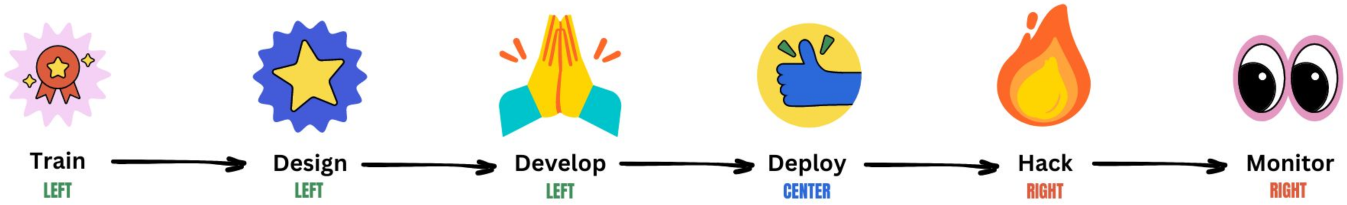
Shift Left on Security

XTC Berlin - August 2023 Edition
Olga Casian



Train → Design → Develop → Deploy → Hack → Monitor

LEFT LEFT LEFT CENTER RIGHT RIGHT

This is how development looks like

Shift Left on Security

is about integrating security practices into the development process
as opposed to making it a separate phase that happens
downstream of the development process

Motivation

- cheaper and easier security management
  - TopData Breach Fines & Violations (2012-2023)

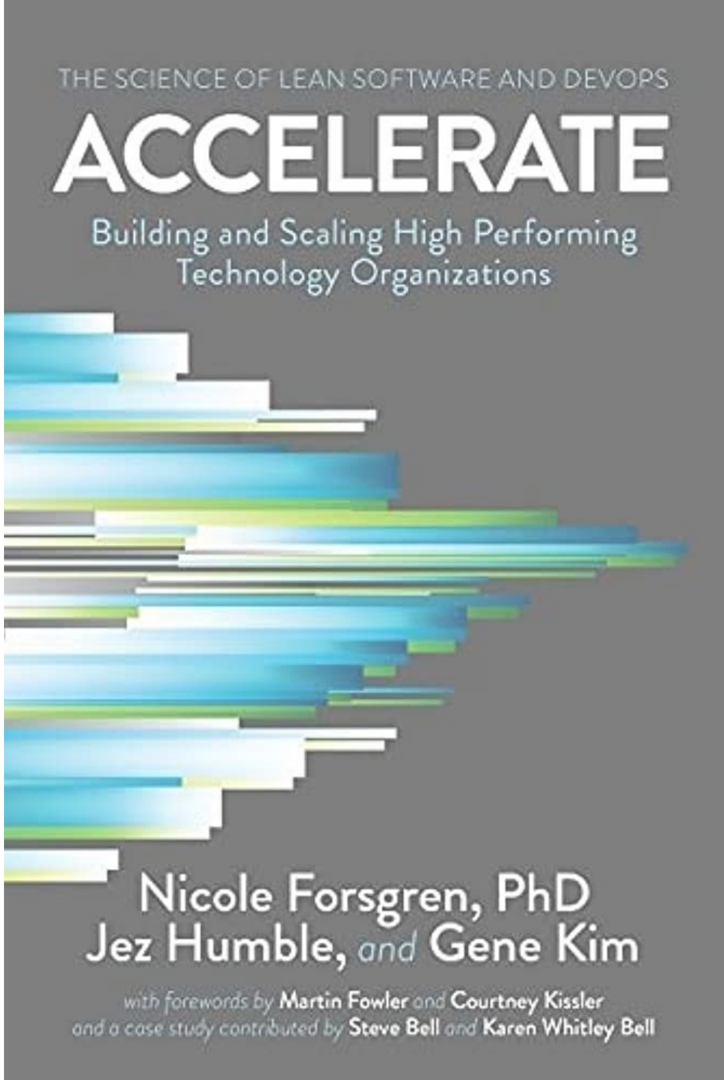
1. Facebook: $5 billion
2. Didi Global: $1.2 billion
3. Amazon: $886 million
4. Equifax: $700 million
5. Epic Games: $520 million
6. T-Mobile: $500 million
7. Home Depot: $200+ million
8. Capital One: $190 million
9. Google: $170 million
10. Twitter: $150 million

Motivation

- infosec teams don't have the capacity to review often deployments
- infosec is often understaffed at organizations
  - 1 infosec per 10 devops per 100 developers
- people who build the software know it the best

The research

- discussed in the “Accelerate” book
- research: companies following it
  - have improved delivery performance
  - have improved security quality
  - have improved communication between developers and infosec teams
  - spend significantly less time remediating security issues



THE SCIENCE OF LEAN SOFTWARE AND DEVOPS

ACCELERATE

Building and Scaling High Performing Technology Organizations

Nicole Forsgren, PhD
Jez Humble, *and* Gene Kim

with forewords by Martin Fowler *and* Courtney Kissler
and a case study contributed by Steve Bell *and* Karen Whitley Bell

How to ensure that it does not impact negatively the delivery performance?

- should be integrated into the entire lifecycle
- infosec teams
  - provide required support, training and tooling
  - make it easy to achieve
- developers integrate it into the development process

Static Application Security Testing (SAST)

- accesses the source code to identify weaknesses that may lead to vulnerabilities

ktlint

VERACODE

trivy

QL

aqua
tfsec

Dynamic Application Security Testing (DAST)

- specification-based testing on running application, without requiring in-depth knowledge
- identifies issues with requests, responses, interfaces, scripts, injections, authentication, and sessions

fluid attacks

we hack your software

PT Application Inspector

Interactive Application Security Testing (IAST)

- combining static and dynamic approaches, performs testing on application and data flow using predefined test cases

Checkmarx

Invicti

CONTRAST SECURITY

Software Composition Analysis (SCA)

- analyzes used dependencies to identify known vulnerabilities
- notifies of any available patches or updates

OSV | Open Source Vulnerabilities

Dependabot

Application Security Testing as a Service (ASTaaS)

- an external company performs testing by combining static and dynamic approaches, including penetration testing and API evaluation

SYNOPSYS®

MICRO FOCUS®

Fortify

Application Security

Questions to discuss

- What can go wrong while applying Shift Left on Security practices and how to prevent it?
- What was the most helpful tool in your experience?