ByteLearned

# Cyber Security

## Complete Beginner Guide

What it is • How it helps • Daily job responsibilities • Career roadmap

bytelearned.online | info@bytelearned.online | 7396633051

| 4 Big Topics | 8 CIA Pillars | 5-Phase Roadmap | Job Guide Fresher+Senior | Salary Benchmarks |
|---|---|---|---|---|

## 01 | WHAT IS CYBER SECURITY?

Cyber security is the practice of protecting computers, servers, mobile devices, networks, and data from malicious attacks, unauthorised access, damage, or theft. It covers everything from protecting your personal Gmail account to securing a country's power grid, banking systems, and military networks.

### THE CIA TRIAD — 3 Core Pillars of Cyber Security

| ■ CONFIDENTIALITY | ■ INTEGRITY | ■ AVAILABILITY |
|---|---|---|
| Only authorised people can access data. Example: Your bank password should only be known to you — not hackers, not even the bank employees. | Data must be accurate and not tampered with. Example: When you transfer Rs.500, the amount should not be changed to Rs.5000 by anyone in between. | Systems must be up and accessible when needed. Example: Your UPI app should work during Diwali shopping — not crash due to a DDoS attack. |

### TYPES OF CYBER THREATS

| | |
|---|---|
| ■ **Malware** | Malicious software — viruses, worms, spyware — that infects and damages your system or steals data without your knowledge. |
| ■ **Phishing** | Fake emails, SMS, or websites that trick you into giving your passwords, OTPs, or credit card numbers to criminals. |
| ■ **Ransomware** | Malware that locks all your files and demands money (ransom) to unlock them. Very common against hospitals and businesses. |

| | | |
|---|---|---|
| ■ | **Social Engineering** | Manipulating people psychologically to reveal confidential info. Example: A caller pretending to be your bank manager asking for OTP. |
| ■ | **DDoS Attack** | Overwhelming a website or server with millions of fake requests until it crashes and becomes unavailable for real users. |
| ■ | **Insider Threat** | A current or former employee who deliberately leaks, steals, or damages company data using their access privileges. |
| ■ | **Zero-Day Exploit** | Attacking a software vulnerability that the developer does not know about yet — so no fix (patch) exists. |
| ■ ■ | **Man-in-the-Middle** | Secretly intercepting communication between two parties — like reading your WhatsApp messages on a public WiFi. |

## 02 | HOW CYBER SECURITY HELPS US

| | |
|---|---|
| ■ **Protects your money** Secures online banking, UPI payments, and credit card transactions from fraud. India loses over Rs. 1,000 crore annually to cyber fraud. | ■ **Protects your identity** Stops criminals from stealing your Aadhaar, PAN, passport data to take loans, file false tax returns, or commit fraud in your name. |
| ■ **Secures your devices** Prevents hackers from accessing your smartphone camera, microphone, messages, and photos without your knowledge. | ■ **Protects healthcare data** Hospitals store your blood group, medications, and medical history. A breach can be life-threatening if wrong medication records are entered. |
| ■ **Keeps banking systems running** Ensures ATMs, net banking, stock markets, and payment gateways are not shut down by cyber criminals at critical moments. | ■■ **Protects national security** Power grids, water treatment plants, defence systems, and government databases are protected from enemy cyber attacks. |
| ■ **Safe online shopping** Ensures your card details and address are encrypted when you shop on Amazon, Flipkart, or any e-commerce site. | ■ **Protects businesses** A single data breach costs a company an average of Rs. 17 crore in India. Cyber security prevents this, protecting jobs and reputation. |
| ■ **Safe online education** Protects student data, prevents disruption of online classes, and keeps learning platforms like ByteLearned available and trustworthy. | ■ **Safe internet for everyone** Makes the internet a safer place for children, elderly users, and non-technical people who are most vulnerable to cyber attacks. |

## CYBER CRIME IN INDIA — KEY NUMBERS

| | |
|---|---|
| **Rs. 11,333 Cr+** | Lost to cyber fraud in India in 2023 (MHA report) |
| **1 attack every 39 sec** | Frequency of cyber attacks globally on average |
| **Rs. 17 Crore avg** | Average cost of a data breach for Indian companies |
| **3.5 Million+** | Unfilled cyber security job openings globally in 2024 |
| **40% YoY increase** | Rise in cyber attacks in India year over year |
| **95%** | Of all cyber breaches involve human error — training saves millions |

## 03 | DAILY JOB RESPONSIBILITIES

### FRESHER (0-1 Year) — SOC Analyst / Junior Security Engineer

| Starting Salary | Rs. 3.5 LPA – Rs. 6 LPA | Common Role | SOC Analyst Tier 1 |
|---|---|---|---|

| | |
|---|---|
| 1 | **Monitor SIEM Dashboard**<br>Watch Splunk/QRadar all day for alerts. Classify each as true positive (real threat) or false positive (harmless). Log every decision. |
| 2 | **First-Level Incident Response**<br>When an alert fires, acknowledge it in the ticketing system (ServiceNow/JIRA), gather initial info, and escalate to seniors if serious. |
| 3 | **Phishing Email Analysis**<br>Employees forward suspicious emails to the SOC. You analyse the headers, check links on VirusTotal, and determine if it's malicious. |
| 4 | **Vulnerability Scanning**<br>Run Nessus or OpenVAS scans on assigned IP ranges. Compile results into a report and pass to the senior analyst with severity ratings. |
| 5 | **Log Analysis**<br>Review firewall, web server, DNS, and endpoint logs daily. Look for anomalies like repeated failed logins, unusual ports, or data transfers. |
| 6 | **Patch Management Support**<br>Track which systems need security patches applied. Co-ordinate with the IT team to ensure patches are deployed without breaking services. |
| 7 | **Shift Handover & Documentation**<br>At the end of each shift write a handover report. Document every incident, action taken, and any pending investigations for the next shift. |
| 8 | **Security Awareness Support**<br>Help create phishing simulation emails, assist with training materials, and track which employees clicked on simulated phishing emails. |

*Tools used daily as a Fresher: Splunk, Wireshark, Nessus, VirusTotal, Microsoft Defender, ServiceNow, JIRA*

### MID-LEVEL (2–4 Years) — Security Engineer / Penetration Tester

| Salary Range | Rs. 8 LPA – Rs. 18 LPA | Common Roles | Pentester / Security Eng. |
|---|---|---|---|

| | |
|---|---|
| 1 | **Penetration Testing**<br>Conduct full pentest engagements — from scoping and recon to exploitation and report writing. Cover web apps, networks, APIs, and cloud. |
| 2 | **Tier 2 Incident Handling**<br>Investigate escalated incidents in depth. Perform memory and disk forensics, malware analysis, and full containment and remediation. |
| 3 | **SIEM Rule Building**<br>Write new detection use cases and correlation rules to catch emerging threats. Tune existing rules to reduce false positives in Splunk or Sentinel. |
| 4 | **Threat Hunting**<br>Proactively search the environment for hidden threats using the MITRE ATT&CK; framework before automated tools detect them. |
| 5 | **Security Tool Management**<br>Own and maintain firewalls (pfSense), IDS/IPS (Snort/Suricata), EDR (CrowdStrike), and cloud security tools day to day. |
| 6 | **Vulnerability Management**<br>Own the full vulnerability lifecycle — scan, triage, assign to teams, track remediation, and verify fixes. Prepare risk reports monthly. |
| 7 | **Writing Security Reports**<br>Deliver professional pentest reports and incident post-mortems to clients and management with risk ratings and remediation guidance. |
| 8 | **Mentoring Juniors**<br>Review junior analysts' work, provide feedback, guide them through complex investigations, and run knowledge-sharing sessions. |

*Tools used daily: Metasploit, Burp Suite, BloodHound, Splunk, CrowdStrike, Cobalt Strike, AWS/Azure Security, Ghidra*

## SENIOR (5+ Years) — Security Architect / CISO / Security Manager

| Salary Range | Rs. 22 LPA – Rs. 45 LPA+ | Common Roles | Architect / CISO / Manager |
|---|---|---|---|

| | |
|---|---|
| 1 | **Design Security Architecture**<br>Define the entire security framework — Zero Trust model, cloud security strategy, network segmentation, and identity management across the org. |
| 2 | **Risk Management**<br>Identify, assess, and prioritise security risks. Quantify them in business terms (financial impact) and present to the board and C-suite quarterly. |
| 3 | **Compliance & Governance**<br>Ensure ISO 27001, GDPR, India PDPB, PCI-DSS compliance. Lead external and internal security audits. Own all regulatory relationships. |
| 4 | **Lead Incident Command**<br>Take command during major breaches. Co-ordinate IR team, handle communications with legal, management, regulators, and media if needed. |
| 5 | **Security Budget Management**<br>Own and manage the security budget (often crores). Evaluate, purchase, and renew security tools. Negotiate contracts with vendors like CrowdStrike, Palo Alto. |
| 6 | **Build & Lead the Security Team**<br>Hire, train, evaluate and retain a team of 10–50+ security professionals across SOC, red team, GRC, cloud security, and forensics. |
| 7 | **Security Awareness Programs**<br>Drive company-wide security culture. Run phishing simulations, conduct training sessions, measure improvement, and report results to leadership. |
| 8 | **Security Product Roadmap**<br>Define the multi-year security technology roadmap. Decide which tools to adopt (SASE, XDR, SOAR), retire, or upgrade based on the threat landscape. |

*Focus areas: ISO 27001, NIST CSF, MITRE ATT&CK;, Cloud Architecture, Zero Trust, GDPR/India PDPB, Risk Frameworks, Executive Reporting*

# 04 | HOW TO START A CAREER IN CYBER SECURITY FROM SCRATCH

Cyber security is one of the few tech fields where you can go from complete beginner to employed in 6–12 months. You do NOT need a Computer Science degree. You need consistency, curiosity, and daily hands-on practice.

## 1 Build Your Foundation

4–8 Weeks

- **Learn Computer Basics** *How an OS works, file systems, processes, memory. Both Windows and Linux basics are essential for any security role.*
- **Learn Networking Fundamentals** *TCP/IP, DNS, HTTP/S, OSI model, IP addressing, how packets travel across networks. This is the most critical foundation.*
- **Get Comfortable with Linux** *Install Kali Linux in VirtualBox. Learn the terminal daily — most security tools only run on Linux command line.*
- **Basic Scripting (Python or Bash)** *You do not need to be a developer. Learn enough to automate tasks, read scripts, and write simple tools to help your work.*

■ *Start Now: Set up a home lab on your laptop today. VirtualBox is free. Kali Linux is free. All you need is 8GB RAM and an internet connection.*

## 2 Choose Your Career Track

1 Week Decision

Cyber security has two main paths. Pick one to focus on first — you can always learn the other later. Most freshers find it easier to get their first job in Blue Team (SOC Analyst).

- **Red Team (Offensive)** *You attack systems ethically to find weaknesses before real hackers. Roles: Ethical Hacker, Pentester, Bug Bounty Hunter.*
- **Blue Team (Defensive)** *You defend systems — detect, respond, and recover from attacks. Roles: SOC Analyst, IR Analyst, Security Engineer.*
- **Fresher Advice** *Start with Blue Team. SOC Analyst jobs are the most common entry-level positions. Companies hire freshers for SOC daily.*

## 3 Build Practical Skills — Free Lab Platforms

8–16 Weeks

No employer cares about theory alone. Hands-on labs on real (simulated) systems is what separates hired candidates from rejected ones. All platforms below are FREE to start.

- **TryHackMe (tryhackme.com)** *Best for absolute beginners. Guided paths in your browser. Start with the "Pre-Security" and "SOC Level 1" learning paths.*
- **HackTheBox (hackthebox.com)** *More realistic machines. Do this after TryHackMe. Essential for penetration testing track. Shows real-world skills.*
- **OverTheWire — Bandit (overthewire.org)** *Amazing Linux wargames. Learn by breaking things in a completely safe sandboxed environment. 100% free.*
- **DVWA / WebGoat (run locally)** *Intentionally vulnerable web apps you run on your own laptop. Practice SQL injection, XSS, and OWASP Top 10 attacks safely.*
- **Blue Team Labs Online (blueteamlabs.online)** *SOC-focused challenges — SIEM, forensics, threat hunting scenarios. Perfect if you chose the defensive track.*

■ *Tip: Goal: Complete 30+ rooms on TryHackMe and document each one on GitHub. This becomes your portfolio.*

## 4 Get Certified

Pick 1–2 Certs to Start

Certifications prove your skills to employers who cannot interview you on every topic. The right certification gets your resume shortlisted out of hundreds. Start with one focused cert.

- **CompTIA Security+ — Start Here (Freshers)** *Global industry standard. Covers all security fundamentals. Recognised by every major company. Exam cost: ~Rs. 28,000. Best first cert.*
- **eJPT by eLearnSecurity — Offensive Track** *Affordable hands-on exam ($200). Proves real pentesting skills with a practical lab-based test. Best first offensive cert.*
- **CEH (Certified Ethical Hacker) — Popular in India** *EC-Council certification. Many Indian job postings specifically ask for CEH. Good for offensive track freshers.*
- **CompTIA CySA+ — Blue Team Specialist** *Security analyst certification. Focuses on threat detection, analysis, and response. Perfect for SOC Analyst track after Security+.*
- **OSCP — The Gold Standard (Advanced)** *24-hour hands-on practical exam. The most respected pentesting certification globally. Aim for this at 2–3 years of experience.*

■ *Key Advice: Do not wait until you feel "fully ready." Start studying while doing labs simultaneously. The act of studying + practising = the fastest progress.*

## 5 Build Your Portfolio & Get Hired

4–8 Weeks Before Applying

A strong portfolio beats a degree every time in cyber security. Employers want proof you can do the work — not just that you studied it. Here is exactly what to build:

- **GitHub Profile** *Upload your scripts, tools, and lab write-ups. Recruiters check GitHub actively. Even basic Bash or Python scripts show initiative and practice.*
- **Write Lab Write-ups** *After every TryHackMe room or HackTheBox machine, write a detailed walkthrough explaining your thought process. Post on LinkedIn.*
- **Optimise LinkedIn Profile** *Add all tools, certifications, TryHackMe rank, and HackTheBox profile link. Use keywords: "SOC Analyst", "Cyber Security", "Penetration Testing".*
- **One-Page Resume** *Skills section (tools), certifications, a Projects section (home lab + CTF achievements), and education. Keep it strictly one page.*
- **Join the Community** *Discord servers, LinkedIn groups, and local security meetups. Many jobs are found through referrals — not job boards alone.*
- **Where to Apply in India** *TCS, Wipro, Infosys, HCLTech, Deloitte, PwC, KPMG, Paytm, Razorpay, Navi, and any startup. Search "SOC Analyst fresher" on Naukri and LinkedIn.*

■ *Standout Tip: Send your TryHackMe profile and GitHub link with every job application. Most candidates send only a resume — you will immediately stand out.*

## REALISTIC TIMELINE — ZERO TO FIRST JOB

| | | |
|---|---|---|
| Month 1–2 | Foundation | Learn networking, Linux, set up home lab, get comfortable with the terminal and basic co |
| Month 3–4 | Core Skills | Start TryHackMe, learn your chosen track (SOC or Pentest), begin Security+ study along |

| | | |
|---|---|---|
| **Month 5–6** | **Labs + Certification** | Complete 30+ TryHackMe rooms, sit Security+ or eJPT exam, write your first lab walkthr |
| **Month 7–8** | **Portfolio + Apply** | Build GitHub, optimise LinkedIn, polish your resume, start applying for SOC Analyst / Jun |
| **Month 9–12** | **First Job Offer** | With consistent daily practice of 1–2 hours, most freshers land their first role in this windo |

## COMMON MYTHS ABOUT CYBER SECURITY — BUSTED

| | |
|---|---|
| ✗ **"I need a CS degree to get a job"** | Many top security professionals are self-taught. Skills and certifications matter far more than a degree. Companies care about what you can DO. |
| ✗ **"I need to know advanced programming"** | Basic Python or Bash scripting helps but is not required to start. You can get a SOC Analyst job without writing a single line of code. |
| ✗ **"I need expensive equipment and hardware"** | A laptop with 8GB RAM and free tools (VirtualBox, Kali Linux, TryHackMe) is everything you need to learn the entire course. |
| ✗ **"It takes 4 years of study to get a job"** | Consistent daily practice of 1–2 hours per day can take you from zero to employed in 6–12 months. Focus beats duration every time. |
| ✗ **"Cyber security is only for technical geniuses"** | GRC, compliance, awareness, and security management roles need communication skills more than deep technical knowledge. |

## JOB ROLES & SALARY — COMPLETE GUIDE

| Job Role | Track | Experience | Avg Salary India |
|---|---|---|---|
| SOC Analyst Tier 1 / Tier 2 | Blue | 0–1 yr | Rs. 3.5 – 6 LPA |
| Vulnerability Analyst | Blue | 0–2 yrs | Rs. 4 – 8 LPA |
| Penetration Tester (Junior) | Red | 1–2 yrs | Rs. 5 – 10 LPA |
| Security Engineer | Both | 1–3 yrs | Rs. 6 – 14 LPA |
| Incident Responder / DFIR Analyst | Blue | 2–4 yrs | Rs. 8 – 18 LPA |
| Threat Intelligence Analyst | Blue | 2–4 yrs | Rs. 8 – 16 LPA |
| Cloud Security Engineer | Both | 2–4 yrs | Rs. 10 – 22 LPA |
| GRC / Compliance Analyst | GRC | 1–3 yrs | Rs. 5 – 12 LPA |
| Senior Penetration Tester | Red | 4–6 yrs | Rs. 15 – 28 LPA |
| Security Architect | Both | 6–8 yrs | Rs. 25 – 45 LPA |
| CISO / Security Director | Both | 10+ yrs | Rs. 40 – 1 Cr+ |

## TOP COMPANIES HIRING CYBER SECURITY PROFESSIONALS IN INDIA

| | | | |
|---|---|---|---|
| TCS (Tata Consultancy Services) | Wipro | Infosys | HCL Technologies |
| Deloitte | PwC India | KPMG | Ernst & Young (EY) |
| Paytm | Razorpay | PhonePe | Zepto |
| IBM India | Accenture | Capgemini | Cognizant |
| Palo Alto Networks | CrowdStrike | CERT-In (Govt) | DRDO / ISRO (Govt) |