DevSecOps/SecDevOps Checklist v2.0

Plan

- Design security requirement
- Privacy requirement
- Asset Management requirement
- Architecture security requirement
- Secure coding best practices requirement
- Threat modelling
- Compliance requirement
- Infrastructure security requirement

Code

- Credentials & key management
- SCA
- SAST
- Security test cases generation
- Manual code review
- IDE integrated security solutions and plugins
- Source code management
- IAM (Groups, roles, policies & permissions)
- Data backup, restore, recover
- Coding platform security & best practices (GitHub, GitLab, etc.)

Build

- Infrastructure as code security
- Data security
- SSO
- Least privileges
- IAM (Groups, roles, policies & permissions)
- Service accounts
- Dependency
- Database configuration security
- Application configuration management
- Build automation
- Container registry
- IAST
- Image security
- Compliance
- Network security
- AAA (AuthN/AuthZ/Accountability)
- Container orchestration
- Cluster management
- Endpoint security
- Cloud security posture management
- IAM (Groups, roles, policies & permissions)
- Microservice security
- Content delivery & protection

Internal Security Testing

- DAST
- Functional security testing
- Internal red teaming
- Vulnerability management
- Security scanning through open-source tools
- Purple teaming exercise

Release/ Deployment

- Dockers and Kubernetes security
- IAM (Groups, roles, policies & permissions)
- Build process automation security and IAM
- UAT to production security
- Private connectivity & remote access
- Security detection, & monitoring solutions implementation security & review (WAF, SIEM, SOAR, DDOS, etc.)
- Secure and monitor the entire physical and virtual environment
- Certificate management
- Segregation of duties (process, hardware, software, environment)

External Security Testing

- Penetration testing
- External red teaming
- Bugbounty

Security Monitoring

- Security operations monitoring
- Security event monitoring
- Security incident management and monitoring
- Threat intelligence exercises
- Threat hunting exercise
- SIEM
- SOAR
- WAF alerts
- DDOS detection & protection
- Packet Analysis
- IDS/IPS implementation security & review

Run/Operate

- Bug fixes
- Patch management
- Operational security
- Software release integrity check security
- New release security and automation
- Incident management and response
- Cross-team security awareness training (Building culture)
- Version control and metadata management
- Compliance management
- Logging, auditing and monitoring