Use Cases & State of Practice
Working Group

Summary of Work and Potential Next Steps
November 18 2019
Initial approach: gather data

Live interviews to find out how people use SBOM, what works, & what are stumbling blocks

Less mature:
- No SBOM penetration
- No tooling, no readiness
- SBOM not a factor in selection
- “Our vendors are clueless!”
- “SBOM is QA’s problem!”
- “Vetting is too much work!”

More mature:
- Consistent SBOM Everywhere
- Mature tooling
- SBOM contract language
- “We can respond to incidents.”
- “Let’s phase out EoL assets.”
- “SBOM is a forcing function.”
# Software Supply Chain Roles

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Produce</th>
<th>Choose</th>
<th>Operate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>Less unplanned, unscheduled work</td>
<td>A more accurate total cost of ownership</td>
<td>More efficient administration</td>
</tr>
<tr>
<td>Security Risk</td>
<td>Avoid known vulnerabilities</td>
<td>Easier due diligence</td>
<td>Faster identification and resolution. Know if and where specific software is affected</td>
</tr>
<tr>
<td>License Risk</td>
<td>Quantify and manage licenses and associated risk</td>
<td>Easier due diligence</td>
<td>More efficient, accurate response to license claims</td>
</tr>
<tr>
<td>Compliance Risk</td>
<td>Easier risk evaluation. Identify compliance requirements earlier in lifecycle</td>
<td>More accurate due diligence, catch issues earlier in lifecycle</td>
<td>Streamlined process</td>
</tr>
<tr>
<td>High Assurance (See Appendix II)</td>
<td>Make assertions about artifacts, sources, and processes used.</td>
<td>Making informed, attack-resistant choices about components.</td>
<td>Validate claims under changing and adversarial conditions.</td>
</tr>
</tbody>
</table>
Document SBOM Benefits by Supply Chain Role

**Produce Software**
- Less unplanned maintenance work
- Reduce code bloat / streamline component choice
- Understand component and code dependencies
- Know and comply with licensing
- Monitoring/reviewing for vulnerability
- Awareness of component EOL, orphan, etc.
- Streamlined code review
- Streamline release/production
- Enable black- and whitelists
- SBOM and transparency for customers

**Choose Software**
- Identify vulnerable components
- Targeted security analysis
- Verify sourcing
- Compliance with policies
- Awareness of component EOL, orphan, etc.
- Integrate with asset, compliance, ERT systems
- Audit and verify supplier claims
- Show best practices by supplier

**Operate Software**
- Easily ID vulnerabilities
- Drive independent mitigations
- Better risk analysis - “Roadmap for the defender”
- Awareness of component EOL, orphan, etc.
- Streamline administration
An ecosystem perspective

Beyond the specific benefits to stakeholders, broader adoption of SBOM generation and use can help across the ecosystem.

• Accelerated vulnerability management
• Selecting for better suppliers
• Amplified “herd immunity”
• Weathering suppliers going away
• Combined/Cumulative Value
Time to Remediation Case Studies
Without and With SBOM

- **Vulnerability Awareness**
- **Mitigation**
- **Remediation - Parts**
- **Remediation - Compound Parts**
- **Remediation - Final Goods Assembled**
- **Remediation - Operator**
An ecosystem perspective

Beyond the specific benefits to stakeholders, broader adoption of SBOM generation and use can help across the ecosystem.

- Accelerated vulnerability management
- **Selecting for better suppliers**
- Amplified “herd immunity”
- Weathering suppliers going away
- Combined/Cumulative Value
An ecosystem perspective

Beyond the specific benefits to stakeholders, broader adoption of SBOM generation and use can help across the ecosystem.

• Accelerated vulnerability management
• Selecting for better suppliers
• Amplified “herd immunity”
• Weathering suppliers going away
• Combined/Cumulative Value
An ecosystem perspective

Beyond the specific benefits to stakeholders, broader adoption of SBOM generation and use can help across the ecosystem.

• Accelerated vulnerability management
• Selecting for better suppliers
• Amplified “herd immunity”
• Weathering suppliers going away
• Combined/Cumulative Value
SBOM Depth and Effectiveness
Next steps: Potentially transition focus to *Awareness and Adoption*

Some ideas already discussed by the working group:

- A framework to track broader SBOM landscape, engagement needs, etc
- Coordinate with groups engaged in related work
- International context
- FAQs
- Branding to help outreach
- Targeted resources for specific roles: C-suite, project mgmt., product manager, risk manager, staff engineer