

Malik Griffin

Enterprise IT Operations & Cybersecurity Professional

Auburn, AL | 678.382.5547 | Malikf83@gmail.com

LinkedIn: linkedin.com/in/malik-griffin-0a13692a6 | GitHub: github.com/malikomari7 | Credly:

credly.com/users/malik-griffin7

Professional Summary

Cybersecurity professional with 4 years of IT support and security operations experience. Skilled in threat monitoring, incident response, SIEM log analysis, and endpoint security. Adept at managing Active Directory, VPNs, firewalls, and vulnerability remediation in enterprise environments. Proven ability to collaborate with security teams to detect, investigate, and mitigate threats. Certified in cybersecurity with ongoing pursuit of advanced GIAC and CompTIA certifications.

Relevant Experience

IT Operations Service Technician – Neptune Technology Group

June 2024 – Present

- Collaborated with SOC and security teams to triage email phishing reports, investigate suspicious activity, and respond to CrowdStrike and BeyondTrust endpoint alerts.
- Monitored authentication and access control issues through Aruba ClearPass (802.1X / EAP-PEAP) and coordinated with network engineers for resolution.
- Supported firewall rule changes and VPN configurations (Palo Alto/Fortigate) to strengthen enterprise perimeter security.
- Deployed and patched enterprise software using PDQ Deploy and Automox, enforcing security baselines with custom PowerShell worklets.
- Administered Active Directory, password resets, and group policies to ensure proper access management and compliance.
- Participated in 24/7 on-call rotation, providing escalation support for system outages, remote access requests, and security incidents.
- Documented SOPs and incident response steps to standardize SOC procedures and reduce repeat issues.

IT Support Technician (Field Deployment) – MEI, Inc.

January 2020 – August 2022

- Installed and secured enterprise-level medical systems across hospitals and clinics, ensuring HIPAA-compliant device isolation.
- Configured VLANs and router ACLs for segmented traffic; deployed PoE-enabled wireless access points and validated network segmentation.
- Ran and terminated fiber optic cabling for secure data center integration; validated connectivity and performance.
- Partnered with vendors (GE Healthcare, Siemens) to ensure compliance and operational security of deployed systems.
- Authored technical documentation for repeatable troubleshooting and secure deployment procedures.

Self-Study Cybersecurity Projects

August 2022 – Present

- Secure Home Network Setup: Configured firewall, segmented IoT devices, and implemented real-time monitoring.
- Virtualized SOC Lab: Built multi-subnet environment with DHCP, DNS, NAT, and VPN; simulated attacks and analyzed logs with QRadar/Splunk.

Certifications

- CompTIA Security+ (Scheduled – October 30, 2025)
- SANS GIAC Certification (In Progress)
- ISC2 Certified in Cybersecurity – June 2023
- IBM Agile Explorer – September 2022
- IBM Z/OS Pre-Apprenticeship Certification – September 2022

Education

Bachelor of Science in Computer Science: Cybersecurity
Liberty University – Graduated December 2024

Technical Skills

- Security Tools: CrowdStrike, QRadar, Splunk, BeyondTrust, Cyberproof, Automox
- Networking: VLANs, Subnetting, Cisco Meraki, VPNs, Aruba ClearPass, Firewall configuration (Palo Alto/Fortigate)
- Systems: Windows 10/11, Linux, Active Directory, Office 365 Administration, VMware, AWS
- Scripting/Automation: PowerShell, Python, MySQL, Jira, ServiceNow
- Security Practices: Incident Response, Log Analysis, SIEM Monitoring, Endpoint Security, Business Continuity & DR