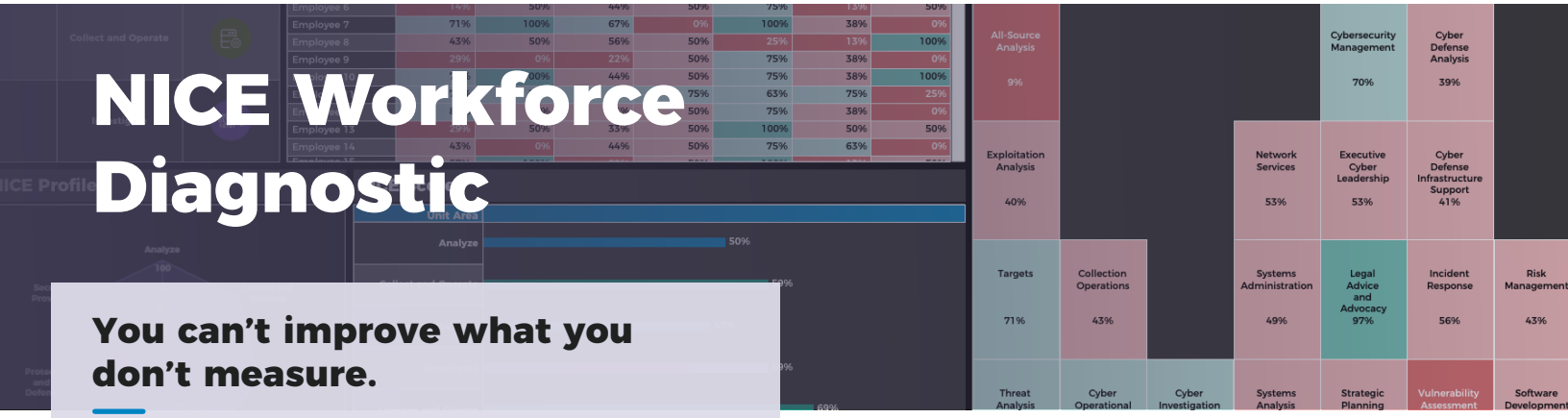
CyberVista®

NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

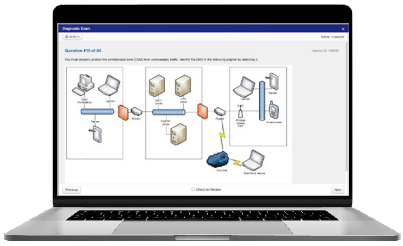
NICE Workforce Diagnostic



You can't improve what you don't measure.

Your organization regularly conducts network scans to find and patch vulnerabilities, so why not do the same with your people? Most cybersecurity leaders don't have a mechanism to accurately measure the current state of their cybersecurity teams. Without objective visibility, training dollars are misallocated.

CyberVista created the **NICE Workforce Diagnostic** to provide cybersecurity leaders with a foundation for making smarter cybersecurity training and talent decisions.



NICE Workforce Diagnostic question examples.

What is the NICE Workforce Diagnostic?

The NICE Workforce Diagnostic provides cybersecurity leaders with a baseline into competency areas of strength and weakness covering all seven categories of the Workforce Framework for Cybersecurity (NICE Framework). Developed by NIST, the NICE Framework establishes a common lexicon of cybersecurity-related competencies that can be applied to any organization and cybersecurity job role. As the name suggests, the NICE Workforce Diagnostic is a diagnostic solution designed to help organizations align their people initiatives to the NICE framework.

The diagnostic is delivered in two parts. First, participating practitioners complete an initial assessment that can be completed in 45 minutes or less. Unlike knowledge assessments or employee screening tools, the diagnostic includes questions that go beyond simple multiple choice to truly capture comprehension at the practitioner level.

Upon your team's completion of the diagnostic assessment, designated leaders will gain access to an interactive **Insights Dashboard**. The dashboard includes filters for demographics, job roles, experience, and specific areas of the NICE Cybersecurity Workforce Framework to uncover further insights and to support talent applications and initiatives.

What's included?

Diagnostic Assessment (Practitioner Participation)

- Web-based 45-minute diagnostic exam
- Personal Performance Tracker to review results and scoring
- Detailed explanations with links to the NICE Framework

Insights Reporting (Leadership Deliverables)

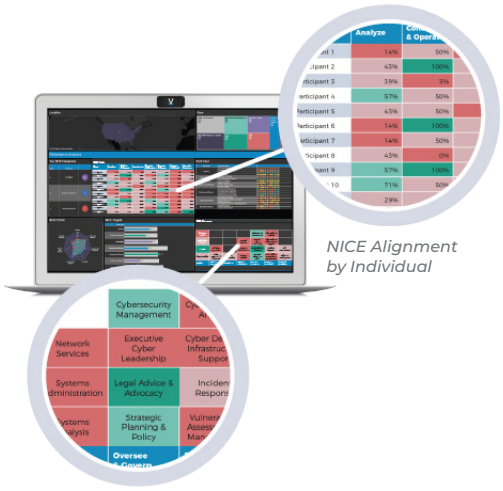
- Insights Dashboard with performance and demographics data

Why pursue a diagnostics-first approach?

A diagnostics-first approach empowers cybersecurity leaders to make informed decisions on the state of their cyber teams prior to spending the thousands (or perhaps millions) of dollars they commit annually to training. Your organization saves precious time and money by only deploying training in areas that have a positive impact on closing persistent skills gaps.

Signal to your practitioners that investments in training are purposeful and relevant to their roles. When has a one-size-fits-all bootcamp or subscription helped to answer the question *"did this make us better at what we do?"* Investing and training in the areas that are needed most not only improve employee job performance, but have a positive ripple-effect that improve employee satisfaction, retention, and career path opportunities.

Insights Dashboard



NICE Alignment by Individual

NICE Alignment in Aggregate

When should my organization use the NICE Workforce Diagnostic?

The diagnostic is an applicable solution for any organization looking to improve decision making regarding cybersecurity workforce development. Some specific applications include:

Prioritizing training deployment and spend. Organizations can be more deliberate in how funds are allocated when they know exactly where team members need training. Using a quantified approach, the NICE Workforce Diagnostic informs you of where your training dollars are best suited for maximum return on investment.

Verifying competencies for specific roles. The NICE Workforce Diagnostic can baseline, verify, and compare individual or aggregate team scores to expected competency outcomes for different cybersecurity roles.

Cross-skilling current talent based on proficiencies. The diagnostic can serve as a guiding point to facilitate career growth, lateral movements, or expansion of responsibilities. Rather than hiring new employees for the skills listed on their resume, the insights uncovered after a diagnostic assessment allow you to utilize your current talent to their maximum potential.

Onboarding talent into specific roles. Leveraging the NICE Workforce Diagnostic during onboarding can identify where individuals excel, then allocate new cohorts to teams that can best take advantage of their knowledge and skills. Furthermore, organizations can hire entry-level talent and administer relevant training based on the outcomes of the diagnostic, resulting in savings on both ends—wages and training spend.

Modernizing cybersecurity job roles and expectations. Many organizations are utilizing the NICE Framework to develop their cybersecurity workforce strategy. This diagnostic helps to inform those strategic decisions by measuring talent according to the NICE Framework, giving you visibility on which teams and skill-areas to prioritize.

Gain data-driven insights.

Let's talk.

We look forward to helping you train with purpose.

For further information on developing a diagnostics-first approach to your cybersecurity workforce, please email **sales@cybervista.net** or call **844-558-4782.**

CyberVista