|  |  |  |
| --- | --- | --- |
|  |  | |
| **Harish Katherla**  Mobile: +91-7337560390 ~ E-Mail: [Harishkatherla7@gmail.com](mailto:Harishkatherla7@gmail.com)  **Professional Summary**   * Capable of working independently and involving senior analysts as necessary * Communicate the severity of the threat and recommendations for remediation to the customer and other cyber security personnel through written and verbal media * Follow detailed processes and procedures to analyze, escalate, and assist in remediation of critical information security incidents * Configuring and monitoring Security Information and Event Management (SIEM) platform for security alerts. Integrate and work with the firm’s Managed Security Services Provider (MSSP) services. * Hands-on experience on various tools like **Logrhythm, Alien Vault, Splunk, FireEye, Mimecast, RSA Net- witness and ECAT, Symantec EDR , Resilient (SOAR)**. |  |
| **WORK EXPERIENCE** |
| **Jr. Data Service Engineer**  **Since June’21 to Oct ‘23: Centific National private limited**  **Key Result Areas:**   * Responsible for working in a 24x7 Security Operation Center (SOC) environment and monitoring alerts using LogRhythm and Azure Sentinel * Working knowledge on SOAR platform (**Resilient**) * Analyzing phishing and spam emails on email filtering solution at our email gateway FireEye * Hands-on knowledge on Crowdstrike Falcon * Follow detailed processes and procedures to analyze, escalate, and assist in remediation of critical information security incidents * To monitor, decide, remediate a security event to a False Positive/True Positive and take necessary action   **TRAINING AND CERTIFICATION** |
| * Trained in Crowdstrike EDR.Logrythm SIEM and other various Email Gateways * Trained in Certified Ethical Hacker (CEH). * Trained in Cisco CCNA.RHCSA * Trained in MCSA * Introduction to LogRhythm Analyst & Administrator * Trained in Splunk 7.x Fundamentals * Trained in VAPT (Vulnerability Assessment Penetration Testing).   **IT - SKILLS** |
| Vulnerability Assessment Tools Nessus, Qualys  SIEM Tools: Logrhythm, Alienvault, Splunk  Other Tools: Crowdstrike EDR, Resilient-SOAR,ZeroFox  Ticketing Tool: Service desk plus, SericeNow  Email Gateway: Mimecast, FireEye, Microsoft Defender  **EDUCATION** |
| **2020 B.com in** Wesley Degree & PG College, Begumpet  **Known Languages**: English, Hindi, Telugu |