James A. Coleman

owner@jamesacoleman.com | www.jamesacoleman.com | www.linkedin.com/in/cyberheim

Data Protection | Information Safeguarding | IT Transformation

SUMMARY OF QUALIFICATIONS

Multifaceted **Cybersecurity Analyst** and **Network Engineer** with over five years of cumulative project experience **mitigating system vulnerabilities** and **network threats**.

An influential communicator who **collaborates** effectively with project teams (IT, engineers, and developers) on network troubleshooting, **risk assessments**, and adopting security-related improvement methods. Seamlessly **conveys** potential threats to technical and non-technical audiences in a hybrid work environment.

Committed to ongoing professional development through the **continuous learning** of cybersecurity trends and their impact on computer systems and enterprise infrastructure. Qualifies for any level of security clearance if needed.

Additional security processes, systems, and related software platforms:

- **Cyber Frameworks** and **Models:** MITRE ATT&CK | NIST | ISO 27000/27001 | SOC2 | Zero Trust
- **Anti-Virus Measures, Malware Blocking, Firewalls, EPM, Dark Web Triaging,** and **Access Control Lists (ACL):** Fortinet, PFSense
- **Endpoint/Extended Detection and Response (EDR/XDR):** Elastic
- **Security Information and Event Management (SIEM**): Security Onion, Splunk
- **Threat Intelligence:** OpenCTI
- **Penetration Testing**: Kali Linux | Metasploit
- **Network Tools / Vulnerability Assessments:** SolarWinds, Wireshark, Nmap
- **Intrusion Detection** and **Prevention (IDS/IPS)**: OpenCanary
- **Containers:** Docker
- **Networking:** Cloud | LAN/WAN | SAN | VPN | HPE | Juniper | Ivanti | Tailscale
- **Internet Protocols**: TCP/IP | DNS | DHCP | IPsec | Wireguard
- **Operating Systems / Cloud:** Unix/Linux | Windows | MacOS | Android | iOS | AWS | Azure
- **Virtualization**: Type 1 & 2 Hypervisors | VMware | Proxmox
- **Databases:** Active Directory | Entra ID | SQL
- **AI / LLM**: Prompt Engineering, Model/Algorithm Coding, Slurm
- **Languages:** Python | JSON | HTML | Markdown
- **Knowledge/Workflow Management:** Confluence | ServiceNow
- Microsoft Office

Certifications:

- CompTIA **(CSCP, CCAP)**
- CompTIA **(Cloud +, Security +, Network +)**
- Fortinet **(FCA)**
- FEMA National Incident Management System (NIMS): ICS-100

PROFESSIONAL EXPERIENCE

Network Security Engineer | University of North Georgia (July 2024 – Present)

- Designs, implements, and maintains robust network security infrastructures, including firewalls, VPNs, intrusion detection/prevention systems, and cloud security solutions, to safeguard university systems against cyber threats.
- Conducts proactive monitoring and incident response, ensuring device hardening and the integrity of authentication infrastructures, while maintaining comprehensive documentation for audit and compliance purposes.
- Evaluates and integrates emerging technologies, assessing potential risks and impacts on university network infrastructure, and ensuring alignment with institutional projects and advanced computing initiatives.
- Collaborates with Information Security teams on investigations, assists in wireless network design and diagnostics, and provides flexible support across multiple campuses, including availability during maintenance windows as needed.

IT / Network Support Technician | Forsyth County Schools (Dec 2022 - July 2024)

- Managed multi-site IT system support and equipment deployment impacting over 500 employees. Accountable for providing additional layers of network security to safeguard sensitive data against sophisticated cyber threats.
- Implemented and configured multi-factor authentications (MFA) ensuring enhanced security protocols meet the school district's rigid requirements.

Technical Field Supervisor | Department of Commerce - U.S. Census Bureau (June 2020 - Nov 2020)

- Designed and executed extensive IT field training and security measures to ensure the safeguarding of personally identifiable information (PII) for over 112 team members. Delivered remote software support using advanced mobile device management (MDM) systems.

Independent Technical Security Consultant | Forsyth County Sheriff's Office (June 2016 - July 2016)

- Commissioned by a local police department to develop a secure communication system linking their mobile command center to hostage negotiation and SWAT vehicles. This eventually enabled a centralized incident command management system.

EDUCATION

University of North Georgia | **Bachelor of Science** - **Criminal Justice and Intelligence Analysis**
University of North Georgia | **Master of Science – Computer Science, Cybersecurity Concentration**

AFFILIATIONS

ISACA (Information Systems Audit and Control Association) | Atlanta Charter
SANS (SysAdmin, Audit, Network, and Security) | Community Member
INMA (InfraGard National Members Alliance) | Atlanta Charter

PROJECTS

Home Lab | VMWare ESXi, Baremetal Hypervisor, Dell Server, Networking, Juniper, Fortinet, HPE, OpenCTI**,** Security Onion Solutions, Tailscale, Ubiquiti.