Alpha-Omega

QUARTERLY REPORT
Q2 2025

Where we are

TODAY

Q2 2025

SUMMARY

Alpha-Omega continues to build strong momentum, with major progress across ecosystems and the launch of impactful new initiatives. We hosted a well-attended in-person Roundtable at Open Source Summit North America in Denver, which sparked rich conversations across the community, alongside a dedicated in-person meeting of the Security Corps of Engineers that same day. We partnered with the Sovereign Tech Agency to organize a Maintain-a-Thon at the United Nations Open Source Week, and our ongoing collaborations with partners like the Python Software Foundation, Rust Foundation, Apache, Eclipse, and Ruby Central continue to deliver meaningful results—from deploying trusted publishing and SBOM support to advancing malware detection, reproducible builds, and new models for security governance. With broad collaboration, technical innovation, and a growing emphasis on sustainability, the open source ecosystem is taking confident, coordinated steps toward a more secure and resilient future.

NEW ENGAGEMENTS

We're excited to announce a new engagement with the Open Source Technology Improvement Fund (OSTIF), focused on a comprehensive security and quality evaluation of the widely-used Python libraries Paramiko and Cryptography. Paramiko is a pure-Python SSHv2 implementation that underpins tools like Fabric, while Cryptography is a critical Python/Rust library providing cryptographic primitives to over 25,000 projects. This engagement will assess Paramiko's codebase, CI/CD pipeline, dependency usage, and resistance to known SSH attacks, along with a focused review of Cryptography's integration with rust-openssl to ensure secure and correct usage. While the core cryptographic libraries (OpenSSL, rust-openssl, pynacl, bcrypt) are not the primary focus, their invocation by Paramiko and Cryptography will be scrutinized. The review is also expected to identify areas for potential improvements in testing, security posture, and long-term project resilience, contributing to the broader open-source software supply chain hardening efforts.

EXISTING ENGAGEMENTS

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

- Apache Software Foundation
- Eclipse Foundation
- Linux Kernel
- OpenJS /Node.js
- Ruby Central
- Rust Foundation
- Python Software Foundation
- ISRG / Prossimo
- PyCA
- Bytewhisper Security
- OSTIF

A FEW NOTABLE WORK UPDATES FROM GRANTEES

Apache Software Foundation

The Apache Trusted Release (ATR) platform made steady progress this quarter, with development focused on aligning the new release pipeline with Apache's Release Policy. An internal "alpha" test is underway with six PMCs (Airflow, Commons, Logging, Maven, Pekko, and Tomcat), emphasizing implementation of policy gates and receiving positive early feedback.

Ongoing efforts include refining tooling to help communities self-identify their projects and products, improving public release metadata formats and locations, and planning an upgrade from Nexus v2 to Nexus v3 to better enable modern workflows and expanded distribution options. Additionally, collaboration with the ASF Board is underway to enhance tooling to better support project and release lifecycle management. A public beta is targeted for later this year.

Rust Foundation

Major strides were made across Rust's security initiatives over the past quarter, particularly around Trusted Publishing and The Update Framework (TUF). With our support, crates.io is close to fully enabling Trusted Publishing, following an RFC co-authored with Trail of Bits. Backend architecture, GitHub integration, and user-facing tools are nearly complete, and a new effort to surface vulnerabilities using the RustSec Advisory Database on crates.io is underway. TUF progressed with three repository implementations, early client tooling, and scalability analysis—ultimately favoring Merkle tree-based models. Work on Capslock has begun, with a plan to emit Rust call graphs in a language-agnostic format, supported by refactoring the Painter tool into a standalone library.

Additional milestones include migrating Rust repositories to Infrastructure as Code, exploring Terraform Cloud for secure deployment, and officially bringing the Ferrocene Language Specification under Rust Project governance. RustWeek capped off the quarter with key discussions on security, safety-critical systems, and Rust/C++ interoperability, alongside participation at Open Source Summit and OpenSSF Day.

Python Software Foundation

Security efforts in the Python ecosystem made strong progress in Q2, led by Security Developer-in-Residence Seth Larson and PyPI Safety & Security Engineer Mike Fiedler. Seth drove key improvements in SBOM support, including the acceptance of PEP 770 and supporting tooling for wheel and vendor metadata. He also coordinated multiple security advisories, supported policy efforts like the European Union's Cyber Resilience Act, and represented the project at major events including PyCon US, OpenSSF Community Day, Open Source Summit, and the UN's Open Source Week.

Mike focused on malware response and platform hardening, processing hundreds of reports, improving PyPI's quarantine system, removing over 13,000 invalid accounts, and implementing protections against domain expiration attacks—advancing PyPI toward OpenSSF's Authentication: Level 2 goal. Both Seth and Mike engaged actively in community events and standards discussions, furthering trusted publishing, threat modeling, and supply chain security across Python's packaging ecosystem.

Ruby Central

In Q2, Samuel Giddins and Marty Haught made significant progress enhancing the Ruby ecosystem's security and infrastructure. Samuel focused on advancing support for prebuilt binaries (wheels) in RubyGems and Bundler by refactoring platform matching logic and prototyping compatibility with Python's platform tags. He also led discussions on binary transparency at Open Source Summit, aiming to establish a cross-registry logging system. Additionally, Samuel contributed to the phased wind-down of the CocoaPods repository in collaboration with OpenSSF and engaged Ruby core teams on build reproducibility and native extension topics.

Marty finalized and launched the updated RubyGems.org policies, clarifying deletion rules and starting work on lifecycle and ownership policies. He completed the Organizations beta, successfully onboarding Amazon Web Services as the first user, and launched the Ruby security working group forum to foster community collaboration. Marty also strengthened international community ties through his keynote at Baltic Ruby and follow-up events in the UK, which highlighted opportunities for sustainable funding and education about Ruby Central's role.

Meanwhile, Colby drafted the Stage 1 Single Sign-On migration plan for RubyGems.org, which is currently under review with security advisors, with next steps focused on finalizing the plan and preparing for user migration.
Together, these efforts reflect a strong push toward improving ecosystem security, governance, and long-term sustainability across the Ruby community.

Q2 AO BLOGS

Alpha Omega Presents | OpenJS Security Update: March–April 2025
CRustabilities: Capabilities, Rust and Capslock
Strengthening Rust Security with Alpha-Omega: A Progress Update
Making PyPI's test suite 81% faster
The Open Source AI Security Series: Prompt Injection | Divan Jekels of Bytewhisper Security
Sneak peek: A new ASN.1 API for Python | William Woodruff, Trail of Bits
Raising the Security Bar: Eclipse Foundation Rapid Security Reviews Launching in 2025
REPORT: An Overview of Cyber Security Funding for Open Source Software

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

OKR UPDATES

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 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 published in October 2025. Our next Alpha-Omega public meeting will take place on August 6, 2025 (all are welcome), and our next quarterly meeting will take place on Thursday November 6th. 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