Secureworks®

WHITE PAPER

The Challenges of Hiring as Cybersecurity Evolves

Identifying Hurdles in Cybersecurity Talent Acquisition

The scope of security has rapidly expanded in recent years to address an evolving threat landscape, digital transformation initiatives, remote work, and mobile computing. These changes have created major challenges for hiring managers. The skills required to manage security environments have grown faster than the number of people who can do those tasks. An additional 4 million professionals are needed to close the gap, according to one estimate.[1]

The skills gap isn't just a supply issue. Security managers can't wish an elite pool of qualified professionals into existence – the impetus for that comes from outside organizations. But managers can make their company more attractive to talent. The hiring landscape is competitive and if your organization is not telling a good story to jobseekers, it's unlikely you'll attract the best talent. On top of that, some hiring managers are still hiring for what was needed four years ago. This is a bad sign in an industry that changes as rapidly as ours. As security continues to evolve, consider the following hiring challenges you'll likely need to navigate to succeed.

Job candidates can infer a lot about your company from a simple job posting. More than half of cybersecurity professionals surveyed said that a lack of clarity in a job description implied the organization lacked understanding of security.

A Competitive Job Market

Not every company is a multinational corporation with wide name recognition able to attract the top talent by name alone. Most organizations compete with their peers for a smaller talent pool and struggle to stand out. It may seem like other companies have more attractive security operations or are in a more interesting industry for security talent. In some cases, the other companies hiring are based in locations with a larger talent pool and amenities that make them more appealing to job hunters.

Every job and organization offer a unique set of challenges to security professionals. Hiring good security professionals requires communicating those challenges and opportunities in a compelling and engaging way. Some of your peers may face the same challenges you do, but if they are hiring successfully then they are probably telling a more attractive story. Job candidates can infer a lot about your company from a simple job posting. More than half of cybersecurity professionals surveyed said that a lack of clarity in a job description implied the organization lacked understanding of security.[2] This is not a position you want your company to be in when the demand for talent far exceeds the supply. Accurately marketing your organization plays a large role in the hiring process today.

A competitive job market is also one of the reasons that many security professionals change jobs regularly. While higher salaries can be motivating factors, talented security analysts are in high demand, and naturally gravitate toward organizations that offer a wider narrative and purpose. A good story about the position and company can encourage employees to join a company and stay for longer too. For some organizations, offering remote work flexibility can also help broaden the potential job candidates beyond those in a limited geographical area.

[1] (ISC)², (ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide

[2] (ISC)², Hiring and Retaining Top Cybersecurity Talent

Constant Industry Change

Security changes quickly and can take organizations by surprise. In the last five years alone, different tools and solutions have proliferated at a rapid pace. For many companies, some of the hires they made a few years ago no longer fit the program. Additionally, organizations sometimes struggle to understand what the next five years could hold for their organization, and what that means for how to hire the right people.

When a gap opens up in your team, you could start by assessing whether filling it directly makes sense for your future strategy. Many of the functions in security are changing or disappearing as technology enables teams to focus less on triage and platform management, and more on finding threats. The future of security looks different for many organizations and this impacts who you should hire. As things like security analytics technology spread, some organizations are placing a greater value on employees understanding security fundamentals.

Generally, it's easier for someone who understands security fundamentals to learn a tool than it is for someone who knows a tool to learn the security basics.

An Abundance of Specialists

Organizations with limited resources can struggle to get the balance between hiring specialists or generalists for their operation. The need for specialists is clearer in large corporations with big security programs, but for many smaller companies, this isn't the case. In recent years, popular tools have required full-time management. Many companies will hire employees who specialize in operating a tool. This works if the individual understands security principles and can grow with the security program. However, if that employee doesn't know security fundamentals and your needs evolve, that could leave you with a gap.

Companies should decide what their needs are. Generally, it's easier for someone who understands security fundamentals to learn a tool than it is for someone who knows a tool to learn the security basics. Another factor hiring managers should consider is the role of vendors in their program. Vendors are often staffed with some of the world's best specialists. If your vendor has a great incident response (IR) team, for example, maybe you don't need someone with deep IR experience on your own team.

Some advanced vendor technologies also make it easier for analysts to carry out previously specialized tasks. This often broadens the scope of the job, which is better suited to security generalists. Specialists are often also harder to hire and keep as they need to be stimulated by their work, otherwise they're liable to leave for a new challenge. Whatever the right balance between generalists and specialists for your organization, you'll need separate strategies for keeping each kind of employee happy and challenged in their job.

Reactive Hiring

Business moves quickly and security needs to keep up. This presents significant challenges when hiring. Organizations frequently post a position online and wait for the applications to come in. It can take weeks or months before somebody is hired, depending on the processes at a company. One survey revealed that on average, it took 3.5 months to hire a SOC analyst with an additional 3.8 months to train the new hire.[3] More time will pass before the new hire adjusts fully to your security environment and program. Where will the business be by then? This is one of the ways security falls behind the speed of the business.

Some organizations are changing their hiring practices to keep up. The best-prepared companies learn to treat business approval for new hires as a box-ticking process once everything else is in place. Hiring managers for these enterprises have a stack of resumes to reference whenever it looks like a job will open up. Certain managers use social media as another channel for hiring. Many security professionals cultivate a following across social media by sharing expertise. Top security managers follow people they think would be a good fit, then use social media to send messages when they know of a coming vacant position. Social media can also function as a way for security leaders to promote themselves, their security operation, and their organization to make it attractive and visible to potential employees.

The best-prepared companies learn to treat business approval for new hires as a box-ticking process once everything else is in place.

Poor Retention

The next challenge after hiring someone is keeping them. Turnover can be high in security, with analysts moving on if they feel unchallenged or burnt out. On average, organizations may see around three SOC analysts fired or resigned in one year.[4] This is partly a result of the industry direction in the last five to ten years. Many security environments and tools now require significant management and administration, all while bombarding analysts with a high level of low fidelity alerts. Analysts often feel they don't get enough time to do the things they enjoy, such as incident investigation.

Some jobs provide a narrow focus to security professionals which can lead to boredom. Most analysts want to learn new skills, but some jobs don't offer enough growth or career development opportunities. An (ISC)^2 study revealed that 81% of cybersecurity professionals anticipated needing to obtain additional certifications or training as they prepare for future roles.[5] In organizations where retention is good, there is usually a clear path for future development that each employee can work toward. Companies may also benefit by investing in analyst training or certifications. Analysts will get to grow their skill set, which can lead to better job satisfaction and a more talented team. Security leaders who include employee retention in their strategy will see benefits both to their security posture as well as employee morale.

[3] Ponemon Institute, The Economics of Security Operations Centers: What is the True Cost for Effective Results?

[4] Ponemon Institute, The Economics of Security Operations Centers: What is the True Cost for Effective Results?

[5] (ISC)^2, Strategies for Building and Growing Strong Cybersecurity Teams

Smaller security operations are more limited in their options when it comes to developing staff. Many use vendor expertise as a way to help staff learn on the job, and some security teams use newer tools like software that can reduce noise, and enable teams to spend more time on investigation, detection, and response tasks.

Hiring for the Right Skills

Security tools keep getting better, but despite widespread hype, very few modern solutions are turnkey. Most require some input from the security team, and often that means programming. These skills help your team write, or tweak, countermeasures as needed. C and C++ languages are useful for malware analysis, while Python is often used to execute and automate tasks.

Although soft skills are not always associated with cybersecurity, the future of security is looking more consultative and collaborative than before. As software and technology remove some of the burdens of traditional analyst work, your team may find themselves increasingly speaking to vendors to validate conclusions, question response actions, or to flag and discuss concerns. This evolved analyst role requires the ability to work well with others on a broader range of activities than before.

As software and technology remove some of the burdens of traditional analyst work, your team may find themselves increasingly speaking to vendors to validate conclusions, question response actions, or to flag and discuss concerns.

You'll probably also need to identify who on your team is good at assessing vendors. If that person is a busy analyst, you may need to allow them time to critically assess the options for the solutions you need. While this doesn't necessarily require people skills, they are beneficial if you want the analyst to also make vendor contact to discuss potential solutions.

Prepare for the Future of Security

The threat landscape is constantly changing, and with it comes new security solutions and ways of operating. As software and AI take over repetitive analyst tasks, the range of tasks staff perform will likely broaden. This trend will also benefit security generalists, who understand security principles and can apply them from event analysis through to incident response. Software and technology will enable security teams to do tasks that would have been too difficult before. Because security evolves quickly, hiring just for what you need today can cause problems in the medium term.

The market for top security talent is still tough for most organizations. Finding the best person for the job requires a proactive hiring approach and an ability to distinguish your organization from the competition. Hiring and retention strategies should be a key part of any security program. With a plan in place, you can mitigate challenges of finding and keeping gifted security professionals.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp

Availability varies by region.