Quenton “SecurityQ” Carr

Cybersecurity Engineer & Threat Hunter — AI-Powered Defense

Dallas–Fort Worth, TX • www.securityq.org • contact@securityq.org • linkedin.com/in/securityq • github.com/githubscrtq

Summary

Hands-on defender with DFIR, threat hunting, and SOC engineering experience. Builds threat-informed detections, automates investigations in Python, and validates hypotheses in a Proxmox-based Home SOC (Security Onion + Wazuh) to cut time-to-detect and time-to-contain. Collaborates closely with IR, detection engineering, intel, and vulnerability management.

Core Skills

- Threat Hunting (MITRE ATT&CK;, hypothesis-driven hunts, Sigma/KQL)
- DFIR (triage, timelines, evidence packaging, chain of custody)
- Microsoft 365/XDR, Defender for Endpoint, Defender for Cloud
- Identity & Access: Entra ID P2, Conditional Access, SSPR/MFA
- Network Telemetry: Zeek/Suricata, SPAN/VLANs, Security Onion
- Automation: Python, PowerShell, log enrichment, IOC pivoting
- AI/ML for security workflows; LLM-assisted playbooks & guardrails
- Platforms: Proxmox, Linux, Windows Server, virtualization, GPU acceleration

Experience

Security Analyst / Threat Hunter — Btechnical Group (Dallas Cowboys)

Dallas, TX • Nov 2021 – Jun 2025

- Led hypothesis-based hunts across endpoint, identity, email, and network telemetry; partnered with IR and detections to operationalize findings.
- Built/tuned SIEM detections (KQL/Sigma) for post-exploitation, credential access, and suspicious persistence.
- Delivered daily threat snapshots and executive briefings; reduced alert fatigue by improving signal quality and documenting repeatable playbooks.

Principal Cybersecurity Consultant & Threat Hunter — SECURITYQ LLC

Dallas, TX • Jan 2020 – Nov 2021

- Performed DFIR engagements: evidence acquisition, timeline analysis, and legally defensible packaging with hash manifests.
- Automated IOC triage (VirusTotal, GreyNoise, Shodan) and correlated artifacts to user/entity risk to guide containment.
- Deployed Home SOC stacks (Security Onion, Wazuh) with SPAN VLANs to replicate attacker paths and validate detections.

Senior System Administrator (Amtrak National Project) — Halifax Corporation of Virginia

Manassas, VA • Mar 2006 – Sep 2012

- Managed Amtrak Altiris deployment server; executed national break-fix & rollout programs (awarded ~$1M contract).
- Repaired HP mini PCs and PTT thin clients; monitored the nationwide thin-client fleet and maintained imaging baselines.
- Coordinated with field engineers to minimize downtime and standardize builds across sites.

Selected Projects

- **SilentQ DFIR** — Automated evidence collector & timeline builder; outputs cryptographic manifests for chain of custody.
- **AI GuardRail Lab** — Hands-on lab for LLM prompt-injection defenses, OSINT enrichment, and policy-based red teaming.
- **Home SOC** — Proxmox + Security Onion + Wazuh with SPAN VLANs, GPU-assisted inference, daily threat reports, and hunt notes.

Education & Certifications

- Microsoft Certified: Azure AI Fundamentals (AI-900) — 2023
- Microsoft Certified: Azure Fundamentals (AZ-900) — 2024
- TryHackMe: SAL1 (SOC Analyst Level 1) — Certification/Badge
- Additional: SSCP Prep (LinkedIn Learning), Jr. Penetration Tester (TryHackMe)

Tools & Platforms

Microsoft 365/XDR, Defender for Endpoint/Cloud, Entra ID P2, KQL, Sigma, Elastic, Zeek/Suricata, Security Onion, Wazuh, Windows/Linux, Proxmox, Python, PowerShell, Git/GitHub, Docker, CUDA/PyTorch.