

# SBOM – POC Manufacturer Perspective

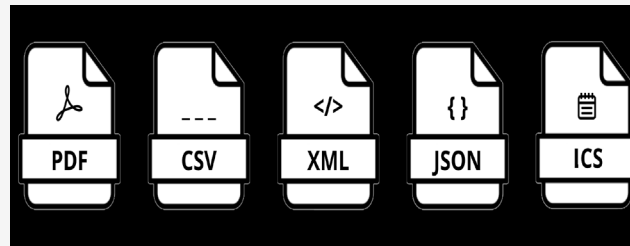
POC lessons and challenges



# Steps in SBOM POC

## 1 Information Gathering

```
Macintosh-08250@ccc94c-4:pdf_press_ppohler$ ./build.sh
./build.sh: line 2: >: command not found
adding: LICENSE-5-STEPS.txt (deflated 50%)
adding: README.md (deflated 40%)
adding: docs/ (stored 0%)
adding: docs/PDF_Press_User_Guide.html (deflated 60%)
adding: docs/PDF_Press_User_Guide.pdf (deflated 11%)
adding: docs/pdf_press_guide.md (deflated 61%)
adding: system/ (stored 0%)
adding: system/expressionengine/ (stored 0%)
adding: system/expressionengine/third_party/ (stored 0%)
adding: system/expressionengine/third_party/pdf_press/ (stored 0%)
adding: system/expressionengine/third_party/pdf_press/config.php (deflated 46%)
adding: system/expressionengine/third_party/pdf_press/doopdf/ (stored 0%)
adding: system/expressionengine/third_party/pdf_press/doopdf/composer.json (deflated 48%)
adding: system/expressionengine/third_party/pdf_press/doopdf/CONTRIBUTING.md (deflated 52%)
adding: system/expressionengine/third_party/pdf_press/doopdf/doapdf.php (deflated 66%)
adding: system/expressionengine/third_party/pdf_press/doopdf/doapdf_config_custom.inc.php (deflated 66%)
adding: system/expressionengine/third_party/pdf_press/doopdf/doapdf_config.inc.php (deflated 66%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/ (stored 0%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/absolute_positioner.cls.php (deflated 70%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/abstract_renderer.cls.php (deflated 77%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/attribute_translator.cls.php (deflated 80%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/autoload.inc.php (deflated 50%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/block_frame_decorator.cls.php (deflated 70%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/block_frame_reflower.cls.php (deflated 70%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/block_positioner.cls.php (deflated 50%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/block_renderer.cls.php (deflated 73%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/cached_pdf_decorator.cls.php (deflated 76%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/canvas.cls.php (deflated 75%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/canvas_factory.cls.php (deflated 59%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/cellmap.cls.php (deflated 76%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/cpdf_adapter.cls.php (deflated 72%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/css_color.cls.php (deflated 66%)
adding: system/expressionengine/third_party/pdf_press/doopdf/include/doapdf.cls.php (deflated 70%)
```



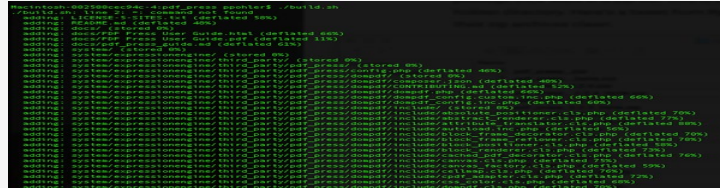
## 2 Generating machine/human readable document

## 3 Distributing/Sharing SBOM

# Steps in SBOM POC

## 1 Information Gathering

- Application Components
- Platform Components



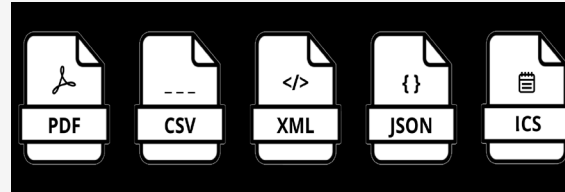
Product Team	SCA Tools	License Clearance Team	Manual Inventory List	SW Build Team (CI)	Vulnerability Monitoring
<ul style="list-style-type: none"><li>- WMI and Powershell</li><li>o Too much of unwanted data!</li><li>o Missing non-installable components</li></ul>	<ul style="list-style-type: none"><li>- Open source and commercial SCA</li><li>o Most are good in identifying open source or COTS components</li><li>o Missing some custom built components</li></ul>	<ul style="list-style-type: none"><li>- Licensing components list</li><li>o Not able to get complete list of components</li></ul>	<ul style="list-style-type: none"><li>- MDM inventory of product's components</li><li>o Use Excel macro to create SBOM</li><li>o Webform data entry</li></ul>	<ul style="list-style-type: none"><li>- Export build script</li><li>o Missing Platform components</li><li>o Missing manufacture's name</li></ul>	<ul style="list-style-type: none"><li>- 3<sup>rd</sup> Components monitoring</li><li>o Has all information for SBOM and VEX</li><li>o Need to ensure Data completeness</li></ul>

# Steps in SBOM POC

---

2

Generating machine/human readable document



- Content
  - Baseline elements established by the Framing Working Group
- Formats
  - SPDX, SWID and CycloneDX
  - POC has established SPDX and SWID
  - SPDX and CycloneDX have tool support
- Tools
  - Custom Excel script files
  - Web based data entry form
  - Manufacturer custom tools
  - SCA tools generate SPDX or custom format
- Challenges
  - Component ID
    - Software Identity
    - purl, CPE names
  - Component patch information in SBOM
  - Missing SBOM from supply chain
  - Linking Primary SBOM, and Medical device for better asset management
  - SBOM Verification - Is SBOM complete?

# Steps in SBOM POC

---

## 3 Distribution/Sharing SBOM



- BOX folder with Excel registry for now
- Future thoughts...
  - Host in common public domain
  - Authenticated common domain
  - Manufacture specific domain
  - Provided by Medical Device, when applicable

## ? Guidance/playbook document in progress