OpenSSF

OPEN SOURCE SECURITY FOUNDATION

2024 Annual Report

openssf.org

Contents

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2024 By The Numbers

2,239
technical contributors
across all OpenSSF Projects

8 Working Groups 37 Technical Initiatives

126 Members from 15 regions and 19 unique industries, surpassing our goal of a 10% increase in general membership with a current rise of 15%.

The OpenSSF Best Practices Badge has 7,680 participating projects, with 1,544 earning at least a passing badge.

OpenSSF helps developers to develop secure software:

Over 8,200 enrolled in LFD121 this year, with over 20,000 LFD121 enrollments for all time

(over 28,000 when also including LF104x and their Japanese translations)

With 22 regular contributors, Sigstore has seen a 289.06% increase in commits since 2023

62,618 unique GitHub projects were using Sigstore to sign artifacts and attestations; 144 Million Signatures were logged post general availability (GA)

Allstar now secures 42,361 repositories across over 500 installations on various organizations and user accounts.

OpenSSF Scorecard: Released v5.0.0, featuring Structured Results and Maintainer Annotations. This expands the existing 18 checks into 47 probes providing enhanced granularity and customization.

Boasts 7.6k installs of scorecard-action and 3.4k repositories displaying OpenSSF Scorecard badges in their READMEs.

Malicious Packages: Ingests 25,000 data points to search for malicious packages, including approximately:

- 15K npm packages
- 8K pypi packages
- 1K rubygems
- 1K nuget packages

Alpha-Omega

Awarded 25 grants totaling $5M in 2024 and over $9M to 15+ open source projects since its founding

From the General Manager

Dear OpenSSF Community,

As we wrap up this year, I want to take a moment to acknowledge the significant accomplishments of the OpenSSF community. It has been a year of progress and collaboration, and I deeply appreciate the commitment each of you, our community members, brings to the crucial mission of securing open source software. As governments around the world step up their regulatory efforts, it is our collective response that will carry the day and help developers worldwide secure the software supply chain.

Collaborating with our Governing Board, Working Group members, and Project Leads has shown me the strength of our collective efforts. Our initiatives demonstrate what we can achieve by uniting our diverse talents and perspectives. Each contribution enriches our community and reinforces our goals.

This year, our membership has grown to 126 members across 15 countries, reflecting our expanding global reach and the increasing impact of our work. It's inspiring to see such a diverse array of organizations coming together to champion secure software practices. In education, 12,000 individuals have engaged with our OpenSSF training courses, highlighting the demand for secure software education. Our projects have grown to 14 in number, with an additional 24 technical initiatives underway. The community at large has grown its contributor base by 28%. Perhaps most importantly, our projects have made a real impact on developers by reducing the complexity of SBOM creation and portability (protobom, bomctl) and providing tools to ensure secure practices are easily adopted (Minder). Over 7,500 projects have adopted our best practices, including the Linux Kernel, Kubernetes, Zephyr, CIP, and node.js.

The conversations we've had—within our teams, with public sector partners, and among community members—have provided invaluable insights for shaping our future. I'm particularly excited about our involvement in the Artificial Intelligence Cybersecurity Challenge (AIxCC) with DARPA, where we are developing tools to address vulnerabilities in open source projects.

Looking ahead, I'm optimistic about the opportunities before us. Our work is vital, and together we can make open source and the world more secure. Thank you for your dedication to OpenSSF. I look forward to seeing what we will achieve together in the coming year.

Best regards,
Todd Moore
Interim General Manager of OpenSSF, SVP of The Linux Foundation Operations

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

About the OpenSSF

OpenSSF Mission

The Open Source Security Foundation (OpenSSF) seeks to make it easier to sustainably secure the development, maintenance, release, and consumption of the open source software (OSS) we all depend on. This includes fostering collaboration within and beyond the OpenSSF, establishing best practices, and developing innovative solutions.

OpenSSF Vision

OSS is a digital public good and as an industry, we have an obligation to address the security concerns with the community. We envision a future where OSS is universally trusted, secure, and reliable. Producers of OSS (of all skill levels) have the ability to proactively and retroactively address both existing and emergent security threats through low-friction tooling automation, education, and clear and actionable guidance. This collaborative vision enables individuals and organizations in a global ecosystem to confidently leverage the benefits and meaningfully contribute back to the OSS community.

OpenSSF Values

The OpenSSF serves as a trusted partner to affiliated open source foundations and projects and provides valuable guidance and artifacts that encourage security by design and security by default. OpenSSF initiatives should make security easier for open source maintainers and contributors. Consumers of OSS can leverage the output of the OpenSSF to have clear, consistent, and trusted signals to better understand the security profile of OSS content.

The OpenSSF is committed to encouraging all interested stakeholders to participate in the foundation and its technical initiatives (TIs). The OpenSSF is viewed as an influential advocate for mutually-beneficial external efforts and an educator of policy decision-makers.

More than just advocacy to Diversity, Equity, and Inclusion (DEI) groups, the OpenSSF remains committed to directly facilitating an environment for all perspectives, all backgrounds, and equitable opportunities for global mentorship and education. The OpenSSF remains committed to continuously evolving these efforts to bring more inclusive and diverse software security education; OpenSSF will ensure stakeholders have open and transparent opportunities to engage in and receive value from OpenSSF TIs.

OpenSSF Strategy

The OpenSSF strategy is a set of objectives that aim to enhance the security of OSS by developing tooling and processes that make secure development easier, promote a deeper understanding of best practices, and provide support to innovative technical initiatives. The charter is the source of truth for the OpenSSF, and this strategy builds on the charter.

Objectives focus on tooling and processes designed to ensure consistency, integrity, and risk assessment that strengthen the overall security of the OSS ecosystem. This focus supports the community to develop tooling, processes, and educational assets that accelerate OSS security technical initiatives. Accomplishing these objectives will provide maintainers and contributors of OSS (of all skill levels) the ability to proactively or retroactively address existing and emergent security threats.

The OpenSSF strategy is outlined across three key areas:

- **Catalyst for Change**: OpenSSF acts as a catalyst for change with producers of OSS to improve "secure by design/ default". Drive technical engagement to create integrated tools that remove barriers to adopting security foundations to improve open source software security.
- **Educate & Empower the Modern Developer**: Create and maintain best practices guides & education materials that ensure both current and future OSS developers obtain & maintain sufficient secure development skills. Consumers of OSS can leverage clear, consistent, and easily integrated trusted signals to better understand the security posture of open source content ingested in supply chains.
- **Ecosystem Leader**: Be an influential advocate and provide a thought leadership forum for collaboration with partners, OSS communities, security experts, and industry. stakeholders on matters important to open source software security and supply chain. Participate meaningfully in standards, frameworks and public policy that impact OSS security. Up-level technical aspects of open source software security when needed to engage with governments, industry bodies, and other relevant organizations.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2024 Membership Growth and Engagement Overview

The OpenSSF is dedicated to strengthening the security and resilience of open source software through community engagement and strategic initiatives. Members actively contribute to OpenSSF's technical initiatives and projects, driving collaborative security advancements across the open source landscape.

In 2024, OpenSSF membership saw significant growth, surpassing our goal of a **10%** increase in general membership with a current rise of **15%**. We are also making strong progress in Europe, reaching **82%** of our goal to increase regional membership by **20%**. Notable new members include:

Premier Member

DATADOG

Associate Members

Trifecta Tech Foundation

General Member

ADALOGICS, arm, BOEING, chainloop, Defense Unicorns, embraceableAI, FUJITSU, KEYFACTOR, RESEARCH, GUIDEWIRE, Hedera, herodevs, HONDA The Power of Dreams, PROTECT AI, SIGHUP, StepSecurity

A categorized list of OpenSSF's current members can be found below, organized by membership level: Premier, General, and Associate.

Premier Members

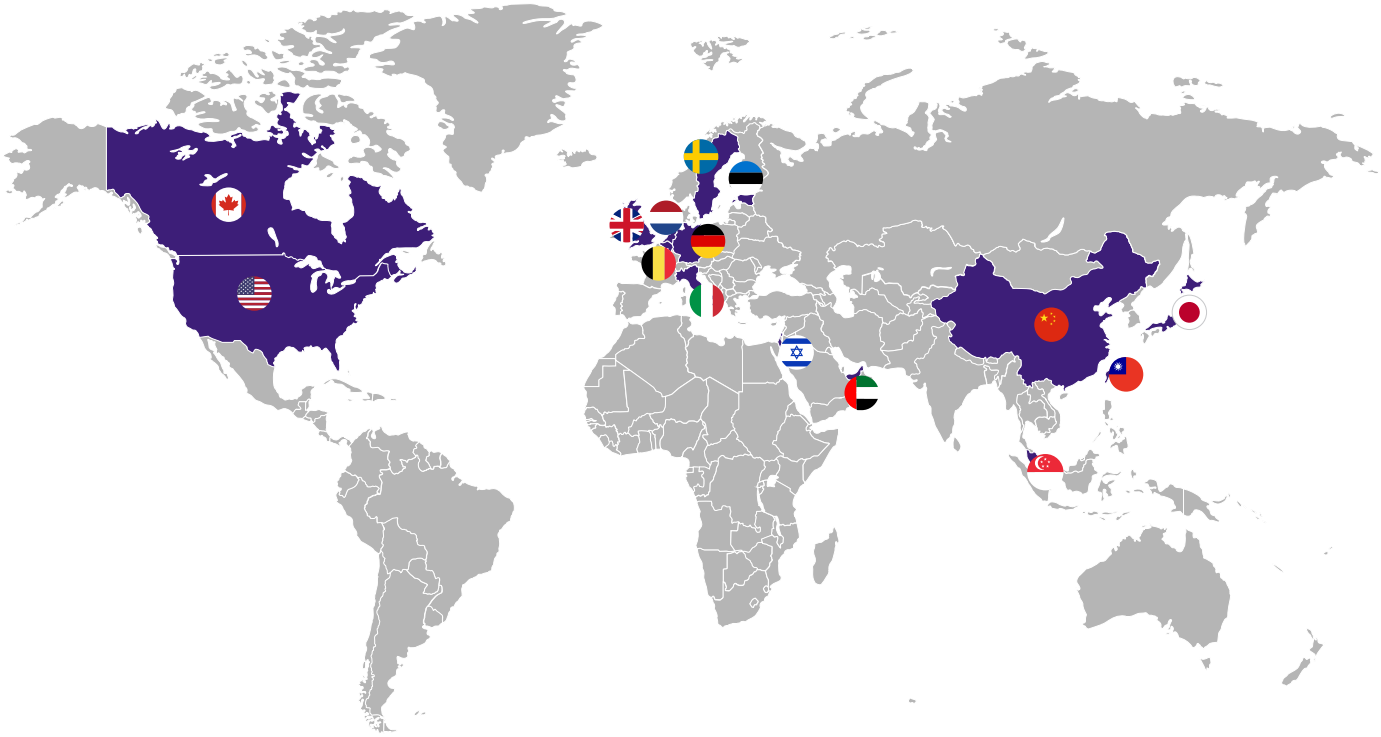
General Members

Associate Members

Join OpenSSF Today

Become an official member of OpenSSF to leverage, influence, and support key security initiatives. To join, please visit our enrollment page: [OpenSSF Membership Enrollment](#).

Member Geography



Member Industries

Governing Board Members

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

ARUN GUPTA
(2024 BOARD CHAIR)
Vice President and General Manager, Open Ecosystem Initiatives, Intel Corporation

BRIAN FOX
CTO, Sonatype

ZACH STEINDLER
Acting OpenSSF TAC Chair & Principal Engineer, GitHub

CHRISTOPHER
"CROB" ROBINSON
Former OpenSSF TAC Chair & Chief Security Architect, OpenSSF

DAVID DESANTO
Chief Product Officer, GitLab (General Mem Rep)

DECLAN O'DONOVAN
VP, Security Architecture, IAM and Application Security, Morgan Stanley

EMILIO ESCOBAR
Chief Information Security Officer, Datadog

ERIC BREWER
VP of Infrastructure & Google Fellow, Google

GRAHAM HILL
Managing Director, Cybersecurity & Technology Controls, JPMorgan Chase

IAN DUNBAR-HALL
Chief Engineer, Lockheed Martin (General Mem Rep)

JAMIE THOMAS
GM, Technology Lifecycle Services, and IBM Enterprise Security Executive

JINGUO CUI
Executive Director of Open Source Security and Infrastructure, Huawei

JOHN ROESE
Global Chief Technology Officer Products and Operations, Dell Technologies

JONATHAN MEADOWS
Head of Cloud Cyber-security Engineering and Software Supply Chain Security, Citibank

JUSTIN CAPPOS
Associate Professor, New York University Tandon School of Engineering (SCIR)

KELLY ANN
Cloud Infrastructure Security Engineer, Apple

MARK RUSSINOVICH
Azure CTO and Technical Fellow, Microsoft

MARK RYLAND
Director, Office of the CISO AWS Security

MICHAEL LIEBERMAN
Co-Founder & CTO, Kusari (General Mem Rep)

MIKE BENJAMIN
Cyber Chief Technology Officer, Capital One

MIKE HANLEY
Chief Security Officer, GitHub

PER BEMING
VP and Head of Standards & Industry Initiatives, Ericsson Group

REBECCA RUMBUL
Executive Director & CEO, Rust Foundation (Associate Mem Rep)

STEPHEN AUGUSTUS
Head of Open Source, Cisco

VINCENT DANEN
Vice President of Product Security, Red Hat

From the Governing Board Chair

The global technology infrastructure relies heavily on open source software (OSS). However, securing this ecosystem is a complex challenge. OpenSSF is dedicated to addressing this challenge by uniting the community, industry, and governance to make OSS more secure.

The Board is Tackling Pressing Challenges in Open Source Security

- **Dependency Vulnerabilities**: Many organizations still face issues with outdated or insecure dependencies, as seen with Log4shell. OpenSSF's GUAC project provides developers and consumers with a visual tool for developers and consumers to track their dependencies and related risks.
- **Typosquatting and Malicious Packages**: Attackers often target software registries by uploading malicious code disguised as popular packages, leading to data theft or malware. OpenSSF partnered with CISA to release the Principles for Package Repository Security, and the OSV project tracks over 26,000 malicious packages to counter these threats.
- **Social Engineering Attacks**: XZ Utils backdoor (CVE-2024-3094) emphasized the risks of social engineering.OpenSSF and OpenJS foundation issued an alert to help open source projects prevent such threats.
- **Supply Chain Attacks**: These attacks exploit vulnerabilities in interconnected software systems. Governments are promoting Software Bill of Materials (SBOMs) to improve transparency and manage supply chain risks. OpenSSF is simplifying SBOM creation and portability with the addition of the protobom and bomctl projects.
- **Regulatory Pressures**: New regulations like the EU Cyber Resilience Act and the U.S. Executive Order on Improving the Nation's Cybersecurity demand stricter compliance in open source. While the CRA enhances cybersecurity, its implementation will have unintended consequences for small businesses, open source communities, and innovation. OpenSSF is working with the EU to ensure a balanced implementation that supports open source.

A Year of Progress and Collaboration

Funding Model: This year, we rolled out a new funding structure for Technical Initiatives to make resource allocation smoother and to increase the impact of OpenSSF projects.

Tabletop Exercises: At SOSS Community Days in North America, Europe, and Japan, we hosted hands-on simulations where participants navigated a fictional vulnerability outbreak, receiving overwhelmingly positive feedback.

OSPO for Good: We teamed up with the United Nations to highlight open source software as a critical digital public good, advocating for its security and sustainability.

As AI adoption grows, I'm excited to see OpenSSF create more tools to make AI and open source more secure and leverage AI to enhance security. I'm eager to raise awareness around open source security and connect with the community to exchange ideas and push boundaries in open source security.

On a personal note, I'm grateful for my first year as Governing Board Chair. The partnership with OpenSSF staff and fellow board members has been strong, and the foundation is on a promising path. I invite you to join us in making the open source ecosystem more secure.

Arun Gupta

2024 Chair of the OpenSSF Governing Board

Vice President and General Manager
of Developer Programs, Intel Corporation

From the TAC Chair

The Technical Advisory Council (TAC) is often referred to as the heart of the Foundation. It plays a key role in facilitating the interests of the Governing Board, while also supporting and motivating the technical membership. The TAC serves as a guiding force for our technical efforts, helping us unite to address major ecosystem challenges.

In 2024, the Foundation's Technical Initiatives (TIs)—a broad term encompassing the technical collaborations within our working groups (WGs), special interest groups (SIGs), and projects—achieved remarkable results for the community. While we will explore the specifics of our TIs later in this report, I'd like to highlight a few key accomplishments. This year, the OpenSSF adopted four new software projects (Protobom, Bomctl, Zarf, RSTUF, and Minder), and some of our most significant projects demonstrated substantial growth and ecosystem impact. Notably, Sigstore graduated to a full project, and Scorecard reached the Incubating stage. We've also collaborated to publish a range of technical guides and training materials, and worked across the industry to improve the security posture of open source software for all.

The TAC expanded this year to 9 seats, with a diverse mix of elected and appointed members. Much work has been done to streamline and simplify the processes that support our community. We successfully launched a concerted effort to support and fund our TIs, which has empowered our members to drive our mission forward. I am personally proud of the commitment and hard work my peers on the TAC have shown, helping us achieve our technical vision and serve our community.

Please enjoy reading about the incredible work our TIs are doing in this report. I hope you'll be inspired to join us in delivering simpler security solutions that maintainers can leverage, while providing signals for downstream consumers as they evaluate the open source software they rely on in their daily work and projects. A heartfelt thank you to all our community members, volunteers, and ecosystem partners who support us every day in making the world a better place.

Christopher "CRob" Robinson
TAC Chair 2023, 2024
OpenSSF

Technical Advisory Council Members

The TAC is composed of 9 individuals that volunteer to help lead our community. It is a mixture of community-elected individuals as well as Governing Board appointed persons. The TAC sits between and coordinates with the Governing Board and the Technical Initiatives that are the "work" of the Foundation.

TAC members sit for a term of two years, and are directly engaged within the Working Groups, SIGs, and projects of the OpenSSF.

ARNAUD LE HORS
OpenSSF TAC Vice Chair & Senior Technical Staff Member - Open Technologies, IBM

BOB CALLAWAY
Tech Lead & Manager, Google Open Source Security Team

CHRISTOPHER "CROB" ROBINSON
Former OpenSSF TAC Chair & Chief Security Architect, OpenSSF

DAN APPELQUIST
Open Source Strategist, Samsung

JAUTAU "JAY" WHITE
Open Source Software and Supply Chain Security Strategy, Microsoft

MICHAEL LIEBERMAN
Co-Founder & CTO, Kusari

MARCELA MELARA
Research Scientist, Intel Labs

SARAH EVANS
Security Research Technologist, Dell Technologies

ZACH STEINDLER
Acting OpenSSF TAC Chair & Principal Engineer, GitHub

OpenSSF Staff

TODD MOORE
Interim General Manager of OpenSSF, SVP of The Linux Foundation Operations

ADRIANNE MARCUM
Chief of Staff

CHRISTOPHER ROBINSON (CROB)
Chief Security Architect

DAVID A. WHEELER
Director, Open Source Supply Chain Security

JEFF DIECKS
Technical Project Manager

KHAHIL WHITE
Technical Program Manager

CHRISTIAN HORCHERT (FUKAMI)
EU Policy Advisor for OpenSSF

KRIS BORCHERS
Technical Project Manager

OpenSSF Support Staff

ANGELAH LIU
Communications & Marketing Manager

JOHN NIRO
Membership Solutions

NAOMI WASHINGTON
Program Manager

RAM IYENGAR
Community Engagement Lead, India

RANDI ARMOUR
Membership Solutions

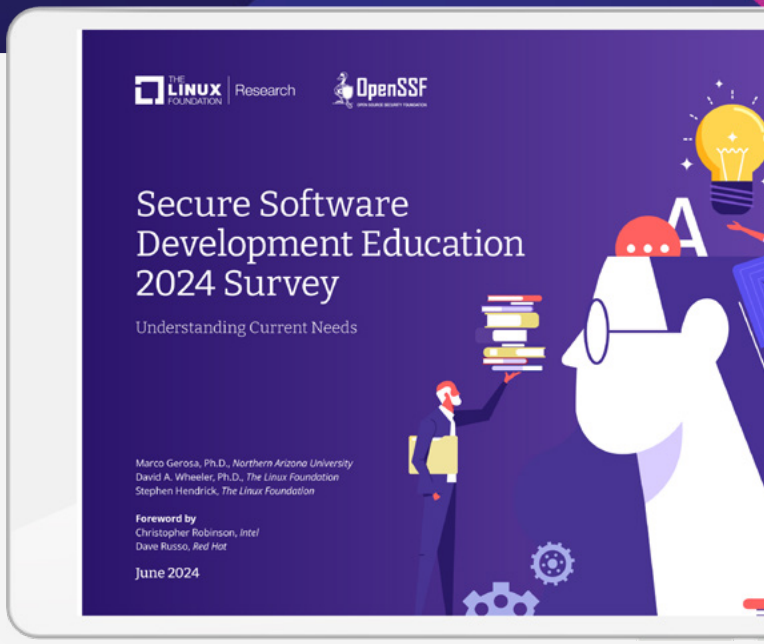
REDEN MARTINEZ
Project Coordinator

RIAAN KLEINHANS
Program Manager

SALLY COOPER
Communications & Marketing Manager

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2024 Highlights



Software Security Education

We've enhanced our free course, Developing Secure Software (LFD121), and its edX equivalents by adding interactive labs. As of now, there are 16 lab-filled sections covering key material, all accessible through a web browser—no software installation required.

Our marketing efforts for LFD121 have been successful. As of mid November, 2024, enrollments have surpassed 8,000, which not only exceeds the total number from 2023 (6,658), but also surpasses our goal of 20% growth (7,990).

In collaboration with LF Research, OpenSSF conducted the Secure Software Development Education 2024 Survey, which revealed valuable insights. Notably, 53% of professionals have not taken a course on secure software development, with 44% citing lack of awareness of good courses. Additionally, 75% of software developers with one year or less of experience were unfamiliar with secure software development.

We continue to refine LFD121, including adding new content on post-quantum cryptography and proper use of regular expressions. We are also working on a new course, Security for Software Development Managers, which we plan to complete and launch in 2024.

Security Guides

- We developed Principles for Package Repository Security and are working with OSS repositories to implement them.

- We developed "Correctly Using Regular Expressions for Secure Input Validation", a new guide for a common security mechanism that is often used incorrectly.

- We updated our existing guides, e.g., "Compiler Options Hardening Guide for C and C++"

- We began work on a draft Python guide, "Secure Coding One Stop Shop for Python"
- We developed the specification Trusted Publishers for All Package Repositories, which aims to reduce the reliance on long-lived tokens or credentials.

Improved OSS Infrastructure & Tooling

We continued to maintain the OpenSSF Best Practices badge, officially establishing its LLC for legal protection and transitioning to the CDLA-Permissive-2.0 license to better accommodate this kind of data. The OpenSSF Scorecard project was also maintained, earning "incubating" status this year. Additionally, the Allstar project was merged into OpenSSF Scorecard to streamline coordination. Sigstore continues to be a growing technical initiative both in its adoption and even hosting its own dedicated conference. The maintainers would like to continue hosting events in 2025.

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 US 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.

The 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 promoted 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, sponsoring the FSFE Youth Hackathon introduced 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 follow-up meetings with the European Commission, providing insights for future CRA-related work.

OpenSSF and Standardardization

OpenSSF is deeply involved in the LF 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. The OpenSSF also cooperates with LF Research on CRA compliance and plans a dedicated CRA workshop with LF 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. OpenSSF applied 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 right 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.

OpenSSF Events

This year, 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. We also hosted SOSS Fusion this year as a standalone OpenSSF event.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Working Groups

WORKING GROUP

AI / ML

This incubating working group is currently in the initial life cycle phases, focusing on addressing open source software security for AI/ML workloads.

GitHub Repo	Leads	Number of Regular Contributors
ossf/ai-ml-security	Jay White, Mihai Maurseac	Approximately 10

2024 HIGHLIGHTS

- Launched a separate project for model signing, developing a proof of concept for model signing with Sigstore, with a stable release planned soon.
- Began collaborating with various other working groups in the AI security space to ensure effective information dissemination among all interested parties.

WHAT'S NEXT

- Aiming for a stable release of the model signing library, compatible with both Sigstore and proprietary PKI solutions, and integration into several ML frameworks and model hubs.
- Plans to support the embedding of additional ML metadata in the signatures and adopt consistent hashing methods for SLSA in the ML workstream, with efforts commencing next year.

WORKING GROUP

Best Practices for Open Source Developers

This group provides open source developers with best practice recommendations and accessible resources to learn and apply them.

Working Group Leads	Number of Regular Contributors
Christopher Robinson (Former Chair), Co-chair: Avishay Balter, Georg Kunz	20

GitHub Repo
ossf/wg-best-practices-os-developers

2024 HIGHLIGHTS

- Added labs to the Secure Development Fundamentals Course (LFD121).
- Launched an awareness campaign around Secure Developer Training and the LFD121 course.
- Conducted numerous conference talks covering topics like the C/C++ Compiler Hardening Options Guide, OpenSSF Scorecard, and Best Practices Badge.
- Engaged in education efforts through the SOSS Taskforce.
- Promoted the adoption of the OpenSSF Security Baseline.
- Collaborated with W3C on Best Practices for Web Developers.
- Received a donation of the Security for Software Development Managers course from Intel.
- Initiated an Academic Accreditation Program with CNCF.
- Hosted OpenSSF Scorecard contributor workshops prior to OSS-NA and SOSS-Fusion conferences.
- Enhanced the C/C++ Compiler Hardening Options Guide.
- Launched a new project donated by Ericsson: Secure Coding One Stop Shop for Python guidelines.
- Released a new guidance document on Correctly Using Regular Expressions.
- OpenSSF Scorecard has released v5, featuring Structured Results (probes) and Maintainer Annotations. It has applied as an OpenSSF Incubating project and adopted Allstar, the OpenSSF Scorecard Monitor, and the OpenSSF Scorecard API Visualizer.

IMPACTS

- Growth of LFD121 enrollment. This year we've had over 8,415 registrations for the Secure Software Development (LFD121) course as of 2024-11-27, exceeding our goal of 7,990 enrollments for 2024. Governing Board members and others have shared our materials and encouraged their organizations to take advantage of this free course.
- Members participated in many conferences, giving talks about our materials and projects. Events included OSS-NA, OSS-EU, Blackhat, RSA, VulnCon, FOSDEM, SBOM-o-rama, NordicCON, and SOSS Fusion.

WHAT'S NEXT?

- Publication of the new Security for Development Managers course.
- Development of a Security Architecture course.
- Rollout of the OpenSSF Security Baseline, including integration into OpenSSF tools (Best Practices Badge, OpenSSF Scorecard, Security Insights, and LFX portal).
- Publication and announcement of Secure Coding One Stop Shop for Python guidelines - Q125
- Announcement & opening of OpenSSF + CNCF Academic Accreditation program at Kubecon
- Publication of the OpenSSF Security Baseline, including adoption by pilot OpenSSF, CNCF, and OpenJS projects. Creation of regulatory compliance matrix to showcase where OpenSSF tools and practices help developers and consumers address compliance regimes.

WORKING GROUP

Diversity, Equity, and Inclusion

This group aims to increase representation and enhance the overall effectiveness of the cybersecurity workforce.

Working Group Leads	Number of Regular Contributors
Marcela Melara, Yesenia Yser, Jay White	Approximately 5
GitHub Repo	
ossf/wg-dei	

2024 HIGHLIGHTS

- Hosted a panel discussion at SOSS Community Day NA '24, addressing the importance of inclusivity and equity in the OpenSSF community. Watch Recording
- Launched monthly community office hours starting in July 2024, featuring expert speakers discussing relevant topics for newcomers and underrepresented groups in OSS and Cybersecurity.
- September office hours focused on "Finding Mentors & Community in OSS and Cybersecurity." Watch Recording
- Full 2024 schedule available here.

IMPACTS

While the working group is still gaining momentum, efforts are concentrated on community building and outreach. The panel discussion helped raise awareness within the greater OpenSSF community. Office hours typically attract 10-20 attendees globally, seeking advice and opportunities in OSS and cybersecurity.

WHAT'S NEXT

- Launch of "Tip of the Month" posts, featuring career tips from OpenSSF community members via blog/social media.
- Drive the creation of LFX Mentorship opportunities to facilitate impactful contributions from newcomers to ongoing OpenSSF projects.
- Establish best practices for inclusive and newcomer-friendly contribution guidelines for OpenSSF projects.

WORKING GROUP

Securing Critical Projects

This group focuses on identifying and allocating resources to secure the critical open source projects essential for our reliance.

Working Group Leads	Number of Regular Contributors
Amir Montazery, Jeff Mendoza	5-10

GitHub Repo

ossf/wg-securing-critical-projects

2024 HIGHLIGHTS

- Adopted a Minimum Viable Security Requirements (MVSR) framework to increase adoption and usability of the Set of Critical Projects.
- Presented the selection process for identifying critical projects.
- Integrated a feed of packages from Reversing Labs for Malicious Packages.
- Worked on improving data quality and software identification issues.
- Enhanced infrastructure for the Criticality Score, allowing consistent execution and increased coverage.
- Release of Census III research.

IMPACTS

- **Malicious Packages:** Ingests 25,000 data points, including approximately:
  - » 15,000 npm packages
  - » 8,000 pypi packages
  - » 1,000 rubygems
  - » 1,000 nuget packages
- **Criticality Score:** Monthly score calculations cover 500,000 projects.

WHAT'S NEXT

- Continue to develop the strategy and roadmap under MVSR to enhance the Set of Critical Projects.
- Refine the definition of "malicious" for the Malicious Packages repository.

WORKING GROUP

Securing Software Repositories

This group collaborates to introduce new tools and technologies that strengthen and secure software repositories. Our current project is the Repository Service for TUF—join us to learn more!

Working Group Leads	Number of Regular Contributors
Dustin Ingram, Zach Steindler	N/A
GitHub Repo	
ossf/wg-securing-software-repos	

2024 HIGHLIGHTS

- Co-published the *Principles for Package Repository Security* with US CISA to help open source package repositories develop security roadmaps.
- Significant progress on RSTUF, evolving from an experimental system to an MVP release suitable for production deployment, aimed at protecting package repository indices.
- Published *Trusted Publishers for All Package Repositories* implementation guidance to enhance secret management in building pipelines across platforms.

IMPACTS

- The *Principles of Package Repository Security* document inspired CISA to host the Open Source Software Security Summit.
- Homebrew's build provenance work was motivated by the group's proposal last year.
- RSTUF proof-of-concept works with RubyGems and PyPI to protect their package indices.
- NuGet's Trusted Publishers specification cited *Trusted Publishers for All Package Repositories* as its foundational basis.
- RFC for Trusted Publishing Support on Crates.io has been published.

WHAT'S NEXT

- Continue publishing implementation guidance on emerging topics relevant to open source package repositories.
- Publish best practices for engaging with open source communities, potentially collaborating with the US public sector.
- Release RSTUF v1.0 and facilitate production deployment to RubyGems and PyPI.

WORKING GROUP

Security Tooling

This group focuses on providing the best security tools for open source developers and aims to make them universally accessible.

Working Group Leads	Number of Regular Contributors
Ryan Ware	5-10
GitHub Repo	
ossf/wg-security-tooling	

2024 HIGHLIGHTS

Protobom

- Protobom was recently accepted as a sandbox project within OpenSSF. This format-agnostic tool enables organizations to both ingest and create Software Bills of Material (SBOMs) for the software they use and develop.

bomctl

- The bomctl project was accepted as a sandbox project. While Protobom serves many use cases effectively, some specific needs require a unique solution. In response, the team developed bomctl, built on the Protobom engine, to address those requirements.
- The SBOM-Everywhere project is focused on creating a comprehensive SBOM tooling catalog and documenting best practices for getting started with SBOMs.

minder

- The Technical Advisory Council (TAC) has approved the sandbox application for Minder, an open source project donated to OpenSSF. Minder adds to the suite of OpenSSF solutions by helping secure open source developer repositories, including implementing policies to ensure long-term security.
- The Fuzzing Collaboration group continues its efforts to educate open source maintainers on how to integrate fuzzing solutions into their projects.

IMPACTS

- OpenSSF's work with SBOMs is at the forefront of innovation. Members continue to identify new areas where they can support the SBOM needs of maintainers and organizations, as demonstrated by their presence at SBOM-A-Rama 2024. These efforts are streamlining SBOM adoption across the ecosystem.
- Fuzzing is another area where developers often struggle to get started. The Fuzzing Collaboration group continues to assist open source projects in adopting fuzzing solutions like OSS-Fuzz.

WHAT'S NEXT

- We will continue to broaden the areas where OpenSSF can assist the ecosystem with SBOMs. Additionally, we will focus on non-SBOM tools like Minder to enhance the portfolio of OpenSSF solutions, while ensuring close collaboration with other OpenSSF tools where there is overlap.

WORKING GROUP

Supply Chain Integrity

This group helps individuals understand and make informed decisions about the provenance of the code they maintain, produce, and use, including projects like GUAC, SLSA, and gittuf.

Working Group Leads	Number of Regular Contributors
Isaac Hepworth, Jay White	25–50
GitHub Repo	
ossf/wg-supply-chain-integrity	

2024 HIGHLIGHTS

- **Projects added:** formally welcomed GUAC, Zarf, and Security Insights to the Supply Chain Integrity Working Group

- SLSA: Specification v1.1 is nearing final draft; changes include an updated threat model and procedures for verifying VSAs. Source Track is in draft. Hardware Attestations Track being defined. Dependencies Track being bootstrapped from S2C2F.

- S2C2F: Continued refinements to core S2C2F specification. Collaborating with SLSA on Dependencies Track. Initiated a new workstream in partnership with AI/ML Security WG around extending S2C2F to AI use cases (e.g. consuming models from HuggingFace).

- gittuf: Active work on real-world pilot, and seeking funding for app hosting.

- GUAC: Joined OpenSSF in March, releasing 15 updates since then, including support for persistent databases and Clearly Defined license information. Welcomed 13 new contributors, along with 2 promotions in the contributor ladder.

- Zarf: onboarding to OpenSSF and readying a 1.0 release candidate for 2024 Q4 release.

IMPACTS

- SLSA continues to gain traction and mindshare as the predominant open supply chain security framework. A number of new tracks are in development to extend its utility and value.
- GUAC's contributions include a case study from Guidewire.

WHAT'S NEXT

- SLSA v1.1 and Source Track, Hardware Attestations Track, Dependencies Track.
- GUAC is working toward its 1.0 release and focusing on database performance tuning.
- Zarf v1.0 release

WORKING GROUP

Vulnerability Disclosures

This group aims to enhance the overall security of the open source ecosystem by advancing vulnerability reporting and communication. They assist OSS maintainers in issuing VEX documents, reducing the burden of triaging vulnerability reports and communicating impact, and enabling VEX feeds to streamline these processes.

Working Group Leads	Number of Regular Contributors
Madison Oliver, Christopher Robinson (Former Chair)	10

GitHub Repo
ossf/wg-vulnerability-disclosures

2024 HIGHLIGHTS

- Published Tabletop Exercise (TTX) collateral.
- Conducted OSS-NA and OSS-EU TTX, with OSS-JP coming soon.
- Launched the SIREN threat intel mailing list.
- Provided updates on OSV and OpenVEX.

IMPACTS

- The group had substantial participation at the 2024 VulnCon vulnerability ecosystem conference, featuring discussions on CVD, open source vulnerability metadata, and VEX/SBOM with 11 members presenting across the 40 sessions at the conference. The OpenSSF sponsored the conference, contributing to its success.
- The TTX sessions at LF events raised community awareness about documenting and practicing cyber-incident processes.
- The SIREN mailing list has become a platform for sharing information about security issues and vulnerabilities actively being exploited in the ecosystem.
- OSV ecosystem adoption this year:
  - Ubuntu
  - Malicious Packages
  - Mageia
  - Chainguard + Wolfi
  - SUSE/openSUSE
  - Red Hat

WHAT'S NEXT

- The call for papers for the 2025 VulnCon will open mid-October.
- Creation and publication of the Coordinated Disclosure Guide for Open Source Consumers.
- Continued ecosystem collaboration on CVE & CNA programs
- Continued ecosystem collaboration on SBoM and VEX
- Further expansion of Tabletop Exercise (TTX) collateral and conference exercises

PROJECT

Sigstore

Working Group Leads	Number of Regular Contributors
TSC (Bob Callaway, Luke Hinds, Trevor Rosen, Santiago Torres-Arias, Priya Wadhwa), Community Chair (Hayden Blauzvern)	22
GitHub Repo	
sigstore	

2024 HIGHLIGHTS

- Sigstore officially graduated as a project within the OpenSSF, marking a significant milestone in its maturity and adoption, which enhances the trustworthiness of software creation and distribution.
- SigstoreCon held in November, co-located with Kubecon, to unite supply chain security communities discussing Sigstore and related SSCI projects.
- Active developments included major releases of sigstore-python, sigstore-java, sigstore-go, and sigstore-ruby, along with the introduction of model transparency for ML model signing.

IMPACTS

- Sigstore has seen significant adoption across multiple package ecosystems, including:
  - » Adoption by npm with support for Sigstore-signed SLSA provenance.
  - » GitHub Artifact Attestations utilizing Sigstore for signed provenance in workflow runs.
  - » Homebrew generates Sigstore-signed provenance for all bottles in `homebrew-core` and verifies them on `brew install`, funded by Alpha-Omega.
  - » PEP 740 approved and adopted by PyPI for index support of Sigstore-signed attestations.
  - » Maven Central supporting Sigstore signature bundles.
  - » PEP 761, a draft proposal to deprecate PGP signatures on CPython releases in favor of Sigstore signatures

WHAT'S NEXT

- Continue supporting OSS package managers as the primary path for Sigstore adoption.
- Redesign Rekor, Sigstore's transparency log, to simplify management and reduce operational costs for both public and private deployments.
- Collaborate with the academic community to enhance trust assurances and privacy guarantees.
- Major releases of sigstore-go, sigstore-ruby, and sigstore-rs are on the horizon.
- Enable cryptographic agility to support post-quantum signing.

PROJECT

Alpha-Omega

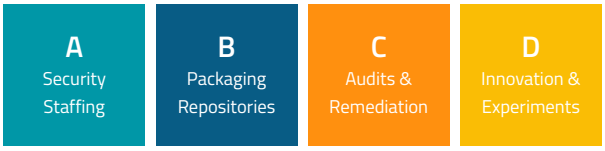
Alpha-Omega → Leverage

Ω → Scale

Alpha-Omega is an associated project of the OpenSSF, established in February 2022, funded by Microsoft, Google, and Amazon, and with a mission to protect society by catalyzing sustainable security improvements to the most critical open source software projects and ecosystems. Alpha-Omega works with the most important open source foundations and organizations to improve security for millions of end-users around the world.

Alpha-Omega spans focused engagements with significant leverage and impact (Alpha) and scaled approaches to address the hundreds of thousands of projects. For example, the Python Software Foundation has used an Alpha-Omega grant to hire Seth Larson as the first ever security engineer-in-residence for the Python ecosystem. His work has been leveraged across the broader Python community. Another Alpha-Omega grant has focused on scaled approaches to auditing the over 700 dependencies of the Airflow project.

In 2024, Alpha-Omega had provided 25 grants totalling over $5M. Since its founding, the project has granted over $9M to over 15 different open source projects and organizations. These grants prioritize engagements that are shovel-ready and for which engineering resources are ready-to-go. These engagements fall into one of four strategic categories:



Alpha-Omega's annual reports as well as the per-project status updates are available on the Alpha-Omega website and GitHub repository.

Projects are OpenSSF Technical Initiatives that support the innovative delivery of security tooling and best practices to secure critical open source software.

The OpenSSF Technical Advisory Council is responsible for the oversight of the various Technical Initiatives (TI) and maintains a project lifecycle for hosted projects. Interested in hosting a project?

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Community Engagement

DevRel & Marketing Advisory Council

The DevRel Community is affiliated with and managed by the Marketing Advisory Council for the purpose of evangelizing the mission and work of the OpenSSF and building strong community outreach around end-users and open source maintainers and contributors. The community's primary goals are to increase tooling adoption in critical OSS projects, build and maintain relationships with the greater end-user and open source communities, and create an "OpenSSF Contributor Community" through easy contributor on-ramps and contributor-led project events.

In 2024, the OpenSSF DevRel community made significant strides in defining its mission, building a strong community foundation, and emphasizing the role of Developer Relations in advancing OpenSSF's growing portfolio of open source projects essential for securing the software supply chain. Early in the year, Tracy Ragan and Kathrine Druckman launched efforts to shape this community, starting with guidelines for a community blog program. Since then, OpenSSF has received numerous submissions on security topics that broaden the conversation on open source software use and security. We have focused on

Katherine Druckman (Intel)

Tracy Ragan (DeployHub)

recruitment and evangelism via conference talks and open office hours, encouraging and providing support for community members to take OpenSSF tools and best practices into their own open source communities.

Looking ahead to 2025, the DevRel community is focused on expanding outreach efforts. Our goal is to drive global adoption of OpenSSF's security tools, developed through the efforts of contributors from around the world, reinforcing the commitment to a more secure open source ecosystem.

DevRel and Marketing Advisory Council Co-Chair:

Katherine Druckman (Intel Corporation)
Tracy Ragan (DeployHub)

Events

SOSS Community Day North America

APRIL 15, 2024 | SEATTLE, WASHINGTON

SOSS Community Day
NORTH AMERICA

SOSS Community Day
NORTH AMERICA

SEATTLE, WASHINGTON
#SOSSCOMMUNITY

POST EVENT REPORT

49% OF ATTENDEES IN TECHNICAL POSITIONS

340 ATTENDEES ATTENDED

345 TOTAL ORGANIZATIONS REPRESENTED

595 ATTENDEES REGISTERED

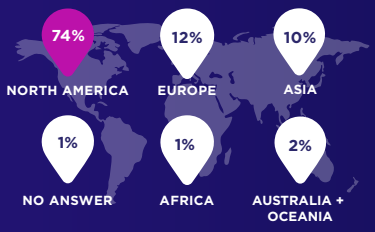
61 CFP SUBMISSIONS

3 KEYNOTES

22 PANELS + TALKS

33% GENDER MINORITY SPEAKERS

ATTENDEES PER REGION

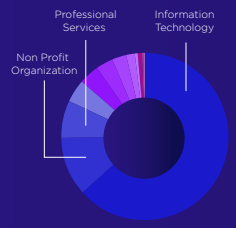


TOP THREE JOB FUNCTIONS:

EXECUTIVE LEADER

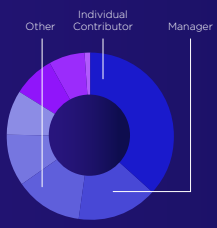
MANAGER - TECHNICAL TEAMS

APPLICATION DEVELOPER (FRONT-END/BACK-END/MOBILE/ FULL STACK)



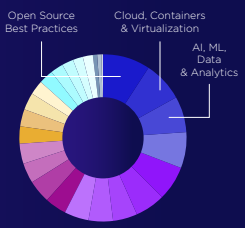
Industry

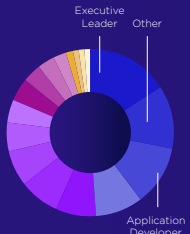
- Information Technology **64%**
- Non Profit Organization **11%**
- Professional Services **7%**
- Telecommunications **4%**
- Industrials **4%**
- Financials **3%**
- Consumer Goods **3%**
- Automotive **2%**
- No Value **0.7%**
- Health Care **0.7%**
- Materials **0.3%**
- Energy **0.2%**



Job Level

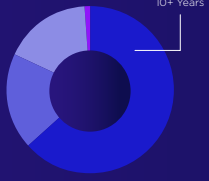
- Individual Contributor **37%**
- Director **16%**
- Manager **13%**
- Other **10%**
- CXO / ED **9%**
- Academic **8%**
- VP / SVP / GM **7%**
- No Answer **1%**





Job Function

- Executive Leader **13%**
- Other **13%**
- Application Developer (Front-end / Back-end / Mobile / Full Stack) **10%**
- Systems / Embedded Developer **10%**
- Manager - Technical Teams **9%**
- Manager - OSPO **8%**
- Architect **8%**
- Manager - Other **4%**
- Legal / Compliance **4%**
- Kernel / Operating Systems Developer **4%**
- DevOps / SRE **3%**
- Marketing **3%**
- Product/Biz Dev **3%**
- Professor / Academic **3%**
- Student **2%**
- Media / Analyst **1%**
- No Answer **1%**



Years of IT Experience

- 10+ Years **63%**
- 0-4 Years **19%**
- 5-9 Years **17%**
- No Answer **1%**

Area of Interest

- Open Source Best Practices **9%**
- Cloud, Containers & Virtualization **8%**
- AI, ML, Data & Analytics **7%**
- DevOps, CI / CD & Site Reliability **7%**
- Cybersecurity **7%**
- Privacy & Security **6%**
- SupplyChain **5%**
- Linux Kernel **5%**
- IoT & Embedded **5%**
- System Engineering **4%**
- Open Source Program Offices **4%**
- Web & Application Development **4%**
- Leadership & Community **4%**
- Leadership & Community **4%**
- Networking & Edge **4%**
- Cross-Technology **3%**
- Open Hardware **3%**
- Diversity, Equity & Inclusion **3%**
- Safety-Critical Systems **3%**
- Security **3%**
- Blockchain **2%**
- Sustainability **2%**
- System Administration **2%**
- Visual Effects **1%**
- Compliance **1%**
- No Answer **0.1%**

SOSS Community Day Europe

SEPTEMBER 19, 2024 | VIENNA, AUSTRIA

SOSS Community Day
EUROPE

SOSS Community Day
EUROPE

VIENNA, AUSTRIA

POST EVENT REPORT

42% OF ATTENDEES IN TECHNICAL POSITIONS

397 ATTENDEES REGISTERED

234 TOTAL ORGANIZATIONS REPRESENTED

307 ATTENDEES ATTENDED

85 CFP SUBMISSIONS

29 CONFIRMED SESSIONS

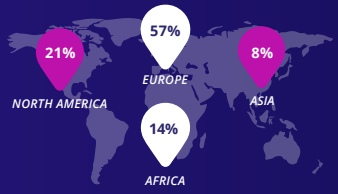
6 KEYNOTES

23 BREAKOUTS

35 SPEAKERS

25% GENDER MINORITY SPEAKERS

ATTENDEES PER REGION

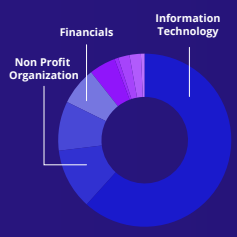


TOP THREE JOB FUNCTIONS:

APPLICATION DEVELOPER
[FRONT-END/BACK-END/MOBILE/FULL STACK]

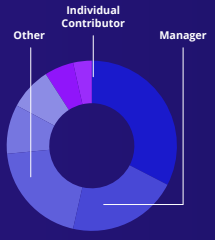
EXECUTIVE LEADER

ARCHITECT



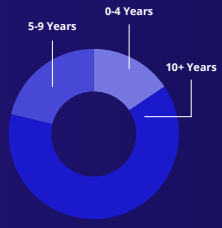
Industry

- Information Technology **59%**
- Non Profit Organization **13%**
- Telecommunications **8%**
- Financials **6%**
- Professional Services **5%**
- Automotive **3%**
- Consumer Goods **3%**
- Industrials **3%**
- Energy **1%**
- Health Care **1%**



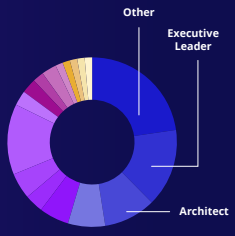
Job Level

- Individual Contributor **33%**
- Manager **21%**
- Other **20%**
- Director **9%**
- CXO / ED **8%**
- Academic **6%**
- VP / SVP / GM **4%**



Years of IT Experience

- 10+ Years 65%
- 5-9 Years 19%
- 0-4 Years 16%



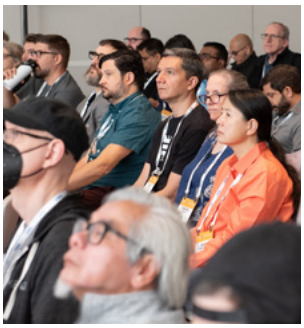
Job Function

- Other **18%**
- Executive Leader **14%**
- Architect **12%**
- Manager - Other **9%**
- Manager - Technical Teams **7%**
- Systems/Embedded Developer **6%**
- DevOps/SRE **6%**
- Application Developer [Front-end/Back-end/Mobile/Full Stack] **6%**
- Manager - OSPO **6%**
- Marketing **4%**
- Student **4%**
- Kernel/Operating Systems Developer **3%**
- Professor / Academic **2%**
- DevOps/SRE/Sysadmin **1%**
- Legal / Compliance **1%**
- Product/Biz Dev **1%**
- Media / Analyst 1%

SOSS FUSION/24

SOSS FUSION

OCTOBER 22-23 | ATLANTA, GEORGIA



SOSS FUSION/24

OCTOBER 22–23, 2024 | ATLANTA, GA
#SOSSFusion

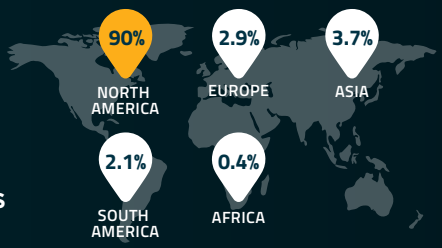
POST EVENT REPORT

241 ATTENDEES REGISTERED

191 ATTENDEES ATTENDED

155 TOTAL ORGANIZATIONS REPRESENTED

ATTENDEES PER REGION



198 CFP SUBMISSIONS

1 CO-LOCATED EVENT

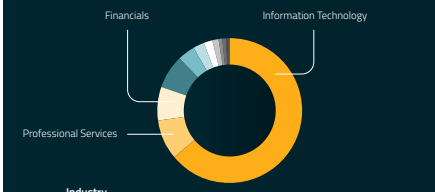
11 KEYNOTES

35 BREAKOUTS

8 LIGHTNING TALKS

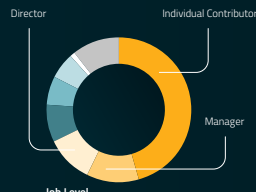
59 NUMBER OF SPEAKERS

17% % GENDER MINORITY SPEAKERS



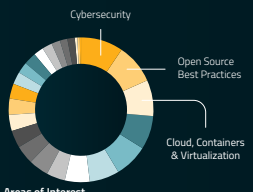
Industry

- Information Technology **63.90%**
- Professional Services **9.13%**
- Financials **7.47%**
- Non Profit Organization **7.47%**
- Health Care **3.73%**
- Telecommunications **2.49%**
- Industrials **2.07%**
- Automotive **1.24%**
- Consumer Goods **0.83%**
- Energy **0.83%**
- No Value **0.83%**



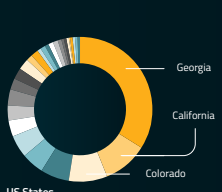
Job Level

- Individual Contributor **45.64%**
- Manager **11.62%**
- Director **10.79%**
- CXO / ED **8.30%**
- Academic **6.22%**
- VP / SVP / GM **5.81%**
- No Value **1.24%**
- Other **10.37%**



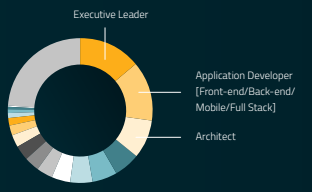
Areas of Interest

- Cybersecurity **65.98%**
- Open Source Best Practices **62.66%**
- Cloud, Containers & Virtualization **54.77%**
- AI, ML, Data & Analytics **53.53%**
- DevOps, CI/CD & Site Reliability **51.45%**
- Privacy & Security **46.47%**
- SupplyChain **37.34%**
- Open Source Program Offices (OSPO) **30.71%**
- Leadership & Community **29.88%**
- System Engineering **29.88%**
- Linux Kernel **26.14%**
- Networking & Edge **25.73%**
- Web & Application Development **24.90%**
- IoT & Embedded **21.99%**
- Diversity, Equity & Inclusion **19.09%**
- Cross-Technology **18.67%**
- System Administration **18.67%**
- Safety-Critical Systems **16.18%**
- Open Hardware **15.77%**
- Sustainability **12.86%**
- Blockchain **12.03%**
- Security **10.37%**
- Visual Effects **4.98%**
- Compliance **2.90%**
- No Value **1.24%**



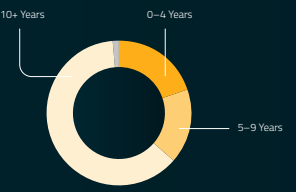
US States

- Georgia **34%**
- California **10%**
- Colorado **8.5%**
- Texas **6.5%**
- New York **5%**
- Washington **5%**
- Florida **3.5%**
- North Carolina **3.5%**
- Virginia **3.5%**
- Massachusetts **2.5%**
- Pennsylvania **2.5%**
- Tennessee **2.5%**
- Illinois **1.5%**
- Oregon **1.5%**
- Alabama **1%**
- Arizona **1%**
- Maryland **1%**
- Michigan **1%**
- Minnesota **1%**
- South Carolina **1%**
- Arkansas **0.5%**
- Delaware **0.5%**
- District of Columbia **0.5%**
- Kentucky **0.5%**
- New Hampshire **0.5%**
- New Jersey **0.5%**
- Ohio **0.5%**
- Oklahoma **0.5%**



Job Function

- Executive Leader **14.11%**
- Application Developer [Front-end/ Back-end/Mobile/Full Stack] **13.28%**
- Architect **8.71%**
- Manager - Other **5.81%**
- Product/Biz Dev **5.39%**
- DevOps/SRE **4.98%**
- Manager - Technical Teams **4.15%**
- Student **3.73%**
- Marketing **3.32%**
- Systems/Embedded Developer **3.32%**
- Manager - OSPO **2.90%**
- Professor / Academic **2.07%**
- DevOps/SRE/Sysadmin **1.66%**
- No Value **1.24%**
- Kernel/Operating Systems Developer **0.83%**
- Legal / Compliance **0.41%**
- Media / Analyst **0.41%**
- Other **23.65%**



Years of IT Experience

- 0–4 Years **19.92%**
- 5–9 Years **16.60%**
- 10+ Years **62.24%**
- No Value **1.24%**

SOSS Community Day
JAPAN

SOSS Community Day Japan

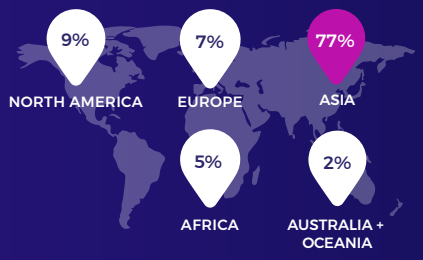
OCTOBER 30, 2024 | TOKYO, JAPAN

SOSS Community Day
JAPAN

TOKYO, JAPAN

POST EVENT REPORT

ATTENDEES PER REGION



203 ATTENDEES REGISTERED

171 ATTENDEES ATTENDED

57% OF ATTENDEES IN TECHNICAL POSITIONS

60 TOTAL ORGANIZATIONS REPRESENTED

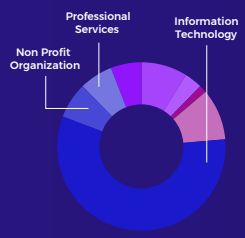
22 CFP SUBMISSIONS

3 KEYNOTES

16 SESSIONS

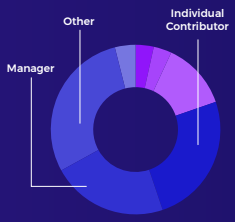
21 SPEAKERS

10% GENDER MINORITY SPEAKERS



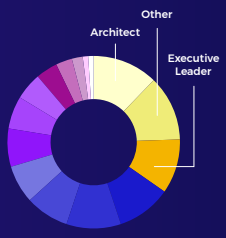
Industry

Information Technology	57%
Industrials	10%
Automotive	9%
Non Profit Organization	7%
Professional Services	6%
Telecommunications	6%
Consumer Goods	3%
Financials	1%



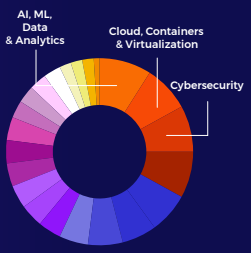
Job Level

Individual Contributor	25%
Manager	22%
Director	13%
VP / SVP / GM	4%
Academic	3%
CXO / ED	3%
Other	29%



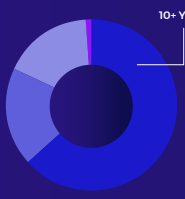
Job Function

Architect	12%
Other	12%
Executive Leader	10%
Manager - Technical Teams	10%
Systems/Embedded Developer	10%
Application Developer (Front-end/Back-end/Mobile/Full Stack)	8%
Kernel/Operating Systems Dev	7%
Manager - Other	7%
Product/Biz Dev	6%
Manager - OSPO	5%
DevOps/SRE	4%
Media / Analyst	3%
Marketing	2%
DevOps/SRE/Sysadmin	1%
Legal / Compliance	1%



Area of Interest

AI, ML, Data & Analytics	9%
Cloud, Containers & Virtualization	8%
Cybersecurity	8%
Open Source Best Practices	8%
DevOps, CI/CD & Site Reliability	7%
IoT & Embedded	6%
Linux Kernel	6%
Networking & Edge	5%
Open Source Program Offices	4%
Privacy & Security	4%
Safety-Critical Systems	4%
Security	4%
SupplyChain	4%
System Engineering	4%
Cross-Technology	3%
Leadership & Community	3%
Open Hardware	3%
Web & Application Development	3%
Blockchain	2%
Sustainability	2%
System Administration	2%
Diversity, Equity & Inclusion	1%



Years of IT Experience

10+ Years	15%
0-4 Years	21%
5-9 Years	17%

SOSS Community Day India

DECEMBER 10, 2024 | DELHI, INDIA

SOSS Community Day India marks an exciting milestone as OpenSSF expands into new regions. This is the first-ever Community Day event hosted in India, taking place in Delhi on December 10, 2024.

The event features an engaging lineup of sessions designed to foster collaboration and share progress on securing open source software.

SESSION HIGHLIGHTS

Welcome & Opening Remarks – Arun Gupta, Vice President and General Manager, Developer Programs, Intel

- *Cooking up Secure OCI Artifacts with SLSA* – Harsh Thakur, Civo & Saiyam Pathak, Loft Labs
- *Building a Security-First Open Source Project: Tools and Best Practices* – Abhinav Sharma, KodeKloud
- *Towards a Quantum-Proof Software Supply Chain with Post-Quantum Cryptographic Algorithms* – Anitha Natarajan & Savita Ashture, Red Hat
- *Who Guards the Guards?* – Arnab Chatterjee, Nomura
- *Patch It Up: Real-Time Vulnerability Management with Kyverno and KubeArmor* – Barun Acharya & Ramakant Sharma, AccuKnox Inc.
- *AI-Driven Policy Automation with Kyverno* – Sonali Srivastava & Pavan N G, InfraCloud
- *Securing CI/CD: Complexity & Inspiration from Runtime Security* – Abhimanyu Dhamija, KoalaLab
- *From CVE Chaos to Control: Building a "0 CVE" Strategy* – Rakshit Gondwal, BuildSafe & Harsh Thakur, Civo
- *Lightning Talk – What Do We Do With All These SBOMs?* – Nikhita Raghunath, Broadcom
- *Connecting the Dots: SBOM and VEX in Software Security* – Rajan Ravi, Red Hat India Pvt. Ltd.
- *Case Study on Adversarial Emulation Using MITRE Caldera for Kubernetes* – Rudraksh Pareek, AccuKnox

SOSS Community Day INDIA

- *From Bloat to Secure: Rethinking Container Base Images for the Modern Security Landscape* – Abhishek Anand, KoalaLab
- *How to Resolve Top 3 Security and Risk Challenges for Enterprises Consuming Open Source* – Nitish Tyagi, Gartner
- *Automating Container Security: Docker Scout in CI/CD for Safer Software Supply Chains* – Pradumna V Saraf, Independent
- *CERT.in Guidelines on Software Bill of Materials (SBOM)* – Biju Nair, Legalitech
- *Adversarial Resilience in Open Source LLMs: A Comprehensive Approach to Security and Robustness* – Padmajeet Mhaske, JP Morgan Chase
- *Quarantining and Locking Down Your Cloud Infrastructure* – Prerit Munjal, KubeCloud
- *Closing Remarks* – Ram Iyengar, Community Engagement Lead - India, OpenSSF

ABOUT SOSS COMMUNITY DAYS

Secure Open Source Software (SOSS) Community Days bring together members from across the security and open source ecosystem to share ideas and advance capabilities that help sustainably secure the development, maintenance, and consumption of open source software (OSS). Learn more about the event here.

"What's in the SOSS?" — An OpenSSF Podcast

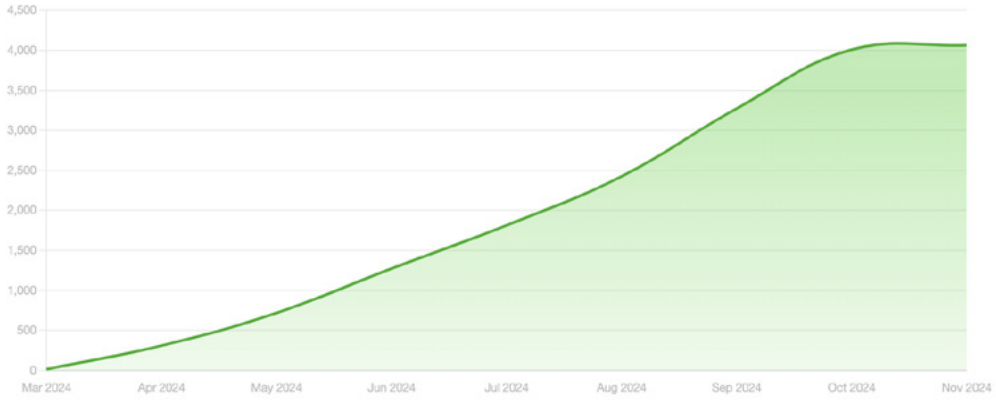
In April, OpenSSF launched "What's in the SOSS?" a bi-weekly podcast hosted by OpenSSF Chief Security Architect Christopher Robinson — aka "CRob" — and former OpenSSF GM Omkhar Arasaratnam. In just seven months, "What's in the SOSS?" has become a go-to content hub for secure open source software insight. It has helped create a broader and more engaged open source community and further strengthened relationships with OpenSSF members.

"What's in the SOSS?" has attracted guests from some of the world's most recognizable tech companies and organizations including Google, OpenAI, GitHub, Dell, Intel, Red Hat, CISA and the Rust Foundation. We are now receiving inbound guest requests from leading vendors and industry organizations — a testament to the program's influence and positive visibility.

SUBSCRIBERS (ONLY APPLE AND SPOTIFY SHARE SUBSCRIBER STATISTICS)

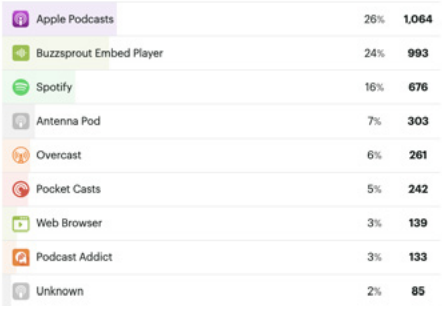
- Total: 230
- Apple Podcasts: 100
- Spotify: 130

DOWNLOADS YEAR-TO-DATE



MOST POPULAR APPLICATIONS FOR DOWNLOADS

- Apple Podcasts: 26% of downloads, 1064 total
- Buzzsprout Embed Player (OpenSSF site): 24% of downloads, 993 total
- Spotify: 16% of downloads, 676 total
- Antenna Pod, 7% of downloads, 303 total
- Overcast, 6% of downloads, 261 total



Most Popular Episodes

WHAT'S IN THE SOSS? PODCAST #13 – GITHUB'S MIKE HANLEY AND TRANSFORMING THE "DEPT. OF NO" INTO THE DEPT. OF "YES AND..."

Published on September 03. 2024
337 DOWNLOADS

WHAT'S IN THE SOSS? PODCAST #11 – GOOGLE'S ANDREW POLLOCK AND ADDRESSING OPEN SOURCE VULNERABILITIES

Published on August 13, 2024
281 DOWNLOADS

WHAT'S IN THE SOSS? PODCAST #9 – SONATYPE'S BRIAN FOX AND THE PERPLEXING PHENOMENON OF DOWNLOADING KNOWN VULNERABILITIES

Published on July 16, 2024
279 DOWNLOADS

Blog & Resources

The OpenSSF blog highlights the community's active contributions toward addressing critical cybersecurity tools and challenges. Through blogs, guest blogs, and case studies, we've shared diverse insights and solutions that drive progress in secure software development and open source security.

Have an idea to share? Submit your blog proposal and contribute to shaping the future of cybersecurity in 2025!

OpenSSF Blogs

The OpenSSF blog is a vital resource for expert insights, detailed analyses, and community updates on key cybersecurity issues. Throughout the year, our blog has featured diverse content that explores the latest developments in secure software development and open source security, including highlights from our participation in key industry events.

- Understanding the CRA: OpenSSF's Role in the Cyber Resilience Act Implementation – Part 1
- The OpenSSF Armored Goose "Honk": Advancing Open Source Security
- How We Can Learn from Open Source Software to Address the Challenges of AI
- OpenSSF Welcomes New Members and Introduces New Initiatives at SOSS Community Day Japan
- OpenSSF Expands Secure Development Course with Interactive Labs
- Cybersecurity Awareness Month 2024: Stay Secure, Stay Informed
- OpenSSF SOSS Fusion Conference Kicks off with Talks from Google and Cisco Executives
- Developer Relations: The Human Connection Driving Open Source Security
- OpenSSF Education Tech Talk Highlights & Future Opportunities
- Recap on SOSS Community Day EU
- OpenSSF at Grace Hopper Celebration 2024: Advancing Diversity and Security in Open Source
- Join Us at the OSS Security Meetup in Tokyo, Japan
- Must-Attend Sessions at SOSS Community Day EU and Open Source Summit Europe 2024
- Prioritizing Security: Key Findings from the OpenSSF Survey for Financial Institutions
- AIxCC Semifinals at DEF CON Showcase AI's Potential in Securing Critical OSS Projects
- A Bird's-Eye View of LFD 121 (Developing Secure Software) — and Why Every Developer Should Take It
- GUAC v0.8.0 Released
- Announcing SigstoreCon: Supply Chain Day!
- Mitigating Attack Vectors in GitHub Workflows
- Call for Proposals: SOSS Community Day Japan 2024
- What's Next for Open Source? Workshop Highlights and Calls to Action to Inspire Progress for Global Sustainability
- OSS Security Adventure: Recap of Recent Security-Focused Events Featuring OpenSSF
- SOSS Community Day EU Agenda Now Live!
- SOSS Fusion 2024 CFP Results: A Look at Our Diverse and Engaging Program
- Celebrating Excellence: An Interview with Golden Egg Award Winner Christopher "CRob" Robinson
- Recognizing Excellence in OSS Community: Golden Egg Award Nominations Are Now Open!
- AI Cyber Challenge (AIxCC) and the Needle Linux Kernel Vulnerability – Part 1

- AI Cyber Challenge (AIxCC) and the Needle Linux Kernel Vulnerability – Part 2
- Learn How To Develop Secure Software!
- Why are Organizations Struggling to Implement Secure Software Development?
- A Deep Dive into SBOMit and Attestations
- Know Your Regular Expressions: Securing Input Validation Across Languages
- July in NYC: Join Us at the United Nations' (UN's) OSPOs for Good 2024 Conference & the "What's Next for Open Source?" Event
- OpenSSF GUAC Tech Talk Highlights
- Final Call: Submit your Technical Initiatives (TI) Funding Request by June 7th, 2024
- The OSS Security Adventure: Exploring the Frontlines of OSS Security through SOSS Policy Summit, RSA Conference, and Japan Meetup
- Beyond the OpenSSF: An Introduction to Other Security Efforts Across the Linux Foundation
- The Opportunity for DEI Participation in the Security Industry (And OpenSSF)
- OpenSSF Joins Open Source Consortium To Define E.U. CRA Security Specifications
- Join Our Upcoming OpenSSF Tech Talk: Proactive Supply Chain Security with GUAC
- Call for Proposals: Submit to Speak at SOSS Community Day Europe
- Unlock the Keys to Improved Software Security
- Recap of SOSS Community Day North America 2024
- Join Us at the OSS Security Meetup in Tokyo, Japan With General Manager Omkhar + SOSS Community Day North America Event Report
- Open Source Security (OpenSSF) and OpenJS Foundations Issue Alert for Social Engineering Takeovers of Open Source Projects
- Unveiling the Golden Egg Award Winners: Celebrating Excellence in Open Source Security
- Sessions You Won't Want to Miss at SOSS Community Day NA and Open Source Summit North America 2024
- "What's in the SOSS?" Podcast is Now Live
- Join us for a TTX: Securing OSS & Empowering Maintainers
- xz Backdoor CVE-2024-3094
- VulnCon 2024 Wrap-up: Securing the Ecosystem through Global Cooperation
- How Intel Uses OpenSSF Scorecard To Better Secure Its Software Portfolio
- Empowering Women in Tech: An Interview on Angela Jeffrey's Journey to Cybersecurity
- OpenSSF Scorecard Tech Talk Highlights
- Driving Change Together: The OpenSSF Takes On VulnCon
- Sigstore Graduates: A Monumental Step Towards Secure Software Supply Chains
- Join OpenSSF for our First Tabletop Exercise (TTX) at SOSS Community Day North America
- How OpenSSF Technical Initiatives Can Receive Strategic Funding
- OpenSSF Releases Plan for Improving Software Developer Security Education

- The India Initiative: An OpenSSF Awareness Program for a Secure Future
- OpenSSF Marketing Advisory Council Aims to Shape the Future of Open Source Security Advocacy
- Participate in Our Survey on Secure Software Development Education!
- OpenSSF and CISA Join Forces to Secure Open Source Software
- Graph for Understanding Artifact Composition (GUAC): Joins OpenSSF as Incubating Project
- OpenSSF Scorecard: Evaluating and Improving the Health of Critical OSS Projects
- Come to First OpenSSF Tech Talk of the Year on Scorecard
- Golden Egg Award: Celebrating Exceptional Contributions in the OpenSSF Community
- SOSS Community Day North America (NA) Agenda Live
- OpenSSF Supports White House's Efforts to Build More Secure and Measurable Software
- Submit to Speak at SOSS Fusion 2024
- OpenSSF Responds to US CISA RFI on Cybersecurity Risk and Secure by Design Software
- Scaling Up Supply Chain Security: Implementing Sigstore for Seamless Container Image Signing
- Alpha-Omega 2023 Annual Report
- Linux Kernel Achieves CVE Numbering Authority Status
- Announcing the First Ever SOSS Fusion Conference: How You Can Get Involved
- OpenSSF Participates in Department of Commerce Consortium Dedicated to AI Safety
- OpenSSF Securing Software Repositories Working Group Releases Principles for Package Repository Security
- Time is of the Essence to Mitigate Vulnerabilities like Leaky Vessels
- Post-Quantum Cryptography Alliance Launch
- CVE-2023-6246 Root Access Vulnerability in glibc
- OpenSSF Champions a More Secure Future in Collaboration with Public Sector
- Maintainer Motivations, Challenges, and Best Practices on Open Source Software Security
- OSS Security Sessions & FOSDEM Survival Guide
- Introducing gittuf: A Security Layer for Git Repositories
- Submit to Speak at SOSS Community Day North America 2024
- OpenSSF Election Results for Technical Advisory Council and Representatives to the Governing Board

Guest Blogs

Guest blogs are an integral part of the OpenSSF community, offering a platform for members to contribute their voices and expertise. These blogs highlight project updates, new innovations, and personal perspectives from those actively working on the front lines of open source security. By inviting community members to share their stories and insights, we enrich the dialogue around securing open source software and emphasize the power of collaboration in tackling today's cybersecurity challenges.

- Red Hat's Collaboration with the OpenSSF and OSV.dev Yields Results: Red Hat Security Data Now Available in the OSV Format
- OpenSSF Adds Minder as a Sandbox Project to Simplify the Integration and Use of Open Source Security Tools
- New Guide for Package Repositories to Adopt Trusted Publishers
- Neo Malware: Malicious Open Source Packages
- How to Make Programming Language Package Repositories More Secure
- Chainguard Enhances Security With OSV Advisory Feed
- Improving OpenSSF Scorecard Scores: StepSecurity Automation for Four Key Checks
- An Open Source Approach to Threat Mitigation in AWS
- Ubuntu Security Notices Now Available in OSV
- Introducing Artifact Attestations—Now in Public Beta
- Enhancing Open Source Security: Introducing Siren by OpenSSF
- Where Does Your Software (Really) Come From?
- DruBOM: An SBOM for Drupal
- Spotlight on the OpenSSF AI/ML Working Group
- Beyond Scores with OpenSSF Scorecard: Granular Structured Results for Custom Policy Enforcement
- Static Binary Analysis: A Final Exam for Software Supply Chain Protection

Case Studies

Case studies serve as powerful testimonials, highlighting how organizations have successfully adopted OpenSSF tools and technologies to enhance their cybersecurity measures. These real-world examples demonstrate the tangible benefits of participating in the OpenSSF ecosystem, showing how collaboration and the use of open source solutions can lead to significant advancements in software security.

- Case Study: Kusari's Implementation of OpenSSF Tools and Services
- Innovative Supply Chain Security for Enterprise Cloud Platform Service
- OpenSSF Case Study: Enhancing Open Source Security with Sigstore at Stacklok
- Introducing Artifact Attestations—Now in Public Beta
- How Intel Uses OpenSSF Scorecard To Better Secure Its Software Portfolio
- Scaling Up Supply Chain Security: Implementing Sigstore for Seamless Container Image Signing

Tech Talks

OpenSSF Tech Talks provide a platform for the community to showcase projects, tools, and innovations, fostering collaboration and driving thought leadership in open source security. Explore this year's talks for inspiration and submit your idea for 2025 to share your work and spark discussions within the OpenSSF community!

JUMPSTART YOUR JOURNEY: MASTERING OSS SECURITY DEVELOPMENT WITH THE LINUX FOUNDATION EDUCATION (2024-10-10)

On-demand video is available.

PROACTIVE SUPPLY CHAIN SECURITY WITH GUAC (2024-06-06)

On-demand video is available.

BUILDING A STRONGER OPEN SOURCE ECOSYSTEM: OPENSSF SCORECARD (2024-03-13)

On-demand video is available.

India Initiative

This year, OpenSSF deepened its engagement with the open source community in India through live streams, meetups, and events like Security Samvad in Pune, CNCF Meetups, and IndiaFOSS 2024. These activities provided hands-on insights into open source security, allowing us to connect with developers and contributors across the region. Looking ahead, OpenSSF is excited to expand its reach in India, fostering collaboration and building a secure open source ecosystem together.

Live streams

MARCH:

- Let's Chat Open Source Security
- How To Secure Open Source Code

APRIL:

- Techniques & Tools: PINNY
- Tools & Techniques: BOLT

MAY:

- Supply Chain Security: Fundamentals and more...
- Building A Culture Of Security

JUNE:

- SLSA, A Security Paradigm For Your Builds
- Tips, Tricks, and Techniques to Ace Supply Chain Security

In-person meetups

MAY:

- May 4th Security Samvad in Pune (with a focus on OpenSSF Scorecard)

JULY:

- Jul 25th Accel Cybersecurity Summit

AUGUST:

- Aug 31st CNCF Aug Meetup: Security Theme (with a focus on GUAC)

OCTOBER:

- Oct 19th CNCF New Delhi Meetup: Secret to Cloud Native Security
- Oct 26th Observability Marathon By-Two Edition - AWS UG Bengaluru x New Relic Oct meet-up

Talks

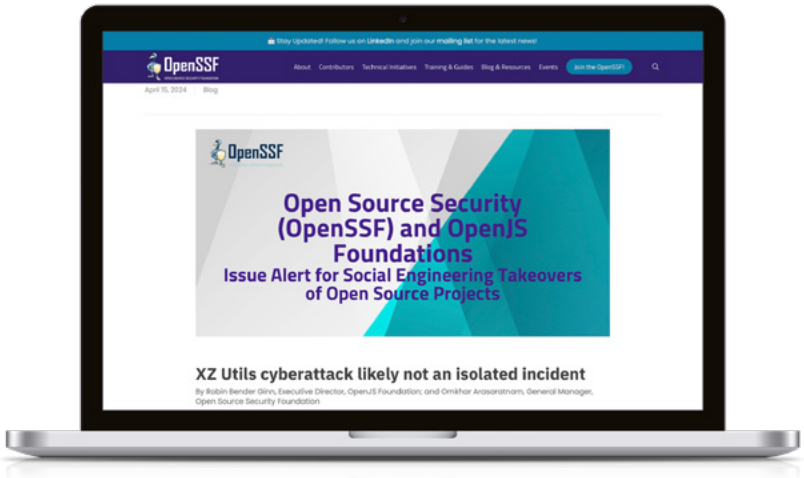
- Is What You See, What You Deploy? AllDayDevOps conference
- Scorecard: Assessments Made Easy KubeCon Hong Kong
- Security: Shift Left, or Swipe Left? DevOpsDays Kerala

Other Events

- IndiaFoss 2024 (Bengaluru, 7th - 8th Sep 2024)

Website

TOP WEB PAGE
Secure Software Development Fundamentals Courses



TOP BLOG POST
Open Source Security (OpenSSF) and OpenJS Foundations Issue Alert for Social Engineering Takeovers of Open Source Projects

Newsletter

8,833
SUBSCRIBERS

19.85%
AVERAGE OPEN RATE

14.93%
AVERAGE CLICK THROUGH RATE

215,671
TOTAL VIEWS

YouTube

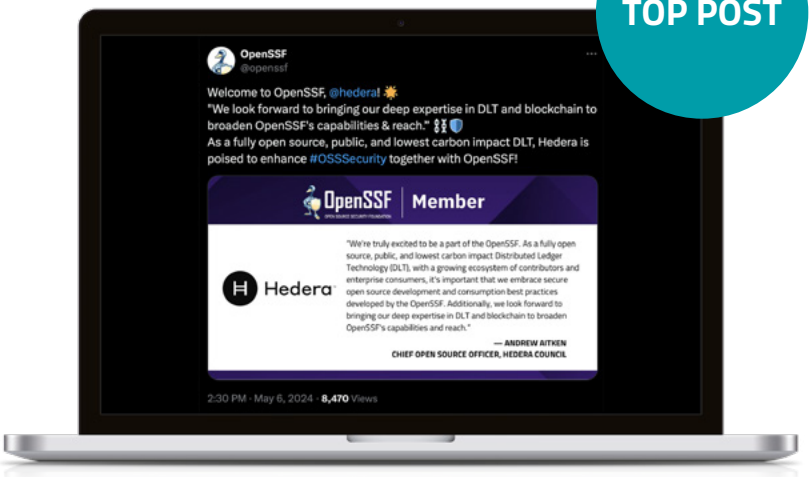
65,559 VIEWS

MOST WATCHED VIDEO
Open Source Security Foundation (OpenSSF) - Who We Are

1.34K SUBSCRIBERS
(49.22% YOY GROWTH)

988 VIDEOS

X



TOP POST

5,574 FOLLOWERS
(+19.25% YOY GROWTH)

551 POSTS

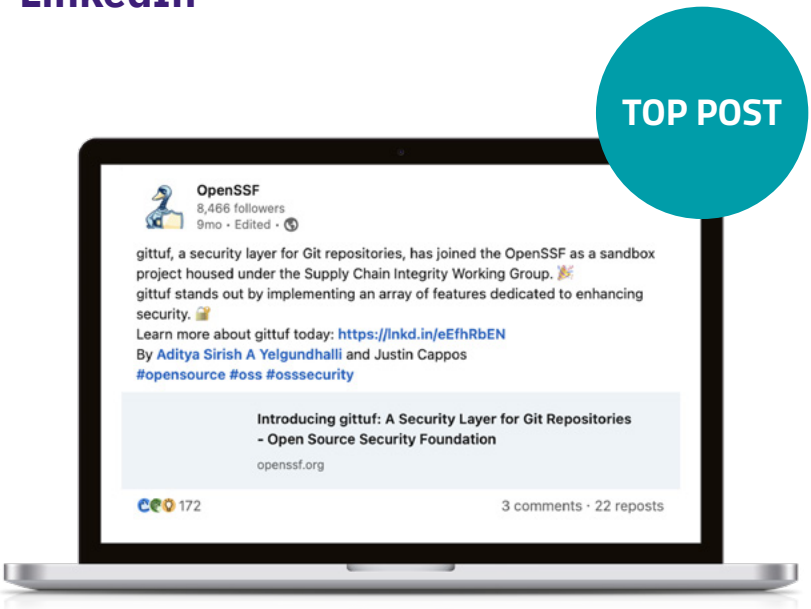
2,180 INTERACTIONS

Mastodon

895 FOLLOWERS

375 POSTS

LinkedIn



8,459 FOLLOWERS
(+98.38% YOY GROWTH)

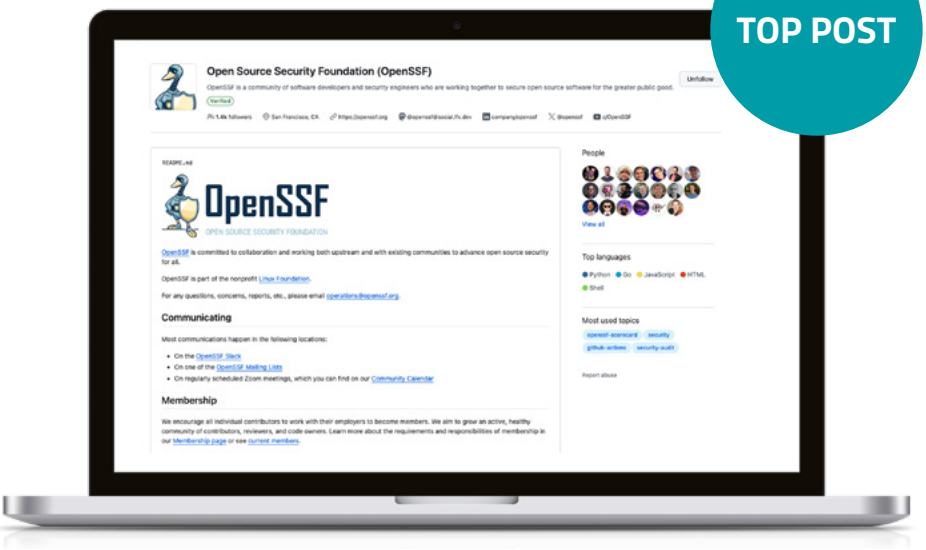
523 POSTS

500,861 IMPRESSIONS

10,067 INTERACTIONS

65 REPOS AND
1398 ACTIVE CONTRIBUTORS

GitHub



1.3K FOLLOWERS
(+52.42% YOY GROWTH)

1,398 CONTRIBUTORS

65 REPOS

18 PROJECTS

77 TEAMS

133 PEOPLE

180 ISSUES

420 PULL REQUESTS

Slack

3,822 USERS

Training & Education - LF Education

SCHOLARSHIPS TO SUPPORT WOMEN IN JORDAN ENTERING THE CYBERSECURITY FIELD

This year, OpenSSF, Linux Foundation Education, and Cloud Native Computing Foundation (CNCF) have teamed up with the US White House National Security Council (NSC) to launch a pilot program offering 250 free security courses and certifications to women in Jordan, including specialized certifications in Kubernetes and Cloud Native Security. Sponsored by OpenSSF and LF T&C, this initiative underscores the commitment to advancing open source security, promoting diversity, equity, and inclusion in cybersecurity, and addressing workforce challenges by empowering women in Jordan with valuable, complementary certifications.

Learn more about this initiative: [OpenSSF, Linux Foundation Training & Certification, and CNCF Announce Scholarships to Support Women in Jordan Entering the Cybersecurity Field in Collaboration with US White House National Security Council]

2024 Enrollment for Secure Software Development Courses

We had a great year helping people learn how to create more secure software. We far exceeded our goal to have 20% more people (7,990) enroll this year in our "Developing Secure Software" (LFD121) free course as compared to last year. Even more took its edX equivalent (LFD104x, LFD105x, and LFD106x). Over 1,000 have taken our courses on Sigstore and OpenSSF Scorecard.

Developing Secure Software - LFD121
2024 - Enrollment: 8,186
Total 2022-2024 Enrollment: 19,980

Securing Your Software Supply Chain with Sigstore - LFS182x
2024 - Enrollment: 91
Total 2022-2024 Enrollment: 1,551

Securing Projects with OpenSSF Scorecard - LFEL1006
2024 - Enrollment: 852
Total 2023-2024 Enrollment: 1,254

Secure Software Development: Requirements, Design, and Reuse - LFD104x
2024 - Enrollment: 1,213
Total 2020-2024 Enrollment: 7,031

Secure Software Development: Implementation - LFD105x
2024 - Enrollment: 605
Total 2020-2024 Enrollment: 3,592

Secure Software Development: Verification and More Specialized Topics - LFD106x
2024 - Enrollment: 477
Total 2020-2024 Enrollment: 3,279

**These numbers have been updated as of November 18, 2024.*

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Making Headlines

Over the past few years, OpenSSF built a solid reputation within the technical community as a trusted resource for best practices and guidance in open source security principles. Our mission for 2024 has been to build on this legacy of influence while extending our reach to publications with greater authority and larger audiences.

This year, we've dramatically increased visibility for the OpenSSF brand as well as OpenSSF projects, programs, members and collaborations. We've established the organization as a resource for expertise, not just on technical topics, but public policy and global trends, such as AI. We've seen more organic mentions of organization projects, research and content than ever before.

The following media highlights showcase the breadth of coverage and reach OpenSSF has achieved this year. With each placement, we elevate our mission to advance open source security and extend our impact across industries and around the world.

Success Metrics

110%

More than doubled the amount of coverage in just 9 months of 2024 (110% increase)

215%

More than tripled the amount of OpenSSF project coverage in just 9 months (215% increase)

>20M

12 media placements in publications with a potential audience of >20 million

>50M

6 media placements in publications with a potential audience of >50 million

10k

Nearly 10,000 social shares of articles mentioning OpenSSF

11

11 press releases announcing new projects, members, collaborations and milestones

Top Campaigns

Thought leadership regarding major vulnerabilities and cybersecurity incidents, such as XZ Utils, OpenSSH, PyPi, and others

OpenSSF launches Siren, the industry's first OSS intelligence resource

LF and OpenSSF publishes research about secure software development education

OpenSSF's participation in the DARPA AI Cyber Challenge

OpenSSF Partners With DHS and CISA to Launch Global Software Supply Chain Project

OpenSSF adds interactive Labs to LFD 121

Media Highlights

Washington Post (138.9M monthly views)
Hackers race to win millions in contest to thwart cyberattacks with AI
OpenSSF founder Brian Behlendorf discussed the importance of open source security as part of a larger story about the DARPA AI Cyber Challenge.

NPR
The Hack that Almost Broke the Internet
Former OpenSSF GM Omkhar Arasaratnam spoke with NPR about the XZ Utils backdoor vulnerability, saying: "I guess this is one of the failure modes of how society has consumed open source. The overhead of having to deal with this stuff can become overwhelming."

Politico (52M monthly views)
Hacking The Gender Gap
Regarding the National Security Council's partnership with OpenSSF and Linux Foundation, which is providing 250 free cybersecurity courses and certifications to Jordanian women, Anne Neuberger, deputy national security adviser for cyber and emerging technology, said, "This will equip women in Jordan with crucial skills and contribute to national security."

Reuters (84M monthly views)
Open source groups say more software projects may have been targeted for sabotage
OpenSSF and OpenJS issued a statement showing the attempt to insert a secret backdoor into XZ Utils was not an isolated incident and that there were multiple JavaScript projects that were also being targeted.

Fortune (36.3M monthly views)
After a failed Linux backdoor attempt grabs headlines, open source leaders warn of more attacks
OpenSSF and OpenJS were quoted regarding XZ Utils and subsequent attacks: "These social engineering attacks are exploiting the sense of duty that maintainers have with their project and community in order to manipulate them. Pay attention to how interactions make you feel. Interactions that create self-doubt, feelings of inadequacy, of not doing enough for the project, etc. might be part of a social engineering attack."

Gizmodo (16.8M monthly views)
Open source Cybersecurity Is a Ticking Time Bomb
OpenSSF and OpenJS were quoted regarding XZ Utils and subsequent attacks: "These social engineering attacks are exploiting the sense of duty that maintainers have with their project and community in order to manipulate them. Pay attention to how interactions make you feel. Interactions that create self-doubt, feelings of inadequacy, of not doing enough for the project, etc. might be part of a social engineering attack."

Other Reports

The Economist, Why is so much of the internet's infrastructure run by volunteers?,(April 23, 2024)

Axios, 1 big thing: Open source developers face a potential crisis, (April 19, 2024)

Quartz, Open source cybersecurity could derail the internet as we know it, (May 10, 2024)

The Register, OpenSSF sings a Siren song to steer developers away from buggy FOSS, (May 20, 2024)

The Hacker News, New OpenSSH Vulnerability Could Lead to RCE as Root on Linux Systems, (July 1, 2024)

TechTarget, Linux group announces Post-Quantum Cryptography Alliance, (Feb. 6, 2024)

CSO, Keeping up with AI: OWASP LLM AI Cybersecurity and Governance Checklist, (March 14, 2024)

Dark Reading, Under-Resourced Maintainers Pose Risk to Africa's Open Source Push, (July 22, 2024)

The New Stack, There Is Just One Way To Do Open Source Security: Together, (October 23, 2024)

ZDNet, Technologist Bruce Schneier on security, society and why we need 'public AI' models, (October 24, 2024)

SC Magazine, Crowdstrike: The Aftermath – PSW #836, (July 27, 2024)

TechStrong, Securing Open Source as Critical Infrastructure with Omkhar Arasaratnam at OSS Seattle 2024, (April 19, 2024)

SiliconANGLE, Enhancing open source security: Collaborative strategies from OpenSSF, (March 21, 2024)

InfoSecurity Magazine, RSAC: Three Strategies to Boost Open source Security, (May 8, 2024)

Help Net Security, One-third of dev professionals unfamiliar with secure coding practices, (July 19, 2024)

InfoQ, Sigstore: Secure and Scalable Infrastructure for Signing and Verifying Software, (Feb 29. 2024)

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Looking Ahead to 2025

As we step into 2025, we want to take a moment to express our heartfelt gratitude for all that our community has achieved. Open source software (OSS) is the backbone of global innovation, and securing it is a responsibility we all share. We are deeply thankful for each of you, whose dedication and hard work are helping to build a safer, more secure future. Together, we are making the world a better place, one line of code at a time!

Looking ahead, we're excited to keep building on this momentum by creating more opportunities to collaborate, connect, and innovate. The heart of OpenSSF's mission lies in this community, and we are committed to amplifying your voices and ensuring your contributions continue to make a lasting impact.

Fostering Collaboration

We'll continue bringing maintainers and organizations together through OpenSSF Community Days, meetups, and Tech Talks—spaces for meaningful discussions and real solutions to the security challenges we all face.

Scaling Community-Driven Efforts

In 2025, we're expanding opportunities for all of you to get involved in key projects like improving the Best Practices Badge, advancing Sigstore, and refining resources like the Compiler Options Hardening Guide. Your contributions—big or small—are what push us forward.

Growing Together

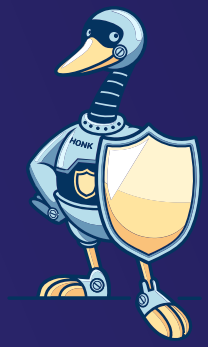
We'll also keep investing in initiatives that make it easier for everyone to get involved, learn, and grow, like the Developing Secure Software course and new resources for managers. With your continued support, we'll keep building a stronger, more secure open source ecosystem.

How You Can Get Involved

- **Join a Working Group**: Contribute to ongoing security initiatives. Get involved here.
- **Explore Membership**: Become a member of OpenSSF and shape the future of open source security. Explore membership opportunities.
- **Follow Us on Social Media**: Stay updated on the latest news by following us on LinkedIn, X, Bluesky, and Mastodon.
- **Subscribe to Our Newsletter**: Get the latest updates delivered straight to your inbox. Subscribe here.
- **Encourage Others to Get Involved in OpenSSF**: Our goals are ambitious yet vital, and we believe they resonate widely—join us in making a difference.

Let's work together to build a secure, resilient open source ecosystem. Join us today and help make 2025 our most impactful year yet!

— The OpenSSF Team



OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Let's work together to build a secure, resilient open source ecosystem. Join us today and help make 2025 our most impactful year yet!

openssf.org/getinvolved

openssf.org