

# Pratik Anil Pawar

[pawar.pratik@hotmail.com](mailto:pawar.pratik@hotmail.com) | +91 9021171814 | [LinkedIn Profile](#)

---

## CAREER SUMMARY

---

Cybersecurity fresher with foundational knowledge in SOC operations, SIEM log analysis, and identity security workflows. Certified in CompTIA Security+ and Google Cybersecurity. Learning hands-on detection scenarios on LetsDefend platform covering SIEM analysis, phishing triage, and malware investigation. Seeking Cyber Security Engineer role to contribute to enterprise security operations.

## TECHNICAL SKILLS

---

- **Core Competencies:** SOC Operations, SIEM Log Analysis, Threat Detection, Incident Response Fundamentals, MITRE ATT&CK Mapping, OWASP Top 10 Vulnerabilities, Zero Trust Principles
- **SIEM & Log Management:** Splunk; Microsoft Sentinel, 365 Security & Compliance Center; Wazuh.
- **Endpoint & Network Security:** Microsoft Intune, Microsoft Defender EDR, CrowdStrike Falcon
- **DLP and Web Proxy:** Netscope, Zscaler
- **Network Packet Inspection and Monitoring:** tcpdump, Nmap, Wireshark
- **Firewalls & Network Defense:** FortiGate, Checkpoint Firewall, Palo Alto Networks, Snort IDS/IPS, Suricata
- **Cloud Security:** Microsoft Defender for Cloud, Azure Security Fundamentals
- **Vulnerability Management:** Qualys
- **AI-Assisted Security:** Microsoft Security Copilot
- **Scripting & Automation:** Python, Bash, GitHub Copilot, Cursor AI
- **Incident Response Capabilities:** Alert triage, IOC enrichment, SIEM log analysis, phishing triage, post-incident reporting, security auditing
- **Ticketing & Collaboration:** Jira
- **Operating Systems:** Windows, Linux (Ubuntu)

## EDUCATION

---

- Bachelor of Science in Electronics – Solapur University, 2025 | CGPA: 9.58
- Senior Secondary (Class 12) – Maharashtra State Board, 2020 | 67.23%
- Secondary (Class 10) – Maharashtra State Board, 2018 | 90.20%

## TECHNICAL PROJECTS

---

### n8n-based Phishing Email Analyzer:

- Engineered an n8n-based workflow to classify emails (Outlook & Gmail) as benign, suspicious, or phishing.
- Integrated Microsoft Graph API and Gmail API to extract MIME headers, URLs, and attachments for threat analysis.
- Automated IOC enrichment via Python reputation checks and Splunk HTTP Event Collector for correlation.
- **Tools Used:** n8n, Python, Splunk, Microsoft Graph API, Gmail API

### LetsDefend Hands-On SOC Detection Labs:

- Learning hands-on detection scenarios covering SIEM analysis, phishing triage, malware investigation, and web attack detection.

## CERTIFICATIONS

---

- [CompTIA Security+](#), 2025
- [Google Cybersecurity](#), 2025