Microsoft

Microsoft Learn

Stay ahead of cyberthreats with security skill-building

Why building security skills across your organization is the key to a resilient future

Table of contents

EXECUTIVE SUMMARY

Defending against cyberthreats starts with your people—empower them to build knowledge and skills with Microsoft Learn

Enabled by decades of evolving technology and groundbreaking innovation, the depth of connectivity that keeps us all linked in this modern digital era has become a catalyst for threat actors to land increasingly sophisticated and costly attacks.

While threat protection has always been critical for every organization, today's security plight has unearthed a fresh sense of urgency, prompting leaders to respond with renewed vigor. Despite growing awareness, many organizations still overlook a critical reality when it comes to implementation: security isn't just a technology issue—it's a human issue. In practice, this means real-time security alerts won't matter if people don't know how to respond to them; the highest-quality security tools won't suffice if people aren't adequately trained on how to use them; and the best-laid plans for a fully staffed security team will fail if people don't feel motivated or supported due to the lack of ongoing learning opportunities and career development.

The global cost of cybercrime is forecast to jump to $23.84 trillion by 2027.[1]

The bottom line: A truly successful security transformation can only be achieved by implementing the right balance of technology investments, security skills, and a learning-first culture.

As a global technology organization, Microsoft has lived this reality, and like many others, we're on a continuous journey of reflection and learning. We've weathered prominent security threats and faced the rapid evolution of the cybersecurity landscape over multiple decades. We've experienced many of the same security challenges as our customers, partners, and countless others, and we recognize the difficulties of building and maintaining security skills in a world where technology never stops changing. Critically, it's this lived experience that has prompted our own restructuring of corporate accountability in an effort to drive change. It's also this experience that informs our belief that every role matters, and every team member must do their part to build a foundation of security skills and knowledge for the future.

Security is everyone's responsibility

The pervasiveness of today's threat landscape points to another sobering reality: a prominent security skills gap impacts all roles, both technical and non-technical, across nearly every industry. Organizations need to rethink how they position security skill-building as a company-wide priority and then elevate that message among team members at every level.

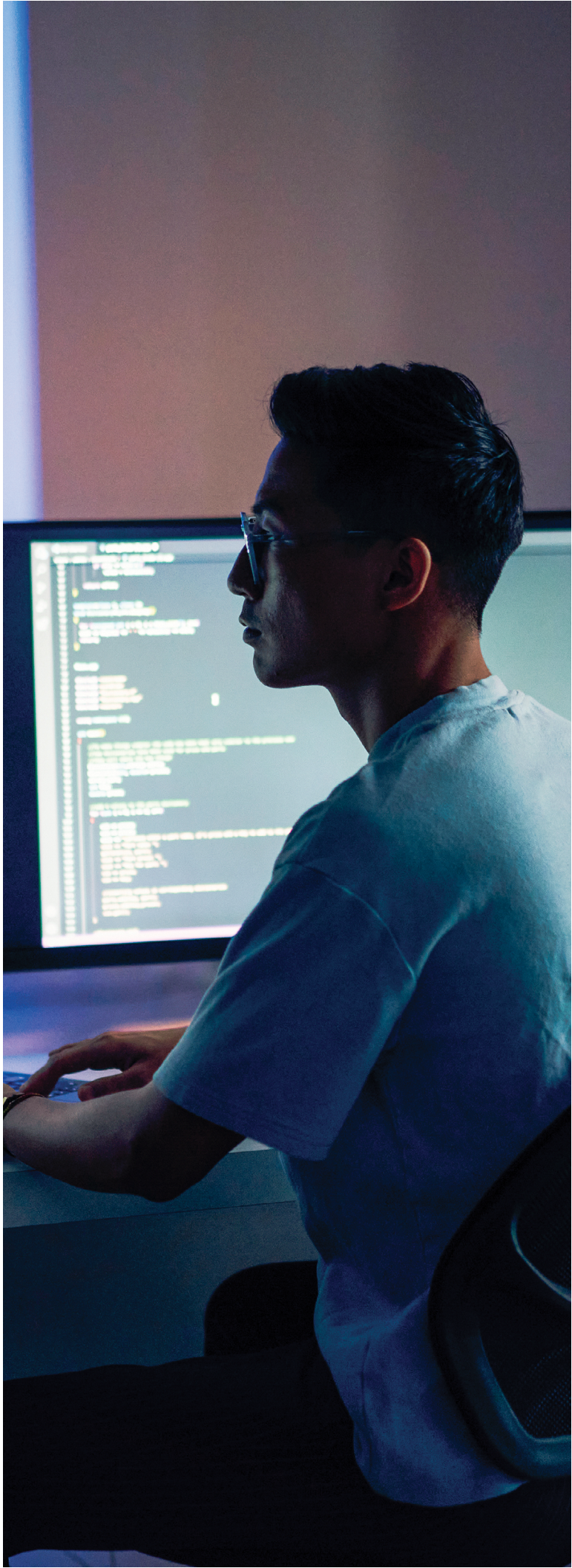
Simply put, it's not enough to focus only on building technical security skills for technical positions. Instead, security skills need to become part of everyone's knowledge base, from leadership to IT to business units—and even end users.

Transforming the security landscape to fight back against modern cyberthreats is a feat no one can accomplish alone. We're here to help. If you're ready to get started, Microsoft Learn has a variety of resources that are not only grounded in the knowledge we've gained from years of supporting our customers and partners, but also carefully designed to benefit users across a wide spectrum of backgrounds, skills, and experiences. Building security skills with Microsoft means laying a foundation that supports continuous learning and fostering a culture in which security is always a collective effort.

Start today with Microsoft Learn, the trusted source to help you build security skills into the fabric of your organization.

Discover how the Security hub on Microsoft Learn can help accelerate your security skill-building journey.

learn.microsoft.com/security



Does your organization have the security skills to defend against growing cyberthreats?

2200
cyberattacks

occur each day, equating to more than 800,000 attacks around the world every year.[1]

76%

of organizations believe security skills are the most difficult technical abilities to recruit for and retain.[2]

Cyberthreats are becoming more sophisticated than ever.

- Now is the time to prioritize security skills.
- Empower your entire organization to prepare, respond, and prevail against an everchanging technology landscape.
- Get started today with the Security hub on Microsoft Learn.

Cybersecurity is a defining challenge for organizations worldwide

Today, digital threats touch every industry and type of organization around the world. It's proof that we're living in a high-stakes era in which technological innovation has become a paradox, acting as both an accelerator of progress toward solving some of the world's most pressing challenges, as well as a carrot for opportunistic threat actors to chase.

We're seeing this scenario manifest in real time all over the world as the frequency, speed, and sophistication of cyberthreats increase, keeping pace with evolving technologies. Consequently, everyone is feeling the impact, and organizations worldwide are navigating transformation on a scale that we haven't collectively experienced before.

Technological change drives new security needs

Our current reality creates some complexities that executive leaders can't afford to overlook—and must instead find new ways to address—as they modernize their systems and integrate new technologies. Take the rapid rise of AI and cloud computing, for example. These technologies, particularly generative AI, have enormous potential to change the security landscape by augmenting the skill, speed, and knowledge of both defenders and attackers. To keep up, organizations must be ready to integrate AI and other technologies into current systems and understand how the subsequent changes will impact their security posture.

Normalizing continuous change

"What we have been experiencing is not a simple one-time change but *the start of an era of continuous changes*. We must assume that business drivers, technology platforms, business models, and security threats will continuously evolve, and build that into our models and perspectives."

Zero Trust Overview and Playbook Introduction[3]

This is prompting leaders to reassess digital readiness and take stock of internal capabilities, particularly around data governance and other AI-driven security measures. It's also leading organizations to consider if their workforces have the knowledge and skills needed to implement current and future security measures to remain vigilant.

The security skills gap is growing

Organizations face tremendous challenges when building security skills. The World Economic Forum reports that the lack of both critical technical skills and soft skills is becoming a significant barrier to success, with 78% of leaders reporting that their organizations lack the in-house skills needed to fully achieve their cybersecurity objectives.[4] The disparity is even more pronounced for small businesses or those that generate lower revenues, like NGOs. In fact, fewer than 15% of NGOs have cybersecurity experts on their staff.[5]

The lack of in-house security skills can be attributed to a slew of factors but based on our conversations with leaders across industries, some of the biggest challenges can be linked to a few common scenarios. First, some organizations might lack the financial resources needed to attract and retain a consistent pipeline of top-tier talent who can bring formalized security training and experience. Instead, they rely on the institutional knowledge of just a few people, elevating the risk of widening the skills gap if one of those few leave and take deep security knowledge with them.

Next, organizations may lack advanced learning resources or dedicated time for ongoing security skills engagement and professional development. In other cases, they're simply not sure how to get started building a security skills strategy as an organization, due in part to a lack of executive sponsorship, concerns over timelines, or the challenge of creating documentation for processes that may not even exist yet.

Regardless of the reason, organizations are left piecemealing their security skill-building efforts together with little consistency. Adding to the dilemma, it seems there's no standardized industry blueprint for recommended security job knowledge, skills, or aptitudes—or even a universally agreed-upon list of roles. Consequently, organizations try to make do with what they have, which often means finding a business team member—perhaps a user education specialist with an interest in security—and teaching them the requisite technical skills. Alternatively, organizations might approach a security team member with the intent to impart education and collaboration skills, hoping that person can help train others. But neither option yields ideal results because the responsibility for understanding and disseminating security skills knowledge rests on the shoulders of too few.

It's not always the budget or personnel setup that holds organizations back from achieving their security goals—it's a cultural disconnect.

Successful security measures hinge on more than meets the eye

It stands to reason that organizations with greater financial resources or those with a robust and clearly defined, highly skilled security team would have the upper hand. Surprisingly, though, it's not always the budget or personnel setup that holds organizations back from achieving their security goals—it's a cultural disconnect.

Even organizations with dedicated IT and security personnel fall into the trap of assuming cybersecurity to be the sole responsibility of the security team, rather than the collective responsibility of the entire organization. A lack of clear organizational messaging and directives for security skill-building leaves personnel searching for their own resources or, worse yet, perpetuates the notion that they don't need to learn any security skills at all.

Failure to portray security skill-building as an organizational priority is a surefire way to compromise all that an organization has worked for. Intentional prioritization and clear messaging around security skill-building, however, can be a tremendous business enabler, ultimately helping teams become more capable and agile when disruptions occur.

78% of leaders report that their organizations lack the in-house skills needed to fully achieve their cybersecurity objectives.[4]

As an organization, navigating these cultural complexities and conversations isn't easy—but it is possible. The responsibility of security should be shared among every person at every level of your organization, and security skill-building should be championed from the top. With a clearly defined path for designated teams, combined with strategic, long-term oversight and consistent messaging at the organizational level, it's very possible for everyone to achieve the requisite level of security skills needed to find success, not only within individual roles, but also as part of a united front. While this process may look different for each organization, the end result is a healthier, more competitive workplace that's primed for a resilient future.

Taking stock of knowledge gaps and learning needs

Reimagining workplace security culture doesn't happen overnight, but with internal alignment and a clear vision, you can begin breaking down silos and creating more opportunity for collaboration and cross-departmental security skill-building. A common route that we've seen prove successful is to take stock of your organizational makeup and determine the types of skills different teams may benefit from learning or expanding.

The breakdown of teams will ultimately look different for each organization, but common groupings might consist of business units, the security team, the IT team, developers, and data specialists. Despite having different accountabilities and dealing with different security-related challenges, it's crucial for these teams to establish an understanding of how to work together to enhance security measures across the organization.

To that end, each team will likely have an established baseline level of security skills and, more importantly, another deeper body of knowledge and skills they need to expand upon—and that's where the real work lies. The expansion and deepening of skills, both security-specific and otherwise, are what will ultimately make each team stronger and better-positioned to collaborate and cross-train, as they'll be establishing skills that other teams can learn from.

Here's what the breakdown of accountabilities and skills might look like for each of those teams:

Business units: The business units within your organization are already well-acquainted with maintaining oversight and decision-making across support functions. The people in executive or C-suite roles, in particular, are also likely accustomed to consulting with other business support functions to help them make informed decisions based on expert information. Like most others, business unit leaders understand that security matters to the health of the business, but the missing link is often a recognition of their own degree of accountability.

Skills to expand: Like all team members, your business unit leaders should understand and embrace the reality that security is an intrinsic part of their jobs. As the risk owners within their respective areas, business unit leaders don't need to possess deep technical knowledge or acute skills across tools and security systems—but they do need to be informed about the breadth of risk and the methods attackers might use. Whether it's phishing emails or fake expense approval requests, business unit leaders need to be able to spot suspicious activity and take immediate steps to remedy the situation. And when it comes to decisions around your organization's security systems, tools, and overall posture, C-suite leaders should regularly consult with security experts in much the same manner they would with finance during an acquisition or media relations during a major release.

Lastly, if your organization's customer-facing field teams have security solutions in their portfolio, it's essential that they understand how to effectively use those solutions and are able to impart sufficient instruction to end users. This may seem like a given, but the reality is that it doesn't always happen—and your solutions are only as effective as the accuracy with which they're being used.

Business units should be prepared to:

- ✓ Spot suspicious activity such as phishing emails
- ✓ Consult with security experts to find solutions
- ✓ Impart security information to end users

Security team: It's safe to assume that most security teams already have the knowledge and skills to understand the methods attackers use, the tools needed to mitigate risk, and the steps to quickly act on threats. Naturally, your organization's security team will have greater technical aptitudes and agility than most other teams when it comes to using security tools and systems. However, they might not always feel prepared to step outside of their siloed security roles and connect with other teams in ways that facilitate cross-functional collaboration and learning.

Skills to expand: The security team is the guardian of critically important knowledge, and no organization can afford to keep this information siloed. Just like other teams need to embrace accountability, so too does your security team—but in a different capacity.

The security role job description needs to undergo a fundamental shift toward collaboration and knowledge sharing. With the increasing speed and sophistication of attacks, your security team needs all the support they can get in the form of organization-wide due diligence. They must be prepared to help make that happen by effectively advising and collaborating with other teams. Conducting regular, proactive risk assessments and inviting other teams to the table, especially developers and data specialists, can be an effective way to start.

Part of this process is recognizing that there's a human element to security, and it takes more than technological know-how to make security a consistent, efficient function of the organization. Understanding what others know and don't know about security and learning how to impart security knowledge in a way that will resonate with different teams will help that process unfold more smoothly.

Security teams should be prepared to:

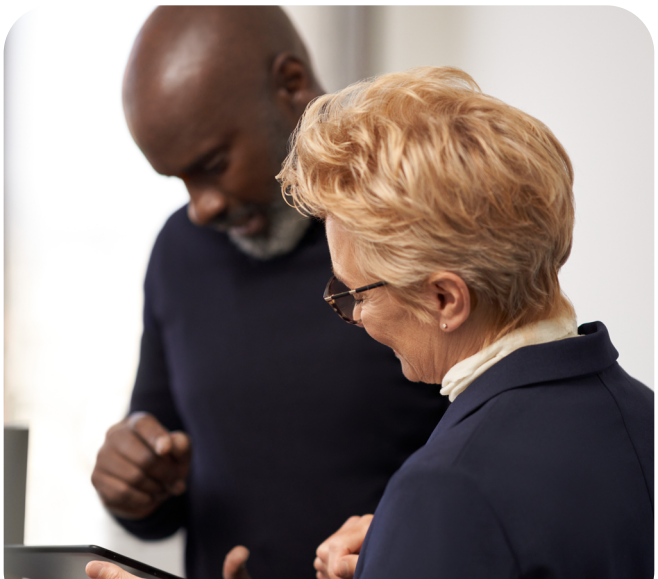
- Advise and collaborate with other teams
- Include developers and data specialists in regular risk assessments
- Understand the human element that makes security a complex responsibility

IT team: As the owners of technology system implementation and maintenance, your organization's IT team likely has more security-related knowledge than some others. Often, though, that knowledge isn't broad or deep enough to form the basis of an effective security strategy, nor is it sufficiently funded to evolve into a transferable skillset.

Skills to expand: One of the most important facets of security for your IT team to embrace is knowing how their roles impact the organization's overall security mission—and that often involves working closely with the security team. That said, it's not unusual to witness some friction between these two teams. They're both responsible for critically important functions that keep the organization operating every day. They both have to regularly navigate stressful scenarios that are taxing for even the most experienced teams, and duties often intersect during high-stakes events like major system upgrades or installations. Yet neither team can reach its full potential without support from the other. In fact, some organizations might house IT roles and security roles within the same team, making it all the more critical to establish consistent communication and collaboration and to understand each other's priorities.

Consider the process of patching and rebooting servers, for example. While an IT team will never just hand over these duties, they should consult with and listen to the security team about what's most important to patch first versus what can wait. With this information the IT team can better determine how to implement patches based on the existing schedule, which will save them time in the long run.

Like other teams across the organization, the IT team should be familiar with the attack techniques used by threat actors, but with increased awareness around how those techniques impact the assets they manage. Whether it's servers, identities, or devices at stake, your IT team should be familiar with where compromises might occur and the subsequent actions to take.



IT teams should be prepared to:

- Understand how their roles impact the organization's security posture
- Seek input from the security team before executing updates
- Understand threat techniques specific to the assets they manage

Developers: Software developers are skilled when it comes to designing with purpose and building for speed and reliability. Most are aware they need to deliver secure code, but they often don't connect with the security team until the code is already written, and by the time security runs checks and provides feedback, developers may have already moved on to another task.

Skills to expand: One of the most critical security skills your developers can possess isn't a hard skill, so much as it is a *mindset*. Security is an element that should underpin the end-to-end development process, rather than serve as a box that gets checked at the beginning or just before a product heads out the door. When developers account for and successfully integrate security at each stage of design, they effectively make the design process itself more secure.

Collaborating with the security team earlier in the design timeline can also help developers ensure they don't waste time and effort on redesigns or rewrites that could have been ironed out sooner. Effective collaboration can also help developers better understand the security team's metrics for success and what they're looking for when reviewing code. Plus, collaborative thinking can help developers ideate around the ways in which an app could be used in unintended—perhaps nefarious—ways, and design more securely with that in mind.

Developers should be prepared to:

- ✓ Reframe their mindset around security as an end-to-end development must-have
- ✓ Seek input from the security team early in the process
- ✓ Understand how threat actors might infiltrate the apps they develop

Data specialists: Your data team enables effective use of data throughout the organization and advises on the storage and analysis tools that provide the most value. As organizations increasingly implement AI-driven security measures, data specialists have a more prominent role to play in fortifying the overall security posture.

Skills to expand: Like developers, data specialists should be mindful when it comes to security as an end-to-end component of the organization's data storage and analysis pipeline, as well as throughout all other tools, methods, systems, and actions they implement. This can happen, in part, by understanding which of the organization's security policies directly impact data use, such as encryption, access controls, and compliance requirements. Like others, data specialists should be aware of the methods threat actors use to infiltrate the organization's data security layer and know immediate steps to take in the event of a data breach. Better yet, data specialists and security teams can work together to develop data-specific components of an organizational incident response plan.

Data specialists should be prepared to:

- ✓ Frame security as an end-to-end component of the data pipeline
- ✓ Understand security policies that impact data use
- ✓ Work with the security team to develop a data-specific incident response plan

Thinking through the breakdown of what different teams need to learn can help shape strategic skill-building plans and provide much-needed perspective into the daily challenges each team faces. But it's not enough to send teams down a new learning path without understanding and adequately conveying why it's necessary for security skills to be integrated into every role across the organization. And that's where it pays for leadership to present a united front and maintain consistent communication around security as an organizational priority.

Changing the conversation from the top-down

For most of us, security is an aspect of daily life—even apart from technology—and we do our best to be diligent despite busy schedules and seemingly nonstop distractions. At times, though, we're all guilty of security mishaps. Maybe it's forgetting to lock the door. Plenty of us have failed to close a window. And how many of us have driven away with the garage door wide open, bicycles and expensive tools exposed to the whole neighborhood? If that's you, you're very likely not alone.

When these things happen, it's often a kind and observant neighbor or, more often than not, sheer luck that saves us from losing valuables. But when it comes to securing business technology, organizations can't afford to rely on the goodwill of one team to consistently amend the oversights of another—or try their luck.

Instead, organizations need to make sure each team is equipped with not only security knowledge and skills, but also ongoing awareness to drive continuous engagement and learning when needs change. With better awareness of what security threats are out there comes better understanding of how those threats might change and manifest, along with potential implications to the organization and its people.

When people have a clearer view of the big picture, they see where they fit in and why their contribution is necessary. A culture of collaboration and support is what elevates that viewpoint and empowers people to weave security into their everyday tasks, from the documents they create and the messages they send to the devices they use and the identities they log in with.

All of these factors help mitigate risk and drive success at an organizational level every day. When an organization is healthy and secure, the organization *and* its people have greater opportunities and become more resilient. Once people embrace this understanding and possess the skills to back it up, they can be more effective in helping others learn the same.

> **When an organization is healthy and secure, the organization *and* its people have greater opportunities and become more resilient.**

Tactical questions help build an organizational strategy

A security strategy will always be most effective when everyone does their part to contribute to the collective wellbeing of the organization, its people, and its customers. For many leaders, changing the culture and the conversation around security skills is one of the hardest parts. Once the journey is underway, leaders can focus on assessing the more tactical pieces of the puzzle that can help build an organizational strategy.

You can start by asking a few key questions

- What learning tools do we currently use to impart security knowledge and help people build skills? Have we received feedback on these tools?
- What communications or documentation do we rely on to inform people about learning strategies and priorities? When was the last time we reviewed our messaging?
- What can a technology partner bring to the table?

Researching these and other questions might take a bit of time, but the answers will help you formulate a more structured approach and consistent messaging around building security skills as an organizational priority.

Key takeaways can help you stay the course

The security skills programs you put in place are only as strong as your organization's ability and willingness to follow through with them—but there are some key takeaways that can help you, as leaders, set the stage for success.

- Don't try to do everything all at once. Instead, ruthlessly prioritize based on your highest-value security needs. You can chip away at the rest.
- Security skill-building will always need to remain a priority, but you can balance the effort by making a long-term learning plan that your organization can work toward in parallel. It doesn't have to be an all-or-nothing venture.
- Accept that this process is a journey and recognize that yours might look different from other organizations.
- Know that your plans will always change, because attackers' plans will always change, too.
- Remember that these transformations are about people as much as they are about technology.

Getting started

Empowered with powerful tools, resources, and support, every team member has the potential to contribute to a more secure and resilient workplace. Taking the next steps to fulfill that potential are within reach.

As you develop your organizational approach to security skill-building, we encourage you to visit our Security hub on Microsoft Learn. Find technical guidance and resources on planning and implementing modern cybersecurity strategy, architecture, processes, and technology. Help your teams build advanced cybersecurity skills and certifications, or offer learning opportunities that help new and aspiring security professionals build their knowledge base.

No matter where you are in your security skill-building journey, Microsoft Learn is ready to meet you there.

Explore the Security hub on Microsoft Learn

learn.microsoft.com/security

Endnotes

[1]World Economic Forum, 2023 was a big year for cybercrime – here's how we can make our systems safer, January 2024.

[2]IDC InfoBrief, sponsored by Microsoft, Skilling Up! Leveraging Full and Micro-Credentials for Optimal Skilling Solutions, doc #US52019124, June 2024.

[3]Mark Simos and Nikhil Kumar, Zero Trust Overview and Playbook Introduction, October 2023.

[4]World Economic Forum, Global Cybersecurity Outlook 2024: Insight Report, January 2024.

[5]Microsoft, Microsoft Digital Defense Report, October 2023.