2024

HACKTHEBOX

How to build a high-performance cyber workforce

Summary

Hundreds of security leaders fight a common, yet brutal, uphill battle: Translating security budgets into a high-performance security function. Despite the increasing investment in technology, we still see a 600% increase in cybercrime year-over-year.Why? Most orgs solve people's problems (and security performance problems) the wrong way. They fixate on processes and technology while neglecting the talent responsible for running all systems.

At Hack The Box (HTB), we see the solution as an investment in people's careers, development, and well-being. Resulting in a better security posture and cybersecurity alignment with business objectives.

In this comprehensive guide for security leaders, you'll leave with practical tips and insights from experts in the industry. After reading you'll:

- ✓ Discover how to attract and retain top cybersecurity talent.
- ✓ Know where to find entry-level talent.
- ✓ Onboard new cybersecurity hires efficiently and effectively.
- ✓ Shift your organization's security culture to one of upskilling and proactiveness.
- ✓ Track the right metrics to prove the worth of investing in your people.
- ✓ Implement a reskilling strategy to develop a cybersecurity A-team.
- ✓ Protect your teams from burnout, retaining your top talent.
- ✓ Connect cybersecurity performance with tangible company goals.

Table of contents

Chapter 1:

4 recruiting strategies that build A-list cyber teams

Security incidents are rising, insurance premiums increasing, and the cost per incident is hard to overestimate. Paired with complex customer environments, cloud adoption, and an increase in remote work, protecting your IT infrastructure is more of a challenge than ever before. The result? We need more cybersecurity professionals. The talent shortage, coupled with an ever-widening skills gap, is burning out teams and, ultimately, raises our susceptibility to the evolving risks we face. This all calls for a new way of hiring.

The huge cyber skills gap

Cybersecurity talent shortages have plagued the industry for years, and they are only getting worse. However, there's a common misconception that there's a lack of entry-level candidates applying for these open cybersecurity positions. The real issue here is that these candidates aren't considered "qualified". A demand for more qualified candidates with practical, real-world experience and skills has created this gap. And with many "entry-level" cybersecurity roles calling for 3-5 years of experience, something has to give.

So, how do we close that gap? We need to redefine what "qualified" means and shift our focus on who the ideal candidate is. By embracing a skill-based hiring culture, we encourage the idea that anyone can become a cybersecurity professional when supplied with the right tools and support. Whether it's someone from your IT team, a recent graduate, or someone from an entirely different career background.

Upgrade your cybersecurity recruitment strategy

1. Focus on skills over certifications

Qualifications and certifications can only tell you so much about a candidate. To properly assess whether a candidate can do the job, you must look at their skill set. But how can we measure these skills? Our Professional Labs build skills that are mapped to the MITRE ATT&CK framework, relating critical skills to real job roles and responsibilities. Tracking these skills makes it easier to upskill (or test candidates) for a certain job role. So, if a candidate uses a platform like HTB, you can immediately see from their profile what areas they are skilled in and where the gaps may be. You can then use customized or pre-built labs to test their skills.

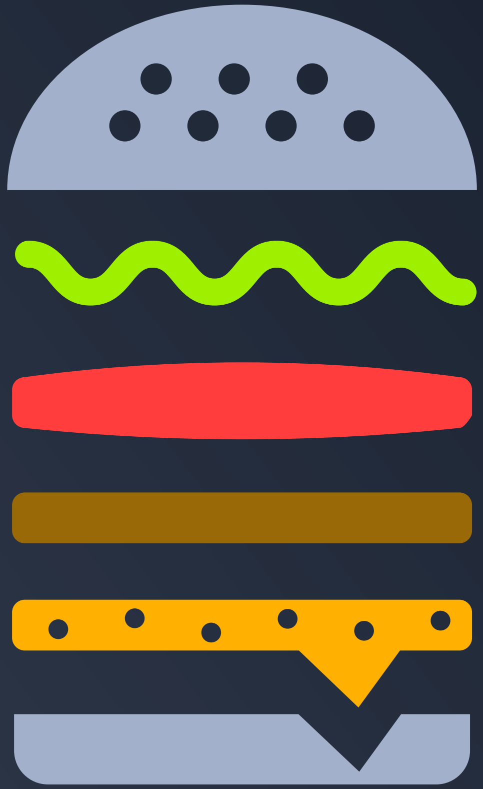
Chapter 1:

4 recruiting strategies that build A-list cyber teams

💡 **Tip:** Managers using the HTB Enterprise Platform can easily search courses using MITRE terminology and assign them based on the techniques and tactics relevant to their teams.

Skills-based hiring also provides some reassurance that your latest hire is already aligned with evolving threat actor tactics, techniques, and procedures (TTPs). This can be helpful when presenting additional investment or potential hires to the wider businesses, you can show the tangible benefits they'll bring to the organization.

Revolutionizing cybersecurity talent acquisition:
A strategic recipe for building elite teams



→ Prioritize skills above certifications & job titles

→ Search for candidates with passion & out-of-the-box thinking

→ Post jobs where candidates are spending time upskilling

→ Make job descriptions accessible with a skills focus & flexibility on experience

→ Have a strong onboarding process that prioritizes upskilling

→ Invest in continuous hands-on learning with new & existing employees

2. Go where the talent is

By depending only on recruitment agencies or simply posting your jobs on popular career boards, you often receive applications with similar experience levels and certifications. This limits the potential pool of candidates, leading you to overlook some fantastic talent.

Instead, hiring managers can adopt a much more precise approach to hiring by targeting cybersecurity professionals on the platforms they use. This saves both time and money, reducing the number of unrelated applications and recruitment fees.

> “
>
> We finally were able to target an audience that exactly matched the type of skills we were seeking. There aren’t any other credible job boards that specialize in penetration testing, Red Team, or just focusing on cybersecurity roles. Hack The Box offered us the opportunity to post jobs directly to a community of hackers.
>
> We got access to profiles that are non-traditional, this broadens your perspective and opens up a whole new addressable market of skilled candidates. Filtering by rank provided an indication of capability. It’s how we found Josiah, who was working in a Blue Team role at the time. His profile likely wouldn’t have reached us via a recruiting agency because it did not meet the typical criteria.
>
> **Tom Williams,** former Principal Consultant at Context Information Security

3. Create a unified hiring vision by aligning teams

To successfully move your organization's cybersecurity hiring into the modern era, you need to ensure that everyone is on board.

HR, talent teams, and hiring managers should balance the new way of thinking about skills over credentials. This will ensure that everyone's on the lookout for the right type of candidate and knows where to find them.

Here are some ways you can get everyone on the same page and involved with the new way of hiring:

→ Provide a walkthrough demonstration of the MITRE ATT&CK Framework and what skills to look out for.

→ Offer a list of websites and platforms to search for cybersecurity talent.

→ Adopt this skills-based hiring culture across the entire organization, not just cybersecurity teams.

→ Have some success stories in mind to back up your reasoning for skills-first hiring over credentials.

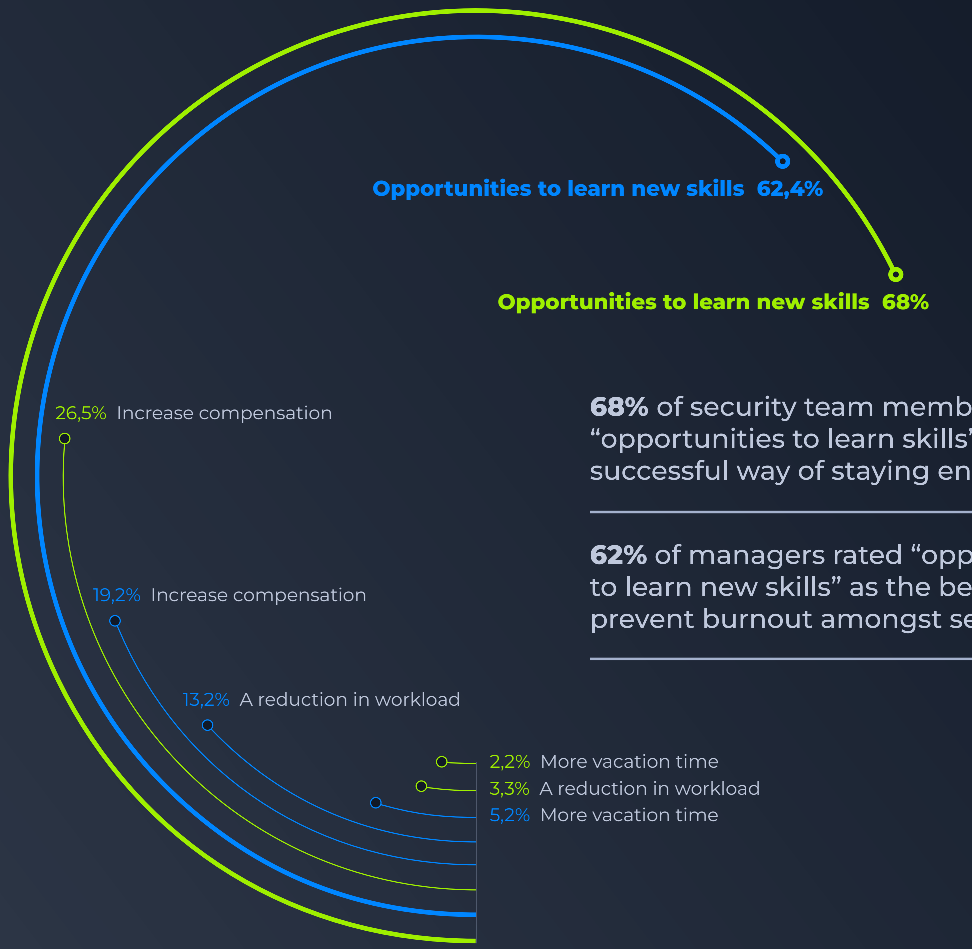
4. Invest in your team

Simply hiring junior employees won't immediately solve the cybersecurity talent shortage. Existing employees also require consistent upskilling to keep pace with the ever-increasing complexity of infosec. And many employees, both junior and senior, actively seek opportunities to develop new skills.

Chapter 1:
4 recruiting strategies that build A-list cyber teams

In our Cyber Attack Readiness Report 2023, we surveyed 803 cybersecurity professionals and found that more than 70% of managers view team events like CTFs as a viable way to raise employee engagement. What's more, 68% of security team members rated "opportunities to learn skills" as the most successful way of staying engaged work. Whilst 62% of managers rated "opportunities to learn new skills" as the best way to prevent burnout amongst security staff.

With dwindling budgets, extra salary compensation isn't always an option. Thankfully, cybersecurity managers are finding that investing in their employees—with fun Capture The Flag (CTF) events and offering a curriculum of upskilling—helps reduce burnout and boost retention.



68% of security team members rated "opportunities to learn skills" as the most successful way of staying engaged at work

62% of managers rated "opportunities to learn new skills" as the best way to prevent burnout amongst security staff

Cybersecurity hiring checklist

- ✓ Prioritize skills above certifications and job titles.
- ✓ Search for candidates with passion and out-of-the-box thinking.
- ✓ Post jobs where candidates are spending time upskilling.
- ✓ Make job descriptions accessible with a skills focus and flexibility on experience.
- ✓ Have a strong onboarding process that prioritizes upskilling.
- ✓ Invest in continuous hands-on learning with new and existing employees.

Chapter 2:

Finding entry-level talent with market-ready skills

The global cybersecurity talent shortage currently stands at almost four million. To fill these roles, more organizations are hiring entry-level talent, but the real challenge is attracting and retaining this talent when the demand is so high. We spoke to industry experts on what steps hiring managers should take to attract, hire, develop, and retain entry-level cybersecurity employees.

Why should you hire junior cybersecurity teams?

By prioritizing hiring junior candidates, you'll be filling that talent shortage whilst also retaining entry-level talent by offering them a place to learn and grow. The fresh perspectives and enthusiasm are also great additions to the team that can help prevent burnout.

Chapter 2:

Finding entry-level talent with market-ready skills

1. Making cybersecurity accessible to fresh talent

The cybersecurity industry is shrouded in mystery for many entry-level candidates, with no clear path from university to their first role. As leaders, we can change this perception by actively reaching out to entry-level talent and attending career fairs.

When students aren't sure that the time and money they are spending on degrees and certifications is worth it, it can be difficult to find motivation to continue. The responsibility rests on cyber leaders to demystify the best path into the industry, providing candidates with a clear goal to work towards.

> “
>
> Utilize specialist security job boards and industry forums, rather than general job boards. This can result in lots of wasted time sifting through candidate profiles that are not suitable for the role. Speak to your team to get tips on the best forums and job boards to post on.
>
> **Tom Williams,** former Principal Consultant at Context Information Security

2. Prioritize pertinent skills, education, and certifications

Cyber hiring managers are often trying to fill a huge variety of roles with different levels of experience and skills required. This means that there's no one-size-fits-all approach to hiring.

However, one fact that remains consistent is that all cybersecurity roles require a combination of hard and soft skills. By getting clear on the skills, education, and certifications you're searching for in a candidate, you'll have a laser focus approach, rather than hoping something sticks.

> “
>
> It is imperative that they have the soft skills, they have to communicate. Our world is so complex that we can't solve it independently, we have to be able to work as a team.
>
> **Matthew Rosenquist,** CISO, Mercury Risk and Compliance, Inc.

3. Clearly define cybersecurity job descriptions

When searching for entry-level cybersecurity professionals, hiring managers are often faced with a lack of “qualified” candidates. But there’s a desperate need to redefine what qualified looks like.

> Focus on essential skills and experience, avoiding unrealistic qualifications or an extensive wish list. Not managing this well can mean that you miss out on a whole host of potentially suitable candidates who will rule themselves out of the process.
>
> **Tom Williams,** former Principal Consultant at Context Information Security

4. Connect HR and hiring managers

HR and hiring managers need to work closely together. Cybersecurity is such a large and sometimes confusing industry that we can't expect HR to immediately know who a good entry-level candidate is. Managers must work closely with HR when creating the job ad, explaining which degrees or certifications are essential, and what tools stand out as a green flag.

> “
>
> HR and the cyber hiring manager should meet early to discuss the role and its requirements in detail to draft a specific job specification and agree on a selection process. This part of the process is often overlooked but is crucial as it provides transparency and sets clear expectations for candidates and internal stakeholders alike.
>
> **Tom Williams,** former Principal Consultant at Context Information Security

5. Retain talent with strong leadership

Show value: in job descriptions and within the role itself, leaders need to show what value they can offer employees. Whether it's upskilling, remote work, flexible hours, or a generous salary.

💡 **Fun fact:** 75% of employees prioritize progressing their skills over pay.

Understand your market: money isn't everything, but companies need to be aware of what the market is paying and match these salaries to attract long-term employees.

Check-in regularly: cybersecurity is stressful and there's often a lot of firefighting involved in many roles. Good leaders check in with their employees and offer solutions to problems.

Chapter 3:

The power of effective cybersecurity onboarding

Recruiting doesn't end after a candidate accepts an offer, it simply moves into the next crucial stage: onboarding. An efficient onboarding process is necessary to retain top-quality talent, especially in an industry that severely lacks employees with experience.

The famous saying: "fail to prepare, prepare to fail" certainly rings true here. You want to set your new cyber team up for success, and an efficient onboarding process is the secret.

Why onboarding is important in cybersecurity

→ Organizations with a strong onboarding process improve new hire retention by 82%.

→ 83% of cybersecurity professionals admit that they or someone in their team have made errors that have led to a breach due to burnout, which is why getting up to speed is essential.

→ An efficient onboarding program results in improved employee engagement, boosted retention rates, reduced chances of burnout, and less strain on senior employees.

Chapter 3:
The power of effective cybersecurity onboarding

1. Conduct a technology induction

A working knowledge of cybersecurity tools and technologies is a critical first step in onboarding.

One of the first stages of the onboarding process should be to provide an inventory of IT products and services in use. However, it's vital to go one layer deeper and provide insights into the role of IT in an organization and how the cybersecurity team contributes to its success.

Reflect your culture
The onboarding process should be immersive and unique to your organization, reflecting the culture and mission.

Go beyond HR
Hiring managers and HR need to collaborate to role-specific onboarding.

Measure success
Use CTFs, and labs to benchmark and measure success, based on your employee's strengths and weaknesses.

Make onboarding long-term
Onboarding should take place over the course of months, not days.

Map training to real-world threats
Making training specific to NIST or MITRE ATT&CK frameworks to ensure that employees learn threat-landscape-connected skills.

Chapter 3:

The power of effective cybersecurity onboarding

2. Share security processes

Every cybersecurity team will have a strategy and processes to ensure they succeed in their roles. It's key that new hires become quickly familiar with these:

- **Objectives:** what's a realistic security posture, and how is success or failure measured? This includes the roles and responsibilities of different team members.

- **Risk factors:** based on your organization's unique structure and risk tolerance, new hires must be aware of the biggest risks to existing infrastructure.

- **Threats:** even if not pertinent to an individual's role, all cybersecurity team members should know where and how to access threat intelligence.

- **Compliance:** depending on your industry, your cybersecurity team will adhere to different compliance regulations. All new hires should know what these are.

3. Introduce the cybersecurity team and best practices

A common aspect of any onboarding process is meeting the wider team and setting up inductions. New cybersecurity hires should meet the team and learn about their roles and how they might work together. This is an excellent opportunity to set up some unique training exercises, such as purple teaming, to help integrate new hires with members of the team they may not always work with.

Some general best practices for onboarding new team members include:

- Security processes such as checklists and general procedures.

- Incident response and event management documentation to help new hires understand their role in the event of a breach.

- The roles and responsibilities of third-party technology.

4. Assess new hires

Before developing an in-depth onboarding upskilling program, it's important to assess and measure the strengths and weaknesses of new hires. By measuring skills early on, you're able to provide new hires with a valuable onboarding experience that quickly gets them up to speed. Offering the ability to upskill right away is more likely to retain and develop talented cybersecurity professionals.

Easi, a Hack The Box client, used our Professional Labs to assess the skills of new hires, refine the onboarding process, and plan the development of new employees.

> "Being able to invite new starters is a great feature. It allows us to more accurately measure a new hire's knowledge and how to build upon it."
>
> **Mickey De Beats,** Red Team CyberSecurity Consultant, Easi

5. Create a training program tailored to industry frameworks

After assessing the skills of new hires, the next step is to create a tailored training program centered around their particular job role. Traditionally, cybersecurity training lacks personalization and relevance to industry job roles and trends, such as the latest CVEs.

💡 At Hack The Box, managers can use the Enterprise Platform to easily search courses using terminology from these frameworks and assign them based on the techniques and tactics relevant to their teams.

Industry frameworks to map skills include:

→ MITRE ATT&CK

→ MITRE DEFEND

→ NIST/NICE

→ The DoD Cyber Workforce Framework (DCWF)

Making your training specific to these industry frameworks is more relevant to real-world scenarios and will ultimately drive new hires to be much better at their jobs.

6. Benchmark learning with CTFs

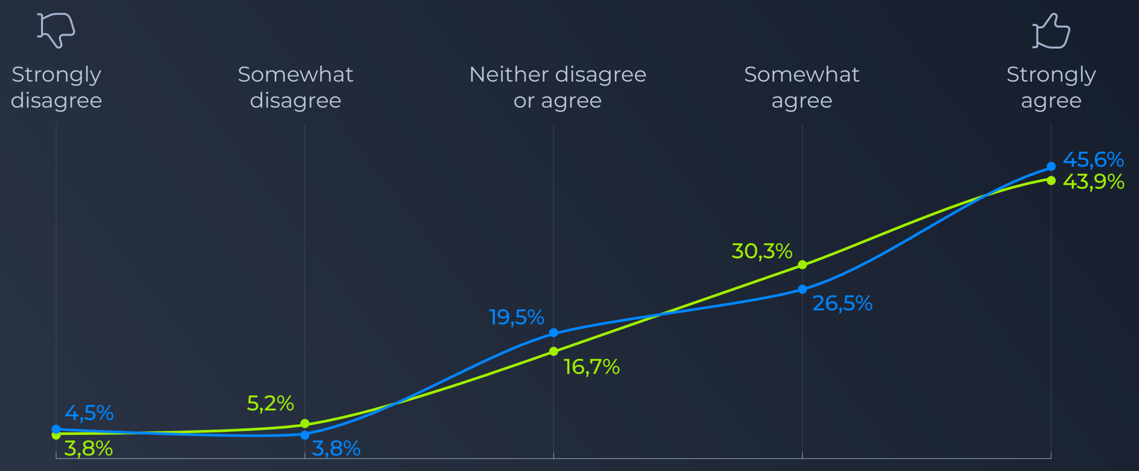
A great cybersecurity onboarding process has measurements in place to track the success and development of an employee. Onboarding data and metrics are essential for the C-suite to follow, helping CISOs drive an overall cybersecurity culture shift.

Capture The Flag (CTF) events are a fun and efficient way to benchmark an employee's learning while offering new opportunities to upskill.

In our Cyber Attack Readiness Report 2023, we interviewed 803 active cybersecurity professionals and found that:

→ More than **70%** of managers view team events like CTFs as a viable way to boost employee engagement.

→ **72%** of managers agree that CTF events can help measure and upskill employees.



- Team events like Capture The Flag (CTF) **help measure & upskill employees**
- Team events like Capture The Flag (CTF) **improvee employee engagement**

Chapter 4:

8 cybersecurity performance metrics you should be tracking

Cyber performance programs invest in the growth and retention of your team. In cybersecurity, this looks like continuous hands-on upskilling, clear career development paths, and battling burnout and fatigue with engaging initiatives. But this isn't just about cybersecurity. It's about aligning performance with your organization's mission.

Why tracking cyber performance is important

Management consultant Peter Drucker famously said, "If you can't measure it, you can't manage it."

How can you know that you're maximizing your cyber performance plans without tracking them? And more importantly, how will key stakeholders witness growth and invest more budget in your cybersecurity initiatives without evidence that they're working? Metrics are the answer. Having the right measurements in place will enable you to optimize upskilling and overall cyber performance. Monitoring the right metrics also means your team is better equipped to deal with emerging threats.

For example, there could be a new type of ransomware attack exploiting a recently discovered vulnerability (CVE). You need to quickly assess whether your team, both blue and red, has the current skills to defend against this specific threat. Tracking the ongoing training and certifications of your team members can give you immediate insight into their readiness and capability to handle such threats.

“

Academic research states that performance evaluation and benchmarking are a widely used method to identify and adopt best practices as a means to improve performance and productivity.

This methodology is particularly valuable when no objective or engineered standard is available to define efficient and effective performance. Leadership and management must be able to quantitatively define progress and improvement and that begins with understanding the starting point.

Dan Magnotta (Mags22), HTB Federal Business Development & Capture Manager, Hack The Box

Tracking security posture

When reporting to the wider business and C-suite, there's a higher focus on financial implications and risk. Whilst these metrics can be greatly improved by cyber performance programs, it's important to track the following and compare improvement throughout the cyber performance process.

After all, your cybersecurity team may have different individual goals and metrics based on their specific job roles, but the wider business will have a broader focus on security posture.

The magic happens when these two align through well-thought-out performance programs.

A checklist to track cybersecurity performance

✓ **Preparedness:** do you have a proactive security posture with regular threat emulation training?

✓ **Time to detection and mitigation:** track the detection, resolution, and containment times.

✓ **Security incidents:** how has the number of security incidents changed and has downtime improved?

✓ **Optimize upskilling:** track the number of employees enrolled in cyber performance programs and monitor performance with regular CTFs.

✓ **Cost per incident:** is this reduced with cybersecutiy performance improvements?

✓ **Track the impacts:** the % time users spend upskilling and % of improved incident response.

✓ **Measure career development:** track job productivity and new skills acquired.

✓ **Employee engagement:** use surveys to track satisfaction and engagement, monitor your team's turnover rate.

How to track cybersecurity performance

1. Metrics to optimize upskilling

Here are some strategies to put in place to track your metrics to optimize upskilling for individuals on teams:

Benchmark existing skills:
track the percentage of team members achieving a specific score range in a Capture The Flag (CTF) event. This can be broken down into different skill areas (e.g., network security, application security) to identify specific skill gaps.

Assign upskilling programs:
track the number or percentage of team members enrolled in and completing upskilling programs aligned with industry standards like MITRE ATT&CK or NIST/NICE frameworks. This also provides an incentive for employees to earn more as they progress through industry frameworks.

Set measurable goals:
specific performance targets based on skill areas. For example, a goal could be to “increase the number of team members proficient in cloud security by 20% within the next six months.”

Regularly assess and monitor progress:
tracking improvements in scores or performance in periodic assessments, such as bi-annual CTF events, tabletop exercises (TTXs), or simulations.

> “
>
> Before I want to know metrics, I need to know outcomes. Once I know the outcomes, I can gather the correct information.
>
> I want to understand and know what my 6-month or 12-month training plan is for each individual. Normally this will be based on a work role from NIST/NICE. As they progress, they then can obtain higher salaries, new skills, etc. So my outcomes are based on frameworks.
>
> Therefore, if I know I have a junior SOC analyst and I will allow them to have 5 hours a week to train, I want to know how long they are on the platform, when are they on the platform, and what they are doing on the platform.
>
> **Dan Magnotta (Mags22),** HTB Federal Business Development & Capture Manager, Hack The Box

2. Measure the impact of cyber performance

Measure the impact of cyber performance with metrics like:

→ % of time users spend upskilling.

→ % of upskilling program completed/ certificates earned.

→ % increased team engagement.

→ % of decreased response time and improved recovery post-incident.

How does this look in action?
Before embarking on your cyber performance program, put together some statistics on data breach costs, for example. Once the upskilling has time to take effect, you can compare these costs from before and after the program. Ideally, they should be lower due to teams containing attacks faster.

3. Track career development

Regularly review individual success by tracking the following metrics:

Job productivity: are they resolving more tickets? Remediating more vulnerabilities? Set targets for what you'd expect after a certain level of upskilling.

Feedback: are they satisfied with the upskilling program? What do managers and colleagues have to say about their improvements?

New skill acquisition: track which skills they are upskilling most frequently in.

Career development: are they on track to be promoted or move laterally in the company? Adopting more blue or red skills?

> I would compare results to the cyber performance training we mapped out for the individual. Are they on track to meet all training requirements? What are the new skills they learned? Are we getting feedback on user satisfaction? Is the intent of the plan aligned with their actual goals and team goals?
>
> **Dan Magnotta (Mags22),** HTB Federal Business Development & Capture Manager, Hack The Box

> Firstly, we monitor the progress of certifications and training. Our employees are encouraged to pursue relevant certifications like OSCP, CRTO, and others. We make 20% of working time available for training and further education. We track the number of certifications obtained, courses completed, or hours dedicated to training.
>
> We also conduct regular skill assessments. These assessments cover various aspects of IT security, from network penetration to social engineering, enabling us to quantitatively measure skill enhancements.
>
> In terms of project performance metrics, we evaluate how effectively our employees identify vulnerabilities, the complexity of the security issues they uncover, the time efficiency in system breaches, and the viability of the security solutions they propose.
>
> **Moritz Samrock,** Red team manager, Laokoon Security

8bit transforms the way their teams upskill with HTB

Using HTB as their workforce development platform transformed 8bit's upskilling process.

Measurable metrics and progress indicators are one of the main reasons why the 8bit team managed to seamlessly onboard five junior team members, practicing on over 300 live targets in just 10 weeks.

→ Read 8bit's case study

4. Employee engagement and retention

So, how can you practically track employee engagement and retention?

Measure employee Net Promoter Score (eNPS): how many cybersecurity employees are likely to recommend your organization as a place to work?

Conduct employee engagement surveys to monitor job satisfaction and engagement before and after upskilling.

Track voluntary employee turnover rate by monitoring your voluntary employee turnover rate. Highly engaged employees are less likely to resign, monitor how this number changes are investing in employee performance.

> “
>
> Another key metric is the contribution to knowledge sharing. This includes internal contributions to our knowledge base, as well as external engagement like articles, workshops, or talks. Innovation is at the heart of what we do. We track the development of new tools, scripts, or methodologies for penetration testing and red teaming, recognizing the impact and originality of these innovations.
>
> Peer and supervisor feedback is integral. This qualitative measure helps us assess soft skills, which are essential in our collaborative and dynamic work environment. Participation in competitions and CTFs (Capture The Flag) is another metric. These events are excellent for applying and testing skills in real-world scenarios.
>
> Lastly, we encourage and track contributions to research and publications in the field. This not only enhances personal growth but also contributes to the broader cybersecurity community.
>
> **Moritz Samrock,** Red team manager, Laokoon Security

Why do cybersecurity teams need to align with organizational goals?

Many cybersecurity teams are purely focused on technical goals. While board members and C-suite executives prioritize business goals, such as increasing the company's profitability, staying ahead of the competition, and being able to pay dividends to investors.

As a result, cybersecurity leaders frequently struggle to illustrate the overall business consequences of potential security risks. This means security requirements often go unnoticed by executives and board members until a significant incident occurs. The more cybersecurity professionals know about business outcomes, the better they understand the "why" of what they are protecting.

Cybersecurity alignment for organizational resilience

Risk management
Focus on mitigating high-impact risks.

Compliance and regulations
Determining your organization's legal obligations aligns cybersecurity upskilling with key areas. For example, safeguarding federal information (FISMA).

Resource allocation
Allocate resources around protecting critical assets.

Demonstrating value
Contributing to the organization's success, protection of assets, and overall resilience demonstrates cybersecurity's value.

Communication and collaboration
Better communicate the importance of their work, gain support, and foster a culture of security.

Crisis management
Minimizing the impact of an incident by prioritizing the recovery of critical systems and data will support the organization's ability to achieve its goals.

What risk scenarios can we expect to face?

Assess recent cyberattacks in your industry and past incidents the organization has faced, to see what lessons can inform your goal-setting process. This will highlight the most relevant risk areas to protect.

Conduct an in-depth risk assessment to evaluate your existing security measures and protocols. This will enable you to pinpoint any weaknesses or deficiencies in your current system that can be addressed through upskilling initiatives.

These risk scenarios can then be emulated through tabletop exercises (TTXs) and Capture the Flag (CTF) events.

Strategic cybersecurity talent development

5 ways to align professional development with company goals

☑ **1. Understand business objectives**
Identify your organization's main objectives and the risks that accompany them. For example, if a goal is to boost market trust and brand reputation, then cybersecurity upskilling can reduce the risk of a data breach.

☑ **2. Identify the crown jewels to protect**
Understand which assets your organization values most. Then build your upskilling program around protecting them.

☑ **3. Learn about past incidents**
Assess recent cyberattacks in your industry and past incidents the organization faced. Then conduct tabletop exercises and CTFs around these scenarios.

☑ **4. Educate on compliance and regulatory requirements**
Identify the industry norms, regulations, and compliance requirements essential for your organization. Ensure your security program can provide evidence of performance that meets these obligations.

☑ **5. Communicate cybersecurity goals with the board of directors**
Track how your upskilling initiatives are positively impacting company goals. For example, % of time users spend upskilling → reduced Time to Detect (TTD) → improved market trust, and brand reputation.

For example, a TTX could test your security team's preparedness by asking how they'd prepare for a suspected attack on your organization's most critical assets. Discussion questions could include:

→ What are the potential threat vectors?

→ Have you considered which attack vectors have been most common over the past month?

→ Have you checked your patch management status?

→ Can you increase the monitoring of your IDS and IPS?

→ Do you have a way of notifying the entire organization of the current threat?

→ Does your incident response plan account for these types of situations?

Direct influence of upskilling on compliance	Indirect influence of upskilling on compliance
Skill alignment with compliance standards: Upskilling programs can be designed to directly address specific regulatory requirements. For instance, if compliance standards require regular risk assessments, training employees in advanced risk analysis techniques ensure that these assessments are performed effectively and according to the latest methods.	**Cultural shift towards compliance:** Continuous upskilling fosters a culture of security awareness and compliance. When employees understand the importance of regulations and are trained in compliance-related processes, they are more likely to adhere to these standards in their daily activities.
Certification and standardization: Many regulations require that certain tasks be performed or overseen by certified professionals. Upskilling programs can help employees gain these necessary certifications (e.g., CISSP, CISA, etc.), directly supporting compliance efforts.	**Adaptation to regulatory changes:** The regulatory landscape is constantly evolving, and upskilling ensures that the cybersecurity team remains current with the latest compliance requirements and technology standards.
Enhanced audit preparedness: A well-trained cybersecurity team is better equipped to handle audits and regulatory inspections. Training in areas like incident response and data protection can streamline the audit process by ensuring that employees know how to provide the necessary documentation and evidence of compliance.	**Innovation and compliance enhancement:** Upskilling can lead to innovation in cybersecurity practices that not only meet but exceed regulatory requirements. For example, training in emerging technologies like AI and machine learning can lead to the development of more sophisticated security measures, which can set new standards in compliance and industry best practices.

Learn how to communicate these goals with the board of directors

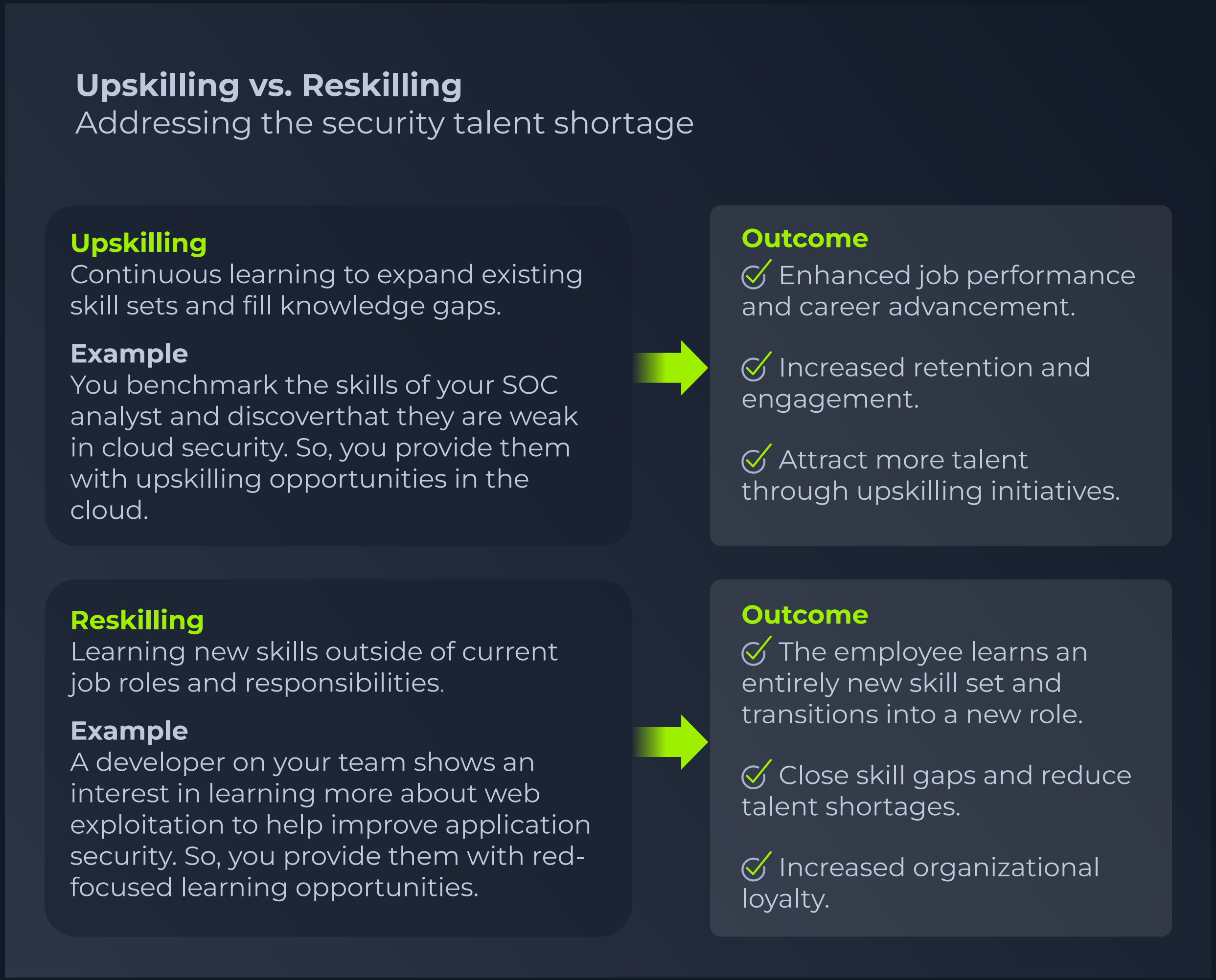
When communicating the benefits of upskilling to the C-Suite and board of directors, it's crucial to align your message with their strategic goals and demonstrate how upskilling can be a key driver of long-term business success. Here's how you might approach it:

- ✓ **Connect upskilling to business objectives:** Start by linking upskilling directly to critical business outcomes. Explain how enhanced skills lead to better risk management, faster threat detection, and more efficient problem resolution, which can all safeguard the company's assets and reputation.
- ✓ **Illustrate indirect benefits:** Highlight the indirect benefits of upskilling, such as increased employee engagement and retention, which are important to the C-Suite. Emphasize that a more skilled workforce can lead to innovation and a stronger competitive edge, ultimately enhancing market trust and brand recognition.
- ✓ **Use data and trends:** Provide data or case studies from similar organizations that have seen success from upskilling initiatives. This evidence can make a compelling case for the potential return on investment.
- ✓ **Address skill gaps:** Identify current skill gaps and how they pose risks to achieving strategic goals. Outline a detailed plan for how upskilling can address these gaps.
- ✓ **Propose a pilot program:** Suggest starting with a pilot upskilling program in a critical area. This approach minimizes initial investment and provides tangible examples of potential benefits before a full rollout.
- ✓ **Emphasize agility and resilience:** Stress that upskilling contributes to organizational agility and resilience, enabling the company to adapt more quickly to market changes and emerging threats.
- ✓ **Show long-term vision:** Align the upskilling initiative with the long-term vision of the organization. Show how continuous learning and development are crucial in keeping pace with technological advancements and industry standards.
- ✓ **Call to action:** Conclude with a clear call to action, such as setting up a committee to explore upskilling strategies or approving a budget for training programs.

Chapter 5:

Implement cybersecurity reskilling & close talent gaps

CISOs, managers, and team leaders are under immense pressure to adapt and innovate. They're tasked with finding creative solutions to the ongoing talent shortages that plague the industry. Amidst these challenges lies a golden opportunity: reskilling initiatives. Reskilling is about tapping into existing talent within your organization and building formidable cybersecurity professionals from the ground up. Not only does reskilling help combat cybersecurity talent shortages, but it also keeps teams engaged, retains people you know and trust, offers new career opportunities, and develops a culture of learning within an organization. The result? A better security posture for your company and a cybersecurity team that's constantly adapting to threats.



Upskilling vs. Reskilling
Addressing the security talent shortage

Upskilling
Continuous learning to expand existing skill sets and fill knowledge gaps.

Example
You benchmark the skills of your SOC analyst and discoverthat they are weak in cloud security. So, you provide them with upskilling opportunities in the cloud.

Outcome

✓ Enhanced job performance and career advancement.

✓ Increased retention and engagement.

✓ Attract more talent through upskilling initiatives.

Reskilling
Learning new skills outside of current job roles and responsibilities.

Example
A developer on your team shows an interest in learning more about web exploitation to help improve application security. So, you provide them with red-focused learning opportunities.

Outcome

✓ The employee learns an entirely new skill set and transitions into a new role.

✓ Close skill gaps and reduce talent shortages.

✓ Increased organizational loyalty.

A five-step plan for reskilling teams into cybersecurity

1. Skills forecasting
- Benchmark the skills of existing cybersecurity teams using Capture the Flag (CTF) events to identify talent gaps.
- Research trending threats and in-demand skills.

2. Identify existing talent
- Don't just focus on technical skills, look for problem-solving abilities, attention to detail, and a passion for cybersecurity.
- Look for job roles with the most transferable skills (like developers or IT staff).

3. Promote a culture of reskilling
- Encourage lateral movement throughout your organization.
- Sell the benefits of a career in cybersecurity to relevant teams.

4. Develop new career pathways
- Hire creatively by exploring skills over degrees and certifications.
- Consider diverse technical backgrounds.

5. Provide mentorship programs
- Match existing employees to cybersecurity veterans to enable reskilling.
- Pair red and blue veterans together to learn from one another.

Chapter 5:

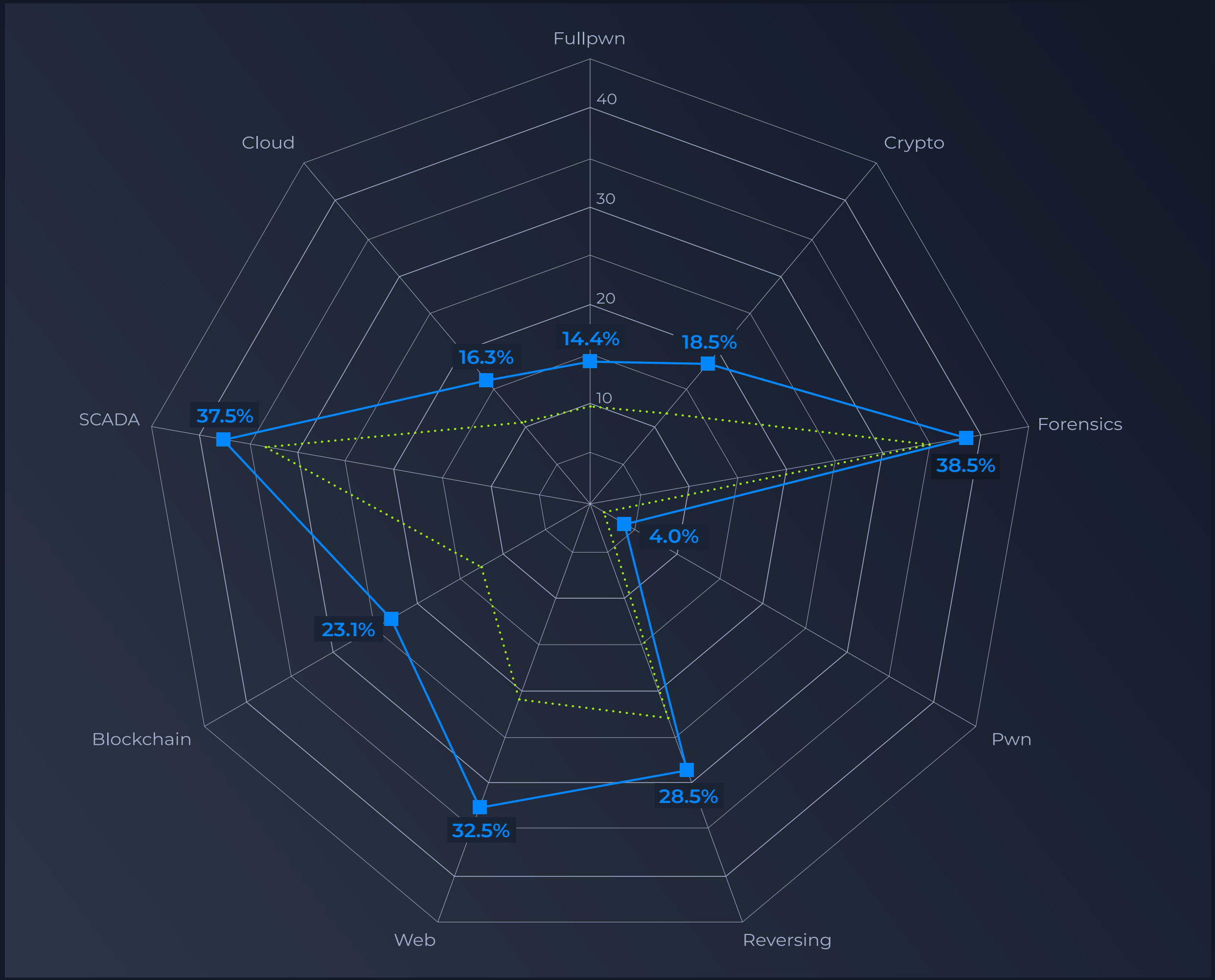
Implement cybersecurity reskilling & close talent gaps

1. Skills forecasting

Benchmark the skills of your existing employees before initiating any reskilling program. You can do this by conducting an event such as Capture the Flag (CTF).

CTFs are gamified competitive cybersecurity events that are based on different challenges or aspects of information security. They'll help your teams identify where specific skill and talent gaps lie.

At Hack The Box, we map these skills to industry frameworks including NIST/NICE and MITRE ATT&CK. This means you can forecast skill shortages that are mapped to specific job roles.



2. Identify existing talent

You can now identify existing employees who are interested in pursuing a career in cybersecurity or possess transferable skills.

However, this doesn't always mean that the skills must be technical. Don't dismiss individuals who lack technical skills as these can be taught with hands-on upskilling. Look for problem-solving abilities, attention to detail, and a passion for staying updated on technology trends and the latest cybersecurity threats.

Pathways to cyber

Reskill your existing internal roles into security

Job role	Reskill	Cybersecurity
IT product support	→	Cybersecurity analyst & incident response
IT engineers	→	Cybersecurity engineers
Developers	→	Cybersecurity engineers, analysts, & penetration testers
UI/UX design	→	Cybersecurity engineer/analyst
Forecasting & strategic planners	→	Threat hunter/threat intelligence analyst
Accountants	→	Cybersecurity analysts

3. Promote a culture of reskilling

Encourage all employees to explore areas that interest them, even if those areas of interest stretch beyond their current job role. You can encourage employees to pursue a new venture in cybersecurity by sharing the following benefits:

Job security and career advancement:
all industries require cybersecurity professionals and many are lacking talent. This makes for a fantastic opportunity for employees to advance their careers further in a field that needs them more than ever.

Lucrative rewards:
compensation, work-life benefits, and upskilling opportunities are significant in the cybersecurity industry, making this a key case for reskilling.

Life-long learning:
being a hugely challenging, dynamic, and stimulating industry, cybersecurity can be a tempting career for those employees with a growth mindset.

4. Develop new career pathways

Professionals with diverse backgrounds that have technical, and non-cyber experience are great candidates for cybersecurity positions. IT and development talent is proving to be a new route into the industry. By facilitating new methods of gaining a foothold in cybersecurity and reskilling on the job, you're not only reducing the talent shortage but making cybersecurity a more attractive career to pursue within your organization.

> Hack The Box offered us the opportunity to post jobs directly to a community of hackers. We got access to profiles that are non-traditional, this broadens your perspective and opens up a whole new addressable market of skilled candidates. Filtering by rank provided an indication of capability. It's how we found Josiah, who was working in a Blue Team role at the time. His profile likely wouldn't have reached us via a recruiting agency because it did not meet the typical criteria.
>
> Not only did we unearth a real gem in Josiah—who went on to become a great asset to the company and is continuing to go from strength to strength in his career—we also saved around 8,000 GBP in potential agency recruitment fees for hiring someone with Josiah's capabilities.
>
> **Tom Williams,** the former Principal Consultant at Context Information Security, shares his experience on hiring non-traditionally

5. Provide mentorship programs

Establishing a mentorship program is a proven formula to help reskill employees in the cybersecurity field. A seasoned security mentor can offer career direction, share knowledge, and help foster new connections. This also provides benefits to the mentor, enabling them to grow their leadership and training skills. Mentorship can even support existing cybersecurity professionals looking to reskill into specialist domains. For example, a SOC analyst might mentor a penetration tester, teaching them how to defend Active Directory (AD) against common vulnerabilities, for instance.

Chapter 6:

How security leaders can protect their teams from burnout

Cyber threats don’t sleep. There’s a constant stream of new tactics, techniques, and procedures (TTPs) and Advanced Persistent Threats (APTs) for cybersecurity professionals to be aware of and defend against.

The continuous monitoring of systems and the looming threat of a devastating cyber attack puts a huge amount of pressure on the shoulders of cyber teams.

Coupled with the extreme shortage of talent and skills in the cybersecurity sector, burnout is a growing problem in the industry.

> “
>
> Burnout is particularly prevalent in the cybersecurity industry due to the high stakes and constant pressure professionals face.
>
> Cybersecurity teams often deal with a high volume of threats, tight deadlines, and the ever-present knowledge that a single oversight could lead to significant breaches. The “always-on” nature of the job, coupled with a global shortage of skilled cybersecurity professionals, means many are working long hours under intense scrutiny.
>
> This relentless pace without sufficient downtime can lead to burnout.
>
> **Andrea Succi,** CISO at Ferrari Group

Why burnout is so common in cybersecurity

Increased threats

Threat actors are getting better at attacking organizations which requires constant vigilance–attackers only needto get it right once, meaning security teams must always be on high alert.

Lack of control

Predicting when and how an attack will happen is difficult, creating a lack of control which adds to the stress of cybersecurity roles.

Unrealistic expectations

Stakeholders may not understand the technicalities of cybersecurity, which can lead to unrealistic deadlines and expectations.

Long working hours

Cyber threats are a 24/7 concern, meaning there's plenty of overtime, especially during or after a breach.

Building cyber strength

How to defeat burnout in security teams

Invest in employee career development

Identify areas of passion with your employees and work with them to develop and upskill in these spheres.

Adopt a human-centered approach to cybersecurity

Encourage taking breaks, flexible hours, mental health days, and a supportive culture. Teams should discuss their daily stresses regularly to lighten the load.

Boost employee engagement with CTFs

Provide employees with opportunities to showcase their skills and compete with one another in Capture the Flag (CTF) events.

Make cybersecurity team's lives easier with awareness training

Advocate for good cyber hygiene across your organization with regular training days and showcase best practices.

Invest in employee career development

It's easy to burn out when your career requires you to be "always on" but doesn't provide any opportunities to advance or learn new skills. This is simply exhausting and unsustainable.

Cybersecurity leaders need to take the time to clearly define their employee's goals and work with them to produce development and upskilling programs.

For example, a SOC analyst may want to learn more about penetration testing. So, they could perform a purple team activity with a penetration tester to see how they exploit system weaknesses.

> "
>
> I had the privilege of being able to implement several initiatives to combat burnout. For instance, I encouraged team members to schedule "no meeting" blocks dedicated to deep work or personal time.
>
> I also planned regular check-ins with my team to discuss workloads, motivations, and personal development goals.
>
> These measures had a significant positive impact on team morale and productivity. It's a commitment I believe should be carried out in any approach to team management, reflecting a sustainable and supportive work environment.
>
> **Andrea Succi,** CISO at Ferrari Group

Adopt a human-centered approach to cybersecurity

The following human-centered initiatives can help combat burnout:

- ✓ **Encouraging regular breaks and time off:** Team members need to take regular breaks throughout the day and use their vacation time. This helps to prevent fatigue and maintain productivity.

- ✓ **Promoting professional development:** By investing in the growth and development of team members, we not only enhance their skills but also increase their engagement and job satisfaction.

- ✓ **Implementing flexible work arrangements:** Flexible work schedules can help team members manage their personal and professional responsibilities more effectively, reducing stress.

- ✓ **Fostering a supportive culture:** Creating an environment where team members feel comfortable discussing stress and workload openly can help in identifying burnout symptoms early and addressing them before they escalate.

- ✓ **Leveraging automation and tools:** Automating repetitive tasks and using tools to streamline workflows can significantly reduce the pressure on cybersecurity teams.

Boost employee engagement with CTFs

Providing employees with opportunities to showcase their skills and compete with one another in Capture the Flag (CTF) events can be incredibly rewarding.

Cyber attack readiness report 2023
Lessons from testing 982 corporate teams and 5,117 security professionals with enterprise-grade security challenges.
HACKTHEBOX

In our cyber attack readiness report, more than 70% of managers viewed team events like CTFs as a viable way to boost employee engagement.

Not only is it a great way for cybersecurity teams to bond and practice their career development. But it's also an opportunity for managers to benchmark their team's skills and identify areas for improvement, alleviating the pressures of tackling unknown issues.

Make cybersecurity team's lives easier with awareness training

Human error can add a great deal more stress and vulnerabilities for cybersecurity teams to handle. Something that can lighten the load and help prevent teams from burning out is making cybersecurity awareness training compulsory company-wide. Here are some key ways to encourage good cyber hygiene at your organization:

- ✓ Have password strength requirements and change passwords frequently.
- ✓ Teach your employees to avoid opening suspicious emails.
- ✓ Avoid downloading unknown content.
- ✓ Encourage managers to limit access to data with strict administrative privileges.
- ✓ Make it easy for employees to ask questions and know who to contact with any cybersecurity concerns.
- ✓ Don't push the blame onto users or implement phishing "tests" to catch employees out. Instead, encourage a culture of awareness.

Cybersecurity burnout is a very real and present danger for CISOs and managers. The implications cannot be taken lightly which is why the above initiatives must be baked into your organization's culture. Here are just a few consequences of burnout:

Poor security posture: human error is one of the leading causes of security breaches. Burned-out employees = more mistakes.

Decreased productivity: to keep up with the demands of the job, cybersecurity employees can't be stressed and burnt out.

High turnover: employees who aren't looked after and engaged may seek a role at a company that has better well-being initiatives or less workload. With a talent shortage in cybersecurity, organizations simply can't afford to lose employees.

Legal consequences: if employees make mistakes that lead to data breaches, this could have legal liabilities.

Be a proactive leader and stop burnout before it has serious consequences by investing in your employees and encouraging them to adopt a healthy work-life balance.

Chapter 7:

Why upskilling is the key to retaining top cybersecurity talent

Cybersecurity training has traditionally been very limited. It'll be a one-off event with an external trainer, cramming as much information into one week as possible. This simply isn't effective. Cybersecurity teams require continuous learning that keeps pace with existing threats, supports their career development, and teaches them skills they can apply to real-life scenarios when under immense pressure.

An adaptive approach does a better job of mitigating business risk and boosting security posture. It's also more engaging for security teams, as their upskilling initiatives are making them better at what they do, every single day.

As a result, you retain an elite security team that's primed to perform better because they're highly engaged and upskilled on cutting-edge vulnerabilities.

☒ 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

3 ways continuous learning retains talent

For CISOs and leaders, building an effective retention strategy is key to closing the skills gap and improving security posture. An effective retention plan also demonstrates resilience by ensuring the security team is continuously upskilled, which reassures the board of directors.

By creating a culture of continuous learning, employees will have a higher incentive to stay loyal to your organization, not to mention improved overall performance on the job.

1. Career development and engagement

Breaking into the field of cybersecurity requires plenty of passion and determination. This means that most cybersecurity professionals are eager for opportunities to learn, develop their skills, and grow in their careers.

This has been proven by our research in our cyber attack readiness report. 68% of security team members rated **“opportunities to learn skills”** as the most successful way of staying engaged at work. This placed higher than increasing compensation, demonstrating just how powerful learning can be in retaining your top talent.

Organizations can demonstrate a commitment to the growth of their cybersecurity team by providing continuous upskilling opportunities.

2. Adaption to new threats

New threats are a constant in cybersecurity and teams need to adapt quickly. This can only be done with continuous upskilling, otherwise teams can grow stagnant.

Make use of platforms like Hack The Box, where we release a new Machine every week, often based on the latest common vulnerabilities and exposures (CVEs). This keeps your team consistently on their toes.

Being a performance center for many different companies, we've noticed that the smartest cyber teams get together regularly for upskilling and knowledge sharing.

For example, Toyota security teams participate in Friday CTFs and love the "show and tell" style of learning they've been advocating to their team.

> “
>
> We use the Dedicated Labs instances for CTFs we host every Friday afternoon. It's a fun and casual way for the team to gather and work together to solve challenges - and our favorite way to end the work week!
>
> **Gabe Lawrence,** VP of Information Security Cyber Protection, Toyota

3. Talent retention

By investing in your team's skills, you're not only improving security posture but are also more likely to retain talent over the long term. Demonstrating a commitment to well-being and career development will set your company apart from potential competitors.

Your most talented employees will be headhunted by other organizations, more so with the talent shortage. On top of this, security teams are close to burning out, with Gartner predicting that 25% of cybersecurity leaders will change jobs by 2025 due to stress.

By supporting your current employees with learning and development opportunities, they are less likely to be tempted by other opportunities.

Accelerate your cyber performance with Hack The Box

We provide a human-first platform for creating and maintaining high-performing cybersecurity individuals and organizations.

Risk mitigation:
Timely content offers training on the latest CVEs in real-world environments, reducing risk and exposure to these vulnerabilities.

Employee retention:
Cybersecurity teams that are offered upskilling opportunities are far more engaged and less likely to burn out.

Performance benchmarking:
Conduct CTFs and gap analysis to identify weaknesses in your security posture.

Workforce development:
Align organizational goals to your cybersecurity KPIs with content categorization and report your success metrics to the board.

Tailored training to industry standards:
HTB content is mapped to MITRE ATT&CK and NIST NICE frameworks so you can assess your cyber preparedness in different areas.

Boost organizational awareness:
HTB can assess cyber readiness and performance company-wide with effective practices like tabletop exercises (TTXs) or nearly practical assessments designed for security staff and non-technical teams.

→ Book a call

→ HTB 14 day free trial

How to build a high-performance cyber workforce

HACKTHEBOX

2024