

Aditi Pandey

+91 9555383986 — aditineerajpandey@gmail.com — [linkedin.com/in/aditi-pandey-033b38251/](https://www.linkedin.com/in/aditi-pandey-033b38251/) — github.com/AditiPandey-111

Profile Summary

Aspiring Cybersecurity Professional with expertise in SOC Operations, Threat Detection, Vulnerability Management, and Penetration Testing. Passionate about securing digital assets, experienced in cloud security, SIEM, incident response, self-built labs and recognised in global cybersecurity competitions.

Education

VIT Bhopal University

Bachelor of Technology in Computer Science and Engineering, CGPA: 8.58/10

Specialisation in Cyber Security and Digital Forensics

Madhya Pradesh, India

Oct. 2022 – 2026

Skills

- **Languages:** Java, Python, MySQL, JavaScript.
- **Cybersecurity Skills:** Linux, VAPT, Web Application Security, SIEM, SOC Operations, Network Security, Cloud Security (AWS, Azure), Tools: Metasploit, Wireshark, Nmap, Burpsuite, Splunk.
- **Soft Skills:** Teamwork, Problem-Solving, Event Management
- **Relevant Courses:** Data Structures and Algorithms, Database Management System, Computer Networking, Security Fundamentals, Cryptography, System Engineering, CEH Ethical Hacker Course, AWS Cloud Practitioner Course.

Project Experience

1. SIEM Integration with AI Chatbot — Microsoft Sentinel Security Automation Project

- Integrated Microsoft Sentinel with ChatGPT via logic applications to automate incident enrichment and response using AI-generated contextual insights from alerts.
- Enhanced detection and triage capabilities, strengthened skills in log correlation, security automation, and AI-driven threat analysis.
- Reduced incident response time by 50% and improved threat detection accuracy through automated AI-powered analysis.

2. Microsoft Sentinel SIEM — Real-time Cloud Threat Monitoring Cloud Security Project

- Deployed Microsoft Sentinel to simulate real-time cloud threat monitoring with Microsoft Entra ID logs and created custom analytics rules.
- Gained hands-on experience in SIEM data flow, incident lifecycle, dashboard visualization, log ingestion, threat detection, and cloud-based security operations.
- Successfully implemented a comprehensive monitoring solution covering 15+ types of security events with real-time alerting capabilities.

3. Email Monitoring System — Real-time Phishing Detection Tool Python Development Project

- Developed a real-time monitoring tool for phishing and policy violations using Python with NLP techniques and ensemble machine learning models.
- Implemented robust email content analysis and threat classification for comprehensive security monitoring.
- Achieved 97% accuracy in phishing detection, reducing manual efforts by 60% and improving threat response time by 40%.

Certifications

- Professional Cyber Security Analyst: IBM
- SOC Fundamentals
- Gen AI: IBM
- Cyber Physical System: NPTEL
- Bits and Bytes of Computer Network: Coursera

Achievements/Extracurricular

- **AmexGirl Hackathon 2024:** Selected up to the prototype round for the American Express Girl Hackathon 2024.
- **LetsDefend Lab:** Successfully caught the first alert and investigated the first incident at LetsDefend Lab.
- **Deloitte:** Cyber Job Simulation, Virtual Internship.
- **Ranked in the Top 3% globally** on TryHackMe.
- Attended Codeforces Div.3 contest.
- Member of Microsoft Club and Insights Club at VIT Bhopal.