HLD

stage 1: Pre-commit

Prettier :
Used to ensure that all code follows a uniform style, making it easier to read and maintain.
TSLint:
Used to detect syntax errors, coding convention violations, and TypeScript-specific code quality issues.
Resume :
Prettier is excellent for code formatting, while TSLint is essential for checking code quality and detecting TypeScript-specific errors.

Commit :

Commitizen :
wish to standardize and improve the quality of their commit messages, thus facilitating maintenance, traceability and automation in their projects.

Analyse Statique :

SonarQube:
focuses on overall code quality with a secondary focus on security.
offers detailed metrics on code quality, which is useful for improving coding practices and maintainability.
Fortify :
mainly focuses on application security.
provides in-depth security scans and helps identify vulnerabilities before they become security risks.
Resume:
SonarQube is often preferred for projects where the quality of the code is paramount. Fortify is preferred for projects where safety is critical, especially in regulated environments.

JUnit:
Designed specifically for Java.
Jest:
Designed specifically for JavaScript and TypeScript.
Resume :
The choice between JUnit and Jest strongly depends on the programming language and the type of project

Test de security :

Snyk :
Type of tool: Security tool for dependency management.
Vulnerability detection , Continuous monitoring and Provides detailed reports and alerts on the vulnerabilities found.
Dependency-Check :
Type of tool: Security tool for dependency management.
Vulnerability detection, Generates detailed reports on vulnerabilities found in dependencies and Ease of use.
Resume:
Snyk is often preferred due to its extensive functionality and multi-language support, while Dependency-Check remains a solid and effective tool for projects mainly focused on Java.

E2E Tests :

Selenium :
Selenium is designed to automate interactions with web browsers by allowing web applications to be tested in different browsers (Chrome, Firefox, Safari, etc.).
Selenium works by using browser APIs to simulate user actions .
Supports a wide range of browsers (Chrome, Firefox, Safari, Internet Explorer, Edge, etc.)
Cypress :
is specifically designed for modern web application testing and used to test web applications in the Chromium browser (and, to some extent, Firefox).
Cypress works directly in the browser

Mainly designed for Chrome and other Chromium-based browsers.
Resume:
Cypress is often chosen for projects requiring quick configuration and testing in modern browsers, while Selenium is preferred for its flexibility and extensive browser support.

Test Dynamique :

OWASP ZAP (Zed Attack Proxy) :
is an open-source web application security testing tool, developed by the OWASP community.
enable developers and security testers to discover security vulnerabilities in web applications.
Cost: Free (open-source).
Acunetix :
is a commercial web application security testing tool developed by a private company.
aims to automate security testing of web applications and detect a wide range of vulnerabilities
Cost: Commercial, with a paid license.
Resume:
OWASP ZAP is ideal for those looking for an open-source and flexible solution, while Acunetix is more suitable for organizations looking for a complete commercial solution with professional support.

Build et Packaging:

Maven :
Java-based project and construction management tool, developed by Apache.
Simplify the management of dependencies and life cycles of Java projects by using XML configuration files (pom.xml).
Gradle :
Modern and flexible construction tool for software projects, developed by Gradle Inc.

To provide a fast and efficient project construction using a DSL (domain-specific language) based on Groovy or Kotlin for the configuration files (build.gradle).
Resume:
Maven is often preferred for its simplicity, its clear structure and its wide ecosystem of plugins, especially for Java projects. Gradle is preferred for its flexibility, performance, and customization capabilities, which makes it ideal for complex projects

Publier dans repository:

Nexus :
is a repository manager that stokke, organizes and distribute software components.
Xray :
is a security and compliance analysis tool for software artifacts.
Scan artifacts and containers for security vulnerabilities and licensing issues.
Integrates closely with JFrog Artifactory

Scan Docker image :

Trivy:
Security scanning tool for containers and other artifacts.
check for vulnerabilities in container images, system files, Git repositories, and more.
Clair :
Static analysis tool for the detection of vulnerabilities in containers.
Analyze container images to detect vulnerabilities using a centralized database.
Resume:
Trivy is generally preferred for its simplicity and efficiency in security scans, while Clair is chosen for its in-depth analysis capabilities and its API integration in more complex environments