Chapter 59
Weaving Security into DevOps Practices in Highly Regulated Environments

Jose Andre Morales
Software Engineering Institute, Carnegie Mellon University, Pittsburgh, USA

Hasan Yasar
Software Engineering Institute, Carnegie Mellon University, Pittsburgh, USA

Aaron Volkmann
Software Engineering Institute, Carnegie Mellon University, Pittsburgh, USA

ABSTRACT

In this article, the authors discuss enhancing a DevOps implementation in a highly regulated environment (HRE) with security principles. DevOps has become a standard option for entities seeking to streamline and increase participation by all stakeholders in their Software Development Lifecycle (SDLC). For a large portion of industry, academia, and government, applying DevOps is a straight forward process. There is, however, a subset of entities in these three sectors where applying DevOps can be very challenging. These are entities mandated by security policies to conduct all, or a portion, of their SDLC activities in an HRE. Often, the reason for an HRE is protection of intellectual property and proprietary tools, methods, and techniques. Even if an entity is functioning in a highly regulated environment, its SDLC can still benefit from implementing DevOps as long as the implementation conforms to all imposed policies. A benefit of an HRE is the existence of security policies that belong in a secure DevOps implementation. Layering an existing DevOps implementation with security will benefit the HRE as a whole. This work is based on the authors extensive experience in assessing and implementing DevOps across a diverse set of HREs. First, they extensively discuss the process of performing a DevOps assessment and implementation in an HRE. They follow this with a discussion of the needed security principles a DevOps enhanced SDLC should include. For each security principle, the authors discuss their importance to the SDLC and their appropriate placement within a DevOps implementation. They refer to a security enhanced DevOps implementation in an HRE as HRE-DevSecOps.

DOI: 10.4018/978-1-6684-3702-5.ch059

1. INTRODUCTION

A highly regulated environment (Hrebiniak & Joyce, 1985; Edwards, 1977; Blau et al., 2000; Rasmussen et al., 2009) (HRE) is typically characterized by the following: air-gapped physical spaces and computer systems with heightened security and access controls, segregation of duties, inability of personnel to discuss certain topics outside of specific areas, and the inability to take certain artifacts off premises. An HRE is put to use when secrecy and controlled access is required for proprietary tools, methods, techniques, and intellectual property. DevOps, with and without a security component, has been proven to increase effectiveness and, most importantly, efficiency of an SDLC. As a result of this, several entities that utilize HREs such as the US Department of Defense (LaPlante & Wisnieff, 2018; Dioguino, 2016) are implementing DevOps into their SDLC. Currently, there is minimal literature on implementing DevOps in an HRE explaining the mechanics, expectations, challenges, realities, and paths to success in comparison to currently used non-DevOps models (Bruza, 2018; Farroha & Farroha, 2014). In this paper, our leverage our experiences with DevOps and security to address these issues. There is no known data set of metrics for DevOps in an HRE and an approach based on the scientific method is not possible at this time. This work seeks to enhance current literature with an experience-based approach to Secure DevOps. For the purpose of this work, the term air-gapped is meant describe physical spaces, personnel, computer systems, and other technologies that are isolated from all entities that are external to the HRE. We have mentioned only some of the characteristics of an HRE as the list changes on a case by case basis. An HRE can be referred to as a closed area, classified space, controlled access area, or Sensitive Compartmented Information Facility (SCIF). The definition of an HRE used in this paper is not the same as government regulation. Those policies are focused on how to conduct business, financial responsibilities, and disclosure filing, just to name a few. Regulatory policies are required for various sectors of industry and overseen by federal agencies such as the U.S. Securities & Exchange Commission (SEC), the U.S. Food and Drug Administration (FDA), and the Federal Communications Commission (FCC).

Each of the previously mentioned obstacles characterizing an HRE can impose several barriers impeding the full incorporation of DevOps (Hüttermann, 2012; Bass, Weber, & Zhu, 2015) practices into a Software Development Lifecycle (SDLC) (Yasar, & Kontostathis, 2016). In this paper, we follow the core DevOps definition of uniting software development and IT operations into one singular process. We focus on implementing the following DevOps principles in an HRE:

1. Open communication between all stakeholders
2. Infrastructure as Code (IaC)
3. Environment parity
4. Centralized documentation
5. Continuous completion and deployment of small tasks
6. Performance monitoring
7. Accurate production environment replication
8. End user feedback loop
9. Automation
10. Software artifact versioning