The Best Cybersecurity Candidate May Not Have the Certification You Asked For

By: Jaiz Anuar

31 August 2025 · Cybersecurity · Leadership · 8 min read

Certification is valuable evidence, but cybersecurity hiring must assess demonstrated capability, judgment, experience and potential.

Cybersecurity job advertisements often begin with a long list of required certifications: CISSP, CISM, CEH, CCSP, OSCP and Security+. Certifications can be valuable. They provide structured learning, introduce recognised concepts and show that a candidate has invested time in professional development.

But organisations should be careful not to confuse certification with capability. A certificate may confirm that someone passed an examination. It does not automatically prove that the person can investigate an incident, design a resilient architecture, challenge a weak recommendation or explain cyber risk to business leaders.

Cybersecurity certification should be considered evidence, not a verdict.

Certification is a signal

Hiring managers need efficient ways to screen applicants. When hundreds of applications are received, certifications provide a simple, recognisable filter. They suggest that a candidate has been exposed to certain frameworks, technologies or security concepts.

The problem begins when the filter becomes the decision. A candidate may have ten years of practical experience securing complex environments but be rejected because one certification is missing. Another may pass screening because several certifications appear on the résumé, even though that person has limited experience applying the knowledge in real situations.

Certification is one signal among many. Education, experience, judgment, communication, curiosity, ethics and the ability to learn are also signals. Strong hiring decisions examine them together.

Experience teaches what examinations cannot

Cybersecurity rarely operates under perfect conditions. Security teams deal with incomplete information, legacy systems, budget constraints, conflicting priorities and business deadlines. They must make decisions even when there is no single correct answer.

An experienced practitioner may know that a recommended control is technically correct but operationally unsuitable, and propose an alternative that achieves the same objective without unnecessary disruption. That judgment is difficult to measure through an examination.

Experience teaches how systems behave after implementation. A control may look effective in a design document but fail because of poor integration, weak ownership or operational complexity. The most valuable cybersecurity lessons are often learned during incidents, difficult projects and unsuccessful implementations. They do not always appear on a certificate.

Certification does not always prove readiness

A certified candidate may understand the definition of incident response, network segmentation or identity governance. But can the candidate apply that knowledge? Can the person investigate an unfamiliar environment, distinguish a critical risk from a theoretical weakness, explain excessive trust, communicate clearly when leaders need an urgent decision and acknowledge uncertainty?

Cybersecurity is not only a technical discipline. It is also a decision-making discipline. Organisations need professionals who can interpret risk, understand context and make proportionate recommendations across technology, operations, risk and business teams. A certification may support these capabilities. It cannot guarantee them.

Candidates without certifications must still demonstrate capability

The argument should not reject all certifications or assume experience is automatically superior. Years of experience do not always equal strong experience.

Candidates without certifications should be able to demonstrate what they know and have achieved: incidents handled, architectures reviewed, controls implemented and decisions influenced. They can describe what failed, what they learned and what they would do differently.

Practical assessments, scenario-based interviews and portfolio reviews can reveal more than a list of credentials. Hiring managers could ask how a candidate would respond if a critical control failed before go-live, assess a high-risk finding with low likelihood, manage a control that disrupted an essential process, challenge a security decision, or learn from a failed implementation.

These questions reveal judgment, curiosity, communication and practical reasoning. They show how candidates think, not only what they remember.

Potential also matters

Cybersecurity changes quickly. A person who does not meet every requirement today may still become an excellent professional if given the right opportunity and support. Curiosity, discipline and willingness to learn are particularly important. Technologies change, threats evolve and certifications expire, but the ability to question assumptions, investigate unfamiliar problems and learn from failure remains valuable.

Organisations that hire only candidates who already satisfy every requirement may overlook people with strong potential and make the cybersecurity talent shortage worse by creating entry barriers that are not essential to the role.

Hire the professional, not the credential

The best cybersecurity candidate may have the certification requested in the job description. But the best candidate may also have developed capability through years of incident response, architecture work, system administration, software engineering, audit, risk management or operational experience.

A certificate should strengthen a candidate’s profile. It should not automatically define the candidate’s value. Hire based on demonstrated capability, relevant experience, judgment and potential.

The objective is not to find the candidate with the longest list of credentials. It is to find the professional who can help the organisation make better security decisions when the answer is not already written in a textbook.

Question assumptions. Share knowledge. Build trust.