DevOps Practices for Building Secure and Resilient Cloud-Native Web Applications

Harigovind V Ramasamy, Long Wang and Richard Harper

{hvramasa, wanglo, reharper}@us.ibm.com

IBM

Abstract — **DevOps is a software engineering practice that is now widely adopted by industry leaders. The combination of DevOps practices and cloud-native technologies has become a game changer for the rapid creation, delivery, and maintenance of secure and resilient web applications. In this tutorial, we give participants first-hand experience in creating, deploying, and managing secure and resilient cloud-native web applications on a geographically distributed, commercial cloud platform using DevOps practices.**

Keywords — DevOps, cloud-native, security, resiliency, cloud

I. LEARNING GOALS

The goals of the tutorial are to enable attendees to

(1) obtain a good understanding of the fundamentals of DevOps practices, and how they differ from traditional methods of software development, delivery, and operations,

(2) learn typical skills and tools in DevOps practices for rapidly creating, deploying and managing secure and resilient cloud-native web applications, and

(3) understand the benefits that DevOps practices hold for security and resiliency.

II. TARGET AUDIENCE

The content is targeted towards a broad audience of users, developers, practitioners, researchers, and students in the area of distributed systems. As DevOps practices and cloud-native technologies become the norm, it is important for the target audience to understand the challenges, opportunities, complexities, and benefits of these practices and technologies. The content level is beginner-to-intermediate, suited for anyone with an undergraduate background in computer science (or equivalent) and basic programming skills.

III. OVERVIEW AND TUTORIAL STRUCTURE

The all-day tutorial consists of three parts. In the first part, we introduce practices and technologies that enable DevOps, such as micro-services, agile methodologies, social coding, infrastructure-as-code, configuration automation, and test-driven development. We familiarize the participants with DevOps concepts such as continuous integration, continuous deployment, and continuous delivery. Through this part, participants will obtain a good understanding of the foundational technologies and practices of DevOps, and how they differ from traditional software development and operations.

In the second part of the tutorial, we examine the implications of DevOps for building secure web applications. We explain how DevOps practices can be weaved into the traditional Secure Software Development Lifecyle model (SDLC) [1]. We then present the OWASP top ten list of web application security risks [2]. To guard against those and similar risks, we provide examples of tools that can be embedded in a DevOps Continuous Integration Continuous Delivery (CICD) pipeline. Such tools facilitate secure software development and delivery into production environments. We reinforce these examples through hands-on exercises.

In the third part of the tutorial, we examine the benefits of DevOps practices for creating resilient applications on the cloud. We present types of failures on the cloud, and methods for handling them. Through hands-on exercises, we guide the participants in creating DevOps toolchains for building, deploying, and managing geo-distributed, disaster-tolerant, highly available web applications that can be updated without any user-perceived downtime. Participants will work in teams, playing the role of DevOps engineers, witness social coding in action, and test the continuous availability of applications despite a (simulated) cloud site outage.

The hands-on exercises will be performed on the IBM Cloud platform [3]. Through these exercises, we guide the attendees towards gaining first-hand appreciation of how DevOps practices allow businesses to innovate at scale with increased agility while simultaneously enabling stability and security.

REFERENCES

[1] R. Kissel, K.M. Stine, M.A. Scholl, H. Rossman, J. Fahlsing, and J. Gulick. 2008. SP 800-64 Rev. 2. Security Considerations in the System Development Life Cycle. Technical Report. NIST, Gaithersburg, MD, United States.

[2] OWASP Top 10 Most Critical Web Application Security Risks, 2017 [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project [Accessed: 13- Aprl- 2018]

[3] IBM Cloud. [Online]. Available: https://www.ibm.com/cloud/ [Accessed: 13- Aprl- 2018]