Raj M. Konkar

Leeds, UK | **+44 7774 738050** | **mailto:konkarraj1234@gmail.com**

LinkedIn: **https://www.linkedin.com/in/raj-konkar-b70b512a0/** | GitHub: **https://github.com/rajkonkar**

Professional Summary

Cybersecurity professional with an MSc in Cybersecurity from the University of York, experienced in SIEM monitoring, intrusion detection, incident triage, and threat hunting across Linux, Windows, and cloud environments. Skilled in analyzing attack chains, reducing false positives, and building SOC labs and security scripts. Pursuing CompTIA Security+ and Google Cybersecurity Certificate to further strengthen incident response expertise.

Core Skills

SOC Operations: Wazuh, Splunk, SOAR Playbooks | Threat Hunting: MITRE ATT&CK, KQL, Log Analysis

Security Tools: Wireshark, Nmap, Metasploit, Burp Suite | Scripting: Python, Bash

Systems/Cloud: Linux, Windows Server, SQL, Azure (fundamentals), AWS basics | Frameworks: Incident Response, NIST CSF, Forensics

Professional Experience

Technical Support Engineer | Karix – Mumbai, India | Jul 2022 – Mar 2023

- Resolved 200+ Linux/SQL incidents, reducing escalations by 30% through effective root-cause analysis.
- Performed log analysis and troubleshooting, reducing mean-time-to-resolution by 40%.
- Monitored Linux servers and SQL databases, improving uptime by 90%.
- Authored documentation that enhanced team knowledge-sharing and support efficiency.

Cybersecurity Projects

- **Wazuh SIEM Lab** – Simulated intrusions, triaged alerts, and tuned rules to reduce false positives.
- **Threat Hunting Scripts** – Python/Bash tools to detect anomalies and privilege escalations, mapped to MITRE ATT&CK.
- **GitHub Tools Repo** – Published reusable scripts for system audits, log monitoring, and alerts.

Education

MSc Cybersecurity | University of York | 2023–2024 | Completed

Certifications

Pursuing: CompTIA Security+, Google Cybersecurity Certificate | Completed: Ethical Hacking (Udemy), Network Security (Udemy)