

# Harshit Garg

LinkedIn | GitHub

Email : [iharshit.garg.cs@gmail.com](mailto: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

- **Programming:** Python
- **Security & Networking:** OSINT, Threat Detection, Incident Response, IAM, Malware Analysis
- **Tools:** Kali Linux, VMWare Workstation, Wireshark, nmap, Cyberchef, Shodan, Metasploit, Docker, Entra ID, SIEM, Virus total

## WORK EXPERIENCE

### Mission Omega

September 2024 - Present

IT & Security Intern

Remote

- Improved security policy organization by analyzing 1800+ policies, reducing redundancy by 30% and ensuring compliance with security standards.
- Automated software license tracking in HaloITSM, improving accuracy by 20% and reducing manual effort in cost analysis.
- Configuring Microsoft Purview, focusing on data classification, risk assessments, and role-based access control (RBAC) to enhance data governance and security measures.

### Georgia State University

January 2025 - Present

Learning Environment Support Technician - IIT

On-Site

- Ensured IT/AV security by managing access control and system integrity across collaborative spaces.
- Resolved 20+ technical support tickets using ServiceNow, improving IT service response time by 25%

## PROJECTS

### 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%.