Sherbano Khan

AI Security & GRC Analyst | Risk Assessment • Compliance • AI Governance

Bay Area, CA | sherbanok97@gmail.com | linkedin.com/in/sherbano-khan | github.com/sherbanokhan

Summary

Cybersecurity professional with a master's degree from UC Berkeley and 4+ years of technology operations experience. Hands-on experience in vulnerability assessments, penetration testing, security audits, and risk mitigation. Skilled in threat modeling, IAM, AI security and governance, software supply chain security, and security frameworks such as NIST and ISO 27001. Strong background in analyzing security risks, evaluating controls, and translating technical findings into actionable recommendations.

Technical Skills

Security Tools: Burp Suite Pro, Wireshark, Nessus, Nmap, Ollama (local LLMs), Git/GitHub, GitHub Actions (CI).
Security: Risk Assessment, Compliance Audits, Vulnerability Management, Security Policy & Controls, Identity Access Management (IAM) & Access Reviews, Multifactor Authentication (MFA) Testing, OWASP Top 10, Security Awareness Training, Threat Analysis, Network Security & Audits, Security Logging, Zero Trust, CVSS Scoring, Cryptography
AI Security & Governance: LLM & AI Agent Security, Prompt Injection Testing, AI Risk Assessment, Risk Registers
Frameworks: NIST CSF, NIST 800-53, NIST AI RMF, ISO 27001, ISO 42001, SOC 2, OWASP LLM Top 10, MITRE ATT&CK/ATLAS
Programming: Python, Java, C/C++, C#, JavaScript, PHP, SQL, HTML/CSS
Systems: Windows, macOS, Linux; POS systems; CMS (WordPress); Microsoft SQL Server, MySQL
Professional: Troubleshooting, Analytical Thinking, Data Analysis and Visualization, Verbal and Written Communication

Experience

Graduate Student Researcher, Master of Information and Cybersecurity **January 2025 – August 2026**
University of California, Berkeley | Berkeley, CA

- Enhanced cybersecurity skills and knowledge through a multi-disciplinary master's degree program. Maintained 3.9 GPA in rigorous coursework in cyber risk management, cryptography, software and network security, web application security, and artificial intelligence and machine learning in cybersecurity.
- Researched malicious domain detection through feature engineering and analyzed software supply chain threat evolution to develop adaptive GRC-aligned risk mitigation strategies.
- Capstone: Led development of Arguss, an autonomous supply chain security platform that scans npm dependencies for vulnerabilities and untrusted sources, auto-remediating low-risk fixes, escalating questionable ones to human reviewers, and blocking dangerous changes.

Web Application Security Intern **January 2026 – April 2026**
University of California, Berkeley | Berkeley, CA

- Collaborated with 5-analyst security team to conduct web application penetration tests and vulnerability assessments across 3 UC Berkeley IT departments, safeguarding systems for 10,000+ employees, faculty, students, and third-party vendors.
- Executed a structured 4-phase testing methodology (discovery, automated scanning, manual validation, reporting) using Burp Suite Pro and custom SQL crawlers, including MFA and IAM control testing against OWASP Top 10 risks.
- Identified and reported 10 vulnerabilities, including 1 critical-risk finding, and delivered risk-mitigation reports to application owners, driving remediation of 100% of identified issues.

Assistant Manager, Technology Operations **April 2021 – July 2025**
FedEx Office | Tracy, CA

- Promoted 3 times in 4 years (Customer Service Consultant → Lead Consultant → Assistant Manager) for consistently strong performance in technology operations and risk management.
- Oversaw technology and compliance operations across 8 locations, supporting 50+ staff and 1,000+ daily users, managing POS terminals, self-service stations, shipping systems, and network equipment to ensure system reliability and secure order processing.

- Reduced system downtime by 20% by troubleshooting and resolving hardware, software, and network issues across POS platforms, improving service continuity.
- Supported internal audits of application access, customer data protection, and system configurations, identifying vulnerabilities and driving stronger security compliance across all locations.
- Trained 50+ staff on cybersecurity awareness, password hygiene, secure system use, and data protection, strengthening security culture and reducing human-error risk.

Infrastructure and Security Intern **May 2023 – August 2023**

NFI INDUSTRIES | *Remote*

- Collaborated with 8 IT staff and achieved proper installation of Windows OS and third-party application patches, security patches and updates, remediating known vulnerabilities and reducing risk across 200+ systems.
- Performed regular cybersecurity audits of network infrastructure using Wireshark and Nmap, scanning for potential security threats and driving timely mitigation.
- Implemented critical security measures, including firewalls, encryption technologies, and access control systems, resulting in an improved cybersecurity posture.

Web Assistant **September 2022 – March 2023**

CALIFORNIA STATE UNIVERSITY, Stanislaus | Turlock, CA

- Maintained the university website (CMS), posting campus events and updating faculty profiles for departments.
- Fixed broken links and replaced expired files to keep website content accurate and current.

CYBERSECURITY AND TECHNICAL PROJECTS

- **AgentGuard (AI Agent Security Lab):** Tested how a local LLM agent (Ollama) with tool access can be tricked by prompt injection into leaking data; ran 3 attack techniques over 15 runs each and scored it CVSS 8.6 (High). A least-privilege allowlist blocked every attack. Wrote a vulnerability assessment, threat model (STRIDE, MITRE ATLAS), and AI governance playbook.
- **Arguss (Capstone):** Autonomous supply chain security platform scanning npm dependencies via a deterministic three-check pipeline (vulnerability, trust, and pipeline analysis) sourced from OSV.dev, GitHub Security Advisories, CVSS/EPSS scoring, CISA KEV, npm registry, and deps.dev. Built a Fix Confidence Engine to auto-merge low-risk fixes, escalate questionable changes for review, and block dangerous ones; Python backend, Jinja2/HTMX/Tailwind frontend; team of 3.
- **AI & Machine Learning Projects:** Built Python-based ML models for data classification, prediction, and pattern recognition using Scikit-learn, Pandas, and TensorFlow, improving accuracy and interpretability.
- **Additional Projects:** CTF competitions (web exploitation, reverse engineering, cryptography, forensics); Gym-Titus web app (Java, SQL, HTML/CSS, 5-student team); Train Reservation System (C++, Java, SQL); Python/SQL-based Computer Inventory Retrieval System.

EDUCATION

University of California, Berkeley

MASTER OF INFORMATION AND CYBERSECURITY (MICS) **|** GPA: 3.9 **August 2026**

- Relevant coursework: Programming Fundamentals for Cybersecurity, Cryptography for Cyber and Network Security, Software Security, AI and Machine Learning in Cybersecurity, Network Security, Cyber Risk Management, Web Application Security, Capstone.

California State University, Stanislaus

BACHELOR OF SCIENCE (B.S.) - COMPUTER SCIENCE **|** GPA: 3.6 | Magna Cum Laude **December 2023**

- Relevant coursework: Data Structures and Algorithms, Object-Oriented Design, Database Management Systems, Assembly Language Programming, Software Engineering Process, Computer Organization and Architecture.