Project 1: DevOps Disruption

Introduction

The term DevOps is the combination of Development and Operation. Software development is usually comprised of two teams: the development team and the IT operation team. The work of the two teams is separated. For a project, the development team will first decide on a plan and then begin to write codes. They build the system from scratch. After they finished the project, the operation team will test the system in the customer's environment and implement it. The operation team gives feedback to the development team about how to fix bugs and how to change codes to improve customer satisfaction. The development team will be waiting for the operation team to finish their job and give feedback. This process extends the whole software development timeline. DevOps is an approach that the development team and the IT operation team will work at the same time to produce the project. DevOps is an important idea because under this model the speed of software development will be significantly improved, increase the frequency of software release, and ensure the reliability of the software which means that improve the ability of software that could function seamlessly in its environmental constraints. Besides, in some projects, because the cybersecurity team will also add to the DevOps team, the security team will have more time and flexibility to secure the project minimizing the project’s vulnerabilities. (Freeman, 2019)

Applications

DevOps has a wide range of tools that development teams can choose from depending on their projects. This part will show how DevOps practices help to solve real-world problems. The first example to show the application of DevOps is the online financial trading company. DevOps help to automate the process of testing, building, and development. It makes the deployment part can be done within 45 seconds which is significantly improved compared to the old approach which usually takes employees long nights to finish it. (Mathur, 2022) The second example is Rabobank. Developers use DevOps practices to reduce bugs by 35% which provides their customers with high-quality applications in a short time by significantly reducing the time for testing. (Mathur, 2022) Those examples show that DevOps changed software development dramatically.

Literature review

This paragraph will focus on cybersecurity in the DevOps approach. Traditionally, after the software was developed, the cybersecurity team will provide recommendations about how to secure the project, and the development team will change codes according to the recommendation. In the DevOps approach, the cybersecurity team will collaborate with DevOps teams to create the project together. It is necessary for Cybersecurity professionals to participate in the development process, communicate with other developers, and provide test cases on the same level as the coding and deployment part. (Watson, 2021) DevOps security approach brings many benefits, but there are also some security threats that need to be overcome. For example, account credentials, tokens, and SSH keys used by DevOps could provide a path for hackers to attack the operations and systems. (Maayan, 2019) Implementing threat modeling to visualize the entire pipeline to check how it could be attacked by hackers is a good idea to improve the security of application development. (Maayan, 2019) Cybersecurity is an important part that cannot be ignored in software development. DevOps provide a way that makes the process of securing codes much faster than before.

Open Source Projects

There are many DevOps open source tools to help developers develop their products such as Jenkins, Chef, Vagrant, and Docker. To combine those tools, it is possible for developers to achieve continuous deployment and automation. Docker provides a security practice for scanning and building secure images in the development workflow. Docker worked with Snyk to design a way for developers to build a secure container that spans multiple teams such as developers, IT operations, and security. The whole process can be summarized in the following steps. First, in the design process, use Snyk Advisor to research base images and test for vulnerabilities. This process can decrease the time that Docker Hub will use to check the vulnerabilities of images in the next step. Docker Hub can scan images automatically once it received the image. After code or images was pushed to software configuration management (SCM), the CI pipeline will be triggered and unit, integration, and functional testing will begin. Then, images will be re-tested for new vulnerabilities. Developers can view and inspect vulnerabilities through Docker Hub. Docker Desktop also provides a report of vulnerabilities statues can be checked by clicking View in Docker Hub. Docker also provides many ways developers can use to improve their security containers. For example, developers can choose the right base image from Docker Hub which contain more than 8.3 million repositories. (Docker, 2022)

Conclusion

DevOps is an idea that combines the development team, IT operations team, and Security team together to increase the ability to release applications and provide services to customers at a faster speed. DevOps security approach brings many benefits to software development. Docker which is one of the DevOps tools provides a way for developers to secure their images in the process of development. By using different DevOps practices and tools, developers can decrease the whole software development timeline which brings a radical change to the software industry.

References

A. Mathur, “16 popular DevOps use cases & real-life applications [2022],” *upGrad blog*, 16-Sep-2022. [Online]. Available: https://www.upgrad.com/blog/devops-use-cases-applications/. [Accessed: 18-Sep-2022].

Docker Hub. “Best practices for scanning images,” *Docker Documentation*, 15-Sep-2022. [Online]. Available: https://docs.docker.com/develop/scan-images/. [Accessed: 18-Sep-2022].

E. Freeman, “DevOps,” *Amazon*, 2019. [Online]. Available: https://aws.amazon.com/devops/what-is-devops/. [Accessed: 18-Sep-2022].

G. Maayan, “DevOps security challenges and how to overcome them,” *CCSI*, 11-Oct-2019. [Online]. Available: https://www.ccsinet.com/blog/devops-security-challenges/. [Accessed:

J. Watson, “DevOps demands a shift from traditional cybersecurity,” *Kovair Blog*, 31-Aug-2021. [Online]. Available: https://www.kovair.com/blog/how-does-devops-demand-a-shift-from-the-traditional-cybersecurity-approach/. [Accessed: 18-Sep-2022].