Retrait de publication de la Série Technique du NIST

Avertissement	
La publication ci-jointe a été retirée (archivée) et n'est fournie qu'à des fins de référence. Elle peut avoir été remplacée par une autre publication (indiquée ci-dessous).	
Publication retirée	
Séries/Numéro	Publication Spéciale du NIST 800-181 (SP 800-181)
Titre	Initiative Nationale pour l'Éducation en Cybersecurité (NICE) Référentiel de compétences pour les professionnels de la cybersécurité
Date(s) de publication	Août 2017
Date de retrait	19 novembre 2020
Note de retrait	La publication SP 800-181 est remplacée dans son intégralité par la publication SP 800-181 Révision 1.
Publication(s) remplaçante(s) *(le cas échéant)*	
La publication ci-jointe a été **remplacée par** la(les) publication(s) suivante(s) :	
Séries/Numéro	Publication Spéciale du NIST 800-181 Révision 1 (SP 800-181 Revision 1)
Titre	Référentiel de compétences pour les professionnels de la cybersécurité (Référentiel NICE)
Auteur(s)	Rodney Petersen, Danielle Santos, Karen A. Wetzel, Matthew C. Smith, Greg Witte
Date(s) de publication	Novembre 2020
URL/DOI	https://doi.org/10.6028/NIST.SP.800-181r1
Informations complémentaires *(le cas échéant)*	
Contact	Computer Security Division (Information Technology Laboratory)
Dernière révision de la publication jointe	
Informations associées	National Initiative for Cybersecurity Education (NICE) : https://nist.gov/nice https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final
Lien vers l'annonce de retrait	

Date de mise à jour : 13 novembre 13 2020

National Institute of Standards and Technology
U.S. Department of Commerce

Publication Spéciale du NIST 800-181

Initiative Nationale pour l'Éducation en Cybersecurité (NICE) Référentiel de compétences pour les professionnels de la cybersécurité

William Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

Cette publication est disponible gratuitement à l'adresse suivante :
https://doi.org/10.6028/NIST.SP.800-181.fre

National Institute of Standards and Technology
U.S. Department of Commerce

Publication Spéciale du NIST 800-181

Initiative Nationale pour l'Éducation en Cybersecurité (NICE) Référentiel de compétences pour les professionnels de la cybersécurité

William Newhouse
Applied Cybersecurity Division
Information Technology Laboratory

Stephanie Keith
Cyber Workforce Strategy & Policy Division
Office of the Deputy DoD Chief Information Officer

Benjamin Scribner
Cyber Education and Awareness Branch
DHS National Protection and Programs Directorate

Greg Witte
G2, Inc.
Annapolis Junction, MD

Cette publication est disponible gratuitement à l'adresse suivante :
https://doi.org/10.6028/NIST.SP.800-181.fre

Août 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Autorité

Cette publication a été élaborée par le NIST conformément à ses responsabilités statutaires en vertu de la loi fédérale sur la modernisation de la sécurité de l'information (FISMA) de 2014, 44 U.S.C. § 3551 et suivants, Public Law (P.L.) 113-283. Le NIST est chargé d'élaborer des normes et des lignes directrices en matière de sécurité de l'information, y compris des critères d'exigence minimaux pour les systèmes d'information fédéraux, mais ces normes et lignes directrices ne s'appliquent pas aux systèmes de sécurité nationale sans l'approbation expresse des fonctionnaires fédéraux compétents ayant autorité sur ces systèmes. Ces lignes directrices sont conformes aux exigences de la circulaire A-130 de l'Office of Management and Budget (OMB).

Aucun élément de cette publication ne doit être considéré comme contredisant les normes et les lignes directrices auxquelles le secrétaire au commerce a donné un caractère obligatoire et contraignant pour les agences fédérales en vertu du droit législatif. Ces lignes directrices ne doivent pas non plus être interprétées comme étant une modification ou un remplacement des pouvoirs existants du secrétaire au commerce, du directeur de l'OMB ou de tout autre fonctionnaire fédéral. Cette publication peut être utilisée par des organisations non gouvernementales sur une base volontaire et n'est pas soumise au droit d'auteur aux États-Unis. Le NIST apprécierait toutefois que la source soit citée.

National Institute of Standards and Technology Special Publication 800-181
Natl. Inst. Stand. Technol. Spec. Publ. 800-181, 144 pages (Août 2017)
CODEN: NSPUE2

Cette publication est disponible gratuitement à l'adresse suivante :
https://doi.org/10.6028/NIST.SP.800-181.fre

Les commentaires sur cette publication peuvent être adressés à :

National Institute of Standards and Technology
Attn: NICE, Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: ncwf@nist.gov

Rapports sur la technologie des systèmes informatiques

Le laboratoire de technologie de l'information (ou ITL pour Information Technology Laboratory) du NIST promeut l'économie américaine et le bien-être public en assurant la direction technique de l'infrastructure nationale de mesure et de normalisation. L'ITL développe des tests, des méthodologies expérimentales, des données de référence, des implémentations de preuves de concept et des analyses techniques pour faire progresser le développement et l'utilisation productive des technologies de l'information. Les responsabilités de l'ITL comprennent l'élaboration de normes et de lignes directrices en matière de gestion, d'administration, en matière technique et physique pour une sécurité et une confidentialité optimales des informations autres que celles liées à la sécurité nationale dans les systèmes d'information fédéraux. La série de publications spéciales 800 rend compte des recherches, des lignes directrices et des efforts de sensibilisation de l'ITL en matière de sécurité des systèmes d'information, ainsi que de ses activités de collaboration avec l'industrie, le gouvernement et les organisations universitaires.

Résumé

Cette publication décrit le référentiel de compétences en cybersécurité de la National Initiative for Cybersecurity Education (NICE), une structure de référence qui décrit la nature interdisciplinaire du travail dans le domaine de la cybersécurité. Il s'agit d'une ressource de référence fondamentale pour décrire et partager des informations sur les métiers de la cybersécurité et sur les connaissances, les capacités et les aptitudes (ou KSA pour Knowledge, Skills, and Abilities) nécessaires pour accomplir des tâches susceptibles de renforcer la situation d'une organisation sur le plan de la cybersécurité. Le référentiel NICE est un lexique partagé et cohérent qui catégorise et décrit les tâches de cybersécurité. Il permet d'améliorer la communication sur la manière d'identifier, de recruter, de développer et de pérenniser les talents dans le domaine de la cybersécurité. Le référentiel NICE est une source de référence à partir de laquelle les organisations ou les filières peuvent élaborer des publications ou des outils supplémentaires qui répondent à leurs besoins de définir ou de fournir des orientations sur différents aspects du développement, de la planification, de la formation et de l'éducation des ressources humaines dans le domaine de la cybersécurité.

Mots clefs

Aptitude ; cybersécurité ; cyberespace ; éducation ; connaissance ; rôle ; capacité ; spécialité ; tâche ; formation ; fonction.

Révisions

Veuillez consulter le site web des révisions du référentiel NICE [1] pour savoir si des mises à jour lui ont été apportées.

Contenu complémentaire

Un tableur de référence pour le référentiel NICE est disponible à l'adresse suivante : https://www.nist.gov/file/372581.

Remerciements

Les auteurs remercient sincèrement les personnes et les organisations des secteurs public et privé pour leurs contributions remarquables, et pour leurs commentaires avisés et constructifs qui ont permis d'améliorer la qualité générale, l'exhaustivité et l'utilité de cette publication. Nous apprécions le leadership et le travail de Rodney Petersen, directeur de l'initiative nationale pour l'éducation à la cybersécurité (ou NICE pour National Initiative for Cybersecurity Education) au NIST. Nous tenons à remercier Tanya Brewer, Dean Bushmiller, Lynne Clarke, Jerri Damavandy, Lisa Dorr, Ryan Farr, Jim Foti, Jodi Guss, Keith Hall, Chris Kelsall, Elizabeth Lennon, Jeff Marron, Joshua Musicante, Stephen Olechnowicz, Lori Pfannenstein, Chuck Romine, Kevin Sanchez-Cherry, Danielle Santos, Stephanie Shively, Matthew Smith, Kevin Stine, Bluma Sussman, Caroline Tan, Baris Yakin et Clarence Williams pour leurs contributions respectives à cette publication.

Le premier référentiel NICE a été soumis à l'avis du public en septembre 2012 et publié dans sa version finale en avril 2013 sous le nom de National Cybersecurity Workforce Framework version 1.0 (référentiel national pour les professionnels de la cybersécurité, version 1.0) [2]. Les auteurs remercient le Dr Jane Homeyer, Anne Quigley, Rex Min, Noel Kyle, Maya Yankelevich et Peggy Maxson pour avoir piloté son élaboration, ainsi que Montana Williams et Roy Burgess pour leur leadership dans l'élaboration de la version 2.0 du National Cybersecurity Workforce Framework, qui a été publiée en avril 2014 [3].

Enfin, les auteurs saluent respectueusement les travaux précurseurs en matière de sécurité informatique qui remontent aux années 1960. La vision, les idées et les efforts constants de ces pionniers de la sécurité informatique servent de fondement philosophique et technique aux tâches, connaissances, capacités et aptitudes mentionnées dans la présente publication.

Note d'information sur les marques déposées

Résumé

L'initiative nationale pour l'éducation à la cybersécurité (ou NICE pour National Initiative for Cybersecurity Education), dirigée par l'Institut national des normes et de la technologie (ou NIST pour National Institute of Standards and Technology) du ministère américain du commerce, est un partenariat entre le gouvernement, les universités et le secteur privé qui vise à dynamiser et à promouvoir un réseau solide et un écosystème en matière d'éducation, de formation et de développement de la main d'œuvre dans le domaine de la cybersécurité. NICE remplit cette mission en coordonnant ses activités avec celles de ses partenaires gouvernementaux, universitaires et industriels afin de tirer parti des programmes qui existent déjà et qui ont fait leurs preuves, de faciliter le changement et l'innovation, et d'apporter son leadership et sa vision afin d'augmenter le nombre de professionnels qualifiés en cybersécurité qui contribueront à assurer la sécurité de notre pays.

NICE s'engage à former une main-d'œuvre spécialisée dans la cybersécurité qui soit compétitive au niveau mondial, depuis l'embauche jusqu'à la retraite, et qui soit prête à protéger notre pays contre les défis actuels et émergents en matière de cybersécurité. NICE encourage les initiatives nationales qui augmentent le nombre de personnes ayant les connaissances, les capacités et les aptitudes nécessaires pour accomplir les tâches requises dans le domaine de la cybersécurité.

Les menaces qui exploitent les vulnérabilités de nos infrastructures informatiques étant de plus en plus nombreuses et évolutives, une main-d'œuvre spécialisée dans la cybersécurité doit être capable de concevoir, de développer, de mettre en œuvre et de maintenir des stratégies défensives et offensives dans le domaine de la sécurité informatique. Une main d'œuvre spécialisée dans la cybersécurité assume des fonctions techniques et non techniques et est composée de personnes compétentes et expérimentées. Ce personnel peut relever les défis inhérents à la préparation des organisations à la mise en œuvre réussie des aspects de leurs missions et de leurs processus opérationnels liés au cyberespace.

Cette publication constitue une référence fondamentale pour aider le personnel à répondre aux besoins d'une organisation en matière de cybersécurité en utilisant un lexique commun et cohérent pour décrire les activités de cybersécurité par catégorie, par spécialité et par rôle. Il fournit un sur ensemble de connaissances, de capacités et d'aptitudes (KSA) en matière de cybersécurité, ainsi que des tâches pour chaque fonction. Le référentiel NICE favorise une communication cohérente au niveau de l'organisation et du secteur de l'éducation, de la formation et du développement de la main-d'œuvre dans le domaine de la cybersécurité.

Un utilisateur du référentiel NICE y fera référence pour différents aspects du développement des effectifs, de l'éducation et/ou de la formation, et lorsque ce référentiel est utilisé au niveau de l'organisation, l'utilisateur doit adapter ce qui en est extrait aux normes, aux réglementations, aux besoins et à la mission de son organisation. Le référentiel NICE est un point de départ de référence pour le contenu des orientations et des lignes directrices sur les parcours professionnels, l'éducation, la formation et les programmes qui délivrent des titres et des certificats.

Le référentiel NICE est une ressource qui renforcera la capacité d'une organisation à communiquer de manière cohérente et claire sur les activités de cybersécurité et ses effectifs

dans ce domaine. Les organisations ou les secteurs peuvent développer d'autres publications ou outils répondant à leurs besoins pour définir ou fournir des orientations sur différents aspects du développement, de la planification, de la formation et de l'éducation des effectifs.

Un tableur de référence [4] est disponible sur le site web du référentiel NICE [5].

Table des matières

Liste des Annexes

Liste des Tableaux

1 Introduction

L'initiative nationale pour l'éducation à la cybersécurité (ou NICE pour National Initiative for Cybersecurity Education), dirigée par l'Institut national des normes et de la technologie (ou NIST pour National Institute of Standards and Technology) du ministère américain du commerce, est un partenariat entre le gouvernement, les universités et le secteur privé qui vise à dynamiser et à promouvoir un réseau solide et un écosystème en matière d'éducation, de formation et de développement de la main d'œuvre dans le domaine de la cybersécurité. NICE remplit cette mission en se coordonnant avec des partenaires gouvernementaux, universitaires et industriels afin de tirer parti des programmes existants qui ont fait leurs preuves, de faciliter le changement et l'innovation, et d'apporter un leadership et une vision afin d'augmenter le nombre de professionnels qualifiés en cybersécurité, contribuant ainsi à assurer la sécurité et la compétitivité économique de notre pays.

NICE s'engage à former une main-d'œuvre spécialisée dans la cybersécurité qui soit compétitive au niveau mondial, depuis l'embauche jusqu'à la retraite, et qui soit prête à protéger notre nation contre les défis actuels et émergents en matière de cybersécurité.

Tout au long de ce document, l'expression "personnel de cybersécurité" désigne une main-d'œuvre dont les fonctions ont un impact sur la capacité d'une organisation à protéger ses données, ses systèmes et ses opérations. Il s'agit de nouvelles fonctions traditionnellement connues sous le nom de fonctions liées à la sécurité des technologies de l'information (TI). Ces rôles ont été ajoutés à ce référentiel afin de souligner leur importance pour la posture globale de cybersécurité d'une organisation. Par ailleurs, certaines des fonctions décrites dans ce document comportent le terme plus court de "cyber", afin d'englober les secteurs dans lesquels le mot cyber est devenu la norme du langage courant dans ce domaine.

Le personnel chargé de la cybersécurité comprend non seulement des employés spécialisés dans les aspects techniques, mais aussi des personnes qui mettent en pratique leurs connaissances en matière de cybersécurité lorsqu'elles préparent leur organisation à mener à bien sa mission. Un personnel de cybersécurité bien informé et compétent est nécessaire pour faire face aux risques de cybersécurité dans le cadre du processus global de gestion des risques d'une organisation.

1.1 Historique du référentiel NICE

Le concept du référentiel NICE a vu le jour avant la création de NICE en 2010 et il est né du constat que le personnel chargé de la cybersécurité n'avait pas été décrit ni évalué. Pour relever ce défi, le Conseil des directeurs de l'information du gouvernement fédéral (Federal Chief Information Officers - CIO) s'est attelé en 2008 à la tâche de fournir un cadre standard pour comprendre les rôles en matière de cybersécurité au sein de l'administration fédérale. Grâce aux contributions de groupes de discussion composés d'experts en la matière issus de nombreuses agences fédérales, ce Conseil a produit un rapport de synthèse qui mentionnait les domaines dans lesquels d'autres efforts de développement professionnel en matière de technologies de l'information étaient déjà en cours, et treize rôles spécifiques ont été identifiés comme étant nécessaires aux agences pour mener à bien leurs travaux en matière de cybersécurité.

S'appuyant sur cette exploration intrinsèquement multidisciplinaire du "domaine" de la cybersécurité, la Comprehensive National Cybersecurity Initiative (initiative nationale globale pour la cybersécurité) a mis l'accent sur la main-d'œuvre et a chargé plusieurs agences de collaborer à l'élaboration d'un référentiel pour la main-d'œuvre dans le domaine de la cybersécurité. La première version a été soumise à l'avis du public en septembre 2011. Les commentaires ont été intégrés dans la version 1.0 [2].

Un examen ultérieur à l'échelle du gouvernement américain a mis en évidence des domaines spécifiques à examiner et à affiner. Le DHS (Department of Homeland Security) a recueilli des informations et validé les recommandations finales par l'intermédiaire de groupes de discussion composés d'experts en la matière issus de l'ensemble du pays, de l'industrie, du monde universitaire et du gouvernement, ce qui a donné lieu à une deuxième version du référentiel NICE, la version 2.0 [3], rendue publique en 2014.

L'OSD (Office of the Secretary of Defense) a développé la version 2.0 grâce à des collaborations internes avec les composantes du service et à des participations externes avec le secteur privé. Les co-auteurs du DHS et du NIST ont travaillé avec l'OSD pour affiner leur travail jusqu'à la présente publication, dans le but de mettre l'accent sur l'applicabilité au secteur privé et de renforcer la vision selon laquelle le référentiel NICE est une ressource de référence à la fois pour le secteur public et le secteur privé.

1.2 Objectif et champ d'application

Cette publication constitue une ressource de référence fondamentale pour aider les organisations à se doter d'un personnel capable de répondre à leurs besoins en matière de cybersécurité. Elle fournit aux organisations un lexique commun et cohérent qui catégorise et décrit les activités en matière de cybersécurité.

L'utilisation du référentiel NICE comme ressource fondamentale améliorera la communication nécessaire à l'identification, au recrutement et au développement des talents dans le domaine de la cybersécurité. Le référentiel NICE permettra aux employeurs d'utiliser un langage ciblé et cohérent dans les programmes de développement professionnel, dans leur utilisation des certifications professionnelles et des titres universitaires, et dans leur sélection d'opportunités de formation pertinentes pour leur personnel.

Le référentiel NICE facilite le recours à une approche cohérente, comparative et reproductible pour sélectionner et spécifier les rôles en matière de cybersécurité pour les postes à pourvoir au sein des organisations. Il fournit également un lexique commun que les organismes éducatifs peuvent utiliser pour élaborer des programmes de formation à la cybersécurité qui préparent mieux les étudiants aux besoins actuels et prévisibles en termes de ressources humaines dans le domaine de la cybersécurité.

L'application du référentiel NICE permet de décrire toutes les activités de cybersécurité. L'un des objectifs d'applicabilité du référentiel NICE est de pouvoir décrire tout emploi ou poste dans le domaine de la cybersécurité en identifiant les éléments pertinents d'un ou de plusieurs composants du référentiel NICE. Pour chaque emploi ou poste, le contexte de la mission ou des processus et priorités de l'entreprise déterminera les éléments à sélectionner dans le référentiel.

Les organisations ou les acteurs du secteur peuvent utiliser le référentiel NICE pour développer des publications ou des outils supplémentaires qui répondent à leurs besoins de définir ou de fournir des orientations sur différents aspects du développement, de la planification, de la formation et de l'éducation des personnels.

1.3 Public/Utilisateurs

Le référentiel NICE peut être considéré comme un dictionnaire non contraignant sur les ressources humaines dans le domaine de la cybersécurité. Les utilisateurs de ce référentiel qui y font référence doivent le mettre en œuvre au niveau local à différentes fins de développement des compétences, d'éducation ou de formation.

1.3.1 Employeurs

L'utilisation du lexique commun du référentiel NICE permet aux employeurs d'inventorier et de développer leurs effectifs dans le domaine de la cybersécurité. Le référentiel NICE peut être utilisé par les employeurs et les dirigeants d'organisations pour :

- Inventorier et suivre leur personnel spécialisé dans la cybersécurité afin de mieux comprendre les points forts et les lacunes en matière de connaissances, de capacités et d'aptitudes, ainsi que les tâches accomplies ;
- Identifier les exigences en matière de formation et de qualification pour développer les connaissances, les capacités et les aptitudes essentielles à l'exécution des tâches de cybersécurité ;
- Améliorer les descriptions de poste et les offres d'emploi en sélectionnant les connaissances, compétences et aptitudes pertinentes, une fois que les rôles et les tâches ont été identifiés ;
- Identifier les fonctions les plus pertinentes et élaborer des parcours de carrière pour aider le personnel à acquérir les compétences requises pour ces rôles ; et
- Etablir une terminologie commune entre les responsables du recrutement et le personnel des ressources humaines (RH) pour le recrutement, la fidélisation et la formation d'une main-d'œuvre hautement spécialisée.

1.3.2 Professionnels d'aujourd'hui et de demain dans le domaine de la cybersécurité

Le référentiel NICE aide les personnes travaillant dans le domaine de la cybersécurité et celles qui souhaiteraient y entrer à explorer les tâches au sein des catégories et des fonctions dans le domaine. Il permet également ceux qui accompagnent ces professionnels, tels que les responsables des ressources humaines et les conseillers d'orientation, d'aider les demandeurs d'emploi et les étudiants à comprendre quelles fonctions en matière de cybersécurité et quelles connaissances, capacités et aptitudes associées sont recherchées par les employeurs pour les emplois et les postes en cybersécurité à pourvoir.

Ces professionnels de la cybersécurité bénéficient d'un avantage supplémentaire lorsque les annonces de postes vacants et les descriptions de postes ouverts utilisent le lexique commun du

référentiel NICE afin de fournir des descriptions claires et cohérentes des tâches et des compétences en matière de cybersécurité qui sont nécessaires pour ces postes.

Lorsque les organismes de formation et de certification du secteur utilisent le lexique commun du référentiel NICE, les personnes travaillant dans le domaine de la cybersécurité, ou celles qui souhaitent y entrer, peuvent trouver des organismes de formation et/ou de certification capables d'enseigner les tâches nécessaires pour obtenir un emploi dans ce domaine ou pour évoluer vers de nouveaux postes. L'utilisation du lexique commun permet aux étudiants et aux professionnels d'obtenir les KSA qui correspondent généralement aux compétences d'une personne qui occupe un poste dans le domaine de la cybersécurité et qui exerce une fonction donnée. Cette compréhension les aide à trouver des programmes d'études qui intègrent des objectifs d'apprentissage et des unités de connaissances correspondant aux compétences et tâches recherchées par les employeurs.

1.3.3 Enseignants/Formateurs

Le référentiel NICE sert de référence aux formateurs pour concevoir des programmes d'études, des programmes de certification ou de diplôme, des programmes de formation, des cours, des séminaires, des exercices ou des exercices qui correspondent aux KSA et aux tâches décrits dans le référentiel NICE.

Les spécialistes de la gestion des ressources humaines et les conseillers d'orientation peuvent utiliser le référentiel NICE comme ressource pour l'exploration des carrières.

1.3.4 Fournisseurs de technologies

Le référentiel NICE permet à un fournisseur de technologies d'identifier les fonctions en matière de cybersécurité ainsi que les KSA et les tâches associés aux produits et services matériels et logiciels qu'il propose. Le fournisseur peut alors créer des supports appropriés pour aider les membres du personnel en charge de la cybersécurité à configurer et à gérer correctement ses produits.

1.4 Organisation de cette Publication Spéciale

Cette publication spéciale est organisée de la façon suivante :

- Le chapitre 2 définit les composantes du référentiel NICE : (i) les catégories ; (ii) les spécialités ; (iii) les fonctions ; (iv) les sur-ensembles de connaissances, de capacités et d'aptitudes qui y sont associés ; et (v) les tâches pour chaque fonction.
- Le chapitre 3 décrit l'utilisation du référentiel NICE.
- Le chapitre 4 indique les domaines dans lesquels d'autres publications, lignes directrices, orientations et outils peuvent renforcer l'impact du référentiel NICE.
- 4.3Annexe A décrit la liste des catégories, des spécialités, des fonctions, des compétences clefs et des tâches du référentiel NICE.
- Annexe B fournit une liste détaillée de chaque fonction, y compris les KSA et les tâches associées.

- Annexe C donne quelques exemples d'outils de développement des ressources humaines.
- Annexe D donne des exemples de documents d'orientation ou de lignes directrices qui renvoient à certains éléments du référentiel NICE.
- Annexe E présente une sélection d'acronymes et d'abréviations utilisés dans ce document.
- Annexe F présente les références citées dans ce document.

2 Référentiel NICE : Composants et relations

2.1 Les composants du référentiel NICE

Le référentiel NICE organise la cybersécurité et les travaux connexes. Cette section présente et définit les principaux éléments du référentiel.

2.1.1 Catégories

Les catégories constituent la structure générale du référentiel NICE. Il existe sept catégories, toutes composées de spécialités et de fonctions. Cette organisation repose sur des analyses approfondies des emplois, et regroupe les travaux et les professionnels qui ont des fonctions en commun, indépendamment des intitulés de poste ou d'autres termes professionnels.

2.1.2 Spécialités

Les catégories contiennent des regroupements de travaux, appelés spécialités. Le National Cybersecurity Workforce Framework (NCWF) version 1.0 [2] comptait 31 spécialités et le NCWF version 2.0 [3] en comptait 32. Chaque spécialité représente un domaine de travail spécifique, ou une fonction, au sein de la cybersécurité et des activités connexes. Dans les versions précédentes du référentiel NICE, des tâches et des KSA étaient associés à chaque spécialité. Les KSA et les tâches sont désormais associés aux fonctions.

2.1.3 Fonctions

Les fonctions sont les regroupements les plus fins des activités de cybersécurité et des activités connexes, ils comprennent une liste d'attributs requis pour remplir cette fonction sous la forme de connaissances, de capacités et d'aptitudes (KSA), ainsi que les tâches accomplies dans le cadre de cette fonction.

Les tâches effectuées dans le cadre d'un emploi ou d'un poste sont décrites en sélectionnant une ou plusieurs fonctions du référentiel NICE qui correspondent à cet emploi ou à ce poste, au service de la mission ou des processus opérationnels.

Pour faciliter l'organisation et la communication des responsabilités en matière de cybersécurité, les fonctions sont regroupées en catégories spécifiques et en spécialités, comme indiqué àAnnexe A.

2.1.4 Connaissances, capacités et aptitudes (ou KSAs pour Knowledge, Skills, and Abilities)

Les connaissances, les capacités et les aptitudes (KSA) sont les attributs nécessaires à l'exercice des fonctions et sont généralement obtenues grâce à l'expérience, à l'éducation ou à la formation.

> **La connaissance** est un ensemble d'informations appliquées directement à l'exécution d'une fonction.

La capacité est souvent définie comme une aptitude observable à réaliser un acte psychomoteur appris. Les capacités dans le domaine psychomoteur décrivent la capacité à manipuler physiquement un outil ou un instrument comme une main ou un marteau. Les capacités nécessaires à la cybersécurité reposent moins sur la manipulation physique d'outils et d'instruments que sur l'application d'outils, de référentiels, de processus et de contrôles qui ont une incidence sur le niveau de cybersécurité d'une organisation ou d'un individu.

L'aptitude est la capacité d'avoir un comportement observable ou un comportement qui aboutit à un résultat observable.

2.1.5 Tâches

Une tâche est un travail spécifique précis qui, combiné à d'autres tâches définies, constitue le travail dans un domaine de spécialisation ou une fonction spécifique.

2.2 Relations entre les composants du référentiel NICE

Les composants du référentiel NICE décrivent les activités de cybersécurité. Comme l'illustre la Figure 1, chaque catégorie est composée de spécialités, chacun d'entre eux étant composé d'une ou de plusieurs fonctions. Chaque fonction comprend à son tour des KSA et des tâches.

Le fait de regrouper les éléments de cette manière simplifie la communication sur les thèmes relatifs aux ressources humaines dans le domaine de la cybersécurité et facilite les correspondances avec d'autres cadres de référence. L'annexe B et une feuille de calcul de référence [4] publiée sur le site web du référentiel NICE [5] qui présente les associations spécifiques entre les fonctions, les KSA et les tâches.

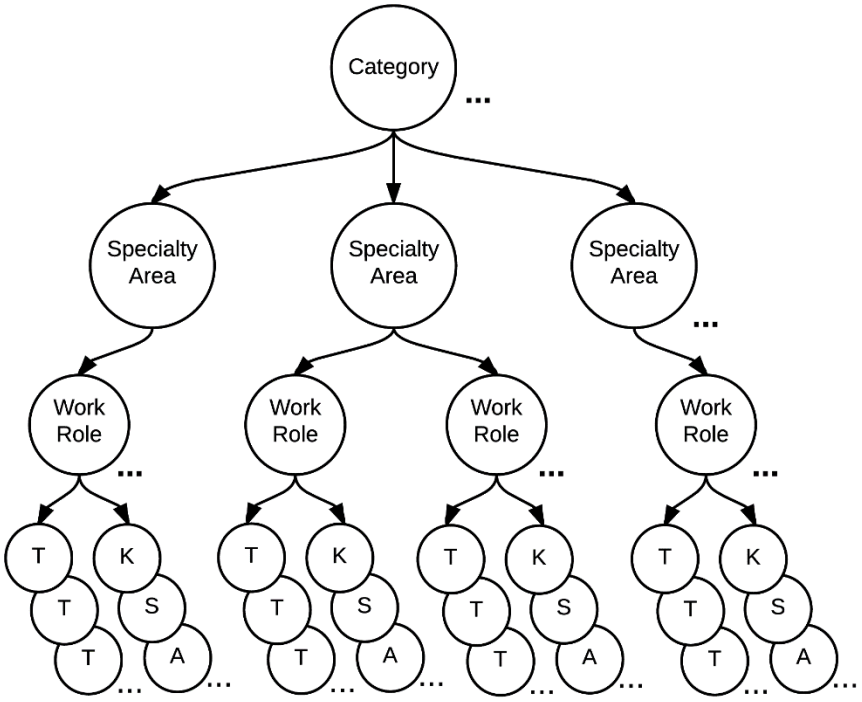

Figure 1 - Relations entre les composants du référentiel NICE

3 Utilisation du référentiel NICE

L'utilisation du référentiel NICE pour comprendre les besoins organisationnels et évaluer dans quelle mesure ces besoins sont satisfaits peut aider une organisation à planifier, mettre en œuvre et contrôler un programme de cybersécurité réussi.

3.1 Identification des besoins en ressources humaines dans le domaine de la cybersécurité

La cybersécurité est un domaine qui évolue et se développe rapidement. Cette progression nécessite la mise en place d'un groupe de professionnels qualifiés pour aider les organisations à assurer les fonctions liées à la cybersécurité. Lorsque les organisations déterminent ce dont elles ont besoin pour gérer correctement les risques présents et futurs en matière de cybersécurité, les dirigeants doivent prendre en compte les capacités et les compétences requises pour le personnel chargé de la cybersécurité.

La **Error! Reference source not found.** montre comment le référentiel NICE constitue une référence incontournable pour aider les employeurs à se doter de collaborateurs compétents et prêts à travailler dans le domaine de la cybersécurité.

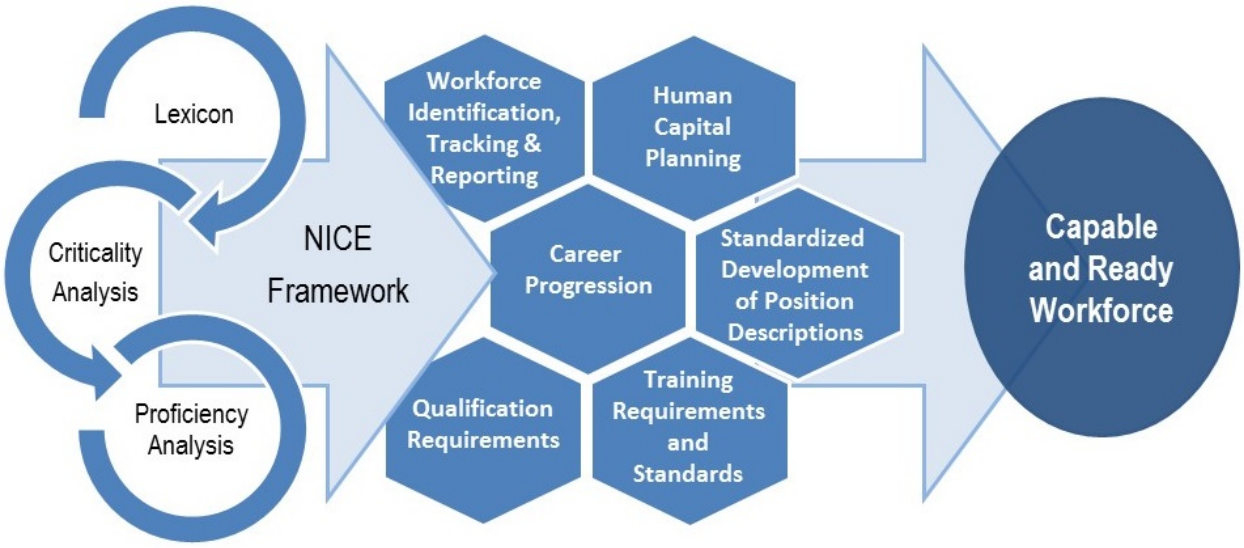

Figure 2 - Éléments de base pour constituer des équipes compétentes et prêtes à intervenir dans le domaine de la cybersécurité

Les flèches circulaires situées à gauche de la Figure 2 correspondent à des activités susceptibles d'avoir un impact sur la capacité d'une organisation à se doter de collaborateurs compétents et prêts à intervenir :

- L'utilisation du lexique commun du référentiel NICE clarifie la communication entre les éducateurs en cybersécurité, les formateurs/certificateurs, les employeurs et les collaborateurs.

- L'analyse de la criticité permet d'identifier les KSA et les tâches qui sont essentielles à la réussite d'une fonction donnée et celles qui sont clefs pour plusieurs fonctions.
- La réalisation d'une analyse des compétences permettra à l'organisation de connaître le niveau attendu pour les postes (par exemple, niveau débutant, expert), postes qui comprennent souvent plus d'une fonction. L'analyse des compétences devrait permettre d'affiner la sélection des tâches pertinentes et des compétences essentielles nécessaires pour les fonctions qui composent ce poste.

Annexe C présente certains outils de développement des ressources humaines qui permettent de recenser les besoins dans le domaine de la cybersécurité.

3.2 Recrutement de personnel hautement qualifié dans le domaine de la cybersécurité

Le recours au référentiel NICE aidera les organisations à réaliser une planification stratégique des ressources humaines et à recruter. Les éléments du référentiel NICE, lorsqu'ils sont utilisés lors de la création ou de la révision des descriptions de postes dans les avis de vacance et les offres d'emploi, aideront les candidats à se diriger vers des postes qui les intéressent et pour lesquels ils sont qualifiés. Les tâches qui servent à décrire les fonctions et les responsabilités d'un poste, ainsi que les compétences et les qualifications requises pour le poste, devraient permettre aux candidats et aux responsables du recrutement de communiquer plus efficacement. Les descriptions de poste et les avis de vacance de poste utilisant la terminologie du référentiel NICE permettent d'établir des critères d'évaluation plus cohérents pour l'évaluation et l'approbation des candidats.

Pour les organisations qui se préoccupent des lacunes en matière de ressources humaines, un examen de la liste des tâches du référentiel NICE peut permettre de déterminer les tâches spécifiques qui ne sont pas exécutées par l'organisation. Ces tâches permettent à l'organisation d'identifier le(s) rôle(s) professionnel(s) et la(les) spécialité(s) qui présentent des lacunes. L'organisation peut plus facilement s'engager avec la communauté des établissements d'enseignement, de formation, de délivrance de titres et de certifications qui adaptent leurs offres au référentiel NICE. L'organisation peut identifier les formations qui permettront aux membres du personnel en poste de combler ses lacunes. Les responsables du recrutement de l'organisation qui utilisent les données tirées du référentiel NICE de cette manière peuvent identifier les candidats qui possèdent les compétences nécessaires pour effectuer les opérations de cybersécurité.

3.3 Éducation et formation des professionnels de la cybersécurité

En identifiant les tâches dans les fonctions, le référentiel NICE permet aux formateurs de préparer les apprenants en leur fournissant les KSA spécifiques à partir desquels ils peuvent démontrer leur capacité à accomplir des tâches de cybersécurité.

Les centres de formation jouent un rôle essentiel dans la préparation et la formation professionnels de la cybersécurité. La collaboration entre les entités publiques et privées, par exemple dans le cadre du programme NICE, permet à ces établissements de déterminer les connaissances et les compétences communes nécessaires. À leur tour, l'élaboration et la mise en

œuvre de programmes d'études harmonisés avec le référentiel NICE permettent aux établissements de préparer les étudiants à acquérir les compétences dont les employeurs ont besoin. À mesure que le nombre d'étudiants trouvant un emploi dans le domaine de la cybersécurité augmentera, de plus en plus d'étudiants seront attirés par les programmes universitaires de cybersécurité comme voie d'accès à une carrière.

3.4 Fidélisation et développement de talents hautement qualifiés dans le domaine de la cybersécurité

Pour disposer d'une main-d'œuvre qualifiée dans le domaine de la cybersécurité, il est essentiel de développer et de fidéliser les talents déjà présents dans l'entreprise. Un collaborateur en poste a des relations, une connaissance des institutions et une expérience organisationnelle qu'il est difficile de remplacer. Le remplacement d'un poste après le départ d'un salarié peut entraîner des frais de publicité et d'embauche, des dépenses de formation, une baisse de la productivité et une détérioration du moral des équipes. La liste suivante illustre quelques-uns des moyens par lesquels le référentiel NICE favorise la fidélisation et le développement des talents dans le domaine de la cybersécurité :

- Les organisations peuvent élaborer des parcours de carrière qui décrivent les qualifications nécessaires pour des ensembles de fonctions de plus en plus stimulantes et en constante évolution, tels que celles énumérées par le référentiel NICE.
- Une compréhension détaillée des KSA et des tâches aide le personnel en place à comprendre les étapes spécifiques nécessaires au développement de ses capacités, ce qui favorise la préparation au poste souhaité.
- Une organisation peut proposer des rotations de personnel afin d'offrir des opportunités de développer et d'utiliser de nouvelles compétences.
- Les organisations peuvent identifier les collaborateurs qui s'efforcent d'améliorer les compétences clefs dans les domaines pertinents, et reconnaître ceux qui obtiennent de bons résultats.
- Les organisations peuvent créer des plans de développement/amélioration pour le personnel afin de l'aider à déterminer comment il peut obtenir les compétences requises pour ses nouvelles fonctions.
- Des possibilités de formation en groupe peuvent être identifiées pour préparer les membres du personnel à améliorer les connaissances, les capacités et les aptitudes communes dans les fonctions d'une organisation.
- Les organisations peuvent utiliser des formations et des examens basés sur des capacités et des aptitudes spécifiques en matière de cybersécurité afin d'évaluer les compétences dans un environnement réaliste.
- Les organisations peuvent utiliser le personnel existant pour répondre aux besoins critiques en personnel de cybersécurité, en tirant parti de la possibilité d'examiner les CV du personnel existant pour identifier ceux qui possèdent les KSA souhaités.
- Le référentiel NICE est utile pour les collaborateurs actuels qui souhaitent changer de poste pour travailler dans le domaine de la cybersécurité. Une organisation peut décrire

les compétences clefs nécessaires pour permettre à un collaborateur fiable occupant un poste sans rapport avec la cybersécurité de s'intégrer au personnel de cybersécurité en prenant en charge des tâches de cybersécurité.

4 Compléments

Les organisations ou les filières peuvent utiliser le référentiel NICE pour élaborer des publications ou concevoir des outils supplémentaires qui répondent à leurs besoins et définissent ou fournissent des orientations sur différents aspects du développement, de la planification, de la formation et de l'éducation des ressources humaines.

Les nouveaux documents de référence qui renvoient à des éléments du référentiel NICE seront partagés via le site web du NICE [5].

Les domaines suivants sont quelques exemples à partir desquels des publications ou des outils supplémentaires pourraient être développés.

4.1 Compétences

Le département de l'emploi et de la formation du ministère du travail [6] définit une compétence comme la capacité d'appliquer ou d'utiliser des connaissances, des aptitudes, des capacités, des comportements et des caractéristiques personnelles pour mener à bien des tâches professionnelles essentielles, des fonctions spécifiques ou pour occuper un rôle ou un poste donné. En plus de l'énumération des KSA techniques, les modèles de compétences prennent également en compte les indicateurs comportementaux et décrivent des considérations non techniques telles que l'efficacité personnelle, les compétences académiques et les compétences sur le lieu de travail. Des informations supplémentaires sur ces considérations sont disponibles sur le site CareerOneStop du ministère du travail [7].

4.2 Intitulés de postes

Les intitulés de poste sont une description du travail ou de la fonction d'un collaborateur au sein d'une organisation. Une mise en correspondance d'exemples d'intitulés de postes avec des spécialités ou des fonctions aiderait les organisations à utiliser le référentiel NICE.

4.3 Documents d'orientation et de recommandation sur la cybersécurité

L'objectif stratégique n° 3 de NICE, Guide Career Development and Workforce Planning, a pour but d'aider les employeurs à répondre aux demandes du marché et à améliorer le recrutement, l'embauche, le développement et la fidélisation des talents dans le domaine de la cybersécurité. L'un des buts de cet objectif stratégique est de publier le référentiel NICE, de le faire connaître et d'en encourager l'adoption. Par adoption, on entend ici l'utilisation du référentiel NICE comme ressource de référence pour les actions liées aux ressources humaines, à la formation et à l'éducation dans le domaine de la cybersécurité.

L'un des moyens d'encourager l'adoption du cadre NICE consiste à inciter les auteurs de documents d'orientation ou de lignes directrices sur la cybersécurité à faire référence aux éléments du cadre NICE dans leur contenu. Trois exemples de publications sont présentés à l'Annexe D.

Annexe A – Liste des éléments du référentiel NICE

A.1 Catégories de personnel du référentiel NICE

Tableau 1 décrit chaque catégorie du référentiel NICE. Chacune comprend une abréviation à deux caractères (par exemple, SP) pour une référence rapide de la catégorie et pour faciliter la création des identifiants des fonctions du référentiel NICE (voir Tableau 3 - Fonctions du référentiel NICE). Cette liste sera mise à jour régulièrement [1]. La source de référence pour la version la plus récente de ce document se trouve dans le tableur de référence de la publication spéciale 800-181 du NIST [4].

Tableau 1 - Catégories de personnel du référentiel NICE

Catégories	Descriptions
Provisionnement sécurisé (SP)	Conceptualise, conçoit, fait l'acquisition et/ou construit des systèmes de technologie de l'information (TI) sécurisés, en étant responsable de certains aspects du développement des systèmes et/ou des réseaux.
Exploitation et maintenance (OM)	Fournir le support, l'administration et la maintenance nécessaires pour assurer l'efficacité et l'efficience des performances et de la sécurité des systèmes de technologie de l'information (TI).
Superviser et gouverner (OV)	Assurer le leadership, la gestion, la conduite ou le développement et la défense des intérêts de l'organisation afin qu'elle puisse mener efficacement ses activités dans le domaine de la cybersécurité.
Protéger et défendre (PR)	Identifier, analyser et réduire les menaces qui pèsent sur les systèmes et/ou réseaux informatiques internes.
Analyser (AN)	Examiner et évaluer de manière très précise les informations reçues en matière de cybersécurité afin de déterminer leur utilité pour le renseignement.
Collecter et exploiter (CO)	Mener des opérations spécifiques de déni et de tromperie et collecter des informations sur la cybersécurité susceptibles d'être utilisées à des fins de renseignement.
Enquêter (IN)	Enquêter sur des événements ou des délits relevant de la cybersécurité et liés à des systèmes informatiques, à des réseaux et à des preuves numériques.

A.2 Spécialités du référentiel NICE

Tableau 2 décrit les différentes spécialités du référentiel NICE. Chaque spécialité comprend une abréviation à trois caractères (par exemple, RSK) pour faciliter l'identification rapide de la spécialité et la création des identifiants des fonctions du référentiel NICE (voir Tableau 3 - Fonctions du référentiel NICE). Cette liste sera mise à jour régulièrement [1]. La source de référence pour la version la plus récente de ce document se trouve dans le tableur de référence de la publication spéciale 800-181 du NIST [4].

Tableau 2 - Spécialités du référentiel NICE

Catégories	Spécialités	Description des spécialités
Provisionnement sécurisé (SP)	Gestion des risques (RSK)	Supervise, évalue et soutient les processus de documentation, de validation, d'évaluation et d'autorisation nécessaires pour garantir que les systèmes de technologie de l'information (TI) actuels et futurs répondent aux exigences de l'organisation en matière de cybersécurité et de risque. Veille au traitement approprié des risques, de la conformité et de la sécurité d'un point de vue interne et externe.
	Développement de logiciels (DEV)	Développe et écrit/code de nouvelles applications informatiques (ou modifie des applications existantes), des logiciels ou des programmes utilitaires spécialisés en suivant les bonnes pratiques en matière d'assurance logicielle.
	Architecture des systèmes (ARC)	Élabore des modèles de systèmes et travaille sur les phases de développement des capacités du cycle de vie des systèmes ; traduit la technologie et les éléments de contexte (par exemple, la législation et la réglementation) en conceptions et en processus de systèmes et de sécurité.
	R&D technologique (TRD)	Conduit les processus d'évaluation et d'intégration des technologies ; fournit et soutient un prototype et / ou évalue son utilité.
	Planification des exigences système (SRP)	Consulte les clients afin de recueillir et d'évaluer les exigences fonctionnelles puis traduit ces exigences en solutions techniques. Fournit des conseils aux clients sur l'utilisation des systèmes d'information pour répondre aux besoins de l'entreprise.
	Test et évaluation (TST)	Élabore et réalise des essais des systèmes afin d'évaluer la conformité aux spécifications et aux exigences en appliquant des principes et des méthodes de planification, d'évaluation, de vérification et de validation efficaces des caractéristiques techniques, fonctionnelles et de performance (y compris l'interopérabilité) des systèmes ou des éléments de systèmes intégrant des technologies de l'information.

Catégories	Spécialités	Description des spécialités
	Développement de systèmes (SYS)	Travaille sur les phases de conception du cycle de vie du développement des systèmes.
Exploitation et maintenance (OM)	Administration des données (DTA)	Crée et administre des bases de données et/ou des systèmes de gestion des données qui permettent le stockage, la consultation, la protection et l'utilisation des données.
	Gestion des connaissances (KMG)	Gère et administre les processus et les outils qui permettent à l'organisation d'identifier, de documenter et d'accéder au capital intellectuel ainsi qu'aux connaissances et aux contenus.
	Service à la clientèle et support technique (STS)	Résout les problèmes, installe, configure, dépanne et assure la maintenance et la formation en réponse aux exigences ou aux demandes des clients (par exemple, support client à plusieurs niveaux). Fournit généralement des informations initiales sur les incidents à la spécialité de réponse aux incidents (IR).
	Services réseaux (NET)	Installe, configure, teste, exploite, entretient et gère les réseaux et leurs pare-feu, y compris le matériel (par exemple, les concentrateurs, les ponts, les commutateurs, les multiplexeurs, les routeurs, les câbles, les serveurs proxy et les systèmes de distribution de protection) et les logiciels qui permettent le partage et la transmission de toutes les transmissions d'informations du spectre afin d'assurer la sécurité des informations et des systèmes d'information.
	Administration des systèmes (ADM)	Installe, configure, dépanne et entretient les configurations de serveurs (matériel et logiciels) afin d'en assurer la confidentialité, l'intégrité et la disponibilité. Gère les comptes, les pare-feu et les correctifs. Responsable du contrôle d'accès, des mots de passe, de la création et de l'administration des comptes.
	Analyse des systèmes (ANA)	Etudie les systèmes et procédures informatiques en place dans une organisation et conçoit des solutions informatiques pour aider l'organisation à fonctionner de manière plus sûre, plus efficace et plus efficiente. Favorise le rapprochement entre l'entreprise et les technologies de l'information (TI) en analysant les besoins et les limites de l'une et de l'autre.
Superviser et gouverner (OV)	Conseil juridique et défense des intérêts (LGA)	Fournit des conseils et des recommandations juridiques à la direction et au personnel sur une variété de sujets relevant du domaine concerné. Plaide en faveur de changements juridiques et politiques et défend les intérêts du client par le biais d'un large éventail de productions écrites et orales, y compris des mémoires et des procédures juridique.
	Formation, éducation et sensibilisation (TEA)	Assure la formation du personnel dans le domaine concerné. Élabore, planifie, coordonne, dispense et/ou évalue des cours, des méthodes et des techniques de formation, selon le cas.

Catégories	Spécialités	Description des spécialités
	Gestion de la cybersécurité (MGT)	Supervise le programme de cybersécurité d'un système ou d'un réseau informatique, y compris la gestion des impacts sur la sécurité de l'information au sein de l'organisation, d'un programme spécifique ou d'un autre domaine de responsabilité, notamment en ce qui concerne la stratégie, le personnel, l'infrastructure, les exigences, l'application des politiques, la planification des mesures d'urgence, la sensibilisation à la sécurité et d'autres ressources.
	Planification et politique stratégiques (PPS)	Élabore des politiques et des plans et/ou préconise des changements de politique pour soutenir les initiatives organisationnelles dans le domaine du cyberespace ou les changements/améliorations nécessaires.
	Cadre en cybersécurité (EXL)	Supervise, gère et/ou dirige le travail et les employés qui effectuent des travaux dans le domaine de la cybersécurité, liés à la cybersécurité et/ou aux opérations cybers.
	Gestion de programme/projet et acquisition (PMA)	Applique la connaissance des données, des informations, des processus, des interactions organisationnelles, des compétences et de l'expertise analytique, ainsi que des systèmes, des réseaux et des capacités d'échange d'informations pour gérer les programmes d'acquisition. Exécute les tâches régissant les programmes d'acquisition de matériel, de logiciels et de systèmes informatiques, ainsi que d'autres politiques de gestion des programmes. Fournit un soutien direct aux acquisitions qui utilisent les technologies de l'information (TI) (y compris les systèmes de sécurité nationale), en appliquant les lois et les politiques relatives aux TI, et fournit des orientations en matière de TI tout au long du cycle de vie de l'acquisition.
Protéger et défendre (PR)	Analyse cyberdéfense (CDA)	Utilise des mesures défensives et des informations recueillies auprès de diverses sources pour identifier, analyser et signaler les événements qui se produisent ou pourraient se produire au sein du réseau afin de protéger les informations, les systèmes d'information et les réseaux contre les menaces.
	Support d'infrastructure cyberdéfense (INF)	Teste, met en œuvre, déploie, entretient, examine et administre le matériel et les logiciels d'infrastructure nécessaires pour gérer efficacement le réseau et les ressources du fournisseur de services qui assurent la défense du réseau informatique. Surveille le réseau pour prendre en charge les activités non autorisées.
	Réponse aux incidents (CIR)	Répond aux crises ou aux situations urgentes dans le domaine concerné afin d'atténuer les menaces immédiates et potentielles. Utilise en fonction des besoins des méthodes d'atténuation, de préparation, d'intervention et de récupération afin de maximiser la survie des personnes, la préservation des biens et la sécurité de

Catégories	Spécialités	Description des spécialités
		l'information. Enquête sur toutes les activités d'intervention pertinentes et les analyse.
	Évaluation et gestion des vulnérabilités (VAM)	Évalue les menaces et les vulnérabilités ; détermine les écarts par rapport aux configurations acceptables, à la politique de l'entreprise ou à la politique locale ; évalue le niveau de risque ; et élabore et/ou recommande des contre-mesures d'atténuation appropriées dans des situations opérationnelles et non opérationnelles.
Analyser (AN)	Analyse des menaces (TWA)	Identifie et évalue les capacités et les activités des cybercriminels ou des entités de renseignement étrangères ; formule des conclusions pour aider à initier ou à soutenir les enquêtes ou les activités des forces de l'ordre et du contre-espionnage.
	Analyse données d'exploitation (EXP)	Analyse les informations collectées afin d'identifier les vulnérabilités et les possibilités d'exploitation.
	Analyse multi-sources (ASA)	Analyse les informations sur les menaces provenant de sources, de disciplines et d'organismes multiples au sein de la communauté du renseignement. Synthétise et place les informations de renseignement dans leur contexte ; en tire des conclusions sur les implications possibles.
	Cibles (TGT)	Applique les connaissances actuelles sur une ou plusieurs régions, pays, entités non étatiques et/ou technologies.
	Analyse linguistique (LNG)	Met en œuvre des compétences linguistiques, culturelles et techniques pour appuyer la collecte et l'analyse d'informations et d'autres activités liées à la cybersécurité.
Collecter et exploiter (CO)	Opérations de collecte (CLO)	Exécute la collecte à l'aide de stratégies appropriées et dans le respect des priorités établies par le processus de gestion de la collecte.
	Planification opérationnelle cyber (OPL)	Effectue un travail approfondi et conjoint de ciblage et de planification de la cybersécurité. Recueille des informations et élabore des plans opérationnels détaillés ainsi que des ordres à l'appui des besoins. Effectue une planification stratégique et opérationnelle sur l'ensemble de la gamme des opérations pour les opérations intégrées dans le domaine de l'information et du cyberespace.
	Opérations cybers (OPS)	Réalise des activités visant à recueillir des éléments de preuve sur des entités criminelles ou des services de renseignement étrangers afin d'atténuer les menaces éventuelles ou en temps réel, de se protéger contre l'espionnage ou les menaces internes, le sabotage par des entités étrangères, les activités terroristes internationales, ou d'appuyer d'autres activités de renseignement.

Catégories	Spécialités	Description des spécialités
Enquêter (IN)	Cyber investigation (INV)	Applique des tactiques, des techniques et des procédures pour une gamme complète d'outils et de processus d'enquête comprenant, entre autres, des techniques d'entretien et d'interrogation, de surveillance, de contre-surveillance et de détection de la surveillance, et met en balance de manière appropriée les avantages des poursuites et ceux de la collecte de renseignements.
	Investigation numérique légale (FOR)	Recueille, traite, préserve, analyse et présente des preuves informatiques à l'appui de l'atténuation de la vulnérabilité des réseaux et/ou d'enquêtes criminelles, frauduleuses, de contre-espionnage ou d'application de la loi.

A.3 Fonctions du référentiel NICE

Tableau 3 fournit une description de chacune des fonctions décrites dans le référentiel NICE. Chaque fonction est identifiée par la catégorie et la spécialité, suivis d'un numéro séquentiel (par exemple, SP-RSK-001 est la première fonction de la catégorie SP et de la spécialité RSK). Certaines descriptions de fonctions proviennent de documents externes (par exemple, la Committee on National Security Systems Instruction [CNSSI] 4009) et incluent ces informations dans la colonne "description". Cette liste sera mise à jour régulièrement [1]. La source de référence pour la version la plus récente de ce document est le tableur de référence pour la publication spéciale 800-181 du NIST [4].

Tableau 3 - Fonctions du référentiel NICE

Catégories	Spécialités	Fonctions	ID des fonctions	Descriptions des fonctions
Provisionnement sécurisé (SP)	Gestion des risques (RSK)	Responsable de l'autorisation / Représentant désigné	SP-RSK-001	Dirigeant ou cadre supérieur ayant le pouvoir d'assumer officiellement la responsabilité de l'exploitation d'un système d'information à un niveau de risque acceptable pour les opérations de l'organisation (y compris la mission, les fonctions, l'image ou la réputation), les biens de l'organisation, les individus, d'autres organisations et la nation (CNSSI 4009).
		Contrôleur de sécurité	SP-RSK-002	Effectue des évaluations indépendantes et complètes des mesures de sécurité managériales, opérationnelles et techniques, ainsi que des améliorations des mesures de sécurité mises en œuvre au sein d'un système d'information ou dont celui-ci a hérité, afin de déterminer l'efficacité globale des mesures de sécurité (telles que définies dans la norme NIST SP 800-37).
	Développement de logiciels (DEV)	Développeur de logiciels	SP-DEV-001	Développe, crée, entretient et écrit/code de nouvelles applications informatiques, des logiciels ou des programmes utilitaires spécialisés (ou modifie des applications existantes)

Catégories	Spécialités	Fonctions	ID des fonctions	Descriptions des fonctions
		Contrôleur de la sécurité des logiciels	SP-DEV-002	Analyse la sécurité des applications informatiques, des programmes informatiques ou des programmes spécialisés, nouveaux ou existants, et fournit des conclusions exploitables.
	Architecture des systèmes (ARC)	Architecte d'entreprise	SP-ARC-001	Développe et maintient des processus d'affaires, de systèmes et d'information pour soutenir les besoins de la mission de l'entreprise ; développe des règles et des exigences en matière de technologies de l'information (TI) qui décrivent les architectures de base et les architectures cibles.
		Architecte sécurité	SP-ARC-002	Veille à ce que les exigences de sécurité des parties prenantes nécessaires pour protéger la mission et les processus opérationnels de l'organisation soient correctement prises en compte dans tous les aspects de l'architecture d'entreprise, y compris les modèles de référence, les architectures de secteurs et de solutions, et les systèmes qui en résultent et qui soutiennent ces missions et processus opérationnels.
	R&D technologique (TRD)	Spécialiste en recherche et développement	SP-TRD-001	Mène des recherches sur l'ingénierie des logiciels et des systèmes et sur les systèmes logiciels afin de développer de nouvelles capacités, en veillant à ce que la cybersécurité soit pleinement intégrée. Il effectue des recherches technologiques approfondies afin d'évaluer les vulnérabilités potentielles des systèmes informatiques.
	Planification des exigences système (SRP)	Planificateur des besoins fonctionnels	SP-SRP-001	Consulte les clients pour évaluer les besoins fonctionnels et les traduire en solutions techniques.
	Test et évaluation (TST)	Spécialiste des essais et de l'évaluation des systèmes	SP-TST-001	Planifie, prépare et réalise des essais de systèmes afin d'évaluer les résultats par rapport aux spécifications et aux exigences, ainsi que d'analyser les résultats des essais et d'en rendre compte.

Catégories	Spécialités	Fonctions	ID des fonctions	Descriptions des fonctions
	Développement de systèmes (SYS)	Développeur de la sécurité des systèmes d'information	SP-SYS-001	Conçoit, développe, teste et évalue la sécurité des systèmes d'information tout au long du cycle de développement des systèmes.
		Développeur de systèmes	SP-SYS-002	Conçoit, développe, teste et évalue les systèmes d'information tout au long du cycle de développement des systèmes.
Exploitation et maintenance (OM)	Administration des données (DTA)	Administrateur de base de données	OM-DTA-001	Administre les bases de données et/ou les systèmes de gestion des données qui permettent de stocker, de consulter, de protéger et d'utiliser les données en toute sécurité.
		Analyste de données	OM-DTA-002	Examine des données provenant de sources multiples et disparates dans le but de fournir des informations sur la sécurité et la protection de la vie privée. Conçoit et met en œuvre des algorithmes personnalisés, des processus de flux de travail et des mises en page pour des ensembles de données complexes à l'échelle de l'entreprise, utilisés à des fins de modélisation, d'exploration de données et de recherche.
	Gestion des connaissances (KMG)	Gestionnaire des connaissances	OM-KMG-001	Responsable de la gestion et de l'administration des processus et des outils qui permettent à l'organisation d'identifier, de documenter et d'accéder au capital intellectuel ainsi qu'aux connaissances et aux contenus.
	Service à la clientèle et support technique (STS)	Spécialiste du support technique	OM-STS-001	Fournit une assistance technique aux clients qui ont besoin d'aide pour utiliser le matériel et les logiciels de l'entreprise conformément aux processus organisationnels établis ou approuvés (c'est-à-dire le plan directeur de gestion des incidents, le cas échéant).
	Services réseaux (NET)	Spécialiste des opérations réseau	OM-NET-001	Planifie, met en œuvre et exploite des services/systèmes de réseau, y compris des environnements matériels et virtuels.

Catégories	Spécialités	Fonctions	ID des fonctions	Descriptions des fonctions
	Administration des systèmes (ADM)	Administrateur système	OM-ADM-001	Responsable de la mise en place et de la maintenance d'un système ou de composants spécifiques d'un système (par exemple, installation, configuration et mise à jour du matériel et des logiciels ; création et gestion des comptes d'utilisateurs ; supervision ou exécution des tâches de sauvegarde et de récupération ; mise en œuvre des mesures de sécurité opérationnelles et techniques ; et respect des politiques et procédures de sécurité de l'organisation).
	Analyse des systèmes (ANA)	Analyste de la sécurité des systèmes	OM-ANA-001	Responsable pour l'analyse et le développement de l'intégration, des tests, des opérations et de la maintenance de la sécurité des systèmes.
Superviser et gouverner (OV)	Conseil juridique et défense des intérêts (LGA)	Conseiller juridique cyber	OV-LGA-001	Fournit des conseils juridiques et des recommandations sur des sujets pertinents liés au droit de l'informatique.
		Responsable de la protection de la vie privée/responsable du respect de la vie privée	OV-LGA-002	Développe et supervise le programme de conformité en matière de protection de la vie privée et le personnel chargé de ce programme, en répondant aux besoins des responsables de la protection de la vie privée et de la sécurité et de leurs équipes en matière de conformité, de gouvernance/politique et d'intervention en cas d'incident.
	Formation, éducation et sensibilisation (TEA)	Créateur de formation en cybersécurité	OV-TEA-001	Élabore, planifie, coordonne et évalue les cours, les méthodes et les techniques de formation et d'éducation en matière de cybersécurité, en fonction des besoins pédagogiques.
		Instructeur en cybersécurité	OV-TEA-002	Élabore et dispense une formation ou un enseignement au personnel dans le domaine cyber.
	Gestion de la cybersécurité (MGT)	Responsable de la sécurité des systèmes d'information	OV-MGT-001	Responsable de la cybersécurité d'un programme, d'une organisation, d'un système ou d'une zone de sécurité.

Catégories	Spécialités	Fonctions	ID des fonctions	Descriptions des fonctions
		Responsable de la sécurité des communications (COMSEC)	OV-MGT-002	Gère les ressources de sécurité des communications (COMSEC) d'une organisation (CNSSI 4009) ou a la garde des clefs d'un système de gestion des clefs cryptographiques (CKMS).
	Planification et politique stratégiques (PPS)	Responsable du développement et de la gestion des effectifs cyber	OV-SPP-001	Élabore des plans, des stratégies et des orientations concernant les effectifs cyber afin de répondre aux besoins en matière de ressources humaines, de personnel, de formation et d'éducation dans le domaine cyber et de tenir compte des modifications apportées à la politique, à la doctrine, au matériel, à la structure des forces et aux besoins en matière de formation et d'éducation dans ce domaine.
		Planificateur de la politique et de la stratégie cyber	OV-SPP-002	Élabore et actualise des plans, des stratégies et des politiques en matière de cybersécurité afin de soutenir et d'aligner les initiatives de l'organisation en matière de cybersécurité et de conformité aux réglementations.
	Cadre en cybersécurité (EXL)	Cadre dirigeant en cybersécurité	OV-EXL-001	Prend des décisions et définit la vision et l'orientation des ressources et/ou des opérations d'une organisation dans le domaine cyber et en rapport avec la cybersécurité.
	Gestion de programme / projet (PMA) et acquisition	Responsable de programme	OV-PMA-001	Dirige, coordonne, communique, intègre et est responsable de la réussite globale du programme, en veillant à l'aligner sur les priorités de l'agence ou de l'entreprise.
		Chef de projet informatique	OV-PMA-002	Gère des projets informatiques.
		Responsable du support produit	OV-PMA-003	Gère l'ensemble des fonctions de support nécessaires pour mettre en œuvre et maintenir l'état de préparation et la capacité opérationnelle des systèmes et des composants.
		Gestionnaire d'investissement/portefeuille informatique	OV-PMA-004	Gère un portefeuille d'investissements informatiques conformes aux besoins globaux de la mission et aux priorités de l'entreprise.

Catégories	Spécialités	Fonctions	ID des fonctions	Descriptions des fonctions
		Auditeur de projet informatique	OV-PMA-005	Effectue des évaluations d'un projet informatique ou de ses composants individuels afin de déterminer leur conformité avec les normes publiées.
Protéger et défendre (PR)	Analyse cyberdéfense (CDA)	Analyste en cyberdéfense	PR-CDA-001	Utilise les données collectées à partir de divers outils de cyberdéfense (par exemple, alertes IDS, pare-feu, journaux de trafic réseau) pour analyser les événements qui se produisent dans l'environnement afin de limiter les menaces.
	Support d'infrastructure cyberdéfense (INF)	Spécialiste du support à l'infrastructure de cyberdéfense	PR-INF-001	Teste, met en œuvre, déploie, entretient et administre le matériel et les logiciels de l'infrastructure.
	Réponse aux incidents (CIR)	Intervenant sur les incidents de cyberdéfense	PR-CIR-001	Enquête, analyse et répond aux incidents cybers dans l'environnement du réseau ou de la zone de sécurité.
	Évaluation et gestion des vulnérabilités (VAM)	Analyste de l'évaluation des vulnérabilités	PR-VAM-001	Procède à l'évaluation des systèmes et des réseaux au sein de l'environnement réseau ou de la zone de sécurité et identifie les cas où ces systèmes/réseaux s'écartent des configurations acceptables, de la politique de la zone de sécurité ou de la politique locale. Mesure l'efficacité de l'architecture de défense en profondeur contre les vulnérabilités connues.
Analyser (AN)	Analyse des menaces (TWA)	Analyste des menaces et des alertes	AN-TWA-001	Élabore des indicateurs cybers pour se tenir au courant de l'état de l'environnement opérationnel fortement évolutif. Recueille, traite, analyse et diffuse les évaluations des cybermenaces et des alertes.

Catégories	Spécialités	Fonctions	ID des fonctions	Descriptions des fonctions
	Analyse données d'exploitation (EXP)	Analyste exploitation	AN-EXP-001	Collabore à l'identification des lacunes en matière d'accès et de collecte qui peuvent être comblées par des activités de collecte cyber et/ou de préparation. Exploite toutes les ressources et techniques d'analyse autorisées pour pénétrer dans les réseaux ciblés.
	Analyse multi-sources (ASA)	Analyste multi-sources	AN-ASA-001	Analyse les données/informations provenant d'une ou de plusieurs sources afin de préparer l'environnement, de répondre aux demandes d'informations et de soumettre les exigences en matière de collecte et de production de renseignements pour soutenir la planification et les opérations.
		Spécialiste de l'évaluation des missions	AN-ASA-002	Élabore des plans d'évaluation et des mesures de performance/efficacité. Réalise des évaluations de l'efficacité stratégique et opérationnelle, selon les besoins, pour les événements cybers. Détermine si les systèmes ont fonctionné comme prévu et contribue à la détermination de l'efficacité opérationnelle.
	Cibles (TGT)	Développeur de cibles	AN-TGT-001	Analyse les systèmes cibles, constitue et/ou tient à jour des dossiers électroniques sur les cibles, en y incluant des données provenant de la préparation de l'environnement et/ou de sources de renseignement internes ou externes. Assure la coordination avec les activités de ciblage des partenaires et les organisations de renseignement, et présente des cibles candidates à des fins d'examen et de validation.

Catégories	Spécialités	Fonctions	ID des fonctions	Descriptions des fonctions
		Analyste réseau cibles	AN-TGT-002	Effectue une analyse avancée des données collectées et des données provenant de sources publiques afin d'assurer le suivi des cibles, d'établir le profil des cibles et de leurs activités et de mettre au point des techniques permettant d'obtenir davantage d'informations sur ces dernières. Détermine la manière dont les cibles communiquent, se déplacent, opèrent et évoluent en se basant sur la connaissance des technologies des cibles, des réseaux numériques et des applications qu'ils contiennent.
	Analyse linguistique (LNG)	Analyste linguistique pluridisciplinaire	AN-LNG-001	Applique son expertise en matière de langue et de culture à la cible, à la menace et aux connaissances techniques pour traiter, analyser et/ou diffuser des informations de renseignement tirées de la langue, de la voix et/ou de documents graphiques. Crée et tient à jour des bases de données et des outils de travail spécifiques à une langue afin de faciliter l'exécution d'actions cybers et d'assurer le partage des connaissances essentielles. Fournit une expertise en la matière dans le cadre de projets interdisciplinaires ou à forte intensité de langues étrangères.
Collecter et exploiter (CO)	Opérations de collecte (CLO)	Gestionnaire de collecte multi-sources	CO-CLO-001	Identifie les autorités et l'environnement de la collecte ; intègre les exigences prioritaires en matière d'information dans la gestion de la collecte ; élabore des concepts pour répondre à l'intention des dirigeants. Détermine les capacités des moyens de collecte disponibles, identifie les nouvelles capacités de collecte, élabore et diffuse des plans de collecte. Surveille l'exécution des tâches de collecte afin de garantir l'exécution efficace du plan de collecte

Catégories	Spécialités	Fonctions	ID des fonctions	Descriptions des fonctions
		Gestionnaire des besoins pour la collecte multi-sources	CO-CLO-002	Évalue les opérations de collecte et élabore des stratégies d'exigences en matière de collecte fondées sur les effets, en utilisant les sources et les méthodes disponibles pour améliorer la collecte. Élabore, traite, valide et coordonne la présentation des besoins en matière de collecte. Évalue les performances des moyens de collecte et des opérations de collecte.
	Planification opérationnelle cyber (OPL)	Planificateur en matière de renseignement cyber	CO-OPL-001	Élabore des programmes de renseignement détaillés pour répondre aux exigences des opérations cybers. Collabore avec les planificateurs des opérations cybers afin d'identifier, de valider et d'établir les besoins en matière de collecte et d'analyse. Participe à la sélection, à la validation, à la synchronisation et à l'exécution des actions cybers. Synchronise les activités de renseignement pour soutenir les objectifs de l'organisation dans le cyberespace.
		Planificateur d'opérations cyber	CO-OPL-002	Élabore des plans détaillés pour la conduite ou le soutien des opérations cybers concernées, en collaboration avec d'autres planificateurs, opérateurs et/ou analystes. Participe à la sélection, à la validation et à la synchronisation des cibles et permet l'intégration pendant l'exécution des actions cybers.
		Planificateur de l'intégration des partenaires	CO-OPL-003	S'efforce de faire progresser la coopération entre les partenaires des opérations informatiques par-delà les frontières organisationnelles ou nationales. Contribue à l'intégration des équipes cybers des partenaires en fournissant des orientations, des ressources et en collaborant à l'élaboration de bonnes pratiques et en facilitant le soutien organisationnel en vue d'atteindre les objectifs dans le cadre d'actions cybers intégrées.

Catégories	Spécialités	Fonctions	ID des fonctions	Descriptions des fonctions
	Opérations cybers (OPS)	Opérateur cyber	CO-OPS-001	Effectue la collecte, le traitement et/ou la géolocalisation de systèmes afin d'exploiter, de localiser et/ou de suivre des cibles d'intérêt. Navigue sur le réseau, effectue des analyses tactiques et, selon les instructions, exécute des opérations sur le réseau.
Enquêter (IN)	Cyber investigation (INV)	Enquêteur en cybercriminalité	IN-INV-001	Identifie, collecte, examine et préserve les preuves en utilisant des techniques d'analyse et d'enquête contrôlées et documentées.
	Investigation numérique (FOR)	Analyste criminalistique dans le domaine judiciaire et du contre-espionnage	IN-FOR-001	Mène des enquêtes détaillées sur les délits informatiques en établissant des preuves documentaires ou physiques, notamment des supports numériques et des journaux associés à des incidents de cyber intrusion.
		Analyste criminalistique en cyberdéfense	IN-FOR-002	Analyse les preuves numériques et enquête sur les incidents de sécurité informatique pour en tirer des informations utiles à l'atténuation des vulnérabilités des systèmes/réseaux.

A.4 Tâches du référentiel NICE

Tableau 4 répertorie toutes les tâches qui ont été identifiées comme faisant partie des fonctions liées à la cybersécurité. Chaque fonction comprend un sous-ensemble des tâches énumérées ici. Cette liste sera mise à jour régulièrement [1]. La source de référence pour la version la plus récente de ce document est le tableur de référence de la publication spéciale 800-181 du NIST [4].

Tableau 4 - Tâches du référentiel NICE

ID des tâches	Description des tâches
T0001	Obtenir et gérer les ressources nécessaires, y compris le soutien de la direction, les ressources financières et le personnel de sécurité clef, pour appuyer les buts et objectifs en matière de sécurité des technologies de l'information (TI) et réduire le risque organisationnel global.
T0002	Acquérir les ressources nécessaires, y compris financières, pour conduire un programme efficace de continuité des opérations de l'entreprise.
T0003	Conseiller la direction générale (par exemple, le directeur des systèmes d'information) sur les niveaux de risque et la posture de sécurité.
T0004	Conseiller la direction générale (par exemple, le DSI) sur l'analyse coût/bénéfice des programmes, des politiques, des processus, des systèmes et des éléments de sécurité de l'information.
T0005	Informer la direction générale ou l'autorité compétente des changements affectant la posture de cybersécurité de l'organisation.
T0006	Défendre la position officielle de l'organisation dans les procédures juridiques et législatives.
T0007	Analyser et définir les exigences et les spécifications en matière de données.
T0008	Analyser et planifier les changements anticipés dans les exigences de capacité des données.
T0009	Analyser l'information pour déterminer, recommander et planifier le développement d'une nouvelle application ou la modification d'une application existante.
T0010	Analyser les politiques et les configurations de cybersécurité de l'organisation et évaluer la conformité avec les réglementations et les directives de l'organisation.
T0011	Analyser les besoins des utilisateurs et les exigences logicielles pour déterminer la faisabilité de la conception dans le respect des contraintes de temps et de coût.
T0012	Analyser les contraintes de conception, analyser les compromis et la conception détaillée du système et de la sécurité, et prendre en compte le support du cycle de vie.
T0013	Appliquer les normes de codage et de test, mettre en œuvre les outils de test de sécurité, y compris les outils d'analyse statique de code de type "fuzzing", et procéder à des revues de code.
T0014	Appliquer une documentation de code sécurisée.
T0015	Appliquer des politiques de sécurité aux applications qui s'interfacent les unes avec les autres, telles que les applications interentreprises (B2B).
T0016	Appliquer des politiques de sécurité pour atteindre les objectifs de sécurité du système.
T0017	Appliquer les principes de l'architecture de sécurité orientée service pour répondre aux exigences de confidentialité, d'intégrité et de disponibilité de l'organisation.
T0018	Évaluer l'efficacité des mesures de cybersécurité utilisées par le(s) système(s).
T0019	Évaluer les menaces et les vulnérabilités des systèmes informatiques afin de définir un profil de risque de sécurité.
T0020	Développer le contenu des outils de cyberdéfense.

ID des tâches	Description des tâches
T0021	Construire, tester et modifier des prototypes de produits en utilisant des modèles de travail ou des modèles théoriques.
T0022	Recenser les mesures de sécurité utilisées pendant la phase d'élaboration des exigences afin d'intégrer la sécurité dans le processus, d'identifier les objectifs de sécurité clefs et de maximiser la sécurité des logiciels tout en réduisant au minimum les perturbations des plans et des calendriers.
T0023	Caractériser et analyser le trafic réseau afin d'identifier les activités anormales et les menaces potentielles pour les ressources du réseau.
T0024	Collecter et tenir à jour les données nécessaires à l'établissement de rapports sur la cybersécurité des systèmes.
T0025	Communiquer l'importance de la sécurité des technologies de l'information (TI) à tous les niveaux de l'organisation.
T0026	Compiler et rédiger la documentation relative au développement du programme et aux révisions ultérieures, en insérant des commentaires dans les instructions codées afin que d'autres puissent comprendre le programme.
T0027	Analyser les fichiers journaux, les preuves et autres informations afin de déterminer les meilleures méthodes pour identifier le(s) auteur(s) d'une intrusion dans un réseau.
T0028	Effectuer et/ou contribuer à des tests d'intrusion autorisés sur les ressources du réseau de l'entreprise.
T0029	Effectuer des tests fonctionnels et des tests de connectivité pour garantir la continuité de l'exploitation.
T0030	Réaliser des exercices de formation interactifs pour créer un environnement d'apprentissage efficace.
T0031	Conduire des entretiens avec des victimes et des témoins et mener des entretiens ou des interrogatoires avec des suspects.
T0032	Effectuer des évaluations de l'impact sur la vie privée (PIA) de la conception de la sécurité de l'application pour les mesures de sécurité appropriées, qui protègent la confidentialité et l'intégrité des données personnelles (PII).
T0033	Effectuer une analyse des risques, une étude de faisabilité et/ou une analyse de compromis pour développer, documenter et affiner les exigences fonctionnelles et les spécifications.
T0034	Se concerter avec des analystes de systèmes, des ingénieurs, des programmeurs, etc. pour concevoir l'application et obtenir des informations sur les limites et les capacités du projet, les exigences de performance et les interfaces.
T0035	Configurer et optimiser les concentrateurs, les routeurs et les commutateurs du réseau (par exemple, protocoles de niveau supérieur, tunneling).
T0036	Confirmer ce que l'on sait d'une intrusion et découvrir de nouvelles informations, si possible, après avoir identifié l'intrusion par une analyse dynamique.
T0037	Construire des chemins d'accès à des suites d'informations (par exemple, des pages de liens) pour faciliter l'accès des utilisateurs finaux.
T0038	Établir un modèle de menace sur la base d'entretiens avec le client et de ses besoins.
T0039	Consulter les clients pour évaluer les exigences fonctionnelles.
T0040	Consulter le personnel d'ingénierie pour évaluer l'interface entre le matériel et le logiciel.
T0041	Coordonner et fournir un soutien technique expert aux techniciens de cyberdéfense à l'échelle de l'entreprise pour résoudre les incidents de cyberdéfense.
T0042	Se coordonner avec les analystes de la cyberdéfense pour gérer et administrer la mise à jour des règles et des signatures (par exemple, systèmes de détection/protection contre les intrusions, antivirus et listes noires de contenu) pour les applications spécialisées de cyberdéfense.

ID des tâches	Description des tâches
T0043	Se coordonner avec le personnel de cyberdéfense à l'échelle de l'entreprise pour valider les alertes réseau.
T0044	Collaborer avec les parties prenantes pour établir le programme, la stratégie et l'assurance de la mission de continuité des opérations de l'entreprise.
T0045	Assurer la coordination avec les architectes et les développeurs de systèmes, selon les besoins, afin de superviser l'élaboration de solutions de conception.
T0046	Corriger les erreurs en apportant les modifications appropriées et en revérifiant le programme pour s'assurer qu'il produit les résultats souhaités.
T0047	Corréler les données relatives aux incidents afin d'identifier les vulnérabilités spécifiques et formuler des recommandations permettant d'y remédier rapidement.
T0048	Créer une copie des éléments de preuve (c'est-à-dire une image numérique légale) qui garantit que les éléments de preuve originaux n'ont pas été modifiés involontairement, pour les utiliser dans le cadre des processus de récupération et d'analyse des données. Cela inclut, sans s'y limiter, les disques durs, les disquettes, les CD, les PDA, les téléphones portables, les GPS et tous les formats de bande.
T0049	Décrypter les données saisies en utilisant des moyens techniques.
T0050	Définir et hiérarchiser les capacités essentielles du système ou les fonctions métier nécessaires à la restauration partielle ou totale du système après une défaillance catastrophique.
T0051	Définir les niveaux appropriés de disponibilité du système en se basant sur les fonctions critiques de celui-ci et s'assurer que les exigences du système identifient les exigences appropriées en matière de reprise après sinistre et de continuité des opérations pour inclure toutes les exigences appropriées en matière de basculement/site alternatif, les exigences en matière de sauvegarde, et les exigences en matière de support matériel pour la reprise/restauration du système.
T0052	Définir la portée et les objectifs du projet en fonction des exigences du client.
T0053	Concevoir et développer des produits de cybersécurité ou des produits basés sur la cybersécurité.
T0054	Concevoir des politiques de groupe et des listes de contrôle d'accès pour assurer la compatibilité avec les normes de l'organisation, les règles de gestion et les besoins.
T0055	Concevoir le matériel, les systèmes d'exploitation et les applications logicielles pour répondre de manière adaptée aux exigences de cybersécurité.
T0056	Concevoir ou intégrer des capacités de sauvegarde des données adaptées dans la conception globale des systèmes, et s'assurer de l'existence de processus techniques et procéduraux appropriés pour les sauvegardes sécurisées des systèmes et le stockage protégé des données de sauvegarde.
T0057	Concevoir, développer et modifier des systèmes logiciels, en utilisant l'analyse scientifique et les modèles mathématiques pour prédire et mesurer les résultats et les conséquences de la conception.
T0058	Déterminer le niveau d'assurance des capacités développées sur la base des résultats des tests.
T0059	Élaborer un plan d'enquête sur un crime présumé, une violation ou une activité suspecte en utilisant des ordinateurs et Internet.
T0060	Comprendre les besoins et les exigences des utilisateurs finaux de l'information.
T0061	Développer et diriger les procédures et la documentation de test et de validation des systèmes.
T0062	Développer et documenter les exigences, les capacités et les contraintes pour les procédures et les processus de conception.

ID des tâches	Description des tâches
T0063	Développer et documenter les procédures opérationnelles standard d'administration des systèmes.
T0064	Examiner et valider les programmes, processus et exigences en matière de data mining et de data warehousing.
T0065	Développer et mettre en œuvre des procédures de sauvegarde et de récupération du réseau.
T0066	Développer et maintenir des plans stratégiques.
T0067	Développer des architectures ou des composants de systèmes conformes aux spécifications techniques.
T0068	Élaborer des normes, des politiques et des procédures en matière de données.
T0069	Élaborer une documentation détaillée sur la conception de la sécurité pour les spécifications des composants et des interfaces afin de soutenir la conception et le développement des systèmes.
T0070	Élaborer des plans de reprise après sinistre et des plans de continuité des opérations pour les systèmes en cours de développement et veiller à ce qu'ils soient testés avant d'être introduits dans un environnement de production.
T0071	Élaborer/intégrer des conceptions de cybersécurité pour les systèmes et les réseaux soumis à des exigences de sécurité à plusieurs niveaux ou à des exigences de traitement de données à plusieurs niveaux de classification principalement applicables aux organisations gouvernementales (par exemple, NON CLASSIFIÉ, SECRET et TOP SECRET).
T0072	Élaborer des méthodes pour contrôler et mesurer les risques, la conformité et les efforts d'assurance.
T0073	Élaborer de nouveaux matériels de sensibilisation et de formation ou identifier ceux qui existent déjà et qui sont adaptés aux publics visés.
T0074	Élaborer des politiques, des programmes et des lignes directrices pour la mise en œuvre.
T0075	Fournir un résumé technique des résultats conformément aux procédures de rapport établies.
T0076	Élaborer des stratégies de réduction des risques pour éliminer les vulnérabilités et recommander des modifications de la sécurité des systèmes ou de leurs composants, le cas échéant.
T0077	Développer un code sécurisé et une gestion des erreurs.
T0078	Développer des contre-mesures spécifiques de cybersécurité et des stratégies de réduction des risques pour les systèmes et/ou les applications.
T0079	Élaborer des spécifications pour garantir que les efforts en matière de risque, de conformité et d'assurance sont conformes aux exigences de sécurité, de résilience et de fiabilité au niveau de l'application logicielle, du système et de l'environnement réseau.
T0080	Élaborer des plans de test pour répondre aux spécifications et aux exigences.
T0081	Diagnostiquer les problèmes de connectivité du réseau.
T0082	Documenter et prendre en compte les exigences de l'organisation en matière de sécurité de l'information, d'architecture de cybersécurité et d'ingénierie de la sécurité des systèmes tout au long du cycle de vie de l'acquisition.
T0083	Établir des états des risques préliminaires ou résiduels en matière de sécurité pour l'exploitation des systèmes.
T0084	Utiliser des processus de gestion de la configuration sécurisée.
T0085	Veiller à ce que toutes les activités d'exploitation et de maintenance de la sécurité des systèmes soient correctement documentées et mises à jour chaque fois que nécessaire.
T0086	Veiller à ce que l'application des correctifs de sécurité pour les produits commerciaux intégrés dans la conception des systèmes respecte les délais imposés par l'autorité de gestion pour l'environnement opérationnel prévu.

ID des tâches	Description des tâches
T0087	Veiller à ce que la chaîne de traçabilité soit respectée pour tous les supports numériques acquis, conformément aux règles fédérales en matière de preuve.
T0088	Veiller à ce que les produits compatibles avec la cybersécurité ou d'autres technologies complémentaires de renforcement de la sécurité ramènent les risques identifiés à un niveau acceptable.
T0089	Veiller à ce que les mesures d'amélioration de la sécurité soient évaluées, validées et mises en œuvre selon les besoins.
T0090	Veiller à ce que les systèmes et les architectures acquis ou développés soient conformes aux lignes directrices de l'organisation en matière d'architecture de cybersécurité.
T0091	Veiller à ce que les inspections, les tests et les examens en matière de cybersécurité soient coordonnés pour l'environnement réseau.
T0092	Veiller à ce que les exigences en matière de cybersécurité soient intégrées dans le plan de continuité du système et/ou de l'organisation.
T0093	S'assurer que les capacités de protection et de détection sont achetées ou développées en utilisant l'approche de l'ingénierie de la sécurité des SI et sont cohérentes avec l'architecture de cybersécurité au niveau de l'organisation.
T0094	Établir et maintenir des canaux de communication avec les parties prenantes.
T0095	Établir une architecture globale de sécurité de l'information de l'entreprise (EISA) avec la stratégie globale de sécurité de l'organisation.
T0096	Établir des relations, le cas échéant, entre l'équipe de réponse aux incidents et d'autres groupes, tant internes (par exemple, le service juridique) qu'externes (par exemple, les organismes chargés de l'application de la loi, les fournisseurs, les professionnels des relations publiques).
T0097	Évaluer et approuver les efforts de développement afin de s'assurer que les mesures de sécurité de base sont correctement mises en place.
T0098	Évaluer les contrats pour s'assurer qu'ils sont conformes aux exigences financières, juridiques et à celles du programme.
T0099	Évaluer les analyses coûts/bénéfices, les analyses économiques et les analyses de risque dans le cadre du processus de prise de décision.
T0100	Évaluer des facteurs tels que les formats de rapport requis, les contraintes de coût et la nécessité de restrictions de sécurité pour déterminer la configuration du matériel.
T0101	Évaluer l'efficacité et l'exhaustivité des programmes de formation existants.
T0102	Évaluer l'efficacité des lois, règlements, politiques, normes ou procédures.
T0103	Examiner les données récupérées pour y trouver des informations pertinentes par rapport au problème posé.
T0104	Fusionner les analyses d'attaques de réseaux informatiques avec les opérations et les enquêtes criminelles et de contre-espionnage.
T0105	Identifier les composants ou les éléments, attribuer les fonctions de sécurité à ces éléments et décrire les relations entre les éléments.
T0106	Identifier d'autres stratégies de sécurité de l'information pour atteindre l'objectif de sécurité de l'organisation.
T0107	Identifier et diriger la résolution des problèmes techniques rencontrés lors des essais et de la mise en œuvre de nouveaux systèmes (par exemple, identifier et trouver des solutions de contournement pour les protocoles de communication qui ne sont pas interopérables).
T0108	Identifier et hiérarchiser les fonctions essentielles de l'entreprise en collaboration avec les parties prenantes de l'organisation.
T0109	Identifier et classer par ordre de priorité les fonctions ou sous-systèmes essentiels nécessaires pour soutenir les capacités essentielles ou les fonctions opérationnelles en vue

ID des tâches	Description des tâches
	d'une restauration ou d'un rétablissement après une défaillance du système ou lors d'un événement de rétablissement du système, sur la base des exigences globales du système en matière de continuité et de disponibilité.
T0110	Identifier et/ou déterminer si un incident de sécurité est une violation de la loi qui nécessite une action juridique spécifique.
T0111	Identifier les failles de codage les plus courantes à un niveau élevé.
T0112	Identifier les données ou les renseignements ayant une valeur probante pour soutenir le contre-espionnage et les enquêtes criminelles.
T0113	Identifier les preuves numériques à examiner et à analyser de manière à éviter toute altération involontaire.
T0114	Identifier les éléments de preuve du délit.
T0115	Identifier les implications des nouvelles technologies ou des mises à jour technologiques sur le programme de sécurité des technologies de l'information (TI).
T0116	Identifier les parties prenantes de la politique de l'organisation.
T0117	Identifier les implications en matière de sécurité et appliquer des méthodologies dans des environnements centralisés et décentralisés à travers les systèmes informatiques de l'entreprise dans le cadre du développement de logiciels.
T0118	Identifier les problèmes de sécurité liés à l'exploitation et à la gestion des logiciels en régime permanent et intégrer les mesures de sécurité qui doivent être prises lorsqu'un produit arrive en fin de vie.
T0119	Identifier, évaluer et recommander des produits de cybersécurité ou des produits compatibles avec la cybersécurité à utiliser dans un système et veiller à ce que les produits recommandés soient conformes aux exigences de l'organisation en matière d'évaluation et de validation.
T0120	Identifier, collecter et saisir des preuves documentaires ou physiques, y compris des supports numériques et des journaux associés à des incidents, des enquêtes et des opérations d'intrusion informatique.
T0121	Mettre en œuvre de nouvelles procédures de conception de systèmes, des procédures d'essai et des normes de qualité.
T0122	Mettre en œuvre des modèles de sécurité pour les systèmes nouveaux ou existants.
T0123	mettre en œuvre des contre-mesures spécifiques de cybersécurité pour les systèmes et/ou les applications.
T0124	Incorporer des solutions de détection des vulnérabilités en matière de cybersécurité dans la conception des systèmes (par exemple : alertes sur les vulnérabilités en matière de cybersécurité).
T0125	Installer et entretenir les systèmes d'exploitation des équipements de l'infrastructure réseau (par exemple, IOS, microprogrammes).
T0126	Installer ou remplacer des concentrateurs, des routeurs et des commutateurs de réseau.
T0127	Intégrer et aligner les politiques de sécurité de l'information et/ou de cybersécurité pour s'assurer que l'analyse des systèmes répond aux exigences de sécurité.
T0128	Intégrer des capacités automatisées de mise à jour ou de correction des logiciels système lorsque cela est possible et élaborer des processus et des procédures pour la mise à jour et la correction manuelles des logiciels système sur la base des exigences actuelles et prévues en matière de délais de correction pour l'environnement opérationnel du système.
T0129	Intégrer les nouveaux systèmes dans l'architecture réseau existante.
T0130	Assurer l'interface avec les organisations externes (par exemple, les affaires publiques, les forces de l'ordre, le commandement ou l'inspecteur général concerné) afin de garantir une

ID des tâches	Description des tâches
	diffusion appropriée et précise des informations sur les incidents et autres informations relatives à la défense des réseaux informatiques.
T0131	Interpréter et appliquer les lois, règlements, politiques, normes ou procédures à des situations spécifiques.
T0132	Interpréter et/ou approuver les exigences de sécurité en fonction des capacités des nouvelles technologies de l'information.
T0133	Interpréter les schémas de non-conformité afin de déterminer leur impact sur les niveaux de risque et/ou l'efficacité globale du programme de cybersécurité de l'entreprise.
T0134	Diriger et aligner les priorités en matière de sécurité des technologies de l'information (TI) sur la stratégie de sécurité.
T0135	Diriger et superviser le budget, la dotation en personnel et les contrats relatifs à la sécurité de l'information.
T0136	Maintenir la sécurité des systèmes de base conformément aux politiques de l'organisation.
T0137	Assurer la maintenance des logiciels des systèmes de gestion des bases de données.
T0138	Assurer la maintenance des outils d'audit de cyberdéfense déployables (par exemple, des logiciels et du matériel spécialisés dans la cyberdéfense) pour soutenir les missions d'audit de cyberdéfense.
T0139	Maintenir des services de réplication d'annuaire qui permettent de répliquer automatiquement les informations des serveurs dorsaux vers les unités frontales par le biais d'un routage optimisé.
T0140	Maintenir les échanges d'informations grâce à des fonctions de publication, d'abonnement et d'alerte qui permettent aux utilisateurs d'envoyer et de recevoir des informations essentielles en fonction des besoins.
T0141	Maintenir le matériel d'assurance et d'accréditation des systèmes d'information.
T0142	Maintenir la connaissance des politiques de cyberdéfense, des réglementations et des documents de conformité applicables, spécifiquement liés à l'audit de cyberdéfense.
T0143	Formuler des recommandations sur la base des résultats des tests.
T0144	Gérer les comptes, les droits réseau et l'accès aux systèmes et aux équipements.
T0145	Gérer et approuver les dossiers d'accréditation (par exemple, ISO/IEC 15026-2).
T0146	Gérer la compilation, le catalogage, la mise en cache, la distribution et l'extraction des données.
T0147	Gérer la surveillance des sources de données relatives à la sécurité de l'information afin de maintenir la connaissance de la position de l'organisation.
T0148	Gérer la publication d'orientations en matière de défense des réseaux informatiques (par exemple, TCNO, Concept of Operations, Net Analyst Reports, NTSM, MTO) à l'intention de l'entreprise.
T0149	Gérer l'analyse des menaces ou des cibles des informations relatives à la cyberdéfense et la production d'informations sur les menaces au sein de l'entreprise.
T0150	Surveiller et évaluer la conformité d'un système avec les exigences en matière de sécurité, de résilience et de fiabilité des technologies de l'information (TI).
T0151	Surveiller et évaluer l'efficacité des mesures de sauvegarde de l'entreprise en matière de cybersécurité afin de s'assurer qu'elles offrent le niveau de protection voulu.
T0152	Surveiller et maintenir les bases de données afin de garantir des performances optimales.
T0153	Surveiller la capacité et les performances du réseau.
T0154	Surveiller et rendre compte de l'utilisation des actifs et des ressources de gestion des connaissances.

ID des tâches	Description des tâches
T0155	Documenter et faire remonter les incidents (y compris l'historique de l'événement, le statut et l'impact potentiel pour une action ultérieure) qui peuvent avoir un impact continu et immédiat sur l'environnement.
T0156	Superviser la gestion de la configuration et formuler des recommandations à ce sujet.
T0157	Superviser le programme de formation et de sensibilisation à la sécurité de l'information.
T0158	Participer à une évaluation des risques en matière de sécurité de l'information dans le cadre du processus d'évaluation et d'autorisation de la sécurité.
T0159	Participer à l'élaboration ou à la modification des plans et des exigences du programme de cybersécurité de l'environnement informatique.
T0160	Corriger les vulnérabilités du réseau afin de garantir la protection des informations contre les tiers.
T0161	Analyser les fichiers journaux provenant de diverses sources (par exemple, journaux d'hôtes individuels, journaux de trafic réseau, journaux de pare-feu et journaux de systèmes de détection d'intrusion [IDS]) afin d'identifier d'éventuelles menaces pour la sécurité du réseau.
T0162	Effectuer la sauvegarde et la récupération des bases de données afin de garantir l'intégrité des données.
T0163	Effectuer le tri des incidents de cyberdéfense, notamment en déterminant la portée, l'urgence et l'impact potentiel, en identifiant la vulnérabilité spécifique et en formulant des recommandations permettant de remédier rapidement à la situation.
T0164	Effectuer des analyses et des rapports sur les tendances en matière de cyberdéfense.
T0165	Effectuer une analyse dynamique pour démarrer une "image" d'un disque (sans nécessairement disposer du disque original) afin de voir l'intrusion telle que l'utilisateur aurait pu la voir, dans un environnement natif.
T0166	Effectuer une corrélation d'événements en utilisant des informations recueillies à partir de diverses sources au sein de l'entreprise afin d'acquérir une connaissance de la situation et de déterminer l'efficacité d'une attaque observée.
T0167	Effectuer une analyse de la signature des fichiers.
T0168	Effectuer une comparaison des hachages par rapport à une base de données établie.
T0169	Effectuer des tests de cybersécurité sur les applications et/ou les systèmes développés.
T0170	Effectuer une investigation numérique légale initiale des images et inspecter les systèmes de l'entreprise afin de déterminer les mesures d'atténuation ou de correction possibles.
T0171	Effectuer des tests d'assurance qualité intégrés pour les fonctionnalités de sécurité et les attaques informatiques.
T0172	Effectuer des investigations numériques légales en temps réel (par exemple, en utilisant Helix en conjonction avec LiveView).
T0173	Effectuer une analyse de la chronologie.
T0174	Effectuer une analyse des besoins pour déterminer les possibilités de solutions nouvelles et améliorées en matière de processus d'entreprise.
T0175	Effectuer des tâches de traitement des incidents de cyberdéfense en temps réel (par exemple, investigations numériques légales, corrélation et suivi des intrusions, analyse des menaces et remédiation directe des systèmes) afin de soutenir les équipes de réaction aux incidents (IRT) déployables.
T0176	Effectuer une programmation sécurisée et identifier les failles potentielles dans les codes afin d'atténuer les vulnérabilités.
T0177	Effectuer des analyses de sécurité, identifier les lacunes dans l'architecture de sécurité et élaborer un plan de gestion des risques de sécurité.

ID des tâches	Description des tâches
T0178	Effectuer des analyses de sécurité et identifier les lacunes de l'architecture de sécurité, ce qui se traduit par des recommandations à inclure dans la stratégie d'atténuation des risques.
T0179	Effectuer des analyses statiques des médias.
T0180	Effectuer l'administration de systèmes sur des applications et des systèmes spécialisés de cyberdéfense (par exemple, antivirus, audit et remédiation) ou des équipements de réseaux privés virtuels (VPN), y compris l'installation, la configuration, la maintenance, la sauvegarde et la restauration.
T0181	Effectuer une analyse des risques (par exemple, menace, vulnérabilité et probabilité d'occurrence) chaque fois qu'une application ou un système fait l'objet d'un changement majeur.
T0182	Effectuer une analyse des logiciels malveillants de niveau 1, 2 et 3.
T0183	Effectuer des étapes de validation, en comparant les résultats réels aux résultats attendus et en analysant les différences pour identifier l'impact et les risques.
T0184	Planifier et mener des examens d'autorisation de sécurité ainsi que l'élaboration de cas d'assurance pour l'installation initiale de systèmes et de réseaux.
T0185	Planifier et gérer la réalisation de projets de gestion des connaissances.
T0186	Planifier, exécuter et vérifier la redondance des données et les procédures de récupération des systèmes.
T0187	Planifier et recommander des modifications ou des ajustements en fonction des résultats des exercices ou de l'environnement du système.
T0188	Préparer des rapports d'audit qui identifient les constatations techniques et procédurales et recommandent des stratégies/solutions de remédiation.
T0189	Préparer des diagrammes de flux de travail détaillés qui décrivent les entrées, les sorties et les opérations logiques, et les convertir en une série d'instructions codées dans un langage informatique.
T0190	Préparer les supports numériques pour l'imagerie en assurant l'intégrité des données (par exemple, les bloqueurs d'écriture conformément aux procédures opérationnelles standard).
T0191	Préparer des cas d'utilisation pour justifier le besoin de solutions spécifiques en matière de technologies de l'information (TI).
T0192	Préparer, distribuer et tenir à jour des plans, des instructions, des orientations et des procédures opérationnelles normalisées concernant la sécurité des opérations du/des système(s) de réseau.
T0193	Traiter les scènes de crime.
T0194	Documenter comme il convient toutes les activités de mise en œuvre, d'exploitation et de maintenance de la sécurité des systèmes et les mettre à jour si nécessaire.
T0195	Fournir un flux structuré d'informations pertinentes (via des portails web ou d'autres moyens) en fonction des exigences de la mission.
T0196	Fournir des recommandations sur les coûts du projet, les concepts de conception ou les modifications de la conception.
T0197	Fournir une évaluation technique précise d'une application logicielle, d'un système ou d'un réseau, en documentant la démarche de sécurité, les moyens et les vulnérabilités par rapport aux exigences de conformité en matière de cybersécurité.
T0198	Fournir des rapports de synthèse quotidiens sur les événements et les activités du réseau en rapport avec les pratiques de cyberdéfense.
T0199	Fournir des orientations en matière de cybersécurité de l'entreprise et de gestion des risques de la chaîne d'approvisionnement pour l'élaboration des plans de continuité des opérations.
T0200	Fournir un retour d'information sur les exigences en matière de réseau, y compris l'architecture et l'infrastructure du réseau.

ID des tâches	Description des tâches
T0201	Fournir aux clients ou aux équipes d'installation des directives pour la mise en œuvre des systèmes développés.
T0202	Fournir aux dirigeants des orientations en matière de cybersécurité.
T0203	Fournir des informations sur les exigences de sécurité à inclure dans les cahiers des charges et autres documents de passation de marchés appropriés.
T0204	Fournir des informations sur les plans de mise en œuvre et les procédures d'exploitation normalisées.
T0205	Fournir des informations sur les activités du référentiel de gestion des risques et les documents connexes (par exemple, les plans de soutien du cycle de vie des systèmes, le concept d'opérations, les procédures opérationnelles et les supports de formation à la maintenance).
T0206	Fournir un encadrement et des orientations au personnel des technologies de l'information (TI) en veillant à ce que ce personnel soit sensibilisé à la cybersécurité et reçoive des informations de base, des connaissances et une formation correspondant à ses responsabilités.
T0207	Fournir un soutien permanent en matière d'optimisation et de résolution des problèmes.
T0208	Fournir des recommandations sur les améliorations et les mises à niveau possibles.
T0209	Fournir des recommandations sur les structures de données et les bases de données qui garantissent une production correcte et de qualité des rapports et des informations de gestion.
T0210	Fournir des recommandations sur les nouvelles technologies et les architectures de bases de données.
T0211	Fournir des informations relatives aux systèmes sur les exigences en matière de cybersécurité à inclure dans les cahiers des charges et autres documents d'achat appropriés.
T0212	Fournir une assistance technique au personnel concerné sur les questions relatives aux preuves numériques.
T0213	Fournir des documents techniques, des rapports d'incidents, des conclusions d'examens d'ordinateurs, des résumés et d'autres informations sur la situation aux quartiers généraux les plus élevés.
T0214	Recevoir et analyser les alertes réseau provenant de diverses sources au sein de l'entreprise et déterminer les causes possibles de ces alertes.
T0215	Reconnaître une éventuelle violation de la sécurité et prendre les mesures appropriées pour signaler l'incident, le cas échéant.
T0216	Reconnaître les artefacts d'investigation numérique légale indiquant un système d'exploitation particulier et en rendre compte avec précision.
T0217	Traiter les implications en matière de sécurité dans la phase de recette des logiciels, y compris les critères d'achèvement, l'acceptation des risques et la documentation, les critères communs et les méthodes d'essais indépendants.
T0218	Recommander des mesures de sécurité, de résilience et de sûreté de fonctionnement nouvelles ou révisées en fonction des résultats des examens.
T0219	Recommander l'affectation des ressources nécessaires pour exploiter et maintenir en toute sécurité les exigences d'une organisation en matière de cybersécurité.
T0220	Résoudre les conflits dans les lois, règlements, politiques, normes ou procédures.
T0221	Examiner les documents d'autorisation et d'assurance pour confirmer que le niveau de risque se situe dans des limites acceptables pour chaque application logicielle, système et réseau.
T0222	Examiner les politiques existantes et celles qui sont en projet avec les parties prenantes.
T0223	Examiner ou mener des audits de programmes et de projets de technologies de l'information (TI).

ID des tâches	Description des tâches
T0224	Examiner la documentation relative à la formation (par exemple, les documents relatifs au contenu des cours [Course Content Documents ou CCD], les plans de cours, les textes destinés aux étudiants, les examens, les programmes d'enseignement [Schedules of Instruction ou SOI] et les descriptions de cours).
T0225	Sécuriser l'équipement électronique ou la source d'information.
T0226	Siéger aux conseils d'administration des agences et aux conseils interagences.
T0227	Recommander des politiques et coordonner leur examen et leur approbation.
T0228	Stocker, extraire et manipuler des données pour l'analyse des capacités et des besoins des systèmes.
T0229	Superviser ou gérer les mesures de protection ou de correction lorsqu'un incident de cybersécurité est détecté ou qu'une vulnérabilité est découverte.
T0230	Soutenir la conception et l'exécution de scénarios d'exercices.
T0231	Fournir un soutien aux activités de test et d'évaluation de la sécurité et de la certification.
T0232	Tester et entretenir l'infrastructure du réseau, y compris les équipements logiciels et matériels.
T0233	Suivre et documenter les incidents de cyberdéfense, de la détection initiale à la résolution finale.
T0234	Suivre les conclusions et les recommandations des audits afin de s'assurer que les mesures d'atténuation appropriées sont prises.
T0235	Traduire les exigences fonctionnelles en solutions techniques.
T0236	Traduire les exigences de sécurité en éléments de conception d'applications, notamment en documentant les éléments des surfaces d'attaque des logiciels, en procédant à une modélisation des menaces et en définissant tout critère de sécurité spécifique.
T0237	Dépanner le matériel et les logiciels du système.
T0238	Extraire des données à l'aide de techniques de fragmentation des données (par exemple, Forensic Tool Kit [FTK], Foremost).
T0239	Utiliser les documents publiés par le gouvernement fédéral et par l'organisation pour gérer les opérations de leur(s) système(s) informatique(s).
T0240	Capturer et analyser le trafic réseau associé à des activités malveillantes à l'aide d'outils de surveillance du réseau.
T0241	Utiliser des équipements et des techniques spécialisés pour cataloguer, documenter, extraire, collecter, emballer et préserver les preuves numériques.
T0242	Utiliser des modèles et des simulations pour analyser ou prévoir les performances des systèmes dans différentes conditions d'exploitation.
T0243	Vérifier et mettre à jour la documentation relative à la sécurité reflétant les caractéristiques de conception de la sécurité des applications/systèmes.
T0244	Vérifier que les principes de sécurité des logiciels d'application, des réseaux et des systèmes sont mis en œuvre comme prévu, documenter les écarts et recommander les actions nécessaires pour les corriger.
T0245	Vérifier que la documentation relative à l'accréditation et à l'assurance des applications logicielles/réseaux/systèmes est à jour.
T0246	Rédiger et publier des techniques de cyberdéfense, des orientations et des rapports sur les constatations d'incidents à l'intention des parties concernées.
T0247	Rédiger du matériel didactique (par exemple, des procédures opérationnelles normalisées, un manuel de production) afin de fournir des directives détaillées au personnel concerné.
T0248	Sensibiliser la direction aux questions de sécurité et veiller à ce que la vision et les objectifs de l'organisation reflètent des principes de sécurité solides.

ID des tâches	Description des tâches
T0249	Effectuer des recherches sur les technologies actuelles afin de comprendre les capacités du système ou du réseau concerné.
T0250	Identifier les capacités cybers pour le développement de matériel et de logiciels personnalisés en fonction des exigences de la mission.
T0251	Élaborer des processus de conformité en matière de sécurité et/ou des audits pour les services externes (par exemple, fournisseurs de services en nuage, centres de données).
T0252	Effectuer les examens requis, le cas échéant, dans l'environnement (par exemple, surveillance technique, examens des contre-mesures [TSCM], examens des contre-mesures TEMPEST).
T0253	Procéder à une analyse binaire sommaire.
T0254	Superviser les normes politiques et les stratégies de mise en œuvre afin de s'assurer que les procédures et les lignes directrices sont conformes aux politiques de cybersécurité.
T0255	Participer au processus de gouvernance des risques pour fournir des risques de sécurité, des mesures d'atténuation et des informations sur d'autres risques techniques.
T0256	Évaluer l'efficacité de la fonction d'approvisionnement pour ce qui est de répondre aux exigences en matière de sécurité de l'information et aux risques liés à la chaîne d'approvisionnement par le biais des activités d'approvisionnement, et recommander des améliorations.
T0257	Déterminer la portée, l'infrastructure, les ressources et la taille de l'échantillon de données afin de s'assurer que les exigences du système sont démontrées de manière adéquate.
T0258	Assurer dans les délais appropriés la détection, l'identification et l'alerte en cas d'attaques/intrusions, d'activités anormales et d'utilisations abusives, et distinguer ces incidents et événements des activités sans danger.
T0259	Utiliser des outils de cyberdéfense pour surveiller et analyser en permanence l'activité du système afin d'identifier les activités malveillantes.
T0260	Analyser les activités malveillantes identifiées afin de déterminer les faiblesses exploitées, les méthodes d'exploitation et les effets sur les systèmes et les informations.
T0261	Contribuer à l'identification, à la hiérarchisation et à la coordination de la protection des infrastructures critiques de cyberdéfense et des ressources clefs.
T0262	Utiliser les principes et pratiques approuvés de défense en profondeur (par exemple, défense en plusieurs endroits, défenses en couches, robustesse de la sécurité).
T0263	Identifier les exigences de sécurité spécifiques à un système de technologie de l'information (TI) dans toutes les phases du cycle de vie du système.
T0264	Veiller à ce que des plans d'action et des étapes ou des plans de remédiation soient en place pour les vulnérabilités identifiées lors d'évaluations des risques, d'audits, d'inspections, etc.
T0265	Assurer la réussite de la mise en œuvre et du bon fonctionnement des exigences de sécurité et des politiques et procédures appropriées en matière de technologies de l'information (TI) qui sont conformes à la mission et aux objectifs de l'organisation.
T0266	Effectuer les tests d'intrusion nécessaires pour les nouvelles applications ou les applications mises à jour.
T0267	Concevoir des contre-mesures et des mesures d'atténuation contre les exploitations potentielles des faiblesses et des vulnérabilités des langages de programmation dans les systèmes et les composants.
T0268	Définir et documenter la manière dont la mise en œuvre d'un nouveau système ou de nouvelles interfaces entre systèmes influe sur le niveau de sécurité de l'environnement existant.
T0269	Concevoir et développer des fonctions de gestion clefs (en rapport avec la cybersécurité).

ID des tâches	Description des tâches
T0270	Analyser les besoins et les exigences des utilisateurs afin de planifier et de mener à bien le développement de la sécurité des systèmes.
T0271	Élaborer des concepts de cybersécurité pour répondre à des besoins opérationnels spécifiques et à des facteurs environnementaux (par exemple, contrôles d'accès, applications automatisées, opérations en réseau, exigences en matière d'intégrité et de disponibilité élevées, sécurité multiniveaux/traitement de plusieurs niveaux de classification, et traitement d'informations confidentielles sensibles).
T0272	Veiller à ce que les activités de conception de la sécurité ainsi que les activités de développement de la cybersécurité soient correctement documentées (en fournissant une description fonctionnelle de la mise en œuvre de la sécurité) et mises à jour si nécessaire.
T0273	Élaborer et documenter les risques liés à la chaîne d'approvisionnement pour les éléments de systèmes critiques, le cas échéant.
T0274	Créer des preuves vérifiables des mesures de sécurité.
T0275	Soutenir les activités de conformité nécessaires (par exemple, veiller à ce que les lignes directrices relatives à la configuration de la sécurité des systèmes soient respectées et que le contrôle de la conformité soit effectué).
T0276	Participer au processus d'acquisition en fonction des besoins, en suivant les pratiques appropriées de gestion des risques liés à la chaîne d'approvisionnement.
T0277	Veiller à ce que toutes les acquisitions, tous les marchés et tous les efforts d'externalisation tiennent compte des exigences en matière de sécurité de l'information, conformément aux objectifs de l'organisation.
T0278	Recueillir les artefacts d'intrusion (par exemple, code source, logiciels malveillants, chevaux de Troie) et utiliser les données découvertes pour permettre l'atténuation des incidents potentiels de cybersécurité au sein de l'entreprise.
T0279	Servir d'expert technique et de liaison avec le personnel chargé de l'application de la loi et expliquer les détails de l'incident, le cas échéant.
T0280	Valider en permanence la conformité de l'organisation avec les politiques/lignes directrices/procédures/réglementations/lois.
T0281	Prévoir les demandes de services en cours et veiller à ce que les hypothèses de sécurité soient réexaminées si nécessaire.
T0282	Définir et/ou mettre en œuvre des politiques et des procédures pour assurer la protection des infrastructures critiques, le cas échéant.
T0283	Collaborer avec les parties prenantes pour identifier et/ou développer des solutions technologiques appropriées.
T0284	Concevoir et développer de nouveaux outils/technologies dans le domaine de la cybersécurité.
T0285	Effectuer des recherches de virus sur les supports numériques.
T0286	Effectuer des investigations numériques légales sur les systèmes de fichiers.
T0287	Effectuer une analyse statique pour monter une "image" d'un disque (sans nécessairement disposer du disque d'origine).
T0288	Effectuer une analyse statique des logiciels malveillants.
T0289	Utiliser la boîte à outils d'investigation numérique légale transportable pour soutenir les opérations, le cas échéant.
T0290	Déterminer les tactiques, techniques et procédures (TTP) pour les séquences d'intrusion.
T0291	Examiner les topologies de réseau pour comprendre les flux de données à travers le réseau.
T0292	Recommander des corrections de vulnérabilité de l'environnement informatique.
T0293	Identifier et analyser les anomalies dans le trafic réseau à l'aide de métadonnées.

ID des tâches	Description des tâches
T0294	Effectuer des recherches, des analyses et des corrélations à partir d'une grande variété d'ensembles de données provenant de toutes les sources (indications et avertissements).
T0295	Valider les alertes des systèmes de détection d'intrusion (IDS) en fonction du trafic réseau à l'aide d'outils d'analyse de paquets.
T0296	Isoler et supprimer les logiciels malveillants.
T0297	Identifier les applications et les systèmes d'exploitation d'un équipement réseau sur la base du trafic réseau.
T0298	Reconstituer une attaque ou une activité malveillante à partir du trafic réseau.
T0299	Identifier les activités de cartographie du réseau et de prise d'empreinte du système d'exploitation (OS).
T0300	Élaborer et documenter les exigences en matière d'expérience utilisateur (UX), y compris l'architecture de l'information et les exigences en matière d'interface utilisateur.
T0301	Élaborer et mettre en œuvre des processus d'audit indépendant de la cybersécurité pour les logiciels d'application, les réseaux et les systèmes et superviser les audits indépendants en cours afin de s'assurer que les processus et procédures opérationnels et de recherche et développement sont conformes aux exigences organisationnelles et aux obligations en matière de cybersécurité et qu'ils sont correctement suivis par les administrateurs de systèmes et les autres membres du personnel chargés de la cybersécurité dans l'exercice de leurs activités quotidiennes.
T0302	Rédiger des clauses contractuelles afin de garantir la sécurité de la chaîne d'approvisionnement, des systèmes, des réseaux et des opérations.
T0303	Identifier et exploiter le système de contrôle des versions à l'échelle de l'entreprise lors de la conception et du développement d'applications sécurisées.
T0304	Mettre en œuvre et intégrer les méthodologies du cycle de développement des systèmes (SDLC) (par exemple, IBM Rational Unified Process) dans l'environnement de développement.
T0305	Effectuer la gestion de la configuration, la gestion des problèmes, la gestion de la capacité et la gestion financière pour les bases de données et les systèmes de gestion des données.
T0306	Soutenir la gestion des incidents, la gestion des niveaux de service, la gestion des changements, la gestion des versions, la gestion de la continuité et la gestion de la disponibilité pour les bases de données et les systèmes de gestion des données.
T0307	Analyser les architectures candidates, attribuer les services de sécurité et sélectionner les mécanismes de sécurité.
T0308	Analyser les données relatives aux incidents pour déceler les tendances émergentes.
T0309	Évaluer l'efficacité des contrôles de sécurité.
T0310	Participer à l'élaboration de signatures qui peuvent être mises en œuvre sur des outils de réseau de cybersécurité en réponse à des menaces nouvelles ou observées dans l'environnement ou l'enclave du réseau.
T0311	Consulter les clients sur la conception et la maintenance des systèmes logiciels.
T0312	Coordonner avec les analystes du renseignement la mise en corrélation des données d'évaluation des menaces.
T0313	Concevoir et documenter des normes de qualité.
T0314	Élaborer un contexte de sécurité des systèmes, un concept préliminaire de sécurité des systèmes (CONOPS) et définir les exigences de base en matière de sécurité des systèmes conformément aux exigences applicables en matière de cybersécurité.
T0315	Élaborer et dispenser une formation technique pour former d'autres personnes ou répondre aux besoins des clients.
T0316	Élaborer ou participer à l'élaboration de modules ou de cours de formation informatisés.

ID des tâches	Description des tâches
T0317	Élaborer ou participer à l'élaboration de travaux pratiques.
T0318	Élaborer ou participer à l'élaboration des évaluations de cours.
T0319	Élaborer ou participer à l'élaboration de normes de notation et de compétence.
T0320	Participer à l'élaboration de plans de développement, de formation et/ou de remédiation individuels/collectifs.
T0321	Développer ou aider à développer des objectifs et des cibles en matière d'apprentissage.
T0322	Élaborer ou participer à l'élaboration de matériels ou de programmes de formation continue.
T0323	Élaborer ou participer à l'élaboration de tests écrits destinés à mesurer et à évaluer les compétences des apprenants.
T0324	Diriger la programmation informatique et l'élaboration de la documentation.
T0325	Documenter l'objectif d'un système et le concept préliminaire des opérations de sécurité du système.
T0326	Utiliser des processus de gestion de la configuration.
T0327	Évaluer les vulnérabilités de l'infrastructure réseau afin d'améliorer les capacités qui sont en train d'être développées.
T0328	Évaluer les architectures et les conceptions de sécurité afin de déterminer l'adéquation de la conception et de l'architecture de sécurité proposées ou fournies en réponse aux exigences contenues dans les documents d'acquisition.
T0329	Respecter les normes et processus du cycle de vie de l'ingénierie des logiciels et des systèmes.
T0330	Maintenir des systèmes de transmission de messages sécurisés.
T0331	Maintenir une base de données de suivi des incidents et de solutions.
T0332	Notifier aux responsables désignés, aux personnes chargées de répondre aux incidents cybers et aux membres de l'équipe du fournisseur de services de cybersécurité les incidents cybernétiques présumés et préciser l'historique, l'état et l'impact potentiel de l'événement en vue d'une action ultérieure conformément au plan d'intervention de l'organisation en cas d'incident cyber.
T0334	Veiller à ce que tous les composants des systèmes puissent être intégrés et alignés (par exemple, procédures, bases de données, politiques, logiciels et matériel).
T0335	Construire, installer, configurer et tester le matériel dédié à la cybersécurité.
T0336	RETIRÉ : Intégré à T0228
T0337	Superviser les programmeurs, les concepteurs, les techniciens, les ingénieurs et autres personnels techniques et scientifiques et leur assigner des tâches.
T0338	Rédiger des spécifications fonctionnelles détaillées qui documentent le processus de développement de l'architecture.
T0339	Diriger les efforts visant à promouvoir l'utilisation par l'organisation de la gestion des connaissances et du partage de l'information.
T0340	Agir en tant que principale partie prenante dans les processus et fonctions opérationnels des technologies de l'information (TI) sous-jacents qui soutiennent le service, fournir des orientations et contrôler toutes les activités importantes afin que le service soit fourni avec succès.
T0341	Plaider en faveur d'un financement adapté des ressources de formation cyber, y compris des cours, des instructeurs et du matériel connexe, tant internes que fournis par la profession.
T0342	Analyser les sources de données afin de formuler des recommandations exploitables.
T0343	Analyser la crise pour assurer la protection du public, des personnes et des ressources.
T0344	Évaluer tous les processus de gestion de la configuration (gestion des changements, de la configuration et des versions).

ID des tâches	Description des tâches
T0345	Évaluer l'efficacité et l'efficience de l'enseignement en fonction de la facilité d'utilisation des technologies pédagogiques et de l'apprentissage, du transfert des connaissances et de la satisfaction des étudiants.
T0346	Évaluer le comportement de la victime, du témoin ou du suspect dans le cadre de l'enquête.
T0347	Évaluer la validité des données sources et des conclusions qui en découlent.
T0348	Contribuer à l'évaluation de l'impact de la mise en œuvre et du maintien d'une infrastructure de cybersécurité spécialisée.
T0349	Recueillir des mesures et des données sur les tendances.
T0350	Réaliser une analyse de marché afin d'identifier, d'évaluer et de recommander des produits commerciaux, des produits prêts à l'emploi du gouvernement et des produits open source à utiliser dans un système et s'assurer que les produits recommandés sont conformes aux exigences de l'organisation en matière d'évaluation et de validation.
T0351	Effectuer des tests d'hypothèse à l'aide de processus statistiques.
T0352	Procéder à l'évaluation des besoins d'apprentissage et identifier les exigences.
T0353	Se concerter avec des analystes de systèmes, des ingénieurs, des programmeurs et d'autres personnes pour concevoir l'application.
T0354	Coordonner et gérer de bout en bout le service global fourni à un client.
T0355	Assurer la coordination avec les experts internes et externes en la matière pour veiller à ce que les normes de qualification existantes reflètent les exigences fonctionnelles de l'organisation et respectent les normes industrielles.
T0356	Assurer la coordination avec les parties prenantes de l'organisation en matière de main-d'œuvre afin de garantir une affectation et une distribution appropriées des ressources en capital humain.
T0357	Créer des exercices d'apprentissage interactifs afin de créer un environnement d'apprentissage efficace.
T0358	Concevoir et développer des fonctionnalités d'administration et de gestion des systèmes pour les utilisateurs bénéficiant d'un accès privilégié.
T0359	Concevoir, mettre en œuvre, tester et évaluer des interfaces sécurisées entre les systèmes d'information, les systèmes physiques et/ou les technologies intégrées.
T0360	Déterminer l'ampleur des menaces et recommander des plans d'action ou des contre-mesures pour réduire les risques.
T0361	Développer et faciliter les méthodes de collecte de données.
T0362	Élaborer et mettre en œuvre des descriptions de poste normalisées sur la base des rôles établis en matière de travaux cybers.
T0363	Élaborer et réviser les procédures de recrutement, d'embauche et de maintien en poste conformément aux politiques actuelles en matière de ressources humaines.
T0364	Développer la structure de classification des domaines de carrière cyber, y compris l'établissement des exigences d'entrée dans les domaines de carrière et d'autres nomenclatures telles que les codes et les identificateurs.
T0365	Élaborer ou contribuer à l'élaboration de politiques et de protocoles de formation en matière de formation cyber.
T0366	Élaborer des perspectives stratégiques à partir de vastes ensembles de données.
T0367	Élaborer les buts et les objectifs des programmes d'études cybers.
T0368	Veiller à ce que les domaines de carrière cyber soient gérés conformément aux politiques et aux directives de l'organisation en matière de ressources humaines.
T0369	Veiller à ce que les politiques et processus de gestion des ressources humaines dans le domaine cyber soient conformes aux exigences légales et organisationnelles en matière

ID des tâches	Description des tâches
	d'égalité des chances, de diversité et de pratiques équitables en matière d'embauche et d'emploi.
T0370	Veiller à ce que des accords de niveau de service (SLA) appropriés et des contrats sous-jacents aient été définis, qui établissent clairement pour le client une description du service et les mesures de contrôle du service.
T0371	Établir des limites acceptables pour l'application logicielle, le réseau ou le système.
T0372	Établir et collecter des mesures pour contrôler et valider l'état de préparation du personnel cyber, y compris l'analyse des données relatives au personnel cyber afin d'évaluer l'état des postes identifiés, pourvus et occupés par du personnel qualifié.
T0373	Établir et superviser les processus de dérogation pour les exigences d'entrée et de qualification en matière de formation dans les domaines de la carrière cyber.
T0374	Établir des parcours de carrière dans le domaine cyber afin de permettre une progression de carrière, un développement volontaire et une évolution dans les domaines de carrière cyber et entre ces domaines.
T0375	Établir des normes en matière d'effectifs, de personnel et d'éléments de données de qualification afin de répondre aux exigences en matière de gestion des effectifs cybers et d'établissement de rapports.
T0376	Établir, doter en ressources, mettre en œuvre et évaluer les programmes de gestion des effectifs cybers conformément aux exigences de l'organisation.
T0377	Recueillir des informations en retour sur la satisfaction des clients et les performances des services internes afin de favoriser une amélioration continue.
T0378	Incorporer un processus de mise à jour de la maintenance des systèmes axé sur les risques afin de remédier aux déficiences des systèmes (périodiquement et hors cycle).
T0379	Gérer les relations internes avec les propriétaires de processus de technologie de l'information (TI) soutenant le service, en contribuant à la définition et à la conclusion d'accords sur les niveaux d'exploitation (OLA).
T0380	Planifier des stratégies pédagogiques telles que des conférences, des démonstrations, des exercices interactifs, des présentations multimédias, des cours vidéo, des cours sur le web pour créer l'environnement d'apprentissage le plus efficace possible, en collaboration avec les éducateurs et les formateurs.
T0381	Présenter des informations techniques à des publics techniques et non techniques.
T0382	Présenter des données dans des formats innovants.
T0383	Programmer des algorithmes personnalisés.
T0384	Sensibiliser la direction à la politique et à la stratégie cybers, le cas échéant, et veiller à ce que des principes solides se reflètent dans la mission, la vision et les objectifs de l'organisation.
T0385	Formuler des recommandations exploitables à l'intention des principales parties prenantes sur la base de l'analyse des données et des résultats.
T0386	Fournir un appui en matière d'enquêtes criminelles aux avocats au cours de la procédure judiciaire.
T0387	Examiner et appliquer les normes de qualification dans le domaine de la carrière cyber.
T0388	Examiner et appliquer les politiques de l'organisation relatives au personnel cyber ou l'influençant.
T0389	Examiner les rapports sur la performance des services, en identifiant les problèmes et les écarts importants, en lançant, le cas échéant, des actions correctives et en veillant à ce que toutes les questions en suspens fassent l'objet d'un suivi.
T0390	Examiner/évaluer l'efficacité du personnel cyber afin d'ajuster les normes de compétence et/ou de qualification.

ID des tâches	Description des tâches
T0391	Soutenir l'intégration du personnel qualifié dans le domaine cyber dans les processus de développement du cycle de vie des systèmes d'information.
T0392	Utiliser la documentation ou les ressources techniques pour mettre en œuvre une nouvelle méthode mathématique, informatique ou de science des données.
T0393	Valider les spécifications et les exigences en termes de testabilité.
T0394	Travailler avec d'autres gestionnaires de services et propriétaires de produits afin d'équilibrer et de hiérarchiser les services pour répondre aux exigences, contraintes et objectifs globaux des clients.
T0395	Rédiger et publier des comptes rendus après action.
T0396	Traiter les images avec les outils appropriés en fonction des objectifs de l'analyste.
T0397	Effectuer une analyse du registre Windows.
T0398	Effectuer la surveillance des fichiers et du registre sur le système en cours d'exécution après avoir identifié l'intrusion par le biais de l'analyse dynamique.
T0399	Saisir les informations relatives aux supports dans une base de données de suivi (par exemple, Product Tracker Tool) pour les supports numériques qui ont été acquis.
T0400	Corréler les données relatives aux incidents et établir des rapports sur la cybersécurité.
T0401	Maintenir un ensemble d'outils de cybersécurité déployables (par exemple, des logiciels/matériels de cybersécurité spécialisés) pour soutenir la mission de l'équipe d'intervention en cas d'incident.
T0402	Allouer de manière efficace la capacité de stockage dans la conception des systèmes de gestion des données.
T0403	Lire, interpréter, écrire, modifier et exécuter des scripts simples (par exemple, Perl, VBScript) sur les systèmes Windows et UNIX (par exemple, ceux qui exécutent des tâches telles que l'analyse de fichiers de données volumineux, l'automatisation de tâches manuelles et l'extraction/le traitement de données à distance).
T0404	Utiliser différents langages de programmation pour écrire du code, ouvrir des fichiers, lire des fichiers et écrire des résultats dans différents fichiers.
T0405	Utiliser un langage open source tel que R et appliquer des techniques quantitatives (par exemple, statistiques descriptives et inférentielles, échantillonnage, conception expérimentale, tests de différence paramétriques et non paramétriques, régression par les moindres carrés ordinaires, ligne générale).
T0406	Veiller à ce que les activités de conception et de développement soient correctement documentées (en fournissant une description fonctionnelle de la mise en œuvre) et mises à jour chaque fois que nécessaire.
T0407	Participer au processus d'acquisition si nécessaire.
T0408	Interpréter et appliquer les lois, statuts et documents réglementaires en vigueur et les intégrer dans la politique.
T0409	Résoudre les problèmes liés à la conception des prototypes et aux processus tout au long des phases de conception, de développement et de pré-lancement du produit.
T0410	Identifier les caractéristiques fonctionnelles et liées à la sécurité afin de trouver des opportunités de développement de nouvelles capacités pour exploiter ou atténuer les vulnérabilités.
T0411	Identifier et/ou développer des outils de rétro-ingénierie pour améliorer les capacités et détecter les vulnérabilités.
T0412	Procéder à des examens des importations/exportations pour l'acquisition de systèmes et de logiciels.
T0413	Développer des capacités de gestion des données (par exemple, gestion centralisée des clefs cryptographiques dans le Cloud) afin d'apporter un soutien au personnel nomade.

ID des tâches	Description des tâches
T0414	Élaborer des exigences en matière de chaîne d'approvisionnement, de systèmes, de réseaux, de performances et de cybersécurité.
T0415	Veiller à ce que les exigences relatives à la chaîne d'approvisionnement, aux systèmes, aux réseaux, aux performances et à la cybersécurité soient incluses dans le contrat et à ce qu'elles soient respectées.
T0416	Permettre la mise en œuvre d'applications à clef publique en exploitant les bibliothèques d'infrastructure à clef publique (PKI) existantes et en intégrant des fonctionnalités de gestion des certificats et de chiffrement, le cas échéant.
T0417	Identifier et exploiter les services de sécurité à l'échelle de l'entreprise lors de la conception et du développement d'applications sécurisées (par exemple, PKI d'entreprise, serveur d'identité fédérée, solution antivirus d'entreprise), le cas échéant.
T0418	Installer, mettre à jour et dépanner les systèmes/serveurs.
T0419	Acquérir et maintenir une connaissance pratique des questions juridiques qui se posent dans les lois, règlements, politiques, accords, normes, procédures ou autres documents en vigueur.
T0420	Administrer le(s) banc(s) d'essai et tester et évaluer les applications, l'infrastructure matérielle, les règles/signatures, les contrôles d'accès et les configurations des plates-formes gérées par le(s) prestataire(s) de services.
T0421	Gérer l'indexation/le catalogage, le stockage et l'accès aux connaissances de l'organisation (par exemple, documents papier, fichiers numériques).
T0422	Mettre en œuvre les normes, les exigences et les spécifications en matière de gestion des données.
T0423	Analyser les menaces engendrées par l'informatique à des fins de contre-espionnage ou d'activité criminelle.
T0424	Analyser et fournir des informations aux parties prenantes qui soutiendront le développement d'une application de sécurité ou la modification d'une application de sécurité existante.
T0425	Analyser la politique cyber de l'organisation.
T0426	Analyser les résultats des tests de logiciels, de matériel ou d'interopérabilité.
T0427	Analyser les besoins et les exigences des utilisateurs pour planifier l'architecture.
T0428	Analyser les besoins en matière de sécurité et les exigences logicielles afin de déterminer la faisabilité de la conception dans le respect des contraintes de temps et de coût et des mandats de sécurité.
T0429	Évaluer les besoins en matière de politique et collaborer avec les parties prenantes pour élaborer des politiques régissant les activités cybers.
T0430	Rassembler et préserver les preuves utilisées dans le cadre de poursuites judiciaires pour des délits informatiques.
T0431	Vérifier la disponibilité, la fonctionnalité, l'intégrité et l'efficacité du matériel informatique.
T0432	Recueillir et analyser les artefacts d'intrusion (par exemple, le code source, les logiciels malveillants et la configuration du système) et utiliser les données découvertes pour permettre l'atténuation des incidents cybers potentiels au sein de l'entreprise.
T0433	Analyser les fichiers journaux, les preuves et d'autres informations afin de déterminer les meilleures méthodes pour identifier le ou les auteurs d'une intrusion dans un réseau ou d'autres délits.
T0434	Encadrer les actes de procédure afin d'identifier correctement les violations présumées de la loi, des règlements ou des politiques/orientations.

ID des tâches	Description des tâches
T0435	Réaliser la maintenance périodique du système, y compris le nettoyage (physique et électronique), la vérification des disques, les redémarrages de routine, les purges de données et les tests.
T0436	Effectuer des essais de programmes et d'applications informatiques pour s'assurer que les informations souhaitées sont produites et que les instructions et les niveaux de sécurité sont corrects.
T0437	Établir une corrélation entre la formation et l'apprentissage, d'une part, et les exigences de l'entreprise ou de la mission, d'autre part.
T0438	Créer, modifier et gérer des listes de contrôle d'accès au réseau sur des systèmes spécialisés de cybersécurité (par exemple, des pare-feu et des systèmes de prévention des intrusions).
T0439	Détecter et analyser les données chiffrées, la sténographie, les flux de données alternatifs et d'autres formes de données dissimulées.
T0440	Saisir et intégrer les capacités essentielles des systèmes ou les fonctions opérationnelles nécessaires à la restauration partielle ou totale des systèmes après une défaillance catastrophique.
T0441	Définir et intégrer les environnements de mission actuels et futurs.
T0442	Créer des formations adaptées au public et à l'environnement physique.
T0443	Dispenser des formations adaptées au public et aux environnements physiques/virtuels.
T0444	Appliquer des concepts, des procédures, des logiciels, des équipements et/ou des applications technologiques aux étudiants.
T0445	Concevoir/intégrer une stratégie cyber décrivant la vision, la mission et les objectifs qui s'alignent sur le plan stratégique de l'organisation.
T0446	Concevoir, développer, intégrer et mettre à jour les mesures de sécurité des systèmes qui assurent la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.
T0447	Concevoir le matériel, les systèmes d'exploitation et les applications logicielles pour répondre de manière adéquate aux exigences.
T0448	Développer l'architecture de l'entreprise ou les composants du système nécessaires pour répondre aux besoins des utilisateurs.
T0449	Concevoir en fonction des exigences de sécurité afin de garantir le respect des exigences pour tous les systèmes et/ou applications.
T0450	Concevoir le programme de formation et le contenu des cours en fonction des besoins.
T0451	Participer à l'élaboration des programmes de formation et du contenu des cours.
T0452	Concevoir, élaborer, mettre en œuvre et maintenir un cadre de gestion des connaissances permettant aux utilisateurs finaux d'accéder au capital intellectuel de l'organisation.
T0453	Déterminer et développer des pistes et identifier des sources d'information afin d'identifier et/ou de poursuivre les responsables d'une intrusion ou d'autres délits.
T0454	Définir les exigences de base en matière de sécurité conformément aux lignes directrices applicables.
T0455	Élaborer des procédures d'essai et de validation de systèmes logiciels, de programmation et de documentation.
T0456	Élaborer des procédures de test et de validation de logiciels sécurisés.
T0457	Élaborer des procédures de test et de validation des systèmes, des programmes et de la documentation.
T0458	Respecter les procédures opérationnelles normalisées de l'organisation en matière d'administration des systèmes.
T0459	Mettre en œuvre des applications d'exploration de données et d'entreposage de données.

ID des tâches	Description des tâches
T0460	Élaborer et mettre en œuvre des programmes d'exploration de données et d'entreposage de données.
T0461	Mettre en œuvre et appliquer les politiques et procédures d'utilisation du réseau local.
T0462	Élaborer des procédures et tester le basculement des opérations système vers un autre site en fonction des exigences de disponibilité du système.
T0463	Élaborer des estimations de coûts pour les nouveaux systèmes ou les systèmes modifiés.
T0464	Élaborer une documentation de conception détaillée pour les spécifications des composants et des interfaces afin de soutenir la conception et le développement du système.
T0465	Élaborer des lignes directrices pour la mise en œuvre.
T0466	Élaborer des stratégies d'atténuation des risques en matière de coût, de calendrier, de performance et de sécurité.
T0467	Veiller à ce que la formation réponde aux objectifs de formation, d'éducation ou de sensibilisation à la cybersécurité.
T0468	Diagnostiquer et résoudre les incidents, problèmes et événements système signalés par les clients.
T0469	Analyser et signaler les tendances en matière de sécurité de l'organisation.
T0470	Analyser et signaler les tendances en matière de sécurité des systèmes.
T0471	Documenter l'état d'origine des preuves numériques et/ou associées (par exemple, au moyen de photographies numériques, de rapports écrits, de vérifications de la fonction de hachage).
T0472	Rédiger, alimenter et publier la politique cyber.
T0473	Documenter et mettre à jour, le cas échéant, toutes les activités de définition et d'architecture.
T0474	Fournir des analyses et des réponses juridiques aux inspecteurs généraux, aux responsables de la protection de la vie privée et au personnel chargé de la surveillance et de la conformité en ce qui concerne le respect des politiques de cybersécurité et des exigences juridiques et réglementaires applicables.
T0475	Évaluer les contrôles d'accès adaptés sur la base des principes du moindre privilège et du besoin d'en connaître.
T0476	Évaluer l'impact des modifications apportées aux lois, réglementations, politiques, normes ou procédures.
T0477	Assurer l'exécution de la reprise après sinistre et la continuité des opérations.
T0478	Fournir des conseils sur les lois, réglementations, politiques, normes ou procédures à la direction, au personnel ou aux clients.
T0479	Utiliser des systèmes de technologie de l'information (TI) et des supports de stockage numérique pour résoudre, enquêter et/ou poursuivre des cybercrimes et des fraudes commis contre des personnes et des biens.
T0480	Identifier les composantes ou les éléments, attribuer des composantes fonctionnelles globales pour inclure les fonctions de sécurité et décrire les relations entre les éléments.
T0481	Identifier et traiter les questions relatives à la planification et à la gestion des personnels cyber (par exemple, le recrutement, la fidélisation et la formation).
T0482	Formuler des recommandations fondées sur l'analyse des tendances en vue d'améliorer les solutions logicielles et matérielles afin d'améliorer l'expérience des clients.
T0483	Identifier les conflits potentiels liés à la mise en œuvre de tout outil de cybersécurité (par exemple, test et optimisation des outils et des signatures).
T0484	Déterminer les besoins de protection (c'est-à-dire les mesures de sécurité) pour le(s) système(s) d'information et le(s) réseau(x) et les documenter de manière appropriée.

ID des tâches	Description des tâches
T0485	Mettre en œuvre des mesures de sécurité pour éliminer les vulnérabilités, atténuer les risques et recommander des modifications de la sécurité des systèmes ou de leurs composants, le cas échéant.
T0486	Mettre en œuvre le cadre de gestion des risques (Risk Management Framework ou RMF) et les exigences en matière d'évaluation et d'autorisation de la sécurité (Security Assessment and Authorization ou SA&A) pour les systèmes de cybersécurité dédiés au sein de l'entreprise, et documenter et tenir à jour les dossiers y afférents.
T0487	Faciliter la mise en œuvre de lois, de règlements, de décrets, de politiques, de normes ou de procédures que ces textes soient nouveaux ou amendés.
T0488	Mettre en œuvre des modèles pour les systèmes nouveaux ou existants.
T0489	Mettre en œuvre des mesures de sécurité des systèmes conformément aux procédures établies afin de garantir la confidentialité, l'intégrité, la disponibilité, l'authentification et la non-répudiation.
T0490	Installer et configurer des systèmes et des logiciels de gestion de bases de données.
T0491	Installer et configurer le matériel, les logiciels et les équipements périphériques pour les utilisateurs du système conformément aux normes de l'organisation.
T0492	Assurer l'intégration et la mise en œuvre de solutions inter domaines (Cross-Domain Solutions ou CDS) dans un environnement sécurisé.
T0493	Diriger et superviser le budget, la dotation en personnel et les contrats.
T0494	Administrer les comptes, les droits réseaux et l'accès aux systèmes et aux équipements.
T0495	Gérer les dossiers d'accréditation (par exemple, ISO/IEC 15026-2).
T0496	Assurer la gestion des actifs et l'inventaire des ressources en technologies de l'information (TI).
T0497	Gérer le processus de planification des technologies de l'information (TI) afin de s'assurer que les solutions développées répondent aux exigences des clients.
T0498	Gérer les ressources des systèmes/serveurs, y compris les performances, la capacité, la disponibilité, l'aptitude au service et la capacité de récupération.
T0499	Atténuer/corriger les lacunes en matière de sécurité identifiées lors des tests de sécurité/certification et/ou préconiser le niveau d'acceptation des risques pour les dirigeants ou les représentants officiels concernés.
T0500	Modifier et entretenir les logiciels existants pour corriger les erreurs, les adapter à un nouveau matériel ou mettre à niveau les interfaces et améliorer les performances.
T0501	Surveiller et maintenir la configuration du système/serveur.
T0502	Surveiller et signaler les performances du système informatique en ce qui concerne la partie client.
T0503	Surveiller les sources de données externes (par exemple, les sites des fournisseurs de cybersécurité, les CERTs (Computer Emergency Response Teams), Security Focus) afin de maintenir à jour l'état des menaces en matière de cybersécurité et de déterminer les problèmes de sécurité susceptibles d'avoir un impact sur l'entreprise.
T0504	Évaluer et contrôler la cybersécurité liée à la mise en œuvre des systèmes et aux pratiques de test.
T0505	Contrôler l'application rigoureuse des politiques, principes et pratiques cyber dans le cadre de la fourniture de services de planification et de gestion.
T0506	Rechercher le consensus des parties prenantes sur les changements de politique proposés.
T0507	Superviser l'installation, la mise en œuvre, la configuration et le support des composants du système.
T0508	Vérifier que les exigences minimales de sécurité sont en place pour toutes les applications.
T0509	Effectuer une évaluation des risques en matière de sécurité de l'information.

ID des tâches	Description des tâches
T0510	Coordonner les fonctions de réponse aux incidents.
T0511	Réaliser des essais de développement sur les systèmes en cours de développement.
T0512	Réaliser des essais d'interopérabilité sur les systèmes qui échangent des informations numériques avec d'autres systèmes.
T0513	Réaliser des essais opérationnels.
T0514	Diagnostiquer le matériel défectueux des systèmes/serveurs.
T0515	Réparer le matériel défectueux des systèmes/serveurs.
T0516	Effectuer des tests, des examens et/ou des évaluations de programmes en toute sécurité afin d'identifier les failles potentielles dans les codes et de réduire les vulnérabilités.
T0517	Intégrer les résultats concernant l'identification des lacunes dans l'architecture de sécurité.
T0518	Effectuer des examens de sécurité et identifier les lacunes en matière de sécurité dans l'architecture.
T0519	Planifier et coordonner la mise en œuvre de techniques et de formats de cours (par exemple, conférences, démonstrations, exercices interactifs, présentations multimédias) afin d'obtenir l'environnement d'apprentissage le plus efficace possible.
T0520	Planifier les techniques et les formats d'enseignement hors salle de classe (par exemple, cours vidéo, mentorat, cours sur le web).
T0521	Planifier la stratégie de mise en œuvre pour s'assurer que les composantes de l'entreprise peuvent être intégrées et alignées.
T0522	Préparer des documents juridiques ainsi que d'autres documents pertinents (par exemple, dépositions, mémoires, affidavits, déclarations, appels, plaidoiries, enquêtes préalables).
T0523	Préparer des rapports pour documenter l'enquête en respectant les normes et les exigences légales.
T0524	Promouvoir le partage des connaissances entre les propriétaires/utilisateurs d'informations par le biais des processus et systèmes opérationnels d'une organisation.
T0525	Fournir des orientations en matière de cybersécurité de l'entreprise et de gestion des risques liés à la chaîne d'approvisionnement.
T0526	Formuler des recommandations en matière de cybersécurité à l'intention des dirigeants sur la base des menaces et des vulnérabilités importantes.
T0527	Contribuer aux plans de mise en œuvre et aux procédures opérationnelles normalisées en ce qui concerne la sécurité des systèmes d'information.
T0528	Contribuer aux plans de mise en œuvre, aux procédures opérationnelles normalisées, à la documentation relative à la maintenance et aux supports de formation à la maintenance.
T0529	Fournir des orientations en matière de politique à la direction, au personnel et aux utilisateurs du domaine cyber.
T0530	Élaborer une analyse des tendances et un rapport d'impact.
T0531	Dépanner les problèmes d'interface matérielle/logicielle et d'interopérabilité.
T0532	Examiner les investigations numériques légales et d'autres sources de données (par exemple, les données volatiles) en vue de la récupération d'informations potentiellement pertinentes.
T0533	Examiner, mener ou participer à des audits de programmes et de projets cyber.
T0534	Procéder à des examens/révisions périodiques du contenu des cours pour en vérifier l'exactitude, l'exhaustivité, la conformité et l'actualité (par exemple, les documents relatifs au contenu des cours, les plans de cours, les textes destinés aux étudiants, les examens, les programmes d'enseignement et les descriptions de cours).
T0535	Recommander des révisions du programme d'études et du contenu des cours sur la base du retour d'information des sessions de formation précédentes.
T0536	Servir de consultant et de conseiller interne dans son propre domaine d'expertise (par exemple, technique, droits d'auteur, presse écrite, médias électroniques).

ID des tâches	Description des tâches
T0537	Soutenir le DSI dans la formulation de politiques liées à la cybersécurité.
T0538	Fournir un soutien aux activités de test et d'évaluation.
T0539	Tester, évaluer et vérifier le matériel et/ou les logiciels afin de déterminer s'ils sont conformes aux spécifications et aux exigences définies.
T0540	Enregistrer et gérer les données de test.
T0541	Remonter des exigences du système aux composants de la conception et effectuer une analyse des lacunes.
T0542	Traduire les capacités proposées en exigences techniques.
T0544	Vérifier la stabilité, l'interopérabilité, la portabilité et/ou l'évolutivité de l'architecture du système.
T0545	Travailler avec les parties prenantes pour résoudre les incidents de sécurité informatique et la conformité aux vulnérabilités.
T0546	Rédiger et publier des recommandations, des rapports et des livres blancs en matière de cybersécurité sur les résultats des incidents, à l'intention des parties prenantes concernées.
T0547	Rechercher et évaluer les technologies et les normes disponibles pour répondre aux exigences des clients.
T0548	Fournir des conseils et des informations pour les plans de reprise après sinistre, les plans d'urgence et les plans de continuité des activités.
T0549	Effectuer des évaluations techniques (évaluation de la technologie) et non techniques (évaluation des personnes et des opérations) des risques et des vulnérabilités des domaines technologiques appropriés (par exemple : environnement informatique local, réseau et infrastructure, périmètre réservé, infrastructure de soutien et applications).
T0550	Formuler des recommandations concernant la sélection de mesures de sécurité économiquement efficaces pour atténuer les risques (par exemple : protection de l'information, des systèmes et des processus).
T0551	Rédiger et publier des documents sur la sûreté de la chaîne d'approvisionnement et la gestion des risques.
T0552	Examiner et approuver une politique de sécurité et de gestion des risques de la chaîne d'approvisionnement.
T0553	Appliquer les fonctions de cybersécurité (par exemple, le chiffrement, le contrôle d'accès et la gestion des identités) pour réduire les possibilités d'exploitation.
T0554	Déterminer et documenter les correctifs logiciels ou le nombre de versions qui rendraient le logiciel vulnérable.
T0555	Documenter la manière dont la mise en œuvre d'un nouveau système ou d'une nouvelle interface entre systèmes influe sur l'environnement actuel et l'environnement cible, y compris, mais sans s'y limiter, sur la posture de sécurité.
T0556	Évaluer et concevoir des fonctions de gestion de la sécurité en rapport avec le cyber.
T0557	Intégrer les fonctions de gestion clefs liées au cyberespace.
T0558	Analyser les besoins et les exigences des utilisateurs afin de planifier et de mener à bien le développement des systèmes.
T0559	Élaborer des conceptions répondant à des besoins opérationnels spécifiques et à des facteurs environnementaux (par exemple, contrôles d'accès, applications automatisées, opérations en réseau).
T0560	Collaborer à la conception de systèmes de cybersécurité afin de répondre à des besoins opérationnels et à des facteurs environnementaux spécifiques (par exemple, contrôles d'accès, applications automatisées, opérations en réseau, exigences en matière d'intégrité et de disponibilité élevées, sécurité multiniveaux/traitement de plusieurs niveaux de classification et traitement d'informations confidentielles sensibles).

ID des tâches	Description des tâches
T0561	Caractériser précisément les cibles.
T0562	Ajuster les opérations de collecte ou le plan de collecte afin de résoudre les problèmes/difficultés identifiés et de synchroniser les collectes avec les exigences opérationnelles globales.
T0563	Contribuer à l'analyse, à la conception, au développement ou à l'acquisition des capacités utilisées pour atteindre les objectifs.
T0564	Analyser le retour d'information pour déterminer dans quelle mesure les produits et services de collecte répondent aux besoins.
T0565	Analyser les demandes de collecte entrantes.
T0566	Analyser l'architecture opérationnelle interne, les outils et les procédures pour trouver des moyens d'améliorer les performances.
T0567	Analyser l'architecture opérationnelle de la cible pour trouver des moyens d'y accéder.
T0568	Analyser les plans, les directives, les orientations et la politique pour déterminer les facteurs susceptibles d'influencer la structure opérationnelle de la gestion des collectes et les besoins (par exemple, la durée, la portée, les exigences en matière de communication, les accords interagences/internationaux).
T0569	Répondre aux demandes d'information.
T0570	Appliquer et utiliser les capacités cybers autorisées pour permettre l'accès aux réseaux ciblés.
T0571	Appliquer son expertise en matière de politique et de processus pour faciliter l'élaboration, la négociation et la dotation interne de plans et/ou de protocoles d'accord.
T0572	Appliquer les compétences en matière de collecte, de préparation de l'environnement et d'engagement dans le domaine cyber pour permettre une nouvelle exploitation et/ou la poursuite des opérations de collecte, ou pour répondre aux besoins des clients.
T0573	Évaluer et appliquer les facteurs et les risques liés à l'environnement opérationnel au processus de gestion de la collecte.
T0574	Appliquer et respecter les statuts, lois, règlements et politiques en vigueur.
T0575	Coordonner le soutien en matière de renseignement aux activités de planification opérationnelle.
T0576	Évaluer les renseignements provenant de toutes les sources et recommander des cibles à l'appui des objectifs des opérations cybers.
T0577	Évaluer l'efficacité des systèmes d'échange et de gestion de l'information existants.
T0578	Évaluer les performances des moyens de collecte par rapport aux spécifications prescrites.
T0579	Évaluer les vulnérabilités de la cible et/ou les capacités opérationnelles afin de déterminer la marche à suivre.
T0580	Évaluer l'efficacité des collectes pour combler les lacunes en matière d'informations prioritaires, en utilisant les capacités et les méthodes disponibles, et adapter les stratégies et les exigences en matière de collecte en conséquence.
T0581	Assister et conseiller les partenaires interagences dans l'identification et le développement des bonnes pratiques pour faciliter le soutien opérationnel à la réalisation des objectifs de l'organisation.
T0582	Fournir une expertise pour l'élaboration de plans d'action.
T0583	Fournir une expertise en la matière pour l'élaboration d'une image opérationnelle commune.
T0584	Maintenir une vision commune du renseignement.
T0585	Fournir une expertise en la matière pour l'élaboration d'indicateurs spécifiques aux opérations cybers.
T0586	Contribuer à la coordination, à la validation et à la gestion des exigences, des plans et/ou des activités de collecte de toutes les sources.

ID des tâches	Description des tâches
T0587	Contribuer à l'élaboration et à l'affinement des besoins prioritaires en matière d'information.
T0588	Fournir une expertise pour l'élaboration de mesures d'efficacité et de performance.
T0589	Contribuer à l'identification des lacunes en matière de collecte de renseignements.
T0590	Permettre la synchronisation des plans de soutien en matière de renseignement entre les organisations partenaires, le cas échéant.
T0591	Effectuer une analyse des activités d'exploitation de l'infrastructure de la cible.
T0592	Contribuer à l'identification des critères de réussite dans le domaine cyber.
T0593	Présenter brièvement l'état actuel des menaces et/ou des cibles.
T0594	Créer et maintenir des dossiers cibles électroniques.
T0595	Classer les documents conformément aux directives de classification.
T0596	Clôturer les demandes d'information une fois qu'elles ont été satisfaites.
T0597	Collaborer avec les analystes du renseignement et les organisations chargées du ciblage dans des domaines connexes.
T0598	Collaborer avec les organisations de développement pour créer et déployer les outils nécessaires à la réalisation des objectifs.
T0599	Collaborer avec d'autres clients, organisations de renseignement et de ciblage intervenant dans des domaines cybers connexes.
T0600	Collaborer avec d'autres organisations partenaires internes et externes sur l'accès aux cibles et les questions opérationnelles.
T0601	Collaborer avec d'autres membres de l'équipe ou des organisations partenaires pour élaborer un programme diversifié de documents à caractère informatif (par exemple, pages web, notes d'information, documents imprimés).
T0602	Collaborer avec le client pour définir les exigences en matière d'information.
T0603	Communiquer les nouveaux développements, les percées, les défis et les enseignements tirés à la direction et aux clients internes et externes.
T0604	Comparer les ressources allouées et disponibles à la demande de collecte telle qu'elle est exprimée dans les exigences.
T0605	Compiler les enseignements tirés de la réalisation des objectifs de collecte de l'organisation par l'activité de gestion des collectes.
T0606	Compiler, intégrer et/ou interpréter les données de toutes sources pour en tirer des renseignements ou des informations sur les vulnérabilités concernant des cibles spécifiques.
T0607	Identifier et analyser les communications des cibles afin de déterminer les informations essentielles au soutien des opérations.
T0608	Analyser les technologies numériques physiques et logiques (par exemple : sans fil, SCADA, télécommunications) afin d'identifier les voies d'accès potentielles.
T0609	Permettre l'accès aux réseaux informatiques et numériques sans fil.
T0610	Effectuer la collecte et le traitement des données sur les réseaux informatiques et numériques sans fil.
T0611	Réaliser des évaluations de fin d'exploitation.
T0612	Exploiter les réseaux informatiques et numériques sans fil.
T0613	Assurer la coordination formelle et informelle des exigences en matière de collecte conformément aux lignes directrices et aux procédures établies.
T0614	Effectuer des analyses approfondies et indépendantes des cibles et des techniques, y compris des informations spécifiques à la cible (par exemple, culturelles, organisationnelles, politiques) qui permettent d'accéder à la cible.
T0615	Effectuer des recherches et des analyses approfondies.
T0616	Effectuer des analyses de réseau et de vulnérabilité des systèmes au sein d'un réseau.
T0617	Effectuer une analyse nodale.

ID des tâches	Description des tâches
T0618	Mener des activités sur le réseau pour contrôler et extraire des données des technologies déployées.
T0619	Mener des activités sur le réseau et hors réseau pour contrôler et extraire des données des technologies automatisées déployées.
T0620	Effectuer la collecte de données open source à l'aide de divers outils en ligne.
T0621	Effectuer un contrôle qualité pour déterminer la validité et la pertinence des informations recueillies sur les réseaux.
T0622	Élaborer, examiner et mettre en œuvre tous les niveaux d'orientation en matière de planification à l'appui des opérations cybers.
T0623	Mener des enquêtes sur les réseaux informatiques et numériques.
T0624	Réaliser des recherches et des analyses sur les cibles.
T0625	Examiner l'efficience et l'efficacité des moyens et ressources de collecte lorsqu'ils sont utilisés pour répondre aux besoins prioritaires en matière d'information.
T0626	Élaborer des plans et des matrices de collecte à l'aide des directives et des procédures établies.
T0627	Contribuer à la planification des actions de crise pour les opérations cybers.
T0628	Contribuer à l'élaboration des outils d'aide à la décision de l'organisation, si nécessaire.
T0629	Contribuer à l'élaboration, à la dotation en personnel et à la coordination des politiques, des normes de performance, des plans et des dossiers d'approbation relatifs aux opérations cybers avec les décideurs internes et/ou externes compétents.
T0630	Incorporer les aspects liés au renseignement dans la conception globale des plans d'opérations cybers.
T0631	Coordonner, avec les responsables des disciplines de collecte, l'affectation des ressources de collecte en fonction des exigences de collecte classées par ordre de priorité.
T0632	Coordonner l'inclusion du plan de collecte dans la documentation appropriée.
T0633	Coordonner l'examen des cibles avec les partenaires appropriés.
T0634	Réaffecter ou réorienter les moyens et ressources de collecte.
T0635	Se coordonner avec les partenaires du renseignement et de la cybersécurité afin d'obtenir les informations essentielles pertinentes.
T0636	Se coordonner avec les planificateurs du renseignement pour veiller à ce que les responsables de la collecte reçoivent les informations requises.
T0637	Se coordonner avec l'équipe de planification du renseignement afin d'évaluer la capacité de satisfaire aux tâches de renseignement assignées.
T0638	Coordonner, produire et suivre les besoins en matière de renseignement.
T0639	Coordonner, synchroniser et rédiger les sections relatives au renseignement dans les plans d'opérations cybers.
T0640	Utiliser les estimations en matière de renseignement pour contrer les actions potentielles des cibles.
T0641	Créer des stratégies d'exploitation complètes qui identifient les vulnérabilités techniques ou opérationnelles qui peuvent être exploitées.
T0642	Se tenir au courant des structures internes et externes de l'organisation, de ses points forts et de l'utilisation du personnel et de la technologie.
T0643	Déployer des outils sur une cible et les utiliser une fois déployés (par exemple : portes dérobées, renifleurs).
T0644	Détecter les exploits contre les réseaux et les hôtes ciblés et réagir en conséquence.
T0645	Déterminer la marche à suivre pour faire face aux modifications des objectifs, des orientations et de l'environnement opérationnel.

ID des tâches	Description des tâches
T0646	Identifier les bases de données, les bibliothèques et les entrepôts du site existant de gestion des collectes.
T0647	Déterminer comment les facteurs identifiés affectent la forme et la fonction de l'architecture d'attribution des tâches, de collecte, de traitement, d'exploitation et de diffusion.
T0648	Déterminer les indicateurs (par exemple, les mesures d'efficacité) les mieux adaptés aux objectifs spécifiques des opérations cybers.
T0649	Déterminer les organisations et/ou les échelons ayant le pouvoir de collecte sur tous les moyens de collecte accessibles.
T0650	Déterminer les technologies utilisées par une cible donnée.
T0651	Élaborer une méthode permettant de comparer les rapports de collecte aux besoins en attente afin d'identifier les lacunes en matière d'information.
T0652	Élaborer des documents de ciblage à partir de toutes les sources de renseignements.
T0653	Appliquer des techniques d'analyse pour obtenir davantage d'informations sur les cibles.
T0654	Élaborer et tenir à jour des plans opérationnels et/ou des plans de crise.
T0655	Élaborer et examiner des orientations spécifiques aux opérations cybers en vue de les intégrer dans des activités de planification plus larges.
T0656	Élaborer et réviser les orientations en matière de renseignement afin de les intégrer dans la planification et l'exécution des opérations cybers.
T0657	Élaborer des instructions de coordination par discipline de collecte pour chaque phase d'une opération.
T0658	Élaborer des plans et des orientations en matière d'opérations cybers pour faire en sorte que les décisions relatives à l'exécution et à l'affectation des ressources soient conformes aux objectifs de l'organisation.
T0659	Élaborer des renseignements détaillés à l'appui des besoins en matière d'opérations cybers.
T0660	Élaborer les besoins en informations nécessaires pour répondre aux demandes d'informations prioritaires.
T0661	Élaborer des mesures d'efficacité et de performance.
T0662	Attribuer les moyens de collecte en fonction des orientations, des priorités et/ou de l'importance accordée aux opérations par la direction.
T0663	Développer des documents d'évaluation de l'efficacité des moyens ou d'évaluation opérationnelle.
T0664	Développer de nouvelles techniques pour obtenir et conserver l'accès aux systèmes cibles.
T0665	Élaborer ou participer à l'élaboration de normes concernant la fourniture, la demande et/ou l'obtention d'un soutien de la part de partenaires extérieurs afin de synchroniser les opérations cybers.
T0666	Élaborer ou façonner des stratégies, des politiques et des activités internationales en matière de cyber-engagement afin d'atteindre les objectifs de l'organisation.
T0667	Élaborer des plans d'action potentiels.
T0668	Élaborer des procédures pour fournir un retour d'information aux gestionnaires de collecte, aux gestionnaires de ressources et aux centres de traitement, d'exploitation et de diffusion.
T0669	Élaborer une stratégie et des processus pour la planification, les opérations et le développement des capacités des partenaires.
T0670	Élaborer, mettre en œuvre et recommander des modifications des procédures et politiques de planification appropriées.
T0671	Élaborer, maintenir et évaluer les accords de sécurité en matière de coopération cyber avec les partenaires extérieurs.
T0672	Élaborer, documenter et valider la stratégie et les documents de planification des opérations cybers.

ID des tâches	Description des tâches
T0673	Diffuser des rapports pour informer les décideurs sur les questions de collecte.
T0674	Diffuser les messages d'attribution des tâches et les plans de collecte.
T0675	Réaliser et documenter une évaluation des résultats de la collecte à l'aide des procédures établies.
T0676	Rédiger des exigences en matière de collecte et de production de renseignements cybers.
T0677	Modifier ou exécuter des scripts simples (par exemple Perl, VBScript) sur des systèmes Windows et UNIX.
T0678	S'engager auprès des clients pour comprendre leurs besoins et leurs souhaits en matière de renseignement.
T0679	Veiller à ce que les efforts de planification opérationnelle soient effectivement transférés aux opérations en cours.
T0680	Veiller à ce que les activités de planification du renseignement soient intégrées et synchronisées avec les calendriers de planification opérationnelle.
T0681	Établir d'autres voies de traitement, d'exploitation et de diffusion pour résoudre les questions ou problèmes identifiés.
T0682	Valider le lien entre les demandes de collecte, les besoins en informations critiques et les besoins prioritaires de la direction en matière de renseignement.
T0683	Mettre en place une activité de gestion du traitement, de l'exploitation et de la diffusion à l'aide d'orientations et/ou de procédures approuvées.
T0684	Estimer les effets opérationnels générés par les activités cybers.
T0685	Évaluer les processus de prise de décision en matière de menaces.
T0686	Identifier les points faibles des menaces.
T0687	Identifier les menaces qui pèsent sur les vulnérabilités de la "Blue Force".
T0688	Évaluer les capacités disponibles par rapport aux effets souhaités afin de recommander des solutions efficaces.
T0689	Évaluer dans quelle mesure les informations collectées et/ou les renseignements produits répondent aux demandes d'information.
T0690	Évaluer les estimations en matière de renseignement afin de soutenir le cycle de planification.
T0691	Évaluer les conditions qui influent sur l'utilisation des capacités de renseignement cyber disponibles.
T0692	Élaborer des stratégies d'analyse de réseau et en évaluer l'efficacité.
T0693	Évaluer dans quelle mesure les opérations de collecte sont alignées sur les besoins opérationnels.
T0694	Évaluer l'efficacité des opérations de collecte par rapport au plan de collecte.
T0695	Examiner les métadonnées et le contenu liés à l'interception en comprenant l'importance du ciblage.
T0696	Exploiter des équipements de réseau, des dispositifs de sécurité et/ou des terminaux ou des environnements à l'aide de diverses méthodes ou outils.
T0697	Faciliter l'accès par des moyens physiques et/ou sans fil.
T0698	Faciliter la mise à jour permanente des données de renseignement, de surveillance et de visualisation pour les gestionnaires de l'image opérationnelle commune.
T0699	Faciliter les interactions entre les décideurs des partenaires internes et externes afin de synchroniser et d'intégrer les plans d'action à l'appui des objectifs.
T0700	Faciliter le partage des "bonnes pratiques" et des "retours d'expérience" dans l'ensemble de la communauté des opérations cybers.

ID des tâches	Description des tâches
T0701	Collaborer avec les développeurs, en transmettant les connaissances cibles et techniques dans les soumissions d'exigences relatives aux outils, afin d'améliorer le développement des outils.
T0702	Formuler des stratégies de collecte fondées sur la connaissance des capacités des disciplines du renseignement disponibles et des méthodes de collecte qui alignent les capacités de collecte multidisciplinaires et les accès sur les cibles et leurs observables.
T0703	Recueillir et analyser des données (par exemple, des mesures d'efficacité) pour déterminer l'efficacité et fournir des rapports pour les activités de suivi.
T0704	Intégrer les plans de soutien aux opérations cybers et à la sécurité des communications dans les objectifs de l'organisation.
T0705	Intégrer le renseignement et le contre-renseignement à l'appui de l'élaboration des plans.
T0706	Recueillir des informations sur les réseaux par des techniques traditionnelles et alternatives (par exemple : analyse des réseaux sociaux, chaînage d'appels, analyse du trafic).
T0707	Générer des demandes d'information.
T0708	Identifier les tactiques et les méthodologies de lutte contre les menaces.
T0709	Identifier toutes les capacités et les limites des partenaires en matière de renseignement à l'appui des opérations cybers.
T0710	Identifier et évaluer les capacités, les exigences et les vulnérabilités critiques en matière de menaces.
T0711	Identifier, rédiger, évaluer et hiérarchiser les besoins en matière de renseignements ou d'informations.
T0712	Identifier et gérer les priorités de la coopération en matière de sécurité avec les partenaires extérieurs.
T0713	Identifier et soumettre les besoins en matière de renseignement afin de déterminer les besoins prioritaires en matière d'information.
T0714	Identifier les forums collaboratifs qui peuvent servir de mécanismes de coordination des processus, des fonctions et des résultats avec des organisations et des groupes fonctionnels déterminés.
T0715	Identifier les lacunes en matière de collecte et les stratégies de collecte potentielles par rapport aux cibles.
T0716	Déterminer les exigences et les procédures de coordination avec les autorités de collecte désignées.
T0717	Identifier les éléments critiques des cibles.
T0718	Identifier les lacunes et les insuffisances en matière de renseignement.
T0719	Identifier les lacunes et les insuffisances en matière de renseignement cyber pour la planification des opérations cybers.
T0720	Identifier les lacunes dans notre compréhension de la technologie des cibles et développer des approches de collecte innovantes.
T0721	Identifier les questions ou les problèmes susceptibles de perturber et/ou de dégrader l'efficacité de l'architecture de traitement, d'exploitation et de diffusion.
T0722	Identifier les composants du réseau et leur fonctionnalité pour permettre l'analyse et le développement d'objectifs.
T0723	Identifier les disciplines de collecte potentielles en vue de les appliquer aux besoins d'information prioritaires.
T0724	Identifier les points forts et les points faibles potentiels d'un réseau.
T0725	Identifier et atténuer les risques qui pèsent sur l'aptitude de la gestion de la collecte à soutenir le cycle de planification, d'opérations et d'objectifs.

ID des tâches	Description des tâches
T0726	Déterminer la nécessité, la portée et le calendrier de la production découlant de la préparation de l'environnement de renseignement approprié.
T0727	Identifier, localiser et suivre les cibles au moyen de techniques d'analyse géospatiale.
T0728	Contribuer à l'élaboration de plans d'action fondés sur des facteurs de menace ou en élaborer de nouveaux.
T0729	Informer les partenaires extérieurs des effets potentiels d'une politique et d'orientations nouvelles ou mises à jour sur les activités de partenariat en matière d'opérations cybers.
T0730	Informer les parties prenantes (par exemple, les gestionnaires de collectes, les gestionnaires de ressources, les centres de traitement, d'exploitation et de diffusion) des résultats de l'évaluation en appliquant les procédures établies.
T0731	Introduire des demandes pour orienter l'attribution des tâches et contribuer à la gestion des collections.
T0732	Intégrer les efforts de planification/ciblage cyber avec d'autres organisations.
T0733	Interpréter les évaluations de la préparation de l'environnement afin de déterminer un plan d'action.
T0734	Émettre des demandes d'information.
T0735	Diriger et coordonner le soutien du renseignement à la planification opérationnelle.
T0736	Diriger ou déclencher des opérations d'exploitation pour appuyer les objectifs de l'organisation et les exigences de la cible.
T0737	Établir un lien entre les besoins prioritaires en matière de collecte et les moyens et ressources optimaux.
T0738	Se tenir au courant des progrès des technologies matérielles et logicielles (par exemple, assister à des formations ou à des conférences, lire) et de leurs implications potentielles.
T0739	Entretenir des relations avec les partenaires internes et externes impliqués dans la planification cyber ou dans des domaines connexes.
T0740	Se tenir au courant de la situation et de la fonctionnalité de l'infrastructure opérationnelle interne.
T0741	Se tenir au courant des exigences en matière de renseignement cyber et des tâches qui en découlent.
T0742	Se tenir au courant des capacités et des activités des partenaires.
T0743	Se tenir au courant de la situation afin de déterminer si des modifications de l'environnement opérationnel nécessitent une révision du plan.
T0744	Tenir à jour les listes de cibles (RTL, JTL, CTL, etc.).
T0745	Formuler des recommandations pour orienter la collecte en fonction des besoins du client.
T0746	Modifier les exigences en matière de collecte si nécessaire.
T0747	Surveiller et évaluer les opérations cybers intégrées afin de déterminer les possibilités d'atteindre les objectifs de l'organisation.
T0748	Surveiller et signaler les changements dans les dispositions, les activités, les tactiques, les capacités, les objectifs, etc. des menaces dans le cadre de séries de problèmes d'alerte pour des opérations informatiques désignées.
T0749	Surveiller les activités de menace validées et en rendre compte.
T0750	Surveiller l'achèvement des efforts de collecte réaffectés.
T0751	Surveiller les sites web de sources ouvertes pour détecter tout contenu hostile visant les intérêts de l'organisation ou de ses partenaires.
T0752	Surveiller l'environnement opérationnel et rendre compte des activités des adversaires qui répondent aux besoins d'information prioritaires des dirigeants.
T0753	Surveiller l'état opérationnel et l'efficacité de l'architecture de traitement, d'exploitation et de diffusion.

ID des tâches	Description des tâches
T0754	Surveiller les réseaux des cibles afin de fournir des indications et des avertissements sur les changements dans les communications des cibles ou sur les défaillances de traitement.
T0755	Surveiller l'environnement opérationnel afin de détecter les facteurs et les risques potentiels pour le processus de gestion des opérations de collecte.
T0756	Exploiter et maintenir des systèmes automatisés permettant d'obtenir et de conserver l'accès aux systèmes cibles.
T0757	Optimiser la combinaison des moyens et des ressources de collecte afin d'accroître l'efficacité et l'efficience par rapport aux informations essentielles associées aux exigences prioritaires en matière de renseignement.
T0758	Produire en temps utile des renseignements sur les opérations cybers et/ou des produits de renseignement sur les indications et les avertissements (par exemple, évaluations de la menace, exposés, études de renseignement, études par pays), en fusionnant toutes les sources.
T0759	Contribuer à l'examen et à l'amélioration de la politique, notamment en évaluant les conséquences de l'adoption ou de la non-adoption d'une telle politique.
T0760	Fournir une expertise aux équipes de planification, aux groupes de coordination et aux groupes de travail, le cas échéant.
T0761	Fournir une expertise et un soutien aux forums de planification/développement et aux groupes de travail, le cas échéant.
T0763	Mener des efforts de planification stratégique à long terme avec des partenaires internes et externes dans le cadre d'activités cybers.
T0764	Fournir une expertise dans le cadre des efforts de planification avec les partenaires internes et externes des opérations cybers.
T0765	Fournir une expertise en matière de conception d'exercices.
T0766	Proposer une politique régissant les interactions avec les groupes de coordination externes.
T0767	Procéder à l'analyse du contenu et/ou des métadonnées afin d'atteindre les objectifs de l'organisation.
T0768	Mener des activités cyber pour dégrader/supprimer les informations résidant dans les ordinateurs et les réseaux informatiques.
T0769	Réaliser des activités d'automatisation du ciblage.
T0770	Caractériser les sites web.
T0771	Fournir une expertise en matière de caractérisation des sites web.
T0772	Préparer les exercices et fournir une expertise en la matière.
T0773	Classer par ordre de priorité les besoins en matière de collecte pour les plates-formes de collecte en fonction des capacités de ces dernières.
T0774	Traiter les données exfiltrées en vue de leur analyse et/ou de leur diffusion aux clients.
T0775	Réaliser des reconstitutions de réseaux.
T0776	Réaliser des produits d'analyse des systèmes cibles.
T0777	Établir le profil des administrateurs de réseaux ou de systèmes et de leurs activités.
T0778	Établir le profil des cibles et de leurs activités.
T0779	Fournir des conseils et une assistance aux décideurs en matière d'opérations et de renseignement pour la réaffectation des moyens et des ressources de collecte en réponse à des situations opérationnelles dynamiques.
T0780	Fournir des conseils et un soutien pour promouvoir la planification de la collecte en tant que composante intégrée des plans de campagne stratégiques et d'autres plans adaptatifs.
T0781	Fournir des recommandations sur le point d'arrivée et le réengagement.
T0782	Fournir des analyses et un soutien pour l'évaluation de l'efficacité.

ID des tâches	Description des tâches
T0783	Fournir un soutien en matière de renseignement courant aux parties prenantes internes/externes essentielles, le cas échéant.
T0784	Fournir des orientations et des conseils axés sur le cyberespace en ce qui concerne les contributions au plan de soutien en matière de renseignement.
T0785	Fournir l'évaluation et le retour d'information nécessaires à l'amélioration de la production de renseignements, des rapports sur le renseignement, des exigences en matière de collecte et des opérations.
T0786	Fournir des informations et des évaluations afin d'informer les dirigeants et les clients, d'élaborer et d'affiner les objectifs, de soutenir la planification et l'exécution des opérations et d'évaluer les effets des opérations.
T0787	Contribuer à l'élaboration et à l'affinement des objectifs, priorités, stratégies, plans et programmes en matière d'opérations cybers.
T0788	Fournir des informations et participer à l'évaluation de l'efficacité après l'action.
T0789	Fournir des informations et participer à l'élaboration de plans et d'orientations.
T0790	Fournir des informations sur les évaluations de l'efficacité du ciblage en vue de l'acceptation par les dirigeants.
T0791	Fournir des informations sur les éléments administratifs et logistiques d'un plan de soutien opérationnel.
T0792	Fournir une analyse et un soutien en matière de renseignement pour les exercices désignés, les activités de planification et les opérations sensibles au facteur temps.
T0793	Fournir un soutien en matière d'efficacité lors d'exercices désignés et/ou d'opérations sensibles au facteur temps.
T0794	Formuler des recommandations en matière d'opérations et de réengagement.
T0795	Fournir un soutien à la planification entre les partenaires internes et externes.
T0796	Fournir des informations géolocalisées exploitables en temps réel.
T0797	Formuler des recommandations en matière de ciblage qui répondent aux objectifs des dirigeants.
T0798	Fournir des produits de ciblage et un soutien au ciblage selon les besoins.
T0799	Fournir un soutien en matière de ciblage sensible au facteur temps.
T0800	Signaler en temps utile les intentions ou activités imminentes ou hostiles susceptibles d'avoir une incidence sur les objectifs, les ressources ou les capacités de l'organisation.
T0801	Recommander l'amélioration, l'adaptation, l'achèvement et l'exécution des plans opérationnels, le cas échéant.
T0802	Examiner les sources d'information appropriées afin de déterminer la validité et la pertinence des informations recueillies.
T0803	Reconstituer des réseaux sous forme de diagrammes ou de rapports.
T0804	Enregistrer les activités de collecte d'informations et/ou de préparation de l'environnement contre des cibles au cours d'opérations conçues pour produire des effets cyber.
T0805	Signaler les intrusions et les événements importants survenus sur le réseau et découlant du renseignement.
T0806	Demander le traitement et l'exploitation d'informations spécifiques à une discipline et diffuser les informations recueillies à l'aide des moyens et ressources de collecte de la discipline, conformément aux orientations et/ou procédures approuvées.
T0807	Effectuer des recherches sur les tendances en matière de communications dans les technologies émergentes (réseaux informatiques et téléphoniques, satellite, câble et sans fil) dans des sources ouvertes et classifiées.
T0808	Examiner et comprendre les objectifs et les orientations de la direction de l'organisation en matière de planification.

ID des tâches	Description des tâches
T0809	Examiner les capacités des moyens de collecte alloués.
T0810	Examiner les orientations en matière de collecte de renseignements pour en vérifier l'exactitude et l'applicabilité.
T0811	Examiner la liste des besoins de collecte classés par ordre de priorité et des informations essentielles.
T0812	Examiner et mettre à jour le plan général de collecte, le cas échéant.
T0813	Examiner, approuver, hiérarchiser et soumettre les besoins opérationnels en matière de recherche, de développement et/ou d'acquisition de capacités cybers.
T0814	Réviser la matrice de collecte en fonction de la disponibilité des moyens et ressources optimaux.
T0815	Nettoyer et réduire au minimum les informations afin de protéger les sources et les méthodes.
T0816	Établir la portée de l'effort de planification du renseignement cyber.
T0817	Servir de canal d'information pour les équipes partenaires en identifiant les experts en la matière qui peuvent aider à enquêter sur des situations complexes ou inhabituelles.
T0818	Assurer la liaison avec les partenaires extérieurs.
T0819	Solliciter et gérer jusqu'à son terme le retour d'information des demandeurs sur la qualité, la rapidité et l'efficacité de la collecte par rapport aux exigences en la matière.
T0820	Préciser les changements apportés au plan de collecte et/ou à l'environnement opérationnel qui nécessitent une réaffectation ou une réorientation des ressources et des moyens de collecte.
T0821	Préciser les collectes et/ou les missions spécifiques à une discipline qui doivent être exécutées à court terme.
T0822	Soumettre les demandes d'informations à la section de gestion des besoins en matière de collecte pour qu'elles soient traitées comme des demandes de collecte.
T0823	Soumettre des demandes de résolution de conflits des opérations cybers ou répondre à de telles demandes.
T0824	Soutenir l'identification et la documentation des effets collatéraux.
T0825	Synchroniser les activités de cyberengagement international et les besoins en ressources associés, le cas échéant.
T0826	Synchroniser les volets cyber des plans de coopération en matière de sécurité.
T0827	Synchroniser l'emploi intégré de tous les moyens de collecte de renseignements internes et de partenaires disponibles, en utilisant les capacités et les techniques de collaboration disponibles.
T0828	Tester et évaluer les outils mis au point localement en vue d'une utilisation opérationnelle.
T0829	Tester les outils et techniques développés en interne par rapport aux outils cibles.
T0830	Suivre l'état d'avancement des demandes d'information, y compris celles qui sont traitées comme des demandes de collecte et des exigences de production, à l'aide des procédures établies.
T0831	Traduire les demandes de collecte en exigences de collecte spécifiques à la discipline concernée.
T0832	Utiliser les résultats du retour d'information (par exemple, les enseignements tirés) pour identifier les possibilités d'améliorer l'efficience et l'efficacité de la gestion de la collecte.
T0833	Valider les demandes d'informations selon les critères établis.
T0834	Travailler en étroite collaboration avec les planificateurs, les analystes du renseignement et les responsables de la collecte pour s'assurer que les exigences en matière de renseignement et les plans de collecte sont exacts et à jour.

ID des tâches	Description des tâches
T0835	Travailler en étroite collaboration avec les planificateurs, les analystes et les responsables de la collecte pour identifier les lacunes en matière de renseignement et veiller à ce que les besoins en matière de renseignement soient exacts et actualisés.
T0836	Documenter les enseignements tirés qui transmettent les résultats d'événements et/ou d'exercices.
T0837	Conseiller les gestionnaires et les opérateurs sur les questions linguistiques et culturelles qui ont une incidence sur les objectifs de l'organisation.
T0838	Analyser et traiter les informations en faisant appel à des compétences linguistiques et/ou culturelles.
T0839	Évaluer, documenter et appliquer la motivation et/ou le cadre de référence d'une cible afin de faciliter l'analyse, le ciblage et les possibilités de collecte.
T0840	Collaborer avec des organisations internes et/ou externes afin d'améliorer la collecte, l'analyse et la diffusion.
T0841	Effectuer des recherches sur la cible à partir de toutes les sources, y compris l'utilisation de documents en source ouverte dans la langue cible.
T0842	Analyser les communications cibles afin d'identifier les informations essentielles à l'appui des objectifs de l'organisation.
T0843	Effectuer un contrôle de qualité et fournir un retour d'information sur les documents transcrits ou traduits.
T0844	Évaluer et interpréter les métadonnées pour rechercher des modèles, des anomalies ou des événements, afin d'optimiser le ciblage, l'analyse et le traitement.
T0845	Identifier les tactiques et méthodologies de lutte contre les cybermenaces.
T0846	Identifier les communications cibles au niveau du réseau global.
T0847	Se tenir au courant des outils et techniques de communication des cibles et des caractéristiques des réseaux de communication des cibles (par exemple, capacité, fonctionnalité, chemins, nœuds critiques) et de leurs implications potentielles pour le ciblage, la collecte et l'analyse.
T0848	Fournir un retour d'information aux responsables de la collecte afin d'améliorer la collecte et l'analyse futures.
T0849	Identifier les langues étrangères et les dialectes dans les données sources initiales.
T0850	Effectuer ou soutenir l'analyse et la cartographie des réseaux techniques.
T0851	Fournir des exigences et des informations en retour afin d'optimiser le développement d'outils de traitement linguistique.
T0852	Effectuer des analyses de réseaux sociaux et les documenter le cas échéant.
T0853	Analyser, identifier et classer par ordre de priorité les documents graphiques (y compris les communications machine-machine) et/ou vocaux cibles.
T0854	Transmettre les informations critiques ou urgentes aux clients concernés.
T0855	Transcrire les documents vocaux cibles dans la langue cible.
T0856	Traduire (par exemple, mot à mot, essentiel et/ou résumés) le matériel graphique cible.
T0857	Traduire (par exemple, mot à mot, essentiel et/ou résumés) des documents vocaux ciblés.
T0858	Identifier la terminologie en langue étrangère dans les programmes informatiques (par exemple, commentaires, noms de variables).
T0859	Fournir un soutien à l'analyse linguistique en temps quasi réel (p. ex. opérations en direct).
T0860	Identifier la terminologie liée à la cybersécurité et à la technologie dans la langue cible.
T0861	Collaborer avec le conseiller général, les affaires extérieures et les entreprises pour veiller à ce que les services existants et les nouveaux services respectent les obligations en matière de protection de la vie privée et de sécurité des données.

ID des tâches	Description des tâches
T0862	Travaillez avec le conseiller juridique et la direction, les services et comités clefs pour veiller à ce que l'organisation dispose et maintienne des formulaires de consentement et d'autorisation appropriés en matière de protection de la vie privée et de la confidentialité, ainsi que des avis et documents d'information reflétant les pratiques et exigences actuelles de l'organisation et de la loi.
T0863	Assurer la coordination avec les organismes de réglementation concernés afin de veiller à ce que les programmes, les politiques et les procédures concernant les droits civils, les libertés civiles et la protection de la vie privée soient traités de manière intégrée et globale.
T0864	Assurer la liaison avec les organismes de réglementation et d'accréditation.
T0865	Travailler avec les affaires extérieures pour développer des relations avec les régulateurs et autres responsables gouvernementaux chargés des questions de protection de la vie privée et de sécurité des données.
T0866	Maintenir une connaissance actualisée des lois fédérales et nationales applicables en matière de protection de la vie privée et des normes d'accréditation, et suivre les progrès des technologies de protection de la vie privée pour assurer l'adaptation et la conformité de l'organisation.
T0867	Veiller à ce que tous les traitements et/ou bases de données soient enregistrés auprès des autorités locales chargées de la protection de la vie privée et des données, le cas échéant.
T0868	Travailler avec les équipes commerciales et les cadres supérieurs pour assurer la sensibilisation aux "bonnes pratiques" en matière de protection de la vie privée et de sécurité des données.
T0869	Collaborer avec la direction de l'organisation pour mettre en place un comité de surveillance de la protection de la vie privée à l'échelle de l'organisation.
T0870	Jouer un rôle de premier plan dans les activités du comité de surveillance de la protection de la vie privée.
T0871	Collaborer à l'élaboration de politiques et de procédures en matière de cybersécurité et de protection de la vie privée.
T0872	Collaborer avec le personnel chargé de la cybersécurité dans le cadre du processus d'évaluation des risques de sécurité afin d'assurer le respect de la vie privée et l'atténuation des risques.
T0873	Assurer l'interface avec la direction générale afin d'élaborer des plans stratégiques pour la collecte, l'utilisation et le partage des informations de manière à en maximiser la valeur tout en respectant les réglementations applicables en matière de protection de la vie privée.
T0874	Fournir des orientations stratégiques aux responsables de l'entreprise en ce qui concerne les ressources et les technologies de l'information.
T0875	Assister le responsable de la sécurité dans le développement et la mise en œuvre d'une infrastructure informatique.
T0876	Coordonner avec le responsable de la conformité de l'entreprise les procédures de documentation et de notification de toute preuve de violation de la vie privée.
T0877	Travailler en coopération avec les unités organisationnelles concernées pour superviser les droits d'accès à l'information des consommateurs.
T0878	Assurer la liaison avec les utilisateurs des systèmes technologiques en matière de protection de la vie privée.
T0879	Assurer la liaison avec le département des systèmes d'information.
T0880	Élaborer du matériel de formation sur la protection de la vie privée et d'autres communications afin de mieux faire comprendre aux employés les politiques de l'entreprise en matière de protection de la vie privée, les pratiques et procédures de traitement des données et les obligations légales.

ID des tâches	Description des tâches
T0881	Superviser, diriger, dispenser ou veiller à ce que soit dispensée la formation initiale et l'orientation en matière de protection de la vie privée à l'ensemble des employés, des bénévoles, des sous-traitants, des alliés, des partenaires commerciaux et des autres tiers concernés.
T0882	Mener des activités continues de formation et de sensibilisation à la protection de la vie privée.
T0883	Collaborer avec le service des affaires extérieures pour établir des relations avec les organisations de consommateurs et d'autres ONG qui s'intéressent aux questions de protection de la vie privée et de sécurité des données, et pour gérer la participation de l'entreprise à des événements publics liés à la protection de la vie privée et à la sécurité des données.
T0884	Travailler avec l'administration de l'organisation, le conseil juridique et d'autres parties concernées pour représenter les intérêts de l'organisation en matière de protection de la vie privée auprès des tiers, y compris les organismes gouvernementaux, qui entreprennent d'adopter ou de modifier la législation, la réglementation ou la norme en matière de protection de la vie privée.
T0885	Rendre compte périodiquement de l'état d'avancement du programme de protection de la vie privée au conseil d'administration, au directeur général ou à toute autre personne ou comité responsable.
T0886	Collaborer avec le service des affaires extérieures pour répondre aux questions de la presse et à d'autres demandes concernant les préoccupations relatives aux données des consommateurs et des employés.
T0887	Assurer la direction du programme de protection de la vie privée de l'organisation.
T0888	Diriger et superviser les spécialistes de la protection de la vie privée et coordonner les programmes de protection de la vie privée et de sécurité des données avec les cadres supérieurs au niveau mondial afin d'assurer la cohérence dans l'ensemble de l'organisation.
T0889	Veiller au respect des pratiques en matière de protection de la vie privée et à l'application cohérente des sanctions en cas de non-respect des politiques de protection de la vie privée pour toutes les personnes faisant partie du personnel de l'organisation, du personnel élargi et de tous les associés commerciaux, en coopération avec les ressources humaines, le responsable de la sécurité de l'information, l'administration et le conseiller juridique, le cas échéant.
T0890	Élaborer des sanctions appropriées en cas de non-respect des politiques et procédures de l'entreprise en matière de protection de la vie privée.
T0891	Résoudre les allégations de non-respect des politiques de confidentialité de l'entreprise ou de la notification des pratiques en matière d'information.
T0892	Élaborer et coordonner un cadre de gestion des risques et de conformité en matière de protection de la vie privée.
T0893	Procéder à un examen complet des projets de l'entreprise en matière de données et de protection de la vie privée et veiller à ce qu'ils soient conformes aux objectifs et aux politiques de l'entreprise en matière de protection de la vie privée et de sécurité des données.
T0894	Élaborer et gérer des procédures à l'échelle de l'entreprise pour veiller à ce que le développement de nouveaux produits et services soit conforme aux politiques de l'entreprise en matière de protection de la vie privée et à ses obligations légales.
T0895	Mettre en place un processus de réception, de documentation, de suivi, d'enquête et d'action pour toutes les plaintes concernant les politiques et procédures de l'organisation en matière de protection de la vie privée.

ID des tâches	Description des tâches
T0896	Établir avec la direction et les opérations un mécanisme de suivi de l'accès aux informations de santé protégées, dans le cadre des compétences de l'organisation et conformément à la loi, et permettre aux personnes qualifiées d'examiner ou de recevoir un rapport sur une telle activité.
T0897	Diriger la planification, la conception et l'évaluation des projets liés à la protection de la vie privée et à la sécurité.
T0898	Mettre en place un programme d'audit interne de la protection de la vie privée.
T0899	Réviser périodiquement le programme de protection de la vie privée en fonction de l'évolution des lois, des réglementations ou de la politique de l'entreprise
T0900	Fournir des orientations en matière de développement et contribuer à l'identification, à la mise en œuvre et à la mise à jour des politiques et procédures de l'organisation en matière de protection de la vie privée, en coordination avec la direction et l'administration de l'organisation ainsi qu'avec le conseiller juridique.
T0901	Veiller à ce que l'utilisation des technologies maintienne et ne dégrade pas les protections de la vie privée en ce qui concerne l'utilisation, la collecte et la divulgation des informations personnelles.
T0902	Contrôler le développement et l'exploitation des systèmes pour s'assurer qu'ils sont conformes aux règles de sécurité et de protection de la vie privée.
T0903	Réaliser des évaluations de l'impact sur la vie privée des règles proposées en matière de protection de la vie privée, y compris le type d'informations personnelles collectées et le nombre de personnes concernées.
T0904	Réaliser des évaluations périodiques de l'impact sur la vie privée et des activités de contrôle de la conformité en coordination avec les autres fonctions d'évaluation de la conformité et des opérations de l'organisation.
T0905	Examiner tous les plans de sécurité de l'information liés aux systèmes afin de garantir l'harmonisation des pratiques en matière de sécurité et de protection de la vie privée.
T0906	Travailler avec l'ensemble du personnel de l'organisation concerné par tout aspect de la divulgation d'informations protégées afin d'assurer la coordination avec les politiques, les procédures et les exigences légales de l'organisation
T0907	Prendre en compte et gérer les demandes individuelles de diffusion ou de divulgation d'informations personnelles et/ou protégées.
T0908	Élaborer et gérer des procédures de vérification et d'audit des fournisseurs pour s'assurer qu'ils respectent les politiques en matière de protection de la vie privée et de sécurité des données et les exigences légales.
T0909	Participer à la mise en œuvre et au contrôle continu de la conformité de tous les accords conclus avec les partenaires commerciaux et les associés commerciaux, afin de s'assurer que toutes les préoccupations, exigences et responsabilités en matière de protection de la vie privée sont prises en compte.
T0910	Agir en tant que conseiller ou collaborer avec lui en ce qui concerne les contrats avec les partenaires commerciaux.
T0911	Atténuer les effets d'une utilisation ou d'une divulgation d'informations personnelles par des employés ou des partenaires commerciaux.
T0912	Élaborer et appliquer des procédures d'action corrective.
T0913	Gérer l'ensemble des plaintes concernant les politiques et procédures de l'organisation en matière de protection de la vie privée, en coordination et en collaboration avec d'autres fonctions similaires et, le cas échéant, avec un conseiller juridique.
T0914	Soutenir le programme de conformité de l'organisation en matière de protection de la vie privée, en travaillant en étroite collaboration avec le délégué à la protection des données, le

ID des tâches	Description des tâches
	responsable de la sécurité du système d'information et d'autres responsables de l'entreprise afin de garantir la conformité avec les lois et réglementations fédérales et nationales en matière de protection de la vie privée.
T0915	Identifier et corriger les éventuelles lacunes de conformité de l'entreprise et/ou les zones de risque afin de garantir une conformité totale avec les réglementations en matière de protection de la vie privée.
T0916	Gérer les incidents et les violations de la vie privée en collaboration avec le responsable de la protection de la vie privée, le responsable de la sécurité de l'information, le conseiller juridique et les unités opérationnelles.
T0917	Assurer la coordination avec le responsable de la sécurité de l'information afin de garantir l'harmonisation des pratiques en matière de sécurité et de protection de la vie privée.
T0918	Établir, mettre en œuvre et maintenir des politiques et des procédures à l'échelle de l'entreprise pour se conformer aux réglementations en matière de protection de la vie privée.
T0919	Veiller à ce que l'entreprise dispose de notices, de formulaires de consentement et d'autorisation et de documents appropriés en matière de protection de la vie privée et de confidentialité.
T0920	Développer et maintenir des communications et des formations appropriées pour promouvoir et former tous les membres du personnel et les membres du conseil d'administration aux questions et exigences de conformité en matière de protection de la vie privée, ainsi qu'aux conséquences de la non-conformité.
T0921	Déterminer les exigences des partenaires commerciaux en ce qui concerne le programme de protection de la vie privée de l'organisation.
T0922	Établir et gérer un processus de réception, de documentation, de suivi, d'enquête et le cas échéant de prise de mesures correctives concernant les plaintes relatives aux politiques et procédures de l'entreprise en matière de protection de la vie privée.
T0923	Coopérer avec les organismes de réglementation compétents et d'autres entités juridiques, ainsi qu'avec les responsables de l'organisation, dans le cadre de tout examen ou enquête de conformité.
T0924	Mener des activités continues de contrôle de la conformité en matière de protection de la vie privée.
T0925	Suivre les progrès des technologies de protection de la vie privée afin de s'assurer que l'organisation les adopte et s'y conforme.
T0926	Élaborer ou contribuer à l'élaboration de matériel de formation sur la protection de la vie privée et d'autres communications afin de mieux faire comprendre aux employés les politiques de l'entreprise en matière de protection de la vie privée, les pratiques et procédures de traitement des données et les obligations légales.
T0927	Nommer et guider une équipe d'experts en sécurité informatique.
T0928	Collaborer avec les parties prenantes clefs pour établir un programme de gestion des risques liés à la cybersécurité.
T0929	Identifier et affecter des personnes à des rôles spécifiques liés à la mise en œuvre du cadre de gestion des risques.
T0930	Établir une stratégie de gestion des risques pour l'organisation qui inclut une détermination de la tolérance au risque.
T0931	Identifier les missions, les fonctions opérationnelles et les processus opérationnels que le système soutiendra.
T0932	Identifier les parties prenantes qui ont un intérêt en matière de sécurité dans le développement, la mise en œuvre, l'exploitation ou le maintien d'un système.

ID des tâches	Description des tâches
T0933	Identifier les parties prenantes qui ont un intérêt en matière de sécurité dans le développement, la mise en œuvre, l'exploitation ou le maintien d'un système.
T0934	Identifier les biens des parties prenantes qui nécessitent une protection.
T0935	Procéder à une évaluation initiale des risques liés aux biens des parties prenantes et mettre à jour l'évaluation des risques en permanence.
T0936	Définir les besoins de protection et les exigences de sécurité des parties prenantes.
T0937	Déterminer l'emplacement d'un système dans l'architecture de l'entreprise.
T0938	Identifier les contrôles communs à l'ensemble de l'organisation qui peuvent être hérités par les systèmes de l'organisation.
T0939	Effectuer une catégorisation de sécurité de deuxième niveau pour les systèmes organisationnels ayant le même niveau d'impact.
T0940	Déterminer les limites d'un système.
T0941	Identifier les exigences de sécurité attribuées à un système et à l'organisation.
T0942	Identifier les types d'informations devant être traitées, stockées ou transmises par un système.
T0943	Catégoriser le système et documenter les résultats de la catégorisation de sécurité dans le cadre des exigences du système.
T0944	Décrire les caractéristiques d'un système.
T0945	Inscrire le système auprès des bureaux de gestion/programmes appropriés de l'organisation.
T0946	Sélectionner les mesures de sécurité pour un système et documenter la description fonctionnelle de la mise en œuvre des mesures de sécurité prévues dans le cadre d'un plan de sécurité.
T0947	Élaborer une stratégie de surveillance de l'efficacité des contrôles de sécurité ; coordonner la stratégie au niveau du système avec la stratégie de surveillance au niveau de l'organisation et de la mission/du processus opérationnel.
T0948	Examiner et approuver les plans de sécurité.
T0949	Mettre en œuvre les contrôles de sécurité spécifiés dans un plan de sécurité ou dans d'autres documents relatifs au système.
T0950	Documenter les modifications apportées à la mise en œuvre des contrôles de sécurité prévus et établir la configuration de base d'un système.
T0951	Élaborer, examiner et approuver un plan d'évaluation des contrôles de sécurité d'un système et de l'organisation.
T0952	Évaluer les contrôles de sécurité conformément aux procédures d'évaluation définies dans un plan d'évaluation de la sécurité.
T0953	Préparer un rapport d'évaluation de la sécurité documentant les problèmes, les résultats et les recommandations de l'évaluation des contrôles de sécurité.
T0954	Mener des actions correctives sur les mesures de sécurité sur la base des conclusions et des recommandations d'un rapport d'évaluation de la sécurité ; réévaluer les mesures correctives.
T0955	Préparer un plan d'action et des étapes sur la base des conclusions et des recommandations d'un rapport d'évaluation de la sécurité, à l'exclusion de toute mesure corrective prise.
T0956	Constituer un dossier d'autorisation et le soumettre à un représentant de l'autorité compétente en vue d'une décision.
T0957	Déterminer le risque lié au fonctionnement ou à l'utilisation d'un système ou à la fourniture ou à l'utilisation de contrôles communs.
T0958	Identifier et mettre en œuvre un plan d'action privilégié en réponse au risque déterminé.
T0959	Déterminer si le risque lié au fonctionnement ou à l'utilisation du système, ou à la fourniture ou à l'utilisation de contrôles communs, est acceptable.
T0960	Surveiller les changements apportés à un système et à son environnement d'exploitation.

ID des tâches	Description des tâches
T0961	Évaluer les mesures de sécurité employées dans le cadre du système et héritées de celui-ci, conformément à une stratégie de surveillance définie par l'organisation.
T0962	Traiter les risques sur la base des résultats des activités de surveillance en cours, de l'évaluation des risques et des points en suspens dans un plan d'action et des jalons.
T0963	Mettre à jour un plan de sécurité, un rapport d'évaluation de la sécurité et un plan d'action et d'étapes sur la base des résultats d'un processus de surveillance continue.
T0964	Rendre compte de l'état de la sécurité d'un système (y compris de l'efficacité des contrôles de sécurité) à un représentant de l'autorité compétente de manière continue, conformément à la stratégie de surveillance.
T0965	Examiner en permanence l'état de sécurité d'un système (y compris l'efficacité des contrôles de sécurité) afin de déterminer si le risque reste acceptable.
T0966	Mettre en œuvre une stratégie d'élimination des systèmes qui exécute les actions requises lorsqu'un système est mis hors service.
T0967	Encourager et promouvoir la surveillance continue au sein de l'organisation.
T0968	Affecter le personnel nécessaire aux groupes de travail chargés de la surveillance continue.
T0969	Déterminer les exigences en matière d'établissement de rapports pour soutenir les activités de surveillance continue.
T0970	Établir des mesures de notation et de classement pour mesurer l'efficacité du programme de surveillance continue.
T0971	Déterminer comment intégrer un programme de surveillance continue dans les structures et les politiques de gouvernance de la sécurité de l'information de l'organisation.
T0972	Utiliser les mesures de notation et de classement de la surveillance continue pour prendre des décisions en matière d'investissement dans la sécurité de l'information afin de résoudre les problèmes persistants.
T0973	Veiller à ce que l'équipe chargée de la surveillance continue dispose de la formation et des ressources (par exemple, le personnel et le budget) nécessaires pour s'acquitter des tâches qui lui sont confiées.
T0974	Collaborer avec les analystes des risques organisationnels pour veiller à ce que les rapports de contrôle continu couvrent les niveaux appropriés de l'organisation.
T0975	Travailler avec les analystes des risques de l'organisation pour s'assurer que les mesures des risques sont définies de manière réaliste afin de soutenir le contrôle continu.
T0976	Travailler avec les responsables de l'organisation pour s'assurer que les données de l'outil de contrôle continu permettent de connaître la situation des niveaux de risque.
T0977	Établir des déclencheurs pour les seuils de risque inacceptables pour les données de surveillance continue.
T0978	Travailler avec les responsables de l'organisation pour établir des catégories de rapports au niveau du système qui peuvent être utilisées par le programme de surveillance continue de l'organisation.
T0980	Désigner une personne qualifiée comme responsable de la gestion et de la mise en œuvre du programme de surveillance continue.
T0981	Identifier les parties prenantes de la surveillance continue et établir un processus pour les tenir informées du programme.
T0982	Identifier les exigences en matière de reporting axé sur la sécurité de l'organisation qui sont satisfaites par le programme de surveillance continue.
T0983	Utiliser les données de surveillance continue pour prendre des décisions d'investissement en matière de sécurité de l'information afin de résoudre les problèmes persistants.

ID des tâches	Description des tâches
T0984	Définir des déclencheurs dans le cadre du programme de surveillance continue qui peuvent être utilisés pour définir un risque inacceptable et entraîner la prise de mesures pour le résoudre.
T0985	Établir des mesures de notation et de classement pour mesurer l'efficacité du programme de surveillance continue.
T0986	Collaborer avec les responsables de la sécurité pour définir les exigences appropriées en matière de rapports de surveillance continue au niveau du système.
T0987	Utiliser les outils et les technologies de surveillance continue pour évaluer les risques en permanence.
T0988	Établir des exigences appropriées en matière d'établissement de rapports conformément aux critères identifiés dans le programme de surveillance continue en vue d'une utilisation dans l'évaluation automatisée des contrôles.
T0989	Utiliser des méthodes d'évaluation non automatisées lorsque les données provenant des outils et technologies de surveillance continue ne sont pas encore suffisantes ou de qualité adéquate.
T0990	Développer des processus avec l'équipe d'audit externe pour partager les informations relatives au programme de surveillance continue et à son impact sur l'évaluation des contrôles de sécurité.
T0991	Identifier les exigences en matière de rapports à utiliser dans l'évaluation automatisée des contrôles pour soutenir la surveillance continue.
T0992	Déterminer comment les résultats de la surveillance continue seront utilisés dans le cadre de l'autorisation permanente.
T0993	Établir un processus et des procédures de contrôle d'accès aux outils et technologies de surveillance continue.
T0994	Veiller à ce que le contrôle d'accès aux outils et technologies de surveillance continue soit géré de manière adéquate.
T0995	Mettre en place un processus permettant de fournir une aide technique aux personnes chargées d'atténuer les effets de la surveillance continue.
T0996	Coordonner les exigences en matière de rapports de surveillance continue entre les différents utilisateurs.
T0997	Définir les responsabilités en matière de soutien à la mise en œuvre de chaque outil ou technologie de contrôle continu.
T0998	Établir une liaison avec le groupe de travail chargé de la notation et des mesures afin de soutenir la surveillance continue.
T0999	Établir et appliquer un processus de gestion de l'introduction de nouveaux risques pour soutenir la surveillance continue.
T1000	Mettre en place un sous-groupe chargé des questions et de la coordination des paramètres de configuration de la surveillance continue.
T1001	Définir les exigences en matière d'outils et de technologies de surveillance continue, de mesure des performances et de gestion.
T1002	Utiliser des notes et des appréciations pour motiver et évaluer les performances tout en répondant aux préoccupations en matière de surveillance continue.
T1003	Travailler avec les responsables de la sécurité (c'est-à-dire les propriétaires de systèmes, les responsables de la sécurité des systèmes d'information, les responsables de la sécurité des systèmes d'information, etc.) pour définir les exigences appropriées en matière de rapports pour la surveillance continue au niveau du système.
T1004	Utiliser les outils de contrôle continu pour évaluer en permanence les risques.

ID des tâches	Description des tâches
T1005	Utiliser les données de contrôle continu pour prendre des décisions d'investissement en matière de sécurité de l'information afin de résoudre les problèmes persistants.
T1006	Réagir aux problèmes signalés lors de la surveillance continue, faire remonter l'information et coordonner une réponse.
T1007	Examiner les résultats du programme de contrôle continu et atténuer les risques en temps utile.

A.5 Descriptions des connaissances du référentiel NICE

Tableau 5 fournit une liste des différents types d'informations directement associées à l'exécution d'une fonction. Une sélection d'identifiants et de descriptions de connaissances tirés de cette liste est incluse pour chaque fonction dans la liste détaillée des fonctions de l'annexe B. Les six premiers sont communs à toutes les fonctions dans le domaine de la cybersécurité. Cette liste sera mise à jour régulièrement [1]. La source de référence pour la version la plus récente de ce document est le tableur de référence de la publication spéciale 800-181 du NIST [4].

Tableau 5 – Descriptions des connaissances du référentiel NICE

ID KSA	Descriptions
K0001	Connaissance des concepts et protocoles réseaux informatiques et des méthodologies de sécurité des réseaux.
K0002	Connaissance des processus de gestion des risques (par exemple, méthodes d'évaluation et d'atténuation des risques).
K0003	Connaissance des lois, des règlements, des politiques et de l'éthique en matière de cybersécurité et de protection de la vie privée.
K0004	Connaissance des principes de cybersécurité et de protection de la vie privée.
K0005	Connaissance des cybermenaces et des vulnérabilités.
K0006	Connaissance des impacts opérationnels propres aux défaillances en matière de cybersécurité.
K0007	Connaissance des méthodes d'authentification, d'autorisation et de contrôle d'accès.
K0008	Connaissance des processus opérationnels applicables et des opérations des organisations clientes.
K0009	Connaissance des vulnérabilités des applications.
K0010	Connaissance des méthodes, principes et concepts de communication qui soutiennent l'infrastructure du réseau.
K0011	Connaissance des capacités et des applications des équipements réseau, y compris les routeurs, les commutateurs, les passerelles, les serveurs, les systèmes de transmission et le matériel connexe.
K0012	Connaissance de l'analyse des capacités et des besoins.
K0013	Connaissance des outils de cybersécurité et d'évaluation des vulnérabilités et de leurs capacités.
K0014	Connaissance des structures de données complexes.
K0015	Connaissance des algorithmes informatiques.
K0016	Connaissance des principes de programmation informatique.
K0017	Connaissance des concepts et des pratiques de traitement des données de criminalistique numérique.
K0018	Connaissance des algorithmes de chiffrement.
K0019	Connaissance des concepts de cryptographie et de gestion des clefs cryptographiques.
K0020	Connaissance des politiques d'administration et de normalisation des données.
K0021	Connaissance des principes de sauvegarde et de récupération des données.
K0022	Connaissance des principes de data mining et de data warehousing.
K0023	Connaissance des systèmes de gestion de bases de données, des langages de requêtes, des relations entre les tables et des vues.
K0024	Connaissance des systèmes de bases de données.
K0025	Connaissance de la gestion des droits numériques.
K0026	Connaissance des plans de continuité d'activité et de reprise après sinistre.

ID KSA	Descriptions
K0027	Connaissance de l'architecture de sécurité de l'information de l'organisation.
K0028	Connaissance des exigences de l'organisation en matière d'évaluation et de validation.
K0029	Connaissance des connexions entre les réseaux locaux et les réseaux étendus de l'organisation.
K0030	Connaissance de l'ingénierie électrique appliquée à l'architecture informatique (par exemple, circuits imprimés, processeurs, puces et matériel informatique).
K0031	Connaissance des systèmes de messagerie d'entreprise et des logiciels associés.
K0032	Connaissance de la résilience et de la redondance.
K0033	Connaissance des mécanismes de contrôle d'accès à l'hôte/au réseau (par exemple, liste de contrôle d'accès, listes de droits).
K0034	Connaissance des services réseau et des interactions des protocoles qui assurent les communications réseau.
K0035	Connaissance de l'installation, de l'intégration et de l'optimisation des composants du système.
K0036	Connaissance des principes d'interaction homme-machine.
K0037	Connaissance du processus d'évaluation et d'autorisation de la sécurité.
K0038	Connaissance des principes de cybersécurité et de protection de la vie privée utilisés pour gérer les risques liés à l'utilisation, au traitement, au stockage et à la transmission d'informations ou de données.
K0039	Connaissance des principes et méthodes de cybersécurité et de protection de la vie privée qui s'appliquent au développement de logiciels.
K0040	Connaissance des sources de diffusion d'informations sur les vulnérabilités (par exemple : alertes, avis, errata et bulletins).
K0041	Connaissance des catégories d'incidents, des réponses aux incidents et des délais de réponse.
K0042	Connaissance des méthodologies de réponse et de traitement des incidents.
K0043	Connaissance des principes et méthodes d'analyse conformes aux normes de l'industrie et acceptées par l'organisation.
K0044	Connaissance des principes de cybersécurité et de protection de la vie privée et des exigences organisationnelles (en matière de confidentialité, d'intégrité, de disponibilité, d'authentification et de non-répudiation).
K0045	Connaissance des principes d'ingénierie des systèmes de sécurité de l'information (NIST SP 800-160).
K0046	Connaissance des méthodologies et techniques de détection des intrusions sur l'hôte et le réseau.
K0047	Connaissance des concepts et référentiels en matière d'architecture des technologies de l'information (TI).
K0048	Connaissance des exigences du cadre de gestion des risques (Risk Management Framework ou RMF).
K0049	Connaissance des méthodes et principes de sécurité des technologies de l'information (TI) (par exemple, pare-feu, zones démilitarisées, chiffrement).
K0050	Connaissance des principes et concepts des réseaux locaux et étendus, y compris la gestion de la bande passante.
K0051	Connaissance des langages informatiques de bas niveau (par exemple, langages assembleurs).
K0052	Connaissance des mathématiques (par exemple, logarithmes, trigonométrie, algèbre linéaire, calcul, statistiques et analyse opérationnelle).
K0053	Connaissance des mesures ou indicateurs de performance et de disponibilité des systèmes.

ID KSA	Descriptions
K0054	Connaissance des méthodes industrielles actuelles d'évaluation, de mise en œuvre et de diffusion des outils et procédures d'évaluation, de surveillance, de détection et de correction de la sécurité des technologies de l'information (TI) utilisant des concepts et des capacités fondés sur des normes.
K0055	Connaissance des microprocesseurs.
K0056	Connaissance de la gestion des accès, des identités et des accès aux réseaux (par exemple, infrastructure à clef publique, Oauth, OpenID, SAML, SPML).
K0057	Connaissance des équipements et des fonctions du matériel réseau.
K0058	Connaissance des méthodes d'analyse du trafic réseau.
K0059	Connaissance des technologies de l'information (TI) et de la cybersécurité qui sont récentes et émergentes.
K0060	Connaissance des systèmes d'exploitation.
K0061	Connaissance de la manière dont le trafic circule sur le réseau (par exemple, protocole de contrôle de transmission [TCP] et protocole Internet [IP], modèle OSI (Open System Interconnection Model), version courante d'ITIL (Information Technology Infrastructure Library)).
K0062	Connaissance de l'analyse de paquets.
K0063	Connaissance des concepts de l'informatique parallèle et distribuée.
K0064	Connaissance des outils et techniques d'optimisation des performances.
K0065	Connaissance des contrôles d'accès fondés sur des politiques et adaptables aux risques.
K0066	Connaissance des évaluations de l'impact sur la vie privée.
K0067	Connaissance des concepts d'ingénierie des processus.
K0068	Connaissance des structures et de la logique des langages de programmation.
K0069	Connaissance des langages de requête tels que SQL (langage de requête structurée).
K0070	Connaissance des menaces et des vulnérabilités en matière de sécurité des systèmes et des applications (par exemple : débordement de mémoire tampon, code mobile, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] et injections, accès concurrents (race conditions), covert channel, relecture, attaques de type "return-oriented", code malveillant).
K0071	Connaissance des concepts de technologie d'accès à distance.
K0072	Connaissance des principes et techniques de gestion des ressources.
K0073	Connaissance des techniques de gestion de configuration sécurisée. (par exemple, les guides techniques de mise en œuvre de la sécurité (STIG), les bonnes pratiques en matière de cybersécurité sur cisecurity.org).
K0074	Connaissance des concepts clefs de la gestion de la sécurité (par exemple, gestion des versions, gestion des correctifs).
K0075	Connaissance des outils, des méthodes et des techniques de conception de systèmes de sécurité.
K0076	Connaissance des théories, des concepts et des méthodes d'administration des serveurs et d'ingénierie des systèmes.
K0077	Connaissance des systèmes d'exploitation des serveurs et des clients.
K0078	Connaissance des outils de diagnostic des serveurs et des techniques d'identification des pannes.
K0079	Connaissance des principes de débogage des logiciels.
K0080	Connaissance des outils, des méthodes et des techniques de conception de logiciels.
K0081	Connaissance des modèles de développement de logiciels (par exemple, modèle en cascade, modèle en spirale).
K0082	Connaissance du génie logiciel.

ID KSA	Descriptions
K0083	Connaissance des sources, des caractéristiques et des utilisations des données de l'organisation.
K0084	Connaissance des principes et des méthodes d'analyse structurée.
K0086	Connaissance des outils, des méthodes et des techniques de conception de systèmes, y compris des outils d'analyse et de conception de systèmes automatisés.
K0087	Connaissance des normes, des politiques et des approches reconnues (par exemple, les normes de l'Organisation internationale de normalisation [ISO]) en matière de conception de logiciels et d'organisations relatives à la conception de systèmes.
K0088	Connaissance des concepts d'administration des systèmes.
K0089	Connaissance des outils de diagnostic des systèmes et des techniques d'identification des défauts.
K0090	Connaissance des principes de gestion du cycle de vie des systèmes, y compris la sécurité et la facilité d'utilisation des logiciels.
K0091	Connaissance des méthodes de test et d'évaluation des systèmes.
K0092	Connaissance des processus d'intégration technologique.
K0093	Connaissance des concepts de télécommunications (par exemple, canal de communication, bilan de liaison système, efficacité spectrale, multiplexage).
K0094	Connaissance des capacités et des fonctionnalités associées aux technologies de création de contenu (par exemple, wikis, réseaux sociaux, systèmes de gestion de contenu (CMS), blogs).
K0095	Connaissance des capacités et des fonctionnalités associées à diverses technologies d'organisation et de gestion de l'information (par exemple, bases de données, moteurs de signets).
K0096	Connaissance des capacités et des fonctionnalités de diverses technologies de collaboration (par exemple, logiciels de travail collaboratif, SharePoint).
K0097	Connaissance des caractéristiques des supports de stockage de données physiques et virtuels.
K0098	Connaissance de la structure hiérarchique des fournisseurs de services de cyberdéfense et des processus au sein de sa propre organisation.
K0100	Connaissance de l'architecture des technologies de l'information (TI) de l'entreprise.
K0101	Connaissance des buts et des objectifs de l'organisation en matière de technologies de l'information (TI).
K0102	Connaissance du processus d'ingénierie des systèmes.
K0103	Connaissance du type et de la fréquence de la maintenance ordinaire du matériel.
K0104	Connaissance de la sécurité des réseaux privés virtuels (VPN).
K0105	Connaissance des services web (par exemple, architecture orientée services, protocole SOAP (Simple Object Access Protocol) et langage de description des services web (WSDL)).
K0106	Connaissance de ce qui constitue une attaque de réseau et de la relation entre une attaque de réseau et les menaces et vulnérabilités.
K0107	Connaissance des enquêtes sur les menaces d'initiés, des rapports, des outils d'investigation et des lois/réglementations.
K0108	Connaissance des concepts, de la terminologie et du fonctionnement d'un large éventail de moyens de communication (réseaux informatiques et téléphoniques, satellite, fibre optique, sans fil).
K0109	Connaissance des composants et des architectures physiques des ordinateurs, y compris les fonctions des divers composants et périphériques (par exemple, CPU, cartes réseau, stockage de données).
K0110	Connaissance des tactiques, techniques et procédures des adversaires.

ID KSA	Descriptions
K0111	Connaissance des outils réseau (par exemple, ping, traceroute, nslookup).
K0112	Connaissance des principes de défense en profondeur et de l'architecture de sécurité des réseaux.
K0113	Connaissance des différents types de communication réseau (par exemple, LAN, WAN, MAN, WLAN, WWAN).
K0114	Connaissance des dispositifs électroniques (par exemple, systèmes/composants informatiques, dispositifs de contrôle d'accès, appareils photo numériques, scanners numériques, agendas électroniques, disques durs, cartes mémoire, modems, équipements réseau, appareils en réseau, dispositifs domotiques en réseau, imprimantes, dispositifs de stockage amovibles, téléphones, photocopieurs, télécopieurs, etc.)
K0115	Connaissance des technologies pouvant être exploitées.
K0116	Connaissance des extensions de fichiers (par exemple, .dll, .bat, .zip, .pcap, .gzip).
K0117	Connaissance des implémentations de systèmes de fichiers (par exemple, New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).
K0118	Connaissance des processus de saisie et de conservation des preuves numériques.
K0119	Connaissance des méthodes de piratage informatique.
K0120	Connaissance de la manière dont les besoins en informations et les exigences en matière de collecte sont traduits, suivis et classés par ordre de priorité dans l'entreprise étendue.
K0121	Connaissance des principes et des techniques de gestion des programmes et des projets de sécurité de l'information.
K0122	Connaissance des implications du matériel, des systèmes d'exploitation et des technologies réseau dans le cadre d'enquêtes.
K0123	Connaissance de la gouvernance juridique en matière d'admissibilité (par exemple, règles de preuve).
K0124	Connaissance des multiples domaines cognitifs et des outils et méthodes applicables à l'apprentissage dans chaque domaine.
K0125	Connaissance des processus de collecte, d'emballage, de transport et de stockage des preuves électroniques tout en maintenant la chaîne de responsabilité.
K0126	Connaissance des pratiques de gestion des risques de la chaîne d'approvisionnement (NIST SP 800-161).
K0127	Connaissance de la nature et de la fonction de la structure d'information de référence (par exemple, la National Information Infrastructure).
K0128	Connaissance des types de données persistantes et de leur collecte.
K0129	Connaissance des outils de ligne de commande (par exemple, mkdir, mv, ls, passwd, grep).
K0130	Connaissance des technologies de virtualisation et du développement et de la maintenance de machines virtuelles.
K0131	Connaissance de la collecte de courrier électronique, des techniques de recherche et d'analyse, des outils et des cookies.
K0132	Connaissance des fichiers système (par exemple, fichiers journaux, fichiers de registre, fichiers de configuration) contenant des informations utiles et de l'endroit où trouver ces fichiers système.
K0133	Connaissance des types de données de criminalistique numérique et de la manière de les reconnaître.
K0134	Connaissance de la criminalistique déployable.
K0135	Connaissance des technologies de filtrage du web.
K0136	Connaissance des capacités des différents systèmes et méthodes de communication électronique (par exemple, courrier électronique, VOIP, messagerie instantanée, forums web, diffusion vidéo en direct).

ID KSA	Descriptions
K0137	Connaissance de la gamme des réseaux existants (par exemple, PBX, LAN, WAN, WIFI, SCADA).
K0138	Connaissance du Wi-Fi.
K0139	Connaissance des langages informatiques interprétés et compilés.
K0140	Connaissance des techniques de codage sécurisé.
K0141	RETIRÉ : intégré dans K0420
K0142	Connaissance des processus, des possibilités et des limites de la gestion des collectes.
K0143	Connaissance des systèmes de collecte frontaux, incluant la capture, le filtrage et la sélection du trafic.
K0144	Connaissance de la dynamique sur le plan social des attaquants informatiques dans un contexte mondial.
K0145	Connaissance des outils de mise en corrélation des événements de sécurité.
K0146	Connaissance des processus de base de l'activité/de la mission de l'organisation.
K0147	Connaissance des problématiques, risques et vulnérabilités émergents en matière de sécurité.
K0148	Connaissance des réglementations en matière de contrôle des importations/exportations et des organismes responsables en vue de réduire les risques liés à la chaîne d'approvisionnement.
K0149	Connaissance de la tolérance au risque de l'organisation et/ou de l'approche de la gestion du risque.
K0150	Connaissance du programme de réponse aux incidents de l'entreprise, des rôles et des responsabilités.
K0151	Connaissance des menaces/vecteurs de menaces actuels et émergents.
K0152	Connaissance des principes et méthodes de sécurité des technologies de l'information (TI) liés aux logiciels (par exemple, modularisation, stratification, abstraction, masquage des données, simplicité/minimisation).
K0153	Connaissance du processus d'assurance qualité des logiciels.
K0154	Connaissance des normes, des processus et des pratiques de gestion des risques de la chaîne d'approvisionnement.
K0155	Connaissance du droit de la preuve électronique.
K0156	Connaissance des règles juridiques en matière de preuve et de procédure judiciaire.
K0157	Connaissance des politiques, des procédures et des réglementations en matière de cyberdéfense et de sécurité de l'information.
K0158	Connaissance des politiques de sécurité des utilisateurs des technologies de l'information (TI) de l'organisation (par exemple, création de comptes, règles relatives aux mots de passe, contrôle d'accès).
K0159	Connaissance de la voix sur IP (VoIP).
K0160	Connaissance des vecteurs d'attaque courants sur la couche réseau.
K0161	Connaissance des différentes types d'attaques (par exemple : attaques passives, actives, d'initiés, rapprochées, de distribution).
K0162	Connaissance des cyberattaquants (par exemple : script kiddies, initiés, soutenus par des États non nationaux et soutenus par des États nationaux).
K0163	Connaissance des exigences essentielles en matière d'achats de technologies de l'information (TI).
K0164	Connaissance des exigences en matière de fonctionnalité, de qualité et de sécurité et de la manière dont elles s'appliquent à des produits spécifiques (c'est-à-dire des éléments et des processus).
K0165	Connaissance de l'évaluation des risques et des menaces.

ID KSA	Descriptions
K0167	Connaissance des techniques d'administration des systèmes, des réseaux et des systèmes d'exploitation.
K0168	Connaissance des lois et statuts applicables (par exemple, les titres 10, 18, 32 et 50 du code des États-Unis), des directives présidentielles, des directives de l'exécutif et/ou des directives et procédures juridiques administratives/pénales.
K0169	Connaissance des politiques, exigences et procédures en matière de sécurité de la chaîne d'approvisionnement des technologies de l'information (TI) et de gestion des risques de la chaîne d'approvisionnement.
K0170	Connaissance des systèmes d'infrastructures critiques utilisant des technologies de l'information et de la communication qui ont été conçus sans tenir compte de la sécurité des systèmes.
K0171	Connaissance des techniques de rétro-ingénierie du matériel.
K0172	Connaissance des middlewares (par exemple, Enterprise Service Bus et Message Queuing).
K0174	Connaissance des protocoles réseaux.
K0175	Connaissance des techniques de rétro-ingénierie des logiciels.
K0176	Connaissance des schémas XML (Extensible Markup Language).
K0177	Connaissance des étapes d'une cyberattaque (par exemple : reconnaissance, balayage, énumération, obtention d'un accès, escalade des privilèges, maintien de l'accès, exploitation du réseau, dissimulation des traces).
K0178	Connaissance des méthodologies, outils et pratiques de déploiement de logiciels sécurisés.
K0179	Connaissance des concepts d'architecture de sécurité des réseaux, y compris la topologie, les protocoles, les composants et les principes (par exemple, l'application de la défense en profondeur).
K0180	Connaissance des principes, des modèles, des méthodes (par exemple, surveillance des performances des systèmes de bout en bout) et des outils de gestion des systèmes de réseau.
K0182	Connaissance des outils et techniques de fragmentation des données (par exemple, Foremost).
K0183	Connaissance des concepts de rétro-ingénierie.
K0184	Connaissance des tactiques, techniques et procédures de lutte contre l'investigation numérique légale.
K0185	Connaissance de la configuration des laboratoires d'investigation numérique légale et des applications de support (par exemple VMWare, Wireshark).
K0186	Connaissance des procédures et des outils de débogage.
K0187	Connaissance de l'utilisation abusive des types de fichiers par les adversaires pour détecter les comportements anormaux.
K0188	Connaissance des outils d'analyse des logiciels malveillants (par exemple, Olly Debug, Ida Pro).
K0189	Connaissance des logiciels malveillants avec détection des machines virtuelles (par exemple, logiciels malveillants avec détection des machines virtuelles, logiciels malveillants avec détection du débogueur et logiciels malveillants décompressés qui recherchent des chaînes liées aux machines virtuelles dans l'équipement informatique de votre ordinateur).
K0190	Connaissance des méthodes de chiffrement.
K0191	Connaissance de l'impact de la mise en œuvre des signatures pour les virus, les logiciels malveillants et les attaques.
K0192	Connaissance des ports et services Windows/Unix.
K0193	Connaissance des fonctions de sécurité avancées de remédiation des données dans les bases de données.

ID KSA	Descriptions
K0194	Connaissance des technologies de gestion des connaissances basées sur le Cloud et des concepts liés à la sécurité, à la gouvernance, à l'approvisionnement et à l'administration.
K0195	Connaissance des normes et des méthodes de classification des données en fonction de leur sensibilité et d'autres facteurs de risque.
K0196	Connaissance des réglementations en matière d'importation et d'exportation liées à la cryptographie et à d'autres technologies de sécurité.
K0197	Connaissance des interfaces de programmation des applications d'accès aux bases de données (par exemple, Java Database Connectivity [JDBC]).
K0198	Connaissance des concepts d'amélioration des processus organisationnels et des modèles de maturité des processus (par exemple, Capability Maturity Model Integration (CMMI) pour le développement, CMMI pour les services et CMMI pour les acquisitions).
K0199	Connaissance des concepts d'architecture de sécurité et des modèles de référence d'architecture d'entreprise (par exemple, Zachman, Federal Enterprise Architecture [FEA]).
K0200	Connaissance des concepts de gestion des services pour les réseaux et des normes correspondantes (par exemple, la version courante d'Information Technology Infrastructure Library [ITIL]).
K0201	Connaissance des techniques et des concepts de rotation des clefs symétriques.
K0202	Connaissance des concepts et des fonctions du pare-feu applicatif (par exemple, point unique d'authentification/d'audit/d'application de la politique, analyse des messages pour détecter les contenus malveillants, anonymisation des données pour la conformité PCI et PII, analyse de la protection contre la perte de données, opérations cryptographiques accélérées, sécurité SSL, traitement REST/JSON).
K0203	Connaissance des modèles de sécurité (par exemple, modèle Bell-LaPadula, modèle d'intégrité Biba, modèle d'intégrité Clark-Wilson).
K0204	Connaissance des techniques d'évaluation de l'apprentissage (rubriques, plans d'évaluation, tests, quiz).
K0205	Connaissance des techniques de base de renforcement des systèmes, des réseaux et des systèmes d'exploitation.
K0206	Connaissance des principes et des techniques de hacking éthique.
K0207	Connaissance de l'analyse des circuits.
K0208	Connaissance de la formation assistée par ordinateur et des services d'apprentissage en ligne.
K0209	Connaissance des techniques de communication secrète.
K0210	Connaissance des concepts de sauvegarde et de restauration des données.
K0211	Connaissance des exigences en matière de confidentialité, d'intégrité et de disponibilité.
K0212	Connaissance des logiciels axés sur la cybersécurité.
K0213	Connaissance des modèles de conception et d'évaluation pédagogiques (par exemple, ADDIE, modèle Smith/Ragan, étapes d'apprentissage de Gagné, modèle d'évaluation de Kirkpatrick).
K0214	Connaissance de la méthodologie d'évaluation du cadre de gestion des risques.
K0215	Connaissance des politiques de formation de l'organisation.
K0216	Connaissance des niveaux d'apprentissage (c'est-à-dire la taxonomie de Bloom).
K0217	Connaissance des systèmes de gestion de l'apprentissage et de leur utilisation dans la gestion de l'apprentissage.
K0218	Connaissance des styles d'apprentissage (par exemple, assimilateur, auditif, kinesthésique).
K0220	Connaissance des modes d'apprentissage (par exemple, apprentissage par cœur, observation).
K0221	Connaissance du modèle OSI et des protocoles réseaux sous-jacents (par exemple, TCP/IP).

ID KSA	Descriptions
K0222	Connaissance des lois, des autorités juridiques, des restrictions et des réglementations applicables aux activités de cyberdéfense.
K0223	RETIRÉ : intégré dans K0073
K0224	Connaissance des concepts d'administration de systèmes d'exploitation tels que, mais sans s'y limiter, les systèmes d'exploitation Unix/Linux, IOS, Android et Windows.
K0226	Connaissance des systèmes de formation de l'organisation.
K0227	Connaissance des différents types d'architectures informatiques.
K0228	Connaissance de la théorie de la taxonomie et de l'ontologie sémantique.
K0229	Connaissance des applications qui peuvent enregistrer les erreurs, les exceptions, les défauts d'application et la journalisation.
K0230	Connaissance des modèles de services Cloud et de la manière dont ces modèles peuvent limiter la réponse aux incidents.
K0231	Connaissance des protocoles, des processus et des techniques de gestion de crise.
K0233	Connaissance du référentiel NCWF (National Cybersecurity Workforce Framework), des fonctions et des tâches, des connaissances, des capacités et des aptitudes qui y sont associées.
K0234	Connaissance de l'ensemble du spectre des capacités cybers (par exemple, défense, attaque, exploitation).
K0235	Connaissance de la manière d'exploiter les centres de recherche et de développement, les groupes de réflexion, la recherche universitaire et les systèmes industriels.
K0236	Connaissance de l'utilisation de Hadoop, Java, Python, SQL, Hive et Pig pour explorer les données.
K0237	Connaissance des bonnes pratiques de l'industrie en matière de centre de services.
K0238	Connaissance de la théorie et des principes de l'apprentissage automatique.
K0239	Connaissance des techniques et méthodes de production, de communication et de diffusion des médias, y compris des moyens alternatifs d'informer par le biais des médias écrits, oraux et visuels.
K0240	Connaissance des systèmes de sécurité à plusieurs niveaux et des solutions interdomaines.
K0241	Connaissance des politiques, des processus et des procédures organisationnels en matière de ressources humaines.
K0242	Connaissance des politiques de sécurité organisationnelles.
K0243	Connaissance des politiques, des processus et des procédures de formation et d'éducation organisationnelles.
K0244	Connaissance des comportements physiques et physiologiques pouvant indiquer une activité suspecte ou anormale.
K0245	Connaissance des principes et des processus d'évaluation des besoins en matière de formation et d'éducation.
K0246	Connaissance des concepts, des procédures, des logiciels, des équipements et des applications technologiques pertinents.
K0247	Connaissance des processus, des outils et des capacités d'accès à distance liés à l'assistance à la clientèle.
K0248	Connaissance de la théorie et de la pratique stratégiques.
K0249	Connaissance des technologies, des processus et des stratégies de support.
K0250	Connaissance des processus de test et d'évaluation des apprenants.
K0251	Connaissance du processus judiciaire, y compris la présentation des faits et des preuves.
K0252	Connaissance des principes et méthodes de formation et d'éducation pour la conception de programmes, l'enseignement et l'instruction des individus et des groupes, et la mesure des effets de la formation et de l'éducation.

ID KSA	Descriptions
K0253	RETIRÉ : intégré dans K0227
K0254	Connaissance de l'analyse binaire.
K0255	Connaissance des concepts d'architecture réseau, y compris la topologie, les protocoles et les composants.
K0257	Connaissance des exigences en matière d'acquisition/de passation de marchés dans le domaine des technologies de l'information (TI).
K0258	Connaissance des procédures, principes et méthodologies d'essai (par exemple, modèle CMMI d'intégration des capacités et de la maturité).
K0259	Connaissance des concepts et méthodologies d'analyse des logiciels malveillants.
K0260	Connaissance des normes de sécurité des données relatives aux informations d'identification personnelle (PII).
K0261	Connaissance des normes de sécurité des données de l'industrie des cartes de paiement (PCI).
K0262	Connaissance des normes de sécurité des données relatives aux informations de santé personnelles (PHI).
K0263	Connaissance des politiques, exigences et procédures de gestion des risques liés aux technologies de l'information (TI).
K0264	Connaissance de la planification de la protection des programmes (par exemple, politiques de sécurité/de gestion des risques de la chaîne d'approvisionnement des technologies de l'information (TI), techniques de lutte contre la falsification et exigences).
K0265	Connaissance de l'infrastructure soutenant les technologies de l'information (TI) en matière de sécurité, de performance et de fiabilité.
K0266	Connaissance de la manière d'évaluer la fiabilité du fournisseur et/ou du produit.
K0267	Connaissance des lois, des politiques, des procédures ou de la gouvernance relatives à la cybersécurité des infrastructures critiques.
K0268	Connaissance de l'investigation numérique légale.
K0269	Connaissance de l'architecture des communications mobiles.
K0270	Connaissance du processus de cycle de vie des acquisitions/approvisionnements.
K0271	Connaissance des structures et des éléments internes des systèmes d'exploitation (par exemple, gestion des processus, structure des répertoires, applications installées).
K0272	Connaissance des outils d'analyse de réseau utilisés pour identifier les vulnérabilités des communications logicielles.
K0274	Connaissance des enregistrements de transmission (par exemple : Bluetooth, RFID (Identification par radiofréquence), réseau infrarouge (IR), Wi-Fi (Wireless Fidelity). radiomessagerie, GSM, antennes paraboliques, Voix sur Internet (VoIP)), et des techniques de brouillage qui permettent la transmission d'informations indésirables, ou qui empêchent les systèmes installés de fonctionner correctement.
K0275	Connaissance des techniques de gestion de la configuration.
K0276	Connaissance de la gestion de la sécurité.
K0277	Connaissance des fonctions de chiffrement des données actuelles et émergentes (par exemple, chiffrement des colonnes et des espaces de tables, chiffrement des fichiers et des disques) dans les bases de données (par exemple, fonctions intégrées de gestion des clefs cryptographiques).
K0278	Connaissance des fonctions de remédiation de données actuelles et émergentes dans les bases de données.
K0280	Connaissance des théories, des concepts et des méthodes d'ingénierie des systèmes.
K0281	Connaissance des catalogues de services des technologies de l'information (TI).
K0282	RETIRÉ : intégré dans K0200

ID KSA	Descriptions
K0283	Connaissance des cas pratiques liés à la collaboration et à la synchronisation des contenus entre différentes plates-formes (par exemple : mobile, PC, Cloud).
K0284	Connaissance du développement et de la mise en œuvre d'un système de gestion des informations d'identification des utilisateurs.
K0285	Connaissance de la mise en œuvre de systèmes de séquestre des clefs d'entreprise pour prendre en charge le chiffrement des données au repos.
K0286	Connaissance des typologies à N niveaux (par exemple, comprenant les systèmes d'exploitation serveur et client).
K0287	Connaissance du programme de classification des informations d'une organisation et des procédures de compromission des informations.
K0288	Connaissance des modèles de sécurité standard de l'industrie.
K0289	Connaissance des outils de diagnostic des systèmes/serveurs et des techniques d'identification des défauts.
K0290	Connaissance des méthodes de test et d'évaluation de la sécurité des systèmes.
K0291	Connaissance des concepts et des modèles d'architecture des technologies de l'information (TI) de l'entreprise (par exemple, architecture de référence, architecture validée et architecture cible).
K0292	Connaissance des opérations et des processus de gestion des incidents, des problèmes et des événements.
K0293	Connaissance de l'intégration des buts et objectifs de l'organisation dans l'architecture.
K0294	Connaissance de l'exploitation, de la maintenance et de la sécurité des systèmes informatiques nécessaires au bon fonctionnement des équipements.
K0295	Connaissance des principes de confidentialité, d'intégrité et de disponibilité.
K0296	Connaissance des capacités, des applications et des vulnérabilités potentielles des équipements réseaux, y compris les concentrateurs, les routeurs, les commutateurs, les ponts, les serveurs, les supports de transmission et le matériel connexe.
K0297	Connaissance de la conception de contre-mesures pour les risques de sécurité identifiés.
K0298	Connaissance des contre-mesures pour les risques de sécurité identifiés.
K0299	Connaissance de la détermination du fonctionnement d'un système de sécurité (y compris ses capacités de résilience et de fiabilité) et de la manière dont les modifications des conditions, des opérations ou de l'environnement affecteront ces résultats.
K0300	Connaissance de la cartographie réseau et de la reconstruction de topologies réseau.
K0301	Connaissance de l'analyse de paquets à l'aide d'outils appropriés (par exemple, Wireshark, tcpdump).
K0302	Connaissance du fonctionnement de base des ordinateurs.
K0303	Connaissance de l'utilisation des outils de sous-réseau.
K0304	Connaissance des concepts et des pratiques de traitement des données d'investigation numérique légale.
K0305	Connaissance de la dissimulation de données (par exemple, algorithmes de chiffrement et stéganographie).
K0308	Connaissance de la cryptologie.
K0309	Connaissance des technologies émergentes susceptibles d'être exploitées.
K0310	Connaissance des méthodes de piratage.
K0311	Connaissance des indicateurs industriels utiles pour identifier les tendances technologiques.
K0312	Connaissance des principes, des politiques et des procédures de collecte de renseignements, y compris des autorisations et des restrictions légales.
K0313	Connaissance des organisations externes et des établissements d'enseignement axés sur le domaine cyber (par exemple, programmes d'études/de formation et recherche et développement dans le domaine cyber).

ID KSA	Descriptions
K0314	Connaissance des vulnérabilités potentielles des technologies industrielles en matière de cybersécurité.
K0315	Connaissance des principales méthodes, procédures et techniques de collecte d'informations et de production, de communication et de partage d'informations.
K0316	Connaissance des plans d'opérations commerciaux ou militaires, des plans d'opérations conceptuels, des ordres, des politiques et des règles permanentes d'engagement.
K0317	Connaissance des procédures utilisées pour documenter et consulter les incidents, les problèmes et les événements.
K0318	Connaissance des outils en ligne de commande du système d'exploitation.
K0319	Connaissance des capacités techniques de livraison et de leurs limites.
K0320	Connaissance des critères d'évaluation et de validation de l'organisation.
K0321	Connaissance des concepts d'ingénierie appliqués à l'architecture informatique et au matériel/logiciel informatique correspondant.
K0322	Connaissance des systèmes embarqués.
K0323	Connaissance des méthodologies de tolérance aux pannes des systèmes.
K0324	Connaissance des outils et applications des systèmes de détection d'intrusion (IDS)/systèmes de prévention d'intrusion (IPS).
K0325	Connaissance de la théorie de l'information (par exemple, codage de source, codage de canal, théorie de la complexité des algorithmes et compression de données).
K0326	Connaissance des zones démilitarisées.
K0330	Connaissance des capacités à identifier avec succès les solutions à des problèmes de systèmes moins courants et plus complexes.
K0332	Connaissance des protocoles réseaux tels que TCP/IP, DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System) et services d'annuaire.
K0333	Connaissance des processus de conception de réseaux, y compris la compréhension des objectifs de sécurité, des objectifs opérationnels et des compromis.
K0334	Connaissance de l'analyse du trafic réseau (outils, méthodologies, processus).
K0335	Connaissance des technologies cybers actuelles et émergentes.
K0336	Connaissance des méthodes d'authentification en matière d'accès.
K0337	RETIRÉ : Intégré dans K0007
K0338	Connaissance des techniques d'exploration de données.
K0339	Connaissance de l'utilisation des outils d'analyse de réseau pour identifier les vulnérabilités.
K0341	Connaissance des politiques de divulgation à l'étranger et des réglementations en matière de contrôle des importations/exportations dans le domaine de la cybersécurité.
K0342	Connaissance des principes, outils et techniques de test d'intrusion.
K0343	Connaissance des techniques d'analyse des causes racines.
K0344	Connaissance de l'environnement des menaces d'une organisation.
K0346	Connaissance des principes et méthodes d'intégration des composants d'un système.
K0347	Connaissance et compréhension de la conception opérationnelle.
K0349	Connaissance des types de sites web, de leur administration, de leurs fonctions et des systèmes de gestion de contenu (CMS).
K0350	Connaissance des systèmes de planification organisationnelle reconnus.
K0351	Connaissance des statuts, lois, règlements et politiques applicables en matière de cyberciblage et d'exploitation.
K0352	Connaissance des formes de besoins, des sujets et des domaines d'intérêt en matière de soutien au renseignement.
K0353	Connaissance des circonstances susceptibles d'entraîner une modification des autorités de gestion de la collecte.

ID KSA	Descriptions
K0354	Connaissance des procédures d'établissement de rapports et de diffusion pertinentes.
K0355	Connaissance des procédures d'établissement de rapports et de diffusion de toutes les sources.
K0356	Connaissance des outils et techniques d'analyse du langage, de la voix et/ou du matériel graphique.
K0357	Connaissance des concepts d'analyse et de leur utilisation dans l'évaluation de l'environnement opérationnel.
K0358	Connaissance des normes d'analyse et de l'objectif des niveaux de confiance des renseignements.
K0359	Connaissance des processus approuvés de diffusion des renseignements.
K0361	Connaissance de la disponibilité, des capacités et des limites des moyens.
K0362	Connaissance des méthodes et techniques d'attaque (DDoS, force brute, spoofing, etc.).
K0363	Connaissance des procédures d'audit et de journalisation (y compris la journalisation sur serveur).
K0364	Connaissance des bases de données disponibles et des outils nécessaires pour évaluer les tâches de collecte appropriées.
K0367	Connaissance des tests d'intrusion.
K0368	Connaissance des composants qui permettent les activités de cybercollecte et/ou de préparation.
K0371	Connaissance des principes des processus de développement des collectes (par exemple, reconnaissance des numéros composés, analyse des réseaux sociaux).
K0372	Connaissance des concepts de programmation (par exemple, niveaux, structures, langages compilés ou interprétés).
K0373	Connaissance des applications logicielles de base (par exemple, stockage et sauvegarde des données, applications de base de données) et des types de vulnérabilités qui ont été trouvées dans ces applications.
K0375	Connaissance des vulnérabilités des applications sans fil.
K0376	Connaissance des clients internes et externes et des organisations partenaires, y compris les besoins d'information, les objectifs, la structure, les capacités, etc.
K0377	Connaissance des normes, politiques et procédures de classification et de marquage pour le contrôle.
K0379	Connaissance des organisations clientes, y compris des besoins d'information, des objectifs, de la structure, des capacités, etc.
K0380	Connaissance des outils et des environnements collaboratifs.
K0381	Connaissance des dommages collatéraux et de l'estimation de leur(s) impact(s).
K0382	Connaissance des capacités de collecte et de leurs limites.
K0383	Connaissance des capacités de collecte, des accès, des spécifications de performance et des contraintes utilisées pour satisfaire au plan de collecte.
K0384	Connaissance de la fonctionnalité de la gestion des collectes (par exemple, postes, fonctions, responsabilités, produits, exigences en matière de rapports).
K0385	RETIRÉ : Intégré dans K0142
K0386	Connaissance des outils de gestion des collectes.
K0387	Connaissance du processus de planification des collectes et du plan de collecte.
K0388	Connaissance des techniques et des outils de recherche et d'analyse des collectes pour le chat/la liste d'amis, les technologies émergentes, le VOIP, le Media Over IP, le VPN, le VSAT/sans fil, le web mail et les cookies.
K0389	Connaissance des sources de collecte, y compris les sources conventionnelles et non conventionnelles.
K0390	Connaissance des stratégies de collecte.

ID KSA	Descriptions
K0391	Connaissance des systèmes, capacités et processus de collecte.
K0392	Connaissance des infections courantes des ordinateurs/réseaux (virus, chevaux de Troie, etc.) et des méthodes de contamination (ports, pièces jointes, etc.).
K0393	Connaissance des équipements de réseau courants et de leur configuration.
K0394	Connaissance des bases de données et des outils de reporting courants.
K0395	Connaissance des principes fondamentaux des réseaux informatiques (c'est-à-dire les composants informatiques de base d'un réseau, les types de réseaux, etc.)
K0396	Connaissance des concepts de programmation informatique, y compris les langages informatiques, la programmation, les tests, le débogage et les types de fichiers.
K0397	Connaissance des concepts de sécurité dans les systèmes d'exploitation (par exemple, Linux, Unix).
K0398	Connaissance des concepts liés aux sites web (par exemple : serveurs/pages web, hébergement, DNS, enregistrement, langages web tels que HTML).
K0399	Connaissance des procédures de planification des actions en cas de crise et de planification en fonction des contraintes de temps.
K0400	Connaissance de la planification des actions de crise pour les opérations cybers.
K0401	Connaissance des critères d'évaluation des produits de collecte.
K0402	Connaissance des facteurs de criticité et de vulnérabilité (par exemple, valeur, récupération, amortissement, contre-mesures) pour la sélection des cibles et leur applicabilité au domaine cyber.
K0403	Connaissance des capacités, des limites et des contributions cryptologiques aux opérations cybers.
K0404	Connaissance des exigences en vigueur en matière de collecte.
K0405	Connaissance des intrusions informatiques actuelles.
K0406	Connaissance des logiciels et méthodologies actuels de défense active et de renforcement des systèmes.
K0407	Connaissance des besoins d'information des clients.
K0408	Connaissance des principes, des capacités, des limites et des effets des cyberactions (c'est-à-dire cyberdéfense, collecte d'informations, préparation de l'environnement, cyberattaque).
K0409	Connaissance des capacités et des référentiels de collecte de renseignements/informations sur le cyberespace.
K0410	Connaissance des lois de l'Internet et de leurs effets sur la planification informatique.
K0411	Connaissance des lois de l'informatique et des considérations juridiques et de leurs effets sur la planification informatique.
K0412	Connaissance du lexique et de la terminologie cyber.
K0413	Connaissance des objectifs, des politiques et des aspects juridiques des opérations cybers.
K0414	Connaissance des processus de soutien ou d'habilitation des opérations cybers.
K0415	Connaissance de la terminologie/du lexique des opérations cybers.
K0416	Connaissance des opérations cybers.
K0417	Connaissance de la terminologie des communications de données (par exemple, protocoles réseaux, Ethernet, IP, chiffrement, équipements optiques, supports amovibles).
K0418	Connaissance du processus de flux de données pour la collecte au niveau du terminal ou de l'environnement.
K0419	Connaissance de l'administration et de la maintenance des bases de données.
K0420	Connaissance de la théorie des bases de données.
K0421	Connaissance des bases de données, des portails et des moyens de diffusion associés.
K0422	Connaissance des processus et procédures de résolution de conflits.

ID KSA	Descriptions
K0423	Connaissance des rapports de résolution de conflits, y compris l'interaction avec les organisations extérieures.
K0424	Connaissance des techniques de déni et de tromperie.
K0425	Connaissance des différents objectifs de l'organisation à tous les niveaux, y compris les niveaux inférieurs, latéraux et supérieurs.
K0426	Connaissance du ciblage dynamique et délibéré.
K0427	Connaissance des algorithmes de chiffrement et des capacités/outils cyber (par exemple, SSL, PGP).
K0428	Connaissance des algorithmes et outils de chiffrement pour les réseaux locaux sans fil (WLAN).
K0429	Connaissance de la gestion de l'information à l'échelle de l'entreprise.
K0430	Connaissance des stratégies et techniques d'évasion.
K0431	Connaissance des technologies de communication évolutives/émergentes.
K0432	Connaissance des problématiques actuelles, émergentes et à long terme liées à la stratégie, à la politique et à l'organisation des cyberopérations.
K0433	Connaissance des implications en matière d'investigation numérique légale de la structure et du fonctionnement des systèmes d'exploitation.
K0435	Connaissance des concepts, principes, limites et effets cybers fondamentaux.
K0436	Connaissance des concepts, de la terminologie et du vocabulaire fondamentaux des cyberopérations (par exemple : préparation de l'environnement, cyberattaque, cyberdéfense), des principes, des capacités, des limites et des effets.
K0437	Connaissance des composants généraux des systèmes SCADA (Supervisory control and data acquisition).
K0438	Connaissance de l'architecture des communications cellulaires mobiles (par exemple, LTE, CDMA, GSM/EDGE et UMTS/HSPA).
K0439	Connaissance des autorités compétentes en matière de ciblage.
K0440	Connaissance des produits de sécurité basés sur l'hôte et de la manière dont ces produits affectent l'exploitation et réduisent la vulnérabilité.
K0442	Connaissance de l'impact des technologies convergentes sur les opérations cybers (par exemple, numérique, téléphonie, sans fil).
K0443	Connaissance de la manière dont les concentrateurs, les commutateurs et les routeurs fonctionnent ensemble dans la conception d'un réseau.
K0444	Connaissance du fonctionnement des applications Internet (SMTP,, courrier électronique basé sur le web, clients de chat, VOIP).
K0445	Connaissance de l'impact des réseaux numériques et téléphoniques modernes sur les opérations cybers.
K0446	Connaissance de l'impact des systèmes modernes de communication sans fil sur les opérations cybers.
K0447	Connaissance de la manière de collecter, de visualiser et d'identifier des informations essentielles sur des cibles d'intérêt à partir de métadonnées (par exemple, courrier électronique, http).
K0448	Connaissance de la manière d'établir des priorités en matière de ressources.
K0449	Connaissance de la manière d'extraire, d'analyser et d'utiliser les métadonnées.
K0450	RETIRÉ : Intégré dans K0036
K0451	Connaissance des processus d'identification et d'établissement de rapports.
K0452	Connaissance de la mise en œuvre des systèmes Unix et Windows qui assurent l'authentification et la journalisation du périmètre, le DNS, le courrier électronique, les services web, le serveur FTP, le DHCP, le pare-feu et le SNMP.
K0453	Connaissance des indications et des avertissements.

ID KSA	Descriptions
K0454	Connaissance des besoins d'information.
K0455	Connaissance des concepts de sécurité de l'information, des technologies de facilitation et des méthodes.
K0456	Connaissance des capacités et des limites du renseignement.
K0457	Connaissance des niveaux de confiance en matière de renseignement.
K0458	Connaissance des disciplines du renseignement.
K0459	Connaissance des exigences en matière d'emploi du renseignement (c'est-à-dire logistique, soutien des communications, manœuvrabilité, restrictions légales, etc.)
K0460	Connaissance de la préparation de l'environnement en matière de renseignement et des processus similaires.
K0461	Connaissance des processus de production de renseignements.
K0462	Connaissance des principes, des politiques, des procédures et des véhicules de communication de renseignements, y compris les formats de rapport, les critères de communication (exigences et priorités), les pratiques de diffusion et les autorités et restrictions légales.
K0463	Connaissance des systèmes d'affectation des besoins en matière de renseignement.
K0464	Connaissance du soutien apporté par le renseignement à la planification, à l'exécution et à l'évaluation.
K0465	Connaissance des capacités et des outils des partenaires internes et externes en matière d'opérations cybers.
K0466	Connaissance des processus de renseignement des partenaires internes et externes et de l'élaboration des besoins en informations et des informations essentielles.
K0467	Connaissance des capacités et des limites des organisations partenaires internes et externes (celles qui ont des responsabilités en matière d'attribution des tâches, de collecte, de traitement, d'exploitation et de diffusion).
K0468	Connaissance des rapports des partenaires internes et externes.
K0469	Connaissance des tactiques internes permettant d'anticiper et/ou d'imiter les capacités et les actions des menaces.
K0470	Connaissance d'Internet et des protocoles de routage.
K0471	Connaissance de l'adressage des réseaux Internet (adresses IP, routage interdomaines sans classe, numérotation des ports TCP/UDP).
K0472	Connaissance des systèmes de détection d'intrusion et du développement de signatures.
K0473	Connaissance des intrusions.
K0474	Connaissance des principaux pirates informatiques et de leurs capacités.
K0475	Connaissance des facteurs clefs de l'environnement opérationnel et de la menace.
K0476	Connaissance des outils et techniques de traitement des langues.
K0477	Connaissance de l'intention et des objectifs des dirigeants.
K0478	Connaissance des considérations juridiques en matière de ciblage.
K0479	Connaissance de l'analyse et des caractéristiques des logiciels malveillants.
K0480	Connaissance des logiciels malveillants.
K0481	Connaissance des méthodes et techniques utilisées pour détecter diverses activités d'exploitation.
K0482	Connaissance des méthodes permettant de vérifier la position et la disponibilité des moyens de collecte.
K0483	Connaissance des méthodes d'intégration et de synthèse des informations provenant de toutes les sources potentielles.
K0484	Connaissance de la collecte à mi-parcours (processus, objectifs, organisation, cibles, etc.).
K0485	Connaissance de l'administration de réseaux.

ID KSA	Descriptions
K0486	Connaissance de la construction et de la topologie des réseaux.
K0487	Connaissance de la sécurité des réseaux (par exemple, chiffrement, pare-feu, authentification, pots de miel, protection du périmètre).
K0488	Connaissance des implémentations de la sécurité des réseaux (par exemple, IDS basé sur l'hôte, IPS, listes de contrôle d'accès), y compris leur fonction et leur emplacement dans un réseau.
K0489	Connaissance de la topologie des réseaux.
K0490	RETIRÉ : Intégré dans K0058
K0491	Connaissance des principes fondamentaux des réseaux et des communications Internet (c'est-à-dire les équipements, la configuration des équipements, le matériel, les logiciels, les applications, les ports/protocoles, l'adressage, l'architecture et l'infrastructure du réseau, le routage, les systèmes d'exploitation, etc.)
K0492	Connaissance des méthodes de collecte non traditionnelles.
K0493	Connaissance des techniques d'obscurcissement (par exemple, TOR/Onion/anonymiseurs, VPN/VPS, chiffrement).
K0494	Connaissance des objectifs, de la situation, de l'environnement opérationnel ainsi que de l'état et de la disposition des capacités de collecte des partenaires internes et externes disponibles pour soutenir la planification.
K0495	Connaissance des opérations en cours et futures.
K0496	Connaissance des contraintes liées aux ressources opérationnelles.
K0497	Connaissance de l'évaluation de l'efficacité opérationnelle.
K0498	Connaissance des processus de planification opérationnelle.
K0499	Connaissance de la sécurité des opérations.
K0500	Connaissance des systèmes, des capacités et des processus de collecte de l'organisation et/ou des partenaires (par exemple, processeurs de collecte et de protocole).
K0501	Connaissance des programmes, stratégies et ressources de l'organisation en matière d'opérations cybers.
K0502	Connaissance des outils et/ou méthodes d'aide à la décision de l'organisation.
K0503	Connaissance des formats de l'organisation pour les rapports sur l'état de préparation des ressources et des moyens, de leur pertinence opérationnelle et de leur incidence sur la collecte de renseignements.
K0504	Connaissance des questions, des objectifs et des opérations de l'organisation dans le domaine cyber, ainsi que des règlements et des directives politiques régissant les opérations cybers.
K0505	Connaissance des objectifs de l'organisation et de la demande associée en matière de gestion de la collecte.
K0506	Connaissance des objectifs de l'organisation, des priorités des dirigeants et des risques liés à la prise de décision.
K0507	Connaissance de l'exploitation des réseaux numériques par l'organisation ou ses partenaires.
K0508	Connaissance des politiques de l'organisation et des concepts de planification pour le partenariat avec des organisations internes et/ou externes.
K0509	Connaissance des pouvoirs, des responsabilités et des contributions de l'organisation et des partenaires à la réalisation des objectifs.
K0510	Connaissance des politiques, outils, capacités et procédures de l'organisation et des partenaires.
K0511	Connaissance de la hiérarchie organisationnelle et des processus de décision cybers.
K0512	Connaissance des concepts de planification organisationnelle.
K0513	Connaissance des priorités organisationnelles, des autorités légales et des processus de soumission des exigences.

ID KSA	Descriptions
K0514	Connaissance des structures organisationnelles et des capacités de renseignement associées.
K0516	Connaissance des équipements et de l'infrastructure des réseaux physiques et logiques, y compris les concentrateurs, les commutateurs, les routeurs, les pare-feu, etc.
K0517	Connaissance du processus d'approbation de la revue de post-mise en œuvre (PIR).
K0518	Connaissance de l'initiation des activités de planification.
K0519	Connaissance des délais de planification, de l'adaptation, de l'action de crise et de la planification en fonction des contraintes de temps.
K0520	Connaissance des principes et pratiques liés au développement des cibles, tels que la connaissance des cibles, les associations, les systèmes de communication et l'infrastructure.
K0521	Connaissance des informations prioritaires, de la manière dont elles sont obtenues, des lieux où elles sont publiées, de la manière d'y accéder, etc.
K0522	Connaissance des besoins et des architectures d'exploitation et de diffusion de la production.
K0523	Connaissance des produits et de la nomenclature des principaux fournisseurs (par exemple, suites de sécurité - Trend Micro, Symantec, McAfee, Outpost et Panda) et de la manière dont ces produits affectent l'exploitation et réduisent les vulnérabilités.
K0524	Connaissance des lois, règlements et politiques applicables.
K0525	Connaissance des produits de planification du renseignement qui sont nécessaires à la planification des opérations cybers.
K0526	Connaissance des stratégies de recherche et de la gestion des connaissances.
K0527	Connaissance des stratégies de gestion et d'atténuation des risques.
K0528	Connaissance des systèmes de communication par satellite.
K0529	Connaissance de l'écriture de scripts
K0530	Connaissance des options matérielles et logicielles de sécurité, y compris les artefacts de réseau qu'elles induisent et leurs effets sur l'exploitation.
K0531	Connaissance des impacts des configurations logicielles sur la sécurité.
K0532	Connaissance du langage spécialisé de la cible (par exemple, acronymes, jargon, terminologie technique, mots de code).
K0533	Connaissance des identificateurs de cibles spécifiques et de leur utilisation.
K0534	Connaissance des processus de gestion, d'affectation et de répartition du personnel.
K0535	Connaissance des stratégies et des outils de recherche de cibles.
K0536	Connaissance de la structure, de l'approche et de la stratégie des outils d'exploitation (par exemple : analyseurs réseau, enregistreurs de frappe) et des techniques (par exemple : obtention d'un accès par porte dérobée, collecte/exfiltration de données, analyse de la vulnérabilité d'autres systèmes du réseau).
K0538	Connaissance des structures organisationnelles des cibles et des menaces, des capacités critiques et des vulnérabilités critiques.
K0539	Connaissance des profils de communication des cibles et de leurs éléments clefs (par exemple, associations de cibles, activités, infrastructure de communication).
K0540	Connaissance des outils et techniques de communication avec les cibles.
K0541	Connaissance des références culturelles, des dialectes, des expressions, des idiomes et des abréviations des cibles.
K0542	Connaissance du développement des cibles (c'est-à-dire des concepts, des rôles, des responsabilités, des produits, etc.)
K0543	Connaissance des délais estimés de réparation et de récupération des cibles.
K0544	Connaissance des techniques et des cycles de vie de la collecte de renseignements et de la préparation opérationnelle des objectifs.
K0545	Connaissance de la (des) langue(s) cible(s).
K0546	Connaissance de l'élaboration des listes d'objectifs (c.-à-d. listes restreintes, interarmées, candidates, etc.).

ID KSA	Descriptions
K0547	Connaissance des méthodes et procédures relatives aux cibles.
K0548	Connaissance des procédures et des acteurs informatiques qui sont la cible ou la menace.
K0549	Connaissance des procédures de contrôle et de validation des cibles.
K0550	Connaissance de la cible, y compris des événements d'actualité associés, du profil de communication, des acteurs et de l'histoire (langue, culture) et/ou du cadre de référence.
K0551	Connaissance des cycles de ciblage.
K0552	Connaissance des mécanismes d'attribution des tâches.
K0553	Connaissance des processus d'attribution des tâches pour les moyens de collecte internes et subordonnés.
K0554	Connaissance de l'attribution des tâches, de la collecte, du traitement, de l'exploitation et de la diffusion.
K0555	Connaissance des protocoles de réseau TCP/IP.
K0556	Connaissance des principes fondamentaux des télécommunications.
K0557	Connaissance de la collecte terminale ou environnementale (processus, objectifs, organisation, cibles, etc.).
K0558	Connaissance des outils et applications disponibles associés aux exigences et à la gestion des collectes.
K0559	Connaissance de la structure de base, de l'architecture et de la conception des applications convergentes.
K0560	Connaissance de la structure de base, de l'architecture et de la conception des réseaux de communication modernes.
K0561	Connaissance des bases de la sécurité des réseaux (par exemple, chiffrement, pare-feu, authentification, pots de miel, protection du périmètre).
K0562	Connaissance des capacités et des limites des capacités de collecte, des accès et/ou des processus nouveaux et émergents.
K0563	Connaissance des capacités, des limites et des méthodes d'attribution des tâches des collectes internes et externes dans la mesure où elles s'appliquent aux activités cybers planifiées.
K0564	Connaissance des caractéristiques des réseaux de communication ciblés (par exemple, capacité, fonctionnalité, chemins, nœuds critiques).
K0565	Connaissance des protocoles courants de mise en réseau et de routage (par exemple, TCP/IP), des services (par exemple, web, courrier électronique, DNS) et de la manière dont ils interagissent pour assurer les communications réseau.
K0566	Connaissance des exigences en matière d'informations critiques et de leur utilisation dans la planification.
K0567	Connaissance du flux de données depuis l'origine de la collecte jusqu'aux référentiels et aux outils.
K0568	Connaissance de la définition de la gestion des collectes et de l'autorité de gestion des collectes.
K0569	Connaissance de l'architecture existante en matière de tâches, de collecte, de traitement, d'exploitation et de diffusion.
K0570	Connaissance des facteurs de menace susceptibles d'avoir une incidence sur les opérations de collecte.
K0571	Connaissance du cycle de retour d'information dans les processus de collecte.
K0572	Connaissance des fonctions et des capacités des équipes internes qui simulent les comportements d'une menace au profit de l'organisation.
K0573	Connaissance des principes fondamentaux de l'investigation numérique légale pour extraire des renseignements exploitables.
K0574	Connaissance de l'impact de l'analyse linguistique sur les fonctions des opérateurs on-net.

ID KSA	Descriptions
K0575	Connaissance des incidences des estimations de personnel des partenaires internes et externes.
K0576	Connaissance de l'environnement de l'information.
K0577	Connaissance des cadres, des processus et des systèmes connexes en matière de renseignement.
K0578	Connaissance des processus d'élaboration des besoins en matière de renseignement et de demande d'informations.
K0579	Connaissance de l'organisation, des rôles et des responsabilités des sous-éléments supérieurs, inférieurs et adjacents.
K0580	Connaissance du format établi par l'organisation pour le plan de collecte.
K0581	Connaissance des cycles de planification, d'opérations et de ciblage de l'organisation.
K0582	Connaissance du processus de planification et de dotation en personnel de l'organisation.
K0583	Connaissance des plans, directives et orientations de l'organisation qui décrivent les objectifs.
K0584	Connaissance des politiques/procédures organisationnelles pour le transfert temporaire de l'autorité de collecte.
K0585	Connaissance de la structure organisationnelle en ce qui concerne les opérations cybers à spectre complet, y compris les fonctions, les responsabilités et les interrelations entre les différents éléments internes.
K0586	Connaissance des résultats de l'analyse des plans d'action et des exercices.
K0587	Connaissance des POC, des bases de données, des outils et des applications nécessaires pour établir des produits de préparation et de surveillance de l'environnement.
K0588	Connaissance des besoins prioritaires en matière d'information des niveaux subordonnés, latéraux et supérieurs de l'organisation.
K0589	Connaissance du processus utilisé pour évaluer la performance et l'impact des opérations.
K0590	Connaissance des processus permettant de synchroniser les procédures d'évaluation opérationnelle avec le processus de demande d'informations critiques.
K0591	Connaissance des responsabilités en matière de production et des capacités d'analyse et de production internes.
K0592	Connaissance de l'objectif et de la contribution des modèles d'objectifs.
K0593	Connaissance de l'éventail des opérations cybers et de leurs besoins, sujets et domaines d'intérêt sous-jacents en matière de soutien du renseignement.
K0594	Connaissance des relations entre les états finaux, les objectifs, les effets, les lignes d'opération, etc.
K0595	Connaissance des relations entre les objectifs opérationnels, les besoins en matière de renseignement et les tâches de production de renseignement.
K0596	Connaissance du processus de demande d'informations.
K0597	Connaissance du rôle des opérations en réseau dans le soutien et la facilitation des opérations d'autres organisations.
K0598	Connaissance de la structure et de la finalité des plans, des orientations et des autorisations propres à l'organisation.
K0599	Connaissance de la structure, de l'architecture et de la conception des réseaux numériques et téléphoniques modernes.
K0600	Connaissance de la structure, de l'architecture et de la conception des systèmes modernes de communication sans fil.
K0601	Connaissance des systèmes/architectures/communications utilisés pour la coordination.
K0602	Connaissance des disciplines et des capacités de collecte.
K0603	Connaissance des modes d'utilisation d'Internet par les cibles ou les menaces.
K0604	Connaissance des systèmes ciblés et/ou de ceux qui représentent une menace.

ID KSA	Descriptions
K0605	Connaissance des notions de basculement, de repérage, de mélange et de redondance.
K0606	Connaissance des processus et des techniques d'élaboration des transcriptions (par exemple, verbatim, essentiel, résumés).
K0607	Connaissance des processus et techniques de traduction.
K0608	Connaissance des structures et des éléments internes des systèmes d'exploitation Unix/Linux et Windows (par exemple, gestion des processus, structure des répertoires, applications installées).
K0609	Connaissance des technologies de machines virtuelles.
K0610	Connaissance des produits de virtualisation (VMware, Virtual PC).
K0611	RETIRÉ : Intégré dans K0131
K0612	Connaissance de ce qui constitue une "menace" pour un réseau.
K0613	Connaissance des planificateurs opérationnels de l'organisation, de la manière et du lieu où ils peuvent être contactés, et de leurs attentes.
K0614	Connaissance des technologies sans fil (par exemple, cellulaire, satellite, GSM), y compris la structure, l'architecture et la conception de base des systèmes modernes de communication sans fil.
K0615	Connaissance des déclarations de confidentialité basées sur les lois en vigueur.
K0616	Connaissance de la surveillance continue, de ses processus et des activités du programme de diagnostic et d'atténuation continus (CDM).
K0617	Connaissance des évaluations automatisées des mesures de sécurité.
K0618	Connaissance de la gestion des actifs matériels et de la valeur du suivi de l'emplacement et de la configuration des équipements et des logiciels en réseau dans les départements, les sites, les installations et, potentiellement, les fonctions de soutien de l'entreprise.
K0619	Connaissance de la gestion des actifs logiciels et de la valeur du suivi de l'emplacement et de la configuration des équipements et logiciels en réseau dans les départements, les sites, les installations et, potentiellement, les fonctions de soutien de l'entreprise.
K0620	Connaissance des technologies et des outils de surveillance continue.
K0621	Connaissance de l'évaluation des risques.
K0622	Connaissance des contrôles liés à l'utilisation, au traitement, au stockage et à la transmission des données.
K0623	Connaissance des méthodologies d'évaluation des risques.
K0624	Connaissance des risques liés à la sécurité des applications (par exemple : liste des 10 principaux risques de l'Open Web Application Security Project).
K0625	Connaissance du fait que les correctifs et les mises à jour logicielles ne sont pas pratiques pour certains équipements en réseau.
K0626	Connaissance des mécanismes de mise à jour sécurisés.
K0627	Connaissance de l'importance du filtrage à l'entrée pour se protéger contre les menaces automatisées qui s'appuient sur des adresses réseau usurpées.
K0628	Connaissance des compétitions cybers comme moyen de développer des compétences en fournissant une expérience pratique dans des situations du monde réel simulées.
K0629	Connaissance de la liste blanche/noire.
K0630	Connaissance des dernières techniques et méthodes d'intrusion et des intrusions documentées externes à l'organisation.

A.6 Descriptions des capacités du référentiel NICE

Le tableau 6 fournit une liste des capacités en matière de cybersécurité. Une capacité est une aptitude observable à réaliser un acte psychomoteur appris. Des descriptions de capacités sélectionnées dans cette liste sont incluses pour chaque fonction dans la liste détaillée des fonctions de l'annexe B. Cette liste sera mise à jour régulièrement [1]. La source de référence pour la version la plus récente de ce document est le tableur de référence de la publication spéciale 800-181 du NIST [4].

Tableau 6 – Descriptions des capacités du référentiel NICE

ID KSA	Descriptions
S0001	Capacité à effectuer des analyses de vulnérabilité et à reconnaître les vulnérabilités des systèmes de sécurité.
S0002	Capacité à allouer une capacité de stockage dans la conception des systèmes de gestion des données.
S0003	Capacité à identifier, capturer, contenir et signaler les logiciels malveillants.
S0004	Capacité à analyser les caractéristiques de capacité et de performance du trafic réseau.
S0005	Capacité à appliquer et à intégrer les technologies de l'information dans les solutions proposées.
S0006	Capacité à appliquer les principes de confidentialité, d'intégrité et de disponibilité.
S0007	Capacité à appliquer les contrôles d'accès à l'hôte/au réseau (par exemple, liste de contrôle d'accès).
S0008	Capacité à appliquer les principes et les techniques d'analyse des systèmes propres à l'organisation.
S0009	Capacité à évaluer la robustesse des systèmes de sécurité et de leur conception.
S0010	Capacité à mener une analyse des capacités et des besoins.
S0011	Capacité à effectuer des recherches d'informations.
S0012	Capacité à établir une cartographie des connaissances (par exemple, une carte des référentiels de connaissances).
S0013	Capacité à effectuer des requêtes et à développer des algorithmes pour analyser les structures de données.
S0014	Capacité à déboguer des logiciels.
S0015	Capacité à mener des activités de test.
S0016	Capacité à configurer et à optimiser des logiciels.
S0017	Capacité à créer et à utiliser des modèles mathématiques ou statistiques.
S0018	Capacité à créer des politiques qui reflètent les objectifs de sécurité du système.
S0019	Capacité à créer des programmes qui valident et traitent des entrées multiples, y compris des arguments de ligne de commande, des variables d'environnement et des flux d'entrée.
S0020	Capacité à développer et à déployer des signatures.
S0021	Capacité à concevoir une structure d'analyse des données (c'est-à-dire les types de données qu'un test doit générer et la manière d'analyser ces données).
S0022	Capacité à imaginer des contre-mesures aux risques de sécurité identifiés.
S0023	Capacité à concevoir des mesures de sécurité fondées sur les concepts et les principes de la cybersécurité.
S0024	Capacité à concevoir l'intégration de solutions matérielles et logicielles.
S0025	Capacité à détecter les intrusions au niveau de l'hôte et du réseau au moyen de technologies de détection des intrusions (par exemple, Snort).
S0026	Capacité à déterminer un niveau de rigueur de test approprié pour un système donné.

ID KSA	Descriptions
S0027	Capacité à déterminer comment un système de sécurité devrait fonctionner (y compris ses capacités de résilience et de fiabilité) et comment les changements dans les conditions, les opérations ou l'environnement affecteront ces résultats.
S0028	Capacité à développer des dictionnaires de données.
S0029	Capacité à développer des modèles de données.
S0030	Capacité à développer des scénarios de test basés sur les opérations.
S0031	Capacité à développer et à appliquer des contrôles d'accès aux systèmes de sécurité.
S0032	Capacité à élaborer, tester et mettre en œuvre des plans d'urgence et de reprise pour l'infrastructure du réseau.
S0033	Capacité à diagnostiquer les problèmes de connectivité.
S0034	Capacité à discerner les besoins de protection (c'est-à-dire les mesures de sécurité) des systèmes d'information et des réseaux.
S0035	Capacité à établir un schéma de routage.
S0036	Capacité à évaluer l'adéquation des conceptions de sécurité.
S0037	Capacité à générer des requêtes et des rapports.
S0038	Capacité à identifier les mesures ou les indicateurs de performance des systèmes et les actions nécessaires pour améliorer ou corriger la performance, par rapport aux objectifs du système.
S0039	Capacité à identifier les causes possibles de la dégradation des performances ou de la disponibilité des systèmes et à lancer les actions nécessaires pour atténuer cette dégradation.
S0040	Capacité à mettre en œuvre, à maintenir et à améliorer les pratiques établies en matière de sécurité des réseaux.
S0041	Capacité à installer, configurer et dépanner les composants des réseaux locaux et étendus tels que les routeurs, les concentrateurs et les commutateurs.
S0042	Capacité à maintenir des bases de données. (c'est-à-dire sauvegarde, restauration, suppression de données, fichiers journaux de transactions, etc.)
S0043	Capacité à assurer la maintenance des services d'annuaire. (par exemple, Microsoft Active Directory, LDAP, etc.).
S0044	Capacité à imiter les comportements des menaces.
S0045	Capacité à optimiser les performances des bases de données.
S0046	Capacité à effectuer des analyses au niveau des paquets à l'aide d'outils appropriés (par exemple, Wireshark, tcpdump).
S0047	Capacité à préserver l'intégrité des éléments de preuve conformément aux procédures opérationnelles standard ou aux normes nationales.
S0048	Capacité à tester l'intégration des systèmes.
S0049	Capacité à mesurer le capital intellectuel et à en rendre compte.
S0050	Capacité à modéliser la conception et à élaborer des cas d'utilisation (par exemple, langage de modélisation unifié).
S0051	Capacité à utiliser des outils et des techniques de test d'intrusion.
S0052	Capacité à utiliser des techniques d'ingénierie sociale (par exemple, phishing, baiting, tailgating, etc.).
S0053	Capacité à régler les capteurs.
S0054	Capacité à utiliser des méthodologies de traitement des incidents.
S0055	Capacité à utiliser les technologies de gestion des connaissances.
S0056	Capacité à utiliser des outils de gestion de réseau pour analyser les schémas de trafic du réseau (par exemple, le protocole simple de gestion de réseau).
S0057	Capacité à utiliser des analyseurs de protocole.

ID KSA	Descriptions
S0058	Capacité à utiliser les outils appropriés pour réparer les logiciels, le matériel et les équipements périphériques d'un système.
S0059	Capacité à utiliser les équipements de réseaux privés virtuels (VPN) et le chiffrement.
S0060	Capacité à écrire du code dans un langage de programmation courant (par exemple, Java, C++).
S0061	Capacité à rédiger des plans de test.
S0062	Capacité à analyser des dumps de mémoire pour en extraire des informations.
S0063	Capacité à collecter des données à partir de diverses ressources de cybersécurité.
S0064	Capacité à élaborer et à exécuter des programmes de formation technique et des programmes d'études.
S0065	Capacité à identifier et à extraire des données d'intérêt judiciaire dans divers médias (c'est-à-dire investigation numérique légale).
S0066	Capacité à identifier les lacunes dans les capacités techniques.
S0067	Capacité à identifier, modifier et manipuler les composants de systèmes sous Windows, Unix ou Linux (par exemple, mots de passe, comptes d'utilisateurs, fichiers).
S0068	Capacité à collecter, traiter, emballer, transporter et stocker des preuves électroniques afin d'éviter l'altération, la perte, les dommages physiques ou la destruction des données.
S0069	Capacité à mettre en place un poste de travail d'investigation numérique légale.
S0070	Capacité à s'adresser à d'autres personnes pour leur transmettre des informations de manière efficace.
S0071	Capacité à utiliser des suites d'outils d'investigation numérique légale (par exemple, EnCase, Sleuthkit, FTK).
S0072	Capacité à utiliser des règles et des méthodes scientifiques pour résoudre des problèmes.
S0073	Capacité à utiliser des machines virtuelles. (par exemple, Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, etc.)
S0074	Capacité à démonter physiquement des ordinateurs personnels.
S0075	Capacité à mener des investigations numériques légales dans plusieurs environnements de systèmes d'exploitation (par exemple, systèmes d'appareils mobiles).
S0076	Capacité à configurer et à utiliser des outils de protection informatique basés sur des logiciels (par exemple, des pare-feu logiciels, des logiciels antivirus, des logiciels anti-espions).
S0077	Capacité à sécuriser les communications réseau.
S0078	Capacité à reconnaître et à catégoriser les types de vulnérabilités et les attaques associées.
S0079	Capacité à protéger un réseau contre les logiciels malveillants. (par exemple, NIPS, anti-malware, restreindre/empêcher les équipements externes, filtres anti-spam).
S0080	Capacité à évaluer les dommages.
S0081	Capacité à utiliser des outils d'analyse réseau pour identifier les vulnérabilités. (par exemple, fuzzing, nmap, etc.).
S0082	Capacité à évaluer l'applicabilité et l'exhaustivité des plans de test.
S0083	Capacité à intégrer des outils de test de sécurité de type "boîte noire" dans le processus d'assurance qualité des versions logicielles.
S0084	Capacité à configurer et à utiliser des composants de protection de réseau (par exemple, pare-feu, VPN, systèmes de détection d'intrusion dans le réseau).
S0085	Capacité à mener des audits ou des examens de systèmes techniques.
S0086	Capacité à évaluer la fiabilité du fournisseur et/ou du produit.
S0087	Capacité à analyser en profondeur les codes malveillants capturés (par exemple, investigation numérique légale des logiciels malveillants).
S0088	Capacité à utiliser des outils d'analyse binaire (par exemple, Hexedit, command code xxd, hexdump).

ID KSA	Descriptions
S0089	Capacité à utiliser des fonctions de hachage à sens unique (par exemple, Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).
S0090	Capacité à analyser un code anormal comme étant malveillant ou bénin.
S0091	Capacité à analyser des données volatiles.
S0092	Capacité à identifier les techniques d'obscurcissement.
S0093	Capacité à interpréter les résultats du débogueur pour en déduire les tactiques, les techniques et les procédures.
S0094	Capacité à lire des données hexadécimales.
S0095	Capacité à identifier les techniques d'encodage courantes (par exemple, disjonction exclusive [XOR], ASCII (American Standard Code for Information Interchange), Unicode, Base64, Uuencode, encodage URL (Uniform Resource Locator)).
S0096	Capacité à lire et à interpréter des signatures (par exemple, snort).
S0097	Capacité à appliquer des mesures de sécurité.
S0100	Capacité à utiliser ou à développer des activités d'apprentissage (par exemple, des scénarios, des jeux pédagogiques, des exercices interactifs).
S0101	Capacité à utiliser les technologies (p. ex. SmartBoards, sites web, ordinateurs, projecteurs) à des fins pédagogiques.
S0102	Capacité à mettre en œuvre des capacités techniques de diffusion.
S0103	Capacité à évaluer le pouvoir prédictif et la généralisation ultérieure d'un modèle.
S0104	Capacité à mener des revues de préparation aux tests.
S0106	Capacité à prétraiter les données (par exemple, imputation, réduction de la dimensionnalité, normalisation, transformation, extraction, filtrage, lissage).
S0107	Capacité à concevoir et à documenter des stratégies globales de test et d'évaluation de programmes.
S0108	Capacité à élaborer des normes de qualification de la main-d'œuvre et des postes.
S0109	Capacité à identifier des modèles ou des relations cachés.
S0110	Capacité à identifier les exigences en matière d'infrastructure de test et d'évaluation (personnes, gammes, outils, instruments).
S0111	Capacité à assurer l'interface avec les clients.
S0112	Capacité à gérer les moyens, les ressources et le personnel d'essai afin d'assurer la réalisation efficace des opérations de test.
S0113	Capacité à effectuer des conversions de format pour créer une représentation standard des données.
S0114	Capacité à effectuer des analyses de sensibilité.
S0115	Capacité à préparer des rapports de test et d'évaluation.
S0116	Capacité à concevoir des solutions de sécurité multi-niveaux/interdomaines.
S0117	Capacité à fournir une estimation des ressources pour le test et l'évaluation.
S0118	Capacité à développer des ontologies sémantiques compréhensibles par la machine.
S0119	Capacité à effectuer des analyses de régression (par exemple, modèle hiérarchique par étapes, modèle linéaire généralisé, moindres carrés ordinaires, méthodes basées sur les arbres, logistiques).
S0120	Capacité à examiner les journaux afin d'identifier les preuves d'intrusions passées.
S0121	Capacité à appliquer des techniques de renforcement du système, du réseau et du système d'exploitation. (par exemple, suppression des services inutiles, politiques de mots de passe, segmentation du réseau, activation de la journalisation, moindre privilège, etc.)
S0122	Capacité à utiliser des méthodes de conception.
S0123	Capacité à effectuer des analyses de transformation (par exemple, agrégation, enrichissement, traitement).

ID KSA	Descriptions
S0124	Capacité à dépanner et à diagnostiquer les anomalies de l'infrastructure de cybersécurité et à les résoudre.
S0125	Capacité à utiliser des statistiques et des techniques descriptives de base (par exemple, normalité, distribution des modèles, diagrammes de dispersion).
S0126	Capacité à utiliser des outils d'analyse de données (par exemple, Excel, STATA SAS, SPSS).
S0127	Capacité à utiliser des outils de cartographie des données.
S0128	Capacité à utiliser les systèmes informatiques relatifs à la main-d'œuvre et au personnel.
S0129	Capacité à utiliser des techniques d'identification et de suppression des valeurs aberrantes.
S0130	Capacité à rédiger des scripts à l'aide de R, Python, PIG, HIVE, SQL, etc.
S0131	Capacité à analyser les logiciels malveillants.
S0132	Capacité à effectuer des analyses au niveau binaire.
S0133	Capacité à traiter les preuves numériques, y compris à les protéger et à en faire des copies légalement valables.
S0134	Capacité à mener des examens de systèmes.
S0135	Capacité à concevoir des plans de test sécurisés (par exemple, unité, intégration, système, acceptation).
S0136	Capacité à gérer les principes, modèles, méthodes (par exemple, contrôle des performances des systèmes de bout en bout) et outils de gestion des systèmes de réseau.
S0137	Capacité à mener des évaluations de la vulnérabilité des applications.
S0138	Capacité à utiliser les capacités de chiffrement et de signature numérique de l'infrastructure à clef publique (PKI) dans les applications (par exemple, courrier électronique S/MIME, trafic SSL).
S0139	Capacité à appliquer des modèles de sécurité (par exemple, le modèle Bell-LaPadula, le modèle d'intégrité Biba, le modèle d'intégrité Clark-Wilson).
S0140	Capacité à appliquer le processus d'ingénierie des systèmes.
S0141	Capacité à évaluer la conception des systèmes de sécurité.
S0142	Capacité à mener des recherches pour résoudre des problèmes inédits au niveau des clients.
S0143	Capacité à assurer la planification, la gestion et la maintenance des systèmes/serveurs.
S0144	Capacité à corriger les problèmes physiques et techniques ayant une incidence sur les performances du système/serveur.
S0145	Capacité à intégrer et à appliquer des politiques qui répondent aux objectifs de sécurité des systèmes.
S0146	Capacité à créer des politiques permettant aux systèmes d'atteindre les objectifs de performance (par exemple, routage du trafic, accords de niveau de service, spécifications de l'unité centrale).
S0147	Capacité à évaluer les mesures de sécurité sur la base des concepts et des principes de la cybersécurité. (par exemple, CIS CSC, NIST SP 800-53, Cybersecurity Framework, etc.)
S0148	Capacité à concevoir l'intégration de processus et de solutions technologiques, y compris les systèmes existants et les langages de programmation modernes.
S0149	Capacité à développer des applications capables d'enregistrer et de traiter les erreurs, les exceptions, les défaillances des applications et la journalisation.
S0150	Capacité à mettre en œuvre et à tester des plans d'urgence et de reprise pour l'infrastructure du réseau.
S0151	Capacité à dépanner les composants de systèmes défaillants (par exemple, les serveurs).
S0152	Capacité à traduire les exigences opérationnelles en besoins de protection (c'est-à-dire en mesures de sécurité).
S0153	Capacité à identifier et à anticiper les problèmes de performance, de disponibilité, de capacité ou de configuration des systèmes/serveurs.

ID KSA	Descriptions
S0154	Capacité à installer des mises à niveau de systèmes et de composants. (c.-à-d., serveurs, appareils, équipements de réseau).
S0155	Capacité à surveiller et à optimiser les performances des systèmes/serveurs.
S0156	Capacité à effectuer des analyses au niveau des paquets.
S0157	Capacité à récupérer les systèmes/serveurs défaillants. (par exemple, logiciel de récupération, grappes de basculement, réplication, etc.)
S0158	Capacité à administrer les systèmes d'exploitation. (par exemple, maintenance des comptes, sauvegardes de données, maintien des performances du système, installation et configuration de nouveaux matériels/logiciels).
S0159	Capacité à configurer et à valider les postes de travail en réseau et les périphériques conformément aux normes et/ou spécifications approuvées.
S0160	Capacité à utiliser la modélisation de la conception (par exemple, le langage de modélisation unifié).
S0161	RETIRÉ : Intégré dans le cours S0160
S0162	Capacité à appliquer diverses techniques de sous-réseau (par exemple, CIDR).
S0163	RETIRÉ : Intégré dans S0060
S0164	Capacité à évaluer l'application des normes cryptographiques.
S0166	Capacité à identifier les lacunes dans les capacités techniques d'exécution.
S0167	Capacité à reconnaître les vulnérabilités des systèmes de sécurité. (par exemple, analyse de la vulnérabilité et de la conformité).
S0168	Capacité à mettre en place des sous-réseaux physiques ou logiques qui séparent un réseau local interne (LAN) d'autres réseaux non fiables.
S0169	Capacité à effectuer des analyses de tendances.
S0170	Capacité à configurer et à utiliser les composants de protection informatique (par exemple, les pare-feu matériels, les serveurs, les routeurs, le cas échéant).
S0171	Capacité à effectuer des évaluations d'impact/de risque.
S0172	Capacité à appliquer des techniques de codage sécurisé.
S0173	Capacité à utiliser des outils de corrélation d'événements de sécurité.
S0174	Capacité à utiliser des outils d'analyse de code.
S0175	Capacité à effectuer une analyse des causes profondes.
S0176	Capacité à mener des activités de planification administrative, y compris la préparation de plans de soutien fonctionnels et spécifiques, la préparation et la gestion de la correspondance et les procédures de dotation en personnel.
S0177	Capacité à analyser les réseaux de communication d'une cible.
S0178	Capacité à analyser les données essentielles d'un réseau (par exemple, les fichiers de configuration des routeurs, les protocoles de routage).
S0179	Capacité à analyser les outils de traitement du langage afin de fournir un retour d'information pour améliorer le développement des outils.
S0180	RETIRÉ : Intégré dans le cours S0062
S0181	Capacité à analyser les données de collecte des points médians.
S0182	Capacité à analyser les communications internes et externes de la cible collectées à partir de réseaux locaux sans fil.
S0183	Capacité à analyser les données de collecte de terminaux ou d'environnements.
S0184	Capacité à analyser le trafic pour identifier les équipements réseaux.
S0185	Capacité à appliquer les méthodes analytiques généralement utilisées pour soutenir la planification et justifier les stratégies et les plans d'action recommandés.
S0186	Capacité à appliquer les procédures de planification de crise.

ID KSA	Descriptions
S0187	Capacité à appliquer diverses méthodes, outils et techniques d'analyse (par exemple, hypothèses concurrentes, chaîne de raisonnement, méthodes des scénarios, détection du déni et de la tromperie, impact élevé/faible probabilité, analyse des réseaux/associations ou des liens, analyse bayésienne, analyse Delphi et analyse des schémas).
S0188	Capacité à évaluer le cadre de référence d'une cible (par exemple, motivation, capacité technique, structure organisationnelle, sensibilités).
S0189	Capacité à évaluer et/ou à estimer les effets générés pendant et après les opérations cybers.
S0190	Capacité à évaluer les outils actuels afin d'identifier les améliorations nécessaires.
S0191	Capacité à évaluer l'applicabilité des outils d'analyse disponibles à diverses situations.
S0192	Capacité à auditer les pare-feu, les périmètres, les routeurs et les systèmes de détection d'intrusion.
S0193	Capacité à respecter les restrictions légales en matière d'informations ciblées.
S0194	Capacité à mener des recherches non attribuables.
S0195	Capacité à mener des recherches en utilisant toutes les sources disponibles.
S0196	Capacité à mener des recherches en utilisant le deep web.
S0197	Capacité à effectuer des analyses de réseaux sociaux, des analyses de listes d'amis et/ou des analyses de cookies.
S0198	Capacité à effectuer une analyse de réseau social.
S0199	Capacité à créer et à extraire des informations importantes à partir de captures de paquets.
S0200	Capacité à créer des exigences de collecte à l'appui des activités d'acquisition de données.
S0201	Capacité à créer des plans à l'appui d'opérations à distance. (par exemple, sites chauds/chauds/froids/alternatifs, reprise après sinistre).
S0202	Capacité à utiliser des techniques d'exploration de données (par exemple, recherche dans les systèmes de fichiers) et d'analyse.
S0203	Capacité à définir et à caractériser tous les aspects pertinents de l'environnement opérationnel.
S0204	Capacité à représenter les données sources ou collatérales sur une carte de réseau.
S0205	Capacité à déterminer les options de ciblage appropriées en évaluant les capacités disponibles par rapport aux effets souhaités.
S0206	Capacité à déterminer les correctifs installés sur divers systèmes d'exploitation et à identifier les signatures de correctifs.
S0207	Capacité à déterminer l'effet de diverses configurations de routeurs et de pare-feu sur les schémas de trafic et les performances du réseau dans les environnements LAN et WAN.
S0208	Capacité à déterminer l'emplacement physique des équipements de réseau.
S0209	Capacité à élaborer et à exécuter des programmes complets d'évaluation des opérations cybers pour évaluer et valider les caractéristiques de performance opérationnelle.
S0210	Capacité à élaborer des rapports de renseignement.
S0211	Capacité à élaborer ou à recommander des approches analytiques ou des solutions à des problèmes et à des situations pour lesquels les informations sont incomplètes ou pour lesquels il n'existe pas de précédent.
S0212	Capacité à diffuser en temps utile des éléments de la plus haute valeur en matière de renseignement.
S0213	Capacité à documenter et à communiquer des informations techniques et programmatiques complexes.
S0214	Capacité à évaluer les accès en fonction de leur valeur en termes de renseignement.
S0215	Capacité à évaluer et à interpréter les métadonnées.
S0216	Capacité à évaluer les capacités disponibles par rapport aux effets souhaités afin de proposer des plans d'action efficaces.

ID KSA	Descriptions
S0217	Capacité à évaluer les sources de données en termes de pertinence, de fiabilité et d'objectivité.
S0218	Capacité à évaluer les informations en termes de fiabilité, de validité et de pertinence.
S0219	Capacité à évaluer les informations pour en reconnaître la pertinence, la priorité, etc.
S0220	Capacité à exploiter/interroger les bases de données de l'organisation et/ou des partenaires.
S0221	Capacité à extraire des informations à partir de captures de paquets.
S0222	Capacité à analyser des fusions.
S0223	Capacité à élaborer des plans d'opération à l'appui des exigences de la mission et de la cible.
S0224	Capacité à répertorier les communications d'une cible.
S0225	Capacité à identifier les réseaux de communication d'une cible.
S0226	Capacité à identifier les caractéristiques du réseau d'une cible.
S0227	Capacité à identifier d'autres interprétations analytiques afin de minimiser les résultats imprévus.
S0228	Capacité à identifier les éléments critiques d'une cible, y compris les éléments critiques dans le domaine cyber.
S0229	Capacité à identifier les cybermenaces susceptibles de mettre en péril les intérêts de l'organisation et/ou de ses partenaires.
S0230	RETIRÉ : Intégré dans S0066
S0231	Capacité à identifier les modes de communication d'une cible.
S0232	Capacité à identifier les lacunes et les limites du renseignement.
S0233	Capacité à identifier les questions linguistiques qui peuvent avoir un impact sur les objectifs de l'organisation.
S0234	Capacité à identifier des pistes pour le développement des cibles.
S0235	Capacité à identifier les langues et dialectes régionaux non ciblés.
S0236	Capacité à identifier les équipements qui fonctionnent à chaque niveau des modèles de protocole.
S0237	Capacité à identifier, localiser et suivre des cibles au moyen de techniques d'analyse géospatiale.
S0238	Capacité à hiérarchiser les informations dans le cadre des opérations.
S0239	Capacité à interpréter les langages de programmation compilés et interprétatifs.
S0240	Capacité à interpréter les métadonnées et le contenu tels qu'ils sont appliqués par les systèmes de collecte.
S0241	Capacité à interpréter les résultats de traceroute, dans la mesure où ils s'appliquent à l'analyse et à la reconstruction de réseaux.
S0242	Capacité à interpréter les résultats des scanners de vulnérabilité afin d'identifier les vulnérabilités.
S0243	Capacité à gérer les connaissances, y compris les techniques de documentation technique (par exemple, page Wiki).
S0244	Capacité à gérer les relations avec les clients, notamment à déterminer leurs besoins/exigences, à gérer leurs attentes et à démontrer leur engagement à fournir des résultats de qualité.
S0245	Capacité à naviguer dans des logiciels de visualisation de réseaux.
S0246	Capacité à normaliser les nombres.
S0247	Capacité à fusionner des données provenant de renseignements existants pour permettre une collecte nouvelle et continue.
S0248	Capacité à effectuer des analyses de systèmes cibles.
S0249	Capacité à préparer et à présenter des briefings.

ID KSA	Descriptions
S0250	Capacité à préparer des plans et la correspondance correspondante.
S0251	Capacité à hiérarchiser les documents en langue cible.
S0252	Capacité à traiter les données collectées en vue d'une analyse ultérieure.
S0253	Capacité à fournir une analyse sur des questions liées à la cible (par exemple, langue, culture, communications).
S0254	Capacité à fournir des analyses pour faciliter la rédaction de rapports après action par étapes.
S0255	Capacité à fournir des informations géolocalisées en temps réel et exploitables, en utilisant les infrastructures de la cible.
S0256	Capacité à comprendre les systèmes cibles ou menaçants par l'identification et l'analyse des liens physiques, fonctionnels ou comportementaux.
S0257	Capacité à lire, interpréter, écrire, modifier et exécuter des scripts simples (par exemple, PERL, VBS) sur des systèmes Windows et Unix (par exemple, ceux qui exécutent des tâches telles que l'analyse de fichiers de données volumineux, l'automatisation de tâches manuelles et l'extraction/le traitement de données à distance).
S0258	Capacité à reconnaître et à interpréter les activités de réseau malveillantes dans le trafic.
S0259	Capacité à reconnaître les techniques de déni et de tromperie de la cible.
S0260	Capacité à reconnaître les opportunités à mi-parcours et les informations essentielles.
S0261	Capacité à reconnaître la pertinence des informations.
S0262	Capacité à reconnaître les changements significatifs dans les modes de communication d'une cible.
S0263	Capacité à reconnaître les informations techniques qui peuvent servir de pistes pour l'analyse des métadonnées.
S0264	Capacité à reconnaître les informations techniques qui peuvent être utilisées comme pistes pour permettre des opérations à distance (les données comprennent les utilisateurs, les mots de passe, les adresses électroniques, les plages IP de la cible, la fréquence du comportement DNI, les serveurs de messagerie, les serveurs de domaine, les informations d'en-tête SMTP).
S0265	Capacité à reconnaître les informations techniques susceptibles d'être utilisées pour le développement de cibles, y compris le développement de renseignements.
S0266	Capacité à utiliser les langages de programmation appropriés (par exemple, C++, Python, etc.).
S0267	Capacité à utiliser la ligne de commande à distance et les outils de l'interface utilisateur graphique (GUI).
S0268	Capacité à rechercher des informations essentielles.
S0269	Capacité à rechercher des vulnérabilités et des exploits utilisés dans le trafic.
S0270	Capacité à faire de la rétro-ingénierie (par exemple, édition hexadécimale, utilitaires d'empaquetage binaire, débogage et analyse des chaînes de caractères) afin d'identifier la fonction et la propriété des outils distants.
S0271	Capacité à examiner et à modifier des produits d'évaluation.
S0272	Capacité à examiner et à modifier les produits de renseignement provenant de diverses sources pour les opérations cybers.
S0273	Capacité à examiner et à modifier des plans.
S0274	Capacité à examiner et à modifier les documents cibles.
S0275	Capacité à administrer des serveurs.
S0276	Capacité à étudier, collecter et analyser les métadonnées des réseaux locaux sans fil.
S0277	Capacité à synthétiser, analyser et hiérarchiser le sens des ensembles de données.
S0278	Capacité à adapter l'analyse aux niveaux nécessaires (par exemple, classification et organisation).

ID KSA	Descriptions
S0279	Capacité à développer des cibles en soutien direct des opérations de collecte.
S0280	Capacité à identifier les anomalies dans les réseaux cibles (par exemple, intrusions, flux ou traitement de données, mise en œuvre de nouvelles technologies par les cibles).
S0281	Capacité à rédiger des documents techniques.
S0282	Capacité à tester et à évaluer des outils en vue de leur mise en œuvre.
S0283	Capacité à transcrire des communications dans la langue cible.
S0284	Capacité à traduire des documents graphiques et/ou vocaux en langue cible.
S0285	Capacité à utiliser des opérateurs booléens pour construire des requêtes simples et complexes.
S0286	Capacité à utiliser des bases de données pour identifier les informations pertinentes pour la cible.
S0287	Capacité à utiliser des données géospatiales et à appliquer des ressources géospatiales.
S0288	Capacité à utiliser plusieurs outils, bases de données et techniques d'analyse (par exemple, Analyst's Notebook, A-Space, Anchory, M3, pensée divergente/convergente, diagrammes de liens, matrices, etc.)
S0289	Capacité à utiliser plusieurs moteurs de recherche (par exemple, Google, Yahoo, LexisNexis, DataStar) et des outils permettant d'effectuer des recherches dans des sources ouvertes.
S0290	Capacité à utiliser des réseaux non attribuables.
S0291	Capacité à utiliser des méthodes de recherche incluant des sources multiples et différentes pour reconstituer un réseau cible.
S0292	Capacité à utiliser des bases de données et des logiciels de ciblage.
S0293	Capacité à utiliser des outils, des techniques et des procédures pour exploiter à distance et établir une persistance sur une cible.
S0294	Capacité à utiliser des outils de traçage et à interpréter les résultats dans le cadre de l'analyse et de la reconstitution d'un réseau.
S0295	Capacité à utiliser divers outils de collecte de données open source (commerce en ligne, DNS, courrier électronique, etc.).
S0296	Capacité à utiliser le retour d'information pour améliorer les processus, les produits et les services.
S0297	Capacité à utiliser des espaces de travail et/ou des outils de collaboration en ligne (par exemple, IWS, VTC, salons de discussion, SharePoint).
S0298	Capacité à vérifier l'intégrité de tous les fichiers. (par exemple, sommes de contrôle, OU exclusif, hachages sécurisés, contraintes de contrôle, etc.)
S0299	Capacité à analyser les cibles des réseaux sans fil, à les modéliser et à les géolocaliser.
S0300	Capacité à rédiger (et à soumettre) des exigences visant à combler les lacunes en matière de capacités techniques.
S0301	Capacité à rédiger des faits et des idées de manière claire, convaincante et organisée.
S0302	Capacité à rédiger des rapports d'efficacité.
S0303	Capacité à rédiger, examiner et modifier des produits de renseignement/d'évaluation liés à la cybersécurité et provenant de sources multiples.
S0304	Capacité à accéder aux informations sur les moyens actuellement disponibles et sur leur utilisation.
S0305	Capacité à accéder aux bases de données où sont conservés les plans, les directives et les orientations.
S0306	Capacité à analyser les orientations stratégiques pour y déceler les questions nécessitant une clarification et/ou des orientations supplémentaires.
S0307	Capacité à analyser les forces et la motivation de la cible ou de la menace.
S0308	Capacité à anticiper les besoins des services de renseignement en matière d'emploi.

ID KSA	Descriptions
S0309	Capacité à anticiper les activités clefs de l'objectif ou de la menace susceptibles d'entraîner une décision de la part des dirigeants.
S0310	Capacité à appliquer des normes analytiques pour évaluer les produits du renseignement.
S0311	Capacité à appliquer les capacités, les limites et les méthodes d'affectation des plates-formes, des capteurs, des architectures et des appareils disponibles en fonction des objectifs de l'organisation.
S0312	Capacité à appliquer le processus utilisé pour évaluer la performance et l'impact des opérations cybers.
S0313	Capacité à formuler un énoncé des besoins et à intégrer des capacités de collecte, des accès et/ou des processus nouveaux et émergents dans les opérations de collecte.
S0314	Capacité à définir les capacités de renseignement disponibles pour soutenir l'exécution du plan.
S0315	Capacité à formuler les besoins des planificateurs interarmées à l'intention des analystes de toutes les sources.
S0316	Capacité à associer les lacunes en matière de renseignement aux exigences prioritaires en matière d'information et aux éléments observables.
S0317	Capacité à comparer les indicateurs/observables avec les besoins.
S0318	Capacité à conceptualiser l'ensemble du processus de renseignement dans les multiples domaines et dimensions.
S0319	Capacité à convertir les exigences en matière de renseignement en tâches de production de renseignements.
S0320	Capacité à coordonner l'élaboration de produits de renseignement sur mesure.
S0321	Capacité à établir une corrélation entre les priorités en matière de renseignement et l'affectation des ressources/ressources en matière de renseignement.
S0322	Capacité à élaborer des indicateurs de progrès/de réussite opérationnelle.
S0323	Capacité à créer et à tenir à jour des documents de planification et à assurer le suivi des services/productions.
S0324	Capacité à déterminer la faisabilité de la collecte.
S0325	Capacité à élaborer un plan de collecte qui montre clairement la discipline pouvant être utilisée pour collecter les informations nécessaires.
S0326	Capacité à faire la distinction entre les ressources théoriques et réelles et leur applicabilité au plan en cours d'élaboration.
S0327	Capacité à s'assurer que la stratégie de collecte exploite toutes les ressources disponibles.
S0328	Capacité à évaluer les facteurs liés à l'environnement opérationnel, aux objectifs et aux besoins en informations.
S0329	Capacité à évaluer les demandes d'informations afin de déterminer s'il existe des réponses.
S0330	Capacité à évaluer les capacités, les limites et les méthodes d'attribution des tâches des capacités de collecte internes, de théâtre d'opération, nationales, de coalition et autres.
S0331	Capacité à exprimer oralement et par écrit la relation entre les limites des capacités de renseignement et les risques liés à la prise de décision, ainsi que les incidences sur l'ensemble de l'opération.
S0332	Capacité à extraire des informations des outils et applications disponibles associés aux exigences en matière de collecte et à la gestion des opérations de collecte.
S0333	Capacité à représenter graphiquement des documents d'aide à la décision contenant des estimations des capacités des services de renseignement et des partenaires.
S0334	Capacité à identifier et à appliquer aux disciplines concernées l'attribution des tâches, la collecte, le traitement, l'exploitation et la diffusion des informations.
S0335	Capacité à identifier les lacunes en matière de renseignement.

ID KSA	Descriptions
S0336	Capacité à déterminer quand les besoins prioritaires en matière d'information sont satisfaits.
S0337	Capacité à mettre en œuvre les procédures établies pour évaluer les activités de gestion et d'exploitation de la collecte.
S0338	Capacité à interpréter les orientations en matière de planification afin de déterminer le niveau de soutien analytique requis.
S0339	Capacité à interpréter les rapports sur l'état de préparation, leur pertinence opérationnelle et leur incidence sur la collecte de renseignements.
S0340	Capacité à surveiller la situation de la cible ou de la menace et les facteurs environnementaux.
S0341	Capacité à surveiller les effets de la menace sur les capacités des partenaires et à maintenir une estimation courante.
S0342	Capacité à optimiser les performances des systèmes de collecte par des ajustements, des essais et des réajustements répétés.
S0343	Capacité à organiser des équipes de planification du renseignement, à coordonner la collecte et le soutien à la production, et à contrôler l'état d'avancement.
S0344	Capacité à préparer et à présenter des rapports, des exposés et des séances d'information, y compris en utilisant des aides visuelles ou des techniques de présentation.
S0345	Capacité à établir un lien entre les ressources/actifs de renseignement et les besoins anticipés en matière de renseignement.
S0346	Capacité à résoudre les conflits d'exigences en matière de collecte.
S0347	Capacité à examiner les spécifications de performance et les informations historiques concernant les moyens de collecte.
S0348	Capacité à spécifier les collectes et/ou les missions qui doivent être menées à court terme.
S0349	Capacité à synchroniser les procédures d'évaluation opérationnelle avec le processus des besoins en informations critiques.
S0350	Capacité à synchroniser les activités de planification et le soutien requis en matière de renseignement.
S0351	Capacité à traduire les capacités, les limites et les méthodes d'attribution des tâches des capacités de collecte organiques, de théâtre d'opération, nationales, de coalition et autres.
S0352	Capacité à utiliser des outils et des environnements collaboratifs pour les opérations de collecte.
S0353	Capacité à utiliser des systèmes et/ou des outils pour suivre les exigences en matière de collecte et déterminer si elles sont satisfaites.
S0354	Capacité à élaborer des politiques qui reflètent les objectifs fondamentaux de l'entreprise en matière de protection de la vie privée.
S0355	Capacité à négocier des accords avec les fournisseurs et à évaluer leurs pratiques en matière de protection de la vie privée.
S0356	Capacité à communiquer avec tous les niveaux de direction, y compris les membres du conseil d'administration (par exemple, compétences interpersonnelles, capacité d'approche, capacité d'écoute efficace, utilisation d'un style et d'un langage adaptés à l'auditoire).
S0357	Capacité à anticiper les nouvelles menaces en matière de sécurité.
S0358	Capacité à se tenir au courant de l'évolution des infrastructures techniques.
S0359	Capacité à faire preuve d'esprit critique pour analyser les modèles et les relations organisationnels.
S0360	Capacité à analyser et à évaluer les capacités et les outils des partenaires internes et externes en matière d'opérations cybers.
S0361	Capacité à analyser et à évaluer les processus de renseignement des partenaires internes et externes et l'élaboration des besoins en information et des informations essentielles.

ID KSA	Descriptions
S0362	Capacité à analyser et à évaluer les capacités et les limites des organisations partenaires internes et externes (celles qui ont des responsabilités en matière d'attribution des tâches, de collecte, de traitement, d'exploitation et de diffusion).
S0363	Capacité à analyser et à évaluer les rapports des partenaires internes et externes.
S0364	Capacité à développer des idées sur le contexte de l'environnement des menaces d'une organisation.
S0365	Capacité à concevoir la réponse aux incidents pour les modèles de services Cloud.
S0366	Capacité à identifier les capacités réussies pour trouver des solutions à des problèmes de systèmes moins courants et plus complexes.
S0367	Capacité à appliquer les principes de cybersécurité et de confidentialité aux exigences organisationnelles (pertinentes pour la confidentialité, l'intégrité, la disponibilité, l'authentification, la non-répudiation).
S0368	Capacité à utiliser l'évaluation des risques pour élaborer des approches rentables et fondées sur les performances afin d'aider les organisations à identifier, évaluer et gérer les risques liés à la cybersécurité.
S0369	Capacité à identifier les sources, les caractéristiques et les utilisations des actifs de données de l'organisation.
S0370	Capacité à utiliser la structure et les processus de reporting des fournisseurs de services de cybersécurité au sein de sa propre organisation.
S0371	Capacité à réagir et à prendre des mesures locales en réponse aux alertes de menaces communiquées par des fournisseurs de services.
S0372	Capacité à traduire, suivre et hiérarchiser les besoins en informations et les exigences en matière de collecte de renseignements dans l'ensemble de l'entreprise étendue.
S0373	Capacité à veiller à ce que les informations relatives à la responsabilité soient collectées pour les éléments qui composent l'infrastructure des systèmes d'information et la chaîne d'approvisionnement des technologies de l'information et de la communication.
S0374	Capacité à identifier les questions de cybersécurité et de protection de la vie privée qui découlent des liens avec les clients internes et externes et les organisations partenaires.

A.7 Descriptions des aptitudes du référentiel NICE

Le tableau 7 fournit une liste des aptitudes en matière de cybersécurité. L'aptitude est la compétence à avoir un comportement observable ou un comportement qui aboutit à un résultat observable. Des descriptions d'aptitudes sélectionnées dans cette liste sont incluses dans chaque fonction dans la liste détaillée des fonctions de l'annexe B. Cette liste sera mise à jour régulièrement [1]. La source de référence pour la version la plus récente de ce document est le tableur de référence de la publication spéciale 800-181 du NIST [4].

Tableau 7 – Descriptions des aptitudes du référentiel NICE

ID KSA	Descriptions
A0001	Aptitude à identifier les problèmes de sécurité systémiques sur la base de l'analyse des données de vulnérabilité et de configuration.
A0002	Aptitude à faire correspondre la technologie du référentiel de connaissances à une application ou à un environnement donné.
A0003	Aptitude à déterminer la validité des données relatives aux tendances technologiques.
A0004	Aptitude à élaborer un programme d'études qui aborde le sujet au niveau approprié pour le public cible.
A0005	Aptitude à décrypter des ensembles de données numériques collectées.
A0006	Aptitude à préparer et à organiser des séances d'information et de sensibilisation pour s'assurer que les utilisateurs des systèmes, des réseaux et des données connaissent et respectent les politiques et les procédures de sécurité des systèmes.
A0007	Aptitude à adapter l'analyse de code aux problèmes spécifiques à l'application.
A0008	Aptitude à appliquer les méthodes, les normes et les approches permettant de décrire, d'analyser et de documenter l'architecture des technologies de l'information (TI) d'une organisation (par exemple, le référentiel TOGAF (Open Group Architecture Framework), le référentiel DoDAF (Department of Defense Architecture Framework), le référentiel FEAF (Federal Enterprise Architecture Framework)).
A0009	Aptitude à appliquer les normes de gestion des risques de la chaîne d'approvisionnement.
A0010	Aptitude à analyser les logiciels malveillants.
A0011	Aptitude à répondre aux questions de manière claire et concise.
A0012	Aptitude à poser des questions de clarification.
A0013	Aptitude à communiquer des informations, des concepts ou des idées complexes de manière assurée et bien organisée par des moyens verbaux, écrits et/ou visuels.
A0014	Aptitude à communiquer efficacement par écrit.
A0015	Aptitude à effectuer des analyses de vulnérabilité et à reconnaître les failles des systèmes de sécurité.
A0016	Aptitude à animer des discussions en petits groupes.
A0017	Aptitude à évaluer la compréhension et le niveau de connaissance de l'apprenant.
A0018	Aptitude à préparer et à présenter des briefings.
A0019	Aptitude à produire de la documentation technique.
A0020	Aptitude à fournir un retour d'information efficace aux étudiants pour améliorer l'apprentissage.
A0021	Aptitude à utiliser et à comprendre des concepts mathématiques complexes (par exemple, mathématiques discrètes).
A0022	Aptitude à appliquer les principes de l'apprentissage des adultes.
A0023	Aptitude à concevoir des évaluations valides et fiables.
A0024	Aptitude à élaborer des consignes et du matériel pédagogique clairs.

ID KSA	Descriptions
A0025	Aptitude à définir avec précision les incidents, les problèmes et les événements dans le système d'enregistrement des pannes.
A0026	Aptitude à analyser les données de test.
A0027	Aptitude à appliquer les buts et objectifs d'une organisation au développement et à la maintenance de l'architecture.
A0028	Aptitude à évaluer et à prévoir les besoins en main-d'œuvre pour atteindre les objectifs de l'organisation.
A0029	Aptitude à construire des structures de données complexes et des langages de programmation de haut niveau.
A0030	Aptitude à collecter, vérifier et valider des données d'essai.
A0031	Aptitude à mener et à mettre en œuvre des études de marché pour comprendre les capacités du gouvernement et de l'industrie ainsi que la tarification appropriée.
A0032	Aptitude à élaborer des programmes d'études destinés à être utilisés dans un environnement virtuel.
A0033	Aptitude à élaborer des politiques, des plans et des stratégies dans le respect des lois, des règlements, des politiques et des normes en matière des activités informatiques de l'organisation.
A0034	Aptitude à élaborer, mettre à jour et/ou maintenir des procédures opérationnelles normalisées (POS).
A0035	Aptitude à décomposer un problème et à examiner les relations entre des données qui peuvent sembler sans rapport entre elles.
A0036	Aptitude à identifier les failles de codage les plus courantes au plus haut niveau.
A0037	Aptitude à tirer parti des bonnes pratiques et des enseignements tirés par des organisations externes et des établissements universitaires traitant de questions cyber.
A0038	Aptitude à optimiser les systèmes pour répondre aux exigences de performance de l'entreprise.
A0039	Aptitude à superviser l'élaboration et la mise à jour de l'estimation des coûts du cycle de vie.
A0040	Aptitude à traduire les données et les résultats des essais en conclusions évaluatives.
A0041	Aptitude à utiliser des outils de visualisation de données (par exemple, Flare, HighCharts, AmCharts, D3.js, Processing, Google Visualization API, Tableau, Raphael.js).
A0042	Aptitude à développer des opportunités de parcours professionnel.
A0043	Aptitude à mener des investigations numériques légales dans et pour des environnements Windows et Unix/Linux.
A0044	Aptitude à appliquer les structures du langage de programmation (par exemple, examen du code source) et la logique.
A0045	Aptitude à évaluer/assurer la fiabilité du fournisseur et/ou du produit.
A0046	Aptitude à surveiller et à évaluer l'impact potentiel des technologies émergentes sur les lois, les règlements et/ou les politiques.
A0047	Aptitude à développer des logiciels sécurisés conformément aux méthodologies, outils et pratiques de déploiement de logiciels sécurisés.
A0048	Aptitude à appliquer les concepts d'architecture de sécurité des réseaux, y compris la topologie, les protocoles, les composants et les principes (par exemple, l'application de la défense en profondeur).
A0049	Aptitude à appliquer les outils, méthodes et techniques de conception de systèmes sécurisés.
A0050	Aptitude à appliquer les outils, méthodes et techniques de conception de systèmes, y compris les outils d'analyse et de conception de systèmes automatisés.
A0051	Aptitude à exécuter les processus d'intégration technologique.

ID KSA	Descriptions
A0052	Aptitude à faire fonctionner les équipements réseaux, y compris les concentrateurs, les routeurs, les commutateurs, les ponts, les serveurs, les supports de transmission et le matériel connexe.
A0053	Aptitude à déterminer la validité des données relatives aux évolutions des effectifs.
A0054	Aptitude à appliquer les méthodes d'ingéniérie pédagogique.
A0055	Aptitude à utiliser des outils de réseau courants (ping, traceroute, nslookup, etc.).
A0056	Aptitude à garantir le respect des pratiques de sécurité tout au long du processus d'acquisition.
A0057	Aptitude à concevoir un programme d'études qui aborde le sujet au niveau approprié pour le public cible.
A0058	Aptitude à exécuter des commandes en ligne du système d'exploitation (par exemple, ipconfig, netstat, dir, nbtstat).
A0059	Aptitude à exploiter les voies LAN/WAN de l'organisation.
A0060	Aptitude à construire des architectures et des cadres.
A0061	Aptitude à concevoir des architectures et des cadres.
A0062	Aptitude à surveiller les mesures ou indicateurs de performance et de disponibilité des systèmes.
A0063	Aptitude à utiliser différents systèmes et méthodes de communication électronique (par exemple, courrier électronique, VOIP, IM, forums web, diffusion vidéo en direct).
A0064	Aptitude à interpréter et à traduire les exigences des clients en capacités opérationnelles.
A0065	Aptitude à surveiller les flux de trafic sur le réseau.
A0066	Aptitude à rechercher avec précision et exhaustivité toutes les données utilisées dans les produits de renseignement, d'évaluation et/ou de planification.
A0067	Aptitude à s'adapter et à travailler dans un environnement de travail diversifié, imprévisible, stimulant et en évolution rapide.
A0068	Aptitude à appliquer les processus approuvés de planification, de développement et de dotation en personnel.
A0069	Aptitude à mettre en œuvre des compétences et des stratégies de collaboration.
A0070	Aptitude à mettre en œuvre des compétences de lecture/réflexion critique.
A0071	Aptitude à appliquer l'expertise linguistique et culturelle à l'analyse.
A0072	Aptitude à formuler clairement les exigences en matière de renseignement sous la forme de questions bien formulées et de variables de suivi des données à des fins de suivi de l'enquête.
A0073	Aptitude à exprimer clairement les besoins en matière de renseignement sous la forme de questions de recherche et de demandes d'information bien formulées.
A0074	Aptitude à collaborer efficacement avec les autres.
A0076	Aptitude à communiquer des informations, des concepts ou des idées complexes avec assurance et de manière bien organisée en utilisant des moyens verbaux, écrits et/ou visuels.
A0077	Aptitude à coordonner et à collaborer avec des analystes au sujet des exigences de surveillance et de l'élaboration d'informations essentielles.
A0078	Aptitude à coordonner les opérations cybers avec d'autres services ou fonctions support de l'organisation.
A0079	Aptitude à coordonner, à collaborer et à diffuser des informations aux organisations subordonnées, latérales et de niveau supérieur.
A0080	Aptitude à utiliser correctement chaque organisation ou élément dans le plan et la matrice de collecte.
A0081	Aptitude à élaborer ou à recommander des approches ou des solutions analytiques à des problèmes et à des situations pour lesquels les informations sont incomplètes ou pour lesquels il n'existe pas de précédent.

ID KSA	Descriptions
A0082	Aptitude à élaborer ou à recommander des solutions de planification pour des problèmes et des situations pour lesquels il n'existe pas de précédent.
A0083	Aptitude à collaborer efficacement au sein d'équipes en mode connecté.
A0084	Aptitude à évaluer la fiabilité, la validité et la pertinence de l'information.
A0085	Aptitude à évaluer, analyser et synthétiser de grandes quantités de données (qui peuvent être fragmentées et contradictoires) en produits de ciblage/renseignement consolidés de haute qualité.
A0086	Aptitude à faire preuve de discernement lorsque les politiques ne sont pas bien définies.
A0087	Aptitude à élargir l'accès au réseau en procédant à l'analyse et à la collecte d'objectifs afin d'identifier les cibles d'intérêt.
A0088	Aptitude à concentrer les efforts de recherche pour répondre aux besoins décisionnels du client.
A0089	Aptitude à fonctionner efficacement dans un environnement dynamique et en évolution rapide.
A0090	Aptitude à travailler dans un environnement collaboratif, en recherchant en permanence la collaboration d'autres analystes et experts, tant internes qu'externes à l'organisation, afin de tirer parti de l'expertise analytique et technique.
A0091	Aptitude à identifier des partenaires externes ayant des intérêts communs en matière d'opérations cybers.
A0092	Aptitude à identifier les lacunes en matière de renseignement.
A0093	Aptitude à identifier/décrire la vulnérabilité de la cible.
A0094	Aptitude à identifier/décrire les techniques/méthodes d'exploitation technique de la cible.
A0095	Aptitude à interpréter et à appliquer les lois, les règlements, les politiques et les orientations en rapport avec les objectifs de l'organisation en matière d'opérations cybers.
A0096	Aptitude à interpréter et à traduire les exigences des clients en mesures opérationnelles.
A0097	Aptitude à interpréter et à comprendre des concepts complexes et en évolution rapide.
A0098	Aptitude à surveiller les opérations des systèmes et à réagir aux événements en réponse à des déclencheurs et/ou à l'observation de tendances ou d'activités inhabituelles.
A0099	Aptitude à faire partie d'équipes de planification, de groupes de coordination et de groupes de travail, selon les besoins.
A0100	Aptitude à mettre en œuvre des tactiques, techniques et procédures de collecte de données sur le réseau, y compris des capacités/outils de déchiffrement.
A0101	Aptitude à exécuter des procédures de collecte sans fil, comprenant des capacités/outils de décryptage.
A0102	Aptitude à reconnaître et à atténuer les biais cognitifs susceptibles d'affecter l'analyse.
A0103	Aptitude à reconnaître et à atténuer le phénomène de tromperie dans les rapports et les analyses.
A0104	Aptitude à vérifier l'exactitude et l'exhaustivité des documents traités dans la langue cible.
A0105	Aptitude à sélectionner les implantations appropriées pour atteindre les objectifs opérationnels.
A0106	Aptitude à adapter les informations techniques et les informations relatives à la planification au niveau de compréhension du client.
A0107	Aptitude à la réflexion critique.
A0108	Aptitude à penser comme les pirates informatiques.
A0109	Aptitude à comprendre les objectifs et les effets.
A0110	Aptitude à utiliser de multiples sources de renseignement dans toutes les disciplines du renseignement.
A0111	Aptitude à suivre l'évolution des lois sur la protection de la vie privée afin de garantir l'adaptation et la conformité de l'organisation.

ID KSA	Descriptions
A0112	Aptitude à travailler avec les services et les unités opérationnelles pour mettre en œuvre les principes et les programmes de l'organisation en matière de protection de la vie privée ainsi que pour aligner les objectifs en matière de protection de la vie privée sur ceux relatifs à la sécurité.
A0113	Aptitude à suivre l'évolution des technologies en matière de protection de la vie privée afin d'assurer l'adaptation et la conformité de l'organisation.
A0114	Aptitude à déterminer si un incident de sécurité viole un principe de protection de la vie privée ou une règle de droit nécessitant une action juridique spécifique.
A0115	Aptitude à élaborer ou à se procurer des programmes de formation qui traitent du sujet au niveau adapté à la cible.
A0116	Aptitude à travailler avec les services et les unités opérationnelles pour mettre en œuvre les principes et les programmes de l'organisation en matière de protection de la vie privée, et à aligner les objectifs de protection de la vie privée sur les objectifs de sécurité.
A0117	Aptitude à hiérarchiser et à affecter correctement et efficacement les ressources en matière de cybersécurité.
A0118	Aptitude à faire le lien entre la stratégie, l'activité et la technologie dans le contexte de la dynamique organisationnelle.
A0119	Aptitude à comprendre les questions de technologie, de gestion et de leadership liées aux processus organisationnels et à la résolution de problèmes.
A0120	Aptitude à comprendre les concepts de base et les questions liées à la cybersécurité et à son impact sur l'organisation.
A0121	Aptitude à partager des informations utiles sur le contexte de l'environnement des menaces d'une organisation afin d'améliorer sa position en matière de gestion des risques.
A0122	Aptitude à concevoir la réponse aux incidents pour les modèles de services Cloud.
A0123	Aptitude à concevoir des capacités permettant de trouver des solutions à des problèmes concernant des systèmes moins courants et plus complexes.
A0124	Aptitude à appliquer les principes de cybersécurité et de protection de la vie privée aux exigences organisationnelles (pertinentes pour la confidentialité, l'intégrité, la disponibilité, l'authentification, la non-répudiation).
A0125	Aptitude à établir et à maintenir des évaluations automatisées des mesures de sécurité.
A0126	Aptitude à rédiger une déclaration de confidentialité sur la base des lois en vigueur.
A0127	Aptitude à suivre l'emplacement et la configuration des équipements et des logiciels en réseau dans l'ensemble des services, des sites, des installations et, éventuellement, des fonctions de soutien de l'entreprise.
A0128	Aptitude à déployer des technologies et des outils de surveillance continue.
A0129	Aptitude à appliquer des techniques de détection d'intrusions au niveau de l'hôte et du réseau à l'aide de technologies de détection d'intrusions.
A0130	Aptitude à faire en sorte que les processus de gestion de la sécurité de l'information soient intégrés dans les processus de planification stratégique et opérationnelle.
A0131	Aptitude à faire en sorte que les hauts responsables de l'organisation assurent la sécurité de l'information pour les informations et les systèmes qui supportent les opérations et les biens placés sous leur contrôle.
A0132	Aptitude à faire en sorte que l'organisation dispose d'un personnel suffisamment formé pour l'aider à se conformer aux exigences de sécurité de la législation, des décrets, des politiques, des directives, des instructions, des normes et des lignes directrices.
A0133	Aptitude à se coordonner avec la haute direction d'une organisation pour fournir une approche globale, à l'échelle de l'organisation, pour traiter les risques - une approche qui permette une meilleure compréhension des opérations de l'organisation.

ID KSA	Descriptions
A0134	Aptitude à se coordonner avec la direction générale d'une organisation pour élaborer une stratégie de gestion des risques pour l'organisation, fournissant une vision stratégique des risques liés à la sécurité pour l'organisation.
A0135	Aptitude à se coordonner avec la direction générale d'une organisation pour faciliter le partage d'informations relatives aux risques entre les responsables des habilitations et d'autres hauts dirigeants de l'organisation.
A0136	Aptitude à se coordonner avec la direction générale d'une organisation pour assurer la supervision de toutes les activités liées à la gestion des risques dans l'ensemble de l'organisation, afin de contribuer à la cohérence et à l'efficacité des décisions en matière d'acceptation des risques.
A0137	Aptitude à se coordonner avec la direction générale d'une organisation pour s'assurer que les décisions en matière d'autorisation tiennent compte de tous les facteurs nécessaires à la réussite de la mission et de l'activité.
A0138	Aptitude à se coordonner avec la direction générale d'une organisation afin d'offrir un forum à l'échelle de l'organisation permettant d'examiner toutes les sources de risques (y compris les risques cumulés) pour les opérations et les biens de l'organisation, ainsi que pour les individus, les autres organisations et la nation.
A0139	Aptitude à se coordonner avec la direction générale d'une organisation pour promouvoir la coopération et la collaboration entre les responsables des habilitations, y compris pour les actions d'habilitation nécessitant une responsabilité partagée.
A0140	Aptitude à se coordonner avec la direction générale d'une organisation pour faire en sorte que la responsabilité partagée du soutien des missions/fonctions opérationnelles de l'organisation par des fournisseurs externes de systèmes, de services et d'applications reçoive la visibilité nécessaire et soit portée à la connaissance des autorités décisionnelles concernées.
A0141	Aptitude à se coordonner avec la direction générale d'une organisation pour identifier la posture de risque de l'organisation sur la base du risque agrégé lié au fonctionnement et à l'utilisation des systèmes dont l'organisation est responsable.
A0142	Aptitude à travailler en étroite collaboration avec les autorités compétentes et leurs représentants désignés afin de contribuer à la mise en œuvre efficace d'un programme de sécurité à l'échelle de l'organisation, ce qui permet d'assurer une sécurité appropriée pour l'ensemble des systèmes et des environnements d'exploitation de l'organisation.
A0143	Aptitude à travailler en étroite collaboration avec les autorités compétentes et leurs représentants désignés afin de veiller à ce que les considérations de sécurité soient intégrées dans les cycles de programmation/planification/budgétisation, les architectures d'entreprise et les cycles de développement des acquisitions/systèmes.
A0144	Aptitude à travailler en étroite collaboration avec les autorités compétentes et leurs représentants désignés afin de s'assurer que les systèmes organisationnels et les dispositifs de contrôle communs sont couverts par des plans de sécurité approuvés et qu'ils disposent d'autorisations à jour.
A0145	Aptitude à travailler en étroite collaboration avec les autorités compétentes et leurs représentants désignés afin de veiller à ce que les activités liées à la sécurité requises dans l'ensemble de l'organisation soient menées à bien de manière efficace, rentable et opportune.
A0146	Aptitude à travailler en étroite collaboration avec les autorités compétentes et leurs représentants désignés afin de veiller à ce que les activités liées à la sécurité fassent l'objet d'un rapport centralisé.
A0147	Aptitude à établir les règles d'utilisation et de protection des informations et à conserver cette responsabilité même lorsque les informations sont partagées avec d'autres organisations ou leur sont communiquées.

ID KSA	Descriptions
A0148	Aptitude à approuver les plans de sécurité, les protocoles d'accord ou d'entente, les plans d'action et les étapes, et à déterminer si des changements importants dans les systèmes ou les environnements d'exploitation nécessitent une nouvelle autorisation.
A0149	Aptitude à assurer une liaison privilégiée entre l'architecte d'entreprise et l'ingénieur chargé de la sécurité des systèmes et à assurer la coordination avec les propriétaires de systèmes, les fournisseurs de mesures de sécurité partagées et les responsables de la sécurité des systèmes en ce qui concerne l'attribution des moyens de sécurité qu'ils soient spécifiques à un système, hybrides ou communs.
A0150	Aptitude, en étroite coordination avec les responsables de la sécurité des systèmes, à conseiller les autorités compétentes, les directeurs de l'information, les responsables de la sécurité des systèmes d'information et le responsable de la gestion des risques (fonction) sur une série de questions liées à la sécurité (par exemple, l'établissement des limites du système, l'évaluation de la gravité des faiblesses et des déficiences du système, les plans d'action et les étapes, les approches d'atténuation des risques, les alertes de sécurité et les effets négatifs potentiels des vulnérabilités identifiées).
A0151	Aptitude à mener des activités d'ingénierie de la sécurité des systèmes (NIST SP 800-160).
A0152	Aptitude à saisir et à affiner les exigences de sécurité et à veiller à ce que ces exigences soient effectivement intégrées dans les produits et systèmes composants par une architecture, une conception, un développement et une configuration de sécurité ciblés.
A0153	Aptitude à utiliser les bonnes pratiques lors de la mise en œuvre des mesures de sécurité au sein d'un système, y compris les méthodologies d'ingénierie logicielle, les principes d'ingénierie des systèmes et de la sécurité, la conception sécurisée, l'architecture sécurisée et les techniques de codage sécurisé.
A0154	Aptitude à coordonner les activités liées à la sécurité avec les architectes de sécurité, les responsables de la sécurité des systèmes d'information, les propriétaires de systèmes, les fournisseurs de mesures de sécurité partagées et les responsables de la sécurité des systèmes.
A0155	Aptitude à procéder à une évaluation complète des mesures de sécurité administratives, opérationnelles et techniques, ainsi que des améliorations des mesures de sécurité employées dans un système ou héritées d'un système, afin de déterminer l'efficacité de ces mesures (c'est-à-dire la capacité des mesures de sécurité à être mises en œuvre correctement, à fonctionner comme prévu et à produire le résultat escompté en ce qui concerne le respect des exigences de sécurité pour le système).
A0156	Aptitude à fournir une évaluation de la gravité des faiblesses ou des déficiences découvertes dans le système et son environnement d'exploitation et à recommander des actions correctives pour remédier aux vulnérabilités identifiées.
A0157	Aptitude à préparer le rapport final d'évaluation de la sécurité dans lequel figurent les résultats et les conclusions de l'évaluation.
A0158	Aptitude à évaluer un plan de sécurité afin d'aider à garantir que le plan fournit un ensemble de contrôles de sécurité pour le système qui répondent aux exigences de sécurité énoncées.
A0159	Aptitude à s'assurer que les exigences fonctionnelles et les exigences de sécurité sont traitées de manière appropriée dans un contrat et que le contractant y répond.
A0160	Aptitude à interpréter les informations recueillies par les outils réseaux (par exemple Nslookup, Ping et Traceroute).
A0161	Aptitude à traduire, à suivre et à hiérarchiser les besoins en informations et les exigences en matière de collecte de renseignements dans l'ensemble de l'entreprise étendue.

ID KSA	Descriptions
A0162	Aptitude à intégrer les exigences en matière de sécurité de l'information dans le processus d'acquisition ; à utiliser les mesures de sécurité de base applicables comme l'une des sources des exigences en matière de sécurité ; à garantir un processus solide de contrôle de la qualité des logiciels ; et à établir des sources multiples (par exemple, des itinéraires de livraison, pour les éléments de systèmes critiques).
A0162	Aptitude à faire en sorte que la sécurité des systèmes d'information, le personnel chargé des acquisitions, les conseillers juridiques et les autres conseillers et parties prenantes concernés participent à la prise de décision dès la définition/l'examen du concept du système et qu'ils soient associés à chaque décision d'étape tout au long du cycle de vie des systèmes ou qu'ils l'approuvent.
A0163	Aptitude à interpréter la terminologie, les lignes directrices et les procédures relatives à la sécurité des communications (COMSEC).
A0164	Aptitude à identifier les rôles et les responsabilités du personnel chargé de la sécurité des communications (COMSEC).
A0165	Aptitude à gérer la procédure de comptabilisation, de contrôle et d'utilisation du matériel de sécurité des communications (COMSEC).
A0166	Aptitude à identifier les types d'incidents liés à la sécurité des communications (COMSEC) et la manière dont ils sont signalés.
A0167	Aptitude à reconnaître l'importance de l'audit du matériel de sécurité des communications (COMSEC) et des comptes.
A0168	Aptitude à identifier les exigences de la comptabilisation en cours de processus pour la sécurité des communications (COMSEC).
A0170	Aptitude à identifier les systèmes d'infrastructures critiques utilisant les technologies de l'information et de la communication qui ont été conçus sans tenir compte de la sécurité du système.
A0171	Aptitude à procéder à l'évaluation des besoins en matière de formation et d'éducation.
A0172	Aptitude à mettre en place un sous-réseau physique ou logique qui sépare un réseau local interne (LAN) d'autres réseaux non fiables.
A0173	Aptitude à reconnaître que les changements apportés aux systèmes ou à l'environnement peuvent modifier les risques résiduels par rapport à l'appétence pour le risque.
A0174	Aptitude à trouver et à naviguer sur le "dark web" en utilisant le réseau TOR pour localiser les marchés et les forums.
A0175	Aptitude à examiner les médias numériques sur plusieurs types de systèmes d'exploitation.
A0176	Aptitude à gérer des bases de données. (c'est-à-dire sauvegarder, restaurer, supprimer des données, des fichiers journaux de transactions, etc.)

Annexe B – Liste détaillée des Fonctions

Cette annexe fournit une description détaillée de chaque fonction du référentiel NICE. Pour chaque fonction, la liste ci-dessous fournit les informations suivantes :

- Le nom de la fonction ;
- Un identifiant unique de la fonction du référentiel NICE, basé sur les abréviations de la catégorie et de la spécialité auxquels cette fonction appartient ;
- La spécialité dans laquelle la fonction réside ;
- La catégorie dans laquelle la fonction réside ;
- Une description de la fonction ;
- Une liste des Tâches du référentiel NICE qu'une personne occupant un poste dans le domaine de la cybersécurité qui comprend la fonction pourrait être amenée à accomplir ;
- Une liste des domaines de connaissances du référentiel NICE qu'une personne occupant un poste dans le domaine de la cybersécurité qui comprend la fonction pourrait être amenée à démontrer ;
- Une liste des capacités du référentiel NICE qu'une personne occupant un poste dans le domaine de la cybersécurité qui comprend la fonction pourrait être amenée à maîtriser ; et
- Une liste des aptitudes du référentiel NICE qu'une personne occupant un poste dans le domaine de la cybersécurité qui comprend la fonction pourrait être amenée à démontrer.

Les tableaux suivants décrivent les fonctions du référentiel NICE à l'aide d'une simple liste de tâches, de connaissances, de capacités et d'aptitudes. La source de référence pour la version la plus récente de ce document se trouve dans le tableur de référence de la publication spéciale 800-181 du NIST (Reference Spreadsheet for NIST Special Publication 800-181) [4]. Le tableur de référence fournit des listes plus détaillées des tâches, des connaissances, des capacités et des aptitudes. Les rôles de travail seront mis à jour périodiquement [1].

B.1 Provisionnement sécurisé (SP)

Nom de la fonction	Responsable de l'autorisation / Représentant désigné
ID de la fonction	**SP-RSK-001**
Spécialité	**Gestion des risques (RSK)**
Catégorie	**Provisionnement sécurisé (SP)**
Description de la fonction	Dirigeant ou cadre supérieur ayant le pouvoir d'assumer officiellement la responsabilité de l'exploitation d'un système d'information à un niveau de risque acceptable pour les opérations de l'organisation (y compris la mission, les fonctions, l'image ou la réputation), les biens de l'organisation, les individus, d'autres organisations et la nation (CNSSI 4009).
Tâches	T0145, T0221, T0371, T0495
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0070, K0084, K0089, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0295, K0322, K0342, K0622, K0624
Capacités	S0034, S0367
Aptitudes	A0028, A0033, A0077, A0090, A0094, A0111, A0117, A0118, A0119, A0123, A0170

Nom de la fonction	Contrôleur de sécurité
ID de la fonction	SP-RSK-002
Spécialité	Gestion des risques (RSK)
Catégorie	Provisionnement sécurisé (SP)
Description de la fonction	Effectue des évaluations indépendantes et complètes des mesures de sécurité managériales, opérationnelles et techniques, ainsi que des améliorations des mesures de sécurité mises en œuvre au sein d'un système d'information ou dont celui-ci a hérité, afin de déterminer l'efficacité globale des mesures de sécurité (telles que définies dans la norme NIST SP 800-37).
Tâches	T0145, T0184, T0221, T0244, T0251, T0371, T0495, T0177, T0178, T0181, T0205, T0243, T0255, T0264, T0265, T0268, T0272, T0275, T0277, T0309, T0344
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0013, K0018, K0019, K0018, K0021, K0024, K0026, K0027, K0028, K0029, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0056, K0059, K0070, K0084, K0089, K0098, K0100, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0287, K0322, K0342, K0622, K0624
Capacités	S0001, S0006, S0027, S0034, S0038, S0073, S0078, S0097, S0100, S0110, S0111, S0112, S0115, S0120, S0124, S0128, S0134, S0135, S0136, S0137, S0138, S0141, S0145, S0147, S0171, S0172, S0173, S0174, S0175, S0176, S0177, S0184, S0232, S0233, S0234, S0235, S0236, S0237, S0238, S0239, S0240, S0241, S0242, S0243, S0244, S0248, S0249, S0250, S0251, S0252, S0254, S0271, S0273, S0278, S0279, S0280, S0281, S0296, S0304, S0305, S0306, S0307, S0325, S0329, S0332, S0367, S0370, S0374
Aptitudes	A0001, A0011, A0012, A0013, A0014, A0015, A0016, A0018, A0019, A0023, A0026, A0030, A0035, A0036, A0040, A0056, A0069, A0070, A0082, A0083, A0084, A0085, A0086, A0087, A0088, A0089, A0090, A0091, A0092, A0093, A0094, A0095, A0096, A0098, A0101, A0106, A0108, A0109, A0117, A0118, A0119, A0111, A0112, A0114, A0115, A0116, A0119, A0123, A0170

Nom de la fonction	Développeur de logiciels
ID de la fonction	SP-DEV-001
Spécialité	Développement de logiciels (DEV)
Catégorie	Provisionnement sécurisé (SP)
Description de la fonction	Développe, crée, entretient et écrit/code de nouvelles applications informatiques, des logiciels ou des programmes utilitaires spécialisés (ou modifie des applications existantes).
Tâches	T0009, T0011, T0013, T0014, T0022, T0026, T0034, T0040, T0046, T0057, T0077, T0100, T0111, T0117, T0118, T0171, T0176, T0181, T0189, T0217, T0228, T0236, T0267, T0303, T0311, T0324, T0337, T0416, T0417, T0436, T0455, T0500, T0553, T0554
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0332, K0342, K0343, K0624
Capacités	S0001, S0014, S0017, S0019, S0022, S0031, S0034, S0060, S0135, S0138, S0149, S0174, S0175, S0367
Aptitudes	A0007, A0021, A0047, A0123, A0170

Nom de la fonction	Contrôleur de la sécurité des logiciels
ID de la fonction	SP-DEV-002
Spécialité	Développement de logiciels (DEV)
Catégorie	Provisionnement sécurisé (SP)
Description de la fonction	Analyse la sécurité des applications informatiques, des programmes informatiques ou des programmes spécialisés, nouveaux ou existants, et fournit des conclusions exploitables.
Tâches	T0013, T0014, T0022, T0038, T0040, T0100, T0111, T0117, T0118, T0171, T0181, T0217, T0228, T0236, T0266, T0311, T0324, T0337, T0424, T0428, T0436, T0456, T0457, T0516, T0554
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0178, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0342, K0343, K0624
Capacités	S0001, S0022, S0031, S0034, S0083, S0135, S0138, S0174, S0175, S0367
Aptitudes	A0021, A0123, A0170

Nom de la fonction	Architecte d'entreprise
ID de la fonction	SP-ARC-001
Spécialité	Architecture des systèmes (ARC)
Catégorie	Provisionnement sécurisé (SP)
Description de la fonction	Développe et maintient des processus d'affaires, de systèmes et d'information pour soutenir les besoins de la mission de l'entreprise ; développe des règles et des exigences en matière de technologies de l'information (TI) qui décrivent les architectures de base et les architectures cibles.
Tâches	T0051, T0084, T0090, T0108, T0196, T0205, T0307, T0314, T0328, T0338, T0427, T0440, T0448, T0473, T0517, T0521, T0542, T0555, T0557
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0024, K0027, K0028, K0030, K0035, K0037, K0043, K0044, K0052, K0056, K0060, K0061, K0063, K0074, K0075, K0082, K0091, K0093, K0102, K0170, K0179, K0180, K0198, K0200, K0203, K0207, K0211, K0212, K0214, K0227, K0240, K0264, K0275, K0286, K0287, K0291, K0293, K0299, K0322, K0323, K0325, K0326, K0332, K0333, K0487, K0516
Capacités	S0005, S0024, S0027, S0050, S0060, S0122, S0367, S0374
Aptitudes	A0008, A0015, A0027, A0038, A0051, A0060, A0123, A0170

Nom de la fonction	Architecte sécurité
ID de la fonction	SP-ARC-002
Spécialité	Architecture des systèmes (ARC)
Catégorie	Provisionnement sécurisé (SP)
Description de la fonction	Veille à ce que les exigences de sécurité des parties prenantes nécessaires pour protéger la mission et les processus opérationnels de l'organisation soient correctement prises en compte dans tous les aspects de l'architecture d'entreprise, y compris les modèles de référence, les architectures de secteurs et de solutions, et les systèmes qui en résultent et qui soutiennent ces missions et processus opérationnels.
Tâches	T0050, T0051, T0071, T0082, T0084, T0090, T0108, T0177, T0196, T0203, T0205, T0268, T0307, T0314, T0328, T0338, T0427, T0448, T0473, T0484, T0542, T0556
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0015, K0018, K0019, K0024, K0026, K0027, K0030, K0035, K0036, K0037, K0043, K0044, K0052, K0055, K0056, K0057, K0059, K0060, K0061, K0063, K0071, K0074, K0082, K0091, K0092, K0093, K0102, K0170, K0180, K0198, K0200, K0202, K0211, K0212, K0214, K0227, K0240, K0260, K0261, K0262, K0264, K0275, K0277, K0286, K0287, K0291, K0293, K0320, K0322, K0323, K0325, K0326, K0332, K0333, K0336, K0374, K0565
Capacités	S0005, S0022, S0024, S0027, S0050, S0059, S0061, S0076, S0116, S0122, S0138, S0139, S0152, S0168, S0170, S367, S0374
Aptitudes	A0008, A0014, A0015, A0027, A0038, A0048, A0049, A0050, A0061, A0123, A0148, A0149, A0170, A0172

Nom de la fonction	Spécialiste en recherche et développement
ID de la fonction	SP-TRD-001
Spécialité	R&D technologique (TRD)
Catégorie	Provisionnement sécurisé (SP)
Description de la fonction	Mène des recherches sur l'ingénierie des logiciels et des systèmes et sur les systèmes logiciels afin de développer de nouvelles capacités, en veillant à ce que la cybersécurité soit pleinement intégrée. Il effectue des recherches technologiques approfondies afin d'évaluer les vulnérabilités potentielles des systèmes informatiques.
Tâches	T0064, T0249, T0250, T0283, T0284, T0327, T0329, T0409, T0410, T0411, T0413, T0547
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0059, K0090, K0126, K0169, K0170, K0171, K0172, K0174, K0175, K0176, K0179, K0202, K0209, K0267, K0268, K0269, K0271, K0272, K0288, K0296, K0310, K0314, K0321, K0342, K0499
Capacités	S0005, S0017, S0072, S0140, S0148, S0172
Aptitudes	A0001, A0018, A0019, A0170

Nom de la fonction	**Planificateur des besoins fonctionnels**
ID de la fonction	**SP-SRP-001**
Spécialité	**Planification des exigences système (SRP)**
Catégorie	**Provisionnement sécurisé (SP)**
Description de la fonction	Consulte les clients pour évaluer les besoins fonctionnels et les traduire en solutions techniques.
Tâches	T0033, T0039, T0045, T0052, T0062, T0127, T0156, T0174, T0191, T0235, T0273, T0300, T0313, T0325, T0334, T0454, T0463, T0497
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0012, K0018, K0019, K0032, K0035, K0038, K0043, K0044, K0045, K0047, K0055, K0056, K0059, K0060, K0061, K0063, K0066, K0067, K0073, K0074, K0086, K0087, K0090, K0091, K0093, K0101, K0102, K0126, K0163, K0164, K0168, K0169, K0170, K0180, K0200, K0267, K0287, K0325, K0332, K0333, K0622
Capacités	S0005, S0006, S0008, S0010, S0050, S0134, S0367
Aptitudes	A0064, A0123, A0170

Nom de la fonction	**Spécialiste des essais et de l'évaluation des systèmes**
ID de la fonction	**SP-TST-001**
Spécialité	**Test et évaluation (TST)**
Catégorie	**Provisionnement sécurisé (SP)**
Description de la fonction	Planifie, prépare et réalise des essais de systèmes afin d'évaluer les résultats par rapport aux spécifications et aux exigences, ainsi que d'analyser les résultats des essais et d'en rendre compte.
Tâches	T0058, T0080, T0125, T0143, T0257, T0274, T0393, T0426, T0511, T0512, T0513, T0539, T0540
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0027, K0028, K0037, K0044, K0057, K0088, K0091, K0102, K0139, K0126, K0169, K0170, K0179, K0199, K0203, K0212, K0250, K0260, K0261, K0262, K0287, K0332
Capacités	S0015, S0021, S0026, S0030, S0048, S0060, S0061, S0082, S0104, S0107, S0110, S0112, S0115, S0117, S0367
Aptitudes	A0026, A0030, A0040, A0123

Nom de la fonction	Développeur de la sécurité des systèmes d'information
ID de la fonction	SP-SYS-001
Spécialité	Développement de systèmes (SYS)
Catégorie	Provisionnement sécurisé (SP)
Description de la fonction	Conçoit, développe, teste et évalue la sécurité des systèmes d'information tout au long du cycle de développement des systèmes.
Tâches	T0012, T0015, T0018, T0019, T0021, T0032, T0053, T0055, T0056, T0061, T0069, T0070, T0076, T0078, T0105, T0107, T0109, T0119, T0122, T0124, T0181, T0201, T0205, T0228, T0231, T0242, T0269, T0270, T0271, T0272, T0304, T0326, T0359, T0446, T0449, T0466, T0509, T0518, T0527, T0541, T0544
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0126, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0332, K0333, K0336
Capacités	S0001, S0022, S0023, S0024, S0031, S0034, S0036, S0085, S0145, S0160, S0367
Aptitudes	A0001, A0008, A0012, A0013, A0015, A0019, A0026, A0040, A0048, A0049, A0050, A0056, A0061, A0074, A0089, A0098, A0108, A0119, A0123, A0170

Nom de la fonction	Développeur de systèmes
ID de la fonction	SP-SYS-002
Spécialité	Développement de systèmes (SYS)
Catégorie	Provisionnement sécurisé (SP)
Description de la fonction	Conçoit, développe, teste et évalue les systèmes d'information tout au long du cycle de développement des systèmes.
Tâches	T0012, T0021, T0053, T0056, T0061, T0067, T0070, T0107, T0109, T0119, T0181, T0201, T0205, T0228, T0242, T0304, T0326, T0350, T0358, T0359, T0378, T0406, T0447, T0449, T0464, T0466, T0480, T0488, T0518, T0528, T0538, T0541, T0544, T0558, T0559, T0560
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0126, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0207, K0212, K0227, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0332, K0333, K0336
Capacités	S0018, S0022, S0023, S0024, S0025, S0031, S0034, S0036, S0060, S0085, S0097, S0136, S0145, S0146, S0160, S0367
Aptitudes	A0123, A0170

B.2 Exploitation et maintenance (OM)

Nom de la fonction	Administrateur de base de données
ID de la fonction	OM-DTA-001
Spécialité	Administration des données (DTAA)
Catégorie	Exploitation et maintenance (OM)
Description de la fonction	Administre les bases de données et/ou les systèmes de gestion des données qui permettent de stocker, de consulter, de protéger et d'utiliser les données en toute sécurité.
Tâches	T0008, T0137, T0139, T0140, T0146, T0152, T0162, T0210, T0305, T0306, T0330, T0422, T0459, T0490
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0020, K0021, K0022, K0023, K0025, K0031, K0056, K0060, K0065, K0069, K0083, K0097, K0197, K0260, K0261, K0262, K0277, K0278, K0287, K0420
Capacités	S0002, S0013, S0037, S0042, S0045
Aptitudes	A0176

Nom de la fonction	Analyste de données
ID de la fonction	OM-DTA-002
Spécialité	Administration des données (DTA)
Catégorie	Exploitation et maintenance (OM)
Description de la fonction	Examine des données provenant de sources multiples et disparates dans le but de fournir des informations sur la sécurité et la protection de la vie privée. Conçoit et met en œuvre des algorithmes personnalisés, des processus de flux de travail et des mises en page pour des ensembles de données complexes à l'échelle de l'entreprise, utilisés à des fins de modélisation, d'exploration de données et de recherche.
Tâches	T0007, T0008, T0068, T0146, T0195, T0210, T0342, T0347, T0349, T0351, T0353, T0361, T0366, T0381, T0382, T0383, T0385, T0392, T0402, T0403, T0404, T0405, T0460
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0016, K0020, K0022, K0023, K0025, K0031, K0051, K0052, K0056, K0060, K0065, K0068, K0069, K0083, K0095, K0129, K0139, K0140, K0193, K0197, K0229, K0236, K0238, K0325, K0420
Capacités	S0013, S0017, S0202, S0028, S0029, S0037, S0060, S0088, S0089, S0094, S0095, S0103, S0106, S0109, S0113, S0114, S0118, S0119, S0123, S0125, S0126, S0127, S0129, S0130, S0160, S0369
Aptitudes	A0029, A0035, A0036, A0041, A0066

Nom de la fonction	Gestionnaire des connaissances
ID de la fonction	OM-KMG-001
Spécialité	Gestion des connaissances (KMG)
Catégorie	Exploitation et maintenance (OM)
Description de la fonction	Responsable de la gestion et de l'administration des processus et des outils qui permettent à l'organisation d'identifier, de documenter et d'accéder au capital intellectuel ainsi qu'aux connaissances et aux contenus.
Tâches	T0037, T0060, T0154, T0185, T0209, T0339, T0421, T0452, T0524
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0094, K0095, K0096, K0146, K0194, K0195, K0228, K0260, K0261, K0262, K0283, K0287, K0315, K0338, K0420
Capacités	S0011, S0012, S0049, S0055
Aptitudes	A0002

Nom de la fonction	Spécialiste du support technique
ID de la fonction	OM-STS-001
Spécialité	Service à la clientèle et support technique (STS)
Catégorie	Exploitation et maintenance (OM)
Description de la fonction	Fournit une assistance technique aux clients qui ont besoin d'aide pour utiliser le matériel et les logiciels de l'entreprise conformément aux processus organisationnels établis ou approuvés (c'est-à-dire le plan directeur de gestion des incidents, le cas échéant).
Tâches	T0125, T0237, T0308, T0315, T0331, T0468, T0482, T0491, T0494, T0496, T0502, T0530
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0053, K0088, K0109, K0114, K0116, K0194, K0224, K0237, K0242, K0247, K0260, K0261, K0262, K0287, K0292, K0294, K0302, K0317, K0330
Capacités	S0039, S0058, S0142, S0159, S0365
Aptitudes	A0025, A0034, A0122

Nom de la fonction	Spécialiste des opérations réseau
ID de la fonction	OM-NET-001
Spécialité	Services réseaux (NET)
Catégorie	Exploitation et maintenance (OM)
Description de la fonction	Planifie, met en œuvre et exploite des services/systèmes de réseau, y compris des environnements matériels et virtuels.
Tâches	T0035, T0065, T0081, T0121, T0125, T0126, T0129, T0153, T0160, T0200, T0232
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0010, K0011, K0029, K0038, K0049, K0050, K0053, K0061, K0071, K0076, K0093, K0104, K0108, K0111, K0113, K0135, K0136, K0137, K0138, K0159, K0160, K0179, K0180, K0200, K0201, K0203, K0260, K0261, K0262, K0274, K0287, K0332, K0622
Capacités	S0004, S0035, S0040, S0041, S0056, S0077, S0079, S0084, S0150, S0162, S0170
Aptitudes	A0052, A0055, A0058, A0059, A0062, A0063, A0065, A0159

Nom de la fonction	Administrateur système
ID de la fonction	OM-ADM-001
Spécialité	Administration des systèmes (ADM)
Catégorie	Exploitation et maintenance (OM)
Description de la fonction	Responsable de la mise en place et de la maintenance d'un système ou de composants spécifiques d'un système (par exemple, installation, configuration et mise à jour du matériel et des logiciels ; création et gestion des comptes d'utilisateurs ; supervision ou exécution des tâches de sauvegarde et de récupération ; mise en œuvre des mesures de sécurité opérationnelles et techniques ; et respect des politiques et procédures de sécurité de l'organisation).
Tâches	T0029, T0054, T0063, T0136, T0144, T0186, T0207, T0418, T0431, T0435, T0458, T0461, T0498, T0501, T0507, T0514, T0515, T0531
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0049, K0050, K0053, K0064, K0077, K0088, K0100, K0103, K0104, K0117, K0130, K0158, K0167, K0179, K0260, K0261, K0262, K0274, K0280, K0289, K0318, K0332, K0346
Capacités	S0016, S0033, S0043, S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158
Aptitudes	S0154, S0158

Nom de la fonction	Analyste de la sécurité des systèmes
ID de la fonction	OM-ANA-001
Spécialité	Analyse des systèmes (ANA)
Catégorie	Exploitation et maintenance (OM)
Description de la fonction	Responsable pour l'analyse et le développement de l'intégration, des tests, des opérations et de la maintenance de la sécurité des systèmes.
Tâches	T0015, T0016, T0017, T0085, T0086, T0088, T0123, T0128, T0169, T0177, T0187, T0194, T0202, T0205, T0243, T0309, T0344, T0462, T0469, T0470, T0475, T0477, T0485, T0489, T0492, T0499, T0504, T0508, T0526, T0545, T0548
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0019, K0024, K0035, K0036, K0040, K0044, K0049, K0052, K0056, K0060, K0061, K0063, K0075, K0082, K0093, K0102, K0179, K0180, K0200, K0203, K0227, K0260, K0261, K0262, K0263, K0266, K0267, K0275, K0276, K0281, K0284, K0285, K0287, K0290, K0297, K0322, K0333, K0339
Capacités	S0024, S0027, S0031, S0036, S0060, S0141, S0147, S0167, S0367
Aptitudes	A0015, A0123

B.3 Superviser et gouverner (OV)

Nom de la fonction	Conseiller juridique cyber
ID de la fonction	OV-LGA-001
Spécialité	Conseil juridique et défense des intérêts (LGA)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Fournit des conseils juridiques et des recommandations sur des sujets pertinents liés au droit de l'informatique.
Tâches	T0006, T0098, T0102, T0131, T0220, T0419, T0434, T0465, T0474, T0476, T0478, T0487, T0522
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0059, K0107, K0157, K0261, K0262, K0267, K0312, K0316, K0341, K0615
Capacités	S0356
Aptitudes	A0046

Nom de la fonction	Responsable de la protection de la vie privée/responsable du respect de la vie privée
ID de la fonction	OV-LGA-002
Spécialité	Conseil juridique et défense des intérêts (LGA)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Développe et supervise le programme de conformité en matière de protection de la vie privée et le personnel chargé de ce programme, en répondant aux besoins des responsables de la protection de la vie privée et de la sécurité et de leurs équipes en matière de conformité, de gouvernance/politique et d'intervention en cas d'incident.
Tâches	T0003, T0004, T0029, T0930, T0032, T0066, T0098, T0099, T0131, T0133, T0188, T0381, T0384, T0478, T0861, T0862, T0863, T0864, T0865, T0866, T0867, T0868, T0869, T0870, T0871, T0872, T0873, T0874, T0875, T0876, T0877, T0878, T0879, T0880, T0881, T0882, T0883, T0884, T0885, T0886, T0887, T0888, T0889, T0890, T0891, T0892, T0893, T0894, T0895, T0896, T0897, T0898, T0899, T0900, T0901, T0902, T0903, T0904, T0905, T0906, T0907, T0908, T0909, T0910, T0911, T0912, T0913, T0914, T0915, T0916, T0917, T0918, T0919
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0066, K0168, K0612, K0613, K0614, K0615
Capacités	S0354, S0355, S0356
Aptitudes	A0024, A0033, A0034, A0104, A0105, A0110, A0111, A0112, A0113, A0114, A0115, A0125

Nom de la fonction	Créateur de formation en cybersécurité
ID de la fonction	OV-TEA-001
Spécialité	Formation, éducation et sensibilisation (TEA)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Élabore, planifie, coordonne et évalue les cours, les méthodes et les techniques de formation et d'éducation en matière de cybersécurité, en fonction des besoins pédagogiques.
Tâches	T0230, T0247, T0248, T0249, T0345, T0352, T0357, T0365, T0367, T0380, T0437, T0442, T0450, T0451, T0534, T0536, T0926
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0059, K0124, K0146, K0147, K0204, K0208, K0213, K0216, K0217, K0220, K0243, K0239, K0245, K0246, K0250, K0252, K0287, K0628
Capacités	S0064, S0066, S0070, S0102, S0166, S0296
Aptitudes	A0004, A0013, A0015, A0018, A0019, A0022, A0024, A0032, A0054, A0057, A0055, A0057, A0058, A0063, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

Nom de la fonction	Instructeur en cybersécurité
ID de la fonction	OV-TEA-002
Spécialité	Formation, éducation et sensibilisation (TEA)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Élabore et dispense une formation ou un enseignement au personnel dans le domaine cyber.
Tâches	T0030, T0073, T0101, T0224, T0230, T0247, T0316, T0317, T0318, T0319, T0320, T0321, T0322, T0323, T0352, T0365, T0367, T0381, T0382, T0395, T0443, T0444, T0450, T0451, T0467, T0519, T0520, T0535, T0536, T0926
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0059, K0115, K0124, K0130, K0146, K0147, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0239, K0245, K0246, K0250, K0252, K0287, K0313, K0319, K0628
Capacités	S0001, S0004, S0006, S0051, S0052, S0053, S0055, S0056, S0057, S0060, S0064, S0070, S0073, S0075, S0076, S0081, S0084, S0097, S0098, S0100, S0101, S0121, S0131, S0156, S0184, S0270, S0271, S0281, S0293, S0301, S0356, S0358
Aptitudes	A0006, A0011, A0012, A0013, A0014, A0015, A0016, A0017, A0018, A0019, A0020, A0022, A0023, A0024, A0032, A0055, A0057, A0057, A0058, A0063, A0066, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

Nom de la fonction	Responsable de la sécurité des systèmes d'information
ID de la fonction	OV-MGT-001
Spécialité	Gestion de la cybersécurité (MGT)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Responsable de la cybersécurité d'un programme, d'une organisation, d'un système ou d'une zone de sécurité.
Tâches	T0001, T0002, T0003, T0004, T0005, T0024, T0025, T0044, T0089, T0091, T0092, T0093, T0095, T0097, T0099, T0106, T0115, T0130, T0132, T0133, T0134, T0135, T0147, T0148, T0149, T0151, T0157, T0158, T0159, T0192, T0199, T0206, T0211, T0213, T0215, T0219, T0227, T0229, T0234, T0239, T0248, T0254, T0255, T0256, T0263, T0264, T0265, T0275, T0276, T0277, T0280, T0281, T0282
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0018, K0021, K0026, K0033, K0038, K0040, K0042, K0043, K0046, K0048, K0053, K0054, K0058, K0059, K0061, K0070, K0072, K0076, K0077, K0087, K0090, K0092, K0101, K0106, K0121, K0126, K0149, K0150, K0151, K0163, K0167, K0168, K0169, K0170, K0179, K0180, K0199, K0260, K0261, K0262, K0267, K0287, K0332, K0342, K0622, K0624
Capacités	S0018, S0027, S0086
Aptitudes	A0128, A0161, A0170

Nom de la fonction	Responsable de la sécurité des communications (COMSEC)
ID de la fonction	OV-MGT-002
Spécialité	Gestion de la cybersécurité (MGT)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Gère les ressources de sécurité des communications (COMSEC) d'une organisation (CNSSI 4009) ou a la garde des clefs d'un système de gestion des clefs cryptographiques (CKMS).
Tâches	T0003, T0004, T0025, T0044, T0089, T0095, T0099, T0215, T0229
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0026, K0038, K0042, K0090, K0101, K0121, K0126, K0163, K0267, K0285, K0287, K0622
Capacités	S0027, S0059, S0138
Aptitudes	A0162, A0163, A0164, A0165, A0166, A0167, A0168

Nom de la fonction	Responsable du développement et de la gestion des effectifs cyber
ID de la fonction	OV-SPP-001
Spécialité	Planification et politique stratégiques (SPP)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Élabore des plans, des stratégies et des orientations concernant les effectifs cyber afin de répondre aux besoins en matière de ressources humaines, de personnel, de formation et d'éducation dans le domaine cyber et de tenir compte des modifications apportées à la politique, à la doctrine, au matériel, à la structure des forces et aux besoins en matière de formation et d'éducation dans ce domaine.
Tâches	T0001, T0004, T0025, T0044, T0074, T0094, T0099, T0116, T0222, T0226, T0341, T0352, T0355, T0356, T0362, T0363, T0364, T0365, T0368, T0369, T0372, T0373, T0374, T0375, T0376, T0384, T0387, T0388, T0390, T0391, T0408, T0425, T0429, T0437, T0441, T0445, T0472, T0481, T0505, T0506, T0529, T0533, T0536, T0537, T0552
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0072, K0101, K0127, K0146, K0147, K0168, K0169, K0204, K0215, K0233, K0234, K0241, K0243, K0309, K0311, K0313, K0335
Capacités	S0108, S0128
Aptitudes	A0023, A0028, A0033, A0037, A0042, A0053

Nom de la fonction	Planificateur de la politique et de la stratégie cyber
ID de la fonction	OV-SPP-002
Spécialité	Planification et politique stratégiques (SPP)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Élabore et actualise des plans, des stratégies et des politiques en matière de cybersécurité afin de soutenir et d'aligner les initiatives de l'organisation en matière de cybersécurité et de conformité aux réglementations.
Tâches	T0074, T0094, T0222, T0226, T0341, T0369, T0384, T0390, T0408, T0425, T0429, T0441, T0445, T0472, T0505, T0506, T0529, T0533, T0537
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0127, K0146, K0168, K0234, K0248, K0309, K0311, K0313, K0335, K0624
Capacités	S0176, S0250
Aptitudes	A0003, A0033, A0037

Nom de la fonction	Cadre dirigeant en cybersécurité
ID de la fonction	OV-EXL-001
Spécialité	Cadre en cybersécurité (EXL)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Prend des décisions et définit la vision et l'orientation des ressources et/ou des opérations d'une organisation dans le domaine cyber et en rapport avec la cybersécurité.
Tâches	T0001, T0002, T0004, T0006, T0025, T0066, T0130, T0134, T0135, T0148, T0151, T0227, T0229, T0229, T0248, T0254, T0263, T0264, T0282, T0337, T0356, T0429, T0445, T0509, T0763, T0871, T0872, T0927, T0928
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0070, K0106, K0314, K0296, K0147, K0624, K0628
Capacités	S0018, S0356, S0357, S0358, S0359
Aptitudes	A0033, A0070, A0085, A0094, A0105, A0106, A0116, A0117, A0118, A0119, A0129, A0130, A0130

Nom de la fonction	Responsable de programme
ID de la fonction	OV-PMA-001
Spécialité	Gestion de programme/projet et acquisition (PMA)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Dirige, coordonne, communique, intègre et est responsable de la réussite globale du programme, en veillant à l'aligner sur les priorités de l'agence ou de l'entreprise.
Tâches	T0066, T0072, T0174, T0199, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0377, T0379, T0407, T0412, T0414, T0415, T0481, T0493, T0551
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270
Capacités	S0038, S0372
Aptitudes	A0009, A0039, A0045, A0056,

Nom de la fonction	Chef de projet informatique
ID de la fonction	OV-PMA-002
Spécialité	Gestion de programme/projet et acquisition (PMA)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Gère des projets informatiques.
Tâches	T0072, T0174, T0196, T0199, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0340, T0354, T0370, T0377, T0379, T0389, T0394, T0407, T0412, T0414, T0415, T0481, T0493, T0551
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0012, K0043, K0047, K0048, K0059, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270
Capacités	S0038, S0372
Aptitudes	A0009, A0039, A0045, A0056

Nom de la fonction	Responsable du support produit
ID de la fonction	OV-PMA-003
Spécialité	Gestion de programme/projet et acquisition (PMA)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Gère l'ensemble des fonctions de support nécessaires pour mettre en œuvre et maintenir l'état de préparation et la capacité opérationnelle des systèmes et des composants.
Tâches	T0072, T0174, T0196, T0204, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0370, T0377, T0389, T0394, T0412, T0414, T0493, T0525, T0551, T0553
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0048, K0059, K0072, K0090, K0120, K0126, K0148, K0150, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0249, K0257, K0270
Capacités	S0038, S0372
Aptitudes	A0009, A0031, A0039, A0045, A0056

Nom de la fonction	Gestionnaire d'investissement/portefeuille informatique
ID de la fonction	OV-PMA-004
Spécialité	Gestion de programme/projet et acquisition (PMA)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Gère un portefeuille d'investissements informatiques conformes aux besoins globaux de la mission et aux priorités de l'entreprise.
Tâches	T0220, T0223, T0277, T0302, T0377, T0415, T0493, T0551
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0072, K0120, K0126, K0146, K0154, K0165, K0169, K0235, K0257, K0270
Capacités	S0372
Aptitudes	A0039

Nom de la fonction	Auditeur de projet informatique
ID de la fonction	OV-PMA-005
Spécialité	Gestion de programme/projet et acquisition (PMA)
Catégorie	Superviser et gouverner (OV)
Description de la fonction	Effectue des évaluations d'un projet informatique ou de ses composants individuels afin de déterminer leur conformité avec les normes publiées.
Tâches	T0072, T0207, T0208, T0223, T0256, T0389, T0412, T0415
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0047, K0048, K0072, K0090, K0120, K0126, K0148, K0154, K0165, K0169, K0198, K0200, K0235, K0257, K0270
Capacités	S0038, S0085, S0372
Aptitudes	A0056

B.4 Protéger et défendre (PR)

Nom de la fonction	Analyste en cyberdéfense
ID de la fonction	PR-CDA-001
Spécialité	Analyse cyberdéfense (CDA)
Catégorie	Protéger et défendre (PR)
Description de la fonction	Utilise les données collectées à partir de divers outils de cyberdéfense (par exemple, alertes IDS, pare-feu, journaux de trafic réseau) pour analyser les événements qui se produisent dans l'environnement afin de limiter les menaces.
Tâches	T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624
Capacités	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370
Aptitudes	A0010, A0015, A0066, A0123, A0128, A0159

Nom de la fonction	Spécialiste du support à l'infrastructure de cyberdéfense
ID de la fonction	PR-INF-001
Spécialité	Support d'infrastructure cyberdéfense (INF)
Catégorie	Protéger et défendre (PR)
Description de la fonction	Teste, met en œuvre, déploie, entretient et administre le matériel et les logiciels de l'infrastructure.
Tâches	T0042, T0180, T0261, T0335, T0348, T0420, T0438, T0483, T0486
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0033, K0042, K0044, K0058. K0061, K0062, K0104, K0106, K0135, K0157, K0179, K0205, K0258, K0274, K0324, K0332, K0334
Capacités	S0007, S0053, S0054, S0059, S0077, S0079, S0121, S0124, S0367
Aptitudes	A0123

Nom de la fonction	**Intervenant sur les incidents de cyberdéfense**
ID de la fonction	**PR-CIR-001**
Spécialité	**Réponse aux incidents (CIR)**
Catégorie	**Protéger et défendre (PR)**
Description de la fonction	Enquête, analyse et répond aux incidents cybers dans l'environnement du réseau ou de la zone de sécurité.
Tâches	T0041, T0047, T0161, T0163, T0164, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0395, T0503, T0510
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0230, K0259, K0287, K0332, K0565, K0624
Capacités	S0003, S0047, S0077, S0078, S0079, S0080, S0173, S0365
Aptitudes	A0121, A0128

Nom de la fonction	**Analyste de l'évaluation des vulnérabilités**
ID de la fonction	**PR-VAM-001**
Spécialité	**Évaluation et gestion des vulnérabilités (VAM)**
Catégorie	**Protéger et défendre (PR)**
Description de la fonction	Procède à l'évaluation des systèmes et des réseaux au sein de l'environnement réseau ou de la zone de sécurité et identifie les cas où ces systèmes/réseaux s'écartent des configurations acceptables, de la politique de la zone de sécurité ou de la politique locale. Mesure l'efficacité de l'architecture de défense en profondeur contre les vulnérabilités connues.
Tâches	T0010, T0028, T0138, T0142, T0188, T0252, T0549, T0550
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0021, K0033, K0044, K0056, K0061, K0068, K0070, K0089, K0106, K0139, K0161, K0162, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0332, K0342, K0344, K0624
Capacités	S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171, S0364, S0367
Aptitudes	A0001, A0044, A0120, A0123

B.5 Analyser (AN)

Nom de la fonction	Analyste des menaces et des alertes
ID de la fonction	AN-TWA-001
Spécialité	Analyse des menaces (TWA)
Catégorie	Analyser (AN)
Description de la fonction	Élabore des indicateurs cybers pour se tenir au courant de l'état de l'environnement opérationnel fortement évolutif. Recueille, traite, analyse et diffuse les évaluations des cybermenaces et des alertes.
Tâches	T0569, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0660, T0685, T0687, T0707, T0708, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0783, T0785, T0786, T0792, T0800, T0805, T0834
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0415, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0471, K0480, K0499, K0511, K0516, K0556, K0560, K0561, K0565, K0603, K0604, K0610, K0612, K0614
Capacités	S0194, S0196, S0203, S0211, S0218, S0227, S0228, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303
Aptitudes	A0013, A0066, A0072, A0080, A0082, A0083, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109

Nom de la fonction	Analyste exploitation
ID de la fonction	AN-EXP-001
Spécialité	Analyse données d'exploitation (EXP)
Catégorie	Analyser (AN)
Description de la fonction	Collabore à l'identification des lacunes en matière d'accès et de collecte qui peuvent être comblées par des activités de cybercollecte et/ou de préparation. Exploite toutes les ressources et techniques d'analyse autorisées pour pénétrer dans les réseaux ciblés.
Tâches	T0028, T0266, T0570, T0572, T0574, T0591, T0600, T0603, T0608, T0614, T0641, T0695, T0701, T0720, T0727, T0736, T0738, T0754, T0775, T0777
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0131, K0142, K0143, K0177, K0224, K0349, K0362, K0417, K0444, K0471, K0560, K0351, K0354, K0368, K0371, K0376, K0379, K0388, K0393, K0394, K0397, K0418, K0430, K0443, K0447, K0451, K0470, K0473, K0484, K0487, K0489, K0509, K0510, K0523, K0529, K0535, K0544, K0557, K0559, K0608
Capacités	S0066, S0184, S0199, S0200, S0201, S0204, S0207, S0214, S0223, S0236, S0237, S0239, S0240, S0245, S0247, S0258, S0260, S0264, S0269, S0279, S0286, S0290, S0294, S0300
Aptitudes	A0013, A0066, A0080, A0084, A0074, A0086, A0092, A0093, A0104

Nom de la fonction	**Analyste multi-sources**
ID de la fonction	**AN-ASA-001**
Spécialité	**Analyse multi-sources (ASA)**
Catégorie	**Analyser (AN)**
Description de la fonction	Analyse les données/informations provenant d'une ou de plusieurs sources afin de préparer l'environnement, de répondre aux demandes d'informations et de soumettre les exigences en matière de collecte et de production de renseignements pour soutenir la planification et les opérations.
Tâches	T0569, T0582, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0642, T0660, T0678, T0685, T0686, T0687, T0707, T0708, T0710, T0713, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0771, T0782, T0783, T0785, T0786, T0788, T0789, T0792, T0797, T0800, T0805, T0834
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0221, K0349, K0362, K0444, K0471, K0560, K0377, K0392, K0395, K0405, K0409, K0427, K0431, K0436, K0437, K0440, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0480, K0511, K0516, K0556, K0561, K0565, K0603, K0604, K0610, K0612, K0614, K0357, K0410, K0457, K0465, K0507, K0533, K0542, K0549, K0551, K0577, K0598
Capacités	S0194, S0203, S0211, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303, S0189, S0254, S0360
Aptitudes	A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0085, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0108, A0109

Nom de la fonction	**Spécialiste de l'évaluation des missions**
ID de la fonction	**AN-ASA-002**
Spécialité	**Analyse multi-sources (ASA)**
Catégorie	**Analyser (AN)**
Description de la fonction	Élabore des plans d'évaluation et des mesures de performance/efficacité. Réalise des évaluations de l'efficacité stratégique et opérationnelle, selon les besoins, pour les événements cybers. Détermine si les systèmes ont fonctionné comme prévu et contribue à la détermination de l'efficacité opérationnelle.
Tâches	T0582, T0583, T0585, T0586, T0588, T0589, T0593, T0597, T0611, T0615, T0617, T0624, T0660, T0661, T0663, T0678, T0684, T0685, T0686, T0707, T0718, T0748, T0749, T0752, T0758, T0761, T0782, T0783, T0785, T0786, T0788, T0789, T0793, T0797, T0834
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0410, K0414, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0457, K0460, K0464, K0465, K0469, K0471, K0480, K0507, K0511, K0516, K0549, K0551, K0556, K0560, K0561, K0565, K0598, K0603, K0604, K0610, K0612, K0614
Capacités	S0189, S0194, S0203, S0211, S0216, S0218, S0227, S0228, S0229, S0249, S0254, S0256, S0271, S0278, S0285, S0288, S0289, S0292, S0296, S0297, S0303, S0360
Aptitudes	A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109, A0085, A0108

Nom de la fonction	Développeur de cibles
ID de la fonction	AN-TGT-001
Spécialité	Cibles (TGT)
Catégorie	Analyser (AN)
Description de la fonction	Analyse les systèmes cibles, constitue et/ou tient à jour des dossiers électroniques sur les cibles, en y incluant des données provenant de la préparation de l'environnement et/ou de sources de renseignement internes ou externes. Assure la coordination avec les activités de ciblage des partenaires et les organisations de renseignement, et présente des cibles candidates à des fins d'examen et de validation.
Tâches	T0597, T0617, T0707, T0582, T0782, T0797, T0588, T0624, T0661, T0663, T0684, T0642, T0710, T0561, T0594, T0599, T0633, T0650, T0652, T0688, T0717, T0731, T0744, T0769, T0770, T0776, T0781, T0790, T0794, T0798, T0799, T0802, T0815, T0824, T0835
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0142, K0349, K0362, K0444, K0471, K0560, K0392, K0395, K0409, K0427, K0431, K0436, K0437, K0440, K0445, K0446, K0449, K0460, K0464, K0516, K0556, K0561, K0565, K0603, K0604, K0614, K0457, K0465, K0507, K0549, K0551, K0598, K0417, K0458, K0357, K0533, K0542, K0351, K0379, K0473, K0381, K0402, K0413, K0426, K0439, K0461, K0466, K0478, K0479, K0497, K0499, K0543, K0546, K0547, K0555
Capacités	S0194, S0203, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0189, S0228, S0216, S0292, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0302, S0360, S0361
Aptitudes	A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

Nom de la fonction	Analyste réseau cibles
ID de la fonction	AN-TGT-002
Spécialité	Cibles (TGT)
Catégorie	Analyser (AN)
Description de la fonction	Effectue une analyse avancée des données collectées et des données provenant de sources publiques afin d'assurer le suivi des cibles, d'établir le profil des cibles et de leurs activités et de mettre au point des techniques permettant d'obtenir davantage d'informations sur ces dernières. Détermine la manière dont les cibles communiquent, se déplacent, opèrent et évoluent en se basant sur la connaissance des technologies des cibles, des réseaux numériques et des applications qu'ils contiennent.
Tâches	T0617, T0707, T0582, T0797, T0624, T0710, T0599, T0650, T0802, T0595, T0606, T0607, T0621, T0653, T0692, T0706, T0715, T0722, T0745, T0765, T0767, T0778, T0803, T0807
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0177, K0349, K0362, K0444, K0471, K0392, K0395, K0431, K0436, K0440, K0445, K0449, K0516, K0379, K0473, K0413, K0439, K0479, K0547, K0487, K0544, K0559, K0389, K0403, K0424, K0442, K0462, K0472, K0483, K0499, K0500, K0520, K0550, K0567, K0592, K0599, K0600
Capacités	S0194, S0203, S0229, S0256, S0228, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0177, S0178, S0181, S0183, S0191, S0197, S0217, S0219, S0220, S0225, S0231, S0234, S0244, S0246, S0259, S0261, S0262, S0263, S0268, S0277, S0280, S0291, S0301
Aptitudes	A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

Nom de la fonction	Analyste linguistique pluridisciplinaire
ID de la fonction	AN-LNG-001
Spécialité	Analyse linguistique (LNG)
Catégorie	Analyser (AN)
Description de la fonction	Applique son expertise en matière de langue et de culture à la cible, à la menace et aux connaissances techniques pour traiter, analyser et/ou diffuser des informations de renseignement tirées de la langue, de la voix et/ou de documents graphiques. Crée et tient à jour des bases de données et des outils de travail spécifiques à une langue afin de faciliter l'exécution d'actions cybers et d'assurer le partage des connaissances essentielles. Fournit une expertise en la matière dans le cadre de projets interdisciplinaires ou à forte intensité de langues étrangères.
Tâches	T0650, T0606, T0715, T0745, T0761, T0837, T0838, T0839, T0840, T0841, T0842, T0843, T0844, T0845, T0846, T0847, T0848, T0849, T0850, T0851, T0852, T0853, T0854, T0855, T0856, T0857, T0858, T0859, TO860
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0143, K0177, K0431, K0449, K0413, K0487, K0462, K0520, K0550, K0567, K0599, K0600, K0417, K0377, K0356, K0359, K0391, K0396, K0398, K0407, K0416, K0476, K0488, K0491, K0493, K0499, K0524, K0532, K0539, K0540, K0541, K0545, K0548, K0564, K0571, K0574, K0579, K0596, K0606, K0607
Capacités	S0187, S0217, S0244, S0259, S0262, S0277, S0218, S0184, S0290, S0179, S0188, S0193, S0195, S0198, S0210, S0212, S0215, S0224, S0226, S0232, S0233, S0235, S0241, S0251, S0253, S0265, S0283, S0284
Aptitudes	A0013, A0089, A0071, A0103

B.6 Collecter et exploiter (CO)

Nom de la fonction	Gestionnaire de collecte multi-sources
ID de la fonction	CO-CLO-001
Spécialité	Opérations de collecte (CLO)
Catégorie	Collecter et exploiter (CO)
Description de la fonction	Identifie les autorités et l'environnement de la collecte ; intègre les exigences prioritaires en matière d'information dans la gestion de la collecte ; élabore des concepts pour répondre à l'intention des dirigeants. Détermine les capacités des moyens de collecte disponibles, identifie les nouvelles capacités de collecte, élabore et diffuse des plans de collecte. Surveille l'exécution des tâches de collecte afin de garantir l'exécution efficace du plan de collecte.
Tâches	T0562, T0564, T0568, T0573, T0578, T0604, T0605, T0625, T0626, T0631, T0632, T0634, T0645, T0646, T0647, T0649, T0651, T0657, T0662, T0674, T0681, T0683, T0698, T0702, T0714, T0716, T0721, T0723, T0725, T0734, T0737, T0750, T0753, T0755, T0757, T0773, T0779, T0806, T0809, T0810, T0811, T0812, T0814, T0820, T0821, T0827
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0431, K0449, K0417, K0579, K0596, K0444, K0471, K0392, K0395, K0440, K0445, K0516, K0560, K0427, K0446, K0561, K0565, K0405, K0480, K0610, K0612, K0353, K0361, K0364, K0380, K0382, K0383, K0386, K0387, K0390, K0401, K0404, K0412, K0419, K0425, K0435, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0482, K0492, K0495, K0496, K0498, K0503, K0505, K0513, K0521, K0522, K0526, K0527, K0552, K0553, K0554, K0558, K0562, K0563, K0569, K0570, K0580, K0581, K0583, K0584, K0587, K0588, K0601, K0605, K0613
Capacités	S0238, S0304, S0305, S0311, S0313, S0316, S0317, S0324, S0325, S0327, S0328, S0330, S0332, S0334, S0335, S0336, S0339, S0342, S0344, S0347, S0351, S0352, S0362
Aptitudes	A0069, A0070, A0076, A0078, A0079

Nom de la fonction	**Gestionnaire des besoins pour la collecte multi-sources**
ID de la fonction	**CO-CLO-002**
Spécialité	**Opérations de collecte (CLO)**
Catégorie	**Collecter et exploiter (CO)**
Description de la fonction	Évalue les opérations de collecte et élabore des stratégies d'exigences en matière de collecte fondées sur les effets, en utilisant les sources et les méthodes disponibles pour améliorer la collecte. Élabore, traite, valide et coordonne la présentation des besoins en matière de collecte. Évalue les performances des moyens de collecte et des opérations de collecte.
Tâches	T0564, T0568, T0578, T0605, T0651, T0714, T0725, T0734, T0809, T0810, T0811, T0565, T0577, T0580, T0596, T0602, T0613, T0668, T0673, T0675, T0682, T0689, T0693, T0694, T0730, T0746, T0780, T0819, T0822, T0830, T0831, T0832, T0833
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0353, K0361, K0364, K0380, K0382, K0383, K0384, K0386, K0387, K0390, K0395, K0401, K0404, K0412, K0417, K0419, K0421, K0425, K0427, K0431, K0435, K0444, K0445, K0446, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0480, K0482, K0492, K0495, K0496, K0498, K0505, K0513, K0516, K0521, K0526, K0527, K0552, K0554, K0558, K0560, K0561, K0562, K0563, K0565, K0568, K0569, K0570, K0579, K0580, K0581, K0584, K0587, K0588, K0596, K0605, K0610, K0612
Capacités	S0304, S0305, S0316, S0317, S0327, S0330, S0334, S0335, S0336, S0339, S0344, S0347, S0352, S0329 S0337, S0346, S0348, S0353, S0362
Aptitudes	A0069, A0070, A0078

Nom de la fonction	Planificateur en matière de renseignement cyber
ID de la fonction	**CO-OPL-001**
Spécialité	**Planification opérationnelle cyber (OPL)**
Catégorie	**Collecter et exploiter (CO)**
Description de la fonction	Élabore des programmes de renseignement détaillés pour répondre aux exigences des opérations cybers. Collabore avec les planificateurs des opérations cybers afin d'identifier, de valider et d'établir les besoins en matière de collecte et d'analyse. Participe à la sélection, à la validation, à la synchronisation et à l'exécution des actions cybers. Synchronise les activités de renseignement pour soutenir les objectifs de l'organisation dans le cyberespace.
Tâches	T0734, T0563, T0575, T0576, T0579, T0581, T0587, T0590, T0592, T0601, T0627, T0628, T0630, T0636, T0637, T0638, T0639, T0640, T0648, T0656, T0659, T0667, T0670, T0676, T0680, T0690, T0691, T0705, T0709, T0711, T0719, T0726, T0728, T0733, T0735, T0739, T0743, T0760, T0763, T0772, T0784, T0801, T0808, T0816, T0836
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0120, K0431, K0417, K0444, K0395, K0445, K0560, K0427, K0446, K0561, K0565, K0480, K0610, K0612, K0435, K0471, K0392, K0440, K0405, K0377, K0349, K0362, K0436, K0379, K0403, K0460, K0464, K0556, K0603, K0614, K0465, K0507, K0598, K0511, K0414, K0577, K0347, K0350, K0352, K0355, K0358, K0399, K0400, K0408, K0411, K0422, K0432, K0455, K0456, K0459, K0463, K0494, K0499, K0501, K0502, K0504, K0506, K0508, K0512, K0514, K0517, K0518, K0519, K0525, K0538, K0566, K0572, K0575, K0578, K0582, K0585, K0586, K0589, K0590, K0591, K0593, K0594, K0595, K0599, K0602
Capacités	S0218, S0203, S0249, S0278, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0272, S0273, S0306, S0307, S0308, S0309, S0310, S0312, S0314, S0315, S0318, S0319, S0320, S0321, S0322, S0323, S0331, S0333, S0338, S0340, S0341, S0343, S0345, S0350, S0360
Aptitudes	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105, A0160

Nom de la fonction	Planificateur d'opérations cyber
ID de la fonction	CO-OPL-002
Spécialité	Planification opérationnelle cyber (OPL)
Catégorie	Collecter et exploiter (CO)
Description de la fonction	Élabore des plans détaillés pour la conduite ou le soutien des opérations cybers concernées, en collaboration avec d'autres planificateurs, opérateurs et/ou analystes. Participe à la sélection, à la validation et à la synchronisation des cibles et permet l'intégration pendant l'exécution des actions cybers.
Tâches	T0734, T0563, T0579, T0581, T0592, T0627, T0628, T0640, T0648, T0667, T0670, T0680, T0690, T0719, T0733, T0739, T0743, T0763, T0772, T0801, T0836, T0571, T0622, T0635, T0654, T0655, T0658, T0665, T0672, T0679, T0699, T0703, T0704, T0732, T0741, T0742, T0747, T0764, T0787, T0791, T0795, T0813, T0823
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0347, K0349, K0350, K0352, K0362, K0377, K0379, K0392, K0395, K0399, K0400, K0403, K0408, K0411, K0414, K0417, K0422, K0431, K0432, K0435, K0436, K0444, K0445, K0446, K0455, K0464, K0465, K0471, K0480, K0494, K0497, K0499, K0501, K0502, K0504, K0506, K0507, K0508, K0511, K0512, K0514, K0516, K0518, K0519, K0525, K0534, K0538, K0556, K0560, K0561, K0565 K0566, K0572, K0576, K0582, K0585, K0586, K0589, K0590, K0593, K0594, K0597, K0598, K0599, K0603, K0610, K0612, K0614
Capacités	S0218, S0249, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0273, S0309, S0312, S0322, S0333, S0209, S0326, S0349, S0360
Aptitudes	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

Nom de la fonction	Planificateur de l'intégration des partenaires
ID de la fonction	CO-OPL-003
Spécialité	Planification opérationnelle cyber (OPL)
Catégorie	Collecter et exploiter (CO)
Description de la fonction	S'efforce de faire progresser la coopération entre les partenaires des opérations informatiques par-delà les frontières organisationnelles ou nationales. Contribue à l'intégration des équipes cybers des partenaires en fournissant des orientations, des ressources et en collaborant à l'élaboration de bonnes pratiques et en facilitant le soutien organisationnel en vue d'atteindre les objectifs dans le cadre d'actions cybers intégrées.
Tâches	T0581, T0582, T0627, T0670, T0739, T0763, T0772, T0836, T0571, T0635, T0665, T0699, T0732, T0747, T0764, T0787, T0795, T0823, T0601, T0760, T0784, T0629, T0666, T0669, T0671, T0700, T0712, T0729, T0759, T0766, T0817, T0818, T0825, T0826
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0431, K0417, K0444, K0395, K0435, K0392, K0377, K0362, K0436, K0379, K0403, K0465, K0507, K0598, K0511, K0414, K0350, K0400, K0408, K0411, K0422, K0432, K0455, K0499, K0501, K0504, K0506, K0508, K0512, K0514, K0538, K0585, K0599
Capacités	S0218, S0249, S0296, S0297, S0185, S0186, S0213, S0250, S0326, S0360
Aptitudes	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

Nom de la fonction	**Opérateur cyber**
ID de la fonction	**CO-OPS-001**
Spécialité	**Opérations cybers (OPS)**
Catégorie	**Collecter et exploiter (CO)**
Description de la fonction	Effectue la collecte, le traitement et/ou la géolocalisation de systèmes afin d'exploiter, de localiser et/ou de suivre des cibles d'intérêt. Navigue sur le réseau, effectue des analyses tactiques et, selon les instructions, exécute des opérations sur le réseau.
Tâches	T0566, T0567, T0598, T0609, T0610, T0612, T0616, T0618, T0619, T0620, T0623, T0643, T0644, T0664, T0677, T0696, T0697, T0724, T0740, T0756, T0768, T0774, T0796, T0804, T0828, T0829
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0021, K0051, K0109, K0142, K0224, K0363, K0372, K0373, K0375, K0379, K0403, K0406, K0420, K0423, K0428, K0427, K0429, K0430, K0433, K0438, K0440, K0452, K0468, K0481, K0485, K0486, K0480, K0516, K0528, K0530, K0531, K0536, K0560, K0565, K0573, K0608, K0609
Capacités	S0062, S0183, S0236, S0182, S0190, S0192, S0202, S0206, S0221, S0242, S0243, S0252, S0255, S0257, S0266, S0267, S0270, S0275, S0276, S0281, S0282, S0293, S0295, S0298, S0299, S0363
Aptitudes	A0095, A0097, A0099, A0100

B.7 Enquêter (IN)

Nom de la fonction	Enquêteur en cybercriminalité
ID de la fonction	IN-INV-001
Spécialité	Cyber investigation (INV)
Catégorie	Enquêter (IN)
Description de la fonction	Identifie, collecte, examine et préserve les preuves en utilisant des techniques d'analyse et d'enquête contrôlées et documentées.
Tâches	[**Remarque** : Certaines de ces activités ne peuvent être réalisées que par du personnel disposant d'une autorité en matière de maintien de l'ordre ou de contre-espionnage.] T0031, T0059, T0096, T0103, T0104, T0110, T0112, T0113, T0114, T0120, T0193, T0225, T0241, T0343, T0346, T0360, T0386, T0423, T0430, T0433, T0453, T0471, T0479, T0523
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0046, K0070, K0107, K0110, K0114, K0118, K0123, K0125, K0128, K0144, K0155, K0156, K0168, K0209, K0231, K0244, K0251, K0351, K0624
Capacités	S0047, S0068, S0072, S0086
Aptitudes	A0174, A0175

Nom de la fonction	Analyste criminalistique dans le domaine judiciaire et du contre-espionnage
ID de la fonction	IN-FOR-001
Spécialité	Investigation numérique (FOR)
Catégorie	Enquêter (IN)
Description de la fonction	Mène des enquêtes détaillées sur les délits informatiques en établissant des preuves documentaires ou physiques, notamment des supports numériques et des journaux associés à des incidents de cyber intrusion.
Tâches	T0059, T0096, T0220, T0308, T0398, T0419, T0401, T0403, T0411, T0425
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0021, K0042, K0060, K0070, K0077, K0078, K0107, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0305, K0624
Capacités	S0032, S0046, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093
Aptitudes	A0005, A0175

Nom de la fonction	**Analyste criminalistique en cyberdéfense**
ID de la fonction	**IN-FOR-002**
Spécialité	**Investigation numérique (FOR)**
Catégorie	**Enquêter (IN)**
Description de la fonction	Analyse les preuves numériques et enquête sur les incidents de sécurité informatique pour en tirer des informations utiles à l'atténuation des vulnérabilités des systèmes/réseaux.
Tâches	T0027, T0036, T0048, T0049, T0075, T0087, T0103, T0113, T0165, T0167, T0168, T0172, T0173, T0175, T0179, T0182, T0190, T0212, T0216, T0238, T0240, T0241, T0253, T0279, T0285, T0286, T0287, T0288, T0289, T0312, T0396, T0397, T0398, T0399, T0400, T0401, T0432, T0532, T0546
Connaissances	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0042, K0060, K0070, K0077, K0078, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0224, K0254, K0255, K0301, K0304, K0347, K0624
Capacités	S0032, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093, S0131, S0132, S0133, S0156
Aptitudes	A0005, A0043

Annexe C – Outils de développement des ressources humaines

C.1 La Cybersecurity Workforce Development Toolkit du DHS

La boîte à outils du DHS pour le développement des ressources humaines en cybersécurité (Cybersecurity Workforce Development Toolkit ou CWDT) [8] aide toute organisation à comprendre ses besoins en ressources humaines et en personnel dans le domaine de la cybersécurité afin de protéger ses informations, ses clients et ses réseaux. Ce kit comprend des modèles de parcours de carrière en cybersécurité et des outils de recrutement permettant de recruter et de conserver les meilleurs talents dans le domaine de la cybersécurité. Le CWDT fournit des outils pour aider à comprendre les risques liés aux effectifs en cybersécurité d'une organisation et à en faire l'inventaire. Les outils du CWDT s'appuient sur les spécialités, les KSA et les tâches du référentiel NICE. Le CWDT note que la première étape de la préparation à la constitution d'un effectif de cybersécurité est une vision commune de l'organisation de son effectif de cybersécurité. Cette vision commune aide les dirigeants à s'adapter à l'évolution de l'environnement et fournit des données qui permettent de mieux ajuster les ressources, d'observer les schémas de travail et de mettre en évidence les zones de risque potentiel. Cette compréhension est particulièrement importante dans l'environnement en constante évolution de la cybersécurité. Le CWDT comprend un modèle de maturité des capacités de planification des effectifs de cybersécurité (CMM), un outil d'auto-évaluation permettant à une organisation d'évaluer la maturité de ses capacités de planification des effectifs de cybersécurité.

Le (CWDT) propose des profils comme guide pour se concentrer sur la fidélisation du personnel à tous les niveaux, qu'il s'agisse de débutants, de personnes en milieu de carrière ou de professionnels chevronnés de la cybersécurité.

C.1.1 Niveaux de compétence et parcours professionnels

L'élaboration et la diffusion de plans de carrière auprès des employés les aideront à identifier leurs niveaux de compétence et à progresser dans le domaine de la cybersécurité.

Le CWDT propose un processus en trois étapes pour définir des parcours professionnels dans le domaine de la cybersécurité au sein de l'organisation.

- Étape 1 - Se familiariser avec les niveaux de compétence et examiner des exemples de parcours professionnels.
- Étape 2 - Utiliser un modèle du CWDT pour créer des parcours professionnels personnalisés en matière de cybersécurité pour votre organisation en remplissant les rubriques "*Suggested Experience & Credentials*", "*Competencies and Sample Skills / KSAs*" et "*Suggested Training & Development Activities*".
- Étape 3 - Partager les parcours professionnels avec les responsables et le personnel chargés de la cybersécurité.

C.2 Outil Baldrige Cybersecurity Excellence Builder Tool

Une fois qu'une organisation a déterminé ses besoins en matière de cybersécurité (par exemple au moyen d'un audit de cybersécurité ou d'une auto-évaluation interne), elle peut s'appuyer sur le

référentiel NICE pour identifier les fonctions et les tâches qui lui permettront de répondre à ces besoins. Alors que des termes généraux, tels que "professionnels de la cybersécurité", ont toujours été utilisés pour mesurer les besoins, la précision apportée par le référentiel NICE constitue une meilleure approche pour décrire les dizaines de fonctions professionnelles distinctes qui sont nécessaires. En identifiant les compétences requises et disponibles, et en identifiant les écarts entre les compétences requises et disponibles, l'organisation peut identifier les besoins critiques. Le référentiel NICE aide une organisation à répondre aux questions suivantes, tirées de l'outil Baldrige Cybersecurity Excellence Builder Tool [9], concernant le maintien d'un environnement de travail efficace et favorable à la réalisation de ses objectifs en matière de cybersécurité :

- Comment évaluez-vous les capacités de votre personnel et ses besoins en matière de cybersécurité ?
- Comment organisez-vous et gérez-vous votre personnel chargé de la cybersécurité afin de définir les rôles et les responsabilités ?
- Comment préparez-vous votre personnel à l'évolution des besoins aussi bien qualitatifs que quantitatifs en matière de cybersécurité ?

Alors que de plus en plus d'organisations évaluent leur main-d'œuvre en cybersécurité, le lexique commun du référentiel NICE permet d'évaluer les capacités et les aptitudes de plusieurs organisations, secteurs industriels et régions.

C.3 Outil Position Description Drafting Tool

L'outil DHS Cyberskills Management Support Initiative PushbuttonPD Tool du DHS [10] permet aux responsables, aux superviseurs et aux spécialistes des ressources humaines de rédiger rapidement une description de poste d'un employé fédéral sans avoir besoin d'une formation approfondie ou de connaissances préalables en matière de classification des postes. Il est conçu pour présenter les termes de plusieurs sources et normes faisant autorité en matière de fonctions, de tâches et de KSA, pour recueillir rapidement les besoins du responsable des ressources humaines et pour les présenter dans un dossier d'embauche consistant qui peut être facilement intégré dans les processus de ressources humaines existants de l'agence. Toute organisation peut expérimenter l'outil PushbuttonPD pour voir comment il intègre le référentiel NICE dans une description de poste.

Annexe D – Correspondance avec les documents d'orientation et les lignes directrices

L'objectif stratégique n° 3 du NICE (Guide Career Development and Workforce Planning) vise à aider les employeurs à répondre aux demandes du marché et à améliorer le recrutement, l'embauche, le développement et la fidélisation des talents dans le domaine de la cybersécurité. L'un des objectifs de ce but stratégique est de publier le référentiel NICE, de le faire connaître et d'en encourager l'adoption. Par "adoption", on entend ici l'utilisation du référentiel NICE comme ressource de référence pour les actions liées aux ressources humaines, à la formation et à l'éducation dans le domaine de la cybersécurité.

L'un des moyens d'encourager l'adoption du référentiel NICE consiste à inciter les auteurs de documents d'orientation ou de lignes directrices sur la cybersécurité à faire référence à certains éléments du référentiel NICE dans le contenu de leurs documents. L'annexe D présente des exemples de correspondances entre publications susceptibles d'encourager l'adoption du référentiel NICE.

D.1 Référentiel de Cybersécurité

En 2014, le NIST a publié le référentiel pour l'amélioration de la cybersécurité des infrastructures critiques (Framework for Improving Critical Infrastructure Cybersecurity) [11], communément appelé "référentiel de cybersécurité" (Cybersecurity Framework). Développé en réponse à l'Executive Order (EO) 13636 [12], le Cybersecurity Framework fournit une approche basée sur la performance et l'efficacité économique pour aider les organisations à identifier, évaluer et gérer les risques liés à la cybersécurité. Il a été élaboré dans le cadre d'une série d'ateliers publics organisés par le NIST afin de mieux comprendre quelles normes et méthodologies sont utiles pour parvenir à une gestion efficace des risques, et comment les bonnes pratiques peuvent être mises en œuvre spontanément pour améliorer la cybersécurité.

La feuille de route du NIST pour l'amélioration de la cybersécurité des infrastructures critiques (*NIST Roadmap for Improving Critical Infrastructure Cybersecurity*) [13] qui accompagne le référentiel de cybersécurité, souligne la nécessité de disposer de personnel qualifié pour répondre aux besoins particuliers des infrastructures critiques en matière de cybersécurité. Elle reconnaît qu'au fur et à mesure de l'évolution des menaces de cybersécurité et des environnements technologiques, le personnel doit continuer à s'adapter pour concevoir, développer, mettre en œuvre, maintenir et améliorer en permanence les pratiques nécessaires en matière de cybersécurité.

Le référentiel de cybersécurité se compose de trois parties : La base du référentiel, les niveaux de mise en œuvre du référentiel et les profils du référentiel. Chaque partie du "Cybersecurity Framework" renforce le lien entre les moteurs de l'entreprise et les activités de cybersécurité. Les éléments de base du référentiel s'articulent de la manière suivante :

- **Les fonctions** organisent les activités de cybersécurité de base à leur niveau le plus élevé. Ces fonctions - identifier, protéger, détecter, répondre et récupérer - sont décrites en détail ci-dessous.

- **Les catégories** sont les subdivisions d'une fonction en groupes d'objectifs de cybersécurité étroitement liés aux besoins et activités programmatiques.
- **Les sous-catégories** subdivisent une catégorie en résultats spécifiques d'activités techniques et/ou de gestion. Elles fournissent un ensemble de résultats qui, sans être exhaustif, contribue à la réalisation des résultats de chaque catégorie.
- **Les références** informatives sont des sections spécifiques de normes, de lignes directrices et de pratiques communes aux secteurs des infrastructures critiques qui illustrent une méthode pour atteindre les résultats associés à chaque sous-catégorie. Les références informatives présentées dans la base du référentiel sont illustratives et non exhaustives. Elles représentent les orientations intersectorielles les plus fréquemment citées au cours du processus d'élaboration du cadre.

Les fonctions de base contribuent chacune à une compréhension de haut niveau des besoins de l'organisation en matière de cybersécurité :

- **Identifier (ID)** - Développer la compréhension de l'organisation pour gérer les risques de cybersécurité pour les systèmes, les actifs, les données et les capacités.
- **Protéger (PR)** - Développer et mettre en œuvre les mesures de protection appropriées pour assurer la fourniture des services d'infrastructure critiques.
- **Détecter (DE)** - Développer et mettre en œuvre les activités appropriées pour identifier l'occurrence d'un événement de cybersécurité.
- **Répondre (RS)** - Développer et mettre en œuvre les activités appropriées pour prendre des mesures en cas de détection d'un événement de cybersécurité.
- **Récupérer (RC)** - Développer et mettre en œuvre les activités appropriées pour maintenir les plans de résilience et restaurer les capacités ou les services qui ont été altérés à la suite d'un événement de cybersécurité.

À bien des égards, ces fonctions sont en corrélation avec les catégories du référentiel NICE. Tableau 8 décrit les relations entre les fonctions du référentiel de cybersécurité et les catégories du référentiel NICE.

Tableau 8 - Correspondance entre les catégories du référentiel NICE et les fonctions du référentiel de cybersécurité

Catégorie du référentiel NICE	Description de la catégorie	Fonction(s) correspondante du référentiel de Cybersécurité
Provisionnement sécurisé (SP)	Conceptualise, conçoit, fait l'acquisition et/ou construit des systèmes de technologie de l'information (TI) sécurisés, en étant responsable de certains aspects du développement des systèmes et/ou des réseaux.	Identifier (ID), Protéger (PR)
Exploitation et maintenance (OM)	Fournir le support, l'administration et la maintenance nécessaires pour assurer l'efficacité et l'efficience des performances et de la sécurité des systèmes de technologie de l'information (TI).	Protéger (PR), Détecter (DE)
Superviser et gouverner (OV)	Assurer le leadership, la gestion, la conduite ou le développement et la défense des intérêts de l'organisation afin qu'elle puisse mener efficacement ses activités dans le domaine de la cybersécurité.	Identifier (ID), Protéger (PR), Détecter (DE), Récupérer (RC)
Protéger et défendre (PR)	Identifier, analyser et réduire les menaces qui pèsent sur les systèmes et/ou réseaux informatiques internes.	Protéger (PR), Détecter (DE), Répondre (RS)
Analyser (AN)	Examiner et évaluer de manière très précise les informations reçues en matière de cybersécurité afin de déterminer leur utilité pour le renseignement.	Identifier (ID), Détecter (DE), Répondre (RS)
Collecter et exploiter (CO)	Mener des opérations spécifiques de déni et de tromperie et collecter des informations sur la cybersécurité susceptibles d'être utilisées à des fins de renseignement.	Détecter (DE), Protéger (PR), Répondre (RS)
Enquêter (IN)	Enquêter sur des événements ou des délits relevant de la cybersécurité et liés à des systèmes informatiques, à des réseaux et à des preuves numériques.	Détecter (DE), Répondre (RS), Récupérer (RC)

D.1.2 Exemple d'intégration du référentiel de cybersécurité au référentiel NICE

Bien que le référentiel de cybersécurité et le référentiel NICE aient été élaborés séparément, ils se complètent l'un l'autre en décrivant une approche hiérarchique pour atteindre les objectifs de cybersécurité. Prenons l'exemple suivant :

La fonction **Répondre** du référentiel de cybersécurité comprend une catégorie **Atténuation (RS.MI)**. Cette catégorie comprend une sous-catégorie, **RS.MI-2**, qui indique que les "incidents

sont atténués". Bien que le référentiel de cybersécurité décrive ce résultat et fournisse plusieurs références informatives concernant les contrôles de sécurité permettant de l'atteindre, il ne fournit aucune indication sur la personne qui devrait être responsable de l'atteinte de ce résultat, ni sur les compétences clefs en matière de sécurité qui s'appliqueraient.

En examinant le référentiel NICE, nous identifions la fonction **Intervenant sur les incidents de cyberdéfense (PR-CIR-001)** dans la catégorie **Protéger et Défendre (PR)**, dans la spécialité **Réponse aux incidents (CIR)**. Nous pouvons examiner la description de cette fonction pour nous assurer qu'elle est conforme au résultat **RS.MI-2** du référentiel de cybersécurité :

> Réagir aux perturbations dans le domaine concerné afin d'atténuer les menaces immédiates et potentielles. Utilise des approches d'atténuation, de préparation, de réponse et de récupération pour maximiser la survie des personnes, la préservation des biens et la sécurité de l'information. Étudie et analyse les activités d'intervention pertinentes et évalue l'efficacité des pratiques existantes et les améliorations à y apporter.
>
> Enquêter, analyser et répondre aux incidents de cybersécurité dans l'environnement du réseau ou de l'enclave.

Annexe A du présent document nous apprend que la personne dont le poste comprend cette fonction pourrait être amenée à effectuer un grand nombre des tâches suivantes, qui correspondent au résultat souhaité du référentiel de cybersécurité :

- **T0041** - Coordonner et fournir un soutien technique expert aux techniciens de cyberdéfense à l'échelle de l'entreprise pour résoudre les incidents de cyberdéfense.
- **T0047** - Corréler les données relatives aux incidents afin d'identifier les vulnérabilités spécifiques et formuler des recommandations permettant d'y remédier rapidement.
- **T0161** - Analyser les fichiers journaux provenant de diverses sources (par exemple, journaux d'hôtes individuels, journaux de trafic réseau, journaux de pare-feu et journaux de systèmes de détection d'intrusion [IDS]) afin d'identifier d'éventuelles menaces pour la sécurité du réseau.
- **T0163** - Effectuer le tri des incidents de cyberdéfense, notamment en déterminant la portée, l'urgence et l'impact potentiel, en identifiant la vulnérabilité spécifique et en formulant des recommandations permettant de remédier rapidement à la situation.
- **T0170** - Effectuer une investigation numérique légale initiale des images et inspecter les systèmes de l'entreprise afin de déterminer les mesures d'atténuation ou de correction possibles.
- **T0175** - Effectuer des tâches de traitement des incidents de cyberdéfense en temps réel (par exemple, investigations numériques légales, corrélation et suivi des intrusions, analyse des menaces et remédiation directe des systèmes) afin de soutenir les équipes de réaction aux incidents (IRT) déployables.

- **T0214** - Recevoir et analyser les alertes réseau provenant de diverses sources au sein de l'entreprise et déterminer les causes possibles de ces alertes.
- **T0233** - Suivre et documenter les incidents de cyberdéfense, de la détection initiale à la résolution finale.
- **T0246** - Rédiger et publier des techniques de cyberdéfense, des orientations et des rapports sur les constatations d'incidents à l'intention des parties concernées.
- **T0262** - Utiliser les principes et pratiques approuvés de défense en profondeur (par exemple, défense en plusieurs endroits, défenses en couches, robustesse de la sécurité).
- **T0278** - Recueillir les artefacts d'intrusion (par exemple, code source, logiciels malveillants, chevaux de Troie) et utiliser les données découvertes pour permettre l'atténuation des incidents potentiels de cybersécurité au sein de l'entreprise.
- **T0279** - Servir d'expert technique et de liaison avec le personnel chargé de l'application de la loi et expliquer les détails de l'incident, le cas échéant.
- **T0312** - Coordonner avec les analystes du renseignement la mise en corrélation des données d'évaluation des menaces.
- **T0164** - Effectuer des analyses et des rapports sur les tendances en matière de cyberdéfense.
- **T0395** - Rédiger et publier des comptes rendus après action.
- **T0503** - Surveiller les sources de données externes (par exemple, les sites des fournisseurs de cybersécurité, les CERTs (Computer Emergency Response Teams), Security Focus) afin de maintenir à jour l'état des menaces en matière de cybersécurité et de déterminer les problèmes de sécurité susceptibles d'avoir un impact sur l'entreprise.
- **T0510** - Coordonner les fonctions de réponse aux incidents.

Par ailleurs, Annexe B permet de connaître le large éventail des compétences clefs en matière de sécurité dont pourrait avoir besoin une personne dont le poste en cybersécurité comprend cette fonction.

Forte de ces informations, une organisation cherchant à atteindre le résultat décrit dans la sous-catégorie **RS.MI-2** du référentiel de cybersécurité peut déterminer si un ou plusieurs membres de son personnel possèdent les compétences nécessaires pour mener à bien les tâches prévues. Si un ou plusieurs KSA font défaut, l'employé souhaitant occuper ce poste de travail saura précisément quels sont les domaines à améliorer et pourra suivre des cours théoriques ou une formation professionnelle afin d'acquérir les connaissances nécessaires. S'il ne trouve pas de personnel, l'employeur dispose de descriptions de tâches spécifiques et d'exigences en matière de KSA qui peuvent être publiées dans une offre d'emploi, ou qui peuvent être utilisées pour le personnel contractuel afin de compléter le personnel existant.

D.2 Ingénierie de la sécurité des systèmes

La publication spéciale (SP) 800-160 du NIST, intitulée *Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure*

Systems [14], traite des activités d'ingénierie nécessaires pour mettre au point des systèmes plus faciles à défendre et plus résistants, y compris les éléments qui composent ces systèmes et les services qui en dépendent. Elle part d'un ensemble de normes internationales bien établies pour l'ingénierie des systèmes et des logiciels et s'appuie sur elles, et intègre des techniques, des méthodes et des pratiques d'ingénierie de la sécurité des systèmes dans ces activités d'ingénierie des systèmes et des logiciels. L'objectif ultime est d'aborder les questions de sécurité du point de vue des exigences des parties prenantes et des besoins de protection, et d'utiliser des processus d'ingénierie éprouvés pour garantir que ces exigences et besoins sont pris en compte avec la fidélité et la rigueur voulues tout au long du cycle de vie du système. Accroître la fiabilité des systèmes est une entreprise d'envergure qui nécessite un investissement substantiel dans les exigences, l'architecture, la conception et le développement des systèmes, des composants, des applications et des réseaux, ainsi qu'un changement culturel fondamental par rapport à l'approche habituelle.

L'introduction d'un ensemble rigoureux, structuré et normalisé d'activités et de tâches d'ingénierie de la sécurité des systèmes constitue un point de départ important et une fonction de stimulation pour amorcer le changement nécessaire. L'objectif ultime est d'obtenir des systèmes sécurisés dignes de confiance qui soient pleinement capables de soutenir des missions et des opérations commerciales critiques tout en protégeant les actifs des parties prenantes, et ce avec un niveau d'assurance compatible avec la tolérance au risque de ces parties prenantes.

La mise en correspondance des éléments du référentiel NICE avec la discipline spécialisée décrite dans le document NIST SP 800-160 permettra de valider ces éléments. Les professionnels de la discipline de l'ingénierie de la sécurité des systèmes deviendront probablement des experts en la matière qui pourront justifier l'ajout de KSA et de tâches supplémentaires au référentiel NICE.

D.3 Codes de l'OPM (Office of Personnel Management) en matière de cybersécurité au niveau fédéral

Le 4 janvier 2017, l'Office of Personnel Management (OPM) des États-Unis a publié un mémorandum [15] intitulé "Guidance for federal agencies assigning new cybersecurity codes to positions with information technology, cybersecurity, and cyber-related functions" (Directives pour les agences fédérales attribuant de nouveaux codes de cybersécurité aux postes ayant des fonctions liées aux technologies de l'information, à la cybersécurité et aux technologies numériques). Ce mémorandum indique que le Federal Cybersecurity Workforce Assessment Act de 2015 [16] exige que l'OPM établisse des procédures pour mettre en œuvre la structure de codification NICE et pour identifier tous les postes civils fédéraux qui nécessitent d'exercer des fonctions liées aux technologies de l'information, à la cybersécurité ou à d'autres fonctions liées aux technologies numériques. Le tableau 9 indique la correspondance entre les identifiants des fonctions du référentiel NICE qui représentent la nature interdisciplinaire du travail de cybersécurité et les codes de cybersécurité de l'OPM qui sont compatibles avec le système d'intégration des ressources humaines de l'OPM (OPM Enterprise Human Resources Integration).

Tableau 9 – Tableau de correspondance entre les identifiants des fonctions et les codes de cybersécurité de l'OPM

ID de fonction	Code OPM	ID de fonction	Code OPM	ID de fonction	Code OPM
SP-RSK-001	611	OV-LGA-001	731	AN-TWA-001	141
SP-RSK-002	612	OV-LGA-002	732	AN-EXP-001	121
SP-DEV-001	621	OV-TEA-001	711	AN-ASA-001	111
SP-DEV-002	622	OV-TEA-002	712	AN-ASA-002	112
SP-ARC-001	651	OV-MGT-001	722	AN-TGT-001	131
SP-ARC-002	652	OV-MGT-002	723	AN-TGT-002	132
SP-TRD-001	661	OV-SPP-001	751	AN-LNG-001	151
SP-SRP-001	641	OV-SPP-002	752	CO-CLO-001	311
SP-TST-001	671	OV-EXL-001	901	CO-CLO-002	312
SP-SYS-001	631	OV-PMA-001	801	CO-OPL-001	331
SP-SYS-002	632	OV-PMA-002	802	CO-OPL-002	332
OM-DTA-001	421	OV-PMA-003	804	CO-OPL-003	333
OM-DTA-002	422	OV-PMA-004	804	CO-OPS-001	321
OM-KMG-001	431	OV-PMA-005	805	IN-INV-001	221
OM-STS-001	411	PR-CDA-001	511	IN-FOR-001	211
OM-NET-001	441	PR-INF-001	521	IN-FOR-002	212
OM-ADM-001	451	PR-CIR-001	531		
OM-ANA-001	461	PR-VAM-001	541		

Annexe E – Glossaire

Les acronymes et abréviations utilisés dans ce document sont définis ci-dessous :

API	Application Programming Interface
CDM	Continuous Diagnostics and Mitigation
CDS	Cross-Domain Solutions
CIO	Chief Information Officer
CKMS	Crypto Key Management System
CMMI	Capability Maturity Model Integration
CMS	Content Management System
CNSSI	Committee on National Security Systems Instruction
COMSEC	Communications Security
COTR	Contracting Officer's Technical Representative
DNS	Domain Name System
EISA	Enterprise Information Security Architecture
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
HR	Human Resource
IDS	Intrusion detection system
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
IRT	Incident Response Teams
ISD	Instructional System Design
ITL	Information Technology Laboratory
KSA	Knowledge, Skills, and Abilities
LAN	Local area network
NICE	National Initiative for Cybersecurity Education
OLA	Operating-Level Agreement
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OS	Operating system
OSI	Open System Interconnection
P.L.	Public Law
PCI	Payment Card Industry
PHI	Personal Health Information
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
PKI	Public key infrastructure
R&D	Research and Design
RFID	Radio Frequency Identification
RMF	Risk Management Framework
SA&A	Security Assessment and Authorization
SDLC	System development life cycle
SLA	Service-Level Agreements
SOP	Standard operating procedures

SQL	Structured query language
TCP	Transmission Control Protocol
TTP	Tactics, techniques, and procedures
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network

Annexe F– Bibliographie

[1] NICE Framework Revision webpage, National Institute of Standards and Technology [Website], https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework/revisions

[2] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 1.0*, https://www.nist.gov/file/359276

[3] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 2.0*, https://www.nist.gov/file/359261

[4] Reference Spreadsheet for NIST Special Publication 800-181 https://www.nist.gov/file/372581

[5] NICE Framework, National Institute of Standards and Technology [Website], https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

[6] U.S. Department of Labor, Employment and Training Administration (ETA) [Website]. https://www.doleta.gov

[7] Competency Model Clearinghouse, Cybersecurity Competency Model, https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

[8] U.S. Department of Homeland Security, Cybersecurity Workforce Development Toolkit (CWDT), https://niccs.us-cert.gov/workforce-development/cybersecurity-workforce-development-toolkit

[9] Baldrige Cybersecurity Excellence Program, National Institute of Standards and Technology [Website], https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

[10] U.S. Department of Homeland Security, CMSI PushButtonPD™ Tool Website, https://niccs.us-cert.gov/workforce-development/dhs-cmsi-pushbuttonpd-tool

[11] *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0,* National Institute of Standards and Technology February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[12] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[13] *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/roadmap-021214.pdf

[14] NIST Special Publication (SP) 800-160, *Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* National Institute of Standards and Technology, November 2016, https://doi.org/10.6028/NIST.SP.800-160

[15] Memorandum on Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions, January 2017, https://www.chcoc.gov/content/guidance-assigning-new-cybersecurity-codes-positions-information-technology-cybersecurity

[16] H.R.2029 - Consolidated Appropriations Act, 2016 which contains Division N-Cybersecurity Act of 2015, https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf