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

Nicholas Shamsfard
Sales Engineer – Nordics & BeNeLux

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

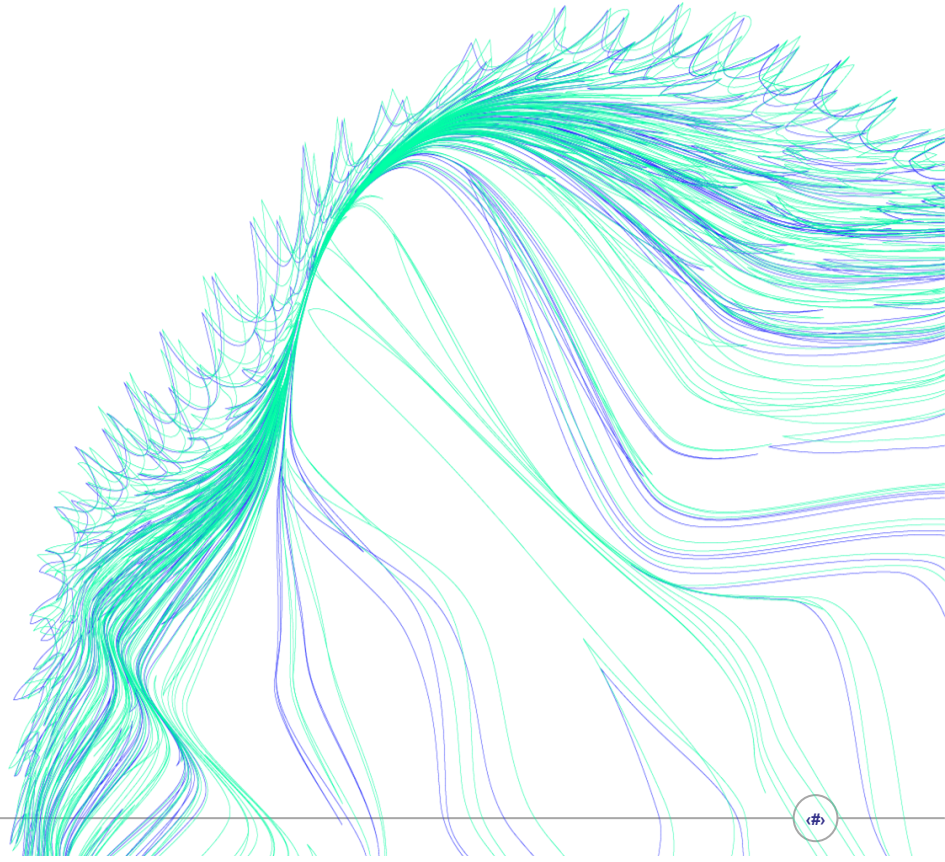
Introduction – Mend.io

Founded in 2011

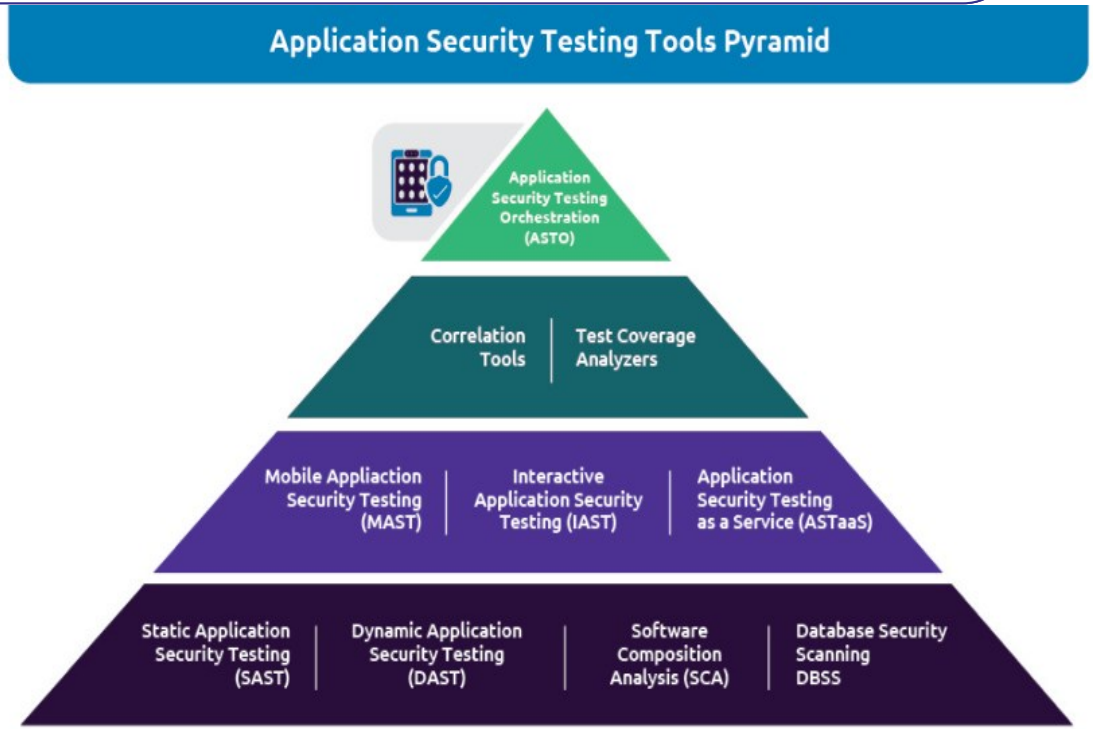
1000+ Customers

Over 1.4m End Users

What is AppSec?

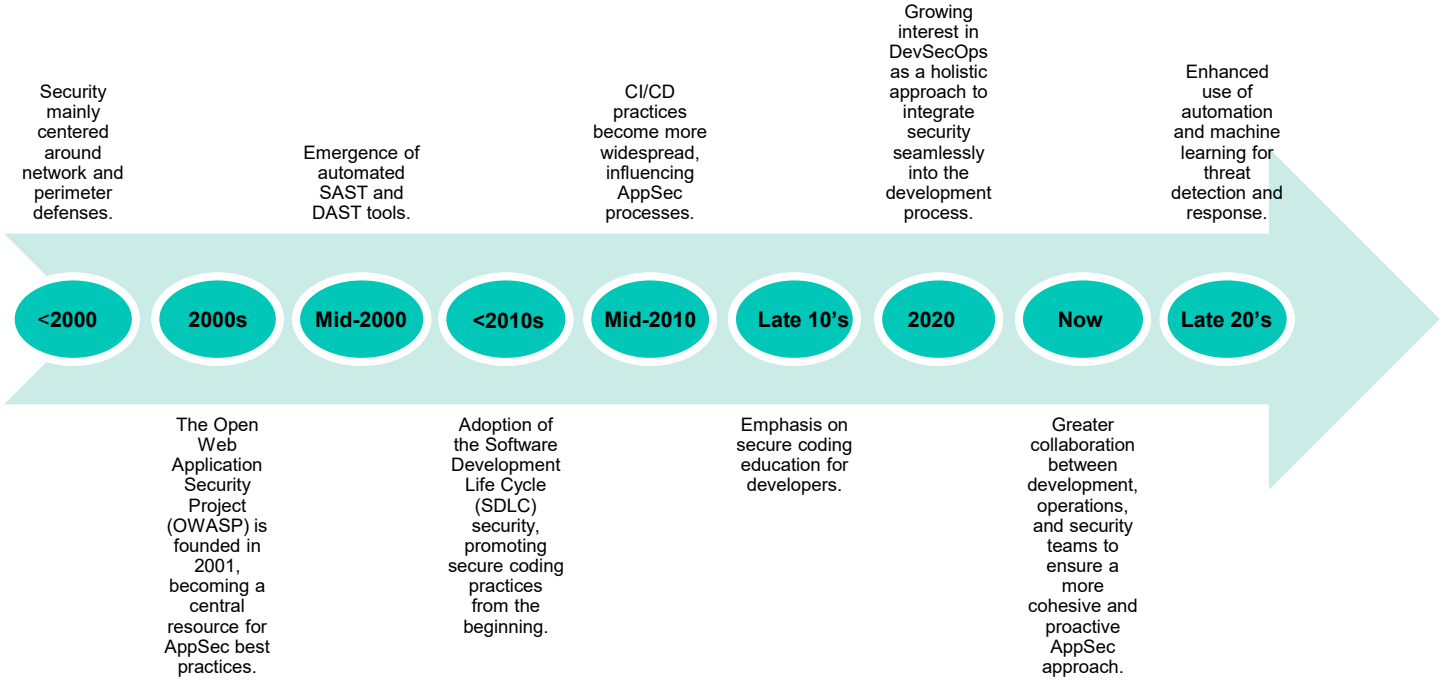


AST Tools Pyramid



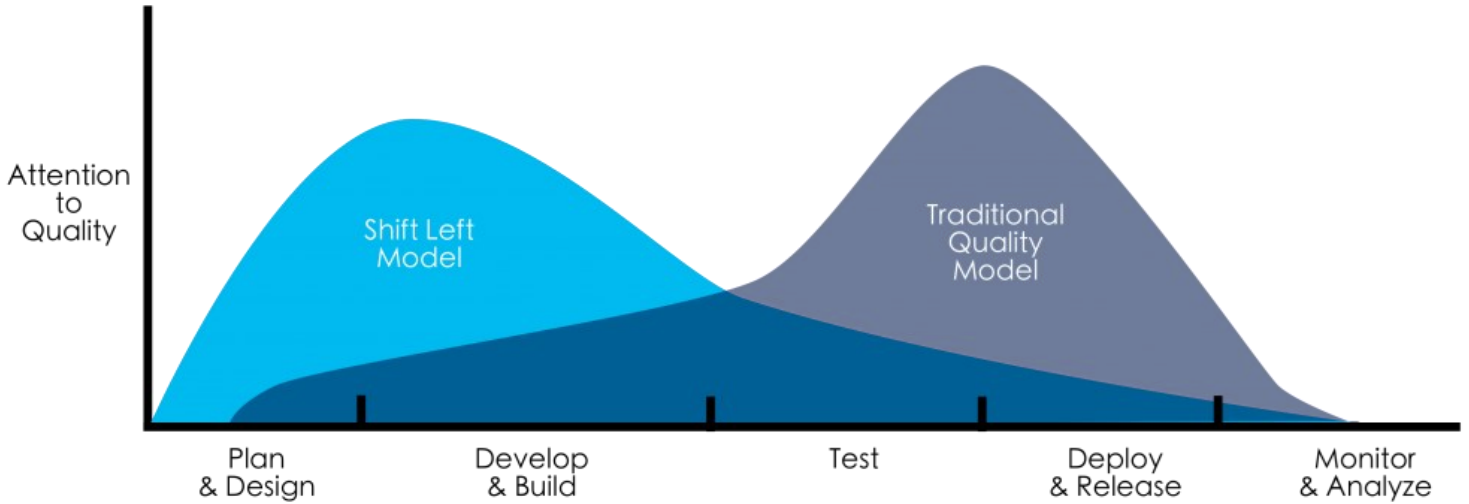
Reference: capgemini.com/2021/04/false-positives-in-web-application-security-take-up-the-challenge/

Where We Have Come From?



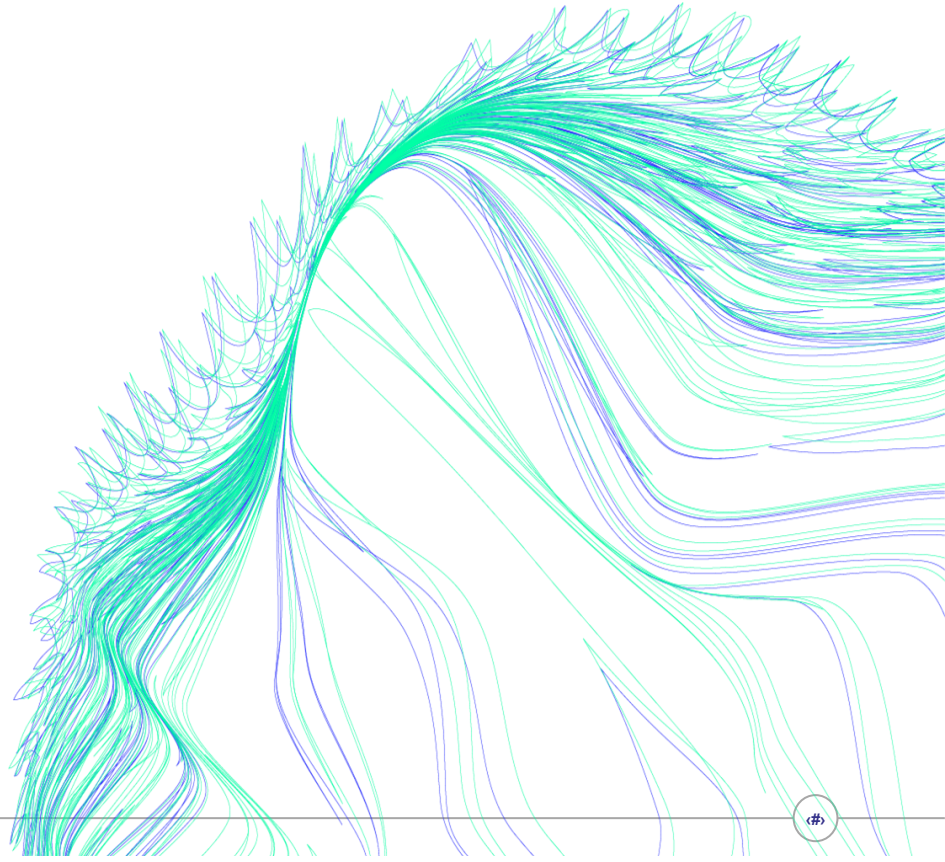
Whitepaper Mind Cloud

AppSec Traditional Approach vs Shift-Left

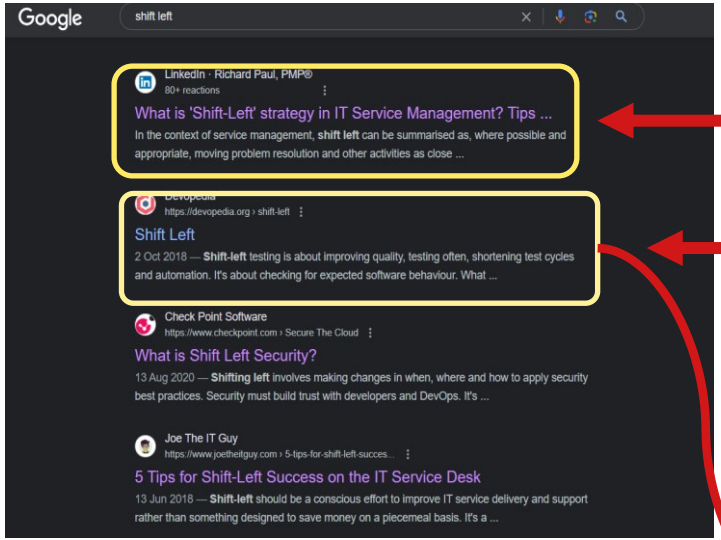


Source: van der Cruijsen 2017.

Shift-Left History



Shift-Left History



This isn't even DevOps

First example related to DevOps/Software Development

2001

The use of the term *Shift-Left Testing* appears in an article published at Dr.Dobb's. The author Larry Smith writes,

> "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

Mend.io Tools

ONE TEAM. ONE MISSION. ONE PLATFORM.

mend.io

Demo Time!

Free Tools You Can Use

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

Questions?