Karthikeyan R

Junior SOC Analyst
+91 6383972347 karthicysec@gmail.com linkedin.com/in/karthicysec
karthicysec.netlify.app

Professional Summary

Junior SOC Analyst with hands-on experience in threat detection, alert triage, and incident response. Skilled in tools like CrowdStrike, Wazuh, Seceon, and Jira, with a strong foundation in SIEM, log analysis, and vulnerability assessment. Passionate about strengthening security posture through proactive threat hunting and teamwork.

Experience

Junior SOC Analyst — Mitigata Cyber Insurance, Bengaluru *May 2025 – Present*

- Monitor and analyze security events using tools such as CrowdStrike, Seceon, Wazuh, and Netwrix to detect and respond to potential threats in real time.
- Manage incident workflows through Jira, ensuring timely resolution, tracking, and documentation of security incidents.
- Perform alert triage, indicator of compromise (IOC) hunting, and detailed log analysis to support threat detection and mitigation efforts.

Cybersecurity Technical Intern — Satcom Infotech Pvt Ltd, Chennai *Feb 2025 – Apr 2025*

- Investigated DLP alerts, identified unauthorized access attempts, and configured Netwrix for enforcing data access controls and encryption.
- Assisted clients by providing technical support for DLP-related issues, including installation, configuration, and troubleshooting of security solutions.

Skills

- **SIEM Tools:** Splunk,Wazuh, Seceon
- **Endpoint Security:** CrowdStrike
- **Ticketing Systems:** Jira, Zammad
- **SOC Operations:** Log Analysis, Alert Monitoring, Alert Triage, IOC Hunting
- **Security Tools:** Wireshark, Nmap, YARA, Netwrix
- **Networking Fundamentals:** TCP/IP, DNS, DHCP, OSI Model
- **Operating Systems:** Windows, Linux (Ubuntu)

Certifications

- **Security Engineer Certificate (Top 5%, Professional)** – Pro5.ai
- **Cybersecurity and Privacy** – NPTEL
- **Linux Foundation Certified System Administrator (LFCS)** – KodeKloud

Education

- **M.Sc. Cybersecurity**, Bharathiar University 2023 – 2025
- **B.Sc. Physics**, PGP College of Arts and Science 2020 – 2023

Projects

CVE-Insight – Vulnerability Detection *(Python, Flask, HTML, NVD 2024)*

- Developed a web-based tool using Flask to analyze the NVD 2024 CVE dataset, enabling efficient vulnerability classification and aiding SOC monitoring operations.
- Automated the generation of detailed PDF reports to support vulnerability documentation and incident response workflows.

Achievements

- **Bugcrowd Hall of Fame:** Reported valid vulnerabilities to organizations like NFL and Air Canada.
- **CTF Participation:** Led **H4x0r_Hunters** (40th in India – CTFtime), ranked Top 4 on **TryHackMe**, and completed 30+ investigations on **BTLO**, focusing on incident response, log analysis, and threat hunting.
- Participated in **TCS HackQuest Season 9 (Round 1)** and **Pentathon CTF**, **Payatu Hiring CTF** gaining hands-on cybersecurity experience.