coresecurity
by HelpSystems

THE MYTH OF THE SKILLS GAP

HOW ORGANIZATIONS CAN GET SMARTER ABOUT PEN-TESTING

TABLE OF CONTENTS

3 Introduction

4 3 Things Holding You Back From Finding Quality Pen Testers

5 Sources of Frustration with Pen-Testing Tools

6 What We Can Learn From the Medical Field

7 Best Practices for Effective Pen-Testing

8 What Makes a Good Pen Tester?

9 Core Impact Is Ready to Help

10 Conclusion

INTRODUCTION

There's a dangerous misconception sweeping the security industry: Hackers and their cunning attacks are more sophisticated than our best efforts to defend against them. It may seem that the skills gap between the attackers and the protectors is so wide and growing so fast that it's impossible to catch up.

It's easy to see why this idea is dangerous. We can't afford to have security pros giving up or rationalizing away breaches because they thought they were inevitable. After all, if the proverbial tortoise believed it was impossible to beat the hare, he would have given up — turning pessimism into a

self-fulfilling prophecy.

In this eBook, we explain why the skills gap is a misconception. We'll explore the challenges surrounding penetration ("pen") testing and provide tips on how you can find qualified pen testers and tools to remediate security weaknesses in your applications, networks, and systems — so you can stay ahead of attackers.

3 THINGS HOLDING YOU BACK FROM FINDING QUALITY PEN TESTERS

Pen-testing keeps you ahead of adversaries by helping you identify security holes before they find them. Most organizations generally understand the critical need for regular and effective penetration testing. But, all too often, they engage in practices that practically guarantee they won't get it.

Here are three ways you might be jeopardizing your ability to find quality pen testers.

1. Demanding perfection

Many organizations only hire the cream of the crop —pen testers who have years of experience and are fully capable of handling a wide variety of tasks in a particular environment. There is little willingness to invest in junior workers who are hungry to expand their skills. But, according to the 2017 Global Information Security Workforce Study, a predicted shortfall of 1.8 million security workers by 2020 means organizations must begin to actively nurture a new wave of personnel.

66%

of global professionals feel there are too few security workers in their departments.

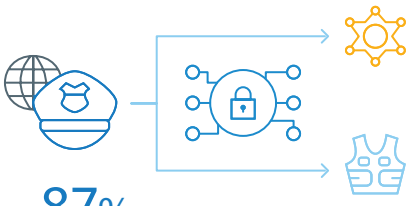
2. Requiring experience with today's hottest technology

Organizations readily admit to feeling overwhelmed by the pace at which technology is advancing. When hiring pen testers, they tend to focus on skill and experience with specific technologies, forgetting that those technologies will soon be obsolete. A better approach is to look for people who have core skills of critical thinking and creativity and a readiness to adapt to new technologies.

3. Focusing too much on certifications

While certifications can be part of the hiring decision, it's essential to look deeper. Many non-certified security workers already have a strong understanding of the concepts and processes involved in pen-testing. Similarly, real-world experience, even outside of

pen-testing, can be as relevant of a proving ground as education. The key is to go beyond a candidate's paperwork and recognize their more fundamental strengths.



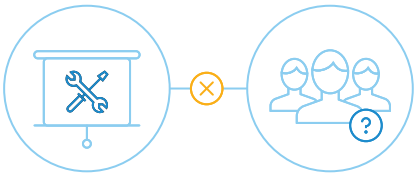
87%

of global security workers started a career other than cybersecurity.

SOURCES OF FRUSTRATION WITH PEN-TESTING TOOLS

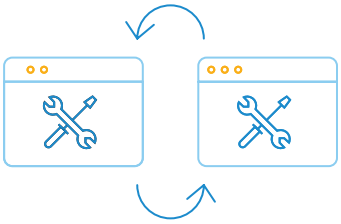
Of course, the perceived lack of good pen testers out there is only half the picture — organizations are also frustrated about pen-testing tools. All too often, they don't realize their full value.

Here are two bad practices that are most commonly to blame:



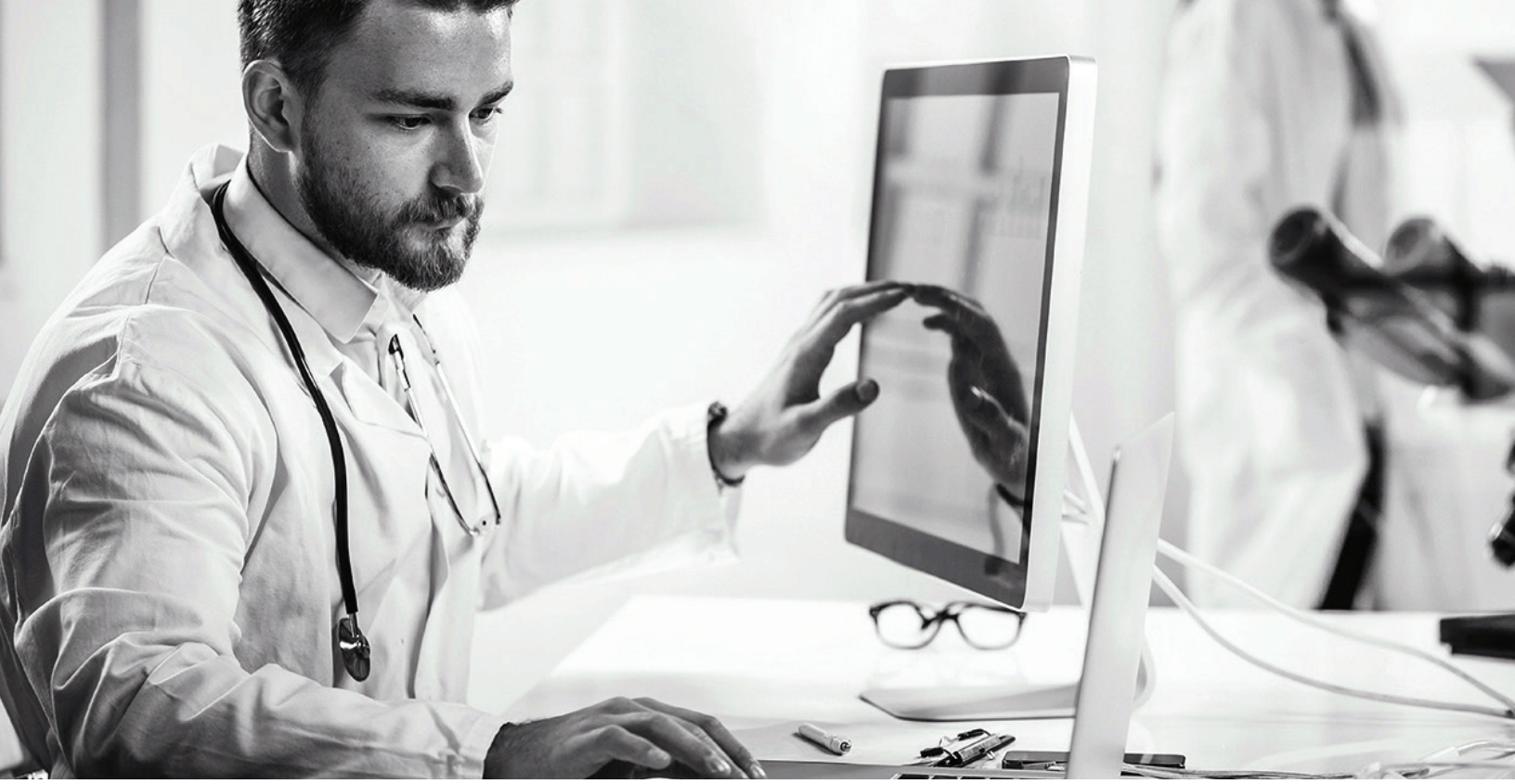
Failure to invest in training

Organizations often purchase pen-testing tools that many of their pen testers have no experience with. They fail to provide the training those people need to use the tools effectively. As a result, the organization never realizes the full value of its investment, or the tool is abandoned altogether because no one understands it.



Constantly changing tools

Pen testers can come and go quickly at companies, and they often have different preferences about which tools they like to use. Indeed, when organizations fail to look for candidates with a flexible skill set, their new hires might not be able to adapt to different tools than they are used to. As a result, organizations keep cycling in new tools, and, as a result, get increasingly frustrated about the associated costs.



WHAT WE CAN LEARN FROM THE MEDICAL FIELD

Like pen-testing, the healthcare sector deals with matters of critical importance while experiencing constant advances in technology. But it handles practitioners and tools in very different ways. Here are some medical approaches that the security sector would do well to learn:

Training – and lots of it

Doctors get training — lots of training. They aren't expected to come out of medical school with all the knowledge and skills they need to be immediately effective. Instead, during their residency, they work with more experienced healthcare professionals to expand their skills and take on increasing levels of responsibility.

Soft skills matter too

While the credentials they hold are important, there is also a focus on their experience, attitude, and foundational abilities, like being able to think critically and work effectively with both patients and data.

Stand by your tools

Healthcare organizations also take a different approach to technology. While doctors might take their favorite stethoscopes with them when they change jobs, they mostly adapt to the tools already in place, rather than requiring a wholesale rip and replace. As a result, the organizations get deeper value from their technology investments. And as technology advances and it makes sense to add or change tools, healthcare providers provide the training they need.

BEST PRACTICES FOR EFFECTIVE PEN-TESTING

Effective pen-testing is not a thing of the past. Any skills gap can be erased by replacing counterproductive habits with these best practices:

Commit to nurturing your staff:

Look for the right foundations in less experienced candidates, such as a solid understanding of pen-testing concepts and practices and a demonstrated ability and eagerness to learn and grow. Then help them develop their talents and expand their experience.

Value your senior talent:

Try to have at least one person with broad experience who can help craft strategy and set priorities, as well as provide mentorship to junior colleagues. This sense of collaboration is empowering to both parties and can lead to a powerful team approach to problem solving.

Look for complementary strengths:

Don't expect any one person to solve all your problems, Individuals have different strengths and weaknesses. The trick to building a strong team is bringing together people whose strengths complement each other.

Don't focus on a single tool:

Similarly, no single tool can solve all your security problems. Just as you put together a team of people with different skills, you'll need to carefully assemble a toolkit that addresses multiple solutions.

Invest in training:

Get maximum value from your purchases by providing training. Remember that nobody can grasp the full functionality of a complex solution in one session; as your pen testers master one capability, ensure they can get training on additional features of the product. And don't swap out a good tool just because your new pen tester hasn't used it before or prefers something else; bring them up to speed on the tools you have. (Of course, you should be open to honest feedback about how the tools compare and be open to switching tools when it makes sense.)

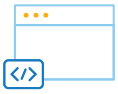
WHAT MAKES A GOOD PEN TESTER?

Effective pen-testing requires good pen testers. We've argued that organizations should be willing to hire more junior testers, and that they should stop focusing on specific credentials or experience with the latest and hottest technology. But what should they be looking for?

Here are the qualities that make a good pen tester:

The ability to think critically:

Problem-solving is at the core of pen-testing, so critical thinking is a crucial skill. Don't hire anyone who can't demonstrate this skill. Interests or degrees in things like engineering, mathematics, and even philosophy or law can be indicative of this ability.



Programming experience:

Experience with software development helps pen testers assess applications from a security standpoint. Being able to read and understand code gives them a leg up on creating their own programs and scripts or modifying existing ones.

Creativity:

With data and algorithms handling more and more of the tedious work, you should rely on your human staff to do what the computers can't –– establish a habit for thinking outside the box. Look for a willingness to challenge limits or approach a problem from multiple perspectives.

A love of learning:

New technologies and methodologies are constantly being developed, and pen testers have to welcome the challenge of exploring them. Be sure to foster this critical characteristic by making sure they have some time set aside for exploring new topics or doing more in-depth research on a topic of interest.

Inherent curiosity:

Look for candidates that want to understand how things work and how they relate to other things. For example, knowing how to configure a firewall or router will help pen testers to do their job. But knowing the underlying concepts and protocols that enable these devices to work can allow a pen tester to do a more complete and thorough job, which will result in better understanding of how to harden your network against attacks.

CORE IMPACT IS READY TO HELP

One more critical best practice is to give your pen-testing team the right tools. Especially if you're hiring more junior staff and developing talent within your organization, you need a pen-testing tool that is powerful, yet easy to use. And you need a vendor that provides ongoing training and support so you can get maximum value from your investment.

A powerful tool that's easy to use

Core Impact is the most comprehensive solution for assessing and testing security weaknesses throughout your organization. Core Impact is the only solution that empowers you to replicate attacks that pivot across systems, devices, and applications to reveal how chains of exploitable vulnerabilities open paths to your organization's

mission-critical systems and data. Yet it offers a simple interface that's easy to learn and easy to use.

Multiple avenues for getting training and help

To ensure you get full value from the solution, no matter what level of experience your pen testers have, Core Impact offers multiple options for training and help:

Initial training:

Ensure your pen testers quickly get comfortable with the core functionality of the product.

On-demand training:

Pen testers can visit the Community Portal at any time to get the training they need to take advantage of additional features of the product and be more efficient and effective in their jobs.

Real-time chat:

Within the same community, discuss challenges or other topics of interest with fellow customers and subject matter experts at any time.

Code repository: S

ave time and increase productivity by taking advantage of the code that others have written and shared.

Question + answer area:

Turn to the Community Portal to quickly get answers to specific questions or indulge that inherent curiosity by exploring what others are trying to do.

Customer success manager:

Reach out to your dedicated CSM who's committed to helping you reap maximum benefits from the tool.

Consulting services

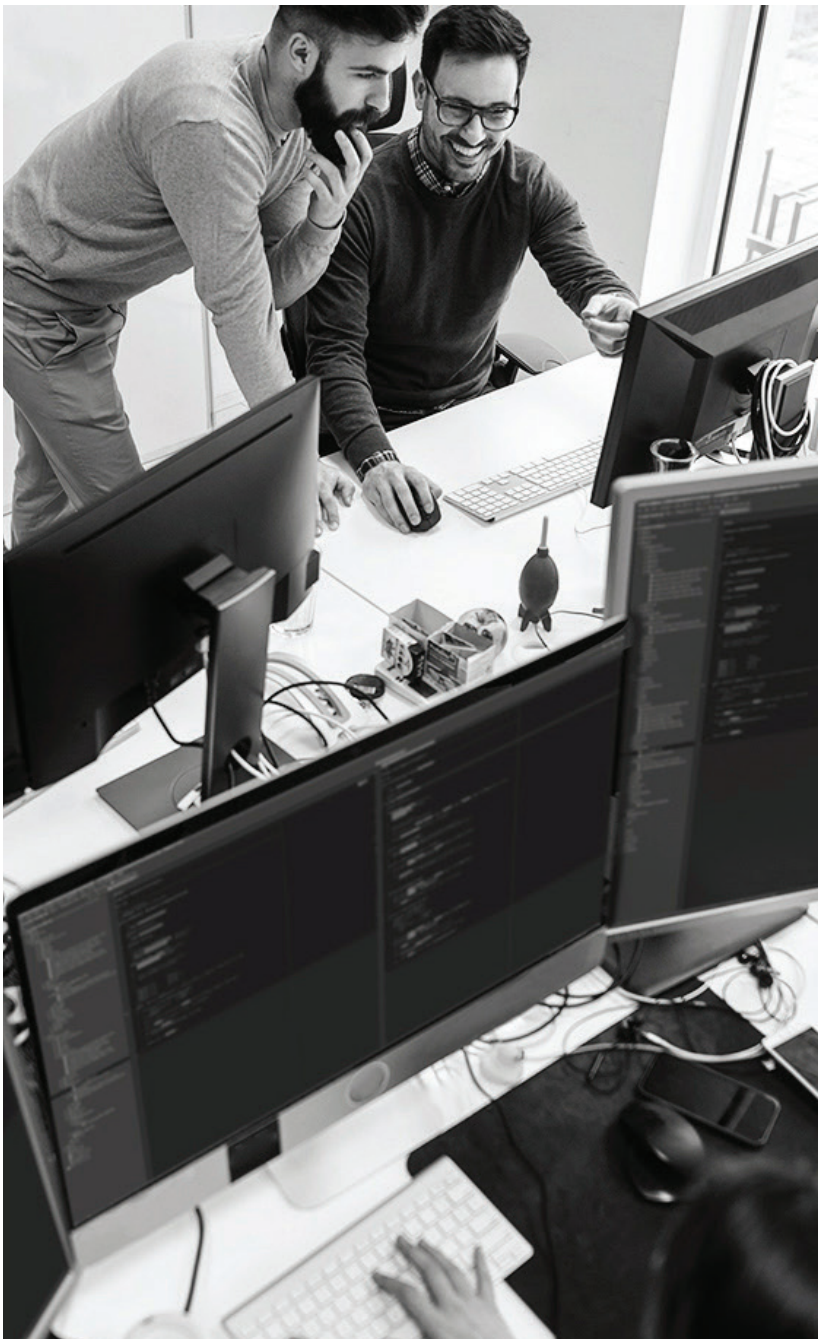
If you prefer, you can also outsource pen-testing to us. Our Security Consulting Services (SCS) delivers comprehensive penetration testing tailored to your needs, including the annual third-party pen-testing mandated for many organizations.

CONCLUSION

There's no question that attacks are becoming more frequent and more sophisticated. But blaming the increase in data breaches on a "skills gap" is insufficient. As the medical profession illustrates, good practitioners don't just materialize out of thin air; people with the right mindset need to be trained and mentored over time. By looking for fundamentals rather than flashy credentials, you can build the pen-testing team you need to get ahead of hackers, and stay ahead.

For learn more about successful pen-testing and how Core Impact can help, please visit

www.coresecurity.com



coresecurity
by HelpSystems

www.coresecurity.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.