Ritika Malhotra

Cybersecurity Analyst

ritika.malhotra@example.com +91 81XXX XXX24 New Delhi, Delhi linkedin.com/in/ritika-malhotra-example

PERSONAL STATEMENT

Cybersecurity analyst with 4 years of SOC and incident-response experience for banking and e-commerce clients. Works with Splunk, Microsoft Sentinel, CrowdStrike EDR and Tenable, maps detections to MITRE ATT&CK, and supports CERT-In incident reporting and ISO 27001 audits.

WORK EXPERIENCE

SOC Analyst L2 · **Indraprastha Cyber Defence Pvt Ltd, New Delhi** Jan 2024 – Present

- Investigate and triage escalated alerts in Splunk and Microsoft Sentinel for 3 BFSI clients, handling about 60 L2 cases a week.
- Tuned 45 correlation rules and suppressed noisy alerts, cutting false positives by 38% and mean time to triage from 40 to 18 minutes.
- Led containment for a phishing-driven credential-theft incident within 2 hours and prepared the CERT-In report within the 6-hour window.
- Wrote 20 playbooks mapped to MITRE ATT&CK for ransomware, account takeover and data exfiltration scenarios.

Security Analyst · **Yamuna Secure Networks, Noida** Jun 2022 – Dec 2023

- Ran monthly vulnerability scans with Tenable Nessus across 1,800 assets and tracked remediation with IT teams, reducing critical findings by 70% in 6 months.
- Monitored firewall, proxy and EDR alerts in a 24x7 SOC and escalated confirmed incidents as per SLA.
- Supported ISO 27001 surveillance audits by preparing evidence for access reviews and log retention.

EDUCATION

B.Tech in Computer Science and Engineering · **Delhi Institute of Engineering and Management, New Delhi** 2018 – 2022

Grade: 8.0 CGPA

SKILLS

Splunk · Microsoft Sentinel · CrowdStrike EDR · Tenable Nessus · Wireshark · MITRE ATT&CK · KQL / SPL queries · Phishing analysis

CERTIFICATIONS

Certified Ethical Hacker (CEH) · **EC-Council**
Dec 2022

CompTIA Security+ · **CompTIA**
Sep 2023

Microsoft Certified: Security Operations Analyst Associate (SC-200) · **Microsoft**
Mar 2025

LANGUAGES

English · Professional

Hindi · Native

Punjabi · Conversational

CORE SKILLS

- Security monitoring
- Incident response
- Threat hunting
- Vulnerability management
- Security reporting

MakeMyPerfectResume · Free