

# Mallikarjun Katti

## Cybersecurity Analyst

✉ mallikarjunkattiz9@gmail.com ☎ 8304028143 📍 Bangalore

🌐 [linkedin.com/in/mallikarjun-katti-665849206](https://www.linkedin.com/in/mallikarjun-katti-665849206)

### PROFILE

Growing Cyber-Security Analyst with over one year of industry experience, possessing specialized knowledge in MSSP deployment and SOC strategies. I am an energetic, self-motivated L1 Analyst with a strong passion for cybersecurity. Continuously learning and eager to tackle new challenges, I have a deep understanding of the importance of the CIA triad.

### EDUCATION

<b>Bachelor of Engineering - (BE)</b> <i>Shetty Institute of Technology</i>	08/2016 – 09/2020 Kalaburgi, Karnataka, India
<b>XIIth PUC - (Science)</b> <i>R D Patil P U College</i>	04/2014 – 05/2016 Sindagi, Karnataka, India
<b>Xth</b> <i>Sri Morarji Desai Residential School</i>	04/2015 – 04/2016 Bengaluru, Karnataka, India

### PROFESSIONAL EXPERIENCE

<b>Cybersecurity Analyst</b> <i>Soffit Infrastructure Services (P) Ltd</i>	11/2023 – 12/2024 Kochi, Kerala, India
---	---

I am currently working as a Cyber security Analyst at Soffit Infrastructure Services Limited. My organization uses the WAZUH SIEM tool, which is an open-source security platform.

In my role, I am responsible for continuous monitoring, checking the dashboard for abnormal spikes, such as any increase or drop in traffic, and analyzing triggered alerts. If the alerts are true positives, I raise tickets using the Jira ticketing tool. I also analyze the flow of these incidents and discuss them with our L2 engineers, depending on the incident. Additionally, I create new alerts, generate dashboard reports, and occasionally work with other stakeholders. That's all about my role. Thank you.

### SKILLS

<b>Network Operation Center- (NOC)</b> Good Knowledge of Network Concepts:-Sophos Firewall, OSI Model, NAT, PAT, Ports & Protocols	<b>Cyber-Security Analyst</b> SIEM Architecture, Splunk Tool, Wazhu Tool, Microsoft Sentinel, Seceon, EDR, Microsoft Defender, Bit-defender, CrowdStrike Falcon, Incident-LifeCycle, LogAnalysis, Active Directory, Security Monitoring, IDS/IPS, SOAR, Play-book, Threat Intelligence, DLP, Basic-Pen Testing
<b>IT-Infrastructure</b> OS, Virtual Box, Linux - Kali, Ubuntu, Red-Hatlinux	

## CERTIFICATES

---

### Technical Introduction to Cybersecurity

FORTINET Training Insitute

### Introduction to the Threat Landscape

FORTINET Training Insitute

### Networking, LINUX, CEH

Blue Shell Technologies

### PHP Developer

Hudson Agile Ventures Pvt Ltd

### Introduction to CISSP Security Assessment & Testing Security Opertion

Simpli-learn Skillup

## LANGUAGES

---

English



Hindi



Kannada



Telugu

