Case Study

Implementing DevSecOps

Secure Pipeline for Application Deployment

Problem Statement:

Project Overview: The goal of this project is to establish a comprehensive DevSecOps pipeline for deploying an application to a Kubernetes cluster. The pipeline will automate the infrastructure setup, source code building, containerization, and deployment processes while integrating robust security testing at each stage. This approach ensures that the application is continuously tested for vulnerabilities and ensures a secure deployment to production. Make sure you are using appropriate tools to build test reports.

The web application code is hosted on the Git repository:
https://github.com/rushtoaksith/Shark-Secure-Pipeline.git

Objective:

The objective is to establish a robust environment for product deployment by integrating continuous integration and deployment (CI/CD) practices across the software development lifecycle (SDLC). It is mandatory to incorporate security testing at every stage, encompassing code development, image and infrastructure building, as well as deployment processes. This entails implementing a Git workflow, constructing a Docker image containing the web application code and dependencies, and orchestrating the deployment of the application within Kubernetes.

Our approach involves testing various components including source code, Infrastructure as Code (IaC), deployment scripts, image vulnerabilities, and the deployment environment for vulnerabilities. Comprehensive reports will be generated and shared with the team to address identified issues promptly.

.

Pre-requisites:

- Windows System: Java 11 or above, Jenkins, Terraform, and required proxy and security tools
  Minimum hardware requirements:
  256 MB of RAM
  1 GB of drive space (although 10 GB is a recommended minimum if running Jenkins as a Docker container)

  Recommended hardware configuration for a small team:
  4 GB+ of RAM
  50 GB+ of drive space

- Linux environment - Ubuntu 20.00 - 2vCPU 4 Gib Memory (t2.medium) - Docker, Kubernetes and required security tools

Tasks to be Performed:

1. **Git Operations**: Add necessary files for a smooth release of the application. Integrate the Git repository with your local system as well as with any other environment as per requirements.

2. **Setting up Infrastructure and Necessary Tools:** This project requires you to work on both a local Windows system and a Linux operating system (AWS instance). You have to install several dependencies according to the source code and security requirements.

3. **Creating and Managing Docker Image:** Implement a stage to build a Docker image encapsulating the web application code and its dependencies. This Docker image serves as a portable and consistent environment for the application.

4. **Security Operations (SAST, SCA, and More):** You need to test all the files and environments used for deploying the application and create reports for developers and architects to validate.

5. **CI/CD:** This includes performing all tasks efficiently wherever possible to ensure faster releases. You might need to create different jobs for tasks like identifying vulnerabilities, hosting infrastructure, and deploying application.