FreeBSD Security Culture

How security audits are improving FreeBSD

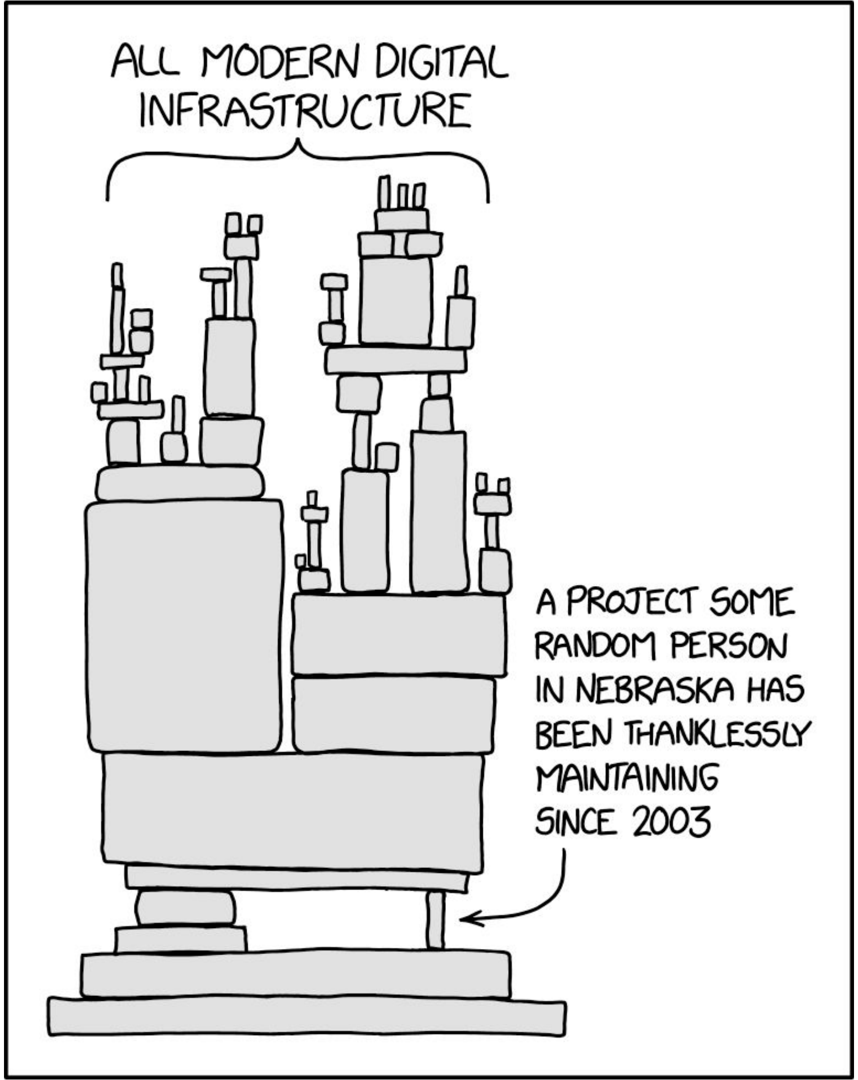
Pierre Pronchery

Security Engineer, FreeBSD Foundation

Michael Winser

Co-founder, Alpha-Omega
xwind.io

Obligatory XKCD Reference



ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

~~Open Source~~ ~~Supply Chain~~ Security Is Hard

Decades of tech debt

Sophisticated Attacks

Immature tools

Dependency webs

Lots of humans

Alpha-Omega Mission

Catalyze sustainable security improvements within the most critical open source projects and ecosystems.

Alpha-Omega Explained

α → Leverage

Ω → Scale

Alpha-Omega By the Numbers

$8.5M

Granted since 2022

30

Full Time Engineers Funded

9160

Repositories Secured

24

Security Audits

11

Security Projects Completed

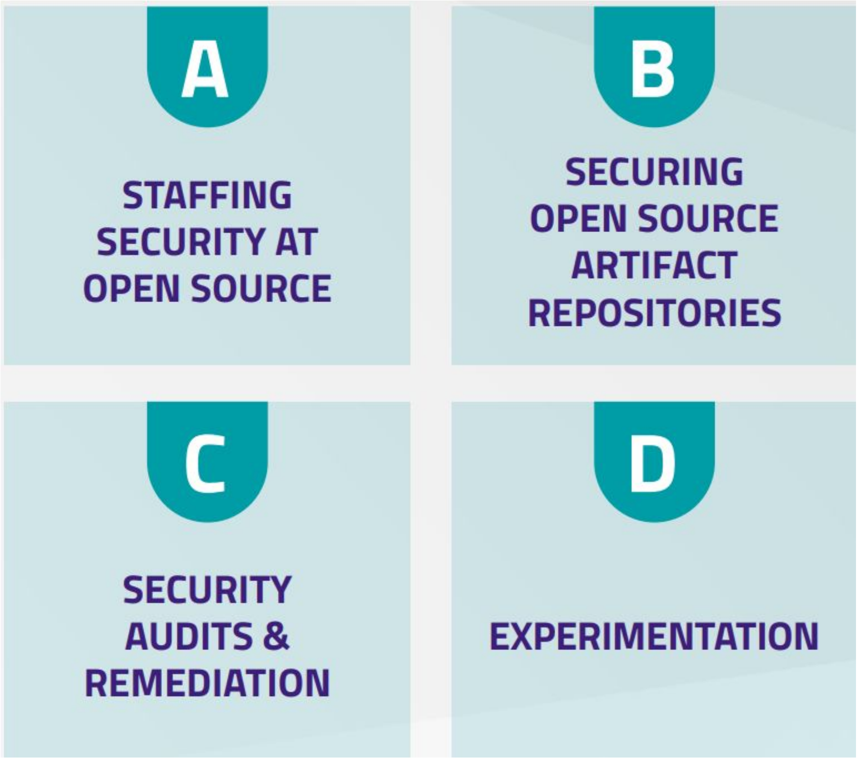
Orgs Funded

21

$4.5M

In Grants in 2024

Alpha-Omega: Our Approach



A

STAFFING SECURITY AT OPEN SOURCE

B

SECURING OPEN SOURCE ARTIFACT REPOSITORIES

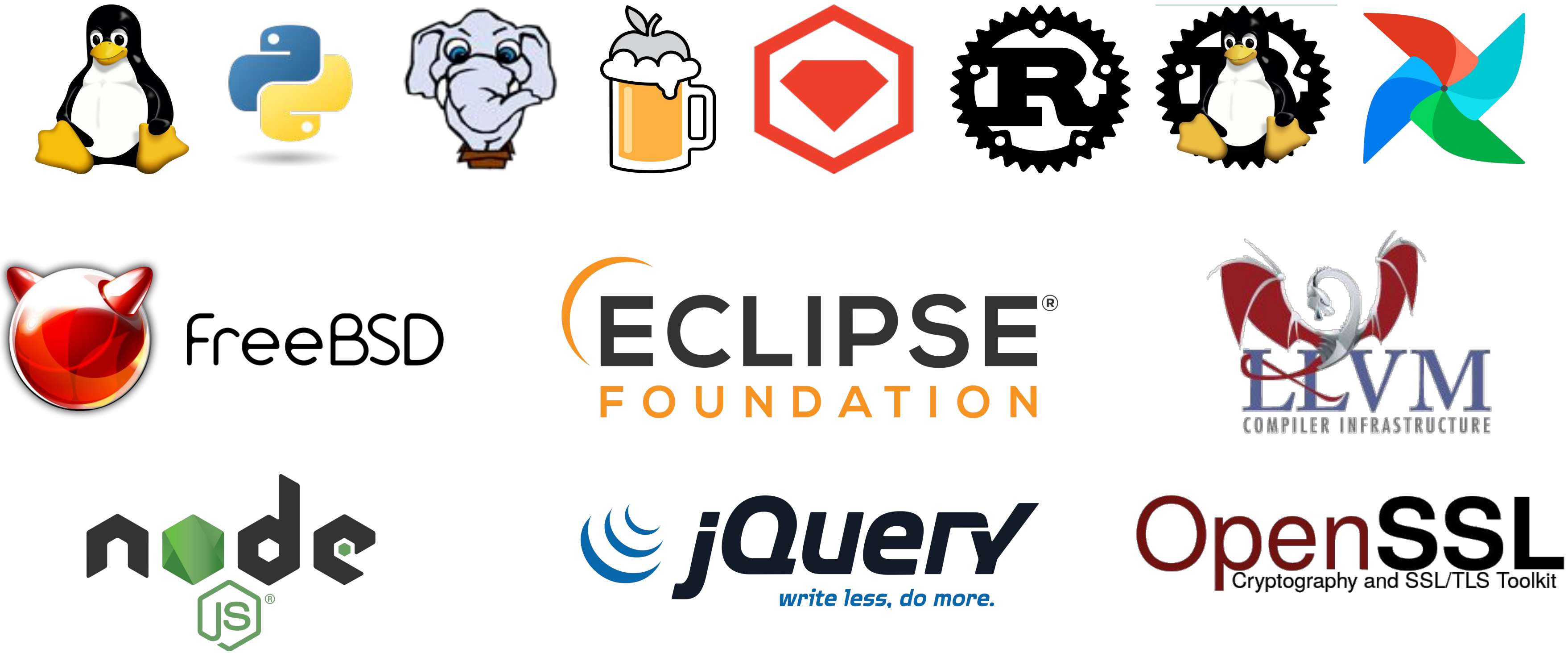
C

SECURITY AUDITS & REMEDIATION

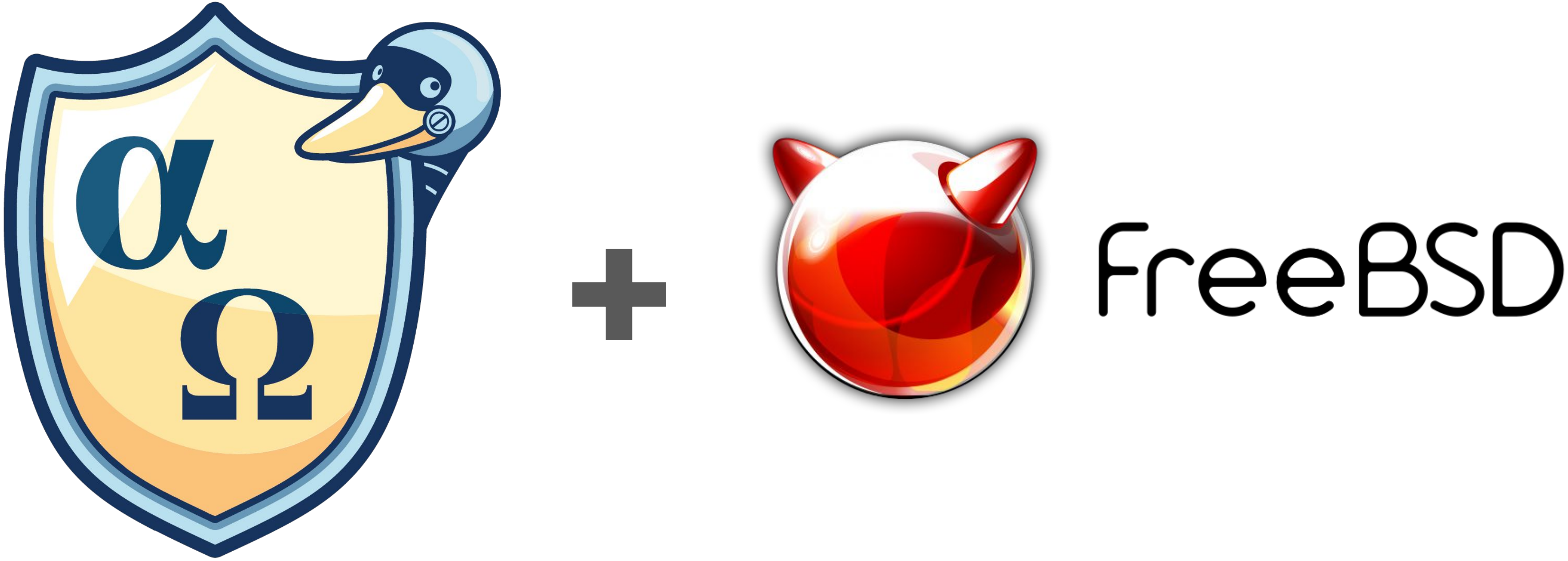
D

EXPERIMENTATION

Alpha-Omega Engagements



How We Came Together



FreeBSD

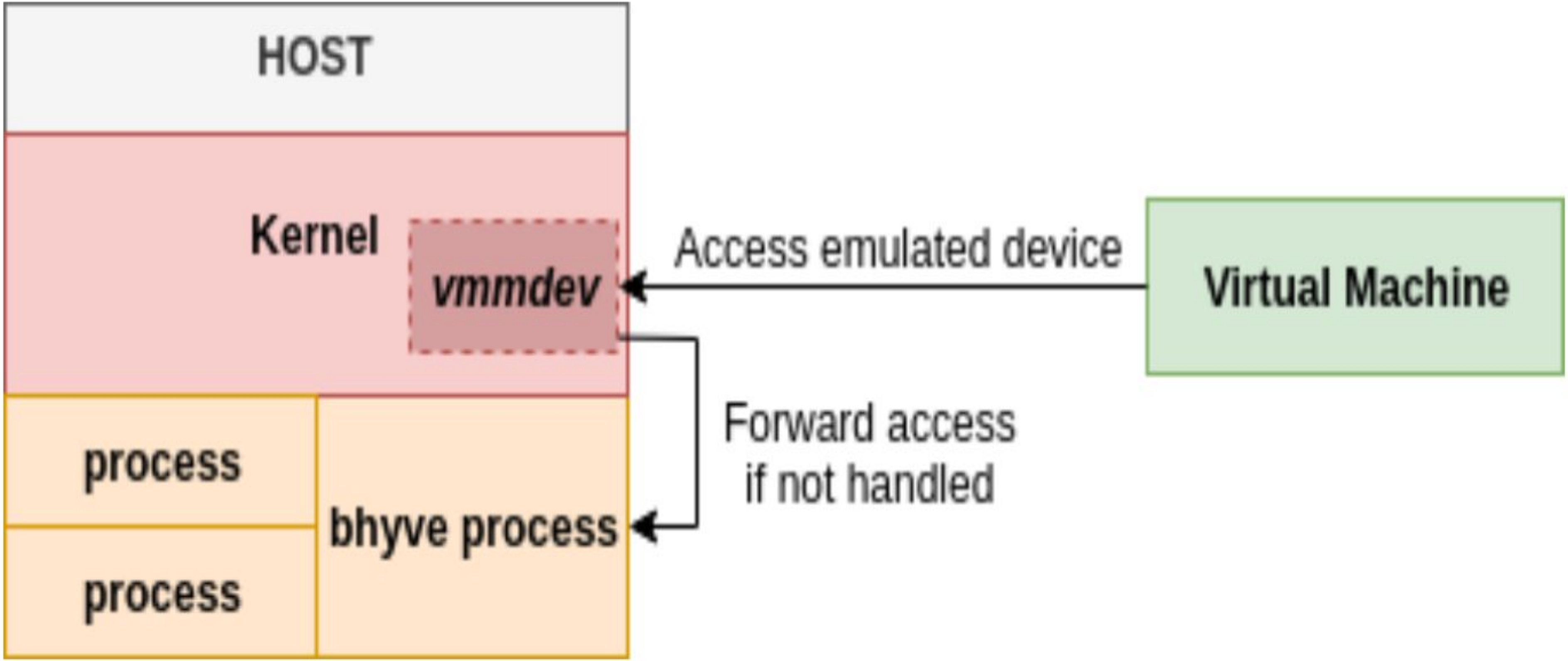
Historical Security Culture

Robust, reliable, stable base: BSD UNIX

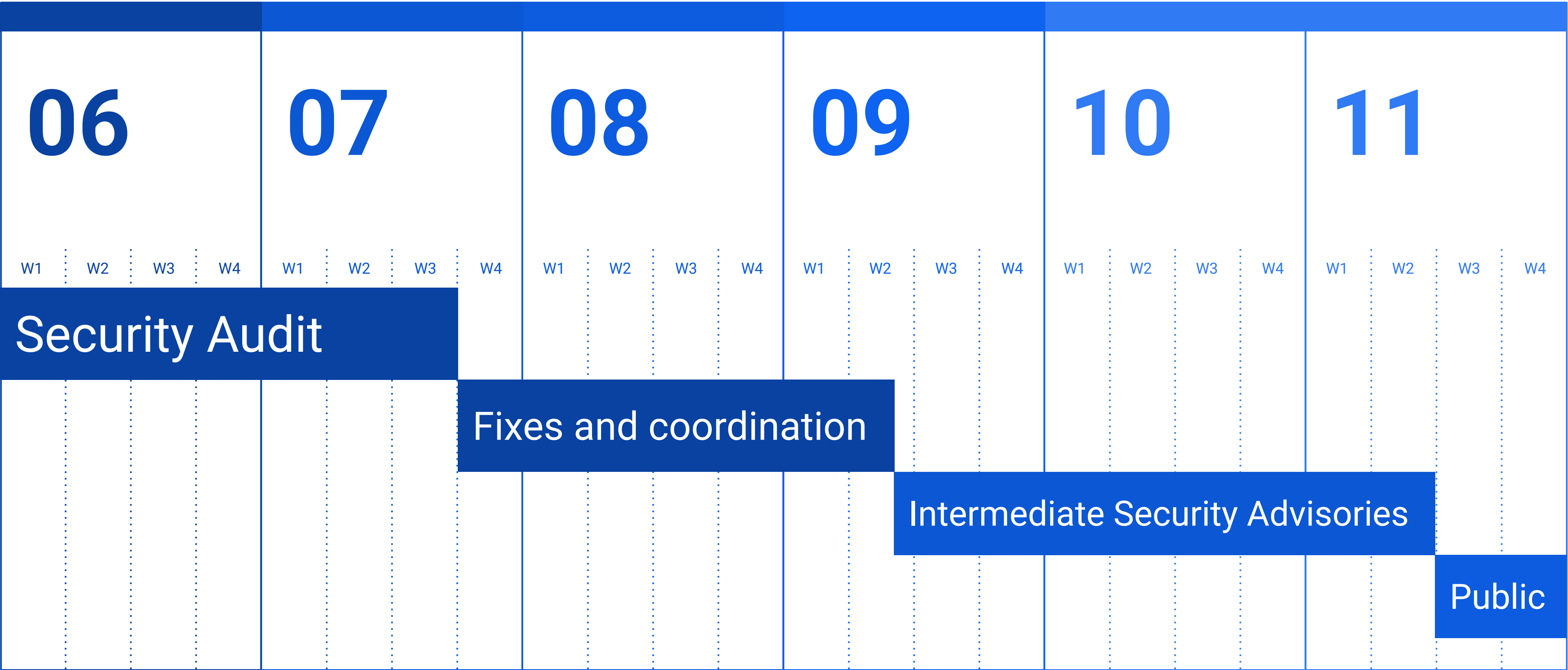
Innovative security features

Early exposure to remote attacks

The Audit Process



Audit, Fixes, and Disclosure Timeline



06

07

08

09

10

11

W1 W2 W3 W4

Security Audit

Fixes and coordination

Intermediate Security Advisories

Public

Vulnerability Classes Identified

bhyve specific issues

TOCTOU

Incorrect reference counting

Missing checks for errors

Integer overflows

Uninitialized variables

Lessons Learned

Proof of Concept **validators** are essential

Complexity is easily underestimated

OpSec could be improved

Funding fixes is just as important

Looking Ahead: Preventative Remediations

Additional **compiler checks**

CI/CD

Extend and improve the **tests**

Code **ownership**

Looking Ahead: Going Beyond

Improve the documentation for developers

BSD-specific security **trainings** & certification

Create an advisory **committee**?

Security Culture Reinvigorated

Security in FreeBSD is more important than ever

There is much work to be done

We need community engagement and prioritization

Get Involved freebsd-security@FreeBSD.org

Thank You

FreeBSD

FOUNDATION

α

Ω

This Deck

go.xwind.io/FreeBSDAudit

Resources

FreeBSD Foundation Releases Bhyve and Capsicum Security Audit Funded by Alpha-Omega Project

Alpha Omega 2024 Annual Report

freebsdfoundation.org - alpha-omega.dev - openssf.org