Alpha-Omega

2024 Annual Report

Contents

Executive Summary

Open source software isn't just another piece of technology—it's the digital bedrock that supports everything from major government operations to the smartphone apps we use every day. Its strength lies in the global network of passionate, too-often-unpaid volunteers who pour their time and expertise into writing and maintaining open source projects. Yet, as we rely on these individuals to secure vital infrastructure, we must acknowledge the immense responsibility they carry and ensure we're not merely shifting more unpaid work onto their shoulders. By investing in resources, offering support, and creating pathways for sustainable contribution, we can protect and strengthen open source software without placing undue burdens on the very people who make it possible.

To everyone who created, maintained, or contributed to an open source project in 2024, thank you.

In 2024, Alpha-Omega issued nearly $4.5 million in grants to improve security in key open source projects. Notably we:

- Helped staff security teams at ten of the most important open source organizations, including the Python Software Foundation, OpenJS, RubyGems, and the Rust Foundation.
- Provided grants to harden critical infrastructure, including the Linux Kernel and Homebrew.
- Paid for security audits of foundational technologies, including OpenSSL.
- Experimented with scaled approaches to finding and fixing vulnerabilities and supported Rust implementations of TLS and the AV1 codec.
- Hosted four roundtable discussions with grant recipients to cross-pollinate expertise and to shape strategies for 2025.

Alpha-Omega is funded by generous and significant donations from Amazon Web Services (AWS), Google, and Microsoft. These grants made it possible to address longstanding security challenges, improve processes, and harden infrastructure within many of the world's most important open source projects and ecosystems. More importantly, we've been able to establish a sustainable culture of security within the communities we work with.

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 2025.

What is Alpha-Omega?

Alpha-Omega is an associated project of the OpenSSF, established in February 2022, funded by Microsoft, Google, and Amazon, and 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.

Alpha-Omega looks for opportunities to fund work that will have broad and high impact. We seek to incubate and catalyze durable change in the projects and organizations we work with. Historically, our investments have targeted ecosystems, core platforms, package managers, programming languages, and foundations that have the organizational intent and ability to improve security for many projects. This often takes the form of staffing security roles that can lead and improve the security culture for entire organizations. Sometimes this starts with a simple audit. We also invest in tooling and solutions that can scale to more than one project by finding or solving entire classes of vulnerabilities across many projects. This epitomizes the range of Alpha-Omega: from highly leveraged organizational and cultural changes to technologies that scale to thousands of projects.

The Alpha-Omega Project values experimentation. While the best way to address security risk within the open source community isn't always clear-cut, 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.

Impact from 2024 Grants

Airflow

The "Airflow Beach Cleaning" project explores an innovative approach of dealing with Open Source Software Supply Chain problems. Building on existing foundations of tools and processes that aim to improve individual projects security posture, processes tooling, Airflow Beach Cleaning project aims to introduce a human factor and harness community interactions between maintainers of the open-source projects that depend on each other in order to raise awareness, contribute to and funnel time, energy, focus and possibly money down the Open-source chain of project dependencies.

The goal of the project is to effectively fund and fuel overall improvements in the security of the whole open-source supply chain of important parts of the ecosystem - starting from the substantial Apache Airflow Python supply chain (more than 700 dependencies) but with the aim of turning it into an industry-wide practice that funding companies and open-source maintainers will be able to adapt and follow in a sustainable way.

The project is on-going - with conversations started with the initial batch of dependencies of Airflow - with already valuable initial feedback and work planned on improving security after getting positive feedback from the maintainers. The early results of this work identified 16 dependency projects to be prioritized for direct engagement from the Airflow committer community. These engagements have already produced new insights and direct improvements (e.g. support for Trusted Publishing) in collaboration with the project maintainers.

Rust

In 2024, the Rust Foundation continued to receive generous funding from OpenSSF's Alpha-Omega project to support our Security Initiative. This helped the Rust Foundation's Security Initiative to strengthen the Rust ecosystem's security infrastructure in 2024.

Security Engineer Walter Pearce and Software Engineer Adam Harvey focused on supply chain security, vulnerability detection, and developing tools to protect the open-source community from potential threats.

Highlights in 2024 include:

- Publishing the TUF RFC, which proposes the adoption and implementation of The Update Framework (TUF) for providing the chain and trust and implementing signatures for crates and releases.
- Further developing Painter, an open source tool for building dependency graph databases.
- Conducting comprehensive provenance tracking for the top 5,000 crates.

Eclipse Foundation

Our goal is to establish the Eclipse Foundation as the leading open source community in demonstrating security best practices. With the support of Alpha-Omega, the Eclipse Foundation Security Team provides the Eclipse Foundation (EF) community with a secure environment for open source software collaboration and innovation. They empower individuals and organisations collaborating on Eclipse Foundation projects to understand, control, safeguard against, and respond to cyber threats.

In 2024 the team established consistent and effective vulnerability management across the over 400 projects at the EF. They presented at VulnCon and continue to speak worldwide about our approach to vulnerability management at scale. In 2024, all vulnerabilities were resolved before disclosure, ensuring that security researchers received timely and efficient communication when reporting new vulnerabilities. Additionally, the team implemented policy measurement and enforcement across 81% of EF repositories on both GitHub and GitLab, leading to the full adoption of MFA for all EF repositories. Over 40% of EF infrastructure has been migrated to the newly integrated IAM, Keycloak, paving the way for MFA on these applications in 2025. Furthermore, Sigstore was added to the existing code-signing infrastructure, making it available to all EF projects.

Leveraging the security posture established by the EF Security Team, the Eclipse Foundation has cemented its credibility as a key stakeholder for institutions and agencies from a cybersecurity perspective. This enabled EF to maintain a leading role in 2024, ensuring that open source communities remain visible to policy-makers, particularly within the European Commission, regarding the Cyber Resilience Act. In April 2024, the Eclipse Foundation spearheaded the creation of the Open Regulatory Compliance Working Group. This collaborative effort will partner with governmental bodies to enable the industry to meet regulatory

requirements while continuing to leverage open source through the software supply chain. Additionally, this initiative will empower open source projects to better address the industry's needs in this rapidly evolving landscape.

FreeBSD

The FreeBSD Project has taken significant steps to enhance its security posture with the support of a $137,500 grant from Alpha Omega, administered by the FreeBSD Foundation. This funding has been pivotal in launching two critical initiatives in June 2024: a comprehensive Code Audit of the bhyve hypervisor and Capsicum sandbox and an ongoing Process Audit of development procedures. These efforts aim to address vulnerabilities, improve security practices, and ensure the long-term resilience of FreeBSD, a key component of global digital infrastructure.

The Code Audit, conducted by security firm Synacktiv, identified critical vulnerabilities in the bhyve hypervisor, including exploits which could allow attackers to escalate privileges from guest virtual machines to host systems. Capsicum's protections were deemed robust, though one critical kernel issue and minor vulnerabilities in optional services were uncovered. The FreeBSD Project's Security Team promptly worked to remediate these vulnerabilities, issuing Security Advisories and using the audit findings to develop strategies for reducing similar vulnerabilities in the future.

The Process Audit, expected to conclude by the end of 2024, is focused on enhancing FreeBSD's development procedures to minimize future security risks. These initiatives reflect the FreeBSD Foundation's commitment to proactive security measures, which includes publicizing audit findings and leveraging them to bolster security practices.

Jenkins

In October 2024, the Alpha Omega Foundation provided a 3-month grant to the Jenkins project to improve the implementation of Content Security Policy (CSP) across the Jenkins ecosystem. The goal is to enhance the security of Jenkins by shielding it from injection attacks like cross-site scripting (XSS).

The project is being led by technical lead Basil Crow, and developers Yaroslav Afenkin and Shlomo Dahan. Over the past two months, the team has made significant progress towards this objective. This work will continue in early 2025.

Linux Kernel

C compilers have been adding a lot of features to them to make common problems be flagged and prevented, but when working with an old legacy codebase like Linux, enabling them can cause lots of churn due to hundreds of false positives and reworks needed. OpenSSF has helped fund work that has allowed Linux to enable many of these new options, such as turning off variable-length-arrays which are tricky to get right. As proof of this, when doing the work, many major bugs were found and fixed that had not been noticed in the past due to memory overwrites happening silently. Another option now enabled is the cast-function-type which is now enabled to ensure that when pointers to functions are passed around by the kernel, they are always of the correct type. Work was also done to help automatically detect string overflows by refactoring code to work properly with the what the compiler expects to be able to track this automatically. Due to this work, new compiler features were developed for the major C compilers to help support strict flexible arrays and to have the compiler automatically track the expected length of fields in a structure, providing these security features to all users of C.

Along with working to enable new security features with the compiler, support to ensure that Linux continues to work properly with the LLVM compiler suite was funded by OpenSSF. New versions of the compiler are tested against the kernel codebase, and required fixes for the kernel are implemented and bugs are reported to the compiler developers as needed. As full support for LLVM is needed for Rust support in Linux, this constant work is essential for the future of the kernel to ensure that the Rust integration works properly over the long-term.

OpenJS

In 2024, the Node.js project made major strides in security, highlighted by proactive measures funded by the Alpha-Omega Project. The engagement resulted in security releases (dealing with 34 reports reported in May) across all active Node.js lines including a collaboration via MITRE with other languages and runtimes. Supported by the OpenJS Foundation and Alpha-Omega's investment in a dedicated full-time security engineer, Node.js was able to move from a reactive to a proactive security stance, reducing response times and increasing release frequency.

Key updates this year included automation improvements that streamline the security release process, including a new command, "git node security,"

which consolidates several manual tasks. The Node.js Permission Model has been actively developed, adding support to Buffers and adjusting the API for better usage for Node.js developers. The Node.js Security Team is constantly improving security across the whole ecosystem. A new policy integrity feature is being developed with Microsoft's collaboration, and a tool to identify vulnerabilities in the Node.js binary (is-my-node-vulnerable) has been released.

The Node.js community also focused on testing enhancements, refining experimental features with the Next 10 Working Group, and increasing contributor engagement through events and a new mentoring channel. Together, these measures reflect a strong commitment to security through both technological improvements and active community involvement.

OpenRefactory

In 2024, Alpha-Omega issued two grants to OpenRefactory. They had different goals. During the first half of the year, the goal was to perform open source security audits at scale. During the second half of the year, the goal was to collaborate with the maintainers of three open source projects (Apache Airflow, Jenkins, Kubernetes), perform in depth analysis of all the supply chain dependencies of the latest release of these projects, provide a unique risk signal about previously undetected vulnerabilities and deliver actionable advice on how to manage the risk. Over the course of 2024, over 9000 packages were analyzed and 30 high severity security and reliability bugs (out of 75 total) were reported. The OpenRefactory team's collaboration with Apache Airflow leadership had a notable impact on improving maintainer response to reported bugs.

OSTIF

Alpha-Omega's partnership with the Open Source Technology Improvement Fund (OSTIF) in 2024 resulted in impactful security improvements in the open source ecosystem. Alpha-Omega sponsored two security engagements which provided tailored security work from independent experts, offered long-term hardening recommendations, and included a new or updated testing suite for the projects. OSTIF audits not only provide immediate feedback and guidance for maintainers, but focus on ways to support project security moving forward. Looking to the future, these projects can confidently move forward knowing that through the efforts of OSTIF and the support of Alpha-Omega, their projects positively reflect the hard work of the project maintainers and security experts to provide secure open source software.

Prossimo

The goal of Internet Security Research Group (ISRG)'s Prossimo project is to bring memory safety to the most critical software infrastructure on the Internet. The shift to memory safe code will eliminate vulnerabilities that lead to security breaches and data leaks that cause personal and financial harm to Internet users, result in the mass denial of essential public services, and threaten basic human rights and safety. Thanks to Alpha-Omega's generous support, in 2024 ISRG improved Internet security by making progress toward three Prossimo initiatives: Rustls, Rust for Linux, and rav1d. Work on Rustls, an open source and memory safe TLS library, centered on improving its performance and functionality to make it competitive with the leading TLS library, OpenSSL, which is not memory safe and thus vulnerable to bugs. Because billions of phones, computers, servers, IoT devices, and embedded systems rely on TLS to securely communicate over networks, providing a memory safe alternative to OpenSSL is critical to increasing Internet security.

Support for the memory safe Rust programming language being merged into the open source Linux kernel in late 2022 was an incredible milestone toward increased security for the Internet and all that depends on Linux. In 2024, we worked with the primary maintainer of Rust for Linux, Miguel Ojeda, to continue to improve the support for Rust in the Linux kernel so that the first major Rust production users can be merged upstream.

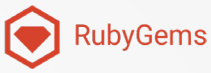
We also undertook work toward building a memory safe AV1 decoder called rav1d, which can be used for both video and images. Complex data parsing is one of the most security-critical operations in modern software and is a particularly big issue for video decoders, with AV1 set to become one of the most important media formats on the Internet. Because of this, it's important that there be a highly performant memory safe AV1 decoder available.

Python Software Foundation

Alpha-Omega's support has enabled the Python Software Foundation to staff our Security Developer-in-Residence Seth Larson full-time in 2024. Seth was able to build the infrastructure for automating CVE record updates and tracking CPython dependencies to generate and publish authoritative accurate Software Bill-of-Materials documents. Seth also secured CPython releases by auditing the entire process, hardening the build pipeline, and fixing issues with Sigstore verification materials. Thanks to this work

Python users can be confident in the security and integrity of their Python application runtime and its dependencies.

From authoring guides and blog posts to speaking at conferences and podcasts, Seth's continued public collaboration across the Python and security communities has catalyzed improvements beyond just the Python ecosystem. Using guides that Seth authored, the Linux kernel became a CVE Numbering Authority and Nuget and Crates.io created proposals to adopt Trusted Publishers.



RubyGems

With Alpha-Omega's support, Ruby Central was able to take on two significant projects in 2024, an external security audit of RubyGems.org and adding Organization Accounts to RubyGems.org. External Security Audit Ruby Central partnered with Trail of Bits for a comprehensive security audit on the RubyGems.org Rails application and its underlying AWS infrastructure. The audit identified 33 issues, including seven medium-severity items and one high-severity item. Notably, most of these findings do not constitute actual security breaches. Our team started addressing each finding as they were reported and used these insights to bolster RubyGems's security posture.

Trail of Bits

Alpha-Omega's funding has enabled Trail of Bits to make **significant security and sustainability improvements** to both Homebrew and the Python Packaging Ecosystem. Through the last 12 months of funding, we have:

- Implemented Sigstore-based attestations and provenance generation for the Homebrew package manager, making Homebrew the **first major packaging ecosystem with pervasive (100%) attestation coverage** for all packages in the official index.
- Implemented a user-side verification flow for all Homebrew attestations, one that requires **no key or identity management.**
- Implemented key **UX, API, and CLI improvements** to the Python reference implementation of Sigstore, enabling both downstream applications (PEP 740 index attestations for PyPI) and serving as reference material for the Ruby and Go Sigstore clients.

Click here to view full Grantee Reports.

Staff Learnings

Getting to watch the Securing Open Source community developing before our eyes has been a highlight. Both our Seattle and Vienna face-to-face roundtables saw different groups of folk that we fund sharing new concepts and concerns with each other, and brainstorming the future. These conversations directly informed our funding ambitions for 2025.

If Alpha represents leverage, Omega is about scale. We have learned a lot as we tried to apply automation to find and fix vulnerabilities across the hundreds of thousands of projects. Our early efforts were akin to sending boats out to the Pacific Garbage Patch. A lot of work was done but the overall impact was diffuse. In 2024 we tried a different approach: just clean one beach at a time. Starting with Apache Airflow we had a specific area of impact and focused on the longer term security posture of all 719 projects in Airflow's dependency graph rather than vulnerabilities. Where we saw the most traction was when Airflow maintainers established a person-to-person connection with their dependencies. Surprise! Humans matter in open source.

In 2024, the OpenSSF Alpha-Omega project has been a catalyst for transformative change. It was inspiring to see dedicated, passionate individuals being empowered *and compensated* to make a broad impact within open source communities. Their willingness to share and cross-pollinate ideas didn't just enhance their own projects—it paid dividends in elevating the entire ecosystem. Essentially, we were able to set the ball in motion and watch it gain momentum, growing and accelerating as it rolled downhill.

While the lack of funding for open-source software (OSS) projects is often lamented, an even more critical gap lies in the scarcity of dedicated time for addressing security concerns. Funding is essential, not just for the projects themselves, but to enable focused efforts on security. This includes resources for personnel, comprehensive audits, development of advanced tooling, and widespread adoption of security best practices. By strategically investing in these areas, Alpha-Omega is empowering several OSS communities to prioritize and tackle systemic security issues, ultimately fortifying the entire OSS ecosystem for the benefit of all.

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 "shovel readiness". 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 years of grants and lessons learned, we have identified four categories of grant funding:

This categorization of investments continues to be 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.

Security Staffing

One of the most impactful ways to change the security culture of a community is to make it someone's job, but it's even more important to have it be the *right* person. We've seen this play out multiple times since our founding, but this is hardly surprising. Open source communities are about people and having a trusted member of the community leading the way can make all a difference.

Another key insight we had is that the set of open source communities is itself a community—bringing security leads together regularly for roundtable discussions have led to shared solutions—a great example of this is the work on Trusted Publishing that is spreading across package managers and being adopted by projects. Another example is the discussion on end-of-life and crisis management for smaller projects. The Alpha-Omega team routinely discusses ideas with our community members and our work has benefited from the feedback received.

Artifact Repositories

Artifact repositories such as those provided by package managers like PyPI or Homebrew, are the "App Stores" of modern software development, and critical points of trust in every developer's workflow. From the XZ Utils attack in March 2023 to regular reports of malware published to npm, we know these central repositories can be juicy targets for malicious actors. But their central role also means Alpha-Omega can have scaled impact—where a security investment can improve security for every package and every user of the ecosystem.

A great example of this is the work we funded with Homebrew to bring build provenance and code signing to practically all projects available through the ecosystem.

Audits & Remediation

Security audits are the "bread and butter" of open source security, and many of our engagements started with an audit and subsequent remediation work. Not only do these audits identify and

address security flaws, we've found them to be a cost-effective catalyst for organizational changes to make security a lasting cultural norm.

In addition to these traditional audits, we also regularly fund "lightweight", narrowly-scoped audits targeting a large number of projects, such as Apache Airflow's "beach cleaning" work with OpenRefactory or the 10,000 PyPI projects scanned.

Innovation & Experimentation

Alpha-Omega was founded with and retains a spirit of experimentation, and while we're smarter than we were when we started, there's still a great deal of learning to do. There are truly difficult problems to be solved, and we recognize the benefits of experimentation and innovation, particularly when used to either catalyze change, horizontal, or vertical.

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 leads Microsoft's open source security team, focused on understanding and addressing emerging software supply chain security threats. They do this by building security tools, advising engineering teams, and evangelizing good practices. Within OpenSSF, Michael co-leads the Alpha-Omega project and. 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 leader of Google's Open Source Security Team (GOSST), spearheading initiatives to bolster the security of open source software, benefiting both Google and the global community. Under his leadership, the GOSST team develops and contributes to projects that address critical areas such as supply chain integrity, observability, and vulnerability management. GOSST also plays a pivotal role in managing essential internet infrastructure services, including OSV, Sigstore, and Certificate Transparency logs. Bob's influence extends to advisory positions in key organizations: he serves as a member of the Technical Advisory Council for the OpenSSF, is a co-founder and technical steering committee member of Sigstore, and represents Google on the Alpha-Omega project leadership team. His extensive experience includes engineering and leadership roles at

Red Hat, NetApp, and IBM. Bob holds a PhD in Computer Engineering from NC State University, where he also shares his expertise 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.

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

Alpha-Omega would grind to halt without the insights, wisdom, and ongoing support of Michelle Martineau and Tracey Li 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.

Mila Zhou (AWS)
Chris “Crob” Robinson (OpenSSF)
Yesenia Yser (Microsoft)
David Nalley (AWS)
Eric Brewer (Google)
Mark Russinovich (Microsoft)

2024 Year In Review

2024 Goals

Catalyze trustworthy and secure software, runtimes, and infrastructure for all the major open source ecosystems through staffing

Impact

Alpha-Omega funded security staffing at PSF, RubyCentral, Eclipse Foundation, Rust Foundation, OpenJS Foundation (by way of Node), Rust-for-Linux, and the Linux Kernel Project. This was an expansion from 2023. We also funded critical improvements to and audits of projects such as RubyGems, PyPI, Python, the Linux Kernel, LLVM, Apache Airflow, and PHP Packagist. All of these efforts resulted in follow-up work done by the project communities.

Lessons learned

- We continue to see that making it someone's job to worry about security and having the right person in that job has the biggest and more durable ROI on security in open source ecosystems.
- The path to self-funded security staffing is a long one but we are seeing how the work we fund has drawn follow-up engagement from the adjacent communities and organizations.

Going forward

We will continue these staffing engagements in 2025. They are effective, leveraged, collaborative, and changing security culture and priorities within their organizations.

The top 10,000 open source projects are free of critical security vulnerabilities

Impact

We scanned over 9,000 projects for the most common vulnerabilities. Just over 70 vulnerabilities and bugs were reported. Although we had hoped to drive adoption of best practices at scale, we did not get this done. We received clear feedback that the long-tail of maintainers would be reluctant to take on "even more work."

Lessons learned

- Open source projects are remarkably secure. Most of the problems come from out-of-date dependencies. Automation is improving but this remains a human-scale problem and many maintainers of the long-tail projects are already working nights and weekends. Adding money isn't a quick fix.
- There are no small dependencies. Every dependency, no matter how large or small, creates build-time and runtime risk for projects that include it.

Going forward

This is an area of active development. We will continue to run experiments. In particular we are interested in public datasets to improve tooling and how AI-based solutions might become practical for small project maintainers.

Enhance Alpha-Omega's effectiveness in driving security improvements through deliberate innovation and experimentation

Impact

In 2024 we funded several new projects and experiments.

- Continued to support Rust for Linux and a port of the AV1 media codecs to Rust
- Several dependency graph focused audits and scans where we looked at the total risk of a project rather just its own code and processes
- Our first audits of popular open source AI libraries and toolkits.
- A project to implement CSP for Jenkins to systematically prevent cross-site scripting attacks via Jenkins Plugins
- Improve PyPI's project-level "lifecycle" functionality, including implementing and improving key features related to PyPI's project deletion, project uploading, and project "status" handling.

Lessons learned

- The AI space is moving very fast and established frameworks for the safe and secure use of AI libraries are not well understood.
- Small, tactical investments in security-related feature development feel right even as it will take time for these projects to yield fruit.

Going forward

- We will continue to fund small to medium project development work and experiments.

Run an operationally efficient and effective program

Impact

Our overheads are very low. With minimal staff and travel expenses, over 91% of the donations from our sponsors go to our grant recipients. The selection of these projects, the support they receive, and the community engagement we create all contribute to successful outcomes for these grants.

Lessons learned

In short, Alpha-Omega is working well.

Going forward

We will continue with the approach we've taken thus far. It's working.

What our community had to say

"Without a doubt Alpha-Omega is dramatically improving the security of the entire open source ecosystem. The tech industry relies on open source to innovate and operate cost effectively. These investments by Alpha-Omega are going to pay dividends for years to come."

– MIKE MILINKOVICH, EXECUTIVE DIRECTOR, ECLIPSE FOUNDATION

"Alpha-Omega have shown clear demonstrable progress in securing open-source ecosystems and critical packages, leveraging the funding made available. Essentially turning money into security in a clearly demonstrable way. The work performed to secure Apache AirFlow for example, significantly improved the security posture of a critical open-source component. Whilst general open sourcing funding will continue to engage the community, it is clear that Alpha-Omega has the ability to move the needle on security to the benefit of all open-source users including Citi."

– JONATHAN MEADOWS, MANAGING DIRECTOR AND TECH FELLOW, CITI

"The Kernel Security Engineers funded by Alpha-Omega are doing amazing work making Linux more secure every month with their constant improvements."

– GREG KROAH-HARTMAN, LINUX KERNEL MAINTAINER

"Maintaining secure open source projects pressures developers at the OpenJS Foundation. An IDC survey funded by Alpha-Omega revealed over 750 million outdated websites, with many collecting sensitive information, and 33% of respondents faced security incidents in the past 24 months. jQuery, used by 90% of websites, struggled with low visibility and fragility. Alpha-Omega funded its modernization, risk research, and a web upgrade campaign. Similarly, two-thirds of Node.js users rely on outdated versions. Legacy software and limited security expertise among contributors amplify risks, where Alpha-Omega provides crucial support."

– ROBIN BENDER GINN, EXECUTIVE DIRECTOR, OPENJS FOUNDATION

"Not only does Alpha-Omega fund the effort, it also creates the platform of exchanging ideas and brainstorming that has proven to be the most important input to the project. What we learned already allowed us to talk about it at Airflow Summit and Community over Code where we involve and enthuse maintainers of the open source projects to approach their supply chain in a similar way."

– JAREK POTIUK, APACHE AIRFLOW PMC AND SECURITY LEAD

"Alpha-Omega serves as a powerful example for the entire industry, showcasing how sustainable investment in open-source security can drive significant impact. We look forward to seeing more private and public stakeholders join forces in our collective effort to strengthen the ecosystem."

– MIRKO SWILLUS, HEAD OF SOVEREIGN TECH FUND

"The Node.js project shows that direct technical assistance is key to open source security. Despite being a healthy, community-led project, Node.js maintainers are overwhelmed by demands from companies that rely on it but contribute little. Many community-led JavaScript projects lack the time, expertise, and resources to address security vulnerabilities on tight timelines. Through Alpha-Omega grants, funding developers for security has proven impactful. In 2021, Node.js lacked a Security Working Group; today, it's robust, doubling security releases and reducing churn, thanks to A-O funding for engineers driving policies, automation, and community growth."

– MATTEO COLLINA, NODE.JS TECHNICAL STEERING COMMITTEE MEMBER, OPENJS BOARD DIRECTOR, CO-FOUNDER & CTO PLATFORMATIC

"In just a few years, we've gone from the dream of memory safety in the Linux kernel to a growing portfolio of Rust-based drivers in development. This is great progress; we've seen activity increase and the community grow. But just as the Linux kernel itself has required ongoing strategic leadership, Rust for Linux needs active maintainership to achieve its greatest impact. The role filled by Miguel Ojeda has a wide set of responsibilities from cultivating the community, to providing important technical contributions, to the thankless "janitorial" work that needs to be done to keep a project organized and moving forward. This work is critical today and will continue to be so for some time."

– JOSH AAS, EXECUTIVE DIRECTOR AND CO-FOUNDER OF ISRG AND PROSSIMO

"The importance of financial support to fund core security work in the Rust ecosystem cannot be overstated. Before funding was secured to support security work in Rust, the three part-time volunteers were limited to reactive support. Alpha-Omega enabled us to hire full-time Security Engineer and Software Engineer roles. Together they have worked on threat models, tooling and security infrastructure. This has significantly reduced security burdens for Rust maintainers and made it easier for contributors to participate in a secure and scalable manner. Having dedicated and experienced Security Engineers on staff enables the Rust Foundation to keep investing in forward-looking and proactive security hygiene, to onboard and mentor newcomers to the space, and to develop sustainable and stable security processes for the wider community."

– REBECCA RUMBUL, EXECUTIVE DIRECTOR AND CEO, RUST FOUNDATION

"The Alpha-Omega team is leveling up open source security, and the FreeBSD Foundation is proud to contribute to this vital work. The insights shared in the FreeBSD Audit report not only serve as a springboard for stronger security within the FreeBSD Project but also highlight how Alpha-Omega is driving real progress across the entire open-source ecosystem."

– ED MASTE, FREEBSD FOUNDATION SENIOR DIRECTOR OF TECHNOLOGY

Grants

Alpha-Omega provided 20 grants to 15 distinct organizations driving security improvements in 2024. The average grant size was $227,445. Work funded by Alpha-Omega in 2024 was supported by a total of $4,548,900 in grants. Historically, these data points have been calculated by tallying the funds distributed in a calendar year. However, beginning in 2024, Alpha-Omega decided to adjust those calculations to reflect the year in which the grant funds are utilized. This adjustment will allow Alpha-Omega's reporting to more accurately reflect the calendar year in which funds are being utilized for security improvement initiatives.

Total grants issued by Alpha-Omega since its inception is nearly $8.6 million

A

SECURITY STAFFING

63%
OF 2024 GRANTS

$2,860,000

B

PACKAGING REPOSITORIES

15%
OF 2024 GRANTS

$662,400

C

AUDITS & REMEDIATION

14%
OF 2024 GRANTS

$626,500

D

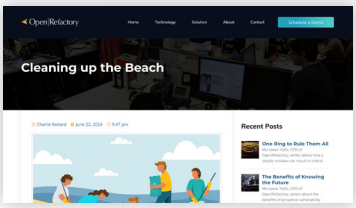
INNOVATION & EXPERIMENTATION

9%
OF 2024 GRANTS

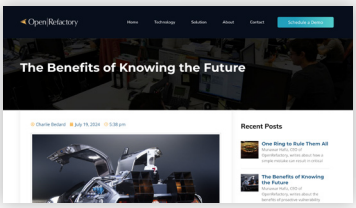
$400,000

Content & Outreach

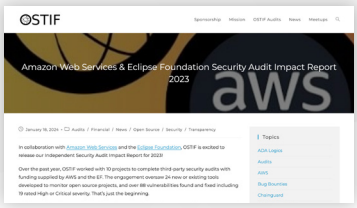
Alpha-Omega and our diverse pool of grant recipients have yielded a variety of content. From thought-provoking blog posts to impactful press releases to educational open source security presentations, our grants have empowered individuals to deliver meaningful contributions. The following examples showcase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



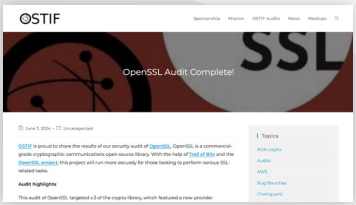
CLEANING UP THE BEACH



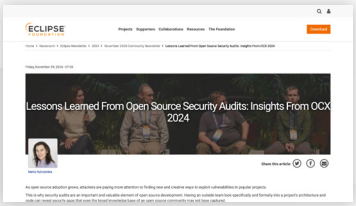
THE BENEFITS OF KNOWING THE FUTURE



AMAZON WEB SERVICES & ECLIPSE FOUNDATION SECURITY AUDIT IMPACT REPORT 2023



OPENSSL AUDIT COMPLETE!



LESSONS LEARNED FROM OPEN SOURCE SECURITY AUDITS: INSIGHTS FROM OCX 2024

STRENGTHENING FREEBSD: ADDRESSING VULNERABILITIES THROUGH SYNACKTIV'S CODE AUDIT

FREEBSD FOUNDATION RELEASES BHYVE AND CAPSICUM SECURITY AUDIT FUNDED BY ALPHA-OMEGA PROJECT

MAJOR SECURITY AUDIT OF CRITICAL FREEBSD COMPONENTS NOW AVAILABLE

2025 and Beyond

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

Alpha Omega OKRs 2025

Our objectives are largely unchanged. At one of our roundtable meetings there was consensus that we and our grant recipients can all do more marketing of the impact we are creating. This isn't just to create buzz but to make it easier to sustain and grow the funding that makes Alpha-Omega possible.

O1: Catalyze trustworthy and secure software, runtimes, and infrastructure for all the major open source ecosystems through staffing

KR 1.1	Fund security improvements and initiatives for at least ten critical open source organizations by the end of 2025.
KR 1.2	For each engagement, confirm progress toward improved security outcomes, evidenced through initial and/or follow-on assessments, monthly reporting, and periodic check-ins.
KR 1.3	Drive the organizations we work with to obtain security funding from at least one organization other than Alpha-Omega, targeting 33% by the end of 2025.
KR 1.4	Organize quarterly roundtables for at least 5 major ecosystems to share information, build connections, and collaborate, resulting in at least one new project or joint publication started in 2025.
KR 1.5	Scaling adoption, consumption, value of OSS Security projects, Getting to sustainability tipping points.

O2: The top 10,000 open source projects are free of critical security vulnerabilities

KR 2.1	Create and collect open data sets of security-related data for open source projects to make the development of scaled security tooling easier and to make the results more consistent.
KR 2.2	Expand the "beach cleaning" approach to at least 3 new projects and develop tooling and playbooks to make it easier and cheaper to do for any project.
KR 2.3	Create an open source "Corps of Engineers" group of security expert engineers who can work within and across their communities to provide security guidance to smaller projects in times of crisis.

O3: Enhance Alpha-Omega's effectiveness in innovation experimentation and marketing

KR 3.1	By the end of 2025, run three experiments to explore new strategies for reducing security risk within the open source ecosystems, share the results/ learnings, using them to refine our overall strategy and objectives for 2025.
KR 3.2	More active internal marketing to stakeholders targeted at specific teams through infographics and marketing assets.
KR 3.3	Continue our progress from 2024 on auditing and improving the security of the top open source AI libraries by developing guidance for organizations that use them to do so securely.

O4: Run an operationally efficient, growing, and effective program

KR 4.1	Allocate at least 85% of our yearly spend to activities directly in support of our mission.
KR 4.2	Receive at least $5 million in renewed funding in 2025.
KR 4.3	For each partner engagement, at least 70% of the objectives defined within the respective agreement are met within the defined time period.
KR 4.4	Develop and deliver quarterly reports. Increase engagement/interest across stakeholders, grant recipients, and other target orgs.
KR 4.5	Jointly fund 3-5 engagements in partnership with other organizations (e.g. Sovereign Tech Agency).

Getting Involved

The Alpha-Omega team welcomes active community participation. We hold public meetings once a month and maintain a public Slack channel. We publish monthly updates on our website and collect detailed updates from our engagement partners in our GitHub repository. We provide regular updates to the OpenSSF Technical Advisory Council (TAC) and maintain close relationships with OpenSSF working groups and projects.

We're also 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.
- **Security 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.
- **Join us on LinkedIn:** https://linkedin.com/showcase/alpha-omega-oss