P IMRAN ALI KHAN
SOC Analyst | Security Operations | Threat Hunting
Chennai, Tamil Nadu | +91 77999 49992 | imranalikhanmay27@gmail.com

PROFESSIONAL SUMMARY

Results-driven **SOC Analyst** with hands-on experience in **threat hunting, security incident monitoring, and log analysis**. Proficient in **FortiSIEM, FortiSOAR, and ServiceNow**, with expertise in **incident response, the MITRE ATT&CK framework, and rule fine-tuning**. Strong analytical skills with a passion for cybersecurity and proactive defense strategies. Certified in **CEH v13 & AWS Cloud Practitioner**. Adept at enhancing security operations through real-time monitoring and risk mitigation. Seeking to leverage expertise in **security operations and threat intelligence** to strengthen organizational security frameworks.

PROFESSIONAL EXPERIENCE

Sify Technologies Limited | Chennai, Tamil Nadu

SOC Analyst L1 | 09/2024 – Present

- Conduct **24/7 real-time monitoring** and analysis of security incidents.
- Serve as the **Single Point of Contact (SPOC)** for customers, ensuring timely response and resolution.
- Perform **in-depth raw log analysis**, escalate security incidents, and recommend remediation steps.
- Optimize security rules by **reducing false positives**, improving detection accuracy.
- Lead **threat hunting** initiatives using external TIPs (VirusTotal, AbuseIPDB, FortiGuard) to detect malicious entities.
- Develop **custom security dashboards** in FortiSIEM for efficient log source monitoring.
- Align incident response strategies with the **MITRE ATT&CK framework**.
- Ensure the **health and performance** of FortiSIEM components (collectors, workers, supervisors).
- Monitor **SOAR playbooks** for automated security incident handling.

Key Achievements:

- Strengthened security posture by integrating **advanced threat intelligence tools** into daily operations.

Sify Technologies Limited | Chennai, Tamil Nadu

SOC Analyst Trainee | **09/2023 – 09/2024**

- Gained hands-on experience in **FortiSIEM-based security monitoring**.
- Trained in **ServiceNow ITSM tool** for incident tracking and resolution.
- Assisted in investigating **real-world security incidents** to enhance threat analysis skills.
- Developed **strong knowledge of network security and cryptographic principles**.
- Achieved **top performer** recognition within the trainee batch due to outstanding analytical skills and initiative.

EDUCATION

- **B.Tech – Computer Science & Engineering** | K.V. Subba Reddy Institute of Technology, Kurnool
- **Diploma – Computer Science & Engineering** | Govt Polytechnic for Minorities College, Kurnool
- **SSC** | Govt Town Model School, Kurnool

TECHNICAL SKILLS

- **Security Tools:** FortiSIEM, FortiSOAR
- **Ticketing Tools:** ServiceNow
- **Core Competencies:** Incident Response, Log Analysis, Threat Intelligence, MITRE ATT&CK, Rule Fine-Tuning, Threat Hunting, Network Security, Security Automation

CERTIFICATIONS

- **Certified Ethical Hacker (CEH v13)** – EC Council
- **AWS Certified Cloud Practitioner**

LANGUAGES

- **English** (Fluent) | **Hindi** (Fluent) | **Telugu** (Fluent)