Divyansh Sharma

+91 6397325703
dsharma.cybersec@gmail.com
LinkedIn — picoCTF: cyberhell — GitHub: Divyanshsharrma

Summary

Entry-level SOC Analyst with hands-on experience in security monitoring, alert triage, log analysis, and incident investigation. Experienced in working with Linux systems, SIEM-based monitoring, threat detection, and vulnerability assessment. Exposure to real-world cybercrime investigations, GRC procedures, and SOC workflows through internships and security projects. Strong interest in blue-team operations, incident response, and continuous security monitoring.

Education

- **MCA, Galgotias University (2023 – 2025)**
  Specialization: Industry-Oriented with Computer Networks & Cybersecurity
- **B.Sc. (Hons) Computer Applications, AMU (2020 – 2023)**

Experience

- **Cyber Security Summer Intern — Gurugram Police** *(Jun 2025 – Jul 2025)*
  Worked on threat analysis, incident handling, evidence documentation, and log review. Assisted in basic digital forensics tasks and interacted with real-world investigative workflows. Studied Governance, Risk & Compliance (GRC) procedures followed in cybercrime investigations.
- **Virtual Cybersecurity Internship — Palo Alto Networks** *(Apr 2024 – Jun 2024)*
  Hands-on experience in SOC operations, log analysis, alert triage, cloud security, and threat intelligence fundamentals. Learned security monitoring, attack vectors, and response workflows through guided virtual labs.
- **Associate Software Engineer — WeVOIS Labs Pvt. Ltd.** *(Jan 2023 – Aug 2023)*
  Designed, developed, and optimized software modules. Improved UI/UX performance, collaborated with frontend teams, and enhanced application efficiency through clean code practices.

Technical Skills

- **SIEM & Monitoring:** Splunk (basic), ELK Stack, Log Analysis
- **Networking & OS:** TCP/IP, DNS, HTTP, Linux, Windows
- **Security Tools:** Nmap, Wireshark, Nessus, Burp Suite, Metasploit, SQLMap
- **Security Skills:** Alert Triage, Incident Handling, Threat Detection, Vulnerability Assessment, Windows Event Logs, False Positive Analysis, Incident Escalation

Projects

- **Blockchain Wallet Scanner (Python + Tkinter)** — Desktop application for scanning Ethereum and Solana wallet addresses. Performs transaction analysis, dApp activity review, and exports findings in JSON, CSV, and PDF formats.
- **LSHA - Linux Security Hardening Auditor (Bash)** — Automated Linux auditing tool that checks misconfigurations, weak password policies, world-writable files, SUID/SGID binaries, open ports, firewall rules, SSH security issues, cron jobs, UID 0 users, and suspicious activity in system logs.
- **Phishing Link Detector Extension** — Browser extension for real-time malicious URL detection. Uses domain reputation checks, obfuscation detection, redirect scanning, TLD risk evaluation, and fake login page identification.

Certifications & Achievements

- Certified Ethical Hacker (CEH)
- Palo Alto Networks — Cybersecurity Fundamentals, Cloud Security Fundamentals, Security Operations Fundamentals
- Participated in ICECI Conference 2023 at Aligarh Muslim University
- Secured 3rd place in Gurugram Cyber Cell CTF competition