DevSecOps 全流程与产品分类

阶段	功能类别	功能说明	常用开源产品	商业/企业版产品
1. Plan（规划阶段）	**安全需求管理**	在需求阶段定义安全策略、安全测试标准、安全门禁	OWASP SAMM、OpenCRE	Jira + Security Plugin、ThreatModeler
	威胁建模（Threat Modeling）	识别系统设计中的潜在安全威胁	OWASP Threat Dragon、Microsoft TMT	IriusRisk
2. Code（开发阶段）	**代码安全检查（SAST）**	静态应用安全测试，扫描源码中的安全漏洞	SonarQube、Semgrep、Bandit（Python）	Checkmarx、Fortify、Veracode
	依赖漏洞扫描（SCA）	检查第三方依赖库的已知漏洞	OWASP Dependency-Check、Syft/Grype	Snyk、WhiteSource、JFrog Xray
	代码签名与完整性校验	确保源代码和构件未被篡改	Cosign、Sigstore	Venafi CodeSign Protect
3. Build（构建阶段）	**构建安全与合规扫描**	对构建产物进行安全与许可证审计	Trivy、Anchore Engine	Prisma Cloud、Aqua Security
	CI/CD 管道安全控制	在CI/CD中集成安全扫描、策略校验	GitHub Actions Security、GitLab Secure	Jenkins + CloudBees Security、CircleCI Security
4. Test（测试阶段）	**动态应用安全测试（DAST）**	模拟攻击测试运行中的Web应用	OWASP ZAP、Wapiti	Burp Suite Pro、Netsparker
	交互式应用安全测试（IAST）	在应用运行时检测漏洞	Contrast Community Edition	Contrast Security、Seeker
	模糊测试（Fuzz Testing）	自动生成异常输入发现漏洞	AFL、OSS-Fuzz、Go-Fuzz	Synopsys Defensics
5. Release（发布阶段）	**容器镜像安全扫描**	扫描Docker镜像中的漏洞与配置风险	Trivy、Clair	Anchore Enterprise、Aqua Trivy Pro
	签名与策略管理	发布前进行镜像签名、策略验证	Notary v2、Cosign	Harbor with Policy Enforcement
6. Deploy（部署阶段）	**基础设施即代码安全（IaC Security）**	检查Terraform/K8s/YAML等配置安全性	Checkov、Terrascan、kube-score	Palo Alto Prisma Cloud、Bridgecrew

阶段	功能类别	功能说明	常用开源产品	商业/企业版产品
	配置合规检测	自动验证系统/云环境配置是否符合基线	OpenSCAP、CIS-CAT	Tenable Cloud Security、Qualys
7. Operate（运行阶段）	**容器与主机运行时安全**	监控容器、进程、网络行为异常	Falco、Sysdig OSS	Aqua Security、Prisma Cloud Defender
	日志与审计分析（SIEM/SOAR）	集中收集日志，检测攻击行为	ELK Stack、Wazuh	Splunk、IBM QRadar、Microsoft Sentinel
	漏洞管理与资产管理	统一跟踪与修复安全漏洞	OpenVAS、Vuls	Qualys VMDR、Rapid7 InsightVM
8. Monitor（持续监控）	**安全监控与告警**	持续监测安全事件、基线偏移	Prometheus + Alertmanager、Grafana Loki	Datadog Security、AWS Security Hub
	合规性与报告	输出安全态势报告与审计追踪	OpenSCAP、DefectDojo	Tenable、ServiceNow Security Ops

baidu/openrasp： 🔥开源RASP解决方案

sbom-tool: SBOM-TOOL 是通过源码仓库、代码指纹、构建环境、制品信息、制品内容、依赖组件等多种维度信息，为软件项目生成软件物料清单（SBOM）的一款CLI工具。