AEGIS

DEVSECOPS

Security Scanning Cheatsheet

SAST, DAST, SCA, and container security tools with pipeline integration examples

Security Scanning Types

SAST (Static Analysis)

Analyzes source code for vulnerabilities without executing it. Catches issues early in development.

When: Every commit, PR

DAST (Dynamic Analysis)

Tests running applications for vulnerabilities by simulating attacks. Finds runtime issues.

When: After deployment to staging

SCA (Software Composition)

Identifies vulnerable dependencies and license issues in third-party packages.

When: Every build, dependency update

Container Scanning

Scans container images for OS and package vulnerabilities, misconfigurations.

When: Image build, registry push

SAST Tools Comparison

Tool	Languages	Integration	Best For
SonarQube	27+ languages	CI/CD, IDE, GitHub	Enterprise, code quality
Semgrep	30+ languages	CLI, CI, GitHub	Custom rules, fast
Checkmarx	25+ languages	Enterprise integrations	Enterprise compliance
CodeQL	8 languages	GitHub native	GitHub repos, free OSS

SCA & Container Tools

Tool	Type	Key Features
Snyk	SCA + Container	Fix PRs, license check, monitoring
Trivy	Container	Fast, comprehensive, easy setup
Dependabot	SCA	GitHub native, auto PRs
Anchore	Container	Policy engine, SBOM
OWASP ZAP	DAST	Free, extensible, API scanning

Severity Thresholds

Severity	CVSS Score	Action	SLA
Critical	9.0 - 10.0	Block deployment	24 hours
High	7.0 - 8.9	Block deployment	7 days
Medium	4.0 - 6.9	Warning, track	30 days
Low	0.1 - 3.9	Log, best effort	90 days

AEGIS

Secure Your Pipeline

Let us help you implement comprehensive security scanning across your software delivery lifecycle.

Contact Us

info@aegisit.ai

(404) 490-0234

aegisit.ai