Alpha-Omega

MONTHLY REPORT NOVEMBER 2024

February 2024

SUMMARY

This month the Alpha Omega team met in person at the Linux Foundation's Member summit in Napa. The team met to reflect on 2024's learnings and plan for 2025. Alpha Omega also had the opportunity to present to the openSSF board and collaborate on how our two foundations can accelerate open source security in the coming year.

NEW ENGAGEMENTS

In November Alpha-Omega renewed its engagements with RubyCentral, Eclipse, and Rust Foundation for 2025. We’re excited to continue these engagements as we build out our 2025 strategic plan and OKRs.

EXISTING ENGAGEMENTS

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

- Node.js
- The Eclipse Foundation
- OpenRefactory
- Linux Kernel
- Ruby Central
- Apache Airflow
- FreeBSD
- PHP (Composer, Packagist)
- Rust Foundation
- Python Software Foundation
- ISRG / Prossimo
- Support of LLVM ports to Debian
- Open Source Technology Improvement Fund
- PyPI
- Jenkins

A FEW NOTABLE WORK UPDATES FROM GRANTEES

PyPI

This month we performed a full documentation migration for all of PyPI's public APIs, feeds, datasets, etc., as scoped in #16541. All public user-facing documentation for PyPI's APIs now lives under https://docs.pypi.org/api/. We also Completed initial development of the "archived" marker feature as #17005; now in final review

Rust for Linux

This month the Linux v6.13 Rust PR was prepared and submitted, containing the work from a multitude of developers and companies, to support the first Rust users that have already landed in Linux (Asix PHY driver, AMCC QT2025 PHY driver, Null Block driver, DRM panic screen QR code generator). Other PRs targeting v6.13 are also landing through their respective subsystems (such as vfs file, vfs pid_namespace, tracepoints, netdev...): an increasing number of kernel subsystems/maintainers are getting involved with Rust. A third rust-fixes PR for v6.12 was also submitted and landed. Additionally, the resolution of a libclang/bindgen double-issue that the kernel was hitting showcased the ongoing collaboration between key distributions such as Debian and Fedora and Rust for Linux.

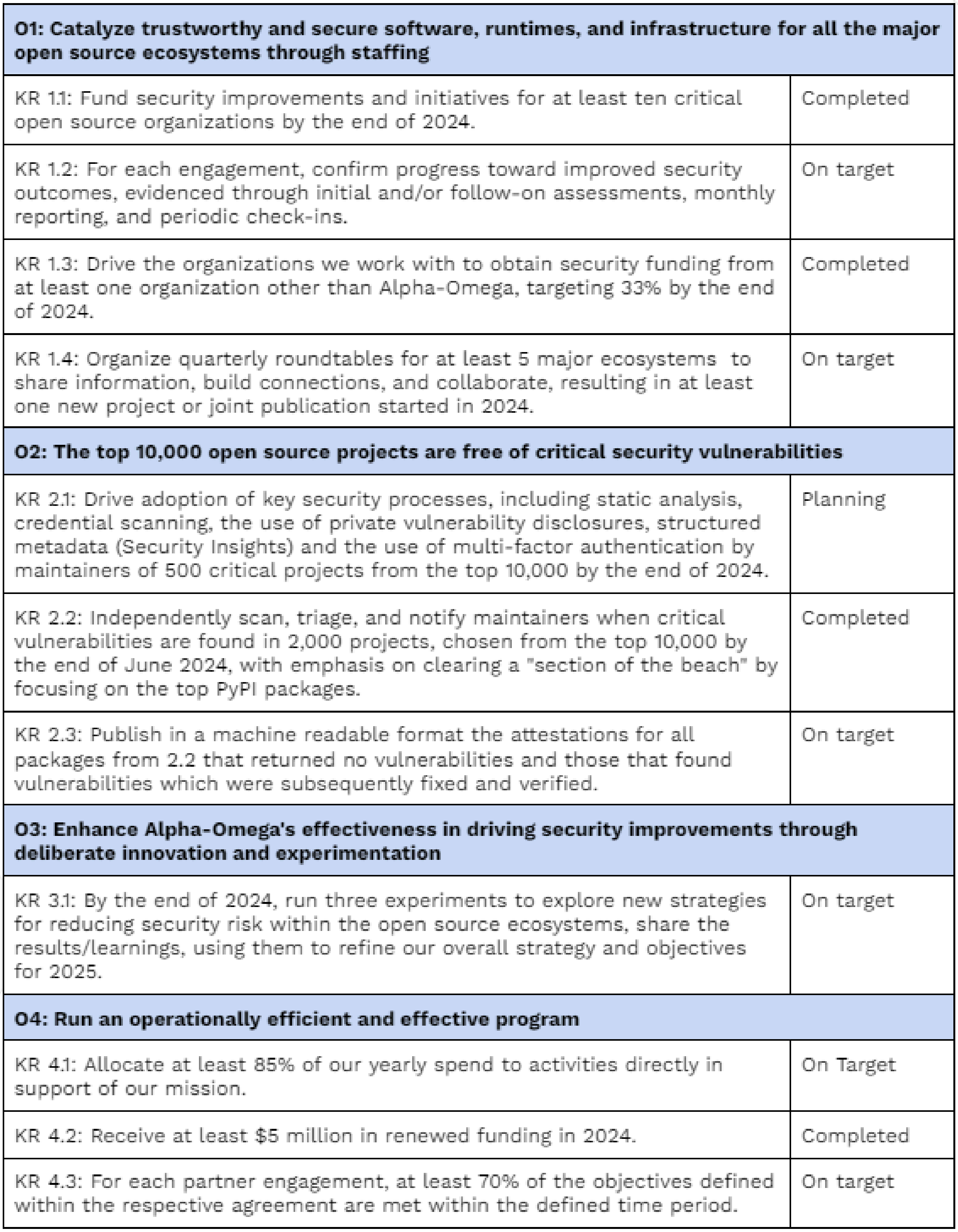
Python Software Foundation

Python packages have a "phantom dependency" problem, many packages contain non-Python software (C, C++, Rust, Go, JavaScript, etc) that can't be described using Python packaging metadata. This means that software composition analysis tools often miss this software. Python is particularly affected by this issue, but many software ecosystems have the exact same problem.

The proposal to solve this issue is providing a mechanism to describe cross-technology software within Python packaging metadata using SBOMs.
Seth has authored a draft Python Enhancement Proposal (PEP) and has circulated the draft within the Python packaging reviewers, SBOM standards communities (both SPDX and CycloneDX), SBOM users working groups. The PEP would provide a mechanism to bundle self-describing SBOM documents into Python package archives. The draft has a sponsor and reviewer: Brett Cannon.

Seth created a fork of auditwheel that implements the draft PEP and published a case study showing that by adding SBOM data to Python wheels that SCA tools are able to properly detect all bundled software within the archive.

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 2024.	Completed
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.	On target
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.	Completed
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.	On target
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.	Planning
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.	Completed
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.	On target
O3: Enhance Alpha-Omega's effectiveness in driving security improvements through deliberate innovation and experimentation	
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.	On target
O4: Run an operationally efficient and effective program	
KR 4.1: Allocate at least 85% of our yearly spend to activities directly in support of our mission.	On Target
KR 4.2: Receive at least $5 million in renewed funding in 2024.	Completed
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.	On target

COMING UP NEXT MONTH

We will be skipping our next update (for December) in favor of a more comprehensive Annual Report which will be available January 13. Our next Alpha-Omega public meeting will take place Wednesday, February 5th. Our next Roundtable will be held on December 11th. 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