|  |  |
| --- | --- |
|  |  |

CS 305 Module Two Static Testing Summary Assignment  
Brandon Coulter  
Southern New Hampshire University

**What is your role in conquering security concerns as a developer? What might that involve?**

As a developer it is in my duties and responsibilities to ensure that the areas of security or concern within a given application that I am working on are up to industry standards and best practices. This involves the use of static testing and manual code review to make certain that the code base used for the project at hand is free of all known vulnerabilities. As described in *DevSecOps A Systemic Approach for Software Development*, “The primary objective is to secure the overall IT systems and business functions to support the growth of the underlying business.” (Jeganathan, 2019) Additionally, as a developer in a DevSecOps environment, it is my responsibility to maintain my knowledge of the most up to date security risks and vulnerabilities; in doing so, this will help the company “build a culture of security” (Jeganathan, 2019) throughout the workplace.

**Where does security fall within the software stack and development life cycle?**

Typically in a normal DevOps environment, security tends to be a secondary thought and thus not always done properly or swiftly. The goal of DevSecOps is to change that by having an environment in which security personal and development teams are working hand in hand together to ensure that DevOps speed is maintained however with security as a forethought. (Jeganathan, 2019) The point of working in this environment is to integrate security into every aspect of the development lifecycle, by having teams that tend not normally work together, collaborate and focus on driving secure products in a swift manner. This mindset provides a means for a company to provide viable products, that are secure and meet all customer requirements, while also being completed in a timely manner.

**How might you add security measures to transform a DevOps pipeline into a DevSecOps pipeline?**

Some additional security measures that can be added to transform a DevOps pipeline into a DevSecOps pipeline include adding features such as static application security testing (SAST) and dynamic application security testing (DAST). Interactive application security testing (IAST) is an additional feature that can be added to transform a DevOps pipeline into a DevSecOps pipeline. (Jeganathan, 2019) This added security measures helps the team to complete security checks and fight against known vulnerabilities within the National Vulnerabilities Database (NVD). Security risk management and security monitoring are additional means of integrating into a DevSecOps pipeline. (Jeganathan, 2019)

**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?**

Included in the plan to secure the DevOps life cycle is to start out with a security assessment, then to continue with role or attribute based access security points, logon safeguards with two factor authentication for critical systems, security of various user access and API keys, and create infrastructure controls. Additionally, following best coding practices while integrating security assessment tools and training developers is also a means of securing the DevOps life cycle. Doing away with vulnerable elements, implementing security unit testing and ensuring proper peer review is conducted will also secure the pipeline. (Jeganathan, 2019) I would recommend this plan as it seems highly methodical with little room for error. This plan seems to cover the bases of security ensuring the proper channels are taken to get to an end product that is secure and up to date with relation to security and security related principles. Following formal plan will only help a team to complete their tasks on time and in a secure manner.

**References:**

Jeganathan, S. (2019, November). *DevSecOps A Systemic Approach to Software Development*. Retrieved July 16, 2022, from http://eds.a.ebscohost.com.ezproxy.snhu.edu/eds/pdfviewer/pdfviewer?vid=2