Institute of Technology

School of Computing

Department of Software Engineering

Software Engineering Tools and Practices

Assignment 1 DevSecOps

NAME: ELIAS NUREDIN

ID:1301011

Summited To: MR.Esmael.M

Summition Date: March 15, 2024

Woldia University

Tabel of Content

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

The initiation of DevSecOps was driven by several software engineering problems and challenges that organizations faced in traditional software development practices. Some of the key issues that led to the adoption of DevSecOps include:

1. Silos between Development, Security, and Operations Teams:

- In traditional software development practices, there were often silos between development, security, and operations teams. This lack of collaboration and communication among these teams resulted in security vulnerabilities being discovered late in the development cycle or even after deployment.

2. Slow Security Testing and Compliance Checks:

- Security testing and compliance checks were typically performed as a separate phase at the end of the development process, leading to delays in identifying and addressing security issues. This approach made it challenging to meet compliance requirements and address security concerns effectively.

3. Manual Security Processes:

- Manual security processes, such as code reviews, vulnerability assessments, and security audits, were time-consuming and error-prone. This manual approach hindered the speed of software delivery and made it difficult to scale security practices across the organization.

4. Lack of Security Awareness Among Developers:

- Developers often lacked awareness of security best practices and were not equipped with the necessary tools and training to build secure applications. As a result, security vulnerabilities were inadvertently introduced into the codebase, increasing the risk of cyber attacks.

5. Inadequate Automation and Continuous Integration/Continuous Deployment (CI/CD):

- Traditional software development practices lacked robust automation processes and CI/CD pipelines for integrating security checks into the development workflow. This led to inconsistencies in security controls and made it challenging to enforce security policies across different environments.

6. Increasing Cybersecurity Threats:

- The rise of sophisticated cyber threats, data breaches, and ransomware attacks highlighted the critical need for organizations to prioritize security in their software development lifecycle. Traditional approaches to security were no longer sufficient to protect against evolving threats.

By addressing these software engineering problems and challenges, DevSecOps aims to integrate security practices into every stage of the software development lifecycle, automate security processes, foster collaboration between teams, and promote a culture of shared responsibility for security. This proactive approach helps organizations build secure, resilient, and compliant software products while accelerating delivery timelines and reducing security risks.

2. What is DevSecOps?

What is DevSecOps?

DevSecOps is the practice of integrating security testing at every stage of the software development process. It includes tools and processes that encourage collaboration between developers, security specialists, and operation teams to build software that is both efficient and secure. DevSecOps brings cultural transformation that makes security a shared responsibility for everyone who is building the software.

What does DevSecOps stand for?

DevSecOps stands for development, security, and operations. It is an extension of the DevOps practice. Each term defines different roles and responsibilities of software teams when they are building software applications.

Development

Development is the process of planning, coding, building, and testing the application.

Security

Security means introducing security earlier in the software development cycle. For example, programmers ensure that the code is free of security vulnerabilities, and security practitioners test the software further before the company releases it.

Operations

The operations team releases, monitors, and fixes any issues that arise from the software.

3. Briefly explain DevSecOps lifecycle?

The 5 DevSecOps Stages

By following these DevSecOps stages, organizations can ensure that security is integrated into every step of the software development and deployment lifecycle, leading to more secure and resilient applications and systems.

1. **Plan:** The planning stage involves defining the objectives, requirements, and security considerations for the software or application being developed. This includes identifying potential security risks and determining the necessary security controls and measures to implement throughout development.

2. **Build:** In the build stage, developers write the code and create the software or application based on the requirements and security guidelines established in the planning stage. Secure coding practices and frameworks are applied to ensure the code is robust and resilient against potential security vulnerabilities.
3. **Test:** The testing stage involves conducting various types of security tests to identify and address any vulnerabilities or weaknesses in the software. This includes static code analysis, dynamic application scanning, penetration testing, and vulnerability assessments.
4. **Release:** The release stage involves preparing the software or application for deployment in a production environment. This includes packaging the code, creating deployment artifacts, and performing final security checks. The release process should ensure that the software is free from known security issues and that all security controls are correctly configured.
5. **Deploy, Operate, and Monitor:** This stage involves deploying the software or application into the production environment, where end users actively use it. During this phase, continuous system monitoring is essential to detect and respond to security incidents or anomalies. Monitoring includes log analysis, threat detection, intrusion detection, and security event management.

4. How dose DevSecOps works?

How Do DevSecOps Work?

DevSecOps is a development philosophy that integrates security into the DevOps process. By leveraging the DevOps flow, DevSecOps is designed to increase collaboration and speed of development while mitigating risks associated with security vulnerabilities.
It facilitates faster application delivery while ensuring robust security practices are in place early on in the dev process cycle rather than bolting it on afterward. Moving further, let's learn more about how DevSecOps work. Read more below:

1. Code

When it comes to DevSecOps, code is one of the very first steps in the DevSecOps flow. Code creates a construct that has both security and development capability. With DevSecOps, code is not just written for development but for security as well.

As part of DevSecOps, when code is deployed, it's also analyzed to ensure it meets security standards and its development objective. This two-pronged approach supports DevSecOps efforts, as developers can write secure code that helps protect the integrity and safety of applications and systems.

2. Build

The DevSecOps flow is a powerful approach that combines the roles of dev, security, and ops into one cohesive unit. It focuses on building better secure systems with an emphasis on collaboration, constant testing, and discovering potential vulnerabilities as software is built. In addition, the dev team works to develop the software with the proper features and functionalities.

At the same time, the security team ensures that all of the security checks are completed properly before it can move forward. Finally, the operations team oversees the entire process while keeping a close eye on any changes that may occur from start to finish.

This helps to ensure applications are built correctly and in a timely manner. A DevSecOps flow also eliminates many manual steps and increases overall productivity for each development project.

3. Store

The DevSecOps Store is a crucial part of this process; it provides resources to support the DevSecOps flow throughout its implementation. This could include pre-built policies, images, and scripts that allow developers to quickly follow DevSecOps best practices without starting from scratch.

It offers manual and automated controls against vulnerabilities, mitigating risks by ensuring DevSecOps is thoroughly applied while providing availability and security robustness across DevSecOps teams.

4. Prep

DevSecOps Prep is the essential first step in DevSecOps flow and focuses on creating a framework for security in order to ensure the software is secure throughout its entire life cycle. This involves identifying weaknesses, recognizing potential risks and threats to the system, assigning roles and responsibilities, and coordinating security objectives with DevOps goals. The overall aim of DevSecOps prep is to develop secure applications quickly while considering compliance with regulations, such as data privacy laws.

With DevSecOps prep set in place, organizations can confidently pursue their DevSecOps objectives while ensuring their data remains secure - whether it be within development cycle or operations phase.

5. Deploy

The DevSecOps flow continues with the deployment step. This is where code and other assets are moved from development to production. This step involves testing and automated security scans to ensure accuracy and functionality before anything is released. Depending on the structure of DevSecOps, deployment can be handled either manually or by a continuous delivery process.

A key goal of DevSecOps is to speed up this process without affecting the accuracy or security of the content being deployed. Additionally, once the changes have been made and verified, DevSecOps ensures that they have been safely packaged for distribution in order to ensure their swift implementation into an environment.

6. Run

The DevSecOps flow runs by initiating the deployment of code applications and running tests in a continuous delivery process. During runtime, DevSecOps checks to see if any security threats have occurred.
From here, it allows Developers to make immediate corrections with automated fixes or manual changes in certain cases.
This saves time, as previously, application deployments were done periodically, making it difficult for developers to pinpoint security errors on the spot. With DevSecOps however, issues can be identified quickly, and responses can be easily streamlined into the deployment flow.

5. Explain well known DevSecOps tools.

What is DevSecOps Tools

DevSecOps tools are a set of software and applications that facilitate the integration of security practices into the software development and operations lifecycle. These tools play a pivotal role in ensuring that security measures are seamlessly woven into every step of the development process – from code creation to deployment and beyond.

Best DevSecOps Tools List for 2024

The need for robust security tools that integrate seamlessly into the development process has become paramount. Here are some of the best DevSecOps tools list you can choose to deploy

1. Veracode

Veracode is an amazing cloud-based security tool created to simplify developer security testing. It provides comprehensive visibility into your application's security posture and offers remediation tips for any vulnerabilities it detects.

2. Checkmarx

Checkmarx provides AI-powered software security solutions that help identify and remediate code vulnerabilities. It integrates easily into your development pipeline and provides actionable insights into your security posture.

3. OWASP ZAP

OWASP ZAP is a free and open-source web application security scanner. It is highly customizable and can identify vulnerabilities in your application and works by intercepting and modifying HTTP

and HTTPS traffic between the web application and client. ZAP has the capability to scan for a range of security issues and includes automated and manual scanning modes.

4. Burp Suite

Burp Suite is a leading platform for web application security testing. It offers a variety of tools to help you identify and remediate vulnerabilities and integrates seamlessly into your DevSecOps pipeline.

5. SonarQube

SonarQube is a popular code quality tool that offers security-focused plugins to help identify code vulnerabilities during development, provides continuous feedback on your code, and enables you to maintain high code quality.

6. Fortify

Fortify is an industry-leading application security tool that offers comprehensive testing capabilities, including static, dynamic, and interactive application security testing. It also offers integrations with leading tools for seamless DevSecOps.

7. Snyk

Snyk is a popular developer-first application security tool that integrates directly into your development tools and workflows. It supports multiple languages and offers actionable insight into your app's security posture.

8. Coverity

Coverity is a static analysis tool that detects and helps you remediate critical software defects that could impact the security of your application. It also offers integrations with all the leading DevSecOps tools, making it a popular choice for large organizations.

10. AppScan

AppScan is a popular application security tool produced by HCL Technologies, a leader in the cybersecurity field. Its AI-powered solution is easy-to-use and supports both static and dynamic applications.

Also read, Best DevSecOps Books

Conclusion

By using these top-quality DevSecOps tools, you can have peace of mind knowing that your application is secure and protected through all stages of development. Choose the ones that best suit

your needs and build a secure DevSecOps pipeline that caters to your business's evolving security requirements.

6. What are the benefits of DevSecOps?

Benefits of DevSecOps

DevOps has transformed the field of the software industry, and integrating security into this paradigm, known as DevSecOps, is elevating software development practices. Embracing DevSecOps offers various advantages, such as:

1) Rapidly Addressing Security Vulnerabilities

A significant advantage of DevSecOps lies in its prompt handling of newly discovered vulnerabilities. By seamlessly incorporating vulnerability scanning and patching into the release cycle, DevSecOps significantly improves the capability to detect and address common vulnerabilities and exposures swiftly. This, in turn, reduces the timeframe during which threat actors can exploit vulnerabilities in public-facing production systems.

2) Shared Responsibility Across Teams

DevSecOps aligns development and security teams from the outset of the development cycle, fostering a collaborative cross-team approach. Rather than adhering to a siloed and disjointed operational approach that stifles innovation and triggers conflicts, DevSecOps encourages teams to synchronize early, promoting effective cross-team collaboration.

3) Improved Application Security

DevSecOps adopts a proactive strategy for addressing security vulnerabilities in the early stages of developing the DevSecOps lifecycle. Development teams in the DevSecOps framework leverage automated security tools to test code and conduct security audits seamlessly, avoiding any hindrance to the development process or the software delivery pipeline.

Throughout different phases of the development process, the DevSecOps lifecycle reviews, audits, tests, scans, and debugging to ensure that the application successfully clears crucial security checkpoints. In the event of security vulnerabilities emerging, collaboration between

application security and development teams ensues, involving a joint effort in conducting security analysis and devising solutions at the code level.

4) Swift and Economical Software Delivery

DevSecOps' quick and secure delivery approach not only saves time but also reduces costs by minimizing the necessity of revisiting processes to address security issues after the fact. Integrating security in this process is efficient and cost-effective, eliminating redundant tasks and unnecessary reworks and reviews, thereby enhancing overall security measures.

5) Suitable for Automation in a Contemporary Development Team

DevSecOps framework empowers software teams to integrate security and observability seamlessly into DevSecOps automation, accelerating the SDLC and ensuring a more secure software release process.

Automated testing plays a crucial role in verifying that integrated software dependencies, such as libraries, frameworks, and application containers, meet the required security standards, especially in the case of unknown vulnerabilities. DevSecOps automation testing confirms that the software has successfully undergone security unit testing across all levels. This comprehensive approach includes testing and securing code through static, dynamic, and dependency analyses before the final software is deployed to production. Automated tools can scan containers and scrutinize their dependencies to identify and report vulnerable components.

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

DevSecOps is a rapidly growing field within the technology industry, and professionals with expertise in this area are in high demand both locally and internationally. Here are some insights into DevSecOps career opportunities, career paths, and potential roles:

1. Local Career Opportunities:

- Many organizations, ranging from startups to large enterprises, are actively looking to hire DevSecOps professionals to strengthen their security practices.

- Local cybersecurity firms, consulting companies, government agencies, and financial institutions often have job openings for DevSecOps engineers, security analysts, and security architects.

- DevSecOps roles can also be found in industries such as healthcare, retail, manufacturing, and technology companies that prioritize security in their software development processes.

2. International Career Opportunities:

- With the increasing global focus on cybersecurity and data protection, DevSecOps professionals have opportunities to work for multinational corporations, cybersecurity firms, and tech companies around the world.

- International organizations, financial institutions, and government agencies often seek DevSecOps experts to enhance their security posture and compliance with regulatory requirements.

- DevSecOps professionals may have the opportunity to work remotely or relocate to different countries to take on challenging roles in cybersecurity and secure software development.

3. Career Path:

- Entry-Level: Junior DevSecOps Engineer, Security Analyst, Security Operations Center (SOC) Analyst.

- Mid-Level: DevSecOps Engineer, Security Consultant, Security Architect, Compliance Analyst.

- Senior-Level: DevSecOps Manager, Chief Information Security Officer (CISO), Security Director, Security Team Lead.

- Specialized Roles: Cloud Security Engineer, Application Security Specialist, Incident Response Analyst.

4. Skills and Certifications:

- To excel in a DevSecOps career, professionals should have a strong understanding of software development, security principles, automation tools, and cloud technologies.

- Certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Certified Cloud Security Professional (CCSP), and DevSecOps Foundation can enhance one's credentials in the field.

5. Continuous Learning:

- The field of DevSecOps is constantly evolving with new technologies and security threats emerging. Continuous learning through training programs, workshops, conferences, and hands-on experience is essential to stay current in the field.

Overall, pursuing a career in DevSecOps offers exciting opportunities for professionals who are passionate about integrating security into the software development lifecycle and protecting organizations from cyber threats. By building a strong foundation of technical skills, security expertise, and industry knowledge, individuals can carve out a rewarding career path in the dynamic field of DevSecOps.

Reference:

https://www.sonatype.com/2021-state-of-devsecops , https://www.veritis.com/blog/what-are-the-phases-of-devsecops/ , https://www.practical-devsecops.com/devsecops-tools/#, https://scantist.com/resources/blogs/what-is-devsecops-a-comprehensive-guide, https://www.relyservices.com/blog/5-devsecops-stages , - "The Phoenix Project: A Novel about IT, DevOps, and Helping Your Business Win" by Gene Kim, Kevin Behr, and George Spafford

,