OWASP SAMM v2 - Lean Security mapping

Software Assurance Lifecycle

Governance

Strategy & Metrics

- Create & Promote
- Measure & Improve
  - Continuous monitoring of security metrics
  - Implement centralised dashboards

Policy & Compliance

- Policy & Standards
- Compliance Management
  - Continuous monitoring of security SLAs
  - Continuous monitoring of security metrics
  - Implement centralised dashboards
  - Performing continuous assurance

Education & Guidance

- Training & Awareness
  - Continuous feedback from prod to dev
  - Provide security training
- Organization & Culture
  - Practice incident response
  - Self-service monitoring for dev & ops
  - Establish a security mindset
  - Establish security satellites

Design

Threat Assessment

- App Risk Profile
  - Performing risk analysis
- Threat Model
  - Performing threat modeling

Security Requirements

- Software requirements
  - Security requirements analysis
- Supplier security
  - Establish security SLAs for cloud providers

Secure Architecture

- Architecture design
- Technology management

Implementation

Secure Build

- Build Process
  - Secure the CI/CD pipeline
- Software Dependencies
  - Scan artifact and source code repos
  - Auto Container Security Scanning
  - Software Composition Analysis

Secure Deployment

- Deployment process
  - Secure the CI/CD pipeline
  - Security configuration automation
- Secret management
  - Implement secrets management

Defect Management

- Defect Tracking
- Metrics & Feedback
  - Continuous monitoring of security metrics
  - Implement centralised dashboards

Verification

Architecture Analysis

- Architecture Validation
  - Continuous monitoring of security controls
- Architecture Compliance

Requirements-driven Testing

- Control verification
  - Performing manual security testing
  - Integrate security tests in unit testing
- Misuse / Abuse testing

Security Testing

- Scalable baseline
  - Performing automated run-time testing
  - Performing automated static testing
- Deep understanding
  - Performing manual penetration testing

Operations

Incident Management

- Incident Detection
  - Continuous monitoring of security controls
  - Continuous monitoring of security SLAs
  - Continuous monitoring of application behavior
- Incident Response
  - Practice incident response

Environment management

- Configuration hardening
  - Continuous monitoring of system metrics
  - Continuous monitoring of security controls
  - Implement automated remediation
  - Security Configuration automation
- Patch & Update

Operational Management

- Data protection
- Legacy management

A B A B A B A B A B