~/ivan-dimitrov — cv.sh

ivan@gevgelija ~$ whoami

IVAN DIMITROV_



• ID_MATCH 1/1

Senior Android Engineer, Mobile Security · Cybersecurity | AppSec Engineer

ivandimitrov.si // ivanmboard@gmail.com // linkedin.com/in/ivan-dimitrov-6566a83aa // github.com/ivanmboard // Gevgelija, North Macedonia

Android engineer with 12+ years of mobile development at 3P Development and a growing focus on mobile and network security. Recent work includes an Android Wi-Fi and BLE security app, a Python network SOC tool, BLE and IoT device fingerprinting, forensic spyware screening of Android devices, and a full security assessment of my own production SaaS. I use AI-augmented engineering (Claude Code agents, rules and hooks) to ship faster, and I verify every step myself.

12+	7	19	11,494
YEARS ANDROID	SECURITY PROJECTS IN 2026	FINDINGS IN A SAAS ASSESSMENT	SPYWARE IOCS SCREENED

$ experience --sort=newest

Feb 2014 - Present LIVE

Android Developer / 3P Development

- 12+ years of Android application development.
- Endorsed for Android development by 30 peers on LinkedIn, 8 of them 3P colleagues.

$ security_projects --year=2026

Jun 2026 - ongoing LIVE

HostLedger / CapScan / Android security app

Kotlin · React Native / TypeScript · ADB

- Android security app with Wi-Fi scanning and protection modules: Wi-Fi Protection, BLE Spam Guard and Pegasus Protection.
- Replaced screenshot and coordinate tapping with uiautomator dumps that use exact element bounds; set the path toward Compose testTag and instrumented tests.

Nov 2026

CarrierPulse / Security assessment of owned infrastructure

OWASP ZAP · Burp Suite · Nuclei · Nmap · SSLyze · Wapiti

- Assessed my own fleet-compliance SaaS (React SPA, Spring Boot API, nginx, Cloudflare): 19 findings, including an origin reachable outside Cloudflare, TLS 1.0/1.1 (PCI-DSS fail), missing HSTS and exposed SSH, MariaDB and FTP.
- Confirmed no SQLi, XSS or injection issues; mapped versions to CVEs and split fixes I own from hosting-provider fixes. Delivered report, attack-surface map, retest checklist and scan scripts.

Oct 2026

Android forensic acquisition / Spyware screening

androidqf · MVT

- Acquired my own Android phone with androidqf and analysed it with the Mobile Verification Toolkit: 11,494 indicators loaded, no high or critical matches.

Sep - Oct 2026

BLE scanner and device identification / Wireless analysis

Python · bleak

- Decoded BLE advertisements through OUI, Bluetooth SIG company-ID and service-UUID layers; identified mesh lights, appliances, soundbars, Apple Find My and Samsung offline-finding beacons.

Jul 2026

V20_SOC_AI / Python network SOC tool

Python · scapy · MITRE ATT&CK

- Event bus, graph store with last-seen aging, MITRE ATT&CK tagging, trust-aware alert rate limiting, ASN and forward-DNS enrichment, and a live terminal dashboard, built over ~19 iterations.
- Live capture with DHCP, mDNS and NetBIOS name extraction and IoT fingerprinting; used it to identify and verify all 8 devices on my home network.

Jun 2026

Windows persistence investigation / Incident root cause

Registry SACL · Event 4657 · PowerShell

- Traced IFEO debugger hijacks that returned after every reboot. A registry audit SACL and Security event 4657 named the writing process; removed it and deployed a boot-persistent SYSTEM monitor that logs full forensic detail.

Jun 2026

NetworkLoggerNMAP / Parallel network scanner

PowerShell · nmap

- Runspace-pool producer/worker design: discovery hands slow nmap -A scans to a capped worker pool, and a ConcurrentQueue feeds a single CSV writer. De-duplication and per-target rescan cooldowns.

$ other_work

Jul 2026 Windows network hardening
Disabled LLMNR, NetBIOS, Print Spooler and CDPSvc; tuned SOC rules to drop recurring false positives.

Jul 2026 Android battery-test harness
Fixed screen locking during automated tests (Stay Awake, keyguard and PIN teardown via ADB).

Jun – Jul 2026 Claude Code workflow engineering
Global and path-scoped rules for Android projects, SessionEnd hooks for cross-session memory, subagents and Agent Teams.

$ early_projects 2011-2013

2013 Share Drive
Mobile app connecting travellers to make trips easier and cheaper. 2nd place, MobileAppCamp; semi-finalist, Venture Out Challenge.

2012 – 2013 PopustiMk
Discount marketplace for businesses and shoppers, with shortest-route directions to the nearest store.

2012 Screen Scratch
Android app using accelerometer input and an overlay UI.

2011 KupiSe
Online shop for gadgets and electronics; early e-commerce build and operation.

$ skills

MOBILE

Android (12+ yrs) · Kotlin · Android Studio · ADB · uiautomator · emulators · React Native / TypeScript

MOBILE SECURITY & FORENSICS

androidqf · MVT · Wi-Fi scanning · BLE protocol analysis

NETWORK SECURITY

Nmap · Wireshark / Npcap · scapy · ARP / DHCP / mDNS / DNS analysis · MITRE ATT&CK · IoT fingerprinting

WEB & APP SECURITY

OWASP ZAP · Burp Suite · Nuclei · SSLyze · Wapiti · TLS / HSTS / CSP / CORS hardening · CVE triage · Cloudflare

WINDOWS INTERNALS & IR

Registry auditing (SACL) · event logs · scheduled tasks · WSL · Defender / AppLocker / Smart App Control

LANGUAGES

Kotlin · Python · PowerShell · TypeScript

AI-AUGMENTED ENGINEERING

Claude Code: rules · hooks · subagents · Agent Teams · plugins

TOOLING

Git · Node.js · JDK 17 · VS Code · Python venvs

$ education

2010 – 2013
Engineer in Informatics, Professional Informatics Studies
Faculty of Computer Science and Engineering (FINKI), Skopje

$ awards

2013 2nd place, MobileAppCamp
Share Drive

2013 Semi-finalist, Venture Out Challenge
Share Drive

$ interests

Hardware and security tinkering (Flipper Zero, BLE / RF), network privacy