Alpha-Omega

QUARTERLY REPORT
Q1 2025

Q1 2025

SUMMARY

Q1 has been a highly productive period, marked by several key initiatives that have laid the foundation for future success. Notably, the formation of The Security Corps of Engineers stands as a significant milestone in enhancing our security capabilities. Additionally, our first Roundtable event proved to be an invaluable platform for collaboration and idea exchange.

The SOSS Policy Day further strengthened our commitment to policy development and advocacy, while our strategic planning efforts for 2025 grant funding set the stage for continued growth and impactful projects in the years ahead. These initiatives reflect our ongoing dedication to innovation and progress.

.

Where we are TODAY

NEW MEMBERS

We're excited to welcome Citi as a general member of Alpha Omega! Their expertise and commitment to security will help drive innovation in open-source security, strengthening our collective efforts to tackle digital challenges.

NEW ENGAGEMENTS

In Q1, Alpha-Omega reaffirmed its dedication to supporting its longstanding grantees with additional funding, while also expanding its Grantee pool by welcoming new organizations and projects. Some of the newcomers include Apache Software Foundation and Byte Whisperer.

EXISTING ENGAGEMENTS

Our existing engagements provide monthly updates to us through our public GitHub repository:

- Apache Software Foundation
- Eclipse Foundation
- Kernel
- OpenJS
- Ruby Central
- Rust Foundation
- Python Software Foundation
- Prossimo
- PyCA (Trail of Bits)
- Byte Whisperer

A FEW NOTABLE WORK UPDATES FROM GRANTEES

Eclipse

The deployment of blueprints across over 240 GitHub organizations managed by Otterdog has streamlined repository creation and ensured consistent security policy, including the automatic addition of SECURITY.md files. While the process generated numerous PRs without significant opposition, some maintainers voiced concerns about high notification volumes. Blueprints are additive and customizable, creating PRs for repository compliance, and can be dismissed if closed without merging.

Otterdog now supports custom GitHub teams for more complex workflows and integrates with the OpenSSF Scorecard API to track repository security. Additionally, the Eclipse Forums were replaced with a static, read-only copy for security reasons.

Eclipse Cont.

The team is enhancing mini-reviews to engage projects, and the release of Otterdog version 1.0 supports adoption and compliance with SLSA Build Level 3. Furthermore, progress on ID validation led to selecting iDenfy for government-issued ID verification, and vulnerabilities were addressed with several published CVEs. Lastly, the team welcomed Kairo de Araujo and is working on filling an open position following the departure of Thomas Neidhart.

OpenJS

In Q1 of 2025 the Node.js project achieved significant progress in areas of security, automation, community engagement, and release management. Key updates included the publication of the first Node.js Maintainers Threat Model and improvements to transparency around access control and security risks.

Automation efforts advanced with the introduction of GitHub Actions for release proposal creation and the streamlined handling of security releases, reducing manual errors and enhancing reliability.

The Node.js Permission Model reached stable status, strengthening security controls, while the is-my-node-vulnerable package was donated to the Node.js organization. The team also issued CVEs for End-of-Life versions to highlight security risks in outdated releases. Additionally, the OpenJS Security Compliance Guide was expanded, and work continued on security tools, including automating vulnerability pull request creation.

These efforts were complemented by improvements in the OpenJS CVE Numbering Authority (CNA) and new initiatives like the development of VisionBoard and FortSphere tools, further bolstering the Node.js ecosystem's security and compliance capabilities.

Python Software Foundation

Mike Fiedler, PyPI's Safety & Security Engineer, focused on enhancing security measures and responding to malware incidents. He handled numerous malware reports, issuing advisories and developing an effective Project Quarantine feature to contain threats. He also worked on automating malware detection and quarantine processes to improve PyPI's response time, explored typo-squatting prevention strategies, and contributed to improving the PyPI Admin UI.

Additionally, Mike enhanced PyPI's security by improving Fastly NGWAF rules and attended discussions on the Cyber Resilience Act. Mike actively engaged with the community through conferences and talks, sharing his experiences and encouraging involvement in open-source security. His ongoing efforts include refining security protocols, contributing to PEP 770 for Software Bill-of-Materials, and collaborating on various maintenance tasks and code reviews.

Prossimo

The Rust for Linux project, aimed at integrating the memory-safe Rust language into the Linux kernel to enhance security and reliability, made significant strides in February 2025. This included publishing the Rust kernel policy to clarify key issues and unblock progress in the kernel community, as well as a keynote presentation at FOSDEM by Miguel Ojeda, which raised the project's visibility and attracted potential contributors.

The project also continued working on merging the first major Rust production drivers, with multiple pull requests prepared for the Linux v6.14 kernel cycle. Ongoing efforts include maintaining and improving Rust support, testing, backporting fixes, managing team activities, and building a strong Rust for Linux community. Additionally, the project focused on technical development, such as refining the build system, while maintaining relationships with stakeholders and organizing events like the Rust for Linux Kangrejos conference.

PyCA (Trail of Bits)

As of January 2025, the PyCA Cryptography Declarative ASN.1 API project began its initial design and development, focusing on Python components with a dataclasses-style public API, typing.Annotated support, and an intermediate representation for integration with Rust components. In February 2025, the team completed the design of the declarative Python API, including the dataclasses-style DSL with typechecking and annotation support, as well as the initial design for an intermediate representation for Rust internals. The team continued to develop the Rust internals, implementing MVP support for serialization and deserialization, and began designing support for non-trivial ASN.1 annotations, such as IMPLICIT and EXPLICIT markers.

Ruby Central

Samuel Giddins has been deeply involved in multiple initiatives, including refining the scope of infrastructure hardening for RubyGems.org following a security audit. He is also working on sigstore-ruby updates, including improved spec compliance and JRuby support. He recently contributed a blog post about handling malicious packages, which was received positively by the community.

Samuel also collaborated on policy development for RubyGems.org, focusing on data usage, gem namespaces, and future governance capabilities. He is driving the adoption of sigstore across popular gems by working directly with maintainers and proposing a "wheels" system for RubyGems to improve gem installation efficiency and security. He has been analyzing ecosystem data, including gem download statistics and public database dumps, while also contributing to broader security and release efforts, such as reproducibility in Ruby release tarballs. Additionally, he gave talks and workshops on Ruby supply chain security and gem development practices.

Meanwhile, Marty Haught focused on compliance work, refining privacy policies and data mapping, as well as advancing the Organizations feature and infrastructure security, including planning for access control improvements. Both have worked on a roadmap for RubyGems.org's future, engaging sponsors and strategizing fundraising.

Rust Foundation

The Rust engineering team is making significant progress with various updates and improvements. Painter is set to release a major update, including customized LLVM-based analysis, cross-crate analysis, improved behavioral analysis, and multi-path resolution for multi-version/feature crates.

Crate scanning infrastructure has been enhanced with new tools, like the mapstic crates for Elasticsearch mappings. On crates.io, Tobias addressed frontend dependency issues by migrating to a well-maintained alternative.

CI efficiency has also seen a 66% reduction in costs due to optimizations. In the community, the Rust Safety Critical Consortium continues its work, with Tobias joining the Axum project as a maintainer.

Additionally, new Rust project goals for verification, mirroring, and CapsLock investigation are underway. At Rust Nation 2025, Adam and Marco presented on crate security and automation tools, respectively. The Rust team is also fostering stronger C++/Rust interoperability and advancing the Ferrocene Language Specification project.

AO HEADLINES

Blogs

- Dealing with (Hypothetical) Sham Packages- Ruby Central
- Package typosquatting detection in {Rust,Dust,Trust,Rut}

PR

- The Apache Software Foundation Announces New Fundraising Program to Support Mission Critical Initiatives for Open Source Projects

Reports

- Alpha Omega Annual Report 2024

OKR UPDATES

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 2024.	
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 2024.	
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: Drive adoption of key security processes, including static analysis, credential scanning, the use of private vulnerability disclosures, structured metadata (Security Insights) and the use of multi-factor authentication by maintainers of 500 critical projects from the top 10,000 by the end of 2024.	
KR 2.2: Independently scan, triage, and notify maintainers when critical vulnerabilities are found in 2,000 projects, chosen from the top 10,000 by the end of June 2024, with emphasis on clearing a "section of the beach" by focusing on the top PyPI packages.	
KR 2.3: Publish in a machine readable format the attestations for all packages from 2.2 that returned no vulnerabilities and those that found vulnerabilities which were subsequently fixed and verified.	
KR 2.4: Open Source Data	
KR 2.5: Towards beach cleaning tooling and playbooks	
KR 2.6: OS Corps of Engineers	
O3: Enhance Alpha-Omega's effectiveness in innovation experimentation and marketing	
KR 3.1: By the end of 2024, run three experiments to explore new strategies for reducing security risk within the open source ecosystems, share the	

OKR UPDATES

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.	
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 2024.	
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: Funding Partnerships 3-5 Partnerships (STF or OTF) and Corporations	

COMING UP NEXT MONTH

Our next Quarterly update will be in August. Our next Alpha-Omega public meeting will take place in person at Open Source Summit North America in Denver, Colorado on Tuesday, June 24th. If you have not received an invite or would like to attend please reach out to info@alpha-omega.dev,

If you have any questions about this update or any of our work, please contact the Alpha-Omega team at info@alpha-omega.dev, reach out to one of us directly, or come say 'hi' on the #alpha_omega channel in the OpenSSF slack.

Bob Callaway, Google
Henri Yandell, AWS
Michael Scovetta, Microsoft
Michael Winser, Technical Strategist, Alpha-Omega