Anthony Mendonca

linkedin.com/in/anthony-mendonca/ | github.com/tmendonca28 | anthonymendonca.me

Technical security professional interested in security engineering, cyber defense & threat hunting

EXPERIENCE

Senior Cybersecurity Consultant

Jan 2023 - Present

Booz Allen Hamilton London, UK

- Threat detection and response uplift for global logistics client:
  - Led incident response for L3 escalations from the client's MSSP, coordinating technical analysis, containment, and recovery efforts.
  - Developed and optimised KQL-based threat detection queries in Microsoft Defender, leveraging IOCs from the CTI team to enhance detection accuracy and reduce false positives.
  - Created detailed mini-playbooks for IOC tracking, outlining roles and responsibilities for CTI and TDR teams to streamline threat response workflows.
- Threat detection uplift for European online retail and fashion client:
  - Enhanced threat detection through the development of 13 targeted SOC use cases covering scenarios such as ransomware, cryptomining, and data exfiltration.
  - Developed adversary-focused threat analysis using the MITRE ATT&CK framework, by building customised TTP heatmaps to prioritise control areas specific to the company's threat landscape.
- Cyber Fusion Centre design and implementation for global shipping and transportation company:
  - Improved security operations efficiency by redesigning roles and responsibilities, aligning with CISO strategy, and addressing existing structural gaps.
  - Developed 5 Incident Response playbooks to be used in scenarios ranging from ransomware and phishing to insider threat.
- Information security effectiveness program development for global electrical engineering and electronics client:
  - Elevated security posture by 25% through the implementation of strategic security metrics covering SOC, CTI and Attack Surface Management (ASM) and a robust governance strategy.
- Red teaming for European e-commerce client:
  - Identified potential phishing targets with 95% success rate using passive reconnaissance tools (theHarvester) during a red teaming engagement.
- Security metrics programme development for global top 5 FMCG:
  - Established a robust security metrics program, enhancing data-driven reporting and analysis, aligned with NIST CSF.

Cyber Risk Consultant

Sep 2021 - Jan 2023

Deloitte London, UK

- Secure network design for a Swiss luxury watch maker:
  - Deployed network segmentation and firewall hardening strategies, leveraging tools like AlgoSec and Cisco ASA to reduce external attack surface by 30%, ensuring compliance with NIST and CIS benchmarks.
  - Conducted adversary-focused threat analysis using the MITRE ATT&CK framework, by building customised TTP heatmaps to identify high-risk areas specific to the company's threat landscape.
- Ransomware server hardening for a global consulting services client:
  - Automated CIS benchmark-aligned configurations using PowerShell scripts and Chef recipes.
- Next generation secure network strategy implementation roadmap for a multinational consulting services client:
  - Developed adoption strategies for Zero Trust by implementing identity-based segmentation, multi-factor authentication, and secure cloud gateways, ensuring end-to-end encryption and least-privilege access across multiple environments.

Cyber Security Intern

Sep 2019 - Jun 2020

British Telecommunications Group Ipswich, UK

- Developed a neural network model that increases the proactive detection of malicious domains by 70%.
- Developed Splunk queries and dashboards to determine root cause analysis of device misconfigurations leading to 75% increase in turnaround time.
- Built automation tools related to detecting secrets exposed on GitHub and DNS hygiene increasing BT's security posture by 80%.
- Developed threat intelligence queries on Microsoft ATP platform using KQL to detect Privilege Escalation.

TECHNICAL SKILLS

Languages: Python, Golang, SQL, JavaScript
Cloud & Deployment: GCP, AWS, Docker, Kubernetes, Chef
Application Security: OWASP Top 10, OAuth, Authc Defense, Authz Defense
Security Skills: Penetration Testing, Threat Modelling, Web Application Firewalls, Reverse Proxies, SAST, DAST, SCA
Security Tools: Wireshark, MISP, Nmap, Burp Suite, TheHive, theHarvester, KQL

PROJECTS

DataDog - Stratus Red Team | *Golang, Dockerfile*

- Open-source contributions by:
  - Improving Makefile for better maintainability.

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

- 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, Numpy, Pandas, Google Colab*

- 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

Queen's University Belfast Belfast, UK

MSc. Applied Cyber Security *Sep 2018 - Jun 2020*

University of Nairobi Nairobi, Kenya

BSc. Computer Science *May 2013 - Sep 2017*

CERTIFICATIONS

GIAC Security Operations (GSOC): Nov 2024 - Nov 2028
GIAC Certified Web Application Defender (GWEB): Jun 2024 - Jun 2028
COMPTIA Security+: Mar 2021 - Mar 2027
GCP Associate Cloud Engineer: Apr 2022 - Apr 2025
Certified DevSecOps Professional