1. SAST (Static Application Security Testing):

- **What it is:** SAST analyzes source code, bytecode, or binaries without executing the application. It identifies potential security vulnerabilities by examining the application's codebase.
- **When it's used:** During development or before the application is deployed (early in the CI/CD pipeline).
- **Example tools:** SonarQube, Checkmarx, Fortify.
- **Purpose:** To detect issues like SQL injection, cross-site scripting (XSS), or insecure coding practices in the code.

---

2. DAST (Dynamic Application Security Testing):

- **What it is:** DAST tests a running application by interacting with it as an attacker would, simulating real-world attacks. It inspects the application's behavior and responses.
- **When it's used:** After the application has been deployed to a staging or test environment (later in the CI/CD pipeline).
- **Example tools:** OWASP ZAP, Burp Suite, Acunetix.
- **Purpose:** To find vulnerabilities like misconfigured servers, authentication flaws, or runtime issues.

---

3. Dependency Scanning:

- **What it is:** This checks third-party libraries and dependencies used by the application for known vulnerabilities. It compares these against public vulnerability databases like CVE (Common Vulnerabilities and Exposures).
- **When it's used:** Throughout the CI/CD pipeline, as dependencies are added or updated.
- **Example tools:** Snyk, Dependabot, OWASP Dependency-Check.
- **Purpose:** To ensure the libraries or frameworks you rely on are secure and up-to-date.

Integration into CI/CD pipelines:

- **What it means:** CI/CD pipelines automate software development, testing, and deployment. By integrating these security testing methods into the pipeline:
    - Developers can detect and address vulnerabilities early.
    - Security testing becomes part of the automated build and deployment process.
    - Secure software is delivered continuously without adding significant manual effort.

In essence, this approach aims to ensure that every piece of software shipped is rigorously tested for security vulnerabilities.