The Great Debate - The Future of SRM by Group 1

DevSecOps

Introduction

DevOps

- DevOps, as from the name, is a combination of software developers (dev) and operations (ops).
- It is a software engineering methodology that combines the work of software development and software operations teams so as to automate and deliver new software updates while guaranteeing their effectiveness, security and reliability (Leite, et al., 2020)
- Its concept commenced in 2008 from Andrew Clay and Patrick Debois' discussions on Agile's drawbacks and they wanted to come up with something better. In 2009, DevOpsDays event was held in Belgium thus spreading the concept even more (Agarwal, 2019), and since then, it has kept on evolving.

Introduction 2

DevSecOps

- Also known as Secure DevOps, DevSecOps emphasizes on integrating security early in the software development lifecycle (SDLC), a practice known as "shifting security to the left, " as opposed to the DevOps model, which assigns security review and testing to separate security teams in the later phases of SDLC.
- Unlike DevOps, DevSecOps is extremely vigilant about integrating security into every phase/stage of software development. (Kumaran, N.D.)

Introduction 3

DevSecOps

- The COVID 19 pandemic is the latest and most powerful accelerant for digitalization.
- This resulting to the use of emerging technologies such as: containerization, edge computing, cloud computing, etc. - to have and continue to increase drastically. All of this points to the need for organizations to take security risk into account throughout the modern software development life cycle.
- DevSecOps adoption is on the rise, and still emerges as a best practice for developing secure, high-quality code.
- For instance, according to GitLab's 2021 Global DevSecOps Survey, 36% of respondents develop software using DevSecOps, compared with only 27% in 2020 (Horwitz, 2022).

Introduction 4

DevSecOps

- As DevSecOps practices grow in 2022, there are several concurrent technology trends that will likely further DevSecOps adoption. These DevSecOps trends will also aid teams as they integrate security and compliance into processes without slowing innovation or creating additional work for already time-strapped teams. (Horwitz, 2022).
  - Increased adoption of Infrastructure as code (IaC)
  - Mounting attacks via vulnerable third-party code
  - AIOps for root-cause analysis becomes critical
  - Weighing ML-based observability vs. AIOps

Introduction 4

DevSecOps

- GitOps becomes the new normal
- Kubernetes infrastructure evolves
- Serverless architecture expands
- Microservices gain ground over monolithic app development

References

- Leite, L. et al., 2020. A Survey of DevOps Concepts and Challenges. *ACM Computing Surveys,* 52(6), pp. 1-35.
- Agarwal, H., 2019. Roadmap to IT Revolution: DevOps History. [Online] Available at: https://www.appknox.com/blog/history-of-devops [Accessed 25 10 2022].
- Kumaran, S. M., N.D.. *DevSecOps-Securing Cyber Security.* [Online] Available at: https://www.nic.in/blogs/devsecops-securing-cyber-security/ [Accessed 25 10 2022].
- Horwitz, L., 2022. The top eight DevSecOps trends in 2022. [Online] Available at: https://www.dynatrace.com/news/blog/top-eight-devsecops-trends/ [Accessed 25 10 2022].