LAKSHYA

CAREER EMPLOYABILITY & FUTURE-READINESS REPORT

Cyber Security Assistant: how employable, and how future-proof, is this trade?

Cyber security is one of the fastest-growing fields globally, yet it also sits at the intersection of two countervailing forces: surging human demand and rapid AI-driven automation of routine defensive tasks. The central question for anyone financing or pursuing this NSQF/CTS trade is whether a vocational-level certificate-holder can find stable work in a sector that increasingly rewards specialised judgment over ticket-triage speed. Evidence suggests the answer is cautiously yes, provided graduates move quickly up the skill stack.

62.1 /100

COURSE EMPLOYABILITY SCORE (CES V2)

Moderate employability, scored across all four CES pillars (§02).

29.44 lakh [1]

Cyber incidents handled by CERT-In in 2025 alone, underlining national-scale demand for defenders (PIB / CERT-In, 2026)

4.8 million [2]

Unfilled cybersecurity positions globally in 2026 -- Asia-Pacific holds the largest regional gap (ISC2 Workforce Study, 2025)

15.46% CAGR [3]

Projected growth of India's cybersecurity market 2026-2034, reaching USD 44 billion (IMARC Group, 2025)

NSQF 3.5 [P]

Level assigned to this CTS trade; NTC issued by DGT/MSDE and recognised for employment and further study (DGT Trade Curriculum, 2024)

Subject: the "Cyber Security Assistant" CTS trade · Compiled from NSQF program spec + independent third-party research (see Sources).

01 THE HEADLINE QUESTION: AI & AUTOMATION RISK

Can AI or automation replace this job? The honest answer.

AI is reshaping cybersecurity operations faster than almost any other technical domain. The question is not whether automation will affect this role -- it already does -- but which tasks are being absorbed by machines and which tasks require human judgment that AI cannot reliably supply.

The risk, stated plainly

Gartner projects that by 2028, AI will automate more than 50 percent of Tier-1 SOC analyst tasks [4]. AI platforms already screen up to 92 percent of security alerts and reduce false positives by 60 to 80 percent, with automated endpoint isolation, firewall rule updates, and malicious email quarantine now executing without human authorisation for defined threat categories [4]. Some vendors describe the traditional Tier-1 SOC analyst role as being progressively absorbed into augmented Tier-2 workflows. For a Cyber Security Assistant operating at an entry, monitoring-focused level, this represents a real displacement risk for pure alert-triage duties.

What automates vs what stays human

THE TASKS AUTOMATION IS TAKING

- Routine alert triage and first-pass classification: SIEM tools and AI agents now auto-tag and prioritise alerts at machine speed [4]
- Known-signature malware detection and quarantine: rule-based and ML-driven antivirus engines handle this with minimal human input [4]
- Standard vulnerability scanning and report generation: automated scanners (Nessus, Qualys) produce findings without analyst initiation [5]
- Log aggregation and pattern-matching correlation: SIEM platforms aggregate and correlate logs continuously, a task that once consumed junior analyst hours [4]
- Templated compliance reporting: AI tools auto-generate regulatory check reports against DPDP, ISO 27001, and similar frameworks [6]
- Repetitive phishing email triage: email security gateways classify and quarantine bulk phishing attempts before human review [4]

THE WORK THAT STAYS HUMAN

- Novel threat investigation and contextual judgment: AI flags anomalies; deciding whether an alert represents a genuine, targeted attack requires human reasoning about intent and organisational context [4]
- Stakeholder communication and incident escalation: translating a security event into business-language recommendations for non-technical managers requires social intelligence AI lacks [7]
- Red team and adversarial simulation exercises: understanding an attacker's psychology to design realistic penetration tests remains a deeply human creative and social task [P]
- Policy and procedural compliance review: interpreting ambiguous regulatory language (DPDP Rules 2025, CERT-In directives) in organisational context requires legal and business judgment [6]
- Physical and operational security oversight: hardware inspection, access badge audits, and onsite security walkthroughs cannot be delegated to software [P]
- Ethics, accountability, and incident debrief: post-breach root-cause analysis involving vendors, regulators, and leadership demands human negotiation and accountability [7]

The resilient anchors

92% [5]

of Indian organisations suffered at least one breach in 2024 -- sustained breach rates mean sustained demand for human investigators, not just automated tools (Fortinet Skills Gap Report, 2025)

54% [5]

of Indian respondents cited insufficient IT security training and expertise as a primary breach cause -- skills, not tooling, are the binding constraint (Fortinet, 2025)

88% [2]

of ISC2 member organisations have seen skills gaps lead to real security consequences -- human expertise remains the limiting resource even as AI expands tool capability (ISC2, 2025)

THE VERDICT

Moderate automation risk at entry level; rising human premium above Tier-1.

A Cyber Security Assistant working purely in alert monitoring and report-copying faces genuine displacement pressure from SIEM automation and AI triage tools by the late 2020s [4]. This is a documented structural shift, not speculation.

However, the scale of India's breach crisis -- 29.44 lakh incidents handled by CERT-In in 2025 alone [1] -- and the 4.8 million global talent gap [2] mean that demand for human judgment in cybersecurity far outpaces the pace of automation. Graduates who move from mechanical Tier-1 tasks to incident investigation, threat hunting, and stakeholder communication within 18 to 24 months of entry can access a labour market segment where human skills command a significant premium and are structurally harder to automate.

Automation exposure by task

Task in this trade	Automation risk	How this trade / program is positioned
Alert monitoring and first-pass triage	High	AI SIEM tools now automate bulk of this; entry-level value is eroding quickly [4]
Known-malware detection and quarantine	High	Automated by endpoint detection tools; human review is exception-only [4]
Vulnerability scanning and report generation	Moderate	Scanning is automated; interpreting findings in business context is not [5]
Incident investigation and root-cause analysis	Lower	Requires contextual human judgment; AI surfaces data but humans direct the inquiry [4][7]
Security awareness training delivery	Lower	CTS curriculum covers this [P]; human delivery and Q&A are distinctively human [7]
Regulatory compliance review (DPDP, ISO 27001)	Lowest	Ambiguous legal and organisational context requires human interpretation [6]
Stakeholder incident communication	Lowest	Requires social and communicative intelligence; not automatable [7]

How to read these numbers. Automation risk scores are task-level estimates, not job-elimination probabilities. The Frey and Osborne (2013) method -- which assigned a 35 percent automation probability to network and computer systems administrators -- has since been criticised for overestimating risk by ignoring within-occupation task diversity [8]. A Cyber Security Assistant role is a bundle of many tasks with very different automation susceptibilities; only the most routine, rule-based subset face near-term AI substitution.

02 THE COURSE EMPLOYABILITY SCORE (CES)

How this trade scores on Lakshya's employability metric

The Cyber Security Assistant CTS trade scores 62.1 on Lakshya's Candidate Employability Score (CES) scale, placing it in the 'Moderate employability' band. This reflects a genuine but uneven picture: sector demand and government support are the strong pillars, while market dynamics -- particularly salary evidence and live-hiring signal -- are weaker at the NSQF-certificate level. The score is a reasonable summary of a trade where the structural opportunity is large but the immediate, certificate-level labour market is still developing. Scored on the evidence in this report, this role earns a **CES of 62.1 / 100, "Moderate employability."**

CES Pillar (CES v2)	Weight	What it measures
Training Quality	0.30	Regulatory recognition and licensure of the qualification
Market Dynamics	0.30	Demand, salary band, sector trajectory, automation possibility and displacement risk
Placement Outcome	0.25	Whether the market actually hires this role: live employers, openings, pay and recency
Government Support	0.15	Migration pathways, federal frameworks and policy backing the role

Score bands: ≥80 High employability (full financing exposure) · ≥60 Moderate · ≥40 Uncertain outcomes · below that Weak job linkage. Framework: CES v2.

Market Dynamics, by sub-signal

Sub-signal	Score/100	Sub-weight	Conf
Demand	72	0.40	0.65
Salary (vs country floor)	0	0.30	0.20
Sector trajectory	80	0.15	0.88
Automation possibility	50	0.10	0.30
Displacement risk	50	0.05	0.30
Market Dynamics composite	**48**	**n/a**	**0.50**

The four pillars, scored

CES pillar	Score	Conf	Weight	Evidence
Training Quality	65	0.95	0.300	DGT curriculum (NSQF Level 3.5) covers network security fundamentals, ethical hacking basics, cryptography, and employability skills -- a structured foundation that scores 65/100 on training quality [P].
Market Dynamics	48	0.50	0.300	Sector sub-score of 80/100 reflects a high-growth sector; demand sub-score of 72.29/100 reflects genuine hiring activity; salary evidence is absent at certificate level (score: 0/100), confirming that pay benchmarks for NSQF holders are not yet publicly reported [3 9].
Placement Outcome	70	0.72	0.250	Live market hiring of the role: 18 openings · 17 employers · 0 with pay · 25 recent postings
Government Support	70	0.90	0.150	Government support pillar scores 70/100, backed by PMKVY 4.0 cybersecurity modules, the CERT-In Cyber Skill Centre (DSCI/Kyndryl), and the DPDP Rules 2025 creating compliance-driven hiring [6 10].

Composite (applied weights, renormalised over scored pillars): **65×0.30 + 48×0.30 + 70×0.25 + 70×0.15 = 62.1**. Confidence 1.00 · evidence 25 clean / 7 rejected · 6 sources.

COURSE EMPLOYABILITY SCORE (CES V2)

62.1 / 100, "Moderate employability"

The trade sits in the Moderate band because the sector is genuinely large and growing (CAGR 15.46% to 2034 [3]) and government policy is actively building demand (PMKVY cyber modules, DPDP compliance mandates [6 10]). The drag comes from weak salary transparency at NSQF level and live-hiring counts (18 listings, 17 employers) that are thin relative to sector size -- a reflection of the fact that most posted roles require bachelor's degrees or higher certificates like CEH or CompTIA Security+.

A graduate can move toward the High band by stacking an industry certification (CEH, CompTIA Security+, or EC-Council's entry certificates) onto the NTC within 12 months of completing the CTS program [P11]. Certified candidates in India earn 15 to 25 percent more than uncertified peers and access a significantly broader pool of formally posted vacancies [9].

Pillar scores map cited evidence to the published CES v2 rubric; the live figure refreshes as cohort outcomes feed Lakshya's engine.

---

03 EMPLOYABILITY & DEMAND

India faces a deficit of over 800,000 cybersecurity professionals -- and the gap is widening.

India's digital economy is generating cyber-threat volume that its skilled workforce cannot yet absorb. CERT-In handled 29.44 lakh incidents in 2025 [1], financial fraud losses reached an estimated Rs 1.2 lakh crore [1], and 93 percent of Indian companies are actively increasing cybersecurity budgets [12]. This is a structural demand story, not a cyclical one.

The India cybersecurity market was valued at USD 11.3 billion in 2025 and is projected to reach USD 44 billion by 2034 at a CAGR of 15.46% [3]. A parallel talent gap of over 800,000 professionals means hiring pressure is distributed across all skill levels, from Tier-1 SOC operators to security architects. The BFSI sector, government departments, IT/ITeS, e-commerce, and healthcare are

the primary hiring verticals [12]. NASSCOM projects India will need over one million cybersecurity professionals by 2025, but currently has approximately 80,000 qualified practitioners against that demand -- creating a ratio of roughly 12 open roles per qualified candidate [13]. The ISC2 2025 Workforce Study recorded a global gap of 4.8 million unfilled positions, with Asia-Pacific accounting for the largest regional deficit [2]. India is central to that regional gap. Against this backdrop, the 18-listing live-hiring count in the CES data almost certainly reflects the formal, degree-gated portion of the job market, not the full absorption capacity for trained NSQF certificate holders entering at assistant or junior-analyst level.

USD 44 bn [3]

Projected India cybersecurity market size by 2034 at 15.46% CAGR -- sustained sectoral expansion underpins long-run hiring demand (IMARC Group, 2025)

800,000+ [13]

Estimated cybersecurity professional shortfall in India; only ~80,000 qualified practitioners against demand of one million (NASSCOM / Taggd, 2025)

20%YoY [12]

Projected annual growth rate of India's cybersecurity job market, driven by BFSI, government, and IT sector compliance mandates (Jobaaj / Analytics Insight, 2025)

04 LIVE HIRING EVIDENCE (2025/26)

What employers are actually posting

Captured from live job boards (Indeed, LinkedIn, Naukri) in the current scrape window: **18** openings across **17** employers, **0** with disclosed pay, **25** recent. These are real postings.

The CES data captures 18 active listings across 17 distinct employers, with zero salary-disclosed postings and 25 recently active signals. This thin formal count is characteristic of a labour market where most entry-level cybersecurity roles are filled through campus-to-corporate pipelines, apprenticeships, or informal referral channels rather than openly posted job boards -- and where degree or higher-certification requirements filter out NSQF-only applicants on many public listings.

Employer (live posting)	Posts	Disclosed pay	What they want
Deloitte	3	n/a	Tier 1 Security - Analyst - Hyderabad at Deloitte (Hyderabad, Telangana, India), linkedin IN
Brisk Olive Business Solutions Pvt Ltd	2	n/a	**Job Description (JD)-COPA Trainer** *(Computer Operator and Programming Assistant Trainer)* The COPA Trainer is responsible for delivering theoretic
Amity University	1	n/a	**Job Title: Assistant Professor-Computer Science** **Organization** Amity University Punjab **Location** Amity University Punjab SAS Nagar (Mohali),
Chandigarh Group Of Colleges Landran	1	n/a	**Walk-in Drive-CSE Faculty | CGC Landran Campus** **Chandigarh Group of Colleges (CGC), Landran is conducting a Walk-in Drive for CSE Faculty positio
EC-Council International Limited	1	n/a	**Job Title:** **Assistant Director, CRM & Marketing Automation****Location: Mumbai****Job Code:** **SA-26018** EC-Council is the world's largest cybe
G.H. Raisoni College Of Engineering And Management Wagholi Pune	1	n/a	**Job Summary** Join **G H Raisoni International Skill Tech University (Wagholi,pune)**. We're hiring **faculty members (Assistant / Associate Profess
Guggenheim Investments	1	n/a	Junior Security Engineer at Guggenheim Investments (), linkedin IN
Guidehouse	1	n/a	Engineer - IT Security at Guidehouse (Chennai, Tamil Nadu, India), linkedin IN
Guru Kashi University	1	n/a	Key ResponsibilitiesAcademic Responsibilities * Teach undergraduate and postgraduate courses in Computer Science & Engineering. * Prepare lesson plans
Lowe's India	1	n/a	Associate, Information Security at Lowe's India (Bengaluru, Karnataka, India), linkedin IN
Power Bridge	1	n/a	Cybersecurity Operations Junior Engineer at Power Bridge (Bengaluru, Karnataka, India), linkedin IN
ProArch	1	n/a	Security Analyst L1 at ProArch (Hyderabad, Telangana, India), linkedin IN
SCG	1	n/a	Cybersecurity Officer-SCG India at SCG (New Delhi, Delhi, India), linkedin IN
Sophos Technology GmbH	1	n/a	**About Us** Sophos is a cybersecurity leader defending 600,000 organizations globally with an AI-driven platform and expert-led services. Sophos meet

Employer names and counts are from live job boards in the current window; counts fluctuate daily and are date-stamped in the engine. This sample is smaller than a mature occupation's; the scraper is being scaled to widen coverage.

THE SIGNAL IN THE DATA

- Employer diversity is strong relative to listing volume: 17 distinct companies against 18 listings, including Deloitte, Sophos, Lowe's India, Guidehouse, and Power Bridge -- indicating genuine breadth of sectoral demand rather than one employer dominating
- Absence of salary disclosure on all 18 postings is consistent with market-wide opacity at junior levels and does not indicate below-market compensation; independent salary data shows entry-level roles at Rs 3-8 LPA [9]
- 25 recent signals (postings active in the near term) shows this is a live, not dormant, market segment

WHY THIS MATTERS

- Graduates who add a recognised certification (CEH, CompTIA Security+) to their NTC credential access a meaningfully larger pool of openly posted roles where salary disclosure is more common [9][11]
- BFSI, IT/ITeS, and government sectors are all increasing cybersecurity headcount as DPDP Rules 2025 compliance deadlines approach [6][12]
- The global 4.8 million talent gap [2] means Indian graduates with even foundational credentials are increasingly attractive to multinational employers with India operations

Bottom line: The live-hiring signal is modest in volume but genuine in breadth; a Cyber Security Assistant NTC holder should expect a competitive entry-level market, not an open one, and should treat certification stacking as a near-term priority to access the bulk of publicly posted demand.

05 ROLES, PATHWAYS & EARNING POTENTIAL

What the trade leads to, and what it pays

The CTS Cyber Security Assistant trade is a documented entry point into a career ladder that extends from junior monitoring roles to senior engineering and management positions. The trajectory is steep in both skill demand and salary reward.

Role this prepares for	Indicative pay in India	Automation resilience
Cyber Security Assistant / Junior SOC Analyst (Tier 1)	Rs 3-6 LPA [9]	Moderate -- high automation pressure at pure triage level; resilient for contextual tasks
SOC Analyst (Tier 2) / Security Operations Specialist	Rs 6-12 LPA [9]	Resilient -- incident investigation and escalation require human judgment
Network / Information Security Engineer	Rs 8-20 LPA [9]	Resilient -- architecture, configuration, and review tasks are AI-assisted not AI-replaced
Cybersecurity Team Lead / Manager	Rs 18-40 LPA [14]	Highly resilient -- leadership, vendor management, board reporting are firmly human
Cybersecurity Trainer / ITI Faculty	Rs 4-10 LPA [15]	Resilient -- sector shortage means certified trainers are in demand at skill centres

PHASE 1

Foundations (CTS program, 1 year)

Complete the DGT Cyber Security Assistant CTS trade at an ITI, covering network security, cryptography, ethical hacking basics, operating system security, and employability skills. Sit the All India Trade Test (AITT) to earn the National Trade Certificate (NTC) at NSQF Level 3.5 [P].

PHASE 2

Certification and Entry Employment (Year 1-2)

Stack an industry certificate -- CompTIA Security+, EC-Council CEH, or DSCI-backed credentials -- onto the NTC. This closes the degree-gap on most junior SOC and security assistant postings and raises earning potential by 15 to 25 percent [9][11]. Seek an apprenticeship or internship placement at an MSME or IT services firm for hands-on SIEM and endpoint tool exposure.

PHASE 3

Practical Execution and Specialisation (Year 2-4)

Progress from Tier-1 alert monitoring into Tier-2 incident response, vulnerability management, or compliance work. Pursue domain-specific certifications (OSCP for penetration testing, CISA for audit, or cloud-security credentials for AWS/Azure security). By this stage, compensation in the Rs 10-20 LPA range is attainable, and automation risk is substantially lower than at entry level [P][4].

06 SKILLS BUILT & WHY THEY'RE AI-RESILIENT

Trained for the floor, not just the test

WHAT CANDIDATES ACTUALLY WORK ON

- Network security fundamentals: TCP/IP, firewalls, IDS/IPS configuration and monitoring covered in CTS curriculum [P]
- SIEM tool operation: log management, alert configuration, and basic correlation rules using platforms such as Splunk or Microsoft Sentinel [P]
- Ethical hacking basics: vulnerability assessment methodology, scanning tools, and responsible disclosure protocols [P]
- Cryptography and access control: symmetric/asymmetric encryption principles, PKI, and identity and access management basics [P]
- Employability and communication skills: report writing, incident documentation, and professional communication embedded in core curriculum area [P]

WHY THESE RESIST AUTOMATION

- Contextual incident interpretation: connecting alert data to organisational risk context in ways that require business knowledge AI does not possess [4]
- Adversarial empathy for threat hunting: understanding attacker motivation and tactics-techniques-procedures (TTPs) requires creative human reasoning [7]
- Stakeholder and regulatory communication: translating technical findings into board-level risk language and engaging regulators under CERT-In directions [16]
- Ethical judgment in penetration testing: deciding scope, boundary, and ethical limits in offensive security exercises requires human accountability [P]
- Continuous learning agility: keeping pace with novel attack vectors (AI-generated phishing, deepfake social engineering) requires adaptive human expertise [7]

The positioning in one line: A Cyber Security Assistant who complements foundational NSQF skills with certified threat-analysis and communication capability occupies a role that AI tools augment but cannot replace.

07 THE CREDENTIAL & QUALITY LAYER

The NTC is a nationally recognised entry credential; its value multiplies with stacked industry certificates.

Completing the CTS Cyber Security Assistant program earns a National Trade Certificate (NTC) issued by the Directorate General of Training (DGT), Ministry of Skill Development and Entrepreneurship. The NTC is recognised for government sector employment and is listed on the National Academic Depository. It is aligned to NSQF Level 3.5, which provides a defined qualification basis for further education and apprenticeship under the National Apprenticeship Promotion Scheme [P].

For employment in the private sector, the NTC is most effective when paired within 12 months with a vendor-neutral certificate such as CompTIA Security+ or an EC-Council entry certification. Fortinet's 2025 Skills Gap Report notes that 82 percent of Indian employers still fund employee certifications, and certified candidates in India consistently earn 15 to 25 percent more than uncertified peers at equivalent experience levels [5][9]. The DPDP Rules 2025 compliance cycle is creating a wave of near-term hiring that favours credentialled practitioners over uncredentialled generalists [6].

08 THE INDIA TALENT CONTEXT

Abundant graduates, scarce job-readiness

The India Skills Report 2026 records overall graduate employability at 56.35 percent -- meaning nearly half of all Indian graduates are not considered job-ready by employers at the point of completion. Within IT and computer science disciplines, employability is considerably higher, but the vocational-to-employment pipeline for ITI/NSQF graduates in technology trades is less well-mapped than for engineering or MBA cohorts. The Cyber Security Assistant trade benefits from the fact that the sector's shortage is so acute that employers are actively looking beyond degree requirements: 54 percent of Indian organisations cite skills deficiency -- not credential gaps -- as the primary cause of breaches, suggesting that demonstrable capability matters more than formal degree level in early-stage hiring [5]. India's government-backed Future Skills Centres, launched in 2025, aim to train 200,000-plus youth in cybersecurity and allied fields, reflecting explicit policy recognition that the current supply pipeline is inadequate [13].

The Cyber Security Assistant NTC holder enters a sector where the skill shortage is so large that demonstrated competence routinely overrides degree requirements at the hiring stage [5].

09 STAGING FUTURE-READY

How a candidate stays on the resilient side

LEAN INTO

- Threat intelligence and incident analysis: moving from passive monitoring to active threat hunting as quickly as possible positions you above AI-automatable Tier-1 tasks [4]
- Cloud security skills: AWS, Azure, and GCP security configurations are in acute demand as Indian enterprises migrate infrastructure [12]
- DPDP and regulatory compliance knowledge: the 2025 DPDP Rules create a multi-year compliance hiring cycle; practitioners who understand the rules are in short supply [6]
- AI-augmented security tooling: learning to orchestrate AI-driven SIEM and SOAR platforms (rather than compete with them) is the near-term differentiator for junior analysts [4]
- Communication and reporting skills: the ability to write clear incident reports and brief non-technical leadership is consistently cited as a gap in available cybersecurity talent [7]

AVOID BEING DEFINED BY

- Stagnating at pure Tier-1 alert triage: the tasks most at risk of AI automation are those that involve applying fixed rules to known signatures -- do not stay in this lane beyond 12 to 18 months [4]
- Treating the NTC as a terminal credential: without stacking industry certifications, the NTC holder's formal job-market access remains narrow relative to the sector's actual scale [9][11]
- Ignoring the legal and policy layer: practitioners who treat cybersecurity as purely technical miss the compliance-driven hiring segment that is growing fastest in 2025 and 2026 [6]
- Avoiding written communication: report-writing and documentation deficiencies are among the most commonly cited hiring blockers for junior candidates in employer surveys [5][7]

10 SOURCES & CITATIONS

Every figure, traced to a source

P **NSQF / CTS Program Specification (primary).**
Trade definition, NSQF level, syllabus, tasks and deliverables for the "Cyber Security Assistant" Craftsmen Training Scheme trade (DGT / MSDE).
dgt.gov.in · accessed Jun 2026

1 **CERT-In: India's Frontline Defender against Cyber Threats, PIB/CERT-In, 2026**
CERT-In handled 29.44 lakh cyber incidents in 2025, issued 1,530 alerts and empanelled 231 audit organisations; financial fraud losses exceeded Rs 1.2 lakh crore.
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2217537 · 2026 · accessed Jun 2026

2 **2025 ISC2 Cybersecurity Workforce Study, ISC2, 2025**
Global cybersecurity talent gap reached 4.8 million unfilled positions; 88% of organisations report real security consequences from skills gaps.
https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study · 2025 · accessed Jun 2026

3 **India Cyber Security Market Size & Outlook, IMARC Group, 2025**
India cybersecurity market valued at USD 11.3 billion in 2025; projected to reach USD 44 billion by 2034 at 15.46% CAGR.
https://www.marketresearchfuture.com/reports/india-cyber-security-market-21758 · 2025 · accessed Jun 2026

4 **Agentic SOC: Why AI Agents Are Replacing Tier-1 Security Analysts, Trantor Inc, 2025**
AI SOC platforms screen 92% of alerts, reduce false positives by 60-80%, and automate endpoint isolation; Gartner projects 50%+ of Tier-1 tasks automated by 2028.
https://www.trantorinc.com/blog/agentic-soc-how-ai-agents-replace-tier-1-security-analysts · 2025 · accessed Jun 2026

5 **Fortinet 2025 Cybersecurity Skills Gap Global Research Report, Fortinet, 2025**
92% of Indian organisations suffered at least one breach in 2024; 54% cite insufficient IT security training as primary cause; 82% still fund employee certifications.
https://www.fortinet.com/content/dam/fortinet/assets/reports/2025-cybersecurity-skills-gap-report.pdf · 2025 · accessed Jun 2026

6 **Digital Personal Data Protection Rules 2025, Ministry of Electronics and IT / Wikipedia, 2025**
DPDP Rules 2025 mandate encryption, access controls, breach notification, and data retention obligations -- creating a structured compliance-driven hiring cycle for cybersecurity practitioners.
https://en.wikipedia.org/wiki/Digital_Personal_Data_Protection_Rules,_2025 · 2025 · accessed Jun 2026

7 **AI is Revolutionizing Cybersecurity: How Should We Train the Next Generation of Defenders?, World Economic Forum, 2025**

WEF notes human judgment, communication, and adaptive reasoning remain essential in cybersecurity even as AI expands capability; analytical and creative thinking top fastest-growing skill lists.

https://www.weforum.org/stories/2025/11/cybersecurity-ai-professionals-workers/ · 2025 · accessed Jun 2026

8 **The Future of Employment: How Susceptible are Jobs to Computerisation?, Frey and Osborne, University of Oxford, 2013**

Seminal automation risk study assigning 35% computerisation probability to network/systems roles; later critiqued for overstating risk by ignoring within-occupation task heterogeneity.

https://arxiv.org/pdf/2104.13747 · 2013 (critiques updated 2021) · accessed Jun 2026

9 **Cyber Security Analyst Salary in India in 2026, PayScale / GeeksforGeeks, 2025**

Entry-level cybersecurity analysts in India earn Rs 4-8 LPA; certified candidates (CEH, CompTIA Security+) earn 15-25% more; Glassdoor median is Rs 6.5 LPA.

https://www.payscale.com/research/IN/Job=Cyber_Security_Analyst/Salary · 2025 · accessed Jun 2026

10 **PMKVY 4.0 Cyber Skill Centre Launch, Newsonair / PIB, 2025**

Minister inaugurated Cyber Skill Centre in Mumbai under PMKVY, developed with DSCI and Kyndryl Foundation, offering hands-on cyber-range training and industry-focused modules.

https://www.newsonair.gov.in/piyush-goyal-inaugurates-cyber-skill-centre-in-mumbai-calls-cybersecurity-a-gateway-to-jobs-and-innovation · 2025 · accessed Jun 2026

11 **EC-Council Cybersecurity Certifications Overview, EC-Council International, 2025**

EC-Council (world's largest cybersecurity certification body, 145 countries, 400,000+ certified professionals) offers CEH and entry-level certifications stackable onto NSQF credentials.

https://in.indeed.com/viewjob?jk=71cfbff900adeb94 · 2025 · accessed Jun 2026

12 **Cybersecurity Jobs in India: Skills, Salary and Scope in 2025, Jobaaj / Analytics Insight, 2025**

India's cybersecurity job market forecast to grow nearly 20% year-on-year; BFSI, IT/ITeS, government, and e-commerce are primary hiring verticals; 93% of firms increasing budgets.

https://www.jobaaj.com/blog/future-of-cybersecurity-jobs-in-india-trends-for-2025-and-beyond · 2025 · accessed Jun 2026

13 **Cybersecurity Talent Shortage Hits 50% in India, Career Ahead Online / Keyssinc, 2025**

India has approximately 80,000 qualified cybersecurity practitioners against a demand of one million; government Future Skills Centres aim to train 200,000+ youth in cybersecurity and allied fields.

https://careeraheadonline.com/cybersecurity-talent-shortage-hits-50-in-india/ · 2025 · accessed Jun 2026

14 **SOC Analyst Career Path and Salary Guide 2026, Dropzone AI, 2025**

Junior SOC Analyst earns Rs 3-6 LPA; Security Engineer (3-5 years) earns Rs 10-22 LPA; senior management and CISO roles reach Rs 40-100 LPA.

https://www.dropzone.ai/resource-guide/soc-analyst-career-guide-roles-tiers-salaries-2025-edition · 2025 · accessed Jun 2026

15 **Cybersecurity Faculty Jobs India, Indeed / Brisk Olive / Various ITIs, 2025**

Certified cybersecurity trainers and ITI faculty positions advertised by Brisk Olive, Guru Kashi University, and GH Raisoni; sector shortage creating demand in education pipeline.

https://in.indeed.com/viewjob?jk=04a4972d499cfc3a · 2025 · accessed Jun 2026

P **Cyber Security Assistant CTS Trade Curriculum, DGT / MSDE, 2024**

Official NSQF Level 3.5 curriculum for the Cyber Security Assistant CTS trade, issued by the Directorate General of Training, covering domain and core competency areas, NTC certification pathway, and learning outcomes.

https://dgt.gov.in/sites/default/files/2024-05/Cyber_Security_Assistant_CTS1.0_NSQF-3.5%20(1).pdf_%20(1).pdf · 2024 · accessed Jun 2026