Scope of Cyber Security in India 2026-2031 PDF

Cyber security has strong long-term scope in India. CERT-In handled 29,44,248 cyber security incidents in 2025, more than double the 2021 count, and the DSCI-SANS 2025-26 report says 73% of enterprises cannot find enough skilled candidates. But the same report warns that AI is reducing some entry-level roles, so freshers need hands-on lab skills, cloud security basics and AI security awareness.

Key takeaways

- CERT-In cyber incidents rose from 14,02,809 in 2021 to 29,44,248 in 2025 (Lok Sabha reply, 24 March 2026).
- DSCI-SANS 2025-26: 73% of enterprises report limited availability of skilled candidates, and 84% of organisations take 1-6 months to fill security roles.
- Entry-level roles are being reduced by AI and automation, while advanced roles stay understaffed (DSCI-SANS 2025-26). Hands-on skill is the key.
- ISC2 2025 study (India): the most needed skills are AI (52%), cloud security (43%) and application security (38%).
- AmbitionBox self-reported pay: Cyber Security Analyst about Rs 4.7-5.2 lakh at 1-3 years; Security Engineer about Rs 10.2-11.3 lakh at 3-6 years (Nov 2026).

Where cyber security stands in India in 2026

Cyber security means protecting computers, networks, apps and data from attacks, theft and damage. As more payments, government services and business systems move online, the need for security keeps rising.

Threats are rising. Data from CERT-In (India's national cyber emergency team), shared in a Lok Sabha reply on 24 March 2026:

Year	Cyber security incidents handled
2021	14,02,809
2022	13,91,457
2023	15,92,917
2024	20,41,360
2025	29,44,248

Skilled people are hard to find. The DSCI and SANS Institute Indian Cyber Security Skilling Landscape Report 2025-26 (released 1 May 2026) found:

- 73% of enterprises and 68% of service providers report limited availability of skilled candidates;
- 84% of organisations take between one and six months to fill a security role;
- 63% of enterprises say candidates lack hands-on practical skills.

But entry-level work is changing. The same report says AI and automation are leading to a reduction in entry-level job roles, while advanced roles remain understaffed. The ISC2 2025 Cybersecurity Workforce Study for India also shows that staff shortages fell from 59% of respondents in 2024 to 48% in 2025, while 97% reported at least one skills need.

Global view: the WEF Future of Jobs Report 2025 ranks Security Management Specialists in the top five fastest-growing jobs and Information Security Analysts in the top 15. It also names Security Management Specialists among India's fastest-growing roles. Naukri JobSpeak reported 18% year-on-year growth for the IT and Information Security function in June 2026.

The clear message: the field is growing, but employers want skill depth, not just a certificate.

Main job roles and what each one does

Role	What you do
SOC Analyst (L1/L2)	Watch security alerts in a Security Operations Centre, check if they are real attacks, and escalate
Cyber Security Analyst	Review logs, run vulnerability scans, apply security policies and respond to incidents
VAPT / Penetration Tester	Ethically hack apps and networks to find weak points before attackers do
Security Engineer	Build and manage firewalls, identity systems, endpoint and cloud security tools
Cloud Security Engineer	Secure AWS, Azure or GCP setups, permissions and data
GRC Analyst	Handle governance, risk and compliance: audits, policies, ISO 27001 and data protection rules
Threat Intelligence Analyst	Track attacker groups and new threats and turn them into defences
Security Architect	Design security for whole systems; a senior role

DSCI-SANS says Security Architects, OT/ICS (industrial systems) specialists and advanced threat intelligence professionals are the hardest to hire. These are senior paths you can grow into.

Skills you need

Foundations

- Networking: TCP/IP, DNS, HTTP, ports, firewalls.

- Operating systems: Linux command line and Windows administration.
- Scripting: Python or Bash for automation.

Security skills

- Log analysis and SIEM tools (for example Splunk, Microsoft Sentinel, Wazuh).
- Vulnerability scanning and basic web app testing (OWASP Top 10).
- Identity and access management.
- Incident response basics.

Skills in highest demand (ISC2 2025 study, India): AI (52% of respondents), cloud security (43%), application security (38%), security analysis (34%) and risk management (32%).

Why data skills help: a lot of security work is reading large amounts of log data. SQL, Python and dashboard skills from data analytics help you spot unusual patterns faster, which is why many SOC teams value analysts with data skills.

Salary path: fresher to 5 years

These are **self-reported salaries on AmbitionBox** (updated November 2026). Each figure is the range AmbitionBox shows for the average in that band. AmbitionBox does not show a 0-1 year band for these roles.

Role	1-3 years	3-6 years	6-9 years
SOC Analyst	Rs 4.3-4.8 lakh	Rs 5.9-6.5 lakh	not shown
Cyber Security Analyst	Rs 4.7-5.2 lakh	Rs 6.9-7.6 lakh	Rs 10.4-11.5 lakh (AmbitionBox estimate)
Security Engineer	Rs 7.2-8.0 lakh	Rs 10.2-11.3 lakh	Rs 16.4-18.1 lakh

Source: AmbitionBox, self-reported, November 2026.

Starting pay in SOC roles is modest. Pay grows faster when you move from monitoring to engineering, cloud security, application security or penetration testing. DSCI-SANS also reports that 70% of providers lose staff mainly to higher-paying competitors, which shows that skilled people have bargaining power.

Year-by-year guide: 2026 to 2031

2026

Learn networking, Linux and security basics. Set up a home lab with free tools and practise on legal platforms such as capture-the-flag (CTF) challenges. Learn SQL and Python for log analysis.

2027

Get hands-on with a SIEM and basic incident response. Earn one respected entry-level certification if you can afford it. Do an internship in a SOC or IT team. DSCI-SANS says 63% of enterprises find candidates lack hands-on skills, so lab work is your edge.

2028

Aim for your first job (SOC L1, security analyst, IT support with security tasks). Start learning cloud security on one platform. Read CERT-In advisories regularly.

2029

Specialise: cloud security, application security, penetration testing, GRC or threat intelligence. Learn how attackers use AI and how to secure AI systems in companies.

2030

WEF's survey runs to 2030 and lists networks and cybersecurity as the second fastest-growing skill group. Aim to work as a security engineer or specialist by now, with real incident and project experience.

2031

No trusted source publishes job or salary forecasts for India beyond 2030, so the 2029, 2030 and 2031 notes below are skills guidance, not predictions. Senior paths such as security architect, OT/ICS security and threat intelligence are the ones DSCI-SANS already reports as hardest to fill.

How AI is changing cyber security

- **Attackers use AI.** ISC2's 2025 India study lists AI-driven threats such as social engineering (41%), data leakage (31%) and deepfakes (30%).
- **Defenders use AI too.** In the same study, 77% of organisations are using, testing or evaluating AI security tools, and 85% of teams that adopted them reported significant productivity gains.
- **Basic alert checking is being automated.** DSCI-SANS links AI and automation to fewer entry-level roles. Simple L1 alert triage is the most exposed task.
- **New AI security jobs are appearing.** DSCI-SANS says 83% of organisations call AI and GenAI security skills a critical need, and 78% report high demand for AI Security Engineers.

So learn to work with AI security tools, and learn how to protect AI systems themselves. That combination is where demand is heading.

Who should choose cyber security

Cyber security suits you if you:

- are curious about how systems work and how they break;
- are patient with detailed, careful work such as reading logs;
- can stay calm under pressure during incidents;
- are honest and careful, because you will handle sensitive data and must follow the law.

B.Tech, BCA, MCA and B.Sc (CS/IT) students have an easier start, but many people enter from IT support or networking jobs too. Some SOC roles need shift work, including nights.

Security jobs are not only in IT companies. Banks, insurance firms, telecom companies, hospitals, government bodies and manufacturing plants all need security teams, so you can choose an industry you like. Each industry has its own rules, so learning the compliance basics of one sector helps you stand out.

A 5-step plan for students

1. **Networking and Linux (8 weeks).** Learn how data moves across networks and practise daily on the Linux command line.
2. **Security basics and a home lab (8 weeks).** Learn common attacks and defences. Practise only on legal labs and CTF platforms, never on systems you do not own.
3. **Data skills for security (6 weeks).** SQL, Python and a dashboard tool to analyse logs. This also links well with a data analytics course.
4. **One specialisation (8-12 weeks).** SOC and SIEM, cloud security, or web application testing. Document your lab work as write-ups on GitHub or a blog.
5. **Apply and keep learning.** Target SOC analyst, security analyst and IT security trainee roles. Be ready for practical tests and scenario questions, and follow CERT-In advisories.

Frequently asked questions

Is cyber security a good career in India?

Yes, for people who build hands-on skills. CERT-In handled 29,44,248 incidents in 2025, and DSCI-SANS reports that 73% of enterprises face a shortage of skilled candidates. Entry-level roles are getting fewer, so practical lab skills matter.

What is the salary of a cyber security analyst in India?

AmbitionBox self-reported data (Nov 2026) shows an average range of about Rs 4.7-5.2 lakh at 1-3 years and Rs 6.9-7.6 lakh at 3-6 years. Security engineers earn more, about Rs 10.2-11.3 lakh at 3-6 years.

Can I learn cyber security without coding?

You can start with networking and security tools, but basic Python or Bash scripting helps a lot and is expected in most mid-level roles.

Why does this report link cyber security with data analytics?

A lot of security work means analysing large amounts of log data. SQL, Python and dashboard skills help security analysts find attacks faster.

Is this PDF free?

Yes. Fill in the short form on this page and the PDF downloads right away.

Sources and further reading

- ThePrint: CERT-In cyber security incidents 2021-2025, Lok Sabha reply of 24 March 2026
- DSCI and SANS Institute: Indian Cyber Security Skilling Landscape Report 2025-26, press release (1 May 2026)
- ISC2: India cybersecurity workforce reaches a turning point (2025 ISC2 Cybersecurity Workforce Study)
- World Economic Forum, Future of Jobs Report 2025 (full PDF)
- Naukri JobSpeak, June 2026: AI-ML and fresher hiring lead the charge

- AmbitionBox: SOC Analyst salaries in India (self-reported, updated Nov 2026)
- AmbitionBox: Cyber Security Analyst salaries in India (self-reported, updated Nov 2026)
- AmbitionBox: Security Engineer salaries in India (self-reported, updated Nov 2026)

About this PDF

Prepared by the Uncodemy career team from the public sources listed. We update it every January. Corrections: info@uncodemy.com.

More free resources and courses: uncodemy.com | info@uncodemy.com | +91 98183 66550