

Lessons From Funding Open Source Security Over the Past 3 Years, What's Ahead

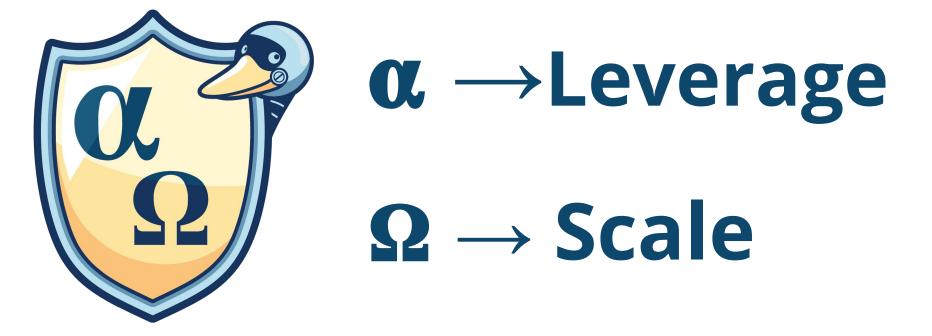
Michael Winser michaelw@xwind.io VulnCon 2025

Alpha-Omega Mission



Catalyze sustainable security improvements within the most critical open source projects and ecosystems.

Alpha-Omega Explained



Alpha-Omega Grants



\$23M Raised

AWS, Google, Microsoft

Citi

Al Libraries Airflow Apache (ASF) Clang Eclipse FreeBSD Homebrew Jenkins JQuery Linux Kernel LLVM NodeJS OpenJS OpenSSL PHP Python Rubygems Rust Scaled OSS Security



Cleaning the Pacific Garbage Patch

You're gonna need a bigger boat



Cleaning one Beach at a time

Security Transformation



All Good Things Start With An Audit



When Security Is Everyone's Job, **Security Is Nobody's Job**



Security Roles Are About Leadership

People > Culture > Processes > Vulns

Security = f(\$)

Shovel Ready Projects

Quick Action and Impact



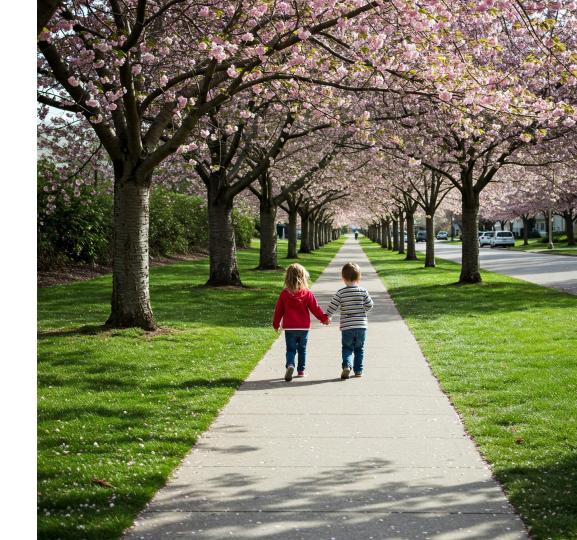
Always create a public good



Look for Leverage



Holding hands Not Hands on



Connecting Communities Across

Ecosystems



Resources + Culture > Money



Open Source funding is not wired for security software engineering

You can't fund more nights and weekends

Growth beats security, even in Open Source

The bad economics of Open Source infrastructure are partially hidden by cloud credits

The business model => funding model

It's All *Your* Code





Free Puppies VS Free Beer



Most of your spend is internal Most of your risk is external



The Evolution of Criticality

ALL MODERN DIGITAL INFRASTRUCTURE

...:

••••

· [IIII]

· 🔛



A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003



Fixing

Forking

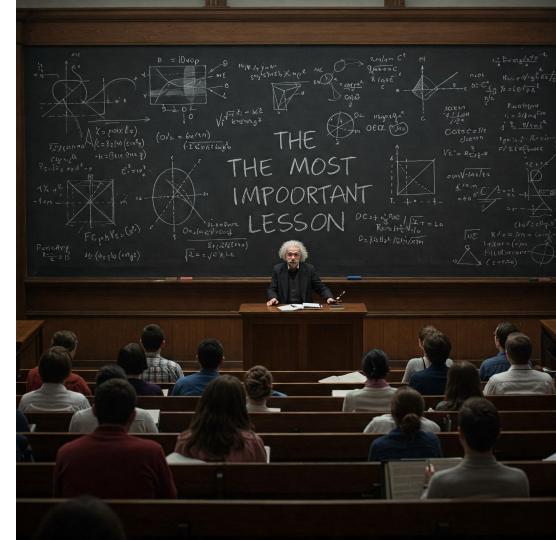
Forgoing

BFS

It's All *Your* Problem

The Most

Important Thing







































































































Keep Going



Taking On Big Problems

Normalizing

Co-funding initiatives

Audits and Rapid Security Reviews (w/ EF and OSTIF)

SLSA, Sigstore, & Security Baseline

Transparent and Reproducible Builds

New Ideas

Safer Al Libraries

Al-powered remediation Common OSS

metadata

Volunteer Fire Dept.

Business models for sustained OSS security

Al-powered audits

Resources

www.alpha-omega.dev

go.xwind.io/3fs

go.xwind.io/eclipsecasestudy

go.xwind.io/ao-lessons-2025

