Will The Real ‘Shift-Left’ Please Stand Up?

Brought to you by mend.io
Tonight’s Agenda

- Introductions
- What is AppSec?
- Shift-Left Historically
- Shift-Left 2.0
- Demonstration
Introduction - Speaker

Lives in Oxford, UK
Worked for Mend for over 2 years
Enjoy a challenge!

Nicholas Shamsfard
Sales Engineer – Nordics & BeNeLux
Introduction – Mend.io

Founded in 2011

1000+ Customers

Over 1.4m End Users
What is AppSec?
AST Tools Pyramid

Reference: capgemini.com/2021/04/false-positives-in-web-application-security-take-up-the-challenge/
Where We Have Come From?

Security mainly centered around network and perimeter defenses.

Emergence of automated SAST and DAST tools.

CICD practices become more widespread, influencing AppSec processes.

Growing interest in DevSecOps as a holistic approach to integrate security seamlessly into the development process.

Enhanced use of automation and machine learning for threat detection and response.

- **<2000**
  - The Open Web Application Security Project (OWASP) is founded in 2001, becoming a central resource for AppSec best practices.

- **2000s**
  - Adoption of the Software Development Life Cycle (SDLC) security, promoting secure coding practices from the beginning.

- **<2010s**
  - Emphasis on secure coding education for developers.

- **Mid-2010**
  - Greater collaboration between development, operations, and security teams to ensure a more cohesive and proactive AppSec approach.

- **Late 10’s**
  - CI/CD practices become more widespread, influencing AppSec processes.

- **2020**

- **Now**

- **Late 20’s**
AppSec Traditional Approach vs Shift-Left

Source: van der Cruijsen 2017.
Shift-Left History
This isn't even DevOps

First example related to DevOps/Software Development

"Shift-left testing is how I refer to a better way of integrating the quality assurance (QA) and development parts of a software project."
None Of These Qualify As Shift-Left

- Just enough coverage
- Piecemeal approach
- Poor workflow
- Manual Approaches
- Stuck in reactive mode
Defining Shift-Left 2.0

- Cover majority of applications
- Automatic Enrollment
- Defined remediation strategy
- Pro-active
- Little Human Interaction
- Little/No Reliance on early SDLC
ONE TEAM. ONE MISSION. ONE PLATFORM.

RENOVATE  SCA  CONTAINER  SAST
Demo Time!
Free Tools You Can Use

- SCA - Renovate
- SCA - OWASP DT
- DAST - OWASP ZAP/Nuclei
- SAST - OWASP Lists
Questions?