Philip Trinh

SNHU/ CS 305

3/19/2023

Module Three Journal

 DevSecOps: A Systemic Approach for Secure Software Development

* What is your role in solving security concerns as a developer? What might solve security concerns as a developer involve?
* My role as a developer in solving security concern involve focusing time to learn and investigate security vulnerabilities and establish plan to fix it. Utilize the tools and technologies at hand such as source code analysis or static application security testing (SAST) process, dynamic application security testing (DAST), and interactive application security testing (IAST), web vulnerability scanners, source code analyzers, etc. As a developer, I also part of the DevOps team and must focus on customer, delivering the needs in a continuous integration and continuous delivery (CI/CD), and continuous security (CS) fashion.

Beside security testing, I also need to implement good and secure coding practice such as avoid common coding mistakes, build quality code, keep software up to date, educate myself on new security risk that can affect my software application, and design secure software architecture.

* Solving security concern as a developer involve focus on security-centric goals to make the organization compliant with regulations and privacy laws. Run many testing tools to figure out if any new or potential security concern identifies within the applications developed. Implement secure and quality coding practices to correct any security concerns if involve coding, update the software application to patch the security concerns and report the security flaws so others can be aware of it.
* Where does security fall within the software stack and development life cycle?
* Security is the foundation requirement for software development, it cannot be compartmentalized as certain individuals’ responsibility, but everyone must be involved in it.

In software stack security also involve in all steps from plan and develop, build, test, secure, store artifact, deploy and operate, monitor, and scale. It follows model of continuous integrate, continuous delivery, continuous security.

* Security seem to only applies at later phases of software development life cycle (SDLC) testing, deployment, and maintenance. Here the team perform testing process to identify any security flaws and fix it up to deployment. The maintenance process involves solving any security problems reported by users or identify by the technical team. However at the early stages of development such as planning, design, development mostly just think about the feature of application will have and meeting requirements, little about security.
* How might you add security measures to transform a DevOps pipeline into a DevSecOps pipeline?
* Follow DevSecOps Culture to add security into all steps of DevOps pipeline. For example, in planning phase, the team should consider what might be a security risk or potential vulnerability to the application base on the feature wanted to implement. During build phase could be implement secure coding practices. Testing phase incorporate tools beside a manual review such as vulnerability scanning, source code analyzers. Deployment phases add configuration and restriction to make the application more secure. During monitor phase watch for any security vulnerability and quickly fix it. In summary, adding security to all phases will help to transform DevOps pipeline into DevSecOps pipeline.
* The article suggests creating and following a plan to secure the entire DevOps life cycle. What is included in the suggested plan, and would you recommend following it?
* The three key features I identified from DevSecOps plan are Continuous integration (CI), Continuous delivery (CD), and Continuous security (CS). I would recommend following it in because this continuous integration, delivery, and security benefits the company and customers by delivering the product secure, fast, and continuously addressing any issue and fix it as soon as possible.

REFERENCES

Jeganathan, S. (November 2019). DevSecOps A Systemic Approach for Secure Software Development [Review of DevSecOps A Systemic Approach for Secure Software Development].