PLEXTRAC EBOOK

Your Guide to Tackling the Cybersecurity Talent Shortage

Attract and retain top talent, even in today's competitive market.

PlexTrac®

Table of Contents

A Crisis Moment for Cybersecurity Hiring

The cybersecurity industry is, in a word, booming. Demand for increased protection against bad actors online has been growing stronger, and thanks to the COVID-19 crisis spurring a spike in eCommerce and remote work, the job market for information security analysts, pentesters, and hackers has never been better.

The open positions are plentiful, the pay is good, and the necessary training has never been more accessible. And yet, despite all of this, security team leaders and hiring managers across the country are asking the same question:

Where on earth is the qualified talent?

In 2021,
68.5%
of businesses worldwide suffered a ransomware attack

State of the Industry

The demand for cybersecurity professionals has never been higher.

As commerce, industry, and infrastructure become more reliant on online operations, the threat of cybercrime has increased in tandem. In 2021, 68.5 percent of businesses worldwide suffered a ransomware attack, and phishing attacks resulted in an economic loss of $17,700 per minute.

Additionally, economic and technological weaknesses exposed by the chaos of the COVID-19 pandemic have ensured that cybersecurity will be a priority across many industries in the coming years. As the economic risk of cybercrime becomes more apparent, company owners, shareholders, and insurance companies are demanding increased security measures. Burning Glass' ***"After the Storm"*** 2021 report projects that the need for workers in the "Readiness Economy," such as cybersecurity and IT, will grow at double the average rate in the coming years.

As the demand for cybersecurity professionals has mounted over the past decade, it is becoming more clear that the labor supply has not matched the pace. According to CyberSeek, in a 12 month period in 2021-22, there was a talent shortfall of nearly 25,000 workers for information security analyst positions alone. Employers are struggling to find qualified employees for their security teams — so much so that cybersecurity vacancies take 21 percent longer to fill than other IT openings.

The Great Resignation of 2022 complicates matters still further. Employees hold more power over their destiny than they have in decades: With a shortage of labor in nearly every industry, workers are able to dictate their own terms. The rise of work from home, assisted by Zoom, Slack, and a host of other technologies, enables them to find employment anywhere, not just in their immediate location. This situation increases the number of companies competing for the same small talent pool.

The combination of competitive pay offerings and a rise in inflation means that workers are asking for (and getting) more than smaller or slower-moving companies are willing to pay. IT and cybersecurity departments, already familiar with the challenges of smaller-than-desired budgets, are feeling more of a crunch than ever as they struggle to come up with sufficiently large salary offers.

Considering all of these hurdles, many employers might despair of finding and retaining the cybersecurity talent that they desperately need. There is clearly a shortage of qualified cybersecurity workers in the US, and this shortage is not likely to resolve quickly. Therefore, since the job market will not easily change, then employers must change their approach — and in some cases, their entire hiring philosophy — to meet their cybersecurity staffing needs.

The Way Forward

The traditional methods used for hiring and retaining cybersecurity talent no longer apply. The current market, both in terms of demand and supply, requires a change in mindset regarding the way we find and train workers. And, after bringing on those hard-won professionals, employers must find innovative methods and tools to retain them for the long-term.

In the following pages, we will take a look at the different stages of an employee's journey, from new hire to established expert, identify their primary pain points, and offer new approaches and tools that will enable both them, and their employers, to thrive.

Attracting Potential Talent

Companies looking to hire fresh cybersecurity talent in today's market are in for a rude awakening, facing a shortage of qualified employees, increased competition from other companies, and changing standards from employees who are placing greater importance on flexibility and work-life balance than ever.

Fortunately, there are many ways that employers can make themselves more attractive to new cybersecurity talent.

It's time to say goodbye to the traditional 9-to-5, 5-days-a-week approach.

Offer Time and Location Flexibility

It's time to say goodbye to the traditional 9-to-5, 5-days-a-week approach. Much as senior management might cling to the old standards, there's simply no need for such rigid business hours, especially when it comes to the creative and highly-technical members of a cybersecurity team.

Hackers will work long, hard hours when they're engaged with a difficult or interesting problem. They will happily burn plenty of midnight oil chasing down an exploit or following an attack path. By forcing them to work within a rigid schedule, you stifle their creativity. As long as the work is done well, and within the necessary time frame, it shouldn't matter if members of your team work 30 hours in one week and 50 hours the next.

This flexible approach should apply to location, as well. Nearly all of the work done in pentesting and red teaming can be performed remotely. Blue teamers might need to be onsite during an event, but much of their work can be done remotely as well. There is no need to demand that your team appear in the office every day — or even live in the same state as the office.

25%
of higher-paying jobs in North America will be remote by the end of 2022

Strategically creating positions that can be fully remote dramatically increases your chances of finding quality talent. According to recent estimates, 25 percent of higher-paying jobs in North America will be remote by the end of 2022, and employers who are slow to adapt to this new expectation will be left with far fewer hiring options. And in an industry like cybersecurity, where so much of the work can be performed remotely, there is no excuse for inflexibility.

LinkedIn's 2022 Global Talent Trends Report reveals that 63 percent of professionals prioritize work-life balance when choosing where to take a job. If employers want to attract top talent, advertising up-front that their employees have the flexibility to work where and when they want will be an effective first step.

63%
of professionals prioritize work-life balance when choosing where to take a job

Focus on Their Strengths

The people who work in cybersecurity choose their profession because they enjoy what they do. An easy way to attract talent is by assuring potential hires that their primary duties will be to pursue their interests and sharpen their skills. If your company posts a job description for hackers or pentesters that includes managing their own projects, liaising with clients, or meeting sales goals, you will be setting yourself up for failure.

Make it clear from the start that project managers or the operations team will set up pentesting engagements, and that tech leads or supervisors will manage the read-outs. By doing so, you'll show that you value the time and talents of your cybersecurity team members.

Prioritize Education and Guidance

Fresh security workers and hackers, when looking at potential employers, will prioritize places where they can expand their skill set. A job description with a limited scope of work and no details about peer guidance and research opportunities will fail to attract the very type of candidate most employers seek — the candidate who wants to grow and make themselves more useful.

You can make a more positive impression by highlighting resources for learning. Show them how to use available tools like PlexTrac's Runbooks feature, which can provide new employees with internal playbooks — documenting the tools, syntax, and exact steps developed by your senior staff — to learn the ropes quickly and easily. Make sure to mention the research and creative opportunities that your security team enjoys. Highlight the blog posts and articles they've written, the classes they've attended, and the speaking engagements they've landed at DEF CON or ShmooCon.

Employers can make a more positive impression by highlighting resources that will help new hires learn the ropes quickly.

Onboarding New Talent

Congratulations! You've landed some promising hires. Your next challenge: how to get them up to speed and ready to work as soon as possible.

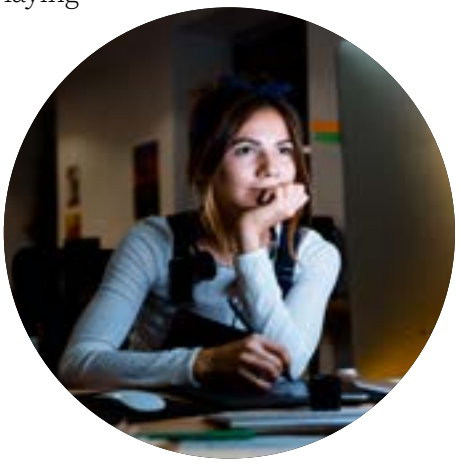
Hiring inexperienced pentesters poses a challenge: They don't have enough skill to work unsupervised, but including them in an engagement tends to slow things down. If your security team is like many right now, your overstretched hackers and pentesters are already busy with the work on hand and might not have much time to help the new hires learn the ropes. And as remote work is still the order of the day for most companies, you will need to get creative to effectively support and train your new hires.

As remote work is still the order of the day for most companies, you will need to get creative to effectively support and train your new hires.

Provide Curriculum to Create Billable Resources

Chances are that your team executes a standard set of basic procedures for an engagement, at least during the first few steps. Documenting these procedures creates a simple, step-by-step guide that new hires with basic skills can follow and learn from.

However, this approach has an up-front drawback: Your team will have to create these documents in the first place. Fortunately, there are tools available to make this process easier. For example, PlexTrac allows your team to script all of your team's engagements in real time, laying everything out as a runbook for an inexperienced pentester to follow, without requiring extra steps from your veteran talent. This lets the new employees follow specific procedures without extensive teaching or monitoring.



PlexTrac also enables lower-level and less experienced employees to perform many testing functions on their own. Using Runbooks, you can script testing procedures, run the test, record the results, and assign and track remediation. All of this information can also be sliced and diced into robust analytics and output in reports in your custom templates. With all this automated functionality, new hires can start executing basic operations and generating billable hours with minimal delay.

Offer Mentorship Programs

You can ease the integration of new talent by assigning a mentor to them, who will act as a professional and social guide within the team and the company. Mentors can teach junior employees how to handle new problems, and offer a safety net when they reach beyond their current skill set. Mentorship can be a fast-track for less-experienced employees to get up to speed in new procedures and roles, and studies have shown that it improves the performance and job satisfaction of the mentor as well.

Maximizing Existing Talent

Until the cybersecurity talent shortage is tackled, many security teams will continue to be shorthanded. For the manager facing staffing shortages, budget challenges, and the time constraints that come with increasing attacks and breaches, it is vital to find creative and viable ways to maximize their existing resources.

Invest in Education

Professional development opportunities attract talent and provide excellent return-on-investment (ROI) for employers, yet many organizations have tight limits on education spending, arguing that paying for certifications and classes is too risky because the employees will leave for better-paying jobs that they're now qualified for. This risk is far lower than most employers think, and employees are more likely to show good will towards companies that provide them with education opportunities. According to an extensive worker survey by LinkedIn, the best way for employers to improve company culture is by offering more professional development opportunities. Hackers, pentesters, operators, and blue teamers enjoy a challenge, especially if it means that they're gaining useful skills.

Hackers, pentesters, operators, and blue teamers enjoy a challenge, especially if it means that they're gaining useful skills.

Enact a Pro-Failure Policy

Nobody likes to fail, but the fear of failure and the consequences of failure can keep people from trying anything new. This can limit your team from acquiring new skills and making the most of their knowledge. In order to counteract this, have a written policy that's in favor of failure. Establish a culture that makes failure a part of the learning process and, if employees have followed procedures to the best of their ability and still failed, applaud them for their efforts.

Encourage Information Sharing

The best security teams share information and look out for each other. Not every team member can excel in all areas — each member will have their strengths and weaknesses, and when they are encouraged to share their strengths with the team, every member will benefit.

How can you encourage your team to share information? Ask team members to share lessons they learned from the classes or seminars they attend. Schedule brown bag sessions and ask someone to share a skill that they're passionate about. After some of your team attends a conference, ask them to send an email to the whole team sharing their favorite session and a line about what made it so interesting to them.

Even small shares can strengthen a team. Recommending a great new restaurant to visit when team members are on site with clients can help a team feel cohesive, even when they're miles apart.

Implement Collaboration Technology

Whether your team is all on-site or spread across states (or countries), maximizing their talent requires smoothing the path of collaboration as much as possible. Ensure that they have all of the tools that they need for communication, but not so many that messages are getting lost in the forest of channels and applications.

PlexTrac enables collaboration across the cybersecurity workflow. Every feature of PlexTrac is designed to foster sharing of collective activities and knowledge with robust role based access controls (RBAC) to ensure appropriate permissions. Reports, Assessments, Analytics, and Runbooks features all capture data, store information, allow the user to manipulate and act on that information, and output results in a variety of forms and formats. PlexTrac centralizes all the data and workflows so everyone on the team regardless of seniority and experience can benefit from the collective knowledge of the team and immediately add value.

Retaining Top Talent

Your security team is staffed, trained, and working efficiently. But now is not the time for complacency — you need to make sure that your team members are supported, encouraged, and sufficiently engaged and challenged so that they will happily stay with your company for the long term.

Here are some easy ways that your team can eliminate busywork, streamline reporting, and reduce burnout.

Make sure that your team members are supported, encouraged, and sufficiently engaged and challenged.

Set Aside Time for Creativity, Research, and Rest

Hackers are notorious for working long hours when they're invested in an interesting project. Add this tendency to the fact that most security teams have a regular backlog of work, and burnout can become a very real risk. It is crucial to monitor your team for signs of stagnation or exhaustion, which can in turn lead to mistakes, lower morale, and dissatisfaction.

Purposefully block out times for rest and recovery. Check in with the team (or team leads) to ensure that members have the time to pursue work and research that excites them. If they are interested in industry events or continuing education, make sure that they have the time to pursue those. Establishing a department culture where taking refresh time is encouraged, and even expected, will give your team permission to take care of themselves.

Streamline Pentest Report Language

Pentesters and hackers certainly didn't get into cybersecurity for the opportunity to write reports, but reports are still an important aspect of the job. Clients depend on your team to create thorough, clear reports about how they were able to hack them, and how to prevent it in the future.

Many security team members struggle to report their findings well. Too often, reports contain vulnerability finding descriptions that are loosely cribbed from Nessus descriptions — it can be difficult to come up with original descriptions for vulnerabilities that have been well-defined since

1998. It creates a far better impression if your team writes custom vulnerability descriptions, which can then be reused for future reports (saving time and effort down the road).

Use a Quality Reporting System

For many teams, crafting reports entails wrestling with Microsoft Word or markdown language templates that can be cumbersome to keep current, as even small document-wide changes like the copyright date can be a chore to update. And when it comes to compiling findings within the templates, there are the hurdles of getting each section aligned, placing tables in the right locations, adding evidence and graphs, and wrangling with fonts and formatting.

Ideally, your team would have an optional reporting system that included some key features:

1. **Permissions and authentication.** Some people need to see the report during the report generation process, while others only need to see a draft or the final product. Ideally, the system would include a well-designed client portal to allow clients to participate in the readout, have access to the report during the retest, and update the team when the report is ready for final remediation reporting.

2. **Integrated ticketing.** The ability to take findings and automatically add them to Jira or ServiceNow (or a similar ticketing system) eliminates one whole manual process.

3. **Reusable findings and narratives.** A busy security team will want narrative sections that they can build with pre-existing sections that can be reused for multiple clients.

4. **Flexible hosting.** An ideal reporting system will provide flexibility for where the data and report are hosted. Some customers may insist that their data is the only data in their instance; therefore, that data needs to be kept separate or hosted on-prem on their site.

5. **Quality assurance and editing features.** Editing tools such as fully-functional WYSIWYG editors and global find-and-replace tagging can shave hours off of the reporting process.

6. **Tool integrations.** Your team will want the ability to import data from as many tools as possible, as well as parse the output from those tools in different ways that make the results of the report more actionable.

PlexTrac's reporting system provides all of these reporting features and many more, all created to save your team time and hassle. The readout and attack path visualization capabilities help your team to accurately and smoothly describe the results of the test. You can also easily associate files or images of raw evidence findings so you can demonstrate results and answer deep technical questions as if you participated directly in the test. The Attack Path page provides a way for pentesters to visualize and graphically recreate the attack chain. This makes it easy for everyone on the readout to understand what happened and what the risk is to the organization.

PlexTrac's reporting system provides all of these reporting features and many more, all created to save your team time and hassle.

The Future of Cybersecurity Hiring: New Mindset, New Tools

We find ourselves in a new and uncharted region of employer-employee relations. The past two years have upended the way that most of the world works, and the recent Great Resignation movement has significantly altered the priorities and preferences of the workforce. This shift in expectations held by employees, coupled with the significant talent shortfall that the cybersecurity industry can expect to face for some time to come, demands that executives, hiring managers, and team leads update their approach to hiring, onboarding, maximizing, and retaining talent.

The modern cybersecurity worker prioritizes a reasonable work-life balance, opportunities for growth and education, and a healthy and positive work environment. It is up to employers to meet these expectations by offering flexible hours and remote work options, encouraging team members to hone their skill set and pursue further education, and fostering an environment of collaboration, safety, and creativity. The companies that fail to adapt to the priorities of their new talent doom themselves to stagnation, high employee turnover, and an immature cybersecurity function.

One of the best ways that employers can successfully assist their security teams is by providing them with the best tools available, which can enable collaboration, simplify the reporting process, guide new talent in work processes, and ease communications with all stakeholders. PlexTrac offers a flexible, comprehensive platform for cybersecurity reporting and workflow management that offers all of these features and many more, encouraging security team cooperation and cross-training in all aspects of engagement.

To learn more about how the PlexTrac platform can help you make your team more attractive to prospective talent, check out

Optimize the Business of Purple Teaming: The Cybersecurity Team's Guide to Improving Effectiveness with PlexTrac, or

Crushing the Reporting Time Suck: The Security Consultant's Guide to Improving Productivity with PlexTrac

to discover how PlexTrac can streamline many of your team's administrative and reporting tasks, leaving them with more time and freedom to pursue the tasks they enjoy.

Interested in learning more about the many benefits of PlexTrac? ***Book a demo today.***

PlexTrac is a proactive cybersecurity reporting platform built to streamline the report writing of a variety of security assessments, provide a richer remediation and collaboration experience and make it easier to ensure teams are focusing on the right security work. For more information, please visit www.plextrac.com

PlexTrac®