Hariharan T

Email: thiruhari444@gmail.com
GitHub: github.com/00112244
Linkedin: linkedin.com/in/t-hariharan
Mobile: +91 9597188422

OBJECTIVE

Motivated and detail-oriented final-year Computer Science Engineering graduate specializing in IoT and Cyber Security, with hands-on experience in Cyber Security, SOC Operations, Digital Forensics, and Incident Response. Adept at threat analysis, incident handling, and security monitoring through academic projects and internships. Seeking an entry-level cybersecurity role to leverage technical expertise, analytical skills, and a passion for security to strengthen an organization's cybersecurity posture and drive proactive threat mitigation.

EDUCATION

Manakula Vinayagar Institute of Technology, Puducherry, India — November 2021 – May 2025
Bachelor of Technology in Computer Science and Engineering (IoT & Cyber Security) — **CGPA: 8.1**

SRVS National Higher Secondary School, Karaikal, India — Graduated: 2021
Higher Secondary Certificate (HSC) — **Percentage: 81.04%**

Karaikal Ammayar Higher Secondary School, Karaikal, India — Graduated: 2019
Secondary School Leaving Certificate (SSLC) — **Percentage: 78.6%**

SKILLS SUMMARY

- **Tools:** Splunk, LogRhythm, ELK Stack, EnCase Forensic, Autopsy, Volatility, Snort, Suricata, TheHive, Wireshark, Nmap, Nessus, OpenVAS, Metasploit, Burp Suite, Google Cloud IAM, Microsoft Sentinel
- **Languages**: Python (Utilized for Projects), SQL (SQL Injection)
- **Frameworks**: MITRE ATT&CK,NIST, ISO/IEC 27001
- **Area of Expertise**: Security Operations Center (SOC), Digital Forensics, Incident Response, Threat Hunting, Network Security, Vulnerability Management, Penetration Testing, Cloud Security, Identity and Access Management (IAM)
- **Technologies**: Generative AI (LLM models), Microsoft Copilot

PROJECT

Engineer Strengthening Cybersecurity with Wazuh

- Streamlined data collection and reporting procedures, reducing processing time by 20% enhancing efficiency.
- Deployed Wazuh agents on Kali Linux and Windows to enable real-time malware detection, system monitoring, and automated incident response.
- Customized detection rules and integrated CVE vulnerability feeds, reducing threat detection time by 35% and improving security posture.
- Centralized log Management using the Elastic Stack (ELK), developing dashboards that accelerated forensic investigations by 40%.
- Strengthened operational resilience and enhanced threat visibility across diverse environments.

Snort IDS/IPS Implementation and Configuration

- Configured and optimized Snort IDS/IPS on both virtual and local machines to monitor, detect, and prevent network-based attacks.
- Authored over 20+ custom Snort rules for real-time threat identification, achieving a 30% increase in detection accuracy.
- Designed an efficient alert and logging system to streamline incident response workflows and improve threat analysis speed by 25%.
- Elevated network security defenses while gaining deep practical experience in IDS/IPS management.

Windows Event Logs Forwarding to Splunk Using Universal Forwarder

- Engineered seamless Windows Event Log forwarding to Splunk via Universal Forwarder on an Ubuntu VirtualBox, achieving real-time log centralization.
- Automated cross-platform log ingestion and analysis, boosting system visibility by 35% and supporting proactive incident detection.
- Enhanced operational efficiency by designing dashboards and alerts, reducing log investigation time by 28%.
- Developed expertise in Splunk architecture, log management, and cybersecurity operations across hybrid environments.

CERTIFICATES

Security Blue Team - Blue Team Junior Analyst
- Proficient Gained foundational skills in SOC operations, threat detection, incident response, and digital forensics.

IBM - Penetration Testing, Incident Response and Forensics Certificate
- Developed skills in ethical hacking, penetration testing methodologies, incident handling, and forensic analysis.

Google Cybersecurity Certification
- Completed extensive training in security operations, network defense, threat mitigation, and risk management.

Infosec - Cyber Incident Response and Threat Hunting Specialization Certification
- Specialized in proactive threat hunting, digital forensics, and incident response planning across various cyber environments.