GURUKIRAN NAGARAJ

SOC ANALYST

+91 8197816440 | Gurukiran.r.nagaraj@gmail.com

CAREER SUMMARY:

Cybersecurity professional with **2.5 years of experience in SIEM (QRadar)** and incident management. Skilled in threat detection, incident response, and vulnerability assessments to enhance security posture. Strong analytical, teamwork, and communication skills, with a proven track record of reducing security incidents and improving system defenses.

EDUCATION:

Electrical and Electronics Engineering. (BE-EEE).

S.G Balekundri institute of technology - Belagavi. Karnataka **(Aug 2016-Aug 2020)**

TECHNICAL SKILLS:

- IBM QRadar
- Security monitoring
- SOAR
- VirusTotal
- Izoolabs
- Qualys
- Symantec EDR
- Recorded Future
- IOC's
- Malware analysis
- Cloud security
- Phishing Analysis

EXPERIENCE:

Deloitte India LLP. Thane, Mumbai | SOC Analyst L1 (Consultant) **(Oct 2023 to Nov 2024)**

- Monitored security alerts generated by **SIEM (QRadar)** and analyzed them using run-books and various security tools.
- Investigated QRadar alerts, identified potential threats, and escalated true positives to the respective team in SOAR for incident response.
- Assisted in **root cause analysis (RCA)** of security incidents and collaborated with the Incident Management team for resolution and closure.
- Supported the L2 team in generating and reviewing **weekly security** reports.
- Documented all analyzed alerts for **future reference** and compliance.
- Hands-on experience with security solutions including **Antivirus**, **Firewall**, **IPS**, **Proxy**, and **WAF**.
- Drafted and maintained **shift handover reports** for next shift persons.

Crystal Solutions Ltd, Mumbai | SOC Analyst L1 **(May 2022 to oct 2023)**

- Real-time monitoring of security alerts and events using IBM QRadar, conducting initial investigations within SLA.
- Analyzed alerts using tools and databases like **VirusTotal** and **AbuseIP**.
- Identified false positives and escalated **true positives** to senior analysts for further action.
- Documented incident details, **investigation findings**, and response actions for reporting and future reference.
- Collaborated with IT and security teams to resolve incidents and implement **preventive measures** to enhance system security.

CERTIFICATION:

- Foundations of Operationalizing MITRE ATT&CK.