SBOM + Security = Fun

CNCF Community Salzburg, 2022-03-01

Christian Köberl

All-end developer and software gardener.

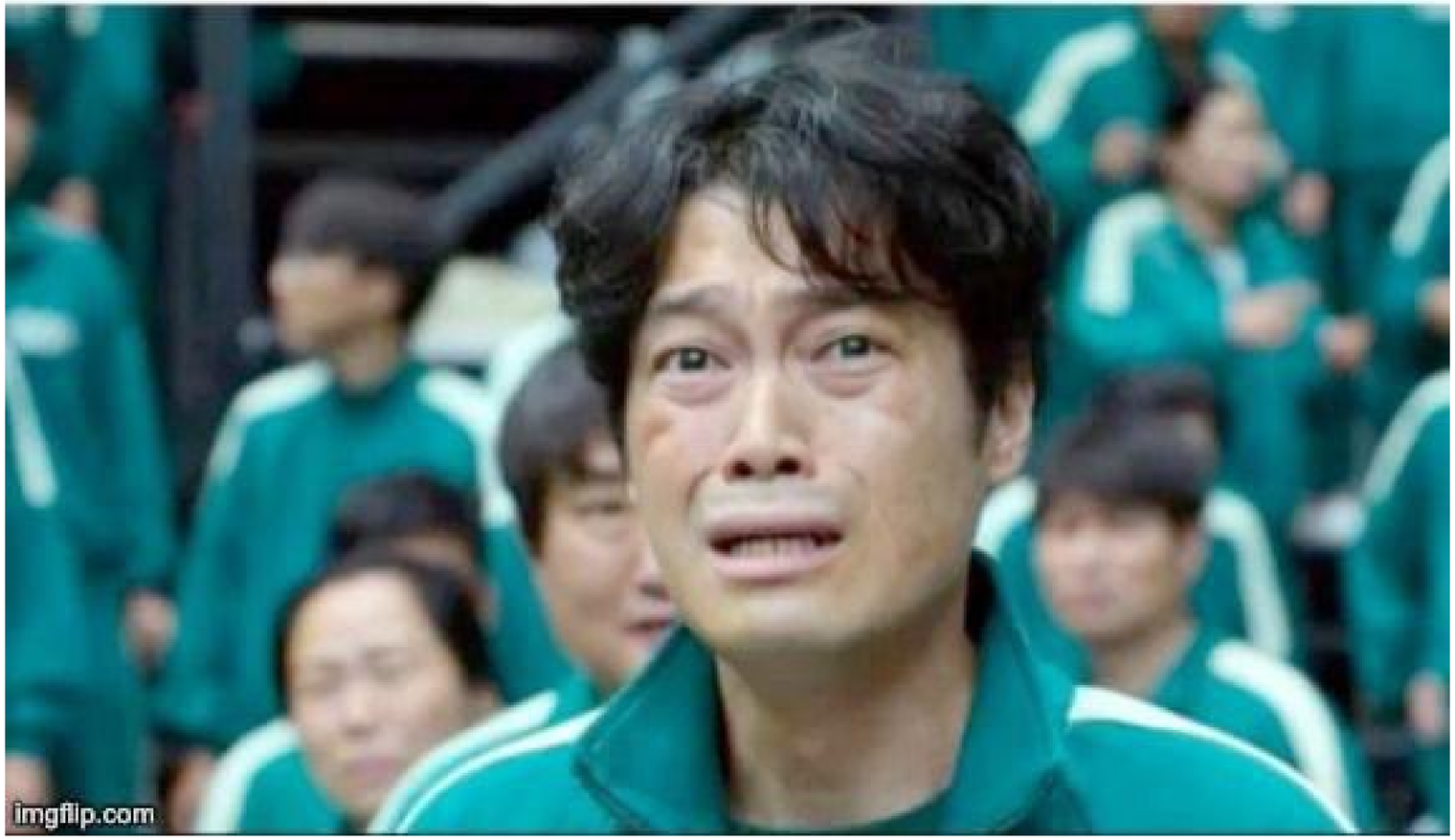
Chief Technical Architect @ Porsche Informatik.

derkoe

derkoe

derkoe.dev

Your next task is to
figure out which applications
in your org use log4j



What is a Software Bill Of Materials (SBOM)?

- List of all software components (aka dependencies)
- Including versions
- Including all transitive dependencies
- Usually also including the license

SBOM Standards

The Software Package Data Exchange® (SPDX®)

An open standard for communicating software bill of material information, including components, licenses, copyrights, and security references.

CycloneDX

OWASP CycloneDX is a lightweight Software Bill of Materials (SBOM) standard designed for use in application security contexts and supply chain component analysis.

syft

"A CLI tool and Go library for generating a Software Bill of Materials (SBOM) from container images and filesystems."

- Scans the file system recursivley for packages (finds packages in packages).
- Creates reports in different formats: SPDX, CycloneDX, JSON (syft)
- No licenses are detected (except OS packages)
- Grype security scanner builds on top of syft

Demo

syft as CLI

SBOM Operator

- https://github.com/ckotzbauer/sbom-operator
- Kubernetes operator
- Scans images of all Pods with syft
- Stores results in Git or OWASP Dependency Track

Demo

syft Kubernetes Operator

Sources

- OWASP CycloneDX
- Understanding SBOM standards: CycloneDX, SPDX, SWID
- https://www.cisa.gov/sbom
- Executive Order on Improving the Nation’s Cybersecurity
- https://github.com/anchore/syft
- Open Source Security Podcast