Aditi Pandey

Email: aditineerajpandey@gmail.com
LinkedIn: https://www.linkedin.com/in/aditi-pandey-033b38251/
Mobile: +91 9555383986
GitHub: https://github.com/AditiPandey-111

Education

- **VIT Bhopal University** — Bhopal, India
  Bachelor of Technology in Computer Science and Engineering; CGPA: 8.59 — Oct. 2022 – 2026
  Specialization: Cyber Security and Digital Forensics
- **GN National Public School** — India
  Intermediate in Science: 74.6% — 2022
- **N.S. Children Academy** — India
  Matriculation: 91.5% — 2020

Skills

- **Cybersecurity Skills:** Cyber Threat Intelligence, Vulnerability Management, Offensive Security, SOC Analysis, Incident Response, Threat Detection, Security Automation, Penetration Testing
- **Security Tools:** Microsoft Sentinel, Maltego, Autopsy, Wireshark, FTK, SIEM Platforms, Network Security Monitoring, Digital Forensics Tools
- **Technical Skills:** Python (Security Scripting), Java, Linux, Network Security, Rest APIs, Cloud Security (AWS, Azure), Database Security (MySQL, PostgreSQL)
- **Methodologies:** Agile (Scrum), DevSecOps, Risk Assessment, Compliance Management, Security Architecture

Project Experience

- **SIEM Integration with AI Chatbot Security Automation Project** — *Microsoft Sentinel & ChatGPT Integration*
  - Integration: Integrated Microsoft Sentinel with ChatGPT via Logic Apps to automate incident enrichment and response using AI-generated contextual insights from alerts.
  - Skills Developed: Enhanced detection and triage capabilities, strengthened skills in log correlation, security automation and AI-driven threat analysis.
  - Impact: Reduced incident response time by 50% and improved threat detection accuracy through automated AI-powered analysis.
- **Microsoft Sentinel SIEM Cloud Security Project** — *Real-time Cloud Threat Monitoring*
  - Implementation: Deployed Microsoft Sentinel to simulate real-time cloud threat monitoring with Microsoft Entra ID logs and created custom analytics rules.
  - Experience Gained: Hands-on experience in SIEM data flow, incident lifecycle, dashboard visualization, log ingestion, threat detection, and cloud-based security operations.
  - Achievement: Successfully implemented comprehensive monitoring solution covering 15+ security event types with real-time alerting capabilities.
- **Email Monitoring System Python Development Project** — *Real-time Phishing Detection Tool*
  - Development: Developed a real-time monitoring tool for phishing and policy violations using Python, NLP, and machine learning.
  - Results: Achieved 97% accuracy in phishing detection, reducing manual efforts by 60% and improving threat response time by 40%.
  - Technical Implementation: Utilized advanced NLP techniques and ensemble machine learning models for robust email content analysis and threat classification.

Certifications

- **IBM Cyber Security Analyst:** Professional certification in cybersecurity analysis and incident response.
- **SOC Fundamentals:** Security Operations Center fundamentals and best practices.

Achievements & Extra-Curriculars

- **Amex Girl Hackathon 2024:** Selected up to the prototype selection round for the American Express Girl Hackathon 2024, focusing on cybersecurity solutions.
- **LetsDefend Lab:** Successfully caught the first alert and investigated the first incident at LetsDefend cybersecurity lab, demonstrating practical SOC analyst skills.
- **Cybersecurity Core Courses:** Cyber Physical Systems, Cybercrime and Laws, Advanced Cyber Security, Computer Networks and Security
- **Digital Forensics:** Forensic Chemistry, Digital Forensics, IBM Cyber Security Analyst Professional Program

Languages & Hobbies

Languages: English, Hindi **Hobbies:** Dance, Drawing, Reading