SIDNEY THOMAS
North Carolina| sidneythomasworkcontact@gmail.com | LinkedIn sthomas35 | https://sid-sec.com/

PROFESSIONAL PROFILE

IT support and systems administration professional with experience providing Level 1 and Level 2 technical support across environments supporting 1,000+ devices and hundreds of users. Experienced in security monitoring, troubleshooting, Active Directory administration, endpoint management, log analysis, and documentation. Strong foundation in networking, Windows and Linux systems, and cybersecurity principles through professional experience, academic coursework, and hands-on lab environments. Seeking to leverage technical support and monitoring experience in a Security Operations Center (SOC) environment focused on continuous monitoring, alert triage, compliance, and incident response.

TECHNICAL SKILLS

- **Cybersecurity:** Security Monitoring, Alert Triage, Incident Investigation Support, Log Analysis, Vulnerability Scanning (Lab/Academic), Access Control, Patch Management, Security Documentation, Security Policies & Compliance Fundamentals, Risk Assessment Fundamentals
- **Networking**: TCP/IP, Subnetting, Routing, DNS, DHCP, Firewalls, VPNs, Network Troubleshooting, Packet Analysis, VoIP Troubleshooting
- **Systems Administration**: Windows Server & Client Administration, Active Directory (Users, Groups, GPOs), Microsoft 365, Linux Administration (Ubuntu/Mint), Endpoint Deployment, User Account Management
- **Tools & Platforms**: Wireshark, Nmap, OpenVAS, Zabbix, VirtualBox, VMware, Hyper-V, GNS3, AnyDesk, Salesforce
- **Programming & Scripting**: Python (Automation Basics), PowerShell, Bash, SQL Fundamentals
- **Soft Skills**: Analytical Problem Solving, Technical Documentation, Task Prioritization, Cross-Team Collaboration, Attention to Detail, Customer Support

---

EXPERIENCE

Combined Public Communications – Cold Spring, KY
IT Support Specialist, Level 2 | Nov 2024 – May 2025
IT Support Specialist, Level 1 | July 2024 – Nov 2024

- Monitored system performance, user activity, and network connectivity across multiple facilities, investigating anomalies and escalating issues as appropriate.
- Supported user account provisioning, access management, endpoint configuration, and security policy enforcement in Active Directory environments.

- Applied security-related configuration changes, patching activities, and access updates to maintain system integrity and reduce operational risk.
- Investigated and resolved technical incidents involving workstations, applications, network connectivity, and user access.
- Maintained detailed incident documentation and resolution records to support root-cause analysis, audit readiness, and operational reporting.
- Collaborated with technical teams to troubleshoot infrastructure issues and improve monitoring and support processes.
- Recognized by the CTO for resolving a complex access control issue that allowed users to exit a locked-down environment, strengthening system security and reducing organizational risk.
- Achieved record training completion time and became a trusted resource for peer mentorship and technical knowledge sharing.

Additional Experience: Harbor Freight - Logistics Member (July 2023 - Dec 2023) Avi Food Systems – Food Worker (Jun 2022 – Dec 2022) | Kroger Marketplace – Grocery Clerk (Mar 2019 – Jan 2021)

EDUCATION

Northern Kentucky University – Highland Heights, KY
Bachelor of Science, Information Technology – Network & System Admin Track
(Graduation date: June 2026)

Gateway Community and Technical College – Florence, KY
Associate of Science, Information Technology (Aug 2021 – Jul 2024) | GPA: 4.0
Certifications earned: **Computer Technician, Microsoft Enterprise Administrator, Microsoft Network Administrator and Information Security Specialist**

CERTIFICATIONS

CompTIA Security+ (In Progress)

RELEVANT COURSEWORK, LABS AND PROJECTS

- **Self-Administered Home Lab Environment:** featuring a multi-system virtualized network designed to simulate attacks on Windows systems using Parrot OS, with security events monitored and analyzed in Splunk.
- **Network Security & Vulnerability Labs**: Configured firewalls, VPNs, ACLs, and performed vulnerability scans with Nmap and OpenVAS.
- **Security+ Master Study Document:** Created a comprehensive personal guide covering