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**, **President's List for Multiple Semesters**.

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*

- Reduced policy redundancy by **30%** by consolidating **1,800+** security policies to meet **NIST** compliance.
- 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, **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**

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

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 with **VirusTotal**, improving threat response efficiency by **15%**.