ANTHONY MENDONCA

LinkedIn | GitHub | Blog

Technical cybersecurity professional with experience across threat detection, security engineering, risk management and malware development. Seeking hands-on, multidisciplinary, security engineering roles with a focus on detection engineering, threat intelligence and offensive security.

Skills

- **Languages**: Python, Golang, SQL
- **Application Security**: OWASP Top 10, OAuth, Authc Defense, Authz Defense
- **Security Skills**: Threat Modelling, SAST, DAST, SCA, DevSecOps, CTI
- **Security Tools**: Nmap, BloodHound, Mythic C2, GitHub Actions, Seatbelt

Professional Experience

Senior Consultant, Cyber

Booz Allen Hamilton **(Jan 2023 - Present)**

Security Engineering & Threat Detection

- Led a major enhancement of global retail client's detection engineering and SIEM effectiveness by tuning existing Microsoft Sentinel rules, improving signal fidelity, and developing new high-value detection logic targeting Active Directory, service class OS, VPNs, firewalls and other network anomalies
- Built and optimized 30+ KQL-based detection rules in Microsoft Sentinel using CTI-driven IOCs, reducing false positives and improving detection rule fidelity.
- Developed 13 high-priority use cases for ransomware, data exfiltration, and cryptomining; mapped to MITRE ATT&CK and prioritized based on client's threat landscape.
- Delivered a CISO-facing detection strategy and roadmap that mapped log source gaps to business risks and defined Priority Intelligence Requirements (PIRs) aligned to the client's threat landscape.

Cyber Fusion & Incident Response

- Led redesign of a global Cyber Fusion Centre, aligning team roles with CISO strategy and operational needs.
- Authored 5 incident response playbooks covering ransomware, insider threat, phishing, and malware enabling structured response processes and faster containment.

Cyber Risk

- Led a cyber capability maturity assessment for a global online travel client, identifying critical risks across people, process, and technology; delivered tailored threat landscape, gap analysis, and prioritized roadmap reports that enabled executive alignment and sequenced remediation initiatives based on risk appetite.
- Designed and implemented a security effectiveness program for a global electronics client, elevating posture by 25% through development of strategic metrics and governance, enabling leadership to track residual risk and validate effectiveness of compensating controls against NIST CSF.

Cyber Risk Consultant

Deloitte **(Sept 2021 - Jan 2023)**

- Designed secure network architectures and implemented Zero Trust strategies across multiple clients, reducing attack surface and enhancing compliance.
- Automated ransomware server hardening using PowerShell and Chef, aligning with CIS benchmarks.
- Performed adversary-focused threat analysis using MITRE ATT&CK, developing TTP heatmaps to prioritize cybersecurity control investments.

Certifications

GIAC Penetration Tester (GPEN): Oct 2025 - Oct 2029
GIAC Security Operations Certified (GSOC): Nov 2024 - Nov 2028
GIAC Web Application Defender (GWEB): Jun 2024 - Jun 2028
COMPTIA Security+: Mar 2021 - Mar 2027
Certified DevSecOps Professional
INSEAD Mastering Creative Thinking

Projects

DataDog - Stratus Red Team | Golang, Dockerfile

Open-source contributions to DataDog's Stratus Red Team project:

- Developed MITRE ATT&CK coverage matrix and featured in March 2025's DataDog Security Digest
- Improving Makefile for better maintainability

Deep Learning for Network Intrusion Detection | Python, PyTorch, Google Colab

MSc. Thesis project:

- Created a network intrusion detection classifier that discerned between malicious and normal network traffic
- Done with an emphasis on deep learning using Recurrent Neural Networks and Multilayer Perceptrons

DeepPhishing | Python, Keras, Google Colab

Investigated the use of Recurrent Neural Networks in detecting malicious domains:

- Developed a Long Short-term Memory (LSTM) model to detect and classify malicious (from PhishTank database) and benign domains (from Cisco Umbrella 1 million)

Education

MSc. Applied Cyber Security at Queen's University Belfast (Sept 2018 - Jun 2020)
BSc. Computer Science at University of Nairobi (May 2013 - Sept 2017)