

Charles Tucker

Los Angeles, CA | chucktuck21@yahoo.com | 626-522-5125

LinkedIn: <https://www.linkedin.com/in/charles-tucker-843239355/>

GitHub: <https://github.com/RealPhantomLee> (Private repos — available upon request)

Vulnerability Management / Security Analyst

Security+ certified cybersecurity professional with an investigations and operations background. Hands-on in vulnerability assessment fundamentals, Linux administration, log analysis, and SIEM monitoring through documented labs. Known for clear reporting, evidence-based analysis, and disciplined incident escalation—ready to support vulnerability remediation workflows and SOC operations.

CORE SKILLS

- Vulnerability Management: vulnerability assessment concepts, risk prioritization (CVSS fundamentals), remediation tracking, patch validation concepts
- Security Operations: alert triage, log analysis, event correlation fundamentals, incident documentation, escalation workflows
- Systems & Networking: Linux CLI, users/permissions, processes/services, TCP/IP fundamentals, ports/protocols, troubleshooting
- Tools & Platforms: Wazuh (SIEM/EDR lab), Kali Linux, virtualization (VM labs), encrypted persistent environments, Python scripting fundamentals
- Investigation Strengths: OSINT, evidence collection, timeline building, report writing, risk awareness

CERTIFICATIONS

- CompTIA Security+ (Certified, 2026)
- Google Cybersecurity Professional Certificate (Coursera)
- TryHackMe: hands-on labs and skills practice

PROJECTS

Completed

- Kali Linux Virtual Security Lab (VM): maintained repeatable test environment for security tooling practice and Linux operations
- Encrypted Persistent Live USB (Kali): built portable encrypted workspace for consistent, secure tooling across multiple systems
- Raspberry Pi Security Lab System (custom build): configured dedicated Linux lab device for administration practice and security tooling
- Custom Desktop Build: lab hardware build, OS configuration, and troubleshooting baseline

In Progress

- SIEM & Endpoint Monitoring Lab (Wazuh): building log monitoring workflows for alert review/triage and investigation practice
- Microsoft Azure Security Lab: cloud VM deployment, network security controls (NSG/firewall rules concepts), logging/monitoring fundamentals

EXPERIENCE

Private Investigator / Surveillance Investigator — Advantage Investigations

Mar 2025 – Present

- Conduct investigations using OSINT, pattern analysis, and evidence collection; produce clear, defensible reports and timelines
- Identify anomalies, document findings, and communicate results with accuracy under time-sensitive conditions

Executive Protection / Security Specialist — J Blair Group, Inc.

Jan 2024 – Mar 2025

- Performed risk assessments, monitored environments for suspicious activity, and followed escalation procedures
- Maintained accurate documentation and operational communication during incidents

EDUCATION

Associate of Arts (A.A.), Criminal Justice — Citrus College