

JOHAN LINÅKER

HASMOSS - Health and Security Management for Open Source Software

Open Source is a building block

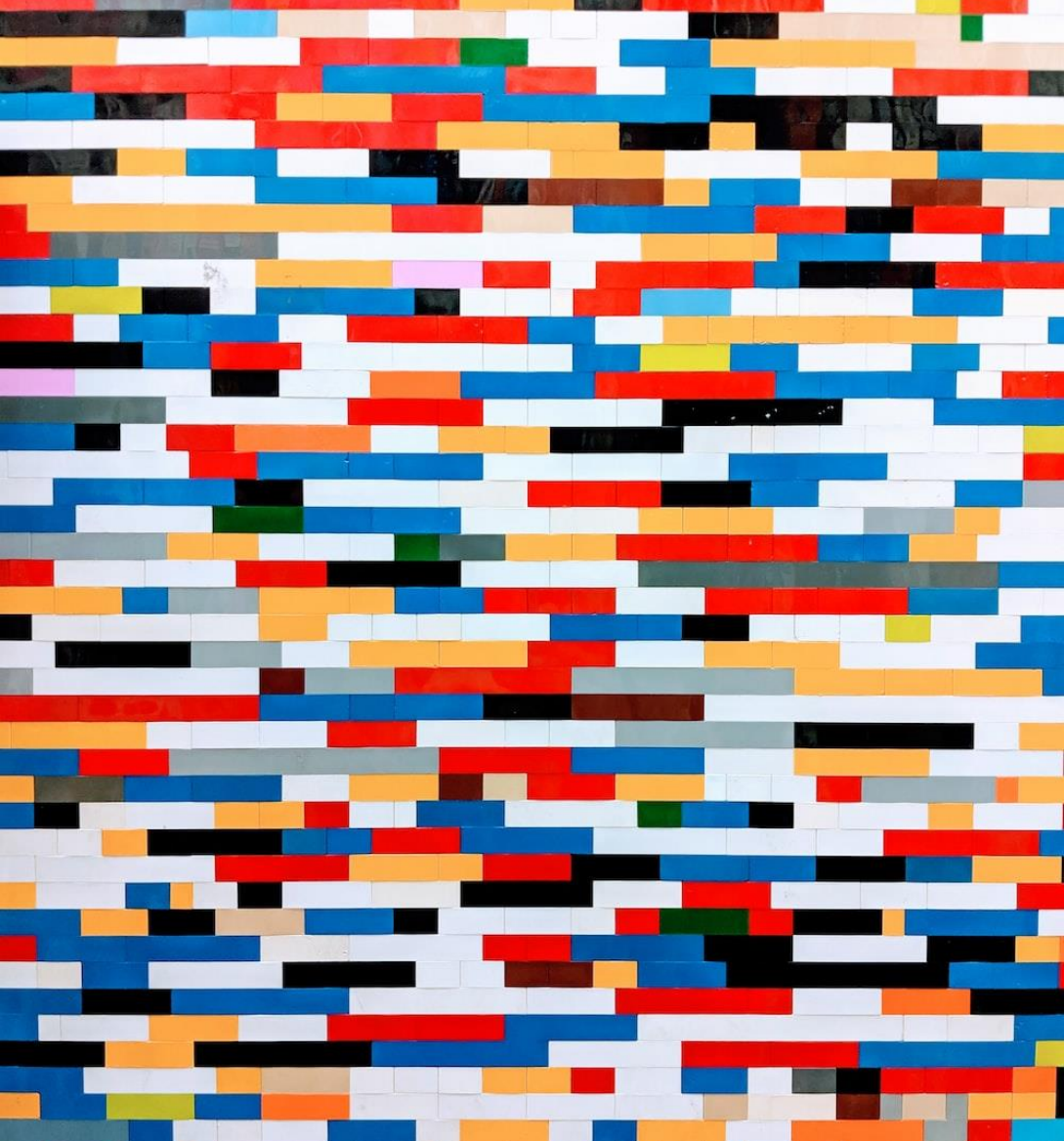
- A means to create, share, and distribute reusable and modifiable bricks
- Present in > 90 % of today's software
- But who guarantees their quality and that they are safe to use?







Photo by Xavi Cabrera | <https://unsplash.com/photos/kn-UmDZQDjM>



Open Source Software and our Digital Infrastructure

- Open Source Software makes up a vitale building block in our digital infrastructure
- Needs maintenance as with physical infrastructure to stay secure and robust



Open Source Software and our Digital Infrastructure

- Open Source Software makes up a vitale building block in our digital infrastructure
- Needs maintenance as with physical infrastructure to stay secure and robust



Open Source Software Health

- An Open Source Software project's capability to stay viable and maintained over time without interruption or weakening



Open Source Software Health

- Productivity: There is an active development of the project
- Robustness: The development is open and spread out on several (independent) individuals
- Openness: Users of the project can influence and contribute to the development of the project



How can we find the cracks and bumps before they appear?

How can we avoid them?

How can we mitigate them?



By Considering the Health of Open Source in your Intake Process

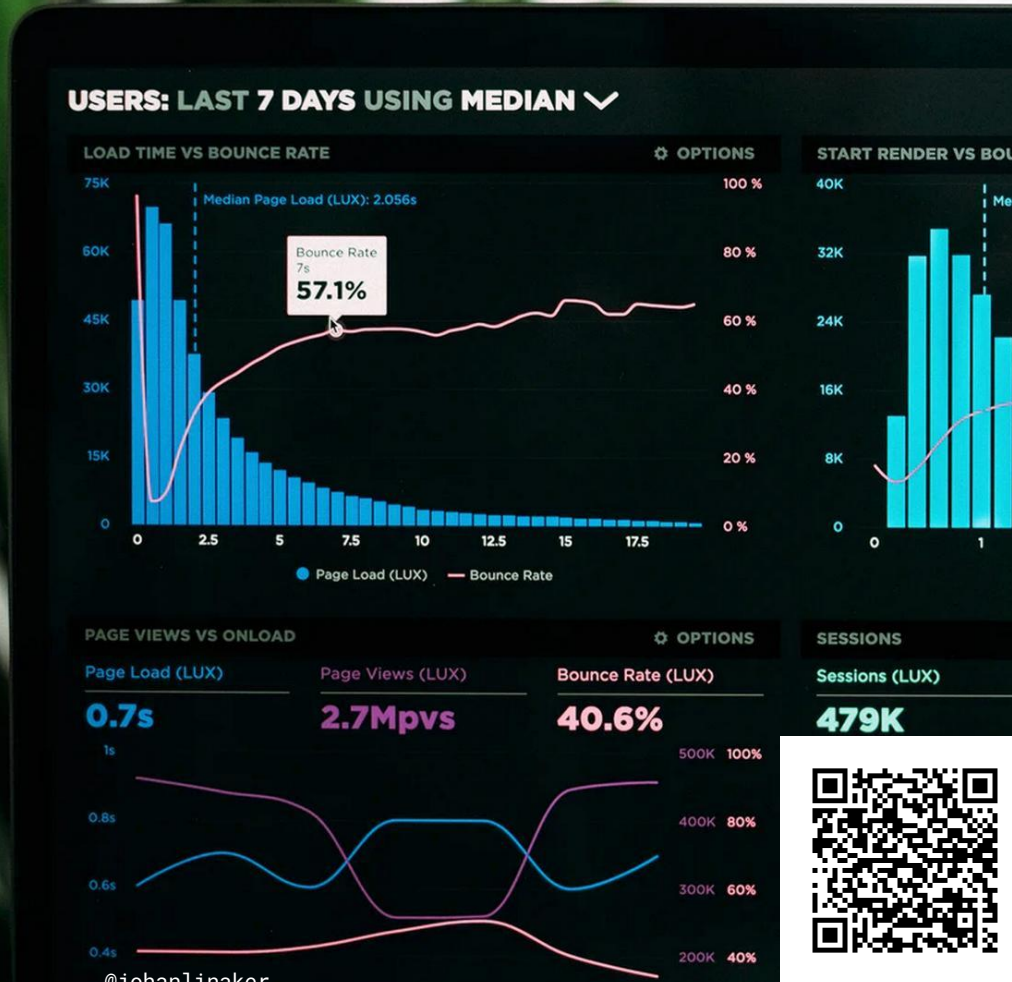
- Goals:
 - Enable health analysis at intake and acquisition of OSS, and ongoing consumption
 - Enable sourcing decisions and proactive health improving measures



* <https://bit.ly/3AM5NR8>



HASMOSS – Health and Security Management for Open Source Software



Partners



SCANIA



debricked

Observers



Ericsson Software Technology





What can we find in literature?

- 146 studies
- 107 characteristics (+associated metrics)
- Divided over 15 themes
- Supplementary material:
<https://doi.org/10.6084/m9.figshare.20137175>
- Paper:
<https://www.ri.se/sites/default/files/2022-09/opensym2022-6%20%281%29.pdf>



@johanlinker

Photo by Jared Craig | <https://unsplash.com/photos/HH4WBGNYltc>



What does practice say?

- Interview survey + case study at Scania
- Validates but narrows down characteristics to smaller groups
- Need for automation
- Need to consider
 - Size & complexity
 - Strategic importance
 - Life-cycle stage
 - Governance and ownership
- Study ongoing

Framework structure

- Level of abstraction
 - Network-level
Characteristics related to the Overarching software ecosystem or network that the OSS project is part
 - Project-level
- Socio-technical dimension
 - Actors
Human and Community-related characteristics
 - Software
Technical and project-related characteristics
 - Orchestration
Governance-related characteristics

Future work

- Gather metrics and data sources from practitioners through observations, and contrast to what we've found in literature
- Investigate applicability and possibility to automate and quantify characteristics with industry partner (ongoing)



