

JACOB COOK

Sacramento, CA | (916) 709-1794 | jacobcookofficial@gmail.com

LinkedIn: [jcook-dev](#) | GitHub & Portfolio: [jacobdcCook](#)

EDUCATION & CERTIFICATIONS

WGU: MS, Cybersecurity (2026) | CSUS: BS, Computer Science (2024) GPA 3.50
CompTIA Security+ Certified (Score: 805/900) — Jan 2026
AI finalist, merit based scholarship matching application

TECHNICAL SKILLS

- Cybersecurity: Network Defense, Vulnerability Assessment, Incident Response, Cryptography, Firewall Configuration, CompTIA Security+
- Systems: Linux, Docker, Kubernetes, Azure AD, Cloudflare Tunnels, VirtualBox, Wireshark, PLC Troubleshooting, Root Cause Analysis
- Software Architecture: Python, FastAPI, JavaScript, React, Node.js, TypeScript, SQL, Git, PWA, AI API Integration

TECHNICAL PROJECTS

Daily Wellness Scheduler (AI-Driven Security & Architecture) 2025 – Present

- Architected full-stack app using FastAPI and Next.js for secure health data management and AI coaching
- Implemented end-to-end encryption for local storage and configured Azure AD authentication ensuring privacy
- Deployed self-hosting infrastructure utilizing Cloudflare Tunnels protecting home network from external threats
- Utilized prompt engineering accelerating development and integrating AI document processing features

Industry-Sponsored AI Platform (G3-GPT) 2024 – 2024

- Designed intelligent RAG platform using Pinecone and OpenAI facilitating enterprise document retrieval
- Engineered role-based access control systems enforcing strict data privacy for corporate stakeholders
- Collaborated with team of six engineers delivering production-ready AI help desk solution for industrial client

Security+ Engineering Lab Series 2025 – Present

- Simulated enterprise networks conducting vulnerability assessments and applying encryption in virtual environments
- Documented technical procedures and incident response commands demonstrating Security+ domain mastery

PROFESSIONAL EXPERIENCE

Target Distribution Center 2019 – 2025

Warehouse Operations (Engineering & Facilities Support)

- Optimized industrial systems ensuring high availability and operational security via proactive monitoring
- Sustained material handling infrastructure via hardware diagnostics minimizing operational downtime
- Administered hardware configuration updates and performed root cause analysis on critical system failures
- Validated system interoperability between industrial sensors and backend servers ensuring secure data reporting
- Executed technical change management procedures maintaining compliance with enterprise security standards

ADDITIONAL INFORMATION

- Passionate for camping, mountain biking, and hiking which drives resilience and situational awareness
- Explores emerging cybersecurity trends and technical innovations maintaining edge in security landscapes
- Dedicated to continuous professional growth and technical learning within complex enterprise environments