HACKUP TECHNOLOGY

The Art of Security · Coimbatore · Since 2013

EC-Council Accredited Training Center

PROGRAMME SYLLABUS · 2027 INTAKE

Diploma in Cyber Security

A 6-month career programme that takes you from the basics to job-ready skills in network defence, ethical hacking and SOC operations, with three EC-Council certification tracks and a supervised capstone in our live VAPT and SOC team.

EC-Council CND | EC-Council CEH v13 | EC-Council CSA

AI for Cyber Security in every month | Capstone with Hackup VAPT/SOC team

6 months
Start from scratch

Classroom + online
Ganapathy, Coimbatore or live online

Weekday + weekend
Batches to suit students and working professionals

Jan 2027
Next batch starts in the first week

hackuptechnology.com · +91 93620 12339 · info@hackuptechnology.com

PROGRAMME OVERVIEW

Built for what security teams actually hire for

Most entry-level security job descriptions ask for the same things: solid networking and operating-system basics, some scripting, the ability to find and explain vulnerabilities, and the ability to watch logs and respond to an alert. This programme is built around those requirements, in that order.

You start from scratch with the foundations, then move through network defence (CND), ethical hacking (CEH v13) and SOC operations (CSA). You finish with a supervised capstone project alongside Hackup's own VAPT and SOC practitioners, the team that secures 100+ organisations.

DURATION **6 months**	MODE **Classroom (Ganapathy, Coimbatore) or live online**
BATCHES **Weekday and weekend batches**	NEXT BATCH **First week of January 2027**
CERTIFICATION TRACKS **EC-Council CND, CEH v13, CSA**	PROGRAMME FEE **Contact us for fees and batch timings**

Who this programme is for

- Graduates and final-year students (B.E., B.Tech, B.Sc, BCA, MCA and others) who want a career in Cyber Security
- IT, networking and support professionals moving into security roles
- Career switchers ready to put in steady practice: we start from scratch, including coding basics
- Working professionals who need weekend or online batches

Entry requirements: basic computer skills and a willingness to practise regularly. No prior security experience is needed. A free 1:1 counselling session before you join checks your background and recommends the right batch.

DETAILED CURRICULUM

The 6-month roadmap

Month	Focus	Certification track
1	Foundations from scratch: networking, Linux, Windows, Python and scripting basics, AI assistants for security work	Foundation assessment
2	Network defence: protect, detect and respond on enterprise networks	EC-Council CND (312-38)
3–4	Ethical hacking: the full attack lifecycle with AI-assisted techniques	EC-Council CEH v13 (312-50)
5	SOC operations: SIEM, alert triage, threat hunting, incident response	EC-Council CSA (312-39)
6	Supervised capstone in Hackup's VAPT/SOC team, portfolio and interview preparation	Hackup Diploma in Cyber Security

MONTH 1

Foundations from scratch

Everything later in the programme builds on this month. **Outcome:** you can explain how data moves across a network, work confidently on Linux and Windows, and write small Python scripts to automate security tasks.

Networking

- OSI and TCP/IP models, IP addressing and subnetting
- Routing, switching, VLANs, NAT, DHCP and DNS
- HTTP/HTTPS, TLS, email protocols
- Packet capture and analysis with Wireshark

Linux

- Command line, file system, users and permissions
- Processes, services, package management
- Logs, networking commands, SSH
- Bash scripting basics

Windows

- Windows internals, users, groups and permissions
- Active Directory basics: domains, users, group policy
- Event logs and Sysmon basics
- PowerShell for administrators

Python and scripting

- Python syntax, data types, functions, files
- Working with APIs, JSON and regular expressions
- Writing a port scanner and a log parser
- Web basics: requests, cookies, sessions
- Using AI assistants safely to write and review scripts

MONTH
2

Network defence

EC-Council CND

The defender's view of an enterprise network, following the Protect, Detect, Respond and Predict approach of EC-Council's Certified Network Defender. **Outcome:** you can harden networks and endpoints, monitor traffic and logs, and take the first steps in an incident.

1. Network attacks and defense strategies
2. Administrative network security
3. Technical network security
4. Network perimeter security
5. Endpoint security: Windows, Linux, mobile and IoT
6. Administrative application security
7. Data security
8. Enterprise virtual, cloud and wireless network security
9. Network traffic monitoring and analysis
10. Network logs monitoring and analysis
11. Incident response and forensic investigation
12. Business continuity and disaster recovery
13. Risk management and attack surface analysis
14. Threat prediction with cyber threat intelligence

Build a defended network
Configure a firewall, IDS/IPS rules and VPN in a lab network, then test what gets through.

Harden endpoints
Apply security baselines to Windows and Linux machines and verify them against a checklist.

Read the traffic
Spot scans, brute-force attempts and suspicious connections in packet captures and firewall logs.

MONTHS
3–4

Ethical hacking

EC-Council CEH v13

The attacker's view: how real attacks are planned and carried out, and how each one is detected and stopped. Follows the official 20-module CEH v13 curriculum, with AI-assisted techniques across the course. **Outcome:** you can run a structured vulnerability assessment on networks, systems and web applications, and explain each finding and its fix.

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. Vulnerability Analysis
6. System Hacking
7. Malware Threats
8. Sniffing
9. Social Engineering
10. Denial-of-Service
11. Session Hijacking
12. Evading IDS, Firewalls and Honeypots
13. Hacking Web Servers
14. Hacking Web Applications
15. SQL Injection
16. Hacking Wireless Networks
17. Hacking Mobile Platforms
18. IoT and OT Hacking
19. Cloud Computing
20. Cryptography

Map a target like an attacker

Reconnaissance and scanning of a lab network: live hosts, open ports, services and versions.

Break and fix a web app

Exploit SQL injection and XSS in a deliberately vulnerable application, then write the developer fix.

Capture, crack and defend

Capture traffic, crack weak hashes and see why strong hashing and MFA stop the attack.

All hacking practice takes place in isolated lab environments or on targets with written authorisation. Professional ethics and the legal side of security testing in India are covered from day one.

MONTH
5

SOC operations

EC-Council CSA

The Blue Team workflow used in a Security Operations Centre, following EC-Council's Certified SOC Analyst curriculum. **Outcome:** you can work as an L1 SOC analyst: triage SIEM alerts, investigate, escalate with evidence and document an incident.

1. Security Operations and Management
2. Understanding Cyber Threats, IoCs and Attack Methodology
3. Log Management
4. Incident Detection and Triage
5. Proactive Threat Detection
6. Incident Response
7. Forensic Investigation and Malware Analysis
8. SOC for Cloud Environments

Triage an alert flood
Work through SIEM alerts from a simulated attack and separate real threats from noise.

Hunt for IoCs
Search Windows, Linux and network logs for suspicious logins, processes and connections.

Run an incident end to end
Contain, collect evidence, build the timeline and write the incident report.

TOOLS YOU WILL USE

Kali Linux · Wireshark · Nmap · Burp Suite · Metasploit · Nessus / OpenVAS · SQLmap · John the Ripper / Hashcat · pfSense · Snort / Suricata · Splunk · ELK / Wazuh · Sysmon · Python · PowerShell · MITRE ATT&CK

MONTH 6

Capstone with Hackup's VAPT and SOC team

This is what makes the diploma different. You work on a supervised project with the practitioners who deliver Hackup's VAPT and SOC services, following the same methods, checklists and report standards. **Outcome:** a real project for your portfolio and interview stories you can back up.

TRACK A · OFFENSIVE

VAPT project

- Scoping and rules of engagement
- Web application and API assessment
- Network vulnerability assessment
- Risk rating of findings
- A professional report with clear fixes, reviewed by a senior tester

TRACK B · DEFENSIVE

SOC project

- Log onboarding and SIEM use cases
- Detection rules for common attacks
- Alert triage and escalation
- Incident handling and timeline
- An incident report and shift handover, reviewed by a SOC lead

TRACK C · AI SECURITY

AI chatbot security project

- Threat model of an AI chatbot or agent
- Testing against the OWASP Top 10 for LLM Applications
- Prompt injection and data leakage tests
- Fixes and guardrails
- A test report reviewed by Hackup's AI security team

Capstone work is supervised and limited to lab environments and authorised scopes. No client data leaves Hackup's controlled environment.

Career readiness

- Resume and LinkedIn profile for security roles
- GitHub portfolio: scripts, write-ups and capstone summary
- Technical and HR mock interviews
- Placement assistance: job referrals and interview coordination

AI FOR CYBER SECURITY

AI is built into every month

Attackers now use AI to write phishing, find weaknesses and automate attacks, and security teams use it to sort alerts and speed up investigations. Instead of a separate add-on, AI for Cyber Security runs through the whole diploma, so you learn to use AI as a professional tool and to secure AI systems themselves. Everything is practised in labs, and you always verify what an AI tool tells you.

Month	AI for Cyber Security topics
1	How AI and large language models work, at a practical level. Using AI assistants safely to write, explain and review Python scripts and to read logs. What never to paste into an AI tool.
2	AI and machine learning in network defence: anomaly detection on traffic and logs, and where it fails. Protecting company data when staff use AI tools.
3–4	AI-assisted reconnaissance and vulnerability analysis, as covered in CEH v13. AI-generated phishing and social engineering. Lab: prompt injection against a test chatbot, mapped to the OWASP Top 10 for LLM Applications.
5	AI in the SOC: using AI to summarise alerts and draft detection rules, and checking its output. Spotting deepfake voice and video fraud. Investigating an AI-assisted attack.
6	Optional Track C capstone: security testing of an AI chatbot or agent with Hackup's AI security team. Awareness of AI governance, including ISO/IEC 42001.

Why it matters for your career: employers increasingly ask how candidates use AI responsibly and whether they understand AI risks such as prompt injection and data leakage. You will be able to show both, with lab work to back it up.

The diploma does not include a separate AI certification. AI topics are taught by Hackup Technology alongside the EC-Council curriculum.

ROLES THIS PROGRAMME PREPARES YOU FOR

SOC Analyst (L1)
Monitor alerts, triage and escalate incidents

Security Analyst
Vulnerability management, hardening and monitoring

Junior Penetration Tester / VAPT Analyst
Assess web apps, APIs and networks; write reports

Network Security Engineer
Firewalls, IDS/IPS, VPN and secure network design

Incident Response Associate
Contain incidents, collect evidence, document timelines

Cyber Security Associate
Entry roles across IT services, banks and product companies

ASSESSMENT AND CERTIFICATION

How you are assessed

Component	What it involves
Lab work	Lab exercises completed and reviewed every module
Monthly assessments	Practical and written checks at the end of each month
Capstone review	Report and presentation reviewed by Hackup practitioners
Hackup Diploma in Cyber Security	Awarded by Hackup Technology on completing the programme, assessments and capstone
EC-Council CND, CEH v13, CSA	Awarded by EC-Council on passing the official exams (312-38, 312-50, 312-39). Training follows the official EC-Council curriculum.

WHY HACKUP TECHNOLOGY

Since 2013
A Coimbatore cyber security company, not only a training centre

EC-Council accredited
Accredited Training Center for official EC-Council programmes

Practitioner trainers
20+ member security team that secures 100+ organisations

Rated 4.8 on Google
By 4,300+ reviewers (as of November 2026)

NEXT BATCH · FIRST WEEK OF JANUARY 2027

Contact us for fees and batch timings

Weekday and weekend batches, classroom or live online. Book a free 1:1 counselling session or a free lab demo at our Ganapathy centre.

+91 93620 12339
Call or WhatsApp

info@hackuptechnology.com
Email

hackuptechnology.com
Website

Ganapathy, Coimbatore
Classroom and labs

EC-Council, CND, CEH and CSA are trademarks of EC-Council. Placement assistance includes resume support, interview preparation and job referrals; it is not a job guarantee. Syllabus content may be updated to follow changes in EC-Council curricula and industry practice.