Varsha Desai.

Security Analyst -L1 (Deliotte With third party payroll of Apslog Pune)

Email : desaivarsha1498@gmail.com

Contact Number : +917385441322

OBJECTIVES :

An experienced information security professional with strong Cyber Security, management skills & soaring interest in cutting edge security trends that require profound reading and experimentation. Fully Committed to understand and re-invent processes to develop innovative approach towards problem solving. Always eager to learn more tricks from all team members adding to holistic knowledge gain in a way that is beneficial to the company while enhancing productivity and reputation.

SKILLS HIGHLISTS

- Domain : Security Operations & Security Monitoring.
- Understanding of SIEM Network architecture.
- SIEM (Security Information and Event Management) Tools: **Splunk and Qradar.**
- Good knowledge of Reference Set, Active list, Rules & IOCs configuration in SIEM (**Elastic**)
- Technical Knowledge: SIEM (Splunk , Q-Radar), EDR (CrowdStrike, Microsoft Defender), Suspicious File Analysis (Palo Alto Wildfire,), Firewall(Fortinet, SOPHOS, Checkpoint, PaloAlto), Antivirus(SOPHOS, Mcaffe), Proxy (Zscalar,), Incident Response, Suspicious Email Analysis & Information Security Advisories.

CERTIFICATIONS & KEY ACHIEVEMENTS

- Certified Fortinet NSE1 & NSE2 in April 2023.
- Certified Fortinet NSE1 CCSA Trained from IP Solution.
- Fortinet Firewall trained from Fortinet.
- Attended Multiple Webinars on Cyber security & conducted sessions/training for new comers, freshers.

EXPERIENCE:

- **Security Analyst | Deliotte With third party payroll of Apslog Pune |Shared SOC & Security Monitoring (January2022 –Till Now)**
- Security Operation, Event detection & Investigation (L1):
- Experience on SIEM (Security Information and Event Management) tools like Monitoring real-time events using **Qradar & Splunk.**
- Hands on experience with tools and process used in security solution like Endpoint security and Response, Cycber Incidents response and investigation, IPS/IDS, Email security, Vulnerability Assessment, Malware Analysis etc.
- Monitoring, analyzing and responding to Security Alerts, infrastructure threats, vulnerabilities and Targeted phishing sites by SIEM Tool.
- Conduct thorough investigation of security events generated by our detection mechanisms such as SIEM, , EDR, XDR, IDS/IPS, WAF, Firewall, Proxy, Database.
- Incident Handling, Investigate, collaborate and report on root-cause-analysis of malware attacks.
- Implementation of new rules and use cases. Review & Fine tuning of existing & recently implemented use cases.
- Implementation of various ideas in current project and developed the processes.
- Experience and creating case for the security threats and forwarding it to onsite SOC team for further investing and action.
- Implemented best practices for incident response and investigation, correlation trainings for team to maintain the SLA.
- Installation of Application software and Antivirus software& Installing the Operating Software such as

windows.

- Review security-related events, reports & incidents escalated by SOC engineers(L1), assessing severity, criticality and priority.
- Based on network devices, operating systems and platform of client's environment, creating customer specific security reports and monthly dashboard as well as finetuning on client requirements.
- Advise and implement necessary changes required to counter the attack or improvise security standards. Keep the security systems up to date and contributing to security strategies.
- Maintain record of reporting & non-reporting devices on daily basis & present this reports in weekly meeting with Project Manager & respective stakeholders.
- Co-ordinate with SOC Team regarding client queries & provide solution within SLA time.
- Perform use-case review activity on quarterly basis.
- Block IOCs on Security solutions.

Education

- **Bachelors in Business Administration** | Shivaji University | 2020 .

HOBBIES

- I like spending time in learning of New cyber security concepts & share it with my team mates specially for newcomers & freshers. Because Freshers are not getting/learning required skills for Industry in their college life.
- I usually spend my leisure time in Photography, Listening Music, meditation & Exercise.

Varsha Desai.