Day - 2

26 November 2025 10:15

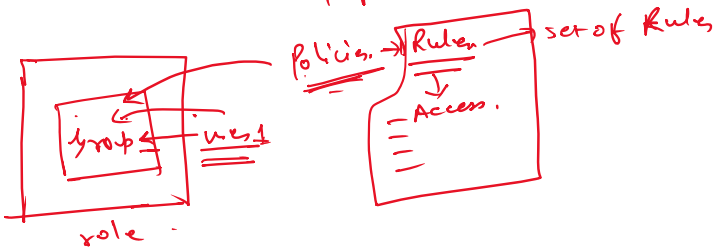
OWASP:- Open Web App. Security Project

↓

NIST - Set the security standards.

To diff. Category :-

(1) Broken Access control - User Permission not Properly set.




(2) Cryptographic failure :-

Improper Certificate Handling.
Storing Data in Plain Text
Weak Algorithms.

(3) Injection :- SQL Injection
Command Injection
Template Injection.

(4) Insecure design :- (1) Architectural flaws.
(2) Bad threat modelling.

(5) Security Misconfiguration :-

(1) S3 - Public
(2) Default Cred.
(3) Port open.

(6) Vulnerable & outdate content :-

(1) Dependent libraries
(2) O.S. patches

(7) Identification & Weak Authentication :-

(1) Weak Authentication
(2) Bad token Handling.

(8) Software & Data Integrity failure.

(9) Security logging & Monitoring failure.

⑨ Security logging & Monitoring failure.

Splunk


⑩ SSRF (Server Side Request Forgery)

* Sonar quality gate :- set the condition to check whether it is healthy state or not.

Pass - Allow to proceed
Fail - Fail at the certain stage.

Why ?

1. Enforce shift-left approach.
2. Automate code standards.
3. Prevent low quality code.

Key category :-

1. Leak Period | New Code.
2. Overall code (less strict)
   1. Security
   2. Maintainence
   3. Coverage
   4. Duplication.

Trivy :- open source, all-in-one security scanner.

- Container Scanning
- filesystem
- Vulnerability Scanning.
- IaC Security Scanning.
- K8S

Image - trivy image

Trivy

Vulnerability & Code Scanning.

SAST + IaC + SCA

Image, FS, IaC, Secret

Fail the build, if any vulnerability

Misconfig. (Terraform)

Detect Secret

Vulnerability

Li.

SonarQube

Code Quality & Secure Codig.

Full SAST

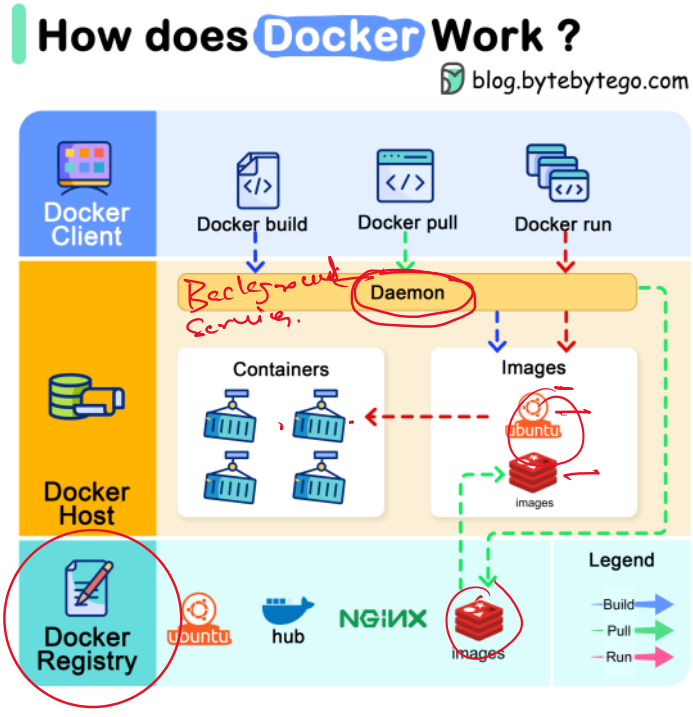
Application Code Scanning (Java, nodejs, Python)

Quality gate with condition

Not work on mis config.

Not extension.

Docker :-




(1) Docker Engine

(2) Docker Image

(3) Docker Registry.

(4) Docker Containers

Docker file ⟶ Docker Image

(1) App + Dependencies

(2)

Docker Registry

① Where the images will be stored.

- Docker Hub
- Amazon ECR
- Azure ACR