MAYANK BINWAL

MOB. – +91 6396841225 || MAYANKBINWAL639@GMAIL.COM || 66-C, POCKET-A2, MAYUR VIHAR PHASE-3, DELHI – 110096

Objective

Enthusiastic and driven SOC Analyst with a passion for cybersecurity and real-time threat analysis. Adept at using security tools such as SIEM, firewalls, and antivirus systems to detect anomalies and protect networks from potential breaches. Seeking a position where I can contribute to proactive security measures and gain further expertise in incident response and threat mitigation.

Technical Skills

- Familiar with Security Information and Event Management (SIEM) tools like Splunk.
- Knowledge of security monitoring, incident detection, and escalation processes in a Security Operations Centre (SOC) environment.
- Basic understanding of networking protocols such as TCP/IP, DNS, HTTP/HTTPS, SSH, and SMTP.
- Experience in using ticketing systems (e.g., JIRA) for managing and tracking incidents.
- Take follow ups on the raised incidents and closing of the tickets based on client evidence or response.

Experience

CONCENTRIX PVT LTD as OPERATION REPRESENTATIVE
Oct. 2022 to Dec. 2024

- Proficient in Security Information and Event Management (SIEM) tools like Splunk, including advanced correlation rule creation, monitoring, and incident escalation.
- Acted as the first responder during security events, investigating and analyzing cyberattacks, reviewing incident alerts.
- Utilized CrowdStrike Falcon EDR to monitor, detect, and respond to threats across endpoints, reducing incident response time.
- Monitored real-time security events and handled incidents using SEIM tools, including Alert Logic, ensuring timely incident resolution and escalations
- Authored and updated system configuration documentation, standard operating procedures (SOPs), and troubleshooting guides, ensuring all systems followed best practices.
- Investigate malicious phishing emails, domains and Ips using Open-Source tools and recommend proper blocking based on analysis
- Understanding the urgency of an incident and working independently as well as co-ordinately with the L1 and L2 Team for further action.
- Working on assigned ticket queue, understanding and exceeding expectations on all tasked commitments.

Certifications

- Introduction to Cybersecurity | Cisco Networking Academy program
- Endpoint security | National Skill Development Corporation (Cisco Networking Academy program)
- Splunk core user certification guide | Udemy

Academic Credentials

- **Bachelor in Commerce**
  Kumaun university (Nainital)
  August 2018 to November 2021
- **Intermediate from CBSE board**
  Universal convent sr. sec. school (Nainital)

April 2016 to March 2018

- **High school from CBSE board**

  Doon modern academy (NAINITAL)

  April 2014 to March 2016

Personal Details

- Father's name : Mr. Satish Chandra Binwal
- DOB: 10 - 02 - 2001
- Marital Status: Single
- Language known: English & Hindi
- Gender: Male