Référentiel de certification

Responsable en cybersécurité	
Bloc n°1	**Piloter la cyberprotection des systèmes et réseaux informatiques** ▪ Appuyer le responsable de la sécurité des systèmes d'information (RSSI) ou le directeur des systèmes d'information (DSI) ▪ Contribuer à l'amélioration de la sécurité technique du système d'information ▪ Administrer la sécurité des systèmes et des éléments actifs réseau
Bloc n°2	**Contrôler et auditer le niveau de cybersécurité d'un système d'information** ▪ Évaluer le niveau de conformité d'un système d'information ▪ Éprouver le niveau de sécurité d'un système d'information ▪ Proposer un plan d'action à l'issue d'un audit
Bloc n°3	**Superviser la cybersécurité des systèmes d'information** ▪ Diriger l'action d'une équipe de techniciens au sein d'un centre de supervision ▪ Améliorer les dispositifs de détection ▪ Diriger les différentes phases de réponse sur incident dans le périmètre d'un centre de supervision ▪ Assurer la formation du personnel
Bloc n°4	**Conduire une investigation numérique dans le domaine de la cybersécurité** ▪ Mener des investigations en réponse sur incident ▪ Capitaliser le résultat des investigations

Bloc n°1 : Piloter la cyberprotection des systèmes et réseaux informatiques (1/2)			
RÉFÉRENTIEL D'ACTIVITÉS ET DE COMPETENCES		RÉFÉRENTIEL D'EVALUATION	
ACTIVITÉS	COMPÉTENCES	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<u>Activité 1.1 :</u> **Assurer la sécurité organisationnelle et technique**	**C1 : Appuyer le responsable de la sécurité des systèmes d'information (RSSI) ou le directeur des systèmes d'information (DSI)** ▪ contribuer à l'élaboration des moyens et procédures CYBER au profit d'une ou plusieurs autorités qualifiées et autorités d'emploi ; ▪ concourir à la rédaction des documents réglementaires d'organisation et de conduite de la cybersécurité de l'entité d'emploi ; ▪ organiser, conduire et contrôler la mise en œuvre des mesures locales CYBER ; ▪ préparer son unité à une homologation et/ou contrôle d'un système d'information ; ▪ évaluer et rendre compte du niveau de sécurité organisationnel du périmètre d'emploi ; ▪ conduire l'analyse des risques pesant sur un périmètre informatique défini ; ▪ réaliser et animer des séances de sensibilisation au profit des utilisateurs et des administrateurs ; ▪ conseiller le directeur de l'entité sur les actions de cyberprotection. **C2 : Contribuer à l'amélioration de la sécurité technique du système d'information** ▪ assurer une veille technologique et le suivi des études amont du domaine cyber ; ▪ anticiper et proposer les nouveaux besoins cyber relatifs à son périmètre de responsabilité ; ▪ évaluer et rendre compte du niveau de sécurité technique du périmètre d'emploi ; ▪ développer les compétences en cybersécurité des administrateurs et des utilisateurs des systèmes informatiques ; ▪ proposer les solutions de chiffrement adaptées au niveau de sécurité attendu.	**<u>Par formation</u>** Epreuves écrites, orales et mises en situation professionnelles visant à démontrer la capacité du candidat à assurer la gouvernance de la sécurité des systèmes et réseaux informatiques **<u>Par VAE :</u>** Étude du livret II et entretien avec le jury visant à démontrer la capacité du candidat à assurer la gouvernance de la sécurité des systèmes et réseaux informatiques.	Le candidat : ▪ s'appuie sur ses connaissances étendues de la réglementation en matière de cybersécurité pour assister la direction des systèmes d'information (DSI) dans la rédaction des documents internes cadrant la sécurité informatique ou de rédiger des déclinaisons spécifiques ; ▪ assure un suivi longitudinal du respect de l'application des mesures de sécurité à partir duquel il établit des mesures correctives et des indicateurs relatifs au niveau de sécurité des SI ; ▪ mène une analyse de risque au standard EBIOS en vue de conduire une démarche d'homologation ou de vérifier la conformité avec un référentiel de sécurité numérique. ; ▪ organise et anime des séances de sensibilisation particularisées en fonction de son auditoire (utilisateur, administrateurs, concepteur …) ; ▪ définit et met en place un processus de veille technologique pertinent vis-à-vis des actifs permettant d'anticiper les futurs menaces et préparer les contre-mesures ; ▪ assiste les équipes projets pour identifier les solutions de sécurité les plus pertinentes vis-à-vis des exigences de sécurité et en valide l'implémentation.

Bloc n°1 : Piloter la cyberprotection des systèmes et réseaux informatiques (2/2)			
RÉFÉRENTIEL D'ACTIVITÉS ET DE COMPETENCES		RÉFÉRENTIEL D'EVALUATION	
ACTIVITÉS	COMPÉTENCES	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<u>Activité 1.2:</u> **Assurer l'administration de la sécurité des systèmes et du réseau**	**C3 : Administrer la sécurité des systèmes et des éléments actifs réseau** ▪ proposer ou développer les outils et procédures de sécurisation des architectures réseaux et les services associés ; ▪ définir et mettre en œuvre les règles et outils d'administration sécurisés ; ▪ définir et appliquer la politique technique de gestion des droits d'accès aux ressources informatiques ; ▪ exploiter et préserver les journaux d'évènements des systèmes ; ▪ appliquer les mesures prioritaires de lutte informatique défensive en réaction à un incident de sécurité ; ▪ établir et diffuser un compte-rendu d'incident précis ; ▪ apporter un soutien technique aux actions de résolution des incidents de sécurité ; ▪ concourir aux processus de lutte informatique défensive.	**<u>Par formation</u>** Épreuves écrites, orales et mises en situation professionnelles visant à démontrer la capacité du candidat à assurer la gouvernance de la sécurité des systèmes et réseaux informatiques **<u>Par VAE :</u>** Étude du livret II et entretien avec le jury visant à démontrer la capacité du candidat à assurer la gouvernance de la sécurité des systèmes et réseaux informatiques.	Le candidat : ▪ maitrise les principes d'utilisation et de fonctionnement des principaux équipements (firewall, équipement de chiffrement …) et produits de sécurité (antivirus, HIDS …) ; ▪ définit les règles de configuration des équipements de sécurité et valide avec les administrateurs système, les stratégies de sécurité et des autres composants du système d'information ; ▪ rédige les procédures d'exploitation sécurisée adaptées en cohérence avec la politique de sécurité de l'entreprise et des guides de sécurisation (ANSSI, NIST, CIS …) ; ▪ centralise et analyse l'ensemble des évènements de sécurité remontés par les composants des systèmes d'information placés sous sa responsabilité pour identifier des incidents relevant de la cybersécurité ; ▪ applique et coordonne les mesures de réaction immédiates suite à la découverte d'un incident cyber et garantit la conservation des preuves en vue d'une éventuelle judiciarisation ou intervention d'une équipe de réponse sur incident.

Bloc n°2 : Contrôler et auditer le niveau de cybersécurité d'un système d'information (1/2)			
RÉFÉRENTIEL D'ACTIVITÉS ET DE COMPETENCES		RÉFÉRENTIEL D'EVALUATION	
ACTIVITÉS	COMPÉTENCES	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<u>Activité 2.1 :</u> **Contrôler et auditer un système d'information**	**C4 : Évaluer le niveau de conformité d'un système d'information** ▪ constituer et maintenir à jour les référentiels techniques et organisationnels à appliquer lors de conduite des audits de sécurité ; ▪ assurer une veille technologique active sur les risques pesant sur les systèmes informatiques du ministère des armées ; ▪ mener seul ou en équipe une investigation technique sur un périmètre défini ; ▪ mener seul ou en équipe une investigation liée à l'environnement technique du système d'information ; ▪ mener seul ou en équipe une investigation liée à l'environnement organisationnel d'un système d'information ; ▪ conduire sur plateforme des tests et études de produits de sécurité afférents aux audits techniques ; ▪ élaborer les synthèses et rédiger les rapports d'audit et contrôle ; **C5 : Éprouver le niveau de sécurité d'un système d'information** ▪ réaliser des tests d'intrusion sur un système informatique ▪ rédiger un rapport de test d'intrusion technique.	**<u>Par formation</u>** Épreuves écrites, orales et mises en situation professionnelles visant à démontrer la capacité du candidat à évaluer et identifier les non-conformités et les vulnérabilités d'un système d'information et de proposer un plan de remédiation **<u>Par VAE :</u>** Étude du livret II et entretien avec le jury visant à démontrer la capacité du candidat à évaluer et identifier les non-conformités et les vulnérabilités d'un système d'information et de proposer un plan de remédiation.	Le candidat : ▪ maintient à jour ses connaissances de la réglementation, des lois applicables en matière de sécurité informatique et de la norme ISO 27002 pour délivrer des avis pertinents, argumentés et au plus proche de l'état de l'art; ▪ se réfère aux principaux schémas d'attaque d'un système informatique pour identifier les vulnérabilités exploitables des systèmes étudiés ; ▪ identifie de manière détaillée les non-conformités techniques ou organisationnelles d'un système d'information par rapport à un référentiel établi ; ▪ éprouve la sécurité d'un système en utilisant ses connaissances des techniques et procédures de PENTEST ; ▪ rédige des rapports précisant : la liste des non-conformité et/ou des vulnérabilités constatées et établis des recommandations adaptées en faisant preuve d'une bonne aisance rédactionnelle en français et en anglais.

Bloc n°2 : Contrôler et auditer le niveau de cybersécurité d'un système d'information (2/2)			
RÉFÉRENTIEL D'ACTIVITÉS ET DE COMPETENCES		RÉFÉRENTIEL D'EVALUATION	
ACTIVITÉS	COMPÉTENCES	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<u>Activité 2.2 :</u> **Conseiller le chef de l'organisme sur les actions à mener suite à un audit**	**C6 : Proposer un plan d'action à l'issue d'un audit** ▪ identifier et formaliser les non-conformités des systèmes et organisations par rapport à un référentiel défini ; ▪ proposer les évolutions nécessaires à la mise en conformité de l'organisation ou du système d'information contrôlé ; ▪ concevoir les tableaux de suivi des actions demandées suite à audit ou contrôle ; ▪ proposer les évolutions de codes informatiques requis pour accroître le niveau de sécurité applicatif ; ▪ proposer des évolutions techniques sur le paramétrage et la configuration des équipements du système d'information ; ▪ communiquer et argumenter de manière adaptée selon l'interlocuteur.	**<u>Par formation</u>** Épreuves écrites, orales et mises en situation professionnelles visant à démontrer la capacité du candidat à évaluer et identifier les non-conformités et les vulnérabilités d'un système d'information et de proposer un plan de remédiation **<u>Par VAE :</u>** Étude du livret II et entretien avec le jury visant à démontrer la capacité du candidat à évaluer et identifier les non-conformités et les vulnérabilités d'un système d'information et de proposer un plan de remédiation.	Le candidat : ▪ s'appuie sur le rapport d'audit pour identifier l'ensemble des non-conformités à traiter ; ▪ propose des axes d'amélioration technique et organisationnelle réalistes en fonction des contraintes propres à chacune des activités concernées par ces non-conformités ; ▪ conçoit des indicateurs pertinents et précis permettant d'informer les acteurs concernés sur le niveau de sécurité et l'état d'avancement des actions de remédiation.

Bloc n°3 : Superviser la cybersécurité des systèmes d'information (1/3)			
RÉFÉRENTIEL D'ACTIVITÉS ET DE COMPETENCES		RÉFÉRENTIEL D'EVALUATION	
ACTIVITÉS	COMPÉTENCES	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<u>Activité 3.1 :</u> **Coordonner les recherches dans l'identification des incidents de cybersécurité**	**C7 : Diriger l'action d'une équipe de techniciens au sein d'un centre de supervision** ▪ exploiter des systèmes de cybersurveillance et de détection d'événements de sécurité ; ▪ conduire une recherche des éléments précurseurs d'une agression informatique ; ▪ interpréter les détections afin de qualifier un incident ; ▪ compléter au besoin les travaux des techniciens en cybersécurité ; ▪ croiser les constats avec d'autres sources ou d'autres informations ; **C8 : Améliorer les dispositifs de détection** ▪ réaliser une veille technologique sur les menaces et les vulnérabilités des systèmes ; ▪ rédiger des règles de détection pour répondre à de nouvelles menaces. ▪ maintenir à jour le catalogue des indicateurs de compromission ▪ caractériser la menace en s'appuyant sur une bonne connaissance régulièrement mis à jour des MOA adverses	**<u>Par formation</u>** Épreuves écrites, orales et mises en situation professionnelles visant à démontrer la capacité du candidat à superviser, détecter et proposer des solutions de résilience suite à incident cyber. **<u>Par VAE :</u>** Étude du livret II et entretien avec le jury visant à démontrer la capacité du candidat à démontrer la capacité du candidat à superviser, détecter et proposer des solutions de résilience suite à incident cyber.	Le candidat : ▪ maitrise les principes de fonctionnement et les technologies utilisées au sein d'un security operation center (SOC) lui permettant de diriger un centre de supervision ; ▪ identifie aisément les incidents en s'appuyant sur ses connaissances approfondies des techniques couramment utilisées par les attaquants informatiques ; ▪ interprète avec justesse l'ensemble des éléments identifiés par un SOC ou ceux provenant d'autres sources pour qualifier un incident de sécurité ; ▪ s'appuie sur son expertise pour assister les équipes de supervision et valider au besoin leurs travaux ; ▪ réalise une veille technologique sur les menaces et les vulnérabilités des systèmes adaptée aux systèmes informatiques supervisés afin d'avoir un état de la menace exacte ; ▪ optimise les capacités de détection du SOC en ajoutant ou en modifiant des règles existantes afin d'identifier des attaques passées ou en cours non détectées.

Bloc n°3 : Superviser la cybersécurité des systèmes d'information (2/3)			
RÉFÉRENTIEL D'ACTIVITÉS ET DE COMPETENCES		RÉFÉRENTIEL D'EVALUATION	
ACTIVITÉS	COMPÉTENCES	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<u>Activité 3.2</u> : **Réagir face à une menace identifiée**	**C9 : Diriger les différentes phases de réponse sur incident dans le périmètre d'un centre de supervision** ▪ faire appliquer les directives et procédures de réaction prédéfinies, y compris les procédures d'alerte ; ▪ faire appliquer les ordres techniques de lutte informatique défensive ; ▪ caractériser la menace cyber ; ▪ transmettre les éléments pertinents aux organismes tiers participant à la recherche sur événement ; ▪ préserver les traces et preuves à des fins d'analyse ; ▪ transmettre les éléments de façon rigoureuse aux analystes.	**<u>Par formation</u>** Épreuves écrites, orales et mises en situation professionnelles visant à démontrer la capacité du candidat à superviser, détecter et proposer des solutions de résilience suite à incident cyber. **<u>Par VAE :</u>** Étude du livret II et entretien avec le jury visant à démontrer la capacité du candidat à démontrer la capacité du candidat à superviser, détecter et proposer des solutions de résilience suite à incident cyber.	Le candidat ▪ adapte le mode de fonctionnement des équipes de supervision en fonction du niveau de risque ; ▪ applique et coordonne les mesures de réaction suite à l'identification d'un incident cyber et garantit la conservation des preuves avant une éventuelle judiciarisation ou intervention d'une équipe de réponse sur incident ; ▪ identifie les impacts potentiels d'un incident cyber sur les actifs de l'entité ; ▪ conseille les administrateurs du SI sur les moyens de réponse à cet incident ; ▪ assure la transmission de l'ensemble des informations nécessaires à l'intervention d'une équipe de réponse sur incident (CERT).

Bloc n°3 : Superviser la cybersécurité des systèmes d'information (3/3)			
RÉFÉRENTIEL D'ACTIVITÉS ET DE COMPETENCES		RÉFÉRENTIEL D'EVALUATION	
ACTIVITÉS	COMPÉTENCES	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<u>Activité 3.3 :</u> **Développer le niveau de compétence technique des techniciens**	**C10 : Assurer la formation du personnel** ▪ concevoir et rédiger des scénarii d'entrainement adaptés au profits des équipes de supervision ; ▪ former les techniciens et opérateurs du centre supervision ; ▪ évaluer les techniciens et opérateurs du centre de supervision .	**<u>Par formation</u>** Épreuves écrites, orales et mises en situation professionnelles visant à démontrer la capacité du candidat à superviser, détecter et proposer des solutions de résilience suite à incident cyber. **<u>Par VAE :</u>** Étude du livret II et entretien avec le jury visant à démontrer la capacité du candidat à démontrer la capacité du candidat à superviser, détecter et proposer des solutions de résilience suite à incident cyber.	Le candidat : ▪ évalue le niveau de compétence des équipes dont il a la responsabilité ; ▪ rédige et réalise un plan de formation adapté au besoin des équipes de supervision ; ▪ anime des séances de formation cohérentes avec les besoins de formation ; ▪ prépare, organise et anime des entrainements pour maintenir et développer les compétences et performances des équipes dont il a la responsabilité.

Bloc 4 : Conduire une investigation numérique dans le domaine de la cybersécurité (1/2)			
RÉFÉRENTIEL D'ACTIVITÉS ET DE COMPETENCES		RÉFÉRENTIEL D'EVALUATION	
ACTIVITÉS	COMPÉTENCES	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<u>Activité 4.1 :</u> **Rechercher et analyser les éléments permettant de caractériser une attaque cyber**	**C11 : Mener des investigations en réponse sur incident** ▪ exploiter les éléments recueillis par des sondes gouvernementales ou commerciales de supervision des réseaux ; ▪ collecter les traces, codes informatiques et preuves lors d'un incident de sécurité ; ▪ réaliser l'analyse post mortem (inforensique) d'un système ayant subi un incident de sécurité ; ▪ analyser les traces, codes informatiques et preuves collectés ; ▪ garantir la préservation et l'intégrité des éléments collectés afin d'être juridiquement recevable ; ▪ réaliser une analyse dynamique d'un code malveillant dans un environnement sécurisé ; ▪ évaluer les impacts avérés et potentiels d'incidents informatiques et tenant compte de contextes sensibles.	**<u>Par formation</u>** Épreuves écrites, orales et mises en situation professionnelles visant à démontrer la capacité du candidat à caractériser une attaque et adapter sa stratégie de gestion de crise en fonction des retours d'expérience. **<u>Par VAE :</u>** Étude du livret II et entretien avec le jury visant à démontrer la capacité du candidat à caractériser une attaque et adapter sa stratégie de gestion de crise en fonction des retours d'expérience.	Le candidat : ▪ maitrise parfaitement les méthodes et procédure de collectes de preuves numériques via l'analyse de support numérique, le prélèvement de mémoire sur en système en fonction ou via une capture réseau ; ▪ garantit la préservation de la preuve en faisant preuve d'une rigueur absolue dans l'application des méthodes de prélèvements ; ▪ identifie parmi les éléments collectés les artefacts concomitants à un incident cyber ; ▪ réalise une analyse comportementale d'un malware dans un environnement sécurisé (sandbox) ; ▪ Identifie les impacts potentiels d'un incident cyber sur les actifs de l'entité.

Bloc 4 : Conduire une investigation numérique dans le domaine de la cybersécurité (2/2)			
RÉFÉRENTIEL D'ACTIVITÉS ET DE COMPETENCES		RÉFÉRENTIEL D'EVALUATION	
ACTIVITÉS	COMPÉTENCES	MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
<u>Activité 4.2 :</u> **Concevoir et/ou abonder une base de connaissances et rédiger les rapports d'investigation**	**C12 : Capitaliser le résultat des investigations** ▪ étudier les éléments issus des analyses pour déterminer les stratégies d'attaque et de propagation de codes malveillants ; ▪ construire et capitaliser un référentiel de données pertinentes à partir des informations recueillies à des fins de retour d'expérience ; ▪ rédiger et transmettre les rapports d'incident et d'analyse ; ▪ proposer des solutions de renforcement à long terme du niveau de sécurité des systèmes ; ▪ maintenir les bases de connaissances des indicateurs de compromission.	**<u>Par formation</u>** Épreuves écrites, orales et mises en situation professionnelles visant à démontrer la capacité du candidat à caractériser une attaque et adapter sa stratégie de gestion de crise en fonction des retours d'expérience. **<u>Par VAE :</u>** Étude du livret II et entretien avec le jury visant à démontrer la capacité du candidat à caractériser une attaque et adapter sa stratégie de gestion de crise en fonction des retours d'expérience.	Le candidat : ▪ capitalise le résultat des investigations pour identifier la stratégie et les outils d'attaque utilisés afin de mettre à jour l'état de la menace et les chemins d'attaques utilisés ; ▪ synthétise le résultat des investigations au sein de document en français ou en anglais dont la technicité est adaptée à son destinataire ; ▪ élabore des marquants d'attaque conforme aux schémas identifiés ; ▪ entretient une base de connaissance des méthodes et des marquants d'attaque ; ▪ organise ou anime la stratégie de gestion de crise en s'appuyant sur les retours d'expérience.