Mohammed Salman

Cybersecurity Analyst · SOC · Red Team · DFIR

📍 Hyderabad, India ☎ +91 9392964293 ✉ mohammedsalman6944@gmail.com

🔗 www.linkedin.com/in/mohammed-salman04

PROFESSIONAL SUMMARY

Cybersecurity practitioner combining defense and offense: build and tune SOC workflows, execute red-team style evaluations, and perform DFIR investigations to close detection gaps. Hands-on with training labs and clear incident playbooks used by peers.

EXPERIENCE

Cybersecurity Intern — CodeZen Eduversity (ISO Certified)

Aug 2025 – Present

- Operate SOC monitoring and triage security incidents; escalate and document findings.
- Design and execute red-team style engagements to evaluate detection & response readiness.
- Lead DFIR activities: evidence collection, static/dynamic malware analysis, and reporting.
- Proactive detection using SIEM and endpoint telemetry, with measurable tuning improvements.

Security Analyst Intern — Infotact Solutions

Mar 2025 – Jun 2025

- Built cybersecurity labs for blue/red team exercises and internal training curricula.
- Configured and optimized SIEM platforms (Splunk, Wazuh, ELK) for log ingestion and alerting.
- Tuned IDS/IPS rulesets to reduce false positives and increase signal quality.
- Deployed deception assets to capture adversary TTPs and generate intelligence reports.

Security Analyst Intern — Full Stack Academy

Aug 2024 – Nov 2024

- Monitored environments with Microsoft Sentinel, Wazuh, and Splunk for anomalous activity.

- Conducted forensic investigations and log analysis to trace incidents end-to-end.
- Performed offensive testing to identify vulnerabilities and recommend remediation.

EDUCATION

BCA — Dhruva Degree College

Jun2022–Jun2025 · GPA:8.0

Coursework: Networking, Databases, Programming, Web Technologies

Intermediate (MPC)

2020–2022 · GPA:7.0

Mathematics, Physics, Chemistry; strengthened analytical thinking, problem-solving, and technical foundation

SSC

2019–2020 · GPA: 10.0

Core foundation in Science, Mathematics, and Languages; academic excellence and discipline

SKILLS

- SOC Monitoring & Incident Response
- Detection Engineering & Intelligence
- Red Teaming & Adversary Emulation
- Digital Forensics & Malware Analysis
- SIEM / EDR / IDS-IPS Tuning
- Python & Bash Scripting
- Security Lab Architecture

TOOLS & TECH

Splunk · Wazuh · Microsoft Sentinel · ELK · Suricata · Snort · Ghidra · Volatility

CERTIFICATIONS

- CodeZen Eduversity — SOC / Red Teaming / DFIR (Internship, ISO-aligned)
- Hands-on labs: SIEM, Forensics, IDS/IPS, Investigation

PROJECTS

- Self-hosted CTF Lab: Deployed a vulnerable web lab with SQLi, XSS, LFI challenge tracks.
- Deception Network & Analysis: Traps captured attacker activity; analyzed to extract IOCs.
- Investigation Toolkit: Scripts to parse SIEM alerts and enrich events for faster investigation.

- Collaborated with peers to improve detection workflows and optimize SOC processes.

ACHIEVEMENTS & IMPACT

- Organized and managed a self-hosted CTF lab for peer learning.
- Led a small cybersecurity team and ensured smooth project completion.
- Consistently delivered assigned tasks on time while maintaining quality and accuracy.