DEVADATH A

Cybersecurity Analyst

devadathnair4397@gmail.com | +91 9496113175 | linkedin.com/in/devadathcyber001 | devadathappu.github.io/profile/

Professional Summary

CEH-certified B.Tech Computer Science graduate with practical experience in SIEM monitoring, threat detection, and vulnerability assessment through hands-on projects. Recognized by NASA, OpenAI, and DHS for responsible disclosure, demonstrating strong analytical skills and attention to detail. Skilled in detection rule creation, threat hunting, and incident documentation, eager to contribute to real-world security operations.

Education

Bachelor of Technology in Computer Science and Engineering, Nov 2020 – Jun 2024
APJ Abdul Kalam Technological University

- Programming, Databases, Computer Networks.

Cybersecurity Professional Training (Diploma-equivalent), Aug 2024 – May 2025
Techbyheart Academy, Bangalore

- SOC operations, ethical hacking, security testing.

Technical Skills

SIEM and Monitoring: Splunk Enterprise, ELK Stack, Wazuh, log analysis, alert triage, incident response

Vulnerability Assessment & Pentesting: Burp Suite Pro, OWASP ZAP, Nessus, Metasploit, VAPT methodologies

Network and Security Technologies: Wireshark, Nmap, Snort IDS/IPS, firewall concepts, protocol analysis

Threat Intelligence: MISP, AlienVault OTX, VirusTotal, OSINT techniques

Cybersecurity Knowledge: OSI & TCP/IP models, IP addressing, subnetting, SQL Injection, Brute Force, ARP Spoofing

Frameworks and Standards: OWASP Top 10, ISO/IEC 27001 (controls & compliance basics), SOC operations, incident response lifecycle

Operating Systems: Kali Linux, CentOS, Windows

Certifications

Certified Ethical Hacker (CEH), EC-Council	May 2025
Advanced SOC Analyst (ASA), Techbyheart Academy	Aug 2025
Certified Security Tester (CST), Techbyheart Academy	Aug 2025
Google Cybersecurity Professional Certificate, Coursera	Aug 2024
Introduction to Cybersecurity, Cisco Networking Academy	Aug 2024
CompTIA A+ Network Fundamentals, Coursera	Aug 2024
Linux Crash Course, EC-Council	Jun 2024

Security Achievements

NASA Vulnerability Disclosure Program Recognition (Bugcrowd)	Nov 2024
OpenAI Security Research Program Acknowledgment (Bugcrowd)	Feb 2025

World Health Organization Security Research acknowledgments Jul 2025

U.S. Department of Homeland Security Recognition (Bugcrowd) Nov 2024

Projects and Practical Experience

Institutional Security Assessment - LBS College of Engineering | Nessus, Burp Suite Feb 2025

- Collaborated with the security team to conduct a comprehensive infrastructure assessment using Nessus Professional.
- Identified 5+ critical vulnerabilities using Nessus; achieved 95% remediation in 6 days.
- Discovered authentication bypass impacting 500+ accounts; improved portal security with team fixes.

Capture The Flag (CTF) Platform Development | Web Security, Lab Design Mar 2025

- Designed 8+ vulnerable labs (SQLi, XSS, File Upload, Command Injection, FTP, SSH).
- Built a gamified CTF environment for safe, hands-on exploitation training.

Splunk SIEM Lab Project | Splunk Enterprise, Windows Event Analysis Jan 2025

- Built a Splunk lab to analyze Windows event logs, helping me learn and understand how SOC teams detect threats in real-world attack patterns.
- Investigated and correlated authentication failures to detect brute-force attack patterns using custom search queries.
- Created automated dashboards and alert rules to streamline threat detection and incident response procedures.

ELK Stack Threat Detection Lab | Elasticsearch, Kibana, Winlogbeat, Sigma Rules Apr 2025

- Deployed ELK Stack infrastructure and configured Winlogbeat to centralize log collection and analysis.
- Engineered Sigma-based detection rules and converted them to Lucene queries for advanced threat hunting.
- Analyzed suspicious events in Kibana and documented investigation procedures to practice security operations workflows.

Additional Information

Languages: English (Fluent), Hindi (Intermediate), Malayalam (Native)

Soft Skills: Technical documentation, Cross-functional collaboration, Rapid technology adoption, Security research methodology