AI-Enhanced Application Security: A Modern Approach

OWASP Frankfurt

26.04.2023

Presenter: Diana Waithanji

Agenda

- Benefits of using AI in AppSec
- Limitations of using AI in AppSec
- Addressing the challenges

Diana Waithanji

Believes that data security is a human right

Cybersecurity engineer at SAP SE

OWASP Member

@DianaWaithanji

Diana Waithanji

Views are my own

“As we rely more and more on technology to secure our information and infrastructure, we must use every tool at our disposal to protect ourselves, including AI”

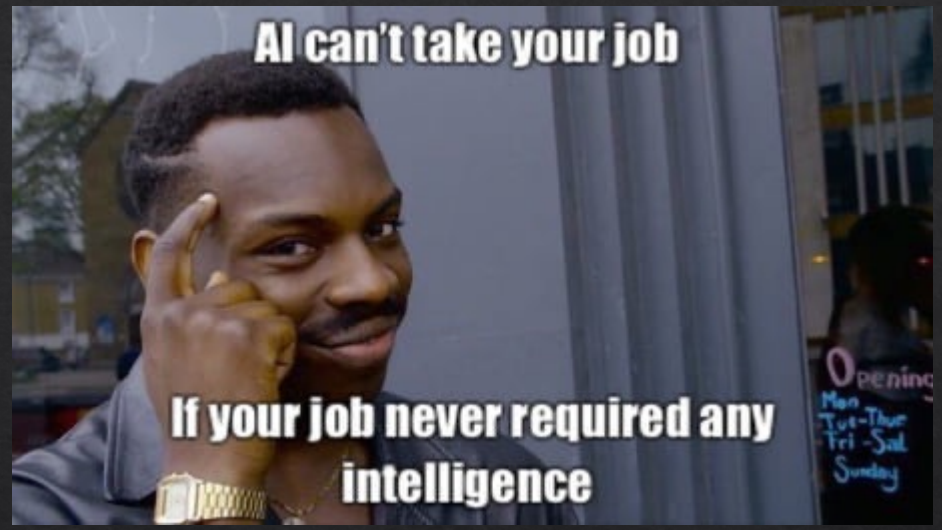
Fei-Fei Li, Co-Director of the Stanford Institute for Human-Centered Artificial Intelligence

Benefits of using AI in AppSec

- Improved threat detection
- Faster response times
- Better accuracy
- Reduced costs

Limitations of using AI in AppSec

- Lack of training data
- False positives
- Limited domain knowledge
- Ethical concerns



Addressing the challenges

- AI algorithms are trained
- Human oversight and intervention
- Ongoing testing and evaluation

Summary

- Benefits of AI: improved threat detection, faster response times, better accuracy, reduced costs
- Management buy-in is key
- OWASP AI Security and Privacy Guide

"In the age of AI, cybersecurity is a race between attackers and defenders. The side with the best AI algorithms will win." - Rodney Joffe, Senior Vice President and Fellow at Neustar

Danke! Asanteni!

Twitter @DianaWaithanji