

Working Groups, Projects, & SIGs

1. INFORM

Vulnerability Disclosures

Efficient vulnerability reporting and remediation

- I. [CVD Guides](#) SIGs
- J. [OSS-SIRT](#) SIG
- K. [Open Source Vuln Schema \(OSV\)](#) project
- L. [OpenVEX](#) SIG
- M. [Vuln Autofix](#) SIG



Identifying Security Threats

Security metrics/reviews for open source projects

- N. [Security Insights](#) project
- O. [Security-Metrics: Risk Dashboard](#) project
- P. [Security Reviews](#) project
- [Security Insights Spec](#) project

Securing Critical Projects

Identification of critical open source projects

- U. [List of Critical OS Prj. components, & Frameworks](#) SIG
- V. [criticality_score](#) project
- W. [Harvard study](#) SIG
- X. [Package Analysis](#) project
- Y. [allstar](#) project

2. EQUIP

Best Practices

Identification, awareness, and education of security best practices

- A. [Secure Software Development Fundamentals courses](#) SIG
- B. [Security Knowledge Framework \(SKF\)](#) project
- C. [OpenSSF Best Practices Badge](#) project
- D. [OpenSSF Scorecard](#) project
- E. [Common Requirements Enumeration \(CRE\)](#) project
- F. [Concise & Best Practices Guides](#) SIGs
- G. [Education](#) SIG
- H. [Memory Safety](#) SIG
- [The Security Toolbelt](#) SIG

Security Tooling

State of the art security tools

- Q. [SBOM Everywhere](#) SIG
- R. [OSS Fuzzing](#) SIG
- [SBOMit](#) project

Supply Chain Integrity

Ensuring the provenance of open source code

- S. [Supply-chain Levels for Software Artifacts \(SLSA\)](#) SIG
- T. [Secure Supply Chain Consumpt Framework \(S2C2F\)](#) SIG
- [Gittuf](#) project

AI/ML Security

AI/ML Security at the Intersection of Artificial Intelligence and Cybersecurity

DevRel

Develop Use Cases and help others learn about security

3. ENGAGE

End Users

Voice of public & private sector orgs that primarily consume open source

- Z. [Supply Chain Attack taxonomy](#) SIG
- AA. [Supply Chain Attack RefArch](#) SIG

Securing Software Repositories

collaboration between repository operators

- AB. [Survey of OSS Repos](#) SIG
- AC. [Repository as a Service](#) Project



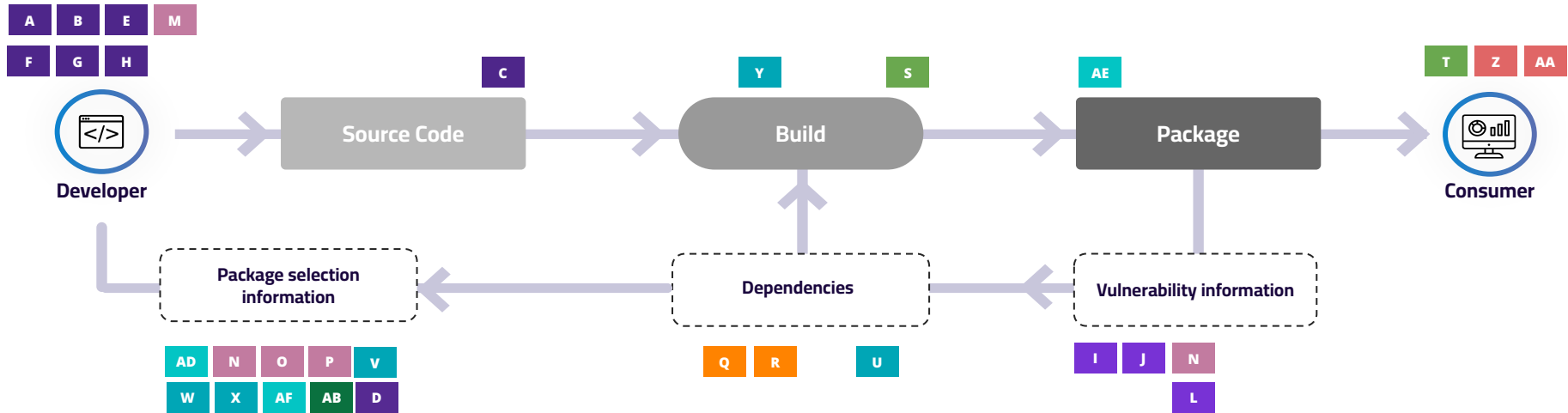
Projects

Category-leading software initiatives

- AD. [Alpha-Omega](#)
- AE. [Sigstore](#)
- AF. [Core Toolchain Infrastructure \(CTI\)](#)



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. [Common Requirements Enumeration \(CRE\)](#) project
- F. [Concise & Best Practices Guides](#) SIGs
- G. [Education](#) SIG
- H. [Memory Safety](#) SIG

Vulnerability Disclosures WG

- I. [CVD Guides](#) SIGs
- J. [OSS-SIRT](#) SIG
- K. [Open Source Vuln Schema \(OSV\)](#) project
- L. [OpenVEX](#) SIG
- M. [Vuln Autofix](#) SIG

Identifying Security Threats WG

- N. [Security Insights](#)
- O. [Security-Metrics: Risk Dashboard](#) project
- P. [Security Reviews](#) project

Security Tooling WG

- Q. [SBOM Everywhere](#) SIG
- R. [OSS Fuzzing](#) SIG

Supply Chain Integrity WG

- S. [Supply-chain Levels for Software Artifacts \(SLSA\)](#) SIG
- T. [Secure Supply Chain Consumption Framework \(S2C2F\)](#) SIG

AI/ML Security

Securing Critical Projects WG

- U. [List of Critical Open Source Projects, components, & Frameworks](#) SIG
- V. [criticality score](#) project
- W. [Harvard study](#) SIG
- X. [Package Analysis](#) project
- Y. [allstar](#) project

End Users WG

- Z. [Supply Chain Attack Taxonomy](#) SIG
- AA. [Supply Chain Attack RefArch](#) SIG

Securing Software Repositories WG

- AB. [Survey of OSS Repos](#) SIG
- AC. [Repository as a Service](#) Project

Associated Projects

- AD. [Alpha & Omega](#) project
- AE. [Sigstore](#)
- AF. [Core Toolchain Infrastructure \(CTI\)](#) support