Marquzes Ford Jr.

(202) 427-5783 • marquzesfordjr@gmail.com

https://linkedin.com/in/marquzesfordjr • http://github.com/marquzesfordjr

SUMMARY

Detail-oriented IT & Cybersecurity student with hands-on experience in infrastructure support, endpoint management, documentation standardization, cloud administration, and technical troubleshooting. Skilled in Azure AD, Windows/Linux systems, ticketing workflows, metrics tracking, and process improvement. Strong analytical ability with experience coordinating tasks, creating technical documentation, and supporting network and system operations.

CERTIFICATIONS & CLEARANCE

CompTIA Security+ • CompTIA Cybersecurity Analyst (CySA+) • CompTIA Security Analytics Professional (CSAP) • Microsoft Azure Fundamentals (AZ-900) • AWS Certified Cloud Practitioner • LPI Linux Essentials

TECHNICAL SKILLS

Infrastructure & Operations: Azure AD, Active Directory, DNS, Endpoint Imaging, System Hardening
Cloud: Microsoft Azure (VMs, NSGs, monitoring)
Tools: Splunk (SIEM), Rapid7, Freshservice (ITSM), Wireshark, SysInternals
Productivity: Microsoft 365 (Outlook, Teams, SharePoint, Excel)
Programming: Python, PowerShell, C, C++
Documentation: SOPs, technical reports, configuration documentation, process checklists

WORK EXPERIENCE

CyberTrust Massachusetts – SOC Analyst Intern | Boston, MA | Feb 2026 – Present

- Tier 2/3 Soc tasked with threat hunting and detection engineering (this will be replaced with bullet point)
- Blank bullets points will change soon
- Blank bullets points will change soon
- Blank bullets points will change soon

Middlesex Savings Bank – System Support Intern | Westborough, MA | May 2025 – Present

- Managed accounts and access controls using **Azure AD & Active Directory**; maintained DNS settings.
- Integrated **Rapid7** scan data into imaging workflow for 100+ endpoints.
- Resolved **50–60 tickets/week** (authentication, connectivity, software issues).
- Imaged and deployed 100+ systems using hardened baselines, reducing setup time by 30% improving endpoint security posture.

KenCove Partners – Information Technology Intern | Remote | Jun 2023 – Aug 2023

- Performed weekly **vulnerability scans** and validated remediation.
- Assisted with **patching, configuration checks, endpoint hardening**.
- Monitored network traffic and supported **incident triage**.
- Authored documentation for **security controls, configurations, and access management**.

PROJECTS

Security Operation Center (SOC) Automation | Tools: Docker, Wazuh, TheHive, Shuffle

- Deployed containerized SOC stack and built an automated triage workflow that reduced alert response time by ~40%.
- Integrated Wazuh with TheHive for automated case creation and alert enrichment.

Intrusion Detection System (IDS) Development | Tools: Wireshark, SysInternals

- Captured and analyzed 200+ packets, developing custom filters that improved malicious-traffic detection accuracy by 25%.
- Authored detailed incident reports and forensic documentation for simulated intrusions.

EDUCATION

University of Massachusetts Lowell (UMass Lowell), Lowell, MA (Expected Graduation May 2026)
Bachelor of Science, Computer Science – Cybersecurity Concentration
Courses: Cyber Crime Investigations, Intro to Computer Security, Computing I-IV, Data Communication I, Database I

Leadership & Achievements

- Assistant Linux Captain & SOC Co-Lead — UMass Lowell CCDC Team
    - **1st Place** NECCDC 2025 • **3rd Place** NECCDC 2024 • **8th Place** NCCDC Nationals 2025