VYSHAK HARIDASAN

Cyber Security Analyst | CEH Certified | SOC Operations | Threat Intelligence Analysis | Cybersecurity Blogger

+91 70925 96063 contact@vyshak.in linkedin.com/in/vyshak-haridasan vyshak.in Chennai, Tamil Nadu, India

SUMMARY

Cybersecurity Analyst with 4 years of experience in SOC Operations, Incident Response, Threat Detection, SIEM Engineering, and Application Security. Experienced in Splunk, The Hive SOAR, phishing investigations, correlation search development, and security monitoring within enterprise environments.

EXPERIENCE

Security Analyst, APAC SMC

BNP Paribas

03/2025 - Present Chennai

- Investigate and triage security alerts across endpoint, network, and SIEM telemetry while supporting APAC security operations, ensuring rapid detection and response in alignment with security operations center (SOC) playbooks
- Conduct in-depth log analysis across multiple data sources (SIEM, endpoint, firewall, and network logs) to support investigations and provide actionable insights to internal security and incident response teams
- Serve as a key point of contact for the cybersecurity hotline, handling real-time escalations and providing technical guidance and solutions to business stakeholders and requesters
- Collaborate cross-functionally with other security teams across APAC region to gather evidence, support incident investigations, and contribute to post-incident reports and continuous improvement efforts
- Prepare detailed analysis reports and documentation for internal stakeholders, ensuring compliance with organizational policies and regulatory requirements

Cyber Security Analyst

Zalaris

07/2022 - 03/2025 Chennai

- Conducted SIEM activities utilizing Splunk to detect and analyze security incidents.
- Within the Security Operations Center (SOC), attentively monitored 24/7 and analyzed security alerts, dashboards and incidents instigated by external threat actors by maintaining SLA.
- Developed and tuned 20+ Splunk correlation searches to improve threat detection coverage and reduce false positives.
- Conducted penetration testing for internal web applications on a regular basis using automated solution Performed Grey box application security testing for web applications using OWASP WSTG.
- Regularly reviewed over 20 user-flagged phishing emails per day, identified malicious content, and implemented measures to block and prevent their spread within the organization's network.
- Research and stayed updated on IT security trends and security concepts to develop best practices for IT security.

TECHNICAL SKILLS & SECURITY TOOLS

SECURITY OPERATIONS

Incident Response | Threat Detection | Threat Hunting | Phishing Analysis | Detection Engineering | Security Monitoring

SECURITY TECHNOLOGIES

Splunk Enterprise | The Hive SOAR | MITRE ATT&CK | SPL

APPLICATION SECURITY

Burp Suite | OWASP WSTG | Nessus | Nmap

THREAT INTELLIGENCE AND OSINT

VirusTotal | AlienVault OTX | AbuseIPDB | GreyNoise | Shodan

AUTOMATION AND SCRIPTING

Python

CERTIFICATIONS

HTB CDSA (In Progress)
Hack The Box Academy

Certified Ethical Hacker (CEH)
EC Council

Cisco Cyber Security essentials
Cisco Networking Academy

Cisco Intro to Cybersecurity
Cisco Networking Academy

EDUCATION

Master of Computer Applications

Dr. MGR Educational and Research Institute

11/2021 - 05/2023 Chennai

CGPA **8.03** / 10.00

- I obtained my Master of Computer Applications degree from Dr. MGR Educational and Research Institute, specializing in computer science and Cyber Security Disciplines, achieving a CGPA of 8.03

B. Com (General)

Ramakrishna Mission Vivekananda College (Autonomous)

06/2018 - 07/2021 Chennai

CGPA **7.35** / 10.00

- Completed Bachelor of Commerce in General Studies at Ramakrishna Mission Vivekananda College (Autonomous), achieving a CGPA of 7.35

COMMUNITY & ACHIEVEMENTS

Currently top 1% in TryHackMe, which is one of the most well-known online Cyber Security training platforms

Student Council Member in Ramakrishna Mission Vivekananda College (2019-2021)

Former Member of TamilCTF team (Top CTF team from India)

SECURITY RESEARCH & PROJECTS

Threat Intelligence Automation

- Developed a Python-based IOC enrichment tool integrating VirusTotal, AbuseIPDB, and AlienVault OTX APIs.
- Automated extraction and analysis of indicators from security investigations, reducing manual enrichment effort.

Cybersecurity Research Blog | blog.vyshak.in

- Published technical analysis of cybersecurity vulnerabilities, attack techniques,defensive security practices and mitigation guidance.
- Authored detailed research on React2Shell (CVE-2025-55182), covering exploitation methodology, detection opportunities, and mitigation strategies.
- Published analysis of CopyFail (CVE-2026-31431), a Linux privilege escalation vulnerability, including attack-chain breakdown and defensive recommendations.
- Regularly write about emerging threats, CVEs, and cybersecurity events for the security community.

LANGUAGES

English

Tamil

Malayalam