Ucheoma Okoma

California, USA
909-925-7235
ucheoma.okoma@cgu.edu
Personal Portfolio

Security Engineer I

PROFESSIONALSUMMARY

Passionate Information SecurityEngineer with expertise in AI privacy, threat management, and cloud/IoT security. Experienced in incidentresponse, digital forensics, and CTI-driven investigations, with strong skills in documenting findings and collaborating across teams. Skilled in applying cyber kill chains, OSINT, and frameworks like NIST CSF, ISO27001, and MITRE ATT&CK to guide detection engineering and secure solution design. Recognized for clearcommunication, effective teamwork, and continuous learning through certifications, CTFs, and conferences.

PROJECTS

AI Privacy-Aware Chatbot | Python, Fast API, Tkinter, OpenRouter (Claude)

- Built a local AI chatbot with sensitive-data redaction (paths, hashes, emails, passwords) achieving 85%
- accuracy in lab testing, while maintaining full functionality and compliance-ready workflows. Implemented anonymous logging (session IDs, timestamps, redacted data) for admin use only, projected to boost user trust/adoption by ~75%.

TryHackMe – Personal Labs (Ongoing) | Burp Suite, OWASP ZAP, Metasploit

- Completed the Junior Penetration Tester path, exploiting OWASP Top 10 vulnerabilities and building
- threat models with the OWASP Risk Rating methodology, achieving 99.99% flaw detection in lab tasks. Integrated OWASP ZAP into a CI/CD pipeline for automated vulnerability testing, reducing manual effort by ~40%.

IoT Security with AWS & Suricata | AWS IoT Core, EC2, Suricata, Filebeat, Kibana

- Designed and monitored an IoT network with AWS IoT Core and EC2, streaming MQTT sensor data into
- Kibana dashboards and enabling real-time threat monitoring. Deployed Suricata IDS with custom detection rules and integrated Filebeat pipelines, reducing false positives by ~50% and strengthening incident response.

SKILLSSUMMARY

- **Cybersecurity Solutions**: IAM, EDR, SIEM, DLP, AppSec (OWASP Top 10)
- **Cloud & Infrastructure**: AWS (IoT, EC2, S3, Cloud Security), Azure (basic), Docker
- **Systems & Networking**: Linux, Windows Server, IDS/IPS, Firewalls, VPN, TCP/IP, DNS
- **Tools**: Suricata, ELK Stack, Snort, Nmap, Wireshark, Metasploit, Volatility, FTK Imager, Git
- **DevOps & Automation**: CI/CD pipelines, Bash scripting, Terraform (intro)
- **Programming**: Python, SQL, JavaScript, Java, PowerShell
- **Frameworks & Standards**: NIST CSF, ISO/IEC 27001, MITRE ATT&CK, SAST/DAST.

EDUCATION

MS. Information Systems & Technology, ClaremontGraduateUniversityCA,USA May 2027
Concentration in Cybersecurity

Post-Graduate Certificate | Seneca College | ON, CA August 2025
Concentration in Cybersecurity & Threat Management

CERTIFICATIONS

- CompTIA Security+
- AWS Certified Cloud Practitioner
- AWS Academy Cloud Security Foundations
- TryHackMe Junior Penetration Tester