SHANNON A. SMITH

Security Operations | Threat Detection | Incident Response | Automation & AI

Durham, NC | 919-475-0777 | shannon.a.smith1223@gmail.com | LinkedIn | Portfolio | GitHub | Credly

PROFESSIONAL SUMMARY

Cybersecurity professional and U.S. Navy veteran who builds working SOC detection tooling, not just lab exercises — including a three-phase SOC pipeline, progressively built from alert triage through MITRE ATT&CK mapping to a stateful, self-directing investigation agent, alongside hands-on log, network, and forensic investigations across Windows and Linux systems. Strong foundation in the incident response lifecycle, SIEM analysis (Splunk), and attacker methodology, built through a competitively-selected spot in the WiCyS / SANS Security Training Scholarship (GFACT, GSEC completed; GCIH in progress). Seeking a Security Operations, Detection Engineering, or SOC Analyst role.

TECHNICAL SKILLS

Security Operations & SIEM: Splunk, log analysis, alert triage, incident investigation, threat hunting
Detection & Automation: Python, PowerShell, Bash, log parsing, workflow automation
Network & Endpoint Security: TCP/IP, DNS, Wireshark, Zeek, Snort, Nmap
Security & Assessment Tools: Burp Suite, Nessus, Hydra, CyberChef, Metasploit
Systems & Virtualization: Windows 10/11, Linux (Ubuntu, Kali), VMware, Docker
Frameworks & Concepts: MITRE ATT&CK, incident response lifecycle, least privilege, defense-in-depth, vulnerability management

CERTIFICATIONS

- GIAC Security Essentials Certification (GSEC) | Jul 2026
- GIAC Foundational Cybersecurity Technologies (GFACT) | Mar 2026
- Certified Ethical Hacker (CEH) | Jun 2025
- UiPath Certified RPA Associate | May 2025
- Splunk Certified Core Power User | Mar 2025
- CompTIA Linux+ | Feb 2025
- CompTIA Security+ (DoD 8570/8140) | Dec 2024
- CompTIA A+ | Dec 2024

In Progress:
- GIAC Certified Incident Handler (GCIH) | target Nov 2026

TECHNICAL & LAB EXPERIENCE

SOC Detection & Investigation Pipeline — *github.com/shannonasmith/AI-Security-Portfolio*
- A 3-phase SOC system, each phase expanding on the last: an alert-triage engine, a MITRE ATT&CK mapping layer (hybrid TF-IDF/embedding/rule scoring), and a stateful agent that investigates evidence and scores its own confidence.
- Phase repos: Alert Analyzer | ATT&CK Mapper | Agentic Engine

Selected Investigations & Labs — *shannonasmith.github.io/cyber.html*
- Traced attacker access patterns in Linux auth logs and enterprise DNS logs using Splunk.
- Performed multi-tool network and web app enumeration to validate unauthorized access paths.
- Threat actor write-ups: NotPetya, Wizard Spider, and Uber/Lapsus$ — attack-chain and tradecraft analysis.

WiCyS / SANS Security Training Scholarship | Sep 2025 – Present
- Selected competitively based on technical assessments and CTF performance, advancing through all five tiers of the national scholarship — SANS Beginner CTF, TryHackMe gamified learning, SEC275/GFACT, SEC401/GSEC, and current SEC504/GCIH.
- Completed SEC275 (GIAC Foundational Cybersecurity Technologies) and SEC401 (GIAC Security Essentials), covering system security, networking, cryptography, defensible network architecture, and Windows/Linux hardening.
- Currently completing SEC504 (GIAC Certified Incident Handler), covering the incident-handling lifecycle, computer crime investigation, and attacker tools including Nmap, Metasploit, and Netcat.
- Applied skills in hands-on labs across Ranges.io and TryHackMe, including forensics, web vulnerabilities, and privilege escalation exercises.

Cyber Security Expert Program | Intellectual Point | Oct 2024 – Aug 2025

- Completed 540 hours of hands-on cybersecurity training spanning SOC operations, network defense, and systems administration, aligned to Security+, Linux+, and CEH coursework.
- Performed security monitoring and alert triage using Splunk SIEM; conducted vulnerability assessments and simulated incident investigations using Kali Linux and Burp Suite.
- Built and hardened Linux systems in lab environments, applying networking and access-control fundamentals across enterprise-style network topologies.

Information Technology Training Program | NPower | Aug 2024 – Dec 2024

- Installed, configured, and supported Windows, Linux, and macOS systems in lab environments, troubleshooting hardware, software, and peripheral issues.
- Applied core networking fundamentals — TCP/IP, ports, protocols, and connectivity troubleshooting — to diagnose and resolve system issues.
- Completed CompTIA ITF+ and A+ coursework alongside Google IT Support training, building a foundation in end-user support and IT service delivery.

PROFESSIONAL EXPERIENCE

Technical Operations Supervisor | U.S. Navy | Aug 2004 – Aug 2008

- Led and supervised 20+ personnel in technical operations, maintenance, and troubleshooting for mission-critical equipment.
- Directed incident response and preventative maintenance to sustain high system availability under operational pressure.
- Built training programs that achieved a 100% team qualification rate.

Property Manager | Lampe Management Company | Jul 2009 – Jan 2022

- Utilized SiteLink (SaaS property management platform) daily for tenant accounts, billing, and reporting — hands-on exposure to day-to-day SaaS platform operations.
- Managed tiered access control (gate and keypad tied to tenant billing status) and coordinated a multi-vendor stack (fire alarm, elevator, HVAC, cameras, pest control) — identifying issues and routing them to the right vendor.
- Authored Standard Operating Procedures from scratch, including vendor escalation paths and incident reporting, where none existed before.
- Reduced past-due accounts by 52% and increased revenue by 30%, while maintaining near-100% occupancy across 120,000+ sq. ft. of commercial property.

Operations & Logistics Coordinator | Queen of Wines, LLC | 2017

- Coordinated inventory tracking, financial records, and vendor operations.
- Improved workflow accuracy and efficiency.

EDUCATION

- Master of Information Technology | Virginia Tech | 2023
  Graduate Certificates: Software Development, Cybersecurity Policy
- B.S., Technical Management | DeVry University | 2017

PROFESSIONAL AFFILIATIONS

- Member, Women in CyberSecurity (WiCyS)