Simplifying the World of Open Source Usage for Financial Institutions

James McLeod
Director of Community
FINOS

Jeff Crum
Senior Director of Product Marketing
WhiteSource
Traditional Solution Oriented Business Models

In traditional business models, value creation is linear and one-way.

- Production
- Distribution
- Marketing
- Consumer
Linear Development with Extended Lead Time

- OSS Consumption
- Development
- Integration Testing
- Quality Testing
- Security Testing

Testing Failure
DevOps Automation Reduces Development Cycles

[Diagram showing various tools and processes related to DevOps]

Real-Time Security Scanning Adds Sec to DevOps

GitHub

WhiteSource

GitHub

WhiteSource

Continuous Agile Delivery
FINOS Publishes New Responsible Disclosure Policy

Don’t Alert Bad Actors to New Open Source Vulnerabilities!

The new FINOS Responsible Disclosure policy provides guidance to teams when communicating New, Ongoing, Identified, Patched and Released vulnerabilities.

- Privately report issues to FINOS PMC
- Team works privately to resolve Issue
- New release made including issue fix
- Vulnerability announced only when safe

These steps stop bad actors from being alerted to new open source vulnerabilities.

The FINOS Responsible Disclosure policy is available for review on FINOS wiki.

https://finosfoundation.atlassian.net/wiki/spaces/FINOS/pages/1230176257/Security+vulnerabilities+responsible+disclosure
Implementing GitOps and Shifting Further Left

Git as the “Single Source of Truth” for Declarative Infrastructure and Applications

- Increased Productivity
- Enhanced Developer Experience
- Improved Stability

- Higher Reliability
- Consistency and Standardization
- Stronger Security Guarantees
Platforms Thrive in an Open ecosystem

In Platform business models
Value creation is two-way and continuous
So how can you shift left security successfully?
How left can you go?

Who owns it?

Shifting left the right tools
When is the optimal point to integrate security checks into the SDLC?
Detecting Issues as Early as Possible Has Multiple Benefits

The cost of fixing security and quality issues is rising significantly, as the development cycle advances.

<table>
<thead>
<tr>
<th>Coding</th>
<th>Build</th>
<th>QA &amp; Security</th>
<th>Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>$80/Defect</td>
<td>$240/Defect</td>
<td>$960/Defect</td>
<td>$7,600/Defect</td>
</tr>
</tbody>
</table>
66% of companies have already implemented application testing during or even pre-build stage.

In what stage of the SDLC do you spend most of your time implementing security measures?

- 36% Before build
- 30% Build
- 33% Post build
If the goal is to integrate security pre-build, then who should own application security in the organization?

72% of the respondents stated that the ownership over AppSec lies in the software development side.
Research shows organizations of all sizes are shifting their operational security to software development teams.

Who owns security in your organization, by company size?

- **DevOps**: 20% (751-1000), 19% (1001-5000), 19% (Over 5000)
- **Developers**: 27% (751-1000), 22% (1001-5000), 19% (Over 5000)
- **Team leaders on software development teams**: 28% (751-1000), 26% (1001-5000), 31% (Over 5000)
- **Security teams**: 25% (751-1000), 30% (1001-5000), 31% (Over 5000)
What are the “right” tools?

Both teams need security tools, but in order to shift left security you need to empower your developers.

**Governance solutions**
- Used by security teams and management to get full visibility and control over the security risks in their software.

**Developers tools**
- Used by developers to remediate vulnerabilities.
WhiteSource Complete Solution

Caters to security managers, DevOps professionals, and developers
WhiteSource Product Portfolio

WhiteSource for DEVELOPERS

WhiteSource CORE

PLAN ➔ CODE ➔ BUILD ➔ DEPLOY ➔ MAINT.
1. How left can you go?
2. Who owns it?
3. Shifting left the right tools