RÉFÉRENTIEL DE LA CERTIFICATION
Expert en cybersécurité des Systèmes d'Information (BADGE)– EPITA

BLOC 1 : Sécuriser et superviser le système d'information (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 **Sécurisation des réseaux et infrastructures** • Création de la cartographie du SI • Cloisonnement des réseaux • Administration sécurisée d'un SI • Configuration des systèmes de contrôles d'accès • Analyse de transaction au sein d'un réseau • Analyse des attaques réseau	**C1** **Mettre en œuvre dans l'entreprise les bonnes pratiques d'administration du réseau** en créant une cartographie réseau intégrant tous ses composants, en configurant les contrôles d'accès, en cloisonnant les différentes parties du réseau et en interprétant les résultats des outils de surveillance d'infrastructures **afin d'organiser, créer et maintenir la sécurité du système d'information** **C2** **Identifier les problématiques de sécurité au sein d'un réseau** en interprétant les transactions entre les systèmes présents sur le réseau et en détectant les attaques de sécurité sur le réseau **pour prévenir les incidents de sécurité dans l'entreprise**	**Mise en situation professionnelle (C1-C4)** Sous la forme d'un projet pédagogique, le candidat devra créer l'organisation d'un réseau et sa cartographie. Il devra statuer sur la configuration des équipements et proposer des solutions permettant de détecter des attaques. Il devra aussi identifier les problématiques de sécurité en fonction de l'environnement et les corriger si besoin.	**C1** **Le candidat :** • Préconise une séparation du réseau prenant en compte la sécurité et le cloisonnement • Crée une cartographie réseau : elle comprend de manière exhaustive l'ensemble des composants • Gère les contrôles d'accès • Interprète les résultats d'outils de surveillance réseau **C2** **Le candidat :** • Décrit les transactions réseaux effectuées entre des équipements • Préconise des solutions pour détecter de potentielles attaques.
A2 **Sécurisation du cloud** • Définition d'une architecture de sécurité intégrant les services hébergés dans le cloud • Mise en place de la sécurité pour des micro-services • Automatisation de la sécurité dans un environnement cloud.	**C3** **Choisir et implémenter une stratégie de sécurité *cloud*** en analysant les architectures de sécurité des fournisseurs de *cloud*, en identifiant les problématiques de sécurité spécifiques aux micro-services, en intégrant au besoin les micro-services au sein de l'infrastructure traditionnelle et en réalisant l'automatisation des tâches opérationnelles de sécurité dans le *cloud* **afin de gérer la sécurité des services hébergés dans le *cloud*.**		**C3** **Le candidat :** • Identifie les problématiques spécifiques à la gestion des micro-services • Recommande les usages appropriés à l'utilisation des services *cloud* • Propose l'automatisation de tâches spécifiques pour la sécurité des services présents dans une infrastructure *cloud*.
A3 **Sécurisation des systèmes industriels** • Identifications des composants d'un écosystème SCADA ("Supervisory Control And Data Acquisition ", système de contrôle et d'acquisition de données) • Déterminer les risques de sécurité d'un système industriel au niveau technique et organisationnel • Appliquer une isolation d'un système industriel.	**C4** **Remédier aux risques des systèmes industriels dans un SI** en identifiant les composants d'un écosystème d'automates de gestion et de contrôle, les protocoles et architectures courants SCADA, en identifiant les vulnérabilités majeures de cybersécurité industrielle et les risques associés, en déterminant les risques inhérents à une architecture, et en choisissant les solutions appropriées, **afin de prévenir les dangers de sécurité générés par les équipements industriels.**	Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.	**C4** **Le candidat :** • Identifie les composants d'un système industriel • Propose des solutions adaptées aux spécificités SCADA • Détermine les risques et vulnérabilités liés à un système industriel et propose une solution adaptée au contexte.

A4 **Mise en œuvre des tests d'intrusion** • Utilisation d'un test d'intrusion dans une démarche de sécurité • Participation à un test d'intrusion • Identification des faiblesses du SI. • Prise en considération des faiblesses humaines et de leurs impacts.	**C5** **Effectuer des tests d'intrusions** en considérant les problématiques de sécurité opérationnelle, en sélectionnant le type de tests d'intrusion approprié, en utilisant les outils pour identifier des vulnérabilités et en construisant une campagne ciblée d'hameçonnage **afin d'identifier les vulnérabilités et faiblesses du SI et les failles humaines**	**Mise en situation professionnelle (C5)** Sous forme d'exercices pratiques, le candidat devra retrouver des failles de sécurité au sein d'un système informatique, exploiter ces vulnérabilités et ensuite sélectionner parmi plusieurs choix la solution appropriée. Pour valider, le candidat devra avoir résolu les deux tiers des épreuves.	**C5** **Le candidat :** • Sélectionne le type de tests d'intrusion approprié en fonction du cas • Utilise les outils permettant de réaliser un test d'intrusion • Exploite les vulnérabilités découvertes et propose des solutions pour améliorer la sécurité du SI.
A5 **Protection des données personnelles** • Identification des problématiques liées à la réglementation sur les données personnelles (LIL/RGPD) • Élaboration et application de processus garantissant le respect du RGPD	**C6** **Vérifier la conformité des pratiques dans l'entreprise à la législation sur les données personnelles** en prenant en compte les termes de la Loi Informatique et Libertés et du RGPD, en adoptant les bons réflexes dans la pratique quotidienne de la protection des données et en choisissant des solutions permettant une protection efficace des données à caractère personnel, **pour s'assurer que l'ensemble des procédures respectent les exigences légales.**	**Mise en situation professionnelle (C6)** Sous la forme d'un projet pédagogique, le candidat rédige un document décrivant le comportement attendu des collaborateurs d'une structure pour le respect de la protection des données à caractère personnel. Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.	**C6** **Le document rédigé par le candidat :** • Est conforme aux termes de la loi informatique et liberté et le RGPD • Comprend des procédures et des solutions permettant la continuité de la protection des données personnelles pendant les activités de l'entreprise.
A6 **Mise en place de la politique de sécurité** • Utilisation des normes ISO 27000 dans la politique de sécurité • Formalisation d'un guide et d'une charte SSI • Conception d'un document de référence pour la politique de sécurité • Prise en compte de l'accessibilité pour les Personnes en situation de handicap	**C7** **Concevoir un document de référence qui formalise la politique de sécurité** en évaluant les problématiques de sécurité et de gestion des données au sein d'un SI, en appliquant la série de normes ISO 27000, en utilisant le système développé par le NIST et en suivant le guide de l'ANSSI **pour orchestrer une politique de sécurité des SI pertinente**. **C8** **Intégrer les problématiques d'accessibilité dans la politique de sécurité** en évaluant les solutions retenues, en identifiant les aménagements raisonnables nécessaires et en appliquant le RGAA **afin d'assurer un niveau d'accessibilité des politiques de sécurité à toutes les parties concernées dans la structure.**	**Mise en situation professionnelle (C7-C8)** Sous la forme d'un projet pédagogique, le candidat rédige un document de référence destiné à l'ensemble de la structure documentant la politique de sécurité. Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.	**C7** **Le document rédigé par le candidat :** • Prend en compte la sécurité du SI et la gestion des données en son sein • Se base sur l'ensemble des documents de références permettant la formalisation d'une politique de sécurité. **C8** **La politique de sécurité rédigée par le candidat :** • Tient compte des problématiques d'accessibilité : les problématiques d'accès sont identifiées • Propose des aménagements dédiés en appliquant le RGAA.

BLOC 2 : Sécuriser les données, les projets et les développements

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**
A7 **Suivi d'un projet informatique :** • Expression du besoin et recueil d'information • Rédaction d'un cahier des charges. • Suivi du projet (méthode classique et approche Agile)	**C9** **Intégrer les enjeux de cybersécurité dans les projets informatiques de l'entreprise,** en cadrant l'expression du besoin par une note de synthèse, en structurant les différentes parties d'un cahier des charges liées à sécurité, en appliquant la méthodologie du projet (classique ou Agile) et en prenant en compte les étapes du projet, **afin d'assurer la prise en compte des enjeux de cybersécurité tout au long du cycle de vie des projets d'un point de vue métier.**	**Mise en situation professionnelle (C9-C10)** Sur la base d'un projet pédagogique d'analyse d'un projet informatique, le candidat expose son analyse en tenant compte des informations qui lui sont données et propose l'intégration de la sécurité dans ce projet.	**C9** **Dans l'analyse du candidat, on retrouve :** • Un besoin clairement identifié, les problématiques et risques de cybersécurité liés au projet sont analysés • Une méthodologie pertinente au regard du projet : les interventions liées à la cybersécurité sont planifiées et adaptées aux étapes du projet informatique • Les ressources humaines et matérielles nécessaires à ces interventions sont identifiées.
A8 **Sécurisation des projets informatiques** • Conception des éléments de sécurité du projet • Participation au développement du projet en prenant en charge les problématiques de sécurité • Correction des vulnérabilités informatiques du projet existant • Mise en place de tests de sécurité • Déploiement du projet informatique dans un environnement de production sécurisé.	**C10** **Implémenter les éléments ayant un impact sur la sécurité informatique du projet tout au long de son cycle de vie,** en concevant un système de droits et de privilèges, en organisant la gestion des vulnérabilités, en définissant et réalisant des tests de sécurité, en employant les technologies d'isolation et en organisant la mise en production, **afin de mettre en place et de maintenir un projet informatique de manière sécurisée.**	Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.	**C10** **Le candidat analyse l'intégration de la sécurité numérique dans le projet. Il vérifie et propose si nécessaire :** • L'identification des éléments critiques • Une méthode appropriée pour gérer les droits et privilèges • Un système de veille et de correctifs des vulnérabilités • L'utilisation de technologies d'isolation • La planification de tests de sécurité
A9 **Sécurisation des développements web** • Développement d'applications web sécurisées • Correction des vulnérabilités des applications web • Audit de sécurité d'applications web (pentest web) • Mise en place de solution de protection et de surveillance d'applications web.	**C11** **Prévenir et corriger les vulnérabilités des applications web**, en appliquant les standards spécifiques aux applications web, en respectant les bonnes pratiques de développement et en apportant les corrections, **afin de concevoir des applications web sécurisées et de pallier les failles des applications existantes.** **C12** **Contrôler la sécurité d'une application** en effectuant des audits de sécurité, en déployant des outils de protection et de surveillance, **afin de garantir un haut niveau de sécurité et d'en assurer la pérennité.**	**Mise en situation professionnelle (C11-C12)** Sous forme d'exercices pratiques, le candidat devra retrouver des failles de sécurité dans des applications qui lui sont soumises, exploiter ces vulnérabilités et ensuite sélectionner parmi plusieurs choix la solution appropriée. Pour valider, le candidat devra avoir résolu les deux tiers des épreuves.	**C11** **Le candidat :** • Préconise la solution optimale pour prévenir les vulnérabilités • Corrige un code vulnérable **C12** **Le candidat :** • Identifie les failles • Récupère des informations en exploitant les vulnérabilités identifiées • Reconnait la solution appropriée
A10 **Sécurisation des données** • Choix d'une solution cryptographique appropriée • Mise en place de systèmes de stockage et de communication chiffrés.	**C13** **Analyser les pratiques de chiffrements et de ségrégation des données** en identifiant les principaux algorithmes de cryptographie moderne, en distinguant leurs différents cas d'utilisation (disque, réseau, base de données), en interprétant un résultat d'étude cryptographique et en sélectionnant la granularité de	**Mise en situation professionnelle (C13-C14)** Sous la forme d'un projet pédagogique, le candidat devra choisir des solutions de cryptographie, sélectionner une méthode pour isoler les données et proposer un système de sauvegarde	**C13** **Le candidat :** • Choisit les algorithmes de cryptographie adaptés au besoin • Propose un modèle de ségrégation des données

• Vérification de l'existence d'un système de sauvegarde sécurisé.	données à chiffrer **afin de choisir et d'appliquer une solution pertinente pour sécuriser les données.** **C14** **Proposer une méthodologie adaptée pour la sauvegarde des données** en analysant les solutions existantes et en sélectionnant la solution adaptée aux données et au besoin de sécurité **afin d'assurer la résilience de l'entreprise.**	Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.	**C14** **La méthodologie de sauvegarde des données retenue par le candidat :** • Est adaptée au besoin de résilience de l'entreprise • Est adaptée au contexte de l'organisation.
A11 **Sécurisation des applications mobiles** • Sécurisation des données dans un téléphone. • Contrôle du respect des bonnes pratiques de sécurité dans les développements mobiles • Identification des vulnérabilités des développements mobiles	**C15** **Prévenir et corriger les vulnérabilités des applications mobiles**, en appliquant les standards spécifiques aux applications mobiles et à l'architecture de sécurité des téléphones, en reconnaissant les schémas classiques de vulnérabilités sur Android et iOS, en utilisant les systèmes de protections des données offerts par les systèmes mobiles, en respectant les bonnes pratiques de développement et en apportant les corrections adaptées, **afin de concevoir des applications mobiles sécurisées et de pallier les failles des applications existantes.**	**Mise en situation professionnelle (C15)** Sous la forme d'un projet pédagogique, le candidat identifie les processus de stockage des données et prévoit un plan de tests de sécurité Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.	**C15** **Le candidat :** • Préconise une solution pour sécuriser les données, adaptée aux besoins de l'application mobile en confidentialité et en intégrité • Etablit un plan de tests de sécurité : il choisit l'outil adapté et définit comment les tests doivent être conduits et quelles sont les attentes spécifiques pour l'analyse des vulnérabilités.

BLOC 3 : Identifier les risques et organiser la 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**
A12 **Mesure des enjeux de sécurité et des facteurs de risques associés** • Identification des différents types d'attaquants et de leurs motivations • Distinction entre les différents incidents de sécurité et leurs impacts • Identification des différents types de cyberattaques et de leurs conséquences • Considération du contexte géopolitique de la sécurité	**C16** **Identifier les enjeux cyber auxquels l'entreprise est confrontée**, en distinguant les différents types d'attaquants, en appréhendant la diversité des motivations, en identifiant les diverses sortes d'attaques et leurs conséquences et en reconnaissant les fragilités les plus courantes des systèmes d'information **pour inscrire la démarche de sécurité dans le contexte global.**	**Mise en situation professionnelle (C16-C20)** Sur la base d'un projet pédagogique, le candidat rédige les documents afférents à la politique de sécurité numérique d'une structure et destinés à l'ensemble des collaborateurs.	**C16** **Le candidat prévoit des documents de sensibilisation qui :** • Expliquent les problématiques de cybersécurité (les enjeux sont pris en compte de manière exhaustive et intègrent les menaces les plus actuelles) • Décrivent les conséquences prévisibles des incidents pour l'entreprise
A13 **Inscription de la sécurité numérique dans démarche de sécurité globale** • Prise en compte des enjeux de la SSI au sein des organisations d'un point de vue structurel • Prise en compte du facteur humain dans la sécurité • Inscription de la sécurité numérique dans la sécurité globale • Prise en compte des problématiques de développement durable	**C17** **Concevoir les principes de sécurité d'une organisation**, en appréhendant les enjeux de sécurité d'un point de vue structurel, en prenant en compte la place du facteur humain à côté du risque technique et en rédigeant un document de politique de sécurité numérique, **afin d'inscrire la sécurité numérique dans la démarche de sécurité globale de la structure.** **C18** **Intégrer les problématiques de développement durable dans la mise en place d'une démarche de sécurité globale**, en évaluant le coût énergétique des mesures envisagées et en identifiant les moyens de réduire la consommation énergétique de ces mesures **afin de limiter l'impact de ces mesures sur l'évolution du climat.**		**C17** **Le candidat rédige une politique de sécurité numérique :** • Intégrant les contraintes structurelles • Prenant en compte le facteur humain : il partage les bonnes pratiques de sécurité à destination de l'ensemble des collaborateurs • S'inscrivant dans la politique de sécurité globale de la structure **C18** **Le candidat intègre les problématiques de développement durable** • Le coût énergétique des mesures préconisées est évalué • Les moyens de limiter les coûts énergétiques des mesures sont identifiés
A14 **Application du droit de la cybersécurité** • Identification des règles de droit applicables en matière de sécurité numérique • Suivi des évolutions légales et des exigences de conformité • Communication avec des services juridiques.	**C19** **Réaliser une veille relative aux problématiques légales liées à la cybersécurité,** en identifiant les règles de droit applicables en matière de sécurité numérique, en différenciant les responsabilités civile et pénale et en suivant les évolutions légales et les exigences de conformité **afin d'échanger avec les services juridiques et de prendre des décisions qui respectent la règlementation en vigueur.**		**C19** **Les exigences légales et règlementaires :** • Sont inscrites dans les documents produits • La procédure de validation par les services juridiques est prévue • Un dispositif de veille et de mise à jour des documents est mis en place

A15 **Identification des acteurs de l'écosystème de la sécurité** • Identifications des structures étatiques et de leur rôle en cybersécurité. • Étude comparative des solutions proposées par les fournisseurs de solutions de sécurité	**C20** **Identifier les différents acteurs de l'écosystème de la cybersécurité étatiques ou industriels,** en comprenant les rôles respectifs des acteurs étatiques et en évaluant les solutions technologiques proposées par différents fournisseurs, **afin de solliciter les acteurs appropriés et de choisir les solutions de sécurité pertinentes et adaptées à la structure.**	Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.	**C20** **Les documents rédigés par le candidat** • Comprennent une liste exhaustive des acteurs de l'écosystème de la cybersécurité étatiques et industriels • Identifient les contacts à solliciter selon les situations et le niveau de menace.
A16 **Analyse et quantification des risques** • Utilisation des normes (ISO 27005, NIST8000) et méthodes (EBIOS, FAIR) de gestion de risques • Réalisation d'une analyse de risque dans le domaine de la cybersécurité • Interprétation des résultats d'une analyse de risque • Définition des objectifs de sécurité	**C21** **Classifier et mesurer les risques de sécurité liés à un système d'information complexe** en identifiant les menaces**,** en utilisant les normes (ISO 27005, NIST8000) et méthodes (EBIOS, FAIR) de gestion de risques **afin de réaliser une analyse de risque.** **C22** **Interpréter les résultats de l'analyse de risque** en intégrant les contraintes liées aux métiers de l'entreprise, en rapprochant la gestion des risques de la sécurité numérique de la gestion des autres risques de sécurité **afin de définir les objectifs de sécurité numérique de l'entreprise.**	**Mise en situation professionnelle (C21-C23)** Sur la base d'un projet pédagogique, le candidat réalise une analyse de risque sur des problématiques de cybersécurité, interprète les résultats de cette analyse et rédige un argumentaire pour faire adopter les solutions qu'il préconise.	**C21** **Le candidat fait une analyse de risque :** • Les menaces sur l'entreprise et son système d'information sont identifiées • La méthodologie retenue est appliquée **C22** **L'interprétation de l'analyse de risque :** • Intègre les contraintes liées aux métiers • Définit les objectifs de sécurité permettant d'atténuer les risques
A17 **Utilisation des techniques d'influence et de négociation pour la mise en œuvre interne de la politique de sécurité** • Utilisation des techniques de négociation au sein d'une entreprise. • Promotion de solution au sein d'une entreprise.	**C23** **Sensibiliser les décideurs de l'entreprise sur la nécessité de la mise en œuvre interne de la politique de sécurité,** en argumentant la pertinence des solutions retenues, en utilisant des techniques d'influence et de négociation et en interagissant avec des acteurs décisionnaires d'une entreprise, **afin de défendre ses solutions et ses préconisations auprès des décideurs et de les faire adhérer à la politique de sécurité.**	Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.	**C23** **Dans le document rédigé par le candidat :** • Les arguments avancés à côté de l'analyse de risque défendent la solution retenue. • Les techniques de négociation sont utilisées (face au jury d'évaluation)

BLOC 4 : Détecter les incidents de sécurité numérique et y répondre

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**

A18
Gestion d'une crise cyber
• Préparation à une crise :
  ○ Création d'une cellule de crise
  ○ Mise en place d'entraînements lors de simulations de crise
• Mise en place un dispositif de gestion de crise :
  ○ Activation de la cellule de crise
  ○ Coordinations des différents acteurs
  ○ Création d'un plan de réaction
  ○ Travail avec les assurances en cybersécurité
• Management de la remédiation après une compromission
  ○ Estimation des impacts techniques et financiers de la crise
  ○ Identification des correctifs à appliquer
• Organisation de la communication
  ○ Mise en place de canaux de communication interne
  ○ Information des tiers
	C24
	Préparer la structure à une crise cyber en créant une cellule de crise, en identifiant le rôle des différents acteurs lors d'une crise, en mettant en place des entraînements et en adaptant ces entrainements aux personnes en situation de handicap **pour être capable de réagir promptement et efficacement en cas de survenue de la crise.**
	
	C25
	Activer la cellule de crise, en assurant la coordination entre les acteurs techniques et décisionnaires de la structure, en contrôlant les relations entre les acteurs externes et internes en charge de résoudre le problème et en échangeant avec les assurances **afin de remédier à l'attaque et d'assurer une continuité de l'activité.**
	
	C26
	Piloter la mise en place du plan de continuité d'activité, en activant les solutions prévues en cas de crise, et en coordonnant les différents acteurs concernés, **afin d'assurer la résilience des applications et des données.**
	
	C27
	Gérer la sortie de crise en estimant les impacts techniques et financiers de l'attaque et en identifiant les correctifs à appliquer et les coûts associés (tout en préservant au maximum les opérations métiers de l'entreprise), **pour régénérer un environnement informatique sécurisé après la compromission**.
	
	C28
	Assurer la communication en interne et en externe lors d'une crise, en mettant en place des canaux spécifiques en interne, en informant les parties tierces concernées, en échangeant avec les autorités appropriées et en expliquant les conséquences aux clients et prestataires, tout en adaptant cette communication aux personnes en situation de handicap **afin de préserver la réputation de la structure, circonscrire les conséquences de la compromission et augmenter l'efficacité de la remédiation.**
		Mise en situation professionnelle (C24-C27)
		Sur la base d'un projet pédagogique de simulation de crise cyber, le candidat réunit la cellule de crise et en supervise le fonctionnement du début de la crise jusqu'à la reprise complète d'activité.
		
		Ce travail fait l'objet d'un rendu écrit et d'une soutenance orale devant le jury d'évaluation.
			C24
			En amont de l'exercice, le candidat doit avoir :
			• Listé les membres qui participeront à la cellule de crise, ainsi que mis en place une procédure pour les contacter de façon certaine
			• Planifié des entrainements
			• Prévu des mesures adaptées pour que des personnes en situation de handicap puissent participer aux entrainements
			
			C25
			Durant l'exercice de crise, le candidat, après avoir activé la cellule, doit :
			• Coordonner les acteurs techniques et décisionnaires : il s'assure de la cohérence entre les décisions et les actions réalisées par les parties prenantes
			• Coordonner les acteurs internes et externes : il répartit les tâches et s'assure de la cohérence des actions réalisées par les parties prenantes
			• Solliciter les assurances : il communique les informations utiles à leur intervention
			
			C26
			Durant l'exercice de crise, le candidat doit :
			• Mettre en place le plan de réaction : il sollicite les acteurs concernés au moment opportun
			• Vérifier le bon déploiement du plan par les acteurs : il constate les avancements et apporte une aide technique
			
			C27
			En sortie de crise, le candidat doit :
			• Estimer les impacts techniques et financiers
			• Identifier les correctifs à appliquer
			
			C28
			Tout au long de l'exercice le candidat s'assure de la maitrise de la communication :
			• En activant des canaux spécifiques en interne : les collaborateurs concernés sont informés de la situation
			• En informant les tiers (clients, fournisseurs, journalistes) : chaque acteur reçoit le niveau d'information adapté
			• En prenant en compte les situations de handicap dans la mise en place de ces mesures

<table>
<tr>
<td>A19
Collecte et analyse forensiques
Collecte et analyse des journaux d’évènements
Utilisation d’un système de management des informations de sécurité (SIEM).
Déploiement d’agents de collecte d’information sur les systèmes
Détection des comportements anormaux dans un système.
Création d’un système d’alertes de sécurité automatisé</td>
<td>C29
Rassembler les données nécessaires à une analyse forensique, en collectant les journaux d’évènements, en utilisant un système de management des informations de sécurité (SIEM), en interfaçant différents équipements réseau au sein du SIEM et en déployant des agents de collecte d’information, afin de réunir les éléments nécessaires pour identifier un attaquant.

C30
Analyser les données collectées en détectant les comportements anormaux, en réalisant une levée de doute et en créant des systèmes d’alertes automatisés afin de détecter les compromissions.</td>
<td rowspan="2">Mise en situation professionnelle (C28-C31)
Sur la base d’un projet pédagogique de simulation de crise cyber, le candidat réalise une collecte et une analyse forensique pour détecter un incident. Il procède ensuite à une analyse technique de l’attaque détectée pour choisir la réponse adaptée.

Ce travail fait l’objet d’un rendu écrit et d’une soutenance orale devant le jury d’évaluation.</td>
<td rowspan="2">C29
Le candidat collecte les éléments nécessaires à l’analyse forensique :
Les informations pertinentes sont récupérées
Les informations sont rassemblées et ordonnées
C30
Le candidat analyse les données collectées :
La levée de doute est effectuée
Les traces laissées par l’attaquant sont isolées
C31
Le candidat analyse l’incident dans sa globalité :
Les techniques de l’attaquant sont identifiées
L’historique de la compromission est établi
L’origine de l’intrusion est retrouvée
Des réponses sont proposées</td>
</tr>
<tr>
<td>A20
Réponse aux intrusions et autres incidents
Identification des différents types d’outils informatiques utilisés par l’attaquant
Détection des actions réalisées par l’attaquant lors d’une compromission
Investigation pour déterminer l’origine de l’intrusion</td>
<td>C31
Analyser une attaque informatique, en utilisant les informations forensiques collectées, en identifiant les différents types de virus informatique et leurs comportements, en réalisant une investigation numérique pour remonter à l’origine de l’intrusion, en observant le comportement de l’attaquant et en interprétant ces résultats avec les outils de renseignement de menace (threat intelligence), pour établir un faisceau de preuves et choisir une réponse stratégique appropriée.</td>
</tr>
</table>

L'obtention de la certification est conditionnée par la validation des 4 blocs de compétences, ainsi que par la validation de la rédaction et de la soutenance finale du mémoire professionnel devant un jury de validation.