**Vamshi Krishna Amuda Email**: [Vamsikrishnaa2018@Outlook.com](mailto:Vamsikrishnaa2018@Outlook.com) **SOC Analyst Mobile**: +91-8374130190

**CAREER OBJECTIVE**

Detail-oriented and proactive Security Operations Center (SOC) Analyst with 3.5 years of experience in cybersecurity monitoring, incident response, and threat analysis. Proven track record of identifying, analyzing, and mitigating potential security threats while ensuring compliance with industry standards and regulations. Strong experience with SIEM tools, incident management, vulnerability management, and real-time security monitoring.

**PROFESSIONAL SUMMARY**

Company: IQVIA Consulting & Information Services India Private Limited (Mar 2022 to Feb 2023)

* SOC Analyst 1

**Company:** GlobalLogic Technologies Private Limited (July 2020 to Mar 2022)

* **Associate Analyst**

**Company:** SATRA INFRASTURCTURES MANAGENT SERVICES PVT LTD (Jan 2019 to Sep 2019)

* **Junior Software Engineer**

Overall, 3.5 years of experience In SOC. Supporting multiple Clients of various regions across the globe and played multiple roles and gained the career growth. L1 support on various security products like Splunk, Malware analysis, Proxy, Firewall, Email gateway, EDR, Phishing emails.

* **CERTIFICATIONS:**
* Certified Splunk Analyst
* Certified Cortex Xsoar Analyst
* Preparing for CEH
* Preparing for CISSP
* **TECHNICAL SKILLS:**
* **SIEM Tools**: Splunk, IBM QRadar, ArcSight, LogRhythm Rapid7, Microsoft Defender, SOAR
* **Incident Response**: Analysis, escalation, containment, and remediation of security incidents
* **Threat Hunting**: Proactive searching for potential threats within networks
* **Network Security**: Firewalls, VPNs, IDS/IPS systems, packet analysis
* **Operating Systems**: Windows, Linux, macOS
* **Security Standards & Frameworks**: NIST, ISO 27001, CIS Controls
* **Programming/Scripting**: Python, Bash, PowerShell
* **Vulnerability Management**: Vulnerability scanning tools (e.g., Nessus, Qualys)
* **Communication & Reporting**: Security incident reports, escalation procedures, and working with management teams
* **Reporting Tools** : Microsoft PowerBI , Excel

**Roles And Responsibilities Covered as Soc Analyst**

* **Technical – SIEM:**
* Having overall 3.5 years of experience in SIEM and expertise on SIEM products like Splunk, Qradar & Sumologic.
* Knowledge of **SIEM, EDR, IDS/IPS, security monitoring, and threat detection.**
* Real time monitoring and analyzing the security alerts triggered in SIEM and escalating the incidents to respective teams.
* Responsible for specialized investigation, threat analysis and remediation in response to notifications from operators
* Identifying machines infected with malware and issue remediation based on the investigation results
* Identifying miss configured policies and suggesting necessary changes
* Sharing the analyzed reports to client on daily, weekly, monthly basis for giving a better insight on network activities
* Raising of incidents and closure as per the SLA
* Adverse knowledge in Documentations – High Level and Low level. Initiated SOC Manual (Complete Inventory and Process Details) and SIEM Newsletter.
* **Operational:**
* Coordinating and managing review calls periodically [quarterly / monthly / weekly] with clients/onsite resources to enhance the process in place for proactive service
* Provide expert analysis to customer of events discovered by Analysts and track it until necessary Root cause is fixed
* Develop operational process and procedures to appropriately analyze, escalate and assist in remediation of critical information security incidents
* High level and low-level documentation for every process followed in team with flow diagrams
* Inventory document for every customer with all process, Escalation Matrix and SLA agreed.
* Part of Global SOC Team Handling clients across globe
* **EDUCATIONAL QUALIFICATION**
* Bachelor of Technology from Malla Reddy Engineering College, with 74% in the year 2018.
* **DECLARATION**
* I hereby declare that the information provided above is true and fair up to the best of my Knowledge.

Place: Hyderabad

Vamshi krishna A