UCHEOMA OKOMA

Cybersecurity | CA, USA | okomaucheoma404@gmail.com | Portfolio

PROFESSIONAL SUMMARY

Cybersecurity engineer-in-training with hands-on experience designing and testing secure cloud and network solutions. Skilled in Python, Java, and Terraform for building, automating, and documenting security configurations across AWS, Docker, and Jenkins environments. Adept at applying threat-modeling (STRIDE, OWASP Top 10), cryptography, and incident response techniques to strengthen data integrity and business continuity. Analytical, detail-oriented, and motivated to learn emerging security technologies.

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 Cloud Practitioner | AWS Cloud Security Foundations | TryHackMe Junior Penetration Tester

SELECTED PROJECTS

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

- Designed and deployed a cloud-based IoT monitoring environment with Suricata IDS and Filebeat pipelines for real-time threat detection.
- Tested and tuned rule sets to reduce false positives by ≈50 % and improve incident response.
- Documented network segmentation, IAM roles, and data-flow diagrams following cloud security best practices.

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

- Built a local chatbot with data-redaction and authentication mechanisms to prevent prompt-injection and data-leakage risks.
- Implemented audit logging and encryption for privacy-compliant session tracking aligned with NIST AI RMF guidelines.

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

- Cybersecurity Operations & Defense – SIEM monitoring, incident response, forensics
- Threat Modeling & Secure Coding – STRIDE framework, OWASP Top 10
- Cloud Security Fundamentals – AWS and Azure architecture controls
- Data Analytics & Big Data Systems – Spark, Hadoop, MapReduce for security data analysis

TECHNICAL SKILLS

- Programming: Python | Java | SQL | .NET (basic)
- Infrastructure & Cloud: Terraform | Docker | Kubernetes | Jenkins | AWS (IoT, EC2, S3) | Azure (basic)
- Cybersecurity: SIEM (ELK/Wazuh) | SOAR (concept) | EDR | Suricata | Snort | Wireshark | Nmap | Metasploit | OWASP ZAP
- Frameworks & Standards: NIST CSF | ISO 27001 | MITRE ATT&CK | OWASP Top 10
- Other: PowerShell | Bash | Git | CI/CD | Microsoft Office (Word, Excel, PowerPoint)

ADDITIONAL HIGHLIGHTS

- Strong analytical and problem-solving skills with high attention to detail.
- Active learner with a solutions-oriented mindset and passion for secure innovation.