Partner Use Case

Robert Bosch GmbH

AI Working Group

Starting point

AI brings novel and unprecedented challenges for security engineering. Systems are no longer developed but trained, which offers additional risks and concrete attack vectors via the data supply chain and data attacks.

Objectives

Bosch has started an activity with partners from industry (Siemens, SAP, and BASF), the Digital Trust Forum, and the German electronics association VDE for making AI trustworthy and communicate these efforts via an AI Trust Label. The process of establishing this label at the European level is ongoing. This will allow future product differentiation with dimensions like “transparency, privacy, fairness, …” that make “trust” concrete and tangible. We contributed this activity in the CoT and established with Siemens a AI working group, as we see it fully in line with Charter of Trust’s objectives and a useful step in extending CoT’s footprint in AI protection and AI trustworthiness.

Description

The approach which CoT’s AI Working Group is following is based on the VCIO approach: Values are defined by criteria, and there are indicators and observables of how these values can be detected in a practical setting. Checklists are provided for five dimensions of digital trust with checklists that help identify and rank observables. By applying this approach companies can prepare themselves for upcoming regulation by the AI Act.

Lessons learned/results

Bosch has applied this approach to various projects within different businesses divisions. As the approach can be coupled with existing quality management processes, the additional overhead is neglectable compared with setting up dedicated AI quality assurance processes from scratch. We therefore recommend this approach for other businesses as well.