Exploring the Emergence and Differentiation of SecDevOps from DevSecOps

Max Wiktorsson, maxwik@kth.se & Emil Härdling, emihar@kth.se
DD2482 Automated Software Testing 2023

We certify that generative AI, incl. ChatGPT, has not been used to write this essay. Using generative AI without permission is considered academic misconduct.

1. Introduction

Historically, most development teams are highly process driven. It resembles a factory line, one activity is started after another is done. It is stated that this has been favorable for developers, as they get to complete one task of code, pass it along, and go on to another task (Reynolds, J., 2022). However, it is also stated that security has ended up becoming all the more an afterthought as in the traditional process of devops, security was not included. Therefore, DevSecOps was developed. DevSecOps promised to include security in the process in addition to development and operations.As with many buzzwords, especially within IT, a lot of different definitions exist and the same word can therefore mean something different to each individual. The integration of security into DevOps is most known as DevSecOps where security is an integral part. However, words such as SecDevOps and DevOpsSec have also been coined and said to either be defined as the same thing or something else. The most popular alternative interpretation of SecDevOps is that it places security as number one priority rather than being of equal importance as development and operations. However, a large number of studies refer to SecDevOps as the same as DevSecOps. This paper aims to give an overview of the current state of these terms and gather the opinions regarding these terms in regards to the domain of DevOps.

2. Background

In order to analyze the similarities and differences of DevSecOps and SecDevOps, a background of both will be given and also a walkthrough on how security is relevant in the DevOps process.

2.1 Implementing security in the DevOps process

The structure of every DevOps project is unique and customized to fit the organization but the parts that make the structure are often common in a broad sense. Both terms of SecDevOps and DevSecOps are depicted as the practice of integration security practices in the DevOps process (Mohan, V., & Othmane, L. B., 2016). The following is a list of elements within DevOps where security is implemented to make for a more secure process.

1. **Container Security**

Containers are a central element of modern DevOps processes which also makes them a primary concern from a security perspective. Container security takes form in three dimensions; *Image scanning, Minimal base images, Drift protection (What is DevSecOps?, 2023)*.

2. **Infrastructure Automation**

Automation is a primary focus in DevSecOps and is heavily used to detect vulnerabilities and configuration issues accores the infrastructure. There are two common automation methods: *Configuration management* and *Infrastructure as Code (Iac).*

3. **Application Analysis**

The process of analyzing the application and finding quality issues or other known vulnerabilities. The application analysis is both conducted on source code and live environments and is often in the form of tools and technologies rather than processes.

4. **Identity and Access Management (IAM)**

A set of methods used to centrally define policies in order to control the access to applications and data. Common methods used in IAM are; Authentication, Authorization and Role-based access controls. IAM can also include access and security around hardware, servers and identity providers.

5. **Network Controls and Segmentation**

The use of containerized applications and microservices has become more popular and thus DevOps teams use methods to segregate, visualize and control the container network. Common method to incorporate security is to implement a container orchestration network security policy to help gain control and visibility.

6. **Data Controls**

Data controls refers to the protection of data in both rest and motion with the goal of preventing unauthorized data leakage. There are three common methods; Encryption, Protection, and Masking.

7. **Auditing, Monitoring, and Alerting**

Closely monitoring the production environment allows for greater insights and faster response time into security incidents. For example using a security information and event management system to centralize event reporting instead of having a separate log for distributed containers and services.

8. **Remediation**

Automatic remediation allows DevOps teams to improve uptime and most importantly prevent threats and breaches from spreading in the environment. The security aspect here is mostly focused on achieving an automatic system to better evaluate and identify threats but it can also allow for greater incident traceability in the environment.

2.2 Interpretation on DevSecOps and SecDevOps

This section will state the two definitions that have been found on the internet in articles and studies that differentiate from each other.

2.2.1 DevSecOps

Development Security Operations (DevSecOps) is a way of working that applies security through scanning, monitoring, and remediation across the software development lifecycle (SDLC). Through a more integrated security aspect within DevOps, it allows organizations to deliver more secure software without compromising time or cost (Myrbakken & Colomo-Palacios, 2017).

DevSecOps is centered around a culture of collaboration between development, operations and security teams. The security team/individuals focus on implementing automatic security controls in order to not hinder DevOps's agility while maintaining a high security standard. Overall, security becomes a layer on top of DevOps, where it affects all the parts from the beginning rather than at the end. The following figure illustrates this view (Sánchez-Gordón, M., 2020).

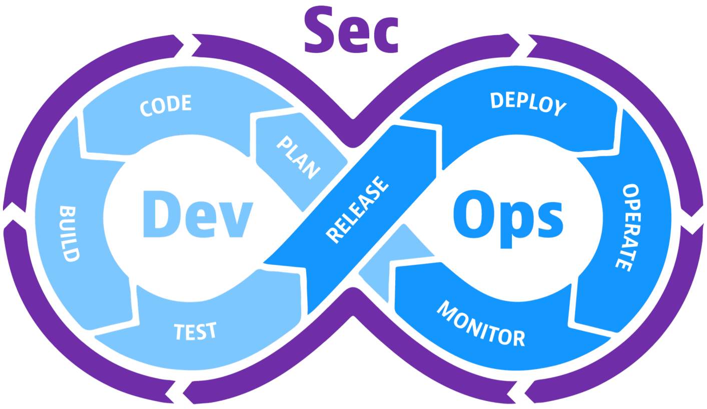

Figure 1, Illustration of DevSecOps

2.3.1 SecDevOps

In SecDevOps, security is embraced in every aspect of software design and operations, and involves integrating security into the development and deployment cycle. The distinction from DevSecOps is the shift of focus and priority of placing security in the beginning of the process rather than in the middle or later stages. Hence, developers are educated and encouraged to incorporate security processes and principles from the start when designing applications (Bhandari, P., 2022). This means that less time and effort is placed on implementing an incident response system and more focused on ensuring high security from the planning stage, effectively turning the traditional funnel process of Development, Operations and Security the opposite way around (Cure, A., 2019). This way of working effectively aims to remove the use of a security team and rather make the developers solely in charge of ensuring high security standards.

3. Analysis

In this chapter the two processes of DevSecOps and SecDevOps are put into context together. The processes will be analyzed where the domain of security and the development process will be examined.

3.1 Similarities between DevSecOps and SecDevOps

As both terms originate from the same source, DevOps, similarities are prone to exist. In order to better state the difference of these terms, a comparison on how they are similar will first be done in hope of getting a more comprehensive understanding. The process and goal of bringing the development and operations team together is similar in both definitions and differentiate very little from each other. What is more particularly noteworthy is that the two definitions share some similarity in their perspective and implementation of security in the DevOps workflow even though they are supposed to be two different ways of working.

What both terms share in security perspective is implementing security throughout the whole SDLC. SecDevOps and DevSecOps try to automate and incorporate security in all aspects in order to achieve a higher observability and overview of the environment and system. Meaning that there is not a designated place within the workflow where security checks are conducted. This similarity can be regarded as one of the reasons why SecDevOps and DevSecOps are often used interchangeably, as they rely on the same fundamental principle that security should be conducted in every step and not just in the beginning, middle or end.

3.2 Differences between DevSecOps and SecDevOps

When distinguishing between these two types of development processes, the nature of how security is integrated in them are the central differences that impact these processes. As DevSecOps is primarily focused at integrating security into the already established process of devops. In term, that means that security will often be integrated in the devops process by running security tests or other security measures on the code that is written, as described in section 2.1.1 in the *Application analysis* step.

SecDevOps on the other hand, have security at its core of the process (Gudepu, R., 2021). One key difference for the two methods of SecDevOps and DevSecOps is that DevSecOps often is depicted as prioritizing the steps of DevOps while implementing security, while SecDevOps prioritizes security as much as the actual steps of DevOps (Gudepu, R., 2021). Meaning that DevSecOps places a bigger emphasis on efficiency. Furthermore, it is stated that security will be implemented in the entire lifecycle of the development process in both processes, there exists differences in how it should be implemented. It is stated that in DevSecOps, security is integrated into the process but that the priority is to integrate testing tools into the pipeline (*What is secure devops? SecDevOps explained,* 2022), which in theory could create a seamless development process. In comparison, SecDevOps is stated to implement security in all parts of the process where it always comes first. In relation to how the team collaboration looks in the two processes there is also a distinction that often is brought up. In DevSecOps the processes around development and security are transparent to all parties in between the two teams. In SecDevOps all parties work regularly together where all parties are responsible for the security. Finally it is also acknowledged that there exists differences in how scans for vulnerabilities are implemented. In DevSecOps security testing has been implemented in the regular development testing, while in SecDevOps security checks will instead be integrated throughout the development process (Chan, Z., 2022). To give an overview of the differences brought up in this section, the differences found are represented in *table 1* below.

Area	**DevSecOps**	**SecDevOps**
Prioritization.	Efficiency of the development process and security is both prioritized.	Security is always prioritization number one.
Implementation of security in the DevOps process.	Security is integrated in the process but focuses on implementing tools för security in the pipeline.	Security is implemented in all parts of the process where it has the highest priority.
Collaboration in between teams.	Processes between development and security teams are transparent.	Teams work closely together where all parties are responsible for security.
Searching for vulnerabilities	In the regular development testing, security testing is implemented.	In the development process, security checks are integrated throughout.

Table 1, Representing the differences between DevSecOps and SecDevOps that has been found in this paper.

3.3 Critique towards the distinction between the terms

Above, perspectives based on sources that explained how the two terms of SecDevOps and DevSecOps could be differentiated was presented. However, there also exist sources that voice their perspective that these two terms actually do not have a basis to be differentiated. In this section, this perspective will be presented in this section to give an overview of the subject at hand.

In an article by Koen Vastmans, he highlights what he finds to be recurring problems within IT and the DevOps industry. He finds that DevOps should not be extended with pre- or suffixes as it only adds complexity and uncertainty to DevOps. Vastmans lifts the argument that if you add a prefix when implementing something to the DevOps way of working then there should also exist ChaosDevOps or ScaledDevOps. This illustrates that SecDevOps and also DevSecOps are unnecessary terms as every DevOps team should aim to incorporate security in their DevOps team. Vastman believes that new terms like these are made up by security companies to easier sell solutions (Vastmans, K., 2022).

In contrast to the article written by Koen Vastmans, a blog by Aria Cyber Security states that the term DevSecOps is badly coined and that SecDevOps should be the only term used to describe security in DevOps team. They explain that incorporating security in the manner of DevSecOps does not give enough time and resources to truly achieve a high degree of security. Instead they believe that SecDevOps is the best approach for a DevOps team and feel that the terms should not be used interchangeably. Important to note here is that like Vastmans stated in his article, the advocate for a new term like SecDevOps is pushed by a security company. (*DevSecOps vs. SecDevOps vs. DevOpsSec: Is there really a difference in these secure DevOps terms?,* 2018)

4. Conclusion

While the two terms of SecDevOps and DevSecOps are closely related, definitions and examples exist that showcase the differences between the two processes. Depending on who you ask, they will give different definitions and perspectives on what DevSecOps is and also if there actually is any difference from SecDevOps.

Multiple conclusions can be made and argued for depending on what one finds to be true or important. One conclusion is that the IT industry is plagued by buzzwords and constantly redefining new processes in order to appear more innovative. Thus, the words SecDevOps and DevSecOps don't differentiate from each other but rather can be used interchangeably.

However, one might argue that there actually is a difference and that SecDevOps is taking the "Shift Left" approach a step further within DevOps by incorporating security truly in the beginning of each step.

The key takeaway here is that the definition of SecDevOps is something everyone has different definitions of and something to be careful with when talking about publicly. There are a lot of developers who even refrain from using any security prefixes accompanied with DevOps due that they find it confusing.

5. References

Aria. (2018, June 14). *DevSecOps vs. SecDevOps vs. DevOpsSec: Is there really a difference in these secure DevOps terms?* Aria Cyber Security. Retrieved May 7, 2023, from https://blog.ariacybersecurity.com/blog/devsecops-vs-secdevops-blog

Bhandari, P. (2022, September 14). *SecDevOps: What is it, and do you need it in your organization?* Continuous Intelligence with Real Time AI. Retrieved May 7, 2023, from https://www.xenonstack.com/insights/secdevops

Chan, Z. (2022, October 28). *AppSec: Secdevops or DevSecOps? do we need to choose? guide to the what and the why*. HackerNoon. Retrieved May 7, 2023, from https://hackernoon.com/appsec-secdevops-or-devsecops-do-we-need-to-choose-guide-to-the-what-and-the-why

Cure, A. (2019, December 12). *What is SecDevOps and why is it so important?* AltexSoft. Retrieved May 7, 2023, from https://www.altexsoft.com/blog/what-is-secdevops/

Gudepu, R. (2021, December 28). *SecDevOps vs DevSecOps: A distinction with a difference*. Security Magazine RSS. Retrieved May 5, 2023, from https://www.securitymagazine.com/articles/96811-secdevops-vs-devsecops-a-distinction-with-a-difference

Mohan, V., & Othmane, L. B. (2016). SecDevOps: Is it a marketing buzzword? - mapping research on security in DevOps. *2016 11th International Conference on Availability, Reliability and Security (ARES)*. https://doi.org/10.1109/ares.2016.92

Myrbakken, H., & Colomo-Palacios, R. (2017). DevSecOps: A Multivocal Literature Review. *Communications in Computer and Information Science*, 17–29. https://doi.org/10.1007/978-3-319-67383-7_2

Reynolds, J. (2022, May 4). *SecDevOps: A practical guide to the what and the why*. Plutora. Retrieved May 7, 2023, from https://www.plutora.com/blog/secdevops-a-practical-guide-to-the-what-and-the-why

Sánchez-Gordón, M., & Colomo-Palacios, R. (2020). Security as culture. *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*. https://doi.org/10.1145/3387940.3392233

Vastmans, K. (2022, May 3). *DevSecOps, SecDevOps or DevOpsSec - really?* LinkedIn. Retrieved May 7, 2023, from https://www.linkedin.com/pulse/devsecops-secdevops-devopssec-really-koen-vastmans

What is DevSecOps? Aqua. (2023, February 27). Retrieved May 4, 2023, from https://www.aquasec.com/cloud-native-academy/devsecops/devsecops/

What is secure devops? SecDevOps explained. Code Signing Store. (2022, April 18). Retrieved May 4, 2023, from https://codesigningstore.com/what-is-secure-devops