

# Sohel Shaikh

SOC Analyst

Sohelshaikh1517@gmail.com

<https://www.linkedin.com/in/sohel-shaikh07/>

+91 7758811454

Pune, Maharashtra, India

Experienced SOC Analyst with 3+ years of expertise in detecting, monitoring and responding to cybersecurity threats. Skilled in using tools like QRadar, Bitdefender, CrowdStrike, XDR, Mimecast, Darktrace and SentinelOne for threat analysis and incident resolution. Proficient in network security, threat intelligence and enhancing incident response strategies to ensure organizational security.

## Work Experience

### Graduate Analyst

SecurityHQ Pvt Ltd | Pune

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.
- 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.
- Track and update incidents and requests based on client updates and analysis results, ensuring accurate documentation.
- Continuously enhance SOC processes, procedures and technologies to improve the effectiveness of security operations.

### Information Security Analyst Intern

Cybervault Securities Pvt Ltd | Pune

Nov 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.

## Core Skills

### IBM QRadar :

Real-Time Monitoring, Log and Event Collection, Threat Intelligence, Incident Response ,Compliance and Reporting, Incident Tracking and Updates.

**SIEM and EDR Tools:** QRadar, LogRhythm, Darktrace, CrowdStrike, Cortex XDR, Bitdefender, SentinelOne, 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, BurpSuite, Nmap, Hydra, Dirbuster.

## **Education**

Dr. Dy Patil College of Arts Commerce and Science

Jun 2022 - Apr 2024

Master of Computer Science GPA : 68.60

Dr. Dy Patil College of Arts Commerce and Science

Jun 2018 - Aug 2021

Bachelor of Computer Science GPA : 80.40

## **Certificates**

Certified Ethical Hacker V12

SC-200 : Microsoft Security Operations Analyst

Crowd strike : SOC Analyst

CompTIA CYSA+