Kyle Kim

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

CAREER OBJECTIVE

Aspiring cybersecurity professional aiming to leverage hands-on experience in vulnerability management, network security, and infrastructure design to contribute to a dynamic security team. Seeking a role where I can apply my skills in system imaging, VLAN segmentation, and secure infrastructure deployment, as well as support SOC operations using SIEM tools like Splunk and Elastic. Currently pursuing a master's in Applied Information Technology and holding certifications including CySA+ and Security+, with a strong interest in expanding into penetration testing and red teaming to enhance offensive security capabilities.

EDUCATION

George Mason University — **Fairfax, Virginia**
Master of Science in Applied Information Technology — ***Jan 2025 – May 2026***

- **GPA:** 3.76/4.00 | Dean's List
- **Relevant Coursework:** DBA, Algorithm/Data Structures, Computing Platforms, Cloud Security, Ethical Hacking

George Mason University — **Fairfax, Virginia**
Bachelor of Applied Science in Cyber Security | Finance Minor — ***May 2024 – Dec 2025***

- **GPA:** 3.85/4.00 | Dean's List
- **Relevant Coursework:** Cyber Security Principles, IT Forensics, Cybersecurity of Data & Software, Security of Information Systems

CERTIFICATIONS

CompTIA Certifications

- **CompTIA CySA+**
- **CompTIA Server+**
- **CompTIA Security+**
- **CompTIA Network+**
- **CompTIA A+**
- **CompTIA ITF+**
- **CompTIA Tech+**

CompTIA Stackable

- **CompTIA CSIS**
- **CompTIA CSAP**
- **CompTIA CIOS**
- **CompTIA CNIP**

Miscellaneous & In Progress

- **CompTIA SecurityX (In progress)**
- **CompTIA Linux+ (In progress)**
- **Google Cybersecurity Professional**
- **AWS Certified Cloud Practitioner (In progress)**

WORK EXPERIENCE

***Cybersecurity Intern* | Mobius** — **Alexandria, Virginia** | Sept 2025 – Present

- Develops and assesses security policies and evaluates compliance requirements, interpreting and executing FedRamp, NIST 800-171, and other technical guidance.
- Administration of Privileged Identity Management, authentication, and governance with Azure AD.
- Sentinel Cybersecurity management, Investigation, Threat hunting and Kusto Query Language proficiency.
- Administration of SharePoint and Teams collaboration platforms, including implementation of Identity and Access policies.
- Managing Azure resources such as virtual machines, virtual networks, role-based access control (RBAC), and various other cloud services.
- Utilized Microsoft Compliance Manager and Microsoft Purview to align security controls and evidence with CMMC Level 2 requirements, ensuring readiness for the upcoming C3PAO (Certified Third-Party Assessment Organization) evaluation.

***Information Technology Security Analyst* | Digital Guardsmen** — **Alexandria, Virginia** | April 2025 – Sept 2025

- Deployed enterprise vulnerability scanning solutions and analyzed compliance scan reports to support client security posture.
- 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 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.
- Configured NVMS7000 surveillance software and integrated IP cameras using PoE injectors connected to a centralized switch, enabling seamless live monitoring and NVR-based video recording.
- Deployed and configured a Proxmox cluster with multiple nodes, creating virtualized environments using imported ISO templates to host isolated VM environments tailored to different client needs and testing scenarios.

- Imaged blade, rack-mounted, and tower servers using standardized system images; tested configurations in staging environments before pushing into production to ensure consistency, security, and performance across client deployments.

***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 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%**.
- Responded to a real-world incident involving a malicious actor exploiting a WordPress vulnerability; isolated the breach, removed the backdoor, patched the vulnerable plugin, and restored the website from a clean backup, successfully minimizing downtime and preventing reinfection.

PROJECTS

Hack The Box CTF | Penetration Testing, Burp Suite, Nmap, Metasploit, Linux, Privilege Escalation *June 2025 - Present*

- Conducted comprehensive enumeration and exploitation using tools like Nmap, Burp Suite, Gobuster, SQLmap, Metasploit.
- Practiced privilege escalation techniques across Linux and Windows environments, including kernel exploits, misconfigured services, and weak permissions.
- Documented walkthroughs and maintained a personal knowledge base for tactics, techniques, and procedures (TTPs) aligned with the MITRE ATT&CK framework and the Cyber Kill Chain.

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.
- Used results to improve local network security posture and harden externally exposed services against similar attacks.

Acne Product Recommender | React Native, Typescript, REST API, NumPy, PostgreSQL, AWS *Oct 2024 – Nov 2024*

- 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.

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.
- Employed FakeDNS to intercept and redirect malicious domain queries within the lab, allowing safe observation of malware's command-and-control (C2) attempts.
- Captured and analyzed malware-generated network traffic using Wireshark to extract Indicators of Compromise (IOCs) and identify hardcoded domains/IPs.
- Executed real-world malware samples in a controlled VM (Windows 10 on VirtualBox) to observe persistence mechanisms, dropped files, and registry changes.

Snort-Based NIDS Deployment | Snort, pfSense, Ubuntu Server, Network TAP, Wireshark *Jan 2025 – Mar 2025*

- Deployed a Network Intrusion Detection System using Snort on a dedicated Ubuntu server to monitor traffic within a segmented lab environment.
- Configured Snort with rulesets to detect malicious activity such as port scans, brute-force attempts, and known signatures.
- Tuned alerts to reduce false positives and categorized threats by severity using Snort's rule tuning and the .conf adjustments.

SKILLS & TECHNICAL TOOLS

Security Tools: Splunk, Metasploit, Wireshark, BurpSuite, DShield, Nessus, OpenVAS, FakeDNS, Snort, VirusTotal, AbuseIPDB
Systems: Active Directory, Group Policy Management, Proxmox, AOMEI Backupper, pfSense, Hikvision, OUs, VLANs
Languages: Python, Bash, PowerShell, Javascript, SQL
Platforms: Windows Server, Kali Linux, Ubuntu, AWS EC2, Raspberry Pi
Familiar With: Tcpdump, MTR, Gobuster, SQLmap, Nmap, Forcepoint, Packet Sniffing, Elastic Stack, Docker, Git, VirtualBox, ISO provisioning