T Mouni Suryanarayana

Email ID: surya.tsetty@gmail.com

Contact: +91- 8106621772

Professional Summary:

- A certified professional with 2.4 years of experience in Information Security as Senior Analyst
- Hands on experience with SIEM tool for logs monitoring and analysis on SOC (**Security Monitoring and Operation) and SIEM (Security Information and Event Management) tools** like monitoring real-time events using **IBM QRadar**.
- Knowledge on **Vulnerability Assessment (Nessus)**
- Knowledge on **SOAR (Resilient)**
- Good knowledge on networking concepts including OSI layers, subnet, TCP/IP, ports, DNS, DHCP, firewall monitoring.

Work History:

Currently working as Senior Analyst with (**Capgemini**) from April 2019 – Till Date
Company: Capgemini
Project: Security Monitoring and Operations
Role: Senior Analyst (L1)

Project Roles and Responsibilities:

- Willingness to work in 24*7 environment Log monitoring and investigation through SIEM solution in rotational 24x7 shifts
- Monitoring 24x7 for P1, P2, P3 alerts in SOC operations for real-time monitoring, analyzing logs from various security/Industrial appliances by using **QRadar**.
- Filling the Daily health checklist. Create, Modify and Update Security Information Event Management (SIEM) Tools.
- Working in GSOC (Global security Operation center) with multiple (21) clients.
- Creating Dashboard on **QRadar** to analyze the Data
- Creation of metrics and support KPIs, Dashboard, Trackers and analyzing daily, weekly and monthly reports.
- Creating the tickets in ticketing tool and Updating the Trackers once it closed.
- Carrying out log monitoring and incident analysis for various devices such as Firewalls, IDS, IPS, database, web servers and so forth
- Create, modify and tune the SIEM rules to adjust the specifications of alerts and incidents
- Work with the customer designated personnel to provide continual correlation rule tuning, incident classification and prioritization recommendations

- Work closely with the assigned Managed Services SIEM resources to ensure client's customized solution is functioning optimally and continuously tuned to the client's needs
- Resolve problems related to Network, Device, Policy, connectivity issues etc.
- Escalating the security incidents based on the client's SLA and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing recommendations regarding security incidents mitigation which in turn makes the customer business safe and secure

Technical Skills/Key Skills:

- SOC (Security Operation Center)
- SIEM (Security Information and Event Management) Tool: IBM QRadar.
- Antivirus: Symantec Endpoint Protection, Microsoft ATP
- AWS Cloud Trail, S3 Buckets
- Devices: Palo Alto, WAF, Fortigate, Zscaler Proxy
- Ticketing Tools: Service Now, BMC Remedy, Salesforce (Nurd)
- SOAR: Resilient
- Spam mail Analysis
- Vulnerability Assessment (Nessus)

Soft Skills

- Flexible approach towards work and ability to work in a team
- Ability to learn fast and work efficiently by training the peer group and junior level associates
- Learn and share attitude

Education:

- B.Tech - G Pullareddy engineering college, JNTUA – 2018.(6.84 CGPA)
- Inter - Narayana Junior college -2013(82.9%)
- 10^{th} – Sri Swamy Vivekananda High school – 2011(84.83%)

Declaration:

I hereby declare that the above-mentioned information is correct up to my knowledge and I bear that responsibility for the correctness of the above-mentioned.

(T Mouni Suryanarayana.)