JAMES MCNEELY

Youngsville, LA 70592 | 337-356-3218 | liquidblu25@gmail.com

PROFESSIONAL SUMMARY

IT service professional with more than two decades of technical support and network installation experience seeking to transition into a Cybersecurity Analyst / SOC Analyst role. Google Cybersecurity Professional Certificate holder with strong analytical skills, meticulous attention to detail, and proven incident management experience. Adept at diagnosing and resolving hardware and software issues for networked devices, coordinating incidents, and maintaining secure configurations. Knowledgeable in industry frameworks (NIST, ISO 27001) and cybersecurity fundamentals. Ready to leverage transferable skills in incident management, root-cause analysis, log analysis, and network troubleshooting to protect organizational assets and support security operations.

CERTIFICATIONS

- Google Cybersecurity Professional Certificate – Coursera (SIEM, Incident Response, Linux, SQL, Python, Security Frameworks)
- Google IT Support Professional Certificate – Coursera (Networking, Troubleshooting, System Administration, Security)
- CompTIA Security+ – In Progress

CORE COMPETENCIES

Security Operations:

Incident Response | Incident Management | Threat Detection | Security Monitoring | Log Analysis | Root-Cause Analysis | Alert Triage | Vulnerability Assessment | Security Awareness Training

Technical Skills:

Network Security | TCP/IP | DNS | DHCP | Firewall Concepts | Access Controls | SNMP | Remote Troubleshooting | Hardware Diagnostics | Software Troubleshooting | Windows | macOS | Linux Fundamentals

Tools & Platforms:

SIEM (Splunk, IBM QRadar, Azure Sentinel – Familiar) | Ticketing Systems | ServiceNow | Remote Desktop Tools | Log Management | Microsoft 365 | Google Workspace

Frameworks & Compliance:

NIST Cybersecurity Framework (CSF) | ISO 27001 | MITRE ATT&CK (Familiar) | Security Best Practices | Data Privacy | Least Privilege | Secure Authentication

PROFESSIONAL EXPERIENCE

Service Manager

Copyfax of Louisiana | Broussard, LA | October 2002 – Present

- Managed incident response for networked copiers, printers, and scanners; performed initial triage, gathered diagnostic information, and executed remote troubleshooting using remote control tools
- Identified and mitigated security vulnerabilities on networked peripherals including unsecured ports, default credentials, and outdated firmware
- Conducted on-site and remote device installations, configuring IP addresses, SNMP settings, and access controls; ensured secure integration with client networks
- Investigated recurring errors by reviewing logs, analyzing firmware updates, and examining user activity; documented root causes and implemented preventative measures
- Maintained accurate incident records, service events, and resolution steps; compiled reports identifying trends and recommending process improvements
- Trained staff on secure handling of customer data, device security protocols, and awareness of phishing and social engineering risks
- Coordinated with vendors to address firmware vulnerabilities and security patches; managed warranty issues and service contracts

Account Associate

Xerox Business Services | Irving, TX | July 1998 – September 2002

- Responded to service incidents for over 100 networked copiers and printers; troubleshot connectivity and performance issues, escalating unresolved problems
- Collected and analyzed usage data and logs; maintained accurate inventory and tracking records for audit and compliance purposes
- Analyzed customer feedback to identify recurring issues; recommended changes to improve device performance and security configurations
- Provided end-user security awareness training on secure printing and scanning practices to protect sensitive documents

EDUCATION & TRAINING

United States Air Force Reserve – Aircraft Electrical & Environmental Systems | San Antonio, TX | 2004 – 2007

Training emphasized strict adherence to safety and security protocols, attention to detail, and technical troubleshooting under pressure

Tarrant County College – Computer & Information Sciences (Some College) | Fort Worth, TX

Coursework in networking fundamentals, operating systems, and programming

PROFESSIONAL DEVELOPMENT

- Actively pursuing CompTIA Security+ certification to solidify knowledge of threat detection, vulnerability management, and incident response
- Completing online courses and labs covering Security Operations Center (SOC) workflows, SIEM fundamentals, and compliance frameworks (NIST CSF, ISO 27001, GDPR)
- Gaining hands-on experience with SIEM platforms including Splunk, IBM QRadar, and Azure Sentinel through lab environments

ADDITIONAL QUALIFICATIONS

- U.S. Citizen; eligible for security clearance
- Available for flexible hours and on-call rotations
- Strong work ethic with commitment to continuous learning in cybersecurity