SCHOOL OF COMPUTING

DEPARTMENT OF SOFTWARE ENGINEERING

SOFTWARE ENGINEERING TOOLS AND PRACTICES

INDIVIDUAL ASSIGNMENT on DevSecOps.

COURSE NAME: SOFTWARE ENGINEERING TOOLS AND PRACTICES

COURSE CODE: SEng3071

NAME: GELETA BIRHANU

ID NO: 14 62 02

Submitted to Mr.ESMAEL

SUBMITTED Date: 21/09/2EC

Contents

Introduction

- **This assignment talks about DevSecOps definition** and info below
- Software engineering problems which was cause for initiation of DevSecOps
- Defines the key benefits of DevSecOps
- Defines about DevSecOps lifecycles
- You get answer about How dose DevSecOps works?
- well known DevSecOps tools
- About Local and international DevSecOps career opportunities, career path
- the key practices of DevSecOps

Software engineering problems which was cause for initiation of DevSecOps

Software engineering problems that caused the initiation of DevSecOps:

• Security vulnerabilities: Traditional software development processes often did not prioritize security, leading to vulnerabilities that could be exploited by attackers.

• Slow and error-prone manual security testing: Security testing was often performed manually, which was slow and error-prone. This meant that vulnerabilities could be missed, or that security fixes could introduce new bugs.

• Lack of collaboration between development and security teams: Development and security teams often worked in silos, which led to a lack of communication and coordination. This made it difficult to identify and fix security vulnerabilities early in the development process.

• Difficulty in keeping up with the pace of software development: The rapid pace of software development made it difficult for security teams to keep up. This meant that security vulnerabilities could be introduced into new software releases without being detected.

DevSecOps aims to address these problems by:

• Integrating security into the software development process from the beginning: Security is no longer an afterthought, but is considered throughout the development lifecycle.

• Automating security testing: Automated security testing tools can be used to quickly and accurately identify vulnerabilities.

• Fostering collaboration between development and security teams: DevSecOps encourages close collaboration between development and security teams, so that security concerns can be addressed early in the development process.

• Providing continuous security monitoring: DevSecOps tools can be used to continuously monitor software for security vulnerabilities, so that they can be fixed quickly.

By addressing these problems, DevSecOps helps to improve the security of software, while also making the development process more efficient and effective.

What is DevSecOps?

DevSecOps is a software development approach that integrates security into the software development process from the beginning. It is a combination of the DevOps and security disciplines, and it aims to improve the security of software while also making the development process more efficient and effective.

DevSecOps teams typically use a variety of tools and techniques to automate security testing and monitoring, and to foster collaboration between development and security teams. This helps to ensure that security is considered throughout the development lifecycle, and that vulnerabilities are identified and fixed early in the process.

Some of the key benefits of DevSecOps include:

• Improved security: DevSecOps helps to improve the security of software by integrating security into the development process from the beginning. This helps to identify and fix vulnerabilities early in the process, before they can be exploited by attackers.

• Faster development: DevSecOps can help to speed up the development process by automating security testing and monitoring. This frees up developers to focus on writing code, and it helps to ensure that security is not a bottleneck in the development process.

• Reduced costs: DevSecOps can help to reduce costs by preventing security breaches. Security breaches can be costly, both in terms of financial losses and reputational damage. DevSecOps helps to prevent these breaches by identifying and fixing vulnerabilities early in the development process.

Overall, DevSecOps is a valuable approach to software development that can help to improve security, speed up development, and reduce costs.

Here are some of the key practices of DevSecOps:

• Security testing is automated: Automated security testing tools can be used to quickly and accurately identify vulnerabilities. This helps to ensure that vulnerabilities are found early in the development process, before they can be exploited by attackers.

• Security is integrated into the development process: Security is no longer an afterthought, but is considered throughout the development lifecycle. This helps to ensure that security vulnerabilities are identified and fixed early in the process, before they can be introduced into production software.

• Development and security teams collaborate closely: DevSecOps encourages close collaboration between development and security teams. This helps to ensure that security concerns are addressed early in the development process, and that security fixes do not introduce new bugs.

• Continuous security monitoring is used: DevSecOps tools can be used to continuously monitor software for security vulnerabilities. This helps to ensure that vulnerabilities are identified and fixed quickly, before they can be exploited by attackers.

By following these practices, DevSecOps teams can improve the security of their software, while also making the development process more efficient and effective.

DevSecOps lifecycle

The DevSecOps lifecycle is a set of practices and activities that integrate security into the software development lifecycle from the beginning. It is a collaborative approach that involves development, security, and operations teams working together to ensure that software is secure and reliable.

DevSecOps lifecycle stages:

The DevSecOps lifecycle typically includes the following stages:

1. Plan: In the planning stage, the team defines the security goals and requirements for the project. This includes identifying the threats that the software is most likely to face, and developing a plan to mitigate those threats.

2. Build: In the build stage, the team develops the software code. Security controls are integrated into the code from the beginning, and automated security testing is used to identify and fix vulnerabilities early in the development process.

3. Test: In the test stage, the software is tested for security vulnerabilities. This includes both automated testing and manual testing. The goal of testing is to identify and fix any remaining vulnerabilities before the software is released to production.

4. Deploy: In the deploy stage, the software is deployed to production. Security measures are put in place to protect the software from attacks, and the software is continuously monitored for security vulnerabilities.

5. Monitor: In the monitor stage, the software is continuously monitored for security vulnerabilities. This includes both automated monitoring and manual monitoring. The goal of

monitoring is to identify and fix any vulnerabilities that may be introduced into the software after it has been deployed to production.

The DevSecOps lifecycle is an iterative process. As new threats are identified, and as the software changes, the team revisits the plan, build, test, deploy, and monitor stages to ensure that the software remains secure.

By following the DevSecOps lifecycle, teams can improve the security of their software, while also making the development process more efficient and effective.

How dose DevSecOps works?

DevSecOps works by integrating security into the software development lifecycle from the beginning. This means that security is considered at every stage of the development process, from planning and design to coding, testing, and deployment.

DevSecOps teams typically use a variety of tools and techniques to automate security testing and monitoring, and to foster collaboration between development and security teams. Some of the key tools and techniques used in DevSecOps include:

• Security testing tools: Automated security testing tools can be used to quickly and accurately identify vulnerabilities in software code. These tools can be used to scan code for known vulnerabilities, and they can also be used to perform penetration testing to identify vulnerabilities that are not known to the public.

• Security monitoring tools: Security monitoring tools can be used to continuously monitor software for security vulnerabilities. These tools can be used to detect suspicious activity, and they can also be used to alert security teams to potential threats.

• Collaboration tools: Collaboration tools can be used to improve communication and coordination between development and security teams. These tools can be used to track security issues, and they can also be used to facilitate discussions between team members.

By using these tools and techniques, DevSecOps teams can improve the security of their software, while also making the development process more efficient and effective.

Here is a simplified overview of how DevSecOps works:

1. Planning: In the planning stage, the team defines the security goals and requirements for the project. This includes identifying the threats that the software is most likely to face, and developing a plan to mitigate those threats.

2. Development: In the development stage, the team develops the software code. Security controls are integrated into the code from the beginning, and automated security testing is used to identify and fix vulnerabilities early in the development process.

3. Testing: In the testing stage, the software is tested for security vulnerabilities. This includes both automated testing and manual testing. The goal of testing is to identify and fix any remaining vulnerabilities before the software is released to production.

4. Deployment: In the deployment stage, the software is deployed to production. Security measures are put in place to protect the software from attacks, and the software is continuously monitored for security vulnerabilities.

5. Monitoring: In the monitoring stage, the software is continuously monitored for security vulnerabilities. This includes both automated monitoring and manual monitoring. The goal of monitoring is to identify and fix any vulnerabilities that may be introduced into the software after it has been deployed to production.

The DevSecOps lifecycle is an iterative process. As new threats are identified, and as the software changes, the team revisits the plan, build, test, deploy, and monitor stages to ensure that the software remains secure.

By following the DevSecOps lifecycle, teams can improve the security of their software, while also making the development process more efficient and effective.

well known DevSecOps tools

Some of the well-known DevSecOps tools include:

- Security testing tools:
  * OWASP ZAP
  * Nessus
  * Qualys Web Application Scanner
  * Burp Suite
  * SonarQube
- Security monitoring tools:
  * Splunk
  * ELK Stack
  * LogRhythm
  * QRadar
  * Sumo Logic
- Collaboration tools:
  * Jira

* Trello

* Asana

* Slack

* Microsoft Teams

In addition to these tools, there are also a number of DevSecOps platforms that provide a comprehensive suite of tools and services for automating and managing the DevSecOps lifecycle. Some of the most popular DevSecOps platforms include:

• AWS DevSecOps: AWS DevSecOps provides a range of tools and services for automating and managing the DevSecOps lifecycle on AWS.

• Azure DevOps: Azure DevOps provides a comprehensive suite of tools and services for planning, building, testing, and deploying software on Azure.

• Google Cloud DevSecOps: Google Cloud DevSecOps provides a range of tools and services for automating and managing the DevSecOps lifecycle on Google Cloud.

• JFrog Artifactory: JFrog Artifactory is a binary repository manager that provides a range of security features, including vulnerability scanning and malware detection.

• Synopsys Black Duck: Synopsys Black Duck is a software composition analysis tool that helps organizations to identify and manage open source software vulnerabilities.

These are just a few of the many DevSecOps tools and platforms that are available. By using these tools, organizations can improve the security of their software, while also making the development process more efficient and effective.

What are the benefits of DevSecOps?

Benefits of DevSecOps:

• Improved security: DevSecOps helps to improve the security of software by integrating security into the software development lifecycle from the beginning. This helps to identify and fix vulnerabilities early in the development process, before they can be exploited by attackers.

• Faster development: DevSecOps can help to speed up the development process by automating security testing and monitoring. This frees up developers to focus on writing code, and it helps to ensure that security is not a bottleneck in the development process.

• Reduced costs: DevSecOps can help to reduce costs by preventing security breaches. Security breaches can be costly, both in terms of financial losses and reputational damage. DevSecOps helps to prevent these breaches by identifying and fixing vulnerabilities early in the development process.

• Improved collaboration: DevSecOps encourages collaboration between development and security teams. This helps to ensure that security concerns are addressed early in the development process, and that security fixes do not introduce new bugs.

• Increased agility: DevSecOps helps to increase agility by enabling organizations to respond quickly to security threats. By automating security testing and monitoring, DevSecOps teams can quickly identify and fix vulnerabilities, which helps to reduce the risk of security breaches.

Overall, DevSecOps is a valuable approach to software development that can help organizations to improve security, speed up development, reduce costs, improve collaboration, and increase agility.

examples of how DevSecOps can benefit organizations:

• Reduced time to market: By automating security testing and monitoring, DevSecOps can help organizations to reduce the time it takes to bring new products and services to market.

• Improved customer satisfaction: By improving the security of software, DevSecOps can help organizations to improve customer satisfaction. Customers are more likely to be satisfied with products and services that are secure and reliable.

• Reduced risk of security breaches: By identifying and fixing vulnerabilities early in the development process, DevSecOps can help organizations to reduce the risk of security breaches. This can protect organizations from financial losses, reputational damage, and legal liability.

Overall, DevSecOps is a valuable approach to software development that can help organizations to achieve a number of benefits, including improved security, faster development, reduced costs, improved collaboration, and increased agility.

About Local and international DevSecOps career opportunities, career path

DevSecOps Career Opportunities

DevSecOps is a rapidly growing field, and there is a high demand for skilled professionals. DevSecOps engineers can work in a variety of industries, including technology, finance, healthcare, and government.

Local DevSecOps Career Opportunities

In most countries, there is a strong demand for DevSecOps engineers. This is due to the increasing awareness of the importance of security in software development. DevSecOps engineers can find jobs in a variety of companies, including startups, small businesses, and large enterprises.

Some of the most common job titles for DevSecOps engineers include:

• DevSecOps Engineer

• Security Engineer

• DevOps Engineer

• Cloud Security Engineer

• Application Security Engineer

International DevSecOps Career Opportunities

The demand for DevSecOps engineers is also strong internationally. This is due to the global nature of the software development industry. DevSecOps engineers can find jobs in a variety of countries, including the United States, the United Kingdom, Canada, Australia, and India.

Some of the most popular destinations for DevSecOps engineers include:

• Silicon Valley, USA

• London, UK

• Toronto, Canada

• Sydney, Australia

• Bangalore, India

DevSecOps Career Path

The career path for DevSecOps engineers is typically as follows:

• Junior DevSecOps Engineer: Junior DevSecOps engineers typically have a few years of experience in software development and/or security. They are responsible for performing basic DevSecOps tasks, such as security testing and monitoring.

• Mid-Level DevSecOps Engineer: Mid-level DevSecOps engineers have several years of experience in DevSecOps. They are responsible for more complex DevSecOps tasks, such as designing and implementing security solutions.

• Senior DevSecOps Engineer: Senior DevSecOps engineers have a deep understanding of DevSecOps principles and practices. They are responsible for leading DevSecOps initiatives and mentoring junior engineers.

Salaries for DevSecOps Engineers

The salaries for DevSecOps engineers vary depending on their experience, skills, and location. However, DevSecOps engineers typically earn higher salaries than software developers and security engineers.

According to Glassdoor, the average salary for a DevSecOps engineer in the United States is $115,000 per year. However, salaries can range from $80,000 to $150,000 per year or more, depending on the factors mentioned above.

DevSecOps is a rapidly growing field with a high demand for skilled professionals. DevSecOps engineers can find jobs in a variety of industries and countries, and they can earn competitive salaries. If you are interested in a career in DevSecOps, there are many resources available to help you get started.

Conclusion

DevSecOps is a software development approach that integrates security into the software development lifecycle from the beginning. It is a collaborative approach that involves development, security, and operations teams working together to ensure that software is secure and reliable.

DevSecOps offers a number of benefits, including:

• Improved security: DevSecOps helps to improve the security of software by integrating security into the software development lifecycle from the beginning. This helps to identify and fix vulnerabilities early in the development process, before they can be exploited by attackers.

• Faster development: DevSecOps can help to speed up the development process by automating security testing and monitoring. This frees up developers to focus on writing code, and it helps to ensure that security is not a bottleneck in the development process.

• Reduced costs: DevSecOps can help to reduce costs by preventing security breaches. Security breaches can be costly, both in terms of financial losses and reputational damage. DevSecOps helps to prevent these breaches by identifying and fixing vulnerabilities early in the development process.

• Improved collaboration: DevSecOps encourages collaboration between development and security teams. This helps to ensure that security concerns are addressed early in the development process, and that security fixes do not introduce new bugs.

• Increased agility: DevSecOps helps to increase agility by enabling organizations to respond quickly to security threats. By automating security testing and monitoring, DevSecOps teams can quickly identify and fix vulnerabilities, which helps to reduce the risk of security breaches.

Overall, DevSecOps is a valuable approach to software development that can help organizations to achieve a number of benefits, including improved security, faster development, reduced costs, improved collaboration, and increased agility.

The Future of DevSecOps

DevSecOps is a rapidly growing field, and it is expected to continue to grow in the years to come. This is due to the increasing awareness of the importance of security in software development. As organizations become more aware of the risks of security breaches, they are increasingly adopting DevSecOps practices to improve the security of their software.

In the future, we can expect to see even more organizations adopting DevSecOps practices. We can also expect to see the development of new DevSecOps tools and technologies. These tools and technologies will make it easier for organizations to implement and manage DevSecOps practices.

As DevSecOps continues to mature, it is likely to become an essential part of the software development process. By integrating security into the software development lifecycle from the beginning, DevSecOps can help organizations to improve the security of their software, speed up the development process, reduce costs, and improve collaboration.

Reference

- **https://cybersn.com/role/devsecops/#:~:text=Role%20overview,stage%20of%20the%20SD LC%20lifecycle.**
- **%20to%20the,before%20the y%20write%20any%20code.**
- **https://www.ibm.com/topics/devsecops#:~:text=The%20two%20main%20benefits%20of,se cure%20code%20faster%20and%20cheaper.**