Sohel Shaikh

Experienced SOC Analyst with 3 years of expertise in monitoring, detecting, and responding to cybersecurity threats. Proficient in advanced threat detection, incident response, and implementing security measures to mitigate risks. Skilled in utilizing industry-leading tools such as QRadar, Bitdefender, CrowdStrike, XDR, Mimecast, Darktrace, and SentinelOne for real-time threat analysis and event resolution. Adept at collaborating with cross-functional teams to ensure adherence to security best practices and industry standards. Committed to enhancing organizational security through proactive threat intelligence, network security, and continuous improvement of incident response strategies.

Sohelshaikh1517@gmail.com 7758811454 Pune, Maharashtra
sohel-shaikh-362329216

WORK EXPERIENCE

SecurityHQ

• Graduate Analyst May 2022 - Present

- Monitor and investigate security events and incidents, providing timely responses and resolutions to mitigate risks and minimize impact.
- Conduct preliminary analysis of security alerts and assess the severity of incidents in accordance with established incident response procedures.
- Provide escalation and coordination of security incidents.
- Track and update incidents and requests based on client updates and analysis results.
- Identify and recommend improvements to the organization's security posture by analyzing trends, evaluating risks, and providing recommendations on effective countermeasures.
- Collaborate with cross-functional teams to ensure the proper implementation of security controls and measures to maintain the confidentiality, integrity, and availability of information assets.
- Participate in the development and maintenance of security policies, procedures, and guidelines.
- Document incidents and maintain accurate and timely incident reports.
- Continuously improve SOC processes, procedures, and technologies to enhance the effectiveness of the security operations center.

Cybervault Securities Pvt Ltd

Information Security Analyst (Intern) Oct 2021 - Mar 2022

- Conduct penetration testing and vulnerability assessments to find security gaps in
- IT infrastructure and systems.
- Assisting in identifying and evaluating potential vulnerabilities in software,
- systems, networks, and applications.
- Whenever necessary, educate staff members about security.
- Identified potential security threats and conducted thorough analysis to respond promptly and effectively.
- Tool Utilization: Gaining hands-on experience with security testing tools, such as
- Metasploit, Burp Suite, Nmap, Wireshark, and more, to simulate real-world
- attacks.

EDUCATION

Dr. Dy Patil College of Arts Commerce and Science

Master of Computer Science - 68.60 June 2022 - April 2024

Bachelor of Computer Science - 80.40 % June 2018 - Aug 2021

Mahatma Gandhi Junior College, Manchar

Higher Secondary School Curriculum - 66.40 % June 2016 - May 2018

Mahatma Gandhi Vidyalaya, Manchar

Secondary School Curriculum - 89.20 % June 2015 - May 2016

Skills and Areas of Expertise

- IBM QRadar: Real-Time Monitoring, Log and Event Collection, Threat Intelligence, Compliance and Reporting, Incident Tracking and Updates.
- SIEM and EDR Tools: QRadar, LogRhythm, Darktrace, CrowdStrike, Cortex XDR, Bitdefender, Sentinel One, Mimecast.
- IT Security: Reconnaissance, Vulnerability Assessment, Incident Management, Email Security.
- Penetration Testing Tools - Gaining hands-on experience with testing tools such as Nikto, Nessus, SQLMap, Wireshark, Metasploit, Burp Suite, Nmap , Hydra, Dirbuster.

CERTIFICATE

- **Certified Ethical Hacker V12**
- **Crowd strike : SOC Analyst**
- **SC-200: Microsoft Security Operations Analyst**
- **CompTIA CYSA+**

Personal Details

- Nationality - Indian
- Gender - Male
- Marital Status - Unmarried
- Date of Birth - 23/02/2001
- Current Location - Pune