Last Updated:07/25

Pratham Deora

Mumbai, INDIA

Portfolio:
Contact no:+91-8005987462
Email : pdeora122@gmail.com
LinkedIn: linkdin/@pratham
GITHUB : git/@pratham
Medium Blog: medium/@pratham
TryhackMe: tryhackme/@pratham

Profile

Cybersecurity professional with experience in the cybersecurity, artificial intelligence, and cloud infrastructure domains. Experience in securing systems, networks, and web applications through vulnerability assessments and risk management. Skilled in Python automation and AI integration, developing tools that enhance threat detection and response capabilities. Knowledgeable in deploying secure infrastructure on AWS and Azure cloud platforms. Technical writer with the ability to explain complex concepts in cybersecurity, AI, and cloud technologies to diverse audiences. Continuously learning new technologies and frameworks across multiple domains to deliver effective solutions.

Skills

Hard Skills:

- SIEM Tools: LogRhythm (hands-on experience), Splunk, Elastic Stack (ELK)
- Threat Detection: Suricata, Snort, Zeek (basic exposure)
- Packet Analysis: Wireshark, TCPDump
- Endpoint Security: Microsoft Defender, CrowdStrike Falcon (familiar)
- Log Analysis: Syslog, Windows Event Logs, Firewall Logs, Proxy Logs
- Ticketing Systems: ServiceNow, JIRA
- Threat Intelligence: VirusTotal, AbuseIPDB, Anomali (basic usage)
- Scripting (Basic): Bash, PowerShell (for automation/troubleshooting)
- Networking: TCP/IP, OSI Model, NAT, DNS, DHCPa

Soft Skills:

- Communication
- Problem Solving
- Adaptability
- Project Management
- Teamwork
- Critical Thinking

Education

09/2022 - 07/2025

Bachelor of Engineering, Computer Engineering, Yadavrao Tasgaonkar Institute of Engineering And Technology, Neral, India

- Key Competencies : Networking, Operating System, Python, Java, Machine Learning, Artificial Inteligence

08/2020 - 08/2022

Diploma, Computer Science & Engineering, Bhausaheb Vartak Polytechnic, Vasai, Maharashtra

- Key Competencies : Web Technology, Software Engineering, Computer Networking.
- Percentage: 81%

Experience

04/2025 - Current

Intern
***DIGIVED ACADEMY*, REMOTE**

- Basics of networking (TCP/IP, ports, protocols)
- Operating systems (Windows, Linux)
- Security fundamentals (CIA triad, firewalls, VPNs)
- Malware analysis, phishing, social engineering
- Cryptography basics
- Incident response
- Vulnerability scanning / penetration testing
- **Tools Practiced**: Wireshark, Kali Linux, Nessus, VirtualBox, Burp Suite.
- **Courses Enrolled:** TryHackMe, Hack The Box, OverTheWire etc.

Projects

- **SIEM Log Monitoring with Splunk** — Built a basic SOC lab to ingest logs and detect brute-force attacks and suspicious IP activity.
- **Threat Hunting on TryHackMe** — Completed multiple incident response and threat detection labs using log correlation and IOC hunting.
- **Network Packet Analysis with Wireshark** — Inspected live packet captures to identify potential MITM and DNS poisoning attempts.

Certificate

2025 CompTIA Security+ (Preparing) CompTIA