Référentiel certification : Mobiliser ses équipes pour protéger son organisation des risques de cybersécurité

Cette certification répond aux enjeux croissants de protection des entreprises face à la multiplication des attaques cyber. Au-delà des collaborateurs des services informatiques, les managers et leurs équipes jouent un rôle clé de première ligne en matière de détection et d'alerte en cas d'incidents afin de protéger les actifs et limiter les impacts sur l'organisation. Ils doivent également se préparer avec leurs équipes afin d'être prêts à réagir en cas d'attaque avérée et pouvoir assurer la continuité des activités critiques. La certification valide dès lors les compétences de management en matière de vigilance (prévention) et de réaction en cas d'actes de cyber malveillance avérés : identifier, classifier les données sensibles et mettre en œuvre les dispositifs pour les protéger, s'assurer de la conformité des usages pour les données personnelles (RGPD), comprendre les stratégies utilisées par les cyber criminels pour organiser les systèmes de défense de l'organisation, identifier les vulnérabilités humaines ou liées aux processus numérisés utilisables par les cyber criminels, mettre au point des solutions pour préserver la continuité de l'activité et minimiser les impacts des actes de cyber malveillance, développer les capacités individuelles et collectives pour réagir et mobiliser les équipe en cas de cyber attaque supposée ou avérée. Elle est particulièrement adaptée aux managers opérationnels, responsables d'un service.

Référentiel de compétences	**Référentiels d'évaluation**	
	Modalités d'évaluation	**Critères d'évaluation**
1. Identifier les actifs clés de l'entreprise pour cibler les actions prioritaires à mener afin de les protéger des conséquences des actes de cyber malveillance (vol, exfiltration, destruction)	Toutes les épreuves de certification se déroulent à l'issue de la formation. **Cas pratique écrit (10mn).** - Cas pratique écrit individuel, le candidat répond à une question ouverte pour identifier les actifs clés et données sensibles à protéger.	Les actifs clés à protéger ont été clairement identifiés Les données sensibles des clients et collaborateurs ont été clairement identifiées.
2. Identifier et évaluer les risques de SSI liés aux actes de cyber malveillance pouvant cibler l'entreprise afin de mettre en place les systèmes de protection adaptés.	**Cas pratique écrit (20mn)**. - Cas pratique écrit individuel, dans lequel une situation est décrite. Le candidat répond à une question ouverte pour identifier les risques de l'entreprise fictive et préconise des solutions.	Les risques de l'entreprise face aux actes de cyber malveillance sont clairement identifiés. Les failles humaines et techniques potentielles dans l'entreprise sont détectées. Le cadre technologique de l'entreprise et de l'architecture informatique est pris en compte dans les préconisations.

3. Appréhender les techniques utilisées par les adversaires cyber-malveillants pour mieux organiser la protection de l'organisation	**- un questionnaire à choix multiples portant sur les connaissances** (durée 15min) Le questionnaire est accessible via une plateforme LMS sécurisée. Il peut également être imprimé et administré en direct. 60% de bonnes réponses sont nécessaires à la validation du questionnaire. Le quiz valide également la compétence 8	Les techniques des acteurs cyber malveillants sont bien identifiées. Les échanges avec les cyber criminels lors d'une attaque sont conformes aux recommandations officielles.
4. Déployer une stratégie pour faire adopter les bonnes pratiques d'hygiène IT et de vigilance afin d'éviter le déclenchement d'actes cyber malveillants	**Cas pratique écrit (20mn)**. - Cas pratique écrit individuel, dans lequel une situation est décrite. A partir des analyses d'actifs clés et de risques cyber effectuées, le candidat met au point une stratégie de protection et de vigilance auprès des collaborateurs.	La stratégie de protection décrite est efficace et permet de réduire les risques cyber dans l'entreprise. Les bonnes pratiques à adopter par les équipes sont formulées de manière précise. La communication auprès des équipes est décrite en détail et permet une mise en place rapide.
5. Conduire une stratégie de continuité d'activité pour minimiser les impacts financiers et assurer la survie économique de l'entreprise en cas d'attaque.	**Cas pratique écrit (15mn)**. - Cas pratique écrit individuel, dans lequel une situation est décrite. Le candidat préconise une stratégie de continuité d'activité afin de maintenir l'activité en cas de cyber-attaque ou de défaillance d'un prestataire.	La stratégie de continuité propose une alternative de fonctionnement sans les outils numériques ou avec des outils alternatifs. Les acteurs et les étapes de la mise en place de la stratégie sont clairement identifiés.
6. Piloter les équipes et parties prenantes internes et externes lors d'une crise cyber afin de restaurer les activités et assurer la survie économique de l'entreprise	**Cas pratique écrit (15mn)**. - Cas pratique écrit individuel, dans lequel une situation de crise cyber est décrite. Le candidat décrit en répondant à des questions ouvertes la manière dont il va réagir, les actions à prendre et personnes à contacter et la communication à adapter.	La situation est analysée et les informations disponibles sont vérifiées. Les actions sont réparties entre les différents acteurs en interne (équipes techniques, opérationnelles…) Les actions préconisées par le candidat permettent de réduire la propagation du malware/ransomware. Les actions préconisées par le candidat permettent de réduire l'impact économique de l'attaque. Le candidat propose une communication adéquate en interne et en externe.

7. Engager ses équipes sur les enjeux de la cyber sécurité en utilisant les leviers managériaux et culturels afin de prévenir les risques cyber.	**Cas pratique oral**. -Le participant accède au contexte de la situation sur la plateforme LMS sécurisée puis s'enregistre en transmettant un message mobilisateur. Il transmet ensuite les ficher(s) audio(s) à l'évaluateur.	Le candidat communique sur les enjeux de la cybersécurité et les risques encourus par l'entreprise. Le candidat utilise des exemples et des histoires pour renforcer le message.
8. Appréhender le cadre juridique en maitrisant les conventions légales et en identifiant les acteurs clés en charge de la cyber sécurité pour assurer une réponse adaptée après une attaque.	**- un questionnaire à choix multiples portant sur les connaissances** (durée 15min) Le questionnaire est accessible via une plateforme LMS sécurisée. Il peut également être imprimé et administré en direct. 60% de bonnes réponses sont nécessaires à la validation du questionnaire. Le quiz valide également la compétence 3	Les acteurs en charge de la cyber sécurité et les acteurs régulateurs sont connus et définis. La méthodologie de référencement et de déclaration aux acteurs publics en charge de la cyber sécurité, en cas de cyber attaque est connue et définie Chacun des droits à respecter pour être en conformité avec la législation sur la protection des données est connu et défini