5 - REFERENTIELS

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**
Bloc 1 : Auditer la sécurité des systèmes d'informations et des systèmes industriels			
Activité 1 : Audit de la sécurité du système d'information et mise en place d'actions préventives en matière de cybersécurité industrielle ● Analyse des besoins de la structure et du S.I. existant ● Préparation du plan d'audit de sécurité du système d'information ● Déploiement des différents audits de la sécurité du système d'information	B1C1 : Analyser les besoins en cybersécurité des systèmes industriels à l'aide de la description des processus de l'entreprise et d'analyses afin d'appliquer les bonnes pratiques pour la sécurité du système d'information.	**Bloc 1 - Épreuve 1 : Rapport écrit** A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, le candidat sera chargé de la réalisation d'un audit de sécurité d'un système d'information industriel. Le candidat sera chargé de rédiger un rapport d'audit contenant les éléments suivants : ● La note de cadrage de l'audit ; ● Le champ de l'audit ; ● La méthodologie d'audit ; ● La synthèse des résultats de l'audit ● Le détail des résultats de l'audit (liste des contrôles effectués, identification des bonnes pratiques) ● La matrice des risques ; ● Le plan d'action proposé ; ● L'état de maturité de la sécurité du système d'information Le rapport sera rédigé en français et présentera une structure organisée avec	Le candidat : ● Rédige une présentation de la structure étudiée conforme ● Réalise une cartographie du système d'information étudié complète : applications, serveurs, infrastructure réseau, équipements de sécurité, postes de travail ● Liste des besoins de sécurité cohérents sur les différentes vues du système d'information étudié ● Réalise une synthèse cohérente des besoins de la structure étudiée ● La restitution est conforme aux normes attendues de rédaction d'un document professionnel de type document long.
	B1C2 : Définir un plan d'audit adapté en termes de moyens, ressources, organisation et contraintes réglementaires afin de déterminer précisément les failles et non conformités du système d'information.		Le candidat : ● Décrit la méthodologie d'audit adoptée de façon conforme ● Inclut une description conforme des éventuels référentiels ou normes applicables.
	B1C3 : Analyser les écarts au regard des référentiels, processus et procédures définis au plan d'audit afin de mettre en place un plan d'actions correctives et/ou préventives pour améliorer la sécurité du système d'information.		Le candidat : ● Présente une méthodologie de cartographie des risques cohérente par rapport à la situation de l'entreprise et argumentée ● Liste les défauts de sécurité

<table>
<tr><td></td><td></td><td>un sommaire.

Au rapport sera associée d'une synthèse soutenue à l'oral d'une durée de 30 minutes.</td><td>constatés en cohérence avec le périmètre étudié
● Propose des actions argumentées en cohérence avec le périmètre étudié pour chaque élément du plan d'action listé</td></tr>
<tr><td></td><td>B1C4 : Établir un plan d'action comportant les mesures techniques et organisationnelles pour corriger les non conformités afin de remédier efficacement aux failles de sécurité et non conformités en mettant en place une stratégie adaptée aux besoins de l'entreprise.</td><td></td><td>Le candidat :
● Présente au minimum une entrée extraite d'une base de connaissance
● Propose une estimation du niveau de sécurité atteint par les configurations et outils proposés pertinent par rapport aux objectifs de sécurité de la structure</td></tr>
<tr><td colspan="4">Bloc 2 : Assurer la gestion opérationnelle de la cybersécurité du système d'information et des systèmes industriels</td></tr>
<tr><td rowspan="2">Activité 2 : Supervision des systèmes d'informations industriels

● Gestion et qualification des alertes de sécurité
● Investigation et traitement des incidents de sécurité
● Gestion de crise de cybersécurité
● Amélioration des capacités de défense et de réaction</td><td>B2C1 : Superviser la sécurité des systèmes industriels en mettant en place des outils logiciels adéquats afin d'établir une surveillance la plus complète et à jour possible de la sécurité du système d'information.</td><td rowspan="2">Bloc 2 - Épreuve 1 : Rapport écrit :
A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, portant sur la mise en application de concepts de gestion des risques et des vulnérabilités au sein d'un système industriel.
Le candidat sera chargé d'établir un rapport d'analyse des risques et des vulnérabilités contenant les éléments suivants :

● Identification des scénarios pris en compte
● Dresser la liste des risques
● Dresser la liste des vulnérabilités
● Règles de surveillance du système de supervision
● Plan de remédiation

Le rapport sera rédigé en français et présentera une structure organisée avec un sommaire.</td><td>Le candidat :
● Rédige une stratégie de supervision adaptée au contexte de sécurité de la structure
● Propose une architecture de supervision cohérente par rapport au contexte technique de la structure étudiée
● Propose des outils de supervision adaptés à l'architecture proposée</td></tr>
<tr><td>B2C2 : Évaluer les risques de sécurité spécifiques aux environnements industriels en les identifiants à l'aide de méthodes adaptées à l'environnement et aux moyens de l'entreprise afin de préparer des mesures de réduction de l'impact lié à ces risques.</td><td>Le candidat présente dans son rapport :
● Une méthode d'analyses de risques cohérente par rapport à la situation de l'entreprise
● L'analyse des risques de sécurité par processus ou par entité y compris la description des échelles utilisées et leurs justifications
● Un plan de traitement des risques et matrices associées modélisant la réduction des risques</td></tr>
</table>

			identifiés à un niveau acceptable pour l'organisation
	B2C3 : Évaluer les vulnérabilités des systèmes informatiques et informatiques industriels à l'aide d'outils spécifiques afin de déterminer le niveau de criticité attribué à chaque vulnérabilité détectée.		Le candidat présente un rapport contenant : ● Une méthode d'analyses des vulnérabilités adaptée au contexte étudié ● Une liste cohérente des vulnérabilités identifiées par rapport au périmètre étudié ● Une liste des scénarios d'exploitation ou scénarios opérationnels correspondants au scénario étudié ● Un plan de traitement des vulnérabilités permettant d'atteindre un niveau de sécurité pertinent par rapport aux objectifs de la structure.
	B2C4 : Détecter les alertes de sécurité à l'aide de la mise en place d'outils et services du système de gestion des événements de la sécurité afin de tenter de détecter les activités suspectes et d'atténuer les menaces.		Le candidat présente une liste de règles de détection permettant de détecter des attaques prédéfinies dans le jeu de données étudiées.
	B2C5 : Gérer des mesures de contournements et/ou un plan de remédiation en s'appuyant sur des solutions techniques précédemment identifiées afin de pallier à de nouvelles occurrences des incidents de sécurité.		● Le candidat a identifié une liste d'actions techniques et/ou organisationnelles de remédiation en cohérence avec le contexte exposé. ● Les actions identifiées sont détaillées, chiffrées et priorisées. (les éléments chiffrées sont juste et les priorités proposées sont adaptées)
	B2C6 : Mener une investigation numérique à l'aide des outils de mesures adéquats en recherchant les causes racines afin de gérer les incidents de sécurité.	**Bloc 2 - Épreuve 2 - Mise en situation professionnelle reconstituée :** Evaluation des compétences à partir d'une mise en situation réelle de travail portant sur la réalisation d'une investigation numérique réalisée sur l'environnement Root-Me PRO (environnements non simulés proposant des challenges). A partir d'un scénario proposé sur la	Le candidat réalise une enquête numérique et trouve le mot de passe lui permettant d'identifier la personne à l'origine de l'attaque.

		plateforme, le candidat réalise différentes analyses à partir des traces disponibles sur un système compromis.	
	B2C7 : Assurer l'amélioration continue des dispositifs de sécurité au moyen d'indicateurs évalués en fonction d'objectifs à atteindre afin de maintenir un niveau de sécurité adapté et assurer la performance du processus de sécurisation de façon continue (ressources humaines et outils de l'entreprise)	**Bloc 2 - Epreuve 3 - Présentation orale** A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, le candidat sera chargé de créer un tableau de bord composé d'indicateurs de sécurité informatique. Le candidat argumente le contenu de son tableau de bord par une présentation à l'oral de 10 minutes.	● Le candidat a identifié dans sa présentation les sources de données adéquates correspondantes aux indicateurs. ● Le candidat a validé une mise à disposition technique correcte des sources de données identifiées. ● La présentation démontre la pertinence des choix des indicateurs sélectionnés eu égard au scénario étudié. ● Le candidat a identifié de façon correcte les parties prenantes au projet. ● Le candidat propose quatre points de contrôle liés à la sécurité informatique cohérents eu égard au scénario proposé.
	B2C8 : Définir les modalités de gestion de crise en mobilisant les ressources techniques et humaines afin d'améliorer les capacités de défense et de réaction de la structure.	**Bloc 2 - Épreuve 4 - Conception et présentation d'un plan de gestion :** A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, le candidat prépare un plan de gestion de crise contenant : ● Propositions de stratégie de gestion de crise ● Fiches réflexes ● Plan de communication par type de parties concernées Le candidat présentera son plan de gestion de crise lors d'un exercice de présentation orale de 20 minutes.	● Le candidat propose la mise en place de mesures garantissant un niveau adapté de résilience eu égard au scénario étudié. ● Le candidat propose un plan permettant l'adaptation de sa structure au fonctionnement en mode de crise cyber : la chaîne d'alerte est formalisée, les critères d'activation sont cohérents par rapport au cahier des charges, les fonctions décisionnelles sont correctement identifiées
	B2C9 : Assurer la communication de crise en formalisant le processus de réponse aux incidents de sécurité afin d'informer efficacement les parties concernées internes et externes et contribuer à limiter les effets néfastes pour l'entreprise.		● Le plan de communication proposé par le candidat tient compte des différents types d'utilisateurs de la structure et propose des actions adaptées en conséquence. ● La liste des parties prenantes à alerter et des contacts d'urgence est cohérente avec les caractéristiques et activités de la structure étudiée. ● Le plan de communication

			présente les actions de simulation adéquates pour améliorer la réponse de la structure à la survenue d'une crise.
Bloc 3 : Conseiller la structure en cybersécurité et organiser sa mise en œuvre			
Activité 3 : Conseil et mise en place des méthodes de gestion et d'organisation de la sécurité des systèmes d'information industriels ● Accompagnement à l'élaboration d'un système de management de la sécurité ● Accompagnement à la certification de systèmes d'informations sensibles ● Définition et mis en place de politiques de sécurité ● Formation et sensibilisation des collaborateurs	B3C1 : Analyser les contraintes fonctionnelles et/ou organisationnelles des systèmes industriels afin d'intégrer les contraintes spécifiques de ces systèmes à la politique de sécurité.	**Bloc 3 - Épreuve 1 : Rédaction de document :** A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, le candidat sera chargé de rédiger une politique de sécurité des systèmes d'information contenant les éléments suivants : ● Analyse des contraintes métiers et réglementaires ● Liste des besoins de sécurité pour la protection de son patrimoine numérique ● Adaptation des processus de sécurité aux menaces et contraintes listées Le document sera rédigé en anglais.	● Le candidat a identifié l'ensemble des contraintes fonctionnelles et organisationnelles de l'environnement étudié. ● Les analyses tiennent compte de l'organisation, de l'environnement réglementaire, des menaces propres au contexte métier.
	B3C2 : Collecter les informations auprès des directions métiers, des services qualité afin d'alimenter des processus de la sécurité informatique et informatique industrielle en cohérence avec les processus et besoins métiers de l'entreprise.		Dans le document rendu, le candidat ● Le candidat a collecté les informations utiles à l'analyse des contraintes métiers et réglementaires. ● Le candidat a renseigné des grilles d'entretien conformes au périmètre étudié.
	B3C3 : Définir la politique de sécurité de l'entreprise à l'aide des différents acteurs et en tenant compte des contraintes internes et externes afin de maximiser la sécurité informatique		● Le candidat présente un document de politique de sécurité qui identifie les enjeux globaux pour la structure étudiée ● Le candidat formalise les exigences de sécurité par grands domaines. ● Le candidat présente un document opérationnel d'exigences de sécurité au regard du scénario étudié.
	B3C4 : Définir la stratégie de sécurité des systèmes d'information industriels à l'aide des différentes analyses d'enjeux, objectifs, procédures existantes afin de s'aligner avec la stratégie de l'entreprise et assurer la sécurité du capital informationnel.	**Bloc 3 - Epreuve 2 : Rédaction de document** A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive portant sur la mise en application de la stratégie de gouvernance de la sécurité des systèmes d'information, le candidat sera chargé de rédiger un document présentant la stratégie de sécurité des	● Le candidat a réalisé les analyses techniques et métiers de façon complète et cohérente par rapport au périmètre étudié. ● Les analyses permettent de hiérarchiser les besoins de sécurité en lien avec les risques spécifiques au contexte exposé. ● Le candidat a défini une cible de sécurité à atteindre en pertinence par rapport au contexte exposé.

		systèmes d'information contenant les éléments suivants : ● Synthèse des analyses techniques et métiers ● Définition de la cible à atteindre ● Liste des projets à réaliser ordonnés dans le temps pour atteindre la cible	● Une stratégie cohérente et chiffrée est définie pour atteindre la cible. ● La stratégie comprend la liste des projets à réaliser, ceux-ci étant hiérarchisés et qualifiés en termes de complexité et de ressources à engager.
	B3C5 : Assurer la continuité d'activité des systèmes industriels en concevant un plan de continuité et de reprise d'activité afin de limiter les effets d'incidents de sécurité sur le fonctionnement normal de l'entreprise.	**Bloc 3 - Épreuve 3 - Rapport écrit :** A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive portant sur la mise en œuvre de plan de continuité et de reprise d'activité, le candidat sera chargé de rédiger une proposition de plan de continuité d'activité contenant : ● Liste des activités essentielles à la continuité d'activité de l'entreprise. ● Choix argumenté du périmètre fonctionnel du plan ● Une matrice d'analyse de risques avec calcul argumenté de la criticité ● La définition des solutions de secours ● Les seuils de déclenchement du plan ● Une procédure de secours informatique ● Le plan de test du PCA Le rapport sera rédigé en français et présentera une structure organisée avec un sommaire.	● Le candidat a identifié l'ensemble des activités essentielles cohérentes par rapport au périmètre étudié. ● Le plan présente uniquement les besoins strictement nécessaires de la structure pour fonctionner en mode dégradé. ● Le candidat a hiérarchisé les risques et a identifié les bons scénarios et les risques prioritaires de façon cohérente. ● Le plan ne se limite pas à un plan de secours informatique ● Les seuils de déclenchement du plan sont justement calculés pour éviter une mise en œuvre hors champ d'application ● Le candidat mentionne le plan qu'il prévoit de mettre en place pour permettre à la structure de se préparer en cas de survenue d'une crise via des actions d'entraînement à fréquence suffisante ● La restitution est conforme aux normes attendues de rédaction d'un document professionnel de type document long.
	B3C6 : Sensibiliser les acteurs et les utilisateurs à la cybersécurité à l'aide d'un plan de formation des équipes techniques et non techniques pour améliorer leur niveau de compréhension des problématiques de sécurité informatique et informatique industrielle.	**Bloc 3 - Épreuve 4 : Présentation orale** A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive portant sur les actions de formation et de communication de	Le candidat démontre dans sa présentation : ● Qu'il a identifié les parties prenantes en cohérence avec la structure étudiée ● Qu'il a ciblé les actions en fonction

		sécurité informatique, le candidat sera chargé de présenter un plan d'actions de sensibilisation du personnel : ● Liste des actions de sensibilisation ● Liste des actions de formation ● Parties prenantes ● Ressources à mettre en œuvre ● Planning de réalisation, fréquence ● Objectifs attendus Le candidat résume son plan dans une présentation orale de 20 minutes.	des catégories de collaborateurs et du niveau de vigilance qui leur est demandé La présentation démontre que les enjeux listés sont en cohérence avec les caractéristiques de la structure étudiée, de son système d'information et de son patrimoine (numérique, industriel…) Les durées et fréquences des actions proposées sont exactes et cohérentes au regard des bonnes pratiques admises
Bloc 4 : Assurer la mise en œuvre des solutions en cybersécurité technique des systèmes d'informations et systèmes industriels			
Activité 4 : Déploiement et administration de l'architecture fonctionnelle et technique de sécurité ● Planification et séquençage du projet de cybersécurité industriel ● Déploiement d'une Architecture technique de sécurité ● Sécurisation des systèmes, services, réseaux et applications ● Mise en place de la veille technique en sécurité système, services, réseaux et applicatifs d'infrastructure et industriels.	B4C1 : Mettre en œuvre des solutions de correction ou de prévention en s'appuyant sur les standards de la sécurité afin de garantir un niveau adapté de sécurité du système d'informations.	**Bloc 4 - Epreuve 1 - Mise en situation professionnelle reconstituée :** Évaluation des compétences à partir d'une mise en situation réelle de travail s'appuyant sur un environnement technique vulnérable à protéger et d'une description associée. Le candidat sera chargé de réaliser une maquette fonctionnelle d'une solution de correction ou de prévention sur l'environnement technique étudié (sous forme de machines virtuelles).	Le candidat réalise une démonstration sur l'environnement technique installé afin de prouver que la solution proposée : ● Permette de corriger les vulnérabilités existantes ● Permette de limiter l'accès aux utilisateurs autorisés ● Permette de surveiller les flux de communication ● Permette de surveiller les traces générées sur les systèmes et applications de l'environnement
	B4C2 : Concevoir une architecture sécurisée système et réseau d'un système d'information industriel à l'aide des bonnes pratiques, de tests, de mesures, d'outils techniques au niveau réseau et système afin d'aligner les infrastructures aux besoins et à la stratégie de sécurité de l'entreprise.	**Bloc 4 - Épreuve 2 - Mise en situation professionnelle reconstituée :** Evaluation des compétences à partir d'une mise en situation réelle de travail portant sur la réalisation d'exploitation de vulnérabilités sur l'environnement Root-Me PRO (environnements non simulés proposant des challenges). A partir d'un scénario proposé sur la plateforme, le candidat réalise différentes analyses et exploitations afin de prendre le contrôle de l'environnement.	● Le candidat présente la liste des scénarios d'exploitation mis en œuvre et des résultats obtenus. ● Sur la base des scénarios mis en œuvre, le candidat présente l'architecture cible à mettre en œuvre pour réduire les vulnérabilités identifiées dans les scénarios. ● Le candidat détaille la liste des mesures de correction ou de prévention à mettre en place en les hiérarchisant par niveau de priorité.

	B4C3 : Concevoir une architecture sécurisée applicative et de données d'un système d'information industriel à l'aide des bonnes pratiques, de tests, de mesures, d'outils techniques au niveau applicatif et données afin d'aligner les infrastructures aux besoins et à la stratégie de sécurité de l'entreprise.		Le candidat présente un rapport contenant l'intégralité des informations suivantes : ● Description des architectures et méthodes de sécurisation des systèmes et réseaux ● Proposition de solutions de sécurité (chaque proposition devra être argumentée fonctionnellement ou financièrement)
	B4C4 : Concevoir des solutions techniques adaptées aux contraintes et spécificités des systèmes industriels afin de sécuriser les infrastructures en tenant compte des environnements des entreprises industrielles.		Le candidat présente un rapport contenant l'intégralité des informations suivantes : ● Indicateurs et tableaux de bord selon les dimensions opérationnelles et stratégiques ● Niveau de sécurité des configurations mises en œuvre ● Modalités d'exploitation des solutions de cybersécurité
	B4C5 : Intégrer des solutions de cybersécurité pour l'infrastructure informatique et l'informatique industrielle afin de mettre en œuvre une architecture sécurisée du système d'information de l'organisation.	**Bloc 4 - Epreuve 3 - Mise en situation professionnelle reconstituée :** Évaluation des compétences à partir d'une mise en situation réelle de travail s'appuyant sur un environnement technique vulnérable à protéger et d'une description associée. Le candidat sera chargé de réaliser une maquette fonctionnelle d'outils de sécurité pour le renforcement d'une architecture informatique vulnérable (sous forme de machines virtuelles).	• La configuration de la solution maquettée respecte les standards préconisés l'éditeur/le concepteur de ladite solution. • La configuration présente un niveau de sécurité conforme au cas étudié • La solution permet le renforcement de l'infrastructure étudiée • La maquette contient une description conforme de l'architecture système et réseau étudiée
	B4C6 : Administrer les solutions de cybersécurité du système d'information industriel à l'aide des éléments de la politique de sécurité de l'entreprise afin d'assurer le fonctionnement opérationnel des systèmes vitaux de l'organisation.	**Bloc 4 - Epreuve 4 : Questionnaire à choix Multiples** : Évaluation de compétences sous forme de test se présentant sous la forme d'une question/affirmation suivie de plusieurs propositions de réponses, parmi lesquelles se trouve(nt) une ou plusieurs réponse(s) correcte(s). Ce QCM est composé de questions autour des manipulations permettant de vérifier des compétences d'administration conformes des principales solutions informatiques de sécurité	Le candidat obtient un minimum de 70 % de réponses correctes au QCM.

<table>
<tr><th colspan="4">Bloc 5 : Piloter la cybersécurité du système d’informations et des systèmes industriels</th></tr>
<tr><td rowspan="4">Activité : Pilotage de la cybersécurité et conception des éléments de politique de cybersécurité
Mise en place des documents de pilotage et des outils de travail collaboratif
Management d'équipe interne et externe à l'entreprise
Assurer une veille technologique et réglementaire
Assurer la prise en compte des aspects sécurité liés à la gestion de projets</td><td>B5C1 : Gérer les différents outils collaboratifs nécessaires à la collaboration et au partage d’informations afin d’assurer la bonne diffusion des informations liées à la sécurité du capital informationnel de l'entreprise auprès de l’ensemble des collaborateurs, nourrir les profils compétences des collaborateurs et ainsi contribuer à la capitalisation des compétences.</td><td rowspan="4">Bloc 5 - Épreuve 1 - Mise en situation professionnelle reconstituée :
Evaluation des compétences à partir d’une mise en situation réelle de travail à partir d’un cahier des charges présentant le besoin d’une entreprise fictive portant sur la mise en œuvre d’outils collaboratifs. Le candidat conçoit une maquette fonctionnelle permettant de gérer et sécuriser l’accès à différents outils collaboratifs contenant à minima :
Un jeu de métadonnées pour caractériser les données
Un système de gestion des documents
Un système de gestion des projets
Un système de communication interne
Un système de support et d’assistance semi-automatisée</td><td>Le candidat propose une maquette basée sur un outil permettant de créer une interface avec une expérience utilisateur moderne, en cohérence avec les applicatifs collaboratifs actuels
La solution proposée présente un jeu de métadonnées cohérent par rapport au périmètre étudié</td></tr>
<tr><td>B5C2 : Organiser les interventions des équipes à l’aide d’outils et méthodes appropriées de gestion de projets et techniques de communication afin d’améliorer la coordination des différentes composantes opérationnelles et décisionnelles de l’entreprise.</td><td>Le candidat propose un outil de gestion de projet collaboratif adapté à la gestion de projet
L’outil doit permettre de gérer les interventions, les plannings, les temps et les communications.
Des notifications automatiques par mail sont justement paramétrées.</td></tr>
<tr><td>B5C3 : Gérer les ressources nécessaires à la sécurité des systèmes d’information industriels à l’aide des procédures de sécurité afin d’optimiser la sécurité et de contribuer au pilotage de l’entreprise.</td><td>Le candidat présente une maquette pleinement fonctionnelle d’un outil de support (configuration initiale réalisée, maquette utilisable)
Différents cas d’assistance et niveaux d’urgence sont prévus afin d’optimiser les traitements des demandes.
Des notifications automatiques par mail sont justement paramétrées.</td></tr>
<tr><td>B5C4 : Assurer la communication interne et externe en matière de sécurité de l'information à l’aide des outils dont l’entreprise est équipée, de plans de communication, de rapports d’activités afin d’atteindre la bonne application des mesures et prévenir les pratiques inadaptées en matière de sécurité des systèmes d’information.</td><td>Le candidat propose un outil collaboratif permettant le partage de documents et d’informations entre des utilisateurs internes et externes.
L’outil doit permettre de rédiger des nouveaux contenus et d’importer des fichiers.
L’outil intègre la possibilité de communiquer sur différents canaux
L’outil inclut des mécanismes de sécurité respectant le principe de moindre privilège.</td></tr>
</table>

	B5C5 : Assurer une veille technique en utilisant les outils adaptés afin d'alimenter une base de ressources sur l'évolution des menaces et les méthodes utilisées ainsi que de leurs effets potentiels.	**Bloc 5 - Épreuve 3 : Mise en situation professionnelle reconstituée.** Évaluation des compétences à partir d'une mise en situation réelle de travail s'appuyant sur un environnement technique à déployer pour l'industrialisation du processus de veille technique. Le candidat sera chargé de réaliser une maquette fonctionnelle d'une plateforme technique choisie parmi les solutions open source du marché (sous forme de machines virtuelles).	Le candidat conçoit une maquette fonctionnelle et démontre que les outils déployés et configurés permettent : ● La consultation d'une plateforme de réponses à incidents ● D'alimenter une base de données de tous les artefacts liés à des actes suspects ou malveillants ● De garder une trace de tous les flux de menaces relevés ● D'automatiser les différents messages qui peuvent remplir la base de connaissances.
	B5C6 : Mener des actions de veille réglementaire en utilisant les outils adaptés afin de garantir un niveau de sécurité du système d'information conforme aux exigences associées.	**Bloc 5 - Épreuve 4 : Rapport écrit** A partir d'une étude de cas fournie sous forme d'un cahier des charges présentant le besoin d'une entreprise fictive, le candidat présente un rapport de veille réglementaire en lien avec le contexte présenté et conforme aux exigences légales et réglementaires. ● Eléments réglementaires en lien avec l'activité du cas présenté. ● Eléments de protection des données personnelles si besoin est Le rapport sera rédigé en français et présentera une structure organisée avec un sommaire.	● Le candidat présente dans son rapport des sources d'information fiables, en cohérence avec le périmètre réglementaire étudié. ● Le candidat a correctement identifié les risques liés au contexte cible. ● L'information collectée apporte des éléments factuels ● La restitution est conforme aux normes attendues de rédaction d'un document professionnel de type document long.