HARISH S U

SOC Analyst | VAPT Fresher | Cybersecurity Professional
Vellore, TamilNadu | +91-8778271624 | harishumachandran@gmail.com | LinkedIn | Portfolio

PROFESSIONAL SUMMARY

Cybersecurity fresher with hands-on experience in SOC operations, SIEM-based threat detection, and VAPT fundamentals. Proficient in Splunk and Wazuh for log analysis and incident investigation. Skilled in detecting brute-force attacks, RDP anomalies, and privilege escalation using Windows Event Logs and Sysmon. Completed intensive Red Team training at Red Team Hacker Academy (Jan–Jun 2026). Familiar with MITRE ATT&CK, ethical hacking tools (Nmap, Metasploit, Burp Suite), and Python/Bash scripting. Completed Deloitte Australia Cybersecurity program; pursuing Certified Ethical Hacker (CEH) certification.

TECHNICAL SKILLS

- **SIEM & SOC Tools:** Splunk, Wazuh, Sysmon, ELK Stack (basic)
- **SOC Operations:** Threat Detection, Log Analysis, Incident Investigation, Alert Triage, Event Correlation, Threat Hunting, MITRE ATT&CK Framework
- **VAPT / Pen Testing:** Nmap, Wireshark, Metasploit, Hydra, Burp Suite, Vulnerability Assessment, Reconnaissance, Exploitation Basics
- **Attack Detection:** Brute Force, RDP Monitoring, Privilege Escalation, PowerShell Attack Detection, Credential Access
- **Operating Systems:** Kali Linux, Ubuntu, Windows Server/Client, Windows Event Logs
- **Networking:** TCP/IP, Firewall Basics, Packet Analysis, Network Monitoring, IDS/IPS
- **Scripting & Dev:** Python, Bash, PowerShell, SQL, React (basic)
- **Cloud & Virtualization:** AWS (basic), VMware, VirtualBox
- **Soft Skills:** Analytical Thinking, Incident Response, Documentation, Problem Solving

TRAINING & PROFESSIONAL DEVELOPMENT

Red Team Training Program | *Red Team Hacker Academy* Jan 2026 – Jun 2026 | *Bengaluru, Karnataka* (Offline)

- Completed an intensive 6-month red team training program covering offensive security techniques, penetration testing methodologies, and adversary simulation.
- Trained in network penetration testing, web application exploitation, Active Directory attacks, and post-exploitation techniques using industry-standard tools.
- Practiced real-world attack scenarios in lab environments, developing skills in privilege escalation, lateral movement, and evasion techniques mapped to MITRE ATT&CK.
- Gained hands-on experience with tools including Metasploit, Burp Suite, Nmap, BloodHound, and custom Python exploit scripts.

PROJECTS

SIEM-Based Threat Detection Platform | *Splunk · Sysmon · Windows Event Logs*

- Engineered a centralized SOC monitoring solution using Splunk and Sysmon, ingesting and analyzing 5,000+ simulated Windows event logs to detect and triage malicious activities across Windows environments.
- Developed 10+ custom Splunk dashboards and alerting rules to visualize brute-force attacks, RDP anomalies, and privilege escalation events, reducing simulated threat detection time by ~40% compared to manual log review.
- Mapped 15+ detections to MITRE ATT&CK tactics Credential Access, Lateral Movement, and Persistence — enabling structured, framework-aligned incident response.

ThreatScan: AI-Powered Email & URL Threat Analyzer | *React · Claude AI · Chrome Extension*

- Developed a Chrome Extension integrated into Gmail to automatically scan emails and embedded URLs for phishing indicators, analyzing 100+ email samples during testing with ~90% detection accuracy.

- Leveraged Claude AI API for NLP-based email content analysis; assigned 0–100 safety scores to flag suspicious content, reducing average user triage time from minutes to under 5 seconds per email.
- Engineered a side panel UI enabling one-click automated scanning of unread messages, eliminating the need for manual copy-paste analysis across 3+ email threat categories.

Sign-to-Speech: Real-Time Gesture Recognition & Voice Generation | *MobileNetV2 · MediaPipe · Python*

- Designed a real-time hand gesture detection system converting 20+ ASL gestures to synthesized speech using deep learning, achieving >95% recognition accuracy on test datasets.
- Integrated MobileNetV2 and MediaPipe pipelines for inference latency under 200ms per gesture; added emergency email alert functionality for critical gestures.
- Built an accessible Tkinter-based UI aimed at assisting people with speech and hearing disabilities, with full functionality on standard webcam hardware.

EDUCATION

Master of Computer Applications (MCA) | *Vellore Institute of Technology* Completed: April 2025 | Vellore, Tamil Nadu
CGPA: 7.83 / 10.0

Bachelor of Computer Applications (BCA) | *KMG College of Arts and Science* Completed: May 2023 | Vellore, Tamil Nadu
CGPA: 7.5 / 10.0

CERTIFICATIONS

- Certified Ethical Hacker (CEH) - EC-Council (In Progress)
- Deloitte Australia Cyber Job Simulation Completion Certificate - May 2025
- Git Training Certification - Simplilearn, May 2025