Ievgen Bondarenko

AI Infrastructure Security Researcher

SECURITY RESEARCH | AI INFRASTRUCTURE | REVERSE ENGINEERING | TECHNICAL EVALUATION

Roseville, California | Remote | US Citizen hi@ibondarenko.com ibondarenko.com github.com/ibondarenko1 LinkedIn

PROFILE

Security researcher focused on AI-serving, cloud, container, and open-source infrastructure. Combines source review, reverse engineering, and reproducible validation to establish root cause, exploitability, and practical impact. Experienced across coordinated disclosure with Google VRP, Microsoft MSRC, and CERT/CC VINCE.

SELECTED SECURITY RESEARCH

Critical MLflow advisory. Credited finder for CVE-2026-64849 and GHSA-7gwp-5pfp-969j. Identified unauthenticated full-read SSRF through redirect and DNS-rebinding bypasses, delivered a working proof of concept, and validated the connection-time IP fix.

Published AI inference CVE. Credited reporter for CVE-2026-46517 and GHSA-9xq9-36w5-q796 in LMDeploy. Reproduced unsafe remote-code trust during model loading, assessed impact, and supported coordinated remediation.

Google Cloud VRP award. Found SSRF, Google API-key disclosure, and response forgery through a request-level provider endpoint override in Google Genkit. The Google Cloud VRP panel triaged and rewarded the report.

Open-source hardening. Contributed 17+ merged security fixes across gVisor, Kubernetes, Microsoft Sentinel, Swift Package Manager, OSV-Scanner, Tink, vLLM, and Google Bumble.

Reverse engineering. Reverse engineered a commercial Bluetooth Mesh device, recovered vendor model opcodes from its Android application, and identified weaknesses in provisioning and node reset behavior.

PROFESSIONAL EXPERIENCE

Security and Compliance Consultant

Apr 2025 - Present

California, Remote

Run application and infrastructure security assessments across cloud, identity, endpoint, and control surfaces. Translate findings into prioritized engineering work and track remediation to closure.

Computer Security Manager

Dec 2022 - Mar 2025

Technohome Inc., Roseville, CA

Owned Windows and Linux endpoint and server security, hardening, patching, access reviews, pfSense rules, network segmentation, event investigation, and incident-response procedures.

Business Ownership and Operations Leadership

Earlier career

United States

Founded and operated an Amazon freight logistics business coordinating several dozen trucks and about 50 outsourced personnel. Managed vendors, operational risk, schedules, and service delivery.

CORE EXPERTISE

Research and validation	Secure code review, SAST, DAST, SCA, root-cause analysis, proof-of-concept development, source-to-sink tracing, fuzz and regression testing, CWE and CVSS analysis, coordinated disclosure
AI and systems security	Model serving and inference, SSRF, local-file access, cloud metadata exposure, containers, sandboxing, Kubernetes, dependency and supply-chain analysis, Bluetooth Mesh
Languages and tooling	Python, Go, C++ audit and analysis, Bash, PowerShell, Linux, Windows Server, Docker, GitHub Actions, Semgrep, Joern, CodeQL, Git

CERTIFICATIONS AND EDUCATION

CompTIA Security+ ce

Microsoft Certified: Security Operations Analyst Associate, SC-200

Sierra College, IT and Cybersecurity Program, Aug 2025 - Present

National Metallurgical Academy of Ukraine, B.S. in Engineering