MNA TECH ACADEMY
LEARN • PRACTICE • SUCCEED

CAREER ROADMAP · 2026 EDITION

AI Security & ML Engineer Career Roadmap 2026

Bridge software security, machine learning, LLM application risk, model evaluation, and secure AI operations.

4	6	12
Skill pillars	Projects	Months

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.

AI Security Intern

Entry role focused on supervised execution and documentation.

Product Security Engineer — AI

Growing role requiring independent investigation and prioritization.

ML Platform Security Engineer

Engineering role connecting security controls with systems and software.

AI Red Team Associate

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 · Engineering Base

Python, data structures, APIs, Git, testing, containers, Linux, statistics, and basic cloud concepts.

Months 3–4 · Machine Learning

Data preparation, training/validation, metrics, overfitting, PyTorch fundamentals, experiment tracking, and model lifecycle.

Months 5–6 · Security Foundations

Threat modeling, application/API security, identity, secrets, supply chain, logging, and secure deployment.

Months 7–8 · AI Threats

Study prompt injection, insecure output handling, data poisoning, model theft, adversarial examples, privacy leakage, and abuse cases.

Months 9–10 · AI Security Engineering

Design gateways, policy checks, sandboxed tools, retrieval authorization, evaluation sets, monitoring, and incident response.

Months 11–12 · Portfolio & Roles

Publish safe evaluation harnesses, model cards, threat models, and secure reference apps; target AI security and ML platform roles.

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
ML model with reproducible evaluation

Project 2
LLM application threat model

Project 3
Prompt-injection evaluation dataset

Project 4
Secure retrieval authorization demo

Project 5
AI system logging dashboard

Project 6
Model supply-chain risk review

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.

- OWASP Top 10 for LLM Applications
- NIST AI Risk Management Framework
- MITRE ATLAS
- ML framework security guidance

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.