YASHES GN

Security analyst

Email: yashes052@gmail.com
LinkedIn: www.linkedin.com/in/yashes-gn
Contact: 9535309120

CAREER OBJECTIVE

IT Security Professional with 2.7 years of experience in Security Operations. Good Understanding of Various SOC Processes like Monitoring, Analysis, Playbooks, Escalations and Cyber Attacks. Experience on working in MSSP. Seeking an Opportunity to join an organization that values innovation by utilizing my skillset in developing strategies for preventing cyber-attacks on corporate systems.

EDUCATIONAL QUALIFICATION

Education	Institution	Year of Passing
Bachelor of Engineering	GM Institute of Technology	2020

ORGANIZATIONAL EXPERIENCE

Organization	DESIGNATION	EXPERIENCE	YEAR
Network Intelligence Pvt. Ltd.	Cyber Security Analyst	2.7+ year	17/01/2022 – 08/10/2024

Current roles and responsibilities:

- Monitoring 24*7 SOC Operations Which Includes Detection, Tracking and Analyzing of Alerts & Incidents.
- Working in MSSP (Managed Security Service Provider) Environment.
- Acknowledging and closing false positives and raising incident for validated incidents.
- Analyzed System risk to identify and implement appropriate security countermeasures.
- Participating in SOC Meetings to discuss about the Alerts, Incidents.
- Deep dive analysis of triggered alerts using SIEM and other analysis tools and also planning, implementing, managing, monitoring and upgrading security measures for the protection of the organizations data, systems and networks.
- Have experience and expertise in Anomaly Detection.
- Performed investing action on phishing emails.
- Responsible for Security Monitoring, Detection, Response and Client Care.
- Preparing and Reviewing Weekly, Monthly, Quarterly reports and Presenting to Internal Senior Management & Clients.
- Prepared SOP and Fine-tune documents for the alert.
- Good Knowledge on XSOAR that how XSOAR automates response actions based on predefined playbooks or workflows. Scheduling the report on XSOAR.
- Presented Knowledge sharing session.
- Regularly Update with Latest Attacks, Threats and Social Engineering Techniques and Their Mitigations
- Drafting Shift Handovers.
- Good network knowledge, OSI layer, TCP/IP, Ports, DNS, DHCP etc.

- Regular review of process and support documentation and amend where necessary.
- Solution based on Information Technology Infrastructure Library (ITIL) best practices that focused on users, process, and technology perspectives of providing business solutions and Maintain SLA on Ticket

Tools and Technology:

- Office Productivity: World, Outlook, Excel, PowerPoint
- SIEM Tools : Qradar, LogRhythm, CY5 and ELK
- Ticketing Tools : Fresh service, Manage engine, service now and Jira
- Business Intelligence Tool : PowerBi
- Palo Alto Cortex XSOAR

Certifiation:

- **EC Council:** Certified Ethical Hacking
- **Palo Alto Cortex Xsoar Certifications.**

DECLARATION

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

Place: Bangalore **Yashes GN**