John Wesley Hallman II

Birmingham, AL area | jwessecurity.com | linkedin.com/in/johnwhallman

PROFESSIONAL SUMMARY

Highly certified and analytical Cybersecurity Professional with a B.S. in Cybersecurity and Information Assurance and over six years of progressive IT experience across systems administration and infrastructure support. Proven track record in monitoring networks, analyzing security logs, maintaining perimeter defenses, and triaging security incidents. Well-versed in leveraging SIEM utilities, deployment of advanced endpoint protection (EDR), threat mitigation, and vulnerability management to protect corporate infrastructure and ensure regulatory compliance.

CERTIFICATIONS

• CompTIA CySA+ (Cybersecurity Analyst) • CompTIA PenTest+ (Penetration Testing) • (ISC)² SSCP (Systems Security Certified Practitioner) • CompTIA Security+
• CompTIA Network+ • CompTIA A+ • CompTIA Project+

TECHNICAL SKILLS

Security Operations: Threat Monitoring, Security Alert Triage, Log Analysis, SIEM (Splunk/Graylog), Incident Response & Incident Containment, Vulnerability Assessment & Patch Management, Risk Mitigation

Endpoint & Systems: Microsoft Defender, Sophos Endpoint Protection, Identity & Access Management (IAM), Active Directory, Group Policy, Office 365 Administration, Windows Server, Linux (Ubuntu, CentOS)

Network Security: TCP/IP Protocols, VLAN Segmentation, VPN Architecture, Firewall Configuration, Wireshark Packet Analysis, Nmap Network Scanning, Multi-Factor Authentication (MFA/2FA)

Scripting & Tools: Python, Bash, PowerShell Automation, ITIL Processes, Technical Documentation

PROFESSIONAL EXPERIENCE

Deskside Support Tech – Allied Digital, Vance, AL April 2026 – Present

- Provide Tier 2 technical support for hardware, enterprise software, and core network connectivity, ensuring robust baseline security postures across corporate endpoints.
- Troubleshoot and resolve complex system performance issues to eliminate technical downtime and maintain operational availability of critical internal networks.
- Collaborate across infrastructure tiers to address endpoint vulnerabilities, support patching workflows, and verify system compliance with security baselines.

I.T. Technician – Kronospan, Anniston, AL Sept 2024 – April 2026

- Supported enterprise infrastructure upgrades and maintained comprehensive system documentation, change logs, and technical security runbooks.
- Managed user identities and privileges via Active Directory and Microsoft Exchange, enforcing least-privilege principles and secure Identity and Access Management (IAM) standards.
- Monitored systems for anomalous activity, diagnosed performance degradation issues, and maintained security layers including multi-factor authentication (MFA).
- Partnered with cross-functional technical teams to validate the integration of security controls and minimize the organizational threat surface.

Junior Network/Systems Administrator – Multimetco Inc., Anniston, AL Aug 2022 – Aug 2024

- Served as primary administrator for Microsoft Office 365, Sophos, and Microsoft Defender; managed conditional access policies, enforced email hygiene, and deployed endpoint security safeguards.
- Monitored, maintained, and hardened Windows Server and Linux environments, implementing routine vulnerability assessments and coordinating patch management.
- Analyzed event logs and threat alerts using open-source SIEM utilities (Graylog) to detect, investigate, and triage potential infrastructure security incidents.
- Maintained network security boundaries by configuring firewall access control lists (ACLs), managing secure VPN tunnels, and verifying VLAN routing.

- Managed incident response escalation pathways, delivering root-cause analysis and executing primary containment measures for service desk escalations.

Technical Support Specialist – Transcom, Remote Apr 2021 – Jul 2021

- Delivered high-quality customer service and technical support, managing competing priorities to quickly isolate and resolve hardware, software, and application access issues.
- Documented precise troubleshooting methodologies, incident details, and resolution steps to streamline knowledge base content and support team efficiency.

EDUCATION

Bachelor of Science in Cyber Security and Information Assurance
Western Governors University | Graduated: August 2025