Rishikesh S. Pokale

Pune, Maharashtra
+91-7028083488 — rishi651113@gmail.com — LinkedIn

Professional Profile

Dedicated and enthusiastic Computer Engineering graduate with hands-on experience as a SOC Analyst in a global cybersecurity environment. Possessing strong expertise in Cyber Security, Computer Networks, Linux, SIEM technologies, and Incident Response. Passionate about inspiring future engineers by combining industry experience with practical, outcome-based teaching methodologies. Seeking an Assistant Professor/Lecturer position where I can contribute to academic excellence while mentoring students with real-world cybersecurity knowledge.

Professional Summary

- Nearly 1 years of professional experience as a Security Operations Center (SOC) Analyst.
- Hands-on experience with IBM QRadar, Microsoft Sentinel, Trend Micro, and Darktrace.
- Strong understanding of Cyber Security, Networking, Linux Administration, Threat Detection, and Incident Response.
- Experienced in SIEM monitoring, log analysis, security investigations, and SLA-driven incident management.
- Passionate about teaching engineering students through practical demonstrations and real-world case studies.
- Excellent communication, presentation, mentoring, and problem-solving skills.

Education

Bachelor of Engineering (Computer Engineering)
KJ College of Engineering and Management Research
Savitribai Phule Pune University 2020–2024
CGPA: 7.0 / 10 (70%)

Professional Experience

SOC Analyst (L1) – SecurityHQ, Pune March 2025 – October 2025

- Monitored enterprise security events using IBM QRadar and Microsoft Sentinel.
- Investigated and triaged cybersecurity incidents by analyzing logs, alerts, and threat intelligence.
- Performed SIEM monitoring, log analysis, threat detection, and incident response activities.
- Managed security incidents while ensuring SLA compliance and accurate documentation.
- Utilized Trend Micro and Darktrace for endpoint and network security monitoring.
- Collaborated with senior analysts to investigate security events and improve detection capabilities.

Subjects Able to Teach

Computer Networks • Cyber Security • Network Security • Information Security • Operating Systems • Linux Administration • Ethical Hacking

Laboratory Skills

IBM QRadar • Microsoft Sentinel • Wireshark • Burp Suite • Nmap • Metasploit Framework • OWASP ZAP • Kali Linux • Windows Security • Linux Administration

Academic Projects

Metasploit Framework Deployment – Configured and exploited intentionally vulnerable machines in a controlled lab environment.
Vulnerability Assessment – Performed reconnaissance, vulnerability identification and exploitation on laboratory systems.
Post Exploitation – Implemented privilege escalation, persistence and payload generation techniques.

Technical Skills

Cyber Security: Incident Response, Threat Hunting, Log Analysis, Risk Assessment, Vulnerability Assessment
Networking: TCP/IP, Routing, Switching, Subnetting, VLAN, VPN, OSPF
Scripting: Bash, Shell Scripting
Operating Systems: Linux, Windows

Certifications

Cisco CCNA • CEH • Red Hat Enterprise Linux (RHEL) • Cisco Introduction to Cyber Security

Strengths

Communication • Student Mentoring • Practical Teaching • Presentation Skills • Problem Solving • Team Collaboration