Open Source Pulling Back the Curtain for Enterprise Adoption

MINNEAPOLIS CYBERSECURITY SUMMIT 2023

Kelley Misata, Ph.D.

About Me

WEARER OF MANY HATS!

A survivor of cyberstalking, now a dedicated security professional devoted to advancing open-source development, fostering innovation, and enhancing nonprofit security as part of critical infrastructure.

PRESIDENT, OISF

SENIOR DIRECTOR OF OPEN SOURCE, CORELIGHT

FOUNDER AND CHIEF TRAILBLAZER, SIGHTLINE SECURITY

FORMER DIRECTOR OF COMMUNICATION, TOR PROJECT

Local governments allegedly targeted with Iranian 'Drokbk' malware through Log4j vulnerability

SolarWinds attack explained: And why it was so hard to detect

Buggy, Vulnerable Open-Source Code Seeps Into Business Tech

Why open-source software supply chain attacks have tripled in a year

IN THE NEWS

Open source risks and vulnerabilities are no longer lurking in the shadows, they impact security across the spectrum.

FREE SOFTWARE

Freedom to use, run, copy distribute, study change, and improve.

OPEN SOURCE

Licensed source code that is open for free use, modification, and distribution.

FREEWARE

Proprietary (usually) software that is free to use.

OPEN SOURCE IS EVERYWHERE

A foundation for MANY commercial codebases and is intertwined in development that many often don't know the open-source components of in their own software.

94M DEVELOPERS ON GITHUB

no longer the special few who are contributing to OS - many on company resources and time

90% COMPANIES USE OPEN SOURCE

often without even knowing it - tracking, prioritizing, engaging with projects is challenging

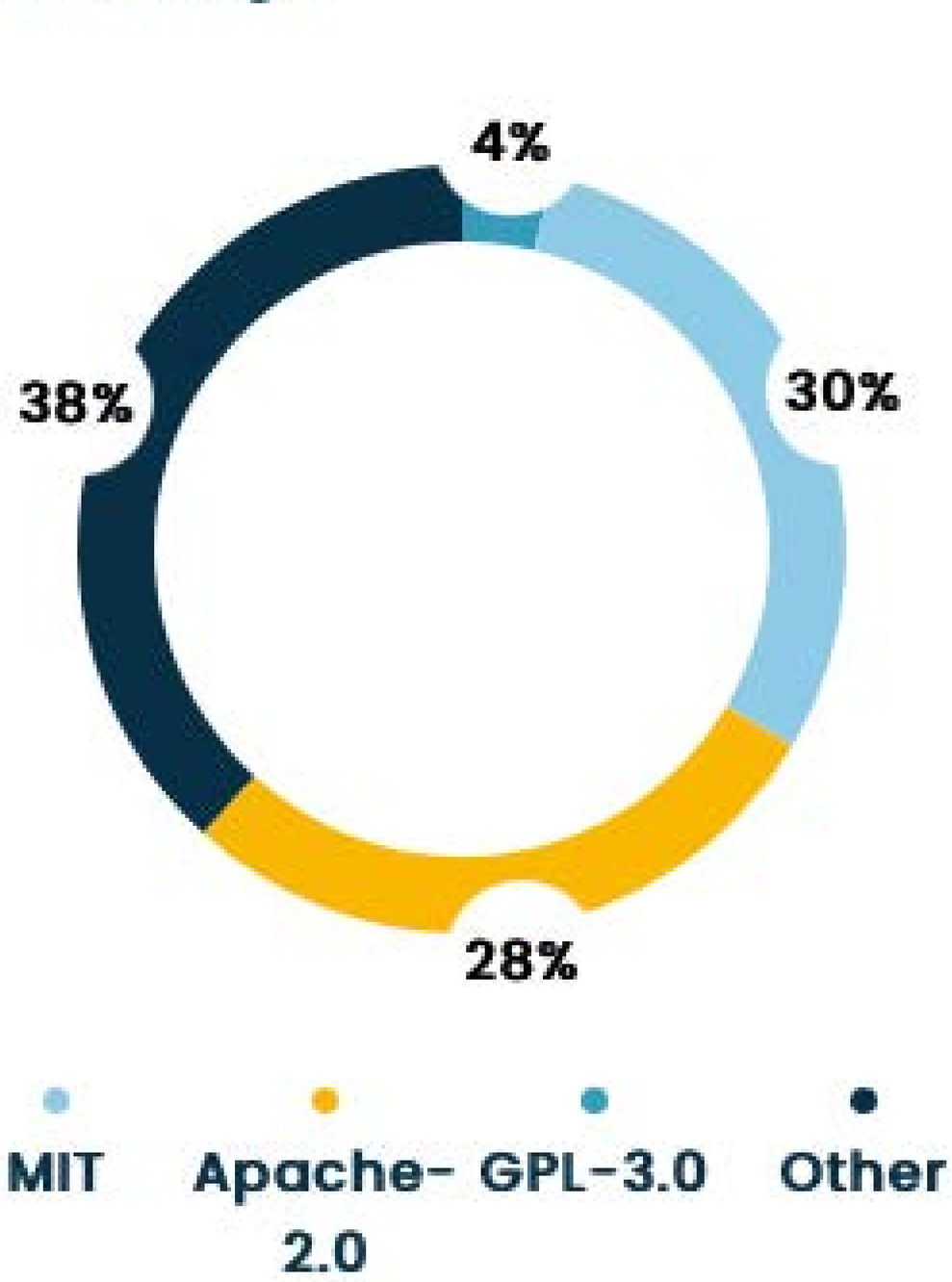
413M CONTRIBUTIONS IN 2022

open source projects are active but not all are healthy

[SOURCE] https://octoverse.github.com

LICENSES ARE KEY!

Understanding the licenses is essential - from highly permissive to restrictive.



[SOURCE] https://www.mend.io/blog/open-source-licenses-trends-and-predictions/
[SOURCE] https://opensourceindex.io

TOP RISKS

2023

1

Known Vulnerability
exploited by an attacker

2

Compromise Legitimate Package
resources that are part of a legitimate project or distribution

3

Named Components
a malicious named component similar to a legitimate project

4

Ignoring It
failure to keep track of open source components across the organization

[SOURCE] https://www.csoonline.com/article/574615/top-10-open-source-software-risks-for-2023.html

STEPS TO TAKE

Some open source projects are part of commercial business models, others operate independently.

Governance

Consider the governance structure of the project and what that means for longevity and sustainability.

Community

Pay attention to the people behind the project and participate.

Roadmap

Evaluate existing roadmaps and the processes by which they are maintained and followed.

COMING!

Complex Licenses

Innovations & Ideas

Attack Vectors

AI & ML

Frameworks

THANK YOU

KELLEY MISATA