OREOLUWA ADEBAYO

616-426-1159 | oadebayo1@hawk.illinoistech.edu | LinkedIn | github.com/0reAde

EDUCATION

- **Illinois Institute of Technology** — M.S. Computer Science, Cybersecurity, Chicago, IL | December 2026
- **Calvin University** — B.S. Engineering, Chemical Engineering, Grand Rapids, MI | May 2021

SECURITY PROJECTS

ML-Based Network Intrusion Detection | Python, scikit-learn, XGBoost, pandas | github.com/0reAde/IDS-Network-Analyzer

- Built an intrusion detection pipeline on 6.3M real network flows from CSE-CIC-IDS2018, a public benchmark of 13 attack types
- Caught a model that scored perfectly in testing but missed 52K+ DoS attacks from a day of traffic it had not seen
- Retrained it to detect all 13 attack types while limiting false alarms, scoring 0.84 macro F1 (1.0 = perfect)
- Ran leakage checks to confirm the model learned attack behavior, not shortcuts, and projected daily alert load to test SOC viability

Job Application Tracker on AWS | Terraform, AWS, Docker, PostgreSQL, GitHub Actions | *In progress*

- Building a three-tier app (CloudFront → ALB → ECS Fargate → Aurora PostgreSQL) as dev and prod from shared Terraform modules
- Users sign in via Cognito, track applications in Postgres, and upload resumes to private S3 through presigned URLs
- Isolating app and database tiers in private subnets across 2 AZs, behind WAF and a CloudFront-only load balancer
- Automating deployments with temporary, auto-expiring AWS credentials (OIDC) instead of stored keys, plus Checkov security scans
- Monitoring with CloudWatch alarms and dashboards, auditing with CloudTrail and Macie, and tracking cost with Infracost

Isolated Cyber Range & Passive Reconnaissance | VirtualBox, Kali Linux, Bash

- Deployed a segmented 4-VM attack lab (Kali; Metasploitable3 and Windows Server 2016 targets) isolated from outside networks
- Mapped 5 Windows security controls (Defender, firewall, IE ESC, DEP, updates) to the attack techniques each one stops
- Enumerated subdomains and org metadata through passive OSINT (CT logs, WHOIS, Shodan) with zero contact to targets

Program Analysis Tooling | Java, Python, Soot, angr, Slither | 2-person team

- Built an Android static analyzer (Soot) that flags apps calling sensitive APIs, checked against 32,000+ permission mappings
- Used angr symbolic execution to automatically find the inputs that make a compiled program reach a chosen line of code
- Built a Slither tool that maps data dependencies in Solidity smart contracts to trace how state flows through a multi-signature wallet

PROFESSIONAL EXPERIENCE

INEOS Styrolution — Process Engineer, Channahon, IL | Jan 2023 – Jul 2024

- Led a dust-collection project that solved a 20-year plant issue, reducing fines by 75% and increasing usable production
- Traced defects to root cause with R&D for major brands including Gillette, cutting complaints from every delivery to 1 in 4–5
- Defined operating envelopes and safety-critical DCS alarms, setting the thresholds that flagged deviation from normal operation

Armstrong Flooring — Process Engineer, Kankakee, IL | Jul 2021 – Jan 2023

- Led plant-side commercialization of a new American hardwood wall tile, which became the company's second-best seller
- Owned process control for plant line operations, leading projects to improve yield, uptime, and OEE
- Traced recurring line shutdowns to a wrap roll setting, eliminating unplanned stops and raising line performance ~25%

CERTIFICATIONS

- **AWS Certified Solutions Architect – Associate** — August 2026
- **CompTIA Security+** — August 2025
- **AWS Certified Solutions Architect – Professional** — *in progress*
- **AWS Academy Graduate** — Cloud Foundations; Cloud Security Foundations

TECHNICAL SKILLS

- **Networking:** TCP/IP, DNS, DHCP, NAT, VLANs, firewalls, 802.11 Wi-Fi, QoS, SIP/VoIP
- **Network Recon & Traffic Analysis:** Nmap, hping3, theHarvester, Maltego, Shodan, Wireshark, tcpdump, Zeek, Scapy, iperf3
- **Offensive & Vulnerability Tools:** Metasploit, Nessus, OpenVAS, Hashcat; vulnerability assessment
- **Security Frameworks:** MITRE ATT&CK, NIST RMF, ISO 27001, eMASS
- **Data Privacy:** k-anonymity, l-diversity, t-closeness, differential privacy (central and local), differentially private ML
- **Security Engineering:** Static and symbolic program analysis, applied cryptography (OpenSSL)
- **Cloud Security & Monitoring:** CloudTrail, CloudWatch, Macie, security groups, bucket policies, VPC routing and segmentation
- **Cloud, Virtualization & Infrastructure:** AWS, Terraform, Docker, Linux, Windows Server, VirtualBox, KVM, Hyper-V, FABRIC, Chameleon Cloud
- **Languages & Libraries:** Python, Java, C, Bash, SQL, HCL, Node.js, REST APIs; scikit-learn, XGBoost, pandas, Soot, angr, Slither, Git

LEADERSHIP

- **National Society of Leaders** | Jan 2026 – Present — Invite-only society, a program that recognizes excellence in a designated field
- **Cyber Hawks, Illinois Institute of Technology** — Executive Board Member | 2025 – Present — Illinois Tech's cybersecurity student organization, providing hands-on cybersecurity experience through seminars, workshops, competitions and CTFs, and project teams