

Ramireddy BharathSimhaReddy

+ Railway kodur #Ramireddybharathsimhareddy@gmail.com „ +91 6305470581

ø Bharathsimha

Career Objective

Eager to apply my knowledge of network security, threat analysis, and incident response in a dynamic environment. Seeking an entry-level Cyber Security Analyst position to contribute to safeguarding digital assets and enhancing the organization's security posture

To obtain a good position in an organization where I could get enough opportunity to prove my potential and commitment

Self- Competencies

-
- Aiming at excellence in work through Self Motivated.
 - Professional attitude towards discipline and punctuality.
 - An active participate of sports events.
 - Team approach to meet challenges
 - Innovative attitude to problem solving.
 - Enthusiast of task achievement

Education

YOGI VEMUNA UNIVERSITY

Dec 2021 – Aug 2024

- Sri VASISTA degree college
- B.sc in Computer Science
- SGPA: 7.5

BOARD OF INTERMEDIATE EDUCATION, AP

mar 2019 – may2021

- Sri Sai ram junior college
- M.P.C
- GPA: 6.5

BOARD OF SECONDARY EDUCATION, AP

mar 2018 - may2019

- Sri THULASI Educational academy
- GPA: 8.8

Certifications & Training

- Cyber Defense Tools training:

Hands on experience with SIEM, EDR, and threat intelligence platforms

- **Incident Response & Mitigation:**

Practical understanding of handling security incident

Projects

- **Incident Response Simulation:**

*Simulated real world incident handling using Splunk and Microsoft Defender.

*Applied security protocols to detect and mitigate threats.

- * **Vulnerability Assessment Report:**

*Conducted Vulnerability scans using Nessus

*Identified and document security gaps with recommended fixes.

Power skills

CYBER SECURITY SIEM: azure Sentinel, Splunk.

EMAIL SECURITY AND PROTECTION: Proof Point, Cisco Iron Port, Microsoft 365

ENDPOINT SECURITY: Microsoft Office 365, Cisco Amp, Microsoft defender, Falcon Crowstrike

VULNERABILITY ASSESSMENT: Nessus, qualys tool, Open VAS

TICKETING SECURITY SKILLS: Cyber Kill Chain, Incident response Life cycle

TOOLS: Microsoft Dynamic, JIAR and service now

OTHER MONITORING TOOLS: Virus total, Abuse IPDB, IP Void, URL void

Languages

- English (Fluent)
- Telugu (native)