THE GOLDEN PATH DOESN'T EXIST YET

What platform teams told us about OpenSSF tools

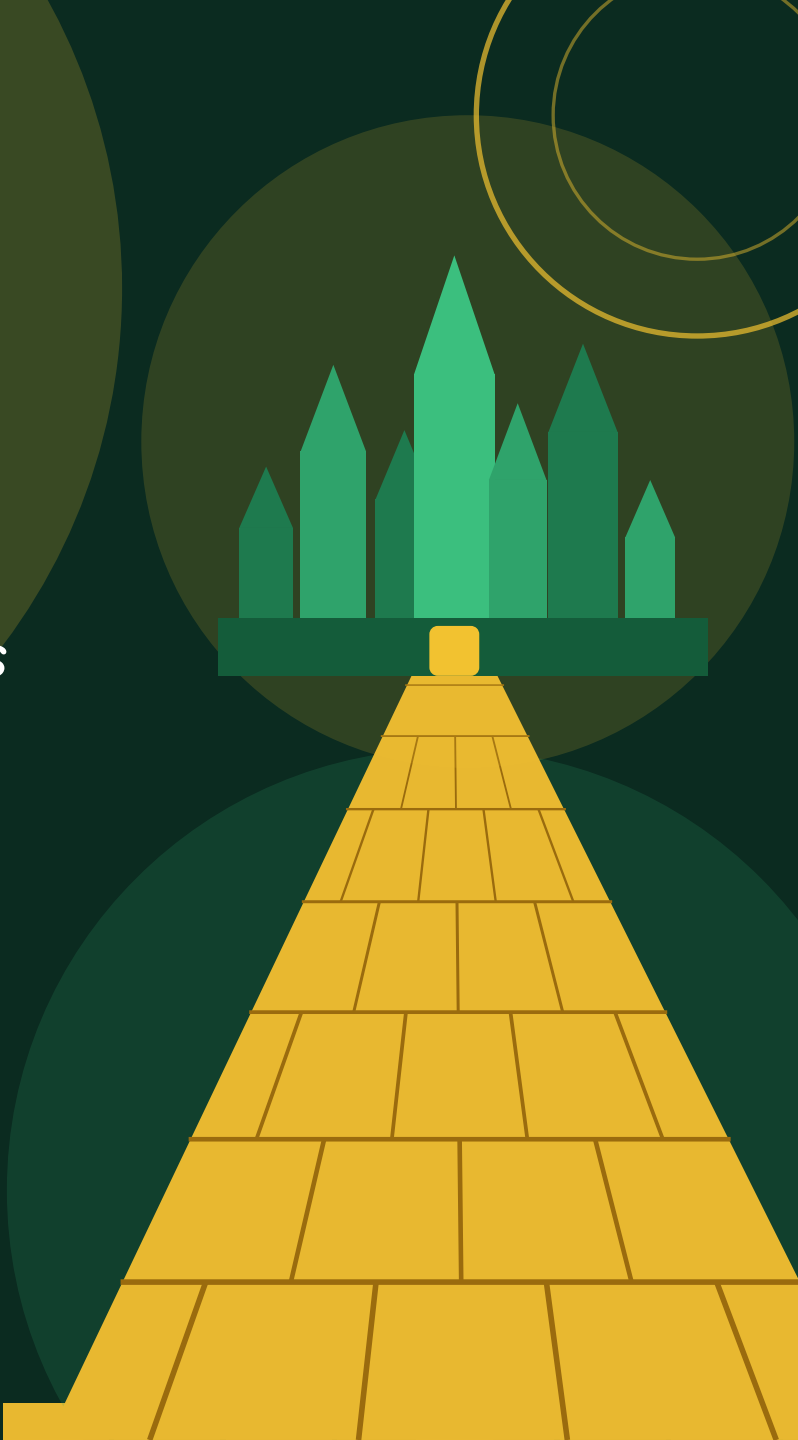
Katherine Druckman · Head of Community & Partnership Engagement, JetBrains

Stacey Potter · Community Manager, OpenSSF

Kadi McKean · OS Community Manager, ReversingLabs

Tabatha DiDomenico · OSS Security Engineer, G-Research Open Source

Open Source SecurityCon · November 9, 2026 · Salt Lake City



ABOUT US · MEET THE PANEL

Your panel



Katherine Druckman

Head of Community & Partnership Engagement, JetBrains

in linkedin.com/in/katherinedruckman



Stacey Potter

Community Manager, OpenSSF / The Linux Foundation

in linkedin.com/in/staceympotter



Kadi McKean

OS Community Manager ReversingLabs

in linkedin.com/in/kadi-grigg/



Tabatha DiDomenico

OSS Security Engineer G-Research Open Source

in linkedin.com/in/tabathad/

CDCON 2026 · THE ROUNDTABLE

We asked platform teams what stands between “good idea” and “working for us.”

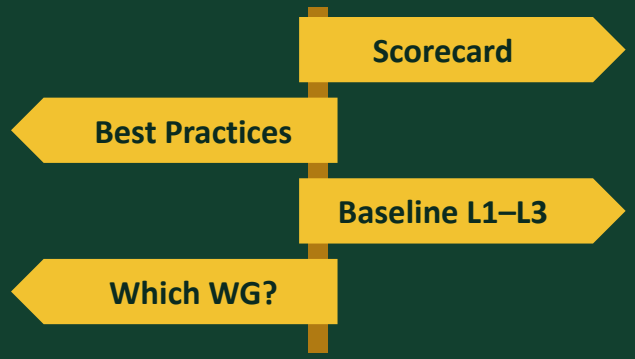
No slides, no demos, no pitches. Practitioners talked; OpenSSF maintainers listened, then answered in the next session.

“We're not here to defend the tools.”

Today, we're asking you the same questions.

FINDING 1 · WE'RE NOT TALKING TO EACH OTHER

Which badge, which level, which project?



Too many badges,
not enough wayfinding.

1. The composite Scorecard score is going away
2. Scorecard v6 will report Baseline conformance
3. The projects are converging to work better together

Start here: persona journeys at openssf.org/getinvolved. “It depends” isn't an answer people can act on.

RELATED OPENSSF PROJECTS

Scorecard

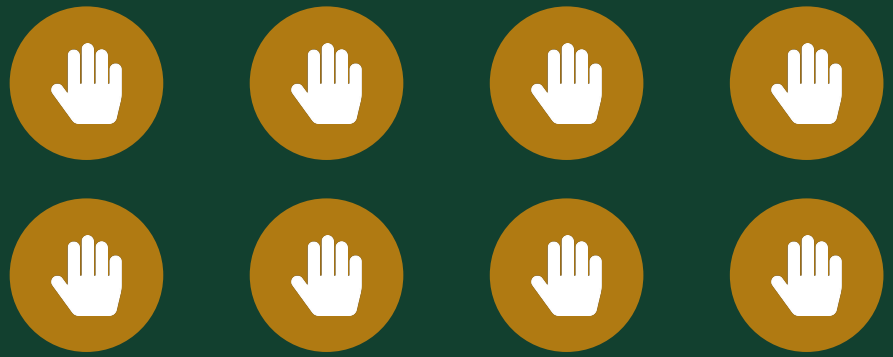
Best Practices Badge

OSPS Baseline

FINDING 2 · THE ADOPTION GAP IS REAL

Is anyone actually implementing SLSA?

HEARD OF SLSA



RUNNING IT IN THEIR BUILD

0

at cdCon, May · **Europe, Oct: a few**

WHY NOT?

- *“We already have this”*
- *“Downstream rebuilds anyway”*
- *“The tooling fought us”*
- *“It needed the internet”*

FINDING 3· A YEAR ON, WE STILL DON'T TRUST OUR SBOMS

Why aren't teams consuming SBOMs?

Inconsistent

different tool, stage = different SBOM

Missing data

no license or supplier

Doesn't travel

which artifact does this go to?

Legal risk

known-wrong = liability

SBOM

RELATED OPENSSF PROJECTS


GUAC


BOMHort


OpenVEX


SBOMit


Protobom


bomctl

THE CLOSEST THING TO A WIZARD

Is there a golden path to the OSPS Baseline?



One bar.
Three levels.

1. OSPS Baseline is the bar, mapped to NIST, the EU CRA, ISO 18974, PCI DSS, BSI, SAMM, and more
2. darnit and Privateer show where you stand
3. darnit and Minder help fix it; Security Insights and Gemara make it machine-readable

An audit doesn't make you more secure. The work still has to get done and once done, keep

RELATED OPENSSF PROJECTS

 Baseline

 Security Insights

 Scorecard

 Privateer

 darnit

 Minder

 Gemara

FINDING 4 · AIR-GAPPED AND REGULATED TEAMS HIT THE WALL FIRST

What breaks without the public internet?





Needs the internet

Sigstore build-out stalled

Hosted runners

hardening costs extra





DIY trust roots

copy TUF metadata by hand

More moving parts

OIDC, Fulcio, Rekor, policy





AIR GAP

“It required the public internet.”

FINDING 4 · THE GOLDEN PATH DOESN'T EXIST YET

“I have one security engineer. Where do I start?”

1

usually a generalist,
doing everything else too

1. Start with the problem, not a tool
2. Use platforms that give you security for free
3. Put your one engineer on what they do best

The ask: “I want the golden path — done for me.” It doesn't exist yet.

MEANWHILE · EVERYONE'S LOOKING AT AI

“Do these tools still matter now?”



AI

security with AI,
from AI, and for AI

1. Agents make the same problems happen faster
2. Everyone's looking at AI; the basics still break
3. Provenance matters more: who built this?

October 2026: the headline incidents were the basics — a credential that lived too long, a machine that was trusted when it shouldn’t have been.

YOU'VE ALREADY WALKED PART OF THIS ROAD

Lay one brick.

OpenSSF Project Feedback Survey



Pick your brick

Which of the five have you solved, even partly? SBOMs at scale, SLSA, signing in an air gap, getting a team to the Baseline.

Scan and tell us

Two lines on how you did it. We'll put you on the right call to share it.

Help write the journey

Your story goes into a platform engineer journey on openssf.org/getinvolved. There isn't one yet.

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

The golden path doesn't exist yet.

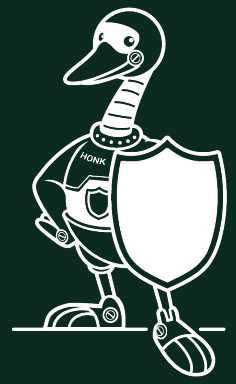
Help us build it, brick by brick.

Feedback Survey

Get involved: openssf.org/getinvolved
Working Group & **Project Calendars** are public: openssf.org/calendar
OpenSSF GitHub repository: github.com/ossf
All projects: openssf.org/projects

Katherine Druckman · Stacey Potter · Kadi McKean · Tabatha DiDomenico

Thank you! Come find us on OpenSSF Slack.



OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Backup slides

For Q&A only.



THE GOLDEN PATH · BASELINE LEVELS 1–3

darnit

A new OpenSSF sandbox project that finds the holes in your project, Baseline Level 1 to Level 3, and helps you darn the ones it can.

github.com/darnitdevorg/darnit

WHAT PROBLEM DOES IT SOLVE?

The Baseline is the destination, but hand-checking 62 controls across every repo, then keeping them green, is work no maintainer has time for.

WHAT IS IT?

Started at Kusari, now an OpenSSF sandbox project with its own TSC. darnit-baseline audits all 62 controls of OSPS Baseline v2025.10.10, Levels 1–3, and never assumes a pass.

HOW DO I ACTUALLY USE IT?

Run /darnit-audit in your coding agent, or darnit audit for a quick check. You get a punch list. Approve the fixes it can open as PRs; settings like branch protection need your forge or Minder.

L1–L3 One command to see where you stand at every Baseline level: a punch list plus a Sigstore-signed attestation.

WHY THIS MATTERS

How do supply chain attacks get in?



The malicious package

Three layers deep in your dependency tree — code you never chose, running with your privileges.



The compromised build

The pipeline is subverted long before your artifact ships. What you built isn't what you wrote.



The opaque release

So opaque that something can go missing for days before anyone notices.

THIS ISN'T HYPOTHETICAL

Has this actually happened?

axios Mar 2026

A maintainer installed malware during a fake company meeting. Two poisoned releases dropped remote access trojans.

LiteLLM Oct 2026

Stolen GitHub tokens ran the real release pipeline against a lookalike fork. Provenance faithfully recorded the wrong source.

Trivy Mar 2026

76 of 77 trivy-action tags force-pushed. CI runs leaked their secrets. A token left over from an earlier breach let them back in.

Mini Shai-Hulud May 2026

One hijacked npm account published 637 malicious versions across 317 packages in 22 minutes, stealing cloud and SSH keys.

WHO'S WORKING ON THIS?

OpenSSF: the foundation behind the tools.

The Open Source Security Foundation is a cross-industry community, hosted by the Linux Foundation, whose mission is to make it easier to sustainably secure how open source is **built, maintained, released, and consumed.**

Developers, security engineers, and maintainers, working together to close these gaps before attackers find them.



OpenSSF

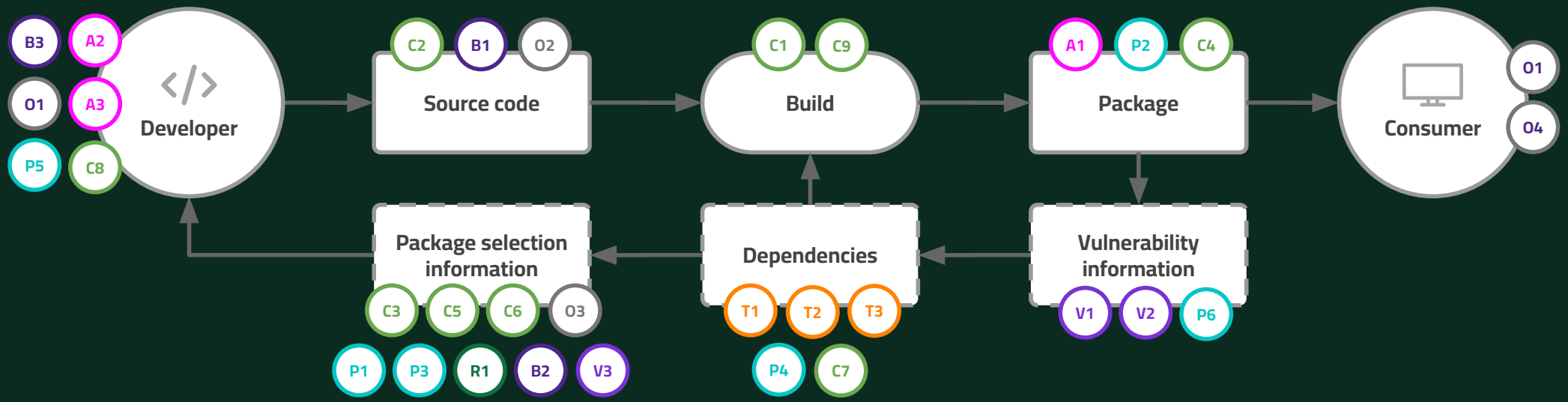
OPEN SOURCE SECURITY FOUNDATION

2020 Founded, under the Linux Foundation

100+ Member Companies contributing

1 goal Improve open source security

OpenSSF Projects Landscape



Best Practices
- B1. OpenSSF Best Practices Badge
- B2. OpenSSF Scorecard
- B3. Concise Guides

Securing Software Repositories
- R1. RSTUF

AI/ML Security
- A1. Model Signing
- A2. OSS-CRS
- A3. Secure Agentic Framework

Global Cyber Policy

Supply Chain Integrity
- C1. SLSA
- C2. Gittuf
- C3. GUAC
- C4. Zarf
- C5, Malicious Packages
- C6, Package Analysis
- C7. BOMHort
- C8. Darnit
- C9. Ampel

Japan

DevRel Community

SBOM & VEX
- T1. SBOMit
- T2. Protobom
- T3. bomctl

Vulnerability Disclosures
- V1. OSV Schema
- V2. OpenVEX
- V3. Criticality Score

BEAR (Belonging, Empowerment, Allyship, and Representation)

ORBIT (Open Resources for Baselines, Interoperability, and Tooling)
- O1. OSPS Baseline
- O2. Minder
- O3. Security Insights
- O4. Gemara
- O5. Privateer

Projects
- P1. Alpha & Omega
- P2. Sigstore
- P3. Core Toolchain Infrastructure (CTI)
- P4. Fuzz Introspector
- P5. OpenBao
- P6. CVE Binary Tool

THE SOFTWARE SUPPLY CHAIN · EVERY STAGE CAN BE ATTACKED

Where can an attacker get in?

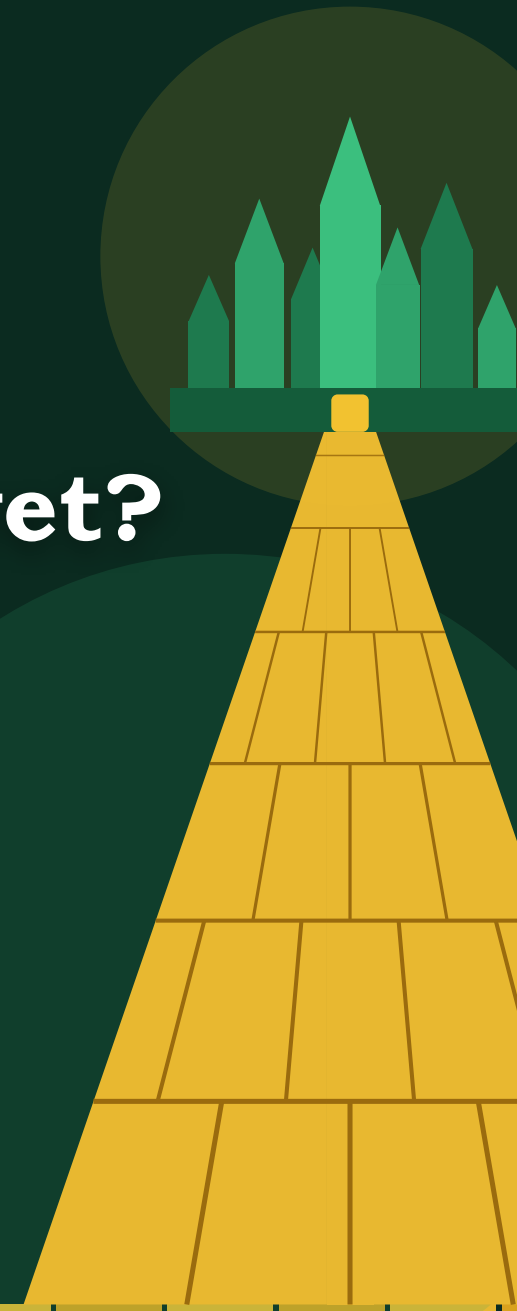


An attacker only needs one weak stage. Every stage has an OpenSSF project that helps — and they report up through working groups you can plug into.

What helps today, and what doesn't yet?

Where OpenSSF tooling meets the blockers, and where it still falls short.

Sigstore · Zarf · GUAC · BOMHort · SLSA · Scorecard
OpenBao · Privateer · OSS-CRS · Alpha-Omega · OSPS Baseline · darnit





PACKAGE · SIGN & VERIFY

Sigstore

Signing and verification made usable, so what you deploy is what was actually built.

sigstore.dev

WHAT PROBLEM DOES IT SOLVE?

Is the artifact I'm about to deploy really the one built from trusted source, unmodified? Old code-signing was so painful almost no one signed.

WHAT DOES IT DO TODAY?

Keyless signing and verification. You authenticate with an identity you already have (Google, GitHub, CI) — **Fulcio** issues a short-lived cert, **Rekor** logs it publicly. No long-lived keys to leak.

WHERE DOES IT STILL FALL SHORT?

Air-gapped teams: verifying works offline with bundles and a current trust root, but keyless signing needs your own Sigstore stack, or keys. Large CI fleets report rate limits and latency.

npm provenance and PyPI attestations are GA, both signed with Sigstore.



DISTRIBUTE · CROSS THE AIR GAP

Zarf

Packages everything an app needs into one archive you carry into a disconnected network and deploy offline.

zarf.dev

WHAT PROBLEM DOES IT SOLVE?

Air-gapped and regulated networks can't pull images, charts, or trust roots from the internet, so teams write their own transfer scripts.

WHAT DOES IT DO TODAY?

Bundles container images, Helm charts, manifests, and SBOMs into one signed package. zarf package create outside the gap; zarf init and zarf package deploy inside it.

WHERE DOES IT STILL FALL SHORT?

Built for Kubernetes targets. Moving the package across the gap is still on you, and keyless Sigstore signing still needs a private stack inside.

2024 Contributed by Defense Unicorns; now an OpenSSF sandbox project.



CONSUME · CORRELATE THE EVIDENCE

GUAC

Graph for Understanding Artifact Composition: one queryable graph of your SBOMs, attestations, and vulnerability data.

guac.sh

WHAT PROBLEM DOES IT SOLVE?

SBOMs, attestations, and vulnerability feeds live in separate places, so “which of our apps ship this vulnerable package?” takes manual digging.

WHAT DOES IT DO TODAY?

Ingests SPDX and CycloneDX SBOMs plus SLSA and in-toto attestations, then adds vulnerability data and Scorecard results. Query the graph over GraphQL.

WHERE DOES IT STILL FALL SHORT?

You run it: backends, ingestion, and deployment gates are your integration work. And the graph is only as accurate as the SBOMs you feed it.

1.0 shipped June 2025; an OpenSSF incubating project since March 2024.



CONSUME · SEE EVERY SBOM AT ONCE

BOMHort

Kubernetes-native SBOM visualization and governance: every SBOM, vulnerability, and license in one dashboard.

bomhort.dev

WHAT PROBLEM DOES IT SOLVE?

Teams that do generate SBOMs end up with thousands of files and no single view of which vulnerabilities and licenses they actually ship.

WHAT DOES IT DO TODAY?

Ingests SPDX, CycloneDX, and in-toto attestations at scale, checks components against OSV with a daily CVE refresh, applies VEX statements, and enforces license policy in one dashboard.

WHERE DOES IT STILL FALL SHORT?

It's brand new, and you run it yourself: Kubernetes, Helm, and a ClickHouse backend. Like GUAC, it's only as accurate as the SBOMs you feed it.

2026 Joined the OpenSSF sandbox in August; formerly SeeBOM.



BUILD · TRUST THE PROCESS

SLSA

An auditable chain of provenance for your software — so you can trust the build, not just the source.

slsa.dev · "salsa"

WHAT PROBLEM DOES IT SOLVE?

Even a signed artifact can be malicious if the build itself was compromised. In October, LiteLLM shipped a release built from a lookalike fork.

WHAT DOES IT DO TODAY?

A specification with many implementations, not one tool. The Build track (L1–L3) proves how an artifact was built; the Source track, approved in v1.2, covers version control.

WHERE DOES IT STILL FALL SHORT?

Hearing of it isn't running it: zero hands at cdCon. Practitioners report brittle provenance generators with silent errors, and hardening hosted runners costs extra.

v1.2 Source track approved Nov 2025. Build Environment and Dependency tracks are still in development.



SOURCE · VET BEFORE YOU TRUST

Scorecard

A fast, objective read on a dependency's security practices before you trust the package.

scorecard.dev

WHAT PROBLEM DOES IT SOLVE?

You have no fast, objective way to judge whether a dependency follows safe practices before you pull it in.

WHAT IS IT?

An automated tool that scans a repo against ~18 security checks and returns a health signal — branch protection, code review, pinned dependencies, dangerous workflows, and more.

HOW DO I ACTUALLY USE IT?

Drop in the GitHub Action, or run the CLI:

```
scorecard --repo=github.com/org/project.
```

Allstar, for org-wide policy, is now self-hosted.

1.3M+ Of the most-used open source projects are continuously evaluated.



DEPLOY · SECRETS THAT EXPIRE

OpenBao

Open source secrets management: credentials issued when you need them and revoked when their lease ends.

openbao.org

WHAT PROBLEM DOES IT SOLVE?

Static tokens and keys live in CI variables, config files, and laptops. Steal one and it keeps working until someone rotates it.

WHAT DOES IT DO TODAY?

Stores and distributes secrets, certificates, and keys. Generates dynamic secrets on demand for systems like AWS and SQL databases; every secret has a lease and is revoked when it ends.

WHERE DOES IT STILL FALL SHORT?

On Kubernetes you run an injector or operator, and auth errors can be hard to debug. Deciding which pipeline or agent gets which secret is still your policy work.

TTL A community fork of HashiCorp Vault under the Linux Foundation; an OpenSSF sandbox project.



DEPLOY · CHECK WHAT'S RUNNING

Privateer

A plugin framework that checks deployed systems against security and compliance controls and reports in a standard format.

github.com/privateerproj

WHAT PROBLEM DOES IT SOLVE?

Controls like the Baseline say what should be true. Someone still has to check, again and again, that it's true of the systems you actually run.

WHAT DOES IT DO TODAY?

The pvtr CLI runs plugins that test systems from a user's and an attacker's point of view, with machine-readable Gemara output. Its GitHub repo scanner checks repos against the OSPS Baseline.

WHERE DOES IT STILL FALL SHORT?

Coverage depends on the plugins that exist for your stack. In the Baseline scanner, Level 1 checks are the most tested; Levels 2 and 3 are still in development.

2026 Joined the OpenSSF sandbox in July, sponsored by the ORBIT working group.



OSS-CRS

FIND & FIX · AI THAT HUNTS BUGS

OSS-CRS

A framework for running the AI cyber reasoning systems from DARPA's AI Cyber Challenge, which find bugs and propose fixes.

github.com/ossf/oss-crs

WHAT PROBLEM DOES IT SOLVE?

The AI Cyber Challenge systems found real bugs, but most depended on the competition's infrastructure and were hard to reuse.

WHAT DOES IT DO TODAY?

A standard interface for LLM-based bug-finding and bug-fixing systems. Runs them against any project in OSS-Fuzz format, combines several in one campaign, and caps CPU and LLM spend per system.

WHERE DOES IT STILL FALL SHORT?

In the project's study of 630 AI-generated patches, 20–40% were wrong even though they passed automated checks. A human still reviews every fix.

2026 Joined OpenSSF in April under the AI/ML Security working group.

THE PEOPLE · FUND THE CRITICAL

Alpha-Omega

Backing the critical, under-resourced projects everyone depends on.

alpha-omega.dev

WHAT PROBLEM DOES IT SOLVE?

The most critical open source is often maintained by unpaid, under-resourced volunteers. The xz backdoor is what that risk looks like.

WHAT IS IT?

An OpenSSF-associated initiative that funds and directly supports security work — 'Alpha' for the biggest, most-depended-on projects, 'Omega' for the long tail of small-but-essential ones.

HOW DO I ACTUALLY USE IT?

Grants, security audits, and embedded security engineers. Real engagements: a PyTorch ExecuTorch audit, Rust infrastructure hardening, and funding to Python/PyPI, OpenSSL, Node.js, and more.

$12.5M in new open source security funding announced via the LF and Alpha-Omega in March 2026.



POLICY · THE ONE YOU CAN'T PATCH WITH CODE

What does the CRA mean for open source?

Most volunteer maintainers have no obligations, but their companies might!

Dec 2024
Entered into force

Sept 2026
Manufacturer reporting — now in force

Dec 2027
Full obligations apply

Why it lands on companies, not you

- The CRA's obligations fall on **manufacturers** placing “products with digital elements” on the EU market.
- Open source is addressed through a dedicated "open source steward" role.

OpenSSF is here to help!

- A public forum helping open source meet global cyber regulation.
- Free resources: the "Understanding the EU CRA" course (LFEL1001) and a CRA Brief Guide for OSS developers.

Plug in: public calls every other Monday · github.com/ossf/wg-globalcyberpolicy · policy.openssf.org
CRA episodes on the “What’s in the SOSS?” podcast



WHOLE PROJECT · START FROM ZERO

OSPS Baseline

A step-by-step framework any project can adopt from zero.

baseline.openssf.org

WHAT PROBLEM DOES IT SOLVE?

Maintainers often don't know what 'good enough' security even looks like — and consumers lack a common bar to point to.

WHAT IS IT?

A tiered checklist of the minimum security controls an open source project should meet, written as unambiguous MUST requirements and organized by maturity level.

HOW DO I ACTUALLY USE IT?

Pick the tier that matches your project's maturity and work the controls. Baseline crosswalks to NIST and EU regulations (including the Cyber Resilience Act) — comply once, reuse everywhere.

2025 GA and date-versioned since. darnit audits all three levels today; Scorecard v6 is being built to report it.