DevSecOps - The New DevOps?

Sara Damne, Frida Wallberg

20 April 2021

1 Introduction

There is an increasing need to implement secure practices in the development of computer systems [1]. Varonis[2] lists statistics made by organizations such as Accenture and IBM. A few of the interesting finds are:

- By IBM; *"The average cost of a data breach is $3.86 million as of 2020."*
- By Accenture; *"Security breaches have increased by 11% since 2018 and 67% since 2014."*
- By Maryland University; *"On average, hackers attack 2,244 times a day."*

Amid the Covid-19 pandemic, there has been an increase in cybercrime. A study made by the FBI shows that the number of reported cybercrimes has risen by 300%[3]. These statistics point out the importance of security in today's software technology systems.

The traditional waterfall model of software development goes through various phases, one after the other. The main characteristics is that every phase has to be completed before the next one can start[4]. Security concerns are treated in the late stages of the project, just before release[5]. This model holds no considerations towards the continuous change in requirements in today´s digital world[4]. DevOps, on the other hand, is a process that goes through development stages over and over again. It allows requirements to be changed, developed, released, and maintained continuously[5].

Several challenges arise with DevOps from a security point of view e.g sacrifice of security for speed/agility[1]. DevOps introduces new threats and vulnerabilities and therefore requires another approach to security than the traditional waterfall model. However, as in the waterfall model, DevOps also treats security concerns in the late stages of a project. This is what DevSecOps addresses. It takes the continuous development process of DevOps and extends it to include security. In DevSecOps, security is treated as an everyday topic implemented in all stages of the workflow[5]. It is clear that security is a big part of development, but is DevSecOps the new DevOps? This essay will introduce DevOps, DevSecOps and the challenges that comes with implementing the security practices needed for DevSecOps.

2 DevOps

DevOps is a combination of *Development* and *Operations*. It improves the performance of software development through change in organizations. The process of DevOps can be seen in figure 1. The different parts of development and operations are put together in a continuous workflow.

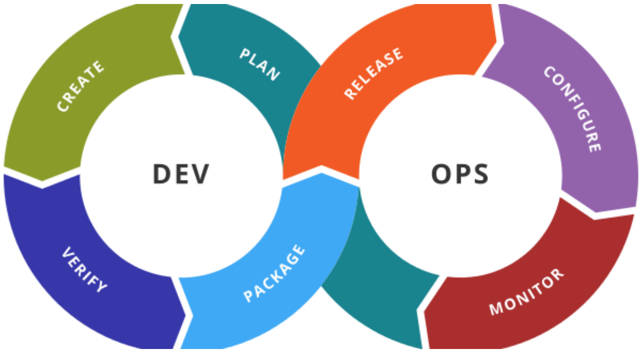

Figure 1: Workflow in DevOps [6]

Features that characterize DevOps can be divided into four categories *culture*, *automation*, *measurement*, and *sharing*. First, DevOps is about changing the culture of an organization to work cross-functional and speed up the development process. Secondly, automation is used to, again, speed up the process and to be able to deploy code frequently. The third category, measurement, includes monitoring and measuring system metrics to avoid failures. Lastly, sharing is a big part of DevOps since working cross-functional requires that teams share both knowledge and data[7].

The goal of DevOps is to completely automate the process of development and delivery which is approached by introducing cross-functional teams [8]. A report made in 2015 found that organizations that have implemented DevOps experience 60 percent less failure and deploy 30 times more. Another study found that almost 90 percent, of the 1425 organizations that were part of the study, planned to conform to a DevOps process within five years. This implies that the majority of the companies have adopted the DevOps way of working[8].

3 DevSecOps

Security is one of the main concerns for those who are reluctant to transition into DevOps. It might be difficult to ensure security with the amount of automation introduced in DevOps[8]. Within DevOps, there is the continuous introduction of new technology to speed up and automate the development process. Every one of these technologies brings a new aspect to the project, and security has to be considered every time a new technology is introduced[9].

Since DevOps makes it possible for developers to deliver and deploy updates and changes at a rapid rate, the security process needs to work at a similar speed to keep the security standards of the product. For an isolated security team, this becomes difficult unless their work is implemented in the DevOps process[8]. Traditionally, the security team looked at the code in the final stages of development just before deployment. This becomes a problem when the development cycles are shorter and requires the security to be more integrated into everyday activities.

DevSecOps (or SecDevOps as it is also referred to) refers to the collaboration between *development*, *security* and *operations*[7]. The term has no clear, agreed-on definition. However, the consensus throughout the field is that DevSecOps is an extension of DevOps and should include all aspects of DevOps with security integrated into the process, as seen in figure 2.

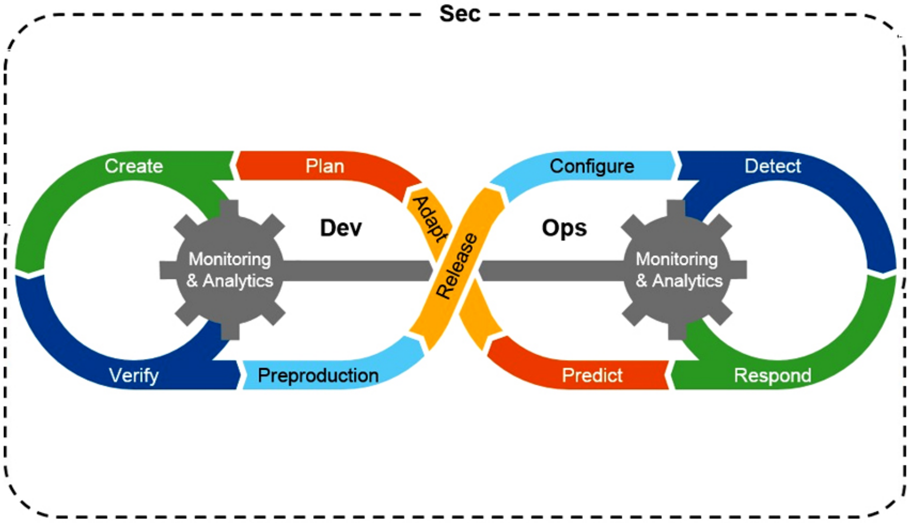

Figure 2: Security implemented in DevOps [10]

DevSecOps in practice includes features that can be divided into the same four categories as regular DevOps. For *culture*, DevSecOps requires that security becomes a part of an organization's culture. It needs to be implemented and adopted by everyone in a team to ensure that the security standards are kept[7]. *Automation* is, as in DevOps, an enormous part of DevSecOps. By automating the security verification, quicker releases are possible, and the development and security QA can work at the same speeds[5]. Automation in DevSecOps means using tools and code to run routine security tests[7]. Some common practices are continuous testing and security as code[1]. *Measuring* in DevSecOps includes keeping logs on different security threats and vulnerabilities within the system. Measuring also includes measuring the monitoring process and system metrics as with DevOps. Lastly, *sharing* largely refers to sharing knowledge. DevSecOps emphasizes the need to educate all team members within security to keep the security process cross-functional. However, sharing also includes developers sharing knowledge and data with security engineers. This so that the security engineers can attack potential problems earlier in the process[7] by doing threat modeling and running risk assessments[1].

4 Tools and practices when integrating Sec in DevOps

The security goal for a software technology company is to secure their customers' digital assets. The book *"Hands on Security in DevOps"* lists three main building blocks when considering security;

- Strategy and metrics, how to set up a security assurance framework.
- Policy and compliance, how to comply to laws which the company is obligated to follow, such as GDPR.
- Education and guidance, how to organize education for the employees and assure that they follow the security regulations.

There are many aspects of DevOps that need specific solutions for how to implement security in their workflow. For example, the use of continuous integration calls for security integration. There are many tools that can be used to keep this automatic. Open source scanning software is available for static code analysis, compile-time software scans for buffer overflows etc. Open-source software saves companies a lot of time and money, but can pose security risks themselves [11].

Another useful tool to help add security practices in the DevOps workflow is a *Security Incident Process*, which describes what should be done in case of a security breach. The first part of the process is *Preparation.* It includes prevention against such an event and a plan for minimizing the damages. Another part is *Detection and analysis*, which is the practice where the company actively searches for potential threats and analyses them. The third process is *Containment and recovery*, a plan for how to recover from an incident and how to isolate the damaged parts from the rest of the technology[9].

To implement a successful DevSecOps process, practices like these play a key part.

5 Challenges with implementing DevSecOps

There are both internal and external challenges with integrating DevSecOps in a team's or company's way of working. Internal challenges are *cultural resistance, solidified organizational structure,* and *high costs.* All three point out the difficulties in fundamentally changing the work process of a team[1].

Implementing DevSecOps, therefore, means implementing a new culture in a workplace. This comes with some challenges since many people are hesitant to change. The tradition is that security aspects are handled at the end of the development life cycle, and changing the workflow to continuously having to consider security vulnerabilities might lead to resistance in the workplace[12].

To implement sharing, new collaborations between developers and security experts have to be formed. This means that new teams have to be created. Security professionals and developers have traditionally worked somewhat against each other, often slowing each other down. Developers implement unsafe code that security experts have to fix. Bridging these two parts of a software development company is however crucial for the DevSecOps aspect of sharing data, knowledge, and education[13].

Automation also brings challenges. Automating security checks by integrating more tests into the verification process could lead to extensive time spent on daily builds. However, adding security tests could lead to vulnerabilities being detected earlier in the process, which could save time later on[5].

Some of the external challenges with implementing DevSecOps are lack of DevSecOps experts, lack of tools, and lack of DevSecOps solutions. These challenges all point to the fact that DevSecOps is a relatively new term that has yet to find a foothold in the industry[1].

Some argue that the term DevSecOps is not necessary and that security should instead be considered in DevOps. This since security is a critical part of software development and implementing DevOps does not imply that any cornerstones of the software development process has been cut out. Still, the consensus remains that security has to be integrated into DevOps to keep a sustainable work process[1].

6 Conclusion

It is inevitable that every software technology company, at some point, needs to consider security in their operations. As the trends show that security breaches are rising and DevOps becomes more and more widespread, it is important to ensure that the security aspect is included. There are challenges with implementing security in DevOps. However, in order to truly take advantage of the benefits of DevOps, facing these challenges and implementing security is necessary. It also becomes easier and easier to implement security in DevOps as more and more tools become available to automate the security verification.

To conclude and answer the initial question *Is DevSecOps the new DevOps?*. There is no doubt that security is highly needed in some way in DevOps. However, this does not imply the need for a new term such as DevSecOps.

References

[1] Runfeng Mao et al. "Preliminary Findings about DevSecOps from Grey Literature". In: *2020 IEEE 20th International Conference on Software Quality, Reliability and Security (QRS)*. IEEE. 2020, pp. 450–457.

[2] Bob Sobers. 2021. URL: `https://www.varonis.com/blog/cybersecurity-statistics/`.

[3] Jenna Walter. *COVID-19 News: FBI Reports 300% Increase in Reported Cybercrimes - IMC Grupo.* 2020. URL: `https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/`.

[4] Charles D. Tupper. "9 - Data Organization Practices". In: *Data Architecture.* Ed. by Charles D. Tupper. Boston: Morgan Kaufmann, 2011, pp. 175–190. ISBN: 978-0-12-385126-0. DOI: `https://doi.org/10.1016/B978-0-12-385126-0.00009-7`. URL: `https://www.sciencedirect.com/science/article/pii/B9780123851260000097`.

[5] Sai Nikesh D. *6 Best Practices for Successful DevSecOps Implementation.* 2019. URL: `https://www.devopsdigest.com/6-best-practices-for-successful-devsecops-implementation`.

[6] *DevOps, CI, CD – vad betyder det egentligen?* 2021. URL: `https://www.frontit.se/inspiration-kunskap/artiklar/devops-ci-cd-vad-betyder-det-egentligen/`.

[7] Nora Tomas, Jingyue Li, and Huang Huang. "An empirical study on culture, automation, measurement, and sharing of devsecops". In: *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security).* IEEE. 2019, pp. 1–8.

[8] Akond Ashfaque Ur Rahman and Laurie Williams. "Security practices in DevOps". In: *Proceedings of the Symposium and Bootcamp on the Science of Security.* 2016, pp. 109–111.

[9] Tony Hsiang-Chih Hsu. *Hands-On Security in DevOps: Ensure continuous security, deployment, and delivery with DevSecOps.* Packt Publishing Ltd, 2018.

[10] Håvard Myrbakken and Ricardo Colomo-Palacios. "DevSecOps: a multivocal literature review". In: *International Conference on Software Process Improvement and Capability Determination.* Springer. 2017, pp. 17–29.

[11] Maria Korolov. *Open source software security challenges persist.* 2018. URL: `https://www.csoonline.com/article/3157377/open-source-software-security-challenges-persist.html`.

[12] Martin Bauer. "Resistance to change—A monitor of new technology". In: *Systems Practice* 4 (June 1991), pp. 181–196. DOI: `10.1007/BF01059564`.

[13] Mark Robinsson. *DevSecOps: A Complete Guide to What, Why, and How - Plutora.* 2021. URL: `https://www.plutora.com/blog/devsecops-guide`.