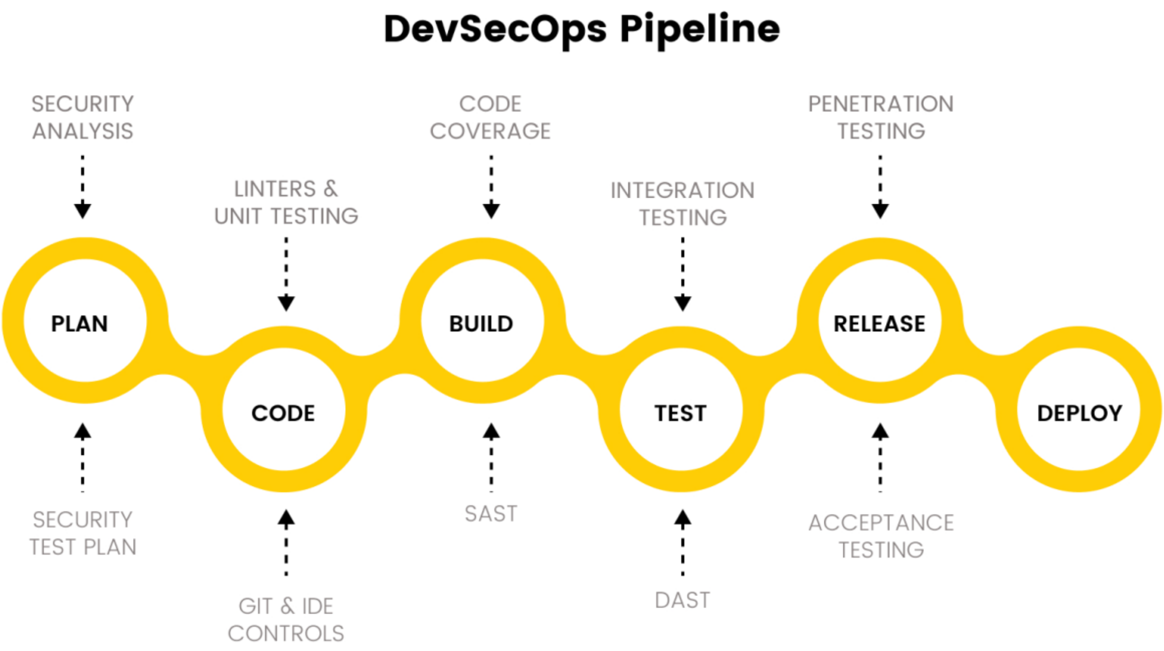
DevSecOps



Code Level Security

- **SCA (Software Composition Analysis)**:
  Checks for vulnerabilities in third-party dependencies.
- **SAST (Static Application Security Testing)**:
  Identifies security issues within the code itself.

Post-Deployment Security

- **DAST (Dynamic Application Security Testing)**:
  Tests the running application for vulnerabilities by simulating attacks.

Understanding CVE in Cybersecurity

CVE Definition

- **CVE (Common Vulnerabilities and Exposures)**:
  A standardized system that assigns unique IDs to publicly known cybersecurity vulnerabilities.

Origin and Purpose

- **Founded in 1999** by the **MITRE Corporation**.
  Funded by the U.S. Department of Homeland Security.
  Facilitates standardized communication and tracking of vulnerabilities.

How CVE Works

- Each CVE has:
  - A **unique identifier** (e.g., CVE-YYYY-NNNNN).

  - A brief **description** of the vulnerability.
  - **References** to additional resources.

Criteria for Inclusion

1. **Independently Fixable**: Resolvable without addressing other issues.
2. **Vendor Acknowledgment**: Recognized by the vendor as a security flaw.
3. **Single Codebase Impact**: Affects a specific software or product.

Importance of CVE

- **Facilitates Communication**: Standardized IDs simplify discussions.
- **Enhances Security Management**: Helps prioritize and address vulnerabilities.
- **Supports Risk Management**: Tools reference CVEs for automated detection.

Key CVE Resources

1. **MITRE CVE Database**: The primary source for CVEs.
2. **National Vulnerability Database (NVD)**: Provides enriched details like severity scores.
3. **CVE Details**: Offers exploits, tools, and additional advisory links.
4. **Vendor Databases**: Tailored CVE data for specific products.

OWASP (Open Web Application Security Project)

Overview

- A nonprofit organization founded in **2001**, aimed at improving software security.
- Offers free, community-driven resources and tools for secure application development.

Key Initiatives

1. **OWASP Top 10**:
   Lists the most critical web application security risks.
   Example: SQL Injection, XSS (Cross-Site Scripting).
2. **Community-driven**:
   Open collaboration for innovation and shared knowledge.
3. **Free Resources**:
   All tools and documentation are accessible to the public.
4. **Global Reach**:
   Over **250 local chapters worldwide** promoting security awareness.

Mission and Vision

- **Mission**: Empower organizations to develop secure software through education, tools, and best practices.
- **Vision**: Eliminate insecure software by addressing key vulnerabilities.
