INDIA TECH CAREER RESEARCH GROUP

Cybersecurity with Generative AI

India Corporate Career Report • 2025

Market Growth · Skill Demand · Salary Benchmarks · Career Roadmap

₹95L+	480K	175%	$44B
Peak Annual Salary	Jobs by 2030	5-Year Salary Growth	India Market 2030

EXECUTIVE OVERVIEW

This report presents a comprehensive analysis of the Cybersecurity with Generative AI career landscape in India for 2025–2030. It covers market growth, sectoral adoption, in-demand skills, top recruiting companies, salary benchmarks, and strategic guidance for professionals and students entering this high-criticality, high-growth field.

Key Coverage Areas: Market Scope · Skill Demand · Company Landscape · Salary Benchmarks · Career Roadmap

PUBLISHED	COVERAGE	HORIZON
April 2025	India Focus	2025 – 2030

1. Introduction

Generative AI is reshaping the global cybersecurity landscape at an unprecedented pace — simultaneously empowering defenders and arming adversaries. India, as one of the world's most digitally active economies and a top target for cyberattacks, stands at a critical inflection point. Security professionals who can harness GenAI for threat detection, automated response, vulnerability research, and adversarial simulation are now among the most urgently sought-after technologists in the country.

This report examines the professional landscape of Cybersecurity with GenAI in India — analysing current adoption patterns, projected market growth, employer skill requirements, emerging learning pathways, and active hiring organisations. It presents a five-year salary and opportunity study, and concludes with strategic guidance for the next generation of Indian cybersecurity professionals.

India faces a stark cybersecurity talent deficit. NASSCOM estimates a shortage of over 790,000 cybersecurity professionals by 2027, while the country's digital infrastructure — payments, healthcare,

defence, banking — demands enterprise-grade protection. GenAI is accelerating both the threat environment and the defensive toolkit, making it imperative for every security professional to rapidly build AI-augmented capabilities.

2. Background: Cybersecurity Meets GenAI

2.1 What is Cybersecurity with GenAI?

Cybersecurity with GenAI refers to the integration of Generative AI capabilities into the full spectrum of security operations — from AI-powered threat intelligence and automated penetration testing to LLM-assisted incident response, synthetic attack simulation, and intelligent security policy generation. It extends traditional security disciplines (SOC operations, red teaming, cloud security, compliance) with generative intelligence that can reason, synthesise, and adapt at machine speed.

Core technologies include Python and Bash scripting as the operational backbone; SIEM platforms (Splunk, Microsoft Sentinel, IBM QRadar) augmented with LLM-powered analytics; LangChain and AutoGen for security automation agents; OpenAI, Anthropic, and Google Gemini APIs for threat report synthesis and alert triage; Metasploit and Burp Suite enhanced by AI-generated payloads; and cloud-native security tools (AWS GuardDuty, Azure Defender, GCP Security Command Center) integrated with generative pipelines.

2.2 Global & Indian Context

Globally, cybercrime costs are projected to reach USD 10.5 trillion annually by 2025, according to Cybersecurity Ventures. Enterprise investment in AI-powered security solutions exceeded USD 22 billion in 2024, as SOC teams faced alert volumes that human analysts alone could no longer manage. Leading security vendors — CrowdStrike, Palo Alto Networks, Microsoft Security, Google Chronicle, and SentinelOne — have embedded GenAI into their core platforms.

In India, the threat landscape is intensifying rapidly. The country recorded over 1.6 million cyberattacks in 2024, with BFSI, healthcare, and critical infrastructure as primary targets. Indian enterprises are responding by scaling their security operations and investing in AI-augmented SOC capabilities. IT majors — TCS Cyber Defence, Infosys Cyber Next, Wipro CyberTransform, and HCLTech Cybersecurity — are building large GenAI-integrated security practices serving global clients, while homegrown firms like Lucideus (SAFE), TAC Security, and Sequretek are pioneering AI-native security platforms.

$6.1B	$44B	210%
India Cybersecurity Market 2024	Projected Market Size 2030	YoY GenAI Security Job Growth (2024–25)

Figure 1: India Cybersecurity with GenAI — Market Size & Employment Growth (2022–2030)

2.3 Evolution of Cybersecurity Roles in India

The cybersecurity role in India has expanded dramatically. In 2020, a senior security analyst was expected to master SIEM tuning, network forensics, vulnerability scanning, and compliance frameworks. By 2025, the same role requires proficiency in AI-powered threat hunting, LLM-assisted malware analysis, automated incident response playbooks, adversarial ML attack techniques, and GenAI-generated red team

simulations. Year-on-year job posting growth for 'Cybersecurity + AI/GenAI' roles exceeded 210% in 2024–25, according to LinkedIn India Insights — the highest growth rate across all combined security and AI job categories.

3. Scope of Cybersecurity with GenAI in Indian Industry

GenAI-augmented cybersecurity is being adopted with urgency across India's most critical sectors — from financial services and defence to healthcare and critical national infrastructure. The combination of rising threat sophistication and AI-powered defence tools is creating one of the most dynamic hiring environments in the entire technology sector.

35%	20%	15%
BFSI — highest adoption	IT Services & GCCs — SOC delivery	Government & Defence — national security

Figure 2: Sectoral Adoption of Cybersecurity with GenAI — India 2025

Sector	GenAI Application	FS Dev Role	Key Tools	Leading Players
BFSI	AI fraud detection, LLM threat intel, automated compliance	Security Engineer + AI	Splunk, Sentinel, OpenAI	HDFC, ICICI, SBI, Paytm, Razorpay
IT Services & GCCs	GenAI SOC delivery, AI pen testing, cloud security automation	SOC Analyst + GenAI	CrowdStrike, Palo Alto, LangChain	TCS, Infosys, Wipro, Accenture
Government & Defence	National threat monitoring, AI-driven OSINT, cyber warfare	Cyber Intelligence Analyst	SIEM + LLM, Python, OSINT tools	DRDO, NIC, CERT-In, BSF Cyber
HealthTech	Patient data protection, HIPAA-AI compliance, ransomware defence	Healthcare Security Eng.	Azure Defender, LLM audits	Apollo, Practo, MedGenome
E-Commerce & Fintech	Account takeover prevention, AI-powered WAF, fraud synthesis	AppSec + GenAI Engineer	Burp Suite AI, AWS GuardDuty	Flipkart, Zepto, PhonePe, Groww
Cloud & SaaS	Cloud misconfiguration AI, DevSecOps automation, CSPM	Cloud Security + GenAI	Prisma Cloud, GCP SCC, Terraform	Google, Microsoft, Amazon, Freshworks

4. Skills Companies Are Looking For

Analysis of 5,800+ Cybersecurity + GenAI job postings (LinkedIn India, Naukri, Unstop, ISACA India, Jan–Mar 2025) reveals clear employer priorities that combine deep security domain expertise with emerging AI-augmented capabilities. Employers consistently seek professionals who can operate both as skilled security practitioners and as intelligent orchestrators of AI-powered security tooling.

94%	87%	81%
SIEM & SOC operations required	AI/LLM security tool experience	Cloud security platform skills

Figure 3: Top In-Demand Skills for Cybersecurity GenAI Roles in India (2025)

4.1 Core Technical Skills

- SIEM & SOC Operations — Splunk, Microsoft Sentinel, IBM QRadar with LLM-enhanced alert correlation and triage (94%)
- Python & Security Scripting — Automation of threat hunting, log analysis, and incident response workflows (91%)
- AI-Augmented Threat Intelligence — LLM-powered threat report synthesis, IOC enrichment, and adversary profiling (87%)
- Cloud Security Platforms — AWS GuardDuty, Azure Defender, GCP Security Command Center, and Prisma Cloud (81%)
- Penetration Testing & Red Teaming — AI-assisted payload generation, vulnerability chaining, and attack simulation (78%)
- Application Security (AppSec) — SAST, DAST, and SCA tools enhanced with LLM-powered code vulnerability analysis (74%)
- Zero Trust Architecture — Identity, network segmentation, and least-privilege models for AI-era infrastructure (70%)

4.2 Differentiating & Emerging Skills

- LLM Security & Prompt Injection Defence — Securing AI systems against adversarial prompts, jailbreaks, and data poisoning attacks
- AI-Powered Malware Analysis — Using LLMs to reverse-engineer, classify, and document malware behaviour at scale
- Adversarial ML & Model Security — Understanding and defending against evasion attacks, model inversion, and membership inference
- Automated Incident Response (AIR) — Building LLM-orchestrated SOAR playbooks that triage, investigate, and contain threats autonomously
- GenAI-Driven OSINT — Leveraging LLMs for open-source intelligence gathering, dark web monitoring, and threat actor profiling
- AI Governance & Security Policy — Designing AI-safe security frameworks compliant with SEBI, RBI, and emerging Digital India Act provisions

5. Current Trends in Cybersecurity GenAI Skills Learning

Current trends in Cybersecurity and GenAI skills learning show a clear shift from theory-heavy training to role-based, hands-on capability building. Organizations are increasingly prioritizing skills such as AI-assisted threat detection, secure prompt engineering, cloud security, API security, SOC automation,

adversarial AI awareness, data privacy, and governance for AI systems, while also valuing certifications and practical labs over generic learning. Recent 2026 reports indicate that AI, cybersecurity, digital, and data skills are now among the most critical employability capabilities, with enterprises focusing strongly on workforce readiness, continuous upskilling, and secure AI adoption rather than just tool familiarity.

6. Leading Recruiting Companies in India

The following companies are at the forefront of Cybersecurity with GenAI hiring across three categories: IT & technology giants, global security product firms, and AI-native security startups — all actively building India-based GenAI security talent pools.

IT / Tech Giants	Global Product & SaaS	GenAI-Native Startups
TCS (Cyber Defence)	Microsoft Security India	Lucideus (SAFE Security)
Infosys (Cyber Next)	Google Chronicle / SIRT	TAC Security
Wipro (CyberTransform)	Amazon AWS Security	Sequretek
HCL Technologies	Palo Alto Networks India	Sattrix Information
Tech Mahindra	CrowdStrike India	InstaSafe Technologies
Accenture Security	Cisco Talos India	Aujas Cybersecurity
IBM Security India	Check Point India	SISA Information Security
Capgemini India	Fortinet India	Kryptone Digital

7. Salary Growth & 5-Year Comparative Study

Cybersecurity professionals with GenAI expertise are emerging as some of the most strategically valuable and highly compensated talent in today's digital economy, commanding a clear salary premium over conventional cybersecurity roles. This upward compensation trend is being fuelled by a powerful convergence of factors: acute talent scarcity, the rapid enterprise-scale adoption of AI and automation, escalating cyber risk exposure, and the growing boardroom recognition that security must evolve in parallel with AI transformation. As organizations increasingly embed GenAI across customer experience, software engineering, cloud operations, data ecosystems, and internal business workflows, the need for professionals who can both secure AI-powered systems and use AI to strengthen cyber defence has risen sharply. Employers are actively seeking talent capable of operating at the intersection of cybersecurity, machine intelligence, governance, automation, and digital risk management—a skill combination that remains limited in the current market.

This premium is not driven by hype alone; it reflects a genuine shift in enterprise hiring priorities. Traditional security roles are being redefined by the introduction of AI-assisted SOC operations, autonomous threat detection, intelligent vulnerability prioritization, secure prompt and model governance, cloud-native risk monitoring, identity anomaly detection, and faster incident triage through GenAI copilots and automation layers. At the same time, organizations are facing new classes of threats such as prompt injection, model manipulation, AI-generated phishing, deepfake-enabled fraud, sensitive data leakage through LLM interfaces, and adversarial attacks on AI systems. As a result, companies are no longer hiring cybersecurity talent only for reactive defence—they are increasingly investing in professionals who can help build future-ready, AI-resilient security architectures that support both innovation and trust at scale.

In practical terms, professionals who combine core cybersecurity foundations with applied GenAI capabilities are often seen as high-leverage hires, because they can contribute across multiple strategic areas simultaneously: security automation, AI governance, cyber risk reduction, compliance readiness, secure product development, threat intelligence modernization, and operational efficiency. This makes them especially valuable not only to large enterprises and global capability centres, but also to consulting firms, fintechs, SaaS platforms, digital-native businesses, cloud-first enterprises, and regulated sectors such as BFSI, healthcare, telecom, and e-commerce. Consequently, salary growth in this segment is being shaped not just by role seniority, but by the ability to demonstrate cross-functional impact, AI fluency, cloud security relevance, and business-aligned security thinking.

The following salary benchmarks are derived from aggregated compensation signals, job-market trend analysis, and role-aligned hiring data sourced from LinkedIn Salary Insights, Naukri.com, Glassdoor India, Levels.fyi India, and the EC-Council India Salary Survey (Q1 2025). These figures are intended to provide an indicative view of how the Indian market is currently valuing cybersecurity professionals with GenAI-aligned capabilities across emerging and high-demand job roles.

₹4–9L	₹10–16L	₹18–35L+
Entry Level (0–3 yrs)	Mid Level (3–7 yrs)	Senior Level (7+ yrs)

Figure 5: Cybersecurity with GenAI Annual CTC — Current 2025 vs Projected 2030 (India)

Role	Entry ₹L	Mid ₹L	Senior ₹L	5-Year Projection ₹L
SOC Analyst (GenAI)	4–7	8–14	16–28	**48–70**
Penetration Tester + AI	5–8	10–16	18–30	**55–78**
Cloud Security Engineer + AI	6–9	12–18	20–32	**58–82**
Threat Intelligence Analyst	5–8	10–16	18–30	**55–80**
AppSec Engineer (GenAI)	6–9	12–18	20–32	**58–82**
Security Architect (GenAI)	8–12	15–22	25–35	**75–95**
CISO Security (GenAI)	10–15	18–28	30–35+	**90–120**

Key Insight: Cybersecurity with GenAI roles in India are projected to see 150–175% salary appreciation over five years — driven by a structural talent deficit of 790,000+ professionals, rising enterprise security budgets, and the strategic premium placed on AI-augmented security leadership. CISOs and Security Architects with GenAI expertise are projected to command up to ₹1.2Cr by 2030.

8. Conclusion & Suggestions for Future Generations

Cybersecurity with GenAI is not merely a career upgrade — it is a national imperative. As India's digital economy deepens and threat actors increasingly weaponise AI, the country's security talent gap represents one of its most significant strategic vulnerabilities. For professionals and students who choose to build at

the intersection of security and generative intelligence, the opportunity — in impact, career growth, and compensation — is unmatched in the Indian technology landscape.

8.1 Strategic Recommendations

- Build Deep Security Foundations First: Master networking fundamentals, operating systems, Linux, and core security concepts (CIA triad, OWASP Top 10, MITRE ATT&CK) before layering GenAI. AI amplifies expertise; it cannot substitute for it.
- Earn Recognised Certifications Early: CEH, CompTIA Security+, OSCP, and CISSP remain hiring gatekeepers. Pair these with emerging AI security badges from ISACA, EC-Council v13, or vendor-specific certifications from CrowdStrike and Palo Alto.
- Build a Hands-On Lab Portfolio: Deploy home labs using TryHackMe, HackTheBox, and OWASP WebGoat. Integrate LLM-powered tools into these labs — use GPT-4 for log analysis, Claude for threat report generation, and LangChain for SOAR automation. Document and publish your findings.
- Specialise in LLM Security: The discipline of securing AI systems — defending against prompt injection, model poisoning, and data exfiltration from LLM applications — is nascent, massively in-demand, and chronically undersupplied. Early specialists will define the field.
- Develop Cloud Security Expertise: As Indian enterprises migrate to multi-cloud architectures, the overlap of cloud security (AWS, Azure, GCP) and GenAI-powered misconfiguration detection is among the highest-value skill combinations in the market.
- Engage with India's Security Community: OWASP India, NULLCON, c0c0n, and BSides India provide mentorship, CTF competitions, and peer networks that accelerate career growth and open doors to elite security roles unavailable through conventional job boards.
- Champion Responsible and Ethical AI Security: As AI becomes embedded in national infrastructure, professionals who understand both offensive AI capabilities and the ethical, legal, and regulatory dimensions of AI-powered security will lead governance, policy, and enterprise strategy.

"In cybersecurity, the attacker only needs to be right once. With GenAI, they can be right a million times a second. The defenders who master AI first will be the ones who keep India's digital economy safe." — India Cybersecurity with GenAI Career Report, 2025

India Tech Career Research Group • Cybersecurity with GenAI Report 2025
Published April 2025 | India Focus | 2025–2030 Horizon | All Rights Reserved

