BloSS@M: Security Assessment Automation with OSCAL

ITL/CSD/OSCAL Team
3rd OSCAL Workshop
Why do we need BloSS@M?

Agencies need

• to acquire software.
• allocate software licenses.
• securely operate and manage the software in their environment.
• understand the impact of that software on their environment.
What is BloSS@M?

A proof-of-concept software asset management system that:

• Enables upward aggregation, downward distribution, and sharing of software assets
• Proposes a mutual trust system where agencies deploy peer nodes in a multi-agency consortium
• Is built using Hyperledger Fabric’s permissioned blockchain
• Demonstrates security assessment automation & continuous ATO with OSCAL
Why DevSecOps?
How do Sec across Dev and Ops?

- Why do we secure first?
- How do we secure first?
- What do we secure first?

Source: Automation Support for Security Control Assessments (NIST IR 8011)
The Best SDLC: DevSecOps with OSCAL

[Diagram of the SDLC process with DevSecOps integration using OSCAL]
Prepare
## Implement

<table>
<thead>
<tr>
<th>Prepare</th>
<th>Category</th>
<th>Select</th>
<th>Implement</th>
<th>Assess</th>
<th>Authorize</th>
<th>Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>threat modeling</td>
<td>threat model</td>
<td>information types</td>
<td>categorize system</td>
<td>select impact level</td>
<td>(automate) test security &amp; privacy controls</td>
<td>begin assessment cycle</td>
</tr>
<tr>
<td>countermeasures</td>
<td>assets</td>
<td>categorize information types</td>
<td>define system capabilities</td>
<td>select security &amp; privacy controls</td>
<td>scope &amp; tailor system controls</td>
<td>implement &amp; document system</td>
</tr>
<tr>
<td>threats</td>
<td></td>
<td></td>
<td>prioritize capabilities</td>
<td>design system</td>
<td>complete assessment and draft report</td>
<td>examine system</td>
</tr>
</tbody>
</table>

**OSCAL**
- Profile
- Custom OSCAL Catalog
- System Security Plan
- Component Definitions

**OSCAL** Plans of Actions & Milestones
- Assessment Plan
- Assessment Results
Authorize
Contact Us
blossom@nist.gov

ITL/CSD/OSCAL Team
3rd OSCAL Workshop