INSTITUTE OF TECHNOLOGY SCHOOL OF COMPUTING DEPARTMENT OF SOFTWARE ENGINEERING

COURSE TITLE: Software Engineering Tools and Practice

Course Code: SEng3051

Name: Ermiyas Molla

Id: 1200763

SUBMITTED TO: ESMAEL M

SUBMITE DATE: 6/7/2016 E.C

Table Content **page**

1. Introduction---------- -------- 3

2. What are the software engineering problems which was cause for intention of DevsecOps ? ---------- -------4

3. what is DevSecOps? ---------- ------5

4. Briefly explain DevSecOps lifecycle? ---------- -----5

5. How does DevSecOps works ?---------- -----6

6. Explain well known DevSecOps tools .---------- -----7

7. What are the benefits of DevSecOps?---------- ----9

8. About local and international DevSecOps career opportunties career path.---------- --10

9.Conclusion---------- ---12

10.Reference---------- ----13

Introduction

DevSecOps, a transformative approach to software development, combines the principles of Development (Dev), Operations (Ops), and Security (Sec) to create a holistic and integrated methodology. By integrating security practices into the DevOps workflow, DevSecOps aims to build a culture of security throughout the software development lifecycle. This proactive approach emphasizes collaboration, automation, continuous monitoring, and a strong security culture to enhance the security posture of software applications. In this evolving digital landscape where cyber threats are constantly evolving, DevSecOps provides organizations with the tools and mindset needed to develop secure, resilient, and reliable software products

1. What are the software engineering problems which was cause for intention of DevsecOps ?

Software engineering problems such as frequent code deployment failures, slow release cycles, inconsistent environments, and lack of collaboration between development and operations teams have led to the emergence of DevSecOps practices. DevSecOps aims to integrate security practices into the software development and deployment process from the very beginning, ensuring that security is not an afterthought but an integral part of the software development lifecycle. By addressing security concerns early on and automating security testing and monitoring processes, DevSecOps helps organizations build more secure and reliable software applications.

Some of the software engineering problems that have led to the rise of DevSecOps include:

- **Security as an afterthought**: Traditionally, security has been considered a separate entity from development and operations, leading to security being added on as an afterthought. This can result in vulnerabilities being introduced during the development process.
- **Lack of collaboration**: In traditional software development processes, developers, operations teams, and security teams often work in silos, leading to a lack of communication and collaboration. This can result in security issues being overlooked or not addressed in a timely manner.
- **Slow response to security threats**: Traditional software development processes often involve long release cycles, making it difficult to respond quickly to security threats or vulnerabilities. DevSecOps aims to integrate security into the development process, allowing for faster responses to security issues.
- **Compliance challenges**: Many industries have strict regulatory requirements around data security and privacy. Traditional software development processes may struggle to meet these compliance requirements, leading to potential legal and financial risks. DevSecOps helps to ensure that security and compliance are built into the development process from the start.
- **Lack of automation**: Manual security testing and deployment processes can be time-consuming and error-prone. DevSecOps emphasizes automation throughout the software development lifecycle, helping to improve efficiency and reduce the risk of human error.

In conclusion, the software engineering problems that have plagued organizations, such as frequent code deployment failures, slow release cycles, inconsistent environments, and lack of collaboration between development and operations teams, have necessitated the adoption of DevSecOps practices. By integrating security into the software development process from the outset, DevSecOps addresses these challenges and ensures that security is a fundamental aspect of the software development lifecycle. Through automation, collaboration, and a proactive approach to security, DevSecOps helps organizations build more secure and resilient software applications, ultimately improving the overall quality and reliability of their software products.

2 . what is DevSecOps?

DevSecOps is a methodology that integrates security practices into the DevOps process, aiming to build security into every stage of the software development lifecycle. It combines development (Dev), operations (Ops), and security (Sec) to create a culture of shared responsibility for security across teams.

In traditional software development processes, security is often considered a separate concern and is addressed at the end of the development cycle. This can lead to vulnerabilities being introduced during the development process, increasing the risk of security breaches and data leaks.

DevSecOps seeks to address these challenges by promoting collaboration between developers, operations teams, and security professionals from the beginning of the development process. By integrating security practices into the DevOps workflow, organizations can ensure that security is a priority at every stage of development, deployment, and operations.

Key principles of DevSecOps include automation of security testing and compliance checks, continuous monitoring and feedback, and proactive threat detection and response. By adopting DevSecOps practices, organizations can improve the overall security posture of their applications and infrastructure while maintaining agility and speed in the software development process.

3. Briefly explain DevSecOps lifecycle?

The DevSecOps lifecycle encompasses the integration of security practices into the entire software development process, from planning and coding to testing, deployment, and operations. Here is a brief overview of the key stages in the DevSecOps lifecycle:

- **Planning:** Security considerations are incorporated into the initial planning phase of the software development process. This includes defining security requirements, threat modeling, and risk assessment.
- **Coding:** Developers write secure code by following best practices and security guidelines. Code reviews and static code analysis tools are used to identify and address security vulnerabilities early in the development process.
- **Building:** Continuous integration (CI) tools automate the build process and run security tests to ensure that the code meets security standards. This stage includes vulnerability scanning, dependency checks, and other security checks.
- **Testing:** Security testing is an integral part of the testing phase in DevSecOps. This includes dynamic application security testing (DAST), penetration testing, and fuzz testing to identify and remediate security issues.
- **Deployment:** Automated deployment pipelines are used to deploy code changes to production environments securely. Security controls such as access controls, encryption, and secure configurations are implemented during deployment.
- **Monitoring:** Continuous monitoring and logging help detect security incidents and anomalies in real-time. Security information and event management (SIEM) tools are used to monitor and respond to security threats promptly.
- **Feedback and Improvement:** Feedback from monitoring and incident response activities is used to improve security practices continuously. Lessons learned from security incidents are incorporated into future development cycles to enhance security posture.

By following this DevSecOps lifecycle, organizations can ensure that security is integrated into every stage of the software development process, leading to more secure applications and infrastructure.

4 . How does DevSecOps works?

DevSecOps works by integrating security practices into the entire software development process, from the initial planning phase to deployment and beyond. Here's how DevSecOps operates:

- **Collaboration:** DevSecOps promotes collaboration between development, security, and operations teams. By breaking down silos and fostering communication, teams can work together seamlessly to address security concerns throughout the development lifecycle.

- **Automation:** Automation is a key aspect of DevSecOps. Security tools and processes are automated wherever possible to streamline security testing, vulnerability scanning, code analysis, and compliance checks. Automation helps identify and remediate security issues quickly and efficiently.
- **Continuous Integration/Continuous Deployment (CI/CD):** DevSecOps emphasizes the use of CI/CD pipelines to automate the build, test, and deployment processes. Security checks are integrated into these pipelines to ensure that code changes meet security requirements before they are deployed to production.
- **Shift Left:** DevSecOps encourages a "shift left" approach to security, meaning that security considerations are addressed early in the development process. By incorporating security from the beginning, teams can identify and mitigate security vulnerabilities before they become more costly to fix later on.
- **Security as Code:** Just like infrastructure as code, DevSecOps treats security as code. Security policies, configurations, and controls are defined in code and managed alongside application code. This allows for consistent and repeatable security practices across environments.
- **Continuous Monitoring:** DevSecOps includes continuous monitoring of applications and infrastructure to detect security incidents in real-time. Monitoring tools provide visibility into security events, logs, and metrics, allowing teams to respond quickly to potential threats.
- **Culture of Security:** DevSecOps fosters a culture of security within organizations. Security awareness training, regular security reviews, and incident response exercises help build a strong security mindset among team members.

By following these principles and practices, DevSecOps enables organizations to build secure, resilient, and compliant software systems while maintaining a rapid pace of development and deployment.

5. Explain well known DevSecOps tools .

There are several well-known DevSecOps tools that help organizations integrate security into their software development process. Here are some popular tools used in the DevSecOps ecosystem:

- **SAST (Static Application Security Testing) Tools:**

- Checkmarx: Checkmarx is a leading SAST tool that scans code for security vulnerabilities during the development process.

- **Veracode**: Veracode offers SAST capabilities to identify and remediate security flaws in applications.

➢ DAST (Dynamic Application Security Testing) Tools:

- **OWASP ZAP (Zed Attack Proxy):** OWASP ZAP is an open-source DAST tool that helps identify security vulnerabilities in web applications.

- **Burp Suite**: Burp Suite is a popular DAST tool used for web application security testing.

➢ IAST (Interactive Application Security Testing) Tools:

- **Contrast Security**: Contrast Security offers IAST capabilities to provide real-time security feedback during development.

- **Micro Focus Fortify**: Micro Focus Fortify includes IAST features to detect and fix security issues in real-time.

➢ Container Security Tools:

- **Docker Bench for Security**: Docker Bench for Security is a tool that checks Docker containers against security best practices.

- **Clair**: Clair is an open-source vulnerability scanning tool for containers that identifies security vulnerabilities in container images.

➢ Security Orchestration, Automation, and Response (SOAR) Tools:

- **Demisto**: Demisto is a SOAR platform that automates incident response processes and integrates with various security tools.

- **Splunk Phantom**: Splunk Phantom is another SOAR tool that helps orchestrate security operations and automate tasks.

➢ Infrastructure as Code (IaC) Security Tools:

- **Terraform**: Terraform is an IaC tool that can be used with security-focused modules and best practices to secure infrastructure deployments.

- **AWS Config:** AWS Config provides configuration management and compliance monitoring for AWS resources.

- **Security Information and Event Management (SIEM) Tools:**

- Splunk: Splunk is a SIEM tool that collects, analyzes, and correlates security event data to provide insights into security incidents.

- IBM Qradar: IBM QRadar is another SIEM platform that helps organizations detect and respond to security threats.

These are just a few examples of the many DevSecOps tools available to help organizations enhance their security posture throughout the software development lifecycle. Organizations should evaluate their specific requirements and choose the tools that best fit their needs.

6. What are the benefits of DevSecOps?

DevSecOps, which combines development, security, and operations practices, offers several benefits to organizations looking to enhance their security posture while maintaining agility and speed in their software development processes. Some of the key benefits of DevSecOps include:

- **Early Detection and Mitigation of Security Vulnerabilities:** By integrating security into the development process from the beginning, DevSecOps enables teams to detect and address security vulnerabilities early in the software development lifecycle. This proactive approach helps prevent security issues from becoming more significant problems later on.
- **Improved Collaboration and Communication:** DevSecOps promotes collaboration between development, security, and operations teams, breaking down silos and fostering better communication. This collaboration ensures that security considerations are integrated seamlessly into the development process, leading to more secure applications.
- **Faster Response to Security Threats:** With DevSecOps practices in place, organizations can respond quickly to security threats and incidents. Automation and continuous monitoring allow teams to detect and mitigate security issues in real-time, reducing the impact of potential breaches.
- **Compliance and Regulatory Alignment:** DevSecOps helps organizations meet compliance requirements and align with regulatory standards by embedding security controls into the development process. This proactive approach ensures that security measures are in place to address compliance needs from the outset.

- **Cost Savings:** Addressing security issues early in the development process can help organizations save costs associated with fixing vulnerabilities in production or post-release. By integrating security into every stage of development, DevSecOps reduces the risk of costly security breaches.
- **Enhanced Trust and Reputation:** Building secure applications through DevSecOps practices enhances customer trust and strengthens an organization's reputation. By prioritizing security throughout the development lifecycle, organizations demonstrate a commitment to protecting customer data and sensitive information.
- **Continuous Improvement:** DevSecOps promotes a culture of continuous improvement by encouraging teams to learn from security incidents, implement feedback loops, and refine security practices over time. This iterative approach helps organizations stay ahead of evolving security threats.

Overall, DevSecOps offers a holistic approach to software development that prioritizes security without compromising speed or agility. By integrating security into every stage of the development process, organizations can build secure, resilient applications that meet the demands of today's dynamic threat landscape.

7. About local and international DevSecOps career opportunity , career path.

DevSecOps professionals have a wide range of career opportunities available to them, both locally and internationally. The demand for skilled DevSecOps practitioners is on the rise as organizations recognize the importance of integrating security into their software development processes. Here are some career paths and opportunities for DevSecOps professionals:

- **Security Engineer/Analyst:** Security engineers or analysts focus on implementing security controls, monitoring systems for security threats, and responding to security incidents. They play a crucial role in ensuring the security of applications and infrastructure.
- **DevSecOps Engineer:** DevSecOps engineers are responsible for integrating security practices into the software development lifecycle. They work closely with development, security, and operations teams to automate security processes and ensure that security is a priority throughout the development pipeline.
- **Security Architect:** Security architects design and implement secure systems and applications by developing security architectures, defining security requirements, and recommending security best practices. They play a key role in ensuring that systems are resilient to cyber threats.

- **Security Consultant:** Security consultants provide advisory services to organizations on security best practices, compliance requirements, and security assessments. They help organizations identify and address security vulnerabilities and develop strategies to improve their security posture.
- **Security Operations Center (SOC) Analyst:** SOC analysts monitor and analyze security events, investigate security incidents, and respond to cybersecurity threats in real-time. They play a critical role in detecting and mitigating security incidents to protect organizational assets.
- **Penetration Tester/Ethical Hacker:** Penetration testers or ethical hackers assess the security of systems and applications by identifying vulnerabilities and simulating cyber attacks. They help organizations proactively identify and address security weaknesses before malicious actors exploit them.

In terms of career opportunities, DevSecOps professionals can find roles in various industries such as finance, healthcare, technology, government, and more. With the increasing emphasis on cyber security and compliance regulations globally, DevSecOps expertise is highly sought after by organizations looking to strengthen their security defenses.

To advance in the field of DevSecOps, professionals can pursue certifications such as Certified DevSecOps Engineer (CDSE), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), or vendor-specific certifications from cloud service providers like AWS, Azure, or Google Cloud.

Networking with industry professionals, attending conferences, participating in online communities, and staying updated on the latest trends in cybersecurity and DevSecOps practices can also help individuals enhance their career prospects and stay competitive in the job market.

Overall, the adoption of DevSecOps is driven by the need for a more secure, collaborative, and efficient approach to software development that addresses these and other software engineering challenges.

Conclusion

In conclusion, DevSecOps is a crucial evolution in the software development process that prioritizes security from the outset. By embedding security practices within the DevOps workflow, organizations can proactively address security vulnerabilities and threats, leading to more secure and resilient software applications. The collaborative nature of DevSecOps encourages communication and cooperation between development, operations, and security teams, fostering a culture of shared responsibility for security. Automation plays a key role in DevSecOps, enabling continuous integration and deployment while ensuring security controls are consistently applied throughout the development lifecycle. Overall, DevSecOps represents a shift towards a more proactive and integrated approach to cybersecurity, helping organizations stay ahead of potential threats and protect their digital assets effectively.

Reference

1.https://techvify-software.com/what-is-devsecops

2. https://www.browserstack.com/guide/devops-lifecycle

3. https://www.practical-devsecops.com/devsecops-tools

4. https://fossa.com/blog/must-have-devsecops-tools

5. https://www.atlassian.com/devops/devops-tools/devsecops-tools