



Contribution ID: 19

Type: **not specified**

Building vs. Buying –A Tale of Developing an In-House SCA Tool

Tuesday 10 June 2025 11:15 (45 minutes)

This presentation will detail the journey of developing an in-house Software Composition Analysis tool, from its inception as a challenge to its realization as a comprehensive, open-source solution. It will cover the motivations, challenges, and unique features of the tool, including dependency checks, custom dashboards, and automatic updates.

In-depth Description:

Diogo Lemos and his team took on the challenge of developing an in-house Software Composition Analysis (SCA) tool rather than opting for market solutions. This presentation will cover the journey of three application security engineers who decided to build a comprehensive, free, and open-source SCA tool. Diogo will discuss the motivations behind this project, the challenges faced, and the unique features of their tool, including custom dashboards, dependency checks, and automatic update features. The talk will also highlight the implementation of a scoring system to assess the security posture of projects.

Innovation and Relevance:

This presentation showcases an innovative approach to software security by detailing the development of a proprietary SCA solution. It highlights the relevance of custom tools in today's security landscape, where tailored solutions can offer significant advantages over commercial products.

Key Takeaway:

Discover the benefits and challenges of developing a custom, open-source Software Composition Analysis tool, including unique features such as dependency checks, automatic updates, and a security scoring system.

Tool Release Announcement:

We will be releasing the Custom Software Composition Analysis (SCA) Tool, an innovative open-source solution designed to enhance software dependency management with features for automated updates, vulnerability assessments, and customized reporting.

Length

45 minutes

Optional: Speaker / convener biography

Primary author: LEMOS, Diogo

Session Classification: Talks

Track Classification: Talks and presentations