

Jamie Barbour-Moore

Email: jbarbourmoore@gmail.com

Phone: 443-472-1638

Portfolio: jbarbourmoore.com

Location: Orlando, FL USA

LinkedIn: linkedin.com/in/jbarbourmoore

GitHub: github.com/jbarbourmoore

TECHNICAL SKILLS

Programming Languages: Java, Swift, Rust, C++, C#, Python, Assembly, PowerShell, HTML, CSS, JavaScript

Operating Systems: Windows, MacOS, Linux (Ubuntu / Kali), iOS, Android

Security Tools: Wireshark, Snort, Splunk, Nmap, Coverity, Metasploit, Wazuh, Nmap, Metasploit Framework

CERTIFICATIONS

- [Associate of ISC2](#)
- [CompTIA CySA+](#)
- [CompTIA A+](#)
- [CompTIA SecurityX \(Formerly CASP+\)](#)
- [CompTIA Pentest+](#)
- [CompTIA Project+](#)

EDUCATION

Master of Science in Cyber Security and Information Assurance, Western Governors University | Salt Lake City, UT **2024**

- Relevant Courses: Cyber Security Management, Security Software Design, Secure Network Design, Cloud Security

Bachelor of Science in Software Development, Western Governors University | Salt Lake City, UT **2023**

- Relevant Courses: Software Engineering, Software Quality Assurance, Project Management, User Interface Design

WORK EXPERIENCE

College Student Technical Specialist, Lockheed Martin | Orlando, FL **2016-2019**

Continuous Integration/Build Team Member, F-35 Autonomous Logistics Information System (ALIS):

- Successfully automated workflow between Coverity, Jira, and VersionOne.
- Ensured transparency into program metrics by using Java and PowerShell to automate tracking metrics on Version One, Coverity, Jira, Confluence, Crucible, Jenkins, GIT, and SVN.

Software Tester, UK Scout:

- Used JUnit and Mockito to create unit tests.
- Decreased testing time by creating solution to automate pressing of virtual buttons using Sikuli.

Cyber Intern, Comtech | Columbia, MD **2015-2016**

Contributed to development and evaluation of new cybersecurity certification tests.

- Created and maintained virtual machines designed to mirror business networks for execution of cybersecurity certification tests.
- Developed and deployed automated tools to monitor and evaluate user activities for cybersecurity risks.

HIGHLIGHTED PROJECTS

Health Tracking Project Including iOS Application and Embedded Wearable, Personal Project **2024 – Present**

- Developing an iOS Health Tracking Application utilizing Swift, SwiftUI and SwiftData with 98% coverage in automated testing.
- Followed the Model-View-View Model architecture design pattern while focusing on accessibility and seamless user experience.
- Developing a wearable device using embedded Rust on an ESP32-S3 with an LED touch screen, accelerometer and gyroscope.

Securing Merged Corporate Networks Using Zero Trust Architecture, Academic Project **2024**

- Determined appropriate upgrades by evaluating networking components, vulnerabilities scans, and servers.
- Implemented zero trust architecture using Cisco Duo, proactively identifying and mitigating vulnerabilities.
- Created associated diagrams and detailed test plans for merged network.
- Verified compliance with PCI-DSS and NIST SP 800-207 regulatory requirements, as well as project budget.

Cloud Security Implementation Plan, Academic Project **2024**

- Assessed security of Microsoft Azure environment, implemented improvements to comply with FISMA and PCI-DSS regulations.
- Minimized risks, ensured robust recovery capabilities, and protected against data loss by enabling Purge Protection on key vault, enforcing principle of least privilege and scheduling automatic backups of virtual machines.

Incident Response, Academic Project **2023**

- Performed simulated incident response to resolve multiple tickets from engineers regarding application server issues.
- Used Wuzah SIEM (Security Information and Event Management) and Task Manager to identify crypto miner infection, configured firewall rules and Windows Defender to mitigate issue, and successfully restored functionality.