

MARSHALL R

SOC Analyst / Security Operations Fresher — Linux — Python Automation
+91-9150321317 — marshall06rs@email.com — [LinkedIn](#) — [GitHub](#) — [Portfolio](#)

EXECUTIVE SUMMARY

Entry-level SOC Analyst (L1) with hands-on exposure to 24x7 security monitoring and alert triage using Splunk SIEM. Experienced in basic Linux and Windows log analysis and understanding of common security threats. Open to 24x7 rotational shifts and eager to grow in a Security Operations role.

EDUCATION

Bachelor of Engineering in Computer Science and Engineering, Jerusalem College of Engineering (2021 – 2025)
CGPA: 7.21
HSC (2020 – 2021) – 79%, SSLC (2018 – 2019) – 67%

SKILLS

Security Tools	Splunk (SIEM), Nessus, Burp Suite, Nmap, Wireshark
SOC Skills	24x7 monitoring, alert triage, incident investigation, escalation
Log Analysis	Linux and Windows logs, basic firewall and network logs
Networking	TCP/IP, DNS, HTTP/HTTPS
Security Concepts	OWASP Top 10, basic incident response
Scripting	Python (basic automation), Bash/Shell (basic)
Version Control	Git, GitHub

EXPERIENCE

Security Operations / IT Security Intern Dec 2024 – Jan 2025
TVS Electronics Ltd – Digital IT Team *Chennai*

- Assisted in reviewing application and system logs for errors, anomalies, and suspicious activity
- Supported basic security checks, secure data handling, and input validation processes
- Participated in incident investigation and supported issue analysis and resolution

Database Intern Jan 2025 – Feb 2025
Leiten Technologies Private Limited *Chennai*

- Worked with SQL databases ensuring secure queries and data integrity
- Assisted backend logic implementation aligned with access control principles
- Supported system monitoring and basic troubleshooting activities.

PROJECTS

Electricity Theft Detection Mechanism (Final Year Project). Built simulation models using MATLAB and PROTEUS to detect abnormal voltage deviations and consumer-end voltage drops indicating electricity theft.

Python Web Application Vulnerability Scanner ([GitHub](#)). Developed a Python-based scanner to detect XSS, IDOR, and SQL Injection vulnerabilities by analyzing HTTP requests and parameters, Mapped identified vulnerabilities to OWASP Top 10 categories

SOC Practice Lab using Splunk ([View](#)). Performed security monitoring and alert triage by analyzing Linux and Windows logs using Splunk. ingested logs into Splunk, created dashboards, and escalated alert investigation.

CERTIFICATIONS

Cybersecurity & Ethical Hacking – Boston Institute of Analytics

Learn Art of Hacking Through Programming – Self Made Ninja Academy