Investigating Generative AI's Impact on Software Organizations' Security Practices: A Multi-Case Study Using Gioia Methodology

About

This study investigates how generative AI can enhance software security practices through a multi-case study involving five different software organizations. Using semi-structured interviews with developers and managers, the research identifies key areas where AI can provide support, while also uncovering the sociotechnical risks that may hinder its adoption.

Problem

Software organizations face a rising number of security threats, and manual security processes are often time-consuming, error-prone, and expensive. While generative AI offers a promising solution to enhance security, its practical impact and the associated risks for software organizations remain largely underexplored.

Study Outcome

- Generative AI can enhance four key security practices: threat assessment, security testing, operational management, and education & guidance.
- Significant sociotechnical risks impede AI adoption, including concerns about inadequate data management, inaccurate AI outputs, and a lack of trust and transparency.
- Key identified risks include insufficient data management, data poisoning, lack of control, and limited data novelty.
- The study proposes a theoretical model that highlights the balance between the perceived benefits and risks of adopting generative AI in security workflows.
- Practitioners must balance AI-driven efficiency with effective risk management, as human validation of AI outputs remains necessary.

Keywords

Generative AI • Security Practices • Software Security • Multi-case study • Gioia Methodology • Sociotechnical Risks • OWASP SAMM