OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Secure Open Source Software Vision Brief 2025

openssf.org

The Open Source Security Foundation (OpenSSF), an initiative of the Linux Foundation, was formed in 2020 as a cross-industry forum to collaboratively improve open source software (OSS) security. Many vulnerabilities have been found in closed source software. However, incidents such as the Log4Shell vulnerability in the OSS component log4j, and the attempted subversion of xz utils, have made many organizations realize how dependent they have also become on the security of OSS. This has led to an increased focus on the need to further improve OSS security.

Turning ideas into action has faced headwinds given socio-economic realities facing the open source community, which often includes maintainers and contributors working outside their day-to-day to create OSS for the greater public good.

The OpenSSF has gained momentum toward improving OSS security (e.g., building off the activities outlined in our Annual Report December 2024). Our accomplishments in 2024 include:

1. **Public Sector Engagement.** Throughout 2024, OpenSSF has been actively engaging with the public sector in the United States and Europe. Here's a snapshot of some of our accomplishments:
    - **United States.** OpenSSF submitted a formal response to the Request For Information (RFI) on Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software issued by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), as well as participating in the CISA Open Source Software (OSS) Security Summit.
    - OpenSSF worked with CISA to develop and foster adoption of the Principles for Package Repository Security. Many repositories have begun implementing its recommendations.
    - OpenSSF is actively supporting the Artificial Intelligence Cyber Challenge (AIxCC) from DARPA and ARPA-H, a competition to develop tools to find and fix vulnerabilities, then release those tools as open source software. We've advised on how to proceed, helped OSS projects understand the competition, and publicly explained how OSS can be a powerful support for technology transition.
    - OpenSSF, in collaboration with CISA and the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), launched protobom, an OSS supply chain tool to read and generate Software Bill of Materials (SBOMs) and file data, as well as translate this data across standard industry SBOM formats.
    - **Europe. Events and Workshops.** In March 2024, OpenSSF successfully hosted the EU Policy Summit in Brussels, strengthening its presence and initiating collaborations on the Cyber Resilience Act (CRA) with EU institutions and member states. Since then, OpenSSF has actively participated in a variety of events, establishing itself as a key player in Brussels for European standardization and open source cooperation. Additionally, the OpenSSF sponsored the FSFE Youth Hackathon, introducing the OpenSSF to emerging talent in the developer community.
    - **Consultations.** OpenSSF contributed to the public consultation for the NIS2 Implementing Act, collaborating in a joint response to highlight differing perspectives between NIS2 and the CRA on open source and its suppliers, aiming to mitigate impacts on the open source ecosystem. This led to follow-up meetings with the European Commission, providing insights for future CRA-related work.

- **OpenSSF and Standardization.** OpenSSF is deeply involved in the Linux Foundation work-streams for the CRA implementation. As one of the most technical foundations active in Brussels, OpenSSF contributes tools, guidance, and collaboration to support technical discussions. OpenSSF also cooperates with Linux Foundation Research on CRA compliance and plans a dedicated CRA workshop with Linux Foundation Europe.
- **Collaboration with other Stakeholders.** OpenSSF's work in Brussels primarily involves regulatory stakeholders in CRA discussions and members of the OpenSSF, as well as broader stakeholders less engaged with other open source groups. Known for technical expertise and practical contributions, OpenSSF facilitates knowledge sharing beyond CRA implementation, bringing a true global perspective on cybersecurity regulation. OpenSSF was accepted to join the European Commission's expert group on the CRA, among 170 organizations.
- **Challenges.** Two main challenges surround CRA engagement: First, coordinating discussions between the appropriate stakeholders for practical outcomes; second, strengthening European membership and community outreach. OpenSSF's influence is growing, but targeted media and outreach strategies are needed to build a robust European audience and member base along with our partners within the Linux Foundation Europe.

2. **OpenSSF Events.** In 2024, the OpenSSF Community Day program expanded to India, adding to its annual conferences in North America, Europe, and Japan. OpenSSF also hosted its inaugural European Policy Summit in Brussels, with plans underway for the upcoming U.S. Policy Summit. These events allow us to engage the passionate local communities, providing access to our large community of cybersecurity experts.

   A popular addition to these Community Days has been the facilitation of cybersecurity tabletop exercises for the community. These mock incidents have helped raise awareness and preparedness of projects and maintainers before they experience an actual incident.

3. **Software Security Education.** In 2024, OpenSSF added more labs in our course on the fundamentals of Developing Secure Software (LFD121) improving its hands-on and in-depth learning. These additions resulted in over 9,300 new developers enrolling in the course with over 29,000 enrollments for all time (all platforms and natural languages). The following courses were added to the education portfolio as well:
   - » Securing Your Software Supply Chain with Sigstore (LFS182)
   - » Securing Projects with OpenSSF Scorecard (LFEL1006)
4. **Security Guides.** Knowledge sharing around development and supply chain security best practices are a cornerstone of much of the foundation's work. Our members have collaborated on developing and improving various guides over the years. These guides help developers, consumers, and the security community to help improve security:
   - » Concise Guide for Developing More Secure Software
   - » Concise Guide for Evaluating Open Source Software
   - » Principles for Package Repository Security
   - » Correctly Using Regular Expressions for Secure Input Validation
   - » Compiler Options Hardening Guide for C and C++
   - » Source Code Management (SCM) Platform Configuration Best Practices
   - » Secure Coding One Stop Shop for Python
   - » Trusted Publishers for All Package Repositories
5. **OSS Security Evaluation.** Simplified obtaining security information about OSS so consumers and maintainers can more efficiently assess OSS security:
   - » **OpenSSF Scorecard.** Automatically assesses OSS projects against various software security criteria. A score is produced that helps OSS consumers estimate the security of the OSS and helps OSS maintainers by giving them a pathway to improve their project's security posture. Allstar is a complementary effort that helps streamline using the Scorecard within a developing organization or project. Scorecard supports GitHub and GitLab and runs a weekly Scorecard scan of over one million OSS projects.

   - » **OpenSSF Best Practices Badge.** Security and sustainment criteria that OSS projects can use to more deeply evaluate their efforts and also help OSS consumers understand their status. For example, requiring at least one developer to know how to design secure software and counter common vulnerabilities, and as significant new functionality is added, the developer must add tests to an automated test suite. We have over 7,900 participating projects.

   - » **Supply-chain Levels for Software Artifacts (SLSA).** SLSA is a framework defining criteria to prevent tampering, improve integrity, and secure packages and infrastructure. SLSA version 1.0 was released in April 2023, focusing on protecting build processes. SLSA was subsequently adopted by npm for package integrity.

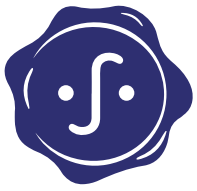
» **Graph for Understanding Artifact Composition (GUAC).** GUAC is a tool that ingests SBOM, vulnerability, attestations, and other metadata about software dependencies within software supply chains. GUAC helps software consumers quickly make sense of the high volumes of metadata about the software they are using so they can make more effective risk-based decisions.

» **Security Baseline.** Based on global cybersecurity frameworks and regulations, the Security Baseline provides a set of criteria in development that both producers and consumers of open source software can leverage to improve the security of their projects and operations.

» **Security Reviews Collection.** We have collected a set of known security evaluations of OSS, enabling others to find and review this information quickly.

6. **Improved OSS Infrastructure & Tooling.** Improving infrastructure and tooling has a broad impact on improving security.

» **sigstore.** Digital signatures help verify software authenticity and counter malicious package attacks. However, past solutions were often impractical for open source. Sigstore, a free digital signing and verification service, addresses this challenge and has seen broad adoption since its General Availability (GA) release in October 2022. It is now used by npm for SLSA provenance, GitHub Artifact Attestations for workflow-run provenance, and Homebrew, which signs and verifies all bottles in homebrew-core (funded by Alpha-Omega). PyPI has adopted PEP 740 for Sigstore-signed attestations, Maven Central supports Sigstore signature bundles, and PEP 761 proposes replacing PGP signatures on CPython releases with Sigstore. Sigstore's transparency log now holds over 170 million signatures across 17,000+ OSS projects, including Kubernetes, CPython, and LLVM. A free course is available for learning how to use Sigstore.



» **Secured Software Repositories.** Secured Software Repositories. Since many OSS packages are acquired through repositories, we are working with repositories to improve their security. We co-published the Principles for Package Repository Security with CISA to help open source package repositories develop security roadmaps. Significant progress has been made on RSTUF, which has evolved from an experimental system to an MVP release suitable for production deployment, aimed at protecting package repository indices. Additionally, we published Trusted Publishers for All Package Repositories, an implementation guide to enhance secret management in building pipelines across platforms. The Principles of Package Repository Security document inspired CISA to host the Open Source Software Security Summit.

» **Better Tooling.** OpenSSF released Fuzz Introspector to improve fuzz testing and fuzz testing tools to enable detecting vulnerabilities before attackers find them.

7. **Vulnerability Finding and Reporting**

» **Alpha-Omega.** This is a significant effort, with $12.5M in corporate sponsorship, to partner with OSS maintainers to systematically find and fix undiscovered vulnerabilities and improve their overall processes. Current partners include the Python Software Foundation (e.g., funding a Python security developer-in-residence), the OpenJS Foundation and jQuery, the Eclipse Foundation, Node.js, and the Rust Foundation. All of these partners manage important, widely-used OSS, so the security improvements we implement together will substantially improve security for all.

» **Security Audits.** We've supported in-depth security audits of some widely used OSS, often via Alpha-Omega, including Eclipse Equinox P2 (a widely used provisioning platform), sigstore, Jackson-Core and Jackson-Databind, slf4j (a logging framework), and Symfony (a widely used PHP framework).

» **Open Source Vulnerability (OSV) Schema.** OSV is a machine-readable format that precisely maps vulnerabilities to open source package versions or commit hashes. OSV enables rapid automatic identification of vulnerable components so projects and organizations can update those components. OSV supports many ecosystems today, some including Rust, Go, Python, Java, JavaScript, C#, PHP, Ruby, AlmaLinux, Rocky Linux, and the Haskell programming language, with a total of 30 ecosystems today.

8. **Research**

» OpenSSF has overseen research such as the Census III of Free and Open Source Software — Application Libraries to identify the most widely-used OSS application libraries and the Secure Software Development Education 2024 Survey. This built on previous work such as our survey on Addressing Cybersecurity Challenges in Open Source Software.

9. **Community Building & Outreach**

» We have held formal OpenSSF Community Days in North America, Europe, India, and Japan, as well as local meetups across the globe to promote the use of OpenSSF resources. Several OpenSSF initiatives have been featured in industry conferences (e.g., GUAC featured at KubeCon North America 2024) highlighting the benefits of our projects and how open source projects can integrate our materials. We've held workshops at our assorted events to help increase awareness and contributions to our SLSA secure supply chain specification and the OpenSSF Scorecard tool that helps users understand the security qualities of the OSS software they use and depend upon every day.

OpenSSF Plans and Potential Partnership

We believe there are many opportunities to collaborate, both on work we intend to do and on possible new work. Collaboration could help the U.S. government to accelerate open source software security initiatives, avoid duplication of efforts (eliminating waste and strengthening results by pooling resources), and enable both the U.S. Government and industry to be seen as partners working together to solve critical issues.

The OpenSSF Intends to do the Following:

1. **OSS Security Education.** We are working with Linux Foundation Education to expand OpenSSF's education portfolio with future courses in active development including the Security for Managers of Software Developers (LFD125) and Understanding the European Union (EU) Cyber Resilience Act (CRA) (LFEL1001) as well an intermediate course on security architecture. The OpenSSF also has partnered with the Linux Foundation Education team in the development of a Global IT cybersecurity skills matrix. This framework will provide practitioners a simple means to understand the common expectations for skills and experiences needed at varying levels in their careers. This skills framework complements more formal methodologies like the NIST NICE framework (who has also been involved in the review of the framework).
2. **Security Guides.** OpenSSF will continue to identify opportunities for developing best practices guides to ease the use of frameworks and international standards that drive development and adoption of secure-by-design and secure-by default technology.
3. **Improved OSS Security Evaluation.** These should help assess the security posture of software and provide methods for more secure-by design and secure-by-default technology.

- **Supply Chain Integrity.** We intend to evolve our existing frameworks SLSA and S2C2F to cover a greater range of functional concerns, enabling open source consumers to more thoroughly assess upstream threats and better manage supply chain risks across their dependency portfolio.
- **Graph for Understanding Artifact Composition.** GUAC is a tool that analyzes metadata around software dependency artifacts such as SBOM and vulnerability reports to provide software consumers more actionable intelligence on the open source software they use everyday.
- **OpenSSF Scorecard.** We plan to improve the detection of security tools and processes and allow customization per policy through the structured results (probes) and maintainer annotations features.
- **OpenSSF Security Baseline.** The Security Baseline is a set of standards-based criteria that open source projects can implement and that downstream consumers can look to for higher degrees of security assurance. Baseline works with many of the OpenSSF's tools such as Scorecard, Best Practices Badges, Security Insights, Minder, SLSA, GUAC, and others.

4. **Improved OSS Infrastructure and Tooling**

- **Improved Integrated Tooling.** Simplified software bill of materials (SBOMs) generation and use for OSS is needed to advance wide-scale adoption and mitigate the risk of unsupported software. The protobom and bomctl projects simplify SBOM creation and portability, and the OpenSSF has a library of existing tools and processes that help generate, translate, and evaluate SBOMs throughout all phases of the lifecycle of the software. The group plans on collaborating on a reference architecture and patterns for implementation to assist upstream projects create useful manifests and allow downstream consumers ingest, interpret, and evaluate these documents.
- **Increase Memory Safety.** Our Memory Safety group will encourage critical OSS projects to move to memory-safe-by-default languages. Where it's not possible or practical, we'll encourage projects to reduce memory safety vulnerabilities.
- **Secured Software Repositories.** Several efforts are underway to improve security for package manager ecosystems including work on PyPI, NuGet, PHP Composer, and Rust Crates. We intend to evaluate more opportunities for expanding security capabilities.

5. **Vulnerability Finding and Reporting.** These align with "coordinated vulnerability disclosure."

- **Open Source Software Security Incident Response Team (OSS-SIRT).** OSS-SIRT is a proposed process and coordinated cross-industry expert group that will be available to help OSS maintainers remediate high-impact security vulnerabilities and related security emergencies. This proposal is another example of our strong partnership with Alpha-Omega.
- **Tabletop Exercises.** We will continue to host the hands-on simulations where participants navigate a fictional vulnerability outbreak, and provide guidance for teams that would like to create their own exercise.

- **Vulnerability Sharing Mailing Lists.** We plan to improve the OpenWall mailing list infrastructure, widely used for OSS vulnerability coordination and continue to promote threat intelligence sharing list, known as Siren, where community members can share threats, indicators of compromise, and discuss suspicious activity they observe within their projects.
- **OpenVEX.** OpenVEX is a specification for vulnerability exchange (VEX) data. It implements the Cybersecurity and Infrastructure Security Agency (CISA) Minimum Elements for VEX. We expect to update its specification and its vexctl tooling. We are working on guidance for security scanner vendors to effectively ingest VEX documents leveraging OpenVEX and any other VEX statements.
- **Vulnerability Disclosures Working Group.** The Vulnerability Disclosure Working Group curates several Coordinated Vulnerability Disclosure (CVD) guides for upstream maintainers as well as security researchers to best interact with upstream projects. The group curates other associated collateral such as a guide for open source projects to become a CNA (CVE Numbering Authority).

6. **Artificial Intelligence/Machine Learning (AI/ML) Security.** DARPA's two-year Artificial Intelligence Cyber Challenge (AIxCC) competition, designed to develop systems to find and fix vulnerabilities in OSS, concludes with the Finals in August. OpenSSF is a competition collaborator to assist in the technology transfer from research to release as OSS projects, helping to secure critical infrastructure. More broadly, OpenSSF is developing an approach to collaborate with the LF AI & Data foundation to establish guidance on AI/ML, so AI/ML will improve (instead of reduce) OSS security.
7. **Research.** We will continue to collaborate with Linux Foundation Research with two studies targeted to publish early in the year to help inform 2025 activities. The CRA Readiness Survey will be a catalyst in galvanizing OpenSSF programming, and the CRA Best Practices report will examine ways certain projects are closing the gap to comply with the CRA.
8. **Community Building and Outreach.** OpenSSF is continually engaging with and expanding the amazing community of people we collaborate with in our shared mission of improving the security of open source software for everyone. A few specific actions we have taken over the recent months include:
   - Through our engagement with two DARPA programs, AIxCC and E-BOSS, we have brought AIxCC competition organizers into our Fuzzing Collaboration Special Interest Group and research teams from the E-BOSS program into our Security Tooling Working Group.
   - Developing a mentorship program to help bring students and career-changers into the world of open source software development and cybersecurity.
   - We're holding a community workshop to discuss synergies and collaboration for the many open source SBOM tools that exist both within and outside of our foundation.
   - Our long-standing collaboration with entities like the Alpha-Omega project and other open source stewards and foundations has helped expand the reach of our collective body of work and made real-world impacts to security for our communities. The 2024 Alpha-Omega report summarizes recent accomplishments.

» Internationally, the OpenSSF and the Linux Foundation has made great inroads to include additional open source communities. We're actively working in India, Japan, Korea, and other countries to bring the body of knowledge and tooling created and maintained by our community.

» Speaking of global public policy, the OpenSSF has held policy summits, bringing together industry, regulators, and public policy experts in both Washington DC (2023), Brussels (2024), and plans to expand this collaboration to such areas as Japan and Korea as cybersecurity becomes a matter of global concern.

9. **Looking Forward**

» Cybersecurity is a team sport that is constantly evolving. We are invested in evolution and keeping an eye on the horizon of technology and adapting as new technology arises or new solutions arise to solve the many challenges of open source developers, consumers, and governments. In the coming year, the OpenSSF will be exploring new or improved work in the following areas:

» Our AI/ML working group continues to discuss the security challenges that exist in this still emerging field. The group plans to develop a reference architecture around implementing DevSecOps practices within AI/ML/LLM/generative AI and work to raise awareness in these communities to get security best practices baked into the development of these critical new technologies.

» Building upon the standards-based criteria that shapes our Security Baseline, the group plans on collaborating with other communities and developing a means of crafting machine-readable attestations and collecting evidence of security practitioners so that downstream communities can be assured of the practices used in their upstream sources.

» One of our core capabilities is providing an open, transparent, and neutral forum for our members and the community to collaborate together on specifications that could one day graduate into internationally-recognized standards. These efforts are crucial to help align desired security outcomes across the ecosystem. The OpenSSF and the broader Linux Foundation will be working on helping shepherd several of our community's specifications along the path to become recognized standards and best practices. Frameworks such as OpenChain, SLSA, OpenVEX, the Open Source Vulnerability schema, and the Security Baseline are in consideration for this process.

» Security frameworks like NIST SP 800-53, the Cyber Security Framework, and NIST SP800-218 (the Secure Software Development Framework) are key factors in helping shape how enterprises develop, ingest, and deploy software. The Security Baseline brings these assorted frameworks and regulations together to highlight where security activities are applicable. The Baseline will be proposed as the standard for all Linux Foundation projects to adopt to showcase where security activities can assist downstream consumers in understanding and justifying their own programs using open source tools.

» As part of our efforts to help educate and prepare our members and the community for emerging regulations, the OpenSSF's Global Cyber Policy working group will be creating a series of educational courses centered around global regulations and cybersecurity frameworks. The first of these offerings should be available later this year in the form of our "CRA 101" instructional course that explains the elements of that law and key capabilities that stakeholders will need to develop in order to assert compliance as that law goes into effect in 2027. This will be the first of many such educational efforts to help prepare both open source developers and open source consumers.

» In partnership with the Cloud Native Computing Foundation (CNCF), the OpenSSF will be rolling out an Academic Accreditation program, where colleges and universities can apply to be credentialed to teach cloud and security coursework determined and curated by industry professionals to help students learn skills to meet the needs of the modern workforce.

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

openssf.org