Yasaswi Gowd **Email:** gowdyasaswi@gmail.com

Contact: 9491666582

Professional Summary:

- Over all 3.3 years of experience in Information Technology.
- Having 3.3 years relevant experience in Information Security and currently working as Security Analyst (**Security Operation Centre team**)
- Hands on experience on Threat analysis and **Security Monitoring and Operation.**
- Experience on **SIEM (Security Information and Event Management) tools** like Monitoring real-time events using Microsoft **Azure sentinel** tool, **IBM Q radar**
- Creating the tickets in Service now and CRM Ticketing tool
- Understanding the incident based on to determine whether it's false or true positive.
- Preparing **daily, weekly and monthly report** as per client requirement.
- Experience on performing log analysis and analysing the crucial alerts at immediate basis.
- Filling the Daily health checklist.
- Security Incident Response and closure of Incidents within SLA using Service Now
- Analysing **Phishing** and Spam related activities and notifying to the users.
- Monitoring and carrying out second level analysis incidents.

Technical Certifications:

- Certified CEH
- Azure AZ-500
- Certified DIGITAL SECURITY FUNDAMENTALS
- Certified CISSP
- Certified CCNA

Technical Skills:

- **SOC** (Security Operation Centre)
- **SIEM** (Security Information and Event Management) Tool: **Microsoft Azure sentinel, IBM QRadar**
- Vulnerability Assessment
- Phishing Email Analysis

Education:

- Completed my graduation in Acharya Nagarjuna University (B.Sc Computers) in 2021.

Work Experience:

- Currently working as **Security Analyst** with **DXC Technology** from Jan - 2022 to Till Date.

Professional Experience:
Company: DXC Technology
Project: Capital One
Role: Information Security Analyst

Description: DXC Technology is a leading global technology services and solutions provider, led by business and Technology Consulting. The company provides technology solutions and services to enterprises across industries such as Banking & Financial Services, Healthcare, Manufacturing, Consumer goods, Travel and Hospitality, through a combination of traditional and newer business models, as a long-term sustainable partner.

Responsibilities:

- Working in Security Operation Center (24x7), monitoring of SOC events, detecting and preventing the Intrusion attempts.
- Responding to various security alerts for various client and scanning for vulnerabilities using tools like NESSUS.
- Monitoring real-time events using SIEM tools like Azure sentinel and IBM Qradar
- Monitoring, analysing and responding to infrastructure threats and vulnerabilities.
- Ad hoc report for various event sources customized reports and scheduled reports as per requirements.
- Collecting the logs of all the network devices and analyse the logs to find the suspicious activities.
- Investigate the security logs, mitigation strategies and responsible for preparing generic security incident reports.
- Responsible to preparing the root cause analysis reports based on the analysis.
- Analysing daily, weekly and monthly reports.
- Creating case for the suspicious issue and forwarding it to Onsite SOC team for further investigation.
- Creating the tickets in ticketing tool.

Trainings Attended:

- ServiceNow Ticketing Tool
- Splunk SIEM
- Rapid7/NexPoseMetaSploit Vulnerability Assessment

Self-Appraisal:

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

Yasaswi Gowd