

SATYANARAYANA MANCHYALA

Security Analyst

Mobile: +91-9502257753

E-Mail: satyamanchyala54@gmail.com

Career Objective:

To associate with an innovative and vibrant organization, allowing me to put my competencies to the best use, to add value to the organization and contribute to my overall growth as an individual.

- A competent professional with 4.4 years of experience in information security as Security Analyst.
- Good knowledge on networking concepts including OSI layers, subnet, TCP/IP, ports, DNS, DHCP etc.
- Good understanding of security solutions like Firewalls (Palo Alto, checkpoint, Fortinet), DLP, Anti-virus, IPS, Email Security etc.
- Experience on **SIEM (Security Information and Event Management) tools** like Monitoring real-time events using **Microfocus Arc Sight, IBM Q-Radar, Splunk and EDR** tool.

Technical Skills:

- **SIEM Tools:** Q-Radar, ArcSight and Knowledge on Splunk Enterprise Security.
- **Phishing Email Analysis**
- **Networking:** Firewall, IDS/IPS, OSI Layers, Web Proxy, WAF, TCP/IP, DNS, DHCP.
- **Ticketing tool:** ServiceNow, Jira.

Education:

B.Tech (Mechanical Engineering) From JNTUK in **2017**.

Professional Experience:

1) HTC Global Services

July 2020 – Till Date

Security Analyst

- Served as Analyst in SOC operations for real-time monitoring, analyzing logs from various security/Industrial appliances by using IBM Q-Radar console, L2 connectivity and troubleshooting of logging issues.
- Administrating various incidents/security alerts triggered in SIEM tool.
- Carrying out log monitoring and incident analysis for various devices such as Firewalls, IDS, IPS, database, web servers and so forth.
- Monitoring 24x7 for Security Alerts and targeted phishing sites by using SIEM tool with the help of technologies such as Watermark, Referrer, Abuse mail box and similar sounding domains.
- Website Anti-Malware and Defacement monitoring and real-time alerting based on anomalies detected.
- Created filters, active channels, queries, Rules, Dashboard etc. in Arc Sight for monitoring purpose.
- Configured reports in IBM Q-Radar Collector and Processor as per the requirement.
- Maintenance of IBM Q-Radar Products (Collector and Processor) like its Health check which also includes Q-Radar content developments i.e., rules, reports and dashboards.

- Knowledge of Installation, Configuration and up gradation of various connectors, and also its troubleshooting.

- **Project roles and Responsibilities:**

- Monitoring the customer network using SIEM tools: IBM Q-Radar, Microfocus ArcSight, Splunk.
- Work closely with business units to ensure that they know what and how to feed data into Q-Radar and to create network hierarchy, classify Log Sources within the Q-Radar SIEM.
- Performing Real-Time Monitoring, Investigation, Analysis, Reporting and Escalations of Security Events from Multiple log sources.
- Maintain keen understanding of evolving internet threats to ensure the security of client networks.
- 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.
- Contacting the customers directly in case of high priority incidents and helping the customer in the process of mitigating the attacks.
- Co-ordinate extensively with networking teams to maintain and establish communication to remote Q-Radar Collectors/Processors.
- Troubleshooting SIEM dashboard issues when there are no reports getting generated or no data available.
- Determine the scope of security incident and its potential impact to Client network and recommend steps to handle the security incident with all information and supporting evidence of security events.
- Creation of reports and dashboards and rules fine tuning.

Additional Skills:

- Routing and Switching
- Hardware/software troubleshooting
- Technical support
- System & software installation
- Troubleshooting network issues
- LAN&WAN support
- Hardware installation
- Network IP configuration
- Backup using putty

Declaration: I Hereby declare that the above given information is correct to the best of my knowledge and belief.

Date: 06-12-2024

(Satyanarayana M)