OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2023 TAC Updates

OpenSSF GB Meeting 23Oct2023

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Agenda

01 **Who** is the TAC?

02 **What** are our current Technical Initiatives?

03 **What** are our key 2023 accomplishments?

04 **What** is planned for 2024+?

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The OpenSSF Technical Advisory Council is responsible for oversight of the various Technical Initiatives of the OpenSSF

7 representatives from across the industry

Meet every 2 weeks to review progress of technical initiatives

Arnaud Le Hors
OpenSSF TAC Vice Chair & Senior Technical Staff Member - Open Technologies, IBM

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

Christopher "CRob" Robinson
OpenSSF TAC Chair & Director of Security Communications, Intel

Dan Appelquist
Open Source & Open Standards Strategy Director, Snyk

Dustin Ingram
Staff Software Engineer at Google & Director at Python Software Foundation

Michael Lieberman
Co-Founder & CTO, Kusari

Zach Steindler
Principal Engineer, GitHub

https://github.com/ossf/tac

OpenSSF Structure

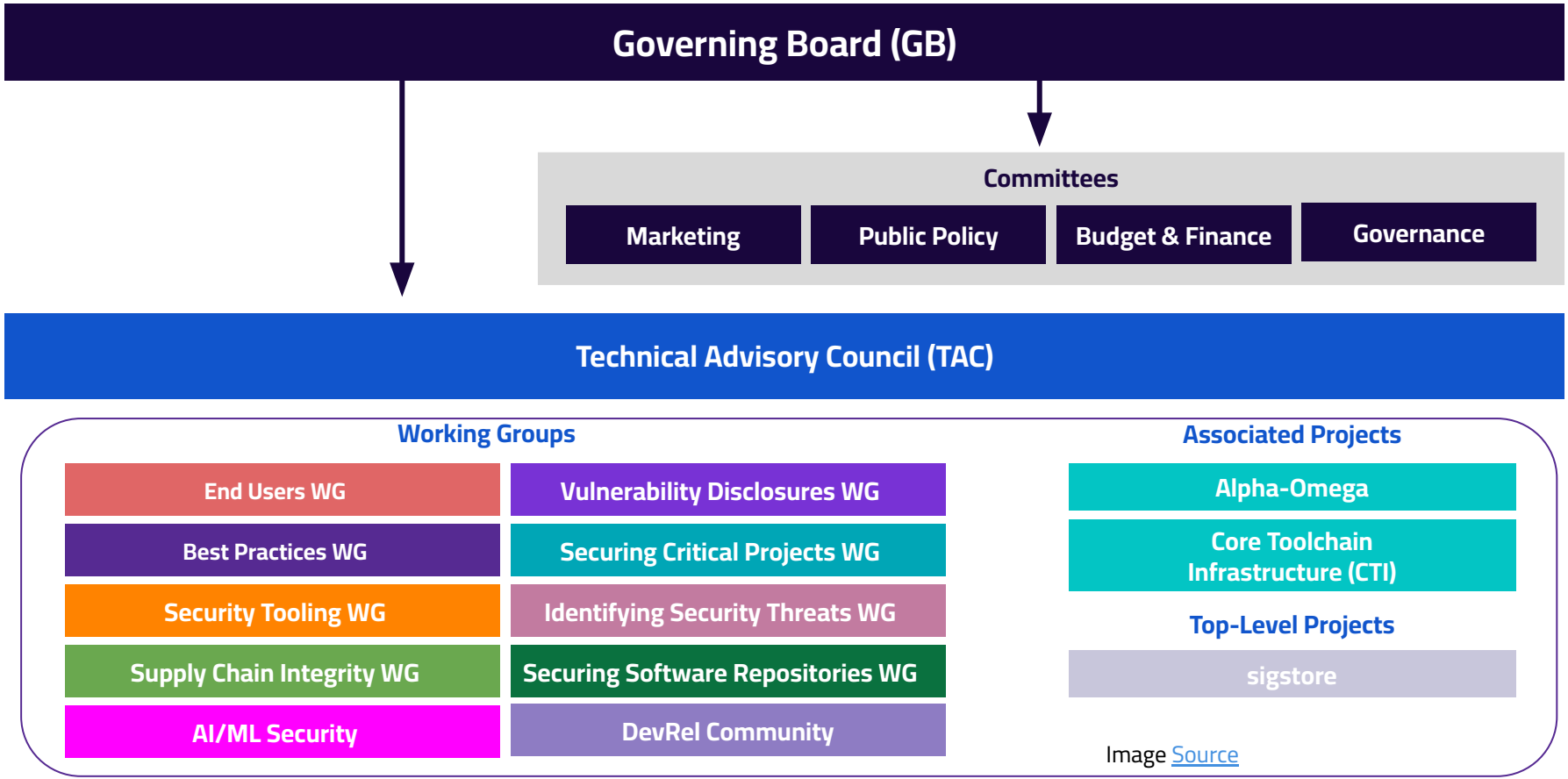


Image Source

OpenSSF Structure

Governing Board (GB)

Governance

Projects

End Us

Best Pra

Security T

Supply Chain

AI/ML Security

DevRel Community

ega

hain
re (CTI)

rojects

Image Source

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

01

WHAT ARE OUR CURRENT TECHNICAL INITIATIVES?

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Recent Additions

- AI/ML working group creation
- SBoMIT sandbox project adoption in the Tooling WG
- gittuf sandbox project adoption in the SCI WG
- RSTUF sandbox project adoption in the Securing Repos WG
- Source Code Management Best Practices Guide

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Improvements

- Publication of the OpenSSF Technical Vision
- Collab on Foundation MVSR & rollout of MVSRs to the Working Groups and projects
- Collab on the Foundation Operating Model
  - streamline & ensure consistency of processes and naming
- Publication of a vulnerability disclosure policy for the foundation
- Collab on TAC Election process & # of TAC seats

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Working Groups, Projects, & SIGs

Vulnerability Disclosures

Efficient vulnerability reporting and remediation

J. **CVD Guides** SIGs

K. **OSS-SIRT** SIG - Mob. Plan

L. **Open Source Vuln Schema (OSV)** project

M. **OpenVEX** SIG

N. **Vuln Autofix** SIG

Best Practices

Identification, awareness, and education of security best practices

A. **Secure Software Development Fundamentals courses** SIG

B. **Security Knowledge Framework (SKF)** project

C. **OpenSSF Best Practices Badge** project

D. **OpenSSF Scorecard** project

F. **Common Requirements Enumeration (CRE)** project

G. **Concise & Best Practices Guides** SIGs

H. **Education** SIG - Mob. Plan

I. **Memory Safety** SIG - Mob. Plan

AN: Secure Software Development Guiding Principles (NEW)

AO: The Security Toolbelt (NEW)

End Users WG

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

AH. Supply Chain Attack taxonomy SIG

AI. Supply Chain Attack RefArch SIG

Identifying Security Threats

Security metrics/reviews for open source projects

P. **Security Insights** project

Q. **Security-Metrics: Risk Dashboard** project

R. **Security Reviews** project

Security Tooling

State of the art security tools

S. **SBOM Everywhere** SIG - Mob. Plan

W. ***OSS Fuzzing*** SIG

AP: SBoMIT spec (NEW)

Supply Chain Integrity

Ensuring the provenance of open source code

Z. **Supply-chain Levels for Software Artifacts (SLSA)** SIG

AB. **Secure Supply Chain Consumpt Framework (S2C2F)** SIG

AQ: gittuf project (NEW)

Securing Software Repositories

collaboration between repository operators

AG. **Survey of OSS Repos** SIG

AM. **Repository as a Service** Project

AR: RSTUF project (New)

Securing Critical Projects

Identification of critical open source projects

AC. **List of Critical OS Prj, components, & Frameworks** SIG

AD. **criticality_score** project

AE. **Harvard study** SIG

AF. **Package Analysis** project

AG. **allstar** project

AI/ML Security

AI/ML Security at the Intersection of Artificial Intelligence and Cybersecurity

DevRel

Develop Use Cases and help others learn about security

Projects

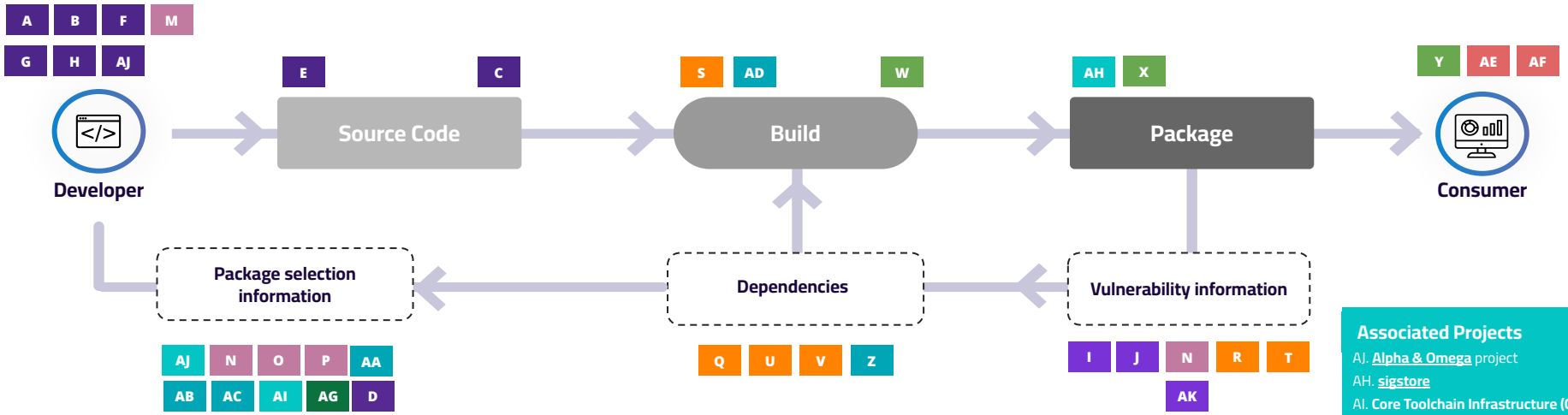
Category-leading software initiatives

AJ. **Alpha-Omega**

AL. **Sigstore**

AM. Core Toolchain Infrastructure (CTI)

How OpenSSF Projects & SIGs Work Together ("CI/CD View")



Associated Projects

AJ. Alpha & Omega project
AH. sigstore
AI. Core Toolchain Infrastructure (CTI) support

Best Practices WG

A. Secure Software Development Fundamentals courses SIG
B. Security Knowledge Framework (SKF) project
C. OpenSSF Best Practices Badge project
D. OpenSSF Scorecard project
E.
F. Common Requirements Enumeration (CRE) project
G. Concise & Best Practices Guides SIGs
H. Education SIG - Mob. Plan
AJ. Memory Safety SIG - Mob. Plan
AN: Secure Software Development Guiding Principles (NEW)
AO: The Security Toolbelt (NEW)

Vulnerability Disclosures WG

I. CVD Guides SIGs
J. OSS-SIRT SIG - Mob. Plan
K. Open Source Vuln Schema (OSV) project
AK. OpenVEX SIG
AL. Vuln Autofix SIG

Identifying Security Threats WG

N. Security Insights
O. Security-Metrics: Risk Dashboard project
P. Security Reviews project

Security Tooling WG

Q. SBOM Everywhere SIG - Mob. Plan
R.
S.
T.
U. OSS Fuzzing SIG
V.

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.
Y. Secure Supply Chain Consumption Framework (S2C2F) SIG

Securing Software Repositories WG

AG. Survey of OSS Repos SIG
AM. Repository as a Service Project

Securing Critical Projects WG

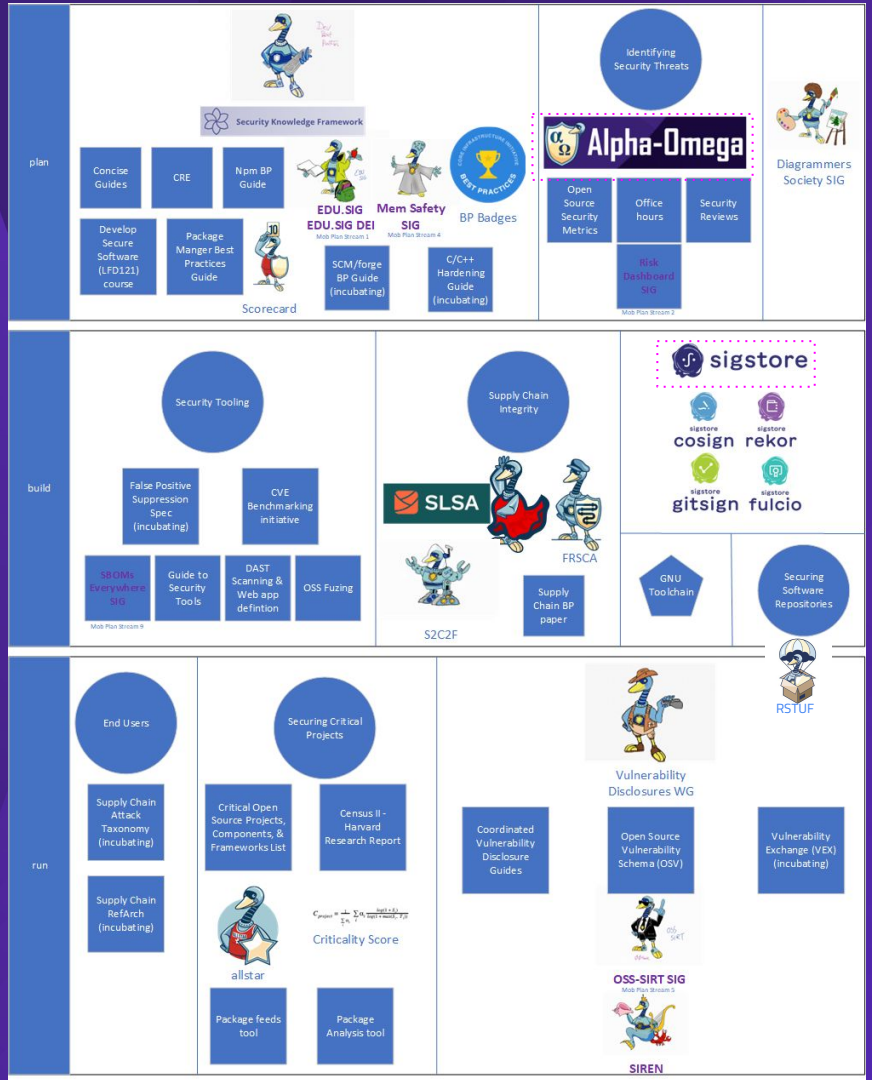
Z. List of Critical Open Source Projects, components, & Frameworks SIG
AA. criticality_score project
AB. Harvard study SIG
AC. package-feeds / package-analysis project
AD. allstar project

AI/ML Security

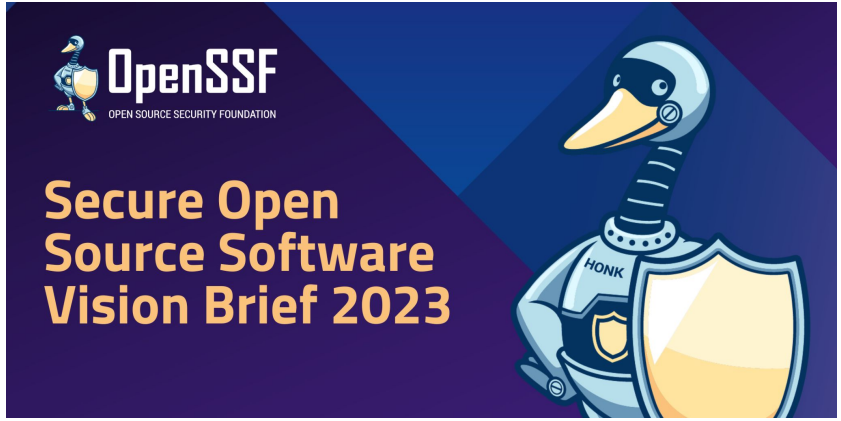
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

02

WHAT HAVE WE ACCOMPLISHED IN 2023?

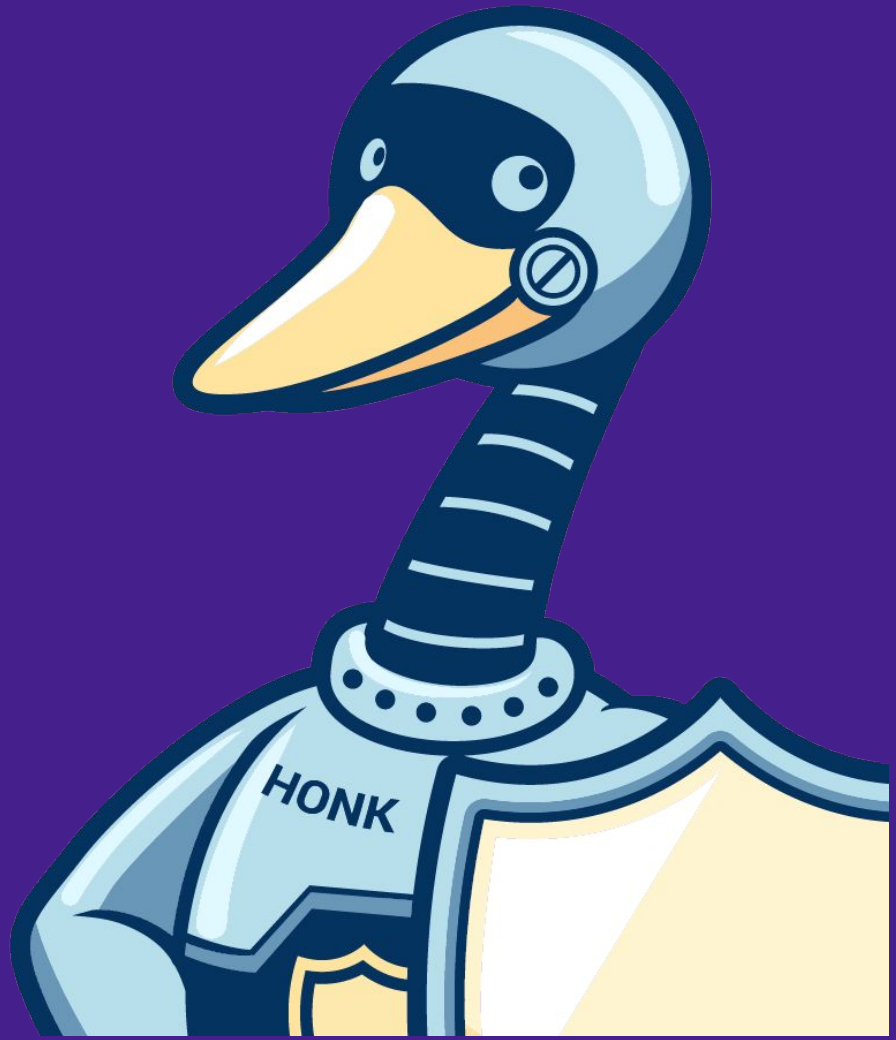


OpenSSF
OPEN SOURCE SECURITY FOUNDATION



The SOSS Vision Brief provides the most comprehensive overview of the Foundation's achievements since the original WDC Summit

https://openssf.org/soss-vision-brief/



We'll quickly touch on several of the highlights

Alpha - Omega successes

Seth Michael Larson - PSF Security Developer-in-Residence

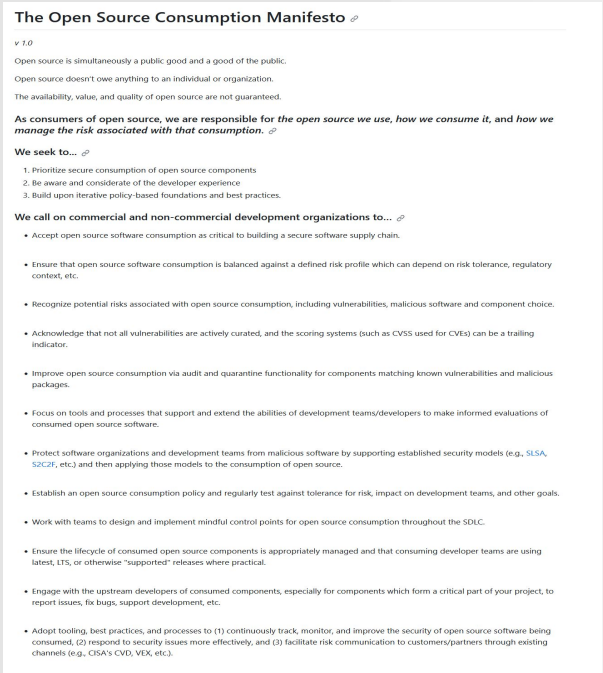
Short List of achievements:

- Signed Releases with sigstore
- Creation of Python Security Response Team (PSRT)
- Became CNA (CVE Numbering authority) for python & pip to control own vulnerabilities
- Open Source Vulnerability DB publication - PSF ADvisory database & PyPA Advisory DB
- Reproducible builds

https://openssf.org/blog/2023/06/22/psf-welcomes-new-security-developer-in-residence-with-support-from-alpha-omega/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The Open Source Consumption Manifesto
Secure Software Development Guiding Principles



The Open Source Consumption Manifesto

v 1.0

Open source is simultaneously a public good and a good of the public.

Open source doesn't owe anything to an individual or organization.

The availability, value, and quality of open source are not guaranteed.

As consumers of open source, we are responsible for *the open source we use, how we consume it*, and *how we manage the risk associated with that consumption.*

We seek to...

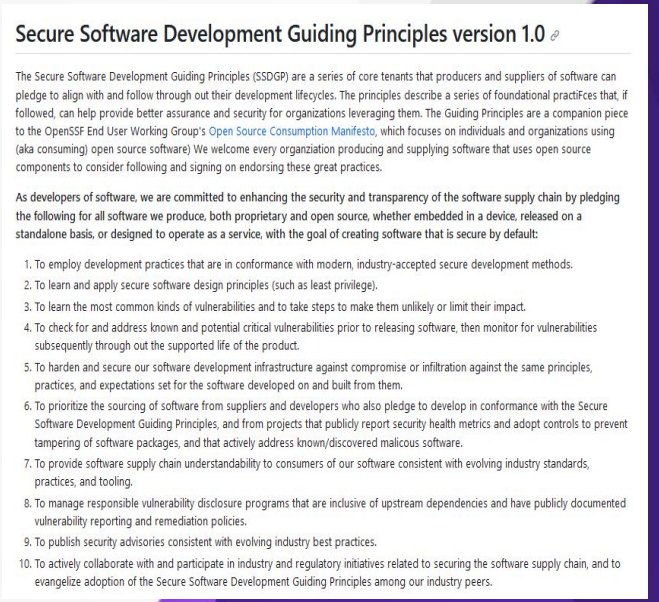
1. Prioritize secure consumption of open source components
2. Be aware and considerate of the developer experience
3. Build upon iterative policy-based foundations and best practices.

We call on commercial and non-commercial development organizations to...

- Accept open source software consumption as critical to building a secure software supply chain.
- Ensure that open source software consumption is balanced against a defined risk profile which can depend on risk tolerance, regulatory context, etc.
- Recognize potential risks associated with open source consumption, including vulnerabilities, malicious software and component choice.
- Acknowledge that not all vulnerabilities are actively curated, and the scoring systems (such as CVSS used for CVEs) can be a trailing indicator.
- Improve open source consumption via audit and quarantine functionality for components matching known vulnerabilities and malicious packages.
- Focus on tools and processes that support and extend the abilities of development teams/developers to make informed evaluations of consumed open source software.
- Protect software organizations and development teams from malicious software by supporting established security models (e.g., SLSA, S2C2F, etc.) and then applying those models to the consumption of open source.
- Establish an open source consumption policy and regularly test against tolerance for risk, impact on development teams, and other goals.
- Work with teams to design and implement mindful control points for open source consumption throughout the SDLC.
- Ensure the lifecycle of consumed open source components is appropriately managed and that consuming developer teams are using latest, LTS, or otherwise "supported" releases where practical.
- Engage with the upstream developers of consumed components, especially for components which form a critical part of your project, to report issues, fix bugs, support development, etc.
- Adopt tooling, best practices, and processes to (1) continuously track, monitor, and improve the security of open source software being consumed, (2) respond to security issues more effectively, and (3) facilitate risk communication to customers/partners through existing channels (e.g., CISA's CVD, VEX, etc.).

https://github.com/ossf/wg-endusers/tree/main/MANIFESTO

Organizations and ICs are invited to read, use, and even pledge to follow these two sets of guidelines!



Secure Software Development Guiding Principles version 1.0

The Secure Software Development Guiding Principles (SSDGP) are a series of core tenants that producers and suppliers of software can pledge to align with and follow through out their development lifecycles. The principles describe a series of foundational practiFces that, if followed, can help provide better assurance and security for organizations leveraging them. The Guiding Principles are a companion piece to the OpenSSF End User Working Group's Open Source Consumption Manifesto, which focuses on individuals and organizations using (aka consuming) open source software) We welcome every organziation producing and supplying software that uses open source components to consider following and signing on endorsing these great practices.

As developers of software, we are committed to enhancing the security and transparency of the software supply chain by pledging the following for all software we produce, both proprietary and open source, whether embedded in a device, released on a standalone basis, or designed to operate as a service, with the goal of creating software that is secure by default:

1. To employ development practices that are in conformance with modern, industry-accepted secure development methods.
2. To learn and apply secure software design principles (such as least privilege).
3. To learn the most common kinds of vulnerabilities and to take steps to make them unlikely or limit their impact.
4. To check for and address known and potential critical vulnerabilities prior to releasing software, then monitor for vulnerabilities subsequently through out the supported life of the product.
5. To harden and secure our software development infrastructure against compromise or infiltration against the same principles, practices, and expectations set for the software developed on and built from them.
6. To prioritize the sourcing of software from suppliers and developers who also pledge to develop in conformance with the Secure Software Development Guiding Principles, and from projects that publicly report security health metrics and adopt controls to prevent tampering of software packages, and that actively address known/discovered malicous software.
7. To provide software supply chain understandability to consumers of our software consistent with evolving industry standards, practices, and tooling.
8. To manage responsible vulnerability disclosure programs that are inclusive of upstream dependencies and have publicly documented vulnerability reporting and remediation policies.
9. To publish security advisories consistent with evolving industry best practices.
10. To actively collaborate with and participate in industry and regulatory initiatives related to securing the software supply chain, and to evangelize adoption of the Secure Software Development Guiding Principles among our industry peers.

https://github.com/ossf/wg-best-practices-os-developers/blob/main/docs/SecureSoftwareGuidingPrinciples.md

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Scorecard 4.12 release & roadmap

4.12 release added GitLab support in addition to the existing GitHub support

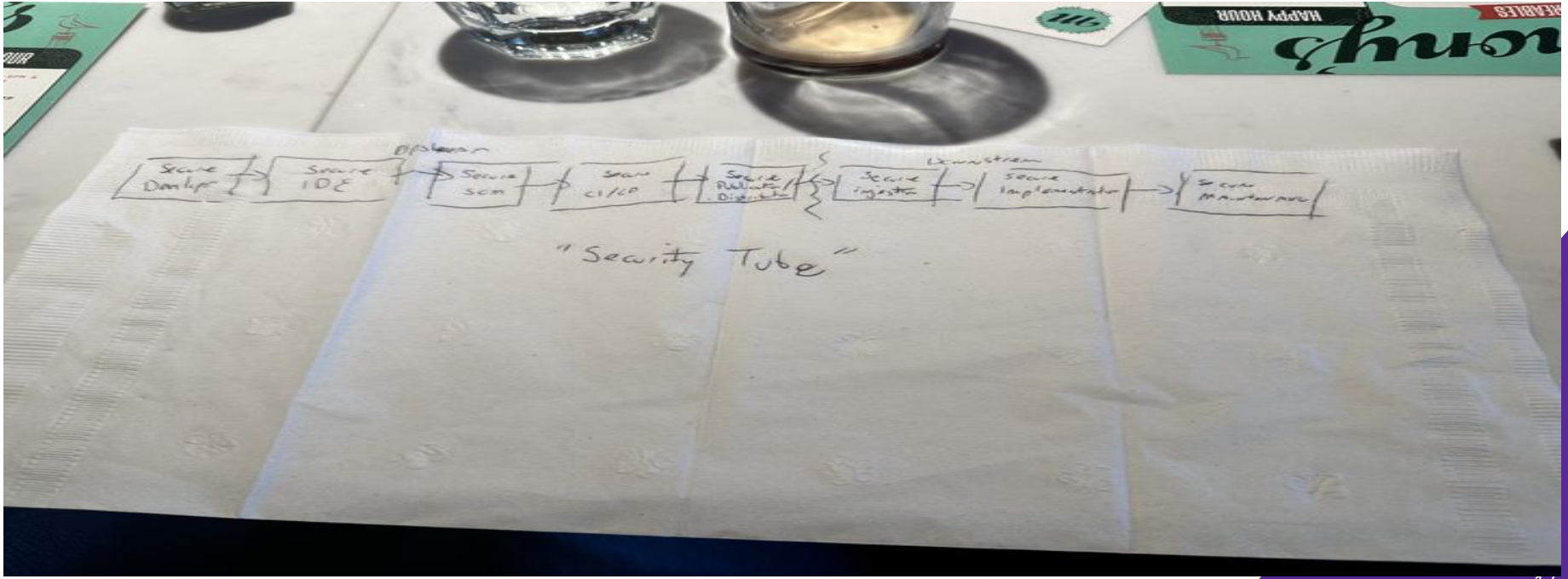
"Both GitLab and GitHub are development platforms focusing on the open source Git system for distributed version control. A whopping 87.2% of surveyed developers rely on Git for version control" - Kinsta "Gitlab vs Github" blog

https://openssf.org/blog/2023/08/28/openssf-scorecard-launches-v4-12-with-support-for-gitlab/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

~~The Sterling Toolchain~~

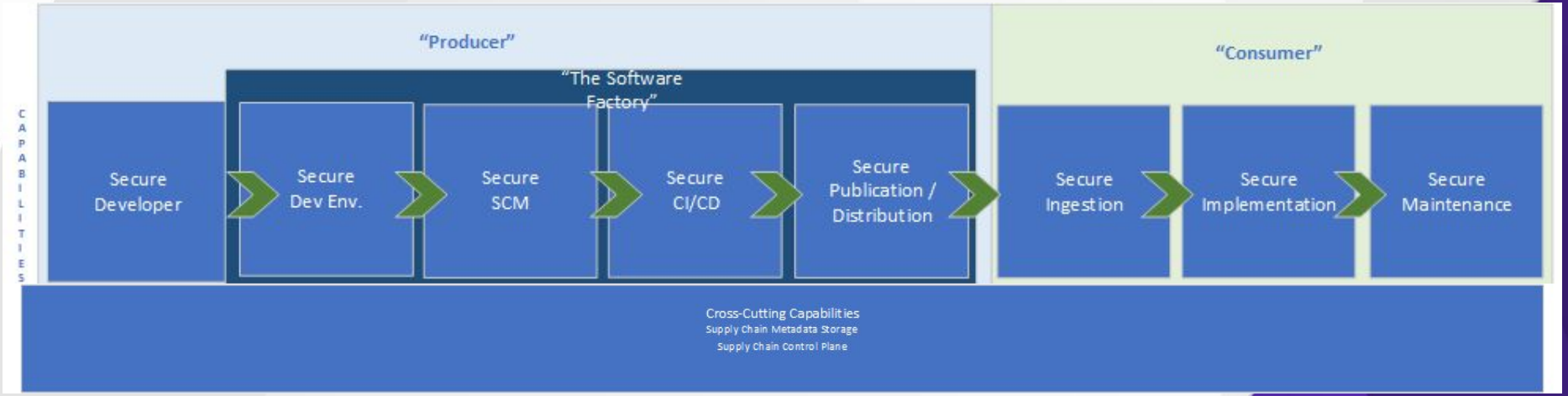
Like all good ideas, ….. it all started with a bar napkin



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The Security Toolbelt

The project formerly known as the “Sterling Toolchain”

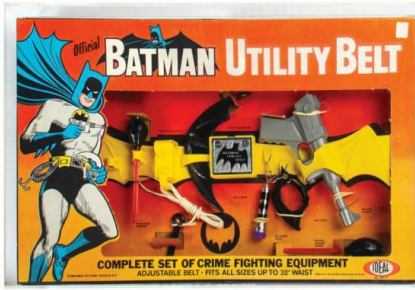


Assemble a “sterling” collection of capabilities (**software frameworks, specifications, and human and automated processes**) that work together to **automatically list, scan, remediate, and secure the components flowing through the software supply chain** that come together as software is written, built, deployed, consumed, and maintained. Each piece of the collection will represent an **interoperable** link in that supply chain, enabling adaptation and integration into the major upstream language toolchains, developer environments, and CI/CD systems. The scanning, remediating, and listing steps will be focused on the core security principles of **security by design** and **secure settings by default**, and the data they depend on will be **constantly updated based on observed threats**.

https://github.com/ossf/toolbelt

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Security Toolbelt Progress since last LFMS



- Team has an MVSR detailing goals and roadmap for delivery
- Team has created list of Capabilities the Toolbelt should deliver
- Team has created a list of Personas and Use Cases the Toolbelt serves and delivers on
- Team is working on set of Threats that affect the security of the OSS Supply Chain
- After Threats are documented, a series of Patterns will be identified that reduce the risk of the Threats
- A gap assessment will be conducted to understand where we lack people, process, & tooling - work to identify community and commercial artifacts that could be used as “patterns in implementation”, recommend creation of missing tools/guidance/processes
- Create Reference Architecture to assist implementors on applying the model
- v1.0 of Toolbelt will be POC’ed with at least 2 critical projects/repositories

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

sigstore goes GA

Notable milestones include use by:

- npm build provenance
- CPython releases
- Kubernetes
- Elastic container images signed with sigstore!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

SLSA major milestone

- v1.0 released!
- npm adoption
- SLSA levels support offered by cloud builders

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

03

2024 AND BEYOND

*"It's easy to say we should do something, but **open source** is **like the tide**. It **does what it wants**"*

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Next Horizon goals

- WG & Project MVSRs with defined roadmaps
- After approval of Operations Model implementation of consistent processes
- Execution on SOSS Task Force deliverables
- Hold Strategic Alignment Summit II to continue alignment of WG & Projects
- Finish v1.0 draft of Security Toolbelt and POC with several projects to validate value

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

04

WHAT CAN YOU DO TO HELP THE PLAN?

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

The single-most critical thing the GB can do to support the TAC, our community, and our assorted Technical Initiatives

A wise man once said:

"I've found it is the small things, everyday deeds of ordinary folk that keeps the darkness at bay.

Even the smallest person can change the course of the future."

Encourage experts from your organization to show up, participate, and collaborate on initiatives that matter

Thank You

CRob_at_Intel_dot_com

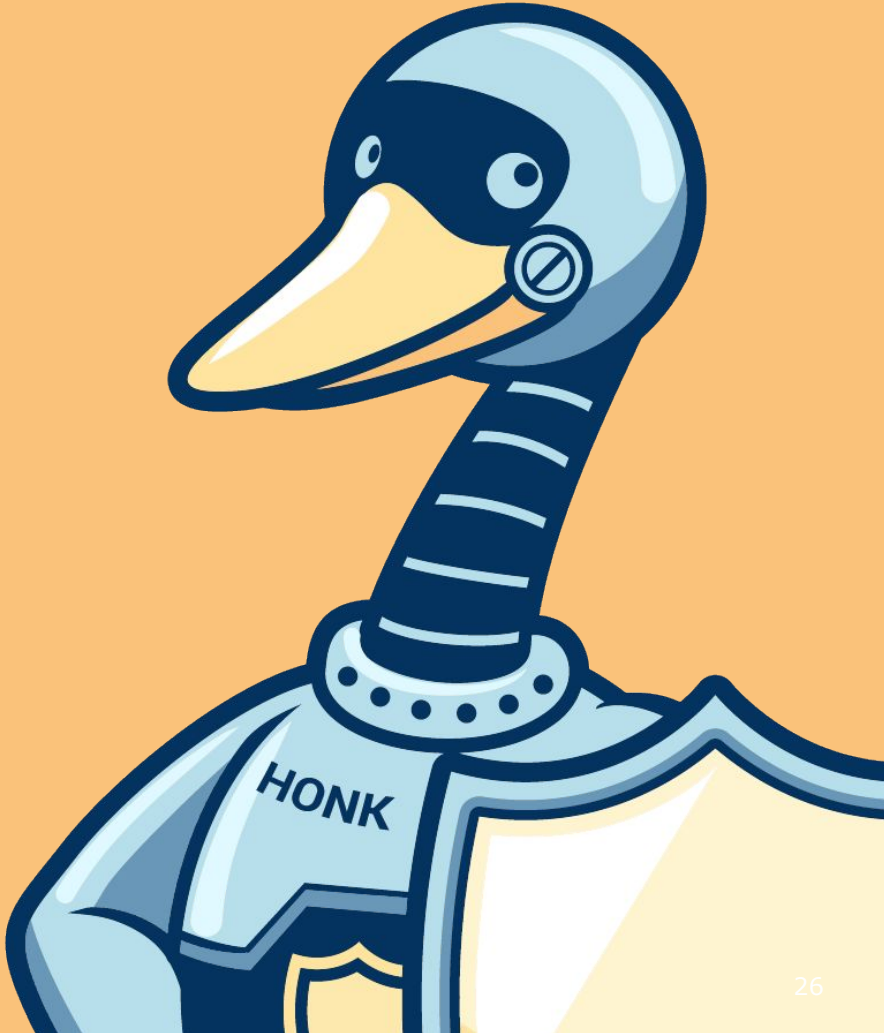
~~@SecurityCRob~~

@SecurityCRob@infosec.exchange

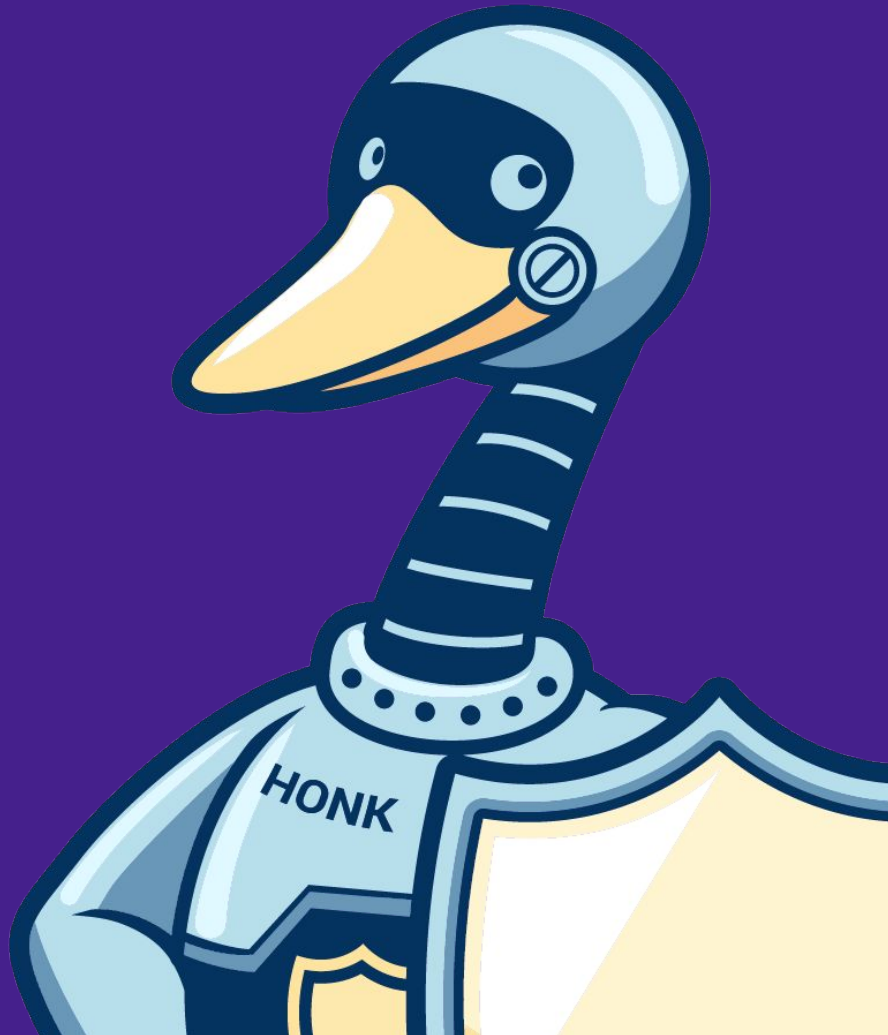
https://github.com/SecurityCRob

The Security Unhappy Hour,
Chips & Salsa

https://www.linkedin.com/in/darthcrob/



#OpenSSF



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

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Follow us on Social Media

[Twitter](#)
@theopenssf

[LinkedIn](#)
OpenSSF

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

[YouTube](#)
OpenSSF

[Facebook](#)
OpenSSF