Stewarding Cybersecurity Awareness via Data & Discovery

Hilary Carter
SVP Research
The Linux Foundation

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

JOIN DISCORD

Collaborate with your team in the workstream channel. Share links, chat, and if something merits discussion, let us know!

#awareness-workstream

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

1. Discovery

Find security resources quickly through LF Security.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

THE LINUX FOUNDATION

Security

A suite of security resources at your fingertips!

Report a Security Vulnerability

Find the latest guidance on how to report vulnerabilities to LF projects and foundations, or with respect to Linux Foundation infrastructure (as a whole), or the main LF website.

Avoiding Social Engineering Takeovers

Read the alert for social engineering takeovers of open source projects to better recognize emerging threat patterns.

https://www.linuxfoundation.org/lf-security

THE LINUX FOUNDATION

Security

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

SPDX

Alpha-Omega

CONFIDENTIAL COMPUTING CONSORTIUM

OPENCHAIN

Post-Quantum Cryptography Alliance

THE LINUX FOUNDATION | Europe

THE LINUX FOUNDATION | Events

THE LINUX FOUNDATION | Research

THE LINUX FOUNDATION | Training & Certification

LF ENERGY

FINOS Fintech Open Source Foundation

LF NETWORKING

https://www.linuxfoundation.org/lf-security

SOSS FUSION/24

THE CONFERENCE FOR SECURE OPEN SOURCE SOFTWARE

SOSS Community Day
INDIA

SOSS Community Day
EUROPE

CLOUDNATIVE SECURITYCON
NORTH AMERICA 2024

CLOUDNATIVE SECURITYCON
NORTH AMERICA 2023
FEBRUARY 1 – 2, 2023

SOSS Policy Summit
EUROPE

2.Data

What’s the state of open source software security?

OPEN SOURCE SECURITY FOUNDATION

2020

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Security Gaps Revealed in 2020 FOSS Contributor Survey

Key finding: There is **a clear need to dedicate more security to FOSS**.

Memorable quotes:

“I find the enterprise of security a **soul-withering chore** and a subject **best left for the lawyers and process freaks**. I am an application developer.”

“I find **security** an **insufferably boring procedural hindrance.**”

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2021

OPEN SOURCE SECURITY FOUNDATION

LF Research launches.

Explores key questions such as:

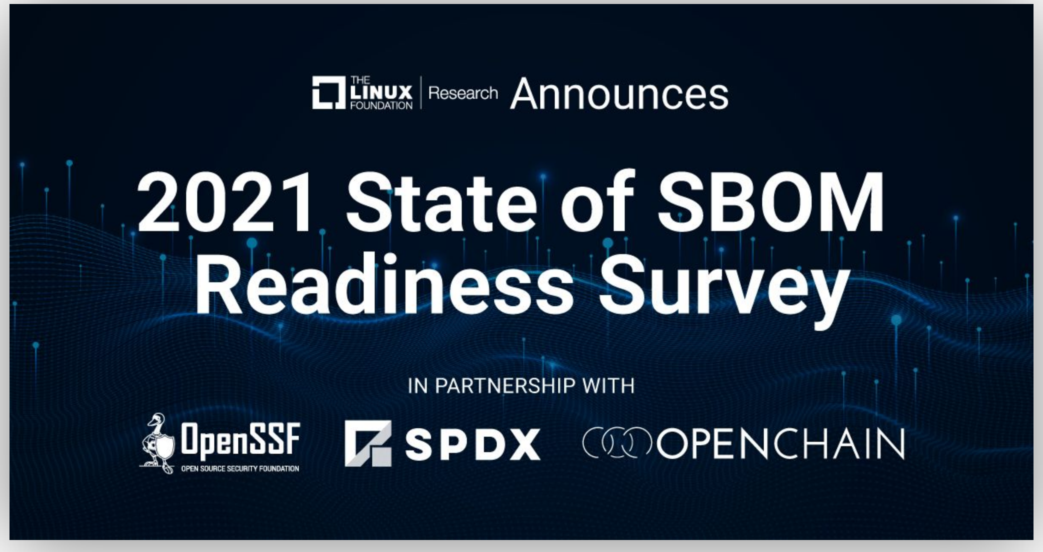
- What is the state of secure software development / SBOM adoption?
- What's the most widely used open source software?
- What do maintainers / developers need to improve OSS security?

Empirical approaches:

- Quantitative
- Qualitative studies
- Mixed methods

https://www.linuxfoundation.org/research

SBOM Readiness Survey Launches following US Executive Order on Improving the Nation’s Cybersecurity



"**SBOMs are no longer optional**. Businesses accelerating SBOM adoption are not only **improving the quality of their software, they are better preparing themselves to thwart adversarial attacks**."
Jim Zemlin, October 2021

Widespread awareness, limited current use, future use likely to increase

Source: https://www.linuxfoundation.org/research/the-state-of-software-bill-of-materials-sbom-and-cybersecurity-readiness

2022
Going deeper into domains

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Census II of Free and Open Source Software – Application Libraries

The persistence of legacy software in the open source space suggests that open source has not escaped the problem of legacy technology.

CENSUS II: LESSON LEARNED

`log4j` showed up as number 38 in the non-npm, direct, version-agnostic packages list.

CENSUS II: RESULTS

Individual developer account security is increasingly important. The OpenSSF encourages the use of MFA tokens to achieve greater account security.

CENSUS II: LESSON LEARNED

The most widely used FOSS is developed by only a handful of contributors. Results in one dataset show that 136 developers were responsible for more than 80% of the lines of code added to the top 50 packages.

CENSUS II: LESSON LEARNED

Source: https://www.linuxfoundation.org/research/census-ii-of-free-and-open-source-software-application-libraries

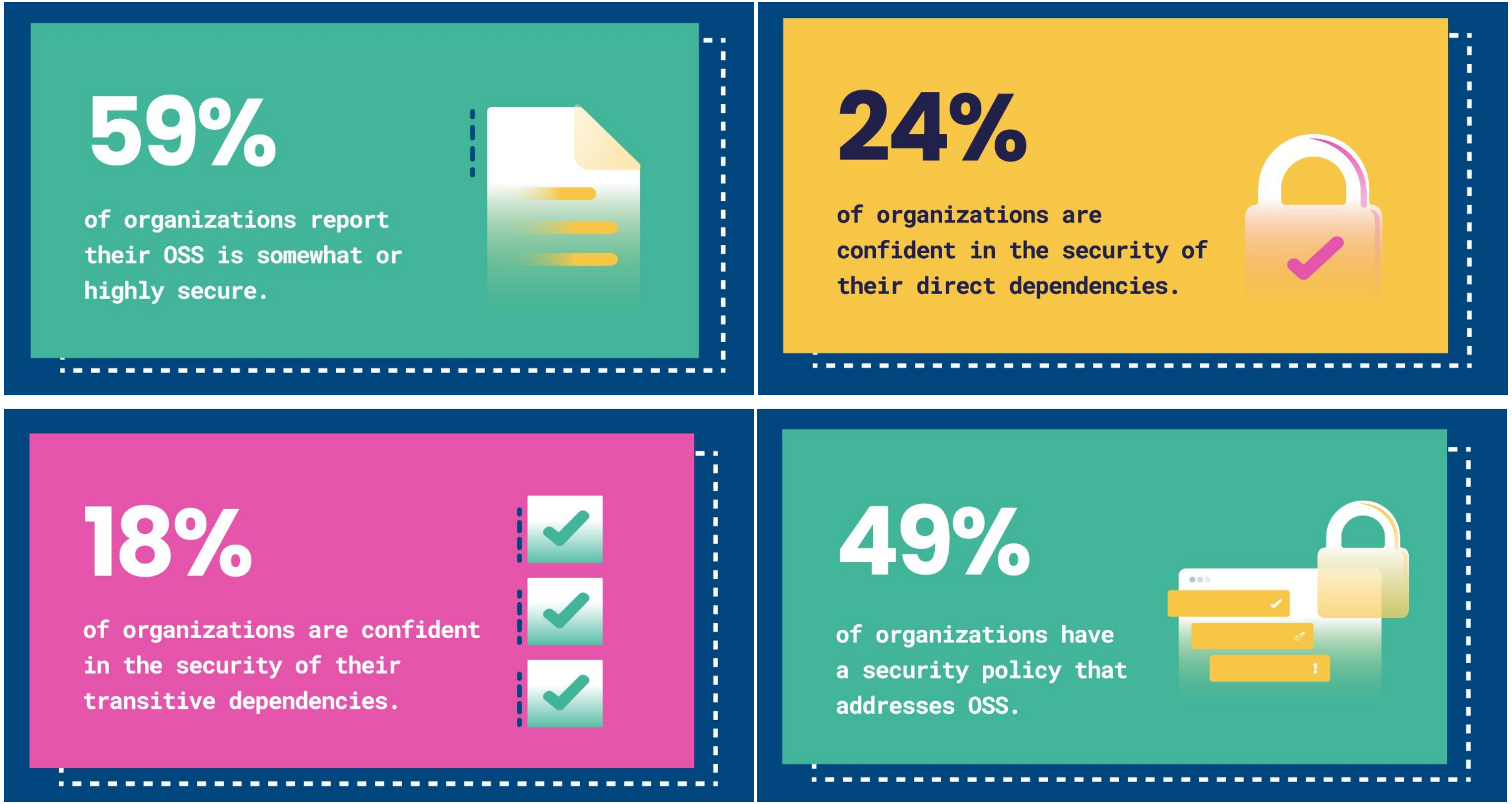
OSS & Cybersecurity Challenges Study

In partnership with Snyk with the help of numerous survey distribution partners, this study explored:

1. The current **state of open source software security**

2. **Methods to address & improve it** (such as static application testing tools & SCA scanning, documentation)

Key findings on the state of security: Room for improvement



Source: https://www.linuxfoundation.org/research/addressing-cybersecurity-challenges-in-open-source-software

Reasons for optimism: Maintainer data segmentation

MAINTAINER PERSPECTIVES ON OSS SECURITY

49% of OSS contributors want **employer incentives** for OSS contributions.

MAINTAINER PERSPECTIVES ON OSS SECURITY

Project documentation is widespread but not ubiquitous:
87% of projects responded that they provide basic documentation.

MAINTAINER PERSPECTIVES ON OSS SECURITY

69% of OSS contributors want **defined best practices** for secure software development.

MAINTAINER PERSPECTIVES ON OSS SECURITY

By the end of 2023, 72% of maintainers and core contributors feel that **OSS will be secure.**

Source: https://www.linuxfoundation.org/research/maintainer-perspectives-on-security

2023:
Gaps persist

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Europe 2023 Spotlight Report Reveals Security Gaps

Improved security ranks lowest as a benefit of open source by survey respondents, and contribution as a way to improve security is least likely to be considered.

There is a lack of maturity when it comes to safely using OSS. Software bills of materials (SBOMs) are not well understood as a security best practice.

THE LINUX FOUNDATION

Source: https://www.linuxfoundation.org/research/world-of-open-source-eu-2023

Global 2023 Spotlight Report Reveals Security Gaps

Source: https://www.linuxfoundation.org/research/world-of-open-source-global-2023

2024:
Expanding research efforts

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Secure Software Development Education Survey & Cloud Native Security Survey

THE LINUX FOUNDATION

2024 Software Security Education Study

SECURE SOFTWARE DEVELOPMENT EDUCATION 2024 SURVEY

69% of professionals rely on on-the-job experience as a learning resource for secure software development, but **it can take more than 5 years of such experience** to achieve familiarity.

SECURE SOFTWARE DEVELOPMENT EDUCATION 2024 SURVEY

53% of professionals, especially those in system operations (72%), have not taken a course on secure software development, largely due to **the lack of awareness about good courses** (44%).

SECURE SOFTWARE DEVELOPMENT EDUCATION 2024 SURVEY

Software developers with **less than one year of experience** report the highest lack of familiarity (75%)

SECURE SOFTWARE DEVELOPMENT EDUCATION 2024 SURVEY

To start mitigating the need for more secure software development education, the OpenSSF selected **Security Architecture as the topic of a new course**.

2024 Cloud Native Security Report: Positive trends

2024 CLOUD NATIVE SECURITY REPORT

84% of organizations report their cloud native applications are **more secure** than they were two years ago.

2024 CLOUD NATIVE SECURITY REPORT

63% of organizations are using static application security testing **(SAST) tools.**

2024 CLOUD NATIVE SECURITY REPORT

67% of respondents use **CNCF webinars / workshops & confer-ences** to stay informed about cloud native security tools & updates.

2024 CLOUD NATIVE SECURITY REPORT

65% of respondents rely on **CNCF best practices** to make progress in securing their cloud native applications.

Cybersecurity Job Skills Framework

Objective

- Develop a **global framework of cybersecurity skills for 14 IT roles** with defined skill levels
- Support IT organizations in crafting cybersecurity strategies

Methodology

Expertise pulled from 2 sources:

- SME reviews and feedback
- Survey - community response

1st phase of the survey

431 completes

- Global survey fielded end of April to mid May
- **66% to 95%** approval rates for job descriptions and cybersecurity responsibilities
- **11k** words of feedback

2nd phase of the survey

874 completes

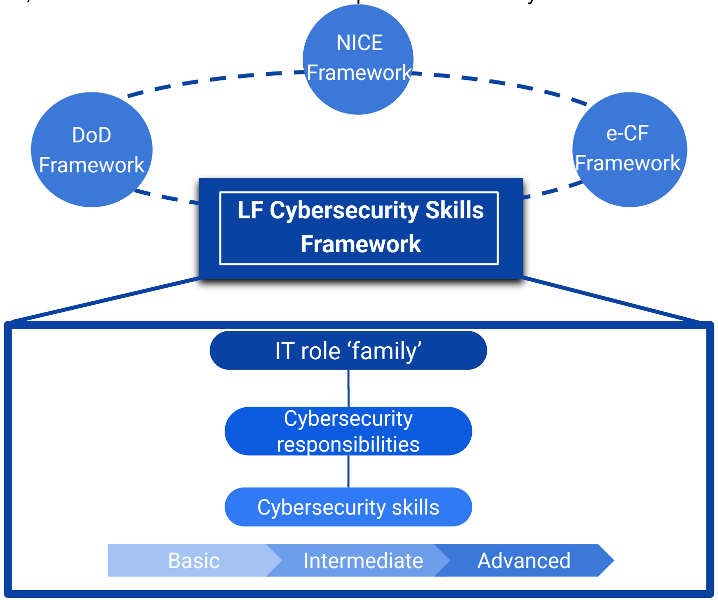
- Global survey fielded early July to early August
- **81% to 97%** approval rates for skillsets
- **13k** words of feedback

Global Cybersecurity IT Skills Framework Roles

Overview: Most IT roles now require specific cybersecurity skills. This research study developed a global reference framework that identifies and describes 14 cybersecurity-related job roles with three levels of baseline skills aligned with job proficiency. The following summary reviews these 14 job roles and their main responsibilities, as well as common cybersecurity skills. The full report describes these roles and their corresponding skillsets in detail, as well as how this framework maps to other industry frameworks.

Roles and their focus areas

1. Web developer: secure coding practices, vulnerability management
2. Software developer: secure software design, authentication and encryption, verification techniques
3. Platform engineer: secure system design and architecture, system hardening and monitoring
4. Systems architect: secure system design, threat modeling, integrating advanced security measures
5. DevOps engineer: secure CI/CD pipelines, secure IaC, dependency management
6. Networking engineer: firewall & access control management, secure network architectures
7. AI engineer: secure data pipelines and AI/ML model security, data protection and compliance
8. Database administrator: database security and access controls, data protection and encryption
9. IT Project manager: manage security integration and compliance, manage recovery plans
10. Solution architect: advanced hardening, strategic governance, cross-domain integration
11. Cybersecurity analyst: security procedures, threat hunting, tool management



Global Cybersecurity IT Skills Framework

12. GRC manager: compliance audits, risk assessment, IT governance, GRC leadership
13. Security administrator: monitoring, incident response, and security operations
14. IT Services management: manage IT services within ITSM frameworks, ensure compliance

Common cybersecurity skills across roles

Security best practices – Adherence to security guidelines and frameworks (e.g., OWASP, ISO 27001).
Compliance and regulations – Knowledge of relevant regulations like GDPR, HIPAA, etc.
Incident response – Ability to respond to and manage security incidents.
Security tools and techniques – Proficiency in security tools (e.g., SIEM, SAST/DAST tools) and methodologies.
Risk management – Understanding and mitigating risks through assessments and threat modeling.

Considerations

Supplementary Skills – The cybersecurity skills outlined are in addition to the core technical and operational skills required for each IT role.
Not Prescriptive – This framework is a starting point, not a prescription. Organizations may need to tailor this framework to fit their unique security posture and industry requirements.

THE LINUX FOUNDATION Research

OpenSSF OPEN SOURCE SECURITY FOUNDATION

LISH Laboratory for Innovation Science at Harvard

Census III of Free and Open Source Software

Application Libraries

Frank Nagle, *Harvard Business School*

Kate Powell, *Laboratory for Innovation Science at Harvard*

Richie Zitomer, *Harvard Business School*

David A. Wheeler, *Open Source Security Foundation (OpenSSF), The Linux Foundation*

In partnership with

FOSSA snyk sonatype BLACKDUCK

December 2024

Census III Key Findings

CENSUS III OF FREE AND OPEN SOURCE SOFTWARE

Legacy software persists in the open source space, making their security as important as their replacement packages.

CENSUS III OF FREE AND OPEN SOURCE SOFTWARE

Among top 50 non-npm projects, **17% had only one developer** & **40% had one or two developers** accounting for more than **80% of commits.**

CENSUS III OF FREE AND OPEN SOURCE SOFTWARE

There are promising efforts to implement a **standardized naming schema** for software components which would improve supply chain security and future census efforts.

CENSUS III OF FREE AND OPEN SOURCE SOFTWARE

Use of components from **Rust package repositories have increased** considerably since Census II, signaling an industry response to memory safety vulnerabilities.

OSPOs are key drivers for OSS & security awareness

Our latest study with the **TODO Group** shows the significance of OSPOs in terms of their impact on open source strategy and their significance to **security best practices**.

There is still room for growth. Our study shows that **while 77% of large organizations have an OSPO, only 19% of small organizations have one**. Implementing an OSPO can **improve license compliance** and increased **transparency**. The report advocates for greater adoption to capitalize on these benefits.

2025:
Upcoming research

Pathways to CRA Best Practices: LF Project Spotlight

Research objectives:

1. Assess the **breadth and depth of the practices** established by these projects **against the industry and regulatory requirements** in Europe and the US pre-CRA,
2. **Identify the gaps between those practices and the requirements** that will come into effect with the CRA.
3. **Identify actions** that will need to be taken for all open source projects to close the gap to fully implement the CRA.

CIVIL INFRASTRUCTURE PLATFORM

Zephyr®

yocto PROJECT

Publication target: **31 January 2025**

Audience:

- Open source ecosystem leaders, both technical & business decision makers.
- Decision makers at manufacturers

3. What's Missing?

Join the the Awareness Workshop to Brainstorm Closing CRA-Specific Awareness Gaps

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Questions?
Thank You!

Greg Kroah-Hartman gregkh@linuxfoundation.org
Christopher Robinson christopher.robinson@linuxfoundation.org
Mirko Boehm mboehm@linuxfoundation.org
Hilary Carter hcarter@linuxfoundation.org