Anthony Mendonca

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

Technical security consultant interested in application security engineering & threat hunting

EXPERIENCE

Senior Cybersecurity Consultant

Jan 2023 - Present

Booz Allen Hamilton London, UK

- Threat detection uplift for European online retail and fashion client: Enhanced threat detection through the development of 13 targeted SOC use cases such as ransomware, cryptomining, and data exfiltration by assessing existing security tooling and using MITRE ATT&CK heatmaps.
- Cyber Fusion Centre design for global shipping and transportation company: Improved security operations efficiency by 60% 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. Developed 25+ threat hunting queries in KQL for the proactive discovery of threats across their environment with a focus on Initial Access, Execution and Data Exfiltration.
- Information security effectiveness program development for global electrical engineering and electronics client: Elevated security posture by 25% through the implementation of strategic security metrics 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

- Developed a secure network design for a Swiss luxury watch maker. This involves implementing network security best practices, conducting threat analysis using the MITRE ATT&CK framework and ultimately building out a network security strategy.
- Developed technical implementation guidance with relation to ransomware server hardening for a global consulting services client. Done using PowerShell scripts and Chef recipes.
- Developed a next generation secure network strategy implementation roadmap that would underpin the global network security transformation for a multinational consulting services client. This included adoption strategies for Secure Access Service Edge and Zero Trust.
- Developed low-level system implementation guidance to improve the current security posture for a national scientific research client. This was a post-vulnerability assessment activity and improved the organisation's security posture by 75%.

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, 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

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

- For my Master's thesis, I worked on creating 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): In progress
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