Anup Gavade

Cyber Security Analyst

Phone: +91-8618287474 | **G-Mail:** gavadeanup8@gmail.com

Linkedin: http://www.linkedin.com/in/anupgavade

Career Objective:

To build my career as a successful security analyst in a major global organization, where I can best utilize my skills to accomplish the organization's goals and objectives, at the same time get an opportunity to expand my knowledge.

Tools and Technologies:

- **SIEM:**
  i. LogRhytm.
  ii. IBM QRadar.
  iii. Azure Sentinel.
- **Endpoint Detection and Response-(EDR):**
  i. CrowdStrike Falcon.
  ii. MS 365 Defender.
  iii. Trend Micro
- **Ticketing tools:**
  i. My Shift.
  ii. ServiceNow.
- **Sandbox:**
  i. ANY.RUN

Work Experience:

Company Name: Cloud4C

Designation: Cyber Security Analyst – L1

(January 4th–2023 **to** till date)

Certifications:

- SOC Experts certified as Security Analyst.
- SPLUNK Fundamentals
- Comptia security +
- NSE 1 and NSE 2

Education:

Bachelor of Engineering in KLE

DR MS Sheshagiri Engineering

College With 7.0 (CGPA), Belagavi.

Summary:

- 2.+ years of the experience in Security OperaΘon Centre-(SOC). Hands on experience on SIEM tools like LogRhythm,

  Azure Sentinel, and IBM QRadar.
- Solid knowledge of network concepts: OSI Model, TCP/IP Model, DNS, DHCP, TCP, UDP and 3Way handshake etc.
- Familiar with the types of cyber attacks like Phishing, DOS/DDOS, Brute force attack, MITM, Sniffing etc.
- Analysing suspicious events and mitigation techniques for different types of cyber-attacks and malware analysis.
- Ability to perform detailed phishing analysis and malware analysis using ANY.RUN sandbox tool.
- Good understanding of various SOC process like monitoring, analysis, SLA's, client meetings and reports.
- Working knowledge on MS Word, MS Excel, and PowerPoint skills.
- Keeping updated with the latest developments in the cyber security landscape.

Roles and Responsibilities:

- 24*7 eyes on glass monitoring and analysis of the triggered alerts by using SOAR, Cortex XSOAR and SIEM: LogRhythm, Azure sentinel and IBM QRadar.
- Performing detailed analysis of phishing E-Mails using ANY.RUN sandbox tool and submit to cyber defence team for further action.
- Investigate and respond to alerts triggered by security control devices, including EDR and E-Mail gateway tools, ensuring shift and appropriate actions are taken.
- Identify the false positive and false negative cases with the help of standard procedures and open-source tools.
- Raising the tickets after analysis that includes all the information about the offence.
- Manage and provide security services to diverse clients in the Oil, Banking, and educational sectors within a managed security service provider-(MSSP) environment.
- Perform critical system monitoring tasks, including restarting collectors and system monitors reporting critical issues, ensuring the health of the security infrastructure.
- Handle floods i.e., multiple alerts triggered for the same use case, maintains composure and efficiency during high-pressure situations.
- Identification of incidents severity and responds according to the SLA's and coordinating with the internal and external stakeholders and resolution of security incidents and breaches.
- Contacting the customers directly in case of high priority incidents and helping the customers in the process of mitigating the attacks.
- Collaborate with the engineering team to implement whitelist conditions based on customer requests, contributing to tailored security solutions.
- Documentation of alerts and daily shift handover.
- Preparation of security incident reports on daily, weekly, and monthly basis for the records and further investigations.
- Willingness to work in any shifts in a job that involves 24*7 security

operation centre environment.