5 – RÉFÉRENTIELS

Université de Technologie de Troyes (UTT)

Intitulé de la certification : Expert en Cybersécurité (MS)

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 l'assainissement et du	**C1.1. Collecter l'ensemble des informations relatives aux incidents informatiques** (journaux d'évènements systèmes et réseau, diagrammes de topologie réseau, images systèmes) à l'aide d'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'évènements 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.	Les traces numériques sont trouvées. 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.

durcissement des systèmes attaqués **A1.2. Analyse de l'incident de cybersécurité** - Contextualisation de l'incident - Modélisation et visualisation de l'incident - Établissement des scenarii potentiels d'incident	**C1.2. Trier les éléments liés à l'incident** en les catégorisant afin d'organiser des éléments de preuves analysables	Il est attendu des candidats la rédaction d'un plan de remédiation. Ils doivent proposer des solutions de sécurité en analysant les solutions existantes sur le marché.	Les éléments collectés sont triés et catégorisés. Les éléments collectés sont priorisés.
	C1.3. Analyser les preuves numériques collectées selon la méthodologie forensique, à l'aide de la collecte de données brutes ou altérées permettant d'identifier la nature de l'incident et de reconstituer 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 maitrisés. Plusieurs hypothèses de cause de l'indicent sont émises à partir des traces.
	C1.4. Contextualiser l'incident en faisant la 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 potentiels d'incident		Les traces non significatives sont éliminées. Les traces pertinentes sont exploitées et contextualisées. Les outils de modélisation et/ou de visualisation sont maitrisés. Le bon scenario est déterminé.

A1.3. Remédiation à l'incident de cybersécurité - Elaboration de recommandations	**C1.5. Elaborer un plan de remédiation** afin d'appliquer les actions nécessaires à la résolution de l'incident telles que décrites dans la politique de sécurité des systèmes d'information (PSSI) en émettant notamment 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.
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. Enrichir la politique de sécurité (PSSI)** et des documents associés avec le RSSI et/ou DSI en utilisant les méthodologies d'analyse de risques telles que Méhari ou EBIOS, ainsi que la norme ISO 27001, 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.
	C1.7. Améliorer de façon continue ses pratiques en coopérant avec des experts à l'aide des outils 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 éviter que d'autres structures ne soient affectées par les mêmes menaces.		La plateforme de partage est mise en place et animée. Le candidat enrichi les bases de partage et capitalise les informations qui en ressortent.
Bloc de compétences capitalisable, obligatoire pour l'obtention du titre (validité du bloc illimitée). L'acquisition du bloc fait l'objet de remise d'un certificat. Le cas échéant, description de tout autre document constitutif de la certification professionnelle. La thèse professionnelle, modalité d'évaluation globale et transversale, doit être validée au même titre que les 4 blocs de compétences pour obtenir la certification.			

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. Supervision des infrastructures et des événements de sécurité - Exploitation du Centre d'Opérations et de Sécurité (SOC)	**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.	Le SIEM est configuré. Les journaux d'évènements sont exploités. Un tableau de bord qui présente l'évènement est élaboré et présenté.
A2.2. Détection des incidents et les menaces - Qualification de la nature des incidents et des menaces - Identification des sources - Blocage de l'accès au système informatique	**C2.2. Détecter en temps réel les incidents et les menaces** en identifiant leurs sources afin de bloquer leur accès au système informatique		L'incident est détecté. La source de l'incident est identifiée. L'architecture est configurée pour bloquer l'accès de la menace identifiée au système.
A2.3. Analyse et catégorisation des codes malveillants - Analyse statique et/ou dynamique (sandbox)	**C2.3. Analyser le code malveillant par les techniques d'analyse** statique et/ou dynamique pour le qualifier et le catégoriser		Le code malveillant identifié est analysé dans le respect des méthodes d'analyse statique et/ou dynamique.

			Le code est qualifié et catégorisé.
A2.4. 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	**C2.4. Produire un correctif** à l'aide de la distribution Kali Linux (langage python, script bash sous linux, exécutable écrit en C++.) qui sera appliqué par les équipes afin de produire une réponse à l'incident.		Les actions correctives à mettre en œuvre sont identifiée. Des programmes de remédiation sont codés. Les codes malveillants et solutions de remédiation sont partagées aux CERT.
	C2.5. Attribuer l'incident en établissant une grille d'analyse d'intrusion en utilisant les méthodes adéquates telles que : • Kill Chain • Diamond Model • La matrice MITRE ATT&CK Afin de modéliser une intrusion ciblée	**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. Le rapport d'investigation est de qualité et exact.

A2.5. 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	**C2.6. Anticiper les futures évolutions des menaces** à l'aide de la mise en place d'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. Les flux de données sont agrégés. L'outil de veille permet la visualisation des résultats.
Bloc de compétences capitalisable, obligatoire pour l'obtention du titre (validité du bloc illimitée). L'acquisition du bloc fait l'objet de remise d'un certificat. Le cas échéant, description de tout autre document constitutif de la certification professionnelle. La thèse professionnelle, modalité d'évaluation globale et transversale, doit être validée au même titre que les 4 blocs de compétences pour obtenir la certification.			

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	**C3.1. Analyser le périmètre d'intervention** des tests d'intrusion (après avoir défini le périmètre d'intervention, et la modalité des tests à utiliser, les outils de la distribution Kali Linux seront utilisés, tels que nmap, metasploit et armitage) afin de lancer des tests cadrés.	**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. L'étude de vulnérabilité récence l'ensemble des failles.
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	**C3.2. 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 (définition du plan d'audit, des scenarii, etc.), 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, les articles 323-1 et suivants notamment, 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.

réalisation de tests d'intrusion - Le cas échéant, création d'outils de tests			
A3.3. Rédaction du rapport de résultat de l'audit de sécurité - Rédaction du plan de remédiation - Emission de propositions de remédiation - Collaboration avec les équipes pour mettre en œuvre les recommandations	**C3.3. 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. Les vulnérabilités identifiées sont exploitées et neutralisées. Le plan de remédiation est élaboré et contient un ensemble de propositions.
Bloc de compétences capitalisable, obligatoire pour l'obtention du titre (validité du bloc illimitée). L'acquisition du bloc fait l'objet de remise d'un certificat. Le cas échéant, description de tout autre document constitutif de la certification professionnelle. La thèse professionnelle, modalité d'évaluation globale et transversale, doit être validée au même titre que les 4 blocs de compétences pour obtenir la certification.			

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. Identification des preuves numériques - Détermination du périmètre technique d'analyse	**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 afin d'évaluer la quantité de données à acquérir.	**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.
A4.2. Définition de la stratégie de préservation des données numériques - Organisation de la traçabilité des preuves numériques - Recensement des actions de préservation à effectuer	**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, 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 méthode employée est expliquée et argumentée. Des inférences et hypothèses sont émises.
A4.3. Collecte des preuves numériques selon la procédure technico-légale - Utilisation des outils de collecte technico-légale	**C4.3. Réaliser la collecte de façon technico-légale** à l'aide d'outils de collecte dédiés soit en extrayant les données sur un support de type clé USB, ou bien, soit en réalisant une copie technico-légale avec des outils open source, tels que dd, dcfldd, présents sur la distribution Kali Linux, ou bien des outils commerciaux comme ftk imager), afin de préserver les preuves numériques.		L'outil de collecte approprié est défini. Les données sont collectées. La procédure technico-légale est respectée.

A4.4. Traitement et analyse des preuves numériques collectées	**C4.4. Analyser des artefacts identifiés** (disque dur, mémoire, traces réseaux, journaux d'évènements, e-mail, navigateurs, smartphones …) afin de tracer les preuves numériques		Les artefacts pertinents sont identifiés. Les outils d'analyse sont maitrisés. La méthodologie et l'organisation de l'analyse est détaillée. La traçabilité est rédigée.
A4.5. Production des preuves numériques analysées - Rédaction du rapport d'analyse - Communication adaptée aux autorités compétentes (forces de l'ordre, magistrat, équipe de réponse à incident)	**C4.5. Rédiger un rapport d'analyse** en adaptant son discours afin de le présenter à divers publics, techniques et institutionnels (forces de l'ordre, magistrat, équipe de réponse à incidents).		Le rapport d'analyse est précis et argumenté. 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 scénario issu de l'analyse est exact.
Bloc de compétences capitalisable, obligatoire pour l'obtention du titre (validité du bloc illimitée). L'acquisition du bloc fait l'objet de remise d'un certificat. Le cas échéant, description de tout autre document constitutif de la certification professionnelle. La thèse professionnelle, modalité d'évaluation globale et transversale, doit être validée au même titre que les 4 blocs de compétences pour obtenir la certification.			