Continuously Integrating Security

Laurie Williams
North Carolina State University
Raleigh, NC, USA
laurie_williams@ncsu.edu

ABSTRACT

Continuous deployment is a software engineering process where incremental software changes are automatically tested and frequently deployed to production environments. With continuous deployment, the elapsed time for a change made by a developer to reach a customer can now be measured in days or even hours. To understand the emerging practices surrounding continuous deployment, three annual one-day Continuous Deployment Summits have been held at Facebook, Netflix, and Google in 2015-2017, where 17 companies have described how they used continuous deployment. This short paper will describe the practices and environment used by these companies as they strive to develop secure and privacy-preserving products while making ultra-fast changes.

CCS CONCEPTS

• **Software and its engineering → Agile software development**;

KEYWORDS

Continuous deployment, software security, DevOps, DevSecOps

ACM Reference Format:
Laurie Williams. 2018. Continuously Integrating Security. In *SEAD'18: IEEE/ACM 1st International Workshop on Security Awareness from Design to Deployment , May 27, 2018, Gothenburg, Sweden.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3194707.3194717

1 INTRODUCTION

Continuous deployment is a software engineering process where incremental software changes are automatically tested and frequently deployed to production environments. With continuous deployment, the elapsed time for a change made by a developer to reach a customer can now be measured in days or even hours. To understand the emerging practices surrounding continuous deployment, three annual one-day Continuous Deployment Summits have been held at Facebook in 2015 [1], Netflix in 2016, and Google in 2017. Over the course of the three years 16 companies have described how they used continuous deployment. The seven companies that have attended all three Summits include Cisco, Facebook, Google, IBM, LexisNexis, Microsoft, Netflix. Four companies have attended two Summits: 18F, SAS, Slack, and Twitter. Disney, Ericsson, Mozilla, Nokia, and Redhat have joined one Summit.

SEAD'18, May 27, 2018, Gothenburg, Sweden

ACM ISBN 978-1-4503-5727-2/18/05.
https://doi.org/10.1145/3194707.3194717

This short paper providing highlights of the keynote will describe the practices and environment used by these companies as they strive to develop secure and privacy-preserving products while making ultra-fast changes. These practices can be organized into three themes: Communication, Culture, and Technical. Each of these themes will be described in the next three subsections.

2 COMMUNICATION

In recent years, the DevOps movement has been influencing software development organizations. With DevOps, communications lines between developers and the operations team that deploy the software are opened up. Developers and operations teams collaborate. More recently, the DevSecOps way of working is emerging. In DevSecOps, the security experts on the team are also in close communication with the developers and operations team. In general, the companies at the Summit had not yet adopted DevSecOps. Instead, most of the organizations had separate security and privacy organizations that served as consultants to the developers. The smaller companies, such as Slack and Twitter, had closer collaboration between the developers and security and privacy teams.

3 CULTURE

Various aspects of a continuous deployment culture contribute to the development of more secure and privacy-preserving code. The rapid customer feedback to the developer after changes are made to the code provide an incentive for the production of high quality code. The developer often must respond directly to field failures (even on nights and weekends) rather than the failures being handled by a support team. Additionally, Summit companies often conducted "*shameless* retrospectives" in which team members shared mistakes that were made to aid in the prevention of other team members making the same mistake. Several Summit companies had a policy of discussing every security and privacy-related failure in one of these retrospectives.

4 TECHNICAL PRACTICES

Several technical practices often adopted by the Summit companies aid in the production of secure and privacy-preserving code. Prior to checking in code, the development team must pass check-in gates which often involve the execution of automated tests and static and dynamic analysis tools, including tools designed to detect security and privacy defects. Additionally, developers use feature flags to prevent customer execution of partially-developed features and to support feature experimentation. The security and privacy experts in the organization often conducted additional checks on changes that had security and privacy implications. The feature flag for these features could not be turned on for customer use until after the additional checks were made the the security/privacy

approval was granted. Finally, once a security vulnerability has been detected, a mitigation must be rapidly and deployed to customers. The infrastructure for deployment enables Summit companies to rapidly and automatically deploy these changes to customers.

ACKNOWLEDGMENTS

The author would like to thank all the participants of the Continuous Deployment Summit for their participation and insight.

REFERENCES

[1] Chris Parnin, Eric Helms, Chris Atlee, Harley Boughton, Mark Ghattas, Andy Glover, James Holman, John Micco, Brendan Murphy, Tony Savor, et al. 2017. The top 10 adages in continuous deployment. *IEEE Software* 34, 3 (2017), 86–95.