independent security evaluators

Security Experts are Scarce: Discover How to Find the Right Partner to Help You Develop In-House Expertise and Empower Your Products with Maximized Security

There are more than 500 cyber attacks every minute. Don't become another statistic. Learn what it takes to protect and secure your application.

THERE IS A SECURITY SKILLS SHORTAGE

The reasons why will surprise you

Let's discuss one of the biggest constraints you'll face: talent. Security requires a highly specialized skill set, which is, unfortunately, in extreme shortage and will continue to be so for the foreseeable future. There are several reasons for this skills shortage:

Formal education isn't optimized to create enough security talent.

Security-specific degree programs are scarce, so most ethical hackers come out of computer science degree programs, which don't treat security as a core discipline.

Security requires extensive real-world experience outside of the classroom.

Aspiring security professionals must obtain experience in their own time in order to prepare for the jobs that they want.

Security has perception issues.

Security is often perceived to be ridiculously hard, so rising computer scientists often pursue other areas instead.

Security is adversarial.

Security is about being more creative than someone else and being interested in tearing apart the work of others.

WHY YOU NEED BOTH IN-HOUSE AND EXTERNAL SECURITY TEAMS

Security is a team sport.

External and internal expertise complement each other. Find people capable of executing the ideas, strategies, and tactics capable of solving your security problems, and then pair them together to magnify each others' impact. Security is a team sport.

YOUR IN-HOUSE SECURITY TEAM

You can, and should, build your own expertise in-house. However, it's going to be a long, difficult road. Over the many years we've been doing this, we've yet to see a company successfully achieve their security mission with only in-house talent alone. That doesn't mean you won't be able to, it just means the odds aren't in your favor.

YOUR EXTERNAL SECURITY TEAM

Your external security partner finds security vulnerabilities and you fix them. Your partner transfers knowledge and you use it to get better. Your external partner is immune to bias, as well as the strong opinions of leaders in your company, so you get the truth, even if it's not what you want to hear.

Together, you and your external partner reduce risk. Win-win.

Separation of duties is a powerful concept that you already see in other areas of your business: your Chief Financial Officer (CFO) works with external accountants, your general counsel works with outside law firms, and your CEO works with the board and other external advisors. It's the same idea with outside security experts: they magnify the impact made by internal resources while delivering benefits you can't get in-house.

It probably won't ever be appropriate for you to make critical decisions without external expertise. **Just look at the type of companies that hire us: Amazon, Google, Microsoft, Netflix, and Adobe**, just to name a few. Talk about enterprises that have robust in-house security teams! Yet they capitalize on external security expertise.

If it works for them, it will work for you too.

CASE STUDIES

How can our findings improve your DevOps?

INDUSTRY-WIDE MISUNDERSTANDINGS OF HTTPS

Most web browsers, historically, were cautious about caching content delivered over an HTTPS connection to disk—to a greater degree than required by the HTTP standard. In recent years, in response to the increased use of HTTPS for non-sensitive data, and the proliferation of bandwidth-hungry AJAX and Web 2.0 sites, some browsers have been changed to strictly follow the standard, and cache HTTPS content far more aggressively than before. HTTPS web servers must explicitly include a response header to block standards-compliant browsers from caching the response to disk—and not all web developers have caught up to the new browser behavior.

ISE identified 21 (70% of sites tested) financial, healthcare, insurance and utility account sites that failed to forbid browsers from storing cached content on disk, and as a result, after visiting these sites, unencrypted sensitive content is left behind on end-users' machines.

Finish reading this case study

View all of our case studies and research papers

SECURITY VULNERABILITIES IN NETWORK ACCESSIBLE SERVICES

Internet of Things (IoT) devices have always been vulnerable to a variety of security issues. In 2013, Independent Security Evaluators (ISE) performed research on IoT devices that showed how rich feature sets could be leveraged to compromise devices. Today, we show that security controls put in place by device manufacturers are insufficient against attacks carried out by remote adversaries. This research project aimed to uncover and leverage new techniques to circumvent these new security controls in embedded devices.

Finish reading this case study

View all of our case studies and research papers

ISE: ETHICAL HACKING TO THE RESCUE

Hit the ground running.

ISE broke into 100 per cent of the systems" - The Globe & Mail

"ISE showed the lack of robust security in important devices that people use every day" - New York Times

Want to talk further about how we can help you with this? Contact us today. Even if we can't help you, we'll refer you to someone who can. After all, that's what security consultants do: We help you solve your problems.

NEED TO PREVENT OR FIX SECURITY PROBLEMS? HAVE AN ONLINE SECURITY QUESTION? WE'D BE HAPPY TO HAVE A CONVERSATION WITH YOU!

Schedule a free call with us today.