

AAKANKSHA

Mob. No: +91-7061692655

Email id: aakankshakumari296@gmail.com

Linked-in profile link: [linkedin.com/in/akanksha-kumari-44432b356](https://www.linkedin.com/in/akanksha-kumari-44432b356)

PROFESSIONAL SUMMARY

Immediate Joiner **SOC Analyst** with 2 years of experience in **monitoring, analyzing, and responding to security incidents**. Proficient in **SIEM tools (QRadar, Splunk), incident response, log analysis, phishing investigation, and threat hunting**. Adept at **analyzing phishing and spam emails**, performing **log analysis**, and managing crucial alerts. Skilled in identifying **false positives**, fine-tuning alerts, and escalating **security events**.

PROFESSIONAL WORK EXPERIENCE

**Innova Solutions - Senior Associate** Bangalore - 24<sup>th</sup> Jun 2024 - Present  
**Roles & Responsibilities:**

- **SOC Analyst** (L1) with 10 months of experience in **monitoring, analyzing, and responding to security incidents**.
- Proficient in using **SIEM tools (Splunk)** for **event correlation** and **incident detection**.
- Skilled in **incident response, log analysis, phishing investigation, and threat hunting**.
- Experienced in **analyzing phishing and spam emails**, performing **real-time log analysis**, and managing **security alerts**.
- Conducts regular **health checks** to ensure system stability and adept at identifying and resolving **false positives**.
- Demonstrated ability to escalate **critical security events** and provide timely support in a fast-paced, high-pressure environment.

**Experis - IT Recruiter and SOC L1** Bangalore – 12<sup>th</sup> Dec 2022 - 11<sup>th</sup> June 2024  
**Roles & Responsibilities:**

- **SOC Analyst** (L1) with 1 year of experience in **monitoring, analyzing, and responding to security incidents**.
- Transitioned from **recruiter** to **Cybersecurity Analyst**, gaining hands-on experience with **SIEM tools (QRadar)** and **EDR tools**.
- Provided **24x7 operational support**, continuously monitoring **security events** and **incidents**.
- Performed **real-time monitoring, investigation, analysis, and reporting of security events** from multiple **log sources**.
- Managed **escalations** and **incident response**, ensuring timely resolution and accurate documentation of **security incidents**.
- Conducted daily reporting of previous shift handover, **IOC sharing**, and breakdown of received alerts to ensure smooth communication across teams.
- Utilized **SIEM tools (QRadar)** and **EDR platforms** to analyze **security events**, perform **threat hunting**, and identify potential **vulnerabilities**.
- Actively worked on **phishing investigations**, analyzing **spam emails**, and resolving **false positives**, fine-tuning alerts to improve system efficiency.

**Intone Networks - Recruiter** Noida - Aug 2022 - Dec 2022  
**Esolutions - IT Recruiter** Noida - Sep 2021 – Aug 2022

SKILLS

- Soc Analyst
- Siem
- Soc
- Edr
- Incident Response
- Security Operations
- Qradar
- Endpoint Security
- Security Operations Center
- Splunk
- Triage
- Phishing
- Malware Analysis
- Log Analysis

EDUCATION

**Degree:** B.COM (Bachelors in Commerce)  
**University:** Gossner College Ranchi University - 2019

PERSONAL DETAILS

**Date of Birth:** 01<sup>st</sup> Oct 1998  
**Languages Known:** English, Hindi  
**Address:** Govindpur Dhanbad Jharkhand

DECLERATION

I hereby declare that the above-mentioned details are true and correct to the best of my knowledge and belief

Date: 19<sup>th</sup> March 2025  
Place: Bangalore Aakanksha