Why Cyber Certifications Matter

As the cybersecurity industry continues to grow and mature, there is an increasing need for validation of critical skills—both for individuals and for the security teams that protect organizations and nations. For more than 20 years, cybersecurity certifications have served as a cornerstone of workforce development, evolving alongside the industry to meet changing threats, technologies, and job requirements.

As training options expand, the narrative around certifications has become muddled with myths that often overlook their real-world value. Below, we address some of the most common misconceptions.

Myth vs. Reality

Myth: Certifications only test knowledge, not skills

Reality: Certifications are developed by active practitioners who perform these roles in real-world environments. Skills are assessed through multiple methods, including scenario-based questions and lab-based testing—similar to how doctors demonstrate competency through hands-on practice. Certifications are aligned with cyber role frameworks such as NICE, ECSF, and DoD 8140, ensuring they reflect practical, job-relevant skills that can translate between industries.

Myth: Certifications are outdated and misaligned with real-world tasks

Reality: Certifications follow best practices that require continuous review and updates. Exam objectives are regularly evaluated and revised by committees of practitioners actively working in

the field. Their ongoing relevance is validated by market adoption and continued growth across the industry.

Myth: Cyber ranges are the future; certifications are the past

Reality: Both serve essential and complementary roles. Cyber ranges are valuable for practicing skills in simulated environments, while certifications validate that those skills meet an established standard. Many certification bodies also operate cyber ranges to help learners assess strengths and identify gaps. Confusion often arises when cyber ranges are positioned as a replacement for certification rather than a supplement. Additionally, as “cyber range” has become a buzzword, it is sometimes used loosely in marketing, further muddying its purpose and value in the marketplace.

Myth: Certifications are barriers rather than enablers

Reality: Certifications developed by C3 members follow international best practices rooted in over a century of skills validation across professions such as medicine, education, and accounting. Psychometric analysis is applied to ensure fairness across demographics and global populations, making certifications legally defensible and equitable. Certifications are often far more affordable than academic degrees, widely respected by hiring managers, and valuable during audits. Many certification bodies also offer scholarships and are increasingly supported by federal and state funding for disadvantaged learners.

Myth: Certifications neglect experience, critical thinking, and soft skills

Reality: Certifications emphasize critical thinking through scenario-based and lab-based testing. Some certifications in cyber require documented professional experience before credentialing. Certifications establish a baseline standard of competence, similar to a medical license or driver’s license—it validates readiness, not mastery. Experience and soft skills are developed through practice, while certifications confirm capabilities required of the practice/profession.

Myth: Certifications focus only on passing exams, not lifelong learning

Reality: Lifelong learning is a core requirement. Certifications mandate continuing education, regular renewals, and proof of ongoing professional development—similar to requirements in medicine and other regulated professions. Certification bodies continually introduce new credentials to address emerging areas such as AI, cloud security, and critical infrastructure.

Why Certifications Remain the Gold Standard

Certifications remain the gold standard in cybersecurity because they are subject to rigorous external oversight, including ANAB accreditation**.** Their effectiveness is continually evaluated through international standards for certification and skills validation, market adoption, and governance by experienced cyber leaders who design the credentials—from the objectives to the exam itself. As a result, external "ratings" of individual certifications by think tanks are often unnecessary, particularly when the evaluations are conducted by individuals outside the industry's stakeholders. The C3 strongly believes these established mechanisms—standards, practitioner oversight, and market validation—ensure certifications continue to meet the evolving needs of the cybersecurity workforce.

Revision History					
Version	Description of Change	Author	Approved By	Approval Date	Effective Date
1.0	• Initial Copy	Brian Correia	C3 Membership	02/17/26	02/17/26

