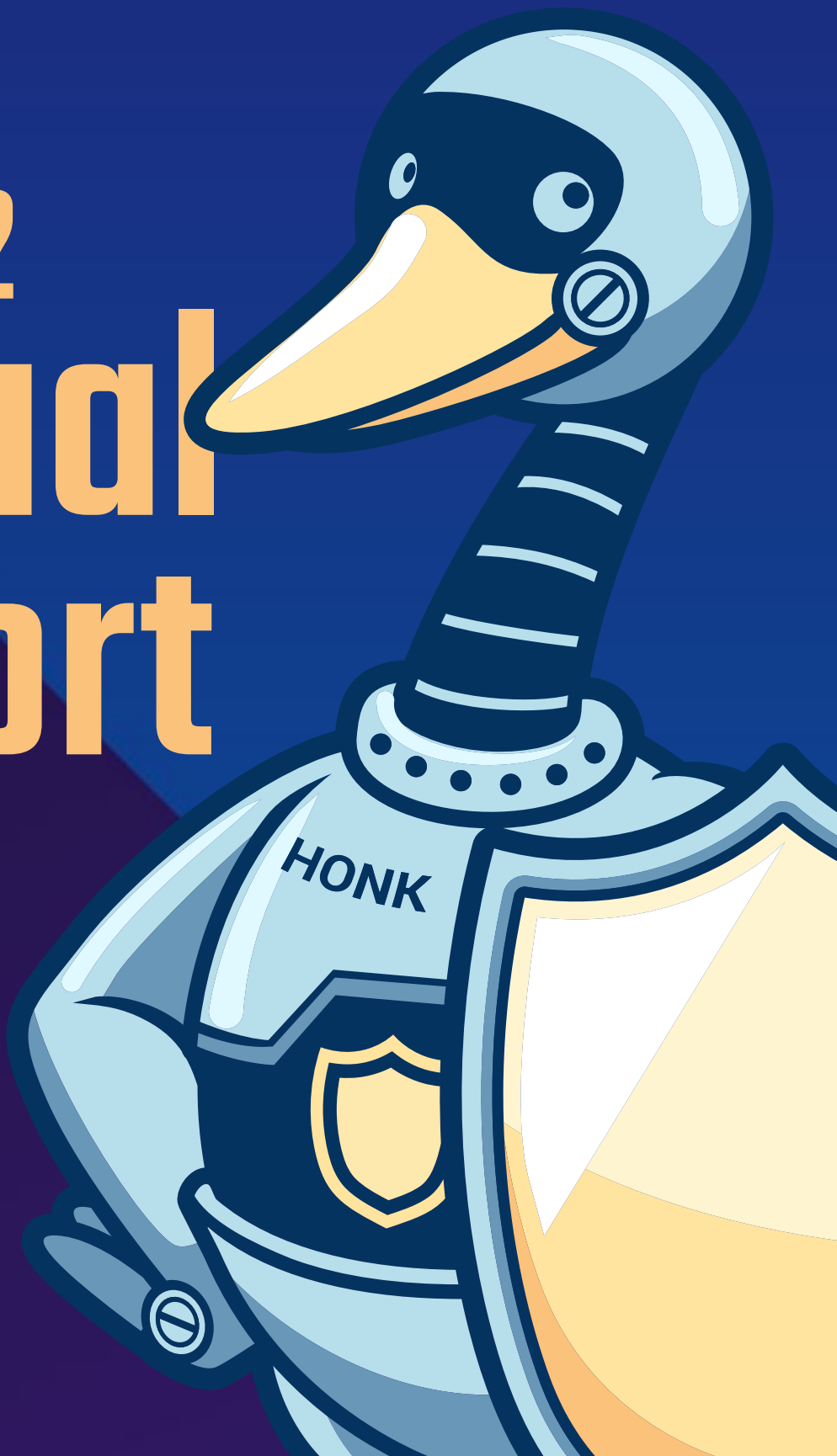
OpenSSF

OPEN SOURCE SECURITY FOUNDATION

2022 Annual Report



openssf.org

Contents

From the General Manager **3**
OpenSSF Members **4**
From the Governing Board Chair **5**
Governing Board Members **6**
2022 Highlights **7**
Open Source Software Security Mobilization Plan **10**
From the Technical Advisory Council Chair **12**
TAC Members **13**
Working Groups **14**
Best Practices for Open Source Developers 14
End Users 15
Identifying Security Threats in Open Source Projects 16
Securing Critical Projects 17
Securing Software Repositories 18
Security Tooling 19
Supply Chain Integrity 20
Vulnerability Disclosures 21
Associated Projects **22**
Alpha-Omega 22
Sigstore 25
Community Engagement **27**

From the General Manager

The Open Source Security Foundation (OpenSSF) is a global collaborative that brings together a community of security experts and security-focused organizations to improve the overall level of security in the open source software ecosystem, and address weaknesses in the global software supply chain. In 2022, we had an impressive year building upon our existing initiatives and creating a foundation for new initiatives and areas of engagement. We expect to build upon our successes and accomplish even more to benefit the open source community in 2023.

The OpenSSF is a thriving, diverse, nonstop community. Across more than 30 different active software projects and technical initiatives, we've been able to have the kind of reach and impact we need to put a dent in the global software security challenges we all know are only getting more intense and more costly.

This is the year that nation-states woke up to the need to consider, incorporate, and invest into the security of open source software, as a part of ensuring the reliability of critical infrastructure. This community is rising to meet that awareness with the kind of rough consensus and running code required to make these efforts truly cross-industry.

Over the course of 2022, OpenSSF membership grew to over one hundred organizations of all kinds. More than six hundred different individuals contributed to our technical initiatives.

"The OpenSSF is committed to collaboration and working both upstream and with existing communities to advance open source security for all."

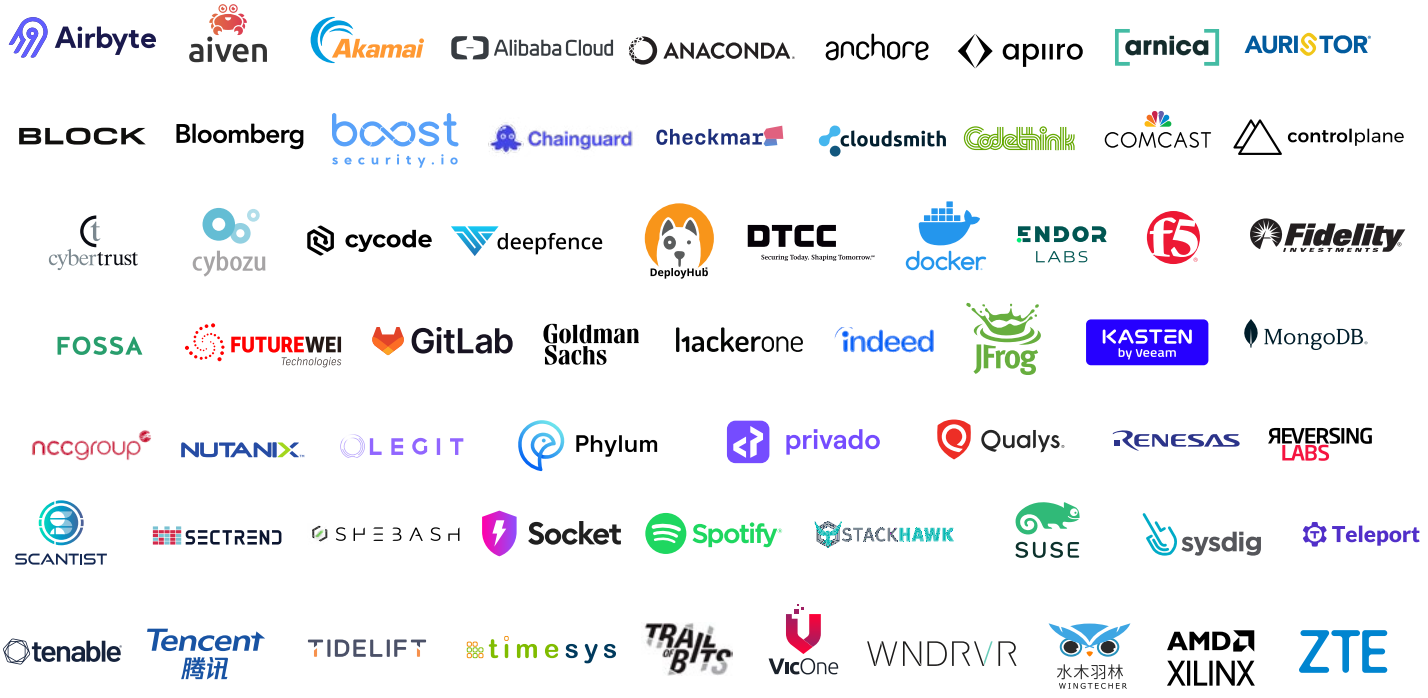
In this annual report, we hear from the Chairs of the Governing Board (GB) and Technical Advisory Council (TAC), take a look at a few of the top highlights of 2022, introduce you to our Working Groups (WGs) and Associated Projects, review the Open Source Software (OSS) Mobilization Plan we released at the the OSS Summit II in collaboration with the US White House, and discuss the impact the OpenSSF has had throughout the course of the year.

Sincerely,
Brian Behlendorf
General Manager
The Open Source Security Foundation

OpenSSF Members

Premier

General



Associate

From the Governing Board Chair

The OpenSSF Foundation has experienced a very busy 2022, as software supply chain security became a topic of serious discussion in corporate organizations and within governments worldwide. The log4j vulnerability announced at the end of 2021 was a catalyst that increased the urgency for industry cooperation across the technology and commercial sectors. To that end, the OpenSSF was in an influential position to recommend a course of action that could advance the security of open source software, by focusing on the fundamentals of tool chain automation, education, vulnerability remediation and transparency. I would like to thank each member of the Foundation for their vigilance, contributions and efforts during 2022.

Let's talk about some of the OpenSSF highlights of the year. Earlier this year, the White House convened several meetings at which both the Linux Foundation and OpenSSF represented the open source developer and commercial ecosystems to discuss challenges. Specifically, the attendees focused on shared ideas to reduce risk and improve resiliency of the open source supply chain. In the Open Source Software Security Summit II in Washington, DC this spring, we presented a ten point plan that could enhance the security of open source software. The OpenSSF made clear our intent to work with the administration across public and private sectors—an important landmark partnership.

I would also like to acknowledge the community for releasing a free online secure software development training course this spring that rewards learners with a two-year certification from the OpenSSF and Linux Foundation, a significant contribution to our education focus. We also announced general availability of Sigstore, a free digital code signing technology for open source projects, a critical element of our tool chain enhancements. Both of these accomplishments were examples of important actions taken on the ten point plan.

Collaboration continued through the year with the first OpenSSF Days held this year in Austin, Texas, Dublin, Ireland, and Yokohama, Japan. There is nothing like the experience of in person collaboration after a pandemic to solve such critical challenges. It was great to hear announcements about new capability, best practices, grants and priorities from our community.

As you can see, there is still a lot of work to be done and a community mentality is needed to understand that security is the responsibility of each developer and not someone else's problem. I cannot stress enough the importance of injecting energy into the community to maintain the efforts around our security priorities. It has been my honor to serve as the Chair of the Board of Directors to the Open Source Security Foundation over the past year and I look forward to amazing outcomes in 2023.

Sincerely,
Jamie Thomas
Chair of the Board of Directors

Governing Board Members

STEPHEN AUGUSTUS
Head of Open Source, Cisco

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

ERIC BREWER
VP of Infrastructure & Google Fellow, Google

BOB CALLAWAY (TAC CHAIR)
Tech Lead & Manager, Google Open Source Security Team

STEPHEN CHIN
VP of Developer Relations, JFrog

KIT COLBERT
Chief Technology Officer, VMware

IAN COLDWATER
Security Community Individual Representative

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

JENNIFER FERNICK
SVP & Global Head of Research, NCC Group

BRIAN FOX
CTO, Sonatype

ARUN GUPTA
Vice President and General Manager, Open Ecosystem Initiatives, Intel Corporation

MIKE HANLEY
Chief Security Officer, GitHub

JOHN HEIMANN
Vice President, Security Programs, Oracle

RAO LAKKAKULA
Executive Director, JPMorgan Chase

ADRIAN LUDWIG
Chief Trust Officer, Atlassian

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

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

TRACY RAGAN
CEO and Co-Founder, DeployHub

SCOTT ROBERTS
Cloud CISO, Coinbase

CLYDE RODRIGUEZ
Vice President of Engineering, Meta

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

GARETH RUSHGROVE
VP of Product, Snyk

MARK RUSSINOVICH
Azure CTO and Technical Fellow, Microsoft

MARK RYLAND
Director, Office of the CISO AWS Security

SUBHA TATAVARTI
CTO, Wipro

JAMIE THOMAS (BOARD CHAIR)
Enterprise Security Executive, IBM

ANDREW VAN DER STOCK
Executive Director, OWASP Foundation

CHRIS WRIGHT
Senior Vice President and Chief Technology Officer, Red Hat

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2022 Highlights

In January 2022, the US White House, along with leaders and experts of many U.S. federal agencies, convened an important cross-section of the open source developer and commercial ecosystem to identify the challenges in the OSS supply chain and share ideas on how to mitigate risk and enhance resilience. Both the Linux Foundation and OpenSSF participated in this meeting. As a follow-up, the OpenSSF hosted the Open Source Software Security Summit II in May, bringing together over 90 executives from 37 companies and US federal government leaders to reach a consensus on critical actions to improve the resiliency and security of the OSS ecosystem.

During Summit II, the OpenSSF released the Open Source Software Security Mobilization Plan and announced $30 million in pledges to improve OSS security. The Mobilization Plan outlines ten streams of investment to rapidly advance well-vetted solutions to make immediate improvements to OSS security worldwide and build a strong foundation for a more secure future. The overarching goals of the plan include: securing OSS production, improving vulnerability discovery and remediation, and shortening ecosystem patching response time. Throughout 2022, the OpenSSF community has acted on the Mobilization Plan and will continue to do so into 2023 and beyond.

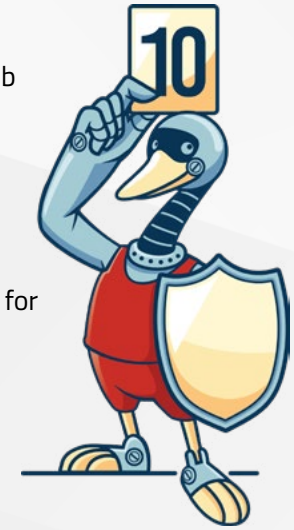
In February 2022, OpenSSF launched the Alpha-Omega Project, an effort to improve the security posture of open source software, with an initial investment of $5 million. The project's "Alpha" portion improves global OSS supply chain security by working with maintainers of the most critical open source projects to help them identify and fix security vulnerabilities. The "Omega" portion focuses on the long tail of OSS projects, helping systematically find and remediate vulnerabilities in at least 10,000 widely deployed open source projects. In 2022, Alpha-Omega issued a cumulative total of over $2 million in grants to the OpenJS Foundation in support of Node.js and jQuery, the Eclipse Foundation, the Python Software Foundation (PSF), and the Rust Foundation.

In October 2022, Sigstore reached general availability at its first ever namesake event, SigstoreCon North America. Sigstore, which facilitates signing, verifying, and protecting software, has continued to see massive contributions and adoption, improving the integrity of the software supply chain and reducing the friction developers face regarding implementing security within their daily work. In June 2022, software developers, DevOps engineers, security engineers, and software maintainers could take the new free course on Securing Your Software Supply Chain with Sigstore.

In developers of critical open source projects' pursuit of encouraging the wider adoption of multi-factor authentication (MFA), the OpenSSF Technical Advisory Council publicly supported, in strong terms, the various efforts to increase the use of MFA in various organizations. The working group also introduced an initial prototype version of the for free MFA tokens to developers of the 100 most critical open source projects in 2021–2022 in what was known as the "Great MFA Distribution."

The Best Practices Working Group introduced an initial prototype version of the Package Analysis Project that addresses the challenge of identifying malicious packages in popular open source repositories.

The Best Practices for Open Source Developers WG increased awareness and education of security best practices through improvements in its free training course Developing Secure Software. This is now available through the Linux Foundation Training & Certification platform, edX, and on various organizations' Learning Management Systems, and it has had over 8,000 enrollments. The course was updated this year to address the attacks that have recently become more prominent (per the CWE Top 25 and OWASP Top 10), as well as adding material to cover topics such as securing systems that use machine learning. The working group also released Concise Guides on Developing More Secure Software and Evaluating Open Source Software and provided an npm Best Practices Guide for those using the popular npm package manager. The OpenSSF Best Practices Badge Program now has over 5,000 participating projects and over 850 passing projects.



The Best Practices WG released new Scorecards features, such as a GitHub Action and REST API, added security checks, scaled-up scans of the open source ecosystem, and badges. Over 1,600 repositories use Scorecards to incorporate best practices into their software development lifecycle for continuous improvement.

The Vulnerability Disclosures WG unveiled the next evolution in improving open source coordination of vulnerability disclosures by crafting a new guide focused on the security researcher or Finder persona with a Guide for Security Researchers to Coordinate Vulnerability Disclosures with Open Source Software Projects.

A key component of the Mobilization Plan is using a software bill of materials (SBOM) as a foundational building block to improve the security posture of the open source ecosystem known as SBOM Everywhere. The SBOM Everywhere Special Interest Group (SIG) sprung up under the Security Tooling WG, and its first effort was to fund work on an SPDX Python library to support SBOM creation and processing.

In June 2022, the Security Tooling WG also released Fuzz Introspector. Many development workflows have come to rely on fuzzing, an automated technique for finding bugs by feeding unexpected inputs into software with the intent to trigger crashes or other problems. Fuzzing plays an important role in vulnerability discovery. However, today fuzzing often hits roadblocks ("blockers") that prevent effective fuzzing of some code areas. Fuzz Introspector provides actionable insights for developers to identify fuzzing coverage blockers so they can be resolved, with the goal of (1) improving projects that use fuzzing and (2) improving fuzzers themselves (by helping tool developers understand current problems).

The OpenSSF Supply Chain Integrity Working Group continues to work on refining the Supply chain Levels for Software Artifacts (SLSA) (pronounced "salsa"). This is a check-list of standards and controls to prevent tampering, improve integrity, and secure packages and infrastructure. A draft is already public, and work continues to refine it for a "version 1.0" release. The working group also began work on the complementary Secure Supply Chain Consumption Framework (S2C2F), to further develop and continuously improve the S2C2F guide. This guide outlines and defines how to securely consume OSS dependencies into the developer's workflow.

The OpenSSF added two new WGs. The Securing Software Repositories WG provides a collaborative environment for aligning on introducing new tools and technologies to strengthen and secure software repositories. The End Users WG represents the interests of public and private sector organizations that primarily consume open source rather than produce it.

We hosted OpenSSF Days in Austin, Dublin, and Yokohama at Open Source Summits North America, Europe, and Japan, as well as an OpenSSF Summit China in Shenzhen, that brought together the open source community to discuss the challenges, big-picture solutions, ongoing work, and successes in securing the OSS supply chain.

In May 2022, OpenSSF GM Brian Behlendorf testified to the U.S. House of Representatives Committee on Science, Space, and Technology about the work being done within the OpenSSF and broader OSS community to improve the security and trustworthiness of open source software.

In June 2022, Jim Zemlin, Executive Director of the Linux Foundation, participated along with government and private-sector leaders in the White House Cyber Workforce and Education Summit, where he discussed approaches on how to develop cybersecurity education that benefits the OSS ecosystem. In December 2022, David A. Wheeler, Director of Open Source Supply Chain Security, was a panelist in a workshop on trustworthy and secure OSS organized by the European Commission.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Open Source Software Security Mobilization Plan

The open source community has become vulnerable to new kinds of attacks on the software supply chain and there have been efforts by many to address those challenges. Those efforts require new processes, new tools, and new initiatives to drive adoption. Heightened interest, particularly by governments of the world, has driven the open source community to respond with **a mobilization plan** to achieve specific security goals.

During the Open Source Software Security Summit II in Washington, DC on May 12–13, 2022, the Linux Foundation and OpenSSF gathered a cross-section of open source developer and commercial ecosystem representatives along with leaders and experts from key U.S. federal agencies to reach a consensus on high-impact actions to take to improve the resiliency and security of open source software. The first-of-its-kind plan to broadly address open source and software supply chain security outlines approximately $150M of funding over two years to rapidly advance well-vetted solutions to the ten major problems facing open source software security. These steps outline concrete actions that are designed to produce immediate improvements and build strong foundations for a more secure future.

FROM THE REPORT

"Smart investments into systematic enhancements in the way OSS is developed, recombined, distributed, and deployed, as well as into specific highly re-used 'critical' pieces, would be a highly leveraged and cost-effective way to reduce the risk for all downstream users. This includes the many proprietary and custom software solutions that incorporate OSS."

The Plan focuses on three overarching goals:

- **Securing OSS Production**: focus on preventing security defects and vulnerabilities in code and open source packages in the first place
- **Improving Vulnerability Discovery & Remediation**: improve the process for finding defects and fixing them
- **Shorten Ecosystem Patching Response Time**: shorten the response time for distributing and implementing fixes

The Plan outlines 10 streams of investment:

1. Baseline Secure Software Development Education
2. Risk Assessment Dashboard for OSS
3. Digital Signatures to Deliver Enhanced Trust
4. Replacement of Non-Memory-Safe Languages
5. Open Source Security Incident Response Team
6. Accelerate Discover and Remediation of New Vulns
7. Third Party Audits/Code Reviews and Remediation
8. Data Sharing to Determine Critical Projects
9. SBOMs Everywhere: Security Use Cases, Tooling
10. Build Systems, Package Managers, and Distribution Systems

From the Technical Advisory Council Chair

The Open Source Security Foundation (OpenSSF) is a community of open source software contributors and users that are working to improve the overall security of the open source ecosystem. Through collaboration on software projects & services, educational materials, and specifications, the OpenSSF delivers prescriptive guidance and tools that helps consumers make more informed decisions about the software they use, and helps producers create and maintain more secure software.

During 2022, the OpenSSF Technical Advisory Council (TAC) approved the creation of two new working groups. The Securing Software Repositories Working Group brings together technical leaders across different programming language ecosystems to discuss and innovate on challenges present in the last mile distribution of software packages to consumers. This unique forum has already generated a survey comparing and contrasting different approaches to security concerns, and identified areas where investment in common services and specifications could yield substantial benefits to all parties.

The End Users Working Group helps to amplify the voice of consumers within the various projects and working groups within the OpenSSF. In addition to ensuring timely feedback is provided on the outputs of the community, the working group also serves as a place where consumer-centric recommendations and best practices guides can be created.

The TAC also approved the creation of a project lifecycle process that aims to bring procedural clarity and enumerate the benefits and expectations of software projects that are part of the OpenSSF. The TAC is hopeful that this process facilitates the creation and/or adoption of additional projects into the foundation that are aligned with our mission and vision for the future of the ecosystem.

Finally, we are excited to see the recent formation of new special interest groups (SIGs), focused on high priority topics such as SBOM adoption, incident response, and education. We sincerely appreciate the contributions of all community members in 2022, and look forward to continuing to innovate on solving the broader security challenges present within the open source ecosystem in 2023 and beyond.

Sincerely,
Bob Callaway, PhD
Chair, OpenSSF Technical Advisory Council

TAC Members

ABHISHEK ARYA
Principal Engineer and Manager, Google Open Source Security Team

AEVA BLACK (TAC VICE CHAIR)
Open Source Hacker, Microsoft Azure Office of the CTO

JOSH BRESSERS
VP of Security, Anchore

BOB CALLAWAY (TAC CHAIR)
Tech Lead & Manager, Google Open Source Security Team

LUKE HINDS
Security Engineering Lead, OCTO, Red Hat

DAN LORENC
CEO, Chainguard

CHRISTOPHER "CROB" ROBINSON
Directory of Security Communications, Intel

Critical Infrastructure Security Summit

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Working Groups

WORKING GROUP

Best Practices for Open Source Developers

This group works to provide open source developers with best practices recommendations and supply easy ways to learn and apply them.

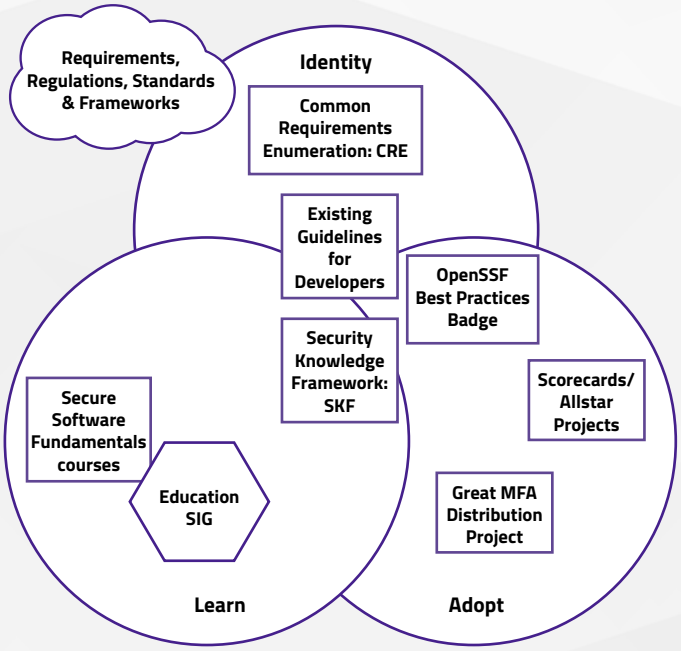
Working Group Git Repo	Working Group Leads	Working Group Membership
github.com/ossf/wg-best-practices-os-developers	Christopher "CRob" Robinson, Intel and Xavier René-Corail, GitHub	18 regular attendees, 20+ intermittent attendees

2022 Highlights

- Concise Guides publication
- OSS-EU OpenSSF Presentation "BEST Practices makes Perfect"
- EDU.SIG

What's Next?

- Publish EDU.SIG Plan
- Secure funding
- Begin work to educate the ecosystem
- C/C++ Compiler Best Practices guide.



WORKING GROUP

End Users

This group represents the interests of public and private sector organizations that primarily consume open source rather than produce it.

Working Group Git Repo	Working Group Leads	Working Group Membership
github.com/ossf/wg-endusers	Jonathan Meadows, Citi and Andrew Aitken, Wipro	15+ representing a strong mix of end users of open source such as banks, transportation, and retail and some producers of open source

Our Mission

The mission of the End Users Working Group is to ensure that the distinct and impactful voice of end users is heard in the development and delivery of the technical vision of the OpenSSF.

Our goals

- Provide the resources required by End Users to develop and implement more efficient and effective strategies, processes, tools, best practices and solutions that secure software supply chains.
- Ensure that the use cases for end user consumption of open source software are understood and factored into OpenSSF programs.
- Provide a forum for learning from the experience and insights of peers.
- Include broad representation from key private industry, public sectors, and multiple geographical regions.
- Establish user representation and active participation in OpenSSF working groups and leadership, both in the TAC and the Governing Board.

2022 Highlights

- Launched the working group with active participation from over 10 organizations.
- Defined an end user threat taxonomy to demonstrate how to align multiple capabilities and pertinent projects to identify and mitigate supply chain and open source software risk.
- Created a set of draft architectures for the consumption of 3rd party software, commercial and open source, across all layers of the software stack from applications and mobile apps down to container technologies and operating systems.
- Participation by members in each relevant OpenSSF working group to ensure the voice of the consumer is incorporated as new initiatives are proposed.

What's Next

- Continued recruitment of end users to ensure all major verticals and geographies are represented.
- Finalization of threat taxonomy and acceptance as standard by OpenSSF.
- Finalization of consumption architectures and acceptance by OpenSSF.

WORKING GROUP

Identifying Security Threats in Open Source Projects

This group enables informed confidence in the security of OSS by collecting, curating, and communicating relevant metrics and metadata.

Working Group Git Repo	Working Group Leads	Working Group Membership
github.com/ossf/wg-identifying-security-threats	Michael Scovetta, Microsoft	10-15 members

Our Purpose

To enable stakeholders to have informed confidence in the security of open source projects. We do this by collecting, curating, and communicating relevant metrics and metadata from open source projects and the ecosystems of which they are a part.

Everyone is welcome to participate in our working group and help build the future. Find us on the OpenSSF public calendar.

2022 Highlights

- Metrics Dashboard provides information on open source software (OSS) packages/projects to help users and potential users to evaluate their risks. We have developed a prototype and are in the early stages of building a full dashboard based on that experience. We expect it will build on the OpenSSF Scorecards, OpenSSF Best Practices badge, contribution data, and vulnerability data (among other data sources).
- Security Reviews collects and curates security reviews performed against OSS, to enable easily finding this information. We published 104 new reviews in 2022.
- Office Hours provides a forum for maintainers to talk to security experts about any (security-related) topic. The first session didn't have any non-expert registrants, which suggests to us the need for more lead time and publicity targeted at potential requestors.
- Security Insights provides a way for OSS maintainers to express information regarding security posture and practices in place in the project in both human-readable and machine-readable format (YAML).

Impact

Growing participation and discussion of what metrics are important for human understanding of risks in OSS projects/packages.

What's Next

- A Virtual Maintainer Summit is being planned for January 2023.
- The Metrics Dashboard SIG is working on scenarios and mockups.
- We'll be scheduling additional Office Hours in early 2023, along with more lead time and publicity targeted at potential registrants.
- We regularly discuss potential new projects; come join in the conversation!

WORKING GROUP

Securing Critical Projects

This group exists to identify and help to allocate resources to secure the critical open source projects we all depend on.

Working Group Git Repo	Working Group Leads	Working Group Membership
github.com/ossf/wg-securing-critical-projects	Amir Montazery, OSTIF and Jeff Mendoza, Google	Average 8-15 participants per meeting

2022 Highlights

- First cut of a set of 100 critical open source projects.
  - » Currently we are refining the process for curating and prioritizing this set.
- Set of 50 projects recommended for security audit.
  - » This was based on the first cut set of 100 followed by some further analysis by the Open Source Technology Improvement Fund.
- Contributed to a number of projects:
  - » Criticality Score
  - » Allstar
- Thanks to funding from OpenSSF and GOSST, Strategic Partner Open Source Technology Improvement Fund (OSTIF) was able to accomplish the following in 2022:

22

Vulnerabilities & CVEs Found and Fixed

9

Critical/High (CVSS >7.0) Findings Fixed

94

Total Security Improvements Made

20

Fuzzers Built or Improved to Continually Monitor Open Source Projects

8

Security Engagements Complete or In Progress

WORKING GROUP

Securing Software Repositories

This group provides a collaborative environment for aligning on the introduction of new tools and technologies to strengthen and secure software repositories.

Working Group Git Repo	Working Group Lead	Working Group Membership
github.com/ossf/wg-securing-software-repos	Dustin Ingram, Google	20 - 40 regular contributors

Our Mission

The "Securing Software Repositories" Working Group is for and focuses on the maintainers of software repositories, software registries, and tools which rely on them, at various levels including system, language, plugin, extensions and container systems. It provides a forum to share experiences and to discuss shared problems, risks and threats. The WG has somewhere between 20 and 40 regular contributors, and has more than 250 members in the OpenSSF Slack.

2022 Highlights

In 2022, the WG Conducted a "landscape" survey of existing capabilities of key software repositories, including potential security gaps or room for improvement, and shared the results. The WG also contributed extensively to guiding and discussing RFCs and proposals on the adoption of key OpenSSF technologies, including Sigstore. The WG also developed and shared a proposal for a "shared helpdesk" to mitigate the burden of increased security measures by software repos.

As a result, we've seen a number of repositories implement new best practices with support from repositories already implementing them (for example, a 2FA mandate on PyPI learned from previous experience with npm) as well as adopt new OpenSSF technologies (for example, npm's adoption of an RFC to use Sigstore and signed attestations).

What's Next

In 2023, the WG aims to further support the adoption of key OpenSSF technologies and best practices in critical software repositories in a comprehensive and unified way, by providing technical guidance, discussion, and possibly the guidance and discussion of OpenSSF funding as well.

WORKING GROUP

Security Tooling

This group's mission is to provide the best security tools for open source developers and make them universally accessible.

Working Group Git Repo	Working Group Lead	Working Group Membership
github.com/ossf/wg-security-tooling	Josh Bressers, Anchore	15 regular attendees in the SBOM Everywhere group

2022 Highlights

A key component of the OSS Mobilization Plan is using a software bill of materials (SBOM) as a foundational building block to improve the security posture of the entire open source ecosystem known as SBOM Everywhere. SBOM Everywhere, as the name suggests, is working towards bringing SBOMs to all of open source in a way that is non disruptive. This year, we introduced the SBOM Everywhere Special Interest Group (SIG), and we are just getting started.

The first effort of the SBOM Everywhere project was to create a plan that enabled the OpenSSF to fund work on the SPDX Python library. We are pleased to announce this plan has been approved and work started on September 1!

SPDX is a standard for describing software bill of materials. This is like an ingredients list for your software. The SPDX specification is an international open standard known as ISO/IEC 5962:2021. While SPDX is one of the standards that describes what a SBOM should look like, the SPDX project also houses a number of technical projects such as tools and libraries for creating and parsing the SPDX SBOM data. The work on these libraries has been done by community volunteers over a long period of time. It has been known for some time that the SPDX Python library needed updating to bring it in line with more modern versions of SPDX and turning the code into something that is easier to maintain to make community contributions less difficult. What the SPDX Python library didn't have was volunteers with the right skills or funding to get the work done. However, the OpenSSF did have funding that could accomplish this.

SBOMs are becoming extremely important. We see them popping up in regulations, legislation, standards, and even formal requirements. We understand making SBOMs easy to use and consume won't be easy, but is extremely important. If SBOMs don't become easier to create, use, store, and distribute, they're unlikely to be used industry wide.

What's next?

Please come and help if you have an interest in securing open source, which is in everything these days. If you create software, you are part of the open source community. The OpenSSF is a diverse community of contributors, there is plenty of work to do, and we would love to have you!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Working Groups and Projects

WORKING GROUP

Supply Chain Integrity

This group is helping people understand and make decisions on the provenance of the code they maintain, produce and use.

The Supply Chain Integrity WG is a community for collaborating to help individuals and organizations assess and improve the security of end-to-end supply chains for open source software. The WG has been a great place for information sharing, presentations, and home to several projects. The current projects sponsored by this working group include SLSA, FRSCA, and S2C2F.

Working Group Git Repo	Working Group Leads
github.com/ossf/wg-supply-chain-integrity	Kim Lewandowski, Chainguard and Dan Lorenc, Chainguard

Working Group Membership

Our regular meetings normally have between 20-30 attendees.

Project Numbers

Supply Chain Integrity: 460 on Slack
SLSA (main channel): 382 on Slack, 30 contributors
FRSCA: 90 people, 16 contributors
S2C2F: 4 contributors

Other Highlights

OSS Compromise dataset | Verizon SLSA case study | CNCF CRI-O project security audit included a SLSA compliance report Eclipse Foundation projects are reporting their SLSA level on their project management pages | Flatcar Linux have adopted SLSA and made their build process SLSA level 3 compliant

Supply chain Levels for Software Artifacts (SLSA)

SLSA (pronounced "salsa") is a security framework, a check list of standards and controls to prevent tampering, improve integrity, and secure packages and infrastructure in your projects, businesses or enterprises. It's how you get from safe enough to being as resilient as possible, at any link in the chain.

2022 Highlights

- SLSA 1.0 draft
- SLSA Survey
- SLSA for Success: Using SLSA to help achieve NIST's SSDF
- General availability of SLSA3 Generic Generator for GitHub Actions
- General Availability of SLSA 3 Go native builder for GitHub Actions
- SBOM + SLSA: Accelerating SBOM success with the help of SLSA

What's next?

- SLSA 1.0 Release
- Conformance program
- Training program

Factory for Repeatable Secure Creation of Artifacts (FRSCA)

FRSCA (pronounced "fresca") aims to help secure the supply chain by securing build pipelines. Adopted into the WG at the beginning of 2022. It is an integration of work across LF groups like CD Foundation, CNCF, and OpenSSF.

2022 Highlights

- SLSA FRSCA Recipe For Secure Supply Chain, with Parth Patel & Michael Lieberman
- Putting the Supply Chain Pieces Together: A Deep Dive into the Secure Software, with Michael Lieberman

The Secure Supply Chain Consumption Framework (S2C2F)

A consumption-focused framework that uses a threat-based, risk-reduction approach to mitigate real world threats in Open Source Software (OSS). Newest, recently adopted SIG in the WG. Blog post here.

WORKING GROUP

Vulnerability Disclosures

This group is improving the overall security of the OSS ecosystem by helping advance vulnerability reporting and communication.

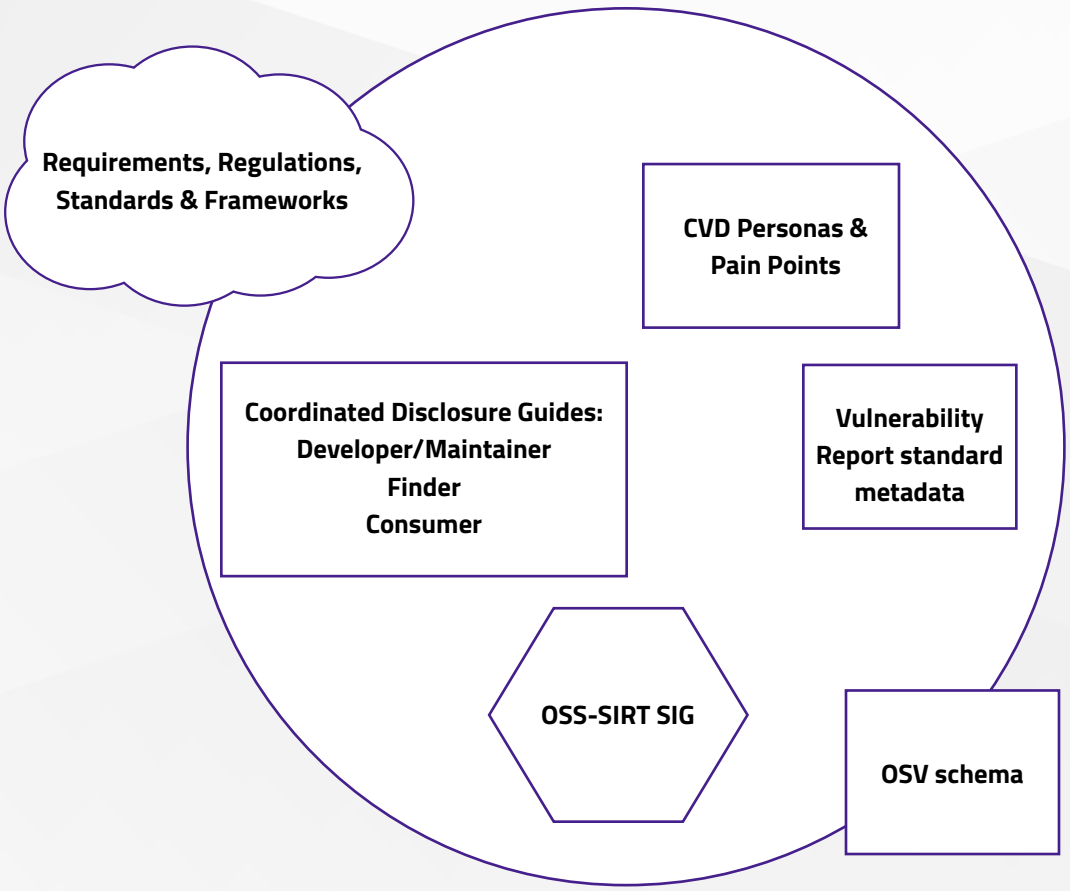
Working Group Git Repo	Working Group Lead	Working Group Membership
github.com/ossf/wg-vulnerability-disclosures	Christopher "CRob" Robinson, Intel	16 regular attendees, 15+ intermittent attendees

2022 Highlights

Published CVD Guide for Finders reporting to OSS Projects, OSS-NA presentations "Zero-Day Preppers" and "Securing Open Source at Scale", OSS-SIRT SIG

What's Next?

Publish OSS-SIRT Plan, secure funding, and begin work on creating team to help coordinate oss vulnerability disclosures, CVD Guide for OSS Consumers (with End Users WG), Incident Playbooks for Maintainers and OSS Projects



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Associated Projects

Alpha-Omega

Alpha-Omega

Alpha-Omega is an OpenSSF project with a mission to protect society by improving the security of open source software through direct maintainer engagement and expert analysis. Through Alpha, we fund security work for some of the most critical open source projects; through Omega, we apply software engineering and security research to identify security across a much wider set of widely-used projects.

Alpha-Omega was formed in February 2022 with $5 million funded jointly by Google and Microsoft. In June 2022, we announced that Google's Secure Open Source Rewards program would join our project, and in early December 2022, we announced that Amazon Web Services would be contributing $2.5 million to Alpha-Omega.

This year, Alpha-Omega has provided in total just over $2 million in funding to five organizations, including Node.js project, the Rust Foundation, the Eclipse Foundation, the Python Software Foundation, and including the jQuery project. This funding is being used to directly improve security within each organization and collectively impacts untold millions of end users. We're grateful to our partners within these foundations as we learn how to most effectively apply funds to improve security outcomes.

Two key highlights from these first few engagements are listed below:

- The Node Security Working Group was re-activated and is building a threat model for Node.js. The group released an experimental permission model for Node modules, a security best practices guide, and have begun adding security checks to their continuous integration system. They've triaged/fixed over 20 vulnerability reports and made multiple security releases.
- The Eclipse Foundation ran Security Scorecards against all projects under the Eclipse Foundation, analyzed the results, and created a prioritized list of activities to focus on to achieve the best and broadest improvements, which include hardening build infrastructure and enabling security tools. Eclipse projects can now declare their SLSA compliance level, and the Eclipse Marketplace has started to enforce the use of HTTPS.

> *"Software security is a never-ending process. This funding is the first step in a journey. We appreciate the support of the Alpha-Omega project, and are committed to using it effectively."*
>
> —MIKE MILINKOVICH, EXECUTIVE DIRECTOR, ECLIPSE FOUNDATION

Through Omega, we released an open-source analysis toolchain designed to target open source packages, and used this toolchain to identify multiple vulnerabilities in critical open source projects.

> *"I am a big supporter of the Alpha-Omega project as a strategic project for open-source software. The project directly improves the security of the open-source ecosystem by partnering with the community, providing results for all users."*
>
> *— JONATHAN MEADOWS, CITI*

In 2023, we plan to continue our focus on direct action, increasing the level of investments we make in critical open source projects while we help the longer tail of projects identify and address critical security vulnerabilities. In addition, we plan to:

- Help make security a first-class citizen in major projects' and foundations' budgets.
- Demonstrate measurable impact through security improvements to the projects we focus on.
- Extend Omega to deliver a scalable approach to vulnerability detection, triage, communication/reporting, and remediation.
- Expand Alpha-Omega to cover additional verticals (e.g. healthcare, automotive, financial services), where the set of critical projects may be very different.

We welcome community engagement and participation. Please connect with us or join us at one of our monthly public meetings.

The Alpha-Omega Core team includes Michael Scovetta (Microsoft), Michael Winser (Google), Yesenia Yser, Jonathan Leitschuh, and Annapurna Veeramachaneni (Citi). We're grateful for the significant support we receive from the Linux Foundation.

For more information on Alpha-Omega, please view our annual report here.

Sigstore

Sigstore is a new standard for signing, verifying, and protecting software.

Sigstore enables developers to validate that the software they are using is exactly what it claims to be using cryptographic digital signatures and transparency log technologies. Sigstore offers a suite of technologies that include Cosign for signing software artifacts, the Fulcio certificate authority, the Rekor transparency log, and Gitsign for signing Git commits. These tools can be used independently, or as one single process, for a holistic approach to open source security.

To address open source and software supply chain security, OpenSSF outlined a 10-point mobilization plan. One of those goals is for 50 of the top 200 projects to adopt an interoperable approach to software signing with Sigstore.

SIGSTORE HIGHLIGHTS

2022 has been an incredible year for the Sigstore project, with many key milestones achieved.

450+	9.4 million+	70+
CONTRIBUTORS	**REKOR SIGNATURES**	**ORGANIZATIONS**

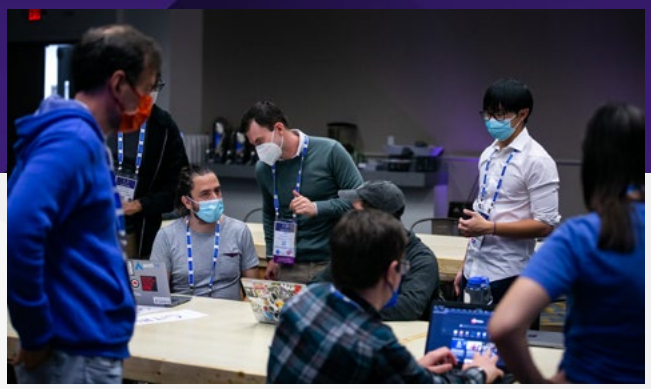
General Availability

Sigstore announced General Availability (GA) for the Rekor transparency log and Fulcio certificate authority public benefit services! The community has been working hard all year to accomplish this milestone, and we are thrilled that open source communities can now confidently rely on Sigstore for production-grade stable services for artifact signing and verification.

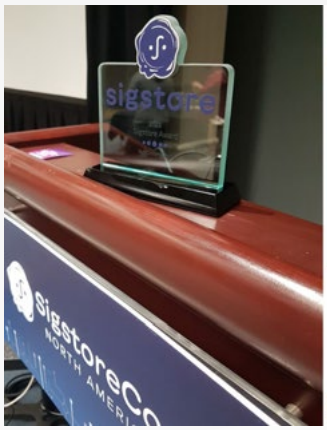
SigstoreCon

The community hosted the first-ever Sigstore event, SigstoreCon, in co-location with KubeCon

OpenSSF
OPEN SOURCE SECURITY FOUNDATION



+ CloudNativeCon North America. The event featured 17 fantastic talks that demonstrated all aspects of our growing ecosystem! The community hosted its first award ceremony and gave out three Sigstore Awards: Best User Adopter: SLSA GitHub Generators, Best Evangelist: Batuhan (developer-guy) Apaydın, and Most Valuable Contributor: Asra Ali.



Sigstore Adoption

Thanks to its ease of use, open source projects have quickly started adopting Sigstore. In May, the Kubernetes ecosystem adopted Sigstore in a landmark move for the Kubernetes 1.24 release. A few months later, the Python community adopted Sigstore for signing CPython releases, with Python 3.11 being the first new version of Python to be signed with Sigstore. Additionally, npm recently announced they are actively working to integrate Sigstore, so all npm packages can be reliably linked to their source code and build instructions. In the Java world, Maven also announced their intent to adopt Sigstore as part of the Maven central platform.

Sigstore looks set to be the fastest adopted open source project in history. To ease adoption of Sigstore in various ecosystems, Sigstore language clients for Python, Java, Javascript, Rust, and Ruby are in development. The Sigstore landscape highlights the growing ecosystem.

> "I gotta say, @projectsigstore is extra dope. This is what modern software signing and verification looks like."
>
> —KELSEY HIGHTOWER

Other Highlights

- "Sigstore: Software Signing For Everybody" has been published in the proceedings of ACM Computer & Communications Security Conference
- OpenSSF announced a new free online training course to help folks use Sigstore to improve the integrity and security of the software supply chain. Enroll Free Today.
- Sigstore published 4 end user case studies to highlight how organizations are using Sigstore today.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Community Engagement

Open Source Security Summit II

May 12, 2022 | Washington, DC

The Linux Foundation and the Open Source Software Security Foundation (OpenSSF) brought together over 90 executives from 37 companies and government leaders from the NSC, ONCD, CISA, NIST, DOE, and OMB to reach a consensus on key actions to take to improve the resiliency and security of open source software.

Open Source Software Security Summit II was a follow up to the first Summit held January 13, 2022 that was led by the White House's National Security Council. The meeting was convened one year after the anniversary of President Biden's Executive Order on Improving the Nation's Cybersecurity during which we delivered the first-of-its-kind mobilization plan to broadly address open source and software supply chain security.

Press Release: Here

Open Source Security Summit in Japan

August 23, 2022 | Tokyo, Japan

Following on the heels of the summit held in conjunction with the White House in the United States, the OpenSSF and Linux Foundation Japan hosted the Open Source Security Summit Japan. We were joined by senior cybersecurity representatives from more than 20 leading Japanese firms, including Hitachi, Fujitsu, LINE, NEC, NTT Data, Toyota, Suzuki, Toshiba, SBI, and OpenSSF members Renesas, Cybertrust and Cybozu, along with senior representation from the Japanese Ministry of Economy, Trade and Industry (METI), AIST, IPA and JP-CERT.

The summit demonstrated a growing interest and priority for governments and industry around the world to concentrate and collaborate on OSS security.

Recap: Here

OpenSSF Day Events

OpenSSF Days brought together the open source community to discuss the challenges, big-picture solutions, ongoing work and successes in securing the open source software (OSS) supply chain. They featured keynotes from OpenSSF contributors and thought leaders. Sessions included presentation, panels, and fireside chats on subjects such as security best practices, vulnerability discovery, securing critical projects, and the future of OSS security.

OpenSSF Day North America

June 20 | Austin, TX, USA

- 11 sessions, 18 speakers
- Registrants: 861: In-Person: 361, Virtual: 500
- Highlights: Here

OpenSSF Day Europe

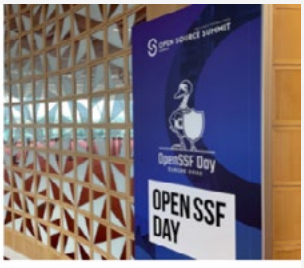
September 13 | Dublin, Ireland

- 11 sessions, 13 speakers
- Registrants: 510: In person: 224, Virtual: 286
- Highlights: Here

OpenSSF Day Japan

December 5 | Yokohama, Japan

- 7 sessions, 7 speakers
- Registrants: 283: In person: 170, Virtual: 113
- Highlights: Here



Event Participation

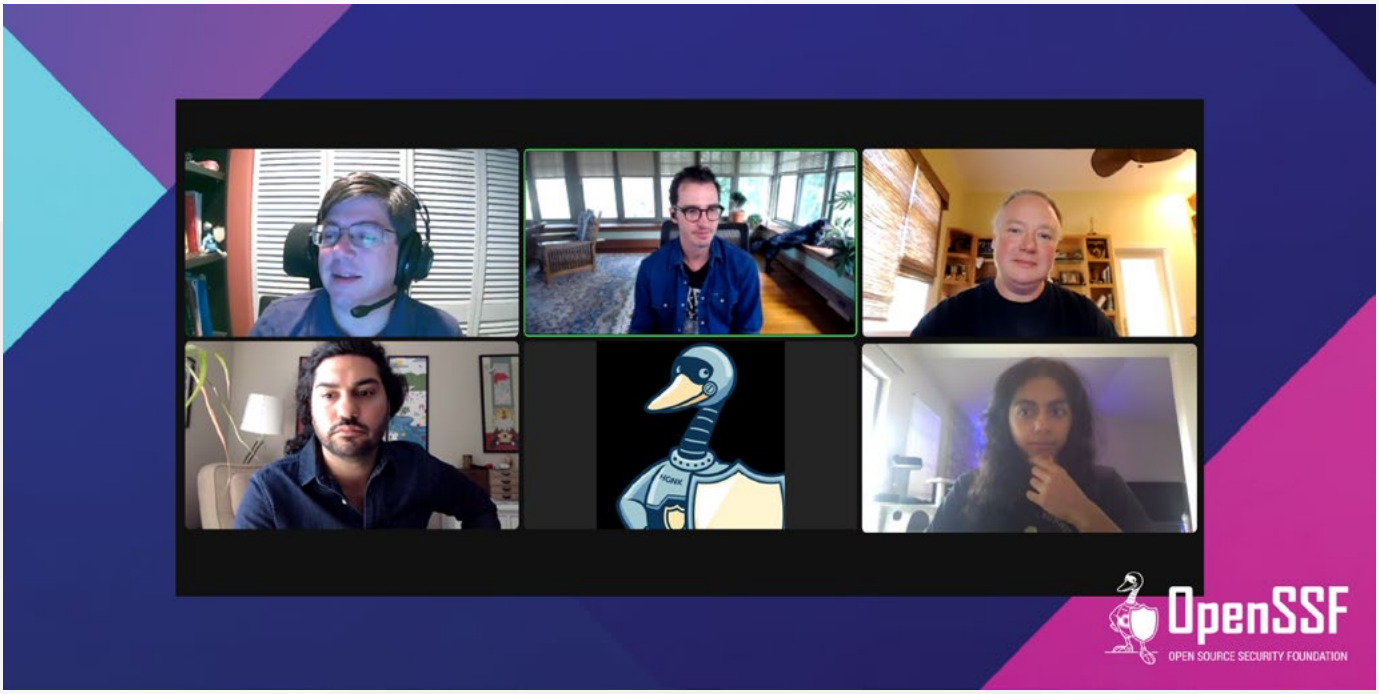
Event
White House Summit on Software Security, Washington, D.C. (1/13)
Security Unhappy Hour, Virtual (2/14)
OpenSSF Town Hall, Virtual (2/23)
LF Webinar: Census II of Open Source Software Application Libraries the World Depends On, Virtual (3/2)
OpenSSF in APAC: How OpenSSF is Combatting Key Software Supply Chain Security Challenges, Virtual (3/24)
FOSSASIA Summit 2022, Virtual (4/8)
Future Compute, Cambridge, MA (5/3)
Testimony to the US House Committee on Science and Technology, Washington, D.C. (5/11)
Open Source Security Summit II, Washington, D.C. (5/13)
OpenJS World, Austin, TX (6/8)
OpenSSF Day at Open Source Summit North America, Austin, TX (6/20)
CSO's Future of Cybersecurity Summit, Virtual (7/19–7/20)
White House Cyber Workforce and Education Summit, Washington, D.C. (7/19)
Summer of Open Source Security, Virtual (7/20)
Fintech Festival India, Hybrid, New Delhi (7/20–7/22)
Open Source China Open Source World Summit, by COPU, Virtual (7/21–7/22)
OpenSSF Meetup in India, Bangalore (7/28)
ApacheCon Asia, Virtual, (7/29–7/31)
In the Nic of Time Podcast, Virtual (8/2)
BlackHat, Las Vegas, NV (8/6–8/11)
DEF CON, Las Vegas, NV (8/11–8/1)
OpenSSF Town Hall, Virtual (8/15)
OpenSSF & Scantist Community Events, Singapore (8/18–8/19)
Open Source Software Security Summit Japan, Tokyo, Japan (8/23)

Event
VMware Explore, San Francisco, CA (8/29–9/1)
OpenSSF Day at Open Source Summit Europe, Dublin, Ireland (9/13)
Grace Hopper Celebration, Orlando, FL (9/20 - 9/23)
Open MainFrame Summit, Philadelphia, PA (9/21–9/22)
Critical Infrastructure Security Summit, Washington, D.C. (9/28 –9/29)
Black Bear Securities event: 'Application Development Best Practices' – Philippines, Virtual (9/30)
AWS ASEAN Security Forum, Singapore (10/4)
Snyk & OpenSSF in APAC: Cybersecurity Challenges in Open Source Software, Virtual (10/5)
ASIFMA Tech & Ops Conference 2022, Hybrid, Singapore (10/5–10/6)
OpenUK's Open Source Software: Infrastructure, Curation and Security Day, London, UK (10/17)
DevOps Enterprise Summit, Las Vegas, NV (10/18)
OSPOlogy.live Workshop, Stockholm, Sweden (10/19 –10/20)
CSDN "The Programmer Festival", China (10/22–24)
JAPAN Security Summit 2022, Japan (10/24)
KubeCon + CloudNativeCon North America 2022, Detroit, MI (10/24 –10/28)
Singapore Fintech Festival, Singapore (11/2–11/4)
NTU-Scantist DevSecOps event, Singapore (11/2)
IOSF and OpenSSF Summit China, Shenzhen, China (11/7)
ACM CCS 2022, Los Angeles, CA (11/7–11/11)
LF Member Summit, Lake Tahoe, CA (11/8–11/10)
DevOps Experience – DevOps Everywhere, Virtual, (11/16)
Internetdagarna, Virtual (11/22—11/22)
SWForum Event, Brussels (12/02)
OpenSSF Day at Open Source Summit Japan, Yokahama (12/05)


Open Source Supply Chain Secure

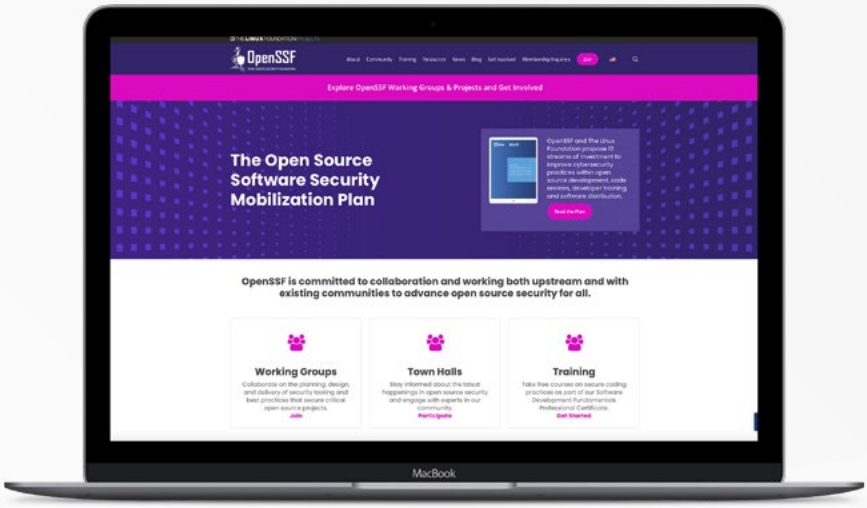
Town Halls

We hosted two Town Halls in February and August of 2022 that were especially for open source software maintainers, contributors, software developers, and OSS users who haven't quite made the leap to join an OpenSSF Working Group or Project yet. We introduced attendees to the OpenSSF, reviewed what's been happening, and shared about what's next. We provided an in-depth tour of several key initiatives designed to help newcomers get involved in the exciting work of the OpenSSF.



Community Engagement Highlights

As of Nov. 30th



Newsletter mailing list

Mailing list	Subscribers	Newsletter open rate	Click rate
Oct	1,254	40.17%	2.75%
Nov	1,489	31.60%	2.91%
Dec	1,631	33.19%	1.69%

Website pageviews: 192,998

Month	Pageviews
Jan	17,024
Feb	21,187
March	14,308
April	13,694
May	35,667
June	18,579
July	13,394
Aug	15,052
Sept	15,939
Oct	14,862
Nov	13,292
Total:	**192,998**

Mobilization Plan: Downloads: 4,009 | **Blogs** posted: 51 | **Slack** participants: 1,725

YouTube

- Subscribers: 623
- Video views: 45,896
- Watch time: 2,100 hours
- Videos posted: 377
- Top video: YouTube

Training

Developing Secure Software Course:

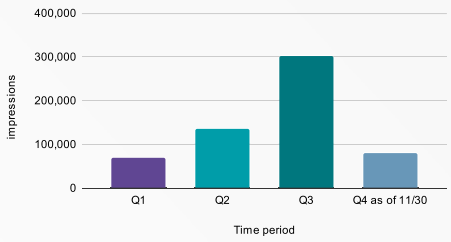
- Enrollment: 8,412 registrants

Securing Your Software Supply Chain with Sigstore Course:

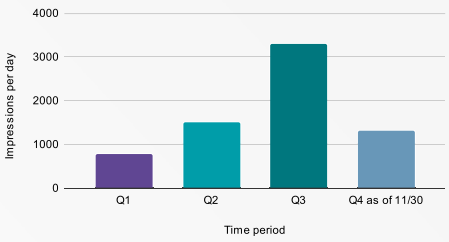
- Enrollment: 741 registrants

Twitter @theopenssf

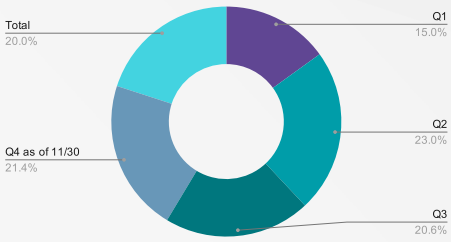
Impressions: 587,900



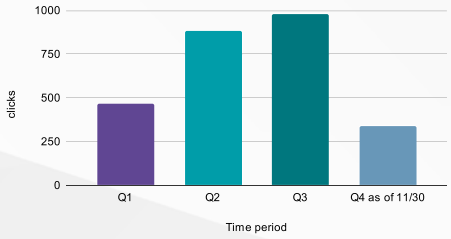
Impressions per day: 6,875



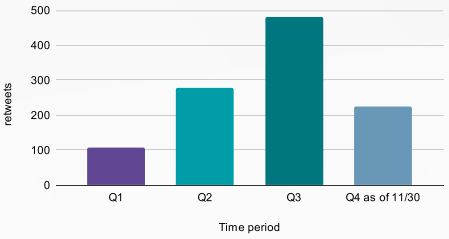
Engagement rate %



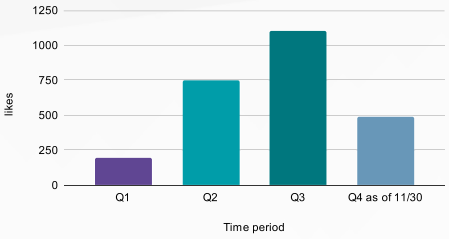
Clicks: 2,667



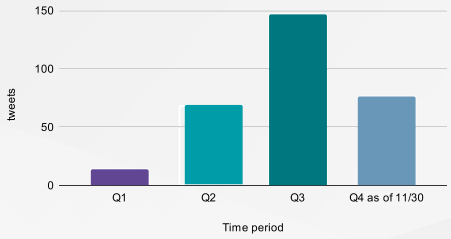
Retweets: 1,091



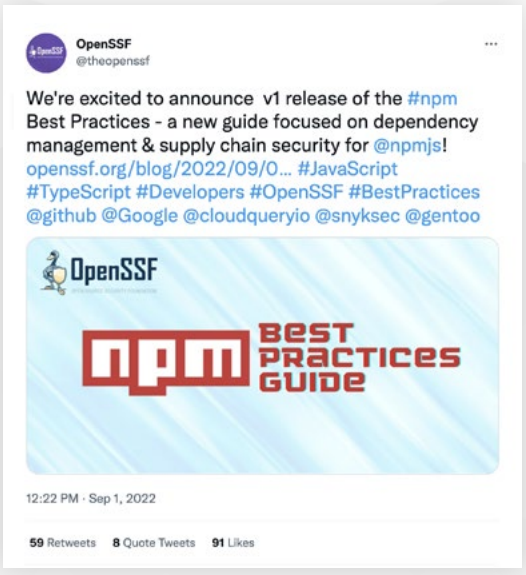
Likes: 2,535



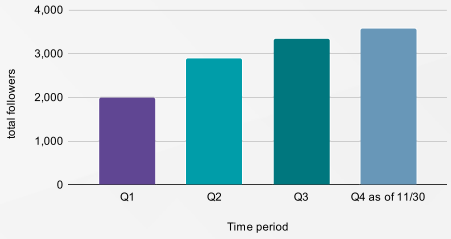
Tweets: 305



Top tweet:

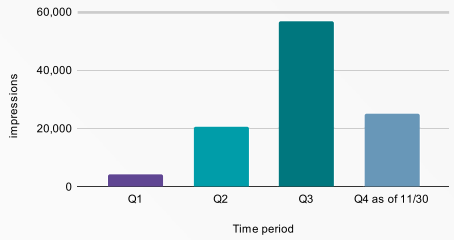


Total Followers: 3,577

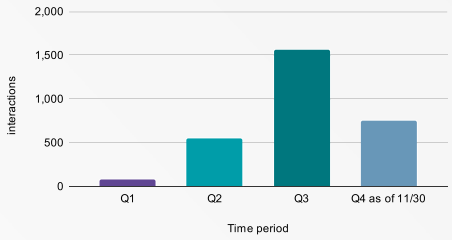


LinkedIn OpenSSF

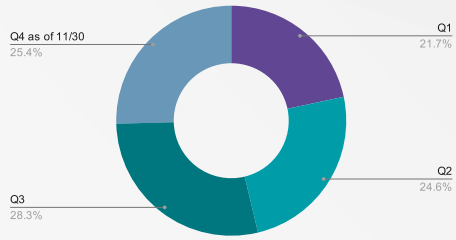
Impressions: 106,476



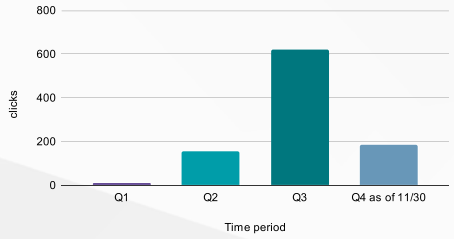
Interactions: 2,937



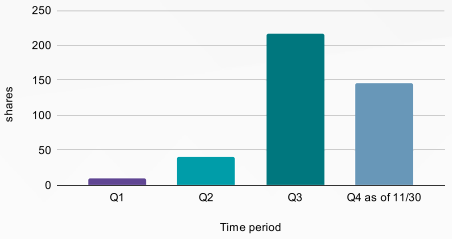
Engagement rate %



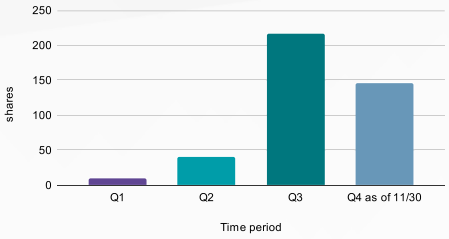
Clicks: 972



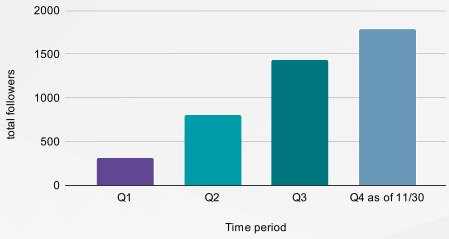
Shares: 414



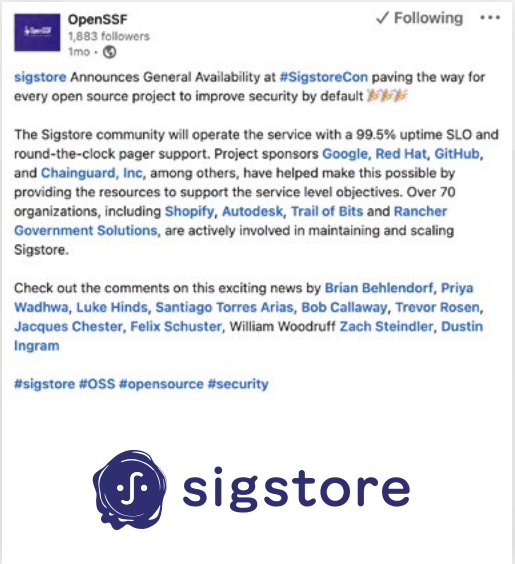
Posts: 240



Total followers: 1,783



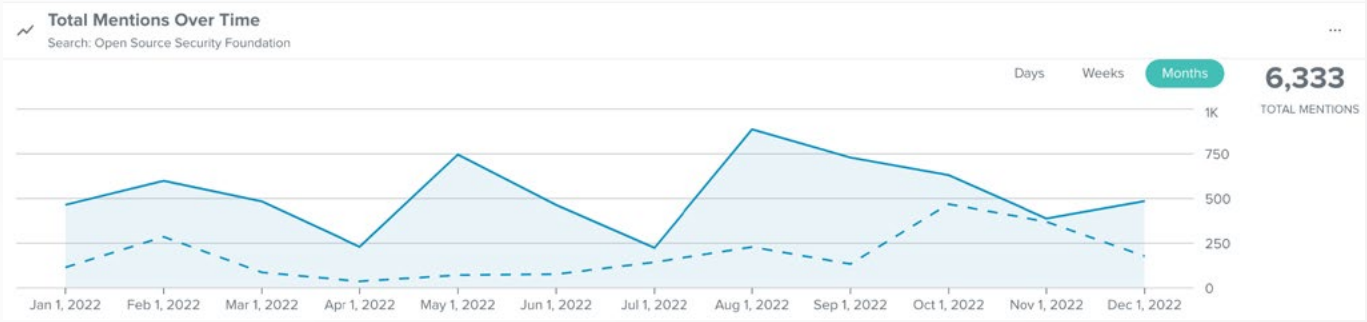
Top post:

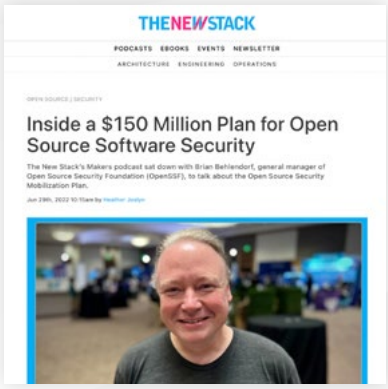


Press Coverage Highlights

Press releases issued: 10

6,333 total mentions year to date in online news and blogs





OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Thank you for a great year! Join us in securing
the open source ecosystem in 2023 and beyond.

openssf.org/getinvolved