Harshit Garg

linkedin.com/in/harshitgarg-cs | github.com/harshitgarg-cs

Email : iharshit.garg.cs@gmail.com

Mobile : +1 (404)-259-0501

Education

Georgia State University

Bachelor of Science in Computer Science — *Atlanta, GA*

- GPA: 3.70; Microsoft Scholar 2024.

Certifications

- ISC2: Certified in Cybersecurity
- Microsoft Cybersecurity Analyst Professional Certificate

Technical Skills

- **Tools:** SIEM, Wireshark, nmap, Entra ID, Kali Linux, Metasploit, Virus Total, CyberChef, Docker, Shodan, VMWare
- **Security & Networking:** Threat Detection, Incident Response, IAM (Identity and Access Management), Malware Analysis, OSINT
- **Programming:** Python

Experience & Projects

Mission Omega — **September 2024 - Present**

IT & Security Intern — *Remote*

- Optimized security policy framework by reviewing and consolidating over 1,800 policies, reduced redundancy by 30%, and ensuring compliance with key security regulations.
- Automated software license assignment by implementing a ticketing workflow in HaloITSM, reducing processing time per request by 80% and saving 3+ hours per week.
- Configuring Microsoft Purview to implement data classification, perform risk assessments, and establish role-based access control (RBAC), enhancing data governance and security measures across the organization.

Georgia State University — **January 2025 - Present**

Learning Environment Support Technician — *On-Site*

- Providing technical support for classroom IT/AV systems, ensuring timely resolution of issues in line with SLAs to minimize downtime
- Efficiently managing and documenting support tickets via ServiceNow, contributing to improved classroom operations and adherence to SLA targets.

Real-Time Intrusion Detection System | *Python, Scapy, Sklearn, NumPy, Threading, Logging, Nmap* — **February 2025**

- Developed a real-time Intrusion Detection System (IDS) using Python, leveraging Scapy for packet capture, machine learning (Isolation Forest) for anomaly detection, and signature-based rules to identify threats, improving network security monitoring.
- Implemented a modular detection pipeline with a traffic analysis engine, hybrid detection mechanisms, and an alert system that logs and escalates threats, increasing system transparency and response efficiency.
- Tested and validated IDS performance using mock attack simulations, including SYN floods and port scans, ensuring accurate threat detection and demonstrating system effectiveness.

Azure Active Directory (Entra ID) | *Azure Active Directory (Entra ID)* — **February 2025**

- Configured Single Sign-On (SSO) and implemented Conditional Access policies & RBACs using Azure AD to secure application access and enhance user authentication.
- Improved security and user experience by enforcing MFA, location-based restrictions, and simplifying login processes through automated configuration.

GSU Technology Immersion Challenge (CTF) sponsored by Truist | *OSINT, CyberChef, Wireshark, Docker* — **November 2024**

- Led Cipher Soldiers as team captain to a top 10 finish (10th of 27 teams) in the CTF challenge, by solving 8 of 10 challenges and earning 4,525 points.
- Enhanced cybersecurity skills across reverse engineering, forensics, cryptography, and pwn categories through strategic problem-solving and collaboration.

Incident Response Simulation | *SIEM, Virus Total, Wireshark, Splunk* — **April 2024**

- Conducted a simulated incident response using Wireshark, Splunk, and SIEM to investigate, detect, and mitigate security threats.
- Analyzed traffic logs, identified anomalies, and assessed IoCs using Splunk and VirusTotal, improving threat response efficiency by 15%.