Skills-Based Approaches to Cybersecurity Talent Management

1 What is Skills-based Hiring?

In the world of cybersecurity hiring, too often employers rely on proxies of employee capability and preparedness, such as advanced degrees, years of experience, and certifications. Doing so, however, can bar wide swaths of the population from desirable careers, limiting the number of candidates in the applicant pool and resulting in slower and less effective hiring.

Skills-based approaches focuses on the job seeker's capabilities and career readiness while increasing and diversifying the pool of prospective talent. Skills-based hiring simplifies position descriptions and engages in a talent management lifecycle that includes defined career paths. It also creates retraining and reskilling opportunities that open doors to new careers, whatever someone's background or education may be.

2 Why Does it Matter?

An employer can begin by evaluating how they communicate their cybersecurity talent needs. Job descriptions that focus on NICE Framework Work Roles more clearly define the work and call out what individuals need to know and what skills they should possess. The employer can assess their current team to identify areas for ongoing skill development and gaps that might require recruiting additional talent.

As part of ongoing performance-based assessments, the employer should provide access to learning that helps employees develop and improve their skills. Ideally, the employer uses a robust learning management system (LMS) and/or learning and employment records (LER) to help their cybersecurity workforce document their achievements. Other methods include developing hands-on learning experiences in the workplace, such as registered apprenticeship programs, that enable employers to have a steady pipeline of new talent.

3 How is it accomplished?

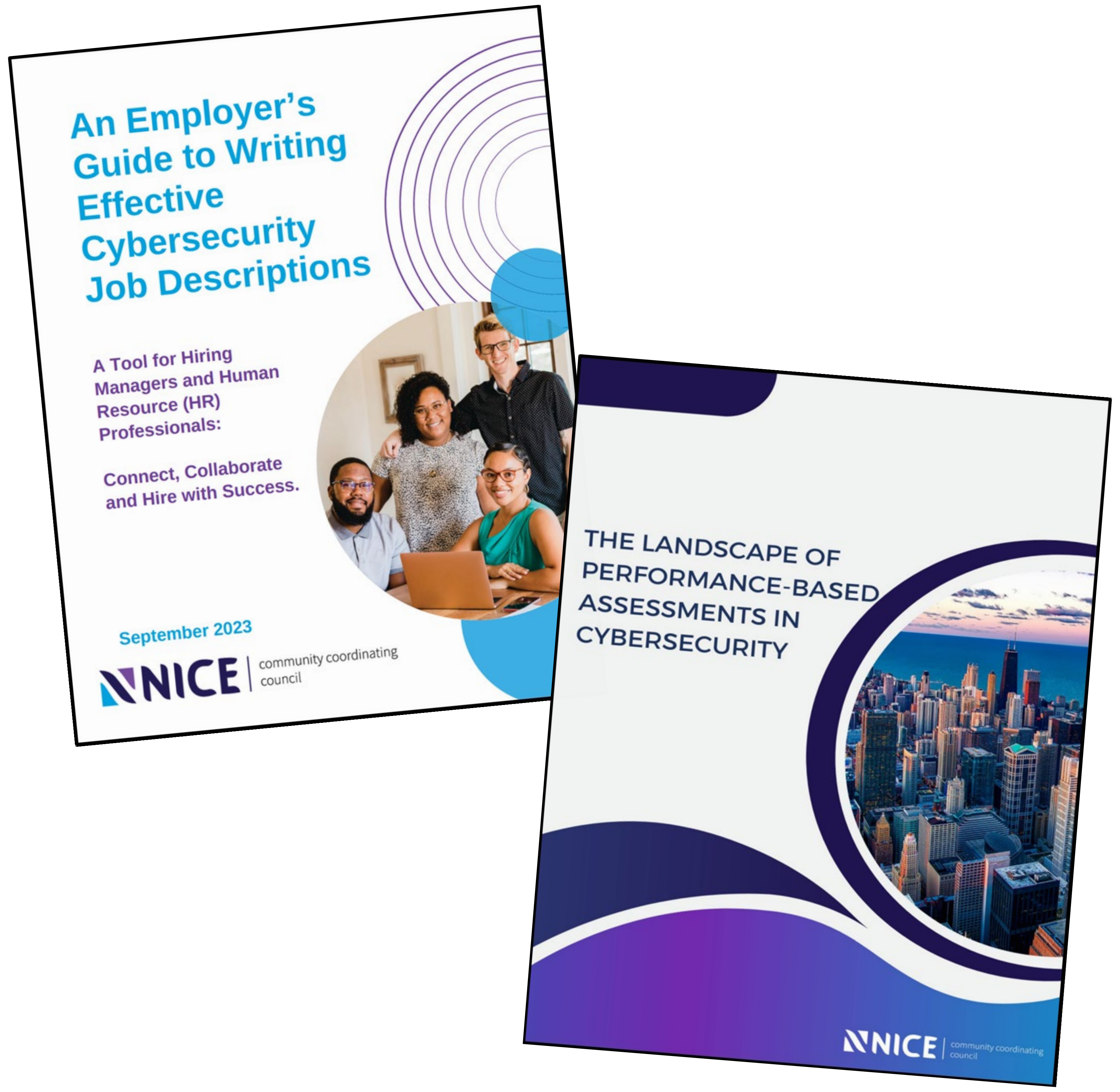
Skills-based hiring has been shown to widen the aperture of candidates eligible for rewarding cybersecurity careers. It reduces barriers to entry, such as required advanced degrees that for many Americans are unattainable. Defining the skills needed for careers in cybersecurity can also lead to greater standardization of entry-level roles. Aspiring cybersecurity professionals are often stymied at the challenge of finding their first job. A standardized approached to evaluating capability can increase candidates' confidence in their career prospects.

The NICE Workforce Framework for Cybersecurity (NICE Framework) uses Task, Knowledge, and Skill (TKS) statements to describe cybersecurity work and individual capabilities. This shared language can be used by both employers and job seekers to communicate which skills are sought as part of cybersecurity work and can be a useful part of any skills-based hiring program.

4 What resources are there?

Community-driven efforts include:

- **An Employer's Guide to Writing Effective Cybersecurity Job Descriptions**
  The NICE Modernize Talent Management Working Group Report
- **The Landscape of Performance-Based Assessments in Cybersecurity**
  The NICE Transform Learning Process Working Group Report
- **NICE Workforce Framework for Cybersecurity (NICE Framework)**
  www.nist.gov/nice/framework



An Employer's Guide to Writing Effective Cybersecurity Job Descriptions

A Tool for Hiring Managers and Human Resource (HR) Professionals:

Connect, Collaborate and Hire with Success.

September 2023

NICE | community coordinating council

THE LANDSCAPE OF PERFORMANCE-BASED ASSESSMENTS IN CYBERSECURITY

NICE | community coordinating council

Author: NICE Program Office (www.nist.gov/nice)