Hack The Box Report Reveals AI-Driven Shift Reshaping Cybersecurity Skills and Talent Strategy

New global data shows AI is changing cybersecurity roles, accelerating demand for advanced capabilities and forcing CISOs to rethink workforce planning

LONDON, UNITED KINGDOM, May 19, 2026 /EINPresswire.com/ -- Hack The Box, the global leader in AI cybersecurity readiness, today released its Cybersecurity Workforce Intelligence Report, revealing how AI is influencing cybersecurity skills, career paths and team structures.

> For CISOs, the challenge is ensuring their teams can operate effectively with AI, and without it when needed."
>
> *Haris Pylarinos, Founder and CEO of Hack The Box*

Based on anonymised data from more than 702,000 cybersecurity professionals across 251 countries and territories, the report highlights a growing shift in training interest toward advanced, AI-related skills and more integrated team models. As AI transforms both attack and defence, the findings show that technology alone is not enough. The effectiveness of the cybersecurity industry will increasingly depend on the depth, adaptability and readiness of the people behind it.

Organisations are accelerating investment in AI security capabilities, with AI penetration testing emerging as a top global training priority, underscoring how quickly AI security is moving from emerging focus to operational necessity.
"AI is creating a divide between teams that can operationalise it and those that can't, and that divide directly translates into risk," said Haris Pylarinos, Founder and CEO of Hack The Box. "For CISOs, the challenge is ensuring their teams can operate effectively with AI, and without it when needed."

AI is raising the bar for cybersecurity teams
Cybersecurity practitioners are increasingly prioritising emerging risks such as prompt injection, model exploitation and agentic AI attacks, signalling a shift in how organisations are preparing their teams. Hack The Box's training data reflects this trend, with Prompt Injection accounting for 29% of challenges solved, Machine Learning Model Exploitation (24%) and Agentic AI Hijacking

(12%) representing the top three dominant areas of focus and most solved challenges within the analysed period.

Haris Pylarinos, Founder & CEO of Hack The Box

At the same time, traditional role boundaries are becoming less rigid. Growing overlap between offensive and defensive training points to a more integrated model of cybersecurity capability development, where practitioners build complementary skills across domains rather than operating in silos. This shift supports a more collaborative, purple-team approach that prioritises adaptability across the full attack-defence lifecycle. The findings suggest that effective teams will increasingly be defined by adaptability, judgment, and cross-functional expertise, challenging CISOs not simply to adopt AI tools, but to ensure their teams have the skills to test, validate, and defend increasingly complex environments.

Structured hands-on training programs are accelerating this transition, with AI-focused training completion rates reaching 64%, reinforcing the role of organisation-led learning in building advanced cybersecurity capabilities.

Meanwhile, the cybersecurity workforce is becoming more globally distributed, with India emerging as a key talent hub alongside the United States, the United Kingdom, France and Brazil, which together account for nearly 36% of global cybersecurity upskilling captured in the report.

Implications for CISOs: Rethinking workforce development strategy
To remain effective in an AI-driven landscape, the report suggests security leaders must:
- Prioritise AI security skills to address emerging attack vectors and secure AI-enabled systems
- Invest in integrated training models that combine offensive and defensive capabilities
- Expand global talent pipelines to access emerging skill hubs and address workforce shortages
- Commit to continuous, hands-on upskilling to maintain operational readiness

Structured, hands-on training programs are proving critical to this effort, with enterprise-led initiatives driving higher engagement and faster adoption of emerging skills compared to self-directed learning.

The full report is available here.

About Hack The Box
Hack The Box is the leading cyber readiness platform for the agentic era, battle-testing and

upskilling both humans and AI agents for organisational 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 defences and reduce breach risk effectively. For more information, visit hackthebox.com.

Tracey Treanor
PRPR Limited
+ +44 1442 245030
email us here