MASANI RAJASHEKAR REDDY

Email: rajashekarreddy.soc@gmail.com

Mobile: +91- 9618035734

PROFESSIONAL SYNOPSIS:

Experienced Cyber Security Professional with 3.5 years of solid IT experience in Cyber Security/SOC working on multiple security tools like SIEM, EDR, V.M, Email Security Gateways etc. And managing multiple clients providing uninterrupted Security Operations.

PROFESSIONAL SUMMARY:

- Experience in deploying and configuration SIEM/SOAR environment.
- Experience in Implementing automation to streamline security operations.
- Assist the SOC in supporting all process, procedures, and plans necessary to run the SOC.
- Working in Security Operation Centre, performing real-time Log monitoring and investigating security incidents.
- Performing incident management based on the incidents identified on the EDR, Email Gateway etc.
- Experience on SIEM (Security Information and Event Management) tools like Monitoring real time events using tools like Microsoft-Sentinel, Splunk.
- Having SOAR experience in Azure Sentinel and ability to create Playbooks and Logic apps and Watch lists on it.
- Having basic knowledge to create playbooks on XSOAR (SOAR)
- Experience in Incident Management, Phishing email analysis, Malware analysis, Log analysis.
- Good knowledge on networking concepts including OSI layers, subnet, TCP/IP, ports, DNS, DHCP etc.
- Good understanding of security solutions like Anti-virus, DLP, proxy, Firewall, IPS, Email Security etc.
- Experience in Monitoring the Daily health checklist.
- Experience in creating the tickets in ticketing tool.

TECHNICAL SKILLS:

- SIEM Solutions (Sentinel, Splunk)
- Ticketing Tool: Service now
- Framework: Cyber Kill Chain, MITRE
- Intermediate Knowledge of PowerShell | Cloud Security (Azure) | Windows Internals
- EDR (Sophos, CrowdStrike, Microsoft defender for endpoint, Tanium)
- Email Security (Avanan, MDCA, Knowbe4)

WORK EXPERIENCE:

Marlabs Innovations Pvt Ltd (April 2024 – Till Now)

YASH Technologies Pvt Ltd (Feb 2022- April 2024) (Health care services)

Roles & Responsibilities:

- Detect incidents by monitoring the SIEM console, rules, reports and dashboards.
- Monitor the log from Firewall, IPS/IDS, Proxy server, AD Server, DNS, DHCP or other Servers.
- Monitoring and Sending alerts to respective teams within the SLA.

- Investigate incident, remediation, and follow-up for incidents.
- Identifying and classifying attempted security incidents, suspicious traffic to client networks.
- Handling various alerts related to possible phishing attack, Logon failure, Authentication failure, failed attempt alert, Data Ex-filtration, Dos attack etc...
- Review, analyse, and respond to security events triggered through the security monitoring systems according to internal security procedures for cyber events.
- Performing the follow up activities to send the reminders to the respective persons or team to take action on raised tickets within a stipulated time.
- Performing ticket closure activities once the action is taken on raised tickets.
- Generate daily incident reports and monthly reports on time. Provide proactive feedback to senior personnel and management as required, Responsible for shift handover.
- Performing Log analysis & analysing the crucial alerts at immediate basis.
- Investigate all Phishing attack events against our group and ensure that appropriate groups are notified.
- Communicate with external team to resolve the queries relating to the raised incidents.

EDUCATION:

Completed B.Tech (Electrical) from Bharat Institute of Engineering and Technology, JNTUH, 2017, 67%. Completed Intermediate from Sri Gayatri Junior College, Board of intermediate, 2013, 95.8%. Completed SSC from Krishnaveni Talent school, Secondary State Board, 2011, 87%.

PERSONAL INFORMATION:

Full Name : Masani Rajashekar Reddy
Father's Name : M Yadagiri Reddy
Date of Birth : 02-11-1994
Languages Known : English, Telugu
Nationality : Indian

DECLARATION :

I, M Rajashekar Reddy hereby declare that the information contained is true and correct to the best of my knowledge and belief.

Date :
Place : Hyderabad (M Rajashekar Reddy)