Kyle Kim

Centreville, VA 20121 | (703) 438-1316 | Kylesonzy@gmail.com | www.kylesonzy.com | LinkedIn

EDUCATION

George Mason University **Fairfax, Virginia**
Master of Science in Applied Information Technology ***Jan 2025 – May 2026***
- **GPA:** 4.00/4.00 | Dean's List
- **Relevant Coursework:** DBA, Cyber Security Principles, Fundamentals of Computing Platforms, Cloud Security, Ethical Hacking

George Mason University **Fairfax, Virginia**
Bachelor of Applied Science in Cyber Security | Finance Minor ***May 2024 – Aug 2025***
- **GPA:** 3.85/4.00 | Dean's List

CERTIFICATIONS

- **CompTIA CySA+, CompTIA Server+, CompTIA Security+, CompTIA Network+, CompTIA A+, CompTIA ITF+, Tech+, CompTIA CSAP, CompTIA CSIS, CompTIA CNIP, CompTIA CIOS, Google Cybersecurity**

WORK EXPERIENCE

Information Technology Security Analyst **| Digital Guardsmen** **Alexandria, Virginia** | April 2025 – Present
- Deployed enterprise vulnerability scanning solutions and analyzed compliance scan reports to support client security posture improvements.
- Designed and configured a secure network rack for internal lab infrastructure; assigned VLANs and subnetted network segments by department to enhance traffic isolation and policy enforcement.
- Created and restored full system images using AOMEI Backupper for efficient workstation deployment and disaster recovery.
- **Implemented GPOs** to standardize workstation configurations, password policies, and control network resources across all departments.
- Configured and managed Active Directory, including the creation and administration of Organizational Units (OUs), user accounts, and group memberships to enforce security policies.

Vulnerability Analyst **| Netflix** **Remote |** May 2025 – July 2025
- Participated in a Pathway Career Accelerator Program, gaining hands-on experience in enterprise cybersecurity operations.
- Categorized and organized data by creating and maintaining detailed spreadsheets to track vulnerability types and system exposure levels
- Joined frequent team meetings to analyze and discuss vulnerability data, referencing frameworks such as CVE, NIST 800-53, and FIPS to assess severity and relevance to organizational assets.

Cybersecurity Compliance Intern **| Lumeria** **Chantilly, Virginia** | Sep 2024 – Jan 2025
- Monitored and analyzed over **50 CVEs** using vulnerability databases and security tools, prioritizing high-risk threats and implementing mitigation strategies using NESSUS.
- Independently ensured compliance with internal security policies and industry standards, preparing documentation for audits and strengthening the organization's overall security posture.

Cybersecurity Analyst Intern **| Pure Sugar Wax** **Centreville, Virginia** | Aug 2024 – Dec 2024
- Deployed and fine-tuned an Intrusion Detection and Prevention System (IDPS), reducing unauthorized access attempts by **40%** and blocking over **60** suspicious activities monthly.
- Implemented a SIEM solution (ELASTIC) to aggregate and analyze logs across website infrastructure, improving anomaly detection accuracy by **30%** and cutting response time to security incidents by **50%**.

PROJECTS

Acne Product Recommender | React Native, Typescript, REST API, NumPy, PostgreSQL, AWS *Oct 2024 – Present*
- Developed mobile application that detects acne types and recommends skincare products based on the analysis.
- Engineered an acne recognition model utilizing YOLOv11, achieving an average accuracy of 90% with confidence intervals.
- Used React Native and integrated OpenAI to match acne detection results with suitable skincare products. Leveraged PostgreSQL and AWS for database management and automated model deployment.

DShield Honeypot | Raspberry Pi, DShield, iptables *Sep 2024 – Present*
- Designed enticing honeypot using DShield on a Raspberry Pi to analyze network-based attack vectors from live threat actors.
- Configured the honeypot to log malicious network traffic, using threat intelligence feeds and data correlation techniques to categorize attack patterns and intrusion attempts.

Splunk Threat Intelligence | AbuseIPDB, VirusTotal, Phantom SOAR, Indexed data *Aug 2024 – Oct 2024*
- Implemented automated incident response actions based on threat intelligence data, such as blocking malicious IP addresses.
- Integrated external threat intelligence feeds from open-source providers into Splunk for real-time monitoring.

Malware Analysis | REMnux, FlareVM, IDA Free, FakeDNS, AWS EC2 *July 2024 – Sep 2024*
- Integrated Nested Virtualization for dynamic malware analysis, leveraging its automated environment to find malicious files.
- Configured FlareVM on AWS EC2 instances for secure, cloud-based malware analysis, utilizing this specialized Linux distribution to reverse engineer and analyze malware samples while isolating them from the primary network.

SKILLS & TECHNICAL TOOLS

Proficient: Network Security, Linux, Metasploit, Security Information and Event Management, Cloud Security, and Hypervisors
Familiar: Nmap, Wireshark, Tcpdump, MTR, Forcepoint, Packet sniffing, Splunk, Burpsuite, NGFW, Active Directory, and pfSense