MARY OMOYELE
Oklahoma City, OK, 73132
580-500-7310 | maryomoyeleo@gmail.com

PROFESSIONAL SUMMARY

A U.S. Air Force Client Systems Technician with secret clearance and a cybersecurity professional with years of hands-on technical and IT Security experience, eager to learn and to contribute to the success of the team through my proven years of experience.

TECHNICAL SKILLS

- Knowledge of Risk Management Framework, NIST SP 800 series, IDS/IPS, threat analysis and network defense.
- Understanding of networking and communication protocols such as TCP/IP, SSL/TLS, UDP, IPSEC, HTTP, HTTPS, BGP and LAN/WAN Technologies.
- Strong knowledge of security code reviews, web application security vulnerabilities such as XSS, CSRF, SQL injection and OWASP top 10 and CWE/SANS Top 25 vulnerabilities.
- Experienced in using security testing tools like Burp Suite, OWASP ZAP, Nmap, Metasploit, Nessus etc.
- Experience with cloud-based security such as AWS, Azure, and Google Cloud Platform (GCP)
- Strong understanding of software development lifecycle (SDLC) from product concept to maintenance.
- Proficient in various programming languages like C++, Python, JavaScript, SQL, PHP etc.
- Strong knowledge of using tools like ConnectWise, ServiceNow, Jira, SolarWinds, Secureworks Taegis XDR.
- Strong knowledge of web applications technology such as HTML, CSS, JavaScript, jQuery etc.
- Proficient in Microsoft Windows and Office Suite, Mac OS, and Linux.
- Excellent analytical, verbal/written communication, interpersonal and multi-tasking skills.
- Detail-oriented, fast learner, ability to work independently and as part of a team.

PROFESSIONAL EXPERIENCE

Unity Technologies – Remote
Application Security Engineer, August 2021 – Present

- Performs regular application security assessments (SAST & DAST), penetration testing, and vulnerability scanning on APIs, web, and mobile applications to identify vulnerabilities and potential security threats.
- Develops and implements security policies, standards, and procedures to ensure compliance with industry standards and regulations such as PCI DSS, HIPAA and GDPR.
- Performs threat modelling to identify and resolve security vulnerabilities and provides remediation steps.
- Conducts code reviews and reports back to the cross-functional teams on how to implement appropriate secure coding practices and resolve security issues.
- Writes comprehensive reports including assessment-based findings for further security system enhancement.
- Uses Jira to create, triage and resolve security incidents tickets and Bug Bounty reports.
- Utilizes security tools like Burp Suite, Nmap, Metasploit, Nessus.
- Conducts security training sessions for developers, stakeholders, and end-users.

Dell Technologies – Remote (Contract)

Threat Detection Analyst, April 2020 – August 2021

- Used SIEM, XDR & EDR tools to perform security monitoring to identify suspicious activities and trends indicative of potential threats.
- Performed monitoring and incident response of cybersecurity events for proper determination of them being false positives or true security threats and risks.
- Monitored logs and reviewed security alerts while identifying, remediating, and escalating incidents.
- Created process documents from security tools into daily security operations.
- Customized scanning rules to reduce false positive events.
- Categorized confidential information and selects the best security controls based on information categorization.
- Implemented and evaluated selected security controls and policies to ensure information security efficacy.
- Used ServiceNow to create, document and resolve cybersecurity incident reports in a timely manner.
- Assisted in updating IT and security policies and procedures and other security documentation.
- Triaged, analyzes, and documents cybersecurity incidents and escalates when necessary.
- Performed installation, configuration, and maintenance of antivirus software on all necessary devices.

Paycom - Oklahoma City, OK
Computer Operator, September 2018 – April 2020

- Utilized job scheduling software to monitor, evaluate critical workflow process, and notify appropriate personnel if any issues are determined.
- Reported, assisted, and documented all issues to the appropriate departmental personnel.
- Monitored database jobs and systems for outages and evaluated critical workflow processes.
- Used Splunk to search and monitor data and security alerts.
- Provided escalation support for various departments and documents all network and security issues.
- Provided technical assistance for computer problems.

University of North Texas - Denton, TX
Help Desk Technician & Web Support, November 2014 - November 2018

- Used FrontRange HEAT for incident management and customer support.
- Created a standard operating procedure to implement security measures and maintain security updates.
- Provided technical support to end-users via phone, email, and remote assistance.
- Performed in-person and remote hardware and software troubleshooting for desktops, laptops, printers and mobile devices through diagnostics techniques.
- Managed Active Directory user accounts and permissions.
- Assisted in maintaining and upgrading network and server infrastructure.
- Conducted regular backups, system updates, security patching and disaster recovery tests.
- Trained end-users on new software applications and systems.
- Performed system imaging and deployment and managed inventory of all hardware and software.

EDUCATION

University of Maryland Global Campus, - Adelphi, MD
B.S. Cybersecurity Management and Policy – 4.00

PROFESSIONAL COURSES AND CERTIFICATIONS

- EC-Council Certified Ethical Hacker
- CompTIA Security+
- ISC2 Certified in Cybersecurity

- IBM Cybersecurity Analyst
- Google Cloud Essentials
- Google IT Support