

Kiori Armani Edwards

Norfolk, VA & Stafford, VA | Kiori.Edwards13@gmail.com | (618) 407-4877 | [Linkedin](#)

OBJECTIVE

I aim to leverage my expertise in cybersecurity, cloud security, and architecture design to develop scalable, secure, and efficient solutions that align with business objectives. I love to learn and I am focused on delivering the best of my abilities to a business environment. My goal is to apply best practices, stay at the forefront of emerging technologies, and deliver impactful solutions that protect business assets and customer data.

EDUCATION

Old Dominion University



Norfolk, Virginia

Bachelor of Science | Major in Cybersecurity | GPA: 3.77 (Magna Cum Laude) | Dean's List 2021-Present

Enrollment: August 2021 - Present

(May 2025 graduation)

Work Experience & Projects

- ❖ **Microsoft: Internship - Cloud Solution Architect** - InfoSec Architects
 - Designed and implemented cloud-based enterprise (Azure) architectures and Generative AI architectures, optimizing scalability and security.
 - Analyzed cybersecurity threats in cloud environments and conducted threat emulation on emerging technologies, including Generative AI, to identify vulnerabilities.
 - Developed CTF objectives for the cloud and Generative AI, enhancing cybersecurity training and awareness.
 - Outlined/Presented how there is a need and opportunity for our higher education to include cybersecurity concepts as inclusive of all IT/cloud curriculum as opposed to add-ons. -  Position Paper
 - Made successful deployments to Azure using- Terraform | Infrastructure as a Code (IaC) | Github (workflow) & Git | Docker | Cloud Adoption Framework | Azure landing zone
 - Proposed an AI model to Microsoft Senior Cloud Solution Architects that assist Cloud Solution Architects -  Final Proposal
- ❖ **Valor Cybersecurity: Internship - Cyber Risk Management Specialist** - Did cybersecurity assessments for Chicken Salad Chick and Jersey Mikes. Worked closely with TJS Financial Solutions by analyzing their security measures and implemented several security solutions to better posture their cybersecurity.
- ❖ **Microsoft Azure Security Analysis & Recommendations**
 - Conducted a comprehensive security analysis of Microsoft Azure, identifying key vulnerabilities such as encryption key management risks, access token abuse, misconfigurations, and phishing threats. Proposed strategic solutions, including implementing Azure Disk Encryption for enhanced cryptographic control, introducing a

two-step authentication process for token security, and leveraging AI-driven phishing detection systems. Emphasized continuous monitoring for misconfigurations to strengthen Azure's security posture - [Microsoft Azure Security Analysis & Recommendation](#)

- ❖ **COVA CCI INNOVATE Cyber Challenge 2025** - Developed an AI model idea that assist architects in their building phases- providing solutions to security vulnerabilities and strengths/weaknesses
- ❖ **COVA CCI Undergraduate Cybersecurity Researcher** - Researched the underlying landscape of Cloud Technology in the school system and Why Cybersecurity should be implemented within the curriculum. ([Research Paper](#))
- ❖ **Cryptocurrency Researcher** - Researched the innovations of cryptocurrency ([Cryptocurrency Project Paper](#))
- ❖ **Cyber Crime Research-** ([Crime Research Project](#))
- ❖ **Securing the pfSense Firewall** - Removed insecure and unneeded protocols while implementing security configuration parameters on network devices and other technologies using secure network administration principles.
- ❖ **Implementing NAT and Allowing Remote Access** - Set up and connected to a remote machine on an external network so it can connect through Remote Access/Virtual Private Network (VPN) to access resources on the internal network.
- ❖ **Implementing Common Protocols and Services** - Used TELNET, Secure Shell (SSH), File Transfer Protocol (FTP), and Secure Copy (SCP) to perform functions between two systems on a network. Examine traffic with Wireshark, through an open source Protocol Analyzer.
- ❖ **Implementing Security Policies on Windows and Linux** - Analyzed a network capture file containing wireless traffic. Examine protocols, Internet Protocol (IP) addresses, and Media Access Control (MAC) addresses, as well as analyze other information from traffic. Used a protocol analyzer called Wireshark using a network capture in pcap format. Filtered packet captures to review the wireless network beacons and application layer traffic: File Transfer Protocol (FTP), telnet, and Post Office Protocol (POP3).
- ❖ **Incident Response Procedures, Forensics, and Forensic Analysis** - Acted as an attacker, exploited a remote system. After attacking the victim machine, analyzed web logs and performed an incident response on a compromised host.

Relevant Coursework

- ❖ **Cybersecurity technology** - Understanding in describing how the components, mechanisms, and functions of cyber systems produce security concerns.
- ❖ **Python** - Acquired a comprehensive understanding of the language's fundamental concepts and its practical applications.

- ❖ **Linux System For Cyber Security** - Using Linux taught me the value of open-source software and the strength of community-driven development, which promotes creativity and collaboration. I also learned a lot about system administration, shell scripting, and command-line programs, which will help me manage and personalize my computing environment more effectively.
- ❖ **Cyber Law** - Dealt with various aspects of cyber law which have allowed me to learn the depth of consequential effects of cyber threats, data breaches, and other security incidents
- ❖ **Cryptography For Cyber Security** - Completed a comprehensive course in cryptography for cybersecurity, focusing on the functionality, evaluation, and application of cryptographic techniques. Gained expertise in the mathematical foundations of cryptology, and the computational and memory requirements of various cryptographic methods. Analyzed the security strengths, risks, and implementation challenges of both hardware and software-based cryptography.
- ❖ **Network System and Security** - Completed an in-depth online course in network systems and security, gaining hands-on experience in key concepts including network technologies, network and information security, and the importance of cryptography.

Learning Activities

- ❖ TryHackMe
- ❖ Old Dominion University CyberOps CTF
- ❖ Cyber Fast Track
- ❖ Cyber-Law
- ❖ picoCTF
- ❖ CS2A

Skills and Proficiencies

- ❖ System Administration
- ❖ Cloud Architecture
- ❖ Cloud Security
- ❖ Network Security
- ❖ Server Administration
- ❖ Microsoft Office Word, Excel, and PowerPoint
- ❖ Python
- ❖ Completed labs practicing Linux Terminal Navigation
- ❖ Attention to detail
- ❖ Strong written and verbal communication skills
- ❖ Willing to work collaboratively

Certifications

- ❖ **Microsoft Certified: Azure Fundamentals - Az-900**

