

OpenSSF Structure

Governing Board (GB)

Committees

Marketing

Public Policy

Budget & Finance

Governance

Technical Advisory Council (TAC)

Working Groups

End Users WG

Vulnerability Disclosures WG

Best Practices WG

Securing Critical Projects WG

Security Tooling WG

Identifying Security Threats WG

Supply Chain Integrity WG

Securing Software Repositories WG

AI/ML Security

DevRel Community

Diversity, Equity, & Inclusion

Associated Projects

Alpha-Omega

Sigstore

Core Toolchain
Infrastructure (CTI)

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



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

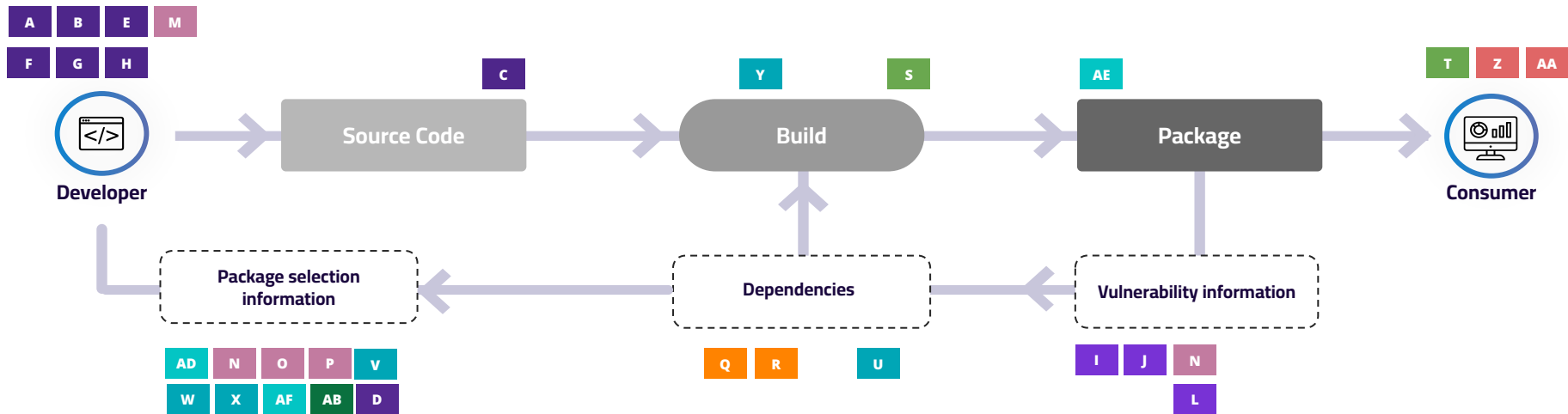
Projects

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

- 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

- 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

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

DevRel Community

Security Tooling

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

Supply Chain Integrity

- S. [Supply-chain Levels for Software Artifacts \(SLSA\)](#) SIG
- T. [Secure Supply Chain Consumption Framework \(S2C2E\)](#) SIG

AI/ML Security

Securing Critical Projects

- 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

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

Securing Software Repositories

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

Diversity, Equity, & Inclusion

Associated Projects

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