How Do You Adapt AppSec to DevOps World

John B. Dickson, CISSP
@johnbdickson
Overview

• DevOps Defined
  • What’s Driving DevOps?
• The State of Application security
• How Security Remains Relevant in a DevOps World
John’s Background

- Application Security Enthusiast
- Helps CSO’s and CISO’s with Application Security Programs
- ISSA Distinguished Fellow
- Security Author and Speaker
- 20 years Experience Across Multinational Corporations
Denim Group Overview

Providing vastly improved application security for mission-critical enterprise applications

ThreadFix
 Powered by Denim Group

The Delivery Platform
 Central Resolution Hub
 Accelerate Remediation

Application Testing
 Quantifies Risk Across the Application Portfolio

DevOps & AppSec
 Transformation Consulting

ADVISORY SERVICES

MANAGED SERVICES

The Delivery Platform

Tweet along: #Sec360

www.Secure360.org
DevOps Defined

• DevOps is a practice that:

  • Emphasizes the tight collaboration and communication of both software developers and IT operations staff

  • Focuses on automating the process of software delivery and infrastructure changes

  • Aims at establishing a culture and environment where building, testing, and releasing software, can happen rapidly, frequently, and more reliably
Aspects of DevOps

• Focuses on time to market over virtually every other requirement

• Focuses on continuous improvement

• Software quality and auditability valued – but as a by-product of speed
CI/CD Eye Chart Test!

Source: https://dzone.com/articles/the-ultimate-devops-tools-ecosystem-tutorial-part
Potential Components of a Secure CI/CD

• Code repository (Git, Subversion)
• CI/CD server (Jenkins, Bamboo)
• Build server(s)
• Unit test suite (JUnit)
• Functional test suite (Selenium)
• Defect tracker
• Application Vulnerability Management Platform
What is Driving DevOps?

- Time-to-Market advantages
- Demand of higher quality software products
- Cost concerns
- Key thought: Like cloud, DevOps will come from business units responding to competitive pressures, not IT or outside pressure

Tweet along: #Sec360
www.Secure360.org
How Did We Get to DevOps?

- Waterfall
- Agile
- DevOps
- Secure DevOps

Business
Development
Operations
Security

Tweet along: #Sec360

www.Secure360.org
The State of Application Security

- Organizations have become better at identifying web application vulnerabilities via automated scanning.
- Automation still only catches 30-50% of application vulnerabilities.
- Organizations have become better at identifying application vulnerabilities than fixing them.
- Much of the effort involves testing and SDLC improvement.
- Chasm still exists between security and development teams.

- AppSec is by no means “solved” but....
Better Security Insight, More Often
So What Does Application Security Want?

• Reduce Risk Exposure
• Introduce Fewer Vulnerabilities
• Find Vulnerabilities Early
• Fix Vulnerabilities Quickly
And What Do DevOps Teams Want?
Application Security Testing in CI/CD Pipelines
AppSec Testing Policies for DevOps
Developer Communications

Hint: Not With These…

Tweet along: #Sec360

www.Secure360.org
How Application Security Remains Relevant in a DevOps World

• Pulling a Tiger by the Tail?
How Application Security Remains Relevant in a DevOps World

• Understand that you will miss things
• Software will be deployed without your knowledge and not security tested (always)
• You will have functionality in your production environment you don’t understand
• Understand your job just got harder
• And you can’t say “no!”
DevOps Concepts if You Take Adaptation Approach

• Automate every security process possible
  • Squeeze application testing cycles and automate entire process
  • Fully automate application vulnerability resolution process
• Consider new technologies such as IAST/RASP
• Incrementally increase application monitoring in production environments – standardize & automate
DevOps Concepts if are Forced to Improvise

• Focus on testing in production environments
  • Create processes and scanning systems to tear down vulnerable functionality
  • Recognize that production is where you might first learn of new features!

• Recognize application attack patterns in production environments via big data
  • Fix vulnerability!

Tweet along: #Sec360
www.Secure360.org