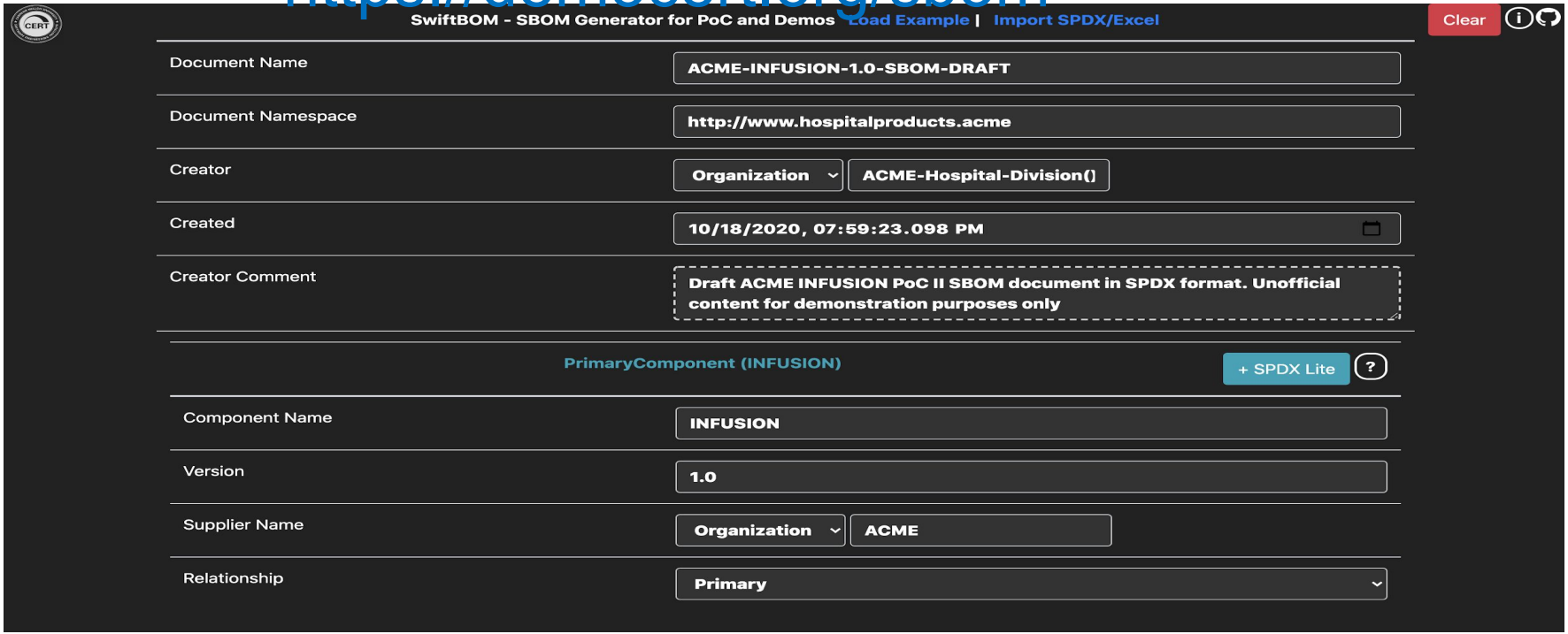




Swap in modules for third party party and replace viz, inputs as needed.

SwiftBOM in action

https://democert.org/sbom



https://youtu.be/pmqGp8TWoF4

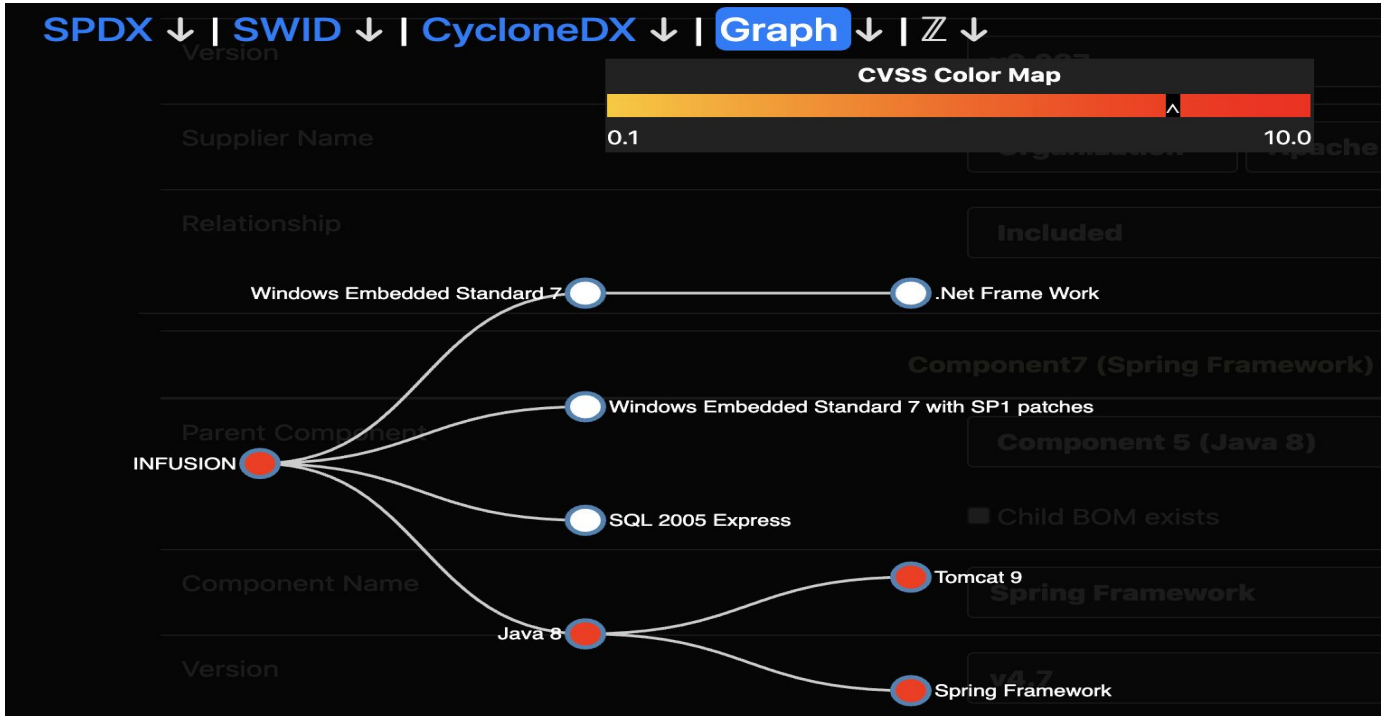
Input formats -

- *Manual Entry*
  - *Context (Header), Component, Sub-Component and relationships*
- *Excel input templates*
  - Excel with same manual input
- SPDX v 2.1
  - SPDX with “CONTAINS” relationships
  - SPDX Lite fields accepted (Optional)
  - Load SBOM edit/replace/remove
  - Merge multiple v2.1 SPDX to one SBOM

Output formats

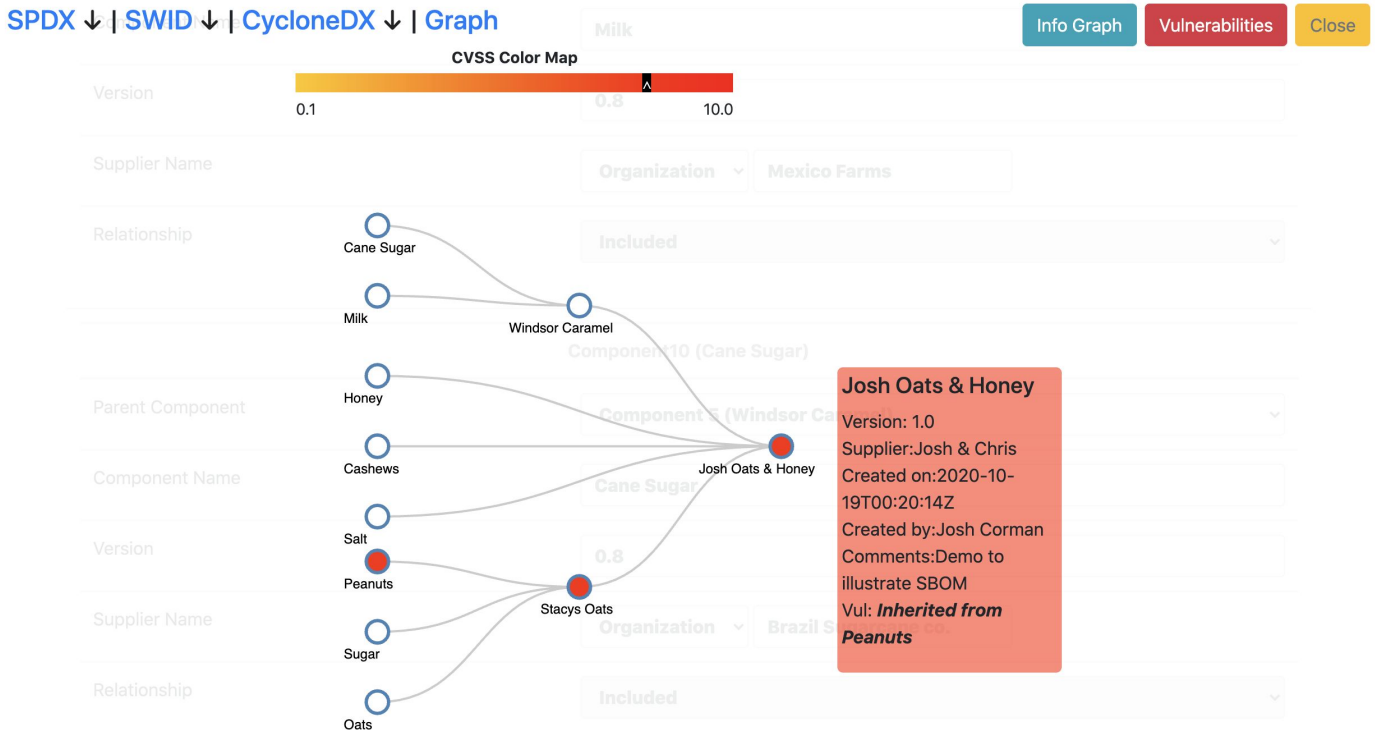
- SPDX 2.1
  - Relationships modeled as “CONTAINS”
  - SPDX Components with distinct SPDX IDS
  - SPDX Lite fields accepted
- Cyclone DX v 1.2
  - XML with UUID local generated for references
  - JSON with all XML data but valid v2.1 JSON schema
- SWID – ISO/IEC Spec
  - Valid SWID XML but lacks relationships
  - Pending some examples in SWID

User-friendly tree graph



Download all formats and download Zipped bundle that contains an image as well

Other use cases



Using, developing and way forward

- Full source available in Git https://github.com/CERTCC/SBOM/
- Privacy - No data is collected, full app is available for offline use, no need to share any data publicly
- As a Node-app this can be used in any mobile app and inputs can integrate to scanners like QR, Barcode and apk or aap scanners
- Try it!
- https://democert.org/sbom/

Playbooks for using “Tools in Operation”

- Concepts of Operation (CONOPS) for how they can be used
  - Generation and Consumption
  - Different Use Cases
    - Software Lifecycle Management
    - Entitlements
    - Vulnerability Management
  - Different Roles in the Supply Chain
    - Third Party Supplier (OSS, Commercial Software)
    - Integrator
    - First-party Developer (Internal Enterprise DevOps)
    - Procurement
    - Compliance (interface with external certifiers, regulators, insurers)

SBOM Consumer Playbook: Overview

- Acquisition of an SBOM from a Supplier
- SBOM Coverage for Software Systems
- SBOM Ingestion and Parsing
- Software Entity Resolution
- Use of Data by Third Party Processes and Platforms (e.g. CMDB, SAM, SOC)
- Ongoing Monitoring
- IP and Confidentiality Status of SBOMS
- Consumer Playbook Draft: https://docs.google.com/document/d/1Ae0l1MDS8m1on58e8mdVIA9NujzPD0k5j352VlDZr9I/edit
- Comments and Feedback Welcome

Next Steps

Priorities for next steps?

- Continue to collect tools
  - Know a tool to be added to each ecosystem document? Put a comment in the document, so it can be added.
  - SWID: http://tiny.cc/SWID
  - SPDX: http://tiny.cc/SPDX
  - CycloneDX: http://tiny.cc/CycloneDX
- Continue to Population of Examples in Phase II - Test Corpus
- Finalize Playbooks
- Collaboration with other health care PoC, other use cases & framing

Volunteers interested on working on above areas? Feedback on proposed approach?

More Info...

Mailing List: ntia-sbom-formats@linuxfoundation.org

Subscribe at: https://lists.linuxfoundation.org/mailman/listinfo/ntia-sbom-formats

Shared Drive:
https://drive.google.com/drive/folders/1KAQ7AWlWMKcSFnRc_S-7XB76xFRRWLmT

Consumer Playbook Draft:
https://docs.google.com/document/d/1Ae0l1MDS8m1on58e8mdVIA9NujzPD0k5j352VlDZr9I/edit

Meetings: Every 2 weeks, next meeting scheduled for July 17 at 11am EST. Contact leads to be added to meeting invite.