RÉFÉRENTIELS DE COMPÉTENCES ET D'ÉVALUATION
RÉPERTOIRE SPÉCIFIQUE
CERTIFICATION « ÉLABORER ET METTRE EN ŒUVRE UNE DÉMARCHE DE CYBERSÉCURITÉ »

REFERENTIEL DE COMPETENCES	REFERENTIEL D'EVALUATION	
	MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
C1. Analyser la vulnérabilité de l'entreprise - en réalisant un inventaire des équipements, des logiciels et des interconnexions avec l'extérieur, - en identifiant les vulnérabilités et les menaces par rapport au système d'information de l'entreprise - en élaborant et en appliquant une politique de veille sur les menaces et les risques internes et externes liés aux attaques de chaîne d'approvisionnement (altération du code, diffusion massive de code malveillant, détournement d'applications légitimes) - en mobilisant les méthodes d'analyse de risques (EBIOS RM, ISO 27005) afin d'évaluer les risques associés à ces vulnérabilités	Cas pratique D'après un cas fictif ou réel, le candidat est chargé d'après la vulnérabilité d'une organisation et son niveau de sécurité. Sur cette base, il élabore une démarche de cybersécurité (politique de sécurité, gestion des accès, sensibilisation des collaborateurs). Il est enfin mis en situation dans le cas d'une cyberattaque. Dans ce cadre, il doit produire un document et le restituer lors d'une soutenance. Ce document comprend : • Le rapport d'audit de cyber sécurité de l'entreprise permettant	Le candidat identifie manière précise les vulnérabilités spécifiques dans le système d'information de l'entreprise : - il utilise correctement et manière appropriée les méthodes de recherche de vulnérabilités telles que l'analyse de code, les scans de vulnérabilités automatisés, les tests d'intrusion. - les méthodes d'analyse des risques EBIOS RM et ISO 27005 sont connues, les enjeux de l'application des étapes d'identification, d'évaluation et de traitement sont maitrisés. - il prend en compte de manière exhaustive les actifs de l'organisation avec l'inventaire des équipements, des logiciels et des interconnexions avec l'extérieurs, il restitue une cartographie et il identifie les vulnérabilités de manière cohérente en fonction de la surface d'attaque potentielle, - le rapport présenté est clair et précis, il restitue les résultats de manière compréhensible et en adéquation avec les informations attendues par les parties prenantes. Le rapport comprend des propositions appropriées pour atténuer les risques identifiés.
C2. Etablir un état des lieux du niveau de sécurité de l'entreprise et du respect de ses obligations règlementaires, - en analysant les responsabilités juridiques de l'entreprise en matière de cybersécurité, - en identifiant les bonnes pratiques ainsi que les points de sécurisation à envisager, - et en dressant un plan de sécurisation du SI et en sensibilisant la direction de l'organisation sur les mesures de protection à adopter et sur la conduite à tenir en cas de crise cyber, afin d'évaluer les besoins et conditions de mise en œuvre d'un futur plan d'amélioration		Le candidat établit un état des lieux du niveau de sécurité de l'entreprise : - il identifie les besoins spécifiques à l'entreprise en matière de cybersécurité : l'ensemble des données numériques de l'entreprise est clairement identifié, les acteurs institutionnels sont identifiés. - il identifie et analyse les différentes catégories de menaces (internes, externes, etc.) : il maitrise les techniques et les vecteurs d'attaques courants qui peuvent affecter le système d'information de l'entreprise, telles que les attaques par injection SQL, les attaques de déni de service distribué (DDoS), les ransomwares, etc. Il identifie et argumente les motivations des attaquants. - il conçoit un plan de sécurisation des SI adapté aux menaces identifiées, comprenant les actions, délais et responsabilités.

C3. Définir une politique de sécurité, - en préconisant une solution de surveillance adaptée (EDR, SIEM…) - et en établissant les règles de sécurité de l'entreprise relatives à l'utilisation des SI, aux mises à jours des appareils, des logiciels et des antivirus, et à la gestion des sauvegardes, afin de sécuriser les données	d'identifier les vulnérabilités (C1) • Le plan d'action à mettre en œuvre à savoir la démarche cybersécurité lors d'un incident (C2 et C3)	Le candidat définit une politique de sécurité : - une documentation est créée : les problématiques sont identifiées, les schémas sont cohérents, la cartographie du SI est réalisée. - les systèmes d'information sont protégés contre les accès physiques illégitimes, les agressions physiques et les événements naturels. - les systèmes d'information sont protégés contre les applications malveillantes ; les réseaux, les équipements, les données et les supports de données sont sécurisés - une veille sur les menaces et risques est mise en place : les outils et sources d'informations pertinents sont utilisés pour la surveillance des menaces, l'évaluation de leur crédibilité est justifiée.
C4. Gérer les identités et contrôles d'accès, - en définissant leurs modalités de gestion, - et en contrôlant tout équipement et personne ayant une relation technique avec le SI, afin de limiter l'accès aux données sensibles	• La restitution de la réalisation du plan d'action (C4 à C7)	Les composants utilisés dans les systèmes d'information sont configurés de manière à limiter leur exposition aux menaces, les informations sont cryptées : - de manière adaptée au type d'information et au niveau de sécurité requis (des restrictions d'accès aux sites sont définies, les accès wifi sont sécurisés, les modalités de connexion à distance sont sécurisés) - en prenant en compte le niveau d'habilitation des utilisateurs (une politique de gestion des droits d'accès informatiques et physiques et une politique de mise à jour et de re-certification de ces droits sont mises en place), - les accès aux informations sensibles sont bien protégés, les modalités d'utilisation des mots de passe sont conformes (mots de passe longs et complexes, individuels, mis à jour régulièrement, avec l'utilisation d'un gestionnaire ou d'un coffre-fort).
C5. Sensibiliser les collaborateurs de l'entreprise, - en établissant un code de bonne conduite comprenant les comportements adaptés et les précautions techniques et juridiques à appliquer, - en organisant la diffusion des bonnes pratiques d'acculturation aux règles d'hygiène fondamentales de la cybersécurité, en prenant les dispositions nécessaires pour l'acculturation des collaborateurs en situation de handicap - et en vérifiant la bonne compréhension des enjeux associés à la cybersécurité par l'ensemble des parties prenantes, sur les différents types de risques et leurs moyens de prévention, l'impact sur la réputation de l'entreprise et les conséquences financières, afin d'infuser une culture de la cybersécurité au sein de l'entreprise		Le candidat restitue l'organisation et l'animation de la sensibilisation des collaborateurs : - il a défini un planning d'intervention et des modalités d'organisation de la sensibilisation, de manière à conscientiser l'ensemble des collaborateurs, - les bonnes pratiques capitalisables ont été identifiées, de manière adaptée à l'activité de l'organisation, aux pratiques des collaborateurs, et aux vulnérabilités identifiées, des dispositions sont prises le cas échéant pour permettre la réception des informations par les collaborateurs en situation de handicap, - il a informé les collaborateurs sur les risques encourus et les responsabilise quant à leur rôle dans la sécurité de l'entreprise, - la documentation conçue est adaptée et attractive, la compréhension des risques et des usages attendus est vérifiée.

C6. Gérer une situation d'urgence par l'alerte et la sécurisation, - en sécurisant les collaborateurs, les lieux et les équipements, en évacuant les lieux si nécessaire, - en alertant les autorités et les organisations pertinentes (banques, CNIL, parties prenantes dont les données personnelles sont exposées…) - en mettant en place une cellule de crise centralisant la réponse à l'incident, et en établissant des outils de communication et de partage d'information, indépendants du système attaqué, - et en déclenchant un plan de continuité de l'activité en prenant en compte les difficultés observées et les optimisations envisagées dans le déroulement de la crise, afin d'assurer une coordination rapide avec les parties prenantes et de minimiser les conséquences négatives de la situation		Le candidat gère une situation d'urgence de manière adaptée : - Il met en place des mesures d'alerte, en fonction du type d'attaque, auprès des autorités, des banques et/ou des parties prenantes. - Il met en place des mesures de sécurisation visant à minimiser les conséquences négatives de la situation d'urgence, que ce soit sur l'enquête à venir, les opérations de l'entreprise, la sécurité des données, la réputation de l'organisation, ou la confiance des parties prenantes. - Il assure la mise en place efficace d'une cellule de crise pour gérer la situation d'urgence, en désignant les responsabilités et les rôles appropriés au sein de l'équipe. - Il déploie un plan de continuité de l'activité, puis de reprise adapté : Il identifie les difficultés rencontrées pendant la crise et propose des améliorations aux procédures existantes, afin d'optimiser la gestion des crises futures. Il réalise une analyse post-crise pour identifier les leçons apprises, les bonnes pratiques et les actions correctives à entreprendre pour renforcer la résilience de l'entreprise. - Il prend des décisions rapides et éclairées, en évaluant les risques et en tenant compte des priorités et des contraintes spécifiques à la situation d'urgence. Une réponse rapide et coordonnée à l'incident est donnée, en mettant en œuvre les procédures de gestion d'incident appropriées. - Il assure une communication claire, précise et efficace avec les parties prenantes internes et externes, y compris les employés, les clients, les autorités réglementaires et les médias. Il met en place des outils de communication et de partage d'informations indépendants du système attaqué, afin de maintenir une communication fluide et sécurisée pendant la crise. - Il prend en compte le stress et la dimension psychologique des personnes touchées par la crise, en adoptant une posture empathique et en fournissant un soutien approprié.

C7. Réaliser les opérations de réponse à incident sans destruction de données ou de traces, - en identifiant des indicateurs de compromission issus des données de surveillance, en évaluant l'étendue et la nature de l'incident, et en isolant l'élément compromis, - en mettant en œuvre un plan d'action et en restaurant les opérations normales, - en documentant les actions réalisées afin de fournir un rapport d'incident détaillé, - en fournissant ensuite aux collaborateurs les outils, la documentation et les méthodes pour éviter le récidive, afin de remédier à la situation et d'assurer la reprise de l'activité		Le candidat réalise les opérations de réponse à un incident : - Les caractéristiques de l'incident sont déterminées (scénario, vecteur, périmètre). - Les critères de suivi et d'évaluation du plan d'action sont justes. - Les critères sont formalisés dans des outils de suivi et d'évaluation permettant le contrôle et l'amélioration continue de la démarche - La remise en service est réalisée progressivement, des points intermédiaires sont réalisés et le risque d'une potentielle récidive est contenu.