



CYBER ATTACK READINESS

Insights on the threat landscape & capabilities of corporate teams in key industries, including tech, finance & government

A REPORT BY  HACKTHEBOX

03 Foreword**06** Methodology

- 2022 Business CTF participants
- Regional breakdown
- Challenge categories

11 Business CTF industry insights

- Best performing industries across all challenge categories
- Average solves per attack category
- Industry-specific strengths and weaknesses
- Average challenge performance per industry

18 3 Reasons why your team should join Business CTF 2023**22** About Hack The Box

FOREWORD

The threat landscape continues to evolve at a rapid pace. Your team's skills, culture, and approach to cyber readiness must adapt and evolve in tandem.

At the grassroots level, keeping pace starts with a culture of efficient training and development that's connected to the live threat landscape. This teaches teams how to emulate, and as a result, defend against, the predatory techniques, tactics, and procedures of modern malicious actors in the wild.

Unfortunately, many cybersecurity talent and skills development initiatives are often overly theoretical and unrealistic. They may help satisfy compliance requirements, but fail to elicit employee engagement, forge technical hands-on expertise, and cultivate a capable, attack-ready culture.

The consequential skills and talent shortage created leaves cybersecurity teams constantly struggling to keep up – as opposed to getting ahead of – emerging threats and vulnerabilities.



DIMITRIOS BOUGIOUKAS

Director, IT Security Training Services @ **Hack The Box**



BETWEEN 2021-2022:

DarkSide's ransomware attack on **Colonial Pipeline** shut down fuel supplies for much of the U.S. East Coast.

The Conti group crippled **Ireland's health service** causing hospitals to shut down.

REvil ransomware halted production at the world's largest meat processor, **JBS**.

\$18 million of Bitcoin and \$15 million of Ethereum was stolen from **Crypto.com**.

Forward-thinking cybersecurity leaders of today must:

- **Understand** their team's strengths and weaknesses
- Routinely **test** their practical skills against realistic, engaging challenges that foster out-of-the-box thinking
- **Invest** in continuous training and initiatives to engage, retain, and develop their organization's biggest asset – people

Hack The Box's annual **Business CTF**, which is the largest free global CTF event for corporate cybersecurity teams, helps organizations do all of the above in an engaging way that increases collaboration and employee engagement.

In this report, you'll find unique industry-specific insights from our 2022 Business CTF competition alongside data on the current threat landscape.

1010111011011011010
1010100001101010100
110101010110100100
1011011110101001001
101101010101

Close to **40%** of data breaches in 2021 preyed on small businesses and only 14% were ready for the attacks. ^[1]

The average cost of a data breach was **\$4.24 M** in 2021, the highest average on record. ^[2]

The worldwide economic impact of cyber crimes is **\$1.141 M** per minute. ^[3]

By 2025, cybercrime is estimated to cost **\$10.5 trillion** globally, increasing by 15% year over year. ^[4]

Pre-register your team
for next year's Business CTF



METHODOLOGY

Hack The Box provides a unified suite of cyber workforce training and development solutions that help global organizations sharpen skills, build specialized teams, boost employee engagement, and confidently recruit top cybersecurity talent.

The data below is based on the 2022 “Dirty Money” edition of Hack The Box’s annual Business CTF competition.

657

TEAMS

2,979

PLAYERS

84

COUNTRIES

1,856

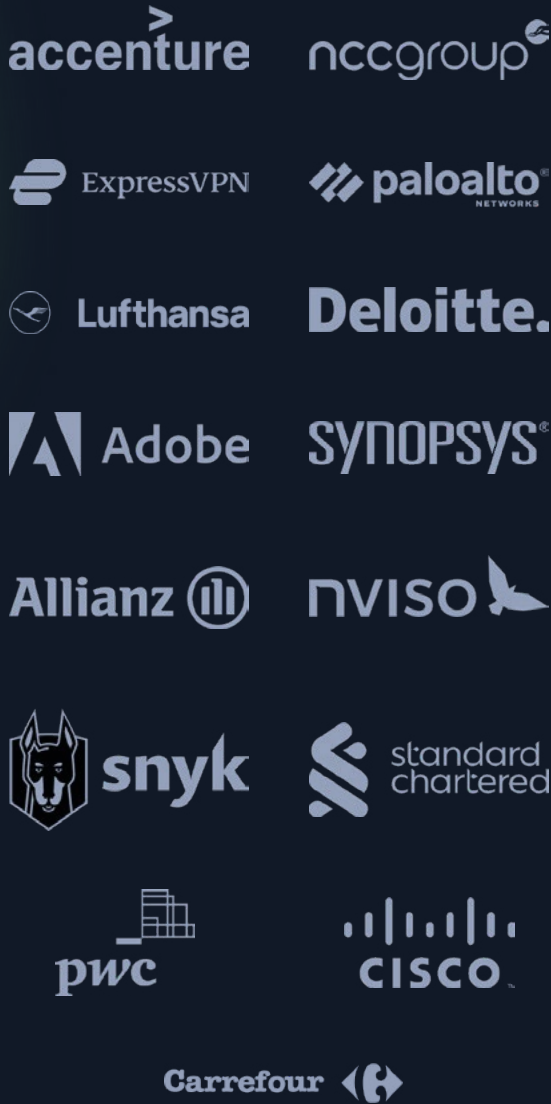
FLAGS SUBMITTED



Featuring jeopardy-style hacking challenges based on real-world vulnerabilities and emerging threats, the CTF tested the practical and collaborative skills of 657 corporate teams and 2,979 players from the world’s largest commercial brands (including Fortune 500 companies) and government entities.

The annual Business CTF by HTB features the latest technologies and vulnerabilities that every security-conscious company should be familiar with. This allows players to enjoy exclusive content and hands-on activities that simulate real-world attacks.

Due to the team-building nature and competitive environment of CTF events, a wide variety of cybersecurity professionals, ranging from CISOs to junior-level employees, collaboratively interact in an environment that cultivates practical skills in the workplace.



During this year's CTF, corporate IT and cybersecurity teams from around the world had their skills stringently tested by pursuing fictional malicious actors engaging in crypto laundering, wire fraud, phishing campaigns, malware, ransomware strains, and more.

2022 Business CTF participants

68%

of business leaders feel their cybersecurity risks are increasing. ^[5]



“

We used the HTB Business CTF to get our interns into the hacking world at the same time as the new hires and the more experienced members sharpened their skills. It was fun as well as rewarding to spend that weekend working together and sharing knowledge. I will definitely join for similar events in the future.

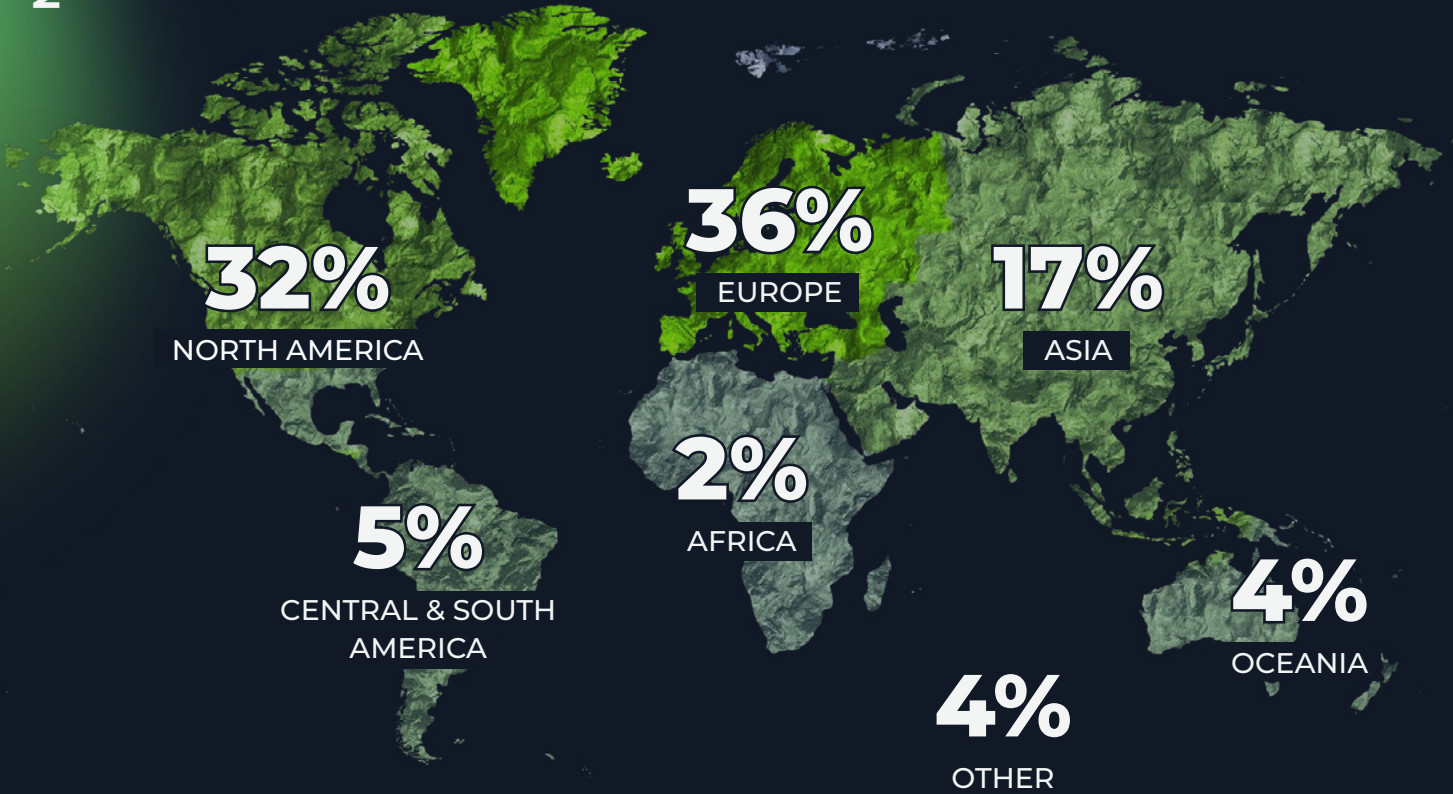
”



**PABLO
RUIZ
ENCINAS**

Security Consultant
@ **Mnemonic**

Regional breakdown



A cyberattack occurs every

39 seconds. ^[6]



In 2021, there were

1,862 breaches.


Nearly 294 million people were impacted, with over 18.5 million records exposed. ^[7]





Challenge categories


 **Cloud** AWS, GCP, and Azure misconfigurations. Teams had to apply real-world privilege escalation techniques and attack paths in cloud environments.


 **Pwn** Binary exploitation through exploiting memory corruption bugs. Teams had to analyze executables, find memory flaws, and chain different techniques to develop an exploit.


 **Crypto** Cryptographic flaws. Teams had to leverage weaknesses in known or custom-made algorithms to decrypt objects with up-to-date cryptological processes.

 **Hardware** Penetrating different hardware systems with software. Teams had to analyze and develop a working exploit for SCADA.

 **Forensics** Analysis of digital forensics artifacts. Teams had to investigate realistic digital forensics artifacts commonly seen in sophisticated cyber security attacks.

 **Reversing** The art of reverse-engineering. Teams had to analyze and identify the behavior of compiled applications by leveraging static and dynamic reverse engineering techniques.

 **HostEx** Host exploitation. Teams had to enumerate the hosts, identify vulnerable entry points, gain an initial foothold, and escalate their privileges to administrator or root.

 **Web** Web-based exploits. Teams had to enumerate, identify vulnerabilities, and exploit a variety of different vulnerable web applications.

BUSINESS CTF INDUSTRY INSIGHTS

Collected from testing 657 corporate teams and 2,979 cybersecurity professionals

Best performing industries across all challenge categories



It comes as no shock to see that **security, consulting, and technology** organizations perform **above average (15.4%)** and are prepared to deal with cybersecurity challenges across a wide range of technologies.

Organizations essential to global infrastructures, such as **government, manufacturing, healthcare, and education** showed less cyber attack readiness, with healthcare scoring **31% lower than the average** solve rate for all challenge categories.

SECURITY	18.9%
CONSULTING	17.4%
TECH	15.8%
FINANCE	15.4%
GOVERNMENT	13.7%
MANUFACTURING	13.5%
HEALTHCARE	10.5%
EDUCATION	7.8%

Browse [cybersecurity & IT courses](#) to upskill employees

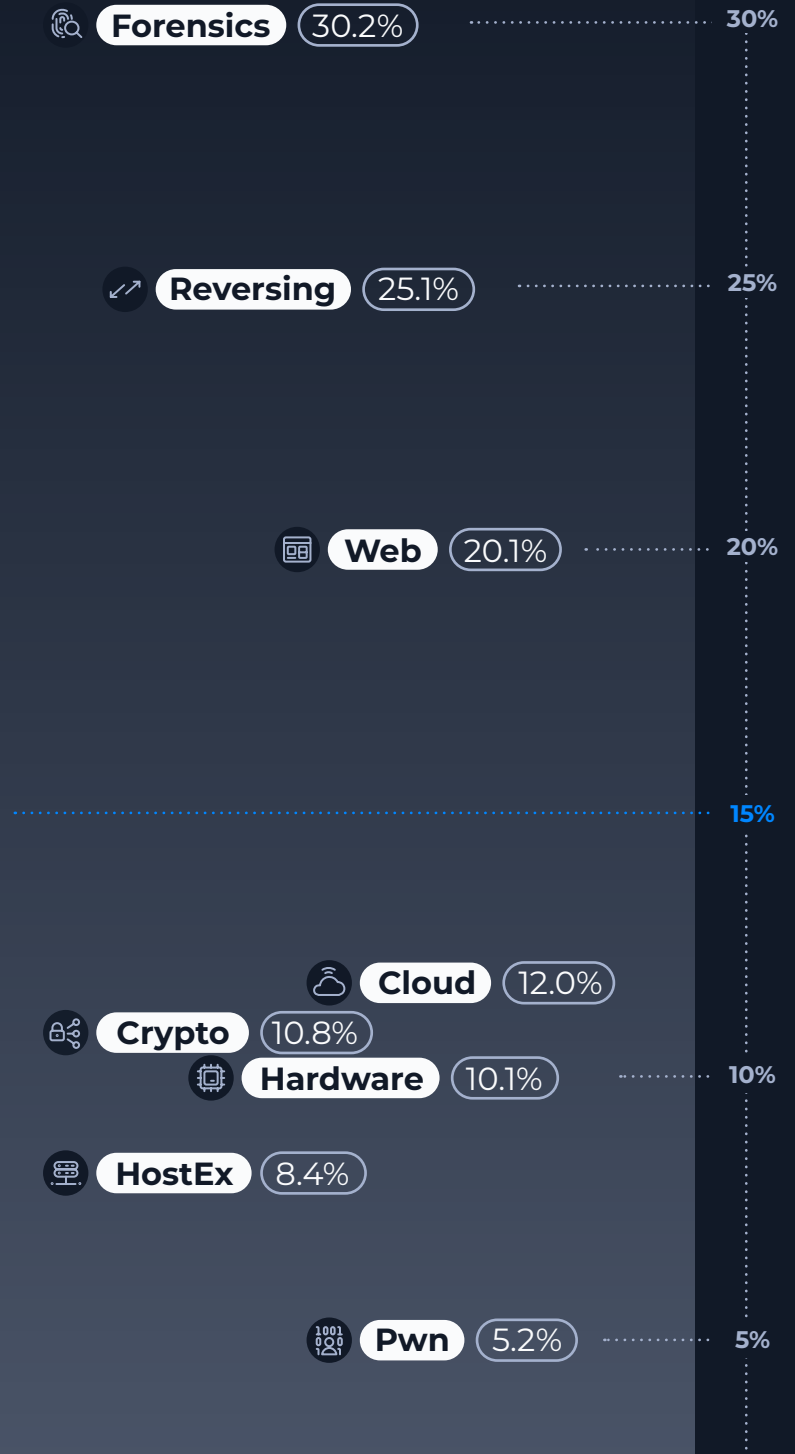


Most organizations performed **above average** when faced with cyber attack challenges that involved **forensics, reversing, and web technologies**. In comparison, cloud, crypto, and hardware technologies, as well as HostEx and pwn challenges, proved to be somewhat testing.

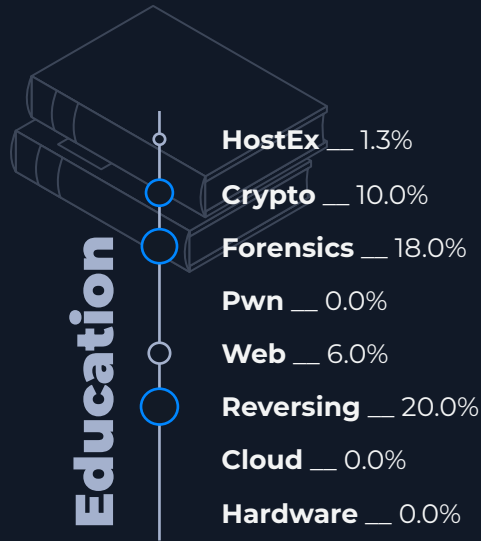
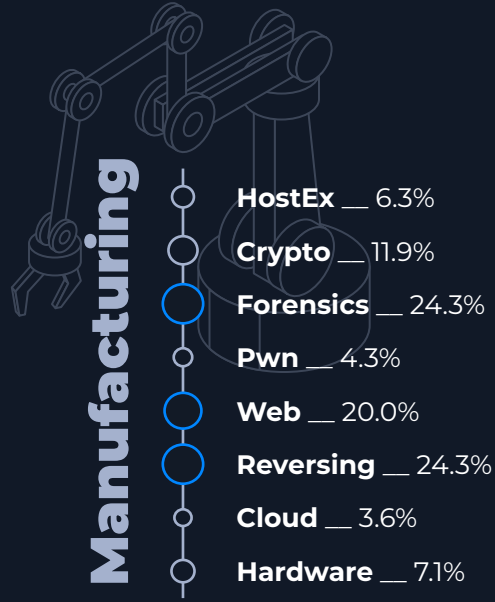
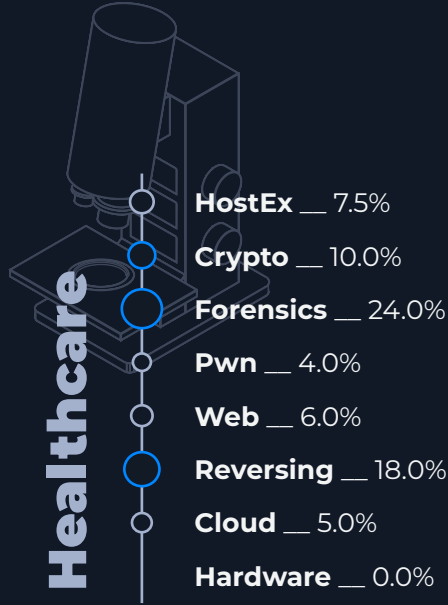
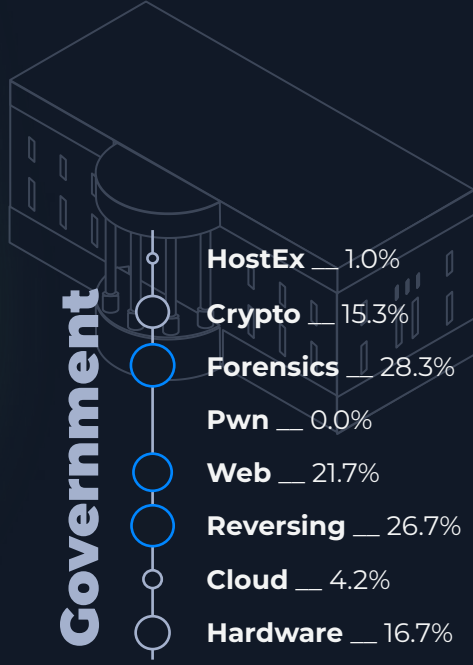
Considering the central role cloud technology and security play in enabling modern organizations to scale, innovate, and manage complex IT infrastructure, the **60% decrease in attack readiness** when comparing forensics (30.2% solve rate) against a category such as cloud (12% solve rate) is noteworthy.

This gap evidences the current **cloud security skills shortage** and highlights the urgent need for IT and cybersecurity leaders to prioritize **cloud security training**.

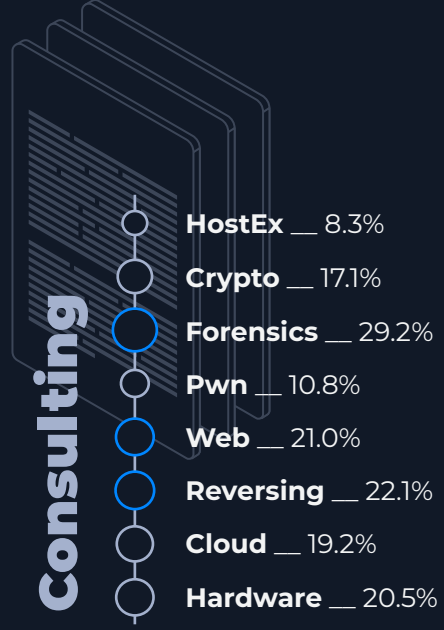
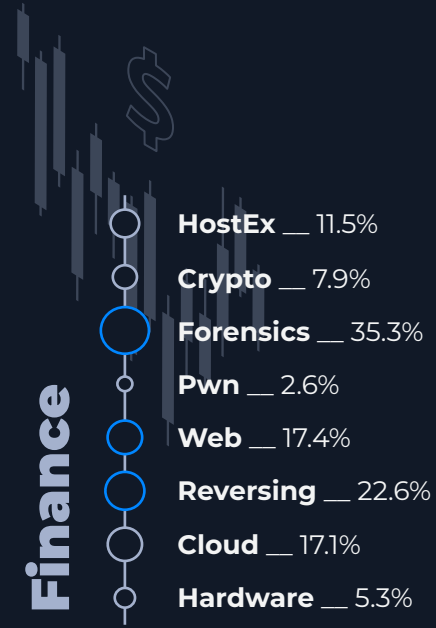
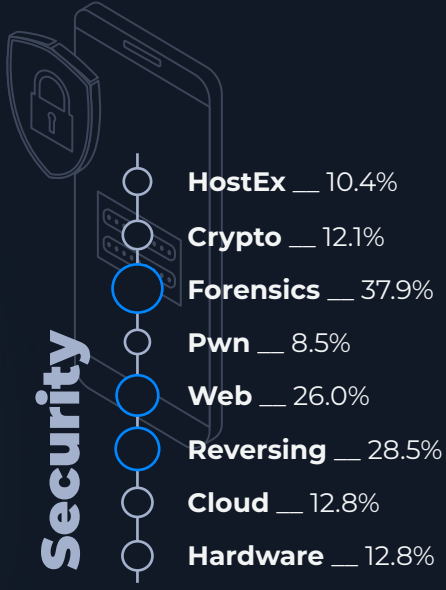
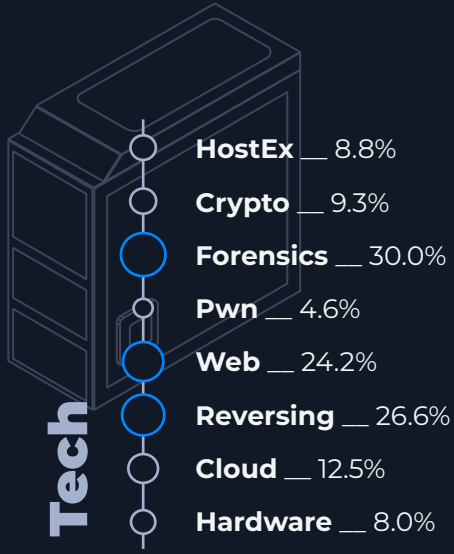
Average solves per attack category



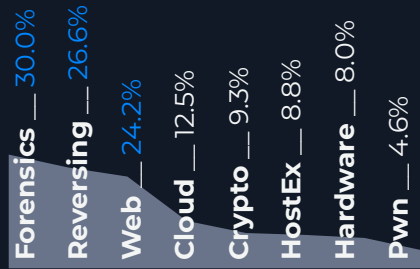
Industry-specific strengths and weaknesses



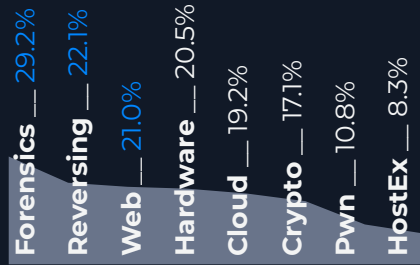
While **security, consulting** and **tech organizations** hold higher average solve rates across all cyber attack challenges, there are noticeable areas of improvement and surprising strengths unique to each industry.



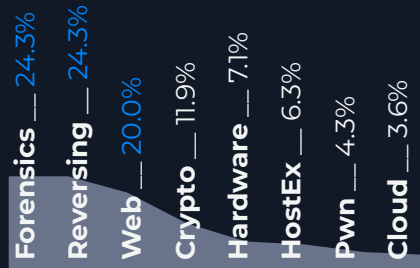
Tech



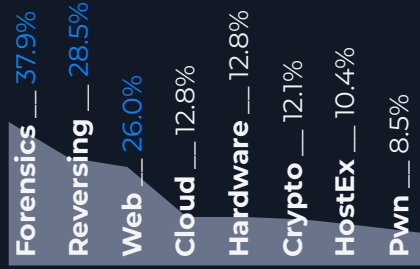
Consulting



Manufacturing



Security



Average challenge performance per industry

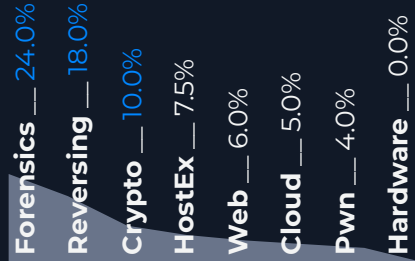
Security teams were the most adept at dealing with attacks involving web, forensics, and reversing. They scored third in cloud security and hardware challenges out of eight industries.

Manufacturing holds the **third lowest average** across all industry categories, but performed relatively well in attacks involving web, forensics, and reversing. Cloud security was the biggest area of improvement for manufacturing teams.

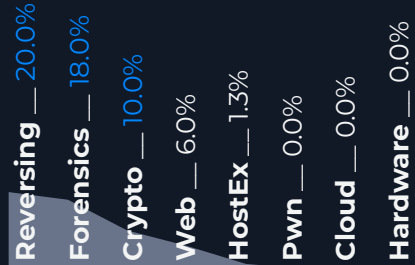
Teams from **consulting** organizations were the best performers in cloud, crypto, hardware, and pwn attacks but were near the median for web, forensics, and HostEx challenges.

Teams in **tech** organizations were among the top three performers in web, forensics, and reversing attacks, but (like teams from other industries) achieved lower scores in cloud, HostEx, pwn, and hardware attack challenges.

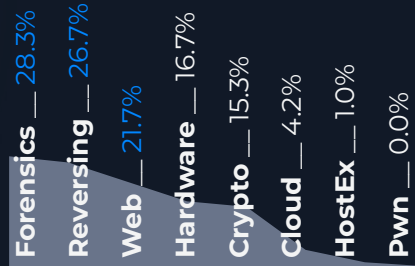
Healthcare



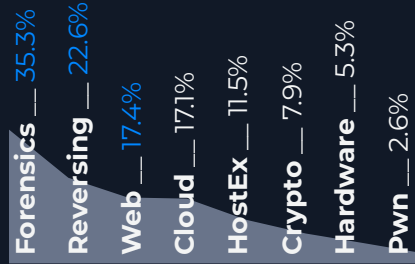
Education



Government



Finance



Finance teams achieved the best results in the HostEx category and were second best in cloud, but came last for solving crypto attack challenges.

Government teams demonstrated strong skills in forensics, reversing, web, and hardware, scoring a top-three position in all categories. Conversely, cloud and HostEx were the biggest areas of improvement for government organizations.

Teams in **educational organizations** showed promise with crypto challenges, but scored the lowest overall across all technologies and challenge types, scoring zero in web, hardware, and cloud.

Healthcare holds the **second lowest average** across all industry categories. However, teams performed relatively well in attacks that involved forensics and reversing.

Pre-register your team
for next year's Business CTF



3 REASONS WHY YOUR TEAM SHOULD JOIN THE NEXT BUSINESS CTF

Boost your team's technical skills,
employee engagement, and
coordination under pressure

01

Test your team's practical cybersecurity skills for free on a premium platform

With the number of threats rising, teams are less attack-ready when it comes to protecting their infrastructure, data, records, and most importantly, people. But how do you fix that?

Focus on practical, hands-on cybersecurity skills that prepare your team for actual threats.

The HTB content team consists of elite, field-tested cybersecurity professionals who develop cutting-edge training content that's practical and engaging for your team.

Our goal is to provide a platform where realistic training can take place without risk to your business, customers, or infrastructure.

By participating, you can benchmark your team's skills in different categories against your industry average while identifying strengths and areas of improvement.

“ Overall the challenges were pretty realistic, which is a big plus for me. I definitely recommend joining the CTF, as it lets you test your skills in realistic scenarios and challenge yourself against the best specialists in the field. We will join again next year.

”



**LUKASZ
LAMPARSKI**

Security Manager and Senior Incident Responder @ **ING Bank**

02

Improve employee engagement and team bonding

Skill level of individual employees isn't the only important factor for an organization to be attack-ready and resilient in the face of cyber threats. Your team's ability to collaborate and coordinate under pressure is vital to identifying, preventing, and improving your overall security posture.

The HTB Business CTF is a great way to introduce beginners to real hacking concepts and keep tenured employees sharp – all while improving employee engagement and retention.

“

We all had a ton of fun and learned a lot. HTB has the best selection of machines out of any CTF, hands down. Getting the team together and working on the challenges together was without a doubt the highlight from my perspective.

”

**HERALD
ANDREASEN**

Founder of **Xormatic**

03

Compete against the best cybersecurity teams (and ethical hackers) in the world

As the Business CTF continues to gain momentum and popularity within the cybersecurity community, we've seen a significant 83% year-over-year increase in participation from businesses of all sizes and industries.

If you're interested in other hands-on training opportunities, explore our **Academy for Business** (perfect for organizations who want to upskill employees with guided, interactive training to reduce onboarding times) and **real-world corporate training labs**.

Hack The Box specializes in distinguished practical and guided cybersecurity training courses 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.

“Amazing experience working with HTB! Not only it is a very complete and fun hacking learning platform, but also the team is full of talent and creativity and will support your CTF setups in a very professional way. I'm looking forward to continuing this great collaboration.”



IGNACIO ARSUAGA

Cybersecurity Enterprise Architect @ **Siemens**

If you'd like to **host your own** Capture The Flag event, visit our **Business CTF page** to get started

ABOUT HTB

Loved by an infosec community of more than 1.6 million members, HTB is helping security leaders across the globe equip their teams with the skills and expertise needed to proactively secure and protect their organizations.

Whether you're sharpening specific techniques, training up junior staff, or looking to recruit skilled cybersecurity talent, Hack The Box has a solution to fit your needs.

Measure, assess, and proactively close your organization's cybersecurity skills gap with a single platform focused on improving cyber workforce training and development.

Get in touch!



Sources:

- [1] <https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref>
- [2] <https://www.ibm.com/security/data-breach>
- [3] <https://www.microsoft.com/en-us/security/business/security-insider/anatomy-of-an-external-attack-surface/cyberthreat-minute/>
- [4] <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>
- [5] <https://www.accenture.com/acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50>
- [6] <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>
- [7] <https://www.nasdaq.com/articles/after-a-decline-in-2020-data-breaches-soar-in-2021>

2022

CYBER ATTACK READINESS

A REPORT BY  HACKTHEBOX