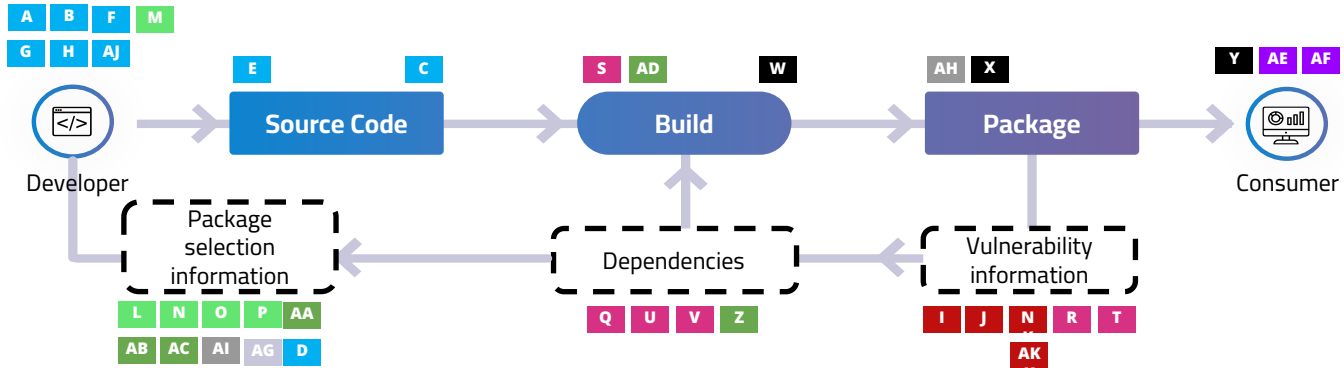


How OpenSSF Projects & SIGs Work Together (“CI/CD View”)



Best Practices WG

- A. **Secure Software Development Fundamentals courses** SIG
- B. **Security Knowledge Framework (SKF)** project
- C. **OpenSSF Best Practices Badge** project
- D. **OpenSSF Scorecard** project
- E. **Great MFA distribution** SIG
- F. **Common Requirements Enumeration (CRE)** project
- G. **Concise & Best Practices Guides** SIGs
- H. **Education** SIG - Mob. Plan
- AJ. **Memory Safety** SIG - Mob. Plan

Vulnerability Disclosures WG

- I. **CVD Guides** SIGs
- J. **OSS-SIRT** SIG - Mob. Plan
- K. **Open Source Vuln Schema (OSV)** project
- AK. **OpenVEX** SIG
- AL. **Vuln Autofix** SIG

Identifying Security Threats WG

- L. **Alpha & Omega** project
- M. **Office Hours** SIG
- N. **Security Insights**
- O. **Security-Metrics: Risk Dashboard** project - Mob. Plan
- P. **Security Reviews** project

Security Tooling WG

- Q. **SBOM Everywhere** SIG - Mob. Plan
- R. **False-Positive Suppression Spec** SIG
- S. [**Guide to Security Tools** SIG]
- T. [**cve-benchmark** SIG]
- U. **OSS Fuzzing** SIG
- V. **DAST scanning & web app**

End Users WG

- AE. **Supply Chain Attack taxonomy** SIG
- AF. **Supply Chain Attack RefArch** SIG

Supply Chain Integrity WG

- W. **Supply-chain Levels for Software Artifacts (SLSA)** SIG
- X. **Factory for Repeatable Secure Creation of Artifacts (FRSCA)** SIG
- Y. **Secure Supply Chain Consumption Framework (S2C2F)** SIG

Securing Software Repositories WG

- AG. **Survey of OSS Repos** SIG

Securing Critical Projects WG

- Z. **List of Critical Open Source Projects, components, & Frameworks** SIG
- AA. **criticality_score** project
- AB. **Harvard study** SIG
- AC. **package-feeds / package-analysis** project
- AD. **allstar** project

Associated Projects

- AH. **sigstore**
- AI. **Core Toolchain Infrastructure (CTI) support**