Sandesh Iyer

sandeshiyer7@gmail.com | (571)-417-8716| linkedin.com/in/sandeshiyer

Education

George Mason University Honors College - College of Engineering and Computing Aug 2025-Present

Bachelors of Science in Cybersecurity Engineering **GPA: 3.97/4.0 (Dean's List)**

Certifications: Google Cybersecurity Certificate | Security+ | Microsoft Azure Fundamentals (AZ-900) |Microsoft Security, Compliance, Identity fundamentals (SC-900)

Related Coursework: Introduction to Cybersecurity, Computer Science Fundamentals, Cybersecurity Fundamentals, System Engineering (In progress), Linear Algebra, Operating Systems (In Progress),

Leadership & Involvement: Peer Mentor @ College of Engineering and Computing | Member @ Hackfax | Member @ Cybersecurity Club | Member @ Indian Student Association

Experience

Cybersecurity Intern, SABCVA – Fairfax VA Mar 2026 - Aug 2026

- Executed security log analysis and incident triage within a SOC environment, investigating alerts, identifying indicators of compromise (IOCs), and supporting threat detection and response efforts
- Developed phishing-awareness and malware-analysis workflows by analyzing attack techniques, documenting findings, and improving organizational defenses against social engineering threats.
- Conducted security risk assessments and policy reviews aligned with NIST CSF and CIS Controls to identify vulnerabilities, recommend mitigations, and strengthen compliance practices.
- Evaluated cloud security configurations and identity-access controls by identifying misconfigurations, applying least-privilege principles, and improving overall security posture.

Security CTF Web Developer/Tester, Hackfax – Fairfax, Virginia Oct 2025 - Feb 2026

- Developed web-based security challenges simulating OWASP Top 10 vulnerabilities, enhancing hands-on cybersecurity training and application security awareness.
- Conducted vulnerability assessments and penetration testing across client-side and server-side applications, identifying security weaknesses and validating remediation strategies.
- Implemented threat modeling and adversarial testing methodologies to evaluate attack paths and strengthen realistic security simulation environments.
- Engineered cybersecurity competition scenarios involving authentication flaws, access control issues, and XSS vulnerabilities, improving secure coding practices and defensive capabilities.

Cybersecurity Engineering Extern, Extern – Remote July 2026 - Aug 2026

- Developed IoT security assessments and threat models to identify vulnerabilities across MQTT-based data pipelines and connected device infrastructure.
- Engineered Python-based anomaly detection prototypes to monitor device behavior, identify suspicious activity, and improve IoT threat detection capabilities. .
- Executed security testing on IoT systems by simulating spoofing, replay attacks, and unauthorized access scenarios to validate defensive controls.
- Implemented cybersecurity recommendations involving TLS/mTLS encryption, device authentication, and incident response playbooks to strengthen critical infrastructure security posture.

Projects

SOC Incident Response

- Analyzed security logs and simulated threat scenarios to perform incident triage, identify indicators of compromise (IOCs), and support defensive response procedures.
- Investigated phishing, malware, and social engineering attacks using security analysis techniques to detect potential threats.
- Developed incident response documentation outlining findings, remediation steps, and security improvement recommendations.
- Applied SOC workflows, SIEM concepts, and endpoint security practices to enhance threat detection and response capabilities.

Professional Cybersecurity Home Lab Environment

- Built a virtual cybersecurity lab using VirtualBox with Kali Linux, Windows 10, and Metasploitable to simulate an enterprise network.
- Configured Active Directory Domain Services, domain controllers, user accounts, authentication, and Windows client domain integration.
- Designed and troubleshot network infrastructure using TCP/IP, DNS, static IP addressing, bridged adapters, and Windows Firewall rules.
- Conducted penetration testing and vulnerability assessments using Kali Linux against intentionally vulnerable systems in an isolated lab environment.

Skills

Programming: Python, Java, JavaScript, HTML

Cybersecurity: Threat Analysis, Incident Response, Vulnerability Assessment, Security Operations (SOC), Endpoint Security, Security Awareness Training

Systems & Networking: Linux, Windows, Linux CLI, TCP/IP, DNS, VPNs, SSH, Network Security, VLANs, Zero Trust

Cloud & Infrastructure: Microsoft Azure, Identity & Access Management (IAM), Cloud Security, Microsoft 365, Google Workspace

Tools: Git, Wireshark, Cisco Packet Tracer, Kali Linux, TryHackMe, Microsoft Defender

Frameworks & Compliance: NIST CSF, CIS Controls, SOC 2, ISO 27001, CMMC

Professional: Technical Communication, Public Speaking, Team Leadership, Agile Collaboration, Project Management