MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

CAREER ROADMAP · 2026 EDITION

# SOC Analyst L1 → L2 → L3 Career Roadmap — India 2026

A practical detection-and-response pathway covering logs, SIEM, EDR, triage, incident handling, and career progression.

| 3 | 8 | 5 |
|---|---|---|
| Role levels | Core skills | Portfolio cases |

MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

# How to use this guide

Treat this roadmap as a competency plan, not a promise of salary or employment. Demonstrated skill, communication, ethics, consistency, and local market conditions all matter.

> **Professional-use notice:** Security testing must stay within systems you own or have explicit written authorization to assess. Standards summaries are educational aids, not certification, legal, or audit advice.

## Inside this resource


**01** **Role & Outcome Map**
Know the work you are preparing to perform and the evidence employers can evaluate.

**02** **12-Month Learning Path**
Progress through foundations, applied practice, portfolio evidence, and job readiness.

**03** **Weekly Operating System**
Build consistency with deliberate practice and visible evidence.

**04** **Portfolio Projects**
Create proof of skill without exposing secrets, customer data, or unsafe instructions.

**05** **Skills & Interview Gates**
Advance only when you can explain, demonstrate, and document the outcome.

**06** **Learning Resources & Next 90 Days**
Start small, measure outputs, and adjust based on evidence.

# Role & Outcome Map

Know the work you are preparing to perform and the evidence employers can evaluate.

### SOC Analyst L1

Entry role focused on supervised execution and documentation.

### MDR Analyst

Growing role requiring independent investigation and prioritization.

### Cybersecurity Operations Analyst

Engineering role connecting security controls with systems and software.

### Incident Response Intern

Specialized role reached through deeper practice and delivery experience.

# 12-Month Learning Path

Progress through foundations, applied practice, portfolio evidence, and job readiness.

### Months 1–2 · Core IT

Networking, Windows/Linux administration, identity, common protocols, security fundamentals, and precise ticket writing.

### Months 3–4 · Logs & SIEM

Learn Windows events, Sysmon, authentication, DNS, proxy, firewall, cloud audit logs, queries, dashboards, and alert context.

### Months 5–6 · L1 Triage

Classify alerts, validate indicators, enrich evidence, map activity, set severity, document escalation, and avoid premature conclusions.

### Months 7–8 · Incident Analysis

Build timelines, investigate phishing, malware execution, account compromise, persistence, and lateral movement in controlled datasets.

### Months 9–10 · Detection Engineering

Write and tune detections, understand false positives, build validation tests, map telemetry gaps, and measure alert quality.

### Months 11–12 · Career Launch

Create case reports and dashboards, practise shift handover and interviews, target SOC/MDR/CSIRT roles, and track applications.

# Weekly Operating System

Build consistency with deliberate practice and visible evidence.

| Weekly block | Suggested activity |
| --- | --- |
| Concept learning | 3–4 hours of focused study and notes |
| Hands-on practice | 5–7 hours in legal labs or datasets |
| Documentation | One polished diagram, write-up, query, or checklist |
| Review | Revisit mistakes and create spaced-repetition cards |
| Community/career | One meaningful interaction, application, or feedback request |

**Rule:** Quality beats streaks. Every practical artifact should show the problem, method, evidence, conclusion, and remediation or improvement.

# Portfolio Projects

Create proof of skill without exposing secrets, customer data, or unsafe instructions.

**Project 1**
Authentication anomaly investigation

**Project 2**
Phishing email and header analysis

**Project 3**
Endpoint process-tree case

**Project 4**
DNS/proxy exfiltration case

**Project 5**
SIEM detection with test dataset

# Skills & Interview Gates

Advance only when you can explain, demonstrate, and document the outcome.

**Foundation gate**
Explain core protocols, operating systems, identity, and troubleshooting without relying on memorized tool output.

**Practitioner gate**
Complete a scoped task, preserve evidence, recognize uncertainty, and recommend an appropriate fix.

**Professional gate**
Prioritize business impact, communicate to different audiences, handle constraints, and improve team process.

**Interview preparation**
Use concise STAR examples grounded in your own projects; never claim tools or findings you cannot explain.

**Job search**
Tailor résumé evidence to role requirements, track applications, request feedback, and iterate monthly.

# Learning Resources & Next 90 Days

Start small, measure outputs, and adjust based on evidence.

- MITRE ATT&CK
- Sigma detection rules
- Microsoft security documentation
- CISA incident response resources

### Days 1–30

Baseline your skills, set up a legal practice environment, and finish one small project.

### Days 31–60

Complete a focused learning path and publish a sanitized, reviewed portfolio artifact.

### Days 61–90

Run a capstone scenario, practise explanation and interview questions, then begin targeted applications or deeper specialization.




# Keep learning. Keep building.

Use this guide as a working plan: practise, document evidence, review outcomes, and improve the next iteration.

mnatech.in @mna_tech_academy +91 9216110094

© 2026 MNA Tech Academy. Original educational resource. Product names and trademarks belong to their respective owners. Verify standards and product details against official sources before production use.