SAIKIRAN CHADA

9480983943 | saikiranchada95@gmail.com

Professional Summary

Highly skilled and dedicated Professional with 5.5 years' experience in the IT industry and 4.5 years' experience in Information Security as a Security Analyst with a proven track record in maintaining robust security operations within a Security Operations Center (SOC) environment. Proficient in analyzing security incidents, implementing effective mitigation strategies, and ensuring the confidentiality, integrity, and availability of critical systems and data. Adept at utilizing cutting- edge security tools and technologies to identify and address vulnerabilities, as well as conducting comprehensive threat assessments. Excellent problem-solving and communication abilities, with a strong commitment to delivering exceptional results in fast-paced and high-pressure situations. Seeking to leverage expertise in SOC operations to contribute to the security posture and success of an organization.

Skills

- Environment: SOC (Security Operation Centre)
- Console: SIEM (Security Information and Event Management)
- SIEM Tools: Splunk, QRadar, Azure Sentinel
- Ticketing Tool: Service Now, BMC Remedy.
- Antivirus: McAfee
- EDR Solutions: CrowdStrike, Microsoft Defender ATP
- Cloud Security: Prisma Cloud, Microsoft Azure Security
- DLP Tools: Forcepoint DLP, Symantec DLP, Digital Guardian (USB and Print Logs)
- Threat Hunting & Analysis: KQL, MITRE ATT&CK, Behavioral Analytics
- Network Security: Firewalls (Cisco, Palo Alto, Fortinet), IDS/IPS, VPN
- Malware Analysis: CrowdStrike Sandboxing, VirusTotal, Any.Run, McAfee Antivirus
- Incident Response & Management: Threat detection, investigation, containment, eradication, and root cause analysis
- Networking Protocols: TCP/IP, intrusion detection, and network traffic analysis
- Firewall, IDS/IPS, Phishing Email Analysis, NMAP, SPAM and DLP, Mail security monitoring.
- VA: Nessus manager,Tenable SC, Burpsuite, Kali Linux

Experience

- **Synoptics technologies Ltd, Mumbai - IND** 09/2024 - Present
  L2 SOC Analyst
- **Virtusa, Bengaluru - IND** 12/2020 - 08/2024
  Security Analyst
  - Worked in a 24/7 Security Operation Centre (SOC) environment, responsible for monitoring SOC events and detecting/preventing intrusion attempts.
  - Demonstrated a comprehensive understanding of security solutions such as Firewalls (Palo Alto, Checkpoint, Fortinet), DLP, Anti-virus, IPS, and Email Security.
  - Responded to various security alerts for multiple clients and conducted vulnerability scans using Qualys.
  - Monitored real-time events using SIEM tools like ArcSight and Splunk.
  - Handled alerts from various security log sources, including Proxy, Anti-Virus, and EDR.
  - Conducted deep dive investigations using Falcon EDR.
  - Monitored, analyzed, and responded to infrastructure threats and vulnerabilities.
  - Conducted phishing and spam email analysis.

- Investigated security logs, developed mitigation strategies, and prepared generic security incident reports.
- Prepared root cause analysis reports based on thorough analysis.
- Analysed daily, weekly, and monthly reports for insights and trends.
- Created cases for suspicious issues and escalated them to the Onsite SOC team for further investigation.
- Monitored websites for malware and defacement, promptly alerting anomalies.
- Troubleshot issues with SIEM dashboards, ensuring proper report generation and data availability.
- Monitored SIEM alerts, analyzed events, and raised security incidents in the ticketing tool ManageEngine.
- Gained experience in monitoring and investigating events in McAfee DLP.
- Monitored security systems and networks for anomalies.
- Investigated security violations, unauthorized access attempts, and virus infections.
- Coordinated responses to security incidents in a timely manner.
- Collaborated with cross-functional teams to improve the overall security posture of the organization.

- **DELTAA Infocom solutions, Bangalore - IND** 08/2019 - 12/2020
  IT System Engineer
  - Implemented and standardized the documentation process for scheduled maintenance plans, ensuring consistency and efficiency.
  - Monitored system performance, promptly identifying, and resolving software/hardware issues to maintain optimal functionality.
  - Utilized a ticketing system to document and track reported issues, ensuring timely resolution and effective communication.
  - Ensured the successful completion of full and incremental data backups, safeguarding critical information.
  - Conducted data restoration for users as required, minimizing downtime, and ensuring data integrity.
  - Proactively applied security updates and patches on servers, desktops, and laptops, bolstering system protection.
  - Configured, troubleshooted, and maintained Windows 2003 and 2008 Servers, ensuring their smooth operation and reliability.

Education

- **AVN Institute of engineering and technology - JNTUH** 2018
  B.Tech(Mech)
  60.78%

Declaration

- I here declare that the above given information is correct to the best of my knowledge and belief.