Bryan Mooney

38 Willett Street • Albany, NY 12210 • bryan@bryanmooney.io • 518-461-9309

Experience

Offensive Security Leader / Delivery & Operations

Leet Cyber Security

Progressed from intern to senior leadership role over 8 years, spanning hands-on offensive security, technical coordination, and company operations.

Key Contributions

- Conducted and led penetration testing, red team and purple team engagements for organizations ranging from SMBs to regulated enterprises.
- Evaluated and challenged EDR, SIEM, and security tooling by actively attempting to bypass them.
- Coordinated and mentored technical staff, standardizing methodologies, and delivery quality.
- Served as primary technical authority for complex engagements and client advisory.
- Oversaw delivery operations, project execution, and internal systems as part of executive leadership.
- Bridged offensive findings to business risk, remediation strategy, and executive decision-making.
- Served as a trusted technical advisor during SOC2, HIPAA, PCI DSS, ISO 27001 and GDPR security efforts.
- Served as a pre-sales technical advisor, shaping service offerings and scoping engagements to ensure technical feasibility, realistic timelines, and defensible security outcomes.

Leadership & Systems Impact

- Served as COO with direct responsibility for delivery execution, project coordination, and technical quality.
- Consistently improved methodology and tooling through threat-intel-backed research and client feedback, shaping service offerings to focus on practical security outcomes.
- Influenced firm direction by grounding strategic decisions in firsthand offensive security experience, delivery capacity, and real-world risk.

Selected Initiatives

- *Security Tool Validation*
  Validated client security investments by actively testing EDR, network detection, and alerting pipelines during real attack simulations, identifying blind spots and false confidence.
- *R&D Architect*
  Led R&D architecture, creating automations ranging from proprietary pentesting tooling to operations and sales automations.
- *AI Implementation*
  Developed and delivered AI training in acceptable use and practical workflows for each department. Improved technical execution with AI, reducing data analysis and report writing by 40%.

Skills

Offensive Security: Penetration Testing, Red Team Operations, Vulnerability Assessment & Management, Adversary TTP Knowledge (MITRE ATT&CK)

Endpoint & Fleet Security: macOS Fleet Management, EDR Deployment & Management, Endpoint Hardening

Cloud & Identity: Microsoft Azure/Azure AD, IAM Frameworks, SAML, OAuth, SCIM

Email Security: SPF, DKIM, DMARC, tools such as Barracuda and Proofpoint, Security Awareness Training and Social Engineering engagements

SaaS Hardening: Google Workspace, GitHub, Zero Trust Architecture (Cloudflare and Zscaler), Secure by Default Design

Data Protection: DLP Controls, Intelligent Groups Management, Data Classification

Automation & Scripting: Bash, Python, Offensive Tooling Automation, AI/LLM Integration, RAG Application Deployment

Frameworks & Compliance: NIST 800-53, NIST CSF, CISA KEV, NVD, HIPAA, SOC2, PCI-DSS, GDPR, ISO 27001

Community Involvement

Mentor – Big Brothers Big Sisters of the Capital Region

- Nominated for Match of the Year as a mentor