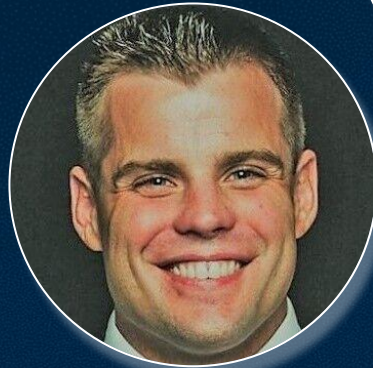


Introducing OSERA: The Open Source Enterprise Resiliency Alliance

Dov Katz, Managing Director,
Morgan Stanley &
Eric Baran Senior Vice President, Sales,
Moderne



We've been working this since December

From early concern to practical proof



1

December

The conversation starts

Practitioners identified the coming burden of open-source resilience.



2

Working group

We organized

Cross-firm team formed to focus on practical action.



3

Priority app

We built tooling

An app helps identify the highest-priority remediation opportunities.



4

4 live patches

We proved the path

With Moderne's help, several firms wired 4 real patches into their supply chains in hours.



Key message: This is not a theoretical conversation – we already have a working model.

Apache Camel

2.25.4+backpatch.001

Java · integration

Bouncy Castle

1.47+backpatch.001

Java · cryptography

Netty

3.10.6.Final+backpatch.001

Java · networking

Spring Framework

5.3.39+backpatch.001

Java · app framework

Prioritise open source remediation with Risk Navigator

Risk Navigator turns dependency and vulnerability data into a practical remediation view: what is exposed, which projects are affected, and where upgrades or backpatches should be prioritised.

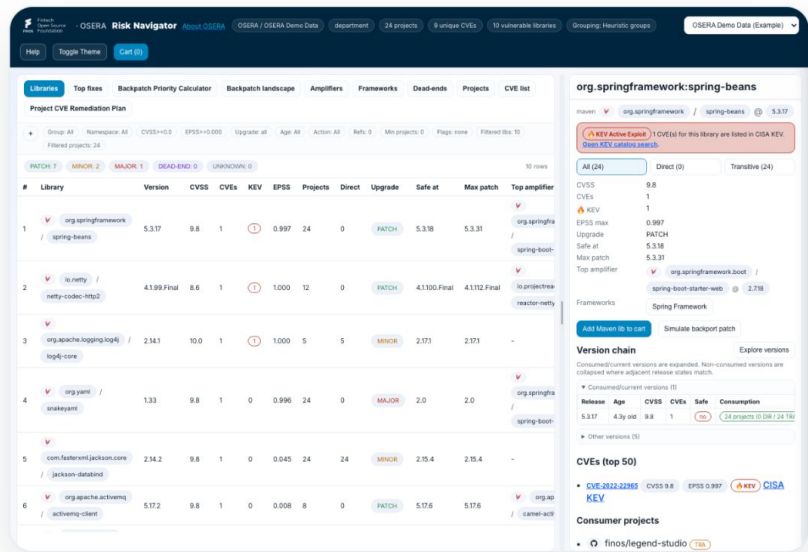
From vulnerable libraries to action

Use the overview to inspect vulnerable packages, CVEs, affected projects, safe versions, and backpatch candidates before bringing work into the OSERA formation process.

- Rank libraries by CVSS, KEV, EPSS, project footprint, and upgrade path.
- See which applications are directly or transitively exposed.
- Identify candidates for upgrade guidance, OpenRewrite recipes, or backpatch work.

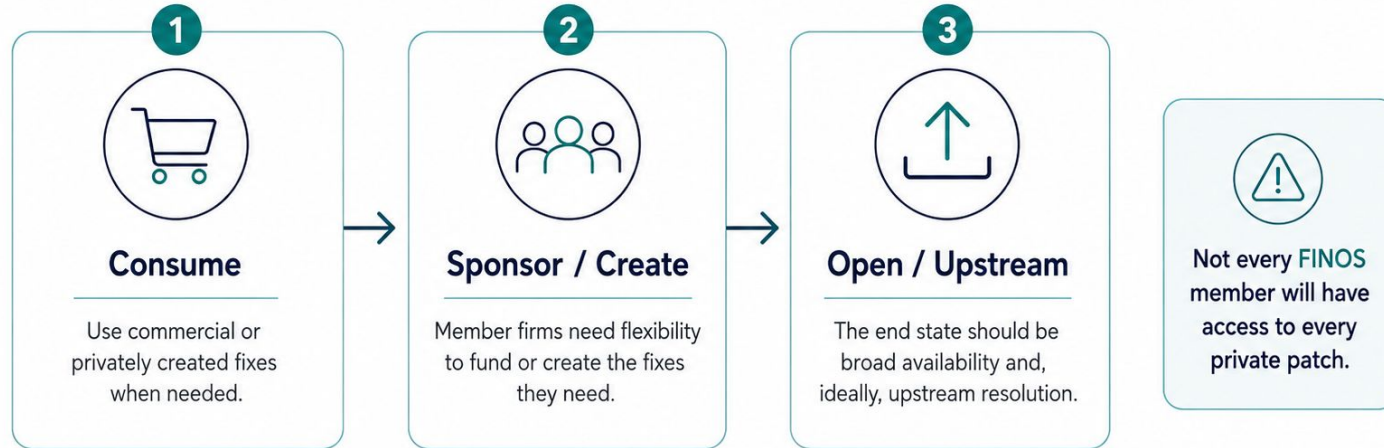
Open Risk Navigator

See related workstreams



Patches alone are not the end game

Private fixes help, but the ecosystem needs an open operating model



Key message: The goal is not just more patches — it is durable, shared remediation paths.

Our guiding principles

How open source security should work in the AI era

1

No monopolies, no capture

No single organisation should control how open source is patched. We strengthen the commons; we do not enclose it.

2

Upstream first

Wherever possible, fixes flow back to the original projects — free, public, and available to the whole community.

3

Coordination is the hard part

Anyone can write a patch. The real work is triage, testing and responsible disclosure — and that takes collective action.

4

Evidence with every fix

A fix should arrive with proof — its origin, contents and testing — so consumers can trust it and show their regulators they did.

5

Automation reduces toil, not accountability

AI can do more of the work, but a human still owns the decision to ship. Speed must never outrun responsibility.

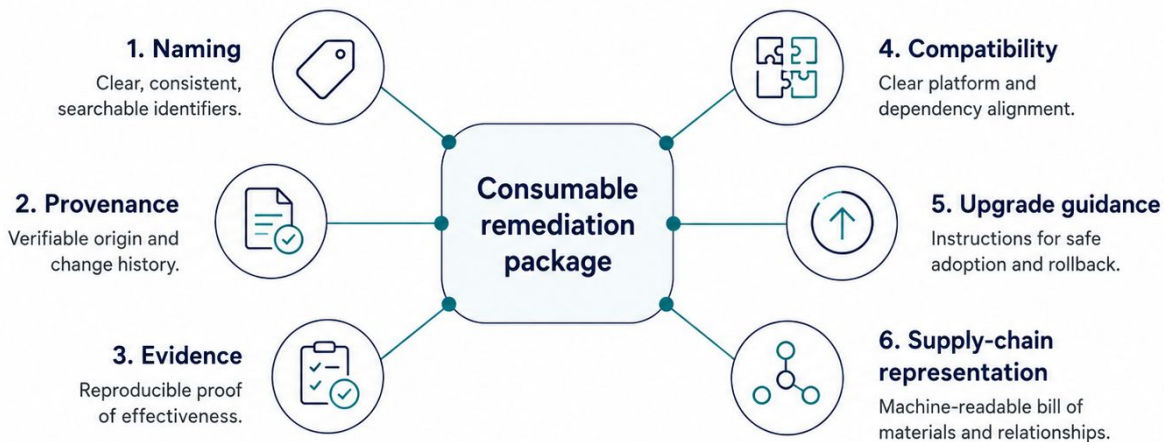
6

Organise globally

Open source crosses every border. So must its defence — for institutions of every size, in every country.

What needs to Standardize

So practitioners can roll fixes into production at scale



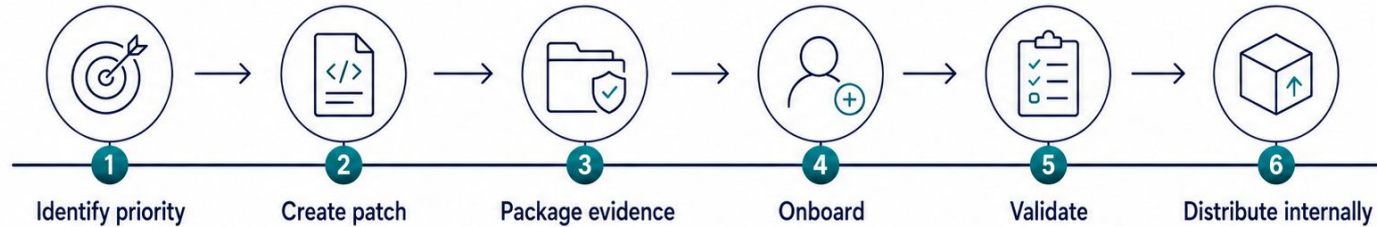
A fix is not truly fixed until it can be rolled into production safely and repeatedly.



Key message: Consistency turns patches into scalable operational outcomes.

Proof of concept: From Patch to Patched in Hours

We validated the workflow end to end



4 live patches



Hours, not months



Several firms wired the patches into compliant software onboarding pipelines to prove the path.



Key message: The technical path already works — now it needs to become repeatable.

What good looks like - and what comes next

Move from ad hoc fixes to a repeatable industry capability

A good remediation package is:



✓ Clearly originated



✓ Consistently described



✓ Automation-ready



✓ Safe to consume at scale

Next step



Join the breakout



Help shape the standards



Bring real supply-chain practitioners into the process



The community now has the chance to turn a working proof into a shared operating model.



Key message: Participation is how this becomes industry infrastructure.



osera.finos.org



ANNOUNCEMENT COMING SOON

AN OPEN, TWO-SIDED PLATFORM

End users and tech producers, in one neutral venue

Not a vendor and not a buyers' club — an open ecosystem. Institutions that **run** open source meet the technology firms with deep upstream expertise that **maintain** it. No single firm sits in the middle.

END USERS · DEMAND

Everyone who runs the software

- Banks, insurers & market infrastructure
- Fintechs
- Regulated enterprises beyond finance
- Technology providers to the sector

Resilient, compliant OSS at a fraction of single-firm cost.

The open, governed platform

FINOS neutral governance · open standards
· per-project funding pools

IP & antitrust

Confidentiality

Open standards

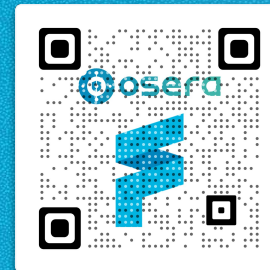
Upstream-first

TECH PRODUCERS · SUPPLY

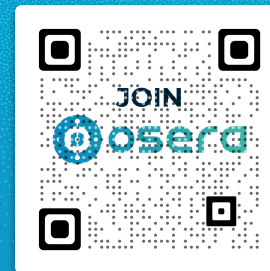
Firms with upstream expertise

- Upstream specialists
- OSS maintainers
- Security & remediation firms
- SIs & consultancies

Reach the whole sector through one neutral channel — no lock-in.



LEARN MORE



JOIN

Incubated in financial services — open to any regulated enterprise that runs the same software.

Two complementary efforts, one coordinated response

UPSTREAM

AKRITES

- Central security response team (SIRT)
- One coordinated disclosure and upstreaming process
- Maintainer of last resort for critical, under-maintained OSS
- Neutral & cross-industry — the shared engine for the commons

One trusted partner for maintainers — not a flood of duplicate reports.

DOWNSTREAM

OSERA

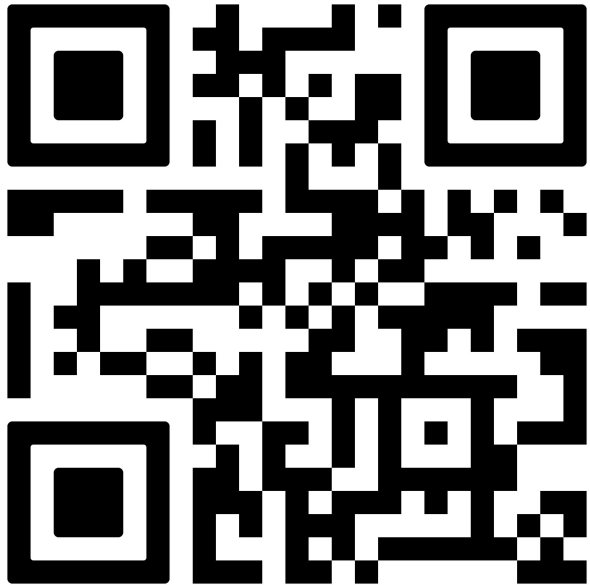
- FINOS Bank-grade neutral governance and collaboration platform
- The sector-specific work: prioritise, maintain, consume, standardise
- A flexible funding model and predictable SLA
- Works in step with Akrites to route disclosure through it and

Incubated in finance; the model extends to any regulated enterprise.

Are we **done** yet?

The Open Data Opportunity

 FINOS  forming



The Value of Open Data on Global Entities

Turning the World's Largest Open Entity Graph into a Catalyst for Collaboration, Innovation, and Transformation

June 2026

Kirsten D. Sandberg
Foreword by Gabriele Colombo, FINOS

finos.org

OPEN DATA ON GLOBAL ENTITIES



“The opportunity for **openly licensed, high-quality, mutually maintained datasets** is simply incredible for every AI technology provider and adopter.”
– Gabriele Columbro,
Executive Director, FINOS

OPEN DATA ON GLOBAL ENTITIES

Graph-based **credit models** link corporate entities and financial data to hone risk assessments, detect distress, inform lending decisions, and strengthen credit monitoring across markets.



OPEN DATA ON GLOBAL ENTITIES



Open entity graphs cut bank costs, fine-tune **capital markets analysis**, and organize company relationships for risk detection, portfolio screening, and regulatory insight across open datasets.

OPEN DATA ON GLOBAL ENTITIES

Open data and AI streamline **trade compliance**, reduce onboarding costs, improve cross-firm identity checks, and accelerate fraud detection through shared entity graphs and automated workflows.





Research



2026 State of Open Source in Financial Services Survey

TAKE THE
SURVEY





OPEN SOURCE
— IN —
FINANCE FORUM

