ANGELIKA WANCOWICZ

Software Engineer

☎ +44 7817 905 492 ✉ angelikamwancowicz@gmail.com 📍 London, UK

ABOUT ME

Cybersecurity-focused Software Engineer with SOC and threat intelligence experience at *BAE Systems*, where I monitored and analysed cyber threats, mapped TTPs to the MITRE ATT&CK framework, and automated analysis workflows using Python. I hold a **BSc(Hons)** in *Computing (Networking, Security & Forensics)* and have applied my skills to build secure full-stack systems, threat classification tools, and AI-driven automation pipelines. Experienced in Python, Django, PostgreSQL, AWS, and secure coding practices, I am committed to continuous learning and developing my professional skills.

SKILLS

Languages & Frameworks: Python, Django, SQL, JavaScript, React JS, jQuery, HTML/CSS, Flask, ElasticSearch, Pandas, NumPy, SciPy.

Databases: PostgreSQL, MongoDB, MySQL.

OS & Platforms: Linux, Git, Bash, Splunk, AWS, Convert (A/B testing), SIEM.

Cyber Security: MITRE ATT&CK, IOC analysis, basic pen testing (Nmap, Burp Suite).

Certifications: MTA: Security Fundamentals

PROFESSIONAL EXPERIENCE

Software Developer

Cosmetify, London July 2024 - January 2026

- Developed and maintained features for an e-commerce platform using Python, Django, PostgreSQL, and JavaScript/jQuery, enhancing core site functionality and reliability.
- Designed and optimised PostgreSQL schemas, improving query efficiency and ensuring data integrity.
- Implemented an automated invoice and payment system, eliminating manual reconciliation and reducing processing time by 70%.
- Built an AI-driven product companion system, generating complementary product suggestions using Python, Django, and LLM models, increasing average order value by 15%.
- Developed a sales reporting platform using Python and Pandas to aggregate, clean, and analyse large datasets and generate sales reports.
- Created an AI chatbot using Kommunicate: Implemented conversational flows, custom intents, and backend logic to ensure accurate and context-aware interactions on a per-order basis.

Software Engineer/Threat Intelligence Analyst

BAE Systems, Remote September 2021 - May 2024

- Developed and deployed machine learning models in Python to automate data classification tasks, reducing manual analysis time by 45% and increasing accuracy by 30%.
- Maintained and implemented backend and frontend code for a threat intelligence platform using React JS, Django, Flask, and MongoDB.

- Designed automation scripts that reduced repetitive engineering tasks (e.g., log parsing, reporting) by 60%, saving approximately 15+ hours/week across the team.
- Led code reviews and mentored one junior developer, resulting in improved code quality and faster onboarding.
- Monitored and analysed real-time cyber threat intelligence feeds, identifying and flagging high-risk activity early, contributing to a 20% reduction in incident response time.
- Monitored and analysed cyber threats using Splunk to identify risks and vulnerabilities, providing actionable insights to enhance organizational security.
- Conducted in-depth research on threat intelligence data, mapping attacks and techniques to the MITRE ATT&CK framework to assess potential impacts and recommend proactive mitigation measures.
- Collaborated with cyber-security teams to design and implement threat detection and incident response strategies, safeguarding sensitive data and systems.
- Produced comprehensive reports and presentations on emerging cyber threats and IOCs.

EDUCATION

Edge Hill University September 2018 - August 2021

BSC(Hons) Computing (Networking, Security & Forensics)

First-class degree.

Our Lady’s Convent High School September 2016 - August 2018

A Levels

NOTABLE PERSONAL PROJECTS

Book Reservation and E-Commerce Platform

Built a full-stack online platform from scratch using Python and Django, featuring RESTful API design, a responsive frontend built with HTML, CSS, and JavaScript, and third-party API integrations including geolocation services. Designed and managed a PostgreSQL database schema and implemented a role-based access control system. Applied security best practices such as CSRF protection, input sanitisation, and secure authentication.

URL Threat Classifier

Python program using a Random Forest classifier to detect malicious vs. benign URLs, achieving 80%+ accuracy on test data, using Pandas and NumPy for data cleaning and preprocessing, and Matplotlib to visualise data patterns and model results.