DARRIN JACKSON

SECURITY ANALYTICS PROFESSIONAL | CYBERSECURITY SPECIALIST

♦ LOUISVILLE, KY 40205 ♦ (502) 436-2329 ♦ Darrinj99@gmail.com ♦ Portfolio: https://darrinj99.github.io/

PROFESSIONAL SUMMARY

Security Analyst with 4+ years of combined civilian and military experience protecting and maintaining mission-critical systems in secure environments. Holds an active Top Secret Security Clearance and certifications including CompTIA Security+, CySA+, and CSAP. Skilled in threat detection, incident response, vulnerability remediation, and system hardening, with hands-on experience in SOC operations, SIEM log analysis, CVE discovery, and compliance with DoD and NIST security standards.

SKILLS

Security Tools & Platforms

• Splunk • Security Onion • OpenVAS • Microsoft Defender • Nessus • Wireshark • Cisco Umbrella • Kali Linux security utilities • Active Directory

Technical Skills

• Endpoint hardening & configuration • Vulnerability scanning & remediation • SIEM log analysis • Network administration • Privileged account management • Patch & identity management • Python • Bash scripting

Security Frameworks & Processes

• Incident response • Threat detection & containment • Risk assessment • NIST 800-53 • CIS benchmarks • DoD STIG compliance • Access control enforcement

PROFESSIONAL EXPERIENCE

IT Support Specialist, 10/2024 - Current
ShipMonk – Louisville, KY

- Deliver Tier 1–2 technical and security support across warehouse operations, rapidly resolving incidents affecting hardware, software, and network availability.
- Troubleshoot and remediate LAN, endpoint, and peripheral issues with a focus on eliminating vulnerabilities and maintaining secure configurations.
- Perform endpoint imaging, user account provisioning/deprovisioning, and device hardening in alignment with corporate security policies and CIS benchmarks.
- Maintain detailed incident and asset records to support audit readiness and compliance verification.

Technical Support Specialist, 04/2024 - Current
Army National Guard – Frankfort, KY

- Diagnose and resolve hardware, software, and network issues on classified and mission-critical systems in secure facilities.
- Configure secure operating environments per DoD cybersecurity standards, manage privileged user accounts, and enforce least privilege access controls.
- Monitor system health, analyze logs for irregularities, and perform threat containment and mitigation to maintain mission readiness.
- Provide cybersecurity training and user awareness briefings to strengthen the organization's overall security posture.

Geospatial Engineer, 01/2017 - Current
Army National Guard – Frankfort, KY
- Lead secure collection, processing, and dissemination of classified geospatial intelligence supporting operational planning.
- Operate GIS platforms in air-gapped, access-controlled environments, ensuring strict compliance with information assurance and data protection policies.
- Integrate geospatial intelligence with cybersecurity considerations for operational planning and risk assessment.

Security Research, Labs & Projects

- Conduct independent vulnerability research, including discovery, reporting, and submission of a CVE affecting networked devices, with documented methodology and remediation guidance.
- Maintain a cybersecurity homelab simulating SOC workflows, vulnerability scanning, and incident response using Security Onion, OpenVAS, Kali Linux, and custom Python/Bash scripts for automation.
- Completed 50+ practical labs on TryHackMe and Hack The Box gaining experience in SIEM log analysis, web application security, and network exploitation.

Education

Bachelor of Science: Cybersecurity and Information Assurance – Western Governors University *(Currently Enrolled)*

Bachelor of Science: Computer Science and Engineering – University of Louisville *(Transferred)*

Military Technical Training – U.S. Army: Basic Leadership Course; Advanced Individual Training – Geospatial Engineering

---

Credentials & Professional Training

- **(06/25) CompTIA Security+:** *Secure network design, risk management, access control policies, and vulnerability remediation.*
- **(06/25) CompTIA CySA+:** *Security operations, SIEM log analysis, threat detection, and coordinated incident response.*
- **(06/25) CompTIA CSAP:** *Security event monitoring, forensic analysis, endpoint hardening, and posture improvement.*
- **Google Cybersecurity Professional Certificate:** *SOC operations, SIEM configuration, vulnerability scanning, Linux hardening, and incident simulations.*
- **IBM IT Fundamentals for Cybersecurity:** *NIST/ISO frameworks, governance and compliance, risk management, and access control models.*
- **(03/24)Top Secret Security Clearance**

Currently Pursuing

- PenTest+
- PCAP
- OSCP

Awards

Army Achievement Medal, Awarded for leading and managing the Geo-Spatial Section during a month-long, 24-hour WarSim exercise. Ensured the delivery of critical intelligence reports and analysis vital for operational success through strategic decision-making, technical proficiency, and effective leadership. 06/23