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

CycloneDX

SPDX

Phase II - Test Corpus

Are there examples that community needs?
How much rigor?
### Tooling Surveys Collected to date:

#### SWID

<table>
<thead>
<tr>
<th>Format Overview</th>
<th>Format Publishing History</th>
<th>Tool Classification Taxonomy</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

#### SPDX

<table>
<thead>
<tr>
<th>Format Overview</th>
<th>Format Publishing History</th>
<th>Tool Classification Taxonomy</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

#### CycloneDX

<table>
<thead>
<tr>
<th>Format Overview</th>
<th>Format Publishing History</th>
<th>Tool Classification Taxonomy</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

- **Proprietary Products**:
  - GitHub
  - Bitbucket
  - Bintray
  - VirusTotal
  - VirusShare
  - WhiteSource
  - Snyk
  - Trivy
  - Yggdrasil

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

- **SWID**: Charles Schmidt <cmsgschmidt@mitre.org>
- **SPDX**: Kate Stewart <kstewart@linuxfoundation.org>
- **Cyclone DX**: Steve Springett <steve.springett@owasp.org>
# Taxonomy used for Classifying Tools

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author during Build</td>
<td>Build</td>
<td>Document is automatically created as part of building an artifact and contains information about the build.</td>
</tr>
<tr>
<td>Author after Creation</td>
<td>Manual</td>
<td>A person will manually fill in the information</td>
</tr>
<tr>
<td></td>
<td>Audit Tool</td>
<td>A source code analysis or audit tool will generate the document by inspection of the artifact and any associated sources.</td>
</tr>
<tr>
<td>Consume</td>
<td>View</td>
<td>Be able to understand the contents in human readable form (picture, figures, tables, text.). Use to support decision making &amp; business processes.</td>
</tr>
<tr>
<td></td>
<td>Diff</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Analyze</td>
<td>Be able to import a document into your system</td>
</tr>
<tr>
<td>Transform</td>
<td>Translate</td>
<td>Change from one file type to another file type while preserving the same information.</td>
</tr>
<tr>
<td></td>
<td>Merge</td>
<td>Multiple sources of documents can be merged together for analysis and audit purposes</td>
</tr>
<tr>
<td></td>
<td>Tool integration</td>
<td>Support use in other tools by APIs, libraries.</td>
</tr>
</tbody>
</table>
SwiftBom – A web based tool to build Software Bill of Material (SBOM)

Vijay Sarvepalli CERT/CC
Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[Distribution Statement A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® is a registered mark of Carnegie Mellon University.
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

Browser

API clients

SwiftBom

Web Application

INPUTS

User Input

SPDX Input

Excel Input

JSON Input

fJSON

APPLICATION

OUTPUTS

SPDX v 2.1 (Core) in RDF Format

CycloneDX v 1.2 (XML and JSON)

SWID ISO/IEC 19770-2:2015 (no relationships)

Tree Graph Visualization
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/1Ae0l1MDS8m1on58e8mdVIA9NujzPD0k5j352VIDZr9I/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](http://tiny.cc/SWID)
  - SPDX: [http://tiny.cc/SPDX](http://tiny.cc/SPDX)
  - CycloneDX: [http://tiny.cc/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-7XB76xFRRWLMrT

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.