ABHISHEK PANDEY

Cyber Security Analyst

7718089020 | abhi.pandey0219@gmail.com | Mumbai | Linkedin

SUMMARY

Skilled Cybersecurity professional with hands-on experience in SOC operations, incident response, and digital forensics. Skilled in monitoring logs, investigating anomalies, and applying security tools such as Splunk, Wireshark, Nmap, and Burp Suite. Familiar with VAPT and OWASP Top 10, with knowledge of frameworks including NIST, MITRE ATT&CK, and ISO 27001. Strong analytical skills with the ability to secure systems and support investigations.

TECHNICAL SKILLS

SIEM: Splunk (basic), log monitoring, Event correlation
Security Tools: Wireshark, Nmap, Autopsy, Burp Suite
Vulnerability Assessment & Penetration Testing (VAPT): Web Application Security Testing
Digital Forensics: Disk imaging, Memory analysis, Log analysis, Mobile analysis
Incident Response: Threat detection, Containment, Recovery
Cryptography: Encryption, Digital Signatures & Certificates, PKI
Security Framework: NIST & MITRE ATT&CK
GRC: ISO 27001, Risk assessment, Security controls, GDPR basics
Networking: Basic knowledge of TCP/IP, DNS, HTTP/S, VPNs, firewalls
Operating Systems: Windows, Linux (basic command line, file structure)
Programming Language: Python

EXPERIENCE

Cybersecurity Analyst – Digital Forensics Expert

Mahen Technologies Pvt. Ltd *Sept 2024 – Aug 2025*

- Conducted forensic acquisition, evidence preservation, and analysis of digital devices while maintaining chain of custody.
- Performed file system, memory, and network investigations using forensic tools.
- Prepared detailed forensic reports to support incident response and compliance.

PROJECTS & HAND ON EXPERIENCE

SOC Analyst (TryHackMe)

- Monitored logs using Splunk, performed alert triage, and investigated anomalies.
- Detected brute-force attacks and analyzed failed login attempts using **Wireshark** and **Nmap**.
- Identified Indicators of Compromise (IoCs) and mapped techniques using **MITRE ATT&CK**.

- Simulated phishing investigations and email header analysis.

CERTIFICATIONS

Cisco Networking Academy – Introduction to Cybersecurity **July 2025**

- Completed foundational training on global threat landscapes, attack vectors, and defense strategies.
- Applied core cybersecurity principles including confidentiality, integrity, and availability (CIA triad).
- Gained knowledge of network security controls such as firewalls, intrusion detection, and access management.
- Studied fundamentals of cryptography, authentication, and securing digital assets.

EDUCATION

- Master's degree in Information Technology 2023-2025

  Sies College of Arts, Science and Commerce, Mumbai

- Bachelor's degree in Information Technology 2020-2023

  Kirti M. Doongursee College, Mumbai

SOFT SKILLS

- Analytical thinking
- Attention to detail
- Communication
- Teamwork
- Quick Learner