Bachelor en Sciences et Ingénierie – Spécialité cybersécurité – Grade de licence

<u>Préambule</u> : Dans le respect de la loi du 11 février 2005 pour l'égalité des droits et des chances, de la version 4.1 du référentiel général d'amélioration de l'accessibilité (RGAA) et de la note de France compétences du 22 avril 2021 ce référentiel d'activités professionnelles prend en compte les situations de handicap afin de permettre au candidat à la certification d'être en capacité de travailler en équipe avec tous les publics, y compris ceux en situation de handicap.
D'autre part des aménagements personnalisés seront mis en place lors de l'épreuve certificative pour tous les candidats en situation de handicap.

REFERENTIEL D'ACTIVITES	REFERENTIEL DE COMPETENCES	REFERENTIEL D'EVALUATION	
		MODALITES D'EVALUATION	CRITERES D'EVALUATION
Activité A1 : Mise en place d'un processus de veille			
A 1 : Réalisation de veilles technologiques sur les nouvelles vulnérabilités et sur les méthodes des attaques relatives aux différents composants du système d'information. En s'appuyant notamment sur les alertes et les rapports gouvernementaux, étatiques ou européens (ANSSI, CNIL, Directive NIS) ou associatifs : Clusif, CESIN, OWASP, MITRE… le titulaire de la certification se doit continuellement de s'informer des évolutions réglementaires et du niveau des risques informatiques liés à l'activité de son organisation (entreprise, association, administration). Il doit également accompagner l'organisation dans l'analyse de cette veille et les évolutions réglementaires ou techniques qui en découlent.	C 1.1 : Identifier les sources et groupes de travail fiables pour détecter les évolutions technologiques des systèmes numériques dont les aspects cyber menaces (colloques, forums, sites, journalistes spécialisés…) C 1.2 : Hiérarchiser et référencer les informations en fonction des risques numériques pour l'organisation afin de prioriser leur prise en compte C 1.3 : Contribuer à l'élaboration d'un bulletin de veille pour diffuser les éléments de la veille numérique et s'assurer qu'il soit accessible à tous, notamment des collègues en situation de handicap C.1.4 : Assurer une veille légale pour respecter la règlementation et les exigences légales en termes	1.Epreuve écrite : Etude de cas réalisée de manière collective sur un facteur de risque : recherche d'un scénario de sources officielles en anglais (CVE, CERT, CSIRT, OWASP, MITRE) en fonction d'un contexte professionnel. Cette étude de cas donne lieu à la réalisation d'un bulletin de veille en français et en anglais qui contextualise et hiérarchise les risques pour l'organisation du scénario. 2.Epreuve orale : restitution en groupe et questions individuelles	Le jury doit vérifier les différents éléments suivants : 1.Cohérence et logique des sources officielles et légales identifiées au regard des facteurs de risques associés au scénario ; respect du RGPD Recoupement des sources afin de vérifier leur adéquation avec le facteur de risque 2.Clarté de la pensée, de l'expression orale, esprit logique et qualité de la présentation

<u>Préambule</u> : Dans le respect de la loi du 11 février 2005 pour l'égalité des droits et des chances, de la version 4.1 du référentiel général d'amélioration de l'accessibilité (RGAA) et de la note de France compétences du 22 avril 2021 ce référentiel d'activités professionnelles prend en compte les situations de handicap afin de permettre au candidat à la certification d'être en capacité de travailler en équipe avec tous les publics, y compris ceux en situation de handicap.
D'autre part des aménagements personnalisés seront mis en place lors de l'épreuve certificative pour tous les candidats en situation de handicap.

	de sécurité de l'information (ANSSI et ENISA) et de protection des données personnelles (RGPD)		
Activité A2 : Surveillance et analyse des traces numériques (logs)			
A 2 : Surveillance par l'observation et l'analyse des logs (traces numériques) Au sein d'une DSI (Direction des Systèmes d'Information) ou d'un SOC (Security Operation Center) le titulaire de la certification contribue à la surveillance, au maintien opérationnel de l'ensemble des équipements numériques de l'organisation et à la protection des données. Il a en sa possession un ensemble d'outils lui permettant de surveiller le système informatique tant sur l'aspect réseau, serveur que service utilisateur. Il doit être capable dans ses activités d'analyser une trace informatique issue d'un système numérique, réagir à une alerte de sécurité, soit en la résolvant soit en alertant sa hiérarchie. Il participe aussi à la mise en place	C.2.1 : Analyser la grammaire et le format des logs afin de permettre leur traitement automatique selon les règles définies C.2.2 : Mettre en œuvre les protocoles de traitement des risques en fonction des alertes afin de contribuer à la résolution du problème C.2.3 : Détecter les dysfonctionnements en cas d'absence de logs ou de logs incomplets afin d'alerter l'environnement de travail (utilisateurs, responsable) C.2.4 : Informer et argumenter auprès de sa hiérarchie afin de l'alerter sur un risque non résolu C.2.5 : Tester les nouveaux protocoles en fonction des	1.Exercice individuel de programmation (1 heure) : développer un « parser de logs » basique selon un scénario proposé 2.Etude de cas (réalisée sur ordinateur) : à partir d'un fichier transmis sur la provenance multiple de traces et d'origines diverses en vue du déclenchement du protocole proposé le plus adéquat i. Mettre en œuvre le ou les protocole(s) ii. Présenter de manière hiérarchisée les protocoles retenus afin de les communiquer à sa hiérarchie iii. Rédaction d'un reporting (état des actions de sécurité au sein de l'organisation), selon les préconisations de l'ANSSI pour assurer le suivi du service.	Le jury doit vérifier les différents éléments suivants : 1.Le programme (parser) réalisé doit être logique, fonctionnel et efficace (en temps et en mémoire) ; il analyse correctement les logs fournis et fait ressortir l'information recherchée à travers le scénario et/ou une erreur dans la grammaire des logs 2.Le choix des protocoles est justifié et argumenté. Ils sont présentés de manière hiérarchisée et le reporting est clair, compréhensible et synthétique et respecte le RGPD.

<u>Préambule</u> : Dans le respect de la loi du 11 février 2005 pour l'égalité des droits et des chances, de la version 4.1 du référentiel général d'amélioration de l'accessibilité (RGAA) et de la note de France compétences du 22 avril 2021 ce référentiel d'activités professionnelles prend en compte les situations de handicap afin de permettre au candidat à la certification d'être en capacité de travailler en équipe avec tous les publics, y compris ceux en situation de handicap.
D'autre part des aménagements personnalisés seront mis en place lors de l'épreuve certificative pour tous les candidats en situation de handicap.

de nouveaux protocoles d'alerte ou de risques et contribue aux analyses post mortem des incidents (forensique). En raison de son accès aux traces informatiques, le titulaire de la certification se doit de respecter le cadre législatif notamment en matière de protection de la vie privée et des données sensibles (RGPD)	nouvelles alertes afin de vérifier leur efficacité C.2.6 : Rédiger des reportings afin de faciliter la continuité du service C.2.7 Renseigner les tableaux de bord rendant compte de l'activité opérationnelle afin de respecter les préconisation de l'ANSSI		
Activité A3 : Détection et qualification des menaces			
A.3 : Investigations suite à incident pour détecter et qualifier les menaces Suite à une levée d'alerte sur une menace supposée ou avérée, le titulaire de la certification participe aux investigations forensiques permettant d'identifier techniquement la menace et ses impacts sur les systèmes numériques et les données de l'organisation ainsi que les actions immédiates ou ultérieures à mener.	C.3.1 : Mettre en œuvre les outils d'investigation numériques appropriés pour établir une levée de doutes afin d'invalider ou de valider l'incident C.3.2 : Contextualiser l'alerte afin d'identifier quels types de réponses à mettre en œuvre et évaluer la gravité des incidents de sécurité C.3.3 : Mettre en place une alerte auprès de la personne concernée ou du responsable hiérarchique afin de qualifier l'action réalisée par l'utilisateur	Etude de cas sur la base d'un scénario proposé : 1.Rechercher les compromissions (*Threat hunting*) : cartographier et identifier les différentes techniques d'attaques à partir du référentiel MITRE (2 heures). 2. Proposer un plan de remédiation (3 heures) en fonction de la nature des attaques et de leur importance (mesures immédiates, recommandations et rappel des règles aux utilisateurs ; informations/alertes/propositions au niveau supérieur technique ou	Le jury doit vérifier les différents éléments suivants : 1.La cartographie réalisée est correcte et exhaustive. Les liens entre les techniques d'attaques sont établis avec le référentiel MITRE. 2.Le plan de remédiation est cohérent et comporte bien un volet d'au moins une dizaine de recommandations pour accompagner le traitement des incidents ; ce plan est destiné au niveau supérieur technique ou hiérarchique.

Bachelor en Sciences et Ingénierie – Spécialité cybersécurité – Grade de licence

<u>Préambule</u> : Dans le respect de la loi du 11 février 2005 pour l'égalité des droits et des chances, de la version 4.1 du référentiel général d'amélioration de l'accessibilité (RGAA) et de la note de France compétences du 22 avril 2021 ce référentiel d'activités professionnelles prend en compte les situations de handicap afin de permettre au candidat à la certification d'être en capacité de travailler en équipe avec tous les publics, y compris ceux en situation de handicap.
D'autre part des aménagements personnalisés seront mis en place lors de l'épreuve certificative pour tous les candidats en situation de handicap.

Le titulaire de la certification va donc réaliser les activités suivantes : - Confirmer ou non la réalité du risque - Identifier l'étendue des systèmes informatiques impactés ou impactables - Définir une liste d'actions immédiates à réaliser - Participer à l'analyse forensique - Rédiger des recommandations sur les mesures immédiates - Identifier le support technique de la menace (malware, virus, fuite de mot de passe, configuration de certains éléments du système d'information, gestion des identités et des accès (IAM) - Communiquer aux personnes ayant eu un comportement inadéquat et aux personnes potentiellement cibles	C.3.4 : Pré qualifier la cyber menace afin d'en évaluer la nature et l'importance C.3.5 : Proposer une série d'actions immédiates sur le système d'information pour réduire ou résoudre le problème C.3.6 : Préconiser des recommandations aux utilisateurs pour répondre à leurs questions afin de partager de bons usages et de bonnes pratiques C.3.7 : Contribuer à la mise en place du service de détection (SIEM, etc)	hiérarchique) pour l'amélioration des procédures.	

<u>Préambule</u> : Dans le respect de la loi du 11 février 2005 pour l'égalité des droits et des chances, de la version 4.1 du référentiel général d'amélioration de l'accessibilité (RGAA) et de la note de France compétences du 22 avril 2021 ce référentiel d'activités professionnelles prend en compte les situations de handicap afin de permettre au candidat à la certification d'être en capacité de travailler en équipe avec tous les publics, y compris ceux en situation de handicap.
D'autre part des aménagements personnalisés seront mis en place lors de l'épreuve certificative pour tous les candidats en situation de handicap.

d'une attaque, les règles à respecter. Dans ce cadre il adapte son discours et les pratiques en fonction des rôles et des personnes concernées (notamment collaborateurs en situation de handicap). - Proposer des expertises extérieures si besoin (préconisation de l'ANSSI)			
Activité A4 : Optimisation des règles			
A 4 : Optimisation des règles Dans son activité de surveillance, le titulaire de la certification se repose sur une automatisation des traitements des traces informatiques issues de l'ensemble des systèmes informatiques de l'organisation (réseaux, serveurs, logiciels…) Cette automatisation est basée sur une ensemble de règles de traitement spécifiques à l'organisation. Le titulaire de la certification contribue à la	C.4.1 : Détecter ou repérer des améliorations possibles des règles mobilisées afin d'en affiner la pertinence et proposer des optimisations C.4.2 : Réunir la liste des règles sources d'anomalies et les traces du fonctionnement des outils en vue de préparer la revue des règles C.4.3 : Contribuer à l'élaboration de propositions d'optimisation afin de participer activement à une réunion de revue de règles	Mise en situation en groupe : 1.Rédiger une revue de règles optimisées. Argumenter le choix effectué et justifier le non besoin éventuel d'optimisation. Proposer quelques voies d'accès pour des collaborateurs en situation de handicap 2.Sur la base d'expressions régulières fournies à partir de différents systèmes (épreuve individuelle et collective réalisée sur ordinateur) : analyser leur optimisation, argumenter et	Le jury doit vérifier les différents éléments suivants : 1.La revue de règles est rigoureuse, l'argumentation est cohérente et appropriée. Le non besoin d'évolution est (éventuellement) justifié. 2.L'analyse de l'optimisation des expressions régulières est argumentée et justifiée. 3.Pertinence des propositions d'améliorations sur les outils de

<u>Préambule</u> : Dans le respect de la loi du 11 février 2005 pour l'égalité des droits et des chances, de la version 4.1 du référentiel général d'amélioration de l'accessibilité (RGAA) et de la note de France compétences du 22 avril 2021 ce référentiel d'activités professionnelles prend en compte les situations de handicap afin de permettre au candidat à la certification d'être en capacité de travailler en équipe avec tous les publics, y compris ceux en situation de handicap.
D'autre part des aménagements personnalisés seront mis en place lors de l'épreuve certificative pour tous les candidats en situation de handicap.

création, maintenance, actualisation de l'ensemble des règles de traitement. Ainsi il doit régulièrement optimiser ou améliorer les règles en cours. Il participe aux revues de règles où une analyse systémique de l'ensemble des règles est réalisée. Le titulaire de la certification veille à ce que les règles respectent le traitement des données (RGPD). Il maintient à jour la documentation. Il collabore à l'amélioration continue des règles et des procédures.	C.4.4 : Mettre en œuvre les optimisations d'expressions régulières (filtres ou capteurs) pour accélérer le traitement des données C.4.5 : Mettre en place une veille permanente sur les outils de détection et de corrélation d'événements (SIEM, etc)	justifier leur choix (exemple : Firewall, accès à privilège, élévation de droits…). 3.Analyse des outils de détection et de corrélation mis en place et proposition d'améliorations	détection et de corrélation, respectant le RGPD
Activité A5 : Configuration des équipements et application de modes opératoires et des procédures			
A.5 : Configuration des équipements et application de modes opératoires et des procédures Pour l'installation ou la maintenance de tout équipement le titulaire de la certification respecte les procédures, règles et	C.5.1 : Paramétrer les équipements selon les normes de sécurité et les règles définies par le client pour les rendre opérationnels dans la chaîne de détection de surveillance C.5.2 : Dérouler un cahier de tests en vue de vérifier le bon fonctionnement des équipements	Mise en situation professionnelle individuelle (des équipements et un cahier des charges sont fournis au candidat.e) 1.Paramétrer les équipements en fonction du cahier des charges (3 niveaux de difficulté en 3 heures) Des anomalies ayant été introduites, il s'agit de repérer et corriger ces anomalies	Le jury doit vérifier les différents éléments suivants : 1.Le paramétrage des équipements est conforme au cahier des charges. Les anomalies sont toutes identifiées et les correctifs proposés sont adaptés et justifiés. La recette est réalisée conformément au cahier des charges.

Bachelor en Sciences et Ingénierie – Spécialité cybersécurité – Grade de licence

<u>Préambule</u> : Dans le respect de la loi du 11 février 2005 pour l'égalité des droits et des chances, de la version 4.1 du référentiel général d'amélioration de l'accessibilité (RGAA) et de la note de France compétences du 22 avril 2021 ce référentiel d'activités professionnelles prend en compte les situations de handicap afin de permettre au candidat à la certification d'être en capacité de travailler en équipe avec tous les publics, y compris ceux en situation de handicap.
D'autre part des aménagements personnalisés seront mis en place lors de l'épreuve certificative pour tous les candidats en situation de handicap.

spécifications liées à cet équipement. Pour cela le titulaire de la certification réalise les activités suivantes : - Dérouler une procédure d'installation ou de maintenance d'un équipement - Tester le matériel et son intégration au système informatique - Contribuer à l'évolution des procédures et/ou modes opératoires, en particulier en fonction des évolutions réglementaires (RGPD) - Participer à la diffusion des procédures et modes opératoires en prenant en compte les fonctions et contextes de chaque collaborateur notamment ceux en situation de handicap	C.5.3 : Repérer les anomalies (configuration des équipements et règles de fonctionnement) et les signaler afin de relancer l'opération de paramétrage C.5.4 : Actualiser l'information concernant les modes opératoires ou procédures afin d'améliorer l'usage des nouveaux équipements C.5.5 : Présenter les évolutions des nouveaux équipements pour former les futurs utilisateurs (et maintenir à jour la documentation)	2.Réaliser la recette (rapport écrit et ou adapté si besoin à une personne en situation de handicap) 3.Présenter à l'oral la recette (40 minutes de préparation ; 15 minutes de présentation ; 15 minutes de questions réponses)	2.La présentation orale est claire, synthétique et reprend l'ensemble des propositions présentées par le candidat.e dans son rapport écrit.