## **NAME:**

## **Email:**

## **Phone:**

**Mobile Security Developer**

### **Professional Summary**

* Mobile Security Developer with **10 years of enterprise experience** building, maintaining, and securing mobile applications with a focus on Runtime Protection Agent SDKs for Android (Kotlin/Java) and iOS (Swift/Objective-C).
* Expert in detecting mobile threats including rooting/jailbreaking, debuggers, Frida, and dynamic instrumentation attacks across both Android and iOS platforms.
* Skilled in implementing low-level system APIs, JNI/C/C++ integrations, and platform security features to protect sensitive enterprise data.
* Proven ability to optimize cross-platform mobile solutions for performance, memory efficiency, and battery consumption while maintaining a lightweight SDK footprint.
* Experienced in developing demo applications for both platforms to demonstrate SDK features and facilitate seamless product integration.
* Strong collaboration with product, QA, and DevOps teams to integrate security agents into existing mobile applications with zero disruption to user experience.
* Hands-on experience with CI/CD pipelines, automated testing, monitoring frameworks, and agile methodologies for enterprise mobile development.
* Skilled in code reviews, mentoring, and providing best practices for secure mobile development across Android and iOS platforms.
* Continuously evaluates emerging mobile threats and implements proactive countermeasures in SDK and application architectures.
* Experienced in creating detailed technical documentation, audit reports, and enterprise-ready deployment guides for mobile security solutions.
* Expertise in troubleshooting, performance profiling, and memory optimization to ensure SDK reliability across a wide range of devices and OS versions.
* Deep understanding of cross-platform development challenges, including platform-specific security quirks, API differences, and threat mitigation strategies.
* Strong knowledge of mobile networking, encryption, certificate pinning, and secure communication channels between apps and backend systems.
* Skilled at automating static and dynamic analysis of mobile apps to detect vulnerabilities and validate threat mitigation mechanisms.
* Adept at mentoring junior developers on secure coding practices, runtime threat detection, and mobile security testing processes.

## **Technical Skills**

| **Category** | **Skills and Technologies** |
| --- | --- |
| **Mobile Platforms & Core Languages** | Android (Kotlin, Java), iOS (Swift, Objective-C), Native/Low-Level (JNI, C, C++) |
| **Mobile Security Focus** | Runtime Protection Agent SDK Development (RPA), Rooting/Jailbreaking Detection, Dynamic Instrumentation (Frida) Detection, Debugger Detection, Tampering Detection, Low-Level System API Integration. |
| **Secure Communication** | Certificate Pinning, Encryption, Token-based Authentication, Secure Data Transmission, Encrypted APIs. |
| **Testing & Quality** | Automated Testing (Appium, Espresso, XCTest), Automated Static/Dynamic Analysis, Performance Profiling, Memory Optimization, Battery Consumption Optimization. |
| **DevOps & Tooling** | CI/CD Pipelines (GitHub Actions, Jenkins), Git, Docker, Firebase (Crashlytics/General), Telemetry Monitoring. |
| **Methodologies & Practices** | Agile/Scrum, Secure Coding Practices, Code Reviews, Cross-Platform Integration, Technical Mentorship. |

### **Professional Experience**

#### **Client:**

**Mobile Security Developer**   
**Environment:** Android (Kotlin, Java), iOS (Swift, Objective-C), JNI/C/C++, CI/CD (GitHub Actions, Jenkins), Docker, Firebase Crashlytics, Agile/Scrum

**Responsibilities:**

* Designed and implemented the Runtime Protection Agent SDK for Android, detecting rooting, debuggers, Frida, and other runtime threats while maintaining a lightweight, high-performance footprint suitable for enterprise mobile applications.
* Built and maintained demo applications for Android and iOS to showcase SDK threat detection capabilities, allowing product and QA teams to validate SDK functionality before production deployment.
* Developed native Objective-C and Swift modules to detect jailbreak attempts and unauthorized instrumentation on iOS devices, ensuring secure mobile environments.
* Integrated JNI and C/C++ components to enhance detection of low-level system attacks on Android devices, improving threat coverage without affecting app performance.
* Implemented secure communication mechanisms, including encrypted APIs, token-based authentication, and certificate pinning for mobile-to-backend interactions.
* Collaborated closely with product teams to integrate the Runtime Protection Agent into client mobile apps, ensuring seamless deployment and minimal disruption to user experience.
* Optimized threat detection algorithms for CPU and memory efficiency, ensuring minimal battery impact across a wide range of devices and OS versions.
* Developed automated testing frameworks to validate SDK functionality using Espresso, XCTest, and Appium for cross-platform threat detection.
* Conducted code reviews and provided technical mentorship to junior developers on secure mobile coding practices, cross-platform threat detection, and JNI/C++ integration.
* Monitored mobile application telemetry and implemented proactive countermeasures against emerging threats, keeping SDKs up to date with the latest mobile attack vectors.
* Researched and evaluated new mobile security techniques, integrating relevant innovations into SDK design and runtime threat detection logic.
* Maintained detailed technical documentation and deployment guides for enterprise mobile applications utilizing the Runtime Protection Agent SDK.
* Participated in Agile ceremonies, sprint planning, and threat mitigation discussions to ensure alignment between security and product objectives.
* Provided detailed reports on mobile threat incidents and recommended actionable improvements for SDK and application-level security.

#### **Client:**

**Mobile Security Developer**   
**Environment:** Android (Kotlin, Java), iOS (Swift), C/C++, Firebase, Jenkins, Git, Agile

**Responsibilities:**

* Developed and maintained the Runtime Protection Agent SDK for Android devices to detect rooting, debugging, and dynamic instrumentation threats while safeguarding sensitive patient data.
* Implemented native Swift and Objective-C modules to identify jailbreak attempts and enhance iOS device security, aligning with HIPAA compliance requirements.
* Created demo applications for Android and iOS to demonstrate runtime threat detection to internal QA teams and stakeholders.
* Integrated low-level system APIs and JNI/C components to monitor device integrity, detect tampering, and block unauthorized activity on both platforms.
* Collaborated with product teams to embed SDK into enterprise mobile applications, providing real-time threat detection without impacting user experience.
* Conducted extensive performance profiling to ensure the SDK remains lightweight and optimized for battery consumption.
* Automated mobile security testing using Appium, Espresso, and XCTest, verifying comprehensive threat detection across Android and iOS platforms.
* Monitored emerging security threats and applied proactive SDK updates to maintain robust protection against new attack vectors.
* Designed secure data transmission using encryption, certificate pinning, and token management to protect sensitive enterprise information.
* Mentored junior developers on cross-platform threat detection strategies and secure coding practices for mobile applications.
* Performed detailed code reviews to ensure adherence to secure coding standards across Android and iOS applications.
* Worked with QA to implement automated regression testing for SDK modules, ensuring consistent threat coverage.
* Documented SDK architecture, threat detection logic, and integration guidelines for enterprise deployment.
* Provided technical support for product integration challenges related to cross-platform mobile security.

#### **Client:**

**Mobile Security Developer**   
**Environment:** Android (Java), iOS (Objective-C), JNI/C/C++, Firebase, Agile/Scrum

**Responsibilities:**

* Implemented Runtime Protection Agent SDK across Android and iOS platforms, focusing on rooting/jailbreaking and debugger detection to secure customer-facing mobile applications.
* Built demo applications for stakeholders to showcase runtime threat detection and SDK functionality.
* Developed native C/C++ modules to extend detection capabilities for low-level system vulnerabilities on Android devices.
* Worked closely with product teams to integrate SDK into production apps, providing actionable threat alerts in real time.
* Conducted cross-platform performance optimization, ensuring SDK modules remain lightweight and performant on both Android and iOS.
* Implemented secure backend communication channels using encryption, token authentication, and certificate pinning.
* Automated static and dynamic testing for SDK modules to ensure consistent protection across mobile OS versions.
* Mentored junior engineers on mobile security principles, threat detection techniques, and secure integration practices.
* Produced detailed technical documentation, integration guides, and deployment instructions for enterprise clients.
* Researched emerging mobile threats and implemented SDK updates to mitigate vulnerabilities proactively.
* Supported DevOps teams in creating CI/CD pipelines for automated SDK deployment.
* Provided technical recommendations to product teams to improve SDK coverage and application security posture.
* Monitored SDK telemetry and generated detailed reports for internal security audits.
* Participated in Agile ceremonies, providing security-focused guidance on mobile application development priorities.

#### **Client:**

**Mobile Security Developer**   
**Environment:** Android (Java), iOS (Objective-C), C/C++, Jenkins, Git, Agile

**Responsibilities:**

* Designed and implemented Android Runtime Protection Agent SDK, detecting rooting, debugging, and malicious instrumentation attempts in real time.
* Developed iOS threat detection modules to identify jailbreaks and prevent unauthorized code execution.
* Built demo applications for Android and iOS to validate SDK functionality for internal teams and stakeholders.
* Integrated JNI/C components to enhance low-level security monitoring and threat detection on mobile devices.
* Worked collaboratively with product teams to integrate SDK into mobile applications with minimal user impact.
* Conducted performance profiling to optimize CPU, memory, and battery usage while maintaining SDK reliability.
* Automated security testing using Espresso and XCTest to ensure cross-platform threat coverage.
* Mentored junior developers on secure coding, threat detection techniques, and cross-platform integration.
* Monitored mobile telemetry to identify unusual device activity and implemented proactive mitigations.
* Documented SDK architecture, threat detection algorithms, and integration procedures for enterprise use.
* Participated in sprint planning and Agile ceremonies to prioritize mobile security enhancements.
* Applied emerging mobile security best practices to update SDK and maintain cutting-edge threat detection.
* Coordinated with QA to ensure end-to-end testing of runtime protection features.
* Provided actionable feedback to product teams regarding mobile security risks and mitigation strategies.

#### **Client:**

**Mobile Security Developer**   
**Environment:** Android (Java), iOS (Objective-C), C/C++, SVN, Jenkins, Agile

**Responsibilities:**

* Developed Runtime Protection Agent SDK for Android and iOS to detect rooting, jailbreaking, debuggers, and dynamic analysis tools.
* Built demo applications to demonstrate SDK functionality and facilitate product integration testing.
* Implemented low-level C/C++ modules to enhance threat detection accuracy on Android devices.
* Integrated SDK into enterprise mobile applications, collaborating closely with product and backend teams.
* Designed secure communication protocols, including encrypted APIs and token-based authentication.
* Conducted code reviews to ensure secure coding practices across mobile platforms.
* Automated mobile security tests for both Android and iOS platforms to validate runtime threat coverage.
* Optimized SDK modules for performance, battery, and memory efficiency while maintaining detection accuracy.
* Mentored junior developers on mobile security best practices and cross-platform integration challenges.
* Maintained detailed technical documentation and integration guides for enterprise deployment.
* Monitored SDK telemetry to detect potential attacks and provided mitigation recommendations.
* Researched emerging mobile threats and implemented timely updates to SDK modules.
* Assisted product teams in embedding the Runtime Protection Agent without impacting application UX.
* Participated in Agile ceremonies and sprint reviews to ensure alignment between security and product objectives.