HACKTHEBOX

Cybersecurity Workforce Intelligence Report: Global Skills, Interests, and Career Trends

Executive Summary

The cybersecurity workforce continues to evolve rapidly as organizations confront increasingly complex threats and technological disruption. This report examines how organizations and cybersecurity professionals are adapting to emerging risks, particularly those driven by artificial intelligence, which are introducing new attack surfaces and reshaping security priorities.

The findings are based on anonymized proprietary Hack The Box (HTB) platform data collected between mid-March and early December 2025, covering 702,226 cybersecurity professionals across 251 countries and territories. This represents one of the most extensive global datasets on cybersecurity talent. The analysis combines self-declared training interests with activity-based insights from approximately 1,500 users engaging with AI/ML labs, enabling a detailed view of skill development trends, experience levels, and career trajectories.

702,226

cybersecurity professionals

#4

AI Penetration Testing training interest

80%+

team engagement in enterprise benchmarks

Top 3

AI attack vectors:

- Prompt Injection
- Model Exploitation
- Agentic AI Hijacking

Key findings

1 AI is reshaping cybersecurity training priorities

AI penetration testing now ranks among the top global training interests, reflecting a rapidly growing demand for AI security skills. Increased focus on attack vectors such as prompt injection, model exploitation, and agentic AI hijacking highlights how quickly the threat landscape is evolving. In response, organizations are investing more in proactive AI security capabilities.

2 Cybersecurity skill development is becoming more integrated

Training patterns show increasing overlap between offensive and defensive skill development. Practitioners across both domains are building complementary capabilities, signaling a move toward more collaborative and integrated security models.

3 Cybersecurity talent development is becoming more global

India and the United States together account for nearly 28% of training interest, reflecting both the scale of the U.S. as a mature cybersecurity market and India's rapid emergence as a high-growth talent hub.

4 Enterprise training drives engagement at scale

Structured, organization-led training programs consistently demonstrate high engagement and strong participation, compared to self-directed learning, while also accelerating the adoption of emerging skills such as AI security.

Taken together, these findings highlight a workforce that is adapting quickly to new technologies and threat models, while also pointing to areas where organizations must continue to invest.

AI Security is a Major Training Priority

1

Artificial intelligence is rapidly emerging as one of the most urgent priorities in cybersecurity. With AI penetration testing ranking #4 globally in training interest, demand for AI security skills is accelerating as organizations expand their use of AI-powered systems and confront increasingly complex attack surfaces.

Training demand is centered on core AI pentesting techniques such as prompt injection, model manipulation, adversarial machine learning, and AI system misconfigurations, highlighting the breadth of risks associated with AI adoption. Enterprise training programs are driving much of this momentum. Organizational learners consistently demonstrate higher engagement and completion rates in AI-focused labs, compared to self-directed learning, with completion reaching 64% in November 2025. This indicates that organizations are proactively building AI security capabilities to address evolving threat landscapes.

AI security has moved from an emerging topic to a core cybersecurity capability.

Convergence Across Offensive and Defensive Domains

2

Training patterns highlight a clear shift toward more integrated, cross-functional skill development. Defensive practitioners are engaging in both defensive (68.36%) and offensive training (77.53%), while offensive practitioners, though still primarily focused on offensive skills (92.94%), are also incorporating defensive capabilities (44.15%)*.

These patterns suggest that organizations are moving beyond traditional red-versus-blue silos toward a more collaborative purple team model, where offensive and defensive capabilities are developed together. This shift aligns with broader industry frameworks such as Continuous Threat Exposure Management (CTEM), which emphasize ongoing validation of security posture through feedback loops between attack simulation and defensive improvement.

This evolution reflects a broader maturation of the cybersecurity landscape. What may appear as an offensive-heavy trend at the surface is, in practice, indicative of a converging skill model, in which professionals across roles are building complementary capabilities to operate more effectively within modern security programs.

		Interests	
		Defensive	Offensive
Current Roles	Defensive	68.36%	77.53%
	Offensive	44.15%	92.94%

Cybersecurity skill development is shifting toward a continuous, integrated model where offensive insights and defensive capabilities evolve together.

*Because users can select multiple training interests, percentages within each role do not sum to 100%.

Global Talent Development Is Expanding

3

Cybersecurity training participation reflects an increasingly global workforce. The top five countries - India, the United States, the United Kingdom, France, and Brazil - account for nearly **36%** of global cybersecurity upskilling activity.

India stands out as a particularly important growth market, where a large digital footprint, a rising role in global technology delivery, and continued policy and industry investment are driving demand for cybersecurity talent while also strengthening the country's capacity to develop it.

Together, these factors suggest that India is becoming more than a large talent pool. It is increasingly emerging as a strategic hub for cybersecurity capability development, particularly as organizations seek to expand access to distributed talent, meet security demands of the AI era, and address persistent workforce shortages.

India is emerging as a critical hub in the global cybersecurity talent ecosystem, offering both scale and growth potential.

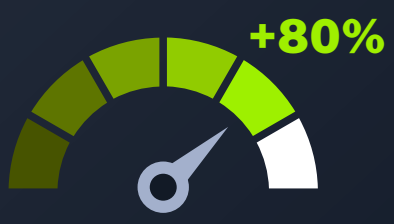
Enterprise Cybersecurity Benchmarks

4

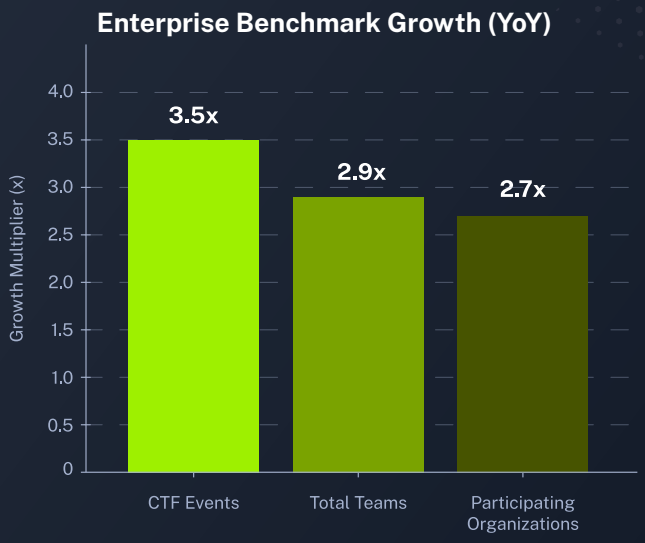
Analysis of enterprise Capture The Flag (CTF) data highlights the growing effectiveness of structured, organization-led cybersecurity training programs. Over the past three years, team interaction rates have consistently exceeded **80%**, indicating strong engagement and sustained participation.

At the same time, enterprise adoption is scaling rapidly. Year-over-year growth includes a **3.5x** increase in CTF events, **2.7x** growth in participating organizations, and **2.9x** growth in total teams, reflecting increased investment in hands-on, assessment-based cybersecurity training. This level of consistency and expansion suggests that structured programs are effective in driving follow-through and maintaining upskilling engagement over time.

These findings reinforce the role of hands-on CTF exercises in driving meaningful skill development, demonstrating that enterprise training programs can deliver both scale and sustained engagement over time.



Consistent participation for 3 consecutive years



Enterprise workforce development through CTF exercises delivers consistent engagement at scale, reinforcing its effectiveness in building cybersecurity capabilities.

Emerging Threat Signals

Training engagement data provides early indicators of emerging cybersecurity risks by revealing where practitioners are actively building skills. The data highlights a clear shift toward AI-driven attack vectors, with three dominant areas of focus.

Prompt Injection is the most prominent, accounting for **29%** of solved challenges within the analyzed period. These attacks exploit a fundamental limitation of AI systems: their inability to reliably distinguish between legitimate instructions and malicious inputs. As a result, attackers can manipulate prompts to override system behavior, bypass safeguards, or extract sensitive information. Their combination of low execution complexity and high defensive difficulty makes prompt injection particularly concerning, especially as it already affects widely deployed systems such as ChatGPT, Claude, and other LLM-based applications.

Machine Learning Model Exploitation represents **24%** of solved challenges. This category includes advanced techniques such as model backdooring, weight extraction, and supply chain compromise. While more technically complex, these attacks carry significant impact, particularly for organizations relying on third-party or pre-trained models.

Agentic AI Hijacking, at **12%**, targets AI agents and autonomous systems by manipulating function-calling logic or retrieval-augmented generation (RAG) workflows. As organizations increasingly adopt AI agents, this vector represents a rapidly evolving threat.

Alongside AI-focused techniques, there is a strong interest in offensive malware capabilities, with **28.89%** of US-based users and **29.93%** of India-based users expressing interest in **Malware and Command-and-Control (C2)** development. Given the scale of these talent pools, this may serve as an early indicator of emerging risk.

Taken together, these signals suggest that the next generation of cybersecurity threats may increasingly center on AI system manipulation and automated attack techniques, and advanced offensive capabilities. At the same time, they reflect a growing effort within the cybersecurity community to build the skills required to understand and defend against these emerging risks.

Training data signals a clear shift toward AI-driven attack vectors, highlighting where the next generation of cybersecurity risks is emerging.

Strategic Recommendations for CISOs and CSOs

The trends identified in this report reinforce several priorities for cybersecurity leadership as AI adoption, workforce pressures, and evolving attack techniques reshape security operations.

Prioritize AI Security Capabilities

As AI becomes embedded in enterprise infrastructure, organizations must ensure security teams can identify vulnerabilities in AI systems, evaluate model risks, and respond to emerging AI attack techniques. Security leaders should ensure teams are prepared not only to prevent these threats, but also to identify, investigate, and respond to them through realistic, scenario-based training and stronger operational readiness.

Enable Integrated Skills Development

Training patterns show increasing overlap between offensive and defensive domains, indicating that practitioners are developing complementary capabilities across both areas. CISOs should reflect this shift by enabling more integrated skill development across teams, combining offensive testing, detection, threat hunting, and response capabilities to support a more collaborative and adaptive security model.

Expand Global Talent Pipelines

With cybersecurity upskilling activity distributed across multiple major markets, organizations should look beyond traditional hiring geographies when building security teams. Expanding access to emerging and distributed talent pools can help address persistent workforce shortages while aligning recruitment strategy with where cyber capability is actively developing.

Treat Continuous Upskilling as Operational Readiness

As attack surfaces expand and threats evolve more rapidly, continuous, hands-on training should be treated as a core component of cybersecurity readiness. Structured enterprise programs, including assessment-based environments such as CTF exercises, help teams maintain the skills needed to detect, investigate, and respond effectively. They also provide CISOs with a scalable way to reinforce engagement, drive follow-through, and validate workforce capability over time.

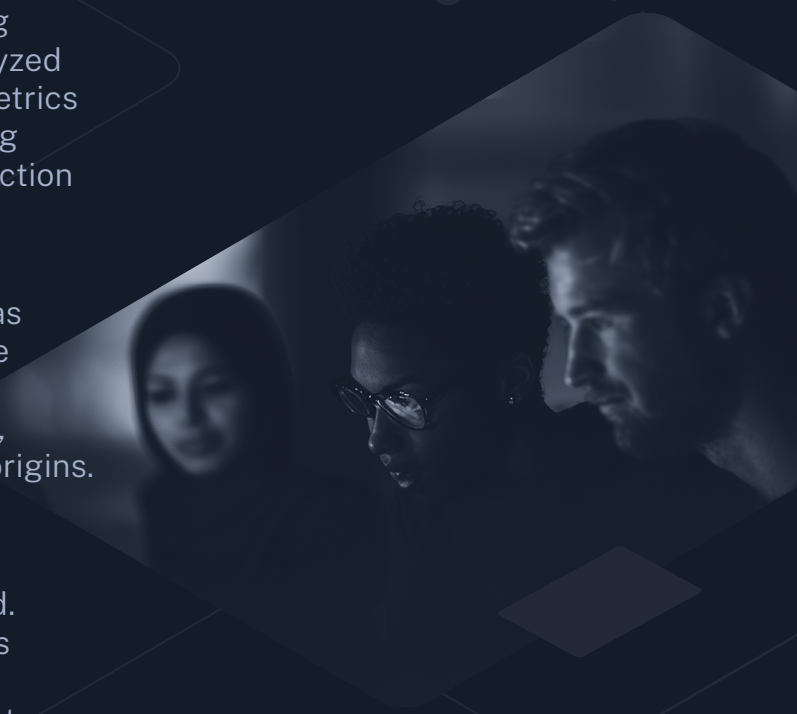
Report Methodology

The dataset comprises 702,226 participants enrolled on the HTB platform, based on anonymized and aggregated intent data. Also, a smaller sub-sample of the total, based on users who participated in AI/ML-focused HTB labs, was used for activity insights (1.5k users). Data collection occurred between mid-March 2025 and early December 2025, captured during the initial user onboarding process and subsequent platform interactions.

In addition, Hack The Box Capture The Flag (CTF) platform data (2023–2025) was analyzed to complement these insights, including metrics such as number of CTF events, participating organizations, total teams, and team interaction rates with training content.

To ensure global consistency and data interoperability, geographic distribution was mapped using the ISO 3166-1 standard. The platform utilizes the Official English Short Names (e.g., Korea, Republic of; Venezuela, Bolivarian Republic of) to categorize user origins.

The analysis focuses on identifying trends in user interests, experience levels, and career goals within the cybersecurity field. A combination of descriptive statistics was used to establish baseline demographics, while comparative analysis was employed to evaluate patterns across different regions and experience tiers. Because users are permitted to select multiple interests simultaneously, the percentages of interests within each “Current Role” category do not sum to 100%.



HACKTHEBOX

Hack The Box is the leading cyber readiness platform for the agentic AI-era, battle-testing and upskilling both humans and AI agents to enhance organizational cyber resilience.

Trusted by the Fortune 500, government agencies, and MSSPs, the platform delivers threat-informed learning paths consisting of real-world scenarios in gamified labs and live-fire simulations that build and validate offensive and defensive cyber capabilities

With a loyal community of more than 4 million members and 800+ enterprise customers, Hack The Box empowers teams and intelligent systems alike to strengthen cyber defenses and reduce breach risk effectively.

For more information,
visit hackthebox.com

Cyber Mastery:
Community Inspired. Enterprise Trusted.

FORRESTER
WAVE LEADER 2026
Cybersecurity Skills And Training Platforms