AGENDA

• Introductions / Background
• Creating an Open Source Strategy
• Challenges vs Best Practices
• Case Studies
• Tools & Resources
Hello, from FOSSA

Kevin Wang, CEO
Background
TODAY, SOFTWARE IS EATING THE WORLD

Over 80% of code in modern a software product is open source.

COMPANIES NO LONGER CONTROL THEIR CODE

CODE COMPLEXITY IN 2018

- Massive Bugs
- Deprecation Dependencies
- Security Breaches
- License Violations
HAVING AN OSS CONSUMPTION STRATEGY IS CRITICAL

“Over the next 10 years, the battles between incumbents and software-powered insurgents will be epic.”

Marc Andreessen,
Wall Street Journal, August 22, 2011

Open source is a critical supplier for software. Companies that excel at open source will excel at software.
INTRODUCING: THE OPEN SOURCE PROGRAMS OFFICE

“"A central open source program office is a designated place where open source is supported, nurtured, shared, explained, and grown inside a company.”"
WHAT IS AN OSPO?

Consumption
(today’s talk)

Contribution

Culture
**Open Source is a New Kind of Vendor**

<table>
<thead>
<tr>
<th></th>
<th>Traditional Vendor</th>
<th>Open Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scale</td>
<td>10s-100s</td>
<td>10,000s – 100,000s</td>
</tr>
<tr>
<td>Complexity</td>
<td>Singular</td>
<td>P2P Supply Chain - “Bubble up” effects</td>
</tr>
<tr>
<td>Control</td>
<td>Direct Relationship</td>
<td>Indirect - Inherited through tooling</td>
</tr>
</tbody>
</table>
ITERATIVELY MANAGE OSS CONSUMPTION

1. Scale  Tooling & automation
2. Complexity  Data-driven policy
3. Control  Enroll developer workflows
Challenges & Best Practices

Running a successful consumption strategy
1. **SCALE Tooling & automation**

### Common Challenges

- Handle chaotic and unpredictable OSS usage from tooling behavior
- Process 100,000+ components per day
- Apply different sensitivities from different teams, locales and distributions

### Best Practices

- Invest in tooling and quality initiatives
- Leverage CICD pipelines and DevOps integrations
- Ask development teams to “pin” versions to reduce intake drift
- Rely heavily on tooling, automated policies and analytics
2. COMPLEXITY  Data-driven policy

Common Challenges

• Sheer scale of policy decisions to prioritize

• OSS use is extremely context-dependent (teams, scope, usage)
  • Licensing p2p, usage
  • Vuln confirmation, bug impact
  • Ship target (dev, production, platform)

• Bubble-up code quality issues

Best Practices

• Collect tons of contextual data and build policy rules around interactions

• Use tooling to automate the majority of policy decisions

• Automate as much as possible, but NOT EVERYTHING
  • Clear escalation paths with built-in data
3. CONTROL Enroll developer workflows

Common Challenges

• OSS issues are sticky – they can be incredibly hard to resolve after they are introduced

• OSS use is nuanced, hard for non-technical employees to remediate

Best Practices

• “Shift-left”, enroll developers and their tooling early on

• Standardize your quality control automation (central CI/CD)

• Create strict automated policies for non-ambiguous cases, but avoid overly-prescriptive process beyond

• Pick tooling and workflow investments that prioritize high automation culture
Case Studies

Advice from various OSPO pioneers & FOSSA partners around Open Source Management
Be a service not a barrier

“Our OSPO’s slogan reminds us to take a helpful posture. Find balance. We’re not paralyzed by risk, we’re practical about addressing it. We don’t get in the way. We are always available to help with any open source issue.”

- Gil Yehuda, Open Source @ Oath / Yahoo

Oath’s OPSO is based on Yahoo’s long standing program, now merged with dozens of internet brands. The OSPO handles everything related to open source, including license review, scanning apps with FOSSA and contributing to hundreds of OSS projects.
Enabling collaboration for everyone, everywhere.

“Our mission is to enable, educate, champion, and foster open source development, adoption, and culture. We are enablers rather than gatekeepers. We value ideas over hierarchy and we do the right thing, period.” ~ Brian Hsieh, Open Source @ Uber
Channel the Zen of Compliance

Don’t Pursue Perfection
Enable Right Behaviors
Respect the License
Listen to the Community
Educate Not Dictate
Automate for Scale

+ Lean on partners and mentors
SUMMARY: Common Learnings

- View the OSPO's function as a facilitator / service provider
- Support the developer workflow; prefer education and collaboration and over quality gating and policy enforcement
- Pursue productivity over perfection – don’t get paralyzed by risk
- Create an open and collaborative culture to evangelize open source
Resources

Tooling & resources to help
TOOLING

FOSSA IS THE “OS” FOR YOUR OSPO

Tooling to build an open source strategy into a modern development workflow

SCAN
BUILD

ALERT
TEST

REPORT
DEPLOY
Key Tooling Requirements

A smart open source inventory with built-in continuous compliance and security

**LICENSING**
License scanning, policy enforcement and compliance documentation on autopilot

**SECURITY**
Realtime vulnerability remediation

**CODE QUALITY**
Dashboards and alerts on the health of your open source inventory
ADDITIONAL RESOURCES

• Participate in the Linux Foundation
• Visit & support the TODO Group’s resources (http://todogroup.org)
• Get involved in the community for OSS sustainability and funding
  • OpenCollective
  • https://medium.com/open-consensus
Learn more at:
http://ospo.io
https://ospo.io/
https://fossa.io/
@getfossa

We’re hiring!
https://fossa.io/careers
THANK YOU