OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Alpha-Omega

Webinar - Feb 16, 2022

What are we going to talk about?

Background

Mission & Vision

The Menu - *What is Alpha and Omega, really?*

How to Contribute

Questions: Please post your questions in the Q&A area

Meet the team

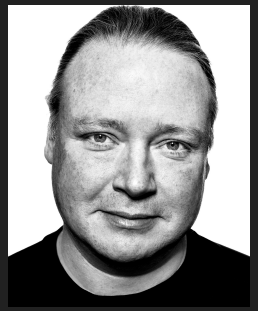
Michael Scovetta

Principal Security PM Manager
Microsoft

Leads OpenSSF's "Identifying Security Threats" working group.

20 years in software security / engineering

@scovetta
linkedin.com/in/scovetta



Brian Behlendorf

General Manager
Open Source Security Foundation

At the Linux Foundation, served as GM for Blockchain, Healthcare and Identity until October of 2021 when he shifted to lead the OpenSSF.

25 years in the open source technology domain as founder, leader, or executive team member.

@brianbehlendorf
llinkedin.com/in/brianbehlendorf

Michael Winser

Group Product Manager, Google
Google Open Source Security Team

38 years in software development

@michaelwinser
linkedin.com/in/michaelw

Background: What is Alpha-Omega?

Open source software is the foundation of practically all modern technology.

Society needs that foundation to be safe, secure, and resilient.

Alpha-Omega is one way to help improve the security of open source software.

It’s an experiment.

Background: What Isn’t Alpha-Omega?

Alpha-Omega is not some things. In particular, it is:

- Not a fund to pay open source project maintainers.
- Not a certification body or process.
- Not a replacement for normal security practices.
- Not a process for forking and taking over open source projects.
- Not a replacement for existing services.
- Not a private 0-day trading club.
- Not a fully-automated scanner that will launch “junk” vulnerabilities to maintainers.

Alpha-Omega Mission

Protect society by improving the security of open source software through direct maintainer engagement and expert analysis

Alpha-Omega Vision

Critical open source projects are secure

Vulnerabilities are found and fixed quickly

What will we do for Alpha?

Through “**Alpha**”, we will work with the maintainers of the most critical open source projects to help them identify and fix security vulnerabilities, and improve their security posture.

What is Alpha's Menu?

Appetizer: We reach out to the project, see if they're interested in learning more, talk to them about their security challenges and where we could have the most impact. If we both decide we want to move forward, we look at the main courses.

Main Course: Includes things like a source code audit, helping the maintainers set up scanning, fuzzing, branch protection, 2FA, and other "Scorecard"-centric processes; perhaps threat modeling, triaging security vulnerability reports, proposing fixes, ensuring the project can be reliably re-built, etc. This list is a bit open-ended at this point and will be refined over time.

Dessert: Retrospective on how things went (impact), how they could have gone better, and what a reasonable cadence for checking in would be.

What will we do for Omega?

Through “**Omega**”, we will identify at least 10,000 widely deployed OSS projects where we can apply automated security analysis, scoring, and remediation guidance to support their open source maintainer communities.

What is Omega's Menu?

Appetizer: Using a combination of existing tools (mostly open source), analyze 10,000 open source projects for critical security vulnerabilities.

First Course: Refine the ruleset, build a system for automating the triage as much as possible, and then use security experts to validate what we find.

Second Course: Reach out to the maintainers, report the issue, offer help fixing, closing the loop.

Dessert: Retrospective on how things are going, improving our tools and processes over time.

How to Contribute

- Get involved in OpenSSF Working Groups
  - Securing Critical Projects
    - Identifying critical open source projects (feed into Alpha & Omega)
  - Best Practices for OSS Developers
    - Building high quality “leave behind” material for maintainers when we engage
  - Vulnerability Disclosures
    - Improve the vulnerability disclosure process
- Join Alpha-Omega announcements mailing list lists.openssf.org/g/alpha-omega-announcements
- Slack channel: #alpha_omega at slack.openssf.org
- Fill out the interest form

Thank You

Alpha-Omega is one way to help improve the security of open source software.

Alpha will work directly with maintainers on the most critical projects

Omega will apply automation to analyze a wider range of critical projects

Get involved by joining OpenSSF working groups:

- Securing Critical Projects
- Best Practices for OSS Developers
- Vulnerability Disclosures

Join the mailing list for future updates

Questions?