# Security at the Speed of DevOps: An application security framework for a Lean/Agile/DevOps environment

Submitted by Katie Dey on Thu, 03/15/2018 - 11:21am. Contributor:
?Larry Maccherone

**BIO**

Larry Maccherone is an industry-recognized thought leader on Lean/Agile, Analytics, and DevSecOps. He currently leads the DevSecOps transformation at Comcast. Previously, Larry led the insights product line at Rally Software which enabled better decisions with data, leveraged big data techniques to conduct groundbreaking research, and offered the first-ever Agile performance benchmarking capability. Before Rally, Larry worked at Carnegie Mellon with the Software Engineering Institute (SEI) and CyLab for seven years conducting research on cybersecurity and software engineering. While there, he co-led the launch of the DHS-funded Build-Security-In initiative. He has also served as Principal Investigator for the NSA's Code Assessment Methodology Project, on the Advisory Board for IARPA's STONESOUP program, and as the Department of Energy's Los Alamos National Labs Fellow.

Contact Larry on his LinkedIn page: https://www.linkedin.com/in/larrymaccherone

**ABSTRACT**

The bad guys don't break in through the highly secure bank vault door; they attack the crumbly bricks and mortar of the vault walls. The same is true for application security. The vast majority of incidents don't target security features like encryption, authentication, and authorization... the bank vault door. Rather, they target vulnerabilities in the "boring", non-security parts of the code... the crumbly bricks and mortar of the vault walls.

The security function is still largely throw-it-over-the-wall at many organizations, but things are changing. There is growing awareness that you cannot prevent the vast majority of incidents with a bolt-on approach to security. You have to produce applications that are free of such vulnerabilities as they are being developed. In other words, you have to BUILD SECURITY IN.

Just like DevOps is a cultural transformation, to BUILD SECURITY IN we need a mindset shift and cultural change. We need DevSecOps.

This talk introduces a DevSecOps manifesto and a process model for achieving a "BUILD SECURITY IN" DevSecOps culture. The framework is designed to sit on top of any SDLC but it is particularly suited

to Lean/Agile environments and even more so to a DevOps environment or in conjunction with an ongoing DevOps transformation.

Learning outcomes:

- The values identified in a DevSecOps manifesto
- The key disciplines of security practice most relevant to development teams
- A maturity scale for these disciplines that you can leverage to incrementally up your application security game
- The key measures that will provide feedback for a data-driven and gamification approach to cultural change
- Common objections from large organization inertia/ossification and how to overcome them
- How to BUILD SECURITY IN rather than bolt it on



Security at the Speed of DevOps: An application security framework for a Lean/Agile/DevOps environment

Presentation Presentations