RESUME

Rajendra Dundannanavar

MOBILE: +91-**9591316940**

E-Mail: Ndrajendra04@gmail.com

Present Address:
#F-02, Venky PG Sector-19 Airoli.
New Mumbai 400708.

Permanent address:
#209 S/o Nagappa Dunadannanavar
Atpo- Balambeed 581101
Tq- Hanagal
Di-Haveri
Karnataka

Personal Data:

Date of Birth	: 04th Nov 1988
Sex	: MALE
Nationality	:INDIAN
Marital Status	: Married

Languages Known:

- English
- Hindi
- Kannada

Strengths:

- Good Listener & Quick learner.
- Strong Technical and Analytical Skills.
- Hard working nature.
  Confident and determined.

Objective:

To achieve success in a challenging environment where my analytical and problem- solving skills can be suitably applied for the growth of my organization which in turn is my growth.

Academic Credentials:

- BE in Electronics & Communication Engineering, AGMR College of Engineering Varur Hubballi (Visvesvaraya Technological University (VTU), Belgaum) in 2016.
- Diploma from Cauvery Polytechnic, Gonikoppal S.kodagu (Dept. of Technical Education, Karnataka) in 2011.
- SSLC from S. S High School, Balambeed (Karnataka Secondary Education) in 2005.

Key Skills:

- IBM Q Radar SIEM
- IBM IPS
- Check Point Firewall
- Phishing/Spam Mail analysis
- DLP (Force Point)
- SMax (Ticketing tool)
- Win collect Troubleshooting’s

Work Experience:

IBM India Pvt Ltd with the Payroll Kwick Box solutions Pvt Ltd.
Work Experience: 0.9 Years (26th july 2021 to till date)
Project: Bank of Baroda Bank
Role: SOC Analyst

Janu's software Pvt Ltd, Chennai.
Work Experience: 1.6 Years (Feb 24th to 23rd July 2021).
Role: SOC Analyst

- RELEVANT EXPERIENCE:2.3 Year
- CURRENT CTC: 3.6 LAKH PER ANNUM
- CURRENT COMPANY: **IBM client Bank of Baroda.**
- NOTICE PERIOD: 30 DAYS
- FLEXIBLE WITH ROTATIONAL SHIFTS

Role and Responsibilities:

- Investigating security threats using SIEM (QRadar) tool, raising incidents and providing recommendation steps for resolution of such issues to the concerned teams.
- Monitoring logs of Windows and Linux Servers, security devices (IPS, IDS and Firewall) and detecting suspicious/malicious activities, Viruses, Worms and Trojans found on customer network.
- Analysis of Phishing/Spam mail reported by the users.
- Performing administrative tasks like health monitoring of SIEM tool.
- Preparing the monthly as well as weekly analysis report after analyzing the customer network for attacks and intrusion after segregation of false positives from the vast number of events detected by various devices.
- Coordinating with security incident handling team (onsite projects team) in providing assistance during investigation and providing any technical escalations if necessary.
- Interaction with the process owners to understand the nature of business, the controls and possible risk.

Declaration:

I hereby declare that information furnished above is true to the best of my knowledge.

Place: Mumbai (Rajendra Dundannanavar)
Date: