2024: OSTIF's Year in Review

A Summary and Discussion of the 2024 Fiscal Year
by an Open Source Security Firm

Prepared by the **Open Source Technology Improvement Fund** **https://ostif.org**

Graphic Design by **Anova Hou**

Hear from our Partners

"A key challenge in open source communities is developing sound security practices to ensure that project can stay ahead of security vulnerabilities and build software that our society can trust. Working with OSTIF is more than just security audits; it's being a partner with our communities in helping them understand threat models and impacts, giving them tools to have a strong security posture."

John Mertic, Director of Program Management - Linux Foundation

“Code reviews and security audits are among the most effective tools for securing our critical digital infrastructure components and form a key pillar of the Sovereign Tech Resilience program. We greatly appreciate OSTIF's approach to security audits, which not only helps these critical components identify and address the most pressing threats but also equips them with tools and practices to enhance their long-term security posture.”

Tara Tarakiyee, Technologist - Sovereign Tech Agency

“nvm has never had a security audit before. OSTIF and the firm they retained were extraordinarily helpful and thorough. The engineers involved were very willing to consider maintainer points of view, and were also quite persuasive – some flags they raised turned out to be nothing, and some turned out to be issues that were more important than they initially seemed, so it was great to surface the best answer with enthusiastic discussion. I look forward to working with OSTIF and 7A Security in the future!”

Jordan Harband, nvm & Open Source Maintainer

Contents

L-R: Helen Woeste, Amir Montazery, and Derek Zimmer in Brussels, Belgium for FOSDEM 2024

OSTIF: An International Network of Trust

A Note from OSTIF

2024 was not an easy year for open source: layoffs, budget cuts, and hacks have made it hard to be certain about the future of our industry. Even with the unknowns, OSTIF has managed to produce an impactful 9th year of open source security work.

From secondary audits with old friends to new projects with experimental uses, this year saw us manage 60 security audits with 11 funders and 6 audit teams. The honor of directing and advancing security research for the benefit of project users and maintainers is not lost on us, and we could not be more grateful for the opportunities afforded to us to work with communities and individuals who also see the positive impact of audit work.

2025 will be our 10 year anniversary. We have completed over 100 audits, identified over 1000 security findings, and provided security tools to dozens of projects. OSTIF has started hosting meetups and has spoken all over the world about the importance of security audits to open source resilience.

We can only dream of what comes next, and in the meantime, we'll be reminding you to code in memory safe languages and change your passwords regularly.

The OSTIF Story

Open Source Technology Improvement Fund, Inc (OSTIF) launched in 2015 as a corporate non-profit organization with a simple mission: **improve the security of Critical Open Source Projects EVERYONE depends on.** The goal -- to address the problem of limited resources with regards to security in open source projects. Furthermore, there was a lack of a transparent, systemic process on how to help open source projects in an effective and repeatable way.

Humble Beginnings

OSTIF built a network of trusted open source security researchers, audit firms, advocates, and project communities from the ground up and honed in on a method to systematically review and audit projects.

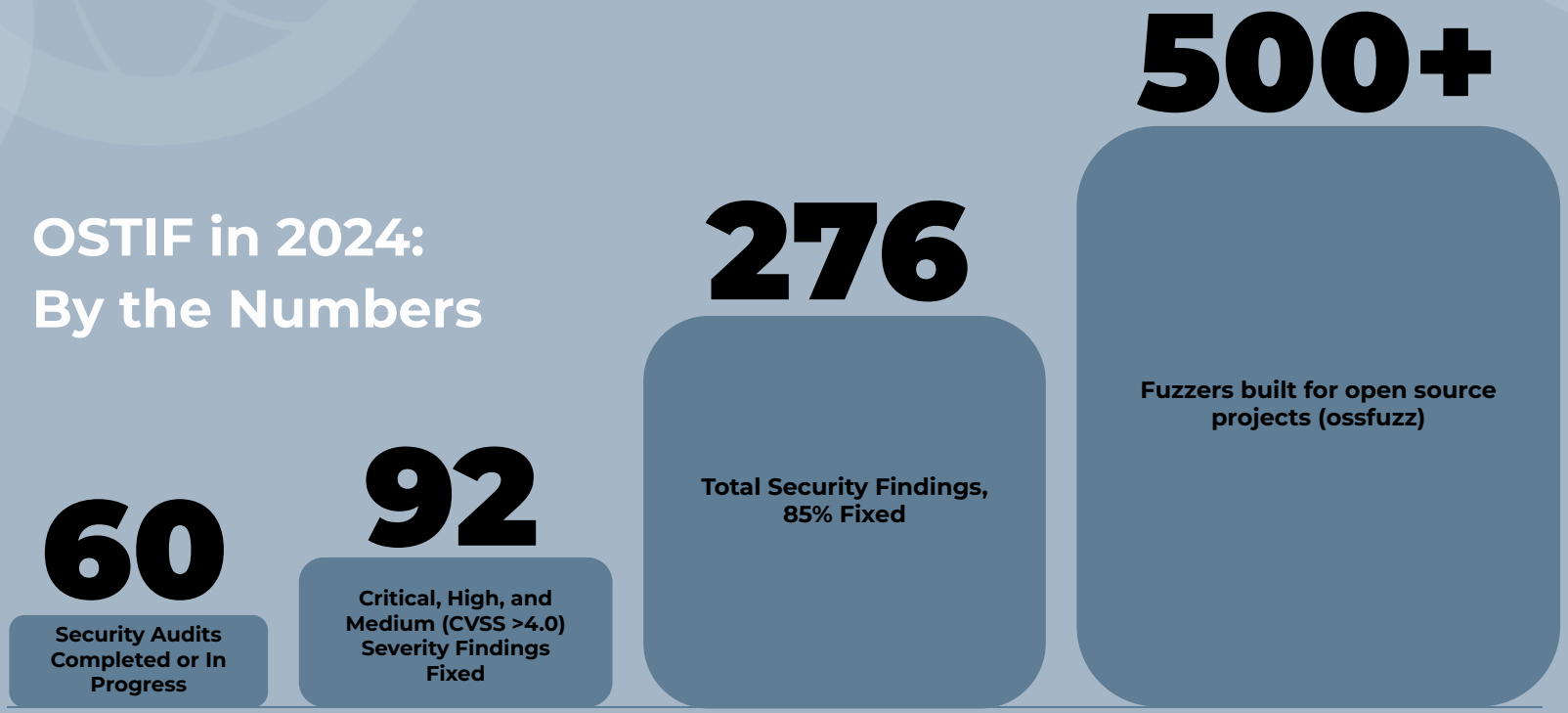
This work has culminated in nearly 16,000 hours of expert security work and the finding and remediation of hundreds of critical and high severity security vulnerabilities.

Amazing Progress

As we look towards our 10 year anniversary, there's a lot to be excited about.

- ➔ Over 100 audits completed for open source projects.
- ➔ Worked in sectors like energy, LLMs, cryptocurrency, cloud computing, disability access, email software, and VPNs.
- ➔ Top 15 fundraiser for open source security.
- ➔ Attended and spoken at numerous international open source conferences.
- ➔ Started online meetups (sign up to present!)

OSTIF in 2024: By the Numbers



$1,850,000

USD Directly Leveraged for Security Audits

Actualizing Security

How We Do What We Do

OSTIF functions at a high level of productivity, output, and generates actual security work. We turn money into security impact through:

- Extensive Professional Relationships.
- Scoping and Scaling our Audits Accurately.
- Emphasis on Communication.
- Investment in Open Source Security Testing.
- Strong Cost and Quality Controls.

Finding a vulnerability in an OSTIF audit will cost you a few thousand dollars. A threat actor finding it before us? That cost is immeasurable and varied.

Our contractors care about open source projects and their health- and their work to help resolve fixes shows it.

OSTIF has a proven process for directing security engagements that promotes open communication, customized scope and objectives, prioritizes project needs, and allows for fixes to be done privately with further aid given if needed.

Cultivating Partnerships

In organizing and managing audits for the Cloud Native Computing Foundation and the funded work by Sovereign Tech Agency, OSTIF has garnered support in the Open Source and Tech communities.

- ➔ Link to all of OSTIF's blog posts
- ➔ Link to all of OSTIF's audit reports

CLOUD NATIVE COMPUTING FOUNDATION

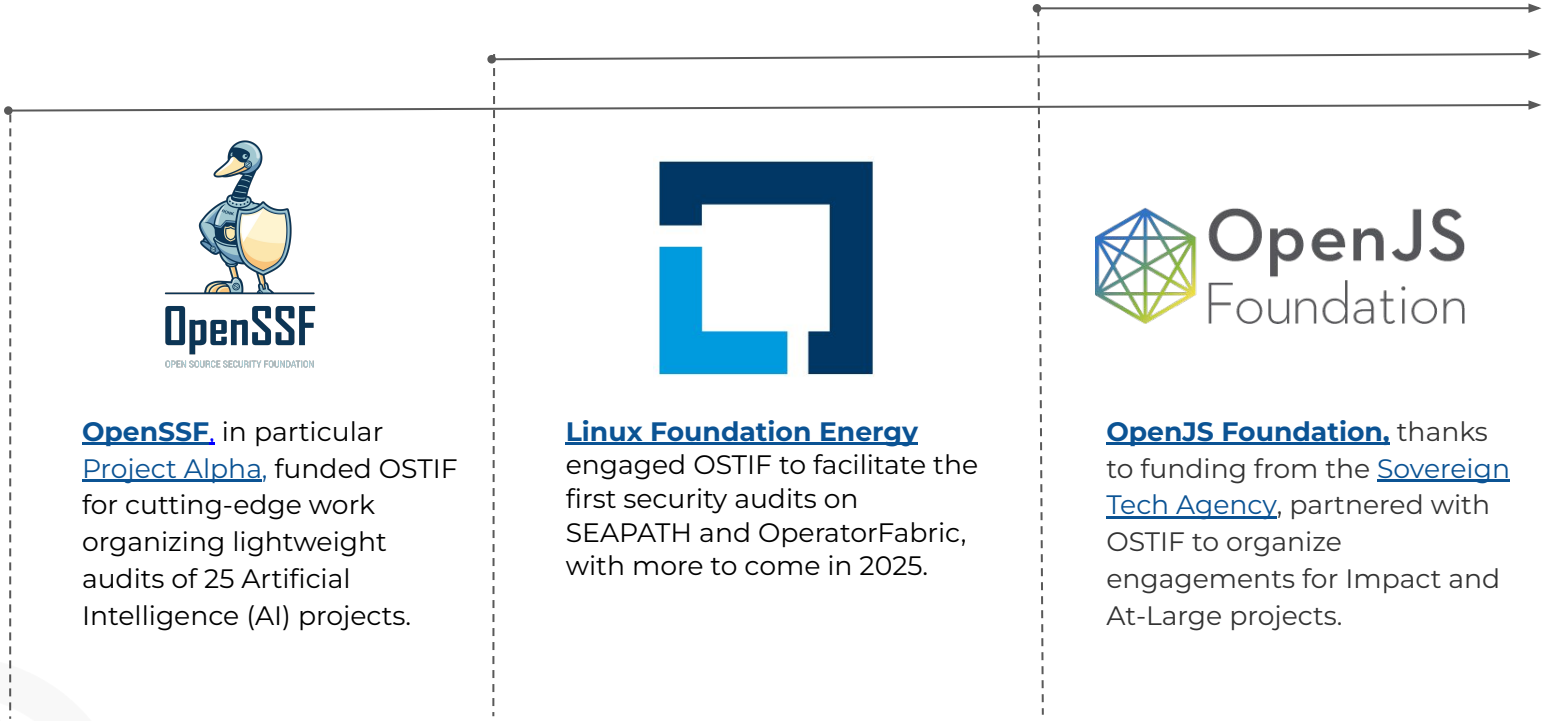
14 CNCF projects have been audited or are currently being audited with OSTIF this year. To date, 13 projects have reached Graduated status with CNCF thanks to OSTIF audits.

Sovereign Tech Agency

The Sovereign Tech Agency partnered with OSTIF as part of their Sovereign Tech Resilience Program to provide security audits to undersupported open source projects. Additional projects were funded through the OpenJS Foundation, for a total of 6 audits in 2024.

New Partners, New Projects

OSTIF got involved in new areas of cybersecurity this year through new partnerships, working in **energy infrastructure, Artificial Intelligence and LLMs,** and **JavaScript.**



OpenSSF, in particular Project Alpha, funded OSTIF for cutting-edge work organizing lightweight audits of 25 Artificial Intelligence (AI) projects.

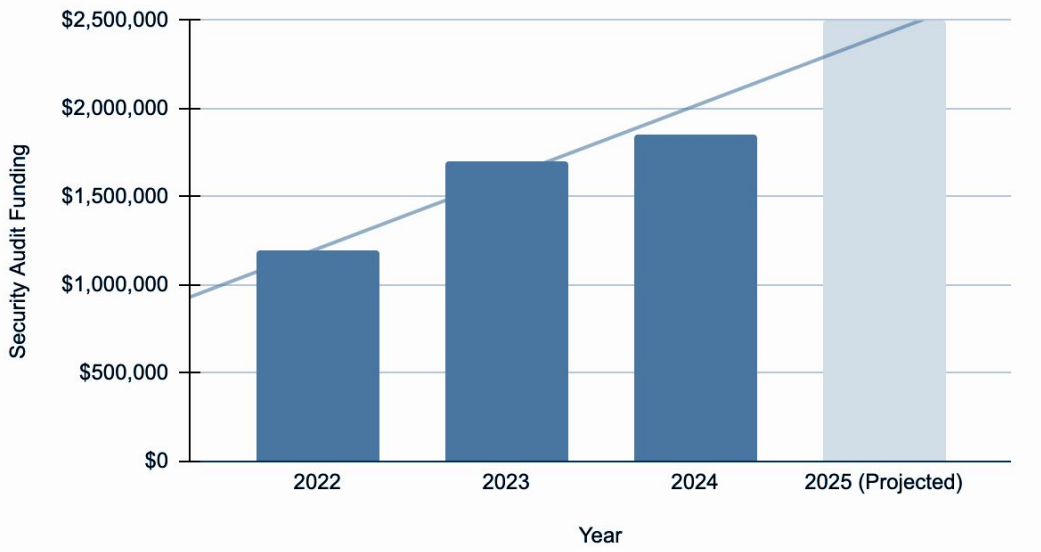
Linux Foundation Energy engaged OSTIF to facilitate the first security audits on SEAPATH and OperatorFabric, with more to come in 2025.

OpenJS Foundation, thanks to funding from the Sovereign Tech Agency, partnered with OSTIF to organize engagements for Impact and At-Large projects.

Fundraising 2022 - 2024

- Almost **$5 MILLION USD** raised for **security audits of critical open source projects.**
- 60 Audits in 2024, an **increase of 240%** from the previous year (25).
- Average of **80% Efficiency Ratio.**

Security Audit Funding vs. Year



Number of Audits (2023 vs. 2024)

How OSTIF Compares

Security Industry

Typical rates can be HIGH

Typical Audit Costs can be MILLIONS
For-profit security firms are typically incentivized to maximize bids.

Exploited Vulnerability cost estimate:
$4,880,000 USD (IBM, 2024)

Unseen costs: added labor of maintainers, administration, and publication/marketing. Commercial engagements rarely if ever include these in budget.

OSTIF

Savings of 30-40%
OSTIF typically receives discounts from audit firms on labor hours because of our working relationship with them.

Budget Controls
OSTIF uses budget controlling measures to ensure audit costs are kept true to value without sacrificing quality.

Av. Cost per found & fixed vuln and implemented tool (in 2024):
$3,700 USD

Unseen savings: administrative efforts, quality and cost control, publication/marketing coordination, maintainer time and labor. This is all included with OSTIF despite lower hourly rates.

Funding Support

Eleven institutions supported security this year by leveraging their money with OSTIF.

The Linux Foundation, Google, and Project Alpha Omega engaged OSTIF to manage security audits for a variety of projects including energy infrastructure, AI security, and fuzzing.

Sovereign Tech Agency, OpenJS Foundation, OpenSSF, Drupal Association and PHP Foundation also supported OSTIF through funding security engagements.

DuckDuckGo directly supported OSTIF through their charitable donations program for a fourth year in a row.

OSTIF is a 501(c)3 nonprofit organization, so funding of all sizes helps further our mission.

Premier Supporters (>$400k)

Sovereign Tech Agency

CLOUD NATIVE COMPUTING FOUNDATION

Platinum Supporters (>$100k)

Alpha-Omega

ECLIPSE FOUNDATION

aws

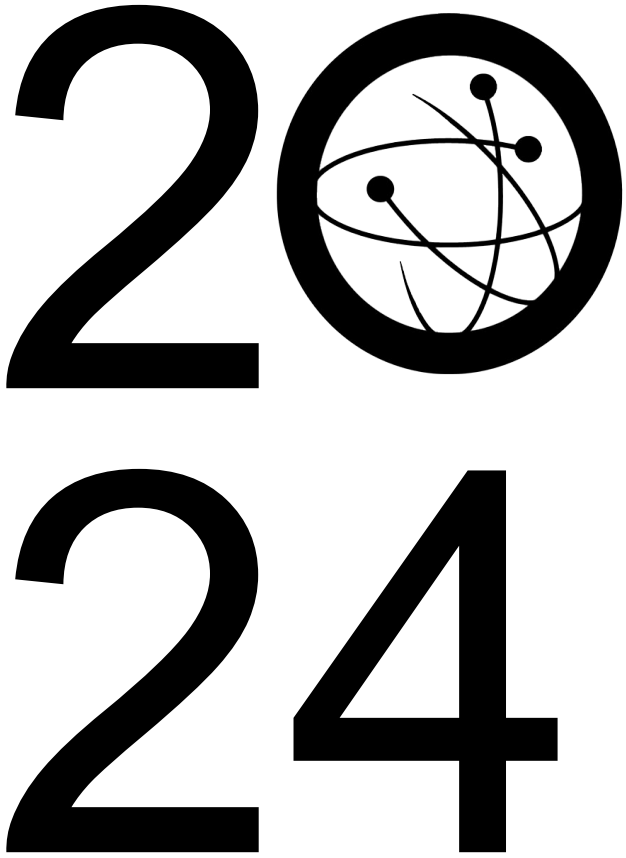
LF ENERGY

Gold Supporters (>$50k)

OpenJS Foundation

The PHP Foundation

Silver Supporters ($25k)



SUPPORT OUR WORK

This past year held a lot of changes for OSTIF. We started with new partners, entered new fields of cybersecurity, and took a critical look at our future as we start our 10th year of existence.

It's been a long (and bumpy) road to reach this point, and we could not be more proud of how we got here. It's all because of those who have believed in us; that a small organization formed solely to support open source security could work with the biggest and most revolutionary firms in the digital world to bring actual security impact to underserved projects.

We look forward to the next decade. Hopefully, you'll be alongside us for the ride- there's a lot of work left to do.

All our best-

Derek Amir Helen

References

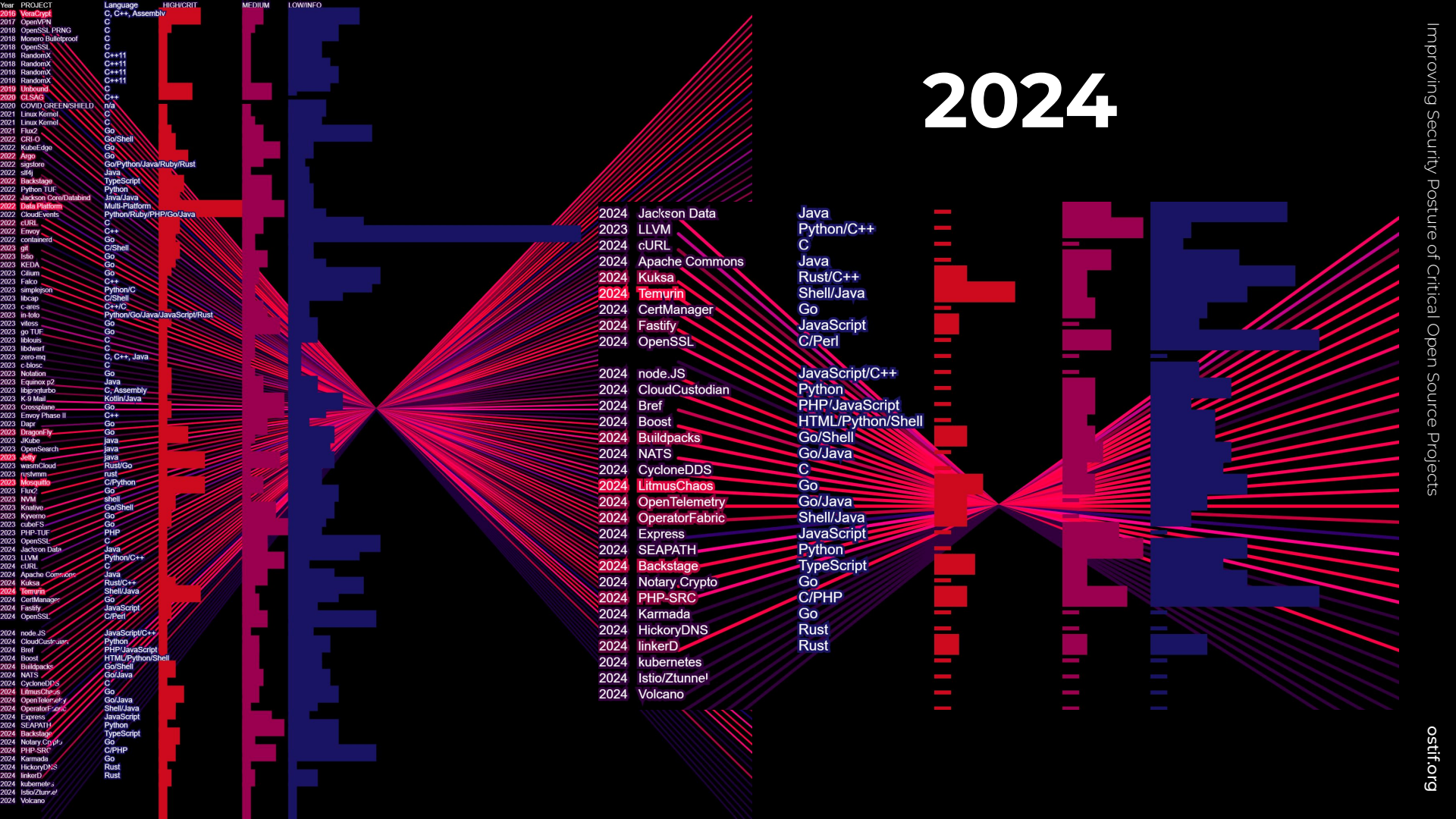
IBM Cost of a Data Breach Report 2024 https://www.ibm.com/reports/data-breach

OSTIF Audits https://github.com/ostif-org/OSTIF/blob/main/Completed-Engagements.md

2024 Reports

Cloud Native Computing Foundation Report https://ostif.org/2024-cncf-ostif-impactreport/

Sovereign Tech Agency Report https://ostif.org/2024-sovtech-audit-report/


2024
Improving Security Posture of Critical Open Source Projects
ostif.org
Year PROJECT Language HIGH/CRIT MEDIUM LOW/INFO
2016 VeraCrypt C, C++, Assembly
2017 OpenVPN C
2018 OpenSSL PRNG C
2018 Monero Bulletproof C
2018 OpenSSL C
2018 RandomX C++11
2018 RandomX C++11
2018 RandomX C++11
2018 RandomX C++11
2019 Unbound C
2020 CLSAG C++
2020 COVID GREEN/SHIELD n/a
2021 Linux Kernel C
2021 Linux Kernel C
2021 Flux2 Go
2022 CRI-O Go/Shell
2022 KubeEdge Go
2022 Argo Go
2022 sigstore Go/Python/Java/Ruby/Rust
2022 slf4j Java
2022 Backstage TypeScript
2022 Python TUF Python
2022 Jackson Core/Databind Java/Java
2022 Data Platform Multi-Platform
2022 CloudEvents Python/Ruby/PHP/Go/Java
2022 cURL C
2022 Envoy C++
2022 containerd Go
2023 git C/Shell
2023 Istio Go
2023 KEDA Go
2023 Cilium Go
2023 Falco C++
2023 simplejson Python/C
2023 libcap C/Shell
2023 c-ares C++/C
2023 in-toto Python/Go/Java/JavaScript/Rust
2023 vitess Go
2023 go TUF Go
2023 tiklouis C
2023 libdwarf C
2023 zero-mq C, C++, Java
2023 c-blosc C
2023 Notation Go
2023 Equinox p2 Java
2023 libjpeg-turbo C, Assembly
2023 K-9 Mail Kotlin/Java
2023 Crossplane Go
2023 Envoy Phase II C++
2023 Dapr Go
2023 DragonFly Go
2023 JKube java
2023 OpenSearch java
2023 Jetty java
2023 wasmCloud Rust/Go
2023 rustvmm rust
2023 Mosquitto C/Python
2023 Flux2 Go
2023 NVM shell
2023 Knative Go/Shell
2023 Kyverno Go
2023 cubeFS Go
2023 PHP-TUF PHP
2023 OpenSSL C
2024 Jackson Data Java
2023 LLVM Python/C++
2024 cURL C
2024 Apache Commons Java
2024 Kuksa Rust/C++
2024 Temurin Shell/Java
2024 CertManager Go
2024 Fastify JavaScript
2024 OpenSSL C/Perl
2024 node.JS JavaScript/C++
2024 CloudCustodian Python
2024 Bref PHP/JavaScript
2024 Boost HTML/Python/Shell
2024 Buildpacks Go/Shell
2024 NATS Go/Java
2024 CycloneDDS C
2024 LitmusChaos Go
2024 OpenTelemetry Go/Java
2024 OperatorFabric Shell/Java
2024 Express JavaScript
2024 SEAPATH Python
2024 Backstage TypeScript
2024 Notary Crypto Go
2024 PHP-SRC C/PHP
2024 Karmada Go
2024 HickoryDNS Rust
2024 linkerD Rust
2024 kubernetes
2024 Istio/Ztunnel
2024 Volcano