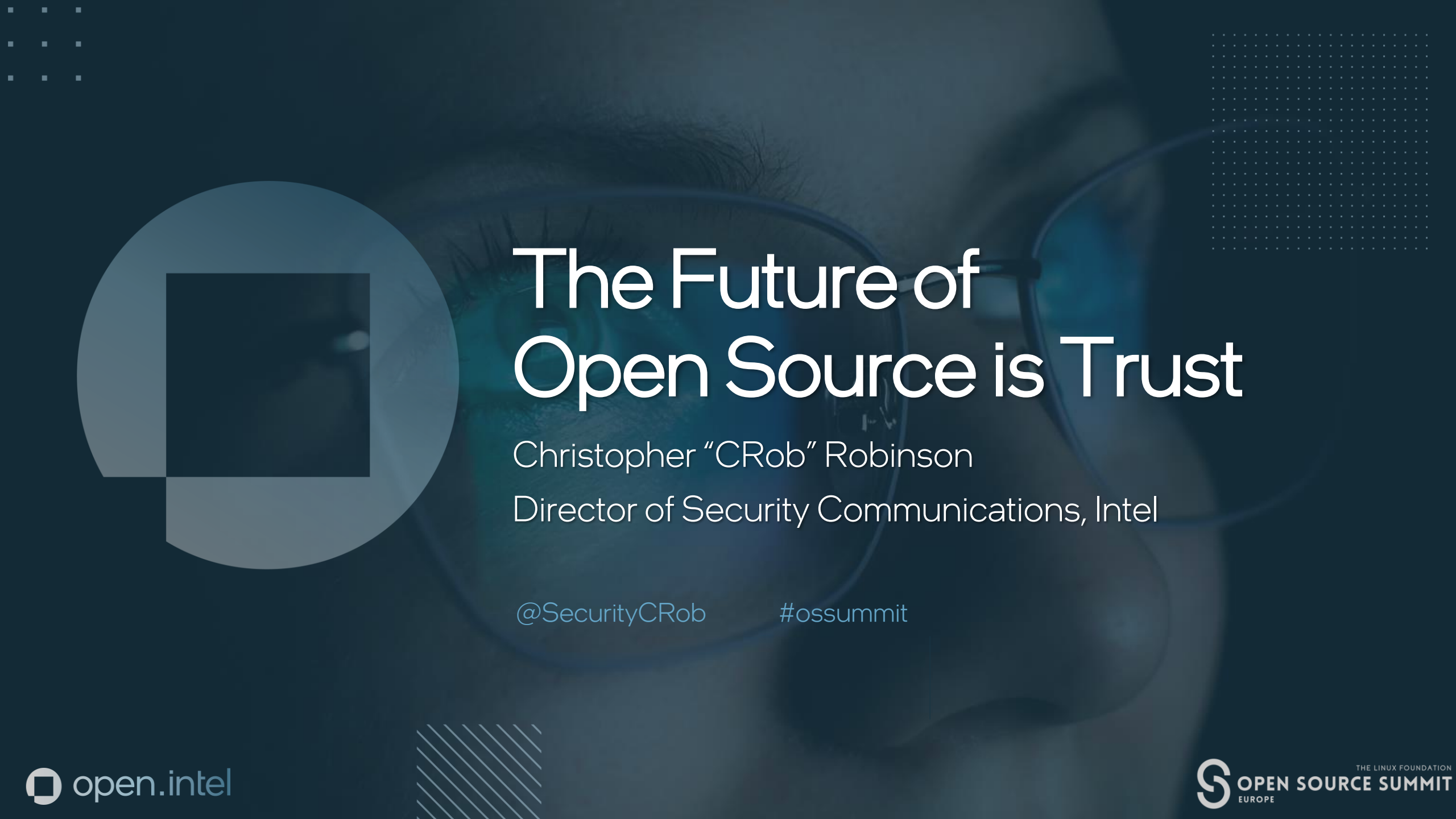


The Future of Open Source is Trust

Christopher "CRob" Robinson

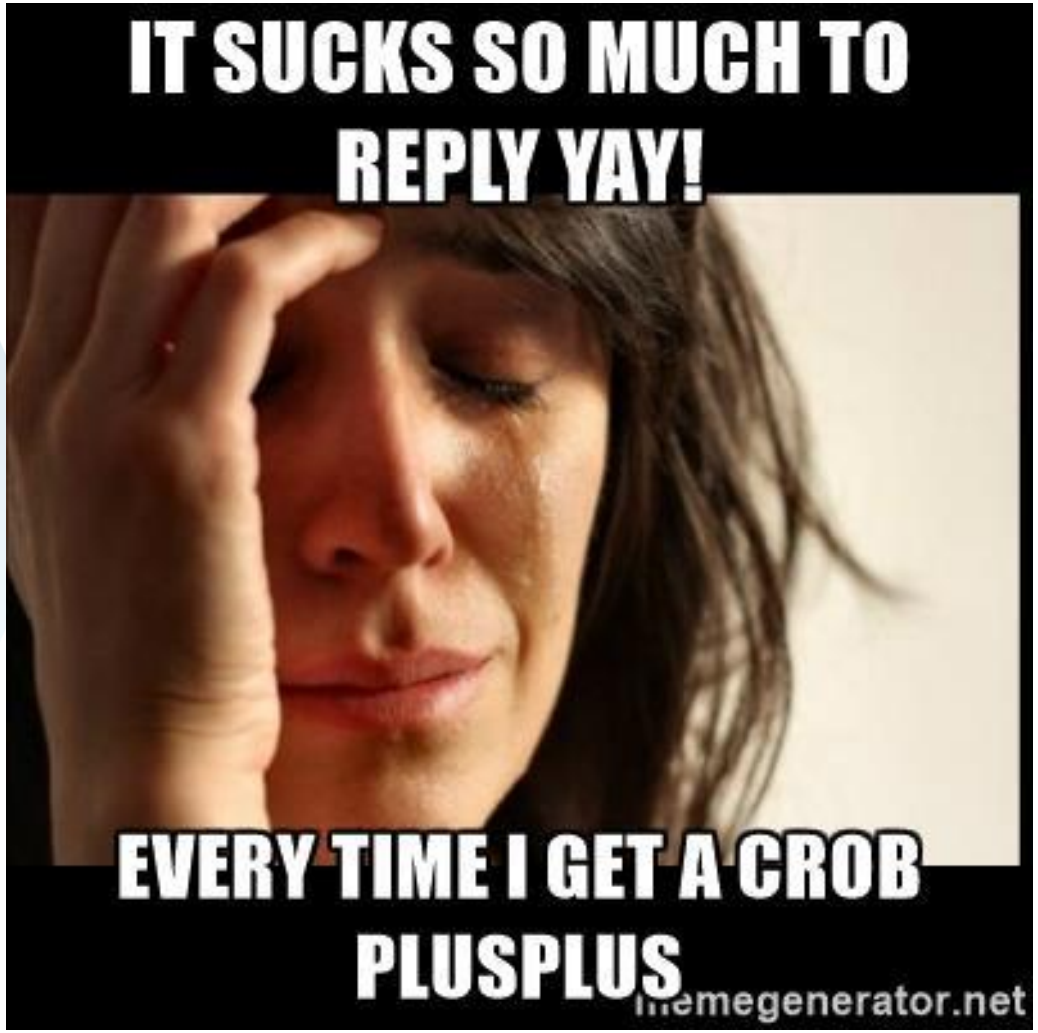
Director of Security Communications, Intel

@SecurityCRob

#ossummit

open.intel

THE LINUX FOUNDATION OPEN SOURCE SUMMIT EUROPE



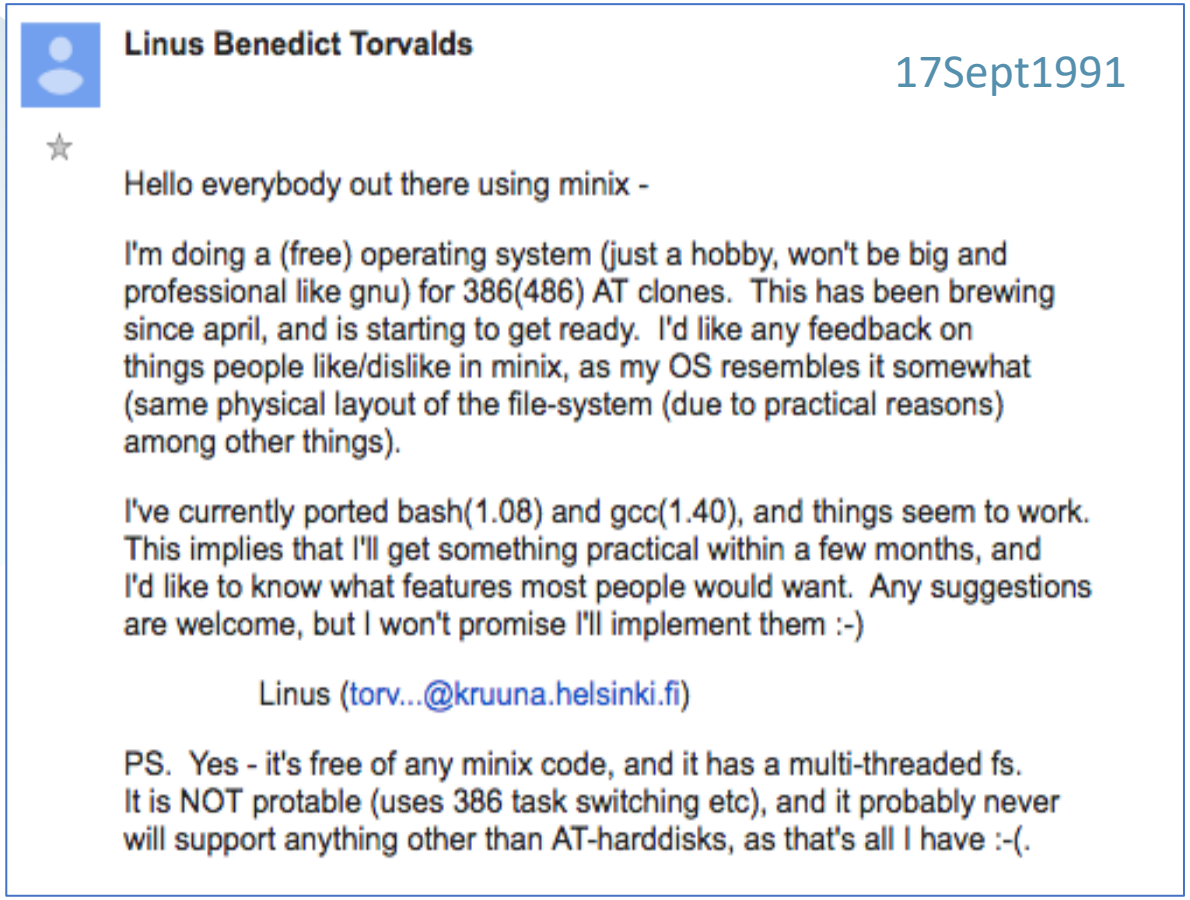
From 2017/09/06 #tam IRC post

[IE@OSS-EU ~]sh$ ./HelloWorld.

- **CRob, n, adj, and v**
  Pronunciation: U.S. (K-rowb)

41st level Dungeon Master
24th level Securityologist

Linux & Open Source were built on a foundation of trust



Linus Benedict Torvalds 17Sept1991

Hello everybody out there using minix -

I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) among other things).

I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want. Any suggestions are welcome, but I won't promise I'll implement them :-)

Linus (torv...@kruuna.helsinki.fi)

PS. Yes - it's free of any minix code, and it has a multi-threaded fs. It is NOT protable (uses 386 task switching etc), and it probably never will support anything other than AT-harddisks, as that's all I have :-(.

As OSS Evolved, so has the Threat Landscape

CVE-2014-0160
04/07/2014

CVE-2014-6271
09/24/2014

CVE-2016-0800
03/01/2016

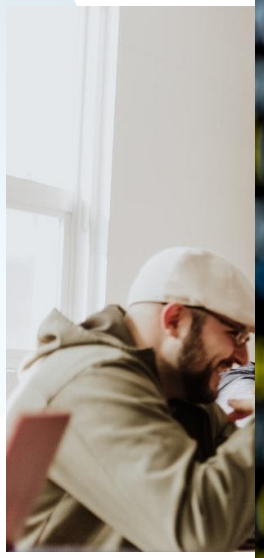
event-stream
crypto miner
Sept – Oct
2018

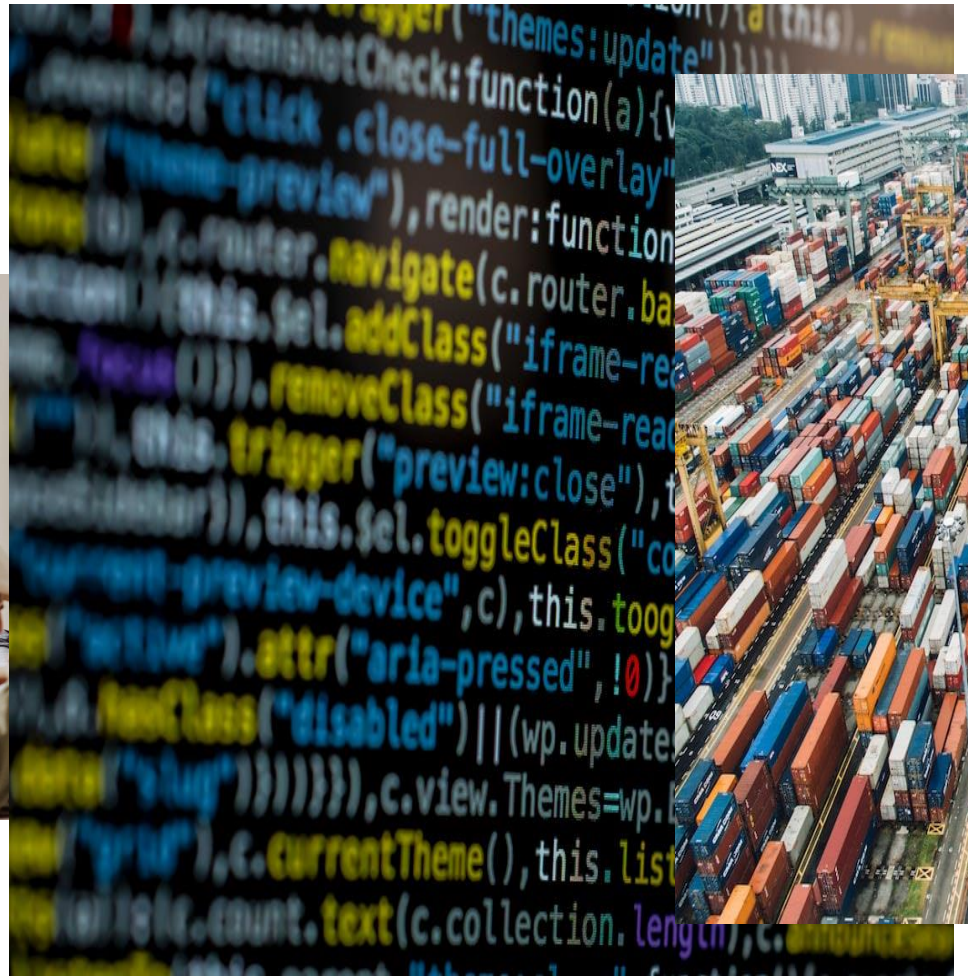
CVE-2020-25705
11/16/2020

CVE-2021-44228
12/10/2021

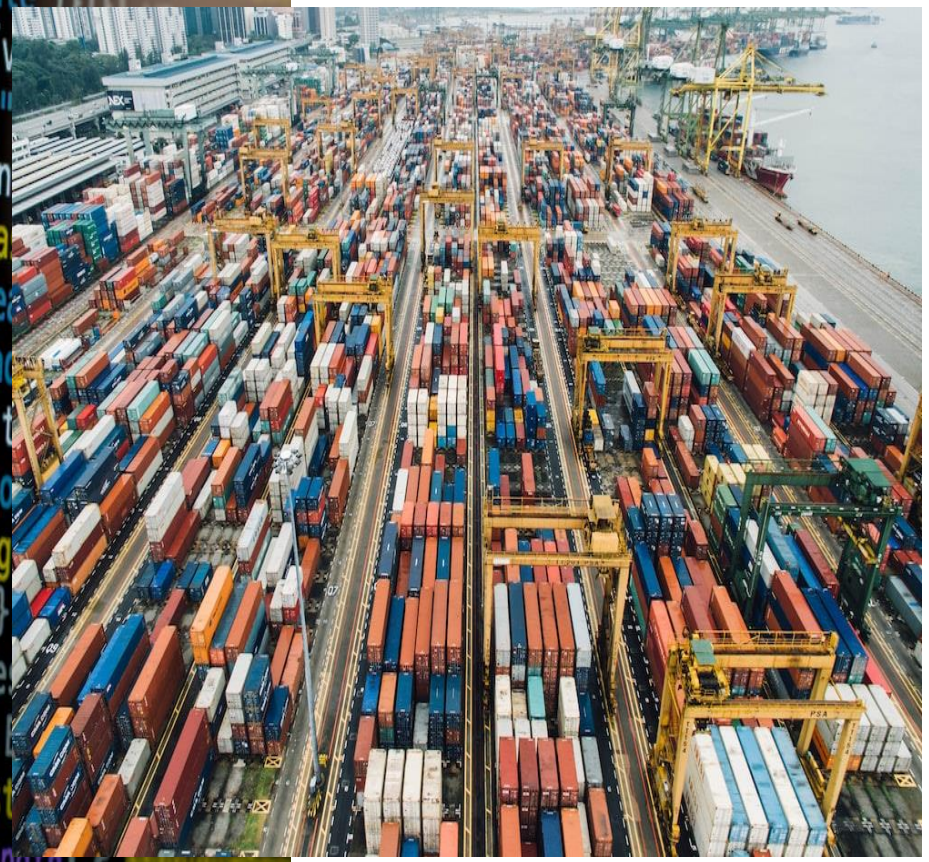
Trust from the foundation, up and down the stack and supply chain

source





source



source

The rising tide lifts all boats

Best Practices for Open Source Developers

This group works to provide open source developers with best practices recommendations, and easy ways to learn and apply them.

GitHub | Slack | Email List

Securing Critical Projects

This group exists to identify and help to allocate resources to secure the critical open source projects we all depend on.

GitHub | Slack | Email List

Supply Chain Integrity

This group is helping people understand and make decisions on the provenance of the code they maintain, produce and use.

GitHub | Slack | Email List

Identifying Security Threats in Open Source Projects

This group enables informed confidence in the security of OSS by collecting, curating, and communicating relevant metrics and metadata.

GitHub | Slack | Email List

Security Tooling

This group's mission is to provide the best security tools for open source developers and make them universally accessible.

GitHub | Slack | Email List

Vulnerability Disclosures

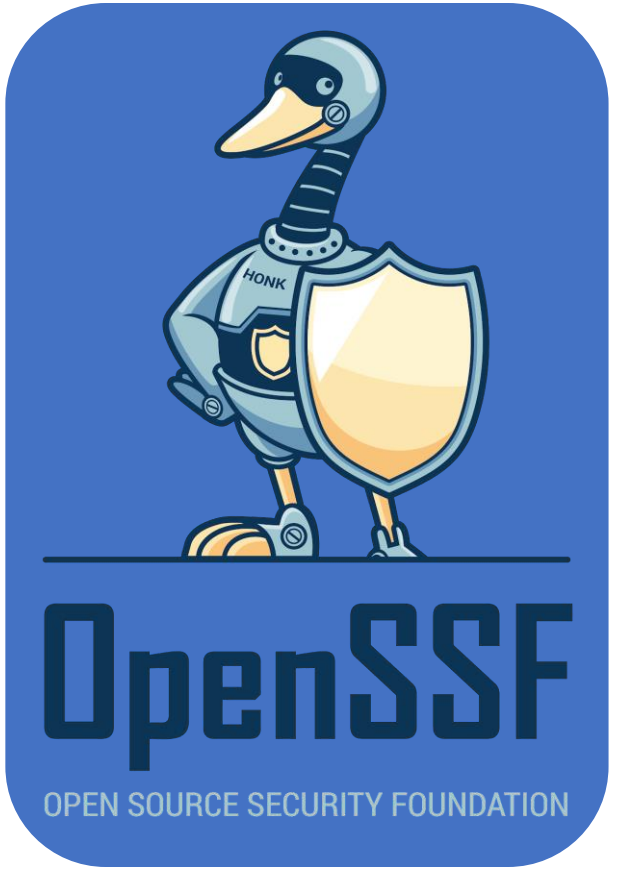
This group is improving the overall security of the OSS ecosystem by helping advance vulnerability reporting and communication.

GitHub | Slack | Email List

Specific Initiative Funds

In addition to the core working groups, OpenSSF is home to important, cross-cutting initiatives and projects that require focused resources and staff. SIFs leverage OpenSSF working groups, external open source projects, and member contributions to make a big impact on the open source ecosystem. Current SIFs are:

- Sigstore
- Project Alpha-Omega
- GNU Toolchain Infrastructure – coming soon



https://openssf.org/community/openssf-working-groups/

Someone IS doing something! (and you can help out, too!)

https://openssf.org/oss-security-mobilization-plan/

Eric S. Raymond, one of open source's founders:

"Given enough eyeballs, all bugs are shallow."

He called it "Linus's Law."


We Are
Building Trust
@OpenAtIntel
open.intel
THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
EUROPE