RÉFÉRENTIELS DE LA CERTIFICATION PROFESSIONNELLE « TECHNICEN VEILLEUR DE CYBERSÉCURITÉ » NIVEAU 5

MODALITÉS D'ÉVALUATION DES COMPÉTENCES

Évaluation des compétences au titre de la formation continue :

Dans le cadre du dispositif de développement de compétences (DDC) et plus particulièrement des formations, les évaluations s'articulent selon une logique de « compétences ». En effet, les référentiels de formation ont été modularisés afin de respecter les compétences détaillées dans le référentiel d'activités et de compétences (RAC) de l'emploi.

Ainsi, les savoirs de référence et procéduraux sont appréciés lors d'évaluations orales ou écrites [questionnaires à choix multiples (QCM), à courte réponse (QCR) ou à court développement (QCD), étude de cas concrets et production rédactionnelle, etc.] assorties de mises en situation contextualisées, d'études de cas et/ou de restitutions technico-opérationnelles.

Les appréciations du collège des instructeurs se structurent selon trois critères :

1. **Les savoirs de référence et connaissances techniques :**

   Il s'agit d'évaluer si le stagiaire mobilise les savoirs procéduraux et techniques nécessaires à la résolution d'un problème donné, dans le champ professionnel concerné (blocs de compétences) en s'appuyant sur l'assimilation réfléchie de savoirs de références.

2. **Les compétences professionnelles :**

   Le champ de ce critère est plus large que le précédent car il consiste à apprécier l'ensemble des savoir-faire du stagiaire et sa bonne appréhension de l'environnement professionnel dans lequel il évolue.

   Les savoir-faire requis peuvent aller de la simple capacité à exécuter une tâche prescrite jusqu'à la gestion de missions /interventions complexes et inédites à mener sous stress intense. En d'autres termes, il s'agit d'apprécier les capacités du stagiaire à mettre en œuvre ses connaissances techniques dans différentes situations se rapportant à divers contextes.

3. **Les aptitudes professionnelles :**

   Les observations lors des mises en situation doivent permettre de les révéler. Ce critère, essentiel au futur emploi, permet d'aller au-delà de la seule appréciation des mérites professionnels antérieurs des stagiaires. Il s'agit d'apprécier un potentiel humain dans un contexte professionnel déterminé, c'est-à-dire sa capacité à s'insérer dans une intervention en environnement hautement incertain et risqué, ainsi qu'à s'adapter aux évolutions et exigences des fonctions associées à l'emploi.

Évaluation des compétences au titre de la VAE :

L'évaluation des compétences s'appuie sur l'étude de la présentation de l'expérience du livret 2 et sur les documents éventuellement annexés, complétée par un entretien avec le jury (présentiel ou à distance), voire par une mise en situation professionnelle simulée ou réelle.

Article L6113-1 En savoir plus sur cet article... Créé par LOI n°2018-771 du 5 septembre 2018 - art. 31 (V)

« *Les certifications professionnelles enregistrées au répertoire national des certifications professionnelles permettent une validation des compétences et des connaissances acquises nécessaires à l'exercice d'activités professionnelles. Elles sont définies notamment par un* ***référentiel d'activités*** *qui décrit les situations de travail et les activités exercées, les métiers ou emplois visés, un* ***référentiel de compétences*** *qui identifie les compétences et les connaissances, y compris transversales, qui en découlent et un* ***référentiel d'évaluation*** *qui définit les critères et les modalités d'évaluation des acquis.* »

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 1 - Opérer le déploiement et l'administration d'une infrastructure sécurisée d'un système d'information en fonction des évolutions de l'organisme. *Le technicien veilleur de cybersécurité a la charge du suivi (installation et configuration des équipements de sécurité), de la sécurisation, de l'évolution et du maintien en conditions opérationnelles des équipements de cybersécurité dans le strict respect des exigences de la politique de sécurité définie au sein de la société afin que cette architecture puisse garantir la sécurité logique et physique du système d'information et des données traitées. Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises..*			
A.1. Déploiement de tout ou partie des architectures sécurisées des systèmes d'information, des systèmes industriels, des systèmes embarqués ou tout objet communicant sécurisé.	*Le technicien veilleur de cybersécurité travaille dans un périmètre donné en respectant les méthodes, normes et standards qui prévalent au sein de cette organisation afin de mettre en place des programmes de sécurité efficients.*		
A1.1 Intégration des équipements de sécurité.	- Intégrer des équipements de sécurité (parefeu, sonde, IDS…) afin de créer une plateforme sécurisée répondant aux exigences de la politique de sécurité en vigueur au sein de l'organisme, en sélectionnant du matériel agréé.	**<u>Voie formative</u> :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles.	- les équipements sont parfaitement installés dans l'infrastructure. - les équipements sont minutieusement configurés. - le déploiement est totalement conforme à la réglementation et à l'état de l'art des équipements de sécurité nécessaires à la protection du SI. - les exigences de sécurité sont pleinement prises en compte.
A1.2 Renforcement de la protection.	- Durcir les systèmes d'exploitation (Windows ou Linux) et la protection des postes de travail dans les domaines bureautique, scientifique et industriel en vue de maintenir l'intégrité des fonctionnalités et la fiabilité de l'ensemble du système, par l'application des paramétrages de sécurité recommandés, l'arrêt ou la désinstallation de services/logiciels et l'installation de logiciels de sécurité.	**<u>VAE</u> :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	- les interventions à effectuer sont recensées avec méthode. - les paramétrages de sécurité sur les systèmes d'exploitation sont correctement effectués. - tous les services/logiciels à désinstaller ont été formellement identifiés. - le choix des logiciels à installer est pertinent. - les postes de travail sont protégés et ne présentent pas de vulnérabilités connues.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 1 - Opérer le déploiement et l'administration d'une infrastructure sécurisée d'un système d'information en fonction des évolutions de l'organisme. *Le technicien veilleur de cybersécurité a la charge du suivi (installation et configuration des équipements de sécurité), de la sécurisation, de l'évolution et du maintien en conditions opérationnelles des équipements de cybersécurité dans le strict respect des exigences de la politique de sécurité définie au sein de la société afin que cette architecture puisse garantir la sécurité logique et physique du système d'information et des données traitées. Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.1. Déploiement de tout ou partie des architectures sécurisées des systèmes d'information, des systèmes industriels, des systèmes embarqués ou tout objet communicant sécurisé.	*Le technicien veilleur de cybersécurité travaille dans un périmètre donné en respectant les méthodes, normes et standards qui prévalent au sein de cette organisation afin de mettre en place des programmes de sécurité efficients.*		
A1.3 -Sécurisation des flux.	- Gérer la sécurisation des flux dans l'intention d'assurer et d'améliorer la confidentialité, l'intégrité, la disponibilité des SI grâce à la réalisation d'une matrice des flux et la mise en place de la segmentation des réseaux.	**Voie formative :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles. **VAE :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	- la matrice des flux est minutieusement décrite. - la segmentation des réseaux est réalisée de manière rigoureuse. - l'identification des flux est rigoureuse. - le filtrage des flux est conforme à la politique de sécurité de l'organisme.
A1.4 - Déploiement des moyens cryptographiques.	- Déployer les moyens cryptographiques adéquats pour assurer l'intégrité et la traçabilité des données transmises/reçues dans le cadre de la défense en profondeur.		- les besoins de chiffrement sont très bien identifiés. - les moyens déployés sont totalement adaptés au niveau de sécurité attendu. - les équipements sont rigoureusement configurés. - des échanges de données entièrement chiffrées sont opérationnels.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 1 - Opérer le déploiement et l'administration d'une infrastructure sécurisée d'un système d'information en fonction des évolutions de l'organisme. *Le technicien veilleur de cybersécurité a la charge du suivi (installation et configuration des équipements de sécurité), de la sécurisation, de l'évolution et du maintien en conditions opérationnelles des équipements de cybersécurité dans le strict respect des exigences de la politique de sécurité définie au sein de la société afin que cette architecture puisse garantir la sécurité logique et physique du système d'information et des données traitées. Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.2. Conduite de l'administration et de l'évolution des équipements de sécurité.	*Le technicien veilleur de cybersécurité travaille en totale autonomie, avec rigueur et le sens de la méthode car l'administration d'une solution de sécurité requiert une attention de tous les instants.*		
A2.1 Anticipation des dysfonctionnements.	- Anticiper les problèmes de fonctionnement des équipements de sécurité par la mise en place de parades technologiques aux incidents envisageables afin d'éviter le traitement des événements via l'application de procédures spécifiques aux dysfonctionnements.	**<u>Voie formative</u> :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles. **<u>VAE</u> :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	- l'analyse des dysfonctionnements potentiel est pertinente. - les dysfonctionnements envisagés sont représentatifs. - des plans de continuité/reprise d'activité sont rédigés. - ces plans de continuité/reprise d'activité sont totalement réalistes et réalisables.
A2.2 Maintien en condition de sécurité.	- Assurer le maintien en condition de sécurité (MCS) de l'ensemble des applications en mettant en œuvre différents scénarios de gestion des correctifs de sécurité ou « patchs » afin de certifier le bon niveau de sécurité de l'infrastructure de l'entreprise.		- les applications entrant dans le périmètre du MCS sont minutieusement identifiées. - les scénarios envisagés en fonction du niveau de criticité de la vulnérabilité sont parfaitement cohérents. - les outils et procédures sont mis en œuvre efficacement. - la mise en œuvre du MCS ne perturbe pas le fonctionnement des systèmes et du réseau.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 1 - Opérer le déploiement et l'administration d'une infrastructure sécurisée d'un système d'information en fonction des évolutions de l'organisme. *Le technicien veilleur de cybersécurité a la charge du suivi (installation et configuration des équipements de sécurité), de la sécurisation, de l'évolution et du maintien en conditions opérationnelles des équipements de cybersécurité dans le strict respect des exigences de la politique de sécurité définie au sein de la société afin que cette architecture puisse garantir la sécurité logique et physique du système d'information et des données traitées. Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.2. Conduite de l'administration et de l'évolution des équipements de sécurité.	*Le technicien veilleur de cybersécurité travaille en totale autonomie, avec rigueur et le sens de la méthode car l'administration d'une solution de sécurité requiert une attention de tous les instants.*		
A2.3 -Sauvegardes.	- Réaliser des sauvegardes complètes et périodiques de l'infrastructure de l'organisme en vue de garantir une restauration rapide du SI suite à une attaque informatique.	**Voie formative :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles. **VAE :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	-la réalisation d'un plan de sauvegarde est totalement fiable. - les procédures de sauvegarde sont réalistes et réalisables. - la remise en route répond aux besoins de disponibilité. - la restauration est de qualité attendue.
A2.4 Sécurisation logique et physique du SI.	- Mettre en place les évolutions nécessaires pour garantir la sécurité logique et physique du SI par l'utilisation de matériels robustes et de moyens adaptés.		- le filtrage des accès physiques et logiques à un serveur ou à un service est efficace. - les mesures de filtrage évoluent de manière pertinente. - la discrimination des accès est méthodique. - les moyens de filtrage et de contrôle d'accès sont pleinement adaptés aux besoins de sécurité.
A2.5 -Contrôle du paramétrage des dispositifs déployés.	- Contrôler méthodiquement le paramétrage de tous les dispositifs de sécurité déployés afin de garantir des applications et une infrastructure informatiques stables et sécurisées.		- les paramétrages permissifs sont immédiatement repérés et corrigés. - la traçabilité des accès est effective. - l'accès aux applications est soumis à conditions.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 2 - Superviser les réseaux et les systèmes d'information de l'infrastructure de l'organisme et assurer une veille technologique et réglementaire en matière de sécurité. *Le technicien veilleur de cybersécurité doit s'organiser pour travailler de façon autonome et efficace pour superviser les réseaux et les systèmes d'information en démontrant un esprit analytique tout en effectuant une veille permettant de garantir la conformité des solutions (actuelles et futures) avec la réglementation en vigueur ainsi qu'une veille en matière de cybersécurité (risques informatiques, failles, vulnérabilités, techniques de protection des systèmes d'information, …). Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.1. Supervision des réseaux.	*Le technicien veilleur de cybersécurité est en charge d'une supervision permanente des réseaux et système d'information avec organisation, méthode et vigilance. Le technicien veilleur de cybersécurité est autonome dans l'exécution de ses tâches mais doit aussi être capable de solliciter sa hiérarchie.*		
A.1.1. Analyse des remontées d'alertes.	- Analyser les différentes remontées d'alertes issues des outils de détection et des comptes rendus afin de détecter les intrusions ou tentative d'intrusion dans le système grâce à des outils d'analyse de données ou des corrélateurs d'événements.	**<u>Voie formative</u> :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles. **<u>VAE</u> :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	-l'exploitation des remontées d'alerte est judicieuse. - l'exploitation des logs est pertinente. - l'utilisation des outils (IPS, IDS, HIDS/NIDS type Suricata…) est parfaitement maîtrisée. - la discrimination entre une menace avérée et une fausse alerte est effectuée de manière méthodique.
A.1.2. Recherche des événements de cybersécurité et des menaces.	- Rechercher (via des outils d'analyse de log) les événements de cybersécurité et les menaces suite à un avis de sécurité afin de dépister une éventuelle intrusion.		- la mise en œuvre d'une méthodologie de recherche de marqueurs caractéristiques d'une attaque est efficace. - les outils d'analyse de log (ELK, Splunk…) sont intelligemment utilisés. - les résultats et conclusions sont probants.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 2 - Superviser les réseaux et les systèmes d'information de l'infrastructure de l'organisme et assurer une veille technologique et réglementaire en matière de sécurité. *Le technicien veilleur de cybersécurité doit s'organiser pour travailler de façon autonome et efficace pour superviser les réseaux et les systèmes d'information en démontrant un esprit analytique tout en effectuant une veille permettant de garantir la conformité des solutions (actuelles et futures) avec la réglementation en vigueur ainsi qu'une veille en matière de cybersécurité (risques informatiques, failles, vulnérabilités, techniques de protection des systèmes d'information, …). Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.1. Supervision des réseaux.	*Le technicien veilleur de cybersécurité est en charge d'une supervision permanente des réseaux et système d'information avec organisation, méthode et vigilance. Le technicien veilleur de cybersécurité est autonome dans l'exécution de ses tâches mais doit aussi être capable de solliciter sa hiérarchie.*		
A.1.3. Automatisation des outils de pilotage.	- Améliorer la supervision de sécurité par l'automatisation des outils de pilotage de la sécurité dans le but de rester réduire les tâches répétitives, chronophages et non essentielles.	**Voie formative :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles.	- l'utilisation des langages de programmation (Python, langage C…) est adaptée. - les scripts permettant le déploiement à grande échelle d'outils de supervision spécifiques ou permettant de mieux collecter les journaux d'éléments sont efficaces et utiles. - les tâches à automatiser sont judicieusement identifiées. - les tâches répétitives, chronophages et non essentielles sont réduites.
A.1.4 Mise en œuvre de tableaux de bord.	- Assurer la tenue des tableaux de bords relatifs à la sécurité du système d'information dans le but d'évaluer le niveau de performance et de sécurité et ainsi aider à la décision.	**VAE :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	- les tableaux de bord sont clairs et permettent de rapidement évaluer la situation. - les indicateurs utilisés sont totalement pertinents. - les points majeurs devant apparaître dans les tableaux de bords sont judicieusement identifiés. - l'évaluation du niveau de sécurité est rapide et efficace.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 2 - Superviser les réseaux et les systèmes d'information de l'infrastructure de l'organisme et assurer une veille technologique et réglementaire en matière de sécurité. *Le technicien veilleur de cybersécurité doit s'organiser pour travailler de façon autonome et efficace pour superviser les réseaux et les systèmes d'information en démontrant un esprit analytique tout en effectuant une veille permettant de garantir la conformité des solutions (actuelles et futures) avec la réglementation en vigueur ainsi qu'une veille en matière de cybersécurité (risques informatiques, failles, vulnérabilités, techniques de protection des systèmes d'information, …). Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises..*			
A.2. Mise en place des veilles normatives, juridiques, gouvernementales et technologiques.	*Le technicien veilleur de cybersécurité doit faire preuve de curiosité intellectuelle car il doit se tenir au courant des nouveaux risques et des nouvelles parades (virus et antidotes). Le technicien, veilleur de cybersécurité doit démontrer une certaine adaptabilité et de l'intérêt car les évolutions technologiques sont rapides et doivent être assimilées afin de pouvoir optimiser l'existant.*		
A2.1 Veille relative aux dispositions réglementaires et professionnelles.	- Appliquer les dispositions réglementaires et professionnelles en vigueur en matière de cybersécurité et de continuité d'activité au sein de son entité.	**<u>Voie formative</u> :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles.	- la vérification que la collecte, le traitement et la conservation des données à caractère personnel sont effectués conformément à la réglementation en vigueur est rigoureuse et méthodique. - l'identification des écarts avec le RGPD est méthodique. - des mesures correctives sont systématiquement mises en œuvre dès qu'un écart avec le RGPD est identifié. - un signalement à la hiérarchie de toute anomalie le méritant est mis en œuvre.
A.2.2 Veille relative aux règlements et standards.	- Assurer une veille sur les règlements et les standards liés aux évolutions législatives et réglementaires en se maintenant à jour des futures modifications afin d'anticiper les changements.	**<u>VAE</u> :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	- les sources de veille sont variées et bien ciblées. - les recherches sont organisées et fournies, au plus près de l'exhaustif. - les caractéristiques des nouvelles technologies disponibles sur le marché sont correctement appréhendées. - le partage du résultat de recherche et de veille est effectué, oralement ou par écrit, avec ses pairs via une participation à des groupes d'échanges ou une inscription à des clubs de la sécurité.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 2 - Superviser les réseaux et les systèmes d'information de l'infrastructure de l'organisme et assurer une veille technologique et réglementaire en matière de sécurité. *Le technicien veilleur de cybersécurité doit s'organiser pour travailler de façon autonome et efficace pour superviser les réseaux et les systèmes d'information en démontrant un esprit analytique tout en effectuant une veille permettant de garantir la conformité des solutions (actuelles et futures) avec la réglementation en vigueur ainsi qu'une veille en matière de cybersécurité (risques informatiques, failles, vulnérabilités, techniques de protection des systèmes d'information, …). Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.2. Mise en place des veilles normatives, juridiques, gouvernementales et technologiques.	*Le technicien veilleur de cybersécurité doit faire preuve de curiosité intellectuelle car il doit se tenir au courant des nouveaux risques et des nouvelles parades (virus et antidotes). Le technicien, veilleur de cybersécurité doit démontrer une certaine adaptabilité et de l'intérêt car les évolutions technologiques sont rapides et doivent être assimilées afin de pouvoir optimiser l'existant.*		
A.2.3 Veille à la protection des données personnelles.	- Assurer une veille réglementaire sur la protection des données personnelles (RGPD) dans une démarche de mise en conformité permanente vis-à-vis du RGPD et de maîtrise des enjeux majeurs (juridiques et financiers) liés à la protection des données personnelles.	**<u>Voie formative</u> :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles. **<u>VAE</u> :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	- l'analyse des dysfonctionnements potentiels est pertinente. - les dysfonctionnements envisagés sont représentatifs. - des plans de continuité/reprise d'activité sont rédigés. - ces plans de continuité/reprise d'activité sont totalement réalistes et réalisables.
A.2.4 Veille technologique.	- Assurer une veille technologique en participant à des conférences ou des démonstrations techniques, en lisant des articles de presse écrite spécialisée ou en consultant des sites internet en matière de cybersécurité. pour collecter les informations utiles sur les nouveaux risques et nouvelles failles de sécurité.		- les applications entrant dans le périmètre du MCS sont minutieusement identifiées. - les scénarios envisagés en fonction du niveau de criticité de la vulnérabilité sont parfaitement cohérents. - les outils et procédures sont mis en œuvre efficacement. - la mise en œuvre du MCS ne perturbe pas le fonctionnement des systèmes et du réseau.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 3 - Gérer les incidents de cybersécurité en assurant les premières réactions et investiguer ces événements de cybersécurité. *Potentiellement sous forte contraintes opérationnelles, faire face aux incidents de sécurité en utilisant les outils de management de la sécurité et réaliser des reporting demandent au technicien veilleur de cybersécurité une résistance au stress pour affronter des situations de crise nombreuses et inattendues et savoir conserver ses capacités dans les situations ponctuellement tendues afin de fournir les moyens nécessaires au bon déroulement de l'activité. L'objectif principal est de rétablir aussi vite que possible le fonctionnement normal des services en minimisant les effets sur l'activité professionnelle, assurant ainsi les meilleurs niveaux de disponibilité et de qualité possibles. Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.1. Gestion des incidents de cybersécurité.	*Sous l'autorité d'un administrateur cybersécurité, le technicien veilleur de cybersécurité s'accommode d'une autonomie partielle pour s'occuper des incidents informatiques et pour appliquer les dispositifs de gestion de crise et de continuité d'activité afin d'accroître la résilience de l'entreprise face à une cyberattaque avérée.*		
A.1.1 Caractérisation de l'incident de cybersécurité.	- Caractériser un événement informatique en un incident de cybersécurité ou en une panne, un dysfonctionnement du système.	**Voie formative :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles. **VAE :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	- la méthodologie employée est efficace. - toutes les informations utiles à la caractérisation sont judicieusement exploitées. - l'analyse de l'évènement est approfondie. - l'analyse de l'évènement est pertinente et les conclusions sont raisonnablement correctes. - l'événement de cybersécurité est correctement caractérisé.
A.1.2 Traitement de l'incident de cybersécurité en cellules opérationnelles.	- Opérer au sein de cellules opérationnelles de gestion de crise pour traiter l'incident le plus rapidement possible en mettant en œuvre les actions décidées en réponse à incident afin que l'organisme reprenne son activité au plus tôt.		- la réactivité est au niveau attendu. - Les fiches reflexes sont scrupuleusement mises en œuvre. - le choix de la procédure à appliquer est judicieux. - les conseils et recommandations pour la reprise de l'activité de l'entreprise sont pertinents.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 3 - Gérer les incidents de cybersécurité en assurant les premières réactions et investiguer ces événements de cybersécurité. *Potentiellement sous forte contraintes opérationnelles, faire face aux incidents de sécurité en utilisant les outils de management de la sécurité et réaliser des reporting demande au technicien veilleur de cybersécurité une résistance au stress pour affronter des situations de crise nombreuses et inattendues et savoir conserver ses capacités dans les situations ponctuellement tendues afin de fournir les moyens nécessaires au bon déroulement de l'activité. L'objectif principal est de rétablir aussi vite que possible le fonctionnement normal des services en minimisant les effets sur l'activité professionnelle, assurant ainsi les meilleurs niveaux de disponibilité et de qualité possibles. Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.1. Gestion des incidents de cybersécurité.	*Sous l'autorité d'un administrateur cybersécurité, le technicien veilleur de cybersécurité s'accommode d'une autonomie partielle pour s'occuper des incidents informatiques et pour appliquer les dispositifs de gestion de crise et de continuité d'activité afin d'accroître la résilience de l'entreprise face à une cyberattaque avérée.*		
A.1.3 Remédiation du système.	- Mettre en œuvre des solutions palliatives ou correctrices qui vont atténuer les conséquences de l'incident de cybersécurité et permettre une poursuite durable de l'activité.	**Voie formative :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles. **VAE :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	- les solutions proposées sont totalement pertinentes. - les solutions proposées sont réalistes et réalisables. - les solutions proposées prennent impérieusement en compte le contexte opérationnel. - la reprise de l'activité ou sa poursuite est pleinement maîtrisée et effective.
A.1.4 Historique et traçabilité des incidents.	- Assurer le suivi des incidents en lien avec la cybersécurité en mettant à jour les différents tableaux de bord relatifs à l'activité de gestion des incidents.		- la mise en place d'une procédure de journalisation, de traçabilité et de suivi des actions engagées est effective. - l'historique de tous les événements est exploitable en permanence. - des indicateurs liés aux incidents sont clairement identifiés. - les indicateurs sont intelligemment exploités.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 3 - Gérer les incidents de cybersécurité en assurant les premières réactions et investiguer ces événements de cybersécurité. *Potentiellement sous forte contraintes opérationnelles, faire face aux incidents de sécurité en utilisant les outils de management de la sécurité et réaliser des reporting demande au technicien veilleur de cybersécurité une résistance au stress pour affronter des situations de crise nombreuses et inattendues et savoir conserver ses capacités dans les situations ponctuellement tendues afin de fournir les moyens nécessaires au bon déroulement de l'activité. L'objectif principal est de rétablir aussi vite que possible le fonctionnement normal des services en minimisant les effets sur l'activité professionnelle, assurant ainsi les meilleurs niveaux de disponibilité et de qualité possibles. Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.2. Investigation des événements de cybersécurité.	*Sous l'autorité d'un administrateur cybersécurité, le technicien veilleur de cybersécurité s'accommode d'une autonomie partielle pour rechercher et analyser les SI corrompus en faisant preuve de rigueur, de disponibilité et de discrétion*		
A.2.1 Relevé de traces d'attaques informatiques.	- Prélever les traces d'une attaque informatique passée ou en cours dans le but de fournir des preuves en cas d'une enquête interne à l'entreprise, voire judiciaire, à l'aide d'outils de forensique informatiques tout en préservant les données originales.	**<u>Voie formative</u> :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles. **<u>VAE</u> :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	- La préservation des données originales est formellement réalisée avant toute analyse. - le matériel adapté est strictement utilisé pour assurer la préservation des preuves. - la traçabilité des données originales est formellement garantie. - l'intégrité des données originales est pleinement assurée.
A.2.2 Recherche des indices de compromission du système d'information.	- Analyser les prélèvements effectués afin de rechercher des indices d'une compromission du système.		- la recherche d'une compromission est minutieuse. - les indices relevés sont concluants. - la méthode employée est rigoureuse.
A.2.3 Création d'un laboratoire d'analyse inforensique.	- Procéder à la création d'un laboratoire d'analyse pour une analyse de premier niveau permettant d'apporter les premiers éléments de preuve.		- l'installation des logiciels d'inforensique est parfaitement maîtrisée. - l'environnement informatique servant à l'analyse est entièrement sécurisé. - l'utilisation des logiciels d'inforensique est totalement adaptée à l'analyse. - l'analyse approfondie des prélèvements est menée de manière minutieuse. - l'analyse du code binaire suspect fournit des informations utiles.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 4 – Contrôler le droit d'accès au système et aux données de l'organisme, sensibiliser et former le personnel et conseiller l'officier de la sécurité des systèmes d'information de l'entreprise *Le technicien veilleur de cybersécurité doit démontrer de la rigueur et un sens de la méthode afin de conduire les habilitations des personnes non seulement pour maîtriser davantage les risques opérationnels liés aux autorisations réellement en vigueur dans la société, mais également pour répondre aux enjeux de conformité réglementaire.* *Pour assurer les actions de communication et de sensibilisation sur les enjeux de sécurité informatique de l'entreprise à l'ensemble du personnel (administrateurs, personnel de direction et utilisateurs), le technicien veilleur de cybersécurité doit faire preuve de diplomatie, d'écoute, d'un sens du dialogue et de persuasion, afin de convaincre les utilisateurs des risques encourus et du bien-fondé des procédures mises en place. Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.1. Participation au contrôle administratif et aux actions de conseil technique.	*Le technicien veilleur de cybersécurité est autonome dans l'exécution de ses tâches en manifestant de la rigueur et un souci du détail pour mener à bien la politique des droits d'accès.*		
A.1.1 Attribution des habilitations.	- Attribuer les habilitations nécessaires aux collaborateurs et mener des revues d'habilitations régulières ou ponctuelles afin de s'assurer que tout le personnel de l'organisme a uniquement accès aux données dont il a besoin.	**Voie formative :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles.	- les accès et privilèges respectent totalement les règles organisationnelles : - le suivi des habilitations est étroitement assuré. - les demandes de renouvellement des habilitations sont transmises en temps et en heure aux personnes dont l'habilitation va expirer. - les dossiers de demande d'habilitation sont parfaitement cohérents avec les règles de filtrage des accès physiques et logiques.
A.1.2 Conseil à l'OSSI de l'organisme.	- Conseiller les acteurs de la sécurité du patrimoine informationnel, sur les problématiques de sécurité dans leur domaine (production, développement, assistance) afin de contribuer à faire évoluer la sécurité selon les besoins et les risques.	**VAE :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire.	- les conseils dispensés à l'équipe dirigeante sont d'une efficacité remarquée pour la prise de de décision. - les conseils fournis augmentent fondamentalement la sécurité globale. - les conseils délivrés sont clairement adaptés au niveau de compréhension technique de la hiérarchie.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 4 – Contrôler le droit d'accès au système et aux données de l'organisme, sensibiliser et former le personnel et conseiller l'officier de la sécurité des systèmes d'information de l'entreprise *Le technicien veilleur de cybersécurité doit démontrer de la rigueur et un sens de la méthode afin de conduire les habilitations des personnes non seulement pour maîtriser davantage les risques opérationnels liés aux autorisations réellement en vigueur dans la société, mais également pour répondre aux enjeux de conformité réglementaire.* *Pour assurer les actions de communication et de sensibilisation sur les enjeux de sécurité informatique de l'entreprise à l'ensemble du personnel (administrateurs, personnels de direction et utilisateurs), le technicien veilleur de cybersécurité doit faire preuve de diplomatie, d'écoute, d'un sens du dialogue et de persuasion, afin de convaincre les utilisateurs des risques encourus et du bien-fondé des procédures mises en place. Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.1. Participation au contrôle administratif et aux actions de conseil technique.	*Le technicien veilleur de cybersécurité est autonome dans l'exécution de ses tâches en manifestant de la rigueur et un souci du détail pour mener à bien la politique des droits d'accès*		
A.1.3 Inventaire du matériel.	- Effectuer le suivi comptable des matériels afin d'avoir une vision en temps réel de l'état de son matériel et procéder aux inventaires réglementaires pour répertorier physiquement les équipements à l'aide d'outils spécifiques.		- la comptabilité des matériels est tenue de façon rigoureuse. - la comptabilité des matériels est minutieusement mise à jour. -la mise en place d'un recensement périodique répond formellement à la réglementation en vigueur. -la chaîne de traçabilité du matériel est indispensablement tenue à jour.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 4 – Contrôler le droit d'accès au système et aux données de l'organisme, sensibiliser et former le personnel et conseiller l'officier de la sécurité des systèmes d'information de l'entreprise *Le technicien veilleur de cybersécurité doit démontrer de la rigueur et un sens de la méthode afin de conduire les habilitations des personnes non seulement pour maîtriser davantage les risques opérationnels liés aux autorisations réellement en vigueur dans la société, mais également pour répondre aux enjeux de conformité réglementaire.* *Pour assurer les actions de communication et de sensibilisation sur les enjeux de sécurité informatique de l'entreprise à l'ensemble du personnel (administrateurs, personnels de direction et utilisateurs), le technicien veilleur de cybersécurité doit faire preuve de diplomatie, d'écoute, d'un sens du dialogue et de persuasion, afin de convaincre les utilisateurs des risques encourus et du bien-des procédures mises en place. Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.2. Collaboration au travail de sensibilisation et de formation de l'ensemble du personnel à l'hygiène informatique et aux risques liés à la cybersécurité et amélioration de ses compétences	*Le technicien veilleur de cybersécurité dispose d'une réelle autonomie dans ses tâches en faisant preuve de pédagogie pour expliquer aux utilisateurs les règles à respecter pour ne pas mettre en danger le système d'information de l'entreprise*		
A.2.1 Sensibilisation des utilisateurs.	- Sensibiliser, par le biais de campagnes de sensibilisation et de séances périodiques, les utilisateurs du système d'information à l'hygiène informatique, aux bonnes pratiques en termes de cybersécurité et aux risques induits afin qu'ils deviennent le maillon fort dans la lutte contre les menaces propres à leur environnement de travail.	**<u>Voie formative</u> :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles.	- la sensibilisation des utilisateurs sur les risques associés à l'utilisation d'une ressource numérique non contrôlée est absolument adaptée. - la mise en avant des bons usages à adopter est réalisée intelligemment. - les utilisateurs sont sensibilisés sur les actions qui peuvent mettre en péril la sécurité. - la pédagogie employée est totalement adaptée à l'auditoire.
A.2.2 Formation et information.	- Contribuer à la mise en œuvre de bonnes pratiques, en proposant de nouvelles procédures, de nouvelles actions qui pourront recueillir l'engagement de tous à respecter les règles de sécurité du système d'information notamment en lien avec la politique de cybersécurité de l'entreprise.	**<u>VAE</u> :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	- les propositions sont fondamentalement réalistes afin d'établir un plan proactif de sensibilisation pour tous. - la formation du personnel en charge des systèmes d'information sur la gestion des incidents liés à la sécurité de l'information est menée intelligemment. - les utilisateurs sont absolument informés sur les procédures à suivre en cas d'incident de sécurité.

			- les utilisateurs sont informés régulièrement sur les risques provenant d'internet et sur les nouvelles menaces qui pèsent sur l'organisme.

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 (dont l'anglais éventuellement, selon les compétences requises)
BLOC DE COMPÉTENCES 4 – Contrôler le droit d'accès au système et aux données de l'organisme, sensibiliser et former le personnel et conseiller l'officier de la sécurité des systèmes d'information de l'entreprise *Le technicien veilleur de cybersécurité doit démontrer de la rigueur et un sens de la méthode afin de conduire les habilitations des personnes non seulement pour maîtriser davantage les risques opérationnels liés aux autorisations réellement en vigueur dans la société, mais également pour répondre aux enjeux de conformité réglementaire.* *Pour assurer les actions de communication et de sensibilisation sur les enjeux de sécurité informatique de l'entreprise à l'ensemble du personnel (administrateurs, personnels de direction et utilisateurs), le technicien veilleur de cybersécurité doit faire preuve de diplomatie, d'écoute, d'un sens du dialogue et de persuasion, afin de convaincre les utilisateurs des risques encourus et du bien-des procédures mises en place. Le technicien veilleur de cybersécurité peut être amené à faire usage de l'anglais selon les compétences requises.*			
A.2. Collaboration au travail de sensibilisation et de formation de l'ensemble du personnel à l'hygiène informatique et aux risques liés à la cybersécurité et amélioration de ses compétences.	*Le technicien veilleur de cybersécurité dispose d'une réelle autonomie dans ses tâches en faisant preuve de pédagogie pour expliquer aux utilisateurs les règles à respecter pour ne pas mettre en danger le système d'information de l'entreprise*		
A.2.3 Bilan du niveau de compétences acquises du personnel en matière de cybersécurité.	- Mesurer l'évolution du niveau de sensibilisation du personnel par le biais de mises en situation ou de questionnaires afin de consolider les résultats des différentes campagnes de cybersécurité.	**<u>Voie formative</u> :** - contrôles de connaissances ; - mises en situation contextualisées ; - études de cas et/ou de restitutions technico-opérationnelles. **<u>VAE</u> :** - étude du livret 2 ; - entretien avec le jury ; - mise en situation simulée ou réelle, si nécessaire	- l'appréciation du niveau de sensibilisation est définie intelligemment. - les outils (questionnaires, quizz, sondages…) mis en place ont permis exactement d'atteindre ce résultat. - la production d'indicateurs permet logiquement de consolider les résultats. - les actions mises en place permettent fondamentalement d'améliorer les compétences des utilisateurs. - les bilans du niveau de compétences acquises des personnels en matière de cybersécurité sont nécessairement exploités pour adapter les sensibilisations suivantes.