Mike DiDomenico

(706)586-9183 | MLD713@iCloud.com | linkedin.com/in/mld713 | MLDiDomenico.com

Highly organized and analytical professional transitioning into cybersecurity, with experience across law enforcement, media production, culinary, and leadership roles. Calm under pressure and strong in critical thinking and problem solving, with a unique blend of technical skill, operational experience, and human-centered problem solving to support secure, data-driven decision making. Driven to pursue cybersecurity to protect sensitive data, safeguard organizations from evolving threats, and help ensure the safety and trust of consumers in an increasingly digital world.

TECHNICAL SKILLS

Network security, Endpoint security, SIEM tools (e.g., Splunk), Log analysis, Threat detection and analysis, Vulnerability assessment, Penetration testing, Incident response, Digital forensics, Identity and Access Management (IAM), Multi-factor authentication (MFA), Access control models (RBAC, ABAC), Encryption and cryptography (AES, RSA, hashing), Public Key Infrastructure (PKI), Firewall configuration, Intrusion Detection/Prevention Systems (IDS/IPS), Security frameworks (NIST, ISO 27001), Risk management, Security auditing, Cloud security fundamentals, Secure network architecture, Malware analysis, Wireshark, TCP/IP networking, Linux/Windows security administration, Microsoft Excel, SQL, AWS Glue, Tableau Public, Python, Jupyter Notebooks, Generative AI applications.

TECHNICAL PROJECTS

Physical Penetration Testing Case Analysis – Coalfire Courthouse Incident

- **Overview:** Conducted an in-depth analysis of a real-world physical penetration testing incident involving the Coalfire Iowa courthouse case, evaluating rules of engagement, legal authority conflicts, and communication breakdowns between state and local agencies.
- **Outcome**: Identified critical gaps in authorization clarity, law enforcement coordination, and contract language, providing actionable recommendations to reduce legal risk and improve future penetration testing engagements.
- **Technical Skills & Tools:** Penetration testing methodologies, physical security assessment, risk analysis, rules of engagement (ROE) evaluation, legal/compliance awareness, threat modeling, security policy analysis, incident analysis.

Cybersecurity Penetration Testing Capstone – Artemis Gas, Inc.

- **Overview:** Conducted a full-cycle black-box penetration test on Artemis Gas, Inc., performing reconnaissance, scanning, vulnerability analysis, and threat assessment to evaluate the organization's external attack surface and security posture.
- **Outcome:** Identified multiple critical and high-risk vulnerabilities (e.g., exposed RDP, SQL injection, default credentials, cloud misconfigurations) and delivered prioritized remediation strategies to reduce risk of system compromise, data breaches, and operational disruption.
- **Technical Skills & Tools:** OSINT, network scanning, vulnerability assessment, web application testing, threat modeling, CVSS risk scoring; nmap, Nessus, OpenVAS, Burp Suite, Nikto, Wapiti, Metasploit, Shodan, DNSdumpster.

RECENT WORK EXPERIENCE – Sous Chef

- Managed high-pressure operations, prioritizing tasks and resolving issues quickly, demonstrating strong problem-solving and an incident response mindset. Trained staff and enforced strict standards, showcasing leadership, attention to detail, and a security-first mindset.

EDUCATION

CompTIA Security + Certification	*May 2026*
*Emory University	Data Analytics Certification*	*September 2025*
Charlotte Technical College, American Culinary Federation Certification	*May 2015*
Western Illinois University, B.S. in Law Enforcement & Justice Administration	*December 1996*