UTKARSH WALCHALE

Certified Ethical Hacker

+91 9403906859 | utkarshwalchale05@gmail.com | GitHub | LinkedIn

EXECUTIVE SUMMARY

Proactive **Cybersecurity Analyst** with hands-on experience in **SOC monitoring, threat analysis, and incident response.** Certified Ethical Hacker (CEH) skilled in identifying, analyzing, and mitigating cyber threats using **SIEM tools, firewalls, and endpoint solutions.** Strong foundation in **network security, log analysis, and cloud environments (AWS & Azure).** Passionate about defending complex infrastructures and contributing to IBM's Cyber Fusion Center mission to secure global clients through innovation, automation, and intelligence-driven defense.

KEY SKILLS

- **Security Operations:** SIEM (Splunk), SOAR, IDS/IPS, EDR/XDR, Log Analysis, Threat Detection
- **Operating Systems:** Linux (Ubuntu, RHEL), Windows
- **Tools & Frameworks:** Wireshark, Suricata, Snort, Nessus, Nmap, Burp Suite, Metasploit
- **Cybersecurity Tools:** Nmap, Burp Suite, Nessus, Metasploit, Wireshark, SIEM, Splunk
- **Networking:** TCP/IP, VPN, DNS, Firewalls, Proxies
- **Scripting:** Python, Bash (for automation and alert parsing)
- **Certifications** – Certified Ethical Hacker (CEH), Upskilling in AI/ML for security

PROJECTS & RESEARCH

AI-Powered Deepfake Detection System (Academic Research Project)

- » Designed a multi-modal AI model to detect manipulated media, focusing on **threat intelligence and anomaly detection**.
- » Applied explainability techniques to improve model transparency for forensic analysis.

SIEM Lab – Brute Force Attack Detection:

- » Simulated SSH brute-force attempts with Hydra, ingested syslog via Splunk Universal Forwarder.
- » Built **SPL correlation searches, dashboards, and automated alerts** for incident detection.

SOC Brute-Force Detection & Analysis

- » Built a **Colab-based brute-force attack detection simulation** with synthetic log generation, feature extraction, and SOC analysis logic.
- » Designed **detection pipelines and visualizations** to identify suspicious login patterns and attacker behavior using Python and pandas.

PROFESSIONAL EXPERIENCE

Cybersecurity Intern | *Omni-Bridge Solutions, Nagpur* **05/2025 – 07/2025**

Key Achievements:

- ▪ Monitored anomalies in databases using **IBM Guardium (DAM tool)**, improving data security posture.
- ▪ Supported **Linux system hardening** and compliance initiatives for enterprise clients.
- ▪ Created governance reports and dashboards for anomaly detection and escalation.

Cybersecurity Intern| Crux HR, Bangalore **02/2025 – 05/2025**

Key Achievements:

- ▪ Performed web app penetration testing using Burp Suite, identified OWASP Top 10 vulnerabilities.
- ▪ Documented issues with risk prioritization and remediation guidance for developers.

EDUCATION & PROFESSIONAL DEVELOPMENT

Bachelor Of Technology (Computer Science and Engineering) - 2025
Walchand Institute of Technology, Solapur. | **CGPA: 9.2**