Alpha-Omega

2023 Annual Report

Contents

Executive Summary 3

What is Alpha-Omega? 4

Sponsors and Supporters 5

Engagement Partners 5

Highlights from 2023 6

How We Work 7

Drivers of Success 7

A four-pronged strategy 8

Leadership Team 9

2023 Year In Review 11

2023 Goals 11

Perspectives of Progress 13

Grants 14

Mentorship Program 14

Omega Toolchain 15

Content and Outreach 15

2024 and Beyond 16

2024 Goals 16

Mission and Scope of the Alpha-Omega Directed Fund 16

Getting Involved 17

Executive Summary

Alpha-Omega issued over $2.8M in grants towards open source security in 2023. These grants had a significant impact on open source security. Our grants helped staff security teams within the Python Software Foundation, the Eclipse Foundation, the Rust Foundation, and OpenJS, representing some of the most used open source languages, ecosystems, and projects.

Alpha-Omega grants are made possible by generous and significant donations from Amazon Web Services, Google, and Microsoft. With these grants, the recipients have addressed longstanding security problems, improved processes, and hardened their infrastructure. Most importantly, they have all established a sustainable culture of security within their communities. Alpha-Omega also directly funded security audits, bug fixes, and development work in critical projects like jQuery, Rustls, Homebrew, and more.

The combination of Alpha-Omega's grants and the energy, leadership, and commitment of the recipients is a formula that worked and we will continue applying it in 2024.

What is Alpha-Omega?

Alpha-Omega's mission is to catalyze sustainable security improvements to the most critical open source software projects and ecosystems.

Alpha-Omega identifies parts of the open source ecosystem where funding security work could have broad and exceptionally high impact. To date, our investments here have been largely focused on improving the security of core platforms and programming languages, as well as foundations that represent a significant number of critical projects.

The Alpha-Omega Project values experimentation. We'll make investments, learn what works and what doesn't, and refine our approach over time. We welcome community input on the methodologies used to select projects and the types of activities that will have the greatest impact.

Sponsors and Supporters

We would like to thank the following organizations for sponsoring and supporting the Alpha-Omega project. With their assistance, improving the security of open source software has been made possible.

Engagement Partners

We'd also like to thank our partner organizations associated with our Alpha engagements; these organizations maintain software used by millions of developers and billions of end-users.

Highlights from 2023

In 2023, Alpha-Omega provided 10 grants to 8 organizations totaling almost 3 million dollars. The average grant size was just over $350,000. Now in its third year, Alpha-Omega has evolved into a Directed Fund and formalized its governance structure. Now with three stakeholders (and sources of funding) the governance model will preserve the efficient decision making that has been a hallmark of Alpha-Omega's success and make it easier to continue raising funds.

The Alpha-Omega grant recipient community achieved a significant amount in 2023. See each organization's annual update later in this report. Below are a few highlights from 2023.

Sigstore adoption continues to grow across the open source ecosystem.

Alpha-Omega funding is driving Sigstore adoption at the ecosystem level. The Python Software Foundation now signs Python and CPython releases with Sigstore with more ecosystem adoption coming soon. The Homebrew project is adding Sigstore to its core packages.

Security champions are driving tangible improvements and cultural change at open source foundations.

Alpha-Omega has helped fund security champion roles at the Python Software Foundation, the Eclipse Foundation, and the Rust Foundation. In all cases, we are seeing significant impact as these individuals are incubating a security culture in their respective communities.

> *"Security in an open community presents its own challenges as well as opportunities. That's why we are grateful for the funding from the Alpha-Omega Project that enabled us to hire Seth Larson, who is both a security expert and a well-loved member of the Python community, to drive this work."*
>
> **— Deb Nicholson, ED, Python Software Foundation**

Alpha-Omega grants are now being followed by direct institutional budgets and fundraising for security staffing and projects.

A core principle of Alpha-Omega is that we are a catalyst for change. At the foundation level this means making security budgets first-class citizens and diversifying funding sources. We've seen great progress in this area with investments from the Sovereign Tech Fund and the Open Tech Fund. Also, both the Rust Foundation and the Eclipse Foundation have included security in their annual budget process. The Eclipse Foundation is creating a Cybersecurity Risk Initiative Working Group.

How We Work

Drivers of Success

Toward achieving the vision of Alpha-Omega, we fund work around critical open source projects that, if funds were available, could make rapid progress toward improving their security posture. Both sides of this are important; we want to direct our limited resources to have the most impact on society, and we want to see that impact demonstrated quickly.

There is no shortage of critical projects, and we aren't convinced there's a way to quantifiably measure the criticality of projects below a certain level of granularity. Is Node.js more or less critical to the open source ecosystem than Python? Is GCC more or less critical than React? While it's an interesting area of research, we don't think it's an important question for us to try to answer; those projects are all critical, and we should consider funding each of them. That said, we are informed by the work of the Securing Critical Projects working group to ensure we remain informed by and focused on the set of critical projects.

From there, we look for points of leverage and projects that are reasonably well understood and ready to start work. This has led us to investments in both ecosystems like Rust and foundations like the Eclipse Foundation, where improvements affect a disproportionate number of end-users. In general, these organizations already have relationships with security talent and the ability to hire and manage their work. This approach allowed us to do more with fewer resources within the Alpha-Omega project.

Our hands-off but tell us-about-it approach is working well. We are at our most effective when we focus on being a catalyst for change in organizations that have the maturity to efficiently take on important security work. We learn the most when the organizations we work with are able to bring their learnings and lessons back to us and to the broader community. We will continue to actively curate these conversations.

A four-pronged strategy

Building on the past two years of grants and lessons learned, we have identified four categories of grants.

This updated categorization of investments has become an important framework for our thinking and grant making process. It allows us to better plan for the longer term and to be clear on our expectations of impact.

A STAFFING SECURITY AT OPEN SOURCE

B SECURING OPEN SOURCE ARTIFACT REPOSITORIES

C SECURITY AUDITS & REMEDIATION

D EXPERIMENTATION

Staffing Security at Open Source Organizations

One of the most impactful ways to change the security culture of an entire community is to make it someone's job. This has been a recurring theme with our grants and has already produced significant impact. This is hardly surprising. Open source communities are about people and having a trusted member of the community leading the way makes a difference.

Securing Open Source Artifact Repositories

Artifact Repositories such as those provided by package managers like PyPi or NPM, are the app stores of software development. As such they are critical points of trust for every developer workflow. However they can also become targets for malicious actors. Their central role means that attacks can have scaled impact. Helping artifact repositories become more secure continues to be an area of leveraged impact for Alpha-Omega.

Security Audits & Remediation

Security Audits are the bread and butter of open source security. Many Alpha-Omega engagements have started with an audit and the subsequent remediation work. Not only do security audits find and reduce risk, they are cost-effective catalysts for organizational changes to make security a cultural norm.

Experimentation

Alpha-Omega was founded with a spirit of experimentation. Much of the book of open source security is still to be written and there are important and hard problems yet to be solved. We are particularly interested in innovations and solutions that will scale to the huge bodies of open source that we cannot address directly.

Leadership Team

The Alpha-Omega project is managed by a core leadership team, including:

Michael Scovetta, Microsoft

Michael Scovetta leads a security team at Microsoft, focused on understanding and addressing emerging security threats related to open source software and the ecosystem around it. He and his team do this by building security tools, advising engineering teams, and evangelizing good practices. Within OpenSSF, Michael co-leads the Alpha-Omega project and co-leads the Metrics & Metadata working group. Michael brings around 25 years of software engineering and security experience and earned a Master of Engineering in Computer Science from Cornell University and Bachelor of Science from Hofstra University.

Bob Callaway, Google

Bob Callaway is the technical lead and manager of the supply chain integrity group in Google's Open Source Security Team. He and his team directly contribute to critical secure supply chain projects and drive communication & adoption of best practices throughout the open source ecosystem. Bob is a member of the Technical Advisory Council for sigstore, a Linux Foundation / OpenSSF set of projects focused on improving transparency and UX of software supply chains. Before joining Google in 2021, Bob was a member of Red Hat's Office of the CTO where he was responsible for emerging technology strategy with strategic partners (including IBM) and a principal architect at NetApp where he focused on contributions to OpenStack and storage automation projects. He holds a PhD in Computer Engineering from NC State University where he also serves as an adjunct assistant professor in the ECE department.

Henri Yandell, Amazon Web Services

Henri specializes in large scale organization of Open Source. Starting as a committer with Jakarta and Apache Commons projects in 2001, he has served on Apache Software Foundation legal and security committees, and as a board member. From 2007 he has led Open Source at Amazon, tackling licensing, upstreaming, company projects, and now the growing field of open source security.

Michael Winser, XWind.io

Michael is a 40 year veteran in the software industry, with over 25 of those years at Google and Microsoft. He co-founded Alpha-Omega while at Google. Michael is an industry expert in software supply chain security, software development, and developer ecosystems. In addition to Alpha-Omega, Michael works with corporations and open source organizations to develop and execute on their security strategy. Michael is also a Security Strategy Ambassador for the Eclipse Foundation.

The impact of the experience in open source, software development, and security that these people bring is significantly enhanced by the strategic reach of their parent organizations and personal networks.

Alpha-Omega would grind to halt without the insights, wisdom, and ongoing support of Michelle Martineau and Naomi Washington from the Linux Foundation.

We would also like to acknowledge the many contributions and continued support of the following individuals. Their support and passion for open source security has been unwavering.

> Aaron Leung (AWS), Anna Veeramachaneni (Citi), Bennett Purcell (OpenSSF), Chris “Crob” Robinson (Intel), David Nalley (AWS), Eric Brewer (Google), Harry Toor (OpenSSF), Jonathan Leitschuh (Alpha-Omega), Jonathan Meadows (Citi), Mark Russinovich (Microsoft), Omkhar Arasaratnam (OpenSSF), and Yesenia Yser (Alpha-Omega).

Decisions are made collaboratively. To date, all significant decisions have been unanimous among the core leadership team.

2023 Year In Review

2023 Goals

Last year we identified four goals for 2023 in our 2022 annual report. Here's a look back at what worked best, what lessons we learned, and how we're moving forward.

Making security a first-class citizen in major projects' and foundations' budgets

Impact Significant. We've seen meaningful cultural changes and prioritization around security in every organization and several have started developing sustainable funding for security.

Lessons learned Even just a single person whose job is about security can have a transformative effect on an entire organization. As we expected, the path to self-sustaining security budgets will take years.

Going forward We're taking a multi-year view when planning for staffing focused grants. Losing the people who have driven such impact would have lasting negative effects.

Demonstrating measurable impact through security improvements to the projects we focus on

Impact Significant. Thanks to the great work by our grant recipients, and their excellent reporting, we've seen significant impact on every project.

Lessons learned Organizations matter. Good things happen when we trust mature organizations with smart people to solve hard problems. Shovel-ready projects (including staffing) are key. Impact measurement is still largely anecdotal and that's OK for now. Metrics are hard.

Going forward We are now highlighting the success factors to future grant recipients and using them in our grant review process.

Accelerating Omega

Impact

Mixed. While we had some success in funding “long tail” analysis through OpenRefactory, we re-evaluated our decision to resource an engineering team to build tools and triage vulnerabilities at scale.

Lessons learned

The long tail is a hard problem with both technical and human challenges. We are not a software engineering organization.

Going forward

Going forward: We will continue to look for and invest in experiments to keep learning about and incubating innovation in scalable solutions to vulnerability discovery and remediation.

Expanding Alpha-Omega into additional verticals

Impact

Incomplete. Supply chain security was a consistent theme at the Open Source Finance Forum but we have yet to make any grants focused on a specific vertical.

Lessons learned

There is interest but it’s going to take a concerted effort to get this started. In particular we were not sufficiently connected to key players in verticals to champion any efforts.

Going forward

We look to partnering with organizations in a given vertical (we are likely to continue conversations with the financial sector) to develop a more specific plan.

Perspectives of Progress

"This year has been defined by transformation, as we've laid a rock-solid foundation for enhancing the Software Supply Chain Security posture of our projects and have expanded our capacity. It marks the beginning of a journey toward realizing our vision and setting a benchmark in the implementation of Open Source Supply Chain Security best practices. We extend our gratitude to the Alpha-Omega project for their continuous support throughout this journey."

– MIKAEL BARBERO, HEAD OF SECURITY, ECLIPSE FOUNDATION

"OSTIF is grateful for the funding to effectively execute security audits of critical open source projects. We build on over 9 years of experience working with open source communities and security specialists, and are proud to have published reports for more than 50 security audits. We hope to collaborate on more projects with Project Alpha in 2024."

– AMIR MONTAZERY, MANAGING DIRECTOR, OPEN SOURCE TECHNOLOGY IMPROVEMENT FUND, INC.

"Thanks to Alpha-Omega's generous support, the Rust Foundation was able to demonstrate that a dedicated investment in security can deliver impactful results in a short period of time when coupled with a comprehensive ecosystem strategy. In 2024, the Rust Foundation Security Initiative will have a second year of funding from Alpha-Omega. This will allow us to build on our foundational work in this space and help ensure that the Rust programming language is safe, secure, and sustainable for everyone."

– REBECCA RUMBUL, EXECUTIVE DIRECTOR & CEO OF THE RUST FOUNDATION

View Grantee Outcomes By Investment

"Lack of memory safety is a crippling problem across widely-used software and we're committed to changing that through ISRG's Prossimo. With funding from OpenSSF's Alpha-Omega project, we're advancing memory safety in the Rustls TLS library and in the Linux kernel. "

– SARAH GRAN, VP, BRAND & DONOR DEVELOPMENT, PROSSIMO

"Securing an entire open source software ecosystem, especially one as diverse and vibrant as Python, requires a consistent investment of time, expertise, and empathy. We are grateful for Alpha-Omega's support in our journey towards a more secure and sustainable Python for everyone."

– SETH LARSON, SECURITY DEVELOPER-IN-RESIDENCE

"Software security is critical and many security vulnerabilities are present in the broadly used open source libraries. Thanks to support from the Alpha-Omega project, OpenRefactory is 'scrubbing' the libraries to detect issues and offer corrections to the maintainers."

– DR. MUNAWAR HAFIZ, FOUNDER AND CEO, OPENREFACTORY, INC.

"Through our work with Alpha-Omega, we've been able to create new processes and protocols to ensure Node.js is secure. Just this year we've released the permission model, significantly reduced response time for security reports and have increased the number of security releases."

– RAFAEL GONZAGA, NODE.JS TECHNICAL STEERING COMMITTEE (TSC) MEMBER

Grants

In 2023, Alpha-Omega provided 10 grants to 8 organizations, totaling $2,841,968 with an average grant size of $355,246, a 38% increase over 2022.

This brings the total grants by Alpha-Omega to $4.9 million.

Alpha Engagement	Date	Amount
Eclipse	January, May, December 2023	$600,000
NodeJS	January 2023	$279,000
Rust	October 2023	$460,000
Homebrew	September 2023	$175,000
OpenSSL	August 2023	$127,968
OpenRefactory	July 2023	$50,000
Prossimo (ISRG)	August 2023	$530,000
Linux Kernel	December 2023	$620,000
	Total	**$2,841,968**

Mentorship Program

The Alpha-Omega Summer 2024 Mentorship Program connected senior software security engineers with newcomers to open source, software development, and security research. Entry-level contributors had the opportunity to help accelerate Alpha-Omega's mission under the guidance of experienced mentors.

To encourage Diversity, Equity, and Inclusion (DEI) and to provide guidance to those entering the cybersecurity field, the Alpha-Omega mentors, Jonathan Leitschuh and Yesenia Yser, introduced the idea of the mentorship program. The goal was to have the mentees work on the Omega toolchain and enhance the vulnerability process and usage of Open Rewrite and CodeQL.

Read about the mentorship program through the mentor and mentee perspectives.

Omega Toolchain

In October 2023, we decided to stop working on the Omega Toolchain project. The project's mission was to build the tools and processes for conducting automated campaigns that discover, triage, and remediate security findings to significantly reduce the presence of security vulnerabilities, at scale, from the open source software ecosystem. The team did excellent work and we learned a lot. We decided that the short and medium term ROI of this work did not match the other important work that Alpha-Omega is doing. The overall mission of Alpha-Omega hasn't changed, nor has our desire to fix the most critical projects and ecosystem while also scaling solutions for "the rest" of the open source community. Of course, all of the source code for the Omega Toolchain is open source and is available for anyone to use.

Content and Outreach

Alpha-Omega and our diverse pool of grant recipients have yielded a variety of content. From thought-provoking blog posts to impactful press releases to educational open source security presentations, our grants have empowered individuals to deliver meaningful contributions. The following examples showcase some of the work produced, illustrating the positive outcomes and diverse range of content.

- How bulk pull requests help scale open source bug fixes
- Alpha-Omega Summer Mentorship 2023 – An In-Depth Look from a Mentor's Perspective
- Experiences from the Alpha-Omega Mentorship Program Mentees
- Advancing Rustls and Rust for Linux with OpenSSF Support
- OpenJS Foundation Warns Consumer Privacy and Security at Risk in Three-Quarters of a Billion Websites
- Alpha-Omega Grant To Help Homebrew Reach SLSA Build Level 2
- Alpha-Omega to Continue Support of Rust Foundation Security Initiative in 2024
- Adding build provenance to Homebrew

2024 and Beyond

As we enter the third year of Alpha-Omega, we've learned what worked for us and what we can improve on. Here are some of our goals for next year.

2024 Goals

Sustain and support the multi-year staffing efforts we started. The impact and insights coming from these projects is invaluable. We're going to keep stoking the fires on the teams we've started and champion sustained funding.

Collect and share insights across our grant recipients. If there's one common theme across all of our engagements it's that we are all learning and we can all benefit from each other's experience. For 2024 we're making this an explicit goal. We have some ideas about how and we'll experiment.

Continue to explore the long tail. Our own organization is not the place for software R&D but we are still very keen to see progress in this area. We'll look to fund small experiments that build on our past work and which will help us shape a longer term plan.

Develop partnerships with industry vertical associations. We remain interested in understanding how industry verticals can engage with open source security. What are the critical projects, how are they being funded and resourced? We have a lot to learn.

Settle in for the long haul. Alpha-Omega has made it into its third year. It's clear that there are years of work ahead. In 2024 we'll continue to develop our longer-term strategy for funding, grants, and partnerships.

Mission and Scope of the Alpha-Omega Directed Fund

Alpha-Omega has established a Directed Fund and formalized our governance model this year enabling independent decision making and reliable revenue cycles from recurring membership. Additionally, this has allowed Alpha-Omega to have a focused mission and strategy in 2024 and beyond.

The purpose of the Alpha-Omega Project Directed Fund is to raise budget and spend funds with a mission to protect society by catalyzing sustainable security improvements to the most critical open source software projects and ecosystems. The project aims to build a world where critical open source projects are secure and where security vulnerabilities are found and fixed quickly. The Directed Fund will be composed of Premier and General Members, for additional information on joining the mission of Alpha-Omega please visit: alpha-omega.dev

Getting Involved

The Alpha-Omega team welcomes active community participation through a few different vehicles. We hold public meetings once a month and maintain a public Slack channel within the OpenSSF Slack workspace. We provide regular updates to the OpenSSF Technical Advisory Council (TAC) and maintain close relationships with other OpenSSF working groups and projects.

In addition, we're interested in collaborating with individuals and organizations that share our vision and can help us achieve our mission. Specifically, we're interested in these key areas:

- **Funding:** If you represent an organization able to provide funding to the Alpha-Omega project, please contact us.
- **Commercial Tooling:** If you represent a security tool or vendor that can perform leading-edge security analysis of open source projects, please contact us.
- **Critical Projects:** If you represent a critical open source project, believe you have an actionable security-related project, please contact us.
- **Ecosystems, Package managers, and infrastructure:** If you represent a developer ecosystem, package manager, or shared infrastructure for open source developers and you have shovel-ready ideas for security improvements, we'd love to hear from you. Please contact us.