Results report

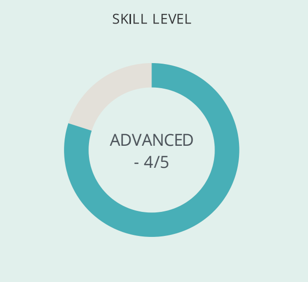
Adaptive CyberCitizen Skills Assessment

Skill Level: Advanced - 4/5

Time: 13:39

Test date: October 6, 2023

1. Result

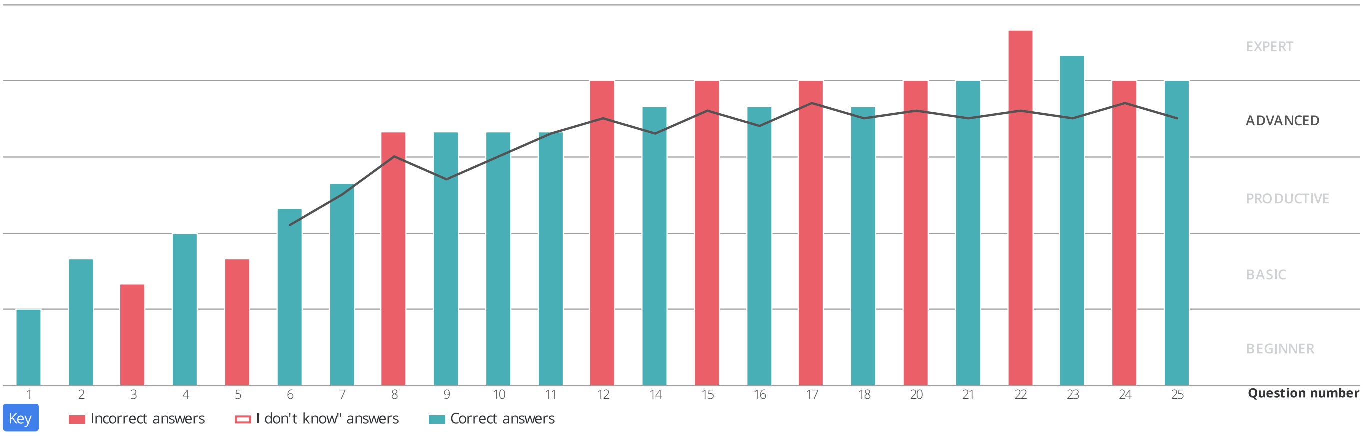


THE CANDIDATE HAS A STRONG MASTERY OF CYBERSECURITY KNOWLEDGE AND ATTITUDES IN THE PROFESSIONAL ENVIRONMENT.

2. Analysis

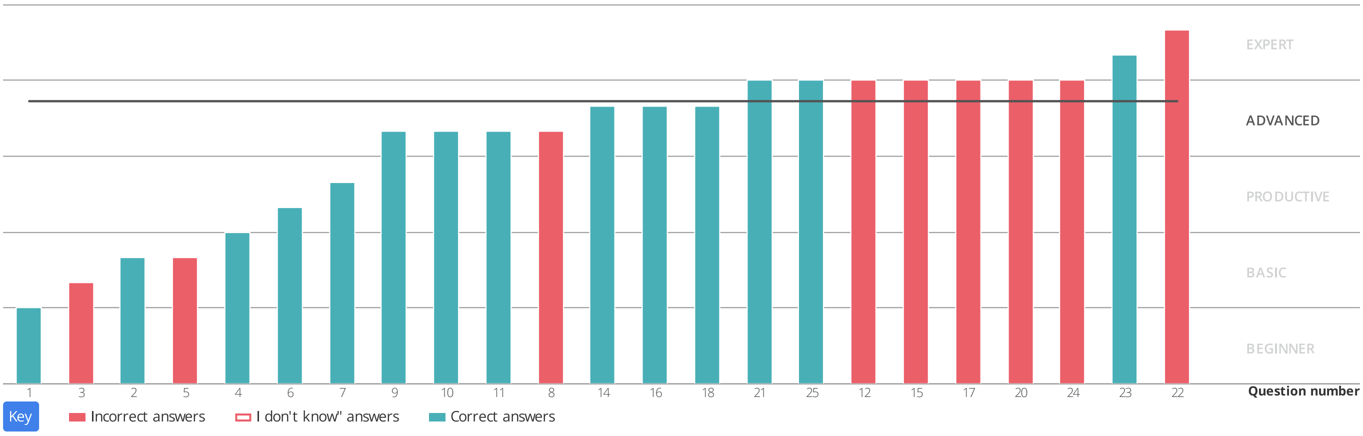
Progressive estimate of candidate level

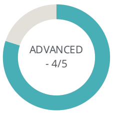
This chart shows how the system adapted the difficulty level of the questions to candidate responses as the test progressed. The grey line shows the candidate's estimated skill level before each question.



Questions ordered by difficulty level

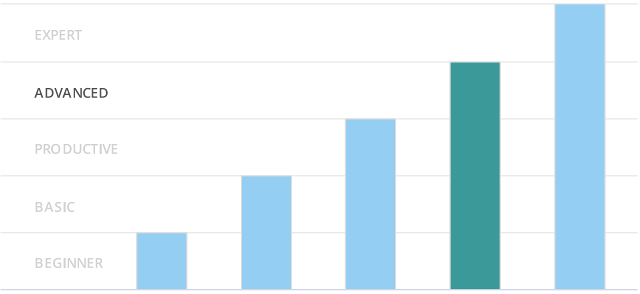
This chart shows the questions the candidate was asked, by level of difficulty.





3. Domains

The cybersecurity world



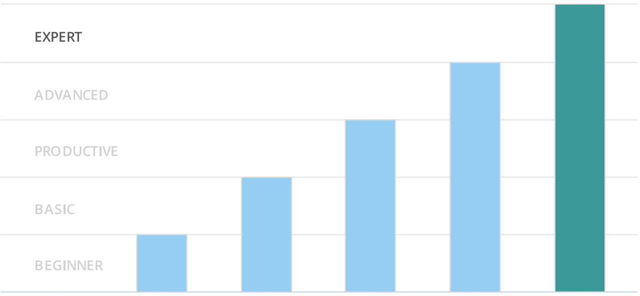
Level description:

Candidates are familiar with all the players (public, private, or individual) in the cybersecurity world, and knows when and why to carry out an intrusion test. They can evaluate the different potential impacts (short or long term) of an attack on a company. They can apply security procedures on their workstation in the event of an attack and collect evidence in case of an attack that could be useful to a technical expert. They fully understand the concept and services associated with authentication and can use a 2-factor authentication.

To go further :

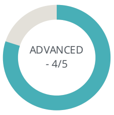
In order to reach the Expert level, candidates will need to be able to assess the criticality of potential attacks based on the unique needs of different companies. They will need to be able to quote and reference the ISO27001 standard, and will be able to identify and analyze the specific risks associated with various types of cyber attacks, including phishing, ransomware and DDoS attacks, within a given company or institution.

Security in the workplace

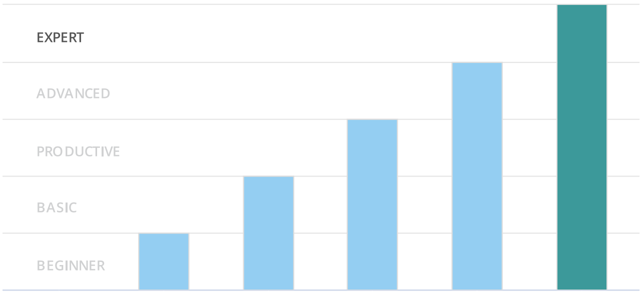


Level description:

Candidates can effectively transfer sensitive data securely, implementing encryption and secure protocols to safeguard information during transmission. Additionally, candidates can track the version of the operating system, ensuring that software remains up-to-date and secure against vulnerabilities. Furthermore, their proficiency extends to securely processing paper documents, employing strategies like physical access controls and document shredding to protect sensitive information offline. Finally, candidates should be capable of disabling a Windows process, a valuable skill when addressing security threats or optimizing system performance.



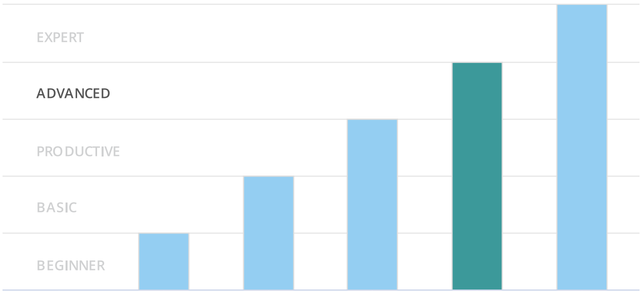
Security on the move



Level description:

Candidates can identify potential risks in a new environment, helping organizations preemptively assess and address vulnerabilities. They can distinguish the benefits and limitations of a professional mobile device management (MDM) service, recognizing how it can enhance device security and manageability while also being aware of its constraints. Additionally, they understand the advantages of using a proxy for security, leveraging it as a protective barrier between internal networks and external threats, while also acknowledging its potential impact on network performance.

Security at home



Level description:

Candidates can detect phishing attempts from various sources and channels (email, text messages, phone calls). They know how to react in case of a doubt to verify the source's legitimacy and know which authority to contact. They fully understand the features and benefits of cloud storage. They can explain the importance of data backup for business continuity (typically in case of a ransomware attack). They can protect their personal information and privacy at home or in a remote work environment. They have awareness of the risks related to their personal data exposure and their ability to protect their privacy.

To go further :

In order to reach the Expert level, candidates should be able to effectively separate the storage of personal and professional documents, maintaining clear boundaries to protect sensitive information. They should have the expertise to prevent the leakage of professional data onto personal or professional social networks, by implementing strict privacy settings and best practices. They will also be able to extract metadata from a file, enabling him to understand the details hidden in documents and improve data management. Finally, they will need to know how to digitally send sensitive files securely, so that confidential information is transmitted with encryption and robust security measures are put in place, minimizing the risk of unauthorized access or data breach.