

Faith O. Olajide

Hagerstown, MD, 21742 | 240-469-0970 | faitholajide1@gmail.com

Skills/Certifications

Technical Skills: Windows OS, Linux, Active Directory, TCP/IP Networking, User Account Administration, Vulnerability Scanning, Log Analysis, Incident Response Support, Network Troubleshooting

Security & Networking Tools: Wireshark, Kali Linux, Packet Tracer, Virtual Machines, Qualys Cloud Agent, Qualys Cybersecurity Asset Management (CSAM)

Programming: Python, SQL

Certifications: SOCOA 1, Qualys CA, Qualys CSAM, Google Cybersecurity Professional

Projects

BCR Cyber Range – Defensive Security Project

- Analyzed simulated network traffic and security events in a live cyber range environment to identify suspicious activity and potential threats
- Investigated cybersecurity incidents using Wireshark, Kali Linux, and SIEM platforms to support threat detection and incident response workflows
- Developed detection logic and documented findings from defensive security exercises involving network traffic analysis and threat investigation
- Performed hands-on incident analysis activities aligned with SOC operations and security monitoring practices

Network Security Internship – The Cyber Ledger

- Completed an 8-week defensive security internship focused on network monitoring, intrusion detection, and cybersecurity analysis
- Analyzed network traffic and investigated simulated threats in hands-on security lab environments
- Strengthened practical knowledge of SOC operations, threat detection, and incident response workflows
- Collaborated with mentors and peers to investigate cybersecurity scenarios and communicate technical findings

Senior Design Project – Phishing Mitigation Using Virtual Machines

- Designed and deployed a virtual machine-based phishing simulation environment to demonstrate workplace phishing attacks and cybersecurity awareness concepts
- Utilized Kali Linux and the Social Engineering Toolkit (SET) to simulate phishing campaigns and analyze attacker techniques
- Applied social engineering and malware analysis concepts to evaluate phishing behaviors and strengthen phishing mitigation strategies
- Documented security findings and developed recommendations to improve cybersecurity awareness and user education

Network Traffic & Log Analysis Labs

- Analyzed network traffic and system logs using Wireshark to identify anomalies, suspicious behavior, and potential threats in virtual lab environments
- Conducted vulnerability assessments and intrusion detection exercises using cybersecurity tools and simulated attack scenarios
- Performed incident response simulations focused on threat investigation, log analysis, and remediation tracking
- Documented technical findings and remediation recommendations to support cybersecurity best practices

Active Directory & IT Support Administration

- Supported Active Directory administration for 800+ users through account provisioning, password resets, and access management tasks
- Resolved 20–30+ technical support tickets daily involving Windows systems, applications, printers, and connectivity issues

- Troubleshoot endpoint, login, and network-related issues using root cause analysis and documentation procedures
- Maintained technical documentation and knowledge base records to improve support efficiency and issue resolution times

Education

Capitol Technology University – Laurel, MD
Bachelor of Science in Cybersecurity

January 2020–April 2024

Relevant Coursework:

Cybersecurity: Network Security, Penetration Testing, Malware Analysis & Reverse Engineering, Digital Forensics & Investigation Process

Networking & Systems: Internetworking with Routers & Switches, Secure System Administration & Operations (UNIX), Operating Systems

Programming & Data: Programming in C/C++, Secure Coding, Database Management

Experience

Capitol Technology University – Laurel, MD

May 2022 – Aug 2024

IT Help Desk Technician

- Resolved 20–30+ technical support tickets daily in a fast-paced environment, supporting Windows systems, applications, and network issues
- Administered Active Directory for 800+ users, including account provisioning, password resets, and access control
- Troubleshoot login, system, and connectivity issues, reducing repeat incidents through root cause analysis and documentation
- Monitored system activity for potential security concerns and escalated suspicious behavior following security best practices
- Documented 100+ incidents and resolutions, improving knowledge base efficiency and response times

Capitol Technology University – Laurel, MD

April 2020 – May 2022

Cybersecurity Technician

- Performed hands-on security analysis in virtual lab environments, including intrusion detection, vulnerability assessment, and threat identification
- Analyzed network traffic and system logs using Wireshark to identify anomalies and suspicious activity
- Conducted vulnerability scans using Qualys tools and supported remediation tracking
- Simulated incident response scenarios to strengthen threat detection and response capabilities
- Documented findings and supported cybersecurity awareness and risk mitigation efforts

Staples – Hagerstown, MD

Mar 2018 – Apr 2020

Service Desk Technician (Tier 1)

- Delivered Tier 1 technical support to 50+ customers per week, resolving hardware, software, and connectivity issues
- Troubleshoot POS systems, Windows/macOS devices, and peripherals, achieving high first-call resolution rates
- Escalated complex issues following SLA guidelines, ensuring timely resolution and customer satisfaction
- Maintained consistent communication with users, improving overall service experience and issue resolution transparency

Harvest Intercontinental Church—Hagerstown, MD

Jan 2018 – Present

Operations & Digital Media Systems Specialist

- Supported and maintained AV, livestream, and network systems for weekly services and events with 100+ attendees
- Troubleshoot hardware, software, and network issues in real time, ensuring minimal system downtime
- Managed digital records and technical documentation, improving system organization and operational efficiency
- Optimized workflows and system usage, enhancing overall reliability of technical operations