

GAJRAJ SINGH

+91 9910147939 • Delhi-94, India • [LinkedIn](#) | [GitHub](#) • gajrajch238@gmail.com

PROFESSIONAL SUMMARY

Entry-level SOC Analyst with practical experience in incident response, log analysis, threat detection, and vulnerability management. Skilled with SIEM tools (Splunk, ELK), Wireshark, Nessus, and Snort/Zeek. Completed SOC Level 1 (TryHackMe) and the 30-Day SOC Challenge, gaining hands-on exposure to alert triage, network forensics, phishing analysis, and endpoint monitoring. Strong grasp of security frameworks (MITRE ATT&CK, NIST CSF, OWASP Top 10). Currently pursuing MCA to further expertise in cybersecurity.

TECHNICAL SKILLS

- **SIEM & Monitoring:** Splunk (Basic), ELK, Wireshark, TcpDump, Log Analysis
- **Threat & Vulnerability Management:** Nessus, Burp Suite, Metasploit, SQLMap, Nikto, OWASP ZAP
- **Endpoint & EDR:** Wazuh, Sysmon, Osquery
- **Incident Response & Forensics:** Phishing analysis, IOC investigation, Volatility, Autopsy (basics)
- **Programming & Scripting:** Python, Bash (for automation & log parsing), C++, Java and C
- **Frameworks:** MITRE ATT&CK, NIST CSF, OWASP Top 10

PROFESSIONAL EXPERIENCE

Security Intern | Cyber Allegiance | Completed April 2025 - June 2025

- Conducted vulnerability assessments and mapped findings to CVSS scoring.
- Reviewed security logs to support proactive detection and container hardening.
- Contributed to secure SDLC pipelines with SAST/DAST reviews.

Cybersecurity Intern | IBM Skillbuild Program | Completed June 2023 - July 2023

- Assisted the SOC team in log analysis, incident response, and alert triage.
- Participated in threat detection exercises and phishing simulations.
- Contributed to training documentation and remediation planning.

PROJECTS

SOC Projects & Training

- SOC Level 1 Path (TryHackMe) + 30-Day SOC Challenge (LinkedIn)
- Completed hands-on labs and challenges simulating SOC workflows:
 - Log Analysis & SIEM: Investigated alerts with Splunk/ELK, built detection rules, and created dashboards.
 - Network Forensics: Analyzed packet captures using Wireshark/TShark; developed Snort/Zeek rules to detect anomalies.
 - Endpoint Monitoring: Used Sysmon, Osquery, and Wazuh for real-time detection and correlation of suspicious activity.
 - Incident Response & DFIR: Practiced evidence collection, containment, and recovery aligned with MITRE ATT&CK.
 - Phishing & Threat Analysis: Examined email headers/payloads, identified IOCs, and conducted malware artifact investigations.

EDUCATION

- **Master of Computer Applications (MCA) (In Progress, Expected 2027)**
Jain University, Bengaluru | 2025–2027
- **Bachelor of Computer Applications (BCA) (Completed)**
JCC Community College, Delhi | 2021–2024

CERTIFICATIONS & TRAINING

- **EC-Council CEH** – Certified Ethical Hacker (Scheduled: Nov 2025)
- **Google Cybersecurity Analyst** Certificate (6-month program)
- **TryHackMe:** SOC Level 1 Path, Junior Penetration Tester Path
- **NPTEL:** Practical Cybersecurity (91%), Ethical Hacking (66%), Cybersecurity & Privacy (57%)