The Mobile Security Lead

The Mobile Security Lead is responsible for leading and implementing security strategies for mobile applications and devices across the organization. This role ensures the security of mobile applications, platforms, and infrastructure through the implementation of security controls, conducting assessments, and working closely with mobile development teams. The position focuses on protecting sensitive data on mobile platforms while maintaining a balance between security and user experience.

Key Accountabilities

- Lead the technical implementation of mobile application security initiatives and strategies
- Design and implement security controls for both iOS and Android platforms
- Conduct mobile application security assessments, penetration testing, and code reviews
- Develop and maintain mobile security standards, policies, and procedures
- Lead security architecture reviews for mobile applications and infrastructure
- Perform mobile threat modeling and risk assessments
- Guide development teams in secure mobile development practices
- Oversee mobile application security testing and vulnerability management
- Implement and maintain mobile device management (MDM) security policies
- Lead incident response for mobile security incidents
- Provide technical mentorship to junior security team members
- Monitor and research emerging mobile security threats and trends

Required Education & Certifications

- Bachelor's degree in Computer Science, Information Security, or related field
- Industry certifications such as:
    - GIAC Mobile Device Security Analyst (GMOB)
    - CISSP (Certified Information Systems Security Professional)
    - OSCP (Offensive Security Certified Professional)
    - Mobile App Security Certification from OWASP
    - Apple Security Certification (preferred)
    - Android Security Certification (preferred)

Experience

- 7+ years' experience in information security or related field
- 5+ years' specific experience in mobile application security
- 2+ years' experience leading technical teams or projects
- Demonstrated experience with:
    - iOS and Android security architectures
    - Mobile application penetration testing
    - Mobile malware analysis
    - Mobile device management solutions
    - Secure coding practices for mobile platforms

Technical Skills & Knowledge

- Mobile Platform Security:
    - Deep understanding of iOS and Android security models
    - Experience with mobile OS security controls
    - Knowledge of mobile hardware security features
    - Understanding of mobile cryptography implementations
- Mobile Application Security:
    - Expert knowledge of OWASP Mobile Top 10
    - Mobile API security
    - Secure data storage on mobile devices
    - Mobile authentication and authorization
    - Secure communication protocols
    - Mobile app code signing and verification
- Security Testing:
    - Mobile application penetration testing
    - Static and dynamic analysis of mobile applications
    - Mobile API security testing
    - Reverse engineering of mobile applications
    - Mobile malware analysis
    - Mobile Device Management:

        - MDM solution implementation and management
        - Mobile security policy enforcement
        - BYOD security controls
        - Mobile container solutions
        - Enterprise mobility management
- Development Knowledge:
        - Understanding of iOS development (Swift/Objective-C)
        - Understanding of Android development (Java/Kotlin)
        - Mobile API development and security
        - Cross-platform framework security (React Native, Flutter,Xamrin)

Technical Competencies

- Mobile Security Architecture
- Application Security Testing
- Threat Modeling
- Incident Response
- Security Controls Implementation
- Mobile Forensics
- API Security
- Cloud Security for Mobile Applications
- Secure Development Practices
- Risk Assessment and Management

Behavioral Competencies

- Technical Leadership: Ability to guide and mentor security team members
- Communication: Excellence in explaining complex security concepts to various audiences
- Collaboration: Strong partnership skills with development teams and stakeholders
- Problem Solving: Advanced analytical and troubleshooting capabilities
- Innovation: Ability to develop creative solutions for complex security challenges
- Adaptability: Flexibility to respond to evolving mobile threats and technologies

Key Success Factors

- Successful implementation of mobile security programs
- Reduction in mobile security incidents and vulnerabilities
- Effective collaboration with mobile development teams
- Timely completion of security assessments and remediation
- Successful implementation of mobile security controls
- Positive team mentorship and knowledge sharing
- Development of secure mobile development guidelines
- Improved mobile security posture across the organization

Additional Responsibilities

- Stay current with mobile security trends and threats
- Participate in mobile security community events and forums
- Contribute to mobile security standards and best practices
- Develop metrics for measuring mobile security effectiveness
- Support audit and compliance requirements for mobile applications
- Assist in budgeting and resource planning for mobile security initiatives