Toll Road Company

Creation of DevSecOps Department

What is DevSecOps?

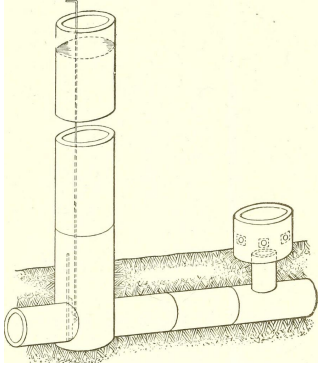
First, what is DevOps ?

- Here at Toll Road Company we have a DevOps department which uses methods and tools to implement IT projects that address business needs.
- The DevOps pipeline stages for the website application development cycle are planning, code and build, test, release and deploy, operate and monitor.
- Devops is integrated with Agile Development where there are many iterations of the software development cycle being processed.

Now, what is DevSecOps?

- DevSecOps is security testing that is tightly integrated with DevOps.
- The DevSecOps will save time and money for Toll Road Company as we bring the web application development project to production.

The DevSecOps Pipeline



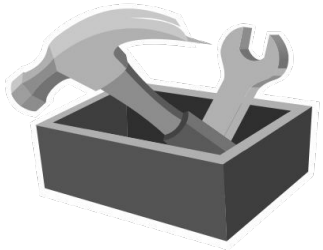
DevOps pipeline consist of all the stages completing before the penetration testing takes place.

- Planning -> Code -> Build -> Test -> Release -> Deploy -> Operate -> Monitor -> Pen Testing

DevSecOps pipeline stages will tightly integrate security in between the stages instead of a one time penetration test. For example, the following security/scanning tools can be used as shown below:

- Planning -> SAST Dependency Check -> Code
- Code -> FindSecBugs -> Build
- Build -> OWASP ZAP -> Test
- Test -> OpenVAS -> Release
- Deploy -> WAF -> Operate

DevSecOps Tools for Testing/Scanning



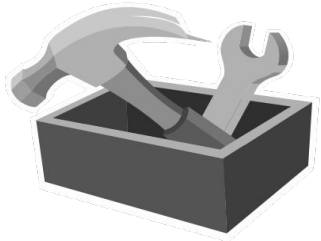
Static application security checking (SAST) dependency check

- reviews source code to check for security vulnerabilities
- examine the text of a program syntactically
- The Toll Road Company during the beginning stage of its customer web application will need to check for vulnerabilities in third party vendor code.

Findsecbugs

- Plugin for Spotbugs (utility to detect Java bugs)
- Adds 135 vulnerabilities types focused on OWASP Top 10 and Common Weakness Enumeration (CWE)
- Toll Road Company website will use this to find security vulnerabilities in its code before the build stage
- If there is at least one high vulnerability found in the code then the build will fail

DevSecOps Tools for Testing/Scanning



OWASP ZAP

- An open-source web application security scanner
- used for dynamic security analysis after the build when code is in operation mode
- It will scan the login page, registration page, and the invoice payment page for secure validation input

OpenVAS

- Before the release of the web application, the company will use an Infrastructure as Code (IAS) tool which will automatically control and customize the required infrastructure
- Used as a complete vulnerability assessment system that can detect security issues in the infrastructure

WAF

- An application firewall that the company will use for its website to filter, monitor and block HTTP traffic to and from its web service.

DevSecOps Cost Benefits

DevSecOps saves money for the company

- If penetration testing is done at the end of the project cycle any security issues will need to be addressed as far back as the planning stage. This means developers will need to work longer hours which will cost the company more money.
- With DevSecOps, however, developers will work less hours and thus save the company money. The developers can run automated scans from the very beginning. Testing for cross-site scripting and sql injections can be done at the beginning and fixed right away instead of waiting unit the end of the project.
- With DevSecOps, there will be recurring asset inventory and automated assessments which will help the company save money long-term.

DevSecOps Time Benefits

DevSecOps saves time for getting its web application into production

- By incorporating security into DevOps, code that contains a bug during development can have a fix started right away. That way the development of the code and the development of the security fix can happen concurrently which will save time.
- Performing automated scans and tests before the code goes into the build stage will save time in case there is a security issue to be addressed. Waiting to address the security issues when the project is almost released means having to go back to the coding stage to rewrite the code. This can take a long time.

DevSecOps Team Building

DevSecOps will need fewer employees

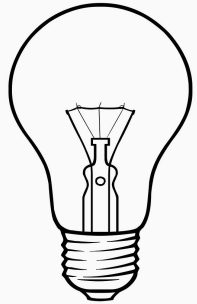
- Penetration testers will not be needed since there will be no pen testing performed when the web application is released.
- The company will need to hire a few DevSecOps personnel with strong cyber security skills to replace the pen testers.
- The DevSecOps employees will train the current developers at the company to perform security scanning and testing.
- A DevSecOps team will save the company money since pen testers will not be needed.

DevSecOps Team Interactions

There needs to be strong collaboration between DevSecOps, IT auditors, IT security, and Software Developers

- DevSecOps will be working along with developers and also will be training them to scan and test security vulnerabilities and bugs before the code goes into the build stage.
- Throughout the cycle from code to release the IT security team will perform vulnerability management.
- After the product is released, the IT auditors will use Inspec. Inspec is an open source project that lets the company define compliance requirements. The company can then run the requirements as automated tests the audit the systems.

DevSecOps Final Thoughts



Key takeaways as to why creating a DevSecOps is high-priority for Toll Road Company

- Data breaches are happening frequently and have become devastating for companies. For Toll Road Company to lower its risk of data breaches it is vital for security to be tightly integrated with its web application development team.
- Toll Road Company uses the Agile methodology to develop its software. For security to keep up with agile, a DevSecOps team is a requirement.
- For security to play a significant role in software development and not be overlooked, the culture at the company must change. There should be constant communication and collaboration between the DevSecOps team, IT auditors, IT security analysts, and software developers.