OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Town Hall

March 16, 2023 | Virtual Event

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Housekeeping

- Thank you for joining us today! We will begin at 10:02a PT.
- While we wait for everyone to join, please take a moment to do one (or more) of the following:
  - Please add questions using the Zoom Q&A feature
  - Follow us on Twitter: @theopenssf, Mastodon: social.lfx.dev/@openssf, & LinkedIn: OpenSSF
  - Visit the website: https://openssf.org
  - Sign up for training: https://openssf.org/training/courses/
- This meeting is being recorded

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Antitrust Policy Notice

- Linux Foundation meetings **involve participation by industry competitors**, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at **http://www.linuxfoundation.org/antitrust-policy**. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Code of Conduct

- The Linux Foundation and its project communities are **dedicated to providing a harassment-free experience** for participants at all of our events, whether they are held in person or virtually.

- All event participants, whether they are attending an in-person event or a virtual event, **are expected to behave in accordance with professional standards**, with both this Code of Conduct as well as their respective employer's policies governing appropriate workplace behavior and applicable laws.

- https://openssf.org/community/code-of-conduct/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Housekeeping

Please submit your questions during the meeting
by using the Q&A feature on Zoom.

Thank you!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Agenda

01
Open Source Security Foundation tour
Brian Behlendorf, General Manager, OpenSSF

02
Addressing security risk with Alpha-Omega
Michael Scovetta, Microsoft

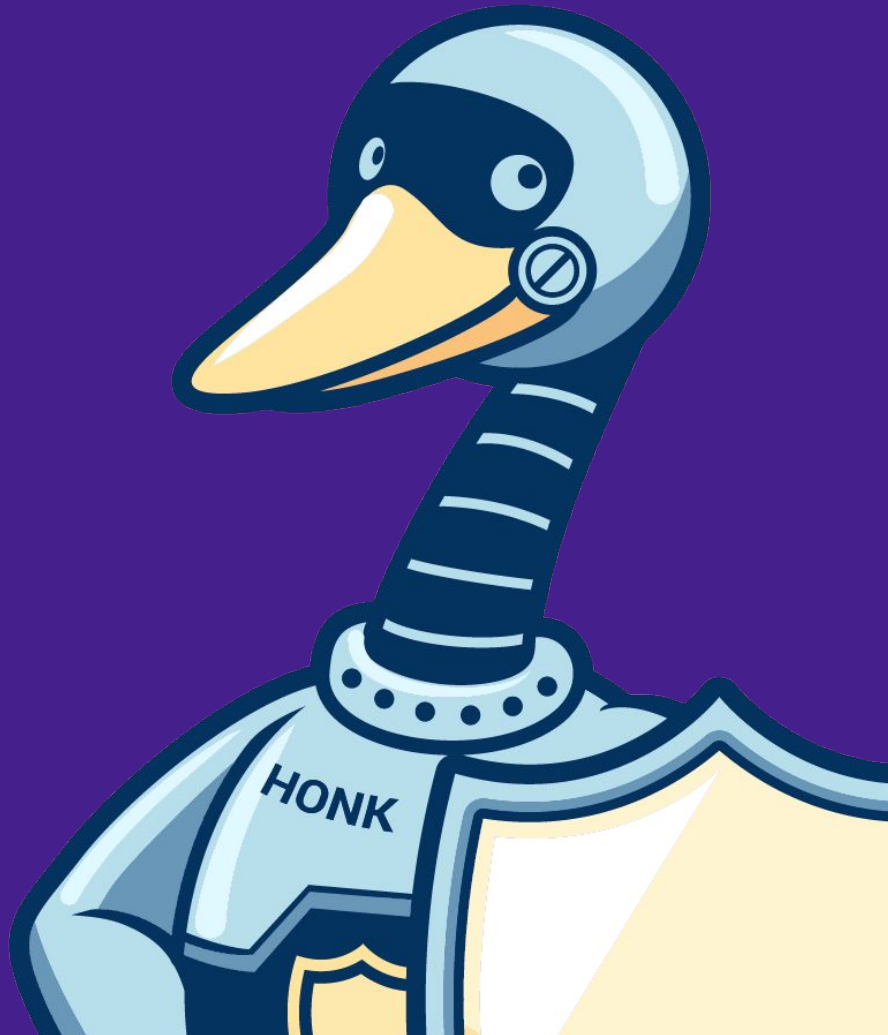
03
What's happening in the SBOM Everywhere group?
Josh Bressers, Anchore

04
Advancing DEI in Open Source Security
Christine Abernathy, F5 and Dr. Jautau “Jay” White, Microsoft

05
How to get involved
David A. Wheeler, Director of Open Source Supply Chain Security, The Linux Foundation

06
Moderated Q&A Session
A time for question and answer with all of the panelists

OpenSSF Tour and Membership Update



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Brian Behlendorf

General Manager, OpenSSF

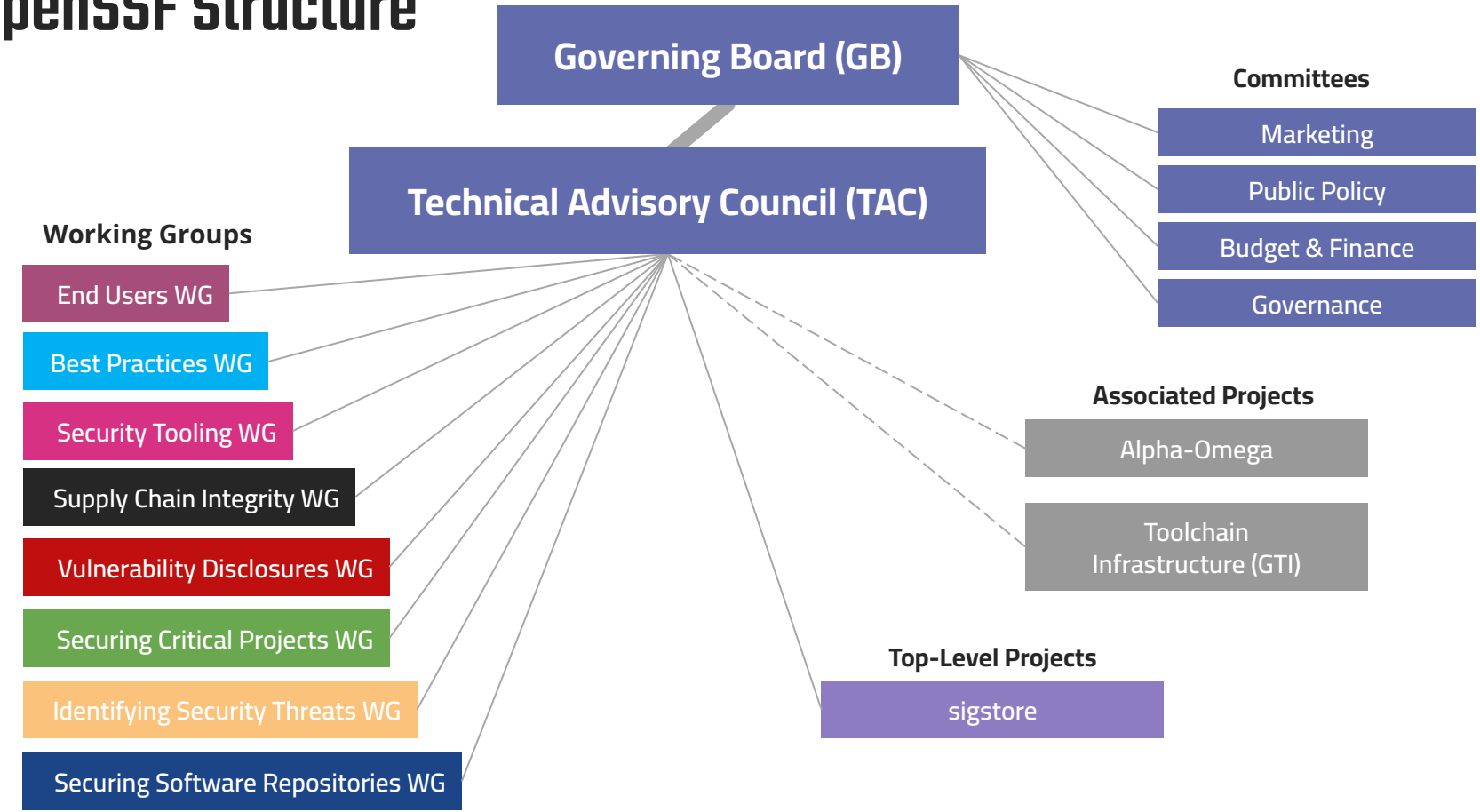
Brian Behlendorf is the General Manager for the Open Source Security Foundation (OpenSSF), an initiative of the Linux Foundation, focused on securing the open source ecosystem. Brian has founded and led open source software communities and initiatives for more than 30 years, first as a co-founder of the Apache Software Foundation and then later as a founding board member of both the Open Source Initiative and the Mozilla Foundation. In parallel, Brian co-founded or was CTO for a series of startups (Wired Magazine, Organic Online, CollabNet) before pivoting towards public service serving the White House CTO office in the Obama Administration and then serving as CTO for the World Economic Forum. Brian joined the Linux Foundation in 2016 to lead Hyperledger, the distributed ledger initiative now core to supply chain traceability and central bank digital currency efforts worldwide, and has led the OpenSSF since September 2021.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

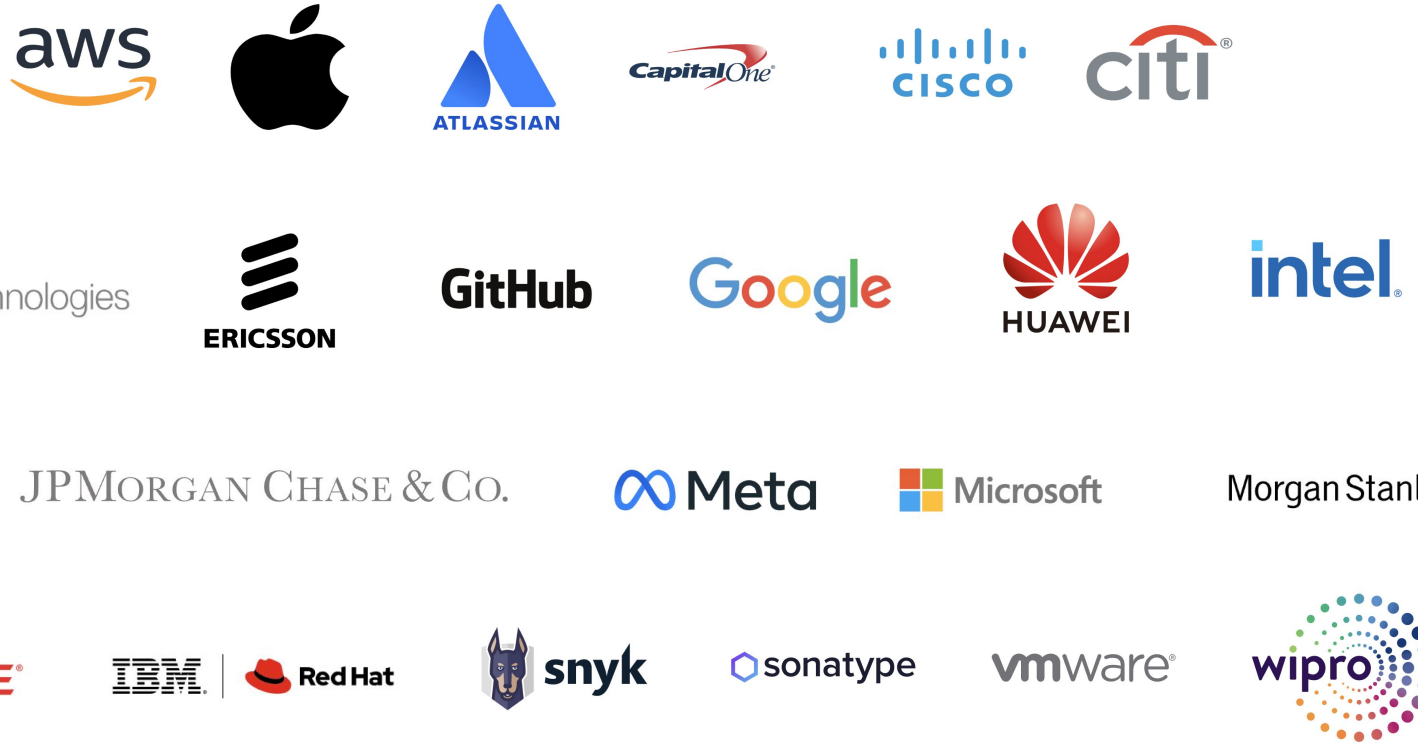
Purpose

To inspire and enable the community to secure the open source software we all depend on, including development, testing, fundraising, infrastructure, and support initiatives driven by Working Groups (non-software focused) and Projects (software focused), each a “Technical Initiative”.

OpenSSF Structure



OpenSSF Premier Members



General and Associate Members

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OpenSSF Membership Exceeds 100 Supporting Organizations!

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Welcome New Members!

GENERAL MEMBERS

amesto Fortytwo

code intelligence

KUSARI

privado

Scotiabank

TII Technology Innovation Institute

ASSOCIATE MEMBERS

OSB Open Source Business ALLIANCE
Bundesverband für digitale Souveränität e.V.

python SOFTWARE FOUNDATION

Is your organization a member?

https://openssf.org/join

Questions? Contact membership@openssf.org

Meet the OpenSSF Governing Board

Adrian Ludwig
Chief Trust Officer, Atlassian

Andrew Van Der Stock
Executive Director, OWASP Foundation

Arun Gupta
Vice President and General Manager, Open Ecosystem Initiatives, Intel Corporation

Bob Callaway
OpenSSF TAC Chair & Tech Lead & Manager, Google Open Source Security Team

Kelly Ann
Cloud Infrastructure Security Engineer, Apple

Kit Colbert
Chief Technology Officer, VMware

Mark Russinovich
Azure CTO and Technical Fellow, Microsoft

Mark Ryland
Director, Office of the CISO AWS Security

Brian Fox
CTO, Sonatype

Clyde Rodriguez
Vice President of Engineering, Meta

Declan O'Donovan
VP, Security Architecture, IAM and Application Security, Morgan Stanley

Duane O'Brien
Director of Open Source, Indeed

Mike Hanley
Chief Security Officer, GitHub

Per Beming
VP and Head of Standards & Industry Initiatives

Rao Lakkakula
JPMorgan Chase

Scott Roberts
Cloud CISO, Coinbase

Eric Brewer
VP of Infrastructure & Google Fellow, Google

Gareth Rushgrove
VP of Product, Snyk

Ian Coldwater
Security Community Individual Representative

Jamie Thomas
OpenSSF Board Chair & General Manager, Systems Strategy and Development, IBM

Stephen Augustus
Head of Open Source, Cisco

Stephen Chin
VP of Developer Relations, JFrog

Subha Tatavarti
CTO, Wipro

Tracy Miranda
Head of Open Source, Chainguard

Jinguo Cui
Executive Director of Open Source Security and Infrastructure, Huawei

John Heimann
Vice President, Security Programs, Oracle

John Roese
Global Chief Technology Officer Products and Operations, Dell Technologies

Jonathan Meadows
Head of Cloud Cybersecurity Engineering and Software Supply Chain Security at Citibank

Vincent Danen
Vice President of Product Security, Red Hat

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Meet the OpenSSF Technical Advisory Council

Abhishek Arya
Principal Engineer and Manager, Google Open Source Security Team

Aeva Black
OpenSSF TAC Vice Chair & Open Source Hacker, Microsoft Azure Office of the CTO

Bob Callaway
OpenSSF TAC Chair & Tech Lead & Manager, Google Open Source Security Team

Christopher Robinson "CRob"
Directory of Security Communications, Intel

Dan Lorenc
CEO, Chainguard

Josh Bressers
VP of Security, Anchore

Luke Hinds
Red Hat

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Meet the OpenSSF Staff

Brian Behlendorf
General Manager

David A. Wheeler
Director of Open Source Supply Chain Security

Donald Liu
Regional Tech Evangelist, Asia Pacific

Jennifer Bly
Senior Marketing & Communications Manager

Jonathan Leitschuh
Senior Software Security Researcher

Julian Gordon
VP Asia Pacific

Khahil White
Program Manager

Michelle Martineau
Program Manager

Randi Armour
Membership Solutions

Yang Hin
Director, China at Linux Foundation Asia Pacific

Yesenia Yser
Senior Software Security Engineer

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Sigstore Announces General Availability

https://openssf.org/press-release/2022/10/25/sigstore-announces-general-availability-at-sigstorecon/

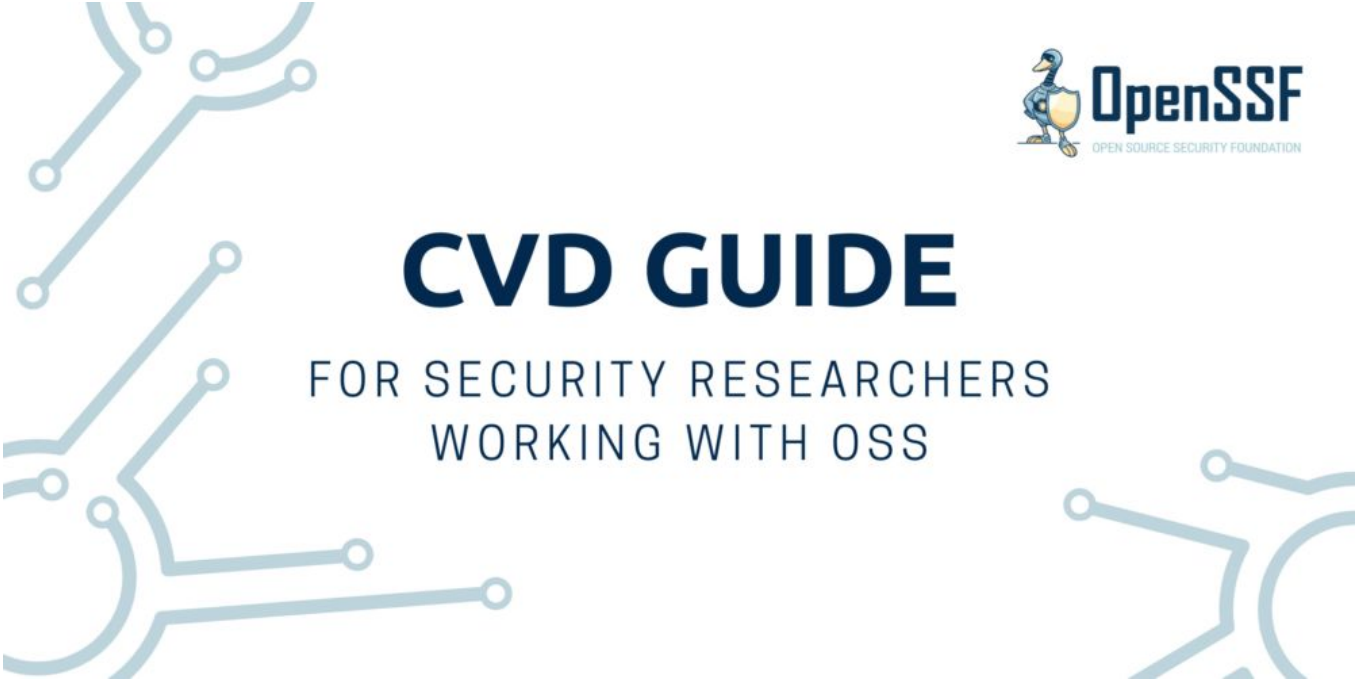
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Concise Guides for Developing More Secure Software and Evaluating Open Source Software

https://openssf.org/blog/2022/09/13/introducing-new-concise-guides-for-developing-more-secure-software-and-evaluating-open-source-software/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Coordination is Key! The OpenSSF's CVD Guide for Finders



https://openssf.org/blog/2022/09/13/coordination-is-key-the-openssfs-cvd-guide-for-finders/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Free OpenSSF Developing Secure Software Training Course Now Available in Japanese

https://openssf.org/blog/2022/12/04/free-openssf-developing-secure-software-training-course-now-available-in-japanese/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OpenSSF Expands Supply Chain Integrity Efforts with S2C2F

https://openssf.org/blog/2022/11/16/openssf-expands-supply-chain-integrity-efforts-with-s2c2f/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Avoiding the Next Log4Shell: Learning from the Log4j Event, One Year Later

https://openssf.org/blog/2022/12/15/avoiding-the-next-log4shell-learning-from-the-log4j-event-one-year-later/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The United States Securing Open Source Software Act: What You Need to Know

https://openssf.org/blog/2022/09/27/the-united-states-securing-open-source-software-act-what-you-need-to-know/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Engaging Policy Makers and the Ecosystem on Open Source Software Globally

https://openssf.org/blog/2022/12/28/engaging-policy-makers-and-the-ecosystem-on-open-source-software-globally/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Introducing the New OpenSSF End Users Working Group

https://openssf.org/blog/2022/09/13/introducing-the-new-openssf-end-users-working-group/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Show Off Your Security Score: Announcing Scorecards Badges

https://openssf.org/blog/2022/09/08/show-off-your-security-score-announcing-scorecards-badges/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2022 Annual Report

https://openssf.org/resources/reports/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Out and About Recent Events

OpenSSF Day Europe

OpenSSF Meetup Tokyo

OpenSSF Day Japan

CloudNativeSecurityCon

OpenSSF Meetup Hong Kong

Speak at OpenSSF Day — May 10th in Vancouver

- Wednesday, May 10th in Vancouver
- @ Open Source Summit North America
- Register
- CFP open for 1 more day! Deadline: March 17th

Addressing security risk with Alpha-Omega

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Michael Scovetta

Principal Security PM Manager, Microsoft

Michael Scovetta is a Principal Security PM Manager at Microsoft, and leads an open source security team focused on understanding emerging security threats and building solutions to mitigate them.

Michael leads the OpenSSF Identifying Security Threats working group and co-leads the Alpha-Omega project.

You can find Michael on the OpenSSF Slack or at michael.scovetta@alpha-omega.dev.

Alpha-Omega

What's New?

- Welcome new team members!
  - Yesenia Yser (Senior Software Engineer)
  - Jonathan Leitschuh (Senior Security Researcher)
  - Bob Callaway (Co-Lead — Google)
  - Brian Russell (Google)

- Our 2022 Annual Report, read at **openssf.org/blog**.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Alpha-Omega

Alpha Engagements

Current:

- Node.js
- jQuery
- Eclipse Foundation
- Rust Foundation
- Python Software Foundation

$2.5 M

Grants awarded

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Alpha-Omega

Year in Review

We've been working hard, and we are proud of what was completed in 2022! Here's a partial list:

- Node.js Security Working Group reactivated with growing participation. Feel free to join!
- Managing more security issues at faster rate with improved processes
- Creating a new Threat Model that provides context on what will and will not be considered a vulnerability in Node.js, which will particularly help inform security researchers
- Adding vulnerability checking for Node.js dependencies
- Building a security Permission Model to avoid third-party libraries accessing machine resources without user consent
- Tracking OpenSSL releases closely, documented in:
  - "Maintaining OpenSSL" for Node.js documentation showing how Node.js checks requirements, extracts new OpenSSL sources, and commits them
- In-person Node.js Collab Summit security breakout
- First Node.js Security Best Practices document published
- Efforts to automate dependency updates

Node.js Security Progress Report – Permission Model Merged

By OpenJS Foundation | March 13, 2023 | Blog, Node.js, Node.js Security

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Alpha-Omega

jQuery CDN

The backend for the jQuery CDN at code.jquery.com was split off to its own servers, separate from other jQuery sites, instead of being co-located on servers that also host releases.jquery.com website. This is to reduce the available attack surface on the CDN service given its wide reach. The new servers are running the latest version of Debian and the provisioning was fully automated using Puppet.

Security improvements

The project's server fleet was last refreshed in 2016, managed by Puppet 3 released that same year. Some older servers still ran Debian 7, released in 2013. The new servers all run with Debian 11 ("Bullseye") as the Linux distribution of choice, managed via Puppet 7.

Server provisions were rewritten from scratch with the latest best practices and a few or no dependencies to minimize exposure. The base setup for all servers also adds tighter firewalls, limits package installations to officially supported Debian channels, improves access control and enables automatic security updates going forward.

Alpha-Omega

Security Audits

We have successfully initiated the 3 security audits that will all be performed by Trail of Bits in collaboration with OSTIF. The projects that will be covered in these audits are:

- Eclipse Jetty: an open-source Java-based web server that provides a HTTP server and servlet container.
- Eclipse JKube: a toolkit for building container images and deploying them to Kubernetes.
- Eclipse Mosquito: an open-source IoT platform that enables the development and management of connected devices.

Hiring

We have build capacity since the beginning of the year, hiring 3 talented people:

- **Marta Rybczynska**, Technical Program Manager. They bring a wealth of experience and knowledge to the team. She initially focusing on improving security / vulnerability policies, procedures, and guidelines that adhere to industry best practices. She started early January.
- **Thomas Neidhart**, Software Engineer. He is initially focusing on SLSA attestation generation and GitHub management tooling. He started mid-January.
- **Francisco Perez**, Software Engineer. He will work closely with Eclipse Foundation Projects to enhance their software supply chain security. He started begining of March.

Alpha-Omega

We are pleased to share that Walter Pearce has joined the Rust Foundation as our new Security Engineer.

31 Jan 2023

GitHub Security Scanning Partnership

The Foundation and the Rust Project (specifically crates.io) are now a GitHub technology partner as a secret scanning integrator. GitHub will scan every commit to a public repository for exposed crates.io keys. GitHub will forward any tokens found to crates.io, who will automatically disable the tokens and notify their owners.

Threat Model

The Foundation's Rust Ecosystem security threat model development is in full force, with Walter taking the lead. After discussions with members of the Rust Project and others in the Rust community, themes have developed and documentation is now being written to describe potential areas of focus and concern. We expect an initial draft of the threat model to be complete by April.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Alpha-Omega

The PSF is hiring a Security Developer-in-Residence!

The Python Software Foundation (PSF) is happy to announce the launch of a year-long security enhancement initiative that will include a security audit and the creation of a new Security Developer-in-Residence role. Generous funding by the OpenSSF's Alpha-Omega Project has made this work possible.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Alpha-Omega

Omega Tools

Omega Analyzer - Collection of 20+ security tools, orchestrated within a Docker container

Omega Triage Portal - Efficiently triage analysis output across thousands of projects

Assurance Assertions - Proof of concept @ bit.ly/assuranceassertions

Omega Moderne Client - Enables automated pull requests using the Moderne SaaS API

All are still very much "in development" and open for contributions!
(including non-code contributions)

Alpha-Omega

Coming Soon...

More Alpha Engagements

More Tools & Experiments

Speaking at Conferences

- Women in CyberJutsu
- Boston AppSec
- OpenSSF Day?

Coming soon!

Outreach & Community

- Alpha-Omega Mentorship Program
- University Vulnerability Outreach Program
- Automated Vulnerability Fix Campaign

Vulnerability Management

- Disclosure Policy & Process
- Automated Vulnerability Reporting

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Alpha-Omega

Get Involved

- Attend a public meeting.
- Help us improve our tools.
- Connect with us on Slack.
- Come chat!

Where to find us:

- #alpha_omega
- github.com/ossf/alpha-omega

What's happening in the SBOM Everywhere group?

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Josh Bressers

Vice President of Security, Anchore

Josh Bressers is the Vice President of Security at Anchore. Josh has helped build and manage product security teams for open source projects as well as several organizations. Everything from managing supply chains, vulnerabilities, security development lifecycle, DevSecOps, security product management, security strategy, and nearly any other task that falls under the security umbrella. Josh co-hosts the Open Source Security Podcast and the Hacker History Podcast. He also is the co-founder of the Global Security Database project to bring vulnerability identification into the modern age.

SBOM Everywhere Group

Motivation

MISSION

Connect those interested in SBOMs to the SBOM resources they need

Work within the “evolving” SBOM community to connect and empower software authors and consumers from all areas of software, including open source and commercial, to create and consume SBOMs. Use the resources available to the OpenSSF to encourage others to collaborate and build the tooling needed for widespread SBOM usage and adoption.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

SBOM Everywhere Group

Objective

- Defining our mission and purpose
- Work **with** the existing efforts
  - Let's not reinvent the wheel
- Funding SPDX Python library
- SBOM landscape
- Connecting OpenSSF resources to open source
  - Go to the projects and help
  - Identify tools
  - Identify projects

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

SBOM Everywhere Group

Join Us!

Every other Tuesday at 11:05 Eastern

Next meeting on March 28

#stream-09-sbom-everywhere on Slack

Feel free to ask on Slack for more details!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Advancing DEI in Open Source Security

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Christine Abernathy

Sr Director Open Source, F5

Christine leads the Open Source Programs Office at F5. Christine joined F5 from Facebook (now Meta Platforms) where she was instrumental in growing their open source presence. Prior roles included Developer Advocate Parse, Facebook Platform and Partner Engineer, Mobile. Before Facebook, Christine headed up engineering at Mshift, a mobile banking software provider, delivering iOS/Android apps and mobile browser-based products. Prior experiences include co-founding Clickmarks, a mobile and enterprise middleware provider.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Dr. Jautau “Jay” White

Security Principal Program Manager, OSS Ecosystem Team, Microsoft

Jay has over 20 years of IT/information security experience including 15 years dedicated to supply chain and cyber risk, security, privacy, and compliance. He provides a combined tactical and strategic balance towards the implementation of enterprise and cyber risk management, security and compliance requirements that aligns to an organization’s broader business strategy. With this experience, Jay can provide tangible value and serve as a practical trusted advisor when making strategic or tactical decisions to build, improve, and properly sustain the organization's security governance posture. Jay promotes the idea that security should not be shrouded in “No,” or preventing or slowing communication and transactions, but instead be a tool used to add value and facilitate a safe, secure, and well trusted “Yes.” Jay believes that companies should go beyond the status quo for their customers and partners and take the teamwork/community approach to understanding business unit needs.

Best Practices WG - Diversity, Equity & Inclusion Subcommittee

OpenSSF Mobilization Plan
Stream 1: **Security Education**

Initial DEI goals:

- Make materials more accessible
- Ensure pathways to success

"This strategy will take a comprehensive and coordinated approach to expanding the national cyber workforce, improving its diversity, and increasing access to cyber educational and training pathways."

– US Cybersecurity Strategy (section 4.6)

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Best Practices WG - Diversity, Equity & Inclusion Subcommittee

What we've been working on

Mapped out 2023 objectives:

- Advocacy and communication
- Research and thought leadership
- Partnership development
- Training and engagement

- Aligned on target group
- Support Alpha-Omega colleges pilot
- Compiled comprehensive list of DEI organizations in security

Best Practices WG - Diversity, Equity & Inclusion Subcommittee

What's next

Lobby for centralized DEI SIG:

- Research and thought leadership
- Umbrella advocacy work

Partnership development

- Align with OpenSSF WGs
- Partner with LF DEI initiatives

Advocacy and communication

- Speak at Open Source Summit NA
- Outreach at security conferences

Training and engagement

- Refine Education SIG plan

Risk

Measuring the education plan effectiveness:

- Creative resourcing for accurate statistics
- Strategic partnerships to provide ethical sources

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Best Practices WG - Diversity, Equity & Inclusion Subcommittee

Join Us!

Every other **Tuesday** at **11:00 AM Eastern**

Next meeting on **March 28**

#stream-01-security-education-dei on Slack

Feel free to ask on Slack for more details!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

How to Get Involved in OpenSSF Working Groups and Projects

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

David A. Wheeler

Director of Open Source Supply Chain Security, Linux Foundation

Dr. David A. Wheeler is an expert on developing secure software and on open source software (OSS) development. He wrote the book “Secure Programming HOWTO” on how to develop secure software, and his work on countering malicious tools (“Fully Countering Trusting Trust through Diverse Double-Compiling (DDC)”) is widely cited. He is the Director of Open Source Supply Chain Security at the Linux Foundation, and teaches graduate courses in developing secure software at George Mason University (GMU).

He is also the lead for the Linux Foundation’s OpenSSF Best Practices badge project. Dr. Wheeler has a PhD in Information Technology, a Master’s in Computer Science, a certificate in Information Security, and a B.S. in Electronics Engineering, all from George Mason University (GMU). He is also a Certified Information Systems Security Professional (CISSP) and a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE).

Working Groups (and their projects & Associated Projects)

Best Practices

Identification, awareness, and education of security best practices

- OpenSSF Best Practices badge
- Scorecards
- Great MFA distribution SIG
- Common Requirements Enumeration (CRE)
- Secure Software Development Fundamentals courses SIG
- Security Knowledge Framework (SKF)

Vulnerability Disclosures

Efficient vulnerability reporting and remediation

- Guide to coordinated vulnerability disclosure for OSS projects
- Vulnerability Disclosures Whitepaper
- osv-schema

End Users WG

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

Top-Level Projects

Category-leading software initiatives

- Sigstore

Identifying Security Threats

Security metrics/reviews for open source projects

- security-reviews,
- Project-Security-Metrics (dashboard)
- SECURITY-IMPACTS.yml spec

Security Tooling

State of the art security tools

- ossf-cve-benchmark
- Web Application Definition spec
- fuzz-introspector

Securing Software Repositories

collaboration between repository operators

- Coming soon!

Supply Chain Integrity

Ensuring the provenance of open source code

- Supply-chain Levels for Software Artifacts (SLSA)
- Software Supply-Chain Consumption Framework (S2C2F)

Securing Critical Projects

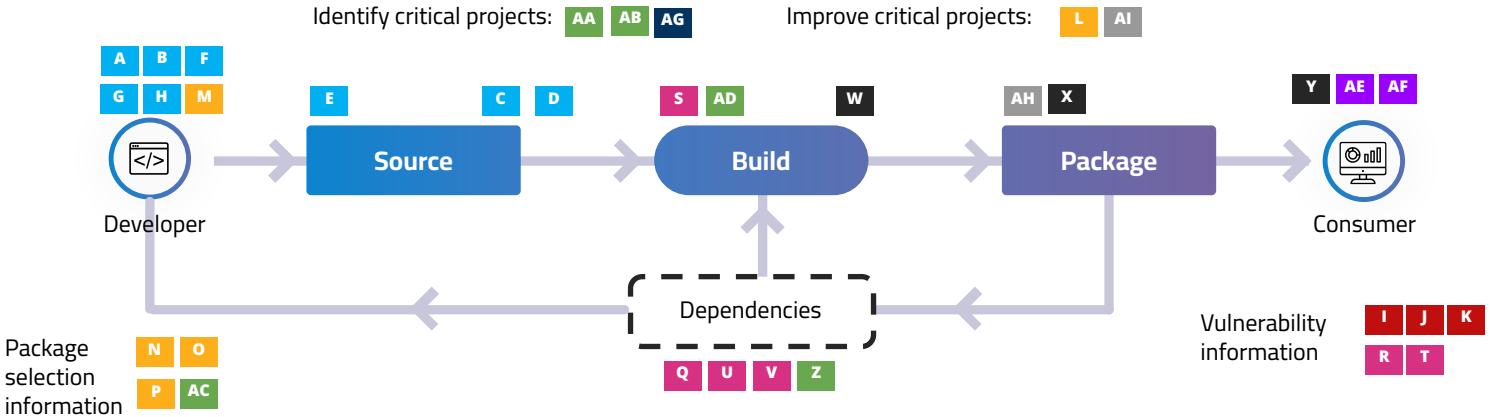
Identification of critical open source projects

- criticality_score
- Harvard research
- package-feeds / package-analysis
- Allstar

Associated Projects

- Project Alpha-Omega
- GNU Toolchain Infrastructure (GTI) support

How OpenSSF Projects & SIGs Work Together



Best Practices WG

- A. Secure Software Development Fundamentals courses SIG
- B. Security Knowledge Framework (SKF) project
- C. OpenSSF Best Practices Badge project
- D. OpenSSF Scorecards project
- E. Great MFA distribution SIG
- F. Common Requirements Enumeration (CRE) project
- G. Concise & Best Practices Guides SIGs
- H. Education SIG

Vulnerability Disclosures WG

- I. CVD Guides SIGs
- J. OSS-SIRT SIG
- K. Open Source Vuln Schema (OSV) project

Identifying Security Threats WG

- L. Alpha & Omega project
- M. Office Hours SIG
- N. Security Insights
- O. Security-Metrics: Risk Dashboard project
- P. Security Reviews project

Security Tooling WG

- Q. .SBOM Everywhere SIG
- R. False-Positive Suppression Spec SIG
- S. Guide to Security Tools SIG
- T. cve-benchmark SIG
- U. OSS Fuzzing SIG
- V. DAST scanning & web app definitions SIG

End Users WG

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

Supply Chain Integrity WG

- W. Supply-chain Levels for Software Artifacts (SLSA) SIG
- X. Factory for Repeatable Secure Creation of Aertifacts (FRSCA) SIG
- Y. Secure Supply Chain Consumption Framework (S2C2F) SIG

Securing Software Repositories WG

- AG. Survey of OSS Repos SIG

Securing Critical Projects WG

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

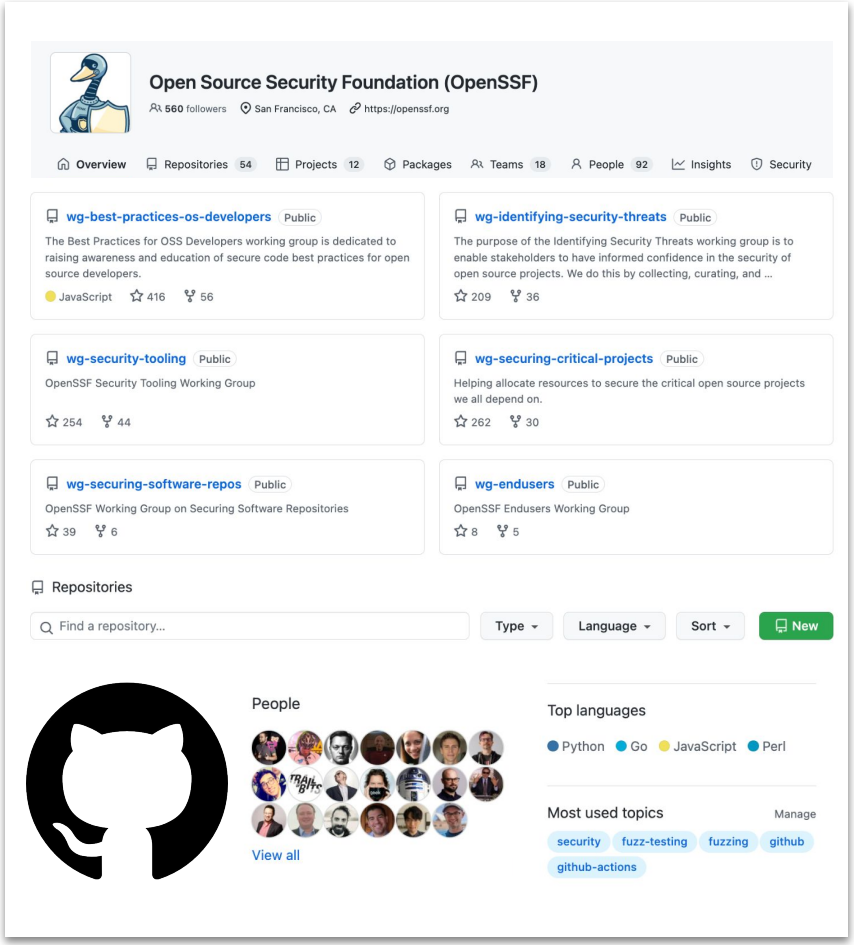
Associated Projects

- AH. sigstore
- AI. GNU Toolchain Infrastructure (GTI) support

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Ways to Participate

- Join the OpenSSF Mailing List
- Follow us on Twitter
- Follow us on LinkedIn
- Follow us on Mastodon
- Follow us on Facebook
- Subscribe to our YouTube Channel
- Join a Working Group/Project
- Access the Public Meetings Calendar
- Participate on Slack
- Follow OpenSSF on GitHub
- Become an Organizational Member



Join a Technical Working Group

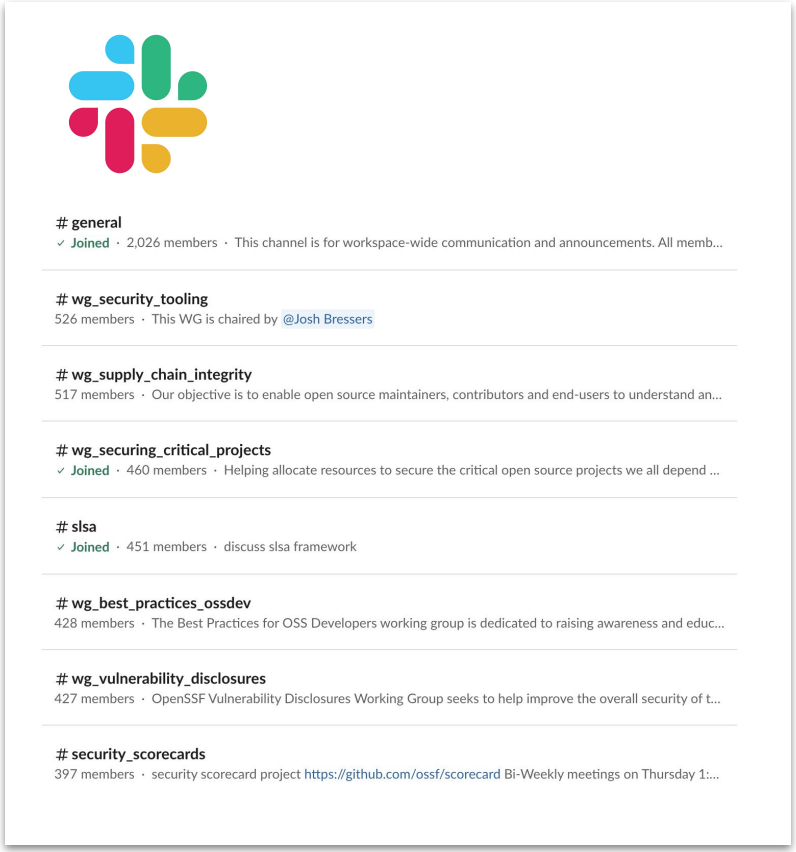
@ossf

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Attend a Public Meeting

bit.ly/ossf-calendar

OpenSSF
OPEN SOURCE SECURITY FOUNDATION



Message on Slack

slack.openssf.org

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Follow us on Social Media

[Twitter](#)
@theopenssf

[LinkedIn](#)
OpenSSF

[Mastodon](#)
social.lfx.dev/
@openssf

[YouTube](#)
OpenSSF

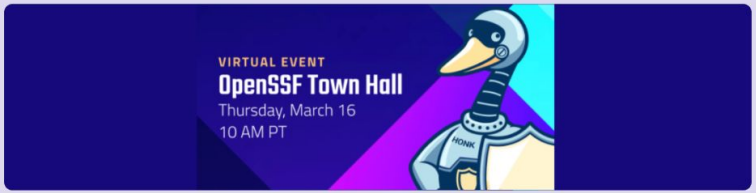
[Facebook](#)
OpenSSF

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Subscribe to the Mailing List

https://openssf.org/sign-up

OpenSSF
OPEN SOURCE SECURITY FOUNDATION



March 2023 OpenSSF Town Hall: How Can We Help You?

How can we help you with your open source security initiatives?

First Name and Last Name

Your answer

How long have you participated in the OpenSSF? *

I'm new, just getting started

Take our survey

forms.gle/FMiEhV7eGc6PjkEW9

Q&A

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Thank You!