CYBERSECURITY CAREER ROADMAP IN INDIA

From Beginner → Job-Ready Cybersecurity Professional

Don't choose a company only for salary or brand name. Ask instead: "Will this job give me the technical exposure to become genuinely good at cybersecurity?"

Cybersecurity spans SOC & threat detection, penetration testing, application security, cloud security, incident response, IAM, GRC, DevSecOps and security engineering. Indian salary data varies widely by role and experience — entry-level SOC Analyst roles run roughly Rs. 4–8 LPA in 2026, with cloud security and pentesting rising considerably with experience. *(EICTA Consortium)*

STEP 1 — Build IT Fundamentals

Understand how computers & networks work before advanced tools:

- Networking: TCP/IP, DNS, HTTP/HTTPS, VPNs, firewalls
- Linux + Windows operating systems
- Command line & system administration
- Authentication & access control
- Databases, web apps, VMs, cloud basics
- Basic Python or Bash scripting

STEP 2 — Security Fundamentals

Core concepts:

- CIA Triad, threats/vulnerabilities/risk
- Malware & phishing
- Encryption vs hashing
- Authentication vs authorization
- Vulnerability mgmt, logging, IR

Attack chain: Recon → Initial Access → Privilege Escalation → Lateral Movement → Exfiltration → Detection & Response

STEP 3 — PICK ONE SPECIALISATION

1. SOC / Blue Team

Best for investigation & analysing suspicious activity.

- SIEM, log analysis, threat detection
- Incident response, EDR
- Network monitoring, threat intel

Path: SOC Analyst → Security Analyst → Incident Responder → Detection Engineer

2. Offensive Security

Best for finding vulnerabilities.

- Web app security, OWASP Top 10
- Network pentesting, Linux
- Burp Suite, Nmap, Metasploit, AD basics

Path: Junior Pentester → Pentester → Red Team → Security Consultant

3. Cloud Security

Strong long-term track as workloads move to cloud.

- AWS/Azure/GCP fundamentals, IAM
- Network security, logging, secrets mgmt
- Containers, Kubernetes, CSPM/CNAPP

Path: Cloud Security Associate → Cloud Security Engineer → Cloud Security Architect

4. AppSec / DevSecOps

Best if you already enjoy coding.

- Secure coding, OWASP, API security
- SAST/DAST, CI/CD security
- Dependency security, threat modelling

Path: AppSec Analyst → AppSec Engineer → DevSecOps Engineer

Only practise offensive techniques in authorised labs, CTFs, or systems you have explicit permission to test.

STEP 4 — DON'T COLLECT CERTIFICATES, BUILD PROOF

Avoid the Course → Certificate → Course loop. Build a documented portfolio instead:

Project 1 — SOC Investigation Lab + generated events + SIEM investigation. Document: what happened, IOC, detection method, action taken.	**Project 2 — Web Security Lab** Authorised vulnerable app. Document SQLi, XSS, broken auth, access-control issues.	**Project 3 — Cloud Security** Cloud lab demonstrating IAM, least privilege, logging, segmentation, monitoring.

Put documentation, diagrams and learnings on GitHub — prove you think like a security professional, not just that you finished a course.

STEP 5 — TARGET THE RIGHT ENTRY-LEVEL ROLES

Don't search only “Cybersecurity Engineer.” Also search:

- SOC Analyst
- Security Analyst
- Junior Security Analyst
- Security Operations Analyst
- Vulnerability Analyst
- IAM Analyst
- GRC Analyst
- Junior Penetration Tester
- Cloud Security Associate
- Application Security Analyst

Your first job doesn't have to be your dream role — get real experience, then specialise.

STEP 6 — WHAT TOP COMPANIES ACTUALLY OFFER

Company	What to know
Google	High technical bar. Focus on networks, OS, coding, security fundamentals, system design. Compensation varies by role/level — no fixed guaranteed figure.
Goldman Sachs	Dedicated cyber defence & threat-management teams: Windows/Linux security, network security, real-time intrusion detection, IR. Reported median comp for India cybersecurity analysts ~Rs. 30L (self-reported, not a guaranteed fresher package). *(Levels.fyi)*
JPMorgan Chase	Cybersecurity & Technology Controls org covers AppSec, Data Protection, Cryptography, DevSecOps, GRC, Network & Infra Security. Note: the $15B figure is JPMorgan's total tech budget, not a cybersecurity-only budget.
HDFC Bank	Dedicated cybersecurity framework: vulnerability mgmt, pentesting, DLP, WAF, DDoS protection, IDS/IPS, next-gen SOC, AI/ML-enabled SIEM, UEBA, zero-trust. Strong exposure to regulated, large-scale environments.
Accenture	Large global security practice: consulting, managed security, AppSec, cloud security, DevSecOps, DLP. Value depends heavily on the project/team you're placed into.
DRDO	Different objective: national-security work, research, government stability. Scientist 'B' starts at Rs. 56,100/month basic pay (7th CPC), not comparable to private-sector trajectories.

STEP 7 — A SIMPLE 6-MONTH ROADMAP

M1

IT Foundation

Networking + Linux + Windows + basic Python

M2

Security Fundamentals

Threats, vulnerabilities, auth, encryption, controls

M3

Hands-on Labs

TryHackMe / HTB / PortSwigger Web Security Academy

M4

Choose Your Track

SOC / Offensive Security / Cloud / AppSec

M5

Build 2–3 Projects

Document everything on GitHub

M6

Job Preparation

Resume, LinkedIn, GitHub, interview prep, apply consistently

THE MOST IMPORTANT RULE

Don't optimise for your first salary. Optimise for your first 2–3 years of learning. A Rs. 6 LPA job investigating incidents, working with SIEM/EDR and analysing vulnerabilities can be more valuable long-term than a higher-paying role where you barely touch cybersecurity.

Fundamentals → Hands-on Skills → Portfolio → First Security Job → Specialisation → Senior Security Role