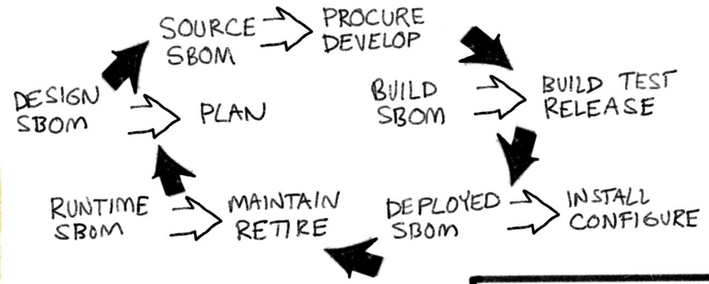
KATE STEWART

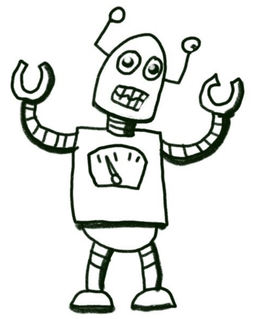
SPDX SBOMs

ENABLING AUTOMATION OF SAFETY & SECURITY ANALYSIS

SBOM: FORMAL REORDING OF DETAILS + SUPPLY CHAIN RELATIONSHIPS OF COMPONENTS USED IN BUILDING SOFTWARE

SW LIFECYCLE





- SOFTWARE IN CRITICAL SYSTEMS

⇒ HEALTHCARE FOOD ENERGY

MIX OF OPEN + PROPRIETARY

98% CODEBASES CONTAIN OSS

70% OSS ON AVERAGE

SHOULD BE THINKING ABOUT SBOM WHEN THINKING ABOUT REQUIREMENTS

GET VISIBILITY BY HAVING TRACEABILITY FROM INCEPTION ALL THE WAY TO THE END

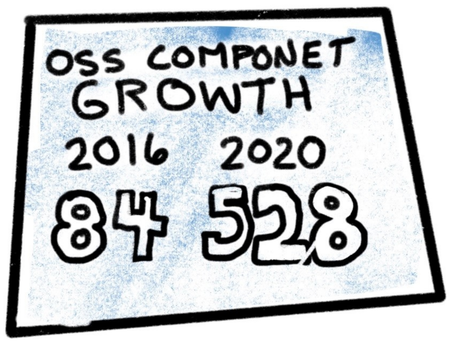
SAFETY STANDARDS

- UNIQUE ID
- DOCUMENTATION
- COMPONENT DEPENDENCIES
- REQUIREMENTS

SPDX **3.0** WILL SUPPORT EXTENSIONS TO PROTECT ELEMENTS

SPDX SOFTWARE PACKAGE DATA EXCHANGE

OPEN SOURCE PRODUCT THAT IMPROVES CONTINUOUSLY

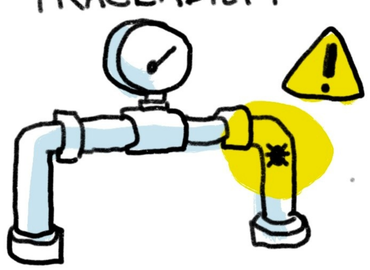


6 SBOM TYPES

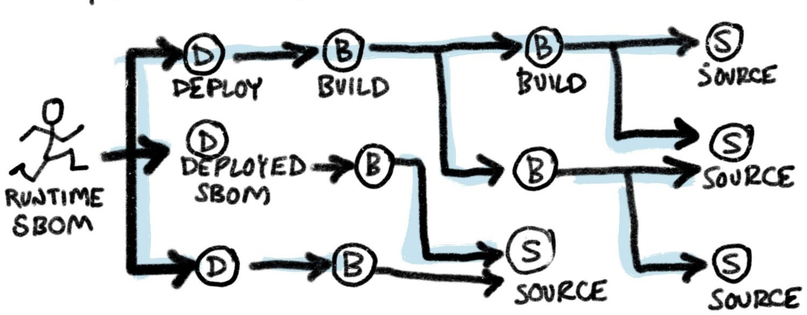
- DESIGN
- SOURCE
- BUILD
- DEPLOY
- RUNTIME
- ANALYZE

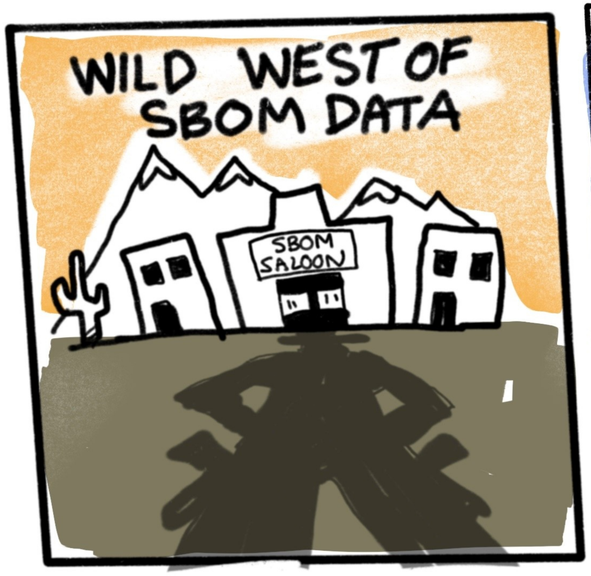
COLLABORATIONS WELCOME AS SPDX 3.0 WORK CONTINUES

DEVSECOPS PIPELINE SUPPORTS TRACEABILTY



TRACEABILTY





COMING SOON

- MORE USE CASES
- SIMPLIFICATION
- FLEXIBILITY