SPDX SBOMs
Enabling Automation of Safety & Security Analysis

- Software in critical systems
  - Mix of open + proprietary
    - Healthcare, food, energy

98% 70%
98% codebases contain OSS, 70% OSS on average

SBOM: Formal recording of details + supply chain relationships of components used in building software

Should be thinking about SBOM when thinking about requirements. Get visibility by having traceability from inception all the way to the end.

SPDX 3.0 will support extensions to protect elements

6 SBOM types
  - Design
  - Source
  - Build
  - Deploy
  - Runtime
  - Analyze

Collaborations welcome as SPDX 3.0 work continues

Wild West of SBOM data

DevSecOps pipeline supports traceability

SW Lifecycle
- Source → Procure
- Develop
- Build
- Test
- Release
- Plan
- Migrate
- Retire
- Deployed
- Install
- Configure

Safety Standards
- Unique ID
- Documentation
- Component dependencies
- Requirements

SPDX software package data exchange
- Open source
- Product that improves continuously

OSS component growth
2016: 84, 2020: 528

COMING SOON
- More use cases
- Simplification
- Flexibility