OFFENSIVE security ®

Selecting the Best Information Security Training for Your Organization

In a recent article published on CSO, John Olstik described the shortage of talent with cybersecurity skills and training as an "industry crisis." He cites that more than half of organizations report a "problematic shortage" with no end in sight[1]. While there are efforts to address this shortage across the public and private sectors, one way corporations are actively dealing with it today is by investing in high quality training to nurture in-house talent.

Choosing the right information security training partner is a critical decision for organizations, especially those looking to realize immediate value from their investment.

Here, we provide you with a few essential points to consider when navigating the information security training landscape and selecting the best provider for your organization.

1. Understand Course Objectives & the Intended Audience
2. The Best Defense is Good Offense
3. Do Your Research
4. Confirm a Hands-On Approach
5. Beware of Hidden Costs
6. Consider Offensive Security

1. Understand Course Objectives & the Intended Audience

The first step in the process should be to clearly define your training objectives. These objectives should help limit your search, allowing you to stay focused on what is actually important to you. Narrow options down to the few that most closely align with your organizational (or team) goals. When looking at the stated objectives of a training program, be wary of those that seem to promise the world. If it sounds too good to be true, it probably is.

Equally important is ensuring the course's level of difficulty aligns with the level of experience your employees have. An easy way to assess how advanced a course might be is by looking at the pre-requisites. An absence of pre-requisites should raise concerns about the depth and quality of the training. For courses that include a significant list of pre-requisites, ensure your employees will have the background knowledge and professional experience needed to be successful.

---

2. The Best Defense is Good Offense

Cybersecurity vendors generally classify training offers as red team (offensive) or blue team (defensive). A traditional defensive approach rests upon the belief that "building bigger fences" will keep intruders out of your systems. While this was an adequate strategy in the past, the increased sophistication of hackers and cyber criminals is forcing organizations to adopt an offensive approach. Unlike defensive security, an offensive strategy empowers information security professionals to proactively uncover vulnerabilities in the company's networks and systems.

Not all training providers will explicitly classify its program as being in one camp or the other. For instances where it is not clear, Michael Kranch suggests looking more closely at the syllabus in his paper "Why You Should Start with the Offense: How to Best Teach Cybersecurity's Core Concepts." Keywords and phrases such as "assessing vulnerabilities," "learning to exploit traffic analysis," and "reverse engineering" indicate offensively-rooted curriculum. Alternatively, courses that include topics like "identifying and applying best practices," or "how to recover from a breach" are indicative of a more defensive approach.[2]

The bottom line is that you will need to ensure the training you invest in is strongly rooted in the offensive mentality. Not only does this provide you with a better return on your investment in training and developing, but it is also integral to successfully protecting your company against increasingly sophisticated cyber attacks.

3. Do Your Research

Look into the minds behind the course - the curriculum developers and content creators. It is important that those involved have a good balance between professional training skills, and real-world experience. Seek out and consider reviews or comments from past students and don't be shy of posting your own questions; you may be surprised at the volume, quality, and depth of responses. Cybersecurity students tend to be passionate, vocal, and extremely candid.

If you're able to find the course author's names, use LinkedIn and Google to find out more about their background. Have they been developing training for a long time? Are they still active as industry professionals?

4. Confirm a Hands-On Approach

Always consider the split between theory and hands-on training. Core competencies are important, but this content should be covered, on an as-needed basis, early in the curriculum. The majority of the course should be focused on developing the student's "security mindset" through highly interactive, hands-on learning.

According to Potter and McGraw, a security mindset leads to uncovering ways to make a system fail as opposed to identifying processes and protocol to keep it running. The theory here is simple - thinking and acting like a cyber-security criminal is the most effective way to uncover and adequately address vulnerabilities[3]. Schneider later stated:

"This kind of thinking is not natural for engineers. The security mindset involves thinking like an attacker, an adversary or a criminal...if you don't see the world that way, you'll never notice most security problems."[4]

5. Beware of Hidden Costs

Many training programs culminate with a certification exam. While this can validate that your employees sufficiently mastered course concepts and skills, most exams are not designed to serve that purpose. Instead, programs leverage certification as a source of revenue, requiring incremental fees to take the exam, receive the certification, retain certification, etc. Look closely at the fine print surrounding certification and check for things like forced membership, ongoing course requirements, or re-certification fees. Be critical of organizations that make students jump through hoops after becoming certified.

6. Consider **Offensive Security**

When it comes to information security training and certification, Offensive Security (OffSec) is the industry-leading provider of online cybersecurity training.

As indicated in the name, OffSec wholly embraces an offensive approach through its integrated, multi-faceted training curriculum. Students learn core concepts upfront and then spend the majority of their time applying core concepts and theory to real-world situations. To encourage hands-on learning and a security mindset, OffSec students are given access to an innovative virtual lab environment where they can safely and legally apply course concepts.

Even OffSec's certification process underscores the importance of hands-on learning and real-world applicability. It takes place within a virtual lab filled with targets across different configurations and operating systems students. Students must to research the network, surface all vulnerabilities, and successfully execute attacks within a 24-hour timeframe. Doing this successfully requires a security mindset as well as a deep and thorough understanding of course concepts. It also requires students to think creatively, maintain incredible endurance, and demonstrate an unwavering strength of character. The exam is deliberately designed to be extremely challenging and as a result, certified individuals are highly respected and valued.

For organizations interested in offering training to their employees, Offensive Security offers the OffSec Flex program. This program enables companies as well as smaller teams to pre-purchase training time and subsequently apply it across OffSec courses and products, as needed, when-needed, for whoever needs it. To encourage investment in offensive cybersecurity training, OffSec contributes bonus funds to any budget, resulting in "free" additional training time.

- ✓ ***Virtual lab for hands-on learning***
- ✓ ***Strong focus on real-world applicability***
- ✓ ***Highly respected within the industry***
- ✓ ***Great option for individuals, organizations, or teams***

Enroll now at offensive-security.com

[1]*Oltsik, John. "The cybersecurity skills shortage is getting worse." CSO, January 10, 2019, www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html*

[2]*Kranch, Michael. (June 2019). "Why You Should Start with the Offense: How to Best Teach Cybersecurity's Core Concepts"*

[3]*Potter, B., and McGraw, G. Software security testing. IEEE Security & Privacy 2, 5 (2004), 81–85.*

[4]*Schneider, B. Inside the Twisted Mind of the Security Professional. Wired (Mar. 2008).*