

Cybersecurity

Course Duration ~75 Hours · 10 Weeks · Live Online · Lab-Heavy · Isolated Practice Environments and a Portfolio of Documented Investigations

Curriculum reviewed: July 2026 — the threat landscape and certification objectives move fast; this syllabus is checked against official sources

Ethical & Legal Use — read first. All offensive and exploitation techniques on this course are taught **for defensive purposes only**, exclusively in isolated lab environments and against deliberately vulnerable practice targets provided for the course. You must **never test systems you do not own or lack written authorisation to test** — unauthorised access to computer systems is a criminal offence, and this course will never ask you to attempt one. The course teaches responsible disclosure and the legal and regulatory context of security work.

Threats & Risk

Detection & SOC

Incident Response

Defensive Labs

AI Security

Governance

In short: Learn to defend real systems. Threats, controls, detection and response — with a lab where you break things you're allowed to break, and then fix them. "Cybersecurity" names an entire field, so this is scoped deliberately as **the foundation course of a security track**: it covers the breadth a practitioner needs before specialising, and goes deep enough on **defensive operations** to make you employable in an entry role — the realistic first job — built around the artefacts employers screen on: a documented home lab, a written vulnerability report, an investigation write-up. It has a wider entry point than the other DevOps courses: reachable from IT support, helpdesk, networking, QA and administration, not only development. It **does not** cover advanced offensive/penetration testing, cloud-provider-specific security in depth, application security/DevSecOps (which live in our Docker & Kubernetes, Terraform and CI/CD courses), or dedicated GRC work — it names those boundaries and points forward to them. Across 10 modules you build a home lab, investigate network traffic, harden identity and endpoints, run a defensive vulnerability assessment in isolated labs, work a Tier 1 SOC queue, respond to a simulated breach, and — a dedicated module barely covered in entry courses — secure AI systems (prompt injection, data/model poisoning, agent tool permissions) and defend against AI-accelerated attacks. Aligned to CompTIA Security+ (objectives refreshed for zero-trust, cloud and current threats), with onward specialisation paths and newer AI-security credentials mapped.

Duration	10 weeks · ~75 hours · live + hands-on	Format	Live online · lab-heavy · isolated practice environments and a portfolio of documented investigations
Prerequisite	General IT literacy and comfort with the command line. Networking basics helpful and reinforced early. No security or programming background required.	Curriculum	10 modules, from security foundations to governance, compliance and a capstone engagement
Certification	Aligned to CompTIA Security+ (the leading vendor-neutral entry credential); onward specialisation paths mapped	Ideal for	Fresh IT graduates, and IT support/helpdesk/networking professionals moving into security — the most common transition path

What This Course Does NOT Cover — and Where It Leads

Naming the boundary is a trust signal. This foundation course deliberately does not cover, and points forward to: **advanced offensive security and penetration testing** (attacker techniques are taught only to a defender's depth); **cloud-provider-specific security** (conceptual, shared-responsibility level only); **application security and DevSecOps** (pipeline, container and supply-chain security live in our Docker & Kubernetes, Terraform and CI/CD courses); and **dedicated GRC / compliance work** (introduced, not specialised). The paths after this course: defensive operations, offensive security, cloud security, application security, and governance/risk/compliance.

Security in the Age of AI — Both Sides

Security is one of the few fields where AI cuts both ways, and this course teaches both. Attackers use it to scale phishing, generate malware variants and accelerate reconnaissance; defenders use it for detection, triage and log analysis. And organisations are deploying AI systems that create genuinely new attack surface — prompt injection, model and data poisoning, insecure agent tool access, and sensitive data leaking

through model interactions. Securing AI systems and defending against AI-accelerated attacks get a dedicated module — barely covered in existing entry courses, and exactly where the field is moving.

Course Highlights

- Every module leads with what you do, detect, defend or respond to — not what you "learn about"
- A home lab you build in week one and use all the way to the capstone
- Defensive operations to employable depth — SIEM, detection engineering, a realistic Tier 1 analyst queue
- A full incident-response exercise with timeline reconstruction and a post-incident report
- Offensive technique taught for defence only, in isolated labs against deliberately vulnerable targets
- Securing AI systems and defending against AI-accelerated attacks — a dedicated module
- A portfolio of the artefacts employers screen on: lab, vulnerability report, investigation write-up
- Zero trust taught as an architectural principle, not a product to buy

Hands-on Projects & Portfolio

- **Home Lab Build** — isolated network, vulnerable targets, monitoring stack — the foundation for everything else
- **Network Traffic Investigation** — capture and analyse a session to identify suspicious activity
- **Vulnerability Assessment** — a lab environment assessed, with a professional written report and prioritised remediation
- **Web Application Security Lab** — against deliberately vulnerable applications, with fixes proposed
- **SOC Simulation** — work a realistic alert queue: triage, escalate and document
- **Detection Engineering** — write and tune rules that catch a simulated attack without drowning in false positives
- **Incident Response Exercise** — full timeline reconstruction and a post-incident report
- **Phishing Analysis** — dissect a real-world-style campaign, including AI-generated lures
- **AI Security Lab** — demonstrate prompt injection and data exposure against a test application, then implement guardrails
- **Capstone** — end-to-end assessment, detection, response and stakeholder presentation

Tools & Stack

Kali Linux · Wireshark · Nmap · Burp Suite · Metasploit (lab only) · OWASP ZAP · Splunk · Elastic Security · Wazuh · Suricata · Nessus or OpenVAS · Sysmon · Velociraptor · Autopsy · MITRE ATT&CK · CIS Benchmarks · NIST frameworks · Active Directory · pfSense · Docker · Python & Bash · TryHackMe-style labs

Certification Alignment

- Mapped to **CompTIA Security+**, the leading vendor-neutral entry-level security certification — whose objectives have been refreshed to include zero-trust architecture, cloud/hybrid security and current threat trends
- Onward defensive analyst, penetration testing and cloud security specialisations mapped as your next step
- Newer vendor-neutral AI-security credentials have started to appear alongside the traditional foundations — this course builds the base for them
- Presented as preparation and alignment — no official partnership or accreditation implied, and no exam outcome guaranteed

Career Outcomes

Security operations is one of the few technical fields with a genuine, sustained shortage of qualified people, and entry-level defensive roles remain among the most accessible ways into the field for candidates without prior security experience. Employers increasingly screen on demonstrable hands-on ability — a documented home lab, a written vulnerability report, an investigation write-up — rather than coursework alone, which is exactly why this course is built around producing those artefacts. This course targets:

- SOC Analyst (Tier 1) · Security Analyst · Information Security Analyst · Incident Response Analyst
- Vulnerability Analyst · Security Engineer (with experience) · GRC / Compliance Analyst · IT professional with security ownership

Who This Course Is For

- Final-year students and fresh IT graduates targeting security roles
- **IT support, helpdesk, desktop and network professionals moving into security** — the single most common and most successful transition path
- System and network administrators taking on security responsibility
- Developers, QA and DevOps engineers who need real security depth rather than a checklist
- Professionals from non-technical backgrounds making a considered career change
- Anyone preparing for a foundational security certification

Module 1: Security Foundations & Risk

7 Hours

YOU BUILD

- A risk assessment of a sample organisation — assets, threats, attack surface and treatment decisions — traced back to the CIA triad, the way a real security programme is justified

TOPICS

- The CIA triad and why every control traces back to it; threat actors and their motivations; attack surface and the kill chain
- Risk assessment and treatment; defence in depth; zero trust as an architectural principle rather than a product
- Thinking like an attacker in order to defend

Assessment: Quiz + Lab

Module 2: Networking & Infrastructure Security

8 Hours

YOU DETECT

- Suspicious activity in a captured traffic sample — reading packets to find what shouldn't be there — on the segmented, monitored home lab you begin building here

TOPICS

- The protocols that matter for security; packet analysis; firewalls and segmentation; VPNs and secure remote access; wireless security
- Network monitoring and intrusion detection; DNS and email as attack vectors
- Reading traffic to find what shouldn't be there

Assessment: Quiz + Lab

Module 3: Cryptography in Practice

7 Hours

YOU DEFEND

- A service against the cryptographic failures that actually cause breaches — misconfigured TLS, weak algorithms, an expired certificate, poor key handling — found and fixed

TOPICS

- Symmetric and asymmetric encryption; hashing and integrity; digital signatures; certificates and public key infrastructure
- TLS in the real world; key management; encryption at rest and in transit
- The practical failure modes — misconfiguration, weak algorithms, expired certificates and poor key handling

Assessment: Quiz + Lab

Module 4: Identity & Access Management

7 Hours

YOU DEFEND

- An identity control plane — multi-factor, least privilege, privileged access management and a clean account lifecycle — configured against a directory, because identity is where modern attacks land

TOPICS

- Authentication factors and multi-factor implementation; passwords, passkeys and modern credentials; single sign-on and federation
- Privileged access management; least privilege and separation of duties; directory services; account lifecycle

- Why identity is the primary control plane in modern environments

Assessment: Quiz + Lab

Module 5: Endpoint, System & Data Security

8 Hours

YOU DEFEND

- Hardened Windows and Linux endpoints with EDR, patch discipline and application allow-listing — and a tested backup-and-recovery treated as the security control it is

TOPICS

- Operating system hardening for Windows and Linux; patch and vulnerability management; endpoint detection and response
- Malware types and behaviour analysis; application allow-listing; backup and recovery as a security control
- Data classification; loss prevention; mobile and remote device security

Assessment: Quiz + Lab

Module 6: Attacks & Vulnerabilities, Hands-On

8 Hours

ETHICAL USE

Every technique in this module is performed **only** in isolated lab environments, against deliberately vulnerable targets provided for the course. You will never be asked to test a system you do not own or lack written authorisation to test.

YOU DO

- A full vulnerability assessment of a lab target — reconnaissance to reporting — producing a professional write-up with prioritised remediation, the artefact that gets you hired

TOPICS

- Reconnaissance, scanning and enumeration; common exploitation classes; the web application vulnerabilities that dominate real incidents
- Social engineering and phishing; password attacks; privilege escalation; lateral movement
- Vulnerability assessment and reporting — all in isolated labs against deliberately vulnerable targets

Assessment: Quiz + Lab

Module 7: Security Operations & Detection

8 Hours

YOU DETECT

- A simulated attack, worked from a realistic Tier 1 analyst queue — triaged, escalated and documented — with tuned detections that catch it without drowning you in false positives

TOPICS

- Logging and what to collect; SIEM fundamentals; writing detections and tuning out noise; alert triage
- Threat hunting; threat intelligence and mapping activity to a recognised adversary technique framework; digital forensics basics
- Working a realistic Tier 1 analyst queue

Assessment: Quiz + Lab

Module 8: Incident Response

7 Hours

YOU RESPOND TO

- A simulated breach, worked end to end — detection, containment, eradication and recovery — with a reconstructed timeline, sound evidence handling, and a post-incident report

TOPICS

- The response lifecycle; preparation and playbooks; detection and analysis; containment, eradication and recovery
- Evidence handling and chain of custody; communication during an incident; post-incident review
- Business continuity and disaster recovery

Assessment: Quiz + Lab

Module 9: AI, Cloud & Modern Attack Surface

8 Hours

YOU DEFEND

- A test AI application against prompt injection and data exposure — demonstrated, then closed with guardrails — plus a cloud environment reviewed for the identity and misconfiguration risks that dominate real cloud incidents

TOPICS

- Securing cloud environments including the shared responsibility model; identity and misconfiguration as the dominant cloud risks; container and supply-chain risk at a conceptual level
- Securing AI systems — prompt injection, data and model poisoning, agent tool permissions, sensitive data exposure through model interactions
- Defending against AI-accelerated attacks including sophisticated phishing and deepfake-assisted social engineering

Assessment: Quiz + Lab**Module 10: Governance, Compliance & Capstone**

7 Hours

YOU RUN

- One end-to-end engagement — assess an environment, find and document weaknesses, detect a simulated attack, respond to it, and present findings to a non-technical stakeholder

TOPICS

- Security policies and standards; recognised control and risk frameworks; audits and evidence
- Privacy and data protection obligations including the regimes that apply to organisations operating in and serving India; vendor and third-party risk; security awareness programmes
- The legal context and responsible disclosure; capstone engagement and stakeholder presentation

Assessment: Capstone Engagement + Report + Presentation