

YOUR NEXT CHAPTER

Practical Cybersecurity

Develop defensive security skills through controlled labs, application reviews, incident exercises and clear technical reporting.

16 WEEKS

Live + recorded + projects

160 TOTAL HOURS

10 hours / week

₹39,900

Tuition before taxes

PLANNED FIRST / FINAL SESSION

2026-11-07 / 2027-02-21

WEEKLY LIVE SCHEDULE

Saturday & Sunday · 18:00-19:30 IST

APPLY BY

2026-11-05

LEARNING-HOUR BREAKDOWN

48 live + 24 recorded + 88 independent practice

Who this is for

- + IT and infrastructure professionals
- + Developers moving toward application security
- + Early-career security practitioners

Before you join

- + Networking and operating-system basics
- + Comfort with a Linux terminal
- + Basic scripting helpful; all exercises use authorised lab environments

Apply free. Your application records interest; it does not confirm admission or reserve a paid seat. All seven tracks run independently. Holiday adjustments will be shared before admission.

WHAT YOU WILL LEARN

A curriculum built for practice.

WEEK 1-2

Security and networking foundations

- + Threat models and security objectives
- + Network protocols and packet analysis
- + Operating-system permissions
- + Lab authorisation and scope

WEEK 3-4

Identity and system hardening

- + Authentication and access control
- + Secure configuration and patching
- + Secrets and credential handling
- + Asset inventory and exposure review

WEEK 5-6

Application security

- + OWASP application risks
- + Input validation and session handling
- + API authorisation checks
- + Secure coding and dependency review

WEEK 7-8

Authorised assessment labs

- + Planning an assessment within scope
- + Proxy-assisted application inspection
- + Reproducible evidence and finding severity
- + Remediation recommendations

WHAT YOU WILL LEARN

A curriculum built for practice.

WEEK 9-10

Detection and log analysis

- + Security logs and event correlation
- + Baseline behaviour and alert triage
- + Detection rules and false positives
- + Analyst reporting and escalation

WEEK 11-12

Incident response

- + Preparation and containment
- + Evidence handling in lab environments
- + Recovery and lessons learned
- + Tabletop incident simulation

WEEK 13-14

Cloud and modern application risks

- + Cloud identity and misconfiguration
- + Container and supply-chain controls
- + AI application data and tool boundaries
- + Risk prioritisation for limited budgets

WEEK 15-16

Capstone and technical reporting

- + Controlled assessment or detection project
- + Validate proposed remediation
- + Write an actionable report
- + Demonstrate findings and answer review questions

Tools and methods

Linux / Wireshark / OWASP ZAP / Burp Suite Community / Wazuh / Python / Docker labs

BUILD AND APPLY

Your learning, put to work.

Capstone directions

Application security review

Assess a deliberately vulnerable local application, explain findings and verify fixes.

Detection and incident lab

Build a sample detection workflow, investigate simulated events and deliver an incident timeline.

Small-company hardening plan

Review a fictional environment and prioritise identity, backups, monitoring and patching improvements.

Instructor expertise we are recruiting

Practising security engineer in application security, SOC or authorised assessment. Ability to supervise controlled labs and teach reporting and remediation. Role-relevant credentials strengthen the profile; no claim of certification exam preparation. Faculty being finalised.

Tuition and application

Launch tuition: ₹39,900 per learner, before applicable taxes. Includes planned live sessions, recordings, resources, assignments and project reviews. Paid tools and external certification exams are extra unless included in your admission offer.

Named faculty, final timetable, final payable amount and written cancellation/refund terms will be confirmed before admission and payment. Six months of post-course resource access is planned. No university affiliation, placement or salary guarantee is offered.

Apply for your November cohort

Visit the ShawGrid Academy website, open this programme and select Apply for this track. Keep the on-screen application reference and downloadable receipt. Email acknowledgements will be enabled after sender verification.