# WOLDIA UNIVERSITY

## Institute of Technology

## School of Computing

### Department of Software Engineering

### Software Engineering Tools and Practices

### Course title: SEng3051

NAME: MEBA TADESSE
ID: 146733

SUBMITTED TO: MR. ISMAEL
SUBMITTION DATE: MAY30/20204

TABLE OF CONTENT

Introduction

Causes for the initiation of DevSecOps ........ 3

DevSecOps ........ 4

Lifecycle of DevSecOps ........ 5

i. Planning and Design: ........ 5

ii. Development: ........ 5

iii. Deployment: ........ 5

iv. Operation: ........ 5

v. Feedback and Improvement: ........ 5

DevSecOps tools ........ 7

Benefits of DevSecOps ........ 8

Opportunities of DevSecOps ........ 9

CONCLUSION ........ 11

# INTRODUCTION

- DevSecOps is a software development approach that integrates security best practices into the entire software development lifecycle, form planning and design to development, deployment, and operation. This assignment covers what DevSecOps mean, how it works, the causes for the initiation, it’s lifecycle, the tools DevSecOps uses, it’s benefit and the opportunity it gives either locally or internationally as well as it’s career use.

1, What are Software engineering problems which was cause for initiation of DevSecOps.

## Causes for the initiation of DevSecOps

- Software engineering problems that contributed to the initiation of DevSecOps include:

- ✓ **Security vulnerabilities:** Traditional software development processes often neglected security considerations, leading to vulnerabilities that could be exploited by attackers.
- ✓ **Slow and manual security processes:** Security reviews and testing were often performed manually, which was time-consuming and prone to errors.
- ✓ **Lack of collaboration between developers and security teams:** Developers and security engineers worked in silos, resulting in a lack of understanding and coordination on security matters.
- ✓ **Reactive security approach:** Security was often treated as an afterthought, with fixes applied reactively after vulnerabilities were discovered.
- ✓ **Increased complexity and scale of software system:** Modern software systems are becoming increasingly complex and interconnected, making it more challenging to ensure their security.

- DevSecOps emerged as a response to these problems by integrating security best practices in to the entire software development life-cycle. By automating security processes, fostering collaboration between teams, and establishing a continuous feedback loop, DevSecOps aims to improve software security, reduce risk, and accelerate software delivery.

- Specific examples of software engineering problems that DevSecOps addresses:

- ✓ **Insecure code:** DevSecOps helps to identify and fix security vulnerabilities in code through automated code analysis and testing.
- ✓ **Configuration errors:** DevSecOps automates the configuration of security setting and infrastructure, reducing the risk of misconfiguration.
- ✓ **Lack of visibility into security risks:** DevSecOps provides real-time visibility into security risks through monitoring and logging tools.
- ✓ **Slow patching and remediation:** DevSecOps automates the patching and remediation of security vulnerabilities, reducing the time it takes to address threat.
- ✓ **Lack of security training for developers:** DevSecOps promotes security training and education for developers, empowering them to write more secure code.

2. What is DevSecOps?

## DevSecOps

- DevSecOps is a software development approach that integrates security best practices into the entire software development lifecycle, form planning and design to development, deployment, and operation.

Key principles of DevSecOps:

- ✓ **Continuous security:** security is considered at every stage of the development process, not as an afterthought.
- ✓ **Collaboration:** Developers, security engineers and operations teams work closely together to ensure security form the beginning.
- ✓ **Automation:** security tools and processes are automated to reduce manual effort and improve consistency.
- ✓ **Feedback loop:** Security vulnerabilities are identified and addressed quickly through a continuous feedback loop.
- ✓ **DevOps:** DevSecOps leverages DevOps principles such as continuous delivery and infrastructure as code.

- Benefits of DevSecOps:

- ✓ **Improved security:** By integrating security into the development lifecycle, vulnerabilities are detected and fixed earlier.
- ✓ **Faster time to market:** Security is not seen as a bottleneck, allowing for faster software releases.
- ✓ **Reduced risk:** Security risks are identified and mitigated throughout the development process, minimizing the likelihood of breaches.
- ✓ **Cost saving:** Automated security tools and processes reduce the need for manual security reviews, saving time and resources.
- ✓ **Increased collaboration:** DevSecOps promotes cross-functional collaboration, fostering better communication and understanding.

- How to implement DevSecOps:

- ✓ **Start small:** begin by integrating  security tools and process in to a specific project or team.
- ✓ **Build a team:** form a team of developers, security engineers and operation professionals.
- ✓ **Automate security:** use tools fore vulnerability scanning, code analysis, and security testing.

- ✓ **Establish and feedback loop:** Implement processes for reporting and addressing security findings.
- ✓ **Train and educate:** Provide training and resources to all team members on DevSecOps practices.

3. Briefly explain DevSecOps lifecycle?

## Lifecycle of DevSecOps

- The DevSecOps lifecycle integrates security practices into all stages of the software development lifecycle, from planning and design to development, deployment and operation. It consists of the following phases:

**i. Planning and Design:**

- Define security requirements and goals, Incorporate security considerations into the software architecture and design, Establish a threat modeling process.

**ii. Development:**

- Implement secure coding practices and use automated security tools.
- Perform regular code reviews and security testing.
- Integrate security into the continuous integration/ continuous delivery(CI/CD) pipeline.

**iii. Deployment:**

- Deploy software into secure environments using infrastructure as code.
- Configure security settings and monitoring tools.
- Perform security testing and vulnerability scanning in production.

iv. **Operation**:

- Monitor and log security events.
- Respond to security incidents and breaches.
- Implement continuous security monitoring and threat intelligence.

**v. Feedback and Improvement:**

- Gather feedback on security vulnerabilities and incidents.
- Analyze security data to identify trends and patterns.
- continuously improve security processes and practice.

- Throughout the lifecycle, there is a strong emphasis on collaboration between developers, security engineers, and operations team. Automated tools and processes are used to reduce manual effort and improve consistency. A continuous feedback loop is established to ensure that security vulnerabilities are identified and addressed quickly.

- By integrating security into every phase of the software development lifecycle, DevSecOps helps organization to build and deploy more secure software, reduce risk and accelerate software delivery.

4. How dose DevSecOps works?

- DevSecOps works by integrating security practices into all stages of the software development lifecycle, from planning and design to development , deployment and operation. It involves collaboration between developers, security engineers and operations teams, as well as the use of automated tools and processes.

Key aspects of how DevSecOps works:

✓ **Security is considered from the beginning:** Secure requirements and goals are defined during the planning and design phase, and security consideration are incorporated into the software architecture and design.

✓ **Automated security tools are used throughout the lifecycle:** Automated tools are used for code analysis, vulnerability scanning, and security testing. These tools help to identify and fix security vulnerabilities early in the development process.

✓ **Security is integrated into the CI/CD pipeline:** Security checks and tests are integrated into the continuous delivery(CI/CD) pipeline. This ensures that security is considered at every stage of the software delivery process.

✓ **Collaboration between teams is essential:** Developers, security engineers and operations team work closely together to ensure that security is shared responsibility This collaboration helps to breakdown silos and improve communication.

✓

✓ **A continuous feedback loop is established:** Security vulnerability and incidents are reported and analyzed, and feedback is used to improve security processes and practice. This continuous feedback loop helps to ensure that security is constantly improving.

Specific examples of how DevSecOps works:

- ✓ Secure code is written using automated tools to identify and fix security vulnerabilities in heir code.
- ✓ **Security testing is performed throughout the development lifecycle:** Security engineers perform regular security testing, including penetration testing and vulnerability scanning, to identify and address security risks.
- ✓ **Infrastructure is provisioned and configures securely:** Operations teams use infrastructure as code to provision and configure secure environments for software deployment.
- ✓ **Security monitoring is continuous:** Security monitoring tools are used to monitor and log security events in production environments. This helps to identify and respond to security incidents quickly.
- ✓ **Security training and education is provided:** Developers, security engineers and operations teams receive regular security training and education to stay up-to-date on the latest security threats and best practices.

- Overall, DevSecOps works by integrating security into every aspect of the software development lifecycle, automating security processes, and fostering collaboration between teams. This helps organizations to build and deploy more secure software, reduce risk and accelerate software delivery.

5. Ex-line well known DevSecOps tools.

## DevSecOps tools

- Five well-known DevSecOps tools are:

- ✓ **JFrog Artifactory:** A binary repository manager that provides security features such as vulnerability scanning, license compliance, and malware detection.

- ✓ **Aqua security:** A container security platform that provides vulnerability scanning, runtime protection and compliance for containerized applications.

- ✓ **Veracode:** A static and dynamic application security testing platform that helps developers identify and fix security vulnerabilities in their code.

- ✓ **Sysdig Secure:** A cloud-native security platform that provides runtime security, vulnerability management, and compliance for containers and kubernetes.

- ✓ **GitLab:** A DevOps platform that includes security features such as code scanning, vulnerability management and compliance scanning.

- These tools are widely used by organizations to implement DevSecOps practices and improve the security of their software development lifecycle. They provide a range of capabilities to help organizations identify and fix security vulnerabilities, enforce security policies and monitor and respond to security events.

6. What are the benefits of DevSecOps?

## Benefits of DevSecOps

- ✓ **Improved security:** DevSecOps integrates security into every stage of the software development lifecycle, reducing the risk of vulnerabilities and breaches.
- ✓ **Faster time to market:** By automating security processes and fostering collaboration, DevSecOps enables organizations to deliver secure software faster.
- ✓ **Reduced risk:** DevSecOps helps organizations to identify and mitigate security risks early in the development process, minimizing the likelihood of costly incidents.
- ✓ **Increased collaboration:** DevSecOps promotes cross-functional collaboration between developers, security engineers, and operations teams, fostering better communication and understanding.
- ✓ **Improved compliance:** DevSecOps helps organizations to meet regulatory compliance requirements by providing visibility into security risks and controls.
- ✓ **Competitive advantage:** Organizations that embrace DevSecOps gain a competitive advantage by delivering more secure and reliable software faster.

Specific examples of benefits of DevSecOps:

- ✓ **Reduced time to patch vulnerabilities:** Automated vulnerability scanning and patching tools help organizations to identify and fix security vulnerabilities quick, reducing the risk of exploitation.

- ✓ **Improved code quality:** static and Dynamic application of testing tools help developers to identify and fix security vulnerabilities in their code, improving the overall quality of software.

- ✓ **Simplified compliance:** DevSecOps platforms provide visibility into security risks and compliance status, making it easier for organizations to meet regulatory requirements.

- ✓ **Reduced downtime:** By identifying and mitigating security risks early in the development process, DevSecOps helps to reduce the risk of outages and downtime.
- ✓ **Increased customer trust:** Organizations that implement DevSecOps can demonstrate to their customers that they are committed to delivering secure software, building trust and loyalty.

- Overall, DevSecOps provides a range of benefits that help organizations to improve their security posture, accelerate software delivery, and gain a competitive advantage.

7. About Local and international DevSecOps career opportunities, career path

## <u>Opportunities of DevSecOps</u>

- DevSecOps is a rapidly growing field with high demand for skilled professionals. Career opportunities exist in a variety of industries, including technology, finance, healthcare, and government.

*** Local Career Opportunities**

- ✓ **DevSecOps Engineer:** Responsible for implementing and maintaining DevSecOps practices within an organization.

- ✓ **Security Engineer with DevSecOps Focus:** Focuses on integrating security into the software development lifecycle and working closely with development teams.

- ✓ **DevOps Engineer with Security Expertise:** Possesses both DevOps and security skills and works to bridge the gap between development and security teams.

- ✓ **Cloud Security Engineer with DevSecOps Experience:** Specializes in securing cloud environments using DevSecOps principles.

- ✓ **DevSecOps consultant:** Provides guidance and support to organizations on implementing DevSecOps practices.

*** International Career Opportunities**

- The demands for DevSecOps professionals is also high internationally. Many multinational companies and organizations are seeking to hire DevSecOps engineers and consultants to help them improve their software security and development practices.

*** Career Path**

- A typical career path for DevSecOps professional might start with a role as a software developer or security engineer. With experience and training, individuals can progress to more senior roles such as DevSecOps engineer, security engineer with DevSecOps focus, or DevSecOps engineer with security expertise.
- Some professionals may also choose to specialize in a particular area of DevSecOps, such as cloud security, container security, or compliance.

-To advance DevSecOps career

- ✓ Gain experience in both software development and security.
- ✓ Obtain certifications in DevSecOps or related fields.
- ✓ Stay up-to-date on the latest DevSecOps trends and best practices.
- ✓ Network with other DevSecOps professionals and attend industry events.
- ✓ Seek opportunities to lead DevSecOps initiatives within your organization.

- DevSecOps is a rewarding and in-demand career field that offers opportunities for both local and international employment. With the right skills and experience, individuals can advance their careers and make a significant contribution to the security and efficiency of software development.

# CONCLUSION

- DevSecOps emerged as a response to these problems by integrating security best practices in to the entire software development life-cycle. By automating security processes, fostering collaboration between teams, and establishing a continuous feedback loop, DevSecOps aims to improve software security, reduce risk, and accelerate software delivery. DevSecOps works by integrating security into every aspect of the software development lifecycle, automating security processes, and fostering collaboration between teams. This helps organizations to build and deploy more secure software, reduce risk and accelerate software delivery. By integrating security into every phase of the software development lifecycle, DevSecOps helps organization to build and deploy more secure software, reduce risk and accelerate software delivery. DevSecOps is a rewarding and in-demand career field that offers opportunities for both local and international employment. With the right skills and experience, individuals can advance their careers and make a significant contribution to the security and efficiency of software development.