Mohammed Salman

Cybersecurity Analyst · VAPT · SOC · Blue Team

Hyderabad, India | +91 9392964293 | mohammedsalman6944@gmail.com | www.linkedin.com/in/mohammed-salman04

PROFESSIONAL SUMMARY

Entry-level Cybersecurity Analyst with hands-on experience in SOC operations, VAPT, and SIEM monitoring across real-world client environments. Proven ability to identify high-severity vulnerabilities, automate security workflows using n8n, and support incident triage and log analysis. Skilled in Splunk, Microsoft Sentinel, Wazuh, OWASP Top 10, and security reporting. Seeking a SOC L1 or Cybersecurity Analyst role to contribute to defensive security operations.

KEY HIGHLIGHTS

- Discovered 10+ high-severity security vulnerabilities across 4 real-world client environments
- Reduced manual SOC and reporting effort by automating workflows using n8n
- Hands-on experience with SIEM monitoring, alert triage, and log analysis
- Strong alignment with SOC L1, VAPT Analyst, and Blue Team roles

EXPERIENCE

Cybersecurity Intern — CodeZen Eduversity (ISO Certified)

Aug 2025 – Present

- Performed Vulnerability Assessment & Penetration Testing (VAPT) for 4 clients (1 international, 3 domestic) across web applications and infrastructure.
- Identified and validated 10+ high-severity and critical vulnerabilities including SQL Injection, Stored/Reflected XSS, Authentication Bypass, Access Control Flaws, and Security Misconfigurations using automated and manual testing.
- Conducted automated vulnerability scanning and exploitation validation, reducing false positives and improving remediation accuracy.
- Designed and implemented an n8n automation workflow to streamline vulnerability reporting and alert correlation, reducing manual security effort by ~30–40%.
- Prepared client-ready VAPT reports with CVSS scoring, PoC, and remediation guidance, aligned with OWASP Top 10 and CWE.
- Supported SIEM configuration and alert tuning using Splunk, Wazuh, and Microsoft Sentinel.

Security Analyst Intern — Infotact Solutions

Mar 2025 – Jun 2025

- Assisted in SOC monitoring and initial security incident triage.
- Conducted log analysis using SIEM platforms and supported IDS/IPS rule optimization.
- Documented incidents, investigation steps, and escalation workflows.

- Performed offensive testing to identify vulnerabilities and recommend remediation.

Security Analyst Intern — Full Stack Academy

Aug 2024 – Nov 2024

- Conducted forensic investigations and log analysis to trace incidents end-to-end.
- Mapped security alerts to MITRE ATT&CK framework for threat classification and analysis.
- Collaborated with peers to improve detection workflows and optimize SOC processes.
- Consistently delivered assigned tasks on time while maintaining quality and accuracy.

SKILLS

Security Domains:

SOC Operations, Incident Response, Vulnerability Assessment & Penetration Testing (VAPT), Web Application Security, Threat Intelligence, DFIR (Basic)

Attack Techniques:

SQL Injection, XSS, LFI, Authentication Bypass, Security Misconfiguration

SIEM & Security Tools:

Splunk, Microsoft Sentinel, Wazuh, ELK, Suricata, Snort

Scripting & Automation:

Python, Bash, n8n Workflow Automation

TOOLS & TECH

Splunk · Wazuh · Microsoft Sentinel · ELK · Suricata · Snort · Ghidra · Volatility · n8n

PROJECTS

Self-Hosted Vulnerable Web Application (CTF Lab)

Designed and deployed a vulnerable web application featuring SQLi, XSS, and LFI challenges. Organized and managed a self-hosted CTF lab for peer learning.

Deception Network & Attack Analysis

Implemented deception assets to capture attacker activity and extract IOCs and TTPs. Traps captured attacker activity; analyzed to extract IOCs.

Investigation Toolkit

Scripts to parse SIEM alerts and enrich events for faster investigation.

CERTIFICATIONS

Ethical Hacker — Cisco Networking Academy (Nov 2023)
Penetration testing, vulnerability assessment, exploitation, and defensive security labs.

Cyber Threat Management — Cisco Networking Academy (Nov 2023)
Threat intelligence, risk assessment, and incident management.

Network Defense Essentials — EC-Council (Nov 2023)

IDS, perimeter defense, and network security best practices.

Responding to a Zero-Day Vulnerability — AIG (Forage) (Jan 2025)

Zero-day response and ransomware mitigation simulation.

Cybersecurity Analyst — AIG (Forage) (Nov 2024 – Jan 2025)

IAM fundamentals, IAM strategy assessment, and enterprise identity solutions.

EDUCATION

BCA — Dhruva Degree College

Jun 2022 – Jun 2025 · GPA: 8.0

Coursework: Networking, Databases, Programming, Web Technologies

Intermediate (MPC) — OS Junior College

2020 – 2022 · GPA: 7.0

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

SSC — OS International School

2019 – 2020 · GPA: 10.0

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

ACHIEVEMENTS & IMPACT

- Delivered VAPT assessments for four real-world clients with professional reports and remediation guidance.
- Discovered 10+ high-severity vulnerabilities across client environments, improving their security posture.
- Automated security workflows using n8n, reducing manual effort by 30–40%.
- Collaborated with peers to improve detection workflows and optimize SOC processes.
- 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.