Référentiel d'activités, de compétences et d'évaluation

Article L6113-1 créé par la 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. »

REFERENTIEL D'ACTIVITES *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**REFERENTIEL DE COMPETENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**REFERENTIEL D'EVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
Bloc 1 : Conseiller une organisation en sécurité des systèmes d'information			
A1 : Apport de son expertise SSI aux organes de direction • **T1.A : Audit des pratiques professionnelles** • **T1.B : Évaluation des risques de cybersécurité**	B1C1 : Auditer les pratiques professionnelles des collaborateurs pour identifier des possibilités d'amélioration dans leur mise en œuvre des normes (RGPD, ISO 2700x, …), des standards et des règles liés à la sécurité informatique dans les architectures de systèmes d'information ou les applications. B1C2 : Élaborer des documents tels que des notes, des guides, des présentations et des directives pour l'organisation dans le but de minimiser les risques en matière de cybersécurité.	ME1 : Étude de cas d'une entreprise qui souhaite renforcer sa posture de sécurité face aux menaces de cyberattaques. À partir des données financières, stratégiques et sur les infrastructures de l'organisation, le responsable de la sécurité des systèmes d'information (RSSI) est chargé de conseiller la direction générale et de mettre en œuvre des stratégies efficaces. À partir de la distribution du cas pratique, les candidats ont 4 heures pour présenter un compte rendu écrit, sous forme d'une présentation professionnelle (Powerpoint ou équivalent), devant un jury. La durée de présentation orale devant le jury est fixée à 30 minutes.	CE1.1 : Toutes les pratiques professionnelles concernées par la cybersécurité sont recensées. CE1.2 : Chaque recommandation formulée est accompagnée d'une proposition d'amélioration. CE1.3 : Les principaux risques cyber sont présentés clairement et explicitement. CE1.4 : Les recommandations stratégiques sont assorties d'actions spécifiques à entreprendre. CE1.5 : L'impact potentiel de chaque recommandation est évalué.

	B1C3 : Évaluer les risques de cybersécurité susceptibles de toucher son organisation afin de renforcer sa résilience cyber.		CE1.6 : Les risques sont identifiés par une analyse de risques complète et documentée.
A2 : Prévention des risques de cybersécurité pour son organisation • **T2.A : Anticipation des risques de cybersécurité** • **T2.B : Sensibilisation des organes de direction**	B1C4 : Sensibiliser ses collaborateurs, ses clients ou sa hiérarchie au risque cyber et à l'intérêt stratégique de la mise en place d'une politique de cybersécurité. B1C5 : Réaliser une veille technologique des solutions et des outils de cybersécurité dans le but de conseiller rapidement son organisation en prévention d'un danger imminent.		CE2.1 : Tous les risques spécifiques à l'organisation sont liés à un outil de prévention. CE2.2 : Les vulnérabilités critiques sont hiérarchisées en fonction de leur impact potentiel afin de favoriser la force de sensibilisation. CE2.3 : Un processus de veille des outils de cybersécurité est proposé.
A3 : Gestion financière d'une entreprise ou d'un service dans le domaine de la SSI • **T3.A : Pilotage financier de l'activité** • **T3.B : Élaboration d'un business plan**	B1C6 : Analyser l'écosystème cyber via une étude de marché et la création d'un business plan afin de convaincre de potentiels investisseurs. B1C7 : Piloter financièrement l'activité d'une entreprise en s'appuyant sur des outils de suivi financier (dashboards, outils de business intelligence, etc.) afin de garantir la viabilité de l'entreprise.		CE3.1 : L'analyse de l'écosystème cyber est exhaustive et chiffrée. CE3.2 : Les projections financières sont détaillées et quantifiées. CE3.3 : L'utilisation des outils de suivi financier est détaillée et quantifiée. CE3.4 : Les dépenses sont alignées avec les objectifs stratégiques énoncés et les données financières fournies.
Bloc 2 : Protéger une organisation contre les menaces numériques			
A4 : Réalisation d'une veille technologique sur l'actualité des vulnérabilités et des	B2C1 : Collecter et analyser les données provenant de sources de renseignements en sources ouvertes (OSINT = Open Source Intelligence) afin de juger des	ME2 : Mise en situation. Le candidat est chargé de la protection des systèmes d'information d'une entreprise technologique qui est	CE4.1 : Des techniques de renseignements sont mises en œuvre, dans le cadre d'une veille technologique sur les

menaces dans le domaine de la cybersécurité • **T4.A : Collecte et analyse d'informations cyber** • **T4.B : Participation aux innovations de la sécurité des SI**	opportunités d'amélioration de la sécurité des données, des systèmes et du réseaux. B2C2 : Analyser les menaces et les incidents (CTI - Cyber Threat Intelligence) après collecte d'informations en utilisant des sources ouvertes et privées ainsi que des outils spécialisés.	régulièrement ciblée par des attaques sophistiquées. En tant que chargé de la cyberdéfense de votre organisation, le candidat doit mettre en place une stratégie complète de veille et de protection. Préalablement, les candidats doivent analyser les menaces pouvant porter sur l'entretien, en fonction du contexte fourni, et après une collecte de données pertinentes.	menaces, sur deux sources différentes minimum. CE4.2 : Une analyse précise de la menace cyber est réalisée à partir des informations trouvées sur l'entreprise en question.
A5 : Protection du SI • **T5.A : Mise en œuvre des outils de sécurité informatique** • **T5.B : Enquête sur les intrusions et incidents de sécurité** • **T5.C : Investigation par examen de la mémoire et des artefacts (Forensic)**	B2C3 : Mettre en œuvre des outils de sécurité informatique pour surveiller, détecter et contrer les menaces, tels que les EDR, les XDR, les pare-feu, les systèmes de détection d'intrusion et les SIEM. B2C4 : Enquêter sur les intrusions et les incidents de sécurité à partir de journaux d'évènements (logs), de rapports d'incidents et toute autre information disponible provenant d'un outil de défense. B2C5 : Réaliser une investigation par examen de la mémoire d'un matériel numérique et des artefacts des systèmes d'exploitation et des réseaux.	Au cours de la mise en situation, des cyberattaques sur un SI sont simulées et des supports mémoires sont fournis aux candidats. Les candidats doivent alors mettre en œuvre des outils de détection et d'analyse des événements. Puis, les candidats doivent déterminer, après plusieurs investigations, la nature des menaces et mettre en œuvre les outils de protection associés. La mise en situation dure 4 heures. Pendant cette durée, les candidats renseignent un rapport faisant état de leur stratégie complète de protection en suivant les directives précitées. Ce rapport est ensuite soutenu devant un jury pendant 30 minutes.	CE5.1 : Les outils de sécurité sont correctement configurés pour répondre aux besoins spécifiques de l'entreprise. CE5.2 : La surveillance et la détection des menaces sont effectives. CE5.3 : L'enquête à partir des journaux d'évènements est menée de manière systématique et conforme aux meilleures pratiques. CE5.4 : Les mesures correctives proposées sont adéquates et préventives. CE5.5 : Une investigation sur au moins un support matériel est réalisée avec précision et exhaustivité.
Bloc 3 : Auditer la sécurité technique d'une organisation			
A6 : Conduite d'un audit de sécurité technique d'une organisation	B3C1 : Réaliser des tests d'intrusion sur les systèmes et les réseaux afin d'identifier leurs vulnérabilités.	ME3 : Mise en situation d'un audit technique sur une organisation.	CE6.1 : Les tests d'intrusion sur les systèmes, les réseaux, les applications web

• **T6.A : Conduite de tests de pénétration sur les SI d'une organisation** • **T6.B : Audit de code source** • **T6.C : Audit de configurations** • **T6.D : Simulation d'une intrusion malveillante**	B3C2 : Réaliser des tests d'intrusion sur les applications web ou mobiles afin d'identifier leurs vulnérabilités. B3C3 : Auditer le code source d'une solution logicielle pour identifier les vulnérabilités et les failles de sécurité. B3C4 : Conduire une simulation d'intrusion malveillante multifactorielle en élaborant puis en exécutant des scénarios d'intrusion qui reproduisent les actions de cybercriminels en utilisant des techniques telles que l'ingénierie sociale, le vol, l'intrusion physique, et autres.	Une entreprise souhaite évaluer la robustesse de sa sécurité informatique. Un auditeur de sécurité (pentester) est chargé de conduire un audit technique complet, en respectant les normes légales et éthiques, et de fournir un rapport détaillé qui permettra d'améliorer la résilience de l'entreprise. Les candidats disposent de 4 heures pour : - Auditer la machine de l'entreprise mise à leur disposition pour déterminer ses vulnérabilités et la compromettre. - Auditer un site web de l'entreprise en question - Élaborer un scénario d'intrusion crédible reproduisant une éventuelle action de cybercriminels à partir des données fournies (notamment sur la situation physique de l'entreprise) dans le scénario de la mise en situation. Les candidats disposent ensuite de 4 heures supplémentaires pour rédiger et rendre un rapport d'audit. Enfin, les candidats présentent leur rapport devant un jury pendant 30 minutes. Le fonctionnement de l'évaluation est proche de celui de la certification OSCP (Offensive Security Certified Professional) proposée par l'organisme Offensive Security. Comparativement, les durées de réalisation et de rédaction ainsi que le nombre de	et mobiles sont réalisés efficacement. CE6.2 : Des vulnérabilités sont identifiées de manière précise. CE6.3 : La machine est compromise à l'issue de la phase d'audit technique. CE6.4 : L'audit du code source est mené de manière approfondie et permet de révéler au moins trois failles. CE6.5 : Au moins un scénario d'intrusion crédible est élaboré afin de reproduire une éventuelle action de cybercriminels.
A7 : Réalisation d'un rapport d'audit technique • **T7.A : Communication adaptée des résultats de l'audit en fonction du public cible** • **T7.B : Classement des vulnérabilités selon leur probabilité et leur impact potentiel**	B3C5 : Rapporter et communiquer les résultats d'un audit ou d'une investigation cyber en adaptant son support et son discours à la diversité du niveau d'expertise du public concerné afin de faire prendre des contre-mesures adaptées et ainsi réduire les risques d'attaque sur l'organisation.		CE7.1 : Les vulnérabilités sont classées selon leur niveau de risque. CE7.2 : Les résultats des audits et des investigations sont rapportés de manière claire et précise. CE7.3 : Le support et le discours sont adaptés au niveau d'expertise du public cible. CE7.4 : Des recommandations pour des contre-mesures appropriées sont fournies
A8 : Respect de la législation lors de la réalisation d'un audit	B3C6 : Réaliser un audit technique en respectant la législation en vigueur (en particulier le code pénal) et l'éthique.		CE8.1 : L'audit technique est réalisé sans enfreindre la législation en vigueur.

• **T8.A : Encadrement du périmètre de l'audit** • **T8.B : Contractualisation avec l'entreprise et respect de l'éthique**		machines à compromettre sont réduites.	CE8.2 : Un exemple de contrat encadrant la réalisation de l'audit technique est établi.
Bloc 4 : Concevoir des solutions techniques sécurisées			
A9 : Conception sécurisée d'une architecture SI • **T9.A : Création de l'architecture SI de façon sécurisé** • **T9.B : Mise en place d'outils de protection sur une architecture SI existante**	B4C1 : Concevoir l'architecture SI de l'entreprise dans le contexte d'un réseau informatique, télécom ou industriel afin de répondre au besoin fonctionnel de l'organisation en prenant en compte le plan de routage, le cloud, la localisation des services, le besoin exprimé de fonctionnalité du SI. B4C2 : Mettre en place des outils et des mesures de protection sur l'architecture SI de l'entreprise dans le contexte d'un réseau informatique, télécom ou industriel afin de rendre opérationnelles les nouvelles fonctionnalités en prenant en compte les solutions logicielles de déploiement d'architecture (ansible, puppet, ...) et les spécificités des systèmes visées (windows, linux, ...).	ME4.A : Exercice pratique d'élaboration d'une architecture SI sécurisée Les candidats devront concevoir une architecture SI répondant à un besoin précis qui sera fourni dans la consigne de l'exercice, en tenant compte des principes de sécurité. Ils devront identifier les composants clés, définir les flux de données, les configurations à mettre en œuvre et intégrer des mesures de sécurité adaptées. ME4.B : Exercice pratique de développement d'une solution logicielle sécurisée Les candidats devront développer une portion d'un logiciel en intégrant des mesures de sécurité adaptées. ME4.C : Exercice pratique de développement d'un outil de sécurité Les candidats devront rédiger un script en langage Python permettant la réalisation d'une tâche ayant pour objectif le renforcement de la résilience cyber d'un SI.	CE9.1 : L'architecture est schématisée sans erreur et selon les conventions d'usage informatiques. CE9.2 : La solution proposée est sécurisée afin de prévenir les intrusions dans le réseau.

A10 : Conception sécurisée d'un logiciel • **T10.A : Création d'un logiciel sécurisé** • **T10.B : Mise en place de solutions sécurisées sur des applications lourdes**	B4C3 : Concevoir des solutions logicielles de façon sécurisée dans les contextes d'une application lourde, du web ou de l'embarqué afin de répondre aux besoins fonctionnels du produit visé en fonction des problématiques algorithmique, de performance, de l'architecture du code, et les interactions avec les bases de données.		CE10.1 : La solution logicielle est fonctionnelle et répond au besoin demandé. CE10.2 : La solution proposée ne présente pas de faille critique de sécurité informatique.
	B4C4 : Mettre en œuvre les solutions logicielles de façon sécurisée dans les contextes d'une application lourde, du web ou de l'embarqué afin de rendre opérationnelles les nouvelles fonctionnalités en prenant en compte les spécificités des langages employés, des bibliothèques de fonctions, et des API de services tiers.		
A11 : Conception d'un outil de sécurité • **T11 : Développement d'un outil de sécurité en langage Python**	B4C5 : Concevoir un outil de sécurité pour répondre à un besoin précis de son organisation.		CE11.1 : Le script fourni est fonctionnel et présente un intérêt certain pour la résilience cyber de l'organisation. CE11.2 : Le script fourni est optimisé.
Bloc 5 : Gérer une crise cyber			
A12 : Prévenir une crise en cybersécurité tout en permettant la continuité et/ou la reprise d'activité • **T12.A : Élaboration d'un plan de prévention des crises**	B5C1 : Contrôler l'application des consignes préventives de sécurité émises en phase conseil et lors de retour d'expérience à destination des équipes techniques afin de se préparer à une crise cyber.	ME5 : Mise en situation au travers d'un scénario de crise proche des scénarios élaborés et recommandés par l'ANSSI (Agence nationale de la sécurité des systèmes d'information), suivie de l'écriture d'un rapport contenant un compte rendu technique et situationnel sur	CE12.1 : Les mesures préventives existantes, notamment les PCA et PRA, sont critiquées pour mettre en lumière leurs limites. CE12.2 : De nouvelles directives préventives sont

• **T12.B : Réalisation de test de résilience et de reprise d'activité**	B5C2 : Planifier les missions des équipes techniques concernant l'application des éléments cyber du PCA et du PRA afin de permettre respectivement la continuité et la reprise d'activité.	le déroulement de la crise ainsi qu'un retour d'expérience dans le but d'améliorer la résilience cyber de l'organisation. Ce rapport est ensuite soutenu devant jury.	suggérées pour renforcer la résilience cyber de l'organisation. CE12.3 : Un plan de gestion de crise est établi avec les rôles de chaque membre de l'équipe technique.
A13 : Gérer une crise de cybersécurité en lien avec les équipes techniques et les institutions • **T13.A : Pilotage de la crise** • **T13.B : Communication avec les institutions lors d'une crise**	B5C3 : Piloter les équipes techniques en situation de crise de cybersécurité afin d'apporter, par son expertise, la capacité de réagir rapidement et de s'adapter aux imprévus non couverts par les documents préventifs préalablement établis (PCA,PRA, autres...). B5C4 : S'appuyer sur les acteurs institutionnels de l'écosystème cyber (DGSI, ComCyberGend, ANSSI, CNIL…) pour aider à la résolution de la crise et initier une action auprès des acteurs appropriés.		CE13.1 : Les imprévus sont gérés avec réactivité. CE13.2 : Les mesures prises permettent d'éviter la propagation de l'attaque. CE13.3 : La gestion de crise proposée permet d'équilibrer les missions de chaque membre de l'équipe technique tout en répondant à leur niveau de compétence. CE13.4 : Une proposition de déclaration de la crise à une institution est établie afin de répondre aux enjeux légaux et permettre d'alerter efficacement sur la menace. CE13.5 : Aucune déclaration d'ordre légal n'est omise.
A14 : Assurer la capitalisation des retours d'incident en mesure préventive et/ou corrective dans le PCA, le PRA, le SI ou la production. • **T14.A : Capitalisation des retours d'incident**	B5C5 : Analyser, en situation de crise de cybersécurité, les écarts entre les documents préventifs préalablement établis (PCA, PRA, autres...) et les incidents rencontrés afin d'alimenter le retour d'expérience. B5C6 : Conduire des enquêtes techniques de réponse à incident lors d'une crise cyber, permettant une identification des origines de l'attaque et une		CE14.1 : Le retour d'expérience rédigé permet la compréhension du scénario de l'attaque (origine, chemin et objectif des attaquants). CE14.2 : Le retour d'expérience rédigé permet la mise à jour des documents préventifs.

• **T14.B : Enquête sur l’origine de la crise et le chemin des attaquants**	compréhension détaillée du modus operandi des attaquants.		CE14.3 : Le retour d’expérience rédigé permet de réduire la durée d’inactivité des services en cas de cyberattaques similaires à l’avenir.