# Tirumani Kumaraswamy

Security Analyst

✉ tkumar.infosec@gmail.com ☎ +91-9491704221

H-No. 2-133/3/A, Sai Ram Homes, Gurramguda, Hyderabad, Telangana, Pin Code - 501510.

16/07/1995 Indian Male

## Profile

Dedicated and skilled Security Operations Center (SOC) Analyst with over 4 years of experience in vulnerability management, threat detection, and incident response. Proven expertise in identifying, evaluating, and mitigating security risks in complex IT environments. Adept at utilizing security tools, conducting vulnerability assessments, and implementing effective security measures to protect sensitive data and infrastructure.

## Tools & Technologies

- **SIEM (Log Analysis):** Splunk, IBM Qradar, Alien Vault USM, ArcSight ESM
- **End Point Security & EDR:** McAfee
- **OSINT:** Virus Total, Hybrid Analysis, IPVoid, AnyRun, URLScan
- **Incident Management:** ServiceNow
- **Web Filtering:** Zscaler ZIA
- **Incident Response Management**
- **Vulnerability & Patch Management:** Rapid 7 IVM
- **Security Incident Monitoring and Analysis**
- **Threat Detection and Response**
- **Threat Hunting & Analysis**
- **Incident Response & Threat Mitigation**

## Education

**Master of Business Administration,** Osmania University 07/2015 – 08/2017 | Hyderabad

## Languages

English | Hindi | Telugu

## Certificates

- Certified Ethical Hacker V9
- Azure Fundamentals (AZ 900)

## Interests

- Playing Cricket
- learning on new skills
- Watching Movies
- Reading blogs for new articles on Security

## Professional Experience

**M3 Solutions Private Limited,** Security Analyst 05/2024 – present | Hyderabad, India

- Monitored and analyzed security events using QRadar SIEM tool.
- Investigated security incidents, performed root cause analysis, and implemented remediation measures.
- Responded to real-time security alerts and escalated incidents as necessary.
- Conducted threat intelligence research to enhance incident response.
- Performed vulnerability assessments and recommended security improvements.
- Created and updated security documentation and incident reports.
- Collaborated with IT and security teams to enhance cybersecurity posture.
- Managed regular vulnerability scans on internal and external assets.
- Assisted in prompt deployment of security patches to reduce risks.
- Contributed to a security audit, mitigating 50+ vulnerabilities.
- Developed a vulnerability prioritization process, reducing remediation backlog by 30%.

**KPMG,** Security Analyst 05/2023 – 05/2024 | Bangalore, India

- Managed client security using SIEM tools (AlienVault USM, Splunk).
- Investigated and escalated incidents (Login Failures, Malware, Phishing, DOS/DDOS).
- Analyzed threats and vulnerabilities using intelligence sources.
- Collaborated with teams to mitigate breaches and minimize impact.
- Developed and maintained incident response procedures and playbooks.
- Deployed NXLog agents and ran vulnerability scans.
- Coordinated patch management and remediation efforts.
- Generated reports and ensured compliance with NIST, PCI-DSS.
- Handled quality calls, escalating as per SLA.
- Conducted health checks on security sensors.
- Reduced false positives with suppression rules.
- Prepared shift handover reports and shared knowledge with team.

**Insta Global Source Pvt Ltd,** Security Analyst 03/2021 – 04/2023 | Hyderabad, India

- Monitored security events and alerts using ArcSight ESM in a 24x7 SOC environment.
- Analyzed network traffic and log data to detect threats and malicious activity.
- Monitored IDS/IPS, firewalls, and endpoint security alerts.
- Investigated incidents, performed root cause analysis, and recommended mitigation actions.
- Troubleshot critical log sources to ensure proper SIEM reporting.
- Created ArcSight content (dashboards, filters, reports, queries).
- Coordinated with incident response teams to contain breaches.
- Developed and maintained SOC documentation (SOPs, incident response plans).
- Trained junior analysts on security tools and procedures.
- Conducted security audits to identify gaps and enhance threat detection.
- Supported vulnerability management by identifying and prioritizing risks.

## Declaration

I hereby declare that the information furnished above is true to the best of my knowledge and if selected, would put in my best efforts for the growth of the organization.

**Kumaraswamy**
Hyderabad