Securing the Software Supply Chain: Transparency in the Age of the Software Driven Society

Chris Hughes
CISO & Co-Founder @ Aquia Inc.
Open Source Adoption – The **Good**

- Open Source expedites innovation
- Creates a robust community and ecosystem
- Enables cross-organizational collaboration
- Metrics:
  - 97% of organizations are using OSS
  - 77% of organizations have increased OSS use
  - 79% of organizations sponsor OSS organizations
  - Highest increases involve OSS DevOps and Cloud-native CI/CD Tools
Open Source Adoption – The **Bad**

- Experts estimate 60-80% of modern software is comprised of OSS (Linux Foundation)
- Software supply chain attacks on the rise
- Many projects supported by unpaid volunteers
- Incidents such as Log4j send organizations scrambling – lack of visibility at the component level
OSS Adoption – What To Do?

- Establishing a robust Cybersecurity Supply Chain Risk Management (C-SCRM) program is a great step forward.
- Engage with orgs such as OpenSSF, LinuxFoundation and others.
- Crowdsourcing is catching on.
- NIST 800-161r1 – Cyber Supply Chain Risk Management Practices for Systems and Organizations – Appendix F
  - Foundational, Sustaining and Enhancing Capabilities
  - SCA/SBOM/VEX, Centralized Hardened Internal Repos of OSS etc.
Timeline of Notable Federal Focus

- May 12th – Cyber EO served as the primary driver for enforcing Federal focus on SW Supply Chain – Specifically Section 4

- NIST has:
  - Held workshops on enhancing C-SCRM
  - Published new Secure Software Development Framework (SSDF)
  - Published C-SCRM Guidance 800-161 Rev1 (May 5th, 2022)
Published capabilities across levels of maturity

- **Foundational**
  - Utilize SSDF Protect/Response guidance
  - Ensure OS components are acquired via secure channels from trustworthy repos

- **Sustaining**
  - Utilize SCA on in-house codebases to look for vulnerable components
  - Create/maintain internal repos or libraries of known/good OSS components for developers to use

- **Enhancing**
  - Prioritize the use of more secure programming languages
  - Automate the pipeline of collecting, storing and scanning OSS components for internal repos prior to introduction to the dev environments

- **OMB Memo M-22-18 “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices”**
  - Agencies MUST obtain self-attestation to conformity with secure software development practices for all third-party software used by the agency (e.g. SSDF and NIST Cyber EO Software Supply Chain Guidance)
  - Agencies may determine a third-party assessment/3PAO is required
  - SBOM’s may be required by agencies in solicitation requirements (must be in formats as defined by NTIA)
CISA/NTIA SBOM Efforts

- Originated at NTIA and now moved over to CISA, along with Dr. Allan Friedman
- Held "SBOM-o-Rama" in late 2021
- SBOM Workstreams 2022
  - Cloud & Online Applications
  - On-Ramps & Adoption
  - Sharing & Exchanging
  - Tooling & Implementation
- Leading Formats
  - SWID
  - CycloneDX
  - SPDX
Notable Industry Efforts

• White House held Software Security Summit in early 2022

• 3 High Level Goals
  • Securing OSS Production
  • Improving Vulnerability Discovery & Remediation
  • Shorten Ecosystem Patching Response Time

• Key Focus Areas:
  • Developer Education/Certification
  • Digital Signatures
  • OpenSSF IR Team
  • SBOM Everywhere
  • Risk Assessment Dashboard – 10k OSS Projects
Guidance Galore

- NIST Secure Software Development Framework (SSDF)
- Supply Chain Levels for Software Artifacts (SLSA)
- NSA/CISA - Securing the Software Supply Chain for Developers
- OWASP Software Component Verification Standard (SCVS)
- Cloud Native Computing Foundation (CNCF) - Software Supply Chain Best Practices

Long story short, we have no shortage of guidance and emerging best-practices but we need to bridge the divide from theory to practice.

Many of the recommended best-practices and guidance also may be difficult particularly for SMB’s to meet, further consolidating access to innovative SMB's and technologies for the Federal Government.
CI/CD Pipelines – The Good

- CI/CD ADOPTION HAS CHANGED THE WAY DEVELOPERS DELIVER SOFTWARE
- HAS ENABLED SECURITY TOOLING AUTOMATION AND INTEGRATION – E.G. "SHIFTING SECURITY LEFT"
- ENABLES ROBUST TOOLCHAINS TO ACHIEVE FULL CI/CD CAPABILITIES AND SECURITY REQUIREMENTS
Many organizations haven’t adopted unified CI platforms, leading to a myriad of integrations and complexity.

While the Pipeline(s) facilitate secure delivery, they are part of your attack surface – organizations must address this.

A compromise of the pipeline leads to massive supply chain security concerns and cascading impacts.

Malicious actors are even compromising signing systems and releasing signed malicious payloads.
CI/CD Pipelines – What to do

• Your CI/CD pipeline enables value delivery but also can be a threat vector
• Cider Security has released excellent CI/CD Risk Lists and Best Practices
• Threat Model/Adversary Emulation
• Supply chain Levels for Software Artifacts (SLSA) - security framework
  • Prevent tampering
  • Improve Integrity
  • Secure Packages
Kubernetes & Containers – Don't Neglect Security

- Palo Alto's Unit 42 discovered 99% of Kubernetes Helm charts in Artifact Hub have insecure configurations.
- Public Container Registries such as Docker Hub, Quay and Google Container Registry containers include critical findings in up to 91% of images.

Recommendations:
- Utilize Container/Manifest Scanning
- Pre-Hardened Images
- Image Signing/Hashing
- Leverage Guidance such as CIS, CNCF, DoD Container Hardening Guide and Kubernetes STIG
- Scan Containers throughout lifecycle
- Update IR Plans and Playbooks to account for Kubernetes and Containers
- These insecure configurations and vulnerabilities exist in IaC too
Kubernetes & Containers

• Kubernetes and Containers are closely linked with Cloud-native architecture and DevSecOps Adoption
• Up to 75% of global organizations have adopted Containers
• Kubernetes is the de-facto Container Orchestration tool of choice
• Reduced development timelines, cost optimization and improved scalability
SaaS Security - The overlooked Software Supply Source

- Organizations are increasingly consuming applications and software in the form of SaaS
- Large enterprises are consuming upwards of 200~ SaaS applications, adding up to 10 new SaaS apps a month
- IT/Security control roughly 20% of SaaS usage
- SaaS consumers should implement SaaS Governance/Security, including SBOM's
- Recent Twilio incident involved 130 other SaaS providers