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 : Traiter les incidents de cybersécurité			
A1.1. Diagnostic de l'incident de cybersécurité et de son ampleur - Recherche des informations liées à l'incident : traces informatiques, journaux d'évènements (log)… - Utilisation des outils de modélisation et/ou de visualisation - Apport d'une remédiation aux incidents de cybersécurité - Assurance de	**C1.1. Coordonner la collecte de l'ensemble des informations relatives aux incidents informatiques** (journaux d'évènements systèmes et réseau, diagrammes de topologie réseau, images systèmes) en utilisant des outils open-source (autopsy, foremost, scalpel, volatility, plaso, log2timeline, etc.) souvent présents sur la distribution Kali Linux afin d'avoir une première idée sur l'ampleur de la crise	• **Cas d'études** Sont fournis aux candidats des journaux d'événements à l'aide desquels ils doivent réunir les traces informatiques liées à l'incident. Le candidat doit trier les journaux d'évènements pour identifier les traces pertinentes. Il est attendu des candidats la rédaction d'un plan de remédiation. Ils doivent proposer des solutions de sécurité en analysant les	- Les traces numériques sont trouvées : la documentation de tous les journaux d'événements et des diagrammes de topologie est complète, les images systèmes sont correctement utilisées avec les outils appropriés, les outils open-source sont correctement appliqués pour recueillir des preuves initiales. - Le scenario est reconstitué sur une ligne de temps. - La ligne de temps des évènements de l'incident est élaborée. - Les traces sont de nature à déterminer un diagnostic complet.

l'assainissement et du durcissement des systèmes attaqués	**C1.2. Trier les éléments liés à l'incident,** en définissant des catégories et en les classant, afin d'organiser des éléments de preuves analysables	solutions existantes sur le marché.	- Les éléments collectés sont triés, catégorisés et priorisés. - Les catégories de tri sont logiquement définies et appliquées de manière cohérente. - Les éléments de preuve sont classés de façon à faciliter leur analyse ultérieure.
A1.2. Analyse de l'incident de cybersécurité - Contextualisation de l'incident - Modélisation et visualisation de l'incident - Établissement des scenarii potentiels d'incident	**C1.3. Analyser les preuves numériques collectées,** en appliquant la méthodologie forensique, à l'aide de la collecte de données brutes ou altérées, en identifiant la nature de l'incident et en reconstituant le déroulement de l'attaque, afin lancer une action interne ou une procédure judiciaire		- La méthodologie forensique est appliquée. - Les outils d'analyse forensique sont maîtrisés - Plusieurs hypothèses de cause de l'indicent sont émises à partir des traces. - L'analyse révèle clairement la nature et le déroulement de l'incident. - Les conclusions tirées sont étayées par des données brutes ou altérées collectées.
	C1.4. Contextualiser l'incident, en établissant une corrélation entre signe d'incident et l'analyse de traces informatiques (informations collectées) à l'aide d'outils de modélisation et/ou de visualisation, afin d'établir des scenarii		- Les traces non significatives sont éliminées. - Les traces pertinentes sont exploitées et contextualisées. - Les outils de modélisation et/ou de visualisation sont maîtrisés. Ils sont

	potentiels d'incident		utilisés pour clarifier le contexte de l'incident. - Les scénarios d'incident proposés sont plausibles et bien soutenus par les preuves analysées
A1.3. Remédiation à l'incident de cybersécurité - Élaboration de recommandations - Organisation de la sensibilisation des collaborateurs	**C1.5. Élaborer un plan de remédiation,** en appliquant les actions de résolution de l'incident dans le respect de la politique de sécurité des systèmes d'information (PSSI), et en définissant des recommandations aux collaborateurs, afin de répondre à la crise cyber		- Les actions sont priorisées. Les recommandations sécuritaires sont écrites en un plan de remédiation et présentées à l'oral aux équipes. - Les solutions de sécurité sont proposées en analysant les solutions existantes sur le marché. - Les contraintes tarifaires et techniques sont prises en compte dans les recommandations. - Les recommandations sont argumentées, les actions de résolution sont pratiques, réalisables et alignées avec les politiques de sécurité.
A1.4. Participation à l'élaboration de la PSSI - Coordination avec le RSSI et/ou DSI - Collaboration avec la Computer Emergency Response Team (CERT)	**C1.6. Organiser la sensibilisation des collaborateurs aux bonnes pratiques en matière de cybersécurité**, en expliquant les vulnérabilités, en présentant les derniers correctifs de sécurité et en mettant en place des cas pratiques portant sur les plans de réponse aux		- Le candidat facilite l'appropriation des pratiques de sécurité par tous les collaborateurs. - Les sessions de sensibilisation incluent des explications claires sur les vulnérabilités et les correctifs, - Les cas pratiques sont pertinents et

	incidents, en prenant les dispositions permettant l'appropriation des informations par tous les publics, y compris en situation de handicap, afin de minimiser les risques et les dommages en cas d'attaques cybernétiques		inclusifs, prenant en compte des dispositions pour les publics en situation de handicap.
	C1.7. Enrichir la politique de sécurité (PSSI) et les documents associés, en coordination avec le RSSI et/ou DSI, en utilisant les méthodologies d'analyse de risques (Méhari, EBIOS) ainsi que la norme ISO 27001, en spécifiant les exigences relatives aux systèmes de management de la sécurité des informations (SMSI) etc., afin d'améliorer la sécurité et la résilience du SI		- La PSSI reflète la stratégique de la direction de la structure. - La liste de documents de références de la SSI (critères d'évaluation, textes législatifs, normes, codes d'éthiques, notes complémentaires…) est complétée. - Le candidat émet des recommandations pour la construction des règles de sécurité. - L'utilisation des méthodologies d'analyse de risques et de la norme ISO 27001 est correctement documentée, - Les mises à jour apportées à la politique sont pertinentes, améliorant la sécurité et la résilience du SI.
	C1.8. Définir des actions d'amélioration continue des pratiques, en coopérant avec des experts à l'aide des outils de		- La plateforme de partage est mise en place et animée. - Le candidat enrichi les bases de

	réponse à incident spécifiques (CERT, plateforme de partage, virus total) dans le but de partager les failles, les vulnérabilités, les indices de compromission, et d'éviter que d'autres structures ne soient affectées par les mêmes menaces		partage et capitalise les informations qui en ressortent. - L'échange d'informations sur les failles et vulnérabilités avec des plateformes extérieures est efficace, - Les actions proposées pour éviter la récurrence des incidents sont pratiques et clairement formulées.

FRANCE compétences

Intitulé : Expert en Cybersécurité (MS)
Université de Technologie de Troyes (UTT)

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 2 : Analyser la menace cyber pesant sur une organisation			
A2.1. Détection des incidents et des menaces - Supervision des infrastructures et des événements de sécurité - Qualification de la nature des incidents et des menaces - Identification des sources - Blocage de l'accès au système informatique	**C2.1. Assurer la supervision des infrastructures et des événements de sécurité**, en exploitant un système de gestion de l'information et des événements de sécurité (SIEM), en utilisant ces informations pour retracer la chronologie d'une cyberattaque, afin de mettre en évidence les signaux faibles qui d'ordinaire passent inaperçus et d'éviter que ces mêmes attaques ne se reproduisent dans le futur	• **Cas pratique** D'après des journaux d'évènements donnés, les candidats doivent détecter les incidents et les menaces afin de les bloquer. Il est attendu que les codes malveillants soient analysés et qualifiés. Les candidats doivent proposer des correctifs.	- La configuration et l'utilisation du SIEM sont optimales pour la détection des signaux faibles - Les journaux d'évènements sont exploités. La chronologie des événements d'une cyberattaque est clairement retracée et documentée. - Un tableau de bord qui présente l'évènement est élaboré et présenté. - Les signaux faibles identifiés sont correctement analysés pour prévenir les récidives.
	C2.2. Détecter en temps réel les incidents de sécurité et les menaces, en identifiant leurs sources et en configurant l'architecture réseau et les systèmes de sécurité, afin de prévenir l'accès non autorisé et de bloquer les tentatives d'intrusion dans le système informatique de l'organisation		- L'incident est détecté. La source de l'incident est identifiée et correctement documentée. - L'architecture réseau et les systèmes de sécurité sont configurés pour bloquer l'accès de la menace identifiée au système.

A2.2. Analyse et catégorisation des codes malveillants - Analyse statique et/ou dynamique (sandbox) - Développement et déploiement d'algorithmes d'IA	**C2.3. Analyser le code malveillant** en employant des techniques d'analyse statique et dynamique, en examinant le comportement du code et en identifiant les signatures et les vecteurs d'attaque potentiels, afin de qualifier et de catégoriser précisément les menaces		- Le code malveillant identifié est analysé dans le respect des méthodes d'analyse statique et/ou dynamique. - Le code est qualifié et catégorisé. - Les signatures et vecteurs d'attaque sont précisément identifiés et catégorisés.
	C2.4. Exploiter l'intelligence artificielle générative, en développant et en déployant des algorithmes d'IA, en simulant des attaques et en analysant des patterns de menaces émergentes, afin d'améliorer continuellement la prévention, la détection et la réaction face aux cyberattaques		- Le candidat développe et déploie efficacement des algorithmes d'IA pour la cybersécurité. - Les algorithmes d'IA générative sont correctement conçus pour simuler des attaques et analyser les menaces, - L'utilisation de l'IA contribue à une amélioration notable de la prévention, la détection et la réponse aux cyberattaques.

A2.3. Remédiation aux menaces - Orientation des équipes techniques quant aux correctifs ou palliatifs à mettre en œuvre - Proposition de programmes - Partage de l'information aux CERT - Conduite d'une investigation en suivant le cycle du renseignement (expression des besoins, collecte, traitement, analyse, diffusion) et en modélisant l'intrusion afin de l'attribuer si possible - Etude du mode opératoire et de la psychologie de l'attaquant - Attribution d'incident	**C2.5. Développer un correctif de sécurité en utilisant la distribution Kali Linux**, en programmant avec le langage Python, en créant des scripts Bash sous Linux, et en écrivant des exécutables en C++, afin de fournir aux équipes les outils nécessaires pour répondre efficacement aux incidents de sécurité.		- Les actions correctives à mettre en œuvre sont identifiée. - Des programmes de remédiation sont codés. - Les correctifs sont bien codés en Python, Bash sous Linux, et C++ et testés pour leur efficacité, - Les outils développés sont adaptés aux besoins spécifiques des équipes pour répondre aux incidents. - Les codes malveillants et solutions de remédiation sont partagées aux CERT.
	C2.6. Attribuer l'incident en établissant une grille d'analyse d'intrusion, en utilisant des méthodes adéquates telles que la Kill Chain, le Diamond Model et la matrice MITRE ATT&CK, afin de modéliser avec précision les intrusions ciblées	• **Test écrit** Evaluation des connaissances visant à évaluer la bonne assimilation des termes et des définitions. • **Cas pratique** D'après un article de blog à modéliser grâce à la matrice MITRE ATT&CK, en Cyber Kill Chain et en Intrusion Diamond Model, le candidat doit rédiger un rapport d'investigation. L'évaluation est orale par les pairs.	- Le candidat est évalué sur l'exactitude des termes employés (weaponisation, Kill Chain…). Le candidat traduit par une modélisation correcte l'article. - Les méthodes telles que la Kill Chain, Diamond Model, et MITRE ATT&CK sont correctement utilisées, - Les modèles d'intrusion sont clairement définis et alignés avec les incidents analysés. - Le rapport d'investigation est de

			qualité et exact.
A2.4. Veille permanente sur les menaces émergentes - Configuration des outils de veille en utilisant le renseignement en sources ouvertes - Entretien des échanges avec les experts internationaux - Production des documents d'analyse pour enrichir les plateformes de partage	**C2.7. Anticiper les futures évolutions des menaces** en mettant en place un système de veille recensant le renseignement en source ouverte (OSINT), les flux de données commerciaux et communautaires, les médias sociaux (SOCMINT), le renseignement d'origine humaine et la capacité d'analyse et de corrélation (HUMINT), les informations provenant du Deep et Dark web, afin de limiter l'exposition de l'entreprise sur les réseaux sociaux, ou sur les moteurs de recherche, limitant ainsi la surface d'attaque que pourrait exploiter un hacker	• **Cas pratique** Les candidats doivent programmer un outil de veille (scrapper) sur les menaces identifiées.	- Les sources sont sélectionnées. La collecte d'informations à partir d'OSINT, SOCMINT, HUMINT, et le Deep et Dark Web est bien intégrée. - Les flux de données sont agrégés. - Les analyses et corrélation des données recueillies sont utilisées pour limiter proactivement la surface d'attaque de l'entreprise. - L'outil de veille permet la visualisation des résultats.

FRANCE compétences

Intitulé : Expert en Cybersécurité (MS)
Université de Technologie de Troyes (UTT)

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 3 : Auditer la sécurité technique d'une organisation			
A3.1. Préparation de l'audit de sécurité - Analyse du périmètre d'intervention (cartographie des infrastructures - SI) - Identification des vulnérabilités - Animation d'une réunion de cadrage	**C3.1. Analyser le périmètre d'intervention pour les tests d'intrusion**, en définissant les modalités et les outils spécifiques à utiliser, notamment nmap, metasploit et armitage de la distribution Kali Linux, afin de réaliser des tests cadrés et précis qui permettent d'identifier les vulnérabilités potentielles dans les systèmes de l'organisation	• **Cas d'étude** D'après un cas d'étude donnée par le formateur, les candidats doivent réaliser une étude de vulnérabilité visant à définir le périmètre des tests d'intrusion.	- Le périmètre d'intervention est cartographié de façon précise, avec une identification claire des systèmes, réseaux ou applications cibles. - Les choix d'outils de distribution sont pertinents et correctement justifiés. - L'étude de vulnérabilité récence l'ensemble des failles.
	C3.2 Animer une réunion de cadrage de la phase d'audit de sécurité, en réunissant les représentants des fonctions de gestion de l'information, de la technologie, et de la conformité, en les sensibilisant sur les objectifs de l'audit, les approches méthodologiques, la planification et les responsabilités partagées, et en identifiant les besoins d'adaptation du dispositif pour les personnes en situation de handicap, pour assurer une exécution cohérente et		- Le candidat facilite efficacement la communication des objectifs et des responsabilités. - L'information sur les objectifs de l'audit et les méthodologies est clairement formalisée. - Les besoins spécifiques d'adaptation pour les personnes en situation de handicap sont clairement identifiés et pris en compte dans la planification. - Les responsabilités de chaque

	complète de l'audit de sécurité		fonction sont explicitées.
A3.2. Réalisation des tests d'intrusion sur les systèmes, les réseaux, les applications web ou mobiles - Utilisation des méthodologies de rétro-ingénierie - Prise en compte des aspects légaux permettant les tests d'intrusion - Identification des vulnérabilités les plus répandues - Application des méthodologies de tests d'intrusion - Utilisation des outils essentiels à la réalisation de tests d'intrusion - Le cas échéant, création d'outils de tests - Validation de l'application des scénarios - Facilitation des échanges entre les parties prenantes	**C3.3. Réaliser des tests d'intrusion** sur les systèmes, les réseaux, les applications web ou mobiles, en utilisant les outils adéquats selon la méthodologie de tests d'intrusion, tout en assurant une veille technique sur les outils d'audit et les pratiques d'attaque et tests d'intrusion dans le respect du Code pénal spécifique à la cybercriminalité, afin d'identifier les services vulnérables et de détecter les éventuelles menaces ou intrusions	• **Cas pratique** Le candidat doit identifier l'ensemble des vulnérabilités dans un serveur. Sont attendus un rapport des résultats et une proposition de correctifs à mettre en place.	- Le plan d'audit et les scenarii sont élaborés. - Les méthodologies d'audit sont respectées. - Les services et les versions qui tournent sur le serveur sont recensés. - Les services et les versions sont identifiés sur les référentiels de vulnérabilité. - Les vulnérabilités sont identifiées, avec documentation des sources de menaces identifiées. - Le respect du Code pénal en matière de cybercriminalité est évident dans toutes les procédures.
	C3.4 Superviser l'application de l'ensemble des protocoles de test, en configurant des environnements de simulation sécurisés pour les tests et en validant l'application des scénarios de test selon les spécifications définies, tout en facilitant un échange régulier d'informations entre les membres de l'équipe technique pour assurer la		- Le candidat assure une supervision rigoureuse des protocoles de test dans un environnement de simulation sécurisé. - Les environnements de simulation sont correctement configurés et sécurisés. - Les scénarios de test sont appliqués selon les spécifications définies sans

	transparence et l'efficacité durant les phases de test.		déviations. - La supervision garantit l'exactitude technique des tests et la non-altération des environnements de production.
A3.3. Rédaction du rapport de résultat de l'audit de sécurité - Rédaction du plan de remédiation - Emission de propositions de remédiation - Présentation des résultats de l'audit - Collaboration avec les équipes pour mettre en œuvre les recommandations	**C3.5. Élaborer un rapport détaillé** des résultats des tests comprenant des captures d'écran des tests et systématiquement, comporter une note explicitant, pour chaque faille ou vulnérabilité découverte, la contre mesure à mettre en place, afin d'éradiquer ou de limiter le risque voire de proposer un plan de remédiation.		- Le rapport des résultats de l'audit est rédigé et détaillé, il inclut des captures d'écran des tests effectués, démontrant clairement les vulnérabilités découvertes. - Les vulnérabilités identifiées sont exploitées et neutralisées. Chaque faille identifiée est accompagnée d'une note détaillée expliquant les contre-mesures ou les recommandations de remédiation. - Le plan de remédiation est élaboré et contient un ensemble de propositions. Les recommandations sont pratiques, réalisables et alignées avec les besoins spécifiques de l'organisation pour limiter ou éradiquer les risques.
	C3.6. Présenter les résultats de l'audit lors d'une session de restitution aux décideurs et aux équipes techniques, en utilisant des outils de visualisations de données pour illustrer les vulnérabilités et		- Le candidat présente clairement les résultats de l'audit aux décideurs et équipes techniques. - Les visualisations de données utilisées illustrent efficacement les

	les impacts potentiels, et en proposant des recommandations claires pour les actions de remédiation, afin de faciliter la prise de décision et la planification des suivis nécessaires.		vulnérabilités et leurs impacts potentiels. - Les recommandations pour les actions de remédiation sont claires, précises, et applicables. - La présentation est adaptée aux éventuels besoins d'adaptation et d'inclusion de l'auditoire. - Le contenu facilite la compréhension et la prise de décision par les décideurs, avec un plan de suivi bien défini pour les actions recommandées.

FRANCE compétences

Intitulé : Expert en Cybersécurité (MS)
Université de Technologie de Troyes (UTT)

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 4 : Réaliser une analyse technico-légale (forensique)			
A4.1. Préparation et collecte des données forensiques - Identification des preuves numériques - Détermination du périmètre technique d'analyse - Définition de la stratégie de préservation des données numériques - Organisation de la traçabilité des preuves numériques - Recensement des actions de préservation à effectuer - Collecte des preuves numériques selon la procédure technico-légale	**C4.1. Identifier le périmètre et l'environnement technique**, en accédant si nécessaire au système d'exploitation ou au matériel pour avoir une vision précise de la volumétrie des données, et en définissant les exigences techniques et opérationnelles de la démarche avec les responsables IT et de projet concernés, afin d'évaluer la quantité de données à acquérir, conformément à la PSSI.	• **Cas d'études** Des cas d'études sont proposés aux étudiants. Ces cas sont fournis sous forme de scénarii comportant des copies de disques durs, des copies de smartphones. Il est demandé à l'étudiant de réaliser une analyse technico-légale des supports fournis à l'aide d'outils dédiés. Il est demandé une restitution écrite relatant le scénario, son analyse ainsi que la présentation synthétique des résultats.	- Le périmètre technique à analyser est identifié précisément. - L'accès et l'identification du système d'exploitation ou du matériel sont réalisés de manière exhaustive. - La détermination de la volumétrie des données est précise et justifie clairement la quantité de données à acquérir.
	C4.2. Définir la stratégie de préservation des données, en considérant la volumétrie des données à analyser, le temps dont on dispose, le matériel de copie dont on dispose, et d'autres contraintes externes, et en s'assurant de la conformité aux normes légales auprès des équipes juridiques, afin de rédiger le document de traçabilité des actions effectuées.		- Le document de traçabilité est rédigé et liste les actions à mettre en œuvre. La stratégie prend en compte la volumétrie des données, le temps disponible, le matériel de copie, et les contraintes externes. - La méthode employée est expliquée et argumentée. - Des inférences et hypothèses sont émises.

	C4.3. Réaliser la collecte de données de manière technico-légale, en utilisant des outils dédiés pour l'extraction des données sur des supports comme les clés USB ou pour la création de copies technico-légales avec des outils open source (tels que dd, dcfldd) et commerciaux (comme FTK Imager), disponibles sur la distribution Kali Linux, et en assurant le respect des politiques internes, de l'éthique et des cadres légaux en lien avec les équipes de sécurité informatique, afin de préserver les preuves numériques dans un contexte d'investigation légale	- L'outil de collecte approprié pour l'extraction et la copie des données est défini. - Les données sont collectées. - La procédure technico-légale est respectée. Les copies technico-légales préservent l'intégrité et la recevabilité des preuves dans un contexte légal.
A4.4. Analyse et rédaction du rapport des preuves numériques - Traitement et analyse des preuves numériques collectées - Rédaction du rapport d'analyse - Communication adaptée aux autorités compétentes (forces de l'ordre, magistrat, équipe de réponse à incident)	**C4.4. Analyser les artefacts numériques identifiés**, tels que disques durs, mémoires, traces réseau, journaux d'événements, emails, navigateurs, et smartphones, en employant des techniques et des logiciels d'analyse forensique avancés, afin de tracer et documenter les preuves numériques pour les besoins d'enquêtes et de conformité légale	- Les artefacts pertinents sont identifiés. La documentation des preuves numériques est exhaustive et soutient les besoins d'enquêtes et de conformité légale. - Les techniques et logiciels d'analyse forensique sont utilisés de manière compétente pour traiter divers types d'artefacts. - La méthodologie et l'organisation de l'analyse est détaillée. La traçabilité est rédigée.

	C4.5. Rédiger un rapport d'analyse forensique, en mettant en avant les implications légales, les recommandations de sécurité et les conclusions techniques essentielles, et en adaptant le discours aux publics techniques et institutionnels (forces de l'ordre, magistrat, équipe de réponse à incidents), et en prenant les dispositions permettant l'accès des informations à tous, y compris en cas de handicap, afin de fournir une communication claire et complète des résultats d'investigation aux parties prenantes concernées		- Le rapport d'analyse est précis et argumenté, il met en évidence les implications légales, les recommandations de sécurité, et les conclusions techniques. - Le rapport d'analyse est fiable et de nature à être présenté aux forces de l'ordre, à un magistrat, ou une équipe de réponse à incident. Le discours est adapté aux différents publics techniques et institutionnels, et prend en compte l'accessibilité pour les personnes en situation de handicap. - Le rapport met en évidence les implications légales, les recommandations de sécurité, et les conclusions techniques. Le scénario issu de l'analyse est adapté.

Chaque bloc de compétences est validé de façon autonome. L'acquisition du bloc fait l'objet de remise d'un certificat.
Les compétences qui composent les blocs sont évaluées de manière indépendante les unes aux autres.
Le titre est obtenu si l'ensemble des blocs est obtenu, ainsi qu'en cas de validation des évaluations finales transverses : la mission en entreprise, la rédaction et la soutenance de la thèse professionnelle.

Mission en entreprise :
Période de formation en milieu professionnel d'une durée minimale de quatre mois équivalent temps plein durant laquelle l'étudiant réalise les missions et les tâches qui lui sont confiées.

Thèse professionnelle : Rédaction d'un mémoire de thèse puis, lors d'une soutenance orale, présentation des données, de la problématique, de l'état de l'art réalisé, des choix méthodologiques et des résultats obtenus. Cette présentation est suivie d'une discussion et d'interaction avec les membres du jury.