## **NAME:**

## **Email:**

## **Phone:**

**Mobile Security Developer**

**Professional Summary**

* Accomplished Mobile Security Developer with 9+ years of enterprise experience designing, building, and securing mobile applications, specializing in Runtime Protection Agent SDKs for Android and iOS to detect rooting, jailbreaks, debuggers, and dynamic instrumentation attacks.
* Expert in Runtime Protection Agent SDK development, capable of detecting rooting, jailbreaking, debuggers, Frida, and other dynamic instrumentation attacks across Android and iOS platforms.
* Proficient in Android (Kotlin/Java) and iOS (Swift/Objective-C) development, with hands-on experience in cross-platform mobile security integration.
* Skilled in leveraging low-level system APIs, JNI, and C/C++ modules to implement robust runtime threat detection mechanisms without impacting app performance.
* Designed and maintained demo applications for Android and iOS, enabling QA teams to validate SDK functionality prior to enterprise deployment.
* Optimized SDK performance to minimize CPU, memory, and battery usage while maintaining high detection accuracy and lightweight footprint.
* Implemented secure communication channels, including token-based authentication, encryption, and certificate pinning for secure app-to-backend data transfer.
* Hands-on experience with CI/CD pipelines (GitHub Actions, Jenkins), Docker, Firebase Crashlytics, and telemetry monitoring to support automated deployment and monitoring.
* Mentored junior developers on secure coding practices, cross-platform SDK integration, and runtime threat detection techniques.
* Conducted static and dynamic analysis, automated testing, and performance profiling to ensure enterprise-grade security and reliability.
* Collaborated with product, DevOps, and QA teams to integrate SDKs seamlessly, ensuring minimal disruption to the end-user experience.
* Monitored emerging mobile threats and implemented proactive countermeasures to enhance SDK protection across diverse device and OS environments.
* Authored comprehensive technical documentation, deployment guides, and audit reports to support enterprise-level SDK adoption.
* Participated actively in Agile/Scrum ceremonies, including sprint planning, retrospectives, and security-focused backlog refinement.
* Strong understanding of cross-platform development challenges, OS-specific security quirks, and best practices for threat mitigation.

**Technical Skills**

| **Category** | **Skills & Technologies** |
| --- | --- |
| Mobile Platforms & Languages | Android (Kotlin, Java), iOS (Swift, Objective-C), JNI, C/C++ |
| Mobile Security | Runtime Protection Agent SDK, Root/Jailbreak Detection, Debugger & Frida Detection, Tampering Detection |
| Secure Communication | Certificate Pinning, Encryption, Token-based Authentication, Encrypted APIs |
| Cloud & Backend | AWS, Azure, Firebase, REST APIs, WebSockets |
| Testing & Quality | Espresso, XCTest, Appium, Static/Dynamic Analysis, Performance & Memory Optimization |
| DevOps & Tooling | CI/CD (GitHub Actions, Jenkins), Docker, Git, Firebase Crashlytics, Telemetry Monitoring |
| Methodologies & Practices | Agile/Scrum, Secure Coding, Code Reviews, Cross-Platform Integration, Mentorship |

**Professional Experience**

**Mobile Security Developer**

**Client:  
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 a high-performance Runtime Protection Agent SDK for Android that actively detects rooting, debugging, Frida instrumentation, and tampering, ensuring enterprise-grade mobile security without impacting app performance.
* Developed native iOS modules in Swift and Objective-C to proactively detect jailbreak attempts and unauthorized instrumentation, enhancing threat coverage across multiple iOS versions.
* Built and maintained cross-platform demo applications to validate SDK functionality for QA teams and product stakeholders, facilitating seamless enterprise deployment.
* Integrated JNI and C++ modules into Android applications to enhance low-level system monitoring and extend runtime threat detection capabilities across all supported devices.
* Implemented secure APIs, certificate pinning, and token-based authentication to protect mobile-to-backend communication, ensuring compliance with enterprise security policies.
* Conducted extensive performance profiling and optimization to minimize CPU, memory, and battery usage while maintaining high detection accuracy.
* Automated SDK testing using Espresso, XCTest, and Appium to validate threat detection across multiple OS versions, devices, and configurations.
* Collaborated closely with product and development teams to integrate SDK functionality seamlessly into enterprise applications, minimizing end-user disruption.
* Mentored junior developers on secure coding practices, SDK integration, and advanced mobile security concepts, fostering team knowledge growth.
* Monitored telemetry and real-time data from SDK deployments to proactively identify and mitigate emerging threats across the mobile fleet.
* Authored detailed technical documentation, deployment guides, and integration manuals to support enterprise clients in SDK adoption and maintenance.
* Participated in Agile ceremonies, including sprint planning, retrospectives, and threat mitigation discussions, ensuring alignment between product and security objectives.
* Conducted code reviews and audits to ensure adherence to enterprise-level secure coding standards and mobile security best practices.
* Researched and evaluated emerging mobile security threats and integrated proactive countermeasures into the SDK design and runtime detection logic.

**Mobile Security Developer**

**Client:  
Environment:** Android (Kotlin/Java), iOS (Swift/Objective-C), JNI/C/C++, Jenkins, Git, Firebase, Agile

**Responsibilities:**

* Developed and maintained the Runtime Protection Agent SDK for Android, detecting rooting, debugging, and dynamic instrumentation attacks to protect sensitive enterprise data across production applications.
* Implemented native iOS SDK modules to detect jailbreak attempts and unauthorized code execution, ensuring compliance with enterprise security and privacy requirements.
* Built demo applications for Android and iOS to demonstrate runtime threat detection capabilities to QA teams and stakeholders, supporting early validation and integration.
* Integrated low-level system APIs and JNI/C++ components to monitor device integrity, detect tampering, and block unauthorized activity across both mobile platforms.
* Conducted extensive performance profiling to ensure SDK modules remain lightweight and optimized for battery efficiency across diverse devices.
* Automated mobile security testing using Appium, Espresso, and XCTest to verify comprehensive threat detection on Android and iOS platforms.
* Collaborated with product teams to embed SDK functionality into enterprise applications, providing real-time threat detection without impacting user experience.
* Implemented secure data transmission using encryption, certificate pinning, and token-based authentication to protect sensitive information.
* Mentored junior developers on cross-platform threat detection, secure coding standards, and SDK integration techniques.
* Performed detailed code reviews to ensure adherence to secure coding and threat mitigation best practices.
* Documented SDK architecture, threat detection logic, and integration procedures for enterprise deployment and support.
* Worked with QA teams to implement automated regression testing for SDK modules, ensuring consistent coverage and detection reliability.
* Provided technical support for integration challenges related to cross-platform SDK deployment, enabling smooth adoption across enterprise apps.
* Participated in Agile ceremonies and threat modeling sessions, providing security-focused guidance for mobile application development priorities.

**Android Developer / Mobile Developer**

**Client:  
Environment:** Android (Java/Kotlin), iOS (Objective-C/Swift), C/C++, Firebase, Agile/Scrum

**Responsibilities:**

* Assisted in developing early-stage Runtime Protection Agent SDK features for Android and iOS, supporting enterprise-level mobile security initiatives.
* Built demo applications on Android and iOS to validate SDK functionality and showcase runtime threat detection to QA and product teams.
* Developed native C/C++ modules to extend low-level system threat detection capabilities, enhancing security coverage across supported devices.
* Integrated secure communication mechanisms using encryption, certificate pinning, and token-based authentication to protect mobile-to-backend data exchange.
* Automated static and dynamic analysis of SDK modules to ensure consistent threat detection and validate mitigation effectiveness across platforms.
* Conducted performance profiling to optimize CPU, memory, and battery usage while maintaining high detection accuracy and minimal footprint.
* Mentored junior engineers on mobile security principles, cross-platform threat detection, and secure SDK integration practices.
* Produced detailed technical documentation and integration guides to support enterprise deployment and maintainability.
* Supported DevOps teams in implementing CI/CD pipelines for automated SDK deployment and testing across Android and iOS platforms.
* Monitored emerging mobile threats and applied proactive SDK updates to maintain protection against new attack vectors.
* Collaborated with product teams to integrate SDK functionality smoothly into enterprise mobile applications.
* Assisted QA teams in automated regression and functional testing of SDK modules to ensure high reliability and security.
* Provided actionable recommendations to product teams to improve SDK coverage and overall mobile security posture.
* Participated actively in Agile sprint planning, backlog refinement, and security-focused discussions.

**Android Developer / Mobile Developer**

**Client:  
Environment:** Android (Java/Kotlin), JNI, C/C++, Jenkins, Git, Agile

**Responsibilities:**

* Developed enterprise Android applications with a focus on performance optimization and secure coding practices to meet client requirements.
* Assisted in initial implementation of Runtime Protection Agent SDK features, contributing to early-stage mobile threat detection efforts.
* Built demo applications for Android to validate SDK functionality and facilitate QA and stakeholder review.
* Integrated JNI and C++ modules to enhance low-level system monitoring and runtime threat detection on Android devices.
* Conducted code reviews to ensure maintainable, secure, and high-quality code standards were consistently followed.
* Optimized applications for CPU, memory, and battery efficiency while maintaining high-quality performance.
* Assisted QA teams with automated testing and regression verification to ensure SDK and application stability across devices.
* Documented application and SDK architecture to support enterprise deployment and knowledge transfer.
* Mentored junior developers on Android development best practices and secure coding techniques.
* Collaborated with DevOps teams to maintain CI/CD pipelines for automated builds, testing, and deployment of Android applications.
* Monitored emerging mobile threats and provided technical recommendations to enhance SDK functionality and application security posture.
* Participated in Agile ceremonies to prioritize features, security enhancements, and project deliverables.
* Assisted in integrating SDK modules with minimal impact on application performance and end-user experience.
* Provided actionable insights to product teams on improving mobile security practices and runtime protection strategies.

**Application Developer**

**Client:  
Environment:** iOS (Objective-C/Swift), Firebase, SVN, Jenkins, Agile

**Responsibilities:**

* Developed enterprise-grade iOS applications, ensuring robust performance, secure data handling, and adherence to best practices for usability and UX design.
* Participated actively in the design and development of application modules to meet functional requirements and enterprise product goals.
* Assisted in implementing early-stage mobile security features, laying the foundation for the future Runtime Protection Agent SDK.
* Built demo applications for QA teams and product stakeholders to validate application functionality and support early-stage testing.
* Collaborated closely with backend teams to integrate APIs, implement secure data handling, and ensure reliable communication between mobile apps and servers.
* Conducted code reviews to maintain clean, maintainable, and secure coding standards across the development team.
* Worked with QA engineers to identify defects, implement fixes, and ensure applications met both functional and security requirements prior to release.
* Participated in Agile ceremonies, including sprint planning, daily stand-ups, and retrospectives, ensuring timely delivery of features and milestones.
* Created detailed technical documentation, integration notes, and support guides for application modules to assist in ongoing maintenance and scaling.
* Assisted in integrating logging, monitoring, and crash reporting frameworks to track application performance, errors, and user interactions effectively.
* Mentored junior developers on iOS development, secure coding, and troubleshooting techniques to foster team growth.
* Optimized application performance, memory usage, and battery consumption across multiple iOS devices and OS versions.
* Collaborated with product teams to review UI/UX flows, ensuring applications met design, usability, and accessibility standards.
* Supported CI/CD pipelines using Jenkins for automated builds, testing, and deployment of iOS applications across environments.