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.* »

Bloc n°1 – Gérer les risques liés à la sécurité de l'information			
RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**

A1 Évaluation des risques T1 Identification des actifs informationnels et des menaces associées T2 : Définition des critères de base tels que les critères d'évaluation du risque, les critères d'impact et les critères d'acceptation des risques T3 Estimation et hiérarchisation des risques	C1 Identifier les actifs informationnels afin de déterminer leur importance pour l'organisation en réalisant un inventaire exhaustif et en évaluant leur criticité. C2 Identifier les sources de menaces en cybersécurité et évaluer leur pertinence en utilisant des méthodes d'analyse appropriées. C3 Évaluer les scenarios stratégiques et opérationnels des sources de menaces identifiées afin d'évaluer leur probabilité d'occurrences en se basant sur une méthode d'analyse de risques (Ex : EBIOS RM) C4 Estimer l'impact potentiel des risques en cybersécurité pour l'organisation en analysant les conséquences possibles sur les actifs informationnels. C5 Classifier les risques identifiés pour prioriser les actions de traitement en utilisant des critères d'impact et de probabilité en hiérarchisant les actions à mener.	E1 : Mise en situation professionnelle Analyse de risque d'un SI. Les candidats se voient présenter un cas d'une entreprise réelle ou fictive à l'aide d'une documentation précise sur son activité et ses ressources incluant son système d'information. Leur tâche est de réaliser et présenter une analyse de risque en adéquation avec les besoins et contraintes de l'organisation et de proposer un plan de traitement des risques.	C1 La liste des actifs informationnels est exhaustive et leur criticité est évaluée de manière précise. C2 Les menaces sont analysées de manière pertinente avec une évaluation rigoureuse de leur probabilité d'occurrence. C3 Les scenarios d'attaques sont identifiés et évalués en fonction de la vraisemblance vis-à-vis du contexte de l'organisation. C4 L'impact potentiel des risques est estimé avec précision, en détaillant les conséquences possibles pour chaque actif informationnel. C5 Les risques sont hiérarchisés de manière logique et cohérente en utilisant des critères d'impact et de probabilité bases sur des référentiels de confiance.

A2 Gestion des risques T1 Mise en œuvre des mesures de sécurité pour traiter les risques identifiés T2 Suivi et réévaluation des risques dans une démarche d'amélioration continue	C6 Élaborer des stratégies de traitement des risques pour répondre aux résultats de l'évaluation des risques en proposant des méthodes de traitement du risque appropriées à l'organisation (réduction / transfert / refus) et en proposant des mesures en adéquation avec la méthode de traitement choisie C7 Mettre en œuvre le plan de traitement des risques en respectant les recommandations de l'analyse de risques afin de répondre aux exigences des normes et des politiques applicables au sein de l'organisation. C8 Suivre et réévaluer les risques de manière continue pour assurer une démarche d'amélioration continue en établissant des indicateurs de performance et de conformité C9 Proposer un plan de remédiation pour le traitement des risques en garantissant la conformité aux besoins et contraintes de l'organisation.		C6 Les stratégies de traitement des risques sont développées et justifiées en fonction des contraintes et ressources de l'organisation C7 Les mesures de sécurité recommandées sont identifiées dans un plan d'action établissant des indicateurs permettant le suivi dans une démarche d'amélioration continue. C8 Les risques sont suivis et réévalués continuellement à travers des tableaux de bord et des rapports périodiques, utilisant des indicateurs de performance (ie résultats de scans de sécurité) pour intégrer la gestion des risques dans un processus d'amélioration continue. C9 Le plan de remédiation est construit et hiérarchisé en prenant en compte les contraintes métiers et le contexte de l'organisation

Bloc n°2 –Protéger un système d'information face à la cyber-menace			
RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**

A1 Identification des besoins de sécurité de l'organisation. T1 Cartographie d'un SI et identification des actifs critiques de l'organisation T2 Mise en place d'un processus de veille en cybersécurité T3 Analyse du système d'information et des mesures de sécurité en œuvre T4 Protection des systèmes d'information T5 Protection des composants logiques	C1 Cartographier un système d'information pour maintenir une vision claire des actifs à protéger en identifiant, classifiant et documentant tous les composants physiques et logiques du système leurs interconnexions, leurs dépendances et leur niveau de criticité. C2 Mettre en place un système de veille pour suivre les flux d'information liés aux menaces et aux vulnérabilités en identifiant et utilisant les sources d'informations pertinentes et en analysant les données recueillies. C3 Évaluer la pertinence des solutions de sécurité en réalisant un audit des mesures mises en œuvre et en évaluant leur impact sur la sécurité du système d'information. C4 Mettre en œuvre des mesures de durcissement du SI pour renforcer sa sécurité et réduire la surface d'attaque en configurant les paramètres de sécurité et en choisissant des mesures de sécurité adaptées à l'organisation. C5 Définir les paramètres de sécurité des composants logiques d'un système d'information, y compris les hyperviseurs, les containers, les orchestrateurs, les applications et les différents services critiques, afin de renforcer leur sécurité en suivant les politiques de l'organisation, et en se basant sur des référentiels de sécurité.	E1 : Mise en situation professionnelle : Renforcer la sécurité technique d'un SI. Les candidats se voient présenter le système d'information d'une organisation réelle ou fictive comprenant notamment : un schéma d'infrastructure, la description des caractéristiques techniques, le registre des données utilisées ainsi qu'un cahier des charges. Leur tâche est de proposer un plan d'action en vue de sécuriser l'infrastructure en veillant à la conformité des solutions proposées vis-à-vis des normes et standards en fonction de l'activité de l'organisation tout en respectant les exigences du cahier des charges.	C1 Les composants matériels et logiques de l'infrastructure sont listés sur un schéma d'architecture et dans des matrices de flux. C2 Un processus de veille en cybersécurité comprenant des sources d'information et des référentiels pertinents, fiables et maintenus à jour est présenté. C3.1. Des solutions adaptées sont proposées pour renforcer la sécurité de chacun des composants du système d'information ainsi que les interconnexions entre les différents sous-systèmes. C3.2 : Les protocoles et les types de données stockées sont listés et respectent les politiques, normes et référentiels de sécurité établis dans l'organisation. C4 Les différents types d'attaque et les risques associés aux actifs sont identifiés. Des mesures de sécurité à mettre en œuvre sont choisis pour chaque composant du système d'information. C5 Les règles de durcissement des systèmes d'exploitation et des

A2 Définition d'un ensemble de mesures de protections des données du SI T1 : Identification des données sensibles de l'organisation et les classifier en respectant les lois, règlements et normes auxquels sont soumis l'organisation T2 : Application de mesure de sécurité des données	C6 Classifier les données sensibles et s'assurer de l'efficience des mesures de sécurité pour en assurer la confidentialité et l'intégrité en garantissant la conformité des usages aux politiques de gestion des identités et des données C7 Appliquer des mesures de sécurité sur les données pour assurer leur confidentialité et leur intégrité en fonction de leur niveau de criticité en se basant sur les référentiels, politiques, normes, lois et règlements auxquels sont soumis l'organisation.		applications respectent les normes, référentiels et politiques de l'organisation et sont soumis aux principes de moindres privilèges tout en respectent les politiques d'accès aux ressources de l'organisation. C6 Les données sont identifiées et classées en fonction des usages et la classification est conforme aux exigences de l'organisation C7 Les algorithmes de chiffrement, de hashage et de signature numérique sont choisis en adéquation avec les référentiels applicables et les besoins de l'organisation.

Bloc n°3 – Assurer la conformité du traitement de l'information au cadre réglementaire et normatif en vigueur dans l'organisation			
RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois vi*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**

A1 Mise en conformité légale et réglementaire T1 Identification des lois et règlements et normes applicables au sein de l'organisation T2 Évaluation de la conformité actuelle des pratiques de l'organisation T3 Développement de politiques, de procédures et de suivi de la conformité	C1 Identifier les lois, règlements et normes applicables au sein de l'organisation afin de garantir la conformité en matière de sécurité des données traitées en effectuant une veille. C2 Évaluer la conformité actuelle des pratiques de l'organisation afin de détecter les écarts par rapport aux exigences légales en réalisant des audits et des revues documentaires. C3 Développer des politiques et des procédures de conformité pour répondre aux exigences légales et réglementaires en élaborant des documents clairs et détaillés.	E1 : Mise en situation professionnelle : Le candidat présente un projet d'étude de conformité légale, réglementaire ou normatif mené de bout en bout sur un sujet de sécurité des données personnelles ou de la sécurité des systèmes d'information par rapport à une loi, une réglementation ou une norme.	C1 Une liste des lois, règlements et normes applicables sont listes de manière exhaustive et leur impact sur l'organisation est clairement expliqué. C2 La conformité actuelle des pratiques de l'organisation est évaluée avec précision, et les écarts par rapport aux exigences sont clairement identifiés. C3 Les politiques et procédures de conformité sont développées de manière détaillée et alignées avec les exigences légales, réglementaires et normatives.

A2 Suivi de la mise en conformité T4 Mise en œuvre des mesures de conformité nécessaires	C4 Mettre en œuvre les mesures de conformité nécessaires afin de corriger les écarts identifiés et de prévenir les non-conformités en suivant un plan d'action structuré et une démarche d'amélioration continue.		C4 Les mesures de conformité nécessaires sont listées de manière rigoureuse et selon le plan d'action structuré.
T5 Formation et sensibilisation des employés sur les exigences légales	C5 Former et sensibiliser les employés sur les exigences légales et normatives afin d'assurer une compréhension et une application adéquates des règlements et procédures en organisant des sessions de formation et en fournissant des ressources pédagogiques adaptées aux personnes en situation de handicap et en évaluant l'efficacité des campagnes de sensibilisation.		C5 Des sessions de formation et les ressources pédagogiques efficaces et adaptées aux personnes en situation de handicap sont proposées et assurent une compréhension adéquate des exigences de l'organisation par les employés.
T6 Suivi de la conformité et amélioration continue	C6 Suivre la conformité de manière continue pour assurer le respect des exigences légales et normatives en établissant des indicateurs de performance et en réalisant des audits réguliers.		C6 Un plan de suivi de la conformité comprenant des indicateurs de performance (ie taux de conformité) sont pertinents et adaptés à l'organisation et des audits réguliers est proposé.
T7 Gestion des incidents de non-conformité et application des correctifs	C7 Gérer les incidents de non-conformité afin de minimiser les impacts légaux et opérationnels en appliquant des procédures de gestion des incidents et des correctifs appropriés.		C7 Des correctifs approprié et minimisant l'impact de non-conformité sont proposés pour chaque incident.
T8 Documentation et communication des efforts de conformité	C8 Documenter et communiquer les efforts de conformité pour démontrer l'engagement de l'organisation en matière de sécurité des données en produisant des rapports détaillés et accessibles.		C8 Les efforts de conformité sont documentés et communiqués de manière claire et détaillée, démontrant l'engagement de l'organisation en matière de sécurité des données.

Bloc n°4 – Piloter un projet et communiquer en cybersécurité			
RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A1. Réalisation d'un projet de cybersécurité T1 : Cadrage d'un projet de cyber sécurité T2 : Réalisation d'un cahier des charges et d'un plan d'assurance qualité T3 Conception d'un plan de gestion T4 Identification des risques T5 Suivi de projet	C1 Identifier une problématique en cybersécurité afin de mettre en place un projet pour la résoudre en intégrant les besoins de l'organisation et en réalisant une veille sur les solutions existantes. C2 Rédiger un cahier des charges du projet pour répondre à la problématique de sécurité identifiée en normalisant le cadre de gestion du projet et les livrables du projet C3 Concevoir un plan de gestion de projet afin d'assurer sa mise en œuvre en appliquant une méthode de gestion de projet définissant des objectifs, un calendrier, un budget et les livrables C4 Identifier les risques liés au projet pour définir les mesures de sécurité nécessaires à mettre en œuvre en respectant l'ensemble des objectifs et contraintes du cahier des charges, du calendrier et du budget. C5 Assurer le suivi de la gestion de l'équipe projet afin d'atteindre les objectifs du projet, par l'application de technique de communication et leadership, en tenant compte des situations de handicap éventuelles de chacun.	E1 : Mise en situation professionnelle : Le candidat doit travailler sur un projet ayant une problématique de cybersécurité clairement définie. Le candidat est libre de choisir la problématique et peut réaliser le projet en groupe. L'évaluation finale se fera au travers d'une soutenance ou les résultats et l'impact du projet seront présentés et devront répondre à la problématique de sécurité identifiée au lancement du projet.	C1 La problématique et l'impact en lien avec la cybersécurité sont clairement définis. Un état de l'art des solutions existantes est présenté. C2 le cahier des charges présente clairement les attentes du projet, ses objectifs, ses résultats attendus, le budget et la planification associés. C3 : Les rôles et responsabilités ainsi que le périmètre du projet sont définis et répondent à une problématique de sécurité identifiée et un plan de gestion du projet est définis et propose un calendrier et un budget prévisionnel en vue de répondre à la problématique du projet. C4 : Les risques principaux pouvant contraindre l'exécution du projet sont identifiés et des mesures pour les éviter sont proposées. C5 : Une méthode de suivi de projet fiable et s'appuyant sur des méthodes de gestion de projet éprouvée (ITIL, SCRUM,

			MSDL..) est présentée. La restitution montre une prise en compte des besoins collectifs et individuels, y compris les situations de handicap éventuelles.
A2. Communication d'une démarche de cybersécurité T1 Sensibilisation aux enjeux d'hygiène numérique : développement et maintien d'une culture de la sécurité de l'information T2 Communication et vulgarisation des enjeux techniques T3 Synthèse des résultats	C6 Sensibiliser tous les membres de l'organisation aux enjeux de la cybersécurité afin de promouvoir des comportements sécurisés et responsables, en adaptant les supports et les méthodes de communication pour les personnes souffrant d'un handicap C7 Développer un plan de communication adapté à l'ensemble des parties prenantes afin de veiller à la bonne application de la PSSI en impliquant la direction. Adapter ce plan à leurs fonctions et à la prise en compte des éventuels enjeux de communication pour les personnes en situation de handicap. C8 Synthétiser les résultats de la démarche afin de communiquer de manière claire et convaincante en identifiant et structurant les éléments clés du projet dans un rapport écrit et une présentation orale.		C6 Les messages de sensibilisation sont clairs et répondent au besoin de sécurité identifié dans le but de promouvoir des comportements sécurisés et responsables. Les supports et méthodes de communication relatifs à la sensibilisation sont adaptés et accessibles aux personnes souffrant d'un handicap. C7 Les communications sont présentées de manière adaptée aux fonctions et aux besoins des différentes parties prenantes en tenant compte des enjeux de communication pour les personnes souffrant de handicap. C8 Le rapport contenant les résultats de l'audit et une évaluation des risques associés est clair, bien structuré et synthétise de manière convaincante les résultats de la démarche en identifiant et présentant les éléments clés du projet. Ce rapport est présenté de façon synthétique pendant la présentation orale.

Bloc de spécialisation n°1 – Mener un audit de sécurité d'un système d'information			
RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A1. Mise en place d'un système de management d'audit de sécurité T1 Définition des objectifs et du programme d'audit T2 Mise en place d'un système de suivi	C1 Définir un contrat et un programme d'audit pour atteindre les objectifs fixés par l'organisation en identifiant les différents rôles et responsabilités et en fixant le périmètre d'audit C2 Définir un système de management de suivi du programme d'audit pour assurer le suivi de l'audit en réalisant une analyse des résultats et en mettant en œuvre un système de gestion et de conservation des enregistrements des résultats d'audit.	E1 : Le candidat réalise un audit de sécurité qu'il soit organisationnel, intrusif, réseau, de vulnérabilités, de code ou de conformité sur une organisation réelle ou fictive. L'ensemble des données nécessaire pour réaliser l'audit est mis à disposition du candidat. Le candidat réalisera l'audit et produira un rapport d'audit conforme au plan d'audit et permettant à l'organisation	C1 Les objectifs, critères et méthodes d'audit sont choisies et documentées. Un programme d'audit répondant au besoin de l'organisation est présenté. C2 Un suivi de l'audit comprenant l'historique des missions et des résultats de chaque réalisation est présenté.

A2 Réalisation d'un audit de sécurité d'un système d'information T4 préparation des activités d'audit	C3 Préparer les activités d'audit afin de suivre le plan d'audit défini en réalisant une revue documentaire et en préparant la répartition des tâches au sein de l'équipe de travail.	d'avoir une vision claire de sa maturité sur le sujet de l'audit. Il défendra ce rapport lors d'une soutenance orale	C3 Les activités d'audit sont identifiées et les rôles et responsabilités sont attribués au sein de l'équipe d'audit.
T5 Suivi des activités d'audit	C4 Suivre les activités d'audit pour répondre au plan d'audit établi en réalisant le suivi documentaire, la communication et la revue des informations produites.		C4 L'audit est mené conformément au plan d'audit et les résultats obtenus sont véritables et revus pour établir la conformité avec le plan d'audit
T6 Préparation et production du rapport d'audit T7 Présentation des résultats	C5 Elaborer l'ensemble des documents nécessaire à la restitution de l'audit pour présenter les résultats obtenus en rédigeant un rapport et une synthèse claire à destination de la direction C6 Présenter les conclusions de l'audit de manière claire et objective pour permettre à l'organisation de prendre des décisions stratégiques en se basant sur des indicateurs et les conclusions de l'audit		C5 Le rapport d'audit répond aux besoins de l'organisation et est conforme au plan d'audit. Ce rapport présente des résultats permettant d'évaluer le niveau de maturité de l'organisation et est défendu lors d'une présentation orale. C6 Les conclusions de l'audit sont clairement établies et permettent à l'organisation de mettre en place une orientation stratégique

Bloc de spécialisation n°2 – Opérer et surveiller les mesures de sécurité d'un SI			
RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A1 Gestion des événements et les incidents de sécurité de l'information T1 Conception d'un processus de gestion des événements et des incidents de sécurité de l'information T2 Identification des pistes d'automatisation et d'outillage concernant l'identification, la gestion des priorités et le traitement des événements et des incidents de cyber sécurité T3 identification et classification d'une série d'incidents de cyber sécurité par l'analyse des journaux d'évènements et des alertes d'outils de surveillance.	C1 Déployer un système de surveillance de l'activité en sécurité de l'information pour détecter les événements et les incidents de sécurité, en intégrant leur traitement dans un processus de gestion d'incident et en prenant comptes des utilisateurs pouvant souffrir de handicap. C2 Concevoir un processus et un flux de traitement des événements et des incidents en s'appuyant sur la norme ISO 27035, pour automatiser le traitement des événements et des incidents C3 Identifier et classifier les alertes d'incidents des différents outils de sécurité présent (SIEM, XDR, EDR, IDS...) pour les intégrer au processus de gestion des incidents de sécurité en les priorisant en fonction du niveau de criticité et de leurs impacts.	E1 : Mise en situation professionnelle : A partir de l'étude d'une organisation fictive ou réelle. Le candidat doit créer un « proof of concept » de mise en œuvre d'un SOC dans l'organisation. Ce « proof of concept » comprend une infrastructure web sur laquelle un SIEM est déployé, des indicateurs sont créés, les processus et procédures de résolution d'incidents établies, suivis et évaluées. Le système est testé par la simulation d'un incident de sécurité.	C1 Face à une série d'événements, les incidents de sécurité sont distingués des faux positifs grâce à l'analyse approfondie des journaux d'évènements. Le tableau de bord est adapté pour les personnes souffrant de handicap. C2 les incidents sont identifiés, classés et assignés aux bons groupes de support. Les procédures sont établies et mises à jour dans un processus d'amélioration continue C3 Les incidents de sécurité sont identifiés et priorisés selon leur niveau de criticité et leurs impacts sur l'organisation.
A2 Traitement des incidents de sécurité T1 Définition d'un plan de traitement d'un incident de sécurité en fonction de son impact sur l'organisation	C4 : Définir une stratégie de traitement des incidents de sécurité pour l'intégrer à l'organisation en veillant à ce qu'elle soit conforme aux processus et procédures en place dans l'organisation (Ex : PRA/PCA) C5 : Définir un plan de traitement d'un incident de sécurité pour identifier son impact sur l'organisation en identifiant les différents sous-systèmes impactés		C4 Les sous-systèmes impactés par une attaque sont clairement identifiés et un plan de traitement est défini pour répondre à l'incident de sécurité et en limiter l'impact sur l'organisation

T2 Suivi du traitement des incidents de sécurité et intégration du processus de traitement dans une démarche d'amélioration continue	par l'attaque et en documentant un plan de résolution d'incident C6 Suivre le traitement des incidents de sécurité afin d'être en mesure d'identifier les forces et faiblesses de l'organisation en mesurant l'efficacité des processus et en l'intégrant dans une démarche d'amélioration continue C7 Vérifier l'efficacité de la stratégie de traitement des incidents de sécurité pour l'intégrer dans une démarche d'amélioration continue en réalisant des tests réguliers des procédures et processus établis (Ex : PRA/PCA)		C5 : Le traitement effectué sur les incidents de sécurité est intégré et conforme aux exigences de l'organisation, notamment le PRA/PCA. C6 Les incidents de sécurité sont suivis grâce à la définition d'indicateur pertinents comme le nombre d'incidents traités ou la durée moyenne de traitement et sont adaptés à l'organisation et des améliorations du processus de traitement sont proposées. C7 Le traitement des incidents est suivi à l'aide indicateur et une revue régulière est prévue et s'intègre aux procédures et processus de l'organisation (Ex : PRA/PCA)

Bloc de spécialisation n°3 – Intégrer des outils de sécurité dans un environnement hétérogène			
RÉFÉRENTIEL D'ACTIVITÉS *décrit les situations de travail et les activités exercées, les métiers ou emplois visés*	**RÉFÉRENTIEL DE COMPÉTENCES** *identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités*	**RÉFÉRENTIEL D'ÉVALUATION** *définit les critères et les modalités d'évaluation des acquis*	
		MODALITÉS D'ÉVALUATION	**CRITÈRES D'ÉVALUATION**
A1. Identification des différents composants et les interconnexions dans un système hétérogène T1 Identification des actifs T2 Conception de l'infrastructure nécessaire au déploiement de la solution de sécurité T3 Identification des impacts potentiels relatifs au déploiement de la solution de sécurité	C1 Identifier l'ensemble des actifs matériels, logiciels et humains nécessaires pour intégrer une solution de sécurité en prenant en compte les différentes interactions des sous-systèmes (Ex : SCADA, IoT, cloud...). C2 Identifier l'ensemble des interconnexions des sous-systèmes pour mettre en œuvre une stratégie de déploiement des outils de sécurité en les intégrant dans un environnement hybride. C3 Identifier les potentiels impacts de la mise en production d'une solution de sécurité afin de l'intégrer dans une infrastructure existante en évitant les phénomènes de régression et en limitant les pannes	Mise en situation professionnelle : A partir d'une infrastructure hétérogène (Industriel ; logistique ; Iot, embarque...) fictive ou réelle, le candidat propose diverses solutions de sécurité à mettre en œuvre pour augmenter la sécurité du traitement et des échanges d'informations. Les solutions mises en œuvre peuvent être du type firewall, IDS, XDR, WAF, NAC, data diode...	C1 L'ensemble de ressources nécessaires au déploiement de l'infrastructure est identifié. C2 Les interconnexions sont identifiées et les solutions proposées s'intègrent à une infrastructure existante. C3 Les impacts potentiels sur l'infrastructure existante sont identifiés et mesures afin de réduire le risque de régression lors du déploiement.
A2 Intégration des mesures de sécurité dans un système hétérogène T4 Déploiement d'une solution en l'intégrant dans un système existant T5 Gestion des interopérabilités et des contraintes métier	C4 Mettre en œuvre des stratégies de déploiement de mesures et services de sécurité pour rendre les sous-systèmes interopérables en les intégrant dans la chaine d'approvisionnement de l'organisation et en respectant les contraintes métiers. C5 Intégrer des mesures et services de sécurité dans un système hybride (Ex : Cloud prive/publique, hyperviseurs/containers...) afin de réduire l'impact d'une attaque sur un sous-système en intégrant cette solution dans l'infrastructure existante.		C4 La solution de sécurité est déployée en mettant en œuvre les bonnes pratiques de cyber-sécurité générales et spécifiques au type d'outil de sécurité déployé. La solution permet de réduire l'impact d'un ou plusieurs types d'attaque. C5 : La solution mise en œuvre a été testée et est conforme aux attentes en termes d'amélioration

T6 Mesure de l'efficacité de la solution de sécurité	C6 Mettre en place des moyens de contrôle et de surveillance des flux pour en garantir la sécurité en prenant en compte l'ensemble des contraintes métiers liés à l'activité de l'organisation. C7 Contrôler l'efficacité des mesures et services de sécurité pour les intégrer dans une démarche d'amélioration continue en définissant des indicateurs et en réalisant des audits réguliers.		de gestion des critères de sécurité (DICA) C6 Des indicateurs clés sont créés en vue de mesurer l'efficacité de la solution de sécurité et permettent le suivi en termes de disponibilité, confidentialité, intégrité et authenticité. C7 Des revues régulières des indicateurs sont prévues et participent à la démarche d'amélioration continue