Education

IET-DAVV *2014*

Bechelor of Engineering

Skills

Incident response, Vulnerability Analysis, IPS/IDS, E-mail phishing, Proxy, Firewall, Log analysis, Device integration, Ticket Creation, expertise SIEM Tool use cases.

Certification

SOC Expert Certified

Attending EDR Crowd Strike Training

Ankur Babele

| H.N. 211, Sounya Green Ville, Awadhpuri, Bhopal (M.P.)
| 7987579283| ankurbabele07@gmail.com

Objective

To obtain a challenging and dynamic role as a SOC Analyst, utilizing my technical skills and knowledge in cyber security, network security, and incident response. My goal is to contribute to the success of the organisation by proactively detecting and responding to security threats, while continuously improving my skills and knowledge to enhance the overall security posture of the company.

Experience

RSOFT SYSTEM AND SERVICE PVT LTD

SOC ANALYST (L1) *Feb - 2022 - Till now*

- worked in a 24*7 Security Operations Center.
- Monitoring the customer using Splunk SIEM.
- Analyzing Real-time security incidents and checking whether they are true positive or false positive.
- Act as First level support for all Security issues.
- Coordinating with Networking teams to maintain and establish communication to remote Splunk.
- investigating malicious phishing e-mails, domains, and IPs using open-source tools and recommending proper blocking based on analysis.
- Working on windows Logs as well as logs from IDS/IPS, Next Generation Firewalls, Anti-virus, Vulnerability Assessment solution.
- Integration of new devices with splunk such as windows.
- Creating Splunk content like correlation Rules, Queries, Reports, Dashboard etc.

MAHENDRA EDUCATION PVT LTD

Instructor and Development Officer *Aug - 2015 - Sep - 2021*

- Creating content to be delivered as lessons, Short Courses, learning Modules etc.
- Managing video schedules and ensuring that they complement ongoing marketing campaigns, based on exhaustive research and analysis.

Worldsec Technologies

Intern *Sep - 2021 - Feb - 2022*

- Hands on experience with Splunk SIEM tool for logs monitoring and Analysis.
- Service now ticketing tool for incident response.
- Good knowledge on networking concepts including OSI layers, subnet, TCP/IP, Ports.