HLD for DevSecOps

Definition :

This HLD for DevSecOps demonstrates how to integrate security practices at each stage of the CI/CD pipeline, ensuring that applications are secure and compliant throughout the development lifecycle.

Detailed Steps of the Architecture

1. **Git Repository**
   - **Description**: Developers commit and push their source code to a version control repository (e.g., GitHub, GitLab, Bitbucket).
   - **Security**: Use SSH keys or two-factor authentication (2FA) to secure repository access.
2. **CI/CD Server (e.g., Jenkins)**
   - **Description**: Jenkins detects new commits and automatically triggers the CI/CD pipeline.
   - **Security**: Secure Jenkins with role-based access control (RBAC) and security plugins.
3. **Security Analysis**
   - **Description**: Tools like SonarQube, Snyk, or Checkmarx analyze the source code for vulnerabilities.
   - **Example**: SonarQube checks for coding best practices and identifies security flaws like SQL injection.
4. **Automated Testing**

- **Description**: Run unit, integration, and functional tests to validate code quality.
- **Example**: JUnit for unit tests and Selenium for end-to-end tests.

5. **Build and Packaging**
    - **Description**: Create builds and package applications into Docker containers.
    - **Security**: Scan Docker images for vulnerabilities before use.(trivy)
6. **Deployment to Test Environment**
    - **Description**: Deploy builds to a test environment orchestrated by Kubernetes
    - **Security**: Use isolated namespaces for testing and network policies to restrict access.
7. **Dynamic Security Scans**
    - **Description**: OWASP ZAP performs security scans on deployed applications to identify real-time vulnerabilities.
    - **Example**: OWASP ZAP can detect vulnerabilities like Cross-Site Scripting (XSS) or SQL injection.
8. **Monitoring and Alerts**
    - **Description**: Prometheus monitors application performance, Grafana visualizes metrics, and PagerDuty manages incident alerts.
    - **Security**: Monitor security logs and generate alerts for anomalies.
9. **Deployment to Production**
    - **Description**: Deploy validated builds to the production environment via Kubernetes

- **Security**: Implement strict access controls and security policies for production deployments.

Stages of DevSecops :

- Git Repository: Developers push code to GitHub.
- CI/CD Server: Jenkins detects commits and triggers the pipeline
- Security Analysis: SonarQube analyzes code for vulnerabilities.
- Automated Testing: Jenkins runs unit tests with JUnit and functional tests with Selenium.
- Build and Packaging: Applications are packaged into Docker containers.
- Deployment to Test Environment: Docker containers are deployed to a Kubernetes test environment.
- Dynamic Security Scans: OWASP ZAP scans the deployed applications for security vulnerabilities.
- Monitoring and Alerts: Prometheus and Grafana monitor performance and metrics, while PagerDuty sends alerts for incidents.
- Deployment to Production: Validated builds are deployed to production in Kubernetes with strict security policies.