Working Groups, Projects, & SIGs

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. 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

Efficient vulnerability reporting and remediation

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

End Users WG

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

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

Identifying Security Threats

Security metrics/reviews for open source projects

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

Security Tooling

State of the art security tools

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**

Securing Software Repositories

collaboration between repository operators

AG. **Survey of OSS Repos** SIG
AM. **Repository as a Service** Project

Supply Chain Integrity

Ensuring the provenance of open source code

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
AI. SCI Positioning SIG

Securing Critical Projects

Identification of critical open source projects

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

Projects

L. Alpha-Omega
Core Toolchain Infrastructure (CTI) support
AH. Sigstore