dipak Kumar Sah

✉ dk7637466@gmail.com ☎ 7250928782 ● ambala, haryana in LinkedIn

PROFILE

Entry-level SOC Analyst with hands-on practice in SIEM log analysis, alert monitoring, and incident triage through TryHackMe labs and security projects. Experienced in detecting credential-based attacks and suspicious access attempts , mapping threats to MITRE ATT&CK, and supporting SOC monitoring workflows.

SKILLS

- Security Operations (SOC): Alert monitoring, incident triage, event correlation, escalation
- SIEM & Log Analysis: Splunk searches, dashboards, alert investigation, log correlation
- Threat Detection: MITRE ATT&CK mapping, brute-force detection, phishing analysis
- Incident Response: Identification, containment, recovery, eradication, RCA
- Networking: TCP/IP, OSI, DNS, HTTP/HTTPS, Firewalls, IDS/IPS, VPN
- Operating Systems: Windows, Linux
- Security Tools: Wireshark, Nmap, Burp Suite, Metasploit, Nessus
- Scripting: Python, Bash, PowerShell (automation basics)

PROJECTS

Investigation of Unauthorized Access Using SIEM 10/2025 – 2026

- Investigated 5000+ authentication Logs to identify unauthorized login attempts
- Correlated user activity across 6–8 systems to detect abnormal behavior
- Validated alerts using IP reputation, timestamps, and event frequency
- Documented findings for 10+ security incidents to support SOC escalation processes

SSH Log Analysis and Threat Detection Using SIEM 06/2025 – 08/2025

- Monitored and correlated 10,000+SSH Logs to detect high-volume login failures and suspicious SSH access activity
- Identified suspicious login patterns and mapped attacks to MITRE ATT&CK(T1110)
- Triaged high-severity alerts and reduced false positives by 30%
- Supported real-time SOC alerting workflows by reviewing 20+ alerts per day

HANDS ON EXPERIENCE

TryHackMe (Ranked Top 9% globally) 2024 – Present
Ambala, Haryana

- Performed SOC-focused labs analyzing 2,000+ security events in SIEM
- Practiced detection of credential abuse, abnormal login behavior, and suspicious account activity
- Conducted basic penetration testing labs across 30+ vulnerable machines
- Used tools such as Nmap, Burp Suite, and Metasploit in 60+ hands-on labs
- Applied MITRE ATT&CK framework for threat and attack technique mapping

EDUCATION

B.Tech(Computer Science & Engineering) 09/2022 – Present
Maharishi Markandeshwar (Deemed to be University) Ambala, Haryana

ACHIEVEMENT

- Cybersecurity101 – TryHackMe
- SOC Level 1 - TryHackMe

LANGUAGES

English

Hindi