

B. Krishna Badri
Soc Analyst
krishnabadrisc@gmail.com
+91-9398645028

Experience Summary:

- Having 3 years of experience in **Cyber Security Operations (SIEM)**.
- Having great exposure on complete incident management Life cycle & Having hands on experience in SOC incident response.
- Exposure on **Defender** for Investigating, Blocking IP's, Hashes and Domains.
- Experience in SOC Monitoring and Incident Response.
- Working on Microsoft **Azure sentinel and Sumo Logic** SIEM tools .
- Creating the tickets in ticketing tool.
- Preparing daily, weekly and monthly **Reports** as per client requirements.
- Malware analysis and investigation on **Phishing/Spam Emails**.
- Worked with core teams to investigate the false and true positive alerts.
- Responsible for following all the steps in **Incident Response Process**.
- Working on Azure sentinel dashboards by collecting IOC things to determine True positive or False Positives.

Certifications:

Certification Name	Certifying Authority
NSE1 & NSE2	Fortinet

Technical Skills:

- Microsoft Sentinel SIEM- Sentinel & Splunk Incident Response
- Microsoft Defender
- CrowdStrike

- Email Security
- SOAR
- Cyber Kill Chain
- ITSM
- Security Operations

Professional Experience:

S.No	Company	Role	Start From
1	HCL Technologies	Soc Analyst	Nov 2020 to March 2024
2	Inspira Enterprise	Soc Analyst M1	March 2024 to till date

Projects Profile:

Environment: Azure Sentinel

Role: Soc Analyst

- Monitoring, analysing the events in SIEM and creating a triage report for the investigation with all the necessary details. Adhering to the process defined by client and escalating the case.
- Creating the tickets in ticketing tool.
- Monitoring and identify positive security events from Microsoft Azure sentinel dashboard, Orion during the shift hours and take necessary action for the critical events that is seen during each shift's hours with deviations for all the environments that we support.
- Understanding the incident based on to determine whether it's false or true positive.
- Following end to end Incident Investigation and Incident Response process, ensuring to Acknowledge and close the investigation within defined SLA.
- Supporting Cyber Security solutions SIEM like Azure sentinel

- Worked as a Security Analyst for SOC 24*7 environment
- Blocking IP's, Hashes and Domains as instructed by client and Running Device scan Whenever needed
- Performs security monitoring, security and data/logs analysis, and forensic analysis, to detect security incidents, and mounts incident response.
- Investigating CrowdStrike Alerts and preparing proper Analysis and closures to meet the Client Requirement and Run scans on Device whenever needed.

Educational Qualification:

- **B.sc(Computers)** in the year 2020 under SKU university , Anantapur.

Key Strengths:

- Self-Motivated, Excellent Time-Management.
- Excellent Interpersonal Skills, positive attitude.
- Good communication, convincing abilities and negotiation skills.

Achievements: Languages Known

- Won prizes by participating in sports activities.
- Also participated in various cultural and social activities alone as well as in groups throughout my educational career.

Personal Details:

Name: B. Krishna Badri

Father Name: B. Raja Gopala Rao

Languages Known: English, Telugu, Kannada, Hindi

D. O.B: 02/02/2000

Mobile- 9398645028

Declaration:

I hereby declare that statements made are true and correct to the best of my knowledge and belief.

Date:

B. Krishna Badri