**Publication Spéciale du NIST 800-181**
**Révision 1**

# Référentiel de compétences pour les professionnels de la cybersécurité (Référentiel NICE)

Rodney Petersen
Danielle Santos
Matthew C. Smith
Karen A. Wetzel
Greg Witte

Cette publication est disponible gratuitement à l'adresse suivante :
https://doi.org/10.6028/NIST.SP.800-181r1.fre

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

**Publication Spéciale du NIST 800-181**
**Révision 1**

# Référentiel de compétences pour les professionnels de la cybersécurité (Référentiel NICE)

Rodney Petersen (Director)
Danielle Santos (Manager of Communications and Operations)
Karen A. Wetzel (Manager of the NICE Framework)
*National Initiative for Cybersecurity Education (NICE)*
*Applied Cybersecurity Division*
*Information Technology Laboratory*

Matthew C. Smith
Greg Witte
*Huntington Ingalls Industries*
*Annapolis Junction, MD*

Cette publication est disponible gratuitement à l'adresse suivante :
https://doi.org/10.6028/NIST.SP.800-181r1.fre

Novembre 2020


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

National Institute of Standards and Technology
*Walter Copan, 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 Rev. 1, 31 pages (Novembre 2020)
CODEN: NSPUE2

Cette publication est disponible gratuitement à l'adresse suivante :
https://doi.org/10.6028/NIST.SP.800-181r1.fre



## Les commentaires sur cette publication peuvent être adressés à :

National Institute of Standards and Technology
Attn : Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
E-mail : NICEFramework@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 clés

Compétence ; cybersécurité ; cyberespace ; éducation ; connaissance ; rôle ; sécurité ; capacité ; tâche ; équipe ; formation ; ressources humaines ; fonction.

## Avis de divulgation de brevets

*AVIS : Le Laboratoire des technologies de l'information (ITL) a demandé aux détenteurs de brevets dont l'utilisation peut être nécessaire pour se conformer aux orientations ou aux exigences de la présente publication de communiquer ces brevets à l'ITL. Toutefois, les détenteurs de brevets ne sont pas tenus de répondre aux appels à brevets de l'ITL et l'ITL n'a pas entrepris de recherche sur les brevets afin d'identifier les éventuels brevets applicables à la présente publication.*

*À la date de publication et à la suite de l'appel à l'identification des brevets dont l'utilisation peut être nécessaire pour se conformer aux conseils ou aux exigences de la présente publication, aucun brevet n'a été signalé à l'ITL.*

*ITL ne prétend pas que des licences ne sont pas nécessaires pour éviter la violation de brevets lors de l'utilisation de la présente publication.*

## Conventions utilisées dans ce document

Conventions utilisées dans ce document

Les termes « doit» et « ne doit pas» indiquent des exigences à respecter strictement pour se conformer à la publication et auxquelles il n'est pas permis de déroger. Les termes « devrait» et « ne devrait pas» indiquent que, parmi plusieurs possibilités, l'une d'entre elles est recommandée comme particulièrement appropriée, sans mentionner ou exclure les autres, ou qu'une certaine ligne de conduite est préférable mais pas nécessairement requise, ou que (dans la forme négative) une certaine possibilité ou ligne de conduite est découragée mais pas interdite. Les termes « pourrait» et « ne devrait pas» indiquent une ligne de conduite admissible dans les limites de la publication. Les termes « peut» et « ne peut pas» indiquent une possibilité et une capacité, qu'elles soient matérielles, physiques ou causales.

Dans l'ensemble du référentiel NICE, les personnes qui travaillent dans le domaine de la cybersécurité - y compris les étudiants, les demandeurs d'emploi et les employés - sont appelées « apprenants». Cette appellation souligne le fait que chaque membre de ces effectifs est également un apprenant tout au long de sa vie.

## Remerciements

Le référentiel NICE a été élaboré par une équipe de rédaction qui comprend des représentants de nombreux départements et agences du gouvernement fédéral des États-Unis. Le National Institute of Standards and Technology souhaite remercier les membres de cette équipe dont les efforts dévoués ont contribué de manière significative à la publication :

William Newhouse, National Institute of Standards and Technology
Pam Frugoli, Department of Labor
Lisa Dorr, Department of Homeland Security
Kenneth Vrooman, Cybersecurity and Infrastructure Security Agency
Bobbie Sanders, Department of Defense
Patrick Johnson, Department of Defense
Matt Isnor, Department of Defense
Stephanie Shively, Department of Defense
Ryan Farr, Department of Defense

Les auteurs et l'équipe de rédaction remercient vivement les personnes et les organisations des secteurs public et privé pour leurs contributions significatives, dont les commentaires réfléchis et constructifs ont permis d'améliorer la qualité générale, l'exhaustivité et l'utilité de la présente publication. Les auteurs apprécient tout particulièrement les nombreuses réponses utiles à l'appel à commentaires du référentiel NICE et à la version préliminaire de la présente publication destinée aux commentaires du public.

De plus, l'équipe apprécie et reconnaît les contributions de ceux qui ont établi les éditions précédentes des référentiels nationaux sur les ressources humaines en cybersécurité, comme décrit sur la page Historique du Centre de ressources du référentiel NICE [1].

## Note aux lecteurs

Bienvenue dans le référentiel NICE (National Initiative for Cybersecurity Education) pour les ressources humaines dans le domaine de la cybersécurité (NICE Framework), Révision 1. Le personnel du programme NICE a reçu d'importants commentaires de la part de la communauté, notamment de nombreuses réponses à une récente demande de commentaires généraux concernant le référentiel NICE, ainsi que des réponses à la version préliminaire publique de cette publication. À la lumière de ces commentaires et de l'écosystème de la cybersécurité, qui évolue rapidement et est connecté, l'équipe de rédaction a décidé d'adopter et de promouvoir les principes d'agilité, de flexibilité, d'interopérabilité et de modularité. C'est pourquoi le référentiel NICE a été remanié afin d'offrir une approche simplifiée pour le développement d'une main-d'œuvre capable de gérer les risques liés à la cybersécurité. Vous trouverez ci-dessous un résumé des changements :

- Les constructions organisationnelles de la révision 1 ont été simplifiées en supprimant les catégories (par exemple, provisionnement sécurisé, superviser et gouverner, protéger et défendre, analyser, etc.) et les spécialités (par exemple, réponse aux incidents, analyse des menaces, gestion de la cybersécurité, etc.). Afin de simplifier une approche qui offre agilité, flexibilité, interopérabilité et modularité aux organisations, la révision 1 présente un ensemble rationalisé de « blocs de construction» composés de tâches, de connaissances et de capacités. Les organisations qui trouvent une utilité aux anciennes catégories et domaines de spécialité peuvent continuer à les utiliser ou créer des équipes autour de ces concepts et les aligner sur cette version du référentiel NICE (voir la section 3.4).
- La révision 1 décrit plusieurs utilisations des Tâches, des Connaissances et des Capacités, y compris des méthodes d'application de celles-ci dans la création de Fonctions. Les utilisateurs des fonctions décrites dans le document original NIST SP 800-181 peuvent continuer à les utiliser ; des mises à jour de ces fonctions pourront être publiées par le NICE à l'avenir [2].

Les relations entre les tâches, les connaissances, les capacités et les aptitudes ont changé. Les descriptions de capacités et d'aptitudes de la version précédente ont été remaniés pour plus de simplicité en descriptions de capacités, qui mettent l'accent sur l'action de l'apprenant. Cette révision décrit les méthodes permettant d'associer les descriptions de connaissances et de capacités aux descriptions de tâches pour divers résultats. Les listes de tâches, de connaissances, de capacités et de rôles professionnels qui étaient auparavant disponibles dans les annexes A et B du référentiel NICE 2017 ont été supprimées de cette version afin de simplifier la maintenance du référentiel et de faciliter les mises à jour de ces listes. Les descriptions des tâches, connaissances et capacités (TKS pour Tasks, Knowledge, and Skills) et les compétences et fonctions professionnelles correspondantes seront conservées en tant qu'artefacts distincts et feront l'objet d'une révision et de mises à jour continues, avec un processus de changement défini et une indication du contrôle de version pour gérer et communiquer les changements. Jusqu'à ce que ces mises à jour aient lieu, les versions antérieures de ces listes resteront à la disposition des utilisateurs dans le centre de ressources du référentiel NICE. À l'appui de l'interopérabilité et de la modularité, les futures mises à jour veilleront à ce que les descriptions correspondent aux définitions finales des descriptions TKS notées ici.

- Pour les lecteurs intéressés par la mise en correspondance de normes, de références ou de ressources avec le référentiel NICE, NICE travaille avec le programme Online Informative Reference (OLIR) afin de développer des modèles pour ces mises en correspondance. Le programme OLIR, géré par le NIST, fournit un processus d'alignement des références aux documents du NIST. En outre, le programme fournit un catalogue de ces références [3].

## Résumé

Chacun d'entre nous, individuellement ou au sein d'une organisation, effectue un travail important qui apporte une contribution à la société. Toutefois, comme l'information et la technologie, y compris de nombreux types de technologies opérationnelles en évolution, deviennent de plus en plus complexes et interconnectées, il peut être difficile de décrire clairement le travail qui est effectué ou que nous souhaitons accomplir, dans ces domaines en particulier. L'initiative nationale pour l'éducation en cybersécurité (NICE) reconnaît que les personnes qui travaillent dans le domaine de la cybersécurité - y compris les étudiants, les demandeurs d'emploi et les employés - apprennent tout au long de leur vie et s'efforcent de mettre en évidence les implications de la cybersécurité dans de nombreux domaines et d'y faire face. Cette catégorie de personnes est désignée dans le présent document à la fois par le terme « apprenants» et parfois par celui de « professionnels de la cybersécurité» , ce qui ne signifie pas que les rôles professionnels et les contenus inclus dans le référentiel NICE ne s'appliquent qu'à ceux qui sont pleinement intégrés dans le domaine de la cybersécurité. Les tâches que ces apprenants accomplissent sont appelées ici « travail de cybersécurité» , et le cadre fournit un moyen de décrire ce travail avec précision afin de soutenir l'éducation ou la formation des apprenants ainsi que le recrutement, l'embauche, la progression et la fidélisation des employés. Le référentiel NICE a été élaboré pour aider à fournir une taxonomie de référence - c'est-à-dire un langage commun - du travail de cybersécurité et des personnes qui l'effectuent. Le référentiel NICE soutient la mission de NICE qui consiste à dynamiser, promouvoir et coordonner une communauté solide travaillant ensemble pour faire progresser un écosystème intégré d'éducation, de formation et de développement des ressources humaines dans le domaine de la cybersécurité. Le référentiel NICE fournit un ensemble d'éléments permettant de décrire les tâches, les connaissances et les capacités nécessaires à l'accomplissement des travaux de cybersécurité réalisés par les individus et les équipes. Grâce à ces éléments, le référentiel NICE permet aux organisations de former leur personnel à la cybersécurité et aide les apprenants à explorer le travail en cybersécurité et à s'engager dans des activités d'apprentissage appropriées pour développer leurs connaissances et leurs capacités. Ce développement profite à son tour aux employeurs et aux employés grâce à l'identification de parcours professionnels qui indiquent comment se préparer au travail dans le domaine de la cybersécurité en utilisant les données des énoncés de tâches, de connaissances et de capacités (TKS) regroupés dans les rôles et les compétences professionnels.

L'utilisation de termes et d'un langage communs permet d'organiser et de communiquer le travail à effectuer et les attributs des personnes qualifiées pour effectuer ce travail. De cette manière, le référentiel NICE contribue à simplifier les communications et à mettre l'accent sur les tâches à accomplir. Enfin, l'utilisation du référentiel NICE améliore la clarté et la cohérence à tous les niveaux de l'organisation, qu'il s'agisse d'un individu, d'un système technologique, d'un programme, d'une organisation, d'un secteur, d'un État ou d'une nation.

## Table des matières

**Résumé** ..... **vii**

**1 Contexte** ..... **1**

1.1 Caractéristiques du référentiel NICE ..... 2

1.2 Objectif et applicabilité ..... 3

1.3 Public ..... 3

1.4 Organisation du présent document ..... 4

**2 Éléments du référentiel NICE** ..... **5**

2.1 Description de tâche ..... 5

2.2 Description de connaissance ..... 6

2.3 Description de capacité ..... 6

**3 Utiliser le référentiel NICE** ..... **8**

3.1 Utilisation des descriptions de tâches, de connaissances et de capacités (TKS) existantes ..... 8

3.2 Création de nouvelles descriptions TKS ..... 9

3.3 Compétences ..... 9

3.3.1 Utilisation des compétences existantes ..... 11

3.3.2 Créer de nouvelles compétences ..... 11

3.4 Fonctions ..... 13

3.4.1 Utilisation des fonctions existantes ..... 14

3.4.2 Créer une nouvelle fonction ..... 15

3.5 Equipes ..... 15

3.5.1 Constituer des équipes avec des fonctions ..... 15

3.5.2 Constituer des équipes avec des compétences ..... 16

**4 Conclusion** ..... **18**

**Références** ..... **19**

**Annexe A— Acronymes** ..... **20**

**Annexe B— Glossaire** ..... **21**

# 1 Contexte

La technologie continue d'évoluer à un rythme de plus en plus rapide. En particulier, la technologie qui facilite l'accès à l'information et son traitement rapide et efficace est en train de changer radicalement. Le travail requis pour concevoir, construire, sécuriser et mettre en œuvre ces données, réseaux et systèmes devient de plus en plus complexe. En outre, la description de ce travail et des personnes qui peuvent l'effectuer reste un défi. Pour aggraver la situation, les organisations utilisent des méthodes variées et créées par elles-mêmes pour tenter de résoudre ce défi.

Cette publication de la National Initiative for Cybersecurity Education (NICE) décrit le Workforce Framework for Cybersecurity (référentiel NICE). Le référentiel NICE aide les organisations à surmonter l'obstacle que représente la description de leurs effectifs à de multiples parties prenantes en présentant une approche modulaire. Grâce à l'utilisation de blocs conceptuels, le référentiel NICE présente un langage commun que les organisations peuvent utiliser en interne et avec d'autres. Cette approche permet aux organisations d'adapter et de mettre en œuvre le référentiel NICE à leur contexte opérationnel unique. En outre, en créant un langage commun, le référentiel NICE abaisse la barrière à l'entrée pour les organisations qui cherchent à entrer et à interopérer avec d'autres organisations.

La figure 1 ci-dessous présente une vue d'ensemble du référentiel NICE. Les principaux éléments du référentiel NICE sont des descriptions de tâches, de connaissances et de capacités (TKS) (expliqués à la section 2) qui sont présentés à côté des concepts qu'ils décrivent. La figure 1 montre qu'il existe deux principaux types de concepts décrits : « le travail» et « l'apprenant» . Il convient de noter que les personnes qui effectuent (ou effectueront) un travail (par exemple, les étudiants, les employés actuels ou les demandeurs d'emploi) apprennent continuellement et atteignent des objectifs, et peuvent se trouver à n'importe quel moment du cycle de vie de l'apprentissage. Le référentiel NICE tente de décrire à la fois « le travail» et « l'apprenant» en des termes génériques qui peuvent être appliqués à toutes les organisations.

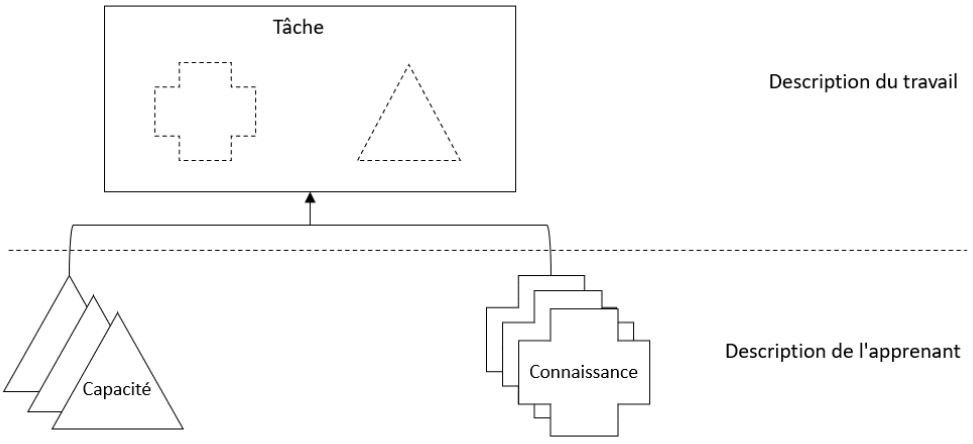


**Figure 1 : Approche par blocs du référentiel NICE**

Le « travail» est ce dont une organisation a besoin pour atteindre ses objectifs en matière de gestion des risques de cybersécurité. Chaque organisation exécute des tâches communes ainsi que des tâches spécifiques au contexte. Par exemple, toutes les organisations ont des tâches de gestion sous une forme ou une autre, alors que seules certaines organisations ont des tâches pour « déployer des systèmes d'énergie en toute sécurité» . Le référentiel NICE fournit aux organisations un moyen de décrire leur travail par le biais de descriptions de tâches qui regroupent des descriptions de connaissances et de capacités.

L'« apprenant» est la personne qui possède les connaissances et les capacités. Le terme d'apprenant s'applique à toutes les personnes concernées par le présent document. Il peut s'agir d'un étudiant, d'un demandeur d'emploi, d'un employé ou d'autres personnes faisant partie de la population active. Dans un contexte organisationnel, les apprenants exécutent des tâches. Dans un contexte éducatif, les apprenants acquièrent de nouvelles connaissances et capacités. Tous les individus sont considérés comme des apprenants en raison de l'éducation ou de la formation qu'ils ont reçue avant d'entrer sur le marché du travail, de la formation continue, de l'auto-apprentissage ou d'un plan de progression de carrière.

Le référentiel NICE permet aux organisations de décrire les apprenants en associant des descriptions de connaissances et de capacités à un individu ou à un groupe. En utilisant leurs connaissances et leurs capacités, les apprenants peuvent accomplir des tâches pour atteindre les objectifs de l'organisation. Même si toutes les organisations n'utiliseront pas tous les concepts relatifs aux apprenants, le référentiel NICE fournit aux organisations un ensemble flexible de blocs de construction à utiliser selon les besoins de leur contexte spécifique. La reconnaissance du rôle que joue l'apprenant dans le développement des capacités à effectuer un travail de cybersécurité renforce également l'applicabilité du référentiel NICE aux organismes d'enseignement et de formation.

En décrivant à la fois le travail et l'apprenant, le référentiel NICE fournit aux organisations un langage commun pour décrire leur travail et leur main-d'œuvre en matière de cybersécurité. Certaines parties du référentiel NICE décrivent un contexte de travail organisationnel (tâches), d'autres parties décrivent un contexte d'apprentissage (connaissances et capacités) et enfin, l'approche modulaire du référentiel NICE permet aux organisations de relier les deux contextes.

En outre, le référentiel NICE fournit un mécanisme de communication entre les organisations au niveau des pairs, au niveau sectoriel, au niveau de l'État, au niveau national ou au niveau international, en utilisant les mêmes blocs de construction. Cette communication peut déboucher sur des solutions innovantes à des défis communs, abaisser les barrières à l'entrée pour les nouvelles organisations et les nouveaux individus, et faciliter la mobilité de la main-d'œuvre.

### 1.1 Caractéristiques du référentiel NICE

Le référentiel NICE est une ressource de référence pour ceux qui cherchent à décrire le travail de cybersécurité effectué par leur organisation, les personnes qui effectueront ce travail et l'apprentissage continu qui sera nécessaire pour effectuer ce travail de manière efficace. La nature du travail et, par conséquent, les effectifs, peuvent être décrits à l'aide des éléments de base de la TKS présentés dans les sections suivantes. Ces blocs de construction intègrent les attributs suivants :

- **Agilité :** Les personnes, les processus et la technologie arrivent à maturité et doivent s'adapter au changement. Par conséquent, le référentiel NICE permet aux organisations de suivre le rythme d'un écosystème en constante évolution.

- **Flexibilité :** Si chaque organisation est confrontée à des défis similaires, il n'existe pas de solution unique à ces défis. Par conséquent, le référentiel NICE permet aux organisations de tenir compte du contexte opérationnel spécifique de l'organisation.

- **Interopérabilité :** Bien que chaque solution aux défis communs soit unique, ces solutions doivent s'accorder sur une utilisation cohérente des termes. Par conséquent, le référentiel NICE permet aux organisations d'échanger des informations sur les effectifs en utilisant un langage commun.

- **Modularité :** Si le risque de cybersécurité reste la base de ce document, il existe d'autres risques que les organisations doivent gérer au sein de l'entreprise. Par conséquent, le référentiel NICE permet aux organisations de communiquer sur d'autres types d'effectifs au sein d'une entreprise et entre les organisations ou les secteurs (par exemple, la protection de la vie privée, la gestion des risques, l'ingénierie/le développement de logiciels).

### 1.2 Objectif et applicabilité

Les organisations gèrent de nombreuses activités différentes (telles que les opérations, les finances, le service juridique et les ressources humaines) dans le cadre de leur fonctionnement global. Chacune de ces fonctions comporte des risques. La technologie étant devenue un facteur déterminant dans la gestion d'une entreprise, les risques liés à la cybersécurité sont également devenus plus importants. Le référentiel NICE aide les organisations à gérer les risques de cybersécurité en fournissant un moyen de parler du travail et des apprenants associés à la cybersécurité. Ces risques de cybersécurité constituent un élément important dans les décisions relatives aux risques de l'entreprise, comme le décrit le rapport Interagency Report 8286 du NIST, intitulé *Integrating Cybersecurity and Enterprise Risk Management (ERM)* [4].

Ce document est un guide potentiel pour les autres fonctions de l'entreprise qui envisagent de créer des référentiels concernant les ressources humaines. Les organisations peuvent accroître leur efficacité en utilisant les mêmes éléments de base pour les différentes fonctions de l'entreprise. Par conséquent, toute organisation peut tirer parti de ce document.

### 1.3 Public

La gestion des effectifs dans le domaine de la cybersécurité concerne de nombreux types de postes et d'organisations. Le présent document s'adresse aux organismes du secteur public, aux organisations privées et à but non lucratif, aux acteurs de l'éducation et de la formation, aux concepteurs de programmes, aux fournisseurs de titres et de certificats, aux professionnels des ressources humaines, aux responsables de l'embauche, aux responsables hiérarchiques, aux responsables de la planification des effectifs, aux recruteurs et à tous les apprenants.

### 1.4 Organisation du présent document

Le reste de cette publication spéciale est organisé comme suit :

- Section 2, Blocs de construction du référentiel NICE : Définit les éléments constitutifs des TKS du référentiel NICE.
- Section 3, Utilisation du référentiel NICE : Décrit les approches courantes de l'utilisation du référentiel NICE.
- Section 4, Conclusion
- Références : Liste des publications connexes citées dans le présent document
- Annexe A, Acronymes : Liste des acronymes et abréviations utilisés dans cette publication

# 2 Éléments du référentiel NICE

Le référentiel NICE (Workforce Framework for Cybersecurity ou encore NICE Framework) repose sur un ensemble de modules distincts qui décrivent le travail à effectuer (sous la forme de tâches) et ce qui est nécessaire pour réaliser ce travail (grâce aux connaissances et aux capacités). Ces éléments constitutifs sont des constructions organisationnelles qui soutiennent la facilité d'utilisation et la mise en œuvre du référentiel NICE. Ils fournissent un mécanisme par lequel les organisations et les individus peuvent comprendre la portée et le contenu du référentiel NICE. Ils sont conçus comme des lignes directrices qui peuvent être utilisées pour améliorer la compréhension plutôt que comme des structures rigides.



## 2.1 Description de tâche

Comme le montre la Figure 1, les descriptions de tâches décrivent le travail, tandis que les descriptions de connaissances et de capacités décrivent l'apprenant. Les descriptions de tâches doivent se concentrer sur le langage organisationnel et les modèles de communication qui apportent de la valeur à l'organisation. Ces énoncés sont conçus pour décrire le travail à effectuer et doivent être alignés sur le contexte de l'organisation.

**Tâche**
Activité visant à atteindre les objectifs de l'organisation.

**Description de tâche**
- Facile à lire et à comprendre
- Commence par l'activité à accomplir
- Ne contient pas l'objectif de la tâche

Les tâches décrivent le travail à accomplir. Une tâche peut être définie comme une activité visant à atteindre les objectifs de l'organisation, y compris les objectifs commerciaux, les objectifs technologiques ou les objectifs de la mission. Les descriptions de tâches doivent être simples. Bien que le travail visé par une description de tâche puisse comporter de nombreuses étapes, comme dans l'exemple ci-dessous, la description elle-même est facile à lire et à comprendre.

La description d'une tâche commence par l'activité exécutée.

Exemple : **Dépanner** le matériel et les logiciels du système.

La description d'une tâche ne contient pas d'objectif, car celui-ci peut varier en fonction des objectifs de la mission et des besoins de l'organisation.

Exemple : Réaliser des exercices de formation interactifs.

Dans l'exemple ci-dessus, le but de ces exercices peut être de créer un environnement d'apprentissage efficace, mais cet objectif n'est pas inclus dans la description de la tâche elle-même.

Comme le montre la Figure 1, les tâches sont liées aux descriptions des connaissances et des capacités. Un apprenant démontrera qu'il possède les connaissances et les capacités nécessaires pour accomplir une tâche (ou sera invité à acquérir les connaissances et les capacités nécessaires pour se préparer à accomplir la tâche). La complexité d'une tâche est expliquée par les descriptions des connaissances et des capacités qui lui sont associées. Dans l'exemple de dépannage ci-dessus, pour dépanner efficacement un logiciel ou un matériel, l'apprenant doit

connaître et comprendre les descriptions des connaissances qui s'y rapportent. Il en va de même pour les descriptions des capacités.

## 2.2 Description de connaissance

**Connaissance**
Un ensemble de concepts accessibles en mémoire.

**Description connaissance**
- Décrit les connaissances fondamentales ou spécifiques
- Plusieurs descriptions peuvent être nécessaires pour accomplir une tâche
- Une seule description peut être utilisée pour accomplir plusieurs tâches différentes

Les descriptions de connaissances sont liés aux descriptions de tâches dans la mesure où l'apprenant ne pourra accomplir la tâche que grâce aux éléments mentionnés dans la description de connaissance. La connaissance est définie comme un ensemble de concepts que l'on peut retrouver dans la mémoire. Les descriptions de connaissances peuvent décrire des concepts fondamentaux ou spécifiques. Plusieurs descriptions de connaissances peuvent être nécessaires pour accomplir une tâche donnée. De même, une description de connaissance peut être utilisé pour accomplir plusieurs tâches différentes.

Les descriptions de connaissances peuvent être fondamentales.

Exemple : Connaissance des menaces et vulnérabilités du cyberespace.

Les descriptions de connaissances peuvent être spécifiques.

Exemple : Connaissance des sources de diffusion d'informations sur les vulnérabilités (par exemple, les alertes des fournisseurs, les avis des gouvernements, l'errata de la documentation sur les produits et les bulletins sectoriels).

Les organisations qui élaborent des descriptions de connaissances doivent tenir compte des différents niveaux de connaissances et d'expertise des apprenants. Un exemple de ces différents niveaux est décrit dans la Taxonomie de Bloom (révisée), qui utilise un langage facilitant l'observation et l'évaluation de l'apprenant [5].

## 2.3 Description de capacité

**Capacité**
La capacité à effectuer une action observable.

**Description de la capacité**
- Décrit des capacités simples ou complexes
- Plusieurs descriptions peuvent être nécessaires pour mener à bien une tâche
- Une seule description peut être utilisée pour accomplir plus d'une tâche

Les descriptions de capacités sont liées aux descriptions de tâches dans la mesure où l'apprenant fait preuve de capacités dans l'exécution des tâches. Un apprenant qui n'est pas en mesure de démontrer la capacité décrite ne sera pas en mesure d'accomplir la tâche qui repose sur cette capacité. Une capacité est définie comme le fait de pouvoir effectuer une action observable. Les descriptions de capacités peuvent décrire des capacités simples ou complexes. Plusieurs descriptions de capacités peuvent être nécessaires pour mener à bien une tâche donnée. De même, l'exercice d'une capacité peut être utilisé pour accomplir plus d'une tâche.

Les descriptions de capacités peuvent être simples.

Exemple : Savoir reconnaître les alertes d'un système de détection d'intrusion.

Les descriptions de capacités peuvent être complexes.

Exemple : Capacité à formuler une hypothèse sur la manière dont un pirate informatique a contourné le système de détection d'intrusion.

Comme le montre la Figure 1, les descriptions de capacités décrivent ce que l'apprenant peut faire et les descriptions de tâches décrivent le travail à effectuer. Par conséquent, il est important de séparer le langage utilisé entre les descriptions de capacités et les descriptions de tâches et d'utiliser des termes qui facilitent l'observabilité et l'évaluation de l'apprenant.

# 3 Utiliser le référentiel NICE

Il convient de noter que, bien que le référentiel NICE (Workforce Framework for Cybersecurity) soit destiné à fournir un ensemble commun d'éléments de base dont chacun peut s'inspirer, certaines organisations jugeront nécessaire d'adapter le modèle pour qu'il corresponde plus étroitement à leur contexte spécifique. Par exemple, un fabricant peut avoir des tâches spécifiques à son secteur ou à son organisation qui ne sont pas décrites dans le référentiel NICE. D'autres peuvent estimer que les tâches sont applicables, mais qu'il est nécessaire d'ajuster ou de développer des descriptions de connaissances et de compétences spécifiques afin d'augmenter la probabilité que les tâches puissent être accomplies conformément à leur contexte spécifique. En tant que tels, ces éléments constitutifs ne se veulent pas rigides ; ils visent plutôt à fournir un langage commun que les organisations ou les secteurs peuvent utiliser de manière bénéfique dans un contexte donné.

Enfin, les exemples d'utilisation des éléments du référentiel NICE présentés ci-dessous sont de nature théorique ou conceptuelle ; une organisation peut utiliser les éléments de n'importe quelle manière pour répondre au mieux aux besoins locaux. Ces exemples ont pour but d'illustrer des approches pratiques potentielles du référentiel NICE qui se sont avérées utiles pour atteindre des objectifs organisationnels communs. Ils guident les organisations ou les secteurs qui cherchent un point de départ plutôt qu'une façon unique d'utiliser le référentiel NICE.

## 3.1 Utilisation des descriptions de tâches, de connaissances et de capacités (TKS) existantes

Les utilisateurs du référentiel NICE font référence à une ou plusieurs descriptions de tâches, de connaissances et de capacités (TKS), telles que décrites dans la section 2, pour décrire à la fois le travail et les apprenants. Les déclarations de tâches sont utilisées pour décrire le travail. Les descriptions de tâches sont associées à des descriptions de connaissances et de compétences. Bien qu'une description de tâche puisse être associée à un ensemble recommandé de descriptions de connaissances et de compétences, les utilisateurs peuvent inclure d'autres descriptions de connaissances et de compétences existantes afin d'adapter les tâches à leur contexte particulier. Les descriptions de connaissances et de compétences sont utilisées pour décrire les apprenants. Les descriptions de compétences et d'aptitudes peuvent être utilisées de différentes manières pour gérer les effectifs de la cybersécurité. Ils peuvent être utilisés en partie, en totalité ou pas du tout, en fonction du contexte propre à l'organisation qui les met en œuvre. Les exemples théoriques d'utilisation ci-dessous illustrent les domaines dans lesquels les descriptions TKS peuvent être mises en œuvre :

- Programme de suivi des capacités des employés pour déterminer les qualifications de promotion
- Connaissances requises pour terminer un cours
- Liste de tâches hebdomadaires à accomplir au sein d'une organisation

Les descriptions et exemples de TKS sont disponibles dans le centre de ressources du référentiel NICE et seront mis à jour, le cas échéant, pour suivre les changements résultant de l'évolution des missions de l'entreprise, des risques ou des technologies émergentes [1].

### 3.2 Création de nouvelles descriptions TKS

Les utilisateurs sont invités à ne pas modifier le texte des descriptions TKS du référentiel NICE existantes. Les descriptions sont destinées à soutenir l'interopérabilité, de sorte que la modification de leur contenu peut entraîner un désalignement ultérieur lors de l'utilisation de sources extérieures. Si une formulation différente est nécessaire dans une description TKS pour soutenir le contexte spécifique d'un utilisateur, une nouvelle description peut être créée.

Les utilisateurs peuvent également créer des descriptions de tâches, de connaissances ou de capacités entièrement nouvelles afin d'adapter l'utilisation du référentiel NICE à un usage local dans leur contexte particulier. Ces descriptions supplémentaires contribueront à la clarté et à la cohérence des discussions internes.



### 3.3 Compétences

Les compétences fournissent aux organisations un mécanisme d'évaluation des apprenants. Les compétences sont définies dans le cadre d'une approche axée sur l'employeur qui permet de comprendre le contexte propre à une organisation. De plus, les compétences permettent aux acteurs de l'éducation et de la formation de répondre aux besoins des employeurs ou du secteur en développant des offres d'apprentissage qui aident les apprenants à développer et à démontrer les compétences. Les compétences se composent d'un nom, d'une description de la compétence, d'une méthode d'évaluation, ainsi que d'un groupe de descriptions TKS associées.

**Compétences**
Un mécanisme permettant aux organisations d'évaluer les apprenants.

**Les compétences sont :**
- Définies dans le cadre d'une approche axée sur l'employeur
- Axées sur l'apprenant
- Observable et mesurable

Les compétences offrent une certaine flexibilité en permettant aux organisations de regrouper diverses descriptions de TKS dans une catégorie globale qui définit un besoin général. Alors qu'une tâche individuelle et les descriptions de connaissances et de capacités qui lui sont associés peuvent rester inchangés, la compétence définie de manière plus générale peut introduire de nouvelles tâches ou même des connaissances et des capacités individuelles - ou supprimer celles qui existent - en réponse à l'évolution des besoins dans un écosystème de cybersécurité en mutation.

Les compétences peuvent être utilisées de différentes manières. Par exemple, comme le montre la Figure 2, une organisation pourrait utiliser les compétences dans le cadre d'un processus de recrutement visant à atteindre des objectifs organisationnels spécifiques. Dans ce cas, les compétences pourraient être définies comme un groupe de descriptions de tâches connexes. L'organisation pourrait ensuite utiliser ces compétences pour évaluer si un candidat peut accomplir ces tâches. Cette évaluation pourrait prendre la forme d'un entretien, d'un test préalable à l'embauche ou d'une observation de l'apprentissage sur le lieu de travail.

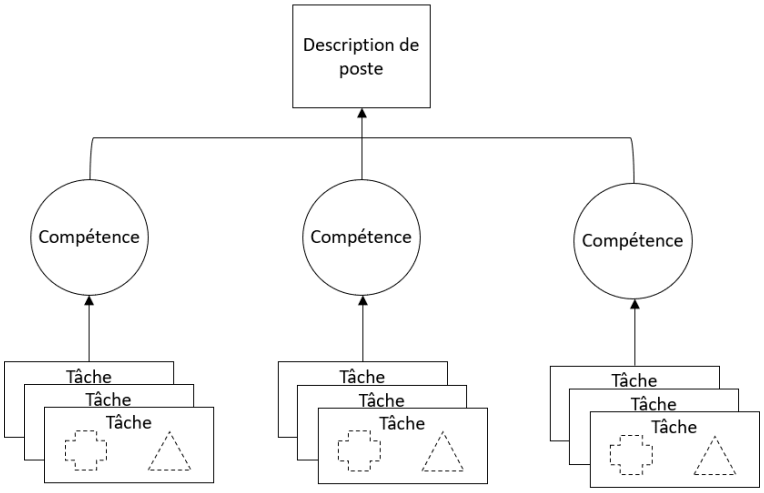


**Figure 2 : Utiliser les compétences pour évaluer les apprenants à l'aide d'une description de poste**

D'autres organisations pourraient utiliser les compétences pour déterminer si un apprenant a atteint un ensemble défini de capacités et de connaissances. Ces organisations pourraient, comme le montre la Figure 3, choisir d'utiliser les compétences comme groupes de descriptions de capacités et de connaissances. Ces organisations pourraient ensuite évaluer les apprenants en fonction de ces descriptions de capacités et de connaissances. Les évaluations peuvent prendre la forme de tests, de démonstrations en laboratoire ou d'évaluations à l'oral.

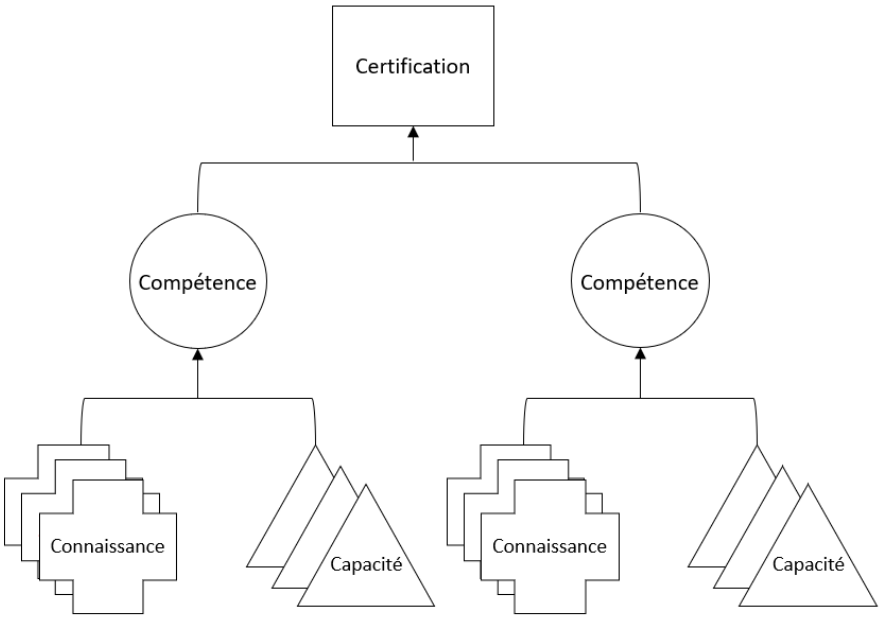


**Figure 3 : Utiliser les compétences pour évaluer les apprenants dans le cadre d'une certification**

Les exemples ci-dessus sont théoriques. Ils peuvent être utilisés en partie, en totalité ou pas du tout, en fonction du contexte spécifique de l'organisation chargée de la mise en œuvre.

### 3.3.1 Utilisation des compétences existantes

Les compétences du référentiel NICE sont un moyen pour les organisations de s'aligner sur le référentiel NICE à un niveau élevé sans entrer dans les détails des descriptions TKS. Les compétences sont un moyen de décrire l'évaluation d'un apprenant. En permettant aux organisations de définir des groupes de descriptions TKS, les compétences leur permettent de communiquer succinctement et d'organiser efficacement leur travail en matière de cybersécurité afin de fournir une vue simplifiée de leurs effectifs. Les compétences peuvent également servir à

- Décrire les types de tâches d'un poste donné
- Suivre les capacités du personnel
- Décrire les besoins de l'équipe
- Démontrer les capacités de l'apprenant

Bien qu'une compétence comporte un ensemble recommandé de descriptions TKS associées, les utilisateurs peuvent ajouter ou supprimer des descriptions existantes afin d'adapter les compétences à leur contexte propre. Toutefois, les utilisateurs sont mis en garde contre la modification du titre ou de la description d'une compétence existante du référentiel NICE. Les compétences sont destinées à soutenir l'interopérabilité, de sorte que la modification de leur contenu peut entraîner un désalignement ultérieur lors de l'utilisation de sources extérieures. Si une formulation différente est nécessaire dans une compétence pour soutenir le contexte spécifique d'un utilisateur, une nouvelle compétence peut être créée comme décrit ci-dessous (voir section 3.3.2).

### 3.3.2 Créer de nouvelles compétences

Certaines organisations peuvent avoir besoin de décrire une compétence pour le contexte spécifique de leur travail en matière de cybersécurité. Le référentiel NICE, élaboré selon le principe de l'agilité, permet aux organisations de décrire une compétence pour répondre à l'évolution de l'écosystème de la cybersécurité. Cela peut se faire en modifiant une compétence existante pour répondre aux besoins propres à l'organisation ou en créant une compétence entièrement nouvelle.

Deux exemples fictifs sont fournis ci-dessous pour expliquer les processus possibles d'utilisation des compétences. Les deux exemples se concentrent sur l'analyse des données pour montrer que la même compétence peut être utilisée selon différentes approches. Par ailleurs, ces exemples développent la Figure 2 et la Figure 3 afin de familiariser le lecteur avec une mise en œuvre éventuelle. Ces exemples utilisent une structure de tableau pour présenter la compétence. Cette approche en tableau est l'une des nombreuses approches qui pourraient être utilisées par une organisation cherchant à mettre en œuvre les compétences.

### Analyse de données - Exemple 1

Le Tableau 1 ci-dessous est informatif et fournit un point de départ pour la construction d'une compétence. La compétence de l'exemple 1 a un nom et une description qui permettent à l'organisation d'identifier rapidement une compétence qui a de la valeur pour sa structure et son contexte organisationnels. En utilisant la méthode d'évaluation « démonstration en laboratoire» , l'organisation évalue un apprenant en lui fournissant un environnement de travail simulé pour accomplir les tâches qui répondent à ses objectifs professionnels. (Notez que le Tableau 1 utilise les Tâches de la version 2017 du référentiel NICE [2]).

**Tableau 1 : Exemple de création d'une nouvelle compétence en analyse de données avec les tâches existantes du référentiel NICE 2017**

| |
|---|
| **Nom de la compétence :** Analyse de données - Exemple 1 |
| **Description de la compétence :** Collecte, synthèse ou analyse de données et d'informations qualitatives et quantitatives provenant de diverses sources en vue de prendre une décision, de formuler une recommandation et/ou de rédiger des rapports, des notes d'information, des résumés analytiques et d'autres types de correspondance. |
| **Méthode d'évaluation :** Démonstration en laboratoire |
| **Description des Tâches** |
| T0007 \| Analyser et définir les exigences et les spécifications en matière de données. |
| 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). |

Dans l'exemple décrit dans le Tableau 1, une organisation peut donner à un apprenant un ordinateur contenant un ensemble de données particulier et connecté au réseau du laboratoire. L'apprenant a ensuite le temps de démontrer son aptitude à utiliser des langages open source pour appliquer des techniques quantitatives aux données. Une partie clef de cette évaluation peut consister à analyser l'ensemble des données pour s'assurer qu'elles répondent à une spécification particulière avant de terminer l'analyse. Grâce à cette évaluation, l'apprenant démontre la compétence « Analyse de données - Exemple 1» telle que définie par l'employeur.

Une compétence entièrement détaillée en matière d'analyse de données pourrait être beaucoup plus vaste. En énumérant les descriptions des tâches au sein de la compétence, l'organisation peut spécifier l'étendue souhaitée de la compétence. Pour faciliter l'utilisation, les Tâches sont référencées avec leurs identifiants du référentiel NICE 2017.

### Analyse de données - Exemple 2

Le Tableau 2, ci-dessous présente un autre point de départ pour la création d'une compétence. L'exemple est informatif ; la description est la même que celle du Tableau 1, mais cet exemple utilise des descriptions de connaissances et de capacités pour construire la compétence.

**Tableau 2 : Exemple de création d'une nouvelle compétence en analyse de données avec des tâches supplémentaires**

| |
|---|
| **Nom de la compétence :** Analyse de données - Exemple 2 |
| **Description de la compétence :** Collecte, synthèse ou analyse de données et d'informations qualitatives et quantitatives provenant de diverses sources en vue de prendre une décision, de formuler une recommandation et/ou de rédiger des rapports, des notes d'information, des résumés analytiques et d'autres types de correspondance. |
| **Méthode d'évaluation :** Test |
| **Description des Connaissances et Capacités** |
| S0013 \| Capacité à effectuer des requêtes et à développer des algorithmes pour analyser les structures de données. |
| 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). |
| S0091 \| Capacité à analyser des données volatiles. |
| K0020 \| Connaissance des politiques d'administration et de normalisation des données. |
| K0338 \| Connaissance des techniques d'exploration de données. |

Dans cet exemple, le Tableau 2 représente une compétence en analyse de données. Cette compétence pourrait être créée par un organisme de certification qui propose un test pour évaluer les apprenants. Le test peut être administré sur papier ou sur ordinateur. En réussissant le test, l'apprenant démontre la compétence « Analyse de données - Exemple 2» telle que définie par l'organisme de certification.

(Notez que le Tableau 2 utilise les descriptions de connaissances et capacités de la version 2017 du référentiel NICE [2]).

### 3.4 Fonctions

Les fonctions sont un cas d'utilisation courant du référentiel NICE. Les fonctions sont une manière de décrire un ensemble de tâches dont une personne est responsable ou dont elle doit rendre compte.

Alors que les référentiels précédents associaient les fonctions de travail à des spécifications de connaissances, de compétences et d'aptitudes, le référentiel NICE encourage une approche plus souple par le biais des tâches. Les fonctions sont composées de tâches qui constituent le travail à effectuer ; les tâches comprennent des descriptions de connaissances et de capacités qui représentent le potentiel de l'apprenant à effectuer ces tâches. Cette approche transitive, illustrée dans la Figure 4, favorise la flexibilité et simplifie la communication.

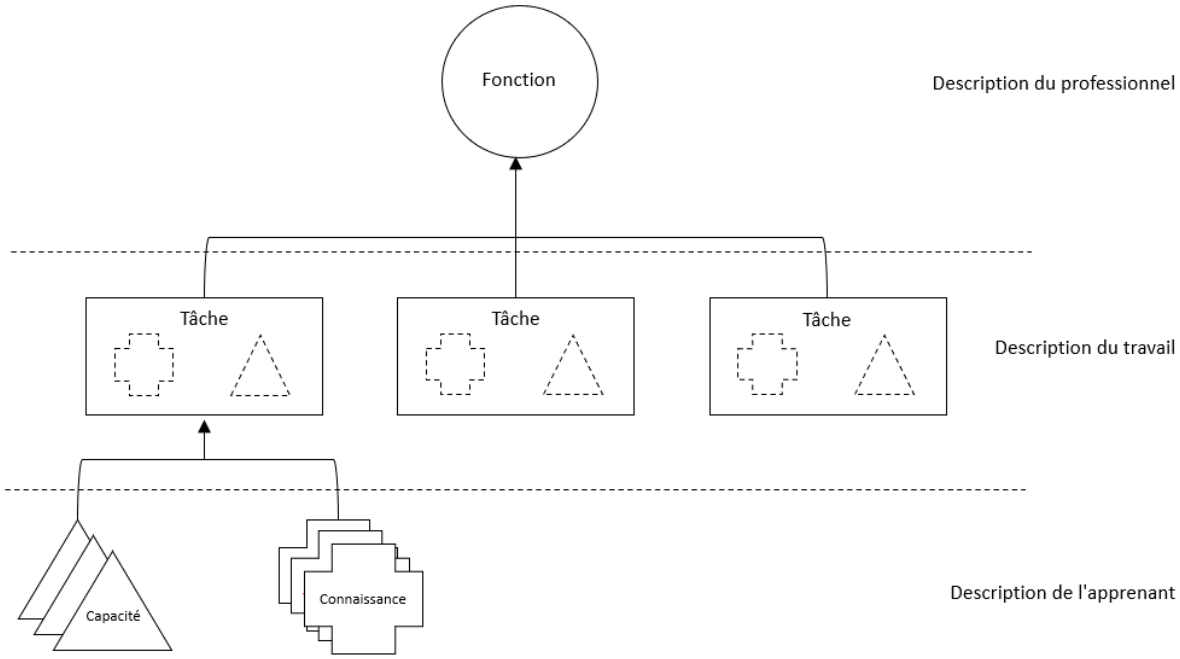


**Figure 4 : Liens entre les fonctions et les blocs de construction**

Les noms des fonctions ne sont pas synonymes d'intitulés de postes. Certaines fonctions peuvent coïncider avec un intitulé de poste, en fonction de l'utilisation des intitulés de poste par l'organisation. De même, les fonctions ne sont pas synonymes de professions.

Une seule fonction (par exemple, développeur de logiciels) peut s'appliquer à des personnes dont l'intitulé de poste est très varié (par exemple, ingénieur logiciel, codeur, développeur d'applications). Inversement, plusieurs fonctions peuvent être combinées pour créer un emploi particulier. Cette approche additive favorise une meilleure modularité et illustre le fait que tous les apprenants sur le marché du travail effectuent de nombreuses tâches dans diverses fonctions, quel que soit leur intitulé de poste. De même, le référentiel NICE ne définit pas de niveaux de compétence (par exemple, basique, intermédiaire, avancé). Ces attributs, ainsi que ceux concernant la compétence avec laquelle un apprenant effectue des tâches, sont laissés à d'autres modèles ou ressources.

### 3.4.1 Utilisation des fonctions existantes

Chaque fonction est destinée à soutenir la réalisation d'objectifs par le biais de tâches. Bien qu'une fonction puisse être associée à un ensemble prédéterminé de tâches, les utilisateurs peuvent inclure d'autres tâches existantes afin d'adapter les fonctions à leur propre contexte. De même, un utilisateur peut souhaiter s'inspirer des fonctions répertoriées ou en ajouter d'autres pour soutenir d'autres objectifs. L'ensemble actuel des composants du référentiel NICE est disponible au Centre de ressources du référentiel NICE [1].

Les utilisateurs sont invités à ne pas modifier en interne le nom et la description d'une fonction existante. Les fonctions sont destinées à favoriser l'interopérabilité, de sorte que la modification de leur contenu peut entraîner un désalignement ultérieur. Si une formulation différente est nécessaire, une nouvelle fonction peut être créée comme décrit ci-dessous.

### 3.4.2 Créer une nouvelle fonction

Les utilisateurs peuvent également créer de nouvelles fonctions afin d'adapter l'utilisation du référentiel NICE à leur propre contexte. Ces fonctions supplémentaires contribueront à la clarté et à la cohérence des discussions internes sur les travaux relatifs à la cybersécurité.

## 3.5 Equipes

De nombreuses organisations ont recours à des équipes pour relever collectivement des défis complexes en réunissant des personnes dont les compétences et l'expérience sont complémentaires. En utilisant des ressources et des perspectives différentes, les équipes permettent aux organisations de gérer les risques de manière globale. Les équipes tirent parti de la spécialisation des connaissances et des processus de chacun de leurs membres pour répartir efficacement le travail. Les équipes peuvent être définies à l'aide de fonctions ou de compétences.

### 3.5.1 Constituer des équipes avec des fonctions

Une approche pour la constitution d'équipes centrée sur les fonctions permet aux organisations de définir quels types de fonctions sont nécessaires pour atteindre les objectifs fixés. Étant donné que les fonctions sont elles-mêmes constituées de compétences, cette approche de la constitution d'équipes commence par le travail à accomplir. Cette approche peut être considérée comme « descendante» .

**Tableau 3 : Exemple d'une équipe de développement de logiciels sécurisée utilisant les fonctions du référentiel NICE 2017**

| Phase du cycle de vie | Fonction |
|---|---|
| Conception | SP-ARC-002 \| Architecte sécurité |
| Construction | SP-DEV-001 \| Développeur de logiciels |
| Déploiement | OM-NET-001 \| Spécialiste des opérations réseau |
| Exploitation | OM-STS-001 \| Spécialiste du support technique |
| Maintenance | OM-DTA-001 \| Administrateur de base de données |
| Décommissionnement | OV-LGA-001 \| Conseiller juridique cyber |

Tableau 3 ci-dessus montre comment créer une équipe de développement de logiciels sécurisée. Les fonctions sont référencées à l'aide de la version 2017 des identifiants des fonctions du référentiel NICE. Les équipes constituées de cette manière commencent par l'identification du travail à accomplir. Dans cet exemple, l'équipe de développement de logiciels sécurisés est organisée par phase du cycle de vie. La première ligne montre que l'équipe prendrait en compte les objectifs de la phase de conception, y compris la planification, et aurait donc besoin d'un architecte sécurité. Tableau 3 est un exemple informatif et ne couvre pas toutes les fonctions qui peuvent être présentes ou nécessaires pour une équipe donnée. Pour plus d'informations,

consultez le référentiel de développement de logiciels sécurisés du NIST (NIST's *Secure Software Development Framework*) [6].

**Tableau 4 : Exemple de création d'une équipe de cybersécurité à l'aide de fonctions du référentiel NICE 2017 et de nouvelles fonctions**

| Fonction du référentiel de Cybersécurité | Fonction |
|---|---|
| Identifier | NouvelleFonction1 \| Gestionnaire des risques |
| Protéger | SP-RSK-002 \| Contrôleur de sécurité |
| Détecter | PR-CDA-001 \| Analyste en cyberdéfense |
| Répondre | PR-CIR-001 \| Intervenant sur les incidents de cyberdéfense |
| Récupérer | NouvelleFonction2 \| Spécialiste des Communications |

Tableau 4 décrit un exemple d'équipe de cybersécurité. Comme l'équipe de développement de logiciels sécurisés, cette équipe est constituée à partir d'une approche centrée sur le travail. En utilisant le cœur du référentiel pour l'amélioration de la cybersécurité des infrastructures critiques (Framework for Improving Critical Infrastructure Cybersecurity), les objectifs de cybersécurité sont sélectionnés, les tâches sont identifiées pour atteindre ces objectifs et les fonctions sont sélectionnées pour définir les rôles nécessaires à la réalisation de ces objectifs [7]. Tableau 4 est un exemple informatif et ne couvre pas toutes les fonctions qui peuvent être présentes ou nécessaires pour une équipe donnée. Deux nouvelles fonctions sont ajoutées pour montrer une approche mixte consistant à utiliser les fonctions existantes (Section 3.4.1) et à créer de nouvelles fonctions (Section 3.4.2). En créant de nouvelles fonctions, l'exemple illustre une approche souple et flexible de l'adaptation du référentiel NICE.

### 3.5.2 Constituer des équipes avec des compétences

Les équipes peuvent également être constituées sur la base des compétences. Cette approche part du principe que les tâches individuelles peuvent être inconnues, mais que les types de compétences nécessaires pour relever le défi sont connus. Cette approche peut être considérée comme « ascendante» . Par conséquent, les équipes constituées de cette manière peuvent aider à identifier les apprenants susceptibles de participer au travail de l'équipe à l'avenir. Ces apprenants peuvent être associés ou non à une fonction et possèdent simplement les compétences nécessaires pour contribuer à la réalisation des objectifs de l'organisation.

Par exemple, une équipe de cybersécurité défensive qui utilise ses compétences pour imiter les techniques d'attaque des adversaires (c'est-à-dire une « Red Team» ) peut être composée des compétences théoriques suivantes :

- Planification de l'engagement
- Règles d'engagement
- Test d'intrusion
- Collecte de données
- Exploitation des vulnérabilités

En créant des équipes ou d'autres groupements de TKS, chaque organisation peut adapter le référentiel NICE de manière à mieux appliquer et communiquer sur les apprenants (et le travail que ces apprenants effectueront) pour permettre la réalisation des objectifs de la mission

# 4 Conclusion

Grâce à l'application de l'approche modulaire décrite dans le référentiel NICE, les utilisateurs peuvent bénéficier d'une méthode cohérente pour organiser et communiquer le travail à effectuer par le biais d'énoncés de tâches et des connaissances et compétences des apprenants qui soutiennent ce travail. Le référentiel NICE aide à guider les efforts des employeurs pour décrire le travail de cybersécurité, ceux des prestataires de formation pour préparer les professionnels de la cybersécurité, et ceux des apprenants pour démontrer leurs capacités à effectuer un travail de cybersécurité.

La capacité à décrire les tâches, les connaissances et les compétences est importante pour garantir une compréhension globale du travail et des effectifs. Le référentiel NICE fournit une ressource de référence évolutive qui peut être appliquée et utilisée par diverses organisations ou secteurs pour décrire le travail à effectuer dans de nombreux domaines. Les avantages pour ces organisations s'inscrivent dans la mission de l'initiative NICE, qui consiste à dynamiser, promouvoir et coordonner une communauté solide travaillant ensemble pour faire progresser un écosystème intégré d'éducation, de formation et de développement des ressources humaines dans le domaine de la cybersécurité.

## Références

[1] National Initiative for Cybersecurity Education (2020) *NICE Framework Resource Center*. Available at https://www.nist.gov/nice/framework

[2] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. https://doi.org/10.6028/NIST.SP.800-181

[3] National Institute of Standards and Technology (2020) *National Online Informative References Program*. Available at https://csrc.nist.gov/projects/olir

[4] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[5] Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. *Theory Into Practice*, 41(4), 212-218. Available at https://www.depauw.edu/files/resources/krathwohl.pdf

[6] Dodson DF, Souppaya MP, Scarfone KA (2020) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.04232020

[7] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

## Annexe A—Acronymes

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

| | |
|---|---|
| ERM | Enterprise Risk Management |
| FISMA | Federal Information Security Modernization Act |
| FOIA | Freedom of Information Act |
| ITL | NIST Information Technology Laboratory |
| K&S | Knowledge and Skill statement(s) |
| NICE | National Initiative for Cybersecurity Education |
| NIST | National Institute of Standards and Technology |
| OLIR | Online Informative Reference |
| OMB | Office of Management and Budget |
| SSDF | Secure Software Development Framework |
| TKS | Task, Knowledge, and Skill statements |

## Annexe B—Glossaire

*Pour un glossaire complet, veuillez consulter le site https://csrc.nist.gov/glossary.*

**Compétence** Mécanisme permettant aux organisations d'évaluer les apprenants.

**Connaissances** Ensemble de concepts qu'on peut retrouver dans la mémoire.

**Capacité** Capacité à effectuer une action observable.

**Tâche** Activité visant à atteindre les objectifs de l'organisation.