



# 2025 Annual Report



[openssf.org](https://openssf.org)

# Contents

<b>Introductory Note.....</b>	<b>03</b>
<b>2025 By the Numbers .....</b>	<b>05</b>
<b>From the General Manager .....</b>	<b>07</b>
<b>About the OpenSSF .....</b>	<b>09</b>
<b>Community Helpers: Who to Ask for Support.....</b>	<b>10</b>
<b>2025 Membership &amp; Engagement Overview .....</b>	<b>11</b>
<b>Governing Board Members .....</b>	<b>14</b>
<b>From the Governing Board Chair .....</b>	<b>15</b>
<b>From the TAC Chair .....</b>	<b>17</b>
<b>Technical Advisory Council Members .....</b>	<b>18</b>
<b>Staff .....</b>	<b>19</b>
<b>2025 Wins &amp; Highlights .....</b>	<b>20</b>

<b>Working Groups / Projects .....</b>	<b>33</b>
AI/ML Security .....	34
Belonging, Empowerment, Allyship, and Representation (BEAR).....	35
Best Practices for Open Source Developers .....	36
Global Cyber Policy.....	37
Open Resources for Baselines, Interoperability, and Tooling (ORBIT).....	39
Securing Critical Projects .....	40
Securing Software Repositories .....	42
Security Tooling .....	43
Supply Chain Integrity .....	45
Vulnerability Disclosures.....	46
OpenSSF Projects and Affiliated Projects .....	47
<b>Community Engagement &amp; Education ....</b>	<b>50</b>
<b>Looking Ahead to 2026 .....</b>	<b>74</b>
<b>Acknowledgments.....</b>	<b>76</b>





# Introductory Note: Securing the Future of Open Source, Together

Welcome to the [Open Source Security Foundation \(OpenSSF\)](#) Annual Report. This year, we invite you to celebrate the progress, creativity, and collaboration that continue to shape a safer and more resilient open source community.

OpenSSF exists to make it easier to sustainably secure the development, maintenance, and consumption of open source software. Our community is grounded in shared values of openness, inclusion, and transparency. These principles remind us that security is not achieved in isolation but through collective effort – by learning together, sharing knowledge, and building trust across boundaries of discipline, geography, and experience. Every contribution, from a single pull request to a global initiative, strengthens the foundation on which our community continues to grow.

In 2025, our work continued to align with our strategic objectives: serving as a catalyst for change through secure-by-design development; educating and empowering the modern developer with resources that build security awareness and skill; and providing leadership across the community through standards, policy engagement, and partnerships that shape the future of open source security.

These goals are reflected across our four foundational pillars:

- **Education:** Expanding practical, accessible learning opportunities that raise the standard of secure development worldwide.
- **Community & Events:** Fostering collaboration through gatherings, workshops, and global conversations that connect and inspire contributors.
- **Policy & Public Sector Engagement:** Engaging constructively with governments and industry leaders to champion balanced, evidence-based approaches to digital trust and software security.
- **Programs & Projects:** Driving innovation through technical initiatives that produce actionable tools, frameworks, and guidance for secure open source software.

This report presents a comprehensive overview of OpenSSF's impact and the collective progress made throughout 2025. It highlights milestones, community initiatives, and technical achievements while addressing the evolving challenges of open source security. Readers will find insights from our leadership and working groups, updates on educational and policy initiatives, and a review of OpenSSF's expanding global presence across major industry events and collaborations. We can't wait for you to read this year's Annual Report and celebrate this year full of collective progress – a reflection of how far we've come and a reminder of the shared journey ahead to secure the future of open source, together.





# OpenSSF

OPEN SOURCE SECURITY FOUNDATION

## 2025 By The Numbers

**267+ active contributors**  
from **112 organizations**  
advancing open source security.



**10 Working Groups** and  
**32 Technical Initiatives**  
(including projects, affiliated projects,  
and SIGs).



**11 community events hosted**  
worldwide, from Seoul to  
Brussels to Atlanta.



ORBIT Working Group

- **20,000+** OSS repos scanned
- Security Insights up **200%** year-over-year.



Criticality Score calculates  
scores monthly for  
**500,000 projects**



 **Alpha-Omega**

- **\$5.8** million invested in 14 critical  
open source projects.
- **60+** audits and engagements completed





Nearly **20,000 course enrollments** across OpenSSF's free training programs. **5,700+ learners** enrolled in Understanding the EU Cyber Resilience Act (LFEL1001).



**117 member organizations** spanning **16 industries** (e.g., finance, cloud, AI, government, academia) and representation across **40+ countries**.



OpenSSF's community participated in **over 60 speaking engagements** across more than **20 external events** throughout the year.



**6.85M+ monthly reach** from the top 5 Media Highlights alone (ZDNET, The New Stack, Infosecurity Magazine, diginomica, Help Net Security).



The **OpenSSF Technical Advisory Council (TAC)** awarded **\$663,248** in funding across **14 Technical Initiatives** to strengthen the security and resilience of the open source software ecosystem.



Member companies collectively represent **\$5 billion in funding**, underscoring the scale and influence of the OpenSSF ecosystem.



### Securing Critical Projects

- **60+ critical OSS projects** received direct security uplift funding.
- **6 new threat models, 52 vulnerabilities fixed, 5 fuzzing frameworks** implemented.



### Malicious Packages

- Storing data on malicious packages across ecosystems
  - **66,000 NPM**
  - **10,000 PyPi**
  - **1,000 RubyGems**
  - **1,000 NuGet**



## From the General Manager

If there is one thing that defines the OpenSSF community, it is resilience.

This year reminded us that our strength does not come from any single project or company. It comes from all of you: the maintainers, developers, researchers, and advocates who show up every day to make open source safer and stronger.

### Building Together Through Change

Like many foundations, we have navigated an evolving landscape this year. The ecosystem faced shifting priorities, but instead of slowing down, our community leaned into the challenge.

Working groups shared resources, projects aligned around common goals, and contributors across the world kept the momentum going. That collective effort is what makes OpenSSF special. When obstacles appear, we do not pause. We collaborate.

### Highlights from a Year of Collective Wins

2025 has been a year of meaningful progress, grounded in the belief that education, tooling, and shared knowledge can move the industry forward.

**Education that Empowers:** We launched and expanded courses that reach developers, managers, and policymakers alike. Security for Software Development Managers (LFD125), Understanding the EU Cyber Resilience Act (LFEL1001), and the new Secure AI/ML-Driven Software Development (LFEL1012) are helping teams build security into every layer of software development.

**Guides and Whitepapers that Inform:** OpenSSF released two new guides and two new whitepapers that make complex topics like dependency management and AI security more approachable.

**Infrastructure and Tooling that Scale:** Across projects, contributors delivered improvements to open source security infrastructure — from strengthening dependency data pipelines to advancing tooling that developers use every day.

**Global Presence and Policy Impact:** We continued to engage governments and the public sector on cybersecurity, particularly through our work around the EU Cyber Resilience Act and the global AIxCC initiative.

OpenSSF's voice resonated at major events not only across North America, but also in Europe, India, Japan, and Korea, where we brought together local open source communities to share solutions and strengthen collaboration.



## Looking Ahead

As we move into 2026, our focus remains clear.

We will continue building the foundation for a secure and sustainable open source ecosystem.

We will keep investing in education, in tools that simplify secure development, and in the global relationships that help this work scale.

Most importantly, we will keep investing in people. This community is not just a network of projects; it is a network of trust, generosity, and shared purpose.

Every contribution, every review, and every piece of feedback makes open source stronger for everyone.

Thank you for showing up, for believing in collaboration, and for proving that together we can make open source security a lasting global good.

**Best regards,**  
**Steve Fernandez**  
**General Manager**  
**Open Source Security Foundation**





# About the OpenSSF

## About the Open Source Security Foundation (OpenSSF)

The [Open Source Security Foundation \(OpenSSF\)](#) is a cross-industry initiative under the [Linux Foundation](#) that brings together software developers, security engineers and organizations worldwide to secure open source software for the greater public good.

Founded in 2020, OpenSSF focuses on collaboration, best practices and tooling to make open source software more trusted, resilient and secure.

Visit [openssf.org](https://openssf.org) to learn how you can join, contribute or engage.

## 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](#), [Mastodon](#) and [YouTube](#).
- **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.



# Community Helpers - Who to ask for support

If you ever need guidance, have questions, or want to get involved, the following community leaders and representatives are great points of contact. You can also reach out in the OpenSSF Slack: <http://slack.openssf.org/>

## Community Leaders



**ZACH STEINDLER**

*OpenSSF TAC Chair and Principal Engineer, GitHub*



**BOB CALLOWAY**

*OpenSSF TAC Vice Chair & Head of Google's Open Source Security Team*

### Working Groups & Project Teams:

You can also direct questions to the leads of any OpenSSF Working Group or project team. They're closely involved with technical deliverables and community initiatives and are always happy to help new contributors!

## General Member Representatives



**TRACY RAGAN**

*CEO and Co-Founder, DeployHub (General Member Rep)*



**IAN DUNBAR-HALL**

*Chief Engineer, Lockheed Martin (General Mem Rep)*



**MICHAEL LIEBERMAN**

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

## Associate Member Representative



**REBECCA RUMBUL**

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





# 2025 Membership & Engagement Overview

OpenSSF's membership community continued to expand and diversify in 2025, reflecting the growing global recognition of open source security as a shared responsibility. With representation spanning cloud providers, semiconductor leaders, financial institutions, government partners, and open source focused startups, the Foundation now brings together one of the most comprehensive ecosystems addressing software supply chain security.

Over the past year, OpenSSF strengthened engagement through new Member Success programs, expanded collaboration with government and policy stakeholders, and introduced opportunities for members to shape AI security strategy, CRA readiness, and global vulnerability disclosure frameworks.

The Foundation also refined its membership structure to align with organizational growth and scale, ensuring sustainable support for key initiatives while delivering increased visibility, influence, and impact for members.

Through this evolution, OpenSSF remains committed to its mission: serving as a neutral, trusted home for collaboration and advancing the security of the open source software.

In 2025, OpenSSF was proud to announce the addition of several new members to its growing community:

## General Members



## Associate Member



## Meet Our Members

### Premier Members



### General Members



### Associate Members



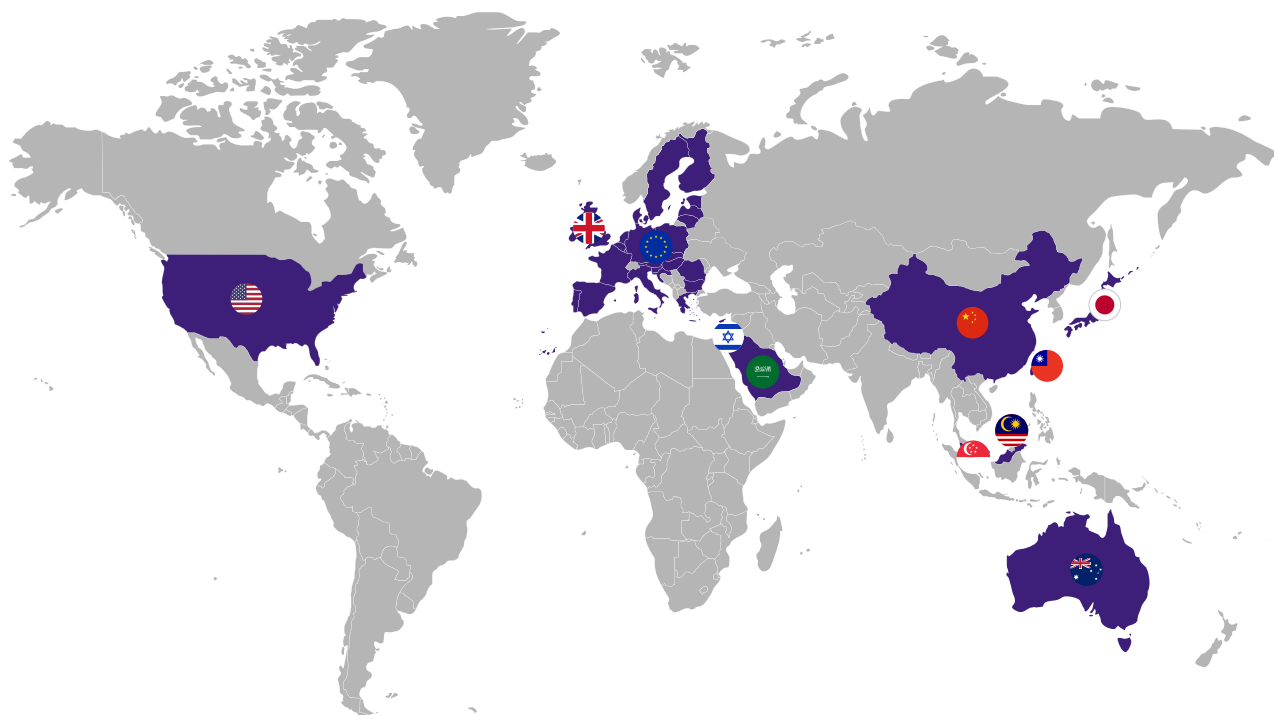
### Join OpenSSF Today

As OpenSSF continues to advance global collaboration on open source security, the role of our members has never been more critical. We invite organizations across every sector; cloud, finance, government, AI, manufacturing, and open source development, to join us in shaping the future of secure software.

Membership provides a direct voice in our technical direction, policy engagement, and global advocacy efforts, while connecting your teams with the leading experts driving solutions to today's most urgent software security challenges.

Join the OpenSSF community and be part of the collective effort securing the foundation of our digital future.

### Member Geography



### Member Industries



# Governing Board Members



**BRIAN FOX**  
CTO, Sonatype



**EMILIO ESCOBAR**  
Chief Information  
Security Officer, Datadog



**ERIC BREWER**  
VP of Infrastructure &  
Google Fellow, Google



**GRAHAM HILL**  
Managing Director, Cybersecurity  
& Technology Controls at  
JPMorgan Chase & Co.



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



**JAMIE THOMAS**  
Chief Client Innovation Officer  
and Enterprise Security  
Executive, IBM



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



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



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



**KELLY ANN**  
Cloud Infrastructure Security  
Engineer, Apple



**MARK RUSSINOVICH**  
OpenSSF Board Chair & 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 LINKSVAYER**  
Vice President of Developer  
Policy, GitHub



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



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



**ROY CROWDER**  
Executive Director -  
Morgan Stanley



**SCOTT SCHENKEIN**  
VP, Distinguished Engineer Cyber  
Security, Capital One



**TRACY RAGAN**  
CEO and Co-Founder, DeployHub  
(General Member Rep)



**VINCENT DANEN**  
Vice President of Product  
Security, Red Hat

## From the Governing Board Chair

This past year has marked great progress for open source security and highlighted OpenSSF's contribution to enhancing the reliability of global software infrastructure. The concept of *secure by design* is increasingly being implemented as a tangible standard across various sectors. OpenSSF remains committed to bringing together developers, enterprises, and governmental bodies to advance this common objective.

### Strengthening the Foundation of Software Security

If 2024 was the year the community proved that collaborative security works, 2025 has been about scaling it. OpenSSF projects have demonstrated measurable impact across various industries, as evidenced by Lockheed Martin's implementation of Bomctl for SBOM management, Kaggle's adoption of Sigstore for signing AI models, Defense Unicorns' integration of Zarf and GUAC, and Docker Hub utilization of OpenSSF tools and standards to strengthen security at the source, enabling organizations to safeguard their pipelines from development through production. Progress has also been made in software attestation and verifiable builds, with insights from confidential computing and hardware-based security being leveraged to enhance open source ecosystems.



### Responding to a Changing Threat Landscape

Attackers are getting more sophisticated, targeting not just code but the trust networks that sustain open source. In 2025, the open source community was rocked by large-scale supply chain attacks in which attackers compromised maintainer accounts and injected malicious code into highly popular packages downloaded billions of times each week. OpenSSF responded with updated best practices, community guidance, and stronger partnerships with public agencies and package registries.

### Enabling AI-Secure Development

AI has changed how developers write and ship code. It has also introduced a new set of risks. Initiatives such as the Secure AI/ML-Driven Software Development course (LFEL1012) and the broader OpenSSF AI Security efforts, including the AI Cyber Challenge (AIXCC), exemplify a commitment to advancing secure development practices. These resources enable developers to understand the responsible use of AI tools and to safeguard data, models, and pipelines throughout the software development lifecycle.

Looking ahead, OpenSSF will continue exploring how confidential computing, trusted execution, and privacy-preserving techniques can further secure AI workflows.

## A Global Community That Keeps Growing

Our community has never been stronger. This year we hosted five Community Days across three continents, launched new working groups focused on global cyber policy and the OSPS Baseline. We also deepened collaboration with governments and international standards bodies to ensure open source perspectives are represented in evolving regulations like the EU Cyber Resilience Act and the U.S. Secure Software Development Framework.

## Looking Forward

Open source forms the backbone of modern computing, bringing with it a collective responsibility to ensure its security and sustainability. Throughout my career, I have been deeply engaged in advancing cybersecurity for both closed and open source software. My involvement in co-founding OpenSSF in 2019, contributing to the vision for confidential computing, and helping launch the Confidential Computing Consortium in 2018 has given me firsthand insight into the evolving landscape of secure software development. These experiences, along with initiatives like making Microsoft's Secure Supply Chain Consumption Framework (S2C2F) available to OpenSSF and guiding Microsoft's Secure Future Initiative, reflect a consistent commitment to aligning industry efforts with open source standards and addressing broad security challenges.

As Chair, my focus is on supporting OpenSSF's mission to address the changing needs of our industry. Looking ahead, OpenSSF will continue to establish and promote standards and tools that empower everyone, from major corporations to individual project maintainers—to develop and use software designed with security at its foundation. By setting benchmarks for controls, repository management, maintainer practices, and build pipelines, we aim to create clear, transparent measures that make software integrity verifiable at every stage. With these standards in place, developer tools can help automatically validate software, reducing manual effort and enhancing trust in the ecosystem.

In addition, OpenSSF is committed to building tooling and systems that enable the community to respond quickly and collaboratively to critical open source vulnerabilities. This approach not only strengthens resilience but also fosters trust throughout the open source ecosystem. By supporting sustainable infrastructure for package managers and working closely with governments and standards bodies to address evolving regulations like the Cyber Resilience Act, OpenSSF is helping to ensure that open source remains innovative, secure, and accessible for all.

What inspires me most is the dedication and ingenuity of this community. The progress we've made together is a testament to the power of collaboration. Thank you to every contributor, member, and partner who continues to make OpenSSF's mission possible.

**Mark Russinovich**  
**OpenSSF Board Chair & Azure CTO and Technical Fellow,**  
**Microsoft**



## From the TAC Chair

Hello OpenSSF Community!

2025 has been a year of ups and downs.

In the public sector, lots of maintainers and consumers of open source software have questions about the European Union Cyber Resilience Act (EU CRA), which is why in 2025 we put together [high-level guidance](#) and a [free course on understanding the EU CRA](#).

We also collaborated with several package repositories on a wide variety of security capabilities, including the release of trusted publishing to [crates.io](#), [npm](#), and [NuGet](#). Trusted publishing helps get passwords and long-lived API keys out of build pipelines, which has [become a target for attackers](#). Package repositories are central to open source and are seeing increasing demands which may require changing their operating model, which we outlined in our open letter [Open Infrastructure is Not Free](#).

This year saw the release of the [SLSA v1.1 specification](#) and we're continuing to see excitement around attestations as the key to understanding your software supply chain security. Sigstore is an incredibly popular way to sign those attestations (without having to manage long-lived keys) and the [Sigstore public good instance transparency log](#) saw an explosion in growth from 5-6 million unique identities per month in January to 14-15 million unique identities per month in September.

We also saw the [adoption of Sigstore in signing AI models including NVIDIA's NGC Catalog](#) based on the [model signing specification](#) of the AI/ML Security Working Group. It was a busy year for AI as we saw the [conclusion of the AI Cyber Challenge](#) to build cyber reasoning systems that demonstrate how LLMs and other AI advances can help defenders keep pace with attackers.

Last but not least, the TAC (in collaboration with staff) [revamped the funding process for OpenSSF technical initiatives](#). In 2024 we funded 5 proposals with \$100,000 and in 2025 we expanded that to funding 14 proposals with \$663,248.00. These proposals spanned security audits, a mentorship program, technical writers, design assistance, and development work, showcasing how OpenSSF technical initiatives are maturing over time, reflected in their evolving needs as they are adopted by wider communities.

Where do we go from here? You needn't worry that we've solved all the problems in securing open source. There's lots to look forward to in 2026, but let's not forget all of our 2025 accomplishments, even when we know there's so much more to do.

More than anything else, what I took away from 2025 is the importance of community. All the security capabilities in the world don't matter unless we're working together towards our common goal of securing open source. There's amazing energy in the OpenSSF, at conferences, in video calls, over online chats, and I can't wait to see what 2026 brings.

See you online,

**Zach Steindler**  
**OpenSSF 2025 TAC Chair**



## Technical Advisory Council Members

The Technical Advisory Council (TAC) develops the overall technical vision and provides oversight of the OpenSSF technical communities. Its functions include:

- Approving, establishing, structuring, organizing, and archiving Technical Initiatives.
- Establishing community norms, workflows, or policies that are not within the scope of any single project.
- Resolving technical matters that affect multiple projects.
- Coordinating cross-project opportunities.



**ZACH STEINDLER**

*OpenSSF TAC Chair and Principal Engineer, GitHub*



**BOB CALLAWAY**

*OpenSSF TAC Vice Chair & Head of Google's Open Source Security Team*



**ARNAUD LE HORS**

*Senior Technical Staff Member - Open Technologies, IBM*



**GEORG KUNZ**

*Open Source Manager - Open Source Program Office - CTO Office, Ericsson*



**JAUTAU "JAY" WHITE**

*Open Source Software and Supply Chain Security Strategy, Microsoft*



**MARCELA MELARA**

*Research Scientist, Intel Labs*



**MICHAEL LIEBERMAN**

*Co-Founder & CTO, Kusari*



**MICHAEL SCOVETTA**

*Principal Security PM Manager, Microsoft*



**STEPHEN AUGUSTUS**

*Technical Architect — Office of the CTO, Bloomberg*



## OpenSSF Staff



**STEVE FERNANDEZ**  
*General Manager*



**ADRIANNE MARCUM**  
*Chief of Staff*



**CHRISTOPHER ROBINSON (CROB)**  
*Chief Technology Officer/Chief  
Security Architect*



**DAVID A. WHEELER**  
*Director, Open Source Supply  
Chain Security*



**JEFF DIECKS**  
*Technical Project Manager*



**KRIS BORCHERS**  
*Technical Project Manager*



**STACEY POTTER**  
*Manager of Community*



**MADALIN NEAG**  
*EU Policy Advisor*

## OpenSSF Support Staff



**ANGELAH LIU**  
*Associate Manager,  
Communications & Marketing*



**JOHN NIRO**  
*Membership Solutions*



**KATE POWELL**  
*Program Manager*



**NAOMI WASHINGTON**  
*Program Manager*



**RAM IYENGAR**  
*Community Engagement Lead, India*



**REDEN MARTINEZ**  
*Project Coordinator*



**SALLY COOPER**  
*Senior Manager,  
Communications & Marketing*



**SUSAN REMMERT**  
*Project Marketer*

# 2025 Wins & Highlights

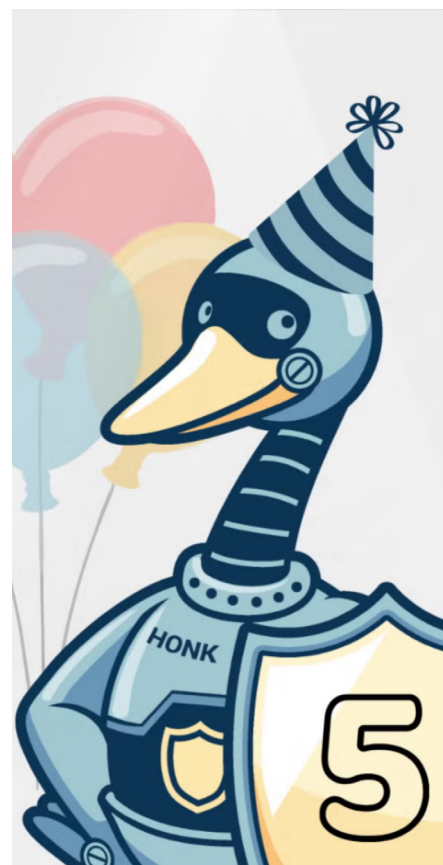
## Foundation-Wide Wins

In 2025, OpenSSF celebrated its five-year anniversary, making significant strides in improving open source security. Key achievements included launching the [Cybersecurity Skills Framework](#) and [Open Source Project Security \(OSPS\) Baseline](#), forming new working groups (ORBIT, Global Cyber Policy), and hosting global events like OpenSSF Community Days and Open Source SecurityCon. The community grew with eight new members and one upgrade, and the OpenSSF Scorecard project underwent a security audit.

Education expanded with new courses on [Security for Software Development Managers \(LFD125\)](#), [Understanding the EU Cyber Resilience Act \(CRA\) \(LFEL1001\)](#), and [Secure AI/ML-Driven Software Development \(LFEL1012\)](#), alongside mentorship programs for projects like gittuf and RSTUF.

Community engagement surged, with a 20% rise in website traffic, 44% growth in the LinkedIn community, and a 45% increase in YouTube subscribers. OpenSSF also broadened its social media presence to include Bluesky and spearheaded an open letter advocating for sustainable investment in open infrastructure.

Technically, OpenSSF funded 14 Technical Initiatives with over **\$663,000** in grants. New research and specifications were released, including the Model Signing (OMS) specification and whitepapers on AI Code Assistant Instructions, SBOM Data, and Visualizing Secure MLOps. These collective efforts demonstrate a maturing community's global impact on open source security.



## Education

### Software Security Education

Education is a key component of our pragmatic strategy for improving the security of open source software (OSS). We cannot hope to defend the digital commons without a massive and scalable effort to increase the practical security knowledge of software developers. The OpenSSF's education initiatives are designed to meet this critical need. While our focus is OSS, closed source software systems are mostly OSS components, are subject to the same attacks, and in many cases are developed by the same people. Therefore, most of our educational materials apply equally to closed source software.

In early 2025, OpenSSF and The Linux Foundation introduced the [Cybersecurity Skills Framework](#) to help organizations and individuals assess and strengthen essential security competencies across a range of technical and leadership roles. The framework maps 14 core IT job families across three proficiency levels and aligns with international standards such as DoD 8140, CISA NICE, and ICT e-CF. It now serves as the foundation for aligning OpenSSF's educational offerings with globally recognized cybersecurity skills and provides a structure for future course development and updates. Following its launch, a live [webinar](#) introduced the framework to hundreds of participants, demonstrating how it supports workforce development, compliance readiness, and open source security maturity assessments.

We created and released three new courses this year:

- [Security for Software Development Managers \(LFD125\)](#). This course focuses on what managers of software developers must know for effective leadership that leads to secure results. This includes strategic and process-oriented security decisions and the skills to look for in software developers.
- [Understanding the EU Cyber Resilience Act \(CRA\) \(LFEL1001\)](#). This course enables developers (including manufacturers and stewards) to understand this key change in the regulatory landscape, helping them navigate compliance and implement necessary controls.

The CRA is having a worldwide impact and it's important for all in software development to understand it.

- [Secure AI/ML-Driven Software Development \(LFEL1012\)](#). This course is for software developers and reviewers who want to strengthen their professional value by using AI assistants securely to produce more secure code and provide sharper reviews.

These are in addition to our existing courses. Our most popular course is "Developing Secure Software", which is available in English and Japanese on both edX (LFD104x & LFD104-JPx) and the Linux Foundation website (LFD121 & LFD121-JP). Considering only this year, our top courses by enrollment (as of 2025-10-22) were:

- [Developing Secure Software](#) (English & Japanese, on LF and edX)



**7,198 ENROLLMENTS**

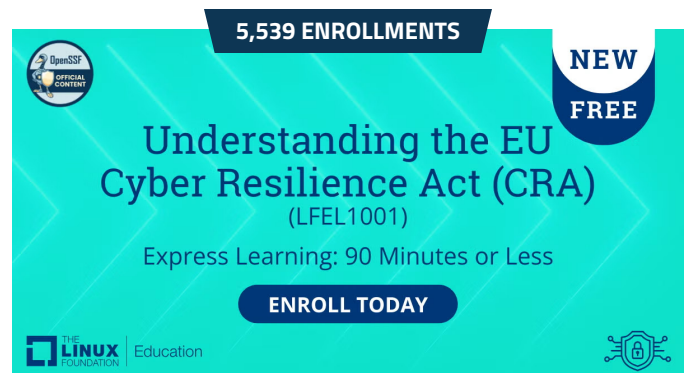
**FREE**

**Developing Secure Software**  
(LFD121)

**ENROLL TODAY**

THE LINUX FOUNDATION Education

- [Understanding the EU Cyber Resilience Act \(CRA\) \(LFEL1001\)](#)



**5,539 ENROLLMENTS**

**NEW FREE**

**Understanding the EU Cyber Resilience Act (CRA)**  
(LFEL1001)

Express Learning: 90 Minutes or Less

**ENROLL TODAY**

THE LINUX FOUNDATION Education

- [Security for Software Development Managers \(LFD125\)](#)



**1,475 ENROLLMENTS**

**NEW FREE**

### Security for Software Development Managers

(LFD125)

**ENROLL TODAY**

THE LINUX FOUNDATION Education

- [Securing Projects with OpenSSF Scorecard \(LFEL1006\)](#)



**841 ENROLLMENTS**

**FREE**

### Securing Projects with OpenSSF Scorecard

(LFEL1006)

Express Learning: 90 Minutes or Less

**ENROLL TODAY**

THE LINUX FOUNDATION Education

- [Securing Your Software Supply Chain with Sigstore \(LFS182\)](#)



**589 ENROLLMENTS**

**FREE**

### Securing Your Software Supply Chain with Sigstore

(LFS182)

**ENROLL TODAY**

THE LINUX FOUNDATION Education

\*Refer to the Education & Training section for additional course information.

The AI course LFEL1012 was released on 2025-10-16, and by 2025-10-31 it had already acquired 335 enrollments. We expect this brand-new course to have many more enrollments in the future, since AI is transforming software development and there are relatively few materials on how to use AI securely in software development.

These huge enrollment figures show that we're improving the education of thousands of developers, and through them, aiding millions of software users. We intend to extend our existing courses to better support the Cybersecurity Skills Framework and to create at least one more class that would further improve our support of that framework.

### Security Guides & Whitepapers

It is easy to become overwhelmed by the sheer volume of information. We have produced a variety of guides and whitepapers to provide simpler paths towards success. Here are some key guides and whitepapers grouped into three categories: AI/ML; CRA/SBOM; and general security best practices.

#### AI/ML

- [“Visualizing Secure MLOps \(MLSecOps\): A Practical Guide for Building Robust AI/ML Pipeline Security”](#): This whitepaper introduces a visual, layer-by-layer framework for integrating security across the machine learning lifecycle, adapting proven DevSecOps strategies for AI/ML environments and leveraging open-source tools like SLSA, Sigstore, and OpenSSF Scorecard.





- **[“Security-Focused Guide for AI Code Assistant Instructions”](#)**: This guide explains how to improve the security of code generated by AI assistants by creating clear and security-focused custom prompts or instructions, addressing potential risks from poorly written or inadequate inputs. This is a key supporting guide for the Secure AI/ML-Driven Software Development (LFEL1012) course and was co-developed by the AI/ML and Best Practices working groups.

### CRA/SBOM

- **[“Cyber Resilience Act \(CRA\) Brief Guide for OSS Developers”](#)**: This practical guide helps open-source developers and contributors understand the implications of the EU’s Cyber Resilience Act on their projects. It was co-developed by the Global Cyber Policy and Best Practices working groups.
- **[“Improving Risk Management Decisions with SBOM Data”](#)**: This document guides organizations on how to effectively use Software Bill of Materials (SBOM) data to make concrete risk-management decisions instead of being “generated to be ignored”.

### General Security Best Practices

- **[“Simplifying Software Component Updates”](#)**: A guide for component creators and users to simplify updates and avoid backward incompatibility issues. This guide was developed in part in response to concerns and issues raised at the [DC Policy Summit 2025](#).

## Community & Events

### Ecosystem Partnerships & Community Collaborations

#### Baseline and ORBIT: Raising the Bar for Open Source Security

In 2025, OpenSSF launched the [Open Source Project Security \(OSPS\) Baseline](#), a community-maintained framework that helps open source projects assess and demonstrate their security readiness. Released on **February 25, 2025**, the Baseline aligns with the **NIST Secure Software Development Framework (SSDF)**, the **EU Cyber Resilience Act (CRA)**, and **ISO 27001**, offering practical,

outcome-based guidance mapped to global standards.

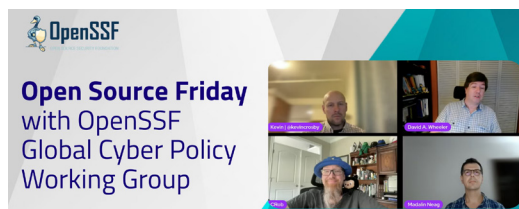
The Baseline defines three maturity levels and eight control categories, providing actionable recommendations on authentication, secure builds, and vulnerability management. A keynote at [Open Source Summit North America](#) and a [Tech Talk](#) highlighted how maintainers and organizations can apply it to align with standards and integrate security into everyday workflows.

The [ORBIT Working Group](#) maintains and extends the Baseline through related projects like Security Insights and Automation Integrations, helping maintainers publish project security data and track improvements over time. Together, the Baseline and ORBIT establish a common foundation for measurable, transparent open source security across the global ecosystem.

#### Collaboration with the GitHub Secure Open Source Fund

OpenSSF was recognized as an Ecosystem Partner in the [GitHub Secure Open Source Fund](#), a program dedicated to strengthening open source security by directly funding maintainers and providing expert guidance. Throughout the year, OpenSSF regularly engaged with GitHub’s Secure OSS cohorts to share security best practices, introduce key OpenSSF projects, and help maintainers improve the resilience of their codebases.

This collaboration also featured in GitHub’s Open Source Friday spotlight, where the OpenSSF Global Cyber Policy Working Group discussed the evolving landscape of cybersecurity regulations such as the EU Cyber Resilience Act (CRA). The session highlighted how community-driven initiatives like the OSPS Baseline and OpenSSF training courses are helping developers, maintainers, and policymakers navigate new compliance requirements. Read more in our blog: [Open Source Friday with OpenSSF – Global Cyber Policy Working Group](#).



## Events & Global Presence



2025 marked a milestone year for OpenSSF's global community engagement. Our presence grew significantly through expanding reach and deepening connections across continents.

### Hosted Events: Building Community Worldwide

Our flagship **OpenSSF Community Days** evolved into a truly global series, touching down on **four continents** and bringing together security practitioners, open source maintainers, and industry leaders. From **Tokyo to Denver, Amsterdam to Hyderabad, and Seoul**, these gatherings served as vital hubs for knowledge sharing and relationship building within regional open source security communities.

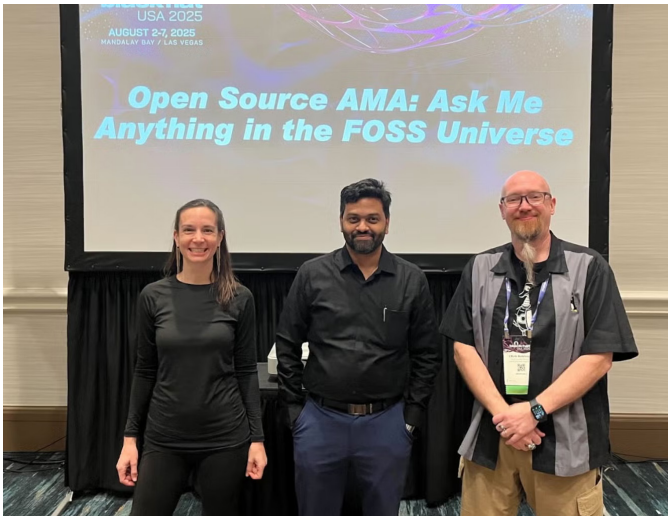
Each Community Day reflected the unique character of its region while reinforcing universal themes: the critical importance of securing the software supply chain, the power of collaborative defense, and the need for accessible security tooling and practices.

Building on this momentum, we co-hosted the inaugural **Open Source SecurityCon North America in Atlanta** alongside the Cloud Native Computing Foundation (CNCF), co-located with KubeCon/CloudNativeCon. This new conference represents an evolution in cross-project collaboration at scale within our open source security and the greater cloud native ecosystem.

### Amplifying Our Voice: Industry Engagement

Beyond our hosted events, OpenSSF's community participated in over **60 speaking engagements** across more than **20 external events** throughout the year. From **Black Hat** and **DEF CON** to regional meetups and specialized forums, our members shared insights, research, and practical guidance with diverse audiences.





We also deepened our engagement with vertical-specific communities through sponsored tracks, including sessions at the **Open Source in Finance Forum** and the **Linux Foundation EU Roadshow's CRA in Practice** sessions in **Belgium**.

### Regional Growth & Cross-Community Collaboration

Most significantly, 2025 demonstrated OpenSSF's commitment to authentic regional presence rather than mere global reach. Our expansion into Asia-Pacific markets – particularly the strong engagement in **Japan, India, and Korea** – reflects the truly international nature of open source development and the universal challenges facing software supply chain security. Co-locating with major open source events like Open Source Summit, KubeCon/CloudNativeCon, and OpenSearchCon enabled natural collaboration and cross-pollination of ideas between security-focused practitioners and the broader open source ecosystem, embedding security thinking throughout the development lifecycle.



As we look ahead, the foundation laid in 2025 – through consistent regional engagement, expanded event formats, and deepened industry partnerships – positions OpenSSF to continue growing as a truly global force for open source security.

**For detailed event information, please see the Community Engagement & Education: Events section.**

### Policy & Public Sector Engagement

#### Cyber Resilience Act (CRA): OpenSSF's Role & Impact

Around the world, governments are stepping up efforts to strengthen cybersecurity, including the U.S. Executive Order on Improving the Nation's Cybersecurity and the EU's Cyber Resilience Act (CRA). While these initiatives aim to make digital systems safer, some measures can unintentionally create challenges for those creating and using open source software (OSS). OpenSSF works with policymakers to build understanding and ensure that cybersecurity progress supports, rather than hinders, the open source community.

Following the [Open Source Software Stewards and Manufacturers Workshop in December 2024](#), OpenSSF launched a new Working Group: [Global Cyber Policy](#). Its goal is simple but ambitious: to stay closely connected with global cybersecurity regulations like the Cyber Resilience Act (CRA) and to make sure open source voices are part of those conversations.

Through its own initiatives and the work of its Standardization and Awareness SIGs, the group brings together experts who help shape practical policies and standards. The focus is on helping developers, companies, and governments meet security and compliance goals, not by adding red tape, but by sharing knowledge, tools, and collaboration opportunities. The group's work is built around a few core ideas:

- Growing education and awareness in the open source community,
- Engaging directly with the public sector to influence meaningful policy,
- Building and adapting tools that make compliance easier,
- Fostering operational collaboration across borders and organizations, all while protecting what makes open source thrive, the collaboration and innovation.

A key priority this year was to build stronger relationships in the European policy ecosystem. One of the biggest wins was deepening our partnership with ETSI, which opened new paths for participation and impact:

- Inside ETSI, OpenSSF now has direct representation and contributes to several standards that touch open source software.
- Through ETSI's *Mode 4* cooperation with CEN/CENELEC, we gained access to additional European standardization activities that were previously closed to most community groups.

This engagement has allowed OpenSSF to create awareness among its members about the latest updates in CRA-related standards and the progress of connected initiatives. Related to these initiatives, OpenSSF is one of the three foundations, recognized as a Type C Organization, actively participating in the [European Commission's CRA Expert Group](#). This group was created to meet the legal obligations of [CRA's Article 26](#) and "facilitate the co-operation and exchange of information and expertise between the Commission and stakeholders" (Group's Terms of Reference)

Additionally, OpenSSF has continued to enhance its informal partnership with BSI (Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security). We have reviewed their relevant works and enriched our Baseline tools with their frameworks. This partnership has been truly two-way - in response, OpenSSF's guidelines and works have been referenced across BSI's publications.

The OpenSSF community has delivered a series of well-regarded artifacts that help address specific stakeholders involved with the CRA. The first was a class created to help simply explain the CRA, the various terms, participants, and requirements. The [Understanding the EU Cyber Resilience Act \(LFEL1001\)](#) quickly became the most popular free class with the LF Education system, with thousands of participants signing up and taking the class within the first week it was offered, a trend that has continued throughout the year.

The next item to highlight is that the community also created a [Brief Guide for OSS Developers for the CRA](#). This concise document describes the law for open source developers and provides clear, simple, actionable advice on what they can expect as the law comes closer to enforcement. The OpenSSF has actively been working on assorted deliverables to support open source developers, open source stewards, as well as manufacturers to help them be prepared for the upcoming deadlines.

The group has held monthly meetings where assorted CRA concepts were discussed in-depth or tools were presented that could assist developers, stewards, and manufacturers to work towards their assorted obligations. These efforts are supported by our deepening relationships within the European standardization community.

OSS is global, so while Europe is important, we have taken other policy-related steps as well. In early 2025 the OpenSSF held a policy summit in Washington, DC. Issues raised and discussed in that forum led to the creation of a new OpenSSF guide ("Simplifying Software Component Updates"). We participated in UN Open Source Week (including its Digital Resilience and Sovereignty Track) at the United Nations. This is all in addition to our work reaching



out to communities around the world as discussed further below.

In the year ahead, OpenSSF plans to strengthen its role in shaping cybersecurity and standardization policy even further. We've already submitted our application to become a liaison organization with CEN/CENELEC, and we're exploring partnerships with ENISA, ECSO, and ITU to extend our collaboration globally.

Beyond policy and standardization, OpenSSF has actively participated in multiple high-profile events, including the [Open Source Congress](#), [OpenSSF Community Day](#) or [European Open Source Security Forum](#). These engagements facilitated direct interaction and scene-sharing with EU officials, OSS community leaders, manufacturers, and other stewards.

Our goal remains consistent: to ensure open source has a strong, informed, and trusted voice in the development of cybersecurity policies in Europe and around the world.



### Artificial Intelligence Cyber Challenge (AIXCC)

The [Artificial Intelligence Cyber Challenge \(AIXCC\)](#), led by [Defense Advanced Research Projects Agency \(DARPA\)](#) in collaboration with ARPA-H, aims to secure open source software through AI. AIXCC competitors have developed AI systems to automatically find and fix cybersecurity vulnerabilities in open source software used in critical public

infrastructure. During the finals of the competition, which concluded at Def Con in August, teams' systems attempted to identify and generate patches for synthetic vulnerabilities across 54 million lines of code. In total, competitors' systems discovered 54 unique synthetic vulnerabilities in the Final Competition's 70 challenges. Of those, they patched 43. Teams also discovered 18 real, non-synthetic vulnerabilities and generated successful patches for 11 of the 18. OpenSSF is assisting in responsible disclosure and patch submission to these open source projects.

OpenSSF served as a challenge advisor to AIXCC to ensure the competition provides solutions that benefit open source culture and community. The systems from the seven finalists were released as open source. The infrastructure and data from the competition was also released as open source to support ongoing research efforts.

OpenSSF's [AI / ML Security Working Group](#) formed a Cyber Reasoning Systems Special Interest Group to support ongoing collaboration by the AIXCC participants and further development of autonomous systems to improve open source software security.



## Programs & Projects

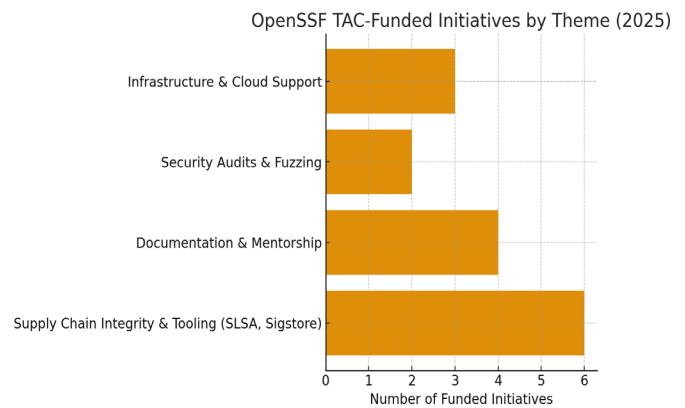
### TI-Funded Projects and Impact

Over the past year, the OpenSSF Technical Advisory Council (TAC) has awarded **\$663,248.00** across **14** Technical Initiatives that strengthen the security and resilience of the open source software ecosystem. These projects span audits, specifications, infrastructure, and community development that advance OpenSSF's mission of making open source software more secure and sustainable.

A major area of investment has been supply chain integrity and tooling to ensure trustworthiness for the entirety of the open source software cycle. Six of the fourteen TIs funded were focused on work related to the Supply-Chain Levels for Software Artifacts (SLSA) framework. Other investments supported the Sigstore ecosystem, including the development of a new log monitoring website with the goal to detect anomalies in code signing infrastructure.

In addition, the TAC funded a summer mentorship program for OpenSSF. Four mentees successfully completed the mentorship by making significant contributions to the gittuf and RSTUF projects. Plans are underway to continue this initiative in Summer 2026.

As shown in the chart below, most of this year's TIs were centered on supply chain integrity and tooling, followed by documentation, infrastructure, and audit-related work. Together, these initiatives reflect OpenSSF's commitment to practical, collaborative solutions that secure the world's open source infrastructure.



### OSS Infrastructure & Tooling Improvements

OpenSSF has highlighted the need for sustainable investment in open infrastructure through a collaborative [open letter](#) that gained broad media visibility. We have also, through a variety of mechanisms, improved OSS infrastructure and tooling throughout 2025 (including the tools we produce). Here are some key achievements (details are available in Technical Initiative [reports](#) to the OpenSSF TAC):

#### Investing in Critical Projects (Alpha-Omega)

The *Alpha-Omega Project* expanded its strategic investment model, building on the momentum of its 2024 success. Throughout Q1 and Q3 2025, the project continued to deliver millions of dollars in grants and security services to the world's most critical open source projects. Key infrastructure initiatives included directly staffing security personnel within major ecosystems like the Python Software Foundation and RubyGems, ensuring a sustainable security focus for projects often maintained by volunteers. Grant funding successfully hardened core infrastructure components like the Linux kernel and the Homebrew package manager through dedicated security audits and the implementation of advanced security

#### Reference:

- <https://github.com/ossf/tac/issues/379>
- <https://github.com/ossf/tac/issues/414>
- <https://github.com/ossf/tac/issues/417>
- <https://github.com/ossf/tac/issues/451>
- <https://github.com/ossf/tac/issues/470>
- <https://github.com/ossf/tac/issues/472>
- <https://github.com/ossf/tac/issues/474>
- <https://github.com/ossf/tac/issues/475>
- <https://github.com/ossf/tac/issues/493>
- <https://github.com/ossf/tac/issues/494>
- <https://github.com/ossf/tac/issues/511>
- <https://github.com/ossf/tac/issues/538>
- <https://github.com/ossf/tac/issues/537>
- <https://github.com/ossf/tac/issues/536>
- <https://github.com/ossf/tac/issues/531>

controls. Alpha-Omega recently [approved](#) funding a series of security audits (6 major, 20 rapid) of popular open source projects through OSTIF, of Eclipse Foundation's OpenVSX to improve its security posture of [ecosyste.ms](#) for improvements such as API authentication, and of funding through OpenReactory to build out VEX automation tooling, with Apache Airflow as an engaged partner.

### Maturing Supply Chain Tooling

A core focus in 2025 was the maturation and adoption of foundational supply chain security tools. The Sigstore project continues to make steps to enable developers to easily create and verify cryptographically signed software artifacts. Sigstore [switched](#) to Rekor on Tiles (aka "Rekor v2") for its transparency log, transitioning its backend to a modern, tile-backed transparency log implementation to simplify maintenance and lower operational costs. Tiles are cheaper to store, trivially cacheable, and reduce the service footprint to simplify deployment complexity.

The Supply Chain Integrity Working Group has [published](#) SLSA 1.2 release candidate 1, including a new source track, and received substantial comments that are being addressed. S2C2F is being integrated into SLSA as the "SLSA Dependency Track" which will eliminate duplication and synthesize the result for all. The Graph for Understanding Artifact Composition (GUAC) project reached a major stability milestone, with its version 1.0 release facilitating broader production use. This infrastructure improvement enables organizations to efficiently analyze complex software supply chain metadata. Furthermore, the OpenSSF welcomed the contribution of Trustify, a tool intended to serve as the unified, central hub for building and

using supply chain knowledge graphs, directly enhancing shared infrastructure and developer tooling for security analysis.

We funded [fuzzing work](#) on the new AI model signing library. This effort found an issue that is being addressed.

### Hardening Repositories

The Securing Software Repositories Working Group made substantial progress on developing [guidance](#) and implementation for package registries (like npm and PyPI), building on work such as our [Principles for Package Repository Security](#). For example:

- [Rust Crates](#), [npm](#), and [NuGet](#) now support Trusted Publishing, following PyPI's lead. Trusted Publishing eliminates the need for secrets to be embedded within a CI/CD pipeline when publishing from it, simplifying deployment and completely eliminating a dangerous supply chain attack that historically has been an easily-made mistake.
- We have refined and released [Crafting a Package Deletion Policy](#) to help package registries counter problems like the 2016 left-pad incident.
- We released [Style Guide for Attestations UI/UX](#), funded work on UI/UX support for attestations on software repos. This is a challenging problem for humans because the average user is unfamiliar with these attestations, yet they must be surfaced in a way that is meaningful, trustworthy, and integrates with the existing interface.

We continue to work to strengthen the overall resilience of the distribution infrastructure upon which all software relies.

#### Reference:

- <https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q1-Repos-WG.md>
- <https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q3-Repos-WG.md>
- <https://github.com/ossf/tac/pull/539/files>
- <https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q3-ST-WG.md>
- <https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q1-SCP-WG.md>
- <https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q3-SCP-WG.md>
- <https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q1-Sigstore.md>
- <https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q3-Sigstore.md>
- <https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q3-Alpha-Omega.md>
- <https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q1-SCI-WG.md>
- <https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q3-SCI-WG.md>

## Media Highlights



**ZDNET** (6,079,719 monthly views)

[The best free AI courses and certificates in 2025 - and I've tried them all](#)

OpenSSF's Secure AI/ML-Driven Software Development course was featured in a round up of the best free AI courses and resources. The course is described as a good starting place for learning secure AI code best practices.



**The New Stack** (589,793 monthly views)

[How the EU's Cyber Act Burdens Lone Open Source Developers](#)

OpenSSF's Christopher "CRob" Robinson sat down with The New Stack Agents podcast to discuss the Cyber Resiliency Act while onsite at Open Source Summit EU.



**Infosecurity Magazine** (115,265 monthly views)

[In Conversation: Learnings for CISOs Post Black Hat and DEF CON](#)

Christopher "CRob" Robinson, OpenSSF's Chief Security Architect, dives into his thoughts following Black Hat USA 2025 and DEF CON 2025. OpenSSF members Trail of Bits, Canonical, and OSTIF are included in this article as well.



**diginomica** (43,854 monthly viewers)

[Building bridges, not burning maintainers - how the CRA is reshaping open source relations](#)

OpenSSF's Christopher "CRob" Robinson was interviewed by diginomica onsite at Open Source Summit EU about the opportunities and challenges ahead related to CRA.



**Help Net Security** (18,700 monthly views)

[The 6 challenges your business will face in implementing MLSecOps](#)

Christopher "CRob" Robinson, OpenSSF's Chief Security Architect, delves into the six major challenges that IT leaders will experience in establishing or maturing their MLSecOps program for Help Net Security.

## Other Coverage

- **Tech.eu**, [Linux Foundation Europe and OpenSSF launch initiative for EU Cyber Resilience Act compliance](#), January 31, 2025
- **ADT Magazine**, [Linux Foundation and OpenSSF to Help Developers Navigate EU Cyber Resilience Act](#), February 12, 2025
- **Dark Reading**, [OpenSSF Sets Minimum Security Baselines for Open Source Projects](#), February 26, 2025
- **SecurityWeek**, [OpenSSF Releases Security Baseline for Open Source Projects](#), February 26, 2025
- **Infosecurity Magazine**, [OpenSSF Releases Security Baseline for Open Source Projects](#), February 27, 2025
- **Help Net Security**, [OSPS Baseline: Practical security best practices for open source software projects](#), February 28, 2025
- **DevOps.com**, [OpenSSF Defines Baseline for Securing Open Source Software](#), March 3, 2025
- **InfoQ**, [OpenSSF Publishes Security Baseline for Open-Source Projects](#), March 5, 2025
- **SD Times**, [OpenSSF creates Project Security Baseline](#), March 10, 2025
- **I-Programmer**, [Why OpenSSF's Baseline Security For Open Source Projects Is Important](#), April 21, 2025
- **ITOps Times**, [Linux Foundation and OpenSSF launch Cybersecurity Skills Framework](#), May 14, 2025
- **SiliconANGLE**, [Linux Foundation debuts Cybersecurity Skills Framework to address enterprise talent gaps](#), May 14, 2025
- **SC Media**, [New Cybersecurity Skills Framework seeks to bolster enterprise talent readiness](#), May 15, 2025
- **Help Net Security**, [Cybersecurity Skills Framework connects the dots between IT job roles and the practical skills needed](#), May 16, 2025
- **Security Boulevard**, [Linux Foundation Shares Framework for Building Effective Cybersecurity Teams](#), May 16, 2025
- **ITdaily**, [Linux Foundation Launches Global Cybersecurity Skills Framework](#), May 19, 2025
- **Linux Insider**, [Is a Security Baseline Enough for Open-Source Software?](#), June 13, 2025
- **theCUBE**, [CRob Robinson, OpenSSF | Open Source Summit 2025](#), June 24, 2025
- **Infosecurity Magazine**, [NSA and CISA Urge Adoption of Memory Safe Languages for Safety](#), June 25, 2025
- **SiliconANGLE**, [How open-source developers can meet global cybersecurity laws — before it's too late](#), June 26, 2025
- **SiliconANGLE**, [Code, community and the future: 13 takeaways from Open Source Summit NA](#), June 28, 2025
- **Techstrong.ai**, [Techstrong TV June 30, 2025](#), June 30, 2025
- **Techstrong.ai**, [Navigating Software Supply Chain Security Challenges with Christopher \(CRob\) Robinson | Open Source Summit NA 2025](#), July 3, 2025



- **Help Net Security**, [The 6 challenges your business will face in implementing MLSecOps](#), August 20, 2025
- **The New Stack**, [What the EU's Cyber Resilience Act Means for Open Source](#), August 21, 2025
- **Infosecurity Magazine**, [CISA Seeks Biden Era's SBOM Minimum Requirements Guideline Change](#), August 25, 2025
- **Tech.eu**, [The World of Open Source Europe report 2025: mapping trends, challenges, and the push for digital sovereignty](#), August 25, 2025
- **Dutch IT Channel**, [OpenSSF honors achievements in open source security and AI](#), August 27, 2025
- **Dutch IT Leaders**, [OpenSSF honors achievements in open source security and AI](#), August 27, 2025
- **ITPro Today**, [New Research Debunks Open Source Business Model Myths](#), August 27, 2025
- **diginomica**, [Building bridges, not burning maintainers - how the CRA is reshaping open source relations](#), August 27, 2025
- **The New Stack**, [The Cyber Resilience Act: Fear, Confusion — And Reassurance](#), August 28, 2025
- **The New Stack**, [TNS Daily | August 29](#), August 29, 2025
- **diginomica**, [Enterprise hits and misses - services firms have an AI market meltdown, but why? Tech earnings roll in, as NVIDIA gets an Alibaba heads up](#), September 2, 2025
- **ITdaily**, [Europe's turn: the opportunities and challenges of open source](#), September 4, 2025
- **Data Center Insider**, [Digital sovereignty is moving to the center of open source strategies](#), September 5, 2025
- **Cybersecurity Dive**, [How AI and politics hampered the secure open-source software movement](#), September 9, 2025
- **Data Center Insider**, [Christopher Robinson on MLSecOps and the Cyber Resilience Act](#), September 10, 2025
- **Infosecurity Magazine**, [In Conversation: Learnings for CISOs Post Black Hat and DEF CON](#), September 10, 2025
- **The New Stack**, [How the EU's Cyber Act Burdens Lone Open Source Developers](#), September 11, 2025
- **The New Stack**, [SBOMs Get a Needed Update for New Threats](#), September 12, 2025
- **InfoWorld**, [More money for open source security won't work](#), September 22, 2025
- **Reversing Labs**, [The call for funding of open-source platforms](#), October 1, 2025
- **ZDNET**, [The best free AI courses and certificates right now](#), October 23, 2025

# Working Group & Project Updates

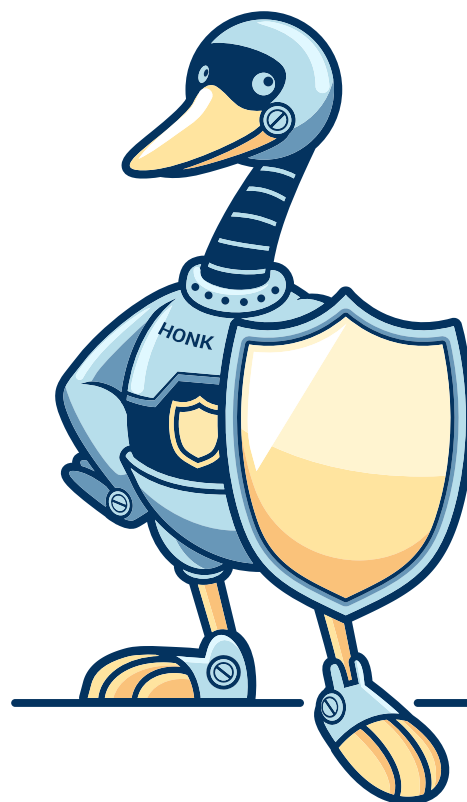
The Open Source Security Foundation (OpenSSF) drives collaboration across the open source ecosystem to secure the software we all depend on. Our Working Groups and Projects form the technical backbone of this mission, each focused on solving specific challenges in open source security, from vulnerability disclosure and supply chain integrity to AI/ML safety and global policy engagement.

In 2025, these initiatives continued to make measurable progress, launching new specifications, advancing cross-foundation collaborations, publishing educational resources, and scaling adoption of open security tools worldwide. Together, they represent the collective technical innovation, community leadership, and shared responsibility that define the OpenSSF community.

The OpenSSF [Technical Advisory Council \(TAC\)](#) oversees all Technical Initiatives (TIs) and maintains the project lifecycle for hosted projects.

Learn more about OpenSSF's technical initiatives and hosted projects on our [Projects page](#).

OpenSSF GitHub Repository: [github.com/ossf](https://github.com/ossf)



## WORKING GROUP

### AI / ML Security

Incubating working group focused on addressing open source software security for AI/ML workloads

#### 2025 HIGHLIGHTS

- Launch of `model-signing` 1.0, and 1.1
  - » Launch of the OMS model signing format spec
- [Visualizing Secure ML Ops](#) whitepaper
- [“Secure AI/ML-Driven Software development”](#) (LFEL 1012) course
- 4 different SIGs:
  - » Model signing
  - » AI Economics for OSS
  - » Safe MCP
  - » Cyber Reasoning Systems

#### IMPACTS

- Working on “security for AI” (safe MCP, model signing, signing agent cards) and “AI for security” (Cyber Reasoning System, DARPA AIxCC, AI economics SIG)
- The central place across the OSS ecosystem for anything related to AI and security. Integration with other working groups in OpenSSF (BEST, Supply Chain Security), Linux Foundation (LF AI & Data Cybersecurity Compliance) and external (Coalition for Secure AI, etc)

Working Group Leads	Number of Regular Contributors
Jay White, Mihai Maruseac	10-20
GitHub Repo	
<a href="https://github.com/ossf/ai-ml-security">ossf/ai-ml-security</a>	

- Coalition for Secure AI whitepaper recommends `model-signing` approach as the way to start securing the ML supply chain

#### WHAT'S NEXT (2026)

- More integrations for model signing. Have model hubs support signing by default and get frontier labs to sign their OSS LLMs.
- Build on top of model signing, project Atlas (Intel) and project Sentry (Purdue) to a unified infrastructure for AI/ML supply chain security covering signing models, datasets, agent cards, etc. as well as generating provenance for all ML artifacts



## WORKING GROUP

# Belonging, Empowerment, Allyship, and Representation



Increases representation and enhances effectiveness of the cybersecurity workforce

## 2025 HIGHLIGHTS

- Ejiri Oghenekome, Sal Kimmich released a three-part blog series on Getting Started in Open Source - two have been released
  - » [From Beginner to Builder: Your First Code Contribution – Open Source Security Foundation](#)
  - » [From Beginner to Builder: Understanding OpenSSF Community and Working Groups – Open Source Security Foundation](#)
- BEAR working group hosted a lunch meetup at the OpenSSF Community Day NA and shared their impact at the OpenSSF booth during Open Source Summit NA.
- The BEAR working group got funding for summer mentees through the Linux Foundation Mentorship program during the summer of 2025. 4 mentees completed this year's mentorship program
  - » Office Hours Highlighting the 4 mentees [https://youtu.be/U-A7AD\\_Qks?si=6y6NPL30z8bbGsAb](https://youtu.be/U-A7AD_Qks?si=6y6NPL30z8bbGsAb)
- There were various types of Office hours hosted in 2025 for a total of nine office hours from January to October

## IMPACTS

- Published beginner-friendly blog series to guide new contributors into OpenSSF, including an office hour focused on the topic and marketing sent out.
- Represented BEAR globally at Python Ghana through Ijeoma's participation and various open source summits

Working Group Leads	Number of Regular Contributors
Jay White, Marcela Melara, Yesenia Yser	5-8
GitHub Repo	
<a href="https://github.com/ossf/wg-dei">ossf/wg-dei</a>	

across the world, such as hosting meetup & booth at OpenSSF Community Day NA and OSS Summit NA.

- Funded & mentored four mentees via Linux Foundation's 2025 summer program.
- Held nine office hours from Jan–Oct 2025, including a mentee showcase session, release of the AI/ML development course, and the beginner-friendly blog series.

## WHAT'S NEXT (2026)

- Meetups in Africa focused on software development, open source, and security to be run by Prince Oforh Asiedu, Seth Mensah, and Aaron Will Djada.
- Assist speakers for PyCon Africa and booth sponsors for potentially The Linux Foundation in the PyCon in Ghana and Africa more generally.
- Continue with the Office Hours.
- Work with the DevRel group to strategize methods to help new contributors for awareness, guidance, and working group alignment.
- Provide support for additional mentorship for open source projects.

## WORKING GROUP

# Best Practices for Open Source Developers

Provides open source developers with best practice recommendations and accessible resources

## 2025 HIGHLIGHTS

- Training courses
  - » [Understanding the EU Cyber Resilience Act \(CRA\) \(LFEL1001\)](#)
  - » [Security for Software Development Managers \(LFD125\)](#)
  - » [Secure AI/ML-Driven Software Development \(LFEL1012\)](#)
  - » [Japanese translation of LFD121](#)
- Concise guides
  - » [Security Focused Guide for AI Code Assistant Instructions](#)
  - » [Cyber Resilience Act \(CRA\) Brief Guide for Open Source Software \(OSS\) Developers](#)
  - » [Simplifying Software Component Updates](#)
  - » [Security Web Application Guidelines](#)
- OpenSSF Scorecard
  - » Release of OpenSSF Scorecard v5.3.0



Working Group Leads	Number of Regular Contributors
Georg Kunz, Avishay Balter	8 - 9
GitHub Repo	
<a href="https://github.com/ossf/wg-best-practices-os-developers">ossf/wg-best-practices-os-developers</a>	

- » Release of Allstar v.4.5



- Memory Safety SIG
  - » [Memory Safety Continuum](#)

## IMPACTS

- The Working Group released multiple training courses hosted by LF Education. The courses are extremely well received with large enrollment numbers.
- The Working Group very effectively collaborated with both the AI/ML Working Group and the Global Cyber Policy WG by jointly developing guides and educational material.

## WHAT'S NEXT (2026)

- The team developing the Python Secure Coding Guide is working towards their first release in early 2026.
- A C/C++ Compiler Annotation Guide is planned for a first release in the beginning of 2026, complementing the existing C/C++ Compiler Option Guide.
- The Education SIG is working on additional education courses and material.

## WORKING GROUP

# Global Cyber Policy

Multi-discipline approach to international regulation and legislation and application of cybersecurity frameworks



## 2025 HIGHLIGHTS

- This group was formed in January 2025, after the Linux Foundation workshop on “Stewards and Manufacturers” in Amsterdam in December 2024. The shape of this group is very much based on the consensus of that workshop. The scope of the group is to provide a forum for our members and the broader community to collaborate on Global Cybersecurity-related legislation, frameworks, and standards which facilitate conformance to regulatory requirements by open source projects and their consumers. We have been holding bi-weekly calls. We have 2 active SIGs - Awareness and Standards. The group is focusing most of its attention on the European Cyber Resilience Act (CRA) with some time put aside to monitor activities in other jurisdictions. We also have drafted a [liaisons list](#) which is a list of external organizations we feel we need to liaise with.
- The group has produced deliverable documents, acted as an outreach vehicle, and also served as a venue to discuss and share information between community members regarding the regulatory landscape and its impacts on industry and the OSS ecosystem.
- We have two working group co-leads: [Daniel Appelquist | Samsung](#) and [Roman Zhukov | Redhat](#), with [Mike Bursell | Confidential Compute Consortium](#) having served well as its initial lead through October 2025. They have been supported by OpenSSF staff including [CRob](#), [Jeff Diecks](#), [Madalin Neag](#), and [David A. Wheeler](#).

Working Group Leads	Number of Regular Contributors
Dan Appelquist, Roman Zhukov	19
GitHub	

[ossf/wg-global-cyber-policy](https://ossf/wg-global-cyber-policy)

- We also operate the “EU CRA Monthly Tech Talk” (née the “CRA Tech Bi-weekly”), the agenda of which is managed by the Awareness SIG.
- We have a regular schedule of calls for our Awareness and Standards SIGs as well as our main working group call. We are working with the ORBIT working group on tooling related issues. We also held a special face-to-face hybrid meeting of the working group at Open Source Summit Europe (in addition to other F2Fs - FOSDEM and OSS NA). The focus of this meeting was to hear from two different organizations about their CRA readiness work and plans as well as the recent call for comments from CISA on [their 2025 Minimum SBOM elements](#).
- We held a workshop at the LF Europe Roadshow in Ghent on the 29th of October for interactive discussions, mirroring the format of last year’s workshop in Amsterdam that kicked our working group.

## IMPACTS

- We have helped to drive global awareness of the CRA and its impacts for manufacturers and for developers. We have helped to launch the successful [Free LF Training on CRA](#) by providing feedback and input, and have >5500 enrollments so far. We have published several blog posts (such as the [recap of the tech talk in June](#) and [Am I a Manufacturer or a Steward](#)) and also the [CRA Brief Guide](#). We have also provided feedback on several OpenSSF documents on open source stewardship within the Linux Foundation.



### WHAT'S NEXT (2026)

- We plan to use the outputs of the workshop at the LF Europe Roadshow in Ghent on the 29th of October to help shape our program of work for 2026. The focus for 2026 will likely be around providing more actionable guidance to manufacturers, maintainers and stewards. Topics to be reviewed include defining security due diligence, whether we need a “baseline for manufacturers”,

how manufacturers can engage with small long-tail up-stream projects, action in ETSI & other standards orgs, working with US and other regulatory regimes, defining a “compliance.md” and looking at the current state of CRA-relevant tooling. We have also proposed a DevRoom for next year’s FOSDEM.





## WORKING GROUP

# Open Resources for Baselines, Interoperability, and Tooling



Focused on the Baseline catalog and supporting tools to implement and assess based on international best practices and regulations

## 2025 HIGHLIGHTS

### IMPACTS

- Organized OSPS Baseline Rollout via LFX, now scanning 20k repositories
- FINOS is now able to link three GRC-related projects together using Gemara
- FINOS TOC has included OSPS Baseline requirements in an upcoming revision to project health checks, tied to maturity levels
- 200% increase in Security Insights adoption this year, following the CNCF Security Slam and LFX alignment



Working Group Leads	Number of Regular Contributors
Eddie Knight, TSC Chair. TSC members: Ben Cotton, John Kjell, Jennifer Power, Travis Truman	Average 10 participants per call
GitHub	
<a href="https://github.com/ossf/wg-orbit">ossf/wg-orbit</a>	

## WHAT'S NEXT (2026)

- Ongoing maintenance and polish of OSPS Baseline and Security Insights
- Continued development of other projects and tools



## WORKING GROUP

# Securing Critical Projects

Identifies and allocates resources to secure critical open source projects

## 2025 HIGHLIGHTS

- The Securing Critical Projects Working Group (WG) advanced multiple large-scale initiatives to strengthen the security posture of widely used open source components across the ecosystem. The group's work focused on driving measurable improvements through coordinated security audits, targeted remediations, and ecosystem-wide collaboration. [Malicious Packages](#) is now a standalone project, split from Package Analysis.
- **Security Audits and Improvements**
  - » Delivered numerous security audits and improvements for high-impact open source projects, including initiatives in collaboration with community partners such as the Open Source Technology Improvement Fund (OSTIF).
  - » Completed audits for several OpenSSF projects, including RSTUF ([RSTUF Audit Complete!](#)) and Security Scorecards ([OpenSSF Scorecard Audit is Complete!](#)).
  - » Supported long-term sustainability by ensuring findings were remediated and by improving threat models, testing infrastructure, and fuzzing capabilities.
- **AI and Critical Infrastructure Initiatives**
  - » Continued collaboration with DARPA's AIxCC Challenge, with OpenSSF and WG partners supporting implementation efforts to improve the resilience of open source AI infrastructure. Work began in mid-2025 and will continue through 2026.

Working Group Leads	Number of Regular Contributors
Amir Montazery, Jeff Mendoza	4-6
GitHub Repo	
<a href="https://github.com/ossf/wg-securing-critical-projects">ossf/wg-securing-critical-projects</a>	

## ▪ Alpha-Omega Engagements

- » Through the Alpha-Omega program, the WG funded and oversaw multiple security uplift efforts for critical OSS components
- » Security Research on 25 Open Source AI Libraries (publication expected Q4 2025)
- » Critical Cryptography Libraries Security Audit (publication expected Q4 2025–Q1 2026)
- » Security Uplift Program: Over 60 critical open source projects undergoing assessment and remediation work
- » Ruby Ecosystem Program: Security audits and fuzz-testing improvements coordinated through cost-sharing between Alpha-Omega and external foundations

## ▪ Collaborative Security Engagements

- » The Working Group strengthened partnerships across the ecosystem, including with the Open Source Technology Improvement Fund, Inc. (OSTIF) ([ostif.org](https://ostif.org)), which advanced to General Member status in 2025 to deepen collaboration on critical project security.

## ▪ [Malicious Packages](#)

- » This is a comprehensive, high quality, open source database of reports of malicious packages published on open source package repositories.
- » Moved to a standalone project, split from Package Analysis



» Storing data on malicious packages across ecosystems

- 66,000 NPM
- 10,000 PyPi
- 1,000 RubyGems
- 1,000 NuGet

» Also supports: Go, Crates, Git Repos, and Maven reports

» New [status page](#)

### ■ [Criticality Score](#)

- » This project implements a quantitative approach to estimating a project's influence and importance
- » Calculates scores monthly for 500,000 projects

### IMPACTS

- Security engagements in 2025 resulted in:
  - » **6** new or updated threat models
  - » **52** issues, findings, or hardening recommendations addressed
  - » **5** testing and fuzzing frameworks implemented or strengthened
- These outcomes demonstrate tangible progress toward the WG's mission of improving the security of the world's most critical open source infrastructure.

### WHAT'S NEXT (2026)

- The Working Group will expand its engagement pipeline to support more projects in need of direct security assistance, with an emphasis on sustainable remediation, ecosystem scalability, and measurable outcomes. Building on 2025's momentum, nearly 100 open source projects have already benefited from targeted security interventions and more will follow in 2026.



## WORKING GROUP

# Securing Software Repositories

Introduces new tools and technologies that strengthen and secure software repositories

## 2025 HIGHLIGHTS

- Trusted publishing, a security capability to get API tokens out of build pipelines, was released for [crates.io](#), [npm](#), and [NuGet](#).
- RSTUF made its v1.0 release to help repositories protect the integrity of their package indices
- Worked with designers to [produce UI/UX guidance for displaying attestations in repositories](#)
- The working group released guidance on [Crafting a Package Deletion Policy](#)

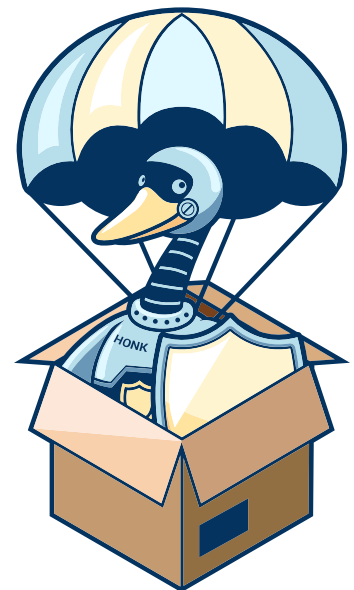
## IMPACTS

- The working group facilitated / supported 8 security capabilities rolled out to 6 package repositories in 2025: in particular provenance verification support for [Maven Central](#) and [Bazel Central](#) as well as the above mentioned trusted publishing for [crates.io](#), [npm](#), and [NuGet](#).
- We hosted numerous discussions in the aftermath of various supply chain attacks on software repositories.

Working Group Leads	Number of Regular Contributors
Dustin Ingram, Zach Steindler	-
GitHub Repo	
<a href="#">ossf/wg-securing-software-repos</a>	

## WHAT'S NEXT (2026)

- Updating [Principles for Package Repository Security](#) with lessons learned from the last 2 years
- Get the repositories together to discuss gaps, roadmaps, and funding generally
- Discuss malware detection, handling, and notifications for repositories



## WORKING GROUP

### Security Tooling

Provides security tools for open source developers and makes them universally accessible

#### 2025 HIGHLIGHTS

- The Security Tooling Working Group advanced several key initiatives this year to strengthen the open source software security ecosystem.
- [OpenBao](#) was accepted as a WG project from LF Edge, met sandbox requirements, and began the incubation process. New features such as Namespaces (tenancy), UI 2.0, and external key management were introduced in v2.3.0, with further scalability and reliability updates planned.



**OpenBao**

- The group launched the Reliable Software Decomposition SIG (originating from the DARPA E-BOSS program) to improve binary analysis and embed metadata in compiler toolchains for enhanced vulnerability assessment.
- [SBOMit](#) continued progress toward incubation and hosted its first workshop in Washington, DC, focusing on in-toto attestations and automation for generating verifiable SBOMs.



**SBOMit**

Working Group Leads	Number of Regular Contributors
Ryan Ware	8–12 active contributors
GitHub Repo	
<a href="https://github.com/ossf/wg-security-tooling">ossf/wg-security-tooling</a>	

- [Minder](#) matured its automation and remediation capabilities, expanding context handling, refining rule creation, and improving interoperability with other OpenSSF tools.



**minder**

- Regular biweekly community calls maintained strong participation from across the ecosystem, including contributors from GitLab, Intel, Lockheed Martin, Target, Oracle, NYU, and others, helping align priorities across multiple subprojects.
- [CVE-Bin-Tool](#) approved by the OpenSSF TAC as a new project, enhancing developers' ability to identify vulnerable dependencies in compiled binaries.

#### IMPACTS

- The WG strengthened interoperability between OpenSSF tooling projects and external ecosystems, lowering barriers for adoption and increasing developer confidence in the security of open source software. By aligning initiatives such as OpenBao, Minder, CVE-Bin-Tool, and SBOMit under a single framework, the WG helped build a more cohesive suite of open tools addressing every stage of the software supply chain. Collaboration through the Reliable Software Decomposition SIG expanded engagement with academic and research communities, furthering innovation in compiler-level security instrumentation.



### WHAT'S NEXT (2026)

- In the coming year, the WG plans to:
  - » Advance SBOMit toward incubation and expand SBOM tooling for supply-chain attestation.
  - » Support OpenBao's graduation milestones and deepen integration with other OpenSSF projects.
  - » Consolidate documentation and maturity tracking across WG projects.
- » Continue expanding the Reliable Software Decomposition SIG and cross-foundation partnerships to advance compiler-integrated metadata approaches.
- » Strengthen inter-WG collaboration, including with the AI/ML Security WG, to align efforts across the evolving open source security landscape.



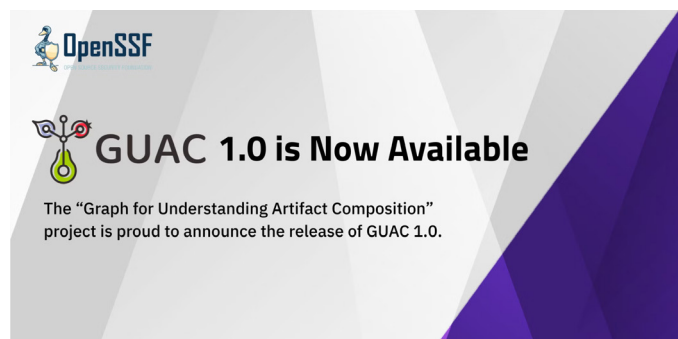
## WORKING GROUP

### Supply Chain Integrity

Helps individuals understand and make informed decisions about code provenance, including projects like GUAC, SLSA, and gittuf

#### 2025 HIGHLIGHTS

- New SLSA Tracks
- Trustify donation under the GUAC umbrella
- GUAC 1.0.0 release



Working Group Leads	Number of Regular Contributors
Isaac Hepworth, Jay White	-
GitHub Repo	
<a href="https://github.com/ossf/wg-supply-chain-integrity">ossf/wg-supply-chain-integrity</a>	

#### IMPACTS

- Projects integrating to support shared capabilities
  - » Zarf and GUAC integration



#### WHAT'S NEXT (2026)

- SCI WG is refreshing the goals and focus areas
  - » Identifying roles and key objectives to foster collaboration and deliver actionable resources.



## WORKING GROUP

# Vulnerability Disclosures

Advances vulnerability reporting and communication to enhance open source security

## 2025 HIGHLIGHTS

- OSV Schema expansion broadened to new ecosystems (Kubernetes, MinimOS, Bellsoft Alpaquita, Hardened Containers, Echo, Julia), improving vulnerability coverage for millions of OSS users and packages.
- OSV Linter enhanced by adding package/version existence checks and `upstream/aliases` validation, improving data quality and usability of OSV records.
- Discussion towards open-sourcing [Advise](#) (formerly VINCE) under the OpenSSF, a platform for multi-stakeholder vulnerability response.
- Participation in [VulnCon 2025](#), with OpenSSF members/projects having notable representation.
- Discussion on [AI-generated/slop security reports](#) and potential guidance for maintainers and reporters. Explored shifting the “security work is special” paradigm, fostering sustainable and inclusive security reporting models.
- Discussion on the need for a [product-first vulnerability disclosure report \(VDR\) specification](#), as highlighted by the CISA software acquisition guide.
- Continued discussions on CVE Program sustainability and contingency planning in response to CVE Program funding risks, ensuring OSS resilience via alternatives like [OSV as potentially a global vulnerability database](#).

Working Group Leads	Number of Regular Contributors
Madison Oliver, CRob	19 unique contributors attending 2+ meetings in 2025
GitHub Repo	
<a href="https://github.com/ossf/wg-vulnerability-disclosures">ossf/wg-vulnerability-disclosures</a>	

## IMPACTS

- Increased OpenSSF presence and influence at industry conferences like VulnCon and collaborated with industry partners like the CVE Program and PURL project.
- Addressing challenges posed by mass generation of low-quality AI-generated security reports and promoting quality reporting.
- Strategic re-evaluation of VDR development, considering collaboration with existing standards bodies like OWASP CycloneDX to avoid fragmentation and leverage established efforts.
- Focus on creating actionable vulnerability information for consumers, emphasizing mitigation and remediation.

## WHAT'S NEXT (2026)

- Continue development and adoption of Advise as an OpenSSF project.
- Complete and promote the [CVD Guide for OSS Consumers](#).
- Engage in ongoing discussions and potential collaborations regarding a standardized, product-centric VDR.
- Develop guidance for evaluating and handling AI-generated security reports.
- Continue to foster global participation in working group meetings.

## OPENSSF PROJECTS AND AFFILIATED PROJECTS

### Sigstore



Provides signing, verification, and transparency tools to improve trust in software supply chains

#### 2025 HIGHLIGHTS

- [Maven Central announced support](#) for Sigstore signatures
- [sigstore-go v1.0 released](#), offering a minimal API for Go applications using Sigstore and conformance with the other Sigstore SDKs
- [Cosign v3 released](#), supporting a standardized [signature bundle format](#) and storing attestations as OCI Image v1.1 referring artifacts
- [Launched Rekor v2](#), a redesigned and modernized signature transparency log, to simplify maintenance and lower operational costs
- Released [Sigstore Transparency Log research dataset](#), a BigQuery dataset for researchers investigating signing in open source
- In collaboration with OpenSSF, NVIDIA and HiddenLayer, [announced model-transparency v1.0](#), making ML models tamper-resistant via transparent signatures
- [NVIDIA announced signed models](#) for the NGC catalog

Working Group Leads	Number of Regular Contributors
TSC (Bob Callaway, Luke Hinds, Trevor Rosen, Santiago Torres-Arias, Priya Wadhwa), Community Chair (Hayden Blauzvern)	55
GitHub Repo	
<a href="#">sigstore</a>	

#### IMPACTS

- As AI becomes a cornerstone for modern development, Sigstore provides authenticity and integrity for ML supply chain security pipelines. The OpenSSF [published a whitepaper](#) and CoSAI [published a whitepaper](#) on ML model security with Sigstore and model-transparency, and a [research paper on ML model supply chain security](#) and how Sigstore can bring transparency to model signing was presented at ICML.

#### WHAT'S NEXT (2026)

- Continue working with OSS package managers to simplify signing and verification
- Support research and experimentation around [post-quantum signing](#)
- Increase the diversity of public log operators and integrate logs into a [public witness network](#)

## OPENSSEF PROJECTS AND AFFILIATED PROJECTS

### Core Toolchain Infrastructure

The Core Toolchain Infrastructure (CTI) Project’s mission is to support the GNU Toolchain community with secure infrastructure and state of the art services required to support the community’s development efforts to be a trusted foundation in a secure supply chain.

#### 2025 HIGHLIGHTS

- CTI TAC and glibc project worked through SSDLC [writeup for glibc and the GNU Toolchain to support the GNU Toolchain](#) moving forward with sustainable and secure infrastructure in 2025/2026.
- CTI TAC guiding a proposal on the use of transparent and auditable access controls for the glibc source repository (gitolite).

Working Group Leads	Website
Carlos O’Donell, David Edelsohn	<a href="https://cti.coretoolchain.dev/">https://cti.coretoolchain.dev/</a>
GitHub Repo	
<a href="https://git.coretoolchain.dev/">https://git.coretoolchain.dev/</a>	

#### WHAT’S NEXT (2026)

- CTI to continue working through the SSDLC to support sustainable and secure development infrastructure for the GNU Toolchain.



**OPENSSEF PROJECTS  
AND AFFILIATED PROJECTS****Alpha-Omega**

In 2025, Alpha-Omega continued its mission to strengthen open source security through high-impact, sustainable investments. Over \$5.8 million was directed to 14 critical open source projects, supporting both targeted engineering engagements and broader ecosystem improvements.

Citi joined as a General Member in May, contributing both funding and engineering support. Alpha-Omega also hosted its Second annual in-person Roundtable at Open Source Summit North America, while participating in key events like the 2025 Policy Summit in Washington, D.C., and the UN Open Source Week Maintain-a-Thon to deepen ecosystem engagement.

Significant project milestones included Rust's Trusted Publishing launch and CVE authority designation, Apache's Trusted Release pipeline pilot, and security upgrades across Python, Node.js, Ruby, Eclipse Foundation, and FreeBSD. In partnership with OSTIF, Alpha-Omega continued to invest in audits of numerous open source projects. These audits are the beginning of many project's security journeys.

Open source projects seeking support for security initiatives are encouraged to submit grant proposals. For more information, visit the [Alpha-Omega website](#) and [GitHub repository](#). Our complete annual report will be released here in early 2026.

**α → Leverage****Ω → Scale**

# Community Engagement & Education

## From the Marketing Advisory Council Chair

Over the past year, the OpenSSF community has continued to expand both its impact and ambition, and the Marketing Advisory Council (MAC) has been honored to help carry that momentum forward. Our role is to amplify the critical work happening across OpenSSF and ensure contributors, maintainers, policymakers, and enterprise leaders clearly understand why securing open source matters and how they can take action.

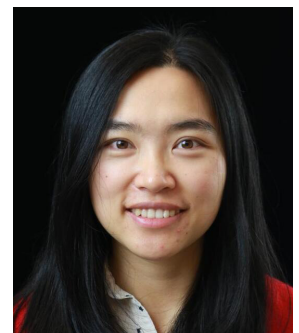
Looking ahead, our focus for 2026 and beyond is clear:

### A SHARED MARKETING VISION FOR 2026

We are developing unified annual marketing themes that invite member collaboration. With shared storytelling moments across the year, members can align their efforts with OpenSSF priorities in ways that advance our mission together.

### ELEVATING LONG TERM SUCCESS STORIES

Many of our security initiatives create impacts that take time, sometimes years, to fully realize. In 2026, we will sharpen our storytelling around these long term wins. By tracking and highlighting meaningful outcomes, we help our members demonstrate the return on their open source security investments and secure continued support inside their organizations.



Mila Zhou, Chair, Marketing  
Advisory Council OpenSSF

### EXPANDING EDUCATION AND AWARENESS

Security improves when knowledge is accessible. Through our programs, content, and campaigns, the MAC will continue to help the world understand not only why open source security matters but also how to adopt



it in a practical way. Whether through widely adopted courses like LFD121, project spotlights, or new persona level communication, we will make it easier for teams to confidently take the next step.

Our success as a foundation is strengthened by the collaboration of our members, contributors, and the greater community, which continues to bring OpenSSF tools and best practices into developer circles around the world.

As we build toward a secure software future, marketing

is more than promotion. It is advocacy, education, and empowerment. I am grateful for the passion and creativity of this community, and I look forward to continuing our work together as we tell the story of OpenSSF's growing impact.

With appreciation,

**Mila Zhou**  
**Chair, Marketing Advisory Council**  
**OpenSSF**

## OpenSSF DevRel Activities Since Late 2024

### MISSION AND STRATEGIC FOUNDATION

The OpenSSF DevRel Community aims to evangelize the OpenSSF's mission and work. It seeks to increase tooling adoption within critical open source projects and foster stronger relationships with both end-user and the wider open source communities.

### CONTENT CREATION AND GLOBAL EVENT PRESENCE

The community maintained a strong global presence through the "What's in the SOSS?" podcast and conference participation at events such as FOSDEM, VulnCon, OpenSSF Community Days, and Open Source Summits worldwide. The community staffed booth spaces, hosted office hours, and presented sessions on topics ranging from security tool adoption to EU Cyber Resilience Act compliance.

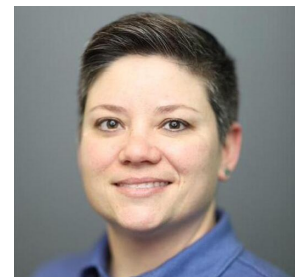
### PROFESSIONAL ELEVATION AND FUTURE DIRECTION

The DevRel Community's work has been bolstered by the establishment of the [Developer Relations](#) Foundation under the Linux Foundation in August 2025, positioning OpenSSF DevRel within a larger professional movement focused on elevating DevRel practices and establishing standardized metrics.

Moving forward, the DevRel community remains committed to expanding adoption of OpenSSF security tools, strengthening relationships with end-users and



Katherine Druckman  
Independent



Stacey Potter  
Manager of Community, OpenSSF

maintainers, and reinforcing its commitment to a more secure open source ecosystem through human-centered approaches that emphasize collaboration and education over compliance theater. It is now focused on building sustainable infrastructure for engagement, developing contextualized materials for newcomers, establishing event strategy frameworks, and enhancing contributor on-ramps.

## Events

### Policy Summit DC

MARCH 4, 2025 | WASHINGTON, DC



## OPEN SOURCE SECURITY FOUNDATION POLICY SUMMIT

WASHINGTON, D.C.  
MARCH 4, 2025

#SOSSPOLICY

### POST EVENT REPORT

**88** ATTENDEES  
REGISTERED

**70** ATTENDEES  
ATTENDED

**62** TOTAL ORGANIZATIONS  
REPRESENTED

VIRGINIA: 16.25%

NEW YORK / CALIFORNIA: 13.75%

DISTRICT OF COLUMBIA: 11.25%

TEXAS: 6.25%

MARYLAND / MASSACHUSETTS /  
COLORADO: 5.00%

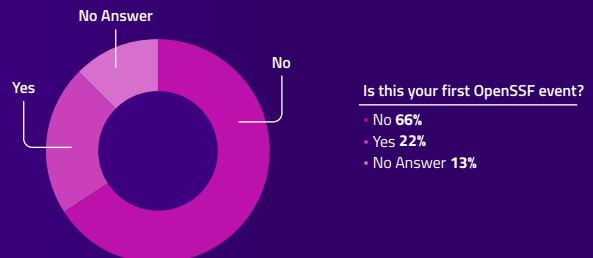
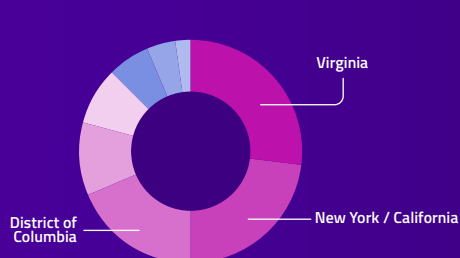
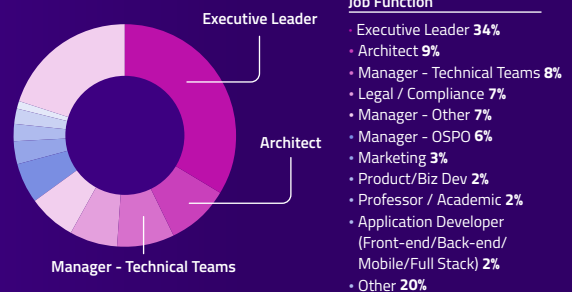
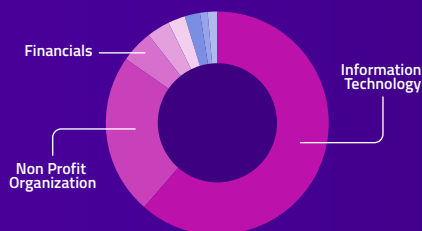
**23**  
SPEAKERS

**35%**  
WOMEN SPEAKERS

**4**  
BREAKOUTS

**5**  
PANEL SESSIONS

**5**  
KEYNOTES



### OpenSSF Community Day Japan

JUNE 18, 2025 | TOKYO, CO-LOCATED WITH KUBECON



### OpenSSF Community Day

JAPAN

TOKYO, JAPAN 2025

#OpenSSFCommunity

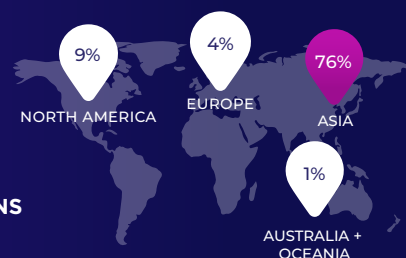
### POST EVENT REPORT

**67** ATTENDEES REGISTERED

**271** ATTENDEES ATTENDED

**182** TOTAL ORGANIZATIONS REPRESENTED

#### ATTENDEES PER REGION



**24**

CFP SUBMISSIONS

**3**

KEYNOTES

**16**

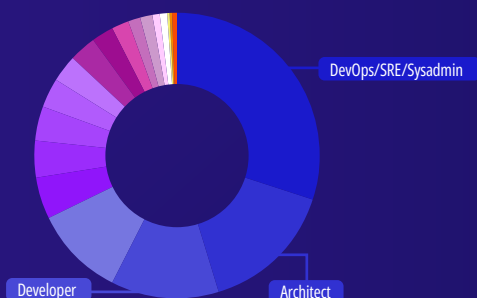
SPEAKERS

**19%**

GENDER MINORITY SPEAKERS

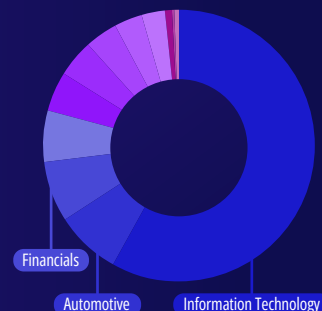
**57%**

POC SPEAKERS



#### Job Function

DevOps/SRE/Sysadmin	30.26%	Manager - OSPO	2.58%
Architect	15.13%	Kernel/Operating Systems Developer	1.85%
Developer	12.18%	IT Operations	1.48%
Other	10.33%	Manager - Technical Teams	1.48%
Executive Leader	4.80%	Professor / Academic	0.74%
Marketing	4.06%	Student	0.74%
Product/Biz Dev	4.06%	Legal / Compliance	0.37%
Application Developer (Front-end/Back-end/Mobile/Full Stack)	3.32%	Manager - Other	0.37%
Business Operations	2.95%	Media / Analyst	0.37%
Systems/Embedded Developer	2.95%		



#### Industry

Information Technology	58.30%
Automotive	7.75%
Financials	7.01%
Telecommunications	6.27%
Professional Services	4.80%
Industrials	4.43%
Non Profit Organization	3.69%
Consumer Goods	3.32%
No Answer	2.95%
Energy	0.74%
Health Care	0.37%
Materials	0.37%

### OpenSSF Community Day North America

JUNE 26, 2025 | DENVER, CO-LOCATED WITH OPEN SOURCE SUMMIT NORTH AMERICA



### OpenSSF Community Day

NORTH AMERICA

DENVER, COLORADO 2025

#OpenSSFCommunity

### POST EVENT REPORT

**149** ATTENDEES REGISTERED

**164** ATTENDEES ATTENDED

**108** TOTAL ORGANIZATIONS REPRESENTED

#### ATTENDEES PER REGION



**72**

CFP SUBMISSIONS

**29**

SESSIONS

**42**

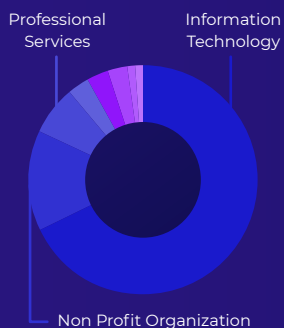
SPEAKERS

**10%**

GENDER MINORITY SPEAKERS

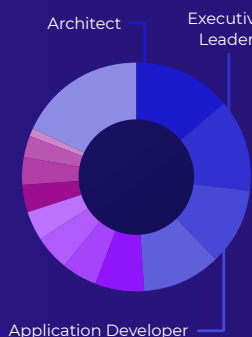
**5%**

POC SPEAKERS



#### Industry

- Information Technology **68%**
- Non Profit Organization **14%**
- Professional Services **7%**
- Consumer Goods **3%**
- Financials **3%**
- Industrials **3%**
- Automotive **1%**
- Telecommunications **1%**



#### Job Function

- Architect **14%**
- Executive Leader **13%**
- Application Developer [Front-end/Back-end /Mobile/Full Stack] **11%**
- Manager - Technical Teams **11%**
- Manager - Other **7%**
- Marketing **5%**
- DevOps/SRE **5%**
- Manager - OSPO **4%**
- Student **4%**
- Product/Biz Dev **4%**
- Legal / Compliance **3%**
- Professor / Academic **1%**
- Other **18%**

### THANK YOU TO OUR SPONSORS



Defense  
Unicorns



DELL Technologies





### OpenSSF Community Day India

AUGUST 4, 2025 | HYDERABAD, CO-LOCATED WITH KUBECON+CLOUDNATIVECON INDIA



OpenSSF Community Day  
INDIA



### OpenSSF Community Day INDIA

August 4, 2025  
HYDERABAD, INDIA  
#OpenSSFCommunity

#### POST EVENT REPORT

**209** ATTENDEES REGISTERED

**232** ATTENDEES ATTENDED

**138** TOTAL ORGANIZATIONS REPRESENTED

#### ATTENDEES PER REGION



**55**

CFP SUBMISSIONS

**17**

SESSIONS

**18**

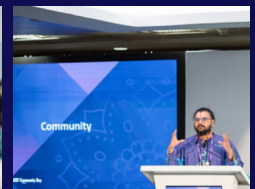
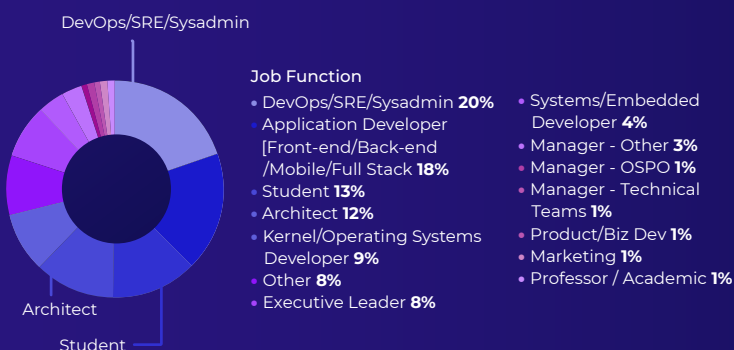
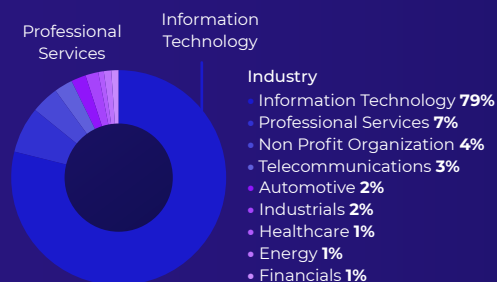
SPEAKERS

**11%**

GENDER MINORITY SPEAKERS

**10**

POC SPEAKERS





### OpenSSF Community Day Europe

AUGUST 28, 2025 | AMSTERDAM, CO-LOCATED WITH  
OPEN SOURCE SUMMIT EUROPE



### OpenSSF Community Day

EUROPE

AMSTERDAM, NETHERLANDS 2025

#OpenSSFCommunity

### POST EVENT REPORT

144

ATTENDEES  
REGISTERED

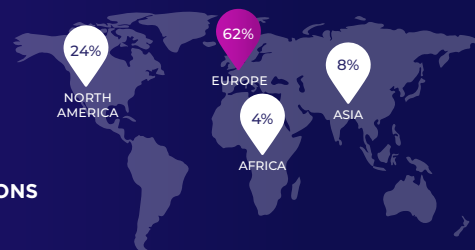
165

ATTENDEES  
ATTENDED

118

TOTAL ORGANIZATIONS  
REPRESENTED

#### ATTENDEES PER REGION



91

CFP SUBMISSIONS

27

SESSIONS

33

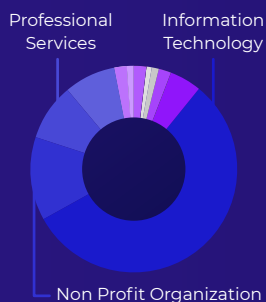
SPEAKERS

18%

GENDER MINORITY SPEAKERS

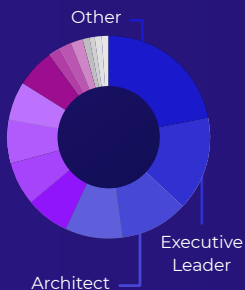
3%

POC SPEAKERS



#### Industry

- Information Technology **56%**
- Non Profit Organization **13%**
- Professional Services **9%**
- Telecommunications **8%**
- Industrials **5%**
- Healthcare **2%**
- Automotive **2%**
- Consumer Goods **2%**
- Energy **1%**
- Financials **1%**
- Materials **1%**



#### Job Function

- Other **23%**
- Executive Leader **15%**
- Architect **12%**
- Manager - Other **9%**
- Systems/Embedded Developer - Other **7%**
- Application Developer (Front-end/Back-end/Mobile/Full Stack) **7%**
- Manager - Technical Teams **7%**

- Manager - Technical Teams **7%**
- DevOps/SRE/Sysadmin **6%**
- Manager - OSPO **5%**
- Kernel/Operating Systems Developer **2%**
- Legal / Compliance **2%**
- Marketing **2%**
- Media / Analyst **1%**
- Professor / Academic **1%**
- Product/Biz Dev **1%**



#### THANK YOU TO OUR SPONSORS

BREAKS



RECEPTION



### European Open Source Security Forum

OCTOBER 30, 2025



BRUSSELS, BELGIUM

#OSSecurityForum

### POST EVENT REPORT

**81** ATTENDEES REGISTERED

**125** ATTENDEES ATTENDED

**100** TOTAL ORGANIZATIONS REPRESENTED

**3**

KEYNOTES

**7**

BREAKOUT SESSIONS

**21**

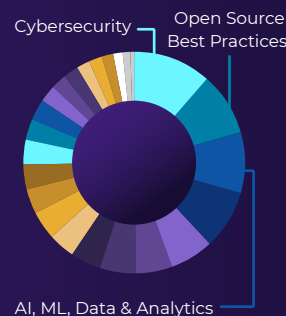
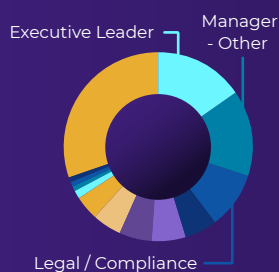
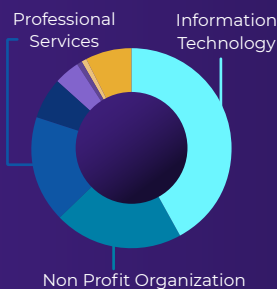
SPEAKERS

**5**

GENDER MINORITY SPEAKERS

**2**

POC SPEAKERS



### OpenSSF Community Day Korea

NOVEMBER 4, 2025 | SEOUL, CO-LOCATED WITH  
OPEN SOURCE SUMMIT KOREA



## OpenSSF Community Day

KOREA

2025 November 4  
SEOUL, KOREA  
#OpenSSFCommunity

### POST EVENT REPORT

**207** TOTAL ATTENDEES  
REGISTERED

**165** TOTAL ORGANIZATIONS  
REPRESENTED

**28**

CFP SUBMISSIONS

**13**

SPEAKERS

**3**

GENDER MINORITY SPEAKERS

**2**

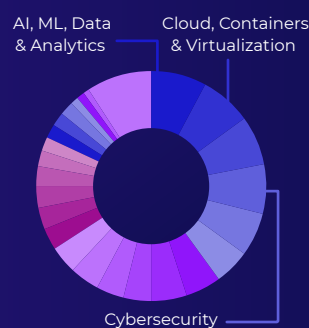
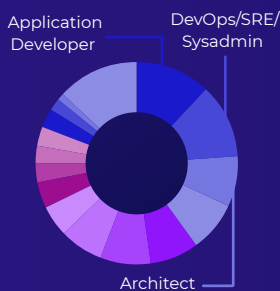
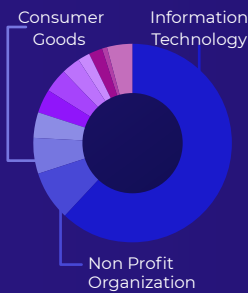
POC SPEAKERS

**8**

BREAKOUT SESSIONS

**3**

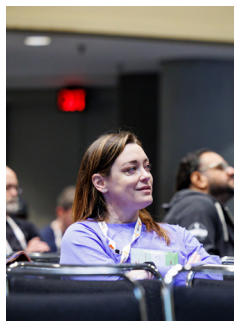
KEYNOTES



- Systems/Embedded Developer **5%**
- Marketing **4%**
- Legal / Compliance **3%**
- Manager - OSPO **3%**
- Manager - Other **3%**
- Professor / Academic **3%**
- Product/Biz Dev **2%**
- Media / Analyst **1%**
- Other **13%**

## Open Source SecurityCon North America

NOVEMBER 10, 2025 | ATLANTA, CO-LOCATED WITH  
KUBECON+CLOUDNATIVECON NORTH AMERICA



ATLANTA, GEORGIA

#securitycon

## POST EVENT REPORT

**152**

SUBMITTED PROPOSALS

**35**

SESSIONS

**46**

SPEAKERS

**38%**

WOMEN OR NON-BINARY

**40**

COMPANIES REPRESENTED

### SPONSORSHIP

DIAMOND SPONSORS



PLATINUM SPONSORS



GOLD SPONSOR





## Education & Training

*\*These numbers have been updated as of November 4, 2025.*

### Developing Secure Software (LFD121)

2025 Enrollment: 6,127  
Total Enrollment: 27,254

### Security for Software Development Managers (LFD125)

2025 Enrollment: 1,485  
Total Enrollment: 1,485

### Understanding the EU Cyber Resilience Act (CRA) (LFEL1001)

2025 Enrollment: 5,571  
Total Enrollment: 5,571

### Security Self-Assessments for Open Source Projects (LFEL1005)

2025 Enrollment: 705  
Total Enrollment: 1,909

### Securing Projects with OpenSSF Scorecard (LFEL1006)

2025 Enrollment: 851  
Total Enrollment: 2,186

### Automating Supply Chain Security: SBOMs and Signatures (LFEL1007)

2025 Enrollment: 922  
Total Enrollment: 3,367

### Secure AI/ML-Driven Software Development (LFEL1012)

2025 Enrollment: 363  
Total Enrollment: 363

### Securing Your Software Supply Chain with Sigstore (LFS182)

2025 Enrollment: 597  
Total Enrollment: 1,200

### Secure Software Development: Requirements, Design, and Reuse (LFD104x)

2025 Enrollment: 1,012  
Total Enrollment: 8,178

### Secure Software Development: Implementation (LFD105x)

2025 Enrollment: 538  
Total Enrollment: 4,208

### Secure Software Development: Verification and More Specialized Topics (LFD106x)

2025 Enrollment: 372  
Total Enrollment: 3,706

### Developing Secure Software - Japanese (LFD121-JP)

2025 Enrollment: 108  
Total Enrollment: 1,098

### Secure Software Development: Requirements, Design, and Reuse - Japanese (LFD104-JPx)

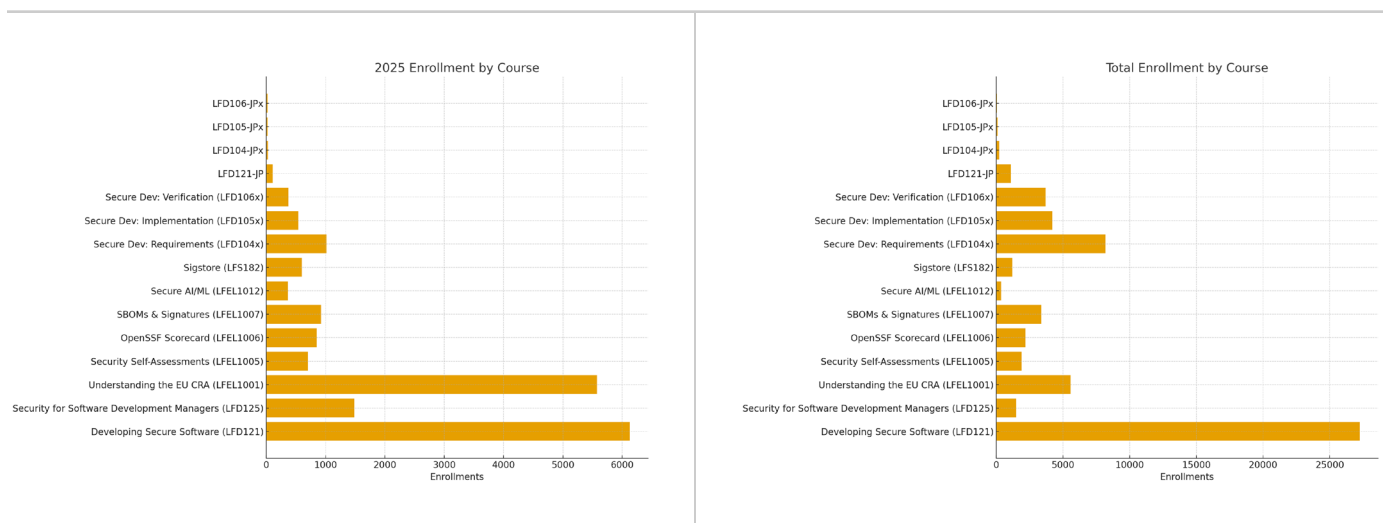
2025 Enrollment: 26  
Total Enrollment: 217

### Secure Software Development: Implementation (LFD105-JPx)

2025 Enrollment: 21  
Total Enrollment: 92

### Secure Software Development: Verification and More Specialized Topics (LFD106-JPx)

2025 Enrollment: 21  
Total Enrollment: 54



## Podcast



In 2025, OpenSSF launched Season two of “What’s in the SOSS?” a bi-weekly podcast hosted by **OpenSSF Chief Security Architect, Christopher Robinson (aka “CRob”)** and welcomed a new co-host **Microsoft Sr. Security Program Manager, Yesenia Yser**. The show continues to expand its reach and impact, delivering deep-dive conversations about topics driving the future of OSS security, including:

- The **Cyber Resilience Act** and global policy frameworks
- **AI/ML security and MLSecOps**
- Sustainable stewardship and **OSS maintainers’ well-being**
- **Trusted publishing** and secure software delivery practices
- **SBOMs**, vulnerability disclosures, and supply chain standards
- Community collaboration across critical open source infrastructure

Episodes now regularly feature **member-spotlight conversations** and **innovation showcases**, giving organizations a platform to share real-world outcomes from investments in secure development.

REACHED OVER 10,000 TOTAL DOWNLOADS ON PODCAST PLAYERS

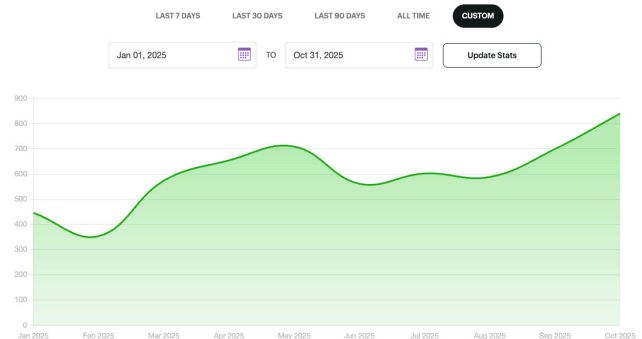


**10,000 Podcast Downloads**






Congrats from  Buzzsprout

**6,025 DOWNLOADS IN 2025**

**6,025 downloads** from **Jan 01, 2025** to **Oct 31, 2025**



**MOST POPULAR APPLICATIONS FOR DOWNLOADS**

	Apple Podcasts	24%	2,724
	Buzzsprout Embed Player	23%	2,640
	Spotify	15%	1,708
	Antenna Pod	8%	907
	Overcast	7%	805

## Most Popular Episodes of 2025

### [KUSARI'S MICHAEL LIEBERMAN TALKS GUAC, SLSA AND SECURING THE OPEN SOURCE SUPPLY CHAIN](#)



**Kusari's Michael Lieberman Talks GUAC, SLSA and Secu**  
What's in the SOSS? An OpenSSF Podcast


15 30 1x More Info Share

00:00 | 21:06

Published on January 07, 2025

**309 DOWNLOADS**

### [RACING AGAINST QUANTUM: THE URGENT MIGRATION TO POST-QUANTUM CRYPTOGRAPHY WITH KEYFACTOR'S CRYPTO EXPERTS](#)



**Racing Against Quantum: The Urgent Migration to Post-**  
What's in the SOSS? An OpenSSF Podcast

15 30 1x More Info Share

00:00 | 30:19

Published on September 09, 2025

**239 DOWNLOADS**

## Cybersecurity Framework Launch



**Cybersecurity Framework Launch**  
What's in the SOSS? An OpenSSF Podcast

15 30 1x More Info Share

00:00 | 20:45

Published on May 20, 2025

**220 DOWNLOADS**

### Blogs

In 2025, the OpenSSF blog continued to be a central hub for open source security insights, featuring original articles, guest contributions, and cross-posts from partners and member organizations. Our thought leadership covered a wide spectrum of topics, from AI/ML security, SBOMs, and supply chain integrity to global policy engagement and community events. Together, these stories reflect the breadth of collaboration, technical innovation, and shared learning that define the OpenSSF community:

1. [SBOMs in the Era of the CRA: Toward a Unified and Actionable Framework](#)
2. [A New Course on Secure AI/ML-Driven Software Development](#)
3. [Announcing the Sigstore Transparency Log Research Dataset](#)
4. [OpenSSF Scorecard Audit is Complete!](#)
5. [Building Security in Open Source for Financial Services: OpenSSF at Open Source in Finance Forum \(OSFF\)](#)
6. [KubeCon + CloudNativeCon North America 2025 Co-Located Event Deep Dive: Open Source SecurityCon](#)
7. [Recap: OpenSSF Tech Talk on Securing the AI Lifecycle](#)
8. [Open Infrastructure is Not Free: A Joint Statement on Sustainable Stewardship](#)
9. [From Beginner to Builder: Your First Code Contribution](#)
10. [From Ghent to Brussels: OpenSSF's Week of Policy and Security in Europe](#)
11. [Improving Risk Management Decisions with SBOM Data: A New Whitepaper from the OpenSSF SBOM Everywhere SIG](#)
12. [New OpenSSF Guidance on AI Code Assistant Instructions](#)
13. [Celebrating the Community: OpenSSF at Open Source Summit and OpenSSF Community Day Europe Recap](#)
14. [Open Source Friday with OpenSSF – Global Cyber Policy Working Group](#)
15. [Recap: OpenSSF Community Day India 2025](#)
16. [OpenSSF Community Day Korea 2025 Agenda Live!](#)
17. [OpenSSF Celebrates Global Momentum, AI/ML Security Initiatives and Golden Egg Award Winners at Community Day Europe](#)
18. [Trustify joins GUAC](#)
19. [What Not to Miss at Open Source Summit & OpenSSF Community Day Europe](#)
20. [Case Study: How LFX Insights and OSPS Baseline Validated GUAC's Security in Under an Hour](#)
21. [OpenSSF at Black Hat USA 2025 & DEF CON 33: AIxCC Highlights, Big Wins, and the Future of Securing Open Source](#)
22. [Securing AI: The Next Cybersecurity Battleground](#)
23. [From Beginner to Builder: Understanding OpenSSF Community and Working Groups](#)
24. [OpenSSF at DEF CON 33: AI Cyber Challenge \(AIxCC\), MLSecOps, and Securing Critical Infrastructure](#)
25. [Visualizing Secure MLOps \(MLSecOps\): A Practical Guide for Building Robust AI/ML Pipeline Security](#)
26. [Celebrating Five Years of OpenSSF: A Journey Through Open Source Security](#)
27. [Speaking, Volunteering, Parenting, and Exploring Nature — My Week at OSS Summit NA 2025](#)
28. [Case Study: Google Secures Machine Learning Models with sigstore](#)
29. [Building India's Open Source Security Community: Join Us in Hyderabad!](#)
30. [New: Cyber Resilience Act \(CRA\) Brief Guide for OSS Developers](#)
31. [Recap: OpenSSF Community Day North America 2025](#)
32. [Recap: OpenSSF Community Day Japan 2025](#)
33. [On-Demand Webinar: Cybersecurity Skills, Simplified](#)



34. [OpenSSF at UN Open Source Week 2025: Securing the Supply Chain Through Global Collaboration](#)
35. [OpenSSF Welcomes New Members and Presents Golden Egg Award](#)
36. [An Introduction to the OpenSSF Model Signing \(OMS\) Specification: Model Signing for Secure and Trusted AI Supply Chains](#)
37. [Member Spotlight: Datadog – Powering Open Source Security with Tools, Standards, and Community Leadership](#)
38. [OpenBao Joins the OpenSSF to Advance Secure Secrets Management in Open Source](#)
39. [Tech Talk Recap | CRA-Ready: How Open Source Projects Can Prepare for the EU Cyber Resilience Act](#)
40. [Case Study: OSTIF Improves Security Posture of Critical Open Source Projects Through OpenSSF Membership](#)
41. [GUAC 1.0 is Now Available](#)
42. [Maintainers' Guide: Securing CI/CD Pipelines After the tj-actions and reviewdog Supply Chain Attacks](#)
43. [From Sandbox to Incubating: gittuf's Next Step in Open Source Security](#)
44. [Choosing an SBOM Generation Tool](#)
45. [OSS and the CRA: am I a Manufacturer or a Steward?](#)
46. [Member Spotlight: Trail of Bits – Driving Open Source Security Through Standards, Prototypes, and Policy](#)
47. [Call for Proposals Now Open for Open Source SecurityCon 2025](#)
48. [Case Study: Ericsson's C/C++ Compiler Options Hardening Guide and OpenSSF Collaboration](#)
49. [Call for Proposals for OpenSSF Community Day Europe Open Through 26 May, 2025](#)
50. [Announcing the Summer 2025 OpenSSF Mentorship Program](#)
51. [New Guide on Simplifying Software Component Updates](#)
52. [OpenSSF Tech Talk Recap: Using the OSPS Baseline to Navigate Standards and Regulations](#)
53. [Recognizing Academic Excellence in Open Source and Secure Software Education](#)
54. [OpenSSF Launches Free Course to Prepare Developers for the EU Cyber Resilience Act](#)
55. [Announcing the Release of "The Memory Safety Continuum"](#)
56. [Repository Service for The Update Framework \(RSTUF\) Reaches New Security Milestone with Successful Audit](#)
57. [Vulnerability Enumeration Conundrum – an Open Source Perspective on CVE and CWE](#)
58. [NEW FREE COURSE: Understanding the EU Cyber Resilience Act \(CRA\) \(LFEL1001\)](#)
59. [Key Takeaways from VulnCon 2025: Insights from the OpenSSF Community](#)
60. [Tech Talk Preview: Strengthening Open Source Through Security Standards and Global Policy](#)
61. [OpenSSF Community Day NA 2025 Agenda Live!](#)
62. [Launch of Model Signing v1.0: OpenSSF AI/ML Working Group Secures the Machine Learning Supply Chain](#)
63. [GuardDog: Strengthening Open Source Security Against Supply Chain Attacks](#)
64. [Beyond the Software Bill of Materials \(SBOM\): Ensuring Integrity with Attestations – Event Recap](#)
65. [What will my business need to do for the EU CRA?](#)
66. [Linux Foundation Research Reports Reveal Wide Spectrum for Cyber Resilience Act Readiness and Compliance](#)
67. [CNCF & OpenSSF Announce Open Source SecurityCon 2025](#)
68. [OpenSSF Policy Summit DC 2025 Recap](#)

69. [OpenSSF Hosts 2025 Policy Summit in Washington, D.C. to Tackle Open Source Security Challenges](#)
70. [NEW FREE COURSE: Security for Software Development Managers \(LFD125\)](#)
71. [2025 OpenSSF Content Themes: Strengthening Open Source Security Throughout the Year](#)
72. [FOSDEM 2025: OpenSSF Community Wrap Up](#)
73. [OpenSSF Announces Initial Release of the Open Source Project Security Baseline](#)
74. [Does the EU CRA affect my business?](#)
75. [Securing Public Sector Supply Chains is a Team Sport](#)
76. [Linux Foundation Europe and OpenSSF Launch Initiative to Prepare Maintainers, Manufacturers, and Open Source Stewards for Global Cybersecurity Legislation](#)
77. [Alpha-Omega 2024 Annual Report](#)
78. [OpenSSF Community Day NA 2025: Call for Proposals Now Open!](#)
79. [Predictions for Open Source Security in 2025: AI, State Actors, and Supply Chains](#)
80. [Accelerating OpenSSF Adoption: Unlocking Scorecard Insights with a Centralized Dashboard](#)
81. [SOSS Community Day India 2024: Wrap Up](#)
82. [CRA Stewards and Manufacturers Workshop: Key Takeaways and Next Steps](#)
83. [Staying OSS Safe During the Holidays](#)
84. [SigstoreCon 2024: Advancing Software Supply Chain Security](#)
85. [Understanding the CRA: OpenSSF's Role in the Cyber Resilience Act Implementation – Part 1](#)
86. [Understanding the CRA: OpenSSF's Role in the Cyber Resilience Act Implementation – Part 2](#)
87. [In the Face of Mounting Regulatory Oversight, Honda and Guidewire Join Industry Leaders Securing Software Development at the Open Source Security Foundation \(OpenSSF\)](#)
88. [The OpenSSF 2024 Annual Report Is Live!](#)
89. [Open Source Usage Trends and Security Challenges Revealed in New Study](#)
90. [Shaping the Future of Generative AI: A Focus on Security](#)
91. [The OpenSSF Armored Goose "Honk": Advancing Open Source Security](#)
92. [How We Can Learn from Open Source Software to Address the Challenges of AI](#)
93. [Red Hat's Collaboration with the OpenSSF and OSV.dev Yields Results: Red Hat Security Data Now Available in the OSV Format](#)

## TOP BLOGS

[Open Infrastructure is Not Free: A Joint Statement on Sustainable Stewardship](#)

9,383 VIEWS

[Predictions for Open Source Security in 2025: AI, State Actors, and Supply Chains](#)

1,877 VIEWS

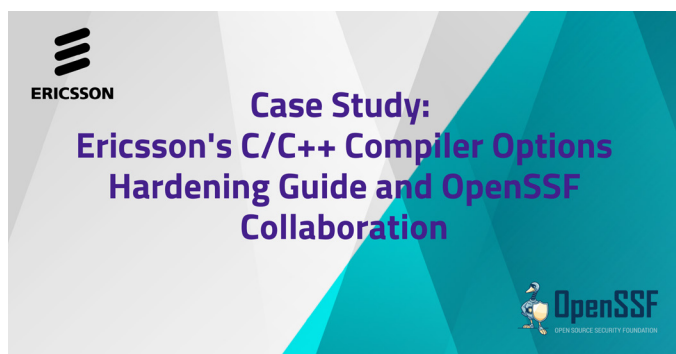
[Launch of Model Signing v1.0: OpenSSF AI/ML Working Group Secures the Machine Learning Supply Chain](#)

1,496 VIEWS

## Case Studies

In 2025, OpenSSF members showcased real-world impact through collaborative case studies highlighting how open source security tools and best practices strengthen software ecosystems. From Ericsson's compiler hardening work and OSTIF's project audits to Google's secure model signing with Sigstore and GUAC's rapid validation using OSPS Baseline, these stories demonstrate the tangible benefits of collective security innovation.

[Case Study: Ericsson's C/C++ Compiler Options Hardening Guide and OpenSSF Collaboration](#)



[Case Study: OSTIF Improves Security Posture of Critical Open Source Projects Through OpenSSF Membership](#)



[Case Study: Google Secures Machine Learning Models with sigstore](#)



[Case Study: How LFX Insights and OSPS Baseline Validated GUAC's Security in Under an Hour](#)





## Tech Talk

In 2025, OpenSSF continued expanding our educational and community outreach efforts by launching a new series of **virtual Tech Talks**. These sessions are designed to deepen understanding of OpenSSF's tools, frameworks, and initiatives that strengthen the security of open source software. Each Tech Talk brings together project maintainers, technical contributors, and security practitioners to explore practical applications and lessons learned across the ecosystem.

All Tech Talk recordings are available on the [OpenSSF YouTube channel](#), and presentation decks can be accessed through the [OpenSSF Tech Talk page](#). Here are some examples:

### [Simplifying DevSecOps in Air-Gapped Environments with Zarf](#)

Nov 6, 2025

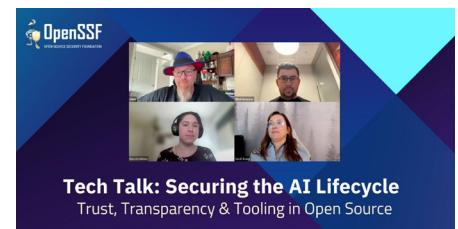
This session introduced **Zarf**, an OpenSSF project that simplifies software delivery in air-gapped and semi-connected environments. Attendees learned how Zarf's **declarative packaging strategy** helps keep Kubernetes and cloud-native workloads secure and operational even without internet access.



### [Securing the AI Lifecycle: Trust, Transparency & Tooling in Open Source](#)

Sep 24, 2025

This 50-minute Tech Talk explored how open source projects and contributors are building **trust into the AI/ML supply chain**, focusing on model signing, reproducibility, metadata, and secure development practices. The discussion highlighted how open collaboration supports responsible and transparent AI.



### [CRA-Ready: How to Prepare Your Open Source Project for EU Cybersecurity Regulations](#)

Jun 12, 2025

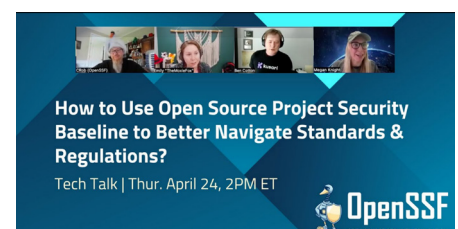
Earlier this year, with the **EU Cyber Resilience Act (CRA)** on the horizon, this session guided participants through how open source projects can proactively align with new cybersecurity requirements. Speakers shared best practices and resources for staying compliant and building resilience early.



### [How to Use the Open Source Project Security Baseline to Better Navigate Standards & Regulations](#)

Apr 24, 2025

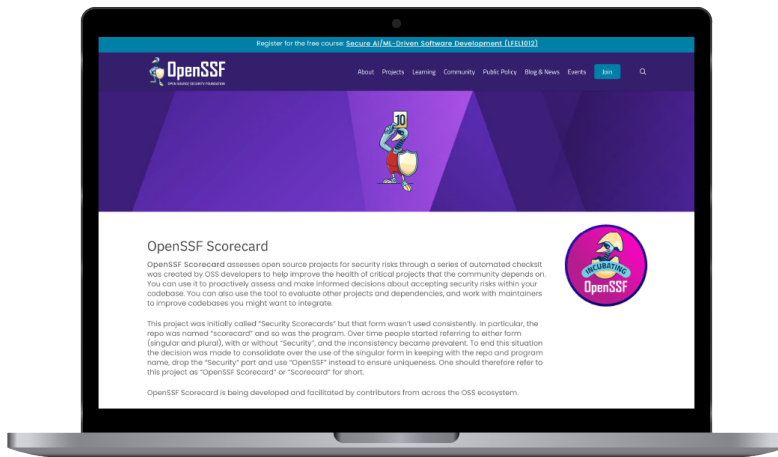
This Tech Talk demonstrated how to apply the **Open Source Project Security Baseline (OSPS Baseline)** to strengthen project security posture and simplify compliance with emerging standards. Attendees gained actionable insights for integrating the baseline into their workflows to support more secure and sustainable open source development.



## Social Media & Website Metrics

*\*These numbers have been updated as of October 31, 2025*

### Website



**360,536** PAGE VIEWS  
(Sources) (20% YoY Growth)

#### Top 3 pages of the year and numbers

<a href="#">OpenSSF Scorecard</a>	<b>14,113</b>
<a href="#">OpenSSF Education</a>	<b>11,828</b>
<a href="#">Open Infrastructure is Not Free: A Joint Statement on Sustainable Stewardship Blog</a>	<b>9,175</b>

### Newsletter



**11,453**  
SUBSCRIBERS



**39.33%**  
AVERAGE  
OPEN RATE



**7.15 %**  
AVERAGE  
CLICK-THROUGH  
RATE



**47,007**  
TOTAL VIEWS

## LinkedIn



**Top Post:** Security Risks Related to Downloading and Running LLMs Locally at #OpenSSFCommunity Day Europe



**12,212** FOLLOWERS  
(44.4% YOY GROWTH)



**365** POSTS

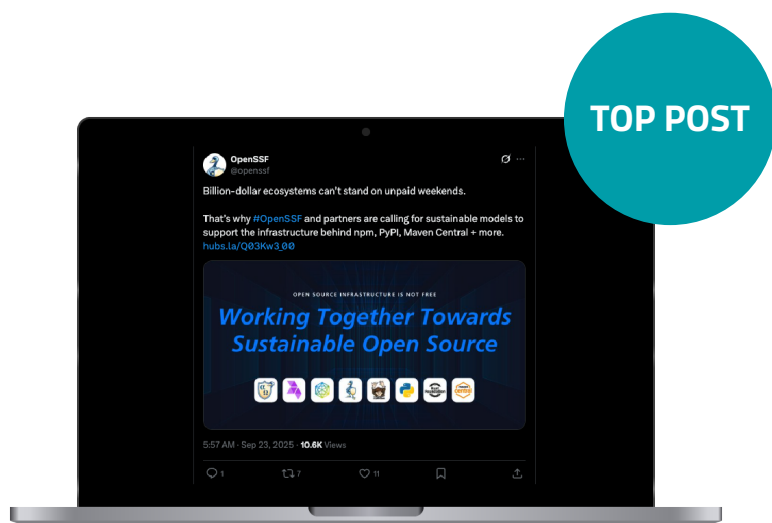


**575,779** IMPRESSIONS



**6.2 %** ENGAGEMENT RATE

## X



**5,705** FOLLOWERS  
(2.4% YOY GROWTH)

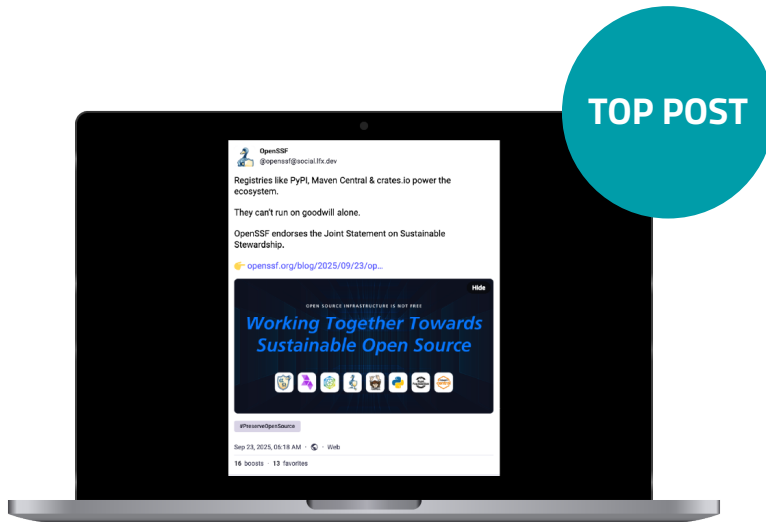


**336** POSTS



**1,482** INTERACTIONS

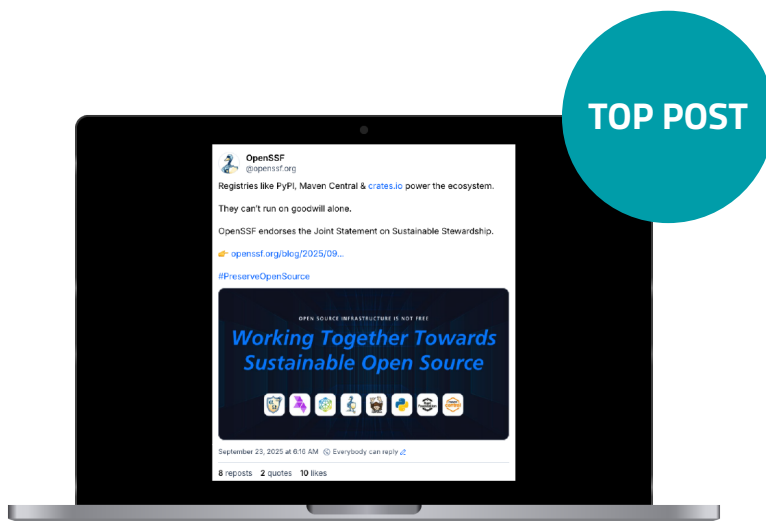
### Mastodon



  
**1,200** FOLLOWERS  
 (34.08 % YOY GROWTH)

  
**397** POSTS

### Bluesky



  
**1,783** FOLLOWERS

  
**218** POSTS



## YouTube

TOTAL YOUTUBE CHANNEL VIEWS  
**97,563**

**TOP  
VIDEO**



**MOST WATCHED VIDEO 374 VIEWS**

[OpenSSF Tech Talk: How to use the OSPS Baseline to Better Navigate Standards and Regulations](#)



**1,940** SUBSCRIBERS  
(44.78% YOY GROWTH)



**244** VIDEOS

## GitHub



**212** CLOSED ISSUES

**81** REPOS

**24** PROJECTS

**88** TEAMS

**149** PEOPLE

**472** ACTIVE CONTRIBUTORS

**200** ACTIVE ORGANIZATIONS

**1146** PULL REQUESTS

**Slack**

 **4,865** USERS

**Stay Connected!**



# Looking Ahead to 2026



2025 was an important year for the OpenSSF – it was a year of measurable progress, global collaboration, and growing maturity as we celebrated five years of collective impact.

A key highlight of 2025 was the tangible impact of Technical Initiative (TI) funding, with the Technical Advisory Council awarding over \$660,000 across 14 initiatives. These investments strengthened supply chain integrity, advanced transparency tooling like Sigstore, supported new specifications such as Model Signing, and enabled community-driven security audits through Alpha-Omega.

As we look ahead to 2026, OpenSSF's focus will deepen around three core goals:

### 1. Scaling adoption and measurable outcomes

We will expand the reach and interoperability of OpenSSF tools, frameworks, and training to embed security into everyday development and measure their ecosystem-wide impact.

### 2. Strengthening technical investment

We'll continue to grow and evolve our TI funding model to accelerate innovation, expand cross-foundation collaboration, and support the maintainers securing the world's most widely used software.

### 3. Driving global alignment and readiness

Through ongoing engagement with governments, standards bodies, and community partners, we will ensure that emerging cybersecurity frameworks, such as the EU Cyber Resilience Act, work in harmony with open source practices.

The work ahead will demand the same transparency, creativity, and shared responsibility that have defined OpenSSF from day one. Together, with our members, contributors, and partners, we will continue building trust and resilience across the software that powers our world.

OpenSSF remains steadfast in its mission: to secure open source for everyone, everywhere.

## 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](#), [Mastodon](#) and [Youtube](#).
- **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.





# Acknowledgments

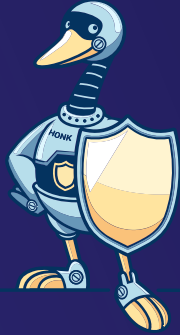
The OpenSSF 2025 Annual Report is the product of a truly global effort across our community. We extend our sincere appreciation to the **Working Group and Project Leads, Technical Advisory Council, and Governing Board** for their leadership, technical excellence, and continued commitment to securing the open source software ecosystem.

A special thank you to our **members and contributors** across 40+ countries whose dedication powers every milestone highlighted in this report.

We also want to recognize the **Marketing Advisory Council, Developer Relations Community, and OpenSSF staff** for their creativity, coordination, and clear communication that bring these achievements to life. Additional thanks to the **Linux Foundation Creative Services, Marketing & PR, Program Management** and **Event teams** for their partnership in developing, designing, and delivering this report.

Finally, to every individual who organized events, event sponsors, mentored contributors, authored resources, or simply championed OpenSSF's mission this year – thank you. All of you have helped improve the security of the open source that we all depend on. The progress reflected in these pages belongs to all of you.





# OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Let's work together to build a secure, resilient  
open source ecosystem. Join us today and help  
make 2026 our most impactful year yet!

[openssf.org/getinvolved](https://openssf.org/getinvolved)

openssf.org

