Référentiel d'activités	Référentiel de compétences	Référentiel d'évaluation	
		Modalités d'évaluation	**Critères d'évaluation**
01. Conduire des tests d'intrusion éthiques			
Collecte et analyse des informations nécessaires à la conduite d'un test d'intrusion éthique	Recueillir les données et renseignements relatifs à la cible, à l'aide de pratiques d'investigation légalement autorisées et d'analyse d'information préalablement dissimulée, en récoltant, croisant ou analysant des données numériques disponibles en source ouverte (OSINT), afin d'identifier les faiblesses du système d'information cible et de déterminer la nature du test d'intrusion.	**Mise en situation simulée** Le candidat devra collecter les informations permettant de déterminer et de déployer une ou plusieurs techniques de tests d'intrusion éthiques. Il sera demandé au candidat d'expliciter sa démarche et de présenter les impacts et les résultats du test d'intrusion conduit. Cette mise en situation s'appuie sur la simulation d'une entreprise fictive et de son Système d'Information déployé et connecté à l'infrastructure physique implémentée dans les locaux du certificateur, avec une liste d'utilisateurs possédant une existence numérique, une gouvernance (organigramme, politiques de sécurité...) et une activité internationale multi-sites. Le candidat présentera la méthodologie et les résultats de ses travaux au cours d'une soutenance orale.	Un rapport d'investigation numérique (OSINT) de la cible est réalisé avec au moins 3 faiblesses identifiées
	Recueillir les données et renseignements relatifs aux actifs du système d'information de la cible, à l'aide d'outils et de techniques d'investigation légalement autorisés (discovery) afin de cartographier les systèmes les plus critiques et les plus exposés, d'identifier leurs vulnérabilités et de déterminer les chemins d'attaque possibles sur ces systèmes.		Une cartographie des systèmes cibles, précisant leur niveau de criticité et leurs vulnérabilités, est réalisée et complétée à au moins 80%
Test d'intrusion éthique par l'exploitation des informations collectées	Conduire des techniques et tactiques d'attaques de cybersécurité sur base des éléments collectés, en collaboration avec les experts (opérationnels métiers et informatiques) afin de prendre le contrôle du système cible.		Un test d'intrusion sur la cible est réalisé et le système cible est contrôlé pour tout ou partie.
	Maintenir le contrôle du système cible en déployant des mécanismes techniques (backdoor, webshell...) afin de contrer les mesures de sécurité proactives.		Au moins une technique d'attaque persistante est déployée pendant le test d'intrusion.
Evaluation de l'impact de compromission du périmètre ciblé par un test d'intrusion éthique	Déterminer les risques et dommages pour le système d'information cible en évaluant l'impact fonctionnel d'une attaque en termes de confidentialité, d'intégrité, de disponibilité et de traçabilité des données, afin de rédiger un rapport de test d'intrusion dans un format prenant en compte les éventuelles situations de handicap.		Un rapport technique de test d'intrusion présentant 80% des risques et dommages possibles pour le système cible est rédigé, dans un format prenant en compte les éventuelles situations de handicap.
Présentation des résultats et des recommandations d'un test d'intrusion éthique	Communiquer l'ensemble des résultats d'un test d'intrusion à travers un rapport de synthèse, dans un format prenant en compte les éventuelles situations de handicap, afin de présenter à l'organisation sa surface d'exposition, ses vulnérabilités, leur criticité et leur impact.		Un rapport de synthèse, vulgarisant les résultats des tests d'intrusion et présentant les risques et dommages pour le système cible, est présenté dans un format prenant en compte les éventuelles situations de handicap.
	Déterminer les mesures de sécurité permettant de traiter les risques et dommages présents dans le rapport de test d'intrusion, en collaboration avec les opérationnels métiers et informatiques, afin d'établir un plan de remédiation adapté.		Un plan de remédiation, contenant des mesures correctives couvrant *a minima* 80% des vulnérabilités identifiées, est rédigé.

Référentiel d'activités	Référentiel de compétences	Référentiel d'évaluation	
		Modalités d'évaluation	**Critères d'évaluation**
02. Configurer les éléments de sécurité des infrastructures et des réseaux			
Configuration des éléments de sécurité des réseaux	Etablir les mesures de sécurité applicables en concevant une infrastructure réseau sécurisée afin de protéger les réseaux WAN, LAN et sans fil.	**Simulation sur plateforme** Il sera demandé au candidat, dans le cadre d'une mise en situation simulée, de sélectionner et configurer les solutions techniques appropriées pour sécuriser une architecture réseaux. Cette simulation repose sur la simulation d'une entreprise fictive et la réplication de son Système d'Information déployé et connecté à l'infrastructure physique implémentée dans les locaux du certificateur simulé. Les éléments suivants seront mis à la disposition du candidat : - un réseau d'entreprise comprenant une zone entreprise, une zone industrielle et une zone démilitarisée ; - un ensemble de pare-feux (Fortinet, Stormshield, Palo Alto, etc.) ; - un ensemble d'EDR (Tethris, HarFangLab, etc.) ; - un ensemble de Cloud Security Posture Management (Palo Alto, Netskope, etc.) ; - un ensemble de solutions de chiffrement (BitLocker, BitDefender, etc.) ; - une PKI (infrastructure de clé publique) avec les politiques associées ; - une intelligence artificielle de type apprentissage automatique ; - des équipements industriels (Schneider, Weidmueller, Siemens, Codra, Hirschmann,...) Le candidat présentera la méthodologie et les résultats de ses travaux au cours d'une soutenance orale.	Au moins 80% des règles d'un pare-feu (firewall) d'une zone délimitarisée (DMZ) entre l'environnement d'informatique de gestion et l'informatique industrielle sont définies
	Configurer les éléments de sécurité des réseaux (firewall, WAF, reverse proxy, NDR...) afin de mettre en place un réseau sécurisé répondant aux exigences de sécurité applicables à l'organisation		- Au moins 80% des règles du pare-feu sont configurées - Seuls les ports autorisés sont ouverts
Configuration des éléments de sécurité des infrastructures informatiques cloud et on premise	Configurer les éléments de sécurité des infrastructures internalisées dites "on-premise" (EDR, PAM...), en s'appuyant sur des politiques internes, guides de bonnes pratiques, référentiels et cadriciels internationaux, afin de détecter et prévenir les comportements déviants des utilisateurs du système d'information.		Une solution d'EDR (HarFangLab, Tehtris...) est configurée et permet de détecter une attaque machine.
	Configurer les éléments de sécurité des infrastructures Cloud (CASB, CSPM, SWG, etc.) en reposant sur des politiques internes, guides de bonnes pratiques, référentiels et cadriciels internationaux afin de sécuriser l'environnement Cloud de l'organisation		Une solution de CSPM (Palo Alto, Netskope...) est configurée et permet de détecter une mauvaise configuration d'une infrastructure cloud déployée en infra as code.
	Déployer des mesures de sécurité opérationnelles (chiffrement, contrôle d'accès, etc.) en s'appuyant sur les politiques internes, guides de bonnes pratiques, référentiels et cadriciels internationaux afin de prévenir les risques de fuite de données.		Une solution de chiffrement de disque (BitLocker, BitDefender...) est déployée et le disque résiste à une attaque par démarrage à froid (cold boot)
Sécurisation des nouvelles technologies de l'information et des communications (objets connectés, intelligence artificielle...)	Configurer les éléments de sécurité des objets connectés industriels (IIoT) et non industriels (IoT), en intégrant les contraintes et spécificités de l'environnement de déploiement (industriel ou tertiaire), afin de garantir l'intégrité et la disponibilité des systèmes.		Un certificat d'identité d'un objet connecté est créé et déployé et répond à la politique d'infrastructure de clé publique.
	Déployer des mesures de sécurité s'appuyant sur l'intelligence artificielle en collaboration avec les experts cybersécurité et les opérationnels métiers, afin de contenir les risques liés au déploiement de l'Intelligence Artificielle au sein d'un Système d'Information.		Une solution de sécurité s'appuyant sur l'intelligence artificielle est déployée et permet de prévenir correctement une tentative d'intrusion sur un système d'information

Référentiel d'activités	Référentiel de compétences	Référentiel d'évaluation	
		Modalités d'évaluation	**Critères d'évaluation**
03. Sécuriser les données et les identités d'un système d'information existant			
Maintien de la sécurité des données d'un système d'information	Mettre en oeuvre les mesures de sécurité des données, en fonction des contraintes et besoins fonctionnels de l'organisation, afin de garantir le niveau de confidentialité, d'intégrité et de disponibilité des données.	**Etude de cas pratique** Il sera demandé au candidat, dans le cadre d'un cas pratique, de rédiger un standard technique de sécurité et d'implémenter des mesures techniques de sécurité afin de sécuriser les données et les identités d'un Système d'Information existant. Ce cas pratique sera conduit dans le contexte de sécurisation d'un Système d'Information. Afin de mener à bien ce pratique, le candidat recevra les éléments suivants : - un jeu des identités - les politiques de sécurité incluant les exigences réglementaires et normatives applicables à l'organisation - un jeu de données simulées de l'organisation - une solution de prévention de fuite de données (DLP) - un outil de gestion des correctifs ("patch management") - une solution technique de type "bastion" - un outil d'authentification multi-facteur (MFA) - un ensemble de solutions de chiffrement (BitLocker, BitDefender, etc.) ; - une PKI (infrastructure de clé publique) avec les politiques associées ; Le candidat présentera la méthodologie et les résultats de ses travaux au cours d'un cas pratique en salle et sur outils informatiques.	2 mesures de sécurité d'échange des données sont correctement mises en place
	Traiter les vulnérabilités d'un projet à déployer sur un système d'information existant, via des solutions automatisées de patch management, afin de limiter les impacts et les risques inhérents à la sécurité des données.		Au moins 80% des vulnérabilités identifiées sont corrigées.
	Déployer des solutions de sécurité permettant de prévenir les risques de fuite de données d'un système d'information existant, afin d'être conforme au système de management de la sécurité de l'information (SMSI).		Le déploiement d'une solution de prévention des fuites de données couvre 80% du jeu de données.
Contrôle des identités et des accès à privilèges au sein d'un système d'information	Mettre en oeuvre les mesures de sécurité et les solutions techniques associées (contrôle d'accès, authentification...) adéquates pour assurer la sécurité des identités humaines, machines et services.		Une solution d'authentification multi-facteurs (MFA) est correctement déployée.
	Déployer un bastion de sécurité en gérant, contrôlant et enregistrant l'accès aux ressources du système d'information, afin de contrôler les accès à privilèges.		80% des comptes à privilèges sont correctement intégrés et contrôlés par le bastion.
Elaboration des standards techniques associés aux solutions de sécurité technique mises en oeuvre	Elaborer les standards techniques de sécurité et la documentation technique, applicables et accessibles aux personnes en situation de handicap, en fonction des solutions techniques mises en oeuvres, afin de répondre aux exigences du système de management de la sécurité de l'information (SMSI).		Un standard technique de sécurité est rédigé en accord avec la politique de sécurité de façon lisible et accessible aux personnes en situation de handicap.

Référentiel d'activités	Référentiel de compétences	Référentiel d'évaluation	
		Modalités d'évaluation	**Critères d'évaluation**
04. Détecter et analyser les événements de cybersécurité			
Définition et analyse du fonctionnement nominal du système d'information	Définir les comportements attendus du système d'information, en collaboration avec les différents experts (experts métier, DSI, fonctions support), afin de formaliser le comportement nominal attendu du système d'information.	**Simulation sur plateforme** Il sera demandé au candidat de collecter et d'analyser les éléments techniques permettant de détecter et qualifier des événements de cybersécurité. Pour ce faire, le candidat sera immergé dans la simulation d'une entreprise fictive et de son Système d'Information. Cette simulation s'appuie sur une plateforme technologique répliquant un Centre Opérationnel de Sécurité (SOC) à taille réelle, déployé et connecté à l'infrastructure physique implémentée dans les locaux du certificateur. Le candidat recevra les éléments suivants : - un système de gestion d'événements de sécurité (SIEM) - un outil d'automatisation et d'orchestration des événements de sécurité (SOAR) - un puits de logs - un playbook - des rapports de CERT - une équipe d'experts métiers pour les jeux de rôles Le candidat présentera la méthodologie et les résultats de ses travaux au cours d'une soutenance orale.	Au moins 80% des comportements légitimes du système d'information simulé sont répertoriés.
	Qualifier un événement de cybersécurité en fonction du comportement nominal du système d'information et des scenarios de gestion d'événements cyber (playbook), afin de le documenter, de déterminer son niveau de criticité et d'appliquer le traitement associé		Au moins 80% des événements de cybersécurité sont qualifiés et documentés.
Définition du processus de collecte des journaux d'événements en fonction des menaces (playbook)	Définir la collecte, la conservation et l'archivage des journaux d'événements (logs) nécessaires, en fonction des scenarios de gestion d'événements cyber (playbooks) et en accord avec les contraintes et exigences de l'organisation (conformité, budget...), pour analyser le fonctionnement du système d'information		Au moins 80% des règles pour la collecte, la conservation et l'archivage des logs sont définies en fonction du playbook.
	Adapter les scenarios de gestion d'événements cyber (playbook) en fonction de l'état la menace afin d'optimiser les détections des évènements de sécurité dans une optique d'amélioration continue		Un playbook est mis à jour en réponse à de nouveaux rapports de menace.
Automatisation et orchestration des règles de corrélation d'événements	Programmer des règles de corrélation d'événements associées aux scenarios de gestion d'événements cyber (playbook) en vue de détecter des événements de sécurité de façon automatisée à travers un système de gestion des événements et des informations de sécurité (SIEM).		- 80% des règles de corrélation sont mises en place dans le SIEM en fonction du playbook. - L'événement cyber décrit dans le playbook est correctement détecté par le SIEM.
	Développer des réponses automatisées, en programmant des règles de corrélation (algorithmes) d'événements et en les intégrant dans un outil d'orchestration, d'automatisation et de réponse aux incidents de sécurité informatique (SOAR), afin d'optimiser le traitement des incidents de sécurité détectés.		Au moins une tâche du playbook est automatisée et correctement implémentée dans le SOAR