DevSecOps - The New DevOps?

Sara Damne, Frida Wallberg

March 2021

1 Introduction

There is an increasing need to implement secure practices in the development of computer systems [1]. Varonis [1] 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%[2]. These statistics point out the importance of security in today's society and the software technology systems that we use.

The traditional waterfall model of software development goes through five distinct phases; requirements, design, implementation, verification, and maintenance[3]. Security concerns are treated in the late stages of the project, just before release[4]. This model holds no considerations towards the continuous change in requirements in today´s digital world[5]. DevOps, on the other hand, is a process that goes through development stages over and over again. It allows requirements to change, developing, releasing, and maintaining continuously[4].

One large risk with DevOps is the impact it has on security. Several challenges arise with DevOps from a security point of view e.g sacrifice of security for speed/agility, an afterthought in the process and environment risks[6]. In short, 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, just before release. This is what DevSecOps addresses. It takes the continuous development and deployment process of DevOps and implements security into that process. DevOps require security to be an everyday topic, therefore the need for DevSecOps[4]. It is clear that security is a big part of DevOps, but will DevSecOps replace DevOps? This essay will look deeper into DevSecOps and investigate if DevSecOps is the new DevOps.

[1] https://www.varonis.com/blog/cybersecurity-statistics/

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 looks as in figure 1. The different parts of development and operations are put together in a continuous workflow.

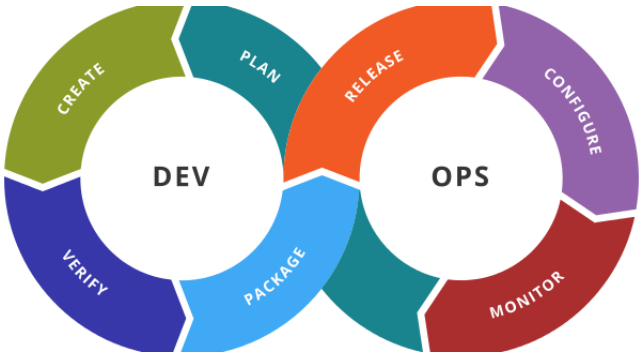

Figure 1: Workflow in DevOps [7]

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 the DevOps process within five years. This would imply that the majority of the companies have adopted the DevOps way of working[9].

Features that characterize DevOps can be divided into four categories culture, automation, measurement, and sharing. First up 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[10].

3 DevSecOps

Security is one of the main concerns for those who are reluctant to transition over to DevOps. It might be difficult to ensure security with the amount of automation introduced in DevOps[9]. 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[11].

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[9]. 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*[1]. 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.

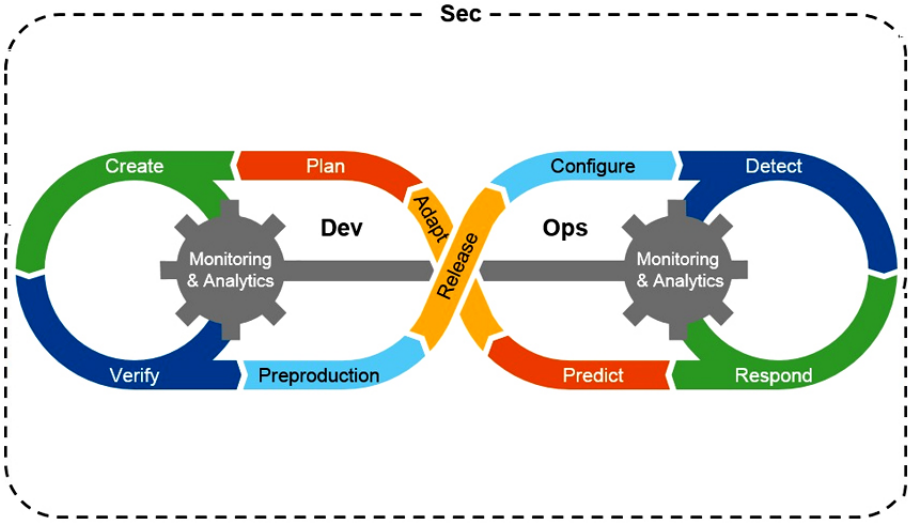

Figure 2: Security implemented in DevOps [12]

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 keep ensure that the security standards are kept[10]. 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[4]. Automation in DevSecOps means using tools and code to run routine security tests[10]. Some common practices are continuous testing and security as code[6]. However, it is important to select the right tools that can integrate security into the organization since more and new tools always bring a certain level och risk[13].

Measuring in DevSecOps includes keeping logs on different security threats and vulnerabilities within the system. Measuring also includes measuring monitoring and measuring 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 for the security engineers to attack potential problems earlier in the process[10] by doing threat modeling and running risk assessments[6].

4 DevSecOps practices

The security goal for a software technology company is to secure their customers digital assets. The books *"Hands on Security in DevOps"* lists three areas as the 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.

In continuous integration, there is a need for different security practices. The development phase requires secure coding, building, testing, and deployment. There exist tools on the market that can be used for security purposes in these phases. Open source scanning software is available for static code analysis. Another useful tool is compile-time software that scans for buffer overflows. This open-source software saves companies a lot of time and money, but it can also pose a security risk. Some also argue that open source software is safer since more people are working on the code. The risk still exists with using code developed by someone else. To improve security when using this type of software, some tools can help you scan these libraries and projects and detect potential risks and vulnerabilities[14].

Another useful thing in software development is *security incident process*, which describes what should be done in case of a security breach. The first part of this document 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[11].

To implement a successful DevSecOps process, practices like these play a key part. Some tools and guides that could be used in DevSecOps development are [15][11];

- OWASP[2] with the SAMMM (Software Assurance Maturity Model) which

[2]https://owasp.org/

can help a company determine the maturity of their security practices. They also publish guides on secure practices.

- Microsoft SDL[3], is a guide to secure practices developed and used by Microsoft.
- SAFECode[4], a non-profit organisation that publishes the *Fundamental Practices for secure software development: Essential elements of a secure development lifecycle program*, a guide to secure coding.

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[6].

As mentioned, culture is one of the pillars of DevSecOps. Implementing DevSecOps, therefore, means implementing a new culture in a workplace. This comes with some challenges since many people are hesitant to change. This could indicate that changing workflow from DevOps to DevSecOps will be met with reluctance. 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[16].

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, which slows down development. Bridging these two parts of a software development company is however crucial for the DevSecOps aspect of sharing data, knowledge, and education[17].

Some of the external challenges with implementing DevOps 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 found a base in the industry[6].

Automation also brings challenges. Automating security checks by integrating more tests into the verification process could lead to extensive time spent on daily builds. Although, adding security tests could also lead to more vulnerabilities being detected early in the process which potentially could save time later on[4].

Some people worry that adapting to security concerns continuously could hinder creativity. For a company to be competitive it has to be innovative and continuously challenge its products and try new ideas. However, no matter what, the final product has to be secure[17].

[3]https://www.microsoft.com/en-us/securityengineering/sdl
[4]https://safecode.org/

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 that improving performance with the help of DevOps does not imply that any cornerstones of software development have been cut out. Still, the consensus remains that security has to be integrated into DevOps to keep a sustainable work process[6].

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 there are many tools available to automate the security verification. On the other hand, these tools can also pose a security threat if they are not scanned properly before use. Useful tools are free guides on secure software development.

To conclude and answer the initial question *Is DevSecOps the new DevOps?*. There is no doubt that security is needed but does the name have to change to implement security? Many companies would label their work process as DevOps, even though they have extensively implemented security, and thus do not use the word DevSecOps.

References

[1] *SecDevOps: Is It a Marketing Buzzword? - Mapping Research on Security in DevOps*. 2016. DOI: 10.1109/ARES.2016.92.

[2] 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/.

[3] URL: https://en.wikipedia.org/wiki/Waterfall_model.

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

[5] 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.

[6] 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.

[7] 2021. URL: https://www.frontit.se/inspiration-kunskap/artiklar/devops-ci-cd-vad-betyder-det-egentligen/.

[8] Christof Ebert et al. "DevOps". In: *Ieee Software* 33.3 (2016), pp. 94–100.

[9] 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.

[10] 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.

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

[12] 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.

[13] *What is DevSecOps?* URL: https://www.redhat.com/en/topics/devops/what-is-devsecops.

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

[15] Laurie Williams. "Secure software lifecycle knowledge area". In: *The National Cyber Security Centre* (2019).

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

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