Contribution ID: **8** Type: **not specified**

Software Bill of Material Deep Dive

Sunday 8 October 2023 14:40 (30 minutes)

Supply chain attacks have surged since 2013, offering attackers an easy and lucrative method to breach vital organizational functions. In the past four years alone, notable supply chain attacks have grown fourfold. This trend is predicted to persist unless effective countermeasures are embraced. In the realm of open science, the heavy dependence on open-source code for scientific software development, coupled with diverse technology use in extensive deployments, presents challenges for asset owners to evaluate and eliminate potential vulnerabilities.

New regulations from the US government (White House executive order EO14028) and the EU commission (E.U. Cyber Resilience Act) now require Service and Equipment suppliers involved in government contracts to publish SBOMs for their commercial products. These SBOMs must adhere to a standardized and openly accessible data format, and support automated identification of existing or potential vulnerabilities, along with strategies for effective mitigation.

This presentation will focus on open-source tools and workflows that leverage SBOM standards and help the CERN Accelerator and Technology Sector inventory and manage vulnerabilites across the multiple platforms and programming languages it employs for its operational software.

Author: COPY, Brice (CERN)

Presenter: COPY, Brice (CERN)