YASH AHIR

Email: ahiryash.07@gmail.com | LinkedIn:www.linkedin.com/in/yashahir

Phone: +91-9604116711 |

CAREER OBJECTIVE

Entry-level SOC Analyst with hands-on experience in security monitoring, threat detection, vulnerability assessment, and incident response. Skilled in SIEM tools, endpoint security, and penetration testing fundamentals. Seeking a SOC role where I can actively monitor threats, document incidents, and learn from senior security analysts in a real-time security operations environment.

EDUCATION

MCA (Engginéering) — Aug 2023- Jun 2025
GES R. H. Sapat College of Engineering, Nashik — **7.63 / 10**

B.Sc (Computer Science) — Aug 2020- Apr 2023
ACS College, Navapur — **9.69 / 10**

TECHNICAL SKILLS

SOC Operations	Security Monitoring, Threat Detection, Threat Hunting, Incident Response, Alert Triage, Incident Documentation
SIEM & Log Analysis	Splunk, Wazuh, Event Analysis
Security & Pentesting Tools	Kali Linux, Nmap, Burp Suite, Metasploit, Wireshark, Nessus, VirusTotal
Vulnerability Management	Vulnerability Assessment, OWASP Top 10, Secure SDLC
Endpoint & Identity Security	Microsoft Defender
Network Security	IDS/IPS Concepts, Packet Analysis, Firewall Basics
Operating Systems	Windows, Kali Linux
Programming & Scripting	Python, C++, Bash
GRC & Compliance	ISO 27001 Basics, NIST CSF, Risk Assessment, Audit Support

TRAININGS

Self Learning on TryHackMe

Key Modules:

- SOC Operations: Log analysis, threat hunting, incident response workflows
- SIEM Fundamentals: Splunk & ELK basics
- Network Security: IDS/IPS, firewall concepts, packet analysis
- Ethical Hacking & Vulnerability Assessment: OWASP Top 10, web app pentesting
- GRC & Compliance: ISO 27001, NIST CSF, risk assessments

PROJECTS

Hands-On SOC Experience (Labs / Home Setup)

- Built a Wazuh SIEM lab to monitor Windows & Linux endpoints; analyzed security alerts using MITRE ATT&CK
- Detected phishing attempts using header analysis & VirusTotal lookup
- Investigated brute-force attempts in Windows logs using Splunk queries
- Created incident reports following NIST IR framework

CERTIFICATIONS

CEH – SevenMentors, Pune
CCNA - SevenMentors, Pune
RedHat Linux - SevenMentors, Pune