Security Practices in DevOps

Akond Ashfaque Ur Rahman
Department of Computer Science
North Carolina State University
Raleigh, NC, USA
aarahman@ncsu.edu

Laurie Williams
Department of Computer Science
North Carolina State University
Raleigh, NC, USA
williams@csc.ncsu.edu

1. INTRODUCTION

DevOps focuses on collaboration between different teams in an organization to achieve rapid deployment of software and services to end-users by automating the software delivery infrastructure. According to Dyck et al. [1] DevOps is a software process that emphasizes collaboration within and between different teams involved in software development. According to a study from CA Technologies [5], 88% of 1425 organization executives stated that they have adopted DevOps, or are planning to adopt DevOps in the next five years. According to Puppet Labs' 2015 State of DevOps Report [2], organizations that have adopted DevOps experienced 60 times fewer failures and deploy 30 times more frequently than organizations that have not adopted DevOps. Despite the popularity, security aspects of DevOps remain a concern for organizations that want to adopt DevOps [5]. In organizations that use DevOps practices, developers can commit and deploy their software changes at a rapid rate using an automated pipeline. At such a rapid rate, if the security team operates in isolation without close collaboration with the development and operations teams, then the rapidly deployed software changes might not undergo the adequate security reviews, potentially leading to vulnerable software. Bringing security principles within the DevOps process can help the organization in achieving better quality of software by integrating security checks into the phases of development, testing, and deployment.

The goal of this study is to aid software practitioners in integrating security and DevOps by summarizing experiences in utilizing security practices in a DevOps environment.

Software practitioners can aid from a study that investigates the security practices used by organizations that have adopted DevOps to integrate security in their organization. In our study we focus on identifying the security practices that can be used, and are actually in use to integrate security in DevOps. We conduct this study by selecting and analyzing a set of 66 Internet artifacts, such as blog posts and video presentations. We then identified a set of software practices used to integrate security in DevOps. Leveraging findings from our analysis of Internet artifacts, we created a survey to further investigate the software practices that are used in the surveyed DevOps organizations to integrate security. The survey was administered to representatives of nine organizations that have adopted DevOps.

HotSoS '16, April 19-21, 2016, Pittsburgh, PA, USA
ACM978-1-4503-4277-3/16/04.
http://dx.doi.org/10.1145/2898375.2898383

We summarize the contributions of this study as follows:

- A list of security practices and an analysis of how they are used in organizations that have adopted DevOps to integrate security; and
- An analysis that quantifies the levels of collaboration amongst the development teams, operations teams, and security teams within organizations that are using DevOps.

2. RESEARCH METHODOLOGY

We describe the major steps of our study in this section. Our first step was to identify and analyze Internet artifacts. We then conducted a survey[1] with nine DevOps organizations to further investigate security practices that they use to integrate security.

2.1 Analysis of Internet Artifacts

We used the Google search engine to identify Internet artifacts, such as blog posts and video presentations. Initially we used the search string "security in DevOps" to identify the necessary set of Internet artifacts in the study. We then extended our list of search strings based on two observations:

- From the top 50 search results for the search string "security in DevOps" we observe that security in DevOps is also referred as "DevSecOps", "SecDevOps", "SecOps", and "RuggedOps"
- Rahman et al. [4] have attributed continuous deployment and continuous delivery to be related to DevOps

Considering the above two observations, we utilized seven search strings to identify the necessary Internet artifacts for the study: "security in DevOps", "DevSecOps", "SecDevOps", "SecOps", "RuggedOps", "Security in Continuous Delivery", and "Security in Continuous Deployment".

We differentiate the two terms 'activity', and 'security practice' to facilitate the discussion. In our study, an activity focuses on achieving a small, well-defined goal that has a tangible output, and a security practice is a collection of activities that can be grouped based on existing similarities within those activities. A security practice is a collection of activities that can be grouped based on existing similarities within those activities. For example, 'use of automation activities' is the practice that contains the activity of 'automation of testing'. We investigated what security practices have software practitioners stated to integrate security in DevOps. To identify these security practices, we read the Internet artifacts and listed each practice. If different terminologies were used for the same practice, then that particular practice is included once for our study. In some Internet artifacts, software practitioners have reported different activities that constitute a certain practice. We read the artifacts, and document each new activity to find such activities. If different terminologies are used to mention the same activity, then we list that activity only once.

[1] http://goo.gl/forms/hH1PuRmg7a

2.2 Analysis of Survey

We surveyed one representative of each of nine organizations that utilize DevOps practices to investigate use of security practices. We designed the survey based on our findings from our analysis of Internet artifacts. In the survey, we asked the survey participants which of the identified security practices they use, along with necessary activities. The survey participants were also provided the option to mention any additional activities that they use to integrate security.

In the survey we asked three questions that assess collaboration between development and operations teams, development and security teams, and security and operations teams. We used a Likert Scale [3] from one to five, where five indicated the highest level of collaboration, and one indicated the lowest. If the DevOps organization did not have any one of the above-mentioned teams, we asked the survey participant to assign zero. Later in our analysis we refer to the collaboration ratings of five, four, three, two, and one respectively as 'highest', 'high', 'moderate', 'low', and 'lowest'.

3. RESULTS

In our study, we analyzed 34 Internet artifacts that are available online[2] and discuss the use of security practices for integrating security in DevOps organizations. From our analysis of these 34 Internet artifacts, we observe four security practices: use of automation activities; collaboration amongst different departments; providing security training for development team members; and use of non-automated security practices.

In our study, we surveyed one software practitioner from each of the nine DevOps organizations. These organizations were: CA Technologies, Cisco Systems, CoolBlue, Facebook, Google, LexisNexis, Mozilla Firefox, Netflix, and SAS. Our survey analysis shows that all the nine organizations use three of the four identified security activities.

3.1 Use of Automation Activities

Automation of all activities related to software development is one of the common software practices used in DevOps culture. In our study we refer to this practice as 'use of automation activities'. This security practice includes five activities that are presented in the 'Name' column of Table 1. In Table 1 'Count' presents the count of Internet artifacts in which the specific automation activity was referred. 'Yes' presents the count of DevOps organizations using a specific activity. 'No' presents the count of DevOps organizations that do not use a specific activity.

Table 1: Use of automation activities

Name	Count	Yes	No
Automation of monitoring	20	8	1
Automation of testing	13	8	1
Automation of code review	11	7	2
Automation of software defined firewall	5	6	3
Automation of software licensing	3	4	5

3.2 Collaboration

Increased collaboration between development teams, security teams, and operation teams have been mentioned in 16 Internet artifacts. All of the nine survey respondents have reported to have separate development and security teams in their organizations. Eight of the nine representatives have reported to have a separate operations team. In Table 2, we present our findings for three types of collaborations namely, 'Dev&Ops', 'Dev&Sec', and 'Sec&Ops'. According to our survey analysis, one DevOps organization did not have a separate operations team, and we exclude that organization from Table 2.

Table 2: Level of collaboration

Level	Lowest	Low	Moderate	High	Highest
Dev&Ops	1	0	1	5	1
Dev&Sec	0	2	4	1	2
Sec&Ops	0	0	4	3	1

3.3 Providing Security Training

Software practitioners also referred security training for development team members to integrate security in DevOps organizations. This practice was mentioned in three Internet artifacts. According to our survey results, seven of the nine DevOps organizations provided security training for their development team members.

3.4 Use of Non-Automated Security Activities

'Use of Non-Automated Security Activities' includes 10 non-automated security activities that are presented in the 'Name' column of Table 3. In Table 3 'Count' presents the count of Internet artifacts in which the security activity was referred. 'Yes' presents the count of DevOps organizations using the activity, and 'No' otherwise.

Table 3: Use of non-automated security activities

Name	Count	Yes	No
Security requirements analysis	6	9	0
Performing security configurations	5	8	1
Performing security policies	5	7	2
Performing manual security tests	5	7	2
Performing compliance requirements	4	7	2
Design review	3	7	2
Input validation	3	6	3
Isolation of untrusted inputs	3	6	3
Threat modeling	3	5	4
Risk analysis	2	5	4

From our analysis of Internet artifacts and survey we make the following observations:

- From Table 1 we observe that common DevOps activities such as automation of monitoring, automation of testing, and automation of code review are used to integrate security in DevOps. Therefore we state that common DevOps activities have the potential of helping DevOps organizations to integrate security.
- From the survey results found in Table 2, we observe seven or more of the nine DevOps organizations having 'Moderate' or higher levels of collaboration between the security team and the other two teams: development, and operations. From this finding we state that security teams actively collaborate with development and operations teams in established DevOps organizations.

[2] http://www.realsearchgroup.org/realsearch/devsecops-ref/

- We identified 10 non-automated security activities from our analysis of Internet artifacts. From Table 3 we observe that five or more of the nine DevOps organizations are using all the 10 non-automated security activities. We observe a certain level of consensus between the stated non-automated security activities in Internet artifacts, and the security activities that are actually in use within DevOps organizations. We observe that security awareness is prevalent amongst established DevOps organizations, considering their use of security activities, such as performing security policies, performing manual security tests, and performing security configurations.

4. REFERENCES

[1] Dyck, A., Penners, R., and Licthter, H. 2015. Towards Definitions for Release Engineering and DevOps, in *Proc. of the Third International Workshop on Release Engineering*, *Florence, Italy*, pages 3-3, May, 2015

[2] Labs, P., and Revolution, IT. 2015 State of DevOps Report | Puppet Labs: 2015. Available: https://puppetlabs.com/sites/default/files/2015-state-of-devops-report.pdf. Accessed: 2016-01-24

[3] Likert, R. 1932. A Technique for the Measurement of Attitudes, in *Archives of Psychology*, vol. 22, no. 140, pages 5-55, June, 1932

[4] Rahman, A., Helms, E., Williams, L., and Parnin, C. 2015. Synthesizing Continuous Deployment Practices Used in Software Development, in *Proceedings of the 13th Agile Conference (AGILE 2015), Washington D.C., USA*, pages 1-10, August, 2015

[5] Technologies, CA. DevOps: The Worst Kept Secret to Winning in the Application Economy: 2014. http://www.ca.com/us/~/media/Files/whitepapers/devops-the-worst-kept-secret-to-winning-in-the-application-economy.pdf. Accessed: 2016-01-24