OWASP SAMM TRAINING

Level - OWASP

Email – contact@DevOpsSchool.com

TRAINING AGENDA

DAY 1

Introduction to OWASP SAMM

- Overview of OWASP SAMM and its objectives
- Why maturity models matter in application security
- SAMM vs OWASP Top 10, ASVS, ISO 27001
- When and where to use SAMM

SAMM Structure & Maturity Levels

- SAMM framework overview
- Business Functions:
    - Governance
    - Design
    - Implementation
    - Verification
    - Operations

- Maturity levels and measurement approach

Governance Function

- Strategy & Metrics
- Policy & Compliance
- Education & Guidance
- Aligning AppSec with business goals

Design Function

- Threat Assessment
- Security Requirements
- Secure Architecture
- Risk-based design decisions

Mapping SAMM to SDLC & DevSecOps

- Embedding SAMM into SDLC phases
- DevSecOps alignment
- Roles and responsibilities
- Security champions model

DAY 2

Implementation Function

- Secure Build practices
- Secure Deployment
- Defect Management
- Dependency and supply-chain security

Verification Function

- Design review practices
- Code review and automated testing
- Penetration testing strategies
- Metrics and coverage tracking

Operations Function

- Incident management
- Environment hardening
- Vulnerability management
- Monitoring and logging

Performing a SAMM Assessment

- Scoping an assessment
- Evidence collection
- Scoring and benchmarking
- Gap analysis

Building an AppSec Roadmap Using SAMM

- Prioritizing improvements
- Short-term vs long-term goals
- Resource and budget planning
- Measuring progress over time

SAMM Integration with Other Standards

- SAMM + ASVS

- SAMM + OWASP Top 10
- SAMM + ISO, SOC 2, PCI DSS
- Enterprise compliance alignment

Real-World Case Studies & Best Practices

- Enterprise SAMM adoption examples
- Common challenges and pitfalls
- Scaling SAMM across teams
- Continuous improvement strategy