




Purav Umesh

 +91-9900085466

 puravumesh33@gmail.com

 Bangalore, Karnataka, India

 www.linkedin.com/in/purav-umesh

Professional Summary

Dedicated and results-driven Cybersecurity professional with hands-on experience as a SOC Analyst. Strong background in threat detection, log analysis, SIEM monitoring, and incident response. Adept at investigating alerts, managing security events, and mitigating risks using industry-standard tools. Committed to protecting organizational assets and proactively improving the security posture through real-time monitoring, documentation, and team collaboration.

Technical Skills

- Cybersecurity Tools: Nmap, Metasploit, Burp Suite, Wireshark, OWASP ZAP, Nuclei, SqlMap, Nessus, Nikto, OpenVAS, Splunk, ELK Stack, Wazuh, QRadar
- Frameworks & Standards: ISO 27001, NIST, OWASP Top 10, MITRE ATT&CK, OSI Model, TCP/IP
- SIEM Monitoring and Analysis
- Security Operations Center (SOC)
- Threat Detection & Response
- Log Analysis & Correlation
- Vulnerability Management
- Network & Endpoint Security
- Incident Handling & Escalation
- Malware & Phishing Investigation

Soft Skills

- Analytical and Problem-Solving Skills
- Clear Communication (Verbal & Written)
- Detail-Oriented Approach
- Team Collaboration
- Quick Learner and Adaptive

Experience

SOC Analyst

RedTeam Hacker Academy – Bangalore, India

– January 2025

- Monitored security alerts using SIEM tools like Splunk and Wazuh.
- Investigated potential threats such as brute-force attacks, phishing, malware infections, and privilege escalation.
- Documented incident details, created playbooks, and improved detection rules.
- Performed log correlation and threat hunting activities to identify hidden anomalies.
- Responded to incidents in real-time, reducing response time by 35%.
- Collaborated with senior analysts and reported critical incidents with complete evidence and mitigation steps.

Education

Bachelor of Commerce (B.Com)

Bangalore University – Cybersecurity Specialization

2022 – 2025

Projects

1. Real-Time Log Monitoring using Wazuh SIEM

- Deployed Wazuh across endpoints and configured custom alert rules.
- Monitored authentication failures, file integrity, and unauthorized access.
- Created dashboards to visualize incident trends and attack patterns.

2. Phishing Attack Simulation & Response

- Conducted a phishing simulation across a test network.
- Detected and analyzed phishing emails and suspicious domains.
- Documented response steps including isolating endpoints and notifying users.

3. Incident Response Playbook Development

- Designed structured playbooks for malware outbreaks, DDoS attacks, and insider threats.
- Streamlined investigation steps, making response more efficient and standardized.

Certifications

- Certified SOC Analyst (CSA) – EC-Council
- Certified IT Infrastructure and Cyber SOC Analyst – RedTeam Hacker Academy
- Certified Penetration Tester (CPT) – RedTeam Hacker Academy