# Babu Rasheed S

**Cyber Security Specialist**

## PERSONAL INFORMATION


**Email**
babu.rasheed73@gmail.com

**Mobile**
(+91) 9663310197


**Total work experience**
17 Years 5 Months

## KEY SKILLS

malware analysis

vulnerability assessment

digital forensics

vulnerability management

threat intelligence & threat hunting

siem

security incident response lead

order management

it support

Effective Team Management

## OTHER PERSONAL DETAILS

| | |
|---|---|
| **City** | Coimbatore |
| **Country** | India |

## LANGUAGES

## PROFILE SUMMARY

With over 17+ years of experience, I am a results-driven cybersecurity professional for last 13+ years, specializing in information security consulting, threat intelligence, and technical leadership. My expertise lies in managing Security Operations Centres (SOCs), implementing effective security solutions, and providing strategic guidance to enhance organizational security posture. My background also includes 4 years of experience in IT support and order management. I am now seeking to leverage my proven track record and expertise to add value in a cyber security role, where I can contribute significantly.

## EDUCATION

**2012**
PG Diploma
**Appin Technologies Lab**

**2007**
B.Sc
**Bhartiyar University, Coimbatore**

**2004**
XIIth
**English**

**2002**
Xth
**English**

## WORK EXPERIENCE

**Jul 2024 - Jan 2025**
Cyber Security Specialist
**Banan Technologies**

- Conducted cyber security assessment on various cyber crime platforms
- Prepared and implemented Data Centre planning for Cyber Security and Network Devices
- Monitored and analysed on Cyber Threat intelligence day to day.

**Mar 2023 - Apr 2024**
Information Security Consultant
**Versos**

Working as a part of cyber Defense team as Threat intelligence consultant, Incident Response, Threat Hunter, SIEM Advisor on Financial sector.

**Dec 2022 - Feb 2023**
Senior SOC Analyst
**Halian**

Worked as part of SOC team as Senior analyst, need to

- Tamil
- Urdu
- English
- Hindi
- Arabic

monitor Multiple client networks with different SIEM tools and investigate the trigged security alerts to make sure it s just operational traffic or False positive or True positive and take action. If any FP need to review and move it to SIEM Admin team for Fine tuning and worked on part of Threat Intelligence team as well.

Jun 2020 - Nov 2022

MSSP SOC Lead

### Netenrich Technologies

Responsible for L2/L3 Incident Response activities and team Management and Responsible for Threat Intelligence feeds and Advisories and Use-case fine tuning to increase Threat Detection capabilities,etc..

Nov 2019 - Apr 2020

Senior IT Security Specialist

### Raksys India LLP

• Providing Security Consulting for complete Client Environment • Recommendations for Security Incidents to prevent from future Threats • SIEM Assessment done and improved usage of SIEM. • Managing and administrating QRadar, Qualys's Guard, Manging SOC team, Web Application Portals • Providing Threat Intelligence Advisories with Prevention Recommendations

Jul 2018 - Nov 2019

Senior Security Analyst

### GBM

A dedicated SECURITY PROFESSIONAL/TECHNOLOGIST with 12+ years of technology development, IT Security, integration, deployment, and management experience, is seeking a position within an aggressively managed organization that can effectively utilize a self-motivated individual, offering proven technical skills in the field of Information Security. I also have expertise in information security, project coordination, determination of scope and priority, project implementation, and training/development of IT staff.

Oct 2017 - May 2018

Associate Consultant Security Intelligence Analytics

### Wipro Technologies

• Worked as part of cybersecurity and risk services team member for multiple projects. • Identifying which ones might be problematic, as well as determining if mission-critical systems are at risk and providing solutions to Mitigate the Risk • Implemented the QRadar SIEM for one of client.

Jun 2017 - Sep 2017

Information Security Consultant

### Versos

Architected and administrated Splunk and Nexpose , Technical Consultant for SIEM Operation and Security Operation Centre ,Lead the Threat intel, Malware Analysis team and provided high level technical support for threat analysis

Dec 2014 - May 2017

Senior Technical Lead

### HAPPIEST MINDS TECHNOLOGIES

• Technical Lead for SIEM Operation and Security Operation Centre • Worked as part of Threat Hunting Analyst. • Uncovering the sophisticated problems by picking up on subtle anomalies • Identified and analysed threats from different threat intel's and altered relevant alerts

Nov 2013 - Nov 2014

Associate Operations Manager

### Cognizant Technologies Solutions

• SOC Solution Architect, Designing, Implementing RSA Envision, McAfee Nitro, IBM Qradar, Setup along with Administrations & Deliverables • Owing day to day activities from SOC prospective • Managing SIEM Operation and Security Operation Centre activities. • Managing Cisco ASA FW for IOC blocking and Fine tuning. • Lead the Threat intel team and provided high level technical support for threat analysis • Recommended pro-active controls for prevailing threats based on analysed threat feeds and Risks in Environment.

Jun 2012 - Oct 2013

System Engineer

### Tata Consultancy Services

• SIEM (Security Incident and Event Management) and Security Product Support Protection Services – Retail Clients across Globe -IT (On Going) at TCS • Providing Tier 4 Support for the customer. Responsible for handling Security Incident and Event management. • owing day to day activities from SOC prospective • Doing Malware Analysis in Cuckoo Sandbox. Worked on Forensic Analysis on SIFT for Linux.

May 2007 - May 2012

Process Specialist

### Infosys

• Provide high-level support to end users for their virus issues • Remote infrastructure management (Wintel) • Analysing Events generated from HIPS, IDS, firewall, windows security events, and antivirus alerts. • Worked as part of order mamgement team as SME

## COURSES & CERTIFICATIONS

- Certified Ethical Hacker
- McAfee certified Product specialist in SIEM
- ITIL
- Certified Threat Intelligence Analyst
- Certified Threat Intelligence Analyst