THE LANDSCAPE OF PERFORMANCE-BASED ASSESSMENTS IN CYBERSECURITY

NICE | community coordinating council

A green paper for discussion from the NICE Community Coordinating Council, Transform Learning Process Working Group, Use of Performance-Based Assessments to Measure Cybersecurity Competencies Project Team.

Greenbook Contributors:
Mike Morris
Richard Spires
Jason Hammon
Marvin Marin
Lori Coombs
Franklyn Nicol
Keith Anderson

The Transform Learning Process Working Group focuses on the NICE Strategic Plan goal to Transform Learning to Build and Sustain a Diverse and Skilled Workforce. The group conducts an ongoing environmental scan of programs, projects, and initiatives related to this strategic plan's goals and objectives to assess the scope and sufficiency of efforts. The group also identify gaps where more attention and effort are needed. The group identifies strategies and tactics to implement the corresponding objectives to this goal.

Authored May 2023
Published March 2024

Table of Contents

Introduction

The objective of this working group project is to start discussions pertaining to performance-based assessments in cybersecurity. To begin drawing the map to guide the discussion, the working group began with questions such as: What are performances of NICE Framework Tasks? Who is doing it? When? Where? Is it effective?

This project falls under the auspices of the Transform Learning Process Working Group as part of the NICE Community Coordinating Council. The focus is on Goal 2 of the NICE Strategic Plan: Transform Learning to Build and Sustain a Diverse and Skilled Workforce. In its recently published Implementation Plan, NICE defined within this goal an objective (2.4) to "Facilitate increased use of performance-based assessments to measure competencies and the capability to perform NICE Framework tasks." This paper addresses aspects identified in the NICE implementation plan that support achieving this objective.

Specifically, our work falls into two strategies:

- NICE 2.4.1: Raise Awareness of the value and importance of using performance-based assessments to measure competencies and the capabilities to perform NICE Framework Tasks.
- NICE 2.4.2: Work to ensure that academic degrees programs and industry-recognized certifications effectively measure the ability to perform NICE Framework Tasks.

As one of the first working groups for this objective, this green paper is exploratory in nature. It is a discussion document that informs, but does not prescribe policy recommendations or decisions. This paper lays groundwork for future discussions and research.

Understanding the problem

What are performance-based assessments of NICE Framework Tasks?

NICE Framework Tasks

NICE Framework Tasks are workforce training or educational in nature. The tasks equate to doing “cybersecurity work” (Petersen et al., 2020). The Workforce Framework for Cybersecurity (NICE Framework) provides a taxonomy and common language to describe work language. The underlying question derived is “Are training providers and educational institutions training students effectively to prove that they can do “cybersecurity work?”

The NICE Framework delineates between tasks, skills, and knowledge with the intent to create a common and consistent lexicon. It is a forward-looking project in a discipline that is constantly changing. As more education and training aligns to the standards, it is natural to begin examining its efficacy. Declarative and procedural knowledge is often interrelated, and both are often used while performing NICE Framework Tasks. A Task is an activity that is directed toward the achievement of organizational objectives. These activities take place over time and generate value to the organization.

In a learning environment, performing a task is always an approximation to actually doing it. It’s “practice” vs. “live gameplay.” The difference is in transferring the activity to a new context. In this model, the best approximations provide experience working with exemplars of work products or processes that can be adapted and utilized in a future form.

A hiring manager might put this in simplistic terms: “Have you done “cybersecurity work” before? Can you do it again here? How shall we know?”

As participants in the education enterprise, an inherent bias of the researchers and this paper is that education and training is working. Providers educate on a selection of knowledge and skills that do generate value; we are now attempting to talk skillfully about it. As a metaphor, we are scientists working with the new tool of a microscope. We understand that a certain medicine is working, but we don’t know what components are most efficacious–we’ve only begun to name what we see.

The researchers acknowledge that the NICE Framework updates frequently in order to mature the field and improve practice across industry, government, and education bodies (National Institute of Standards and Technology, n.d.). There are related projects, working groups, and calls for improvement to the basic building blocks. The exploration into the efficacy of assessment requires that particular tasks, skills, and knowledge remain constant. A first discussion point to consider is:

- Which NICE Framework Task, Knowledge, and Skill statements are reliably constant?

Performance assessments

To capture the full breadth of what a performance may be, the term “Performance Assessment” is loosely used to describe action and doing. In an educational context, it often expresses the opposite of an objective examination where there is one single correct answer (typically chosen out of four). It suggests adaptability and flexibility while meeting the objective. Deliberately leaving the ambiguity of definition permits broad interpretation which is useful in discovering its range and purposes.

To illustrate the discussion around “performance assessment,” take the example of the NICE Framework Task T0708 within the Threat/Warning Analyst work role:

T0708: Identify threat tactics and methodologies.

As a statement, the intent seems clear and purposeful as “cybersecurity work” even without the context of the business objective, which may provide further context, e.g., against companies in a specific industry or against a particular technology. The ability to fully initiate and complete the task surmises a grouping of skills and knowledge. Within the NICE Framework, these statements are grouped together, but not explicitly and logically connected. Some examples include (but not exclusively):

Knowledge:

- K0604: Knowledge of threat and/or target systems.
- K0612: Knowledge of what constitutes a “threat” to a network.

Skills:

- S0229: Skill in identifying cyber threats which may jeopardize organization and/or partner interests.
- S0256: Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships (Cybersecurity & Infrastructure Security Agency, n.d.).

The creation of a performance assessment includes discussion identifying which knowledge and skills are required to do the task, along with the content that would support its acquisition. Once identified, instructors, instructional designers, or assessment developers determine how the task can be demonstrated both in what format and in what context. Formats can include short narrative responses explaining the process or longer hands-on experiences that simulate and use technology experiences. In this example, students can be introduced to a general context and a threat actor and be asked to provide common examples in a written format. Alternatively, the students can demonstrate competency by accessing a simulated database on a virtual network, use tools to test for exploitations, and share findings in a report.

After the “how” is identified, the assessment discussion moves into “to what extent or degree of proficiency.” Bloom’s taxonomy, a decades-old theoretical framework to help educators categorize learning goals, is often used in academia and is a common touch point for addressing particulars. Bloom’s taxonomy references cognitive levels such as remember, understand, apply, analyze, evaluate, and create. The Skills Framework for an Information Age (SFIA) is used within business contexts and is an experience-based framework based on levels of responsibility and skills. Recent NICE Framework updates include a new release entitled *Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework* for use in the workplace (NICE Program Office, 2022). Alternate taxonomies and learning theories provide differing nuances to address proficiency.

Typically, instructors use expert judgment via tools such as rubrics in order to evaluate a submission’s proficiency. In this example, students may be evaluated on

- (Category 1) their ability to identify threat tactics,
- (Category 2) their ability to explain processes or methodologies,
- (Category 3) their ability to evaluate risk and impact,
- (Category 4) their ability to adhere to a set methodology of incident response, or
- (Category 5) their ability to proficiently use tools.

There may be many more categories. These categories may have various relative weights, importance, and evidence. For example, does the evidence provided align to junior, mid-level, senior, expert levels? Are they 50%, 75%, 90% proficient? Does the learner display creativity or process-thinking or troubleshooting? Which category is most valuable to this task?

Moving forward from a single task, the evaluators are also faced with ensuring authenticity of the submission and ensuring it is scored in a valid and reliable way. Is the submitter who they say they are? Is the work original? Would another expert score them differently? Is there variation in how a category could be scored?

As this is just one task, in a work role of nearly 30 tasks, the job of creating performance assessments is time and labor intensive. The ongoing operational support to administer the assessment, especially at scale, is similarly resource intensive.

For many education and training providers, this type of work and assessment is part of the nature of teaching students, even if it's not explicitly stated or logically mapped. Even if current practices do not have reportable evidence on assessment efficacy, graduates are still hired and retained by employers to do “cybersecurity work.” The on-going work is to provide more information to students and employers so that they can align individual capabilities to the organizations needs. New initiatives such as the Open Skills Network are working to bridge that gap ("Open Skills Network," n.d.).

Discussion points

- As there are many NICE Framework Tasks to evaluate, how can instructors quickly create performance assessments?
- Which learning taxonomy is most appropriate for cybersecurity? Does that change according to learning context or in alignment with other NICE initiatives?
- Which components of Performance Assessment evaluation will be most important to assess accurately and why?

Who provides performance-based assessments? Where and when do they happen? What do they look like?

Education and training providers

The discipline of cybersecurity is taught through all typical venues, informal and formal, online or in-person, synchronously or asynchronously. The scope of this discussion focuses on formal providers: traditional education (e.g., universities, colleges, and schools) and the consumer-focused training such as certification providers and bootcamps. Apprenticeships in cybersecurity constitute another formal pathway that are nascent and emerging.

For the audience of the NICE community, only a brief introduction to college programs is necessary. Cybersecurity degrees are typically born out of computer science departments, either as specializations or full degree programs. There are associate, bachelors, masters, and doctorate degrees. Most schools are accredited by organizations recognized by the Department of Education. Many schools seek designation as Centers of Excellence by the National Centers of Academic Excellence in Cybersecurity managed by the National Security Agency’s (NSA’s) National Cryptologic School as an additional measure of quality.

The National Initiative for Cybersecurity Careers and Studies (NICCS) Education and Training Catalog is aligned with the NICE Framework and is a central repository for finding other formal training opportunities ranging from full degree programs, online courses, in-person training directly aligned to a certification, and week-long bootcamps (Cybersecurity & Infrastructure Security Agency, n.d.). These training providers typically teach the skills for career success and can provide certificates of completion, but differ strongly from achieving a certification.

Cybersecurity apprenticeships offer a valuable approach to developing practical skills in the field, placing emphasis on hands-on experience and guidance from experts. Apprenticeships prioritize the opportunity to engage in real work, allowing apprentices to apply their knowledge and techniques in real-world scenarios. The absence of written tests in apprenticeships reflects the focus on practical proficiency rather than theoretical understanding. Instead, apprentices are immersed in the actual work environment, collaborating with seasoned professionals who provide mentorship and guidance throughout the learning process. This apprenticeship model not only fosters the acquisition of essential cybersecurity skills but also cultivates adaptability, critical thinking, and problem-solving abilities. Apprenticeships are labor and resource intensive, requiring significant investment from the organization and the learner.

These education providers teach cybersecurity skills and generally increase a learner’s abilities. The providers certify the investment of time and training by providing a degree or a certificate of completion attesting to the experience. Moreover, there is another avenue to attestation of ability and competency through certifications.

Certifications

Certifications are an attestation by a vendor or a third party that the certification holder has demonstrated through an evaluation that the candidate possesses the minimum skills necessary to be qualified on the certified subject matter. Generally, certifications are issued for a specific tool or subject matter and are not viewed as a license to practice (e.g., medical or teaching license). These providers offer exams that cover topics such as networking, cybersecurity, database management, software development, and more. Examples of well-known IT certification providers include CompTIA, Cisco, Microsoft, and AWS. Many providers offer a variety of certification levels, from entry-level to expert, to accommodate individuals with varying levels of experience and expertise.

Certifications signal mastery of domains or expertise, but how that is achieved depends on the certification provider and the subject matter being tested. Each method of evaluating a candidate has its strengths and weaknesses and can be used as a factor by candidates and hiring managers in determining the validity of the credential.

Exam Formats

The most common format is a proctored examination consisting of multiple-choice questions, where candidates select the correct answer from a list of options. This format is often used for entry-level or foundational certifications, as it can efficiently test knowledge and comprehension of key concepts. This method allows an organization to assess many candidates against a known foundational baseline of knowledge with a minimum of cost. These certifications are not typically considered hands-on or a performance assessment as the primary aim is to assess the candidates fundamental understanding.

As the market matures, along with the advanced nature of the subject matter, certifications are increasingly asking for demonstrations of performance as a part of the certification. A variety of formats may be used. A few examples include short answer and response questions, which require candidates to provide a brief written response to a prompt. This format can test deeper understanding and application of concepts and may be used for more advanced certifications. Some certifications may also have a practical component, where candidates are required to demonstrate their ability to use relevant tools and technologies to complete tasks or solve problems. This format can test practical skills in order to prove technical expertise. These tests are typically proctored exams that require a high degree of preparation and must be completed within an allotted time period.

There are other formats for completing certifications that differ in their quality criteria. Some tests are open-book, multiple choice tests without proctoring. Other tests provide students with an allotted time of 24 hours of access to the test scenarios and require a written submission of what the student accomplished. Some providers are subscription-based, permitting students to work through courses, content, and exercises and awarding a certification of completion. An examination can also be conducted orally (e.g., dissertation defense) or can have the candidate perform the tested function for a referee or panel.

Certifications may also be offered as short-term bootcamps, which provide an immersive learning experience that includes hands-on training, walkthroughs, practices, and outcome-oriented exams. These certifications signal their value through participation in the activities of the subject-matter, whether a final exam is psychometrically validated is typically not advertised. This format can be beneficial for individuals who prefer an intensive learning approach and need to quickly gain new skills and knowledge. Ultimately, the certification examination format will depend on the certification provider and the specific subject matter being tested.

As part of their value proposition, certifications will provide exam outlines, lists of topics covered, and other basic logistical information. They will also often point learners toward partner learning resources for acquiring the ability to comprehend the learning objectives required to pass the test. Most tests are organically created based on market research of the skills required. Competency is the assessment of a candidate's ability to answer sufficiently that they meet the minimum scoring requirement of the certification exam. This is commonly referred to as a cutoff score. The cutoff score is established by the certification organization, sometimes with input from industry, academia or government to understand the requirements for a minimally qualified candidate. This allows any organization that hires a certified candidate to have a level of faith that the candidate can operate to at least the minimum standard as professed by the certification body.

Unlike how a student carries a grade point average (GPA) that provides another educator or university with an understanding of the precision by which a student may be capable (competent) for a specific class/course, certifications are commonly done as pass/fail. However, the strength of that model (each candidate meets the minimum qualification) means that a university could rely on that assessment as a means to grant credit for a similar course and allow the student to take a higher level course.

Discussion points:

- What makes a quality course, training, or certification?

Why does certification of experience matter?

Cybersecurity hiring practices

As shown in other work by the NICE community and cyberseek.org, most cybersecurity jobs are not “entry-level” (Meehan & Strickland, 2022,"Cybersecurity Career Pathway," n.d.). The current state of hiring maintains that there is an incredible demand for cybersecurity talent, but few direct pathways to secure the experience asked for in job postings. Although there is ongoing work to improve job descriptions and decrease minimum requirements, formal degrees remain important. Certifications are an alternate pathway to signaling expertise.

Certifications are used as a proxy for knowledge, skill or ability, as a requirement to occupy a position, and as a means of demonstrating the ability to learn and as a potential precursor for success. Recruiters may filter resumes or applications by looking for specific IT certifications that are relevant to the job requirements. Candidates who possess relevant certifications may be given priority consideration or seen as more qualified for the role. Additionally, IT recruiters may use certifications to validate a candidate's self-reported skills and experience.

Both degrees and certifications provide evidence to hiring managers that applicants have done some “cybersecurity work” previously, which may get them into an interview. Gaining an opportunity to interview is an important step to the process, but not the only step. IT recruiters may also take into consideration other factors such as experience, education, and soft skills when making hiring decisions. Some organizations assess technical skills via whiteboard problems, proposing theoretical situations, or demonstrating performance on a tool. Within the hiring process itself, lies opportunities to demonstrate performance of work role tasks.

Certification value

The value of cybersecurity certifications can be difficult to define and quantify, as it can depend on various factors such as specialization and industry recognition. Certifications that cover emerging technologies or specialized areas, such as cloud security or penetration testing, can hold significant value in the job market as they demonstrate expertise in areas that are in high demand. Brand name recognition can also play a significant role in the value of a cybersecurity certification. Certifications from well-known and respected organizations, such as CompTIA, ISC2, or SANS, can hold more weight and value in the industry due to scarcity, their reputation for rigorous training, and testing standards.

Along with brand name recognition is its inclusion on the Department of Defense (DoD) Approved 8570 Baseline Certifications list. (DoD Cyber Exchange, n.d.) This list provides an equivalency to a DOD ranking of expertise, much like a transfer credit of course requirements met at a college. The Cybersecurity field has strong ties to defense and military organizations and having employees with a certain number or type of certifications can be advantageous to contracting requirements.

Finally, learners may already have competency and ability in a certain area. A certification is a low-cost and lower-time commitment to signal to employers that they have requisite experience. Ultimately, while it can be difficult to quantify the value of cybersecurity certifications, they can provide professionals with valuable skills and knowledge that can help them stand out in a competitive job market.

Discussion points:

- What market data is available to differentiate between the value of each experience?
- Are there coherent and consistent employer strategies to differentiate between candidates with formal degrees, training, and certifications?

Problem summary

To this point, we have worked to raise awareness of the value and importance of assessment in performing NICE Framework Tasks–good assessment is beneficial for learners and employers. It is abundantly clear that many providers provide different opportunities in various formats to learn and practice “cybersecurity work.” Some providers attest through certifications that learners are competent and capable.

These organizations (Traditional Education, Certification Providers, and Employers) are clearly creating standards, defining content, and evaluating proficiency. Within the NICE community, there is clear opportunity for wider partnership in aligning NICE Framework Task, Knowledge, and Skill statements.

At this point, we turn to discovering what performance-based assessments look like in practice–among current educational practitioners, among hiring managers, and in certifications. In order to ensure that academic degree programs and industry-recognized certifications effectively measure NICE Framework Tasks, we begin by surveying the landscape of what is currently in practice.

Performance Assessments in Practice

The project team took a three-pronged approach to examine the extent to which different providers used performance assessments to educate, recruit, and train the cyber workforce, especially the IT industry. First, the researcher surveyed a diverse set of participants from different colleges and universities to gather information about their current practices related to providing and implementing performance-based assessments. The survey asked participants to respond to questions about the types of performance assessments used, how they are administered, and the challenges faced when implementing them.

Second, we surveyed a diverse set of professionals from a large alumni group to understand the approach used to recruit and hire employees. These professionals are responsible for performing and managing IT-related tasks across the public and private sectors and possibly have firsthand experience with the benefits or limitations of signaling proficiency in their respective fields. The researchers asked participants to provide feedback about using performance-based processes to hire employees and the effectiveness of those processes.

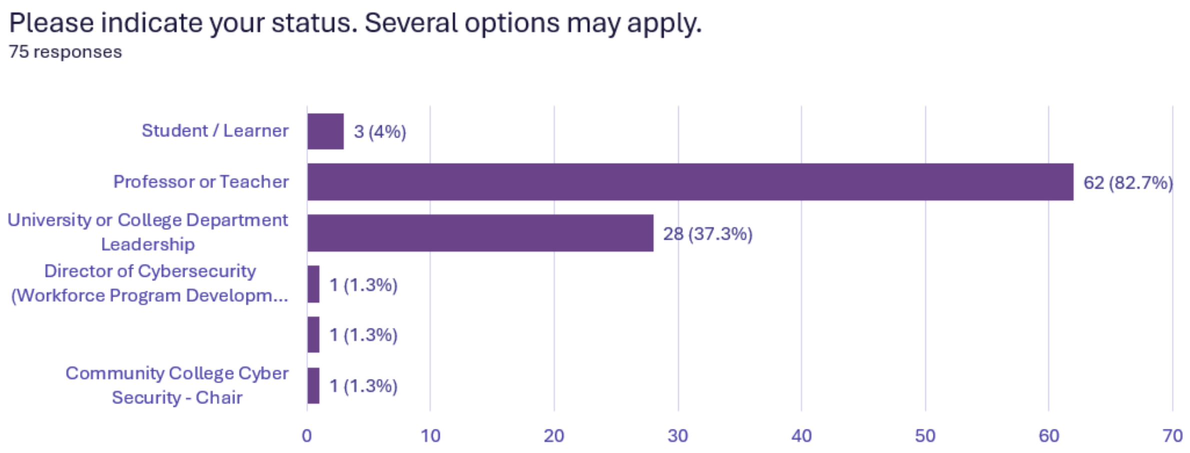
Third, we reviewed multiple IT-related certifications from Paul Jerimy's Certification Roadmap (Jerimy, n.d.) to gain insights into how different providers evaluated the skills and knowledge of professionals within the IT industry. The roadmap identifies multiple certifications in IT-related fields, including communication and network security, security architecture and engineering, asset security, security and risk management, security assessment and testing, software security, and security operations. Using the different IT-related certifications, the researchers performed the following actions:

- judgmentally estimated and categorized the experience level of the certification exam as beginner, intermediate, or expert level;
- identified certifications listed in the DoD-approved certifications;
- determined whether the certifications used multiple-choice or fill-in-the-blanks questions to assess a candidate's aptitude;
- determine whether the certifications used performance-based assessment requiring a candidate to demonstrate knowledge through simulation, lab, and other requirements; and
- determine whether the certifications used a mixture of multi-choice and performance-based assessments.

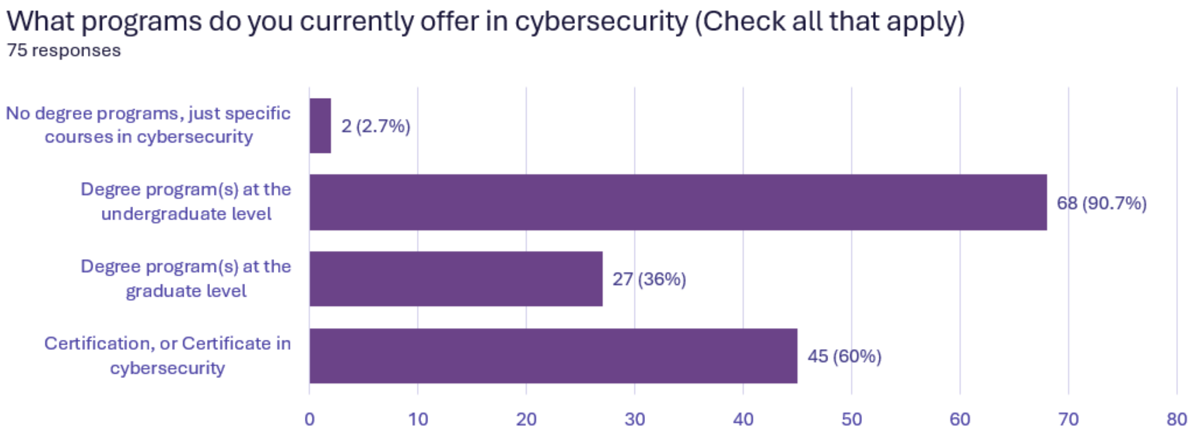
Performing the above actions allowed us to gather and analyze pertinent information related to the use of performance-based assessments. Overall, the researchers used the information to gain insights into the extent to which different providers used performance-based assessments to educate, recruit, and certify the cyber workforce, especially personnel in the IT industry.

College survey

We created and sent a survey to colleges and universities that are designated as National Centers of Academic Excellence in Cybersecurity (NCAE-C). The majority of respondents to the college survey were professors (82.7%, 62 of 74 responses), clearly the direct implementers of courses, assessments, and experience. A minority group (37.3%, 28 of 74 responses) represented college department leadership. The learning experiences exist within a typical college format—courses with lectures and activities over a standard term within a degree program with a small group of students. 90.5% of respondents offered degree programs at the undergraduate level. 36.5% had graduate level degree programs and almost 60% offered a certification or certificate in cybersecurity.

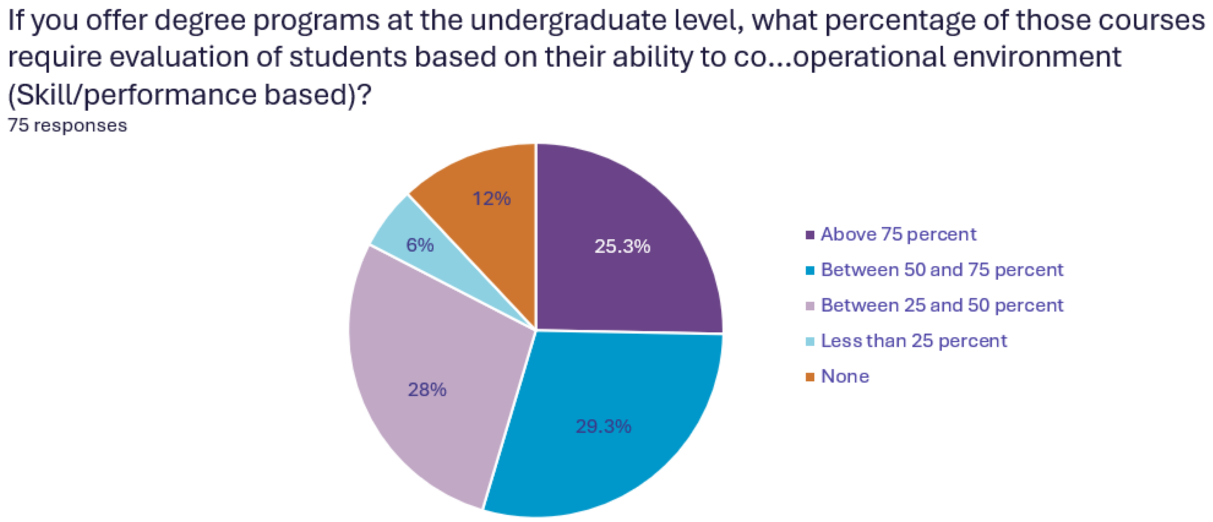


Please indicate your status. Several options may apply.
75 responses



What programs do you currently offer in cybersecurity (Check all that apply)
75 responses

As a degree program represents a significant period of time to interact with students, over 50% of respondents required evaluations of simulated tasks in more than 50% of their instruction. A small minority (17.6%) had less than 25% or no simulated operation environments.


If you offer degree programs at the undergraduate level, what percentage of those courses require evaluation of students based on their ability to co...operational environment (Skill/performance based)?
75 responses

In an open response field, respondents described their performance assessments in a variety of formats:

- Participation in hands-on practices guided by instructors. Instructors would demonstrate a tool or exercise and offer students the ability to follow along.
- Term papers and research projects on various topics including technical components and written explanations.
- In an example of community partnership, students perform for external stakeholders who then submit a survey evaluating the student's performance.
- Many instructors design custom hands-on labs performed on a network they've designed where students can perform tests and objectives.
- Many reported using pre-built simulated lab environments provided by an external vendor. These experiences include connecting to a pre-populated virtual machine. Students follow instructions or meet an objective by investigating the VM or the scenario. These are individual labs or access to an entire cyber range with a scale of task completion. Some cyber range activities are scored by completion or required tasks. *Thirteen responses specifically mentioned cyber range activities*.
- Certain coursework directly aligned with outside certifications and the performance required by those certifications, specifically in problem-based questions.
- Various departments partnered and collaborated with outside organizations to provide access to infrastructure. The NICE Challenge Project provides challenges that students can experience. Project PISCES is a public infrastructure collaboration where students have controlled access to real networks and can investigate areas of concern. The Virginia Cyber Range is a

state initiative that provides a courseware repository for educators and a cloud-hosted exercise area environment.
- Degree programs provide credit for internships and apprenticeships that are locally coordinated. Students work alongside professionals to provide value to the company for practical learning experiences.
- A final professional project/capstone, usually guided, like a thesis or semester long inquiry and exercise. One school appoints the leader of the approved project to create a student team to implement the project, which is then externally vetted by professionals.
- Many schools host clubs and participate in competitions that tend to be extra-curricular in nature. Students work through Capture the Flag exercises with or against competing teams. Subject Matter Experts host webinars and demonstrate tools that students use in the competitions.

Many of these experiences are broadly described and differ in quality, though the inherent value is in the “time on task” and “hands on keyboard.” As most departments and courses are developed by individual faculty, the instruction meets the local needs of students in their various contexts. Outside of using pre-packaged content from well-established organizations, such as the NICE Challenge Project, there is a wide variety of how activities aligned to NICE standards are utilized in the learning experiences.

In a series of questions asking respondents about whether their performance assessments align with NICE Framework Work Role Categories, most respondents share that their programs cover the 7 category areas.

Specialty areas in Protect & Defend and Investigate were the highest reported areas (above 60%). Specialty areas in Collect & Operate and Oversee & Govern were the lowest reported areas (under 40%).

There was strong representation in specialty areas that are directly technical in nature, such as Network Services (85.3%) and Digital Forensics (72.3%).

The lowest reported specialty areas are Technology R&D (8%), Language Analysis (14.7%), and Executive Cyber Leadership (14.7%).

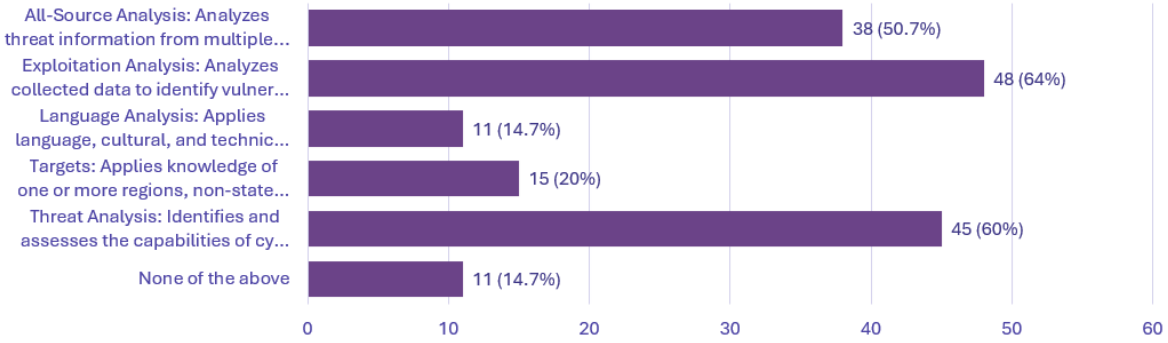
Each category had between 5% and 35% of “none of the above” responses with the relative ranking of lack of performance assessment as follows:

- Collect & Operate (35.1%)
- Oversee & Govern (25.7%)
- Securely Provision (18.9%

- Investigate (17.6%)
- Analyze (14.9%)
- Operate & Maintain (5.4%)
- Protect & Defend (9.5%)

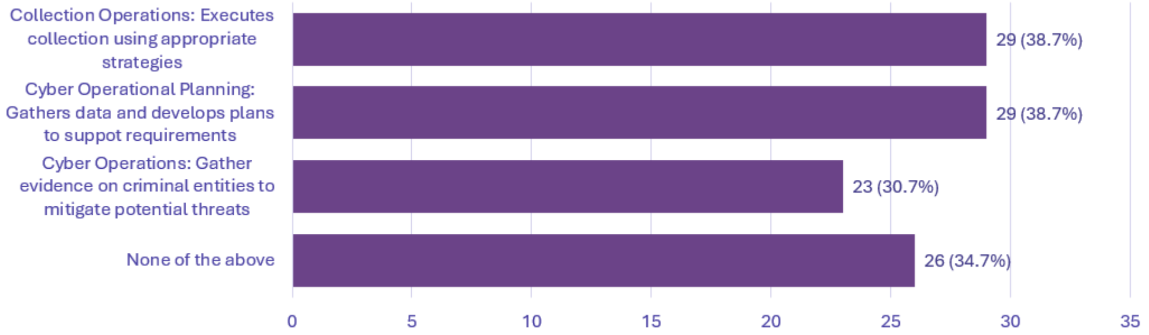
ANALYZE: Does your school utilize performance-based assessments to demonstrate students skills to (can be more than one answer):

75 responses



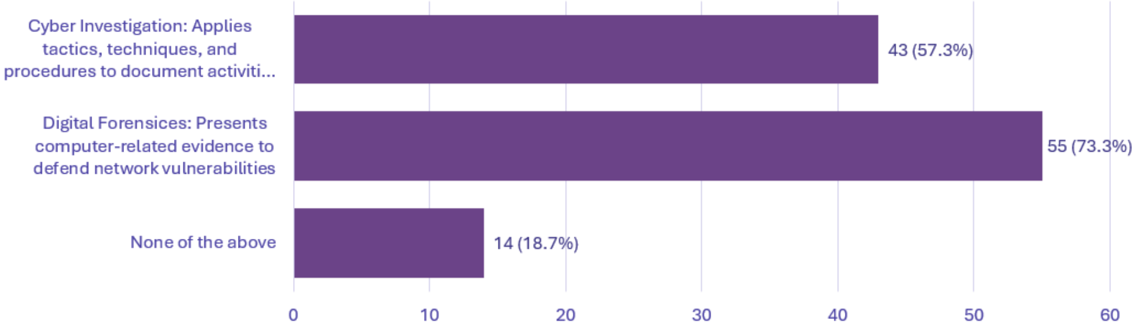
COLLECT & OPERATE: Does your school utilize performance-based assessments to demonstrate students skills to (can be more than one answer):

75 responses



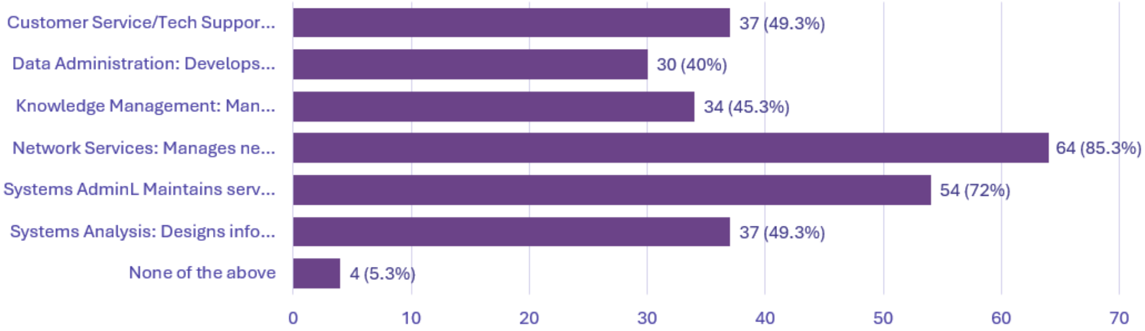
INVESTIGATE: Does your school utilize performance-based assessments to demonstrate students skills to (can be more than one answer):

75 responses



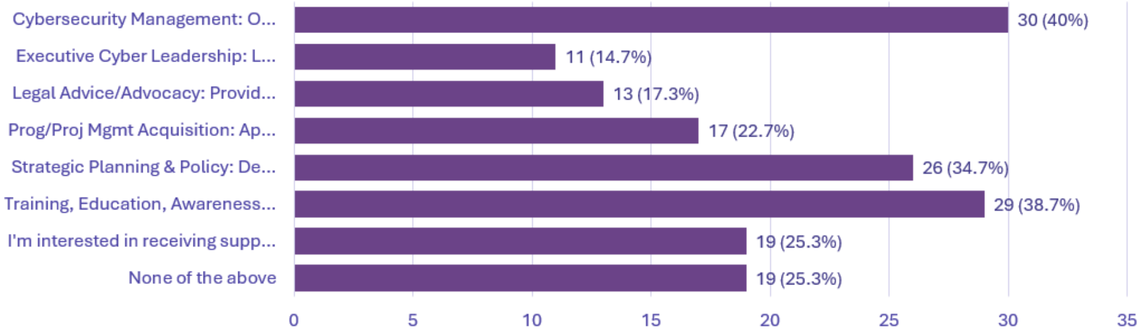
OPERATE & MAINTAIN: Does your school utilize performance-based assessments to demonstrate students skills to (can be more than one answer):

75 responses



OVERSEE & GOVERN: To support cybersecurity activities, please indicate what areas your program highlights. (More than one answer may apply.):

75 responses



Limitations and discussion

The limitations of this particular survey is that respondents were voluntary and were a subset of colleges and universities that are part of the NICE Community. This is broadly the target of the survey—practitioners using performance assessments aligned to NICE. However, standard survey biases apply to the rigor of the instrument as its primary purpose was to provide preliminary qualitative data.

Relating back to the strategy of 2.4.1 Raise Awareness of the value and importance of using performance-based assessments to measure competencies and the capability to perform NICE Framework Tasks, clearly *most instructors value hands-on evaluations and are exemplary in their creativity toward student success*. This is evidenced by the wide variety of examples of performance-based assessments received in the survey responses.

The discussion of this data follows that most cybersecurity performance assessments are locally sourced and are ad hoc implementations at a small scale. There is bias in that most respondents are professors, but the results indicate small, personal efforts aimed at student success. Smaller schools with smaller enrollment and smaller budgets are less likely to be connected to strong industry players and have institutional contracts, especially as cybersecurity is still emerging as a field. These respondents are creative in their implementations and skillsets. They show their devotion to student success by partnering with local industry, providing extra-curriculars, and building their own assessments. This particular group of constituents may benefit most by becoming aware of duplicative efforts, free or low-cost curriculum options, and by sharing ideas with one another.

In terms of alignment with NICE Framework Work Role Categories, there are specialty areas within categories that are underrepresented, possibly due to a few reasons. The first is the school’s alignment to market needs and relative alignment to the NICE Framework. In the case of the specialty area Language Analysis, the work role aligns to Multi-Disciplined Language Analyst which is not a commonly recognized job position nor likely has much local presence unless the school is connected to a government entity. There is more quantifiable student success in aligning to a higher demand field. Another possible explanation is the complexity of creating an environment or assessment to assess the specialty area as well as having university resources to support this boutique section of analysis. Not only is cybersecurity skill required, but also less-typical abilities in foreign languages and cultural expertise. Alternatively, more popular specialty areas use smaller scale technical expertise such as network configuration of firewalls or data forensics on a thumb drive can be created on an individual basis.

There is preliminary data to suggest an opportunity for many schools to find a legal and safe way to simulate performance within the Collect & Operate domain. Although this category, again, may not directly align to their target market, a specific and targeted simulated exercise could introduce students to the area. This could be an opportunity to explore various product companies and their portfolio so that a recommendation could be made to schools looking to implement this NICE Framework Work Role Category. For example, there may be an opportunity for vendors looking for an opportunity to obtain an Authorization to Operate (ATO) may work with government and academia to offer the tool in a limited government environment for real-world testing and use in exchange for the ATO approval. Other lower reported specialty areas may appropriately sit adjacent to what's considered core cybersecurity skills. For example, Legal Advice/Advocacy (17.3%), Prog/Proj Mgmt Acquisition (22.7%), or Test & Evaluation (22.7%) cross fields with other disciplines and may simply not be the focus.

This survey demonstrates that many academic programs directly relate to NICE Framework Work Role Categories, with future work needed to identify and showcase specific examples. From an open-ended response category, it would appear that there are participants willing to share their successes with a wider group. Findings support that there are strong categories and specialty areas that are currently in operation and proving student success.

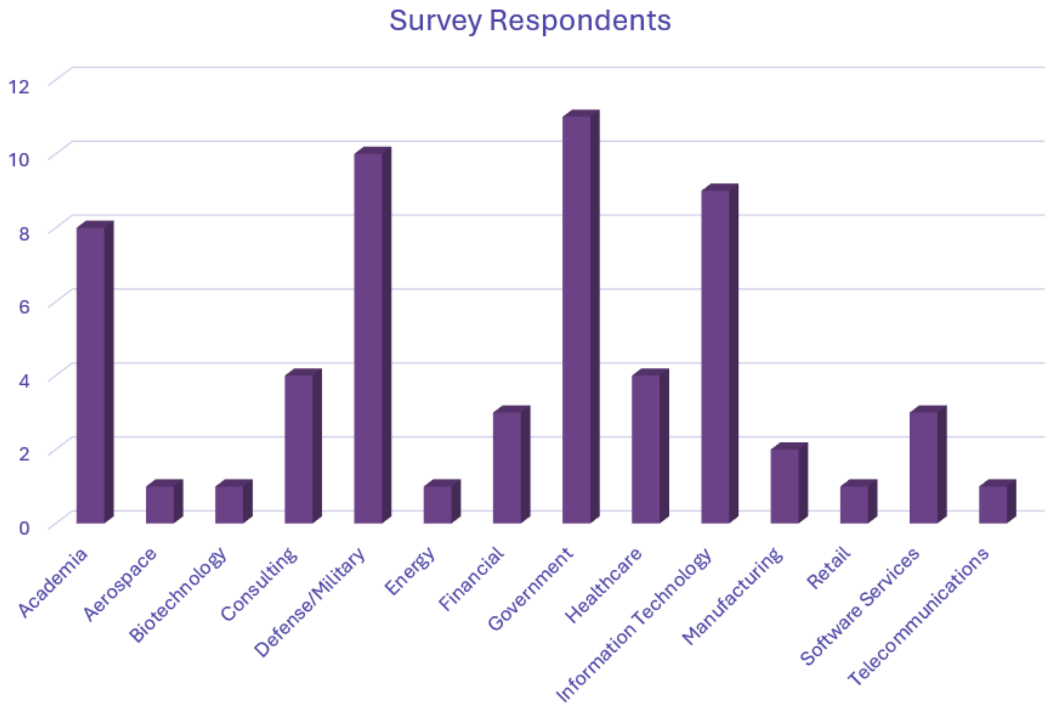
Discussion points:

- If most performance-based assessments are created and used on an individual level, how can we begin to compare efficacy across tasks? Is it appropriate to do so at this time?
- Which Work Roles (and subsequent Tasks) would provide a starting point for an in-depth look at performance-based assessments?

Pre-employment performance assessments

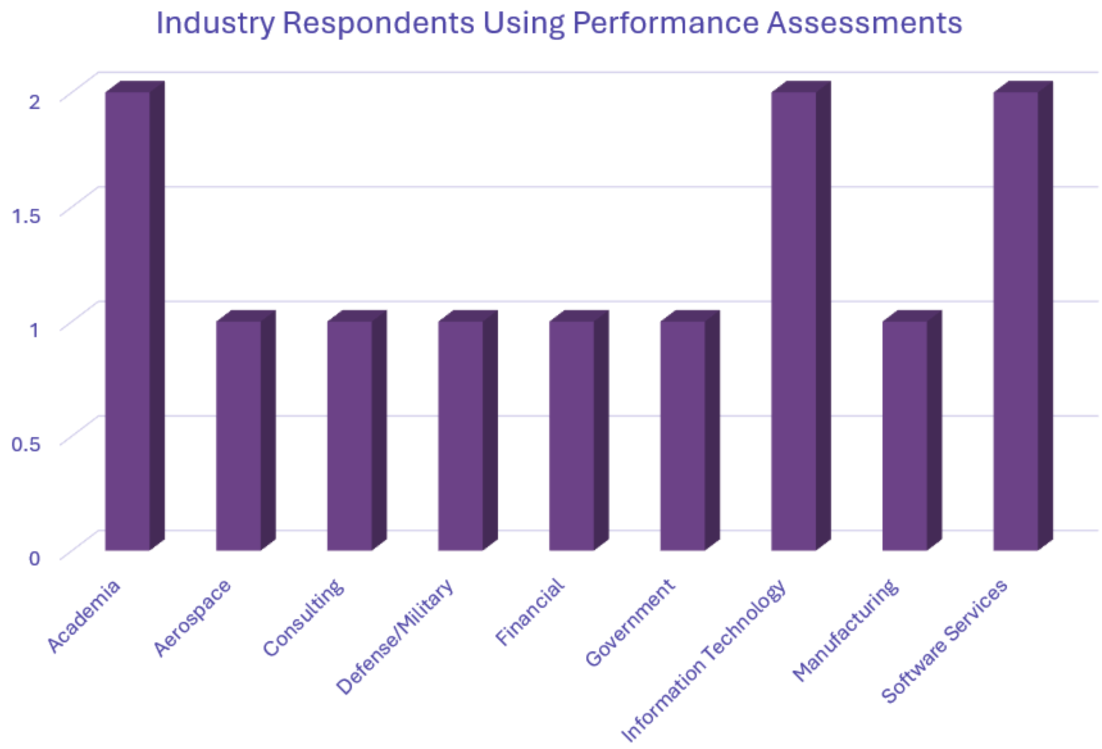
Part of the discovery effort around performance assessments is to understand how employers saw their importance. To start the discussion, the researchers sent a short survey to a large cybersecurity alumni group. The survey recorded the respondent's industry and role, and then followed with two questions: “Does your organization, as part of its normal interview process, utilize performance based (hands-on) tests to demonstrate a candidate's skills?” and “Has it been effective in finding qualified employees?”

Within the reported 60 roles, only two roles were duplicated, showing a great multiplicity of job titles. Similarly, a count of industries showed 22 separate industries, with a greater number in Government (10), Military/Defense (9), and IT Service (7 roles).



The results of the questions are:

- 76% of 60 employers surveyed indicate that they do NOT use a performance task during the interview process.
- The 23% of survey respondents that did use a performance task agreed in saying said “it has been effective to find qualified employees”



Limitations and discussion

The limitation of this particular survey is that respondents were voluntary and were a subset of one particular college’s alumni. Standard survey biases apply to the rigor of the instrument as its primary purpose was to provide preliminary data.

As a discovery process, the variety of roles and industry widely varied showing no one set of roles or industry where a performance assessment hiring practice standard. Conversely, a performance assessment as part of a hiring process is also not a rare occurrence. A hands-on assessment in an interview could be interpreted as a whiteboard scenario, familiarity with a tool and commands, or a take home assignment. The size, scope, and function will vary widely. These standard hiring practices were likely created in-house.

There are companies directly catering to preparing candidates for interviews. Although they typically include coaching, soft skills, and negotiation, there are also assessments for coding expertise and cybersecurity skills. These tests appear to be short (10-60 minutes), can extend to an allotted time such as a 24-hour take home assignment, or can assign challenges to be completed. The SANS CyberTalent Assessments offer 9 tests in topics of Cloud, Penetration Testing, and Digital Forensics. To draw a direct comparison—these outsourced tests are strikingly similar to a mini-certification!

A future discovery process could follow-up with various companies to catalog the types of hands-on activities within a hiring process. Alternatively, a working group could observe and identify various interview services that cater directly to cybersecurity professionals. This list could serve students and institutions in tightening the gap between graduation and first job by setting appropriate expectations and preparation.

Discussion points

- What is the infrastructure in place for employers and hiring managers to identify talent through performance-based assessments?
- Are current hiring practices sufficient for identifying the proficiency of candidates?

Certification landscape analysis

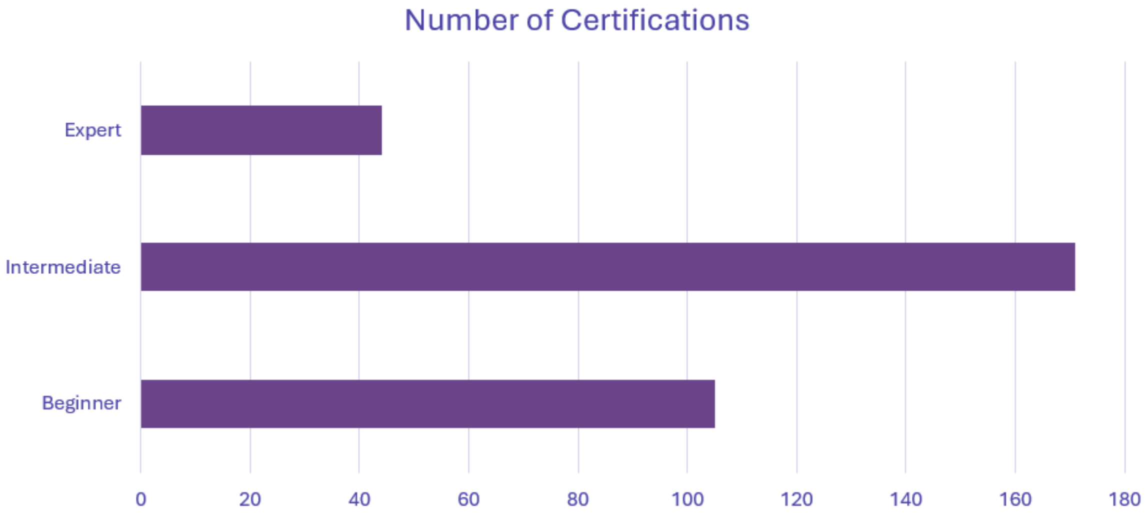
The major contribution of this discovery section is to provide a repository for cybersecurity-related certifications. With this initial step begun, the researchers analyzed the certification's components to ascertain the degree of practical or hands-on approaches. By identifying what exists across the competitive market, we can begin focusing our attention on major providers or through a campaign to urge general adoption of performance assessments.

This work credits Paul Jerimy's Security Certification Roadmap under Creative Commons Attribution-ShareAlike 4.0 International. The roadmap is an initial list of certifications grouped into 8 categories and visually shows relative positioning in terms of content covered and difficulty. Drawing upon this initial list, the working group created a spreadsheet to account for the names and locations of certifications. From this list, we categorized the certifications by whether they use multiple-choice questions to test the candidate's aptitude or if the test required a demonstration of knowledge through a simulation or lab.

From a collection of 339 certifications, less than 10% of beginning, intermediate, and expert certifications use performance assessments to train the cyber workforce:

- Beginning Level – about 4 percent using performance-based assessments
- Intermediate – about 9 percent using performance-based assessments
- Expert – about 5 percent using performance-based assessments

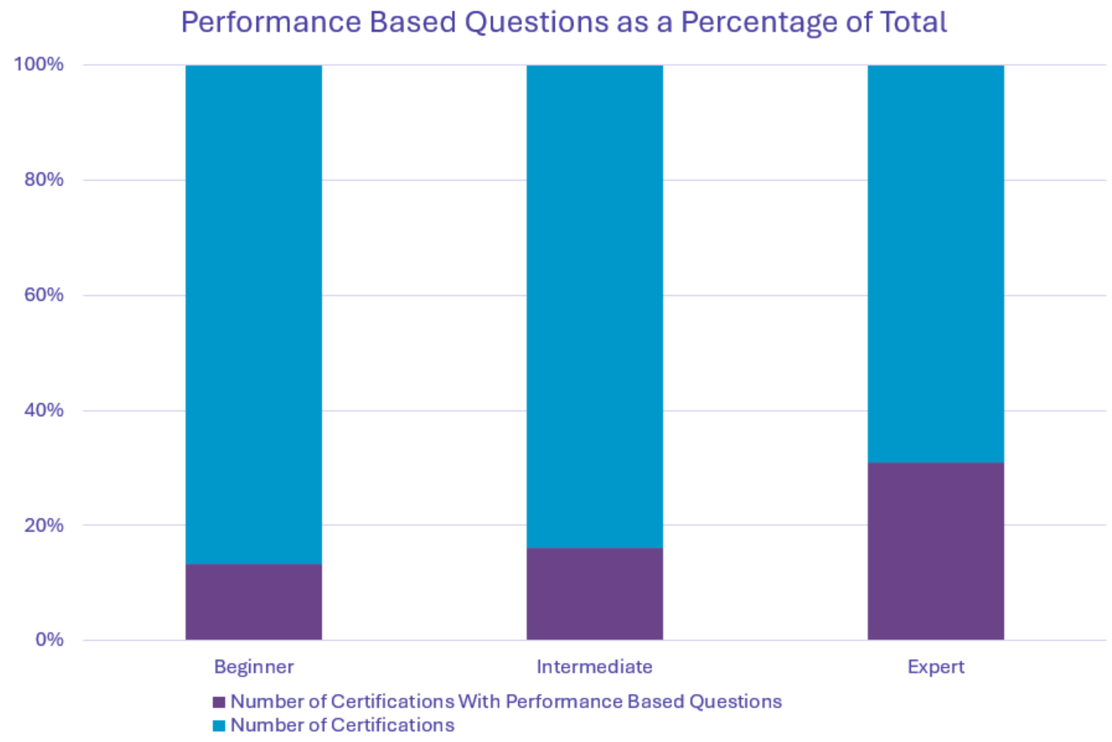
The researchers compiled data on cybersecurity certifications including if they awarded the certification based on passing a multiple-choice examination, used performance-based questions, or did both. Our sample set was divided into Beginner, Intermediate, and Expert-level certifications with a count of 105, 171, and 44 respectively.



Number of Certifications and Approximate Level of Seniority

The majority of certifications are proctored, multiple-choice tests. These, however, are not the only options as some certifications represent a completion of coursework or participation in a bootcamp. Although the majority of certification and training providers are not performance-based, there are many instances (notably CompTIA) where these providers are implementing performance-based items for all certifications regardless of difficulty.

The researchers discovered a trend of performance-based questions being used to assess and demonstrate knowledge in all certifications but with greater emphasis at the expert level.



Performance Based Questions as a Percentage of the Total

Expert-level certifications (31%) required the candidate to demonstrate knowledge through performance-based questions. For example, the Cisco Certified Implementation Expert (CCIE) - Security, requires the candidate to pass two qualifying examinations, one a traditional written exam and the other a hands-on lab. The lowest use of performance-based questions was at the Beginner level with 13.3% over 14 certifications and was predominantly covered by 4 CompTIA certifications accounting for 28.57%.

The researchers also examined the role of certifications that met DoD Instruction 8570 requirements and found of the 25 certifications captured within the dataset, only 4 utilized performance-based questions, accounting for 16% of the total.

Limitations and discussion

The initial list of data compiled is not comprehensive of all certifications but does represent a substantial number of players and certifications. As this first pass was to discover what existed, there is great variety as to format, type, and cost.

There are a lot of cybersecurity certifications! The wide availability demonstrates the breadth of the field and subfields in compliance, project management, and software. One can imagine that a list of over 300 certifications to choose from is difficult for both aspiring candidates and hiring managers. This invariably to the questions of “which are best”, “why?”, and “what should we tell our learners?” These are also the questions that providers ask in order to market their products as they vie for market share and initiate partnerships.

As noted in the prior section, it would appear that many schools and programs are focused locally. Certification providers are focused nationally (even internationally) and must be so for their business models. Here there is potential to illustrate what a high-level certification means in terms of actionable NICE Framework Tasks. There is potential for the NICE Framework Tasks to apply in local/regional contexts resulting in awareness-building case studies and examples. Again, simply “what can a person holding X certification do for me?”

In terms of performance assessments, there is potential in growing assessment capabilities of these certifications. With only 10% of providers using performance assessments, this is an avenue for differentiation among the many competitors.

Another insight gleaned from the data is that a generalizable "technical" skill set seems to be an implicit set of knowledge for advanced certifications. A general skill set would include tech savviness, knowledge of OS, programming, and networking knowledge. Cybersecurity grew out of information technology. However, as more work roles become available in the field and the background of future professionals expand, it may be necessary to question the assumptions of which implicit tech skills matter most for the task at hand. Again, an opportunity to further align framework tasks and prerequisite knowledge to the available certifications.

From this initial list of certifications, there is also an opportunity to formalize criteria for proficiency levels (e.g. basic, intermediate, and advanced) beyond the organization’s own marketing. In addition to the breadth and depth of content, the format of performance or demonstration could be included along with the context of the exam format (proctored, open book, timed), or even the cost. These criteria are open to discussion as they exist outside of a formal training organization and affect candidates holistically—some students do not seek certain certifications because of their time availability, distance from testing centers, or particular circumstances.

Discussion points

- How would we advise students and employers to look at certifications? Which has the most value and why?
- At what point does certification specialization break down where it is not meaningful to students and/or employers?

Conclusion

Performance-based assessments are a future-focused endeavor to train learners to do “cybersecurity work.” As the technology and frameworks change, we expect to see more discussion about how students practice the craft, how teachers evaluate their proficiency, and how useful are those assessments. A lot of the work is currently happening, but nailing down particulars is still underway. The current academic environment and certifications are similarly moving toward offering learners more hands-on opportunities to practice their craft.

This paper has shown that universities and colleges strive to incorporate performance-based assessments aligned to the NICE Framework, but most efforts are individual and small implementations. Similarly, a handful of hiring managers indicate that they are beginning to incorporate performance-based assessments in hiring practices. As for certifications, they are legion. They attest to proficiency, but relatively few incorporate performance-based assessments.

In reviewing this work and our objective, we return to the charter strategy 2.4.1 that focuses on raising awareness of the value and importance of using performance-based assessments. There exists a wealth of experience in building performance-based assessments within the cybersecurity community, both in academia and among certification providers. There is more work to do in identifying what is effective and what is aligned to NICE Framework Tasks.

References

Cybersecurity & Infrastructure Security Agency. (n.d.). NICCS Education and Training Catalog. Retrieved from https://niccs.cisa.gov/education-training/catalog

Cybersecurity & Infrastructure Security Agency. (n.d.). Threat Analysis. Retrieved from: https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/threat-analysis

Cybersecurity Career Pathway. (n.d.). CyberSeek. Retrieved May 11, 2023, from https://www.cyberseek.org/heatmap.html

DoD Cyber Exchange. (n.d.). DoD-Approved 8570 Baseline Certifications. Retrieved from https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/

Jerimy, P. (n.d.). Security Certification Roadmap. Retrieved May 11, 2023, from https://pauljerimy.com/security-certification-roadmap/

Meehan, P., & Strickland, N. (2022, November). Cybersecurity Career-Entry Guidance for Employers Project Team. Employer Perspective on Hiring. National Initiative for Cybersecurity Education Working Group.

National Institute of Standards and Technology. (n.d.). NICE Framework Resource Center. Retrieved from: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

NICE Program Office. (2022, August). Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework. Retrieved from https://www.nist.gov/system/files/documents/2022/08/03/NIST%20Measuring%20Cybersecurity%20Workforce%20Capabilities%207-25-22.pdf

Open Skills Network. (n.d.). Retrieved from: https://www.openskillsnetwork.org/

Petersen, R., Santos, D., Wetzel, K., Smith, M., & Witte, G. (2020, November). SP 800-181 Rev. 1 Workforce Framework for Cybersecurity (NICE Framework). Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Appendix

This paper aligns to the NICE Strategic Plan Implementation Plan in the following areas:

Strategy 2.3.1 Articulate a common definition of credentials that includes a variety of examples for cybersecurity and shows alignment to the NICE Framework

Tactic	Success measure	Evidence
Review and promote a variety of different types of credentials, including degrees, diplomas, licenses, certificates, badges, and professional or industry-recognized certifications.	Evidence of the development of a Cybersecurity Credentials Resource Page	This paper provides a repository of available industry-recognized certifications in the marketplace.
Differentiate credentials, as necessary, by proficiency levels (e.g., basic, intermediate, and advanced)	Evidence of the development of a NIST Publication on Proficiency Levels that provides examples of application to credentials	This paper provides a repository of available industry-recognized certifications in the marketplace, with an initial ranking according to difficulty as a starting point.
Clarify the purpose of a credential when a learner already has the skill	Evidence of how skills can be communicated or documented without a corresponding credential	This paper's Understanding the Problem addresses many components of the value of certifications.

2.3.2 Seek evidence to document and communicate the value of credentials for cybersecurity careers

Tactic	Success measure	Evidence
Describe and differentiate the value of credentials derived from education (2 or 4 year or graduate or professional degrees), training (industry-recognized certifications), on the job learning, or self-paced learning (e.g., MOOC's)	Evidence of a report and other evidence of effective methods or systems for assigning value to credentials	This paper provides a starting point for describing the differences between various learning experiences.
Show the relationship between the effectiveness of the "learning process" for knowledge and skills development and the resulting "credential"	Evidence of a direct connection between described learning outcome and resulting competency	This paper provides a brief discussion of the learning process and the achievement of competency.

2.3.3 Increase the accessibility and affordability of credentials for cybersecurity

Tactic	Success measure	Evidence
Increase awareness of available credentials for cybersecurity-related competencies or work roles	Evidence of a repository or clearinghouse for cybersecurity-related credentials	This paper provides a repository of available industry-recognized certifications in the marketplace.

Strategy 2.4.1: Raise Awareness of the value and importance of using performance-based assessments to measure competencies and the capability to perform NICE Framework Tasks

Tactic	Success measure	Evidence
Describe the purpose and benefits of using performance-based assessments to employers, learners, and education and training providers	Evidence of documents, pamphlets, and online materials that describe the purpose and benefits of using performance-based assessments to employers, learners, and education and training providers	This paper's Understanding the Problem addresses many components of the purpose and benefits of using performance-based assessments.
Identify examples of performance-based assessments (best practices) to raise awareness of what they are	Report that documents current examples of performance-based assessments (best practices)	This paper's Understanding the Problem addresses many components and considerations in building performance-based assessments.
Encourage academia to provide more opportunities for hands-on experiences	Evidence of academic institutions providing more varied opportunities for hands-on experiences	This paper's College Survey shares examples of academic institutions and the hands-on experiences provided. More information could be mined from the open response text within the survey.

Strategy 2.4.2 Work to ensure that academic degree's programs and industry-recognized certifications effectively measure the ability to perform NICE Framework Tasks

Tactic	Success measure	Evidence
Partner with other organizations (to include the Center for Academic	Evidence of an increasing number of certifications that are based on NICE Framework	This paper provides a repository of available certifications in the

Excellence in Cybersecurity and the NSA) to foster the development of methodologies to enhance abilities to measure competencies, particularly skills to perform NICE Framework tasks	tasks	marketplace. Future work could look into how a subset of certifications align to the NICE Framework tasks. It also references the document provided by NICE entitled: Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework
Develop and publish a set of best practices for the development of performance-based assessments (such as the latest techniques for computer-based testing) – this will include process of converting from knowledge-based questions to performance-based questions	Evidence of partnerships with other organizations that foster the development of methodologies to enhance abilities to measure competencies, particularly skills to perform NICE Framework tasks	This paper references the document provided by NICE entitled: Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework along with the Open Skills Network.
Encourage academia to provide more opportunities for hands-on experiences	Evidence of academic institutions providing more varied opportunities for hands-on experiences	This paper’s College Survey shares examples of academic institutions and the hands-on experiences provided. More information could be mined from the open response text within the survey.