DevSecOps Security Controls

DEVELOPMENT

OPERATIONS

SPRINT

SPRINT

SPRINT

SPRINT

1 Secure code training

Engineers gain knowledge and awareness of AppSec principles and responsibilities.

2 Secure by Design

Gather threat and abuse case models and security requirements. Adopt reusable Secure-by-default design patterns.

3 Pre-commit configuration for secret scanning

Secure access to app. code & image repository

Implement least privilege RBAC and n/w isolation to code and private container repository. Infrastructure as code version controlled.

4 Secure access to CI service

Prevent unauthorised manipulation of the pipeline itself with RBAC and separation of duties.

5 Code Analysis

SAST: Analyse code for vulnerabilities. IDE and build server integrated with remediation advice.

6 Composition Analysis

Analyse Third Party/Open Source libraries. Reuse secure code only and comply with OSS licensing.

7 CI Server deploys to test

Automated deployment via Infrastructure as Code

8 Security Tests

DAST: Perform App specific automated security testing and dynamic container analysis.

Validate controls are mitigating the abuse case threat vectors.

9 Security review human logic test

Conduct Penetration testing where it makes sense. (Might not be needed for every sprint).

10 Image Assurance

Validate image integrity signatures, and that assurance policies are met to proceed to prod.

11 Deploy to Production

Automated deployment by Infrastructure as Code. IaC compliance and security testing.

12 Privileged access, secrets management & network isolation

Implement tight network & access policy, by locking down clusters/pods/VMs.

Use secrets management and automated certificate handling.

13 Application Protection

Protect and monitor the app and cluster using RASP/WAF and container sand-boxing

14 Infrastructure & Data Protection

Apply infrastructure hardening, data encryption endpoint protection, DLP and IPS.

15 Vulnerability scanning

Ensure continuous assessment & automated CIS benchmarking of build and deployed images and environments.

16 Continuous monitoring & Incident Response

Analyse intrusion / breach alerts and threat intelligence. Log attacks, behaviours and threats, to respond, learn from, and apply to next sprint.

17 Rinse & Repeat

Improve and enforce governance.

GATES

Automated

Sign-off

SECURITY

v1.0 - Sep 2020

©Copyright 2020 - Accelera Group Pty Ltd