UCHEOMA OKOMA

Cybersecurity | Information Security | CA, USA | ucheoma.okoma@cgu.edu | Portfolio

PROFESSIONAL SUMMARY

Cybersecurity engineer with a growing focus on the intersection of AI, data, and security. Experienced in AI privacy, threat management, and cloud/IoT monitoring, with hands-on work in building privacy-aware chatbots and performing adversarial testing. Background in data analytics using Spark, Hadoop, and MapReduce, enabling the ability to analyze and secure large datasets. Skilled in applying secure coding and threat-modeling principles (STRIDE, OWASP Top 10) to system design and documentation. Naturally curious, research-driven, and always ready and willing to learn emerging methods in AI/ML security and responsible AI practices.

EDUCATION

Claremont Graduate University | CA, USA — Expected May 2027
M.S. Information Systems & Technology (Cybersecurity Concentration),

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

Certifications:
CompTIA Security+ | AWS Certified Cloud Practitioner | AWS Academy Cloud Security Foundations | TryHackMe Junior Penetration Tester

SELECTED PROJECTS

AI Privacy-Aware Chatbot | Python · FastAPI · Tkinter · OpenRouter (Claude)

- Developed a local AI chatbot with built-in sensitive data redaction to prevent prompt-injection and data-leakage risks.
- Implemented anonymous session logging for privacy-compliant analysis, improving user-trust metrics by ~75%.
- Documented security controls and ethical considerations following NIST AI RMF guidelines.

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

- Designed and monitored an IoT network streaming MQTT sensor data into Kibana dashboards for real-time threat analysis.
- Deployed Suricata IDS with custom rules and Filebeat pipelines, reducing false positives by ~50% and enhancing incident response.
- Structured logging and data flows with cloud security principles to support future AI-driven analytics integration.

TryHackMe Labs (Ongoing) | Burp Suite · OWASP ZAP · Metasploit

- Completed the Junior Penetration Tester path, exploiting OWASP Top 10 vulnerabilities and documenting remediation steps.
- Integrated OWASP ZAP into a CI/CD pipeline to automate vulnerability testing, reducing manual effort by ~40%.
- Applied AI red-teaming concepts to test data leakage and injection-style threats in interactive systems.

RELEVANT COURSEWORK & RESEARCH

- Data Analytics & Big Data Systems – developed distributed data pipelines using Spark, Hadoop, and MapReduce.
- Threat Modeling & Secure Coding – Applied STRIDE and OWASP Top 10 principles to design resilient applications.
- Cybersecurity Operations & Defense – hands-on training in SIEM monitoring, incident response, and forensics.

TECHNICAL SKILLS

- Programming & Data: Python, SQL, Java, JavaScript, PowerShell, Bash | Spark, Hadoop, MapReduce
  Cybersecurity Tools: Nmap, Wireshark, Metasploit, Snort, Suricata, ELK Stack, Volatility, FTK Imager, Burp Suite, OWASP ZAP
- Cloud & Infrastructure: AWS (IoT, EC2, S3, Cloud Security), Azure (basic), Docker, Terraform (intro)
  DevOps & Automation: Git, CI/CD Pipelines, Bash Scripting
- Frameworks & Standards: NIST AI RMF, Google SAIF, NIST CSF, ISO 27001, MITRE ATT&CK;, OWASP Top 10