Michael DiDomenico

Atlanta Metropolitan Area | MLD713@iCloud.com | MLD713.com | LinkedIn.com/in/MLDiDomenico

PROFESSIONAL SUMMARY

CompTIA Security+ certified cybersecurity professional pursuing entry-level SOC Analyst roles, and GRC Analyst positions. Backed by 380+ hours of hands-on training in security monitoring, SIEM and log analysis, alert triage, incident detection and response, and threat hunting using MITRE ATT&CK, plus working knowledge of risk assessment and compliance. Completed 50+ technical labs and 35+ real-world projects, including a full-cycle penetration test and a large-scale DDoS incident investigation applying NIST CSF, ISO/IEC 27001, and Zero Trust principles to detect threats, assess risk, and deliver actionable remediation guidance. I bring more than 30 years of work experience with strong investigative, analytical, and report-writing skills, plus a proactive, self-driven approach to identifying needs and driving improvements. Known for staying organized and customer-focused, resilient under pressure, and a clear, collaborative communicator across geographically dispersed teams and all levels of an organization; well suited to the fast-paced triage of a SOC, with the documentation discipline GRC work also demands.

EDUCATION

- **Springboard Cybersecurity Career Trainee —** June 2026
- **Emory University —** Data Analytics (SQL, Python, Excel, Tableau) — September 2025
- **Charlotte Technical College —** American Culinary Federation Certification — May 2015
- **Western Illinois University —** B.S., Law Enforcement & Justice Administration — Dec 1996

CERTIFICATIONS & TRAINING

- **CompTIA Security+ Certification** *May 2026*
- **Cyber Security Governance, Risk, and Compliance (GRC) Mastery** *August 2026*
- **ISO/IEC 27001 Lead Auditor** *August 2026*
- **Security Analyst Level 1 (SAL1) Certification** *In Progress*

TECHNICAL SKILLS

Security Operations (SOC): SOC Monitoring, SIEM & Log Analysis, Alert Triage, Incident Detection & Response, Threat Hunting & Intelligence, Vulnerability Assessment & Scanning, MITRE ATT&CK
GRC (Governance, Risk & Compliance): Risk Assessments & Registers, Risk Treatment Plans, Third-Party/Vendor Risk (TPRM), Security Control Assessments & Gap Analysis, ITGC, Policy Development, Compliance Monitoring, Audit Support, BC/DR
Frameworks & Standards: NIST CSF/SP 800-53/RMF, ISO/IEC 27001, CIS Controls, OWASP Top 10, MITRE ATT&CK, Zero Trust, CVSS, CIA Triad
Identity & Network Security: IAM, RBAC, Least Privilege, MFA, SSO, PAM, TCP/IP, DNS, DHCP, VPN, Firewalls, IDS/IPS, Endpoint Security, DDoS Mitigation
Tools: Splunk, Nessus, OpenVAS, Nmap, Burp Suite, Metasploit, Wireshark, Wapiti, Nikto, Shodan, DNSdumpster, Microsoft Defender, Kali Linux
Cloud, Systems & Data: AWS (EC2, IAM, Security Groups), Windows, macOS, Linux, Active Directory, Microsoft 365, SQL, Python, Excel, Tableau

CYBERSECURITY PROJECT EXPERIENCE *(additional projects available at MLD713.com)*

GRC Mastery Capstone: Enterprise Cybersecurity Program Design & Gap Assessment

- Conducted a full-scope NIST CSF gap assessment across 98 controls spanning Identify, Protect, Detect, Respond, and Recover, uncovering critical deficiencies in identity & access management, vulnerability management, and detection/incident response capability.
- Built a prioritized 3-year cybersecurity uplift roadmap and governance restructuring plan, translating findings into risk-ranked recommendations for executive stakeholders.
- Frameworks & techniques: NIST CSF, gap analysis, risk registers, GRC reporting.

Springboard Cybersecurity Trainee – Projects:

Completed 380+ hours of hands-on training in security operations, GRC, vulnerability assessment, incident response, network security, and penetration testing through 50+ technical labs and 35+ in-depth projects, each completed under 1:1 industry-expert mentorship.

- ***Cybersecurity Penetration Testing Capstone — Artemis Gas, Inc.***
  - Led a full-cycle black-box penetration test covering reconnaissance, scanning, vulnerability analysis, and threat assessment to evaluate the organization's external attack surface.
  - Identified multiple critical and high-risk vulnerabilities — including exposed RDP, SQL injection, default credentials, and cloud misconfigurations — and delivered prioritized, risk-ranked remediation guidance to reduce likelihood of compromise and data breach.
- ***Merging Cybersecurity Infrastructures During a Global Hotel Chain Acquisition***
  - Built a GRC-driven security integration strategy for a global hotel chain acquisition — asset discovery, SIEM consolidation, IAM, risk assessment, and policy harmonization.

PROFESSIONAL EXPERIENCE

Sous Chef

- Managed high-pressure operations and supervised staff. Forging leadership and attention to detail relevant to SOC work.

Production Assistant / Technical Director

- Coordinated production systems and troubleshot issues under deadlines. Comparable to multi-alert SOC monitoring.

Police Officer

- Conducted investigations and wrote detailed incident reports. Analytical and documentation skills transferable to compliance reporting.