CYBER SECURITY TRAINING ENABLES ORGANIZATIONS

TO BUILD BEST-IN-BREED

CYBER SECURITY PROS NEED SKILLS-BASED TRAINING TO STAY ON TOP OF TODAY'S THREAT LANDSCAPE

With two-thirds of today's organizations looking to build cyber security talent in-house, hiring managers consider candidate preparedness a growing priority. As cyber threats evolve and grow at a rate we haven't seen before, cyber security teams must keep pace, meaning the right talent needs to be in place. But fewer than half of organizations are confident in their team's skills to detect and respond to complex cyber incidents.

CHALLENGES TO BUILDING A

Best-In-Class Cyber Security Team

SKILLS GAP PERSISTS

ONLY 1 IN 4

applicants are considered qualified for each open job posting, and filling information security positions can take six months or longer.

NEEDS VARY

Based on Forrester Research's "State of Network Security: 2016-2017" report, organizations in different markets and verticals require different skill sets.

EXPERIENCE COUNTS

55%

of hiring managers believe that practical, hands-on experience is the most important cyber security qualification.

IF YOU CAN'T HIRE THE SKILLS YOU NEED,

Build Them By Continuously Improving Team Skills

In a world where hiring cyber security defenses are not a one-size-fits-all endeavor, quality, performance-based training can help teams fight the advanced cyber threats their organizations face.

GROW YOUR EXISTING TALENT

If you have a way to build cyber security technical skills, you can focus on developing your team rather than expanding it.

THE UPSIDE OF TRAINING

GET THE SKILLS YOU REQUIRE

Your challenges are unique, so an effective training model scales to suit your needs.

TRAIN ON TODAY'S THREATS

Too often, course content is outdated the moment it publishes. Newer, more flexible training models keep pace with today's threat landscape.

YOU CAN BE PARTICULAR

About Your Training Options

Cyber security team leaders understand the upside of training, yet 52% of executives indicated that today's training options made staff only moderately, slightly or not at all prepared. With so much at stake, information security teams can and should be selective about the models they choose.

TAKE THE TIME TO EVALUATE WHAT FEATURES ARE MOST IMPORTANT TO YOU:

Hands-on, practical training

Targeted focus based on your team's specific areas of improvement

Self-paced curriculum available on-demand

Performance-based experience with immediate scoring feedback

Cost-effective

Continuously updated labs based on evolving threats

Live dynamic network environment in tune with today's threats

Easy access/more time spent in the office vs. offsite at trainings

Want a solution that meets all of those needs? Read more about ISACA's Cybersecurity Training Platform and Assessment Tool here: isaca.org/CSXCyberTrainingPlatform

CSX CYBERSECURITY NEXUS™ ISACA®

SOURCE: State of Cyber Security Report, ISACA 2017.