Mobile App Security Testing Implementation Checklist

neontri

Pre-development security requirements:

- [ ] Comprehensive threat model completed and reviewed by security architecture team
- [ ] Security requirements defined using appropriate OWASP MASVS profile based on data sensitivity
- [ ] Development team security training completed with certification and competency validation
- [ ] Secure coding guidelines established, distributed, and integrated into development workflows

Development phase security integration:

- [ ] SAST tools integrated into development environments and CI/CD pipeline with blocking capabilities
- [ ] Code review processes include mandatory security consideration checkpoints and expert validation
- [ ] Third-party library security validation completed before integration with dependency tracking
- [ ] Secrets management implementation validated, tested, and continuously monitored

Pre-release testing and validation:

- [ ] DAST execution completed with all critical and high-severity issues resolved and validated
- [ ] Manual penetration testing performed for applications handling sensitive data or financial transactions
- [ ] Regulatory compliance requirements validated through appropriate testing and documentation
- [ ] Security team formal approval obtained before production deployment with risk assessment

Production deployment and ongoing monitoring:

- [ ] Runtime monitoring and protection systems activated with comprehensive configuration validation
- [ ] Incident response procedures activated with appropriate team notification and escalation paths
- [ ] Regular security assessment schedule established with defined scope and reporting requirements
- [ ] Continuous improvement metrics collection and analysis implemented with executive reporting