Improving Open Source Security for a Sustainable Open Source Ecosystem

Georg Kunz OSPO @ Ericsson 2023-01-23

Open Source Software won!

But is it sustainable?

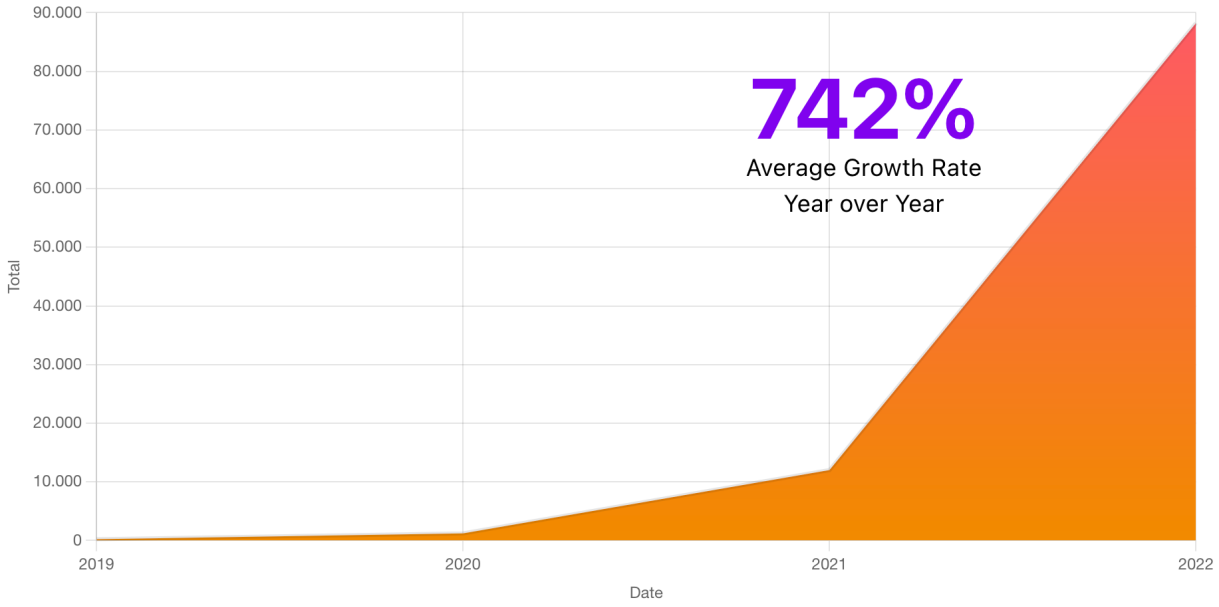
OSPOs need to facilitate open source sustainability!

Securing the supply chain is an immediate contribution to sustainability

Open-Source Security and Sustainability

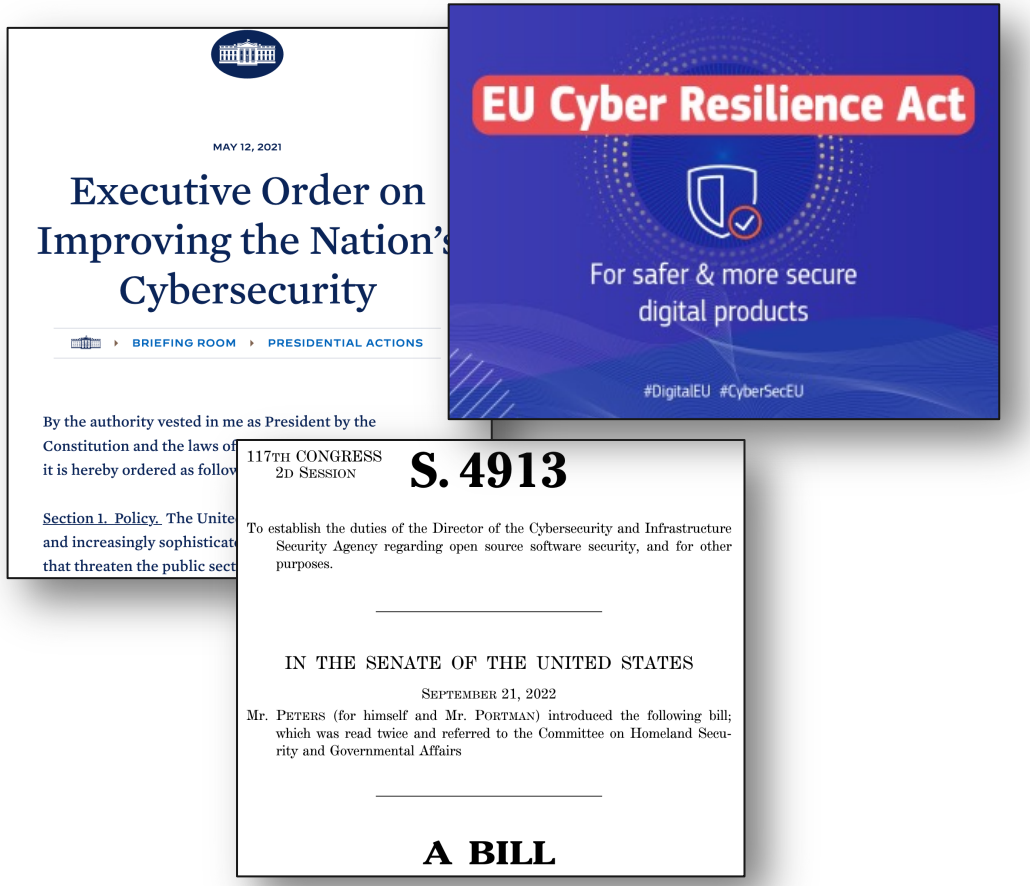
Recent incidents and increasing threat level

FIGURE 1.6. NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS, 2019–2022

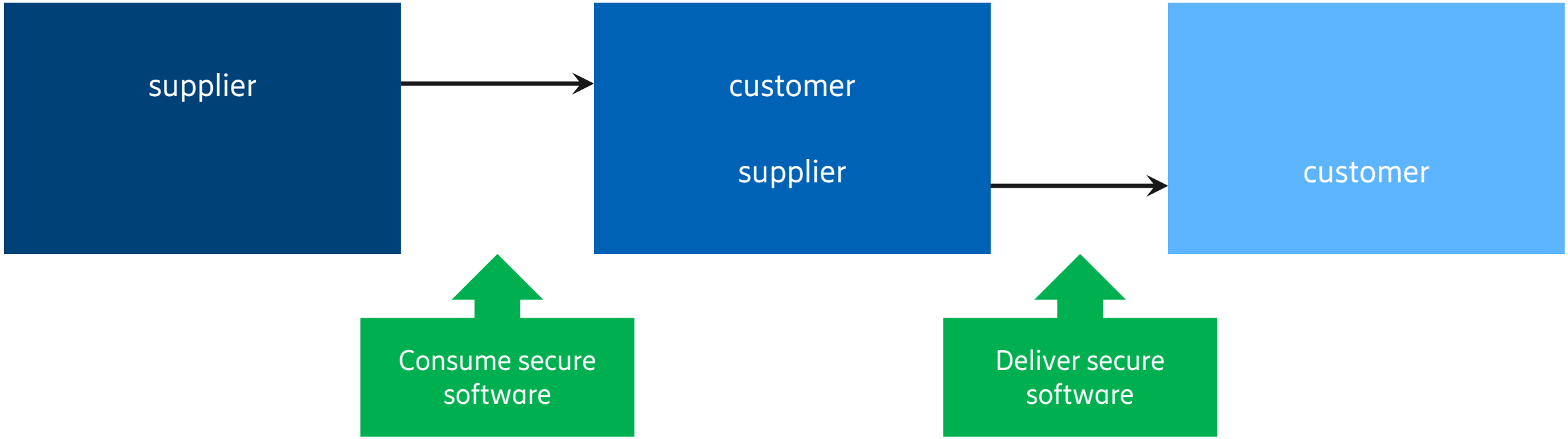


"8th annual State of the Software Supply Chain", Sonatype

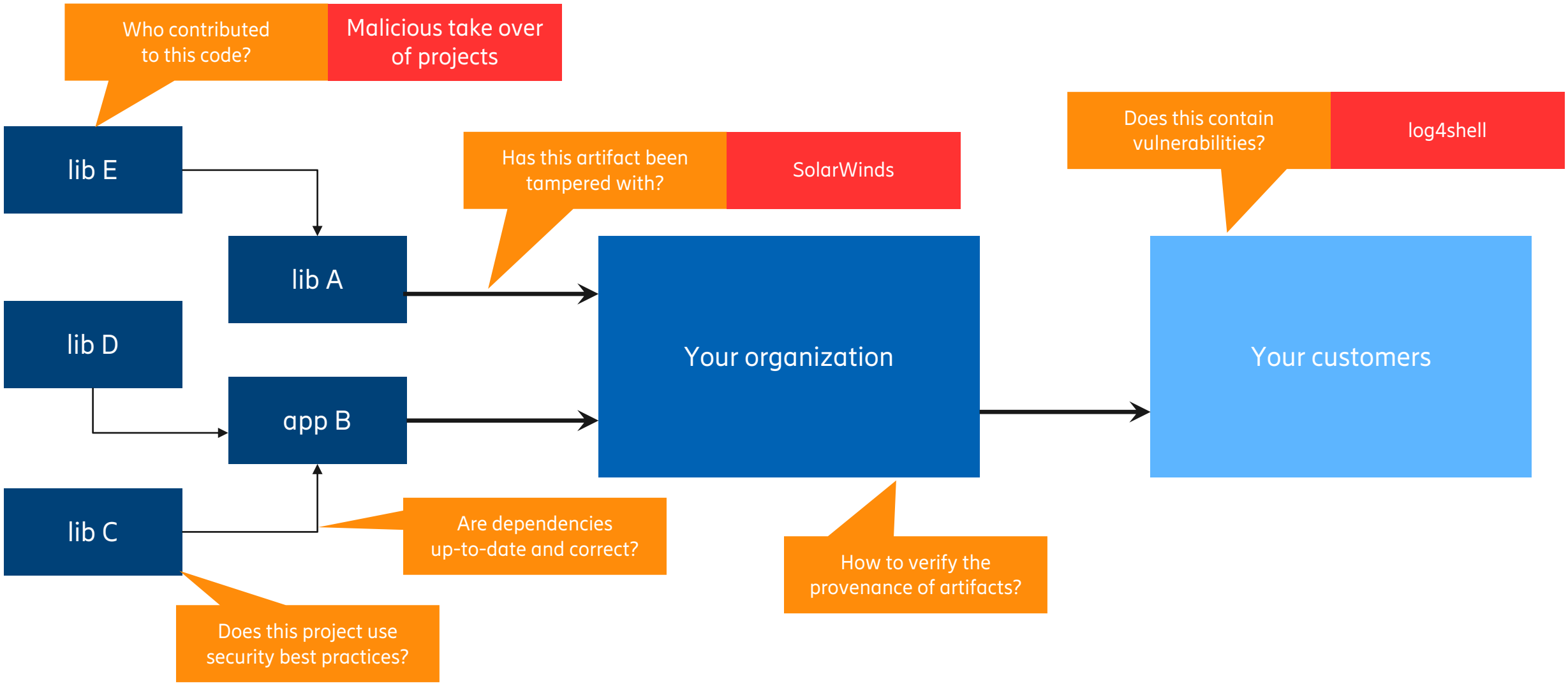
Requirements of Regulators and Customers



Software Supply Chain



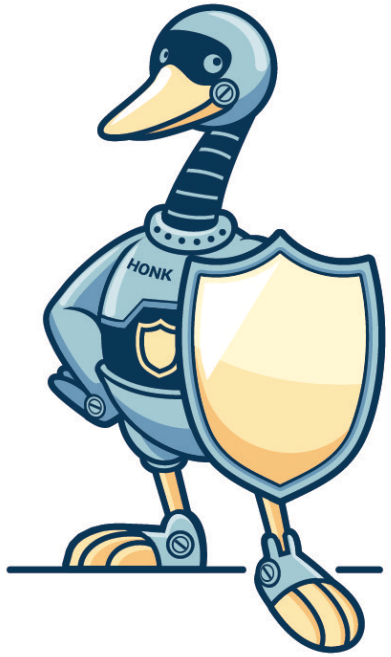
Software Supply Chain – Security Challenges



Software Supply Chain Security Challenges*

- How do we know what's in the software and how to trace vulnerabilities?
- How do we ensure the integrity of software artifacts?
- How can developers learn about security best practices?
- How can we measure and improve the security posture?

* non-exhaustive list



OpenSSF

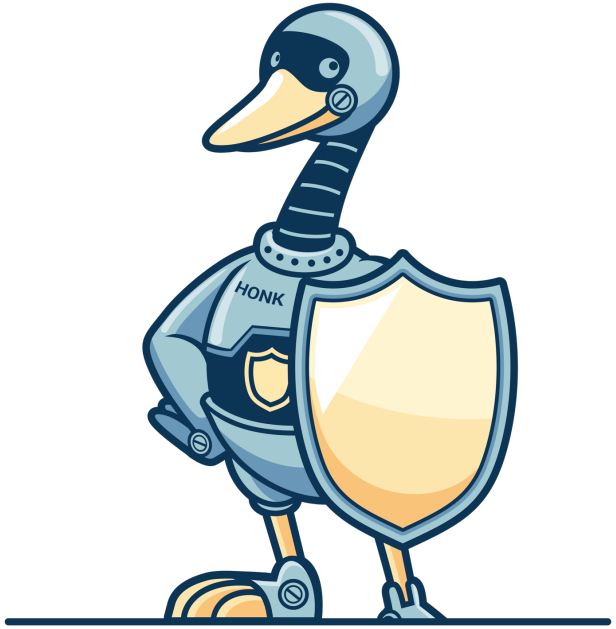
OPEN SOURCE SECURITY FOUNDATION

1Password aws ATLASSIAN CapitalOne cisco citi HUAWEI intel IBM JFrog JPMorgan Chase & Co. Meta

coinbase DELL Technologies ERICSSON Fidelity GitHub Google Microsoft Morgan Stanley ORACLE Red Hat snyk sonatype

About the OpenSSF

- Aims to securing the open source ecosystem by
  - securing investment, resources, and expertise,
  - educating developers in secure software design,
  - establishing best practices in supply chain security,
  - developing and improving tooling for securing software,
  - addressing the security posture of open source projects.



OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Disclaimer

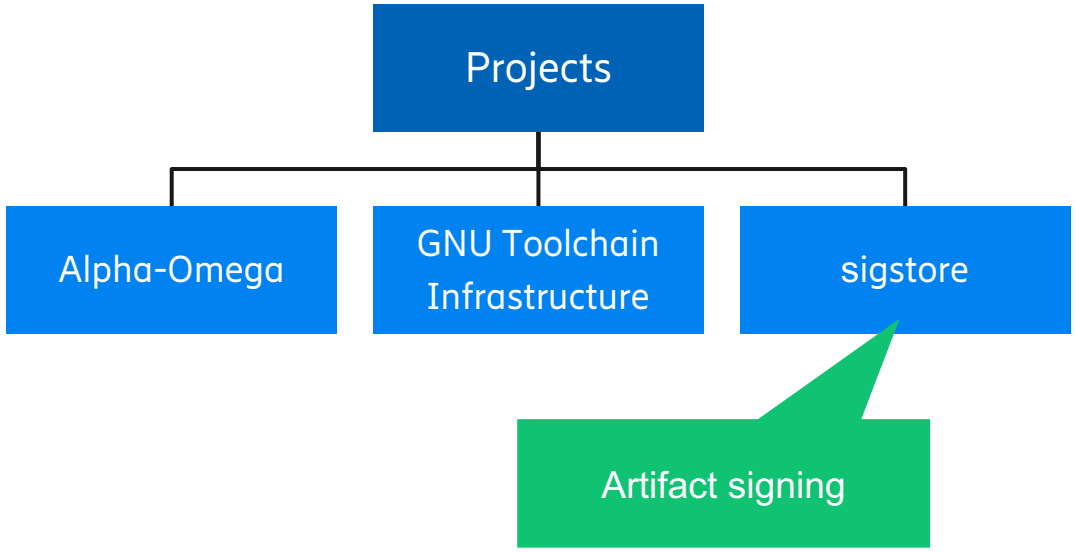
- The supply chain security challenge is broad, wide and deep...

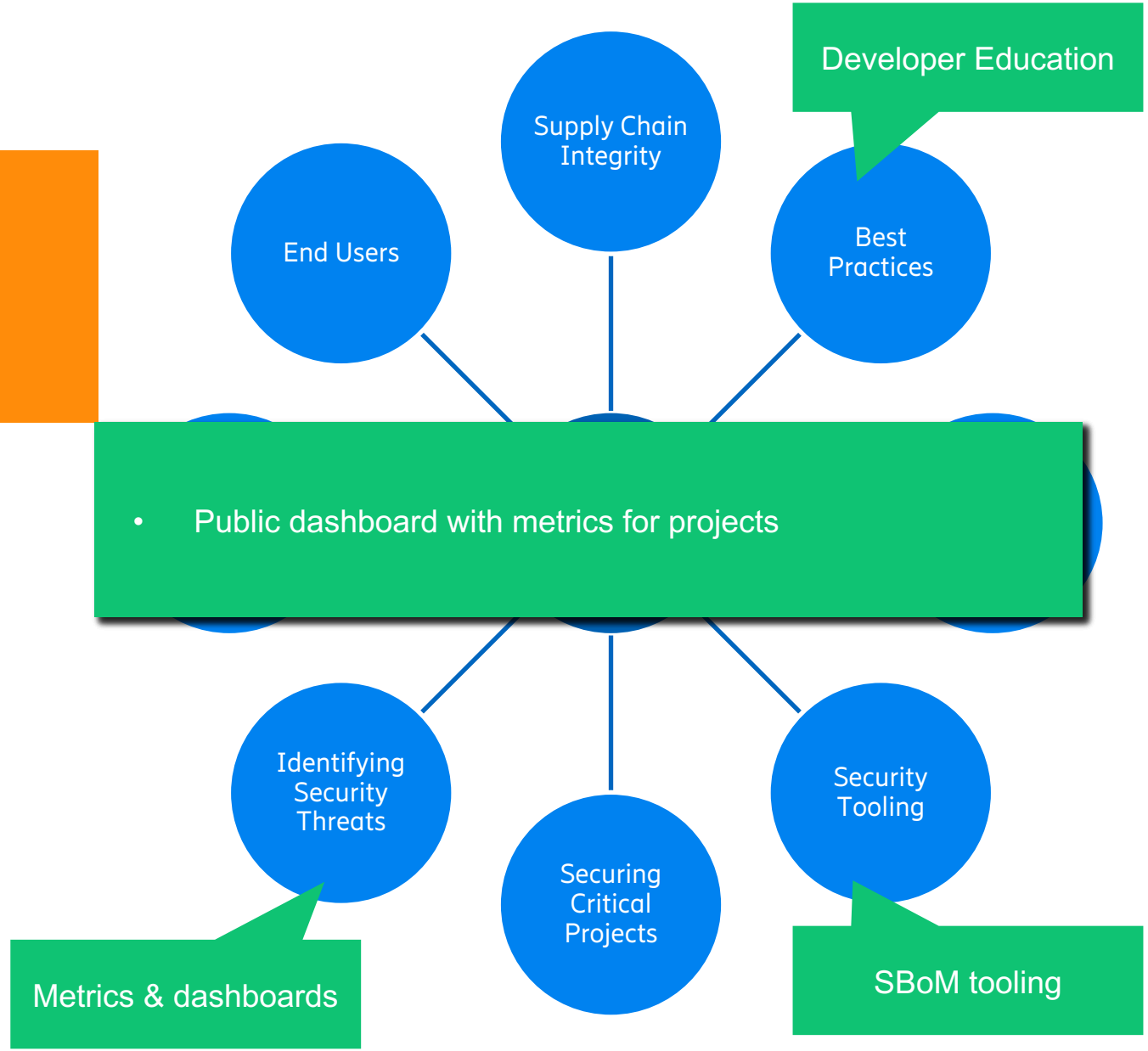
  ... and so are the activities of the OpenSSF.

- I will only be able to dive into a small subset of all activities

OpenSSF Landscape

- How do we know what's in the software?
- How do we ensure the integrity of software artifacts?
- How can developers learn about security best practices?
- How can we measure and improve the security posture?





Best Practices Working Group

- Provide open source developers with best practices and tools
  - Concise Guides + Training
  - Scorecards analysis tool
  - Education SIG
  - OpenSSF Best Practices badge
  - … and more …

Scorecards

- Automatically scores OSS projects based on checks
  - Each related to security, scored `0-10`, weighted average computed

- Value for our OSPO
  - Scorecard provides a list of addressable gaps
  - Framework for guiding contributions and improvements
  - List of tasks to get a development team going

Scorecards Tests

Name	Description
Binary-Artifacts	Is the project free of checked-in binaries?
Branch-Protection	Does the project use Branch Protection ?
CI-Tests	Does the project run tests in CI, e.g. GitHub Actions, Prow?
CII-Best-Practices	Does the project have an OpenSSF (formerly CII) Best Practices Badge?
Code-Review	Does the project practice code review before code is merged?
Contributors	Does the project have contributors from at least two different organizations?
Dangerous-Workflow	Does the project avoid dangerous coding patterns in GitHub Action workflows?
Dependency-Update-Tool	Does the project use tools to help update its dependencies?
Fuzzing	Does the project use fuzzing tools, e.g. OSS-Fuzz?
License	Does the project declare a license?
Maintained	Is the project at least 90 days old, and maintained?
Pinned-Dependencies	Does the project declare and pin dependencies?
Packaging	Does the project build and publish official packages from CI/CD, e.g. GitHub Publishing ?
SAST	Does the project use static code analysis tools, e.g. CodeQL, LGTM (deprecated), SonarCloud?
Security-Policy	Does the project contain a security policy?
Signed-Releases	Does the project cryptographically sign releases?
Token-Permissions	Does the project declare GitHub workflow tokens as read only?
Vulnerabilities	Does the project have unfixed vulnerabilities? Uses the OSV service.
Webhooks	Does the webhook defined in the repository have a token configured to authenticate the origins of requests?

Use Case: Scorecards for metal3

Metal3-io

Metal3 project's own organization.

baremetal-operator

https://github.com/metal3-io/baremetal-operator

Generic score: `5.6`

Check	Score	Finding
Branch-Protection	3/10	CodeOwner review not required in "main", Required reviewers is 0 in "main"
CII-Best-Practices	0/10	Missing self-assessment + badge in README.md
Dependency-Update-Tool	0/10	Configuration not found
Fuzzing	0/10	No fuzzing
Pinned-Dependencies	5/10	Not all deps (Github actions, Dockerfiles) are pinned by hash
SAST	0/10	No SAST checks
Token-Permissions	0/10	Github workflows using token with too many permissions

Best Practices Working Group

- Upcoming activities
  - Guide on recommended compiler flags for C/C++
  - Guide on Software Configuration Mamagement best practices

Tooling Working Group / SBOM Everywhere SIG

- SBOM Everywhere SIG Mission Statement
  - Work within the “evolving” SBOM community to connect and empower that community to create and consume SBOMs. Use the resources available to the OpenSSF to encourage others to cooperate and build the tooling needed for widespread SBOM usage and adoption.

Tooling Working Group / SBOM Everywhere SIG

- Approach
  1. Create a landscape of SBOM tooling, standards, and organizations in the SBOM community
  2. Use OpenSSF resources to encourage SBOM adoption with a focus on creating and consumption
  3. Focus on the near-term wins initially but with end goals in mind
  4. Incentivize and educate producers, consumers, and maintainers to aid adoption of SBOM tooling
  5. Celebrate wins. Make progress and use very visible

See Mission and Purpose document

End Users Working Group

- Purpose
  - Represent the end user's perspective and voice

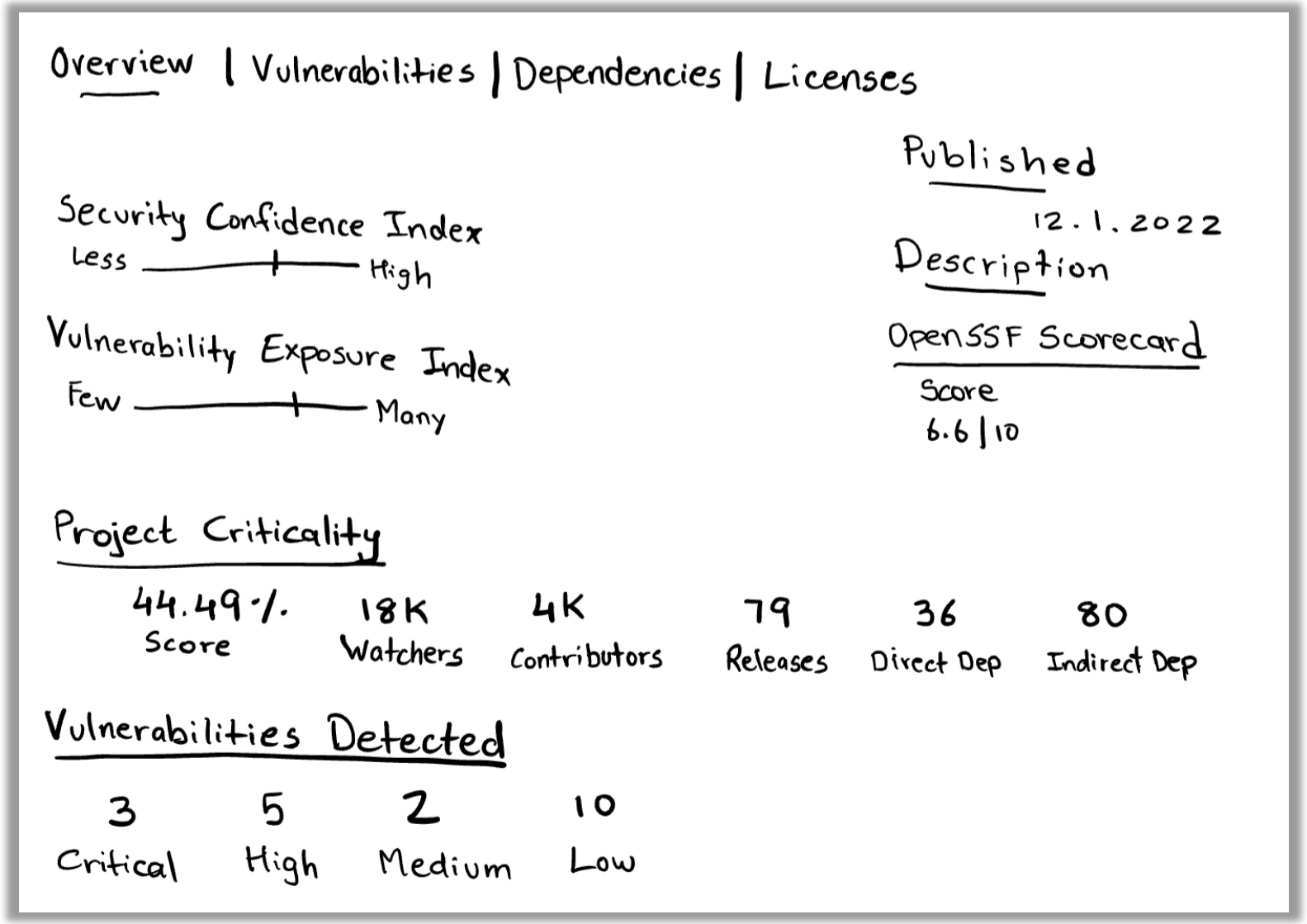
- Current Work Items
  - Taxonomy of software supply chain threats
  - Holistic architecture to address identified threats and map to OpenSSF solutions

- Values
  - Structure complexity of supply chain security
  - Demonstrate the applicability of OpenSSF efforts
  - Facilitate and ease adoption of recommended target solution by end users

Open Source Security Dashboard

- Purpose
  - Provide metrics to help make decisions about using open source software
- Approach
  - Based on existing data OpenSSF Scorecards, OpenSSF Best Practices Badge, LFX, CHAOSS, etc.
- Values
  - Extremely valuable for open source consumption in R&D

Open Source Security Dashboard



TODO Supply Chain Security Working Group

- Proposed Mission
  - Facilitate the support of Supply Chain Security by OSPOs
  - Boosting the sustainability of Open Source Software
- Approach
  - Leverage and compile material for use by OSPOs
  - Bridge between OSPOs and technical communities
- Example artifact
  - Blog post: "How OSPOs Can Be a Key Lever for Open Source Sustainability and Security"
- Discuss and comment on TODO group strategic goals for 2023
  - https://github.com/todogroup/governance/issues/262

Q&A