The Supply Chain Is Broken. We Can Fix It.

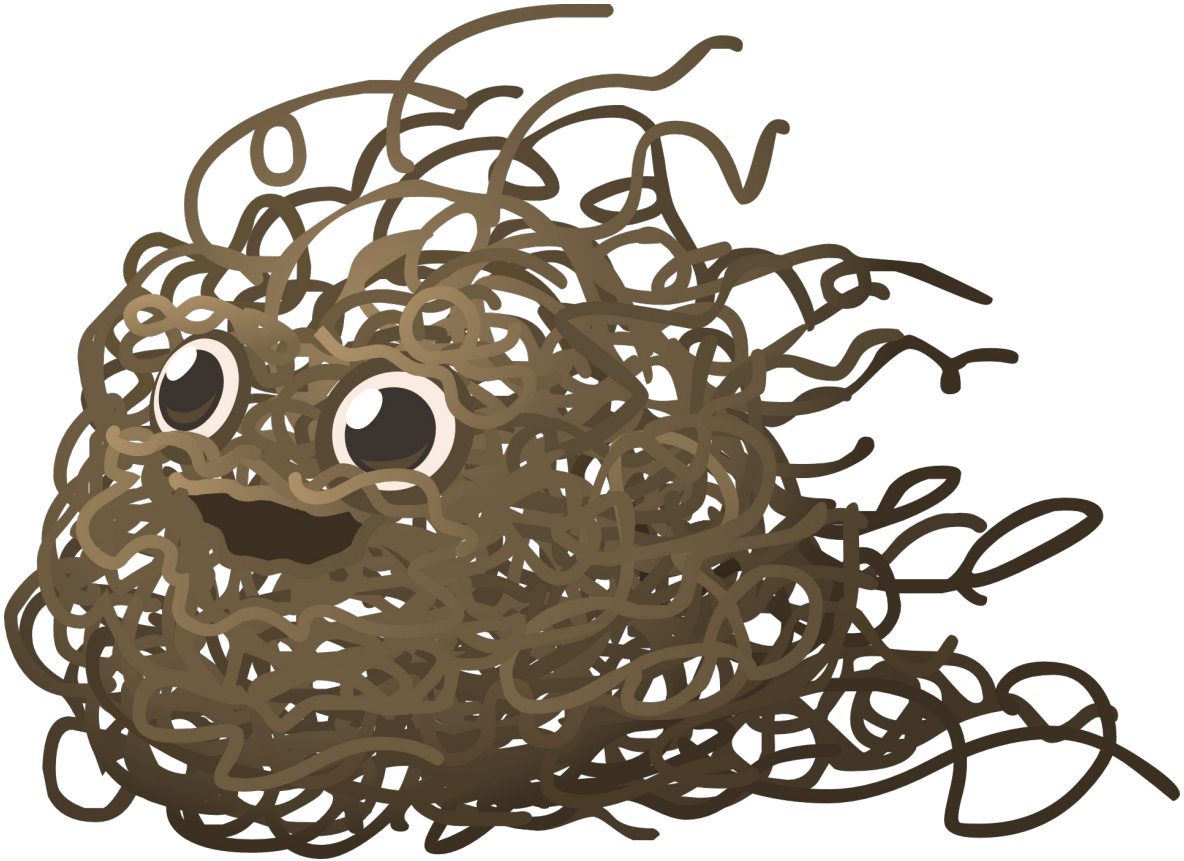
Building Trust in Open Source

THE LINUX FOUNDATION

OPENCHAIN

Our Mental Model Of The Supply Chain

The Actual Supply Chain



THE LINUX FOUNDATION

67.4%

Of managers monitor their supply chain with Excel spreadsheets

https://www.zippia.com/advice/supply-chain-statistics/

62%

Of additional cost with supply chain disruptions

https://www.zippia.com/advice/supply-chain-statistics/

94%

Of companies do not have full visibility of their supply chain

https://www.zippia.com/advice/supply-chain-statistics/

This Is Weird

57%

Of companies see supply chain management as a competitive edge

https://www.zippia.com/advice/supply-chain-statistics/

70%

Of companies see supply chains as a driver for customer service

https://www.zippia.com/advice/supply-chain-statistics/

40%

Savings available for industrial suppliers via optimization

https://www.zippia.com/advice/supply-chain-statistics/

Conclusion: Talking != Doing

As Usual,
Open Source Is Not Special

90+%

Of codebases using open source

https://www.synopsys.com/blogs/software-security/open-source-trends-ossra-report/

81%

Of codebases have security vulnerabilities

https://www.synopsys.com/blogs/software-security/open-source-trends-ossra-report/

53%

Of codebases contain license compliance issues

https://www.synopsys.com/blogs/software-security/open-source-trends-ossra-report/

Don’t Panic

The Secret: Good Processes = Good Supply Chain

Know what you are doing

Know how you are doing it

Use records to make it repeatable

Make a plan to fix problems

We Have An ISO/IEC Standard For Licensing

OpenChain ISO/IEC 5230:2020 is the International Standard for open source license compliance

- Defines the key requirements of a quality open source license compliance program
- Super short and simple, allowing companies of any size and in any market to adopt it

Free self-certification @ www.openchainproject.org

THE LINUX FOUNDATION

We Have A De-Facto Standard For Security

OpenChain Security Assurance Specification 1.0 is the de facto industry standard for open source security compliance

- Defines the key requirements of a quality open source security compliance program
- Super short and simple, allowing companies of any size and in any market to adopt it

Learn more @ www.openchainproject.org

The OpenChain Security Assurance Specification ETA as ISO/IEC standard in mid-2023

We Have An ISO/IEC Standard For SBOM

SPDX ISO/IEC 5962:2021 is the International Standard for software bill of materials

- A common format for organizations to share license compliance, security compliance and other data
- SPDX Version 2.3 (the community rolling release) just out, includes some useful updates related to security

Learn more @ https://spdx.dev

We Have Free Training Courses

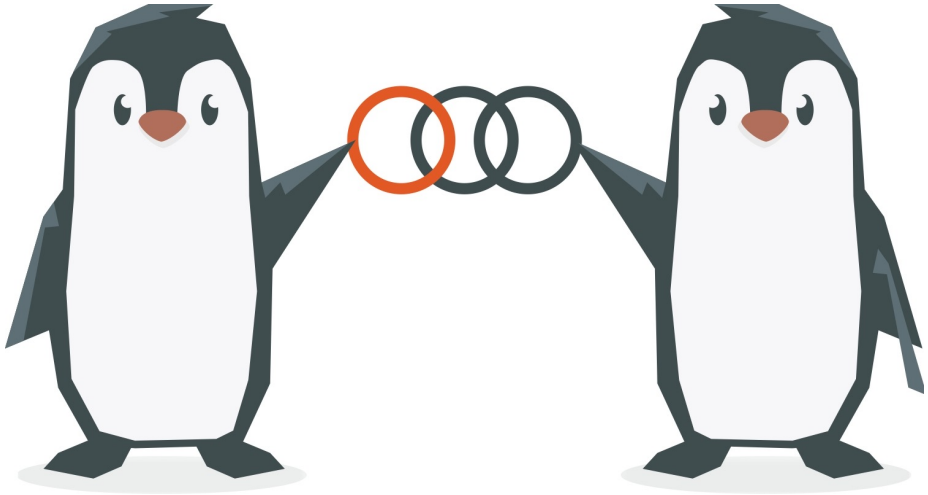
Introduction to Open Source License Compliance Management (LFC193)

Implementing Open Source License Compliance Management (LFC194)

THE LINUX FOUNDATION

We Have Communities To Support You

Join Mailing Lists And Calls



https://www.openchainproject.org/participate

Come To Regional Events

OpenChain UK Work Group
London on October 13th 2022

OSPOlogy.live in Sweden
Stockholm on October 19th– 20th 2022

OpenChain Germany Work Group
Cologne on November 16th 2022

Talk To Me

scoughlan@linuxfoundation.org

THE LINUX FOUNDATION


THE
LINUX
FOUNDATION