



Cybersecurity Training Platforms Buyers Guide

All you need to measure and improve cybersecurity
performance in an ever-changing threat landscape



Table of contents

03.	Executive Summary	15.	Product roadmap 2025
04.	A unique market overview from 850+ customers	16.	User Management
05.	The problem with cyber workforce development	17.	Learning Experience
06.	Use onboarding as your primary risk mitigation strategy	18.	Curriculum Management
07.	Humans remain at the core of cybersecurity	19.	Reporting
08.	Tailored solutions win over one-size-fits-all	20.	Hierarchy of needs
09.	Manage risk with data-driven benchmarking	21.	Professional Services
10.	Proactive security is driving purchasing decisions	22.	Financial Services
11.	Enable purple team operations with realistic exercises	23.	Government
12.	What if we are all doing it wrong?	24.	Choose HTB as your next cyber performance platform
13.	A product designed for cyber performance	25.	Appendix #1
14.	Access an unlimited, threat-aligned content library		Our vendor evaluation toolkit
		26.	Appendix #2
			How to effectively build a business case

Executive Summary

Welcome to the second annual edition of our guide for cybersecurity training buyers, powered by Hack The Box.

Technical leaders are facing a perfect storm of constantly moving goalposts to maintain and ensure cyber resilience. With this guide, we want to empower buyers in any stage of the purchasing process to properly evaluate vendors-making sure that product features, content, and its applications are actually aligned to the core industry needs.

We have collected and summarized data from our customer base, now going beyond 850 organizations worldwide. Based on their best practices, platform activities, and future needs they highlighted, we identified five (5) main trends in the cybersecurity training space:

01. **Cyber workforce development can be costly, slow, and unreliable** if delivered with outdated methodologies, tools, or processes. Buyers are paying more attention

to product features, flexible pricing models, and evaluation from independent sources - such as analyst reports, referrals, webinars, or podcasts.

02. **Humans keep being the center of cybersecurity**, and most of the time the problem. Companies are prioritizing threats strictly related to human errors. In 2025, more than 50% of significant cyber incidents are caused by lack of skills.
03. **Cybersecurity training cannot be a one-size-fits all situation**, as security is fully tied to company and business goals. Vendors must be able to align training materials and schedule to frameworks or specific objectives relevant for the client to achieve business results – not vanity metrics on training engagement.
04. **Organizations are getting more proactive when it comes to security**, with reducing risk as the main reason to invest in new vendors. It is fundamental that your selected vendor provides features and training materials to enable these proactive security operations - focusing on

breaking silos between teams and fostering a purple minded approach by design.

05. **Leadership buy-in is the secret to success (and ROI)**. Buyers should evaluate vendors that provide value beyond security: operations, compliance, engineering, and more. This will help them in driving adoption and demonstrate return of investment.

The 2025 edition of the buyers' guide, we also want to provide practical tools to support your vendor evaluation and purchasing process.

As an appendix of this guide you will find a [business case template](#) and an [evaluation checklist](#) that you can use to decide what your next investment will look like.

Giacomo Bertollo,

Product Marketing @ Hack The Box

A unique market overview from 850+ customers

The best way to guide and support new buyers is by sharing feedback and datapoints from our current, global customer base.

This guide has been built by gathering concrete objectives, needs, and technical requirements that real stakeholders are looking for when selecting their next cybersecurity training solution.

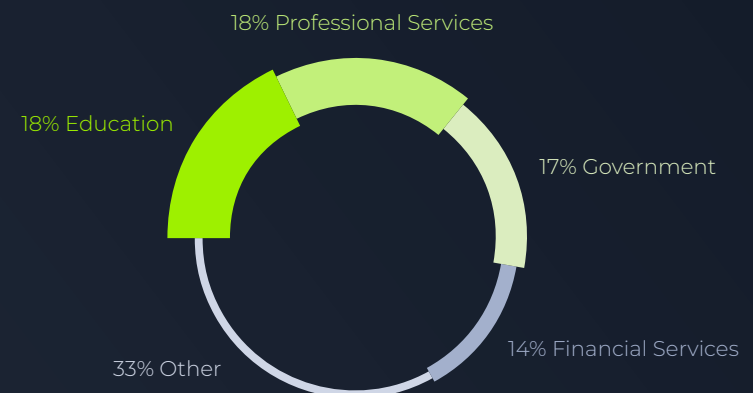
Our intention is to nurture an informed purchasing process by highlighting strategic implementations of our platform, share best practices, and provide an exclusive view into our committed product roadmap – which will clear potential doubts in terms of new features or content releases.

Cybersecurity investment is planned to increase across all organizational sizes (up to 38% for SMBs), while industry verticals become highly regulated – with specific security processes now part of legal mandates.

Our customers by size



Our customers by industry



The problem with cyber workforce development

Enterprises spend 40% of their security budget on its people- but are executives and technical leaders taking the best out of these investments? Building a high-performing cyber workforce can be a long process full of roadblocks and costs that buyers must evaluate carefully.

This visual shows how cyber workforce development is more than a security priority. A complex tech stack can quickly emerge, making it difficult for technical leaders to balance cost against efficiency. **Now more than ever, buyers should prioritize vendors that integrate with multiple other tools and support key practices on a single platform.**



Humans remain at the core of cybersecurity

Most breaches occur because we leave the door open. Based on data from our platforms, most teams are training on vectors and attacks highly focused on human error.

The 2024 Cyber Attack Readiness Report by HTB found that 60% of breaches are attributed to application vulnerabilities, social engineering, and misconfigured permissions.

Regardless of the solution or vendor, buyers must make sure that technology and humans intersect perfectly, aiming to build muscle memory into cyber teams that can be ready to respond timely.

For this reason, the earlier stages of your workforce development strategy are crucial to share cyber resilience: hiring and onboarding new high-performing cyber analysts becomes a fundamental priority.

What threats are organizations prioritizing in the current landscape?

Phishing

Malware

Ransomware

Password Attacks

Social Engineering

What CVEs offensive and defensive teams are learning and practicing?

ADSelfService
(CVE-2021-40539)

MOVEit
(CVE-2023-34362)

PrintNightmare
(CVE-2021-34527)

Looney Tunables
(CVE-2023-4911)

GitLab CE
(CVE-2023-2825)

Use onboarding as your primary risk mitigation strategy

Today, the mission of every cyber leader should be to turn new hires into performing security analysts—avoiding long and inefficient ramping periods.

Hack The Box enables security leaders to design onboarding programs that get cyber talent up to speed quickly, retain employees, and ultimately increase cyber resilience.

For new analysts: Efficient onboarding accelerates adaptation, builds confidence, and enhances skills, allowing new hires to contribute quickly and effectively while staying updated on security protocols.

For managers: Improve team cohesion, reduce induction time, and boost overall productivity, helping new hires integrate smoothly ensuring the achievement of crucial security goals.

For CISOs: Onboarding data and metrics are essential for the C-suite to follow, helping CISOs drive an overall cybersecurity culture shift. Build cyber resilience by equipping employees with the necessary tools and knowledge from day one.

Success stories

nviso 

Created a new HTB-based program, onboarding new hires 3x faster

easi

Prepared new hires covering 55 MITRE ATT&CK tactics and techniques





e-on

Involved 110+ team members within the first month

Tailored solutions win over one-size-fits-all

Cybersecurity departments in global enterprises usually have **more than 10 different subteams**. Each of those subteams comes with different priorities, performance metrics, and skills required to deliver the day-to-day tasks.

Security is a very fragmented field of work, which systematically fails with standardized solutions. Buyers should look for vendors who can provide custom-made plans for each of their teams (or, even better, team members) with granular data reporting and analytics.

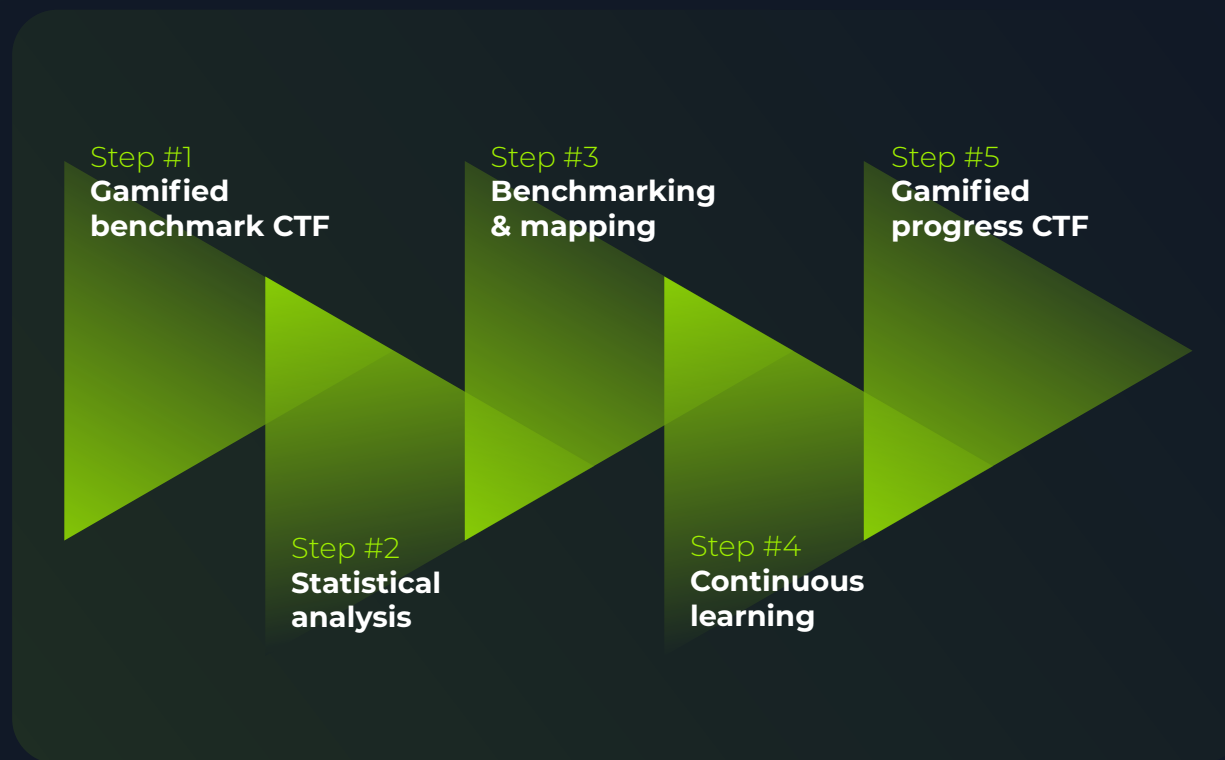
		
		
		

Manage risk with data-driven benchmarking

How often do cyber teams truly know how ready they are?

Our suggestion to buyers is to look further than just technology—but investigate deeper on methodology. Hack The Box enables cyber leaders to assess and benchmark teams using a **repeatable, effective, and easy to deploy** 5-step process—fully customizable to each team's requirements.

Cyber threats today are more adaptive than ever, and so should your approach to assessing skills.



In our annual research, **more than 70%** of cyber professionals and managers agree that CTF events help measure and assess skills while improving team engagement and retention.

Proactive security is driving purchasing decisions

“How do we get ahead of the game?”

This seems to be the biggest question keeping cyber leaders awake at night.

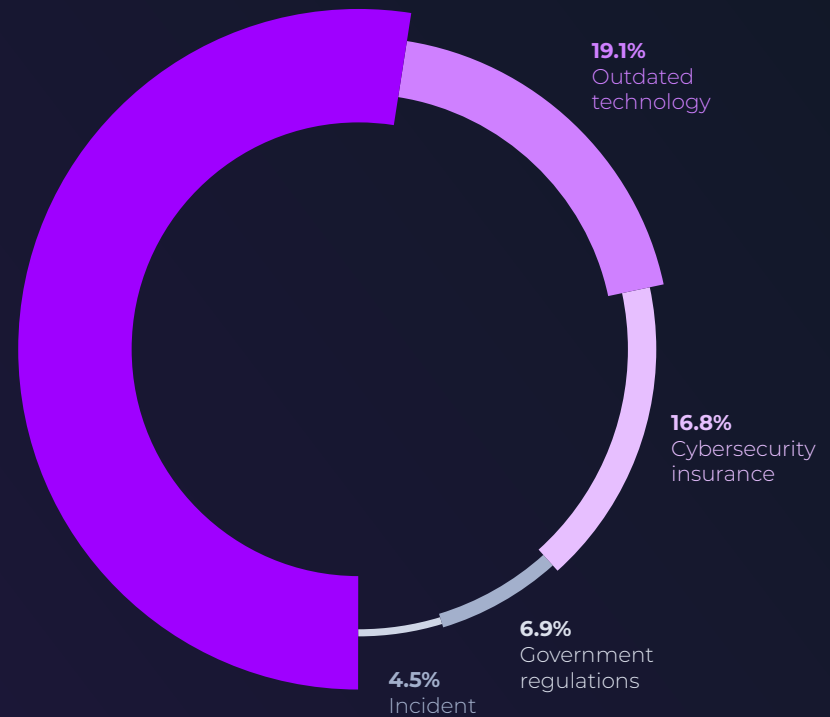
Proactivity seems to dominate the discussion, but the answer from many CISOs and executives isn't exactly encouraging: 40% believe their organizations are poorly prepared to face a potential incident, breach, or crisis.

Organizations today face an evolving and unpredictable threat landscape where attackers leverage advanced techniques, automation, and multi-vector strategies to exploit vulnerabilities, creating a dangerous mix of uncertainty and complexity.

The adoption of a continuous threat exposure management is critical to maintain a proactive and adaptive security posture.

What's the main priority motivating a new security investment?

52.7%
Proactively
reducing risk



Enable purple team operations with realistic exercises

Traditional cybersecurity practices often rely on reactive measures but without ongoing, integrated exercises that test and refine an organization's ability to detect, respond to, and mitigate threats, critical gaps remain unaddressed.

Buyers should source new, modern solutions that integrate and simulate the SIEM, SOAR, and CTI tools they are already using—turning their insights into action.

Hack The Box allows cyber teams to access a unified solution to:

- ✔ Build an effective CTEM framework.
- ✔ Create a tailored battle-zone and bridge gaps between offensive and defensive teams.
- ✔ Implement adversary emulation programs and predict techniques that could exploit your system.
- ✔ Practice new vulnerabilities on CVE-based labs and translate risk into potential financial loss.

Operationalize proactive security practices to quantify cyber risk and outmatch adversaries



What if we are all doing it wrong?

The cyber threat landscape is constantly changing, with new vulnerabilities discovered daily.

On top of that, we're seeing an increase in AI-related emerging threats that security teams need to grasp quickly, while boosting defenses against multiple and adaptive adversarial groups.

The right platform treats cyber professionals as athletes—continuously refining their **performance**, getting them fully ready when the moment comes.



A full bowl of certification acronym soup does not prepare practitioners and teams for the latest attacker techniques, rapidly exploited vulnerabilities, and hidden threats lurking in supply chains.

The Forrester Wave™: Cybersecurity Skills And Training Platforms, Q4 2023

 Cybersecurity training	 Cybersecurity performance
Relies on certifications and multiple-choice questions	Focuses on teaching provable skills for real-world scenarios
Is simply there to tick a box	Offers a human-first approach designed to create and maintain high-performing cyber professionals
One-size-fits-all approach with no flexibility	Is flexible and personalized to individual needs
The training doesn't fit your organization	Aligns with organizational objectives and workforce development
Once certified, the training and learning stops	Goes beyond upskilling and solves issues such as retention, burnout, and provides clear career paths
A one-off training session that's quickly forgotten	A place you return to day in and day out for continuous learning that supports career development

A product designed for cyber workforce readiness

The way we approach cyber readiness is at a turning point, and so is its workforce. Our product is designed to keep teams engaged and motivated, while getting them ready for the next threat that can target the business infrastructure.



Access an unlimited, threat-aligned content library

As a leader in cybersecurity professional development, we are committed to keeping pace with the evolving threat landscape on a weekly basis.

The full list of content planned for the year is extensive, but it can be summarized in 3 main knowledge domains:

AI pentesting and red teaming: A major partnership with Google got us to launch a AI Red Teamer job-role path. This curriculum will be further supported by hands-on labs, aiming to fully cover MITRE Atlas, OWASP LLM and Machine Learning frameworks.

Purple team exercises: Our goal is to foster collaborative security operations in multiple forms, with different content types, covering specifically critical vulnerabilities, processes, and tools from both adversarial and defensive perspectives.

Advanced defensive roles: Our team will gradually release courses and hands-on scenarios covering must-have skills to deliver these roles, starting from detection engineering. This will also be supported by new defensive labs, expanding on the already solid DFIR and SOC catalog.



“

Your provider must keep pace with the evolving threat and technology landscape with R&D and content experts ready and able to release new, relevant training courses and labs on a weekly or biweekly basis.

The Forrester Wave™: Cybersecurity Skills And Training Platforms, Q4 2023

Product roadmap 2025

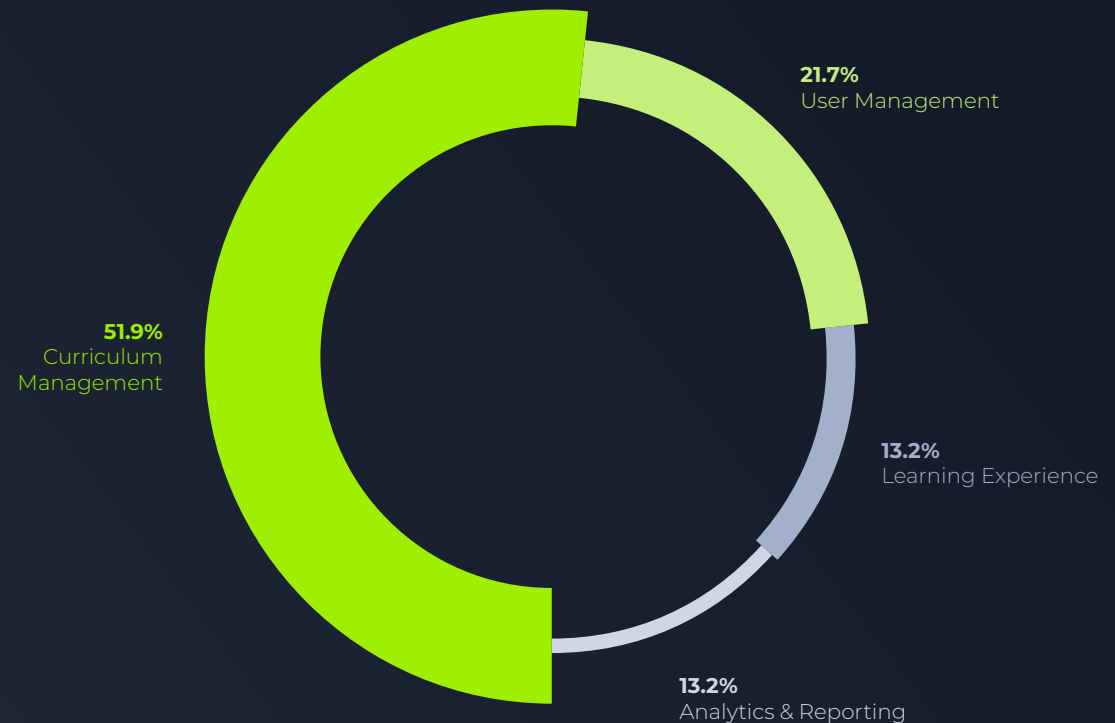
Enable and scale threat readiness

15

Our main goal is to create a long-term solution addressing strategic customer needs.

It is fundamental for buyers not only to know the current capabilities of the vendor, but also verify that the future direction of the product is aligned to mission critical company goals and requirements.

Looking ahead at 2025, We have translated this massive amount of information into 238 improvements, divided into 4 core pillars driving the product direction.



User Management

16



What is it?

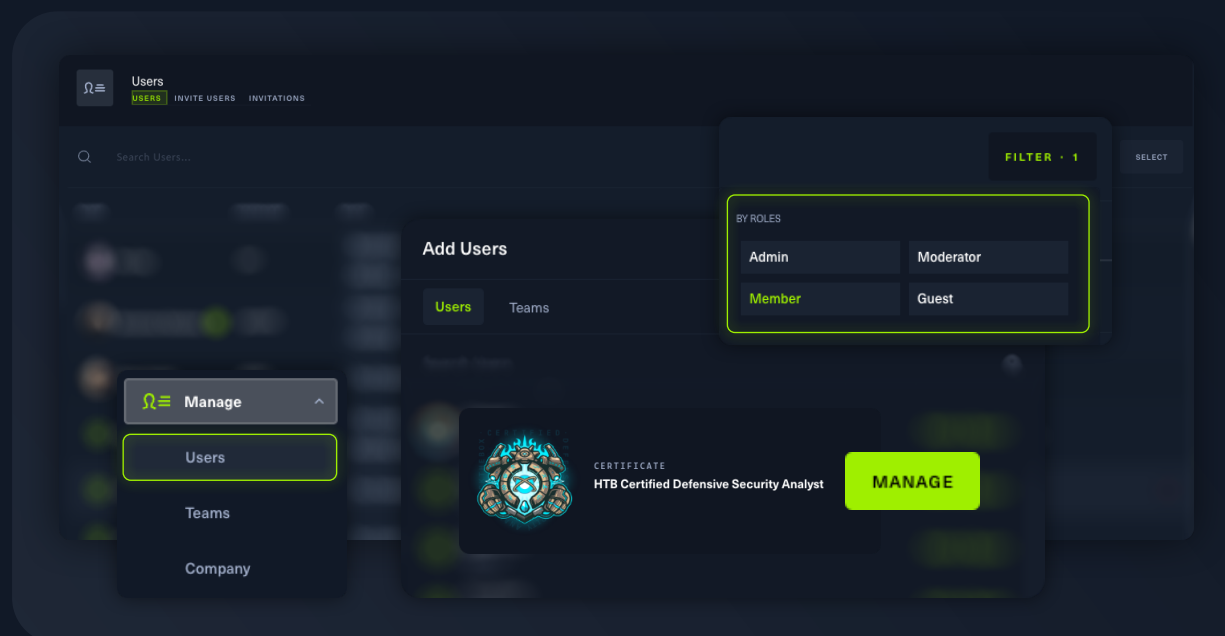
User Management includes all aspects around invitations, roles, permissions assignment, teams and team management, and seat assignment.

We are planning a complete review and revamp of the user management system to:

- Tailor user and license management to the needs of large enterprises.
- Seamlessly enable and scale teams with 500 or even 1,000+ members.
- Support effortless team management between cyber teams (offensive and defensive) or security-adjacent personnel such as developers, general IT staff, and more.
- Continue to expand the list of supported SSO providers.
- Source candidates and manage multiple open job positions on Talent Search.

The new user management interface will be a game-changer in terms of how companies access the platform—allowing

even the largest teams around the world to practice together in a couple of clicks, without unnecessary admin work.



Learning Experience

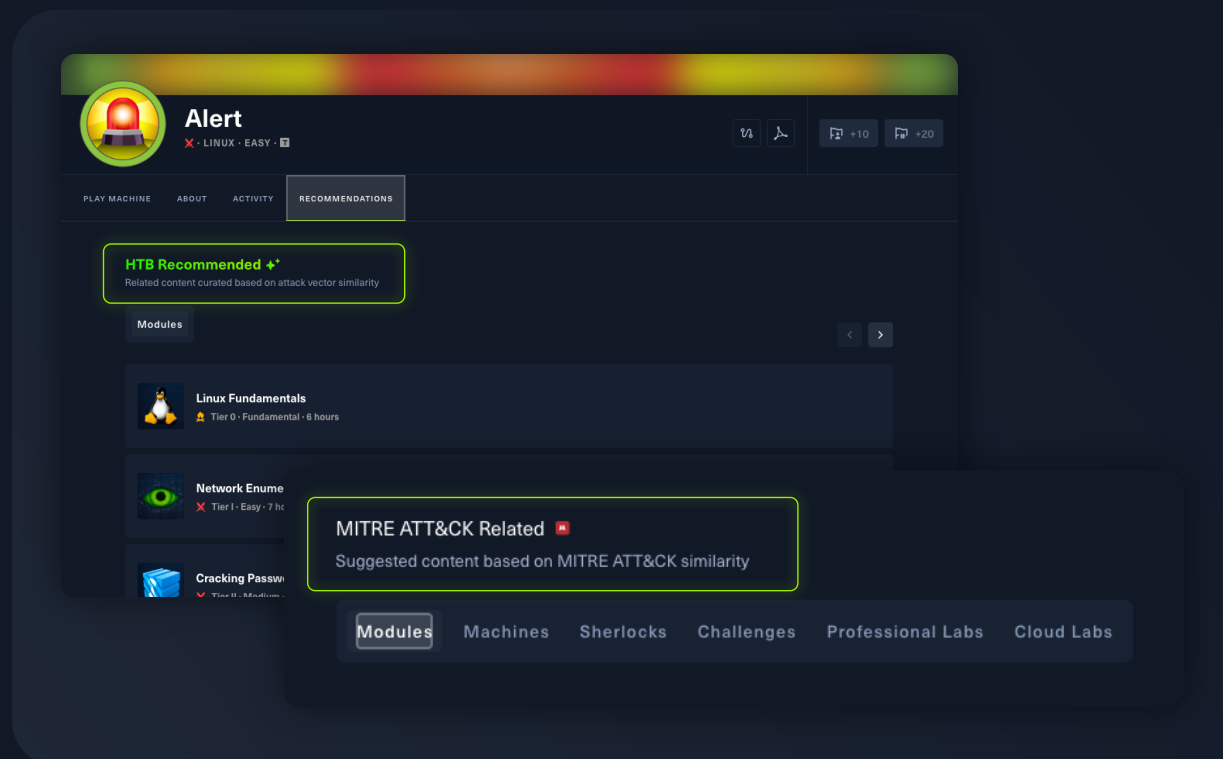


What is it?

By 'learning experience', we mean everything that makes consuming content easier. We are committed to continuously improving this crucial aspect of our product, making sure that cyber teams acquire critical skills better and faster than ever.

We're focusing on the end-user experience, automating the way cyber professionals discover and request courses or labs that match their interests with:

- AI-powered recommendations based on user activity, suggesting related content mapped to the most relevant industry frameworks—MITRE tactics and techniques, NIST job roles or KSATs, and more.
- Improved discoverability for all content types across the platform without limitations tied to user roles or permissions.
- Enhanced features for customizing skills development plans aligned with work roles, organizational needs, or relevant TTPs without relying on admins' approval.



Curriculum Management

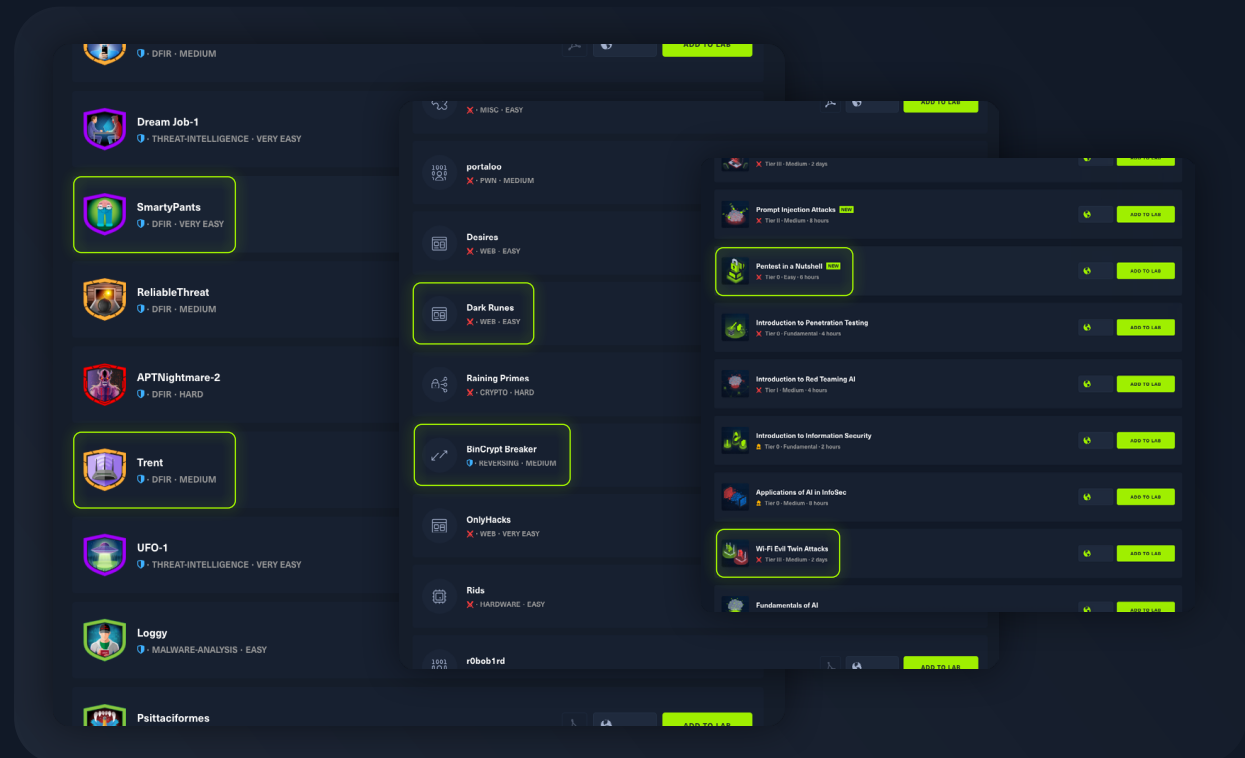


What is it?

This refers to the way teams manage training plans and assign tasks is going to be a major effort on our roadmap. Curriculum Management will be translated into short to medium-term improvements in parallel with a complete overhaul of our approach.

The results from the Q4 2023 Forrester Wave™ report confirmed superior capabilities in content assignment and learning paths flexibility. Our buyers can expect further enhancements that will allow them to:

- Easily navigate the entire Hack The Box content library without silos or limitations.
- Create more custom curricula mixing multiple content types (Modules, Machines, Challenges, Sherlocks) based on cybersecurity job roles or specific attacks and techniques.
- Quickly search, filter, and identify content of interest with a common (and automated) skill taxonomy across all content.



Reporting

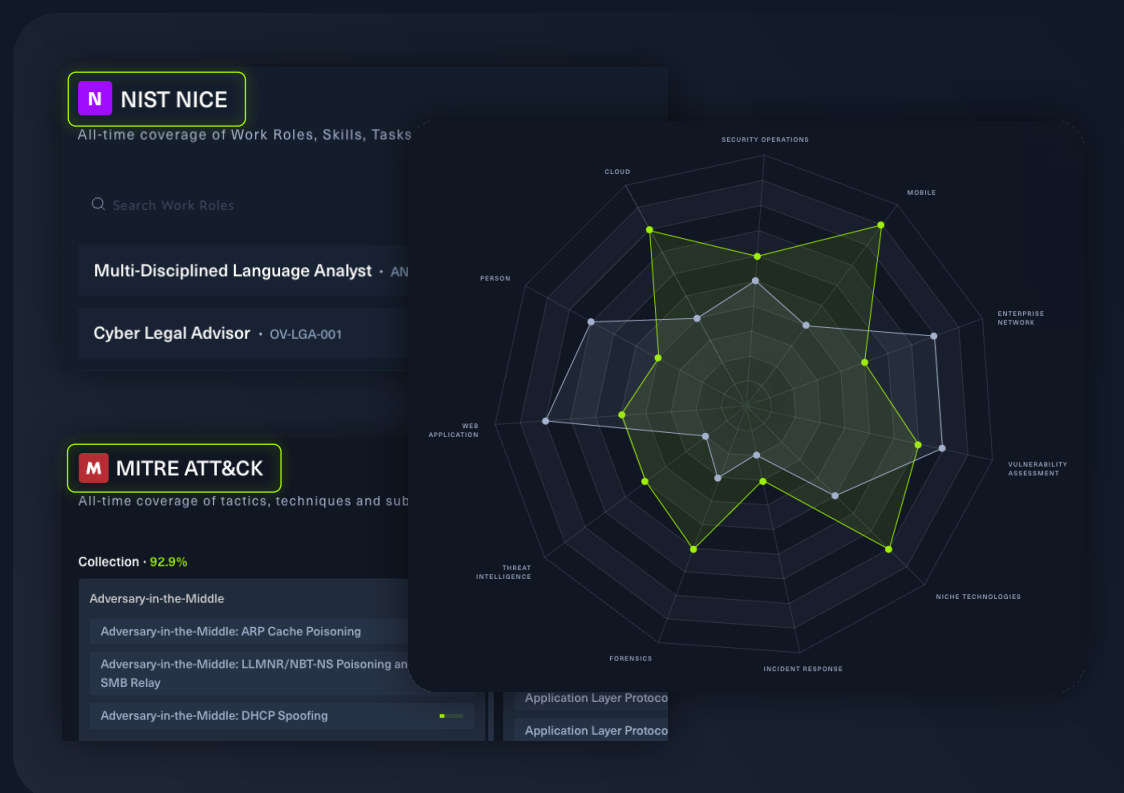


What is it?

Reporting includes all aspects of analytics and data-driven insights present on the platform within the reporting page, overview, leaderboard, and much more.

Our goal is to deliver easily consumable data that helps buyers assess platform activity, track skill development, and provide a clear snapshot of team performance. The reporting section will feature current, new, and refreshed metrics covering:

- Core metrics on team engagement with the platform and skill progression (at individual level, team, or organization—as granular as it gets).
- Impact on crucial business metrics to achieve cyber resilience based on tailored assessments and workforce development plans.
- Unified coverage of industry frameworks based on adversarial techniques and proficiency or crucial job roles or KSATs across the entire content catalog.
- Organization-level insights and sentiment on platform usage and team career development as cybersecurity professionals.



The CISO perspective

Hierarchy of needs

The CISO role keeps gaining importance on a board level, as 64% of times the board agenda always includes cybersecurity as a key topic.

At the same time, CISOs are tasked with managing the workforce in an uncertain landscape (AI to name just one) and a massive tech stack—43 different tools is only the median number.

Modern tech buyers should invest in new solutions that can combine more technical KPIs with concrete business outcomes around crucial processes.

What keeps CISOs awake at night?

01. AI/ML Security
02. Cloud Security
03. Data Security
04. Identity and Access Management (IAM)
05. Vulnerability Management



Industry deep dives

Professional Services

21

Consulting, MSPs, and Professional Services in general face the challenge of high turnovers, putting **knowledge retention** and **cyber readiness** at risk.



In consulting, we struggle to retain talent after they get certified. Once they have the credential, they leave for big tech roles. We need to shift toward skill-based development that actually keeps people engaged.

Jack McAloon,

Cyber Security Manager
@ Accenture

Drive productivity and decrease ramping time through cybersecurity excellence:



Role-specific cyber skills development



Fast-track talent integration



Accelerate efficiency and resilience



Ensure talent retention



Avoid compliance risks



Meet incident response deadlines



Financial Services

Despite advancements in cybersecurity tools and data, the Financial Services sector remains a prime target for sophisticated adversaries and nation-state attacks. Yet many teams struggle to operationalize the vast amounts of threat intelligence they collect.



Compliance frameworks can help reshape the way organizations think about security. In industries like finance, these mandates serve as a foundation for prioritizing cybersecurity strategies and building resilience against evolving threats.

Mo Mohajerani

Compliance Lead and
Security Operations Specialist
@ Paymenttools

Why? Because it takes more than information—it requires strategy, collaboration, and practical execution.

Cyber resilience is now a legal mandate. NIS2, DORA, or SEC ruling are raising the bar for incident response requirements—with crucial practices such as threat-led penetration testing and purple team operations as regulatory requirements. Adopting Hack The Box provides step-by-step guidance on how to implement crucial processes required by most directives and regulations:



Purple Teaming & Threat Intelligence



Incident Management & Reporting



Workforce & Risk Assessment



Secure Software Development



Government

For public sector buyers, the top priority when initiating a purchasing process is **acquiring new skills via upskilling, reskilling, and external hiring** (28%).



HTB has helped us tackle the unique challenges in the government sector by providing up-to-date content with new exploits and real-world scenarios that reflect the latest vulnerabilities, allowing our team practice with the newest exploits and gaining experience in spotting and responding to emerging cyber threats.

Nathan Taylor

Cybersecurity Manager
@ City of Newcastle

This comes as no surprise and directly related to the globalization of cybercrime, now more than ever tied to geopolitical tension and nation-sponsored threat groups.

Investments in cyber workforce development are directly linked to national security:



Election System Security



Cyber Espionage



Ransomware Attacks



Misinformation and Disinformation



Supply Chain Attacks



Choose HTB as your next cyber performance platform

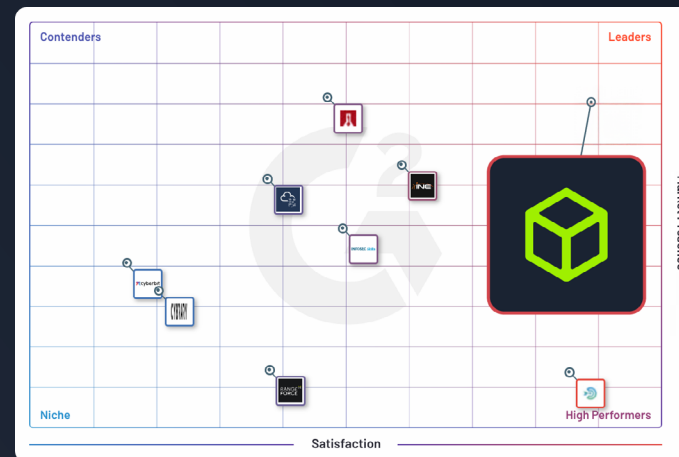
Today's cyber threats present a new challenge to organizations, and unskilled teams pose a real risk to the security of your business.

This is why cybersecurity performance programs and continuous improvement are no longer a nice-to-have: but a necessity.

Hack The Box is recognized by Forrester and G2 as a leader in cybersecurity professional development that keeps pace with the industry and creates high-performing teams.

Book a demo

HTB 14 day free trial



G2 Grid® Scoring for Cybersecurity Professional Development Software



Appendix #1

Your vendor evaluation toolkit

Evaluating vendors, especially software, can be challenging and messy—with multiple stakeholders randomly jumping in at any step of the procurement process.

This handy vendor evaluation toolkit is available for free and will guide you through a comprehensive checklist for your next vendor inspection.

[Download](#)

Appendix #2

How to build an effective business case

Download this template to build a bulletproof business case for your procurement team.

Leadership buy-in is the secret for a seamless vendor onboarding and adoption—that's why we're sharing our secret sauce to get any new investment approved.

[Download](#)

Cybersecurity Training Platforms Buyers' Guide

2025 Edition