Compte Rendu

Evaluation Adaptative CyberCitizen

interpreto

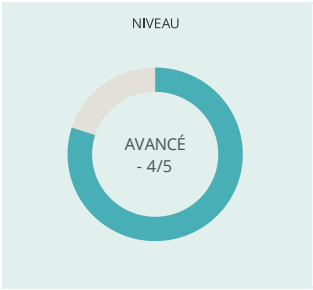
Niveau : Avancé - 4/5

Temps passé : 33mn58s

Test passé le 29 septembre 2023

isograd

1. Résultat

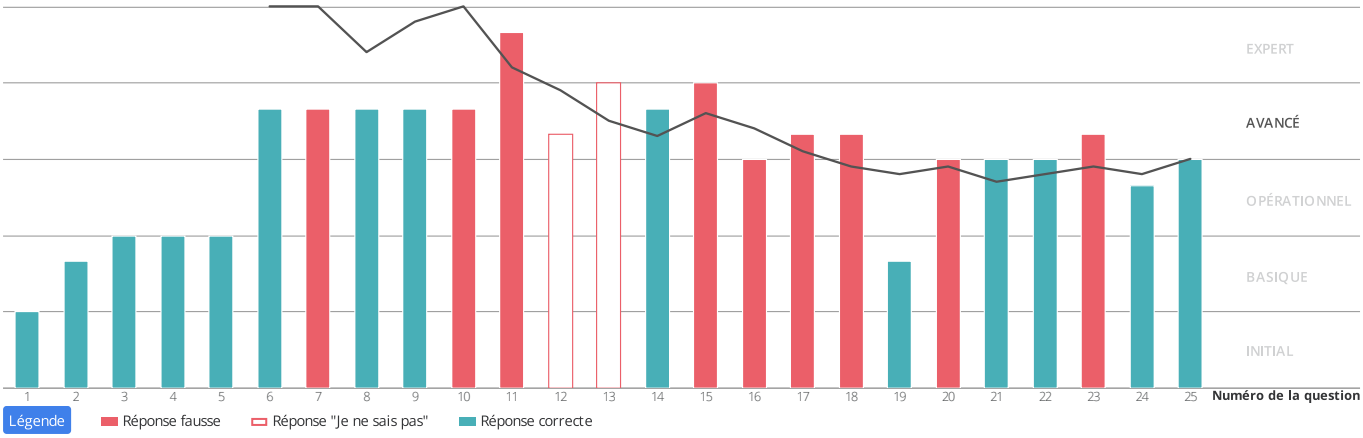


LE CANDIDAT DISPOSE D'UNE BONNE MAÎTRISE DES CONNAISSANCES ET ATTITUDES RELATIVES À LA CYBERSÉCURITÉ DANS LE CADRE PROFESSIONNEL.

2. Déroulement

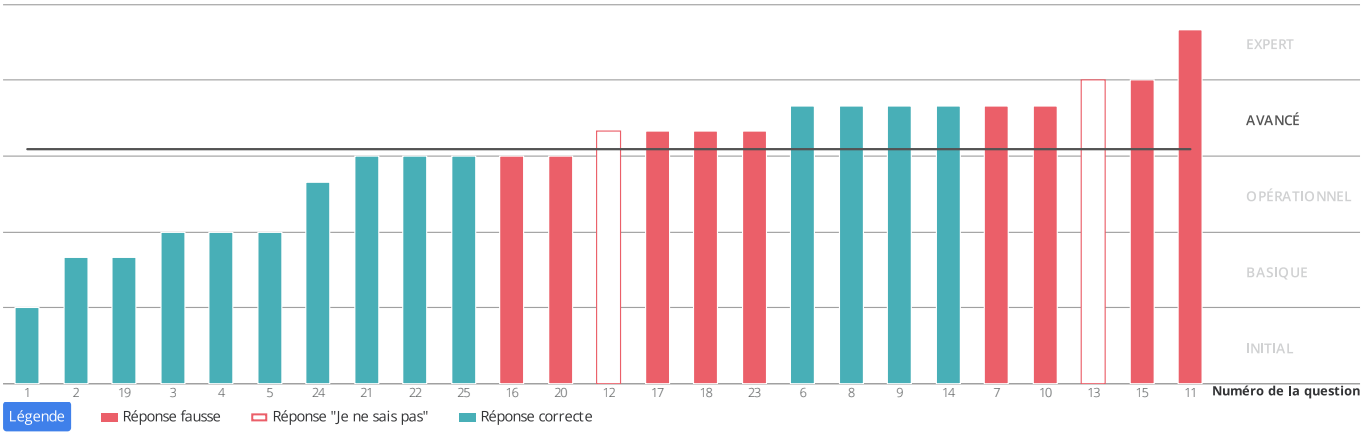
Estimation progressive du niveau du candidat

Ce graphique montre le déroulement du test. Il indique comment le système a adapté les questions aux réponses du candidat. Le niveau estimé du candidat avant chaque question est indiqué par la ligne grise.



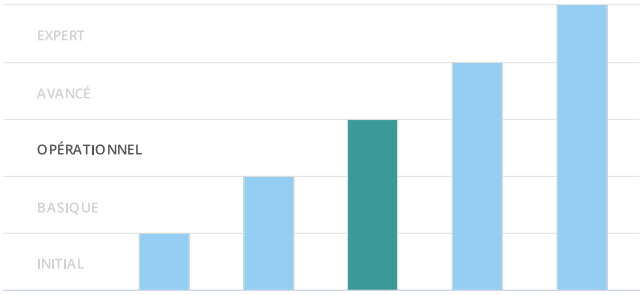
Questions classées par difficulté

Ce graphique montre les questions posées au candidat classées par ordre de difficulté.



3. Compétences

Le monde de la cybersécurité



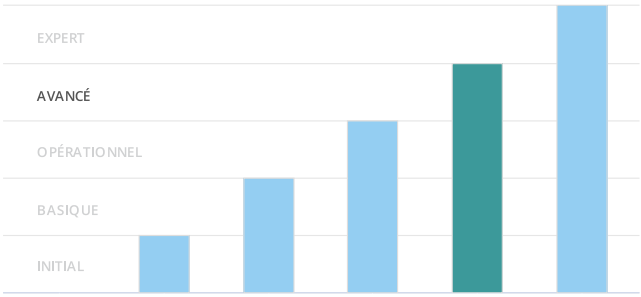
Descriptif de niveau

Le candidat connait les motivations de chaque profil d'attaquant, et leurs principales cibles au sein d'une organisation. Il peut nommer les contacts clés qui ont un rôle dans la cybersécurité d'une entreprise et connaître leurs actions. Il sait qui contacter et comment le faire lorsqu'une attaque est détectée. Il peut reconnaître les principales catégories de vulnérabilités (humaines, techniques ou organisationnelles) et en donner des exemples. Il connaît l'importance de l'utilisation de mots de passe uniques et savent comment les stocker en toute sécurité.

À approfondir :

Afin de monter en compétences et atteindre le niveau Avancé, le candidat devra être en mesure d'évaluer les impacts potentiels de différentes attaques sur une organisation donnée. Il saura appliquer les mesures de sécurité sur son poste de travail et mettre en place une procédure de récupération de preuve d'intrusion. Enfin, il maîtrisera l'utilisation d'un gestionnaire de mots de passes, ainsi que l'utilisation d'une authentification à 2 facteurs.

La sécurité au bureau



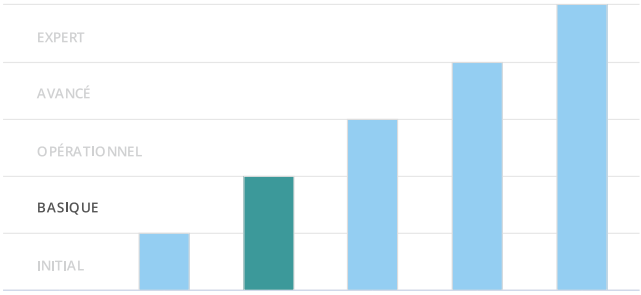
Descriptif de niveau

Le candidat connaît les risques liés à l'installation de logiciels provenant de sources non fiables et peut citer les principales sources et éditeurs de logiciels de confiance. Il sait détecter et réagir à une intrusion potentielle et effectuer une analyse antivirus. Il sait choisir l'outil ou la technique appropriée pour stocker les données de manière sécurisée sur ses périphériques amovibles personnels et sait manipuler des périphériques de stockages inconnus.

À approfondir :

Afin de monter en compétences et atteindre le niveau Expert, le candidat pourra transférer efficacement des données sensibles en toute sécurité, en mettant en œuvre des protocoles de cryptage et de sécurité pour protéger les informations pendant la transmission. Il veillera à ce que les logiciels restent à jour et protégés contre les vulnérabilités et sera familier avec des stratégies telles que les contrôles d'accès physiques et le déchiquetage des documents pour protéger les informations sensibles hors ligne. Enfin, il sera capable de désactiver un processus Windows.

La sécurité en déplacement



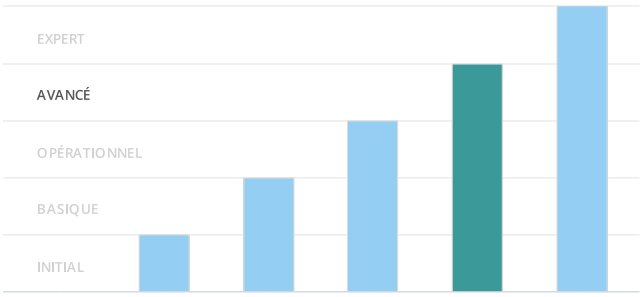
Descriptif de niveau

Le candidat sait comment sécuriser son smartphone avec un code pin et comment le déverrouiller. Il connaît également l'importance de restreindre l'accès aux services sur ses smartphones. Il est conscient du risque d'exposer des données sensibles sur différentes sources numériques et physiques.

À approfondir :

Afin de monter en compétences et atteindre le niveau Opérationnel, le candidat maîtrisera les techniques pour limiter le risque de vol de donnée ou de terminal dans les transports. Il saura sécuriser l'accès aux données et services de son smartphone. Il saura reconnaître et utiliser un réseau sans-fil sécurisé (Wi-Fi, Bluetooth).

La sécurité à la maison



Descriptif de niveau

Le candidat sait détecter les tentatives d'hameçonnage à partir de sources et de canaux variés (courriel, SMS, appels téléphoniques). Il sait comment réagir en cas de doute pour vérifier la légitimité de la source et sait quelle autorité contacter. Il comprend parfaitement les caractéristiques et les avantages du stockage en nuage. Il peut expliquer l'importance de la sauvegarde des données pour la continuité des activités (typiquement en cas d'attaque par ransomware). Il peut protéger ses informations personnelles et sa vie privée à domicile ou dans un environnement de travail à distance. Il a conscience des risques liés à l'exposition de ses données personnelles et de sa capacité à protéger sa vie privée.

À approfondir :

Afin de monter en compétences et atteindre le niveau Expert, le candidat devra savoir séparer efficacement le stockage des documents personnels et professionnels, en maintenant des limites claires pour protéger les informations sensibles. Il devra posséder l'expertise nécessaire pour empêcher la fuite de données professionnelles sur les réseaux sociaux personnels ou professionnels, en mettant en œuvre des paramètres de confidentialité stricts et des bonnes pratiques. Il sera également capables d'extraire les métadonnées d'un fichier, ce qui lui permettra de comprendre les détails cachés dans les documents et d'améliorer la gestion des données. Enfin, il devra savoir envoyer numériquement des fichiers sensibles en toute sécurité afin que les informations confidentielles sont transmises avec un cryptage et mettra en place des mesures de sécurité robustes, minimisant ainsi le risque d'accès non autorisé ou de violation des données.