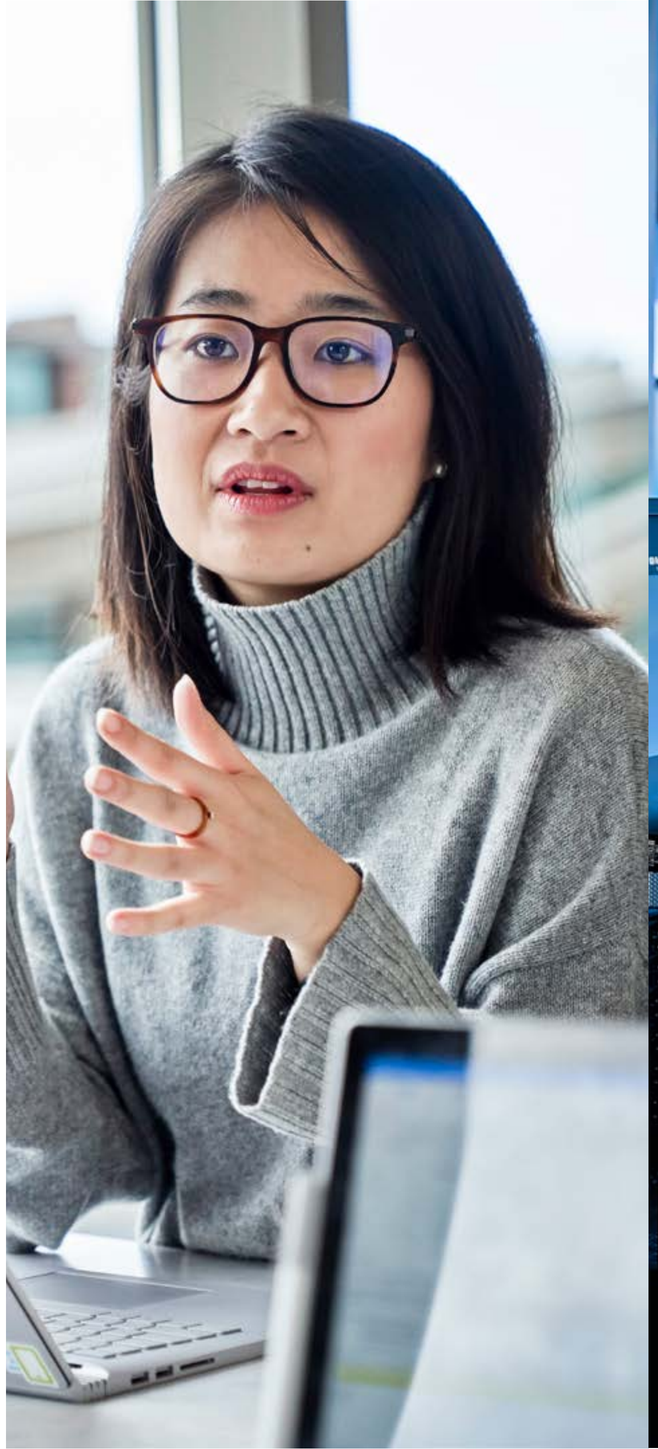
Microsoft

CISO essentials: How to optimize recruiting while strengthening cybersecurity



As a CISO, you face the double challenge of proliferating threats coupled with a shortage of trained and qualified cybersecurity talent. The need for security experts is increasing, but demand is far outstripping supply.

3.5 million

unfilled positions in the security industry by 2021

According to the 2017 Global Information Security Workforce Study, two-thirds of organizations surveyed lacked the number of cybersecurity professionals needed in today's threat climate. More recently, Cybersecurity Ventures estimates the number of unfilled positions in the security industry will be as high as 3.5 million by 2021.

How do you address your organization's talent gap in the short term and long term? What are the tasks that technology can take on to help a short-staffed organization? Which personality or workstyle traits are the best fit for working in the field of AI and automation? What shifts should you make in managing cybersecurity talent in order to increase the retention of the staff you do have?

The answers to these questions lie in taking a parallel, multi-pronged view of both human talent and intelligent technology. It's time to think creatively about who and how you hire. At the same time, consider how intelligent technology can take on the common, fatigue-inducing alert and response tasks in security operations. Read on for four ways to search and recruit beyond the usual suspects, plus four ways to reduce pressure with AI.

4 ways to optimize cybersecurity recruiting

Tech and security needs have changed, and your recruiting practices should, too. To address today's cybersecurity threats effectively, you need more than IT skills. Prior industry experience or a computer science degree are no longer the only indicators of potential. High demand for "white hats" means you have to look beyond the usual STEM suspects: a candidate with a largely self-taught background, or whose résumé shows a history of creative problem-solving and teamwork, could be your greatest hire.

Our industry has a branding issue... the cybersecurity profession isn't about the lone hacker, but the team of white knights—every nation, business, or individual is protected by the work we do in cybersecurity and intelligence. We improve people's lives and keep them safe.

Theresa Payton,
CEO and Chief Advisor,
Fortalice Solutions

01.

Broaden inclusion and diversity efforts

The tech industry has a history of issues when it comes to diversity in the workplace, and lack of inclusive hiring is part of the reason for the talent gap now. For example, there's a shortage of women in cybersecurity, but there's no shortage of talented women workers. To hire effectively among all genders, and especially women, recruiters need to rebrand the work. Cybersecurity and intelligence jobs are less about counter-hacking and more about being passionate about improving people's lives and safeguarding livelihoods. Less "Wargames" and more "Avengers," if you like.

Direct your recruiters to tailor their search and outreach efforts to demographic groups that are underrepresented in technology, such as women, people of color, and LGBTQ+ people. Look beyond academia and traditional staffing agencies. Organizations such as the Security Advisor Alliance, a nonprofit dedicated to supporting and diversifying the cybersecurity industry, can help you get started. And check out the many networking groups on LinkedIn, including "Help a Sister Up," which was created specifically to empower women in cybersecurity.

Also, don't overlook the opportunities in **generational recruiting**. Gen Xers and Boomers in IT can bring their technical savvy to cybersecurity, plus the pragmatism that comes from decades in a constantly evolving industry. Experience, insights, and leadership are especially valuable in breach response and remediation roles. Networking and industry events are good ways to reach Millennial candidates. And for the long term, pay attention to K-12 and collegiate cyber competitions and clubs. Companies are increasingly identifying young talent and introducing them to opportunities in the cybersecurity field.

Our teams need to be as diverse as the problems we are trying to solve. We need to be much more inclusive as an industry and go out and recruit through non-traditional channels.

Ann Johnson,
Microsoft Corporate Vice President,
Cybersecurity Solutions Group

02.

Speak the language of veterans

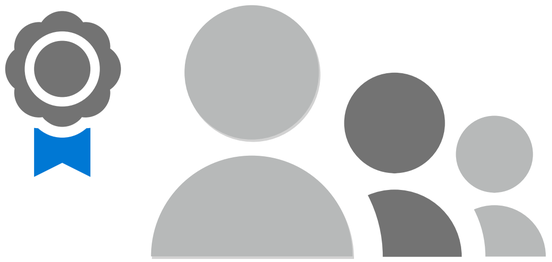
Traits that are strengths in technology—self-motivation, trainability, problem-solving—are hiding in plain sight among our military veterans. In fact, it's hard to imagine another group as primed for the protect-detect-respond needs of enterprise security.

But while there are many veterans with the necessary skills, civilian recruiters often miss them. A veteran's résumé can read like a foreign language, full of military jargon and very specific work contexts that don't easily map to civilian requirements. At the same time, private industry job descriptions don't resonate with ex-military job seekers who are trying to figure out if a role is a good fit.

Recruiters in this space must remember that military service trains people to work cohesively in units. Interviewers must be aware that former soldiers (or Air Force, Navy, Marines, or National Guard veterans) may not be used to taking individual credit for accomplishments or promoting themselves. Consider holding recruiting events at military bases when people are demobilizing. This is a good way to find candidates and learn how to put their recent military experience into your retraining plans. And target areas with Cyber Command units, such as Florida for the Navy and Georgia for the Army.

As with Millennials, veterans' work and communication styles can appear somewhat different from what private industry is used to. Military people tend to have a high regard for leadership, so you'll want to make sure your management teams are encouraging and supporting these different styles, and workers who may approach problem-solving from different angles (a key advantage when assessing threats and vulnerabilities). Also, think about how your organization values security operations, because it will be difficult to retain veterans in environments where this is not considered essential work.

Microsoft actively supports the recruitment of veterans into technology roles. The Microsoft Software & Systems Academy, which provides transitioning service members and veterans with critical career skills, is a good starting point to learn more.



Recruiters need to stop only looking for candidates who check all the skill boxes on a list. You can train anyone to use tools. It takes longer to train people how to adapt and think and problem-solve. Veterans have these skills in spades, and they are highly trainable.

Ryen Macababbad,
Program Manager,
Microsoft Defender ATP (MDATP)

03.

Consider more neurodiverse candidates

Microsoft works actively to better identify and tap neurodiverse talent. The tech industry leads in hiring neurodiverse candidates because many people on the autism spectrum or who have dyslexia are often orthogonal problem solvers, with the ability to focus intensely. Plus, neurodiversity often correlates with an interest in STEM fields.

Despite industry recognition that neurodiverse people are uniquely suited to technology work, this demographic remains largely underemployed. Neurodiverse candidates are often at a disadvantage in interviews and social situations, and thus their unique skills go untapped. To ease these barriers, you will have to think creatively about the terms and criteria your recruiters and managers use to evaluate candidates for cybersecurity roles.

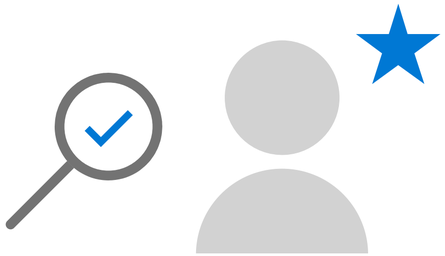
> **Repeatedly overlooked is that people with autism… often have wonderful cognitive abilities when it comes to logic, pattern recognition, precision, and concentration.**

Richard Branson,
Founder of Virgin Group

04.

Locate the white hats in your organization

Last but not least, don't forget the high-value employees within your organization. Your HR department should be able to help you identify, incentivize, and retrain experienced workers who are already vested in the company and who may be eager to reskill in similar or related roles.



Optimize search

- DO go beyond traditional keyword-search recruiting. Look for candidates in diverse contexts and learn to use the terminology that these different groups can recognize.
- DO remember that your organization can teach new tools to anyone who is trained to learn. Look for aptitude for learning and creative problem-solving over specific job experiences, especially among veterans.
- DON'T miss good candidates by trying to fit every possible skill or tool or desired background into an SEO-based requisition.

Theresa Payton, former White House CIO, recommends looking for candidates in **adjacent professions and knowledge areas**, such as forensic science, law enforcement, sociology, and psychology. Professionals from these fields already have the investigative training—and the mindset—to profile the behaviors of threat actors. Their skills can help train AI to respond appropriately in broader contexts, beyond the current profile of cybersecurity professionals.

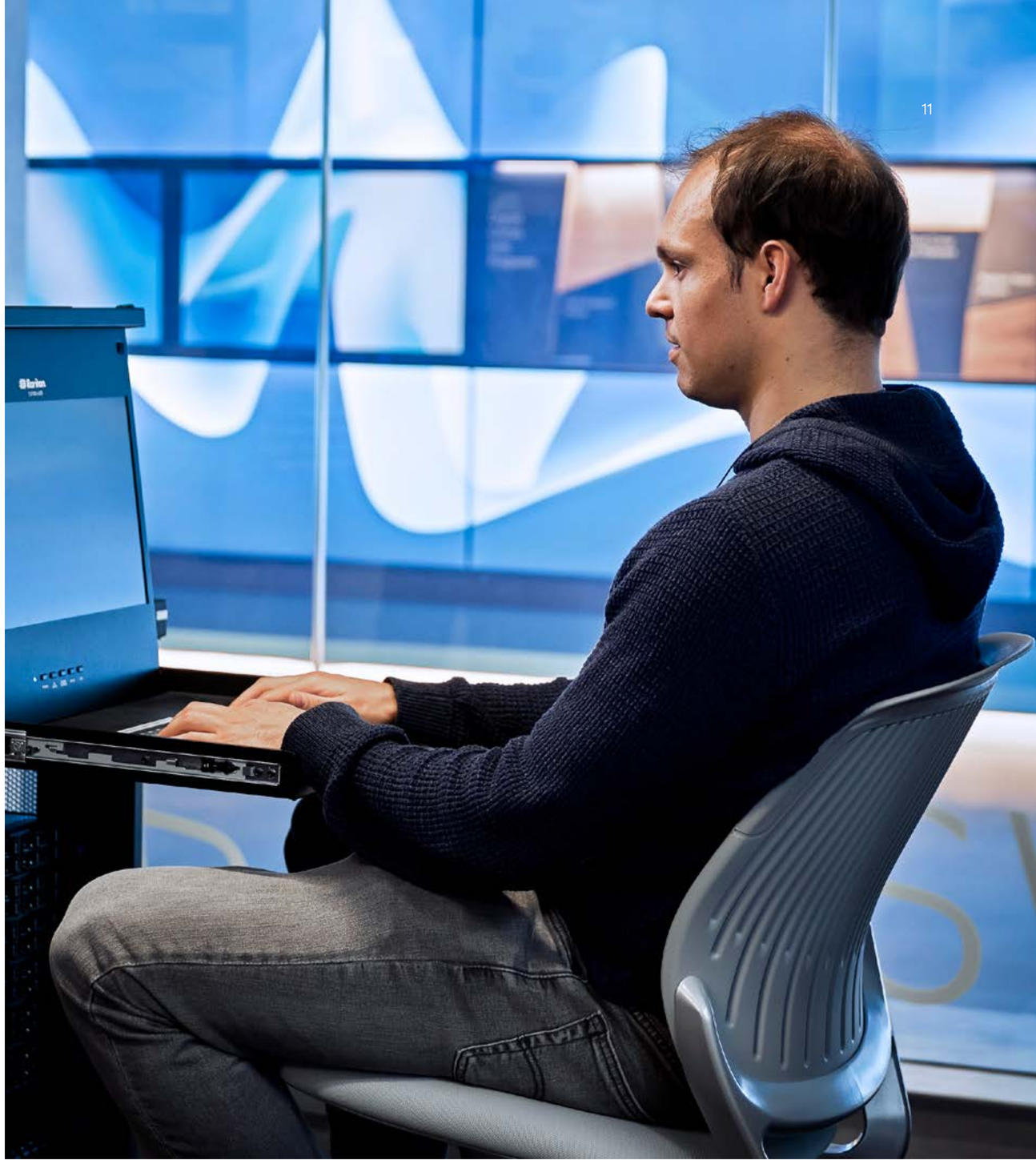
Once you start making associations of skills from other job pools, you can attract broader talent pools generally. Consider hosting meetups externally and brown bags internally so that practitioners are training and coaching each other. Networking and sharing knowledge is an important part of preventing and mitigating serious incidents.

I can find great technical talent that can take care of measuring clients against a check list or compliance framework, but I cannot wire the human to have a compass that's due north, [who has] a desire to passionately protect and defend and go beyond that checklist. If you see that in somebody, you can train them on cybersecurity.

Theresa Payton,
President & CEO,
Fortalice Solutions

4 ways that AI can help you mind the talent gap

While one of the main points of this e-book is that it takes the right combination of people and solutions to enable successful security operations. However, intelligent technology is well-suited to taking on the more repetitive tasks in security, such as noise monitoring and low-level event handling. Think about automation in terms of the security objectives so that human analysts can investigate and remediate complex issues. Here are four areas where AI can help strengthen your security posture.



01.

Threat signal analysis

AI security technology can provide comprehensive, interactive visualizations of attacks and automate responses with security orchestration. For example, Microsoft Azure Sentinel uses dynamic analytics to help you investigate suspicious activities.

You cannot ‘out-hire’ the threats. With that kind of [talent] gap, with all of our training programs and education, it’s still not going to be enough.

Valecia Maclin,
General Manager Engineering,
Customer Security & Trust, Microsoft

> **[We're facing] a 3 million-person shortage in the next two years. That is a huge shortage.**

Ann Johnson,
Microsoft Corporate Vice President,
Cybersecurity Solutions Group

02.

Real-time policy decisions

Automating access decisions based on current risk conditions provides a 24/7 layer of defense to the whole digital estate. First you set the categories and conditions of access in Azure Active Directory (AD) conditional access controls. And then AI in Azure AD determines whether to allow or block access to cloud and on-premises resources in real time, proactively reducing risk.

03.

Automatic investigation and remediation

AI can perform real-time assessments and protect against common threats. Microsoft Defender ATP for example, includes intelligent automation to isolate programs running in browsers from browser-based attacks.

04.

Cloud-driven attack surface reduction

AI can help reduce attack surfaces and assess the impact of individual controls so that you don't have to decide between productivity and locking down environments to secure them. Azure Firewall has the specific ability to update its list of blocked IP addresses based on real-time data feeds powered by the Intelligent Security Graph.

From identifying incoming threats, to optimizing ongoing operations, to recovering from an attack, AI can and should play a part in expanding your security capabilities and using the human element of your cyber defenses most effectively. Also keep in mind possibilities of AI and security will no doubt expand as innovation accelerates and current technologies mature. All the more reason to lay a strong foundation now.

Read the Microsoft Security Intelligence Report

Use real-world insights to help close the security talent gap

Read the report

If you're a CISO faced with complex security needs and too few white hats, it's time to rethink who and how you hire—and how to optimize intelligent technology to hold the line while you reinforce talent. Remember, cultural fit is more important than technical background. Security operations groups need creative problem solvers with a desire to protect, detect, and defend, no matter their age, neurological background, gender, or other identification. By rethinking your approach, you can help develop a diverse, talented staff who can protect, detect, and respond effectively to today's cyberthreats.

Get up to speed on the top trends in the threat landscape.

Visit Microsoft Security >