

Prabhakar Pavan Penumarthi

✉ prabhakarpavan.penumarathi@gmail.com | 📞 +91 9966208050 | 📍 Hyderabad
Security Analyst | SOC Operations | Incident Response & Threat Detection

Professional Summary

Hands-on cybersecurity professional with **2+ years of experience** in SOC operations and vulnerability management. Skilled in **SIEM tools (Splunk, QRadar), malware and email analysis, penetration testing, and secure system configuration** across **Linux and Windows environments**. Adept at **threat detection, incident triage, and remediation strategies**, with hands-on experience in **Nmap, Wireshark, Metasploit, Burp Suite, OWASP ZAP, Shodan, Censys, VirusTotal**. Strong knowledge of **cyber kill chain methodology** and a proven record of improving detection and reducing risk.

Technical Highlights

- **SIEM Tools:** Splunk, IBM QRadar
 - **Vulnerability Assessment & Testing:** Nessus, Qualys, OpenVAS, Burp Suite, OWASP ZAP
 - **Penetration Testing:** Nmap, Wireshark, Metasploit, Nikto
 - **Security Monitoring & Threat Detection:** IOC Analysis, Log Correlation, Threat Detection
 - **Malware & Email Analysis:** Malware Analysis, Phishing Investigation, Sandbox (Cuckoo, ANY.RUN)
 - **EDR:** SentinelOne
 - **Networking:** TCP/IP, Firewalls, IDS/IPS, VPN, VLANs, DHCP, DNS
 - **Operating Systems:** Windows & Linux (Kali, Parrot, Ubuntu)
 - **IT Operations & Security Configurations:** Active Directory, Group Policy, Secure Hardening
 - **ITSM Tools:** ServiceNow (Basic Knowledge)
-

Experience

Security Analyst – SOC Level 1

Karur Vysya Bank, Information Security Group

- Monitored and investigated 500+ daily security events in a 24×7 SOC environment using Splunk SIEM, identifying and escalating critical incidents with 100% SLA compliance.
- Reduced false positives by 20% through advanced log analysis of Windows events, firewall traffic, and IDS/IPS alerts.
- Conducted phishing and malware investigations, mitigating 15+ potential security incidents per month and improving organizational resilience.
- Performed Level 1 triage of endpoint and network threats, coordinating with senior analysts to drive timely incident containment and remediation.
- Enhanced overall SOC efficiency by implementing improved detection rules and streamlined escalation procedures, reducing average response time by 25%.

Cybersecurity Intern / Project Trainee – SOC & Penetration Testing

Independent Projects & Training

- Conducted vulnerability assessments and penetration testing using Nessus, Burp Suite, Nmap, and Metasploit, identifying and documenting exploitable weaknesses.
- Optimized SOC workflows by reducing lab false alerts 15% through improved log analysis and event correlation in Splunk and IBM QRadar.
- Performed malware and phishing investigations on 20+ samples using VirusTotal, Hybrid Analysis, and IBM X-Force, producing actionable reports for incident response practice.
- Hardened Linux and Windows systems with secure configuration, minimizing attack surfaces in simulated enterprise environments.
- Delivered detailed remediation recommendations, increasing SOC lab efficiency by 30% and strengthening security readiness.

Key Projects

- **Windows Security Event Investigation (Splunk):** Detected failed logins, brute-force attempts, and unauthorized access in lab simulations; built correlation rules to strengthen detection.
 - **Simulated SOC & Attack Analysis:** Deployed a lab SOC with Splunk, IBM QRadar, and Open EDR; created custom alerts and correlated logs, reducing false positives by 20% while tracing full attack chains.
 - **Malware Behavior Analysis:** Analyzed malware samples in Cuckoo Sandbox and ANY.RUN; simulated phishing and injection attacks; integrated detection results into SIEM workflows, improving analyst training efficiency by 25%.
-

Certifications

- **CompTIA Security+** – In Progress (Expected 2025)
 - **Google Cybersecurity Certificate** – Coursera (2024)
 - **TryHackMe** – Hands-on Labs & CTF Challenges (Ongoing)
-

Education

- **MBA in Finance & Marketing** – Ideal College, Andhra University
 - **Bachelor of Science (Computers)** – Aditya Degree College
-