HACKTHEBOX

Cyber Attack Readiness Report 2024

Lessons from testing 943 corporate teams and 4,944 security professionals with enterprise-grade security challenges

2024

Table of contents

Summary

Hack The Box (HTB) provides a human-first platform for creating and maintaining high performing cybersecurity individuals and organizations. The platform enables security leaders to sharpen skills, build specialized teams, and boost employee engagement with a suite of cyber workforce development solutions.

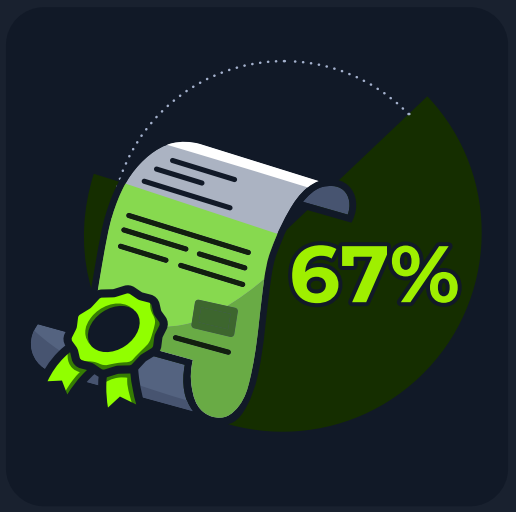
This report shares team performance data from the 2024 edition of HTB's global Capture The Flag (CTF) competition for corporate security teams—also known as HTB Business CTF: The Vault of Hope.

Business CTF is a free annual event hosted by HTB that offers cutting-edge content on emerging technologies and vulnerabilities. This year, 943 security teams and 4,944 professionals worldwide rigorously tested their technical and collaborative skills for a $50,000+ prize pool. In addition to performance data from the CTF event, this report combines insights from a separate user survey of 699 active cybersecurity professionals in the HTB community base.

Key insights

60% of breaches are attributed to **mismanaged permissions**, AppSec, & social engineering

20% of security teams **“rarely” train**



More than 67% of teams turn to **industry certifications & labs** to benchmark skills

Challenge categories explained

Business CTF features jeopardy-style hacking challenges based on the live threat landscape. These challenges help measure an organization's attack readiness by testing a team's ability to detect, respond, and manage real-world attacks.

Forensics
Investigate digital forensics artifacts seen in common cybersecurity attacks and identify the threat actor responsible.

Web
Find and exploit code flaws, misconfigurations, and insecure software in web-based applications or environments.

FullPwn
Develop and conduct a comprehensive attack strategy to gain access to a host and subsequently elevate privileges to the highest level.

Coding
Automate processes tailored to specific tasks and improve problem-solving and automation capabilities.

Pwn
Develop and manage exploits or attacks based on binary files that interact with computer memory and processors.

Cloud
Identify and address common cloud security flaws.

Blockchain
Identify and exploit bugs and misconfigurations to compromise the security of smart contracts.

ICS
Find and secure against vulnerabilities, weaknesses, or flaws that can compromise industrial devices and processes.

Reversing
Discover hidden features in systems that make software or hardware vulnerable to an attack, or uncovering how malware operates and bypasses detection.

Hardware
Identify and exploit vulnerabilities in embedded and IoT systems.

Misc
A mix of unique topics from multiple categories that may test a player's ability to solve a variety of different types of problems. These challenges test a team member's ability to think outside the box and come up with unique technical solutions.

Cryptography
Protect sensitive information from unauthorized access by identifying encryption flaws.

Web technology proves tricker to secure in 2024

Most teams excelled at miscellaneous and hardware challenges, showcasing robust generalist and IoT security skills. High average solve rates in forensics also indicate strong capabilities in post-incident analysis. However, some noticeable skills gaps surfaced. Continuing last year's trend, cloud and blockchain skills gaps continue to rage on with a new contender that teams struggled with this year: web.

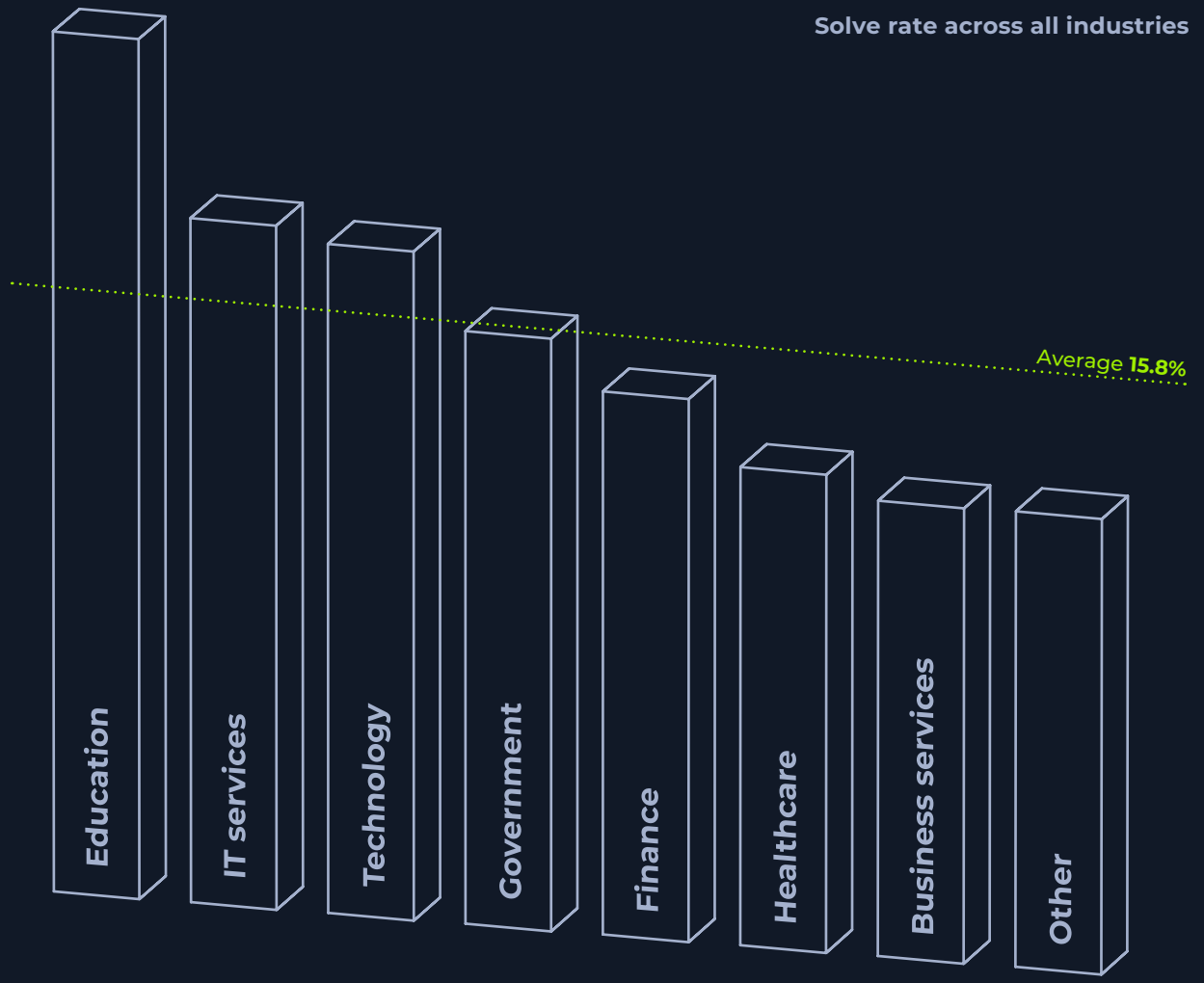
In 2023, web-related challenges saw above-average performance, but the 2024 data tells a different story. Web security ranked 9th out of the 12 challenge categories, with overall solve rates (the combined solve rate for this category from all players) falling below the average.

Best performing industries across all challenges

In 2024, teams in industries such as education, IT services, and technology exceeded the average solve rate of 15.8%, demonstrating a higher level of attack readiness.

IT services and technology sectors in particular showed strong performance in coding, forensics, and hardware security, reflecting their relevance to these industries. Meanwhile, finance, healthcare, and business services teams lagged behind, placing last with below-average solve rates. Business services teams in particular scored 25% lower than average.

Education **22.5%**
IT services **17.9%**
Technology **17.5%**
Government **15.5%**
Finance **14.2%**
Healthcare **12.5%**
Business services **11.9%**
Other **11.9%**

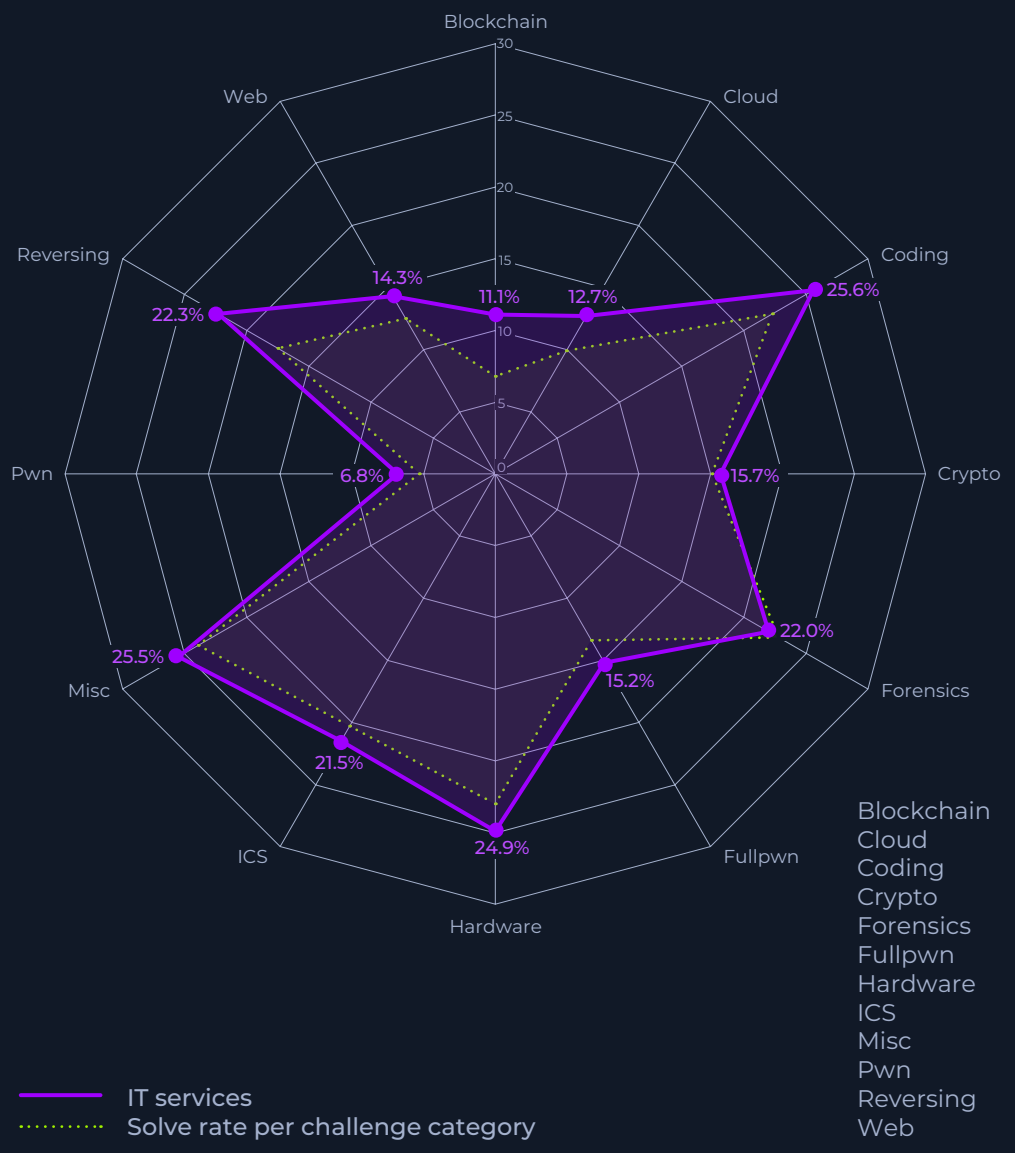


Industries in focus

IT services

Security teams in the IT services sector placed second out of all industries with above-average skills in coding, blockchain, hardware device protection, and web app security. These impressive strengths align with the industry's imperative to integrate security within development lifecycles and safeguard against sophisticated hardware & software attacks.

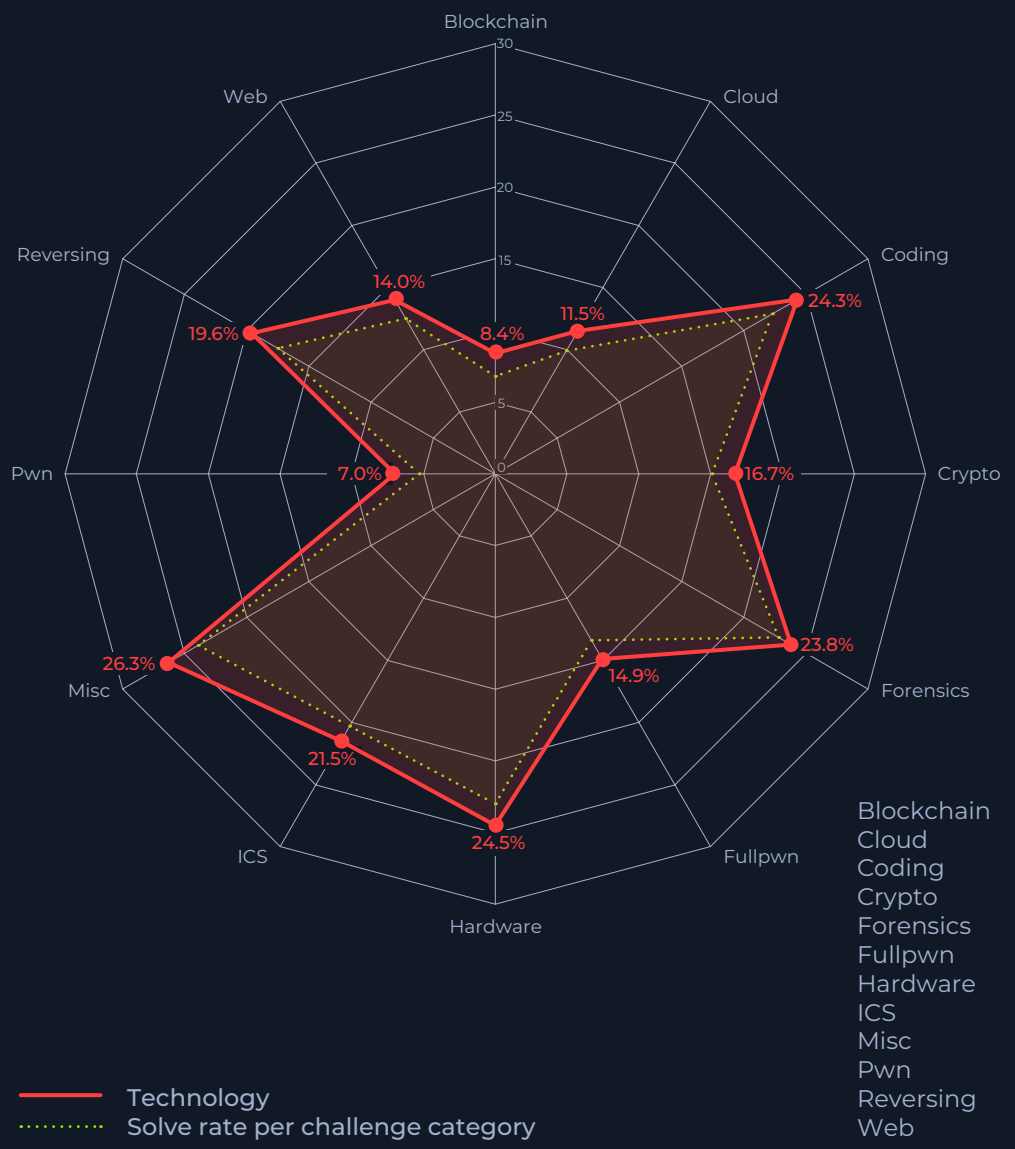
Despite emerging as overall top performers during this year's event, IT services teams score slightly below average at forensics challenges, highlighting the potential need for more attention to investigative and incident response training.



Blockchain	11.1%	6.8%
Cloud	12.7%	9.9%
Coding	25.6%	22.3%
Crypto	15.7%	15.1%
Forensics	22.0%	22.8%
Fullpwn	15.2%	13.4%
Hardware	24.9%	23.0%
ICS	21.5%	20.3%
Misc	25.5%	23.9%
Pwn	6.8%	5.3%
Reversing	22.3%	17.5%
Web	14.3%	12.5%

Industries in focus
Technology

Consistent with their competitive performance in the previous Business CTF events, teams in the technology sector placed third overall and performed above average across all challenge categories. They demonstrate prowess at solving security-related challenges involving cloud, coding, forensics, hardware, and web technology.

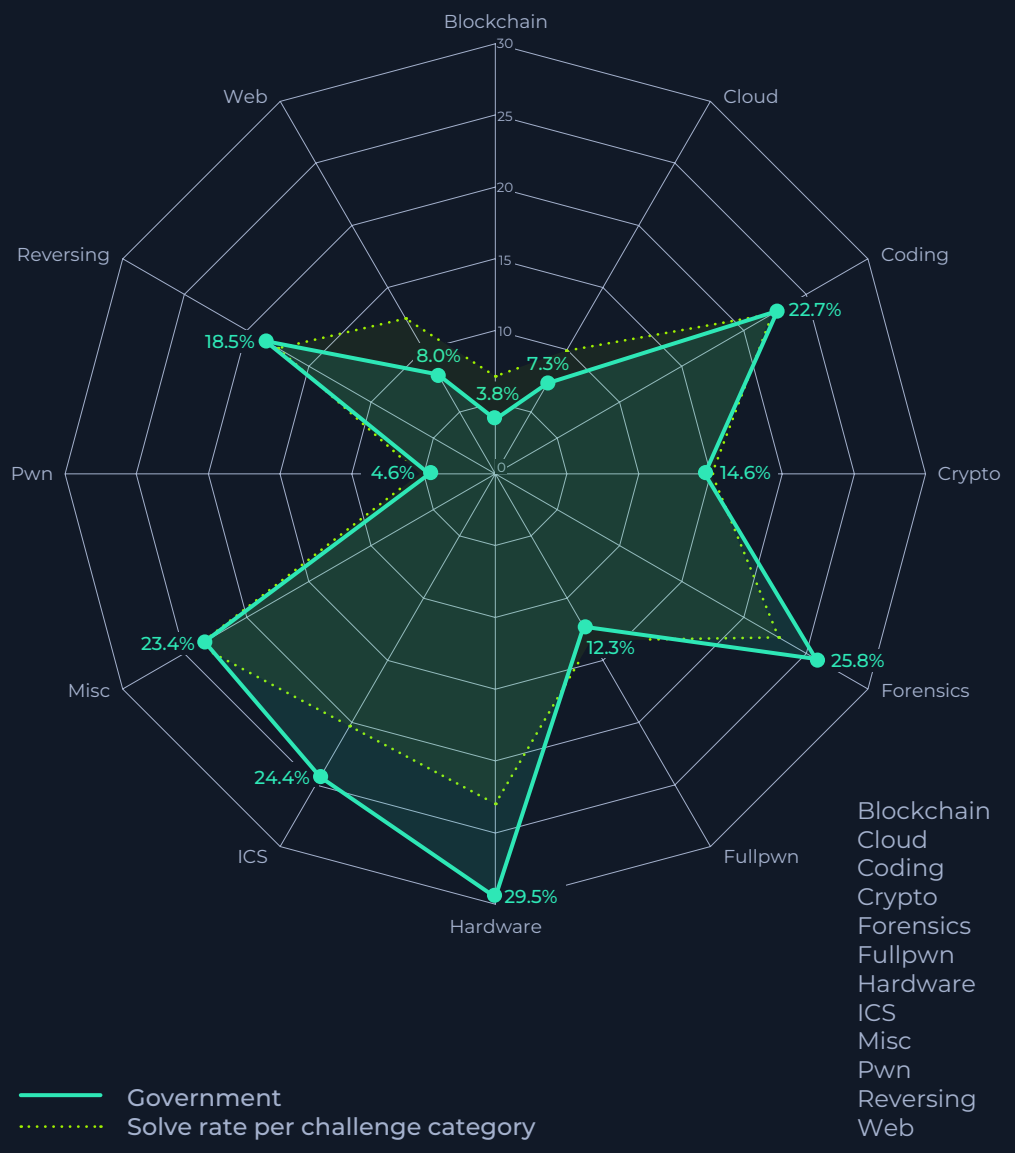


Blockchain	8.4%	6.8%
Cloud	11.5%	9.9%
Coding	24.3%	22.3%
Crypto	16.7%	15.1%
Forensics	23.8%	22.8%
Fullpwn	14.9%	13.4%
Hardware	24.5%	23.0%
ICS	21.5%	20.3%
Misc	26.3%	23.9%
Pwn	7.0%	5.3%
Reversing	19.6%	17.5%
Web	14.0%	12.5%

Industries in focus
Government

While government teams placed fourth with an overall solve rate that's just statistically shy of average, their team performance across specific technologies paints an interesting picture. Government teams are adept in forensics, ICS, and hardware security (where they scored 29.5% higher than average).

These strengths highlight the sector's robust investigative skills and ability to protect physical infrastructure and industrial systems from threats. However, teams also struggle with blockchain and web security, revealing a critical skills gap concerning IoT and web app security.

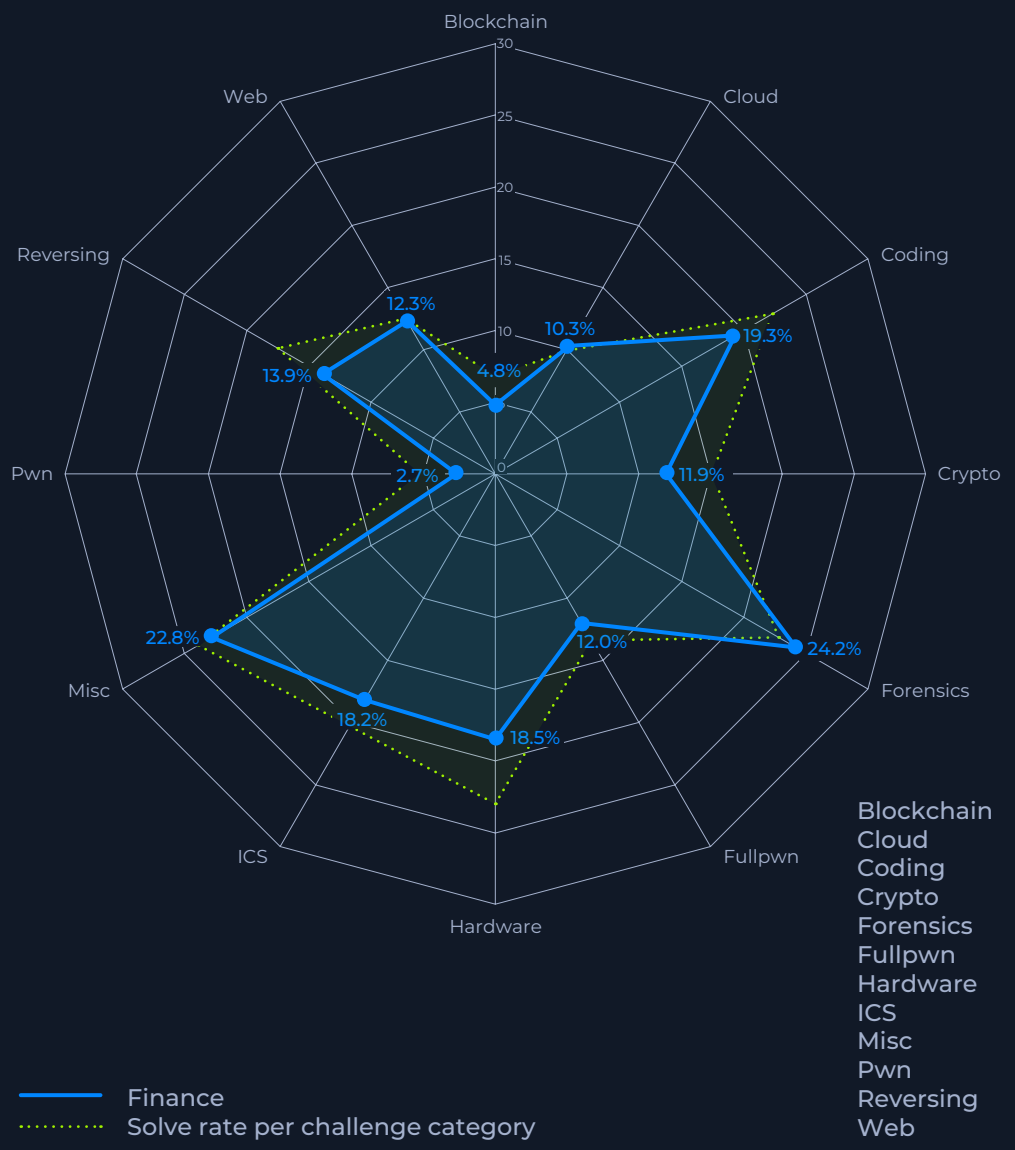


Blockchain	3.8%	6.8%
Cloud	7.3%	9.9%
Coding	22.7%	22.3%
Crypto	14.6%	15.1%
Forensics	25.8%	22.8%
Fullpwn	12.3%	13.4%
Hardware	29.5%	23.0%
ICS	24.4%	20.3%
Misc	23.4%	23.9%
Pwn	4.6%	5.3%
Reversing	18.5%	17.5%
Web	8.0%	12.5%

Industries in focus
Finance

Finance teams placed fifth in terms of overall performance. Their scores present a mixed picture, revealing both strengths and interesting areas of improvement. Strong forensic capabilities (finance teams placed in the top three for the forensics category) reflect the sector's proficiency in investigating breaches and detection.

However, a 22% lower than average performance on solving hardware-related challenges reflects a cause for concern with physical devices, such as payment processors which are essential for financial transactions and an alluring target for threat actors.



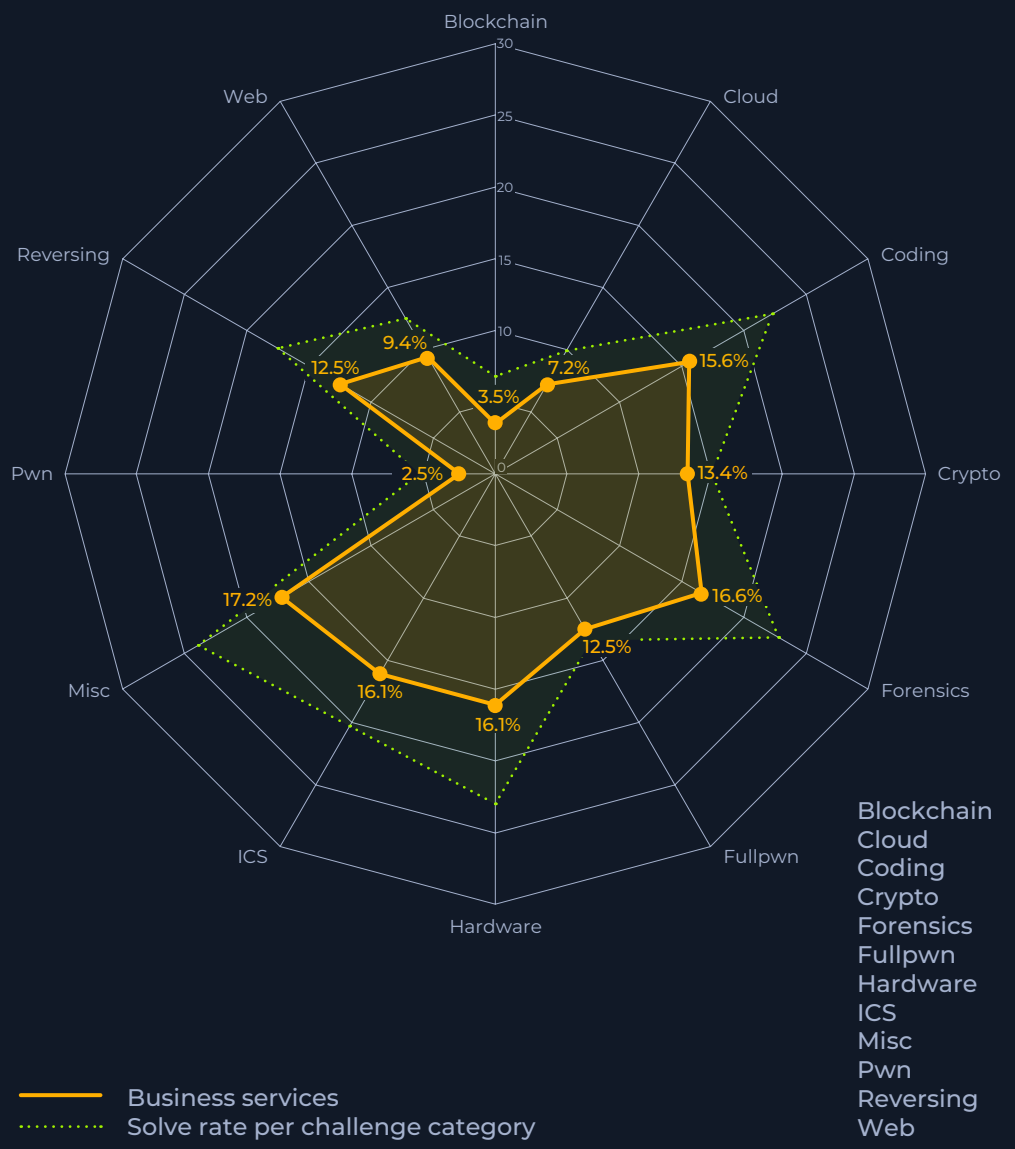
Blockchain	4.8%	6.8%
Cloud	10.3%	9.9%
Coding	19.3%	22.3%
Crypto	11.9%	15.1%
Forensics	24.2%	22.8%
Fullpwn	12.0%	13.4%
Hardware	18.5%	23.0%
ICS	18.2%	20.3%
Misc	22.8%	23.9%
Pwn	2.7%	5.3%
Reversing	13.9%	17.5%
Web	12.3%	12.5%

Industries in focus

Business services

Teams in the business services sector placed last among all the industries categorized, performing below average in all challenges. Their biggest skills gaps were found in coding, forensics, and hardware challenges (in which they performed 30% lower than average).

When considering the potential for security breaches that originate from insecure coding practices, weak breach detection, and poor physical hardware security, these results are a rallying cry for teams in the sector to align their capabilities with the modern threat environment—as safeguarding assets is a must for maintaining trust with clients and partners.



Blockchain	3.5%	|	6.8%
Cloud	7.2%	|	9.9%
Coding	15.6%	|	22.3%
Crypto	13.4%	|	15.1%
Forensics	16.6%	|	22.8%
Fullpwn	12.5%	|	13.4%
Hardware	16.1%	|	23.0%
ICS	16.1%	|	20.3%
Misc	17.2%	|	23.9%
Pwn	2.5%	|	5.3%
Reversing	12.5%	|	17.5%
Web	9.4%	|	12.5%

Survey:

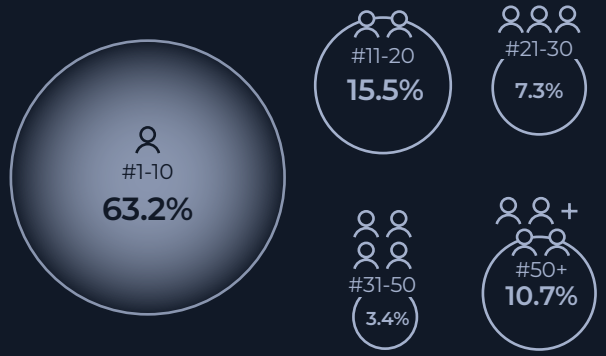
How teams train for the threat landscape

This section combines insights from a separate user survey of 699 active cybersecurity professionals in the HTB user base. These questions range from the common cause of a breach teams have faced, how they train, and their approach to benchmarking skills.

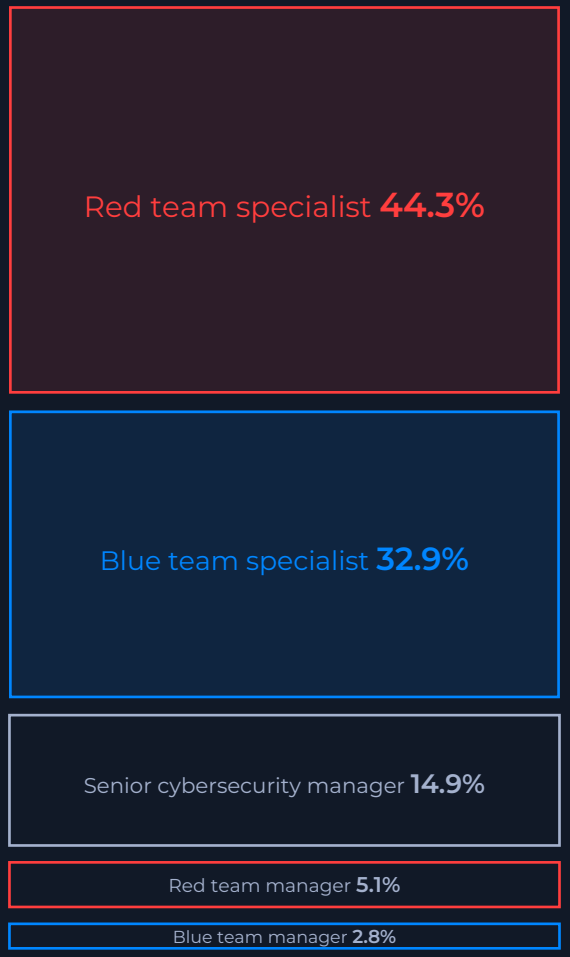
Position on team

Manager or team lead	Employee on a security team
42.1%	57.9%

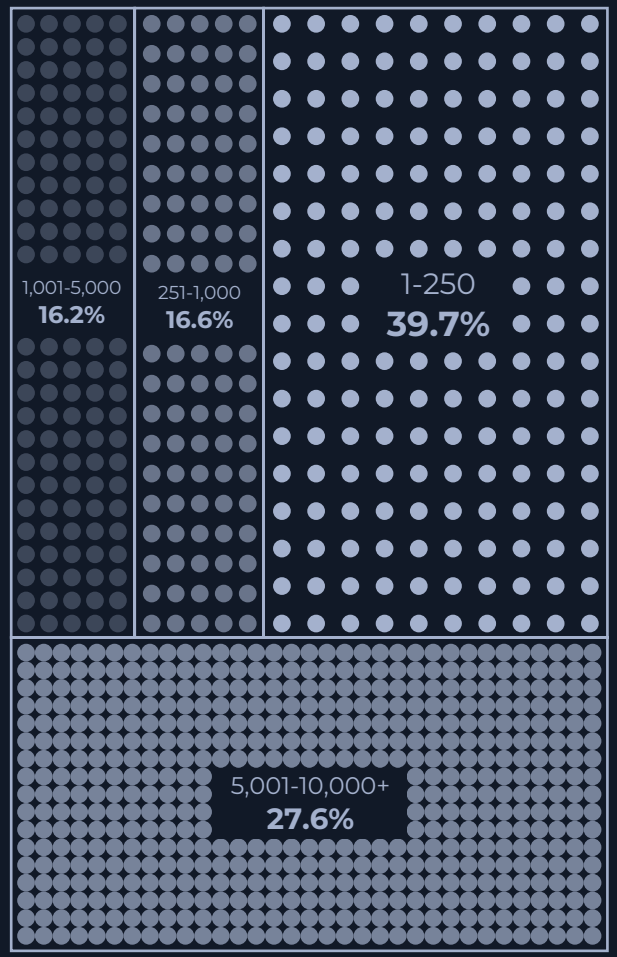
Security team size (by # of employees)



Type of team



Company headcount



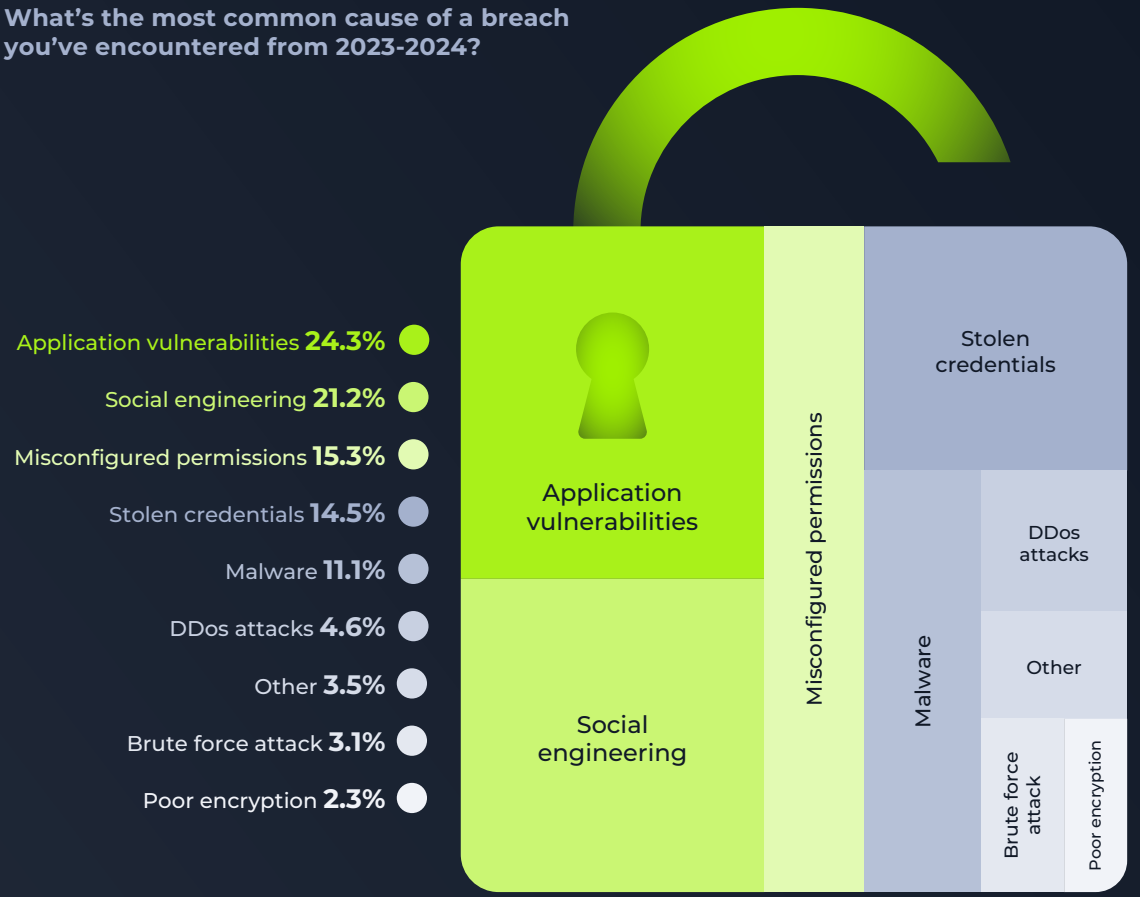
60% of breaches
are attributed to misconfigured permissions, AppSec, & social engineering

60% of breaches professionals faced were caused by a combination of application vulnerabilities, social engineering, and misconfigured permissions, emphasizing the need for secure development practices and comprehensive employee training that focuses on securing the “human” element.

Stolen credentials and misconfigured permissions further stress the importance of strong identity management and regular configuration reviews.

The key takeaway is the vast majority of breaches aren’t triggered by APTs chaining multiple zero-day exploits to compromise an environment. Instead, insecure apps, human error, and misconfigurations continue to “open the door” for bad actors to breach.

What’s the most common cause of a breach you’ve encountered from 2023-2024?



20% of security teams “rarely” train

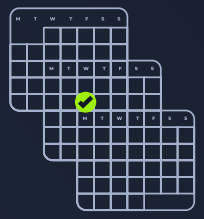
Cybersecurity training frequency is a critical indicator of an organization’s resilience against the threat landscape. While 41.9% of teams train weekly, a concerning 27.9% train quarterly or not at all, leaving dangerous gaps in their defense capabilities.

The 7.9% of organizations not training at all are playing a dangerous game with a critical lack of training on new technology.

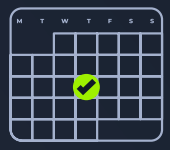
There’s a chance the intensity of new regulatory pressures is motivating senior leaders to support frequent upskilling, as the EU’s NIS2 Directive and the U.S.’s SEC cybersecurity rules both mandate regular security training and faster incident reporting times.

How often does your team engage in training to address emerging threats and vulnerabilities to your attack surface?

We don’t train on new technologies (never)
7.9%



Once per quarter (rarely)
20.0%



Once per month (occasionally)
30.2%

Once per week (frequently)
41.9%

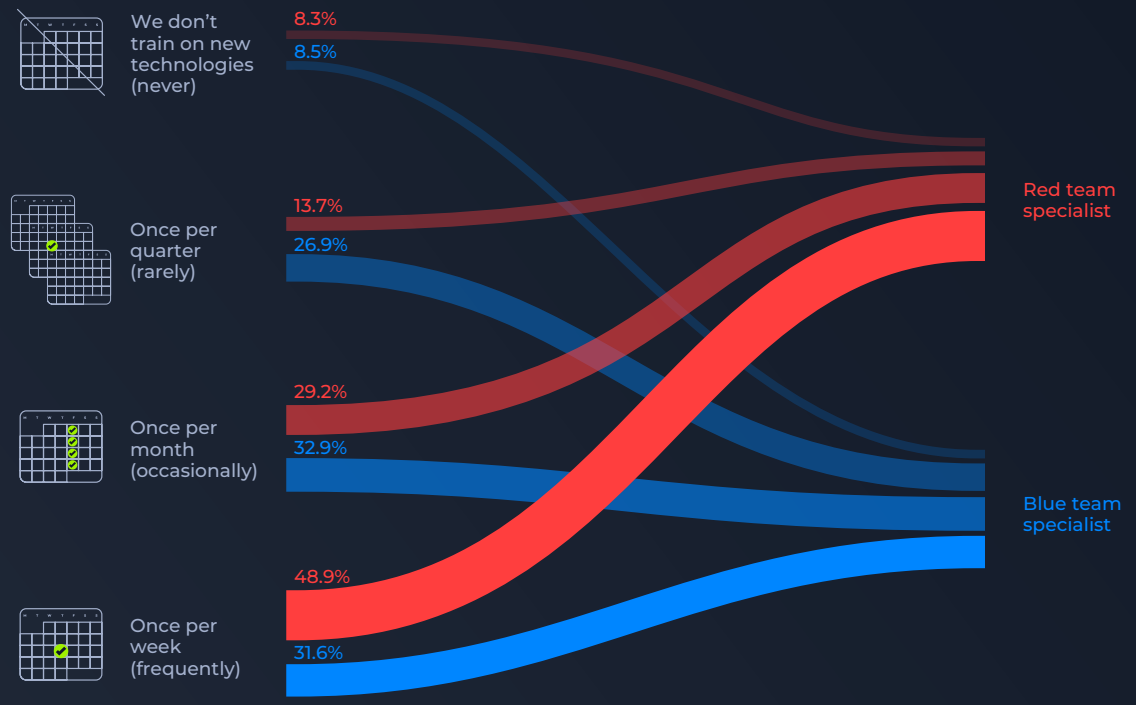
Blue teams get less time to train than red teams

There's a significant disparity in training frequency between red and blue teams. Red team specialists engage in more frequent training, with nearly half completing weekly training compared to less than one-third of blue team specialists training on a weekly basis.

This imbalance could lead to potential vulnerabilities, as defensive teams may not be as up-to-date with emerging threats and attack techniques.

The lower training frequency for blue team specialists is particularly concerning, as they are often the first line of defense against cyber attacks. This disparity suggests a need for organizations to reevaluate their training priorities and ensure that all cybersecurity roles, especially those focused on defense, receive regular and comprehensive training to address emerging threats and vulnerabilities.

How often does your team engage in training to address emerging threats and vulnerabilities to your attack surface?

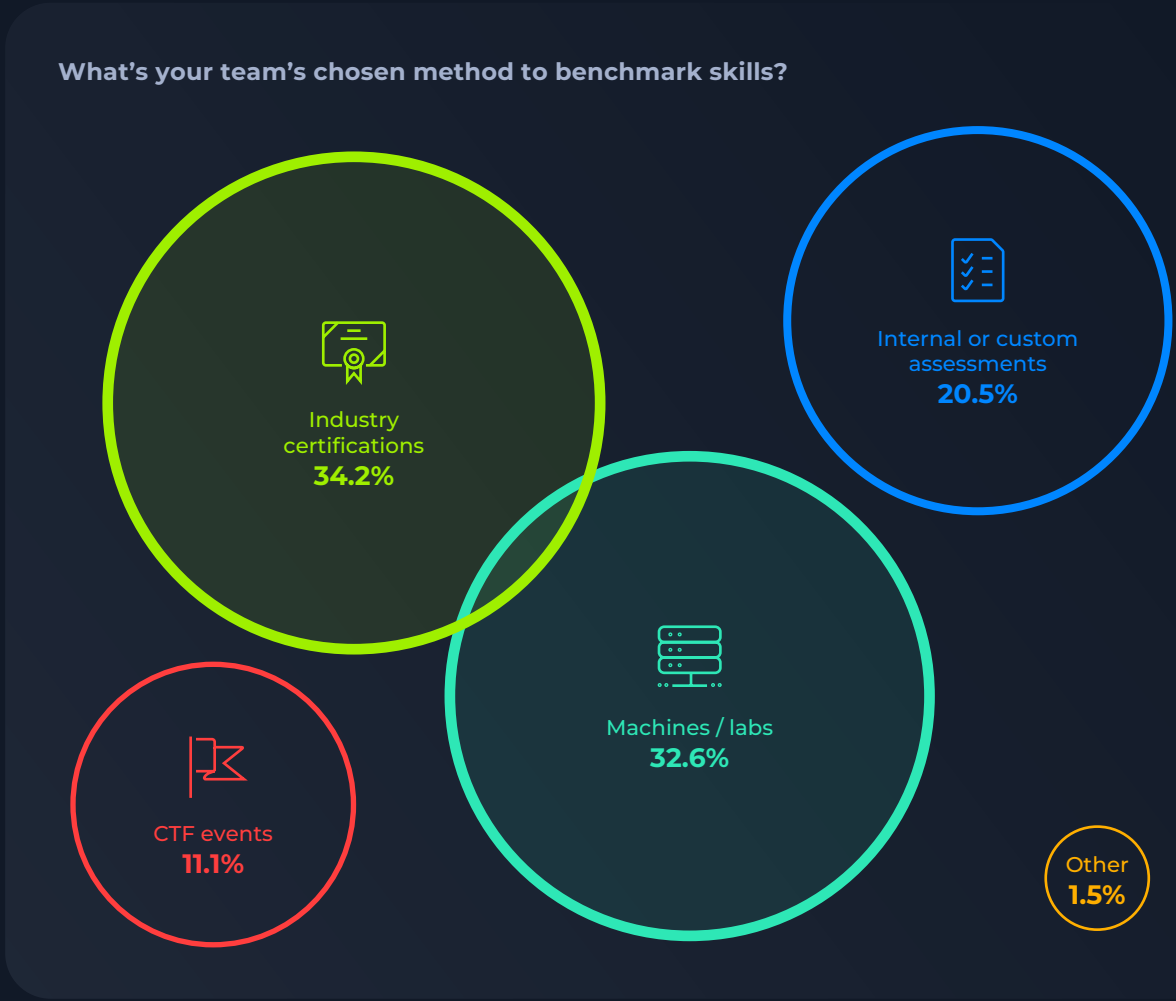


More than

67% of teams turn to industry certifications & labs to benchmark skills

The combination of industry certifications (34.2%) and machines or labs (32.6%) being used by more than 60% of teams for skill benchmarking is significant. It indicates a well-rounded strategy that values theoretical knowledge and practical skills. Industry certifications typically cover standardized knowledge, while machines and labs provide hands-on experience.

The variety of benchmarking methods suggests that organizations recognize the complex nature of cybersecurity skills and employ multiple techniques to evaluate and develop their teams' capabilities.



Accelerate cyber performance with Hack The Box

Loved by a global cybersecurity community of more than three million members, HTB is helping security leaders across the world equip their teams with the skills and expertise needed to proactively secure and protect their organizations.

HTB specializes in defensive and offensive cybersecurity upskilling programs featuring content that's guided, practical, and aligned with the NIST NICE and MITRE ATT&CK frameworks, as well as unrivaled hands-on labs designed to help organizations close skills gaps, hire top talent, and protect infrastructure.

Measure, assess, and proactively close your organization's cybersecurity skill gaps with a single platform focused on developing your cyber workforce.

→ Book a demo

→ HTB 14 day free trial

Cyber Attack Readiness Report

HACKTHEBOX

2024