

# James A. Coleman

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

## Data Protection | Information Safeguarding | IT Transformation

### SUMMARY OF QUALIFICATIONS

Multifaceted **cybersecurity** and **intelligence analyst** 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,** and **Dark Web Triaging**
- **Access Control Lists (ACL)** and **Endpoint Detection and Response (EDR)**
- **Security Information and Event Management (SIEM)**
- **Penetration Testing:** Kali Linux | Metasploit
- **Network Mapping / Auditing** and **Vulnerability Assessments:** Nmap
- **Intrusion Detection and Prevention (IDS/IPS):** Security Onion
- **Containers / Packet Analysis:** Docker | Wireshark
- **Networks:** Cloud | LAN/WAN | SAN | VPN
- **Internet Protocols:** Transmission Control (TCP) | Domain Name Systems (DNS) | DHCP
- **Operating Systems:** Unix/Linux | Windows | MacOS | Android, iOS | AWS | Azure
- **Databases:** Active Directory | SQL **Big Data:** Splunk
- Microsoft Office

Certifications:

- CompTIA (**Security +, Cloud +, Network +**)
- FEMA National Incident Management System (NIMS): ICS-100, Issued January 2024

### PROFESSIONAL EXPERIENCE

**IT Service Desk Coordinator** | University of North Georgia (July 2024 - Present)

- Oversee a single-point-of-contact team across five campuses responsible for the collection and dissemination of information across the entire functional IT structure including information security, networking, and engineering systems.
- Apply trend analysis to improve system performance and proactively address potential issues and threats by monitoring KPIs, patterns, and resources.
- Maintain defense in depth through effective MFA implementation, least privilege access, and effective user awareness and education.
- Lead projects developing and implementing service level agreements, standard operating procedures, onboarding documentation, and educational resources.

### **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.

### **Supervisor - Technology/Mobile Electronics** | Best Buy - Geek Squad (May 2012 - Jan 2018)

- Honed technical leadership expertise supervising eight direct reports with accountability for 40 associates. Provided network troubleshooting on a wide range of devices. Designed and implemented an advanced IoT network to accommodate smart technology for automated security systems.
- Selected by senior management to architect alpha and beta-level RTOS (real-time operating system) programs demonstrating a cutting-edge approach to testing and refining technologies.

## **EDUCATION**

University of North Georgia | **Bachelor of Science - Criminal Justice and Intelligence Analysis**

## **AFFILIATIONS**

**ISACA** (Information Systems Audit and Control Association) | Atlanta Charter

**SANS** (SysAdmin, Audit, Network, and Security) | Community Member

CIS (Criminal Investigative Society) | Former UNG Chapter Vice-President

## **PROJECTS**

**Home Lab** | VMWare ESXi, Baremetal Hypervisor, Dell Server, Networking  
Security Onion Solutions Lab | IDS, SIEM, Threat Hunting