<table>
<thead>
<tr>
<th>PARTS</th>
<th>COMPOUND PARTS</th>
<th>FINAL GOODS ASSEMBLED</th>
<th>OPERATOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>S1</td>
<td>S1</td>
<td>S1</td>
</tr>
<tr>
<td>S2</td>
<td>S2</td>
<td>S2</td>
<td>S2</td>
</tr>
<tr>
<td>S3</td>
<td>S3</td>
<td>S3</td>
<td>S3</td>
</tr>
</tbody>
</table>

**Enterprise**

**Medical**

**Financial Services**

**Industrial**

**Other**
<table>
<thead>
<tr>
<th>PARTS</th>
<th>COMPOUND PARTS</th>
<th>FINAL GOODS ASSEMBLED</th>
<th>OPERATOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>S1</td>
<td>S1</td>
<td>S1</td>
</tr>
<tr>
<td>S2</td>
<td>S2</td>
<td>S2</td>
<td>S2</td>
</tr>
<tr>
<td>S3</td>
<td>S3</td>
<td>S3</td>
<td>S3</td>
</tr>
</tbody>
</table>

**Enterprise**
- Chris Robbins
- Velentium

**Medical**
- Chris Gates
- BoA

**Financial Services**
- Mike Powers
- DoD

**Industrial**
- Josh Corman
- PTC
Architect/Lead

Developers

PSIRT

Monitor NVD
Monitor News

?Coordinated Vulnerability Disclosure?

?Notify CERTs?

?Secure Coding?

New Parts Need

Build

Produce Bill of Materials
Test

Regulator Approval

Notify Regulator

Secure Requirements?

Security Training?
**Procurement**
- IT/Operations
- SoC/NoC/MSSP
- Monitor NVD
- Monitor News
- Monitor Supplier Alerts

**Evaluate SBoM**
- Select/Purchase/MSA Suppliers/Goods
- Seek Least Vulnerable version
- Factor Mitigations
- Test
- Go LIVE!

**Security/Risk**
- Ts & Cs Boilerplate
- RFP Definition
- Request SBoMs
- 20% off if none
- Prohibited Tech?
- Compare Hygiene

**IT/Operations**
- AM I affected?
- WHERE am I Affected?

**SoC/NoC/MSSP**
- Leverage SBoM
- Monitor NVD
- Monitor News
- Monitor Supplier Alerts
<table>
<thead>
<tr>
<th>PARTS</th>
<th>COMPOUND PARTS</th>
<th>FINAL GOODS ASSEMBLED</th>
<th>OPERATOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>S2</td>
<td>S3</td>
<td>S1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>S3</td>
</tr>
<tr>
<td>Chris Robbins</td>
<td>RedHat</td>
<td>Chris Gates</td>
<td>Mike Powers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Velentium</td>
<td>Christiana Health</td>
</tr>
<tr>
<td>Josh Corman</td>
<td></td>
<td></td>
<td>Sounil Yu</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>BoA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bob Martin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DoD</td>
</tr>
</tbody>
</table>

- Enterprise
- Medical
- Financial Services
- Industrial
- $Other
Overall thrust

<table>
<thead>
<tr>
<th>Crawl</th>
<th>Walk</th>
<th>Run</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn to what degree people are using SBoM &amp; friends</td>
<td>Learn <strong>how</strong> people are using SBoM:</td>
<td>Understand near misses: what could SBoM unlock if it met your use cases better?</td>
</tr>
<tr>
<td>Suss out common obstacles</td>
<td>- What works</td>
<td>Understand “rainbow scenarios”</td>
</tr>
<tr>
<td></td>
<td>- What doesn’t work</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- How has it helped or hindered?</td>
<td></td>
</tr>
</tbody>
</table>
Q: Are people using SBoM today?

A: In some industries, yes!

Less mature: healthcare end users, manufacturers w/ huge product catalogs

More mature: DoD, OS packaging, automotive, some medical device manufacturers

Doing their best: middle parts of the supply chain

“We need to know what we’re defending.” —healthcare end user interviewee
Common obstacles to SBoM use

Heavy vetting workload (e.g., Red Hat’s curation of packages)

Uncooperative or clueless vendors

Developer inertia (“this is QA’s problem”)

No way to ingest/manage SBoM even if we had it
How are people using SBoM concepts today?

In what forms?

- Listing of filesystem directories & files ("manifest" or text dump)
- Folder full of software manuals
- Tool outputs from executable/source analysis (Software Composition Analysis)

At what stages of the software supply chain?

- Manufacturer, compound parts assembler, final goods assembler, end user
- End users (except DoD) often have the least leverage
What could SBoM unlock for our interviewees?

Effective incident response via quick search
Richer asset records for inventory management
Tune security tools according to what systems say they’re running
Graceful phasing out of end-of-life/aging systems
SBoM as forcing function: vendors can streamline their own processes
Insights from interviews (n = ~7)

*Supplier selection* is **not** a universal use case for our interviewees. Typically, lack of an SBoM does not disqualify a vendor (except in DoD)

Vulnerability matching & vuln management is a major use case for end users

Ability to ingest/handle SBoMs decreases toward end of supply chain

Demand for features beyond SW name & version number is **low** among our interviewees (except DoD)

Frameworks (e.g., Java) are important to divulge, not just libraries/packages