ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE D'ENREGISTREMENT

5 - REFERENTIELS

Article L6113-1 En savoir plus sur cet article... Créé par LOI n°2018-771 du 5 septembre 2018 - art. 31 (V)
« *Les certifications professionnelles enregistrées au répertoire national des certifications professionnelles permettent une validation des compétences et des connaissances acquises nécessaires à l'exercice d'activités professionnelles. Elles sont définies notamment par un* ***référentiel d'activités*** *qui décrit les situations de travail et les activités exercées, les métiers ou emplois visés, un* ***référentiel de compétences*** *qui identifie les compétences et les connaissances, y compris transversales, qui en découlent et un* ***référentiel d'évaluation*** *qui définit les critères et les modalités d'évaluation des acquis.* »

Candidat en situation de handicap :

Tout candidat peut saisir le certificateur ou un référent handicap d'Airbus. Dans le cadre du respect du règlement d'examen et conformément à ses obligations, le certificateur s'engage à mettre en œuvre les aménagements permettant une compensation du handicap pour rétablir l'égalité des chances entre les candidats lors de l'évaluation des compétences.

L'ensemble des éléments de l'évaluation (matériel, support, temps, format, …) pourront être adapté pour permettre au candidat en situation de handicap de passer les épreuves. Dans certains cas et sur conseil motivé du référent handicap le certificateur peut exempter le candidat de certains critères d'évaluation voire modifier une modalité. Cela ne peut être fait que si ces modifications n'auront pas d'impact sur la capacité professionnelle du candidat ou sur sa pratique du métier d'Analyste en cybersécurité - Secteur aéronautique.

Par ailleurs, le certificateur fait en sorte de mettre en place des modalités d'évaluation les plus inclusives possibles et à préciser les aménagements des épreuves lorsque cela s'avère nécessaire.

<table>
<tr><td rowspan="2">REFERENTIEL D'ACTIVITES

décrit les situations de travail et les activités exercées, les métiers ou emplois visés</td><td rowspan="2">REFERENTIEL DE COMPETENCES

identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</td><td colspan="2">REFERENTIEL D'EVALUATION

définit les critères et les modalités d'évaluation des acquis</td></tr>
<tr><td>MODALITÉS D'ÉVALUATION</td><td>CRITÈRES D'ÉVALUATION</td></tr>
</table>

<table>
<tr><td colspan="4">BLOC DE COMPÉTENCES 1 :
A1 Appliquer la cybersécurité au secteur spécifique de l'aéronautique</td></tr>
<tr><td rowspan="2">A1.1 Etude des métiers l'industrie aéronautique</td><td>C1.1 Mesurer les risques encourus par les éléments IT d'un environnement aéronautique par une veille active afin d'identifier les points de sensibilité de l'industrie à la cybersécurité.

C1.2 Participer et améliorer la veille sur la réglementation de la cybersécurité dans le domaine aéronautique en utilisant les informations mises à disposition (newsletter, plateforme de partage, plateforme de veille active,…) afin de garantir la conformité du système d'information</td><td>A partir d'un cas basé sur les métiers et processus de l'entreprise ou élaboré par un groupe de professeurs, le candidat répond à un QCM portant sur les principaux éléments sensibles à la cybersécurité dans un environnement aéronautique ainsi que sur les éléments de la réglementation s'y rattachant.</td><td>L'évaluation se fait en ayant une note minimale de 12/20 au QCM.</td></tr>
<tr><td>C1.3. Interagir avec les spécialistes industriels (responsables méthodes et outils, responsables de production) en identifiant les processus clés de la production aéronautique pour appliquer les principes de la cybersécurité.</td><td>A partir d'un cas fictif ou réel, le candidat accompagner les spécialistes industriels et les sensibiliser aux problématiques de la cybersécurité. Par la suite, il doit faire une présentation orale à un jury composé des professeurs experts de la matière.

La présentation orale s'appuie sur un support visuel (diaporama) qui devra comprendre à minima:
● Le contexte industriel du cas
● La présentation et l'analyse des composants du cas
● Les processus clés liés aux composants du cas
● Les éléments de cybersécurité à prendre en compte</td><td>L'évaluation mesure l'exhaustivité et la pertinence des réponses apportées en se basant sur les critères suivants:

● La cartographie des composants est complète (serveurs, stations de travail, outils connectés,…) (30%)
● Les processus clés sont identifiés de manière exhaustive (flux de données pris en compte par l'analyse, processus d'utilisation des outils industriel analysés, …) (30%)
● L'application de la cybersécurité est cohérente avec l'environnement aéronautique (en fonction des normes de cybersécurité) (40%)</td></tr>
</table>

			La présentation prendra en compte la diversité du public (adaptation du support et du format du contenu pour les daltoniens et malvoyant par exemple)
A1.2 Exploitation des systèmes, des logiciels de cybersécurité sur les produits aéronautiques	C1.4. Exécuter un test d'intrusion à l'aide d'un ou plusieurs logiciels de cybersécurité sur un système embarqué aéronautique pour tester sa sécurité	A partir d'un cas fictif ou réel, le candidat doit mettre en place une procédure de test d'intrusion et l'exécuter. A l'issue de cette exécution, le candidat effectuera une présentation à l'oral au jury expliquant : ● Le choix des outils et logiciels adéquats pour le test d'intrusion Les éléments démontrant la réussite de l'intrusion le cas échéant ● Les propositions d'amélioration ou de modification de programmation s'il y a lieu (pour renforcer le système d'information de l'entreprise contre l'intrusion) La présentation sera à l'oral grâce à un format diaporama.	L'évaluation mesure l'efficacité des tests d'intrusion en se basant sur les critères suivants : ● La procédure de test d'intrusion est exécutée et complète (40%) ● Les objectifs à atteindre sont documentés clairement et correspondent aux cibles de l'intrusion (niveau de privilèges, information accédée, etc…) (20%) ● La procédure de test est documentée et peut être exécutée par un autre testeur (10%) ● Les éléments critiques issus du test d'intrusion sont identifiés et commentés afin d'être transmis aux responsables du système (30%) La présentation prendra en compte la diversité du public (adaptation du support et du format du contenu pour les daltoniens et malvoyant par exemple)
A1.3 Administration et adaptation d'outils informatiques de sécurité au milieu aéronautique		A partir d'un cas réel ou fictif, le candidat doit produire un dossier contenant : ● Le code informatique ● Les preuves de l'exécution correcte de ce code ● Des propositions d'amélioration le cas échéant ● Le guide d'utilisation	L'évaluation mesure la pertinence du code informatique en se basant sur les critères suivants : ● Le code est fonctionnel (il s'exécute sans erreur et fonctionne tel qu'attendu) (20%) ● La rédaction du code est exhaustive et commentée (l'ensemble des

	C1.5. Mettre à jour et connecter des logiciels en développant des codes informatique afin d'analyser l'activité d'un système d'information en milieu aéronautique	● Les rapports d'analyses Le dossier sera fourni sous la forme de fichiers sources (code informatique lisible et commenté) et de fiches explicatives sur les anomalies, les propositions d'amélioration et les rapports d'analyse.	fonctionnalités sont implémentées et expliquées) (30%) ● Le manuel d'installation est complet permettant à tout utilisateur (qui en a l'utilité et les compétences) de l'installer sans support (20%) ● Le guide d'utilisation permet une utilisation de toutes les fonctionnalités développées (15%) ● Les rapports d'analyse émis sont cohérents vis-à-vis des informations fournis dans le cas d'étude (15%) Le dossier sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …)
BLOC DE COMPÉTENCES 2 : A2 Participer à une politique de sécurité			
A2.1 Participation à la sécurité du système d'information grâce à une veille technologique et réglementaire	C2.1 Vérifier la conformité du système d'information en utilisant les outils de veille mis à disposition (rapports du CERT, plateforme de partage, virus total, outils de veille légale, newsletters,…) afin de garantir le respect des règles légales.	A partir d'un cas réel ou fictif, le candidat doit: ● Répondre à un questionnaire de connaissance sur les règles et normes de cybersécurité ● Etudier un cas pratique de système d'information d'entreprise ● Rédiger d'un rapport des non conformités de sécurité identifiés sur le cas pratique	L'évaluation mesure la capacité à faire de la veille en cybersécurité en se basant sur les critères suivants : ● Les règles et normes de cyber sécurité sont connues (note minimale au questionnaire 12/20) (30%) ● La méthode d'analyse du cas d'étude est choisie et justifiée (30%) ● Les non conformités identifiées

		Le rapport prend la forme d'un manuscrit synthétique.	sont caractérisées (leur impact sur l'entreprise est évalué) (20%) ● Les propositions de gestion des risques sont rédigées clairement (20%) Le rapport sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …). Le questionnaire prendra en compte les réglementations sur le handicap le cas échéant.
A2.2 Pratique d'audits informatiques	C2.2 Faire des analyses d'éléments du système d'information (poste de travail, serveurs, réseau local) en utilisant les guides à disposition afin de vérifier la cybersécurité des éléments.	A partir d'un cas réel ou fictif, le candidat doit produire un rapport d'analyses établissant un état des lieux de la configuration d'éléments du réseau (postes, serveurs, etc.) comprenant les failles et les propositions de traitement. Le rapport prend la forme d'un manuscrit synthétique.	L'évaluation mesure la pertinence des analyses en se basant sur les critères suivants : ● L'identification des éléments du réseau analysés (adresse IP, nom et position sur le réseau) (20%) ● Les règles de cybersécurité choisies et utilisées pour faire l'analyse (40%) ● Les failles de configuration sont rédigées, identifiés et expliquées (20%) ● Les moyens de combler les failles de configuration sont rédigés et expliquées (20%) Le manuscrit sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie

			pour les daltoniens, …).
A2.3 Mise en place des corrections des vulnérabilités	C2.3 Corriger des programmes informatiques en modifiant le code existant afin de supprimer des vulnérabilités le système d'information ● Bash pour l'administration système dans les environnements Unix ● Python pour l'intégration avec l'écosystème sécurité ● SQL pour la connaissance de manipulations de données ● Powershell pour l'intégration dans les environnements Windows	A partir d'un cas réel ou fictif, le candidat doit corriger des codes informatiques et produire un dossier contenant : ● Les preuves d'identification des corrections nécessaires ● Le code informatique actualisé ● Les preuves de l'exécution correcte de ce code ● Des propositions d'amélioration le cas échéant Le dossier sera fourni sous la forme de fichiers sources (code informatique lisible et commenté) et de fiches explicatives sur les corrections apportées, les propositions d'amélioration.	L'évaluation mesure la pertinence du code informatique en se basant sur les critères suivants : ● Identification exhaustive des corrections à faire (30%) ● Corrections proposées cohérentes et fonctionnelles (elles permettent aux programmes de fonctionner tel qu'attendus) (20%) ● Le code est fonctionnel (il s'exécute sans erreur et fonctionne tel qu'attendu) (20%) ● La rédaction du code est exhaustive et commentée (l'ensemble des fonctionnalités sont implémentées et expliquées) (30%) Le dossier sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …).
A2.4 Préconisations d'amélioration de la politique de sécurité	C2.4 Rédiger des rapports proposant des	A partir d'un cas réel ou fictif, le candidat doit produire un rapport d'analyse établissant un état des lieux de la configuration d'éléments du réseau (postes, serveurs, etc.) et des propositions d'améliorations basées sur cette état des lieux. Le rapport comportera aussi une évaluation de l'impact de ses	L'évaluation mesure la pertinence des propositions d'amélioration en se basant sur les critères suivants : ● Identification exhaustive des anomalies (30%) ● Corrections proposées cohérentes et fonctionnelles

	modifications des process de déploiement des outils informatique afin d'améliorer la sécurité lors de leur mise en place	améliorations. Le rapport prend la forme d'un manuscrit synthétique.	(elles permettent aux programmes de fonctionner tel qu'attendus) (20%) ● Le code est fonctionnel (il s'exécute sans erreur et fonctionne tel qu'attendu) (20%) ● La rédaction du code est exhaustive et commentée (l'ensemble des fonctionnalités sont implémentées et expliquées) (30%) Le manuscrit sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …).
BLOC DE COMPÉTENCES 3 : A3 Administrer un système d'information sécurisé			
A3.1 administration et sécurisation des de composants cybersécurité constituant le système d'information	C3.1 Analyser le fonctionnement de programmes et de composants en effectuant des tests de sécurité informatiques et en se basant : ● les outils d'administration et de détection type SIEM, IDS/IPS ● les outils de manipulation de fichiers de logs et savoir analyser des logs pour détecter des anomalies et comportement anormaux ● des outils de test d'intrusion réseau/système	A partir d'un cas réel ou fictif, le candidat doit produire un dossier contenant : ● Les codes informatiques ou les logiciels utilisés pour faire les analyses ● Les preuves d'identification des menaces ● Les corrections des codes informatiques effectuées ● Les preuves de mise du fonctionnement des corrections le cas échéant Le dossier sera fourni sous la forme de fichiers sources (code informatique lisible et commenté) et de fiches explicatives	L'évaluation mesure la pertinence des analyses et des corrections en se basant sur les critères suivants : ● La liste des éléments de sécurité à vérifier est exhaustive (basé sur l'état de l'art) (30%) ● Les moyens d'identifier les vulnérabilités des programmes associées sont définis (liste des logiciels et des documents basée sur les standards en vigueur) (30%) ● Les codes informatiques permettant de corriger les

	pour repérer des potentielles attaques et détecter les points faibles du système d'information	synthétiques des logiciels choisis, des menaces identifiées et corrections apportées.	vulnérabilités sont exhaustif et commenté (l'ensemble des corrections sont implémentées et expliquées) (40%) Le dossier et notamment les fiches explicatives seront rédigées en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …).
A3.2 Déploiement des éléments de sécurité dans le système d'information	C3.2 Déployer des éléments de sécurité (Patchs, Mises à jour, changement de protocoles de communication, …) en appliquant les guides appropriés pour sécuriser des systèmes et logiciels.	A partir d'un cas réel ou fictif, le candidat doit installer et mettre à jour des éléments du réseau et produire un dossier contenant : ● Les éléments de sécurité installés ou mis à jour ● La liste des guides utilisés pour déployer ces éléments ● Les preuves du bon fonctionnement du réseau après ces mis à jour	L'évaluation mesure l'efficacité des installations et des mises à jour en se basant sur les critères suivants : ● La liste des éléments à installer ou à mettre à jour est exhaustive (30%) ● Le choix des guides utilisés est cohérent avec la besoin (30%) ● Le réseau est fonctionnel après les installations et les mises à jour (20%) Le dossier sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …).
A3.3 Génération de rapports de sécurité	C3.3 Automatiser l'analyse du système d'information (journal de bord du système,) par le développement de	A partir d'un cas réel ou fictif, le candidat doit automatiser une production de rapport de cybersécurité et produire un dossier contenant : ● Le code sources des programmes permettant l'automatisation de rapport	L'évaluation mesure la pertinence des rapports d'analyse en se basant sur les critères suivants : ● La rédaction du code est exhaustive et commentée (l'ensemble des fonctionnalités

	programmes afin de s'assurer de l'intégrité du système d'information d'une entreprise	• Les rapports automatisés émis par le ou les programmes • Les éléments démontrant la cohérence des rapports en fonction des informations recueillies lors de l'analyse du système d'information	sont implémentées et expliquées) (30%) • Les rapports émis sont cohérents avec les informations recueillis lors de l'analyse du système d'information (30%) • Le manuel d'installation est complet permettant à tout utilisateur (qui en a l'utilité et les compétences) de l'installer sans support (20%) • Le guide d'utilisation permet une utilisation de toutes les fonctionnalités développées (20%) Le dossier sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …).
BLOC DE COMPÉTENCES 4 : A4 Garantir la sécurité d'un SI			
A4.1 Analyse des risques et des vulnérabilités du système d'information	C4.1 Identifier les risques d'éléments du système d'information en appliquant la méthode EBIOS RM afin d'éviter les	A partir d'un cas réel ou fictif, le candidat doit produire une présentation du cas qu'il aura analysée suivant la méthode EBIOS RM contenant : • Les différents ateliers de la méthode EBIOS • Les hypothèses choisis pour l'application de la méthode EBIOS • Les conclusions concernant les risques	L'évaluation mesure la pertinence et la cohérence de l'application de la méthode EBIOS en se basant sur les critères suivants : • Les hypothèses d'utilisation de la méthode EBIOS sont expliquées et cohérentes (30%) • Les ateliers de la méthode EBIOS sont tous connus et suivis

	vulnérabilités.	● Les préconisations pour limiter l'impact des risques s'il y a lieu La présentation sera évaluée par un jury composé de certificateurs.	(30%) ● Les risques identifiés sont cohérents avec le cas (20%) ● Les préconisations sont pertinentes et exhaustives avec le cas (20%)
A4.2 Mise en place des éléments de sécurité du système d'information	C4.2 Déployer les outils de sécurité (firewall, antivirus) en se basant sur les process de l'entreprise afin de garantir la sécurité du système d'information	A partir d'un cas réel ou fictif, le candidat doit déployer des outils de sécurité et produire une présentation contenant : ● Les différents outils de sécurité à déployer ● Les choix de configurations des différents éléments ● Les preuves du bon fonctionnement du réseau après l'installation des éléments La présentation sera évaluée lors d'un oral par les certificateurs.	L'évaluation mesure l'efficacité du déploiement des outils de sécurité en se basant sur les critères suivants : ● Les configurations des outils sont expliquées et cohérentes avec les standards en vigueur (40%) ● Le réseau fonctionne de manière nominale après l'installation (40%) ● La présentation faite est claire, concise et permet à un lecteur de comprendre les choix qui ont été faits (20%) Le dossier sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …).
A4.3. Collecte des preuves numériques selon les procédures en vigueur	C4.3. Réaliser la collecte de preuves numériques de façon technico-légale à l'aide d'outils de collecte dédiés fournis par la sécurité informatique de l'entreprise afin de préserver les preuves numériques.	A partir d'un cas réel ou fictif, le candidat doit réaliser une collecte de façon technico légale et produire un rapport contenant : ● La liste des éléments pris en compte dans l'analyse technico légale (des copies de disques durs, des copies de smartphones, log, etc)	L'évaluation mesure l'efficacité la collecte technico légale en se basant sur les critères suivants : ● La liste des éléments pris en compte est exhaustive (20%) ● Le choix des outils est cohérent (20%)

		● Le choix des outils pour faire l'analyse technico légale ● Les scénarios d'analyse et les résultats associés	● Les scénarios d'analyse et les résultats sont documentés et expliqués (30%) ● Les résultats de l'analyse permettent de récupérer les données critiques (30%) Le rapport sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …).
A4.4 Sécurisation des réseaux et des accès distants	C4.4 Configurer de façon sécurisée les protocoles de bases (BGP,OSPF, VRRP, etc) en s'appuyant sur les standards en vigueur afin d'augmenter la sécurité d'un réseau	A partir d'un cas réel ou fictif, le candidat doit configurer des protocoles de base et produire un dossier contenant : ● La liste des protocoles à configurer ● Les configurations choisies ● Les explications concernant les choix de configurations	L'évaluation mesure la pertinence des configurations en se basant sur les critères suivants : ● La liste des protocoles est exhaustive (35%) ● Les configurations des protocoles sont expliqués et cohérentes (35%) ● Le réseau fonctionne nominalement après les configurations des protocoles (30%) Le dossier sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …).
BLOC DE COMPÉTENCES 5 : A5 Participer à l'encadrement et à la coordination d'un projet de sécurisation			

ELEMENTS COMPLEMENTAIRES RELATIFS A LA DEMANDE D'ENREGISTREMENT

A5.1 Utilisation de la gestion de projet dans le cadre du déploiement de la cybersécurité	C5.1 Participer au déploiement du système d'information (sur divers environnements techniques : partie du réseau, ensemble de serveurs etc) via les méthodes de gestion de projet (AGILE, SAFE) pour mettre à niveau les différents éléments du système dans une structure complexe	A partir d'un cas réel ou fictif, le candidat participe à un déploiement d'éléments sur le système d'information. Il doit établir un document décrivant : ● L'utilisation de la méthode de gestion de projet (AGILE, SAFE etc et le vocabulaire associé épopée, use case etc…) ● Les éléments garantissant la structure de l'équipe projet (workpackage, SWOT analyse de risque etc….) ● La description du découpage du projet: tâches, itérations, planning ● La prise en compte des situations de handicap le cas échéant Le rapport prend la forme d'un manuscrit synthétique.	Le candidat prendra en compte les situations de handicap lors de son participation à la gestion de projet. Les choix effectués pour le déploiement prendront en compte la diversité des utilisateurs. L'évaluation mesure l'application correcte de la gestion en se basant sur les critères suivants : ● La méthodologie de gestion de projet employée est expliquée et documentée (40%) ● Les tâches et itérations sont définies, argumenté et communiqué à l'équipe projet (30%) ● Les tâches et itérations sont organisées et planifiés (30%) Le manuscrit sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …).
A5.2 Sensibilisation et accompagnement des utilisateurs finaux	C5.2 Sensibiliser les utilisateurs finaux à avoir recours aux bonnes pratiques en diffusant les recommandations de cybersécurité pour améliorer la culture de	A partir d'un cas réel ou fictif, le candidat sensibilise les utilisateurs aux problématiques de la cybersécurité lors de la sélection d'outils informatiques. Il recueille leur besoin et explique les éléments de cybersécurité à prendre en compte. Il doit ensuite produire un dossier contenant : ● Une liste de critères justificatifs des logiciels sélectionnés pour adresser les problèmes identifiés dans le cas étudié	Le candidat prendra en compte les situations de handicap lors de son accompagnement. Les documents qu'il produira ainsi que les choix de logiciels seront adaptés à ces situations (police d'écriture pour les malvoyants, couleurs en cas de daltonisme, …). Le temps alloué à l'accompagnement des utilisateurs pour gérer la crise sera déterminé en

	sécurité.	● Un guide d'installation des logiciels retenus ● Le guide de mise en œuvre des solutions Le dossier sera fourni sous la forme de liste des logiciels accompagnés de la raison de leur sélection, du séquencement de leur installation ainsi que de celui de leur exécution.	prenant en compte la diversité du public accompagné. L'évaluation mesure la pertinence des recommandations en se basant sur les critères suivant : ● Les critères de sélection des outils sont cohérents vis-à-vis des informations fournis dans le cas d'étude (50%) ● Le guide d'installation des logiciels est complet permettant à tout utilisateur (qui en a l'utilité et les compétences) de l'installer sans support (35%). ● Le guide de mise en œuvre permet une utilisation de toutes les fonctionnalités (15%) Le dossier sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …).
A5.3 Accompagnement des utilisateurs lors d'une crise de cybersécurité	C5.3 Accompagner les utilisateurs à la résolution d'une crise suite à un incident de cybersécurité en analysant correctement les informations mises à disposition par les utilisateurs ainsi que par les différents outils d'analyse du système d'information pour garantir la confidentialité et l'intégrité de l'entreprise	A partir d'un cas réel ou fictif, le candidat accompagne les utilisateurs lors d'une crise de cybersécurité en recueillant leurs informations et leurs besoins. Il doit à partir de cet accompagnement produire un dossier contenant : ● Les rapports d'analyse des types d'attaque de cybersécurité associés aux cas étudiés	Le candidat prendra en compte les situations de handicap lors de son accompagnement. Le temps alloué à l'accompagnement des utilisateurs pour gérer la crise sera déterminé en prenant en compte la diversité du public accompagné. L'évaluation mesure la pertinence des recommandations en se basant sur les critères suivant :

		● une liste de recommandations de cybersécurité à mettre en œuvre ● Le guide de mise en œuvre des recommandations proposées Le dossier sera fourni sous la forme de listes d'anomalies et de fiches explicatives sur les anomalies, les propositions d'amélioration et les rapports d'analyse.	● Le rapport d'analyse des types d'attaques émis sont cohérents vis-à-vis des informations fournis dans le cas d'étude (50%) ● La liste des recommandations est réaliste vis-à-vis du cas étudié et aux standards de l'entreprise (35%). ● Le guide de mise en œuvre permet une utilisation de toutes les fonctionnalités développées (15%) Le dossier sera rédigé en prenant en compte la diversité du public (adaptation de la police de caractère pour les malvoyants, colorimétrie pour les daltoniens, …).