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 security policy redundancy by 30%** by reviewing and consolidating **1,800+** security policies, aligning with **NIST** compliance standards.
- **Saved 3+ hours/week** by automating software license requests using a ticketing workflow in **HaloITSM**, reducing request handling time by **80%**.
- **Enhanced data governance and access control** by configuring **Microsoft Purview** to enable **data classification**, **risk assessments**, and **RBAC**.

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**

- **Built a real-time IDS** using **Python**, capturing traffic with **Scapy**, and detecting anomalies with **Isolation Forest** and **signature-based rules**, improving network threat visibility.
- **Increased response transparency and modularity** by designing a pipeline with a **traffic analysis engine**, **hybrid detection**, and an alerting system with logging/escalation.
- **Verified IDS accuracy** by simulating attacks (e.g., **SYN floods**, **port scans**), ensuring precise threat detection and validating system performance.

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%**.