

Dhruv Athaide

• athaidedhruv@gmail.com • linkedin.com/dhruvathaide • github.com/DhruvAthaide • +91 9320693337

Education

Amity University Mumbai

Bachelor's in Computer Application. CGPA: 9.69

Mumbai, India

July 2022 – June 2025

St. Xavier's College

12th Standard, Science Stream

Mumbai, India

Aug 2020 – June 2022

Experience

DeepCytes Cyber Labs

Mumbai, Maharashtra

Cyber Analyst – Red Team & Mobile Security

August 2025 – Present

Android Security Engineer / Mobile Security Engineer (Red Team Focus)

- Lead mobile-focused red-team research and development at Deepcytes, designing Android security, **mobile monitoring (Red Team)**, and anti-forensics tools used in controlled adversary simulations and client investigations.
- Architected a flagship Android WebRTC mobile monitoring platform enabling real-time peer-to-peer streaming of multi-sensor device telemetry for red-team operations.
- Built and optimized **Guardient**, Deepcytes' commercial mobile privacy and threat intelligence platform, enhancing permission-risk analytics, filesystem scanning performance, and behavioral anomaly detection.
- Contributed to the development of a custom secure Android OS for hardened mobile devices, modifying boot processes, system services, and startup configurations to enforce privacy and persistence hardening.
- Designed and implemented a remote detonation and anti-forensics system supporting conditional, silent, and tamper-triggered cryptographic data destruction to protect high-risk assets during compromise scenarios.
- Contributed core detection logic to **NoSurveil**, a BLE-based anti-stalking solution, implementing RSSI-based proximity analysis, tracker classification, movement correlation, and location-linked encounter history.
- Developed a notification listener threat detection framework to identify malicious applications abusing notification access for credential harvesting and covert data exfiltration.

AI and Red Team Lead Intern

Jan 2024 – June 2025

- Managed and mentored a team of **15+ AI Researchers** and **60+ Red Team Members**, increasing project throughput by 15% through structured pipelines and weekly sprint planning.
- Designed and automated **4 core cybersecurity platforms**, including an LMS and Red-Team SaaS interface, improving internal training efficiency and client onboarding across UK, India & Europe.
- Contributed to cyber intelligence research initiatives, strengthening internal threat detection frameworks and improving Deepcytes' analytical accuracy by 10%.

Truboard Partners

Mumbai, Maharashtra

Production & Software Testing Intern

June 2024 – Aug 2024

- Trained a Covenant ML model improving prediction accuracy for business applications and operational workflows.
- Conducted B2B marketplace research, identifying user-behavior insights that guided feature enhancements and improved platform engagement.
- Led development of an asset-monitoring automation system for ride-sharing fleets, reducing operational oversight costs.

DeepCytes Cyber Labs

Mumbai, Maharashtra

AI and Deep Web Intern

June 2023 – Dec 2023

- Contributed to AI-based intelligence-gathering tools improving internal threat-attribution accuracy.
- Supported Deep Web intelligence operations and research pipelines, enhancing cyber intel output quality by 10%.

Selected Engineering Projects

The following projects were developed as part of Deepcytes Cyber Labs UK engagements unless stated otherwise.

Android WebRTC Surveillance & Streaming Platform | Java, Android SDK, WebRTC, Socket.IO, Node.js

- Architected a covert Android surveillance framework for red-teaming and investigative use, enabling real-time peer-to-peer streaming of camera (single & dual), microphone, SMS, call logs, GPS location, notifications, and filesystem data via WebRTC.
- Implemented a persistent background streaming service with auto-restart on boot and app termination, including permission orchestration, stealth service management, and runtime signaling configuration.
- Developed a secure web-based monitoring dashboard using Socket.IO and WebRTC, supporting low-latency video/audio streams, live device telemetry, and remote file exploration with chunked transfer handling.

- Integrated STUN/TURN-based NAT traversal, automatic reconnection logic, and adaptive streaming for reliable cross-network surveillance operations.

Remote Detonation & Anti-Forensics Application | Kotlin, Android SDK, Firebase Cloud Messaging, C++ (NDK)

- Engineered a high-risk data protection application featuring remote and conditional cryptographic wipe mechanisms triggered via secure FCM commands.
- Implemented forensic-grade data destruction using multi-pass overwriting and rotating encryption algorithms (AES-GCM, AES-CTR, ChaCha20-Poly1305) to ensure unrecoverable deletion.
- Designed stealth protections including disguised utility UI, hidden PIN-gated access, SIM-state tamper detection, and uninstall prevention using Device Admin APIs.
- Hardened sensitive logic by offloading API secrets and encryption constants to native C++ (JNI), mitigating static and dynamic reverse engineering.

Guardient – Mobile Privacy & Threat Intelligence Application | Kotlin, Android SDK, C++ (NDK)

- Built a privacy-focused Android security platform featuring app risk classification based on sensitive permissions, installation source, and behavioral indicators.
- Engineered a filesystem threat scanner using an optimized BFS traversal strategy, hashing files (SHA-256) and validating integrity against a secure backend.
- Implemented deep package inspection using PackageManager and AppOpsManager to identify hidden permissions and suspicious app behavior.
- Strengthened application security through native API obfuscation (JNI) and strict ProGuard/R8 hardening for release builds.

NoSurveil – BLE Anti-Stalking & Tracking Detection Application | Kotlin, Android SDK, BLE

- Designed a real-time BLE radar system to detect nearby wireless trackers and devices using RSSI-based distance estimation and signal correlation.
- Implemented a background “Following Detector” to identify devices persistently moving with the user across time and location.
- Added MAC/OUI resolution, device classification, location history, and risk tagging to distinguish benign devices from potential stalking threats.
- Built privacy-first data controls including whitelisting, encrypted exports, and user-governed data retention policies.

LockGuard – Intruder Detection & Access Monitoring App | Kotlin, Android SDK, CameraX

- Developed a privacy-compliant intruder detection system that silently captures photos on failed unlock attempts using DevicePolicyManager events.
- Implemented a resilient foreground capture service with CameraX to ensure reliable operation across lock states and background conditions.
- Added advanced unlock monitoring via Accessibility Services to detect unauthorized successful unlock scenarios.
- Designed a secure, private in-app gallery for evidence review, ensuring all captured data remains isolated within scoped storage.

Notification Listener Threat Detection Tool | Kotlin, Android SDK

- Developed a defensive monitoring application to detect and flag apps requesting Notification Listener privileges commonly abused by spyware and data exfiltration malware.
- Implemented behavioral analysis and permission auditing to alert users of high-risk notification access patterns.

MobileSentinel – Mobile Security & Network Analysis Application | Java, Android SDK, XML, Python

- Developed a cybersecurity-focused Android application providing device vulnerability assessment, permission auditing, process inspection, and network security analysis.
- Implemented live network scanning, local port scanning (1–1024), SSL/cleartext traffic detection, and real-time traffic capture using Android VPN Service APIs.
- Built anti-keylogger detection logic by identifying suspicious overlay applications and monitoring accessibility abuse patterns.
- Integrated clipboard and URL phishing detection using a machine learning-based classification model for real-time threat identification.

Skills & Interests

Programming: Kotlin, Java (Android), Python, C, C++, C#, JavaScript, HTML, CSS, PHP, SQL, Firebase, MongoDB.

Mobile Security & Android Internals: Android Internals (Permissions, Background Services, Boot Processes), App & Device Forensics, Offensive Mobile Tooling, Accessibility Abuse Detection, Network Traffic Monitoring.

Cybersecurity Expertise: Red Teaming, Mobile Exploitation, VAPT (Web & Mobile), OSINT, Incident Response, Threat Intelligence, Malware Analysis, Social Engineering.

Security Tools: Nmap, Frida, Burp Suite, MobSF, Drozer, Metasploit, Wireshark, ADB.

Cloud & DevOps: Docker, Git, Linux, Bash, PowerShell, Azure, CI/CD Pipelines.

Project & Automation Tools: ClickUp, Google Apps Script, Automation Pipelines using Python.

Interests: Mobile Security, Offensive Tool Development, Red Team Operations.

Keywords: Android Security Engineer, Mobile Security, Platform Security, Red Team, Mobile Monitoring, WebRTC, BLE, VPNService, AOSP, DevicePolicyManager, Accessibility Service, Mobile Forensics.

Languages: English, Hindi, Spanish.

Certifications

- *Google Cloud Computing Foundations Certificate*
- *Google Developer Student Club Web Developer Certificate*
- *Google Cloud Certifications Profile*
- *Credly Certifications Profile*