Référentiel de Compétences Cybersécurité : BenchMark

11-2016

Plan

- Contexte
- Définition « compétence »
- Etat de l'art: référentiel compétence en cybersécurité
- Le projet « Référentiel de compétences cybersécurité

Contexte

Cybersécurité

Economique

- Besoin et impact grandissant sur l'économie
- Marché en évolution permanente au niveau de la cybersécurité

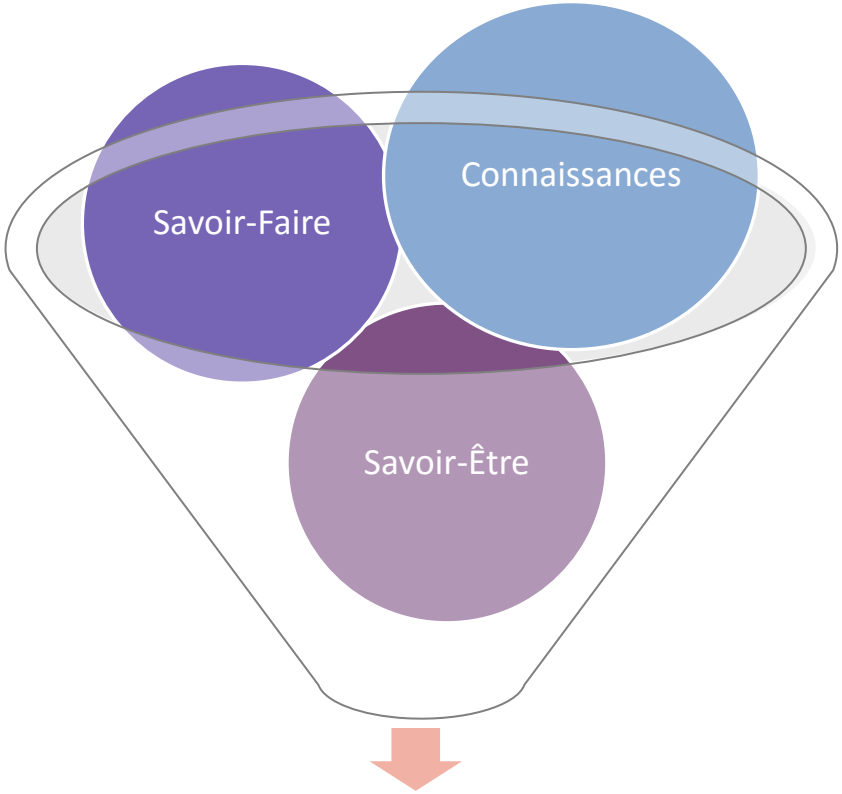
Technologique

- Exigence en termes de compétences de plus en plus élevée
- Technologie en perpétuelle évolution de façon accélérée

Formation Universitaire

- Pas de centralisation des programmes de formations en cybersécurité
- Définition différente des compétences à acquérir au niveau de la cybersécurité d'un établissement à un autre

Définition d'une « Compétence »

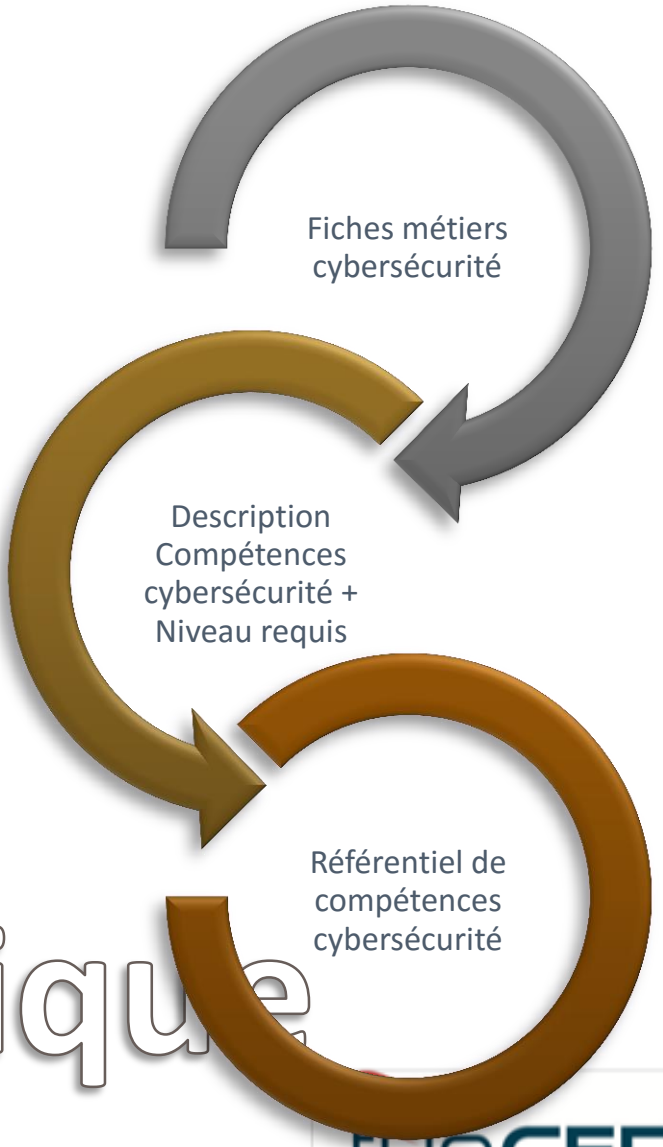


- **E-CF (Eu):** « Une compétence est une capacité démontrée à appliquer des connaissances, des savoir-faire et des savoir-être en vue d'obtenir des résultats observables»

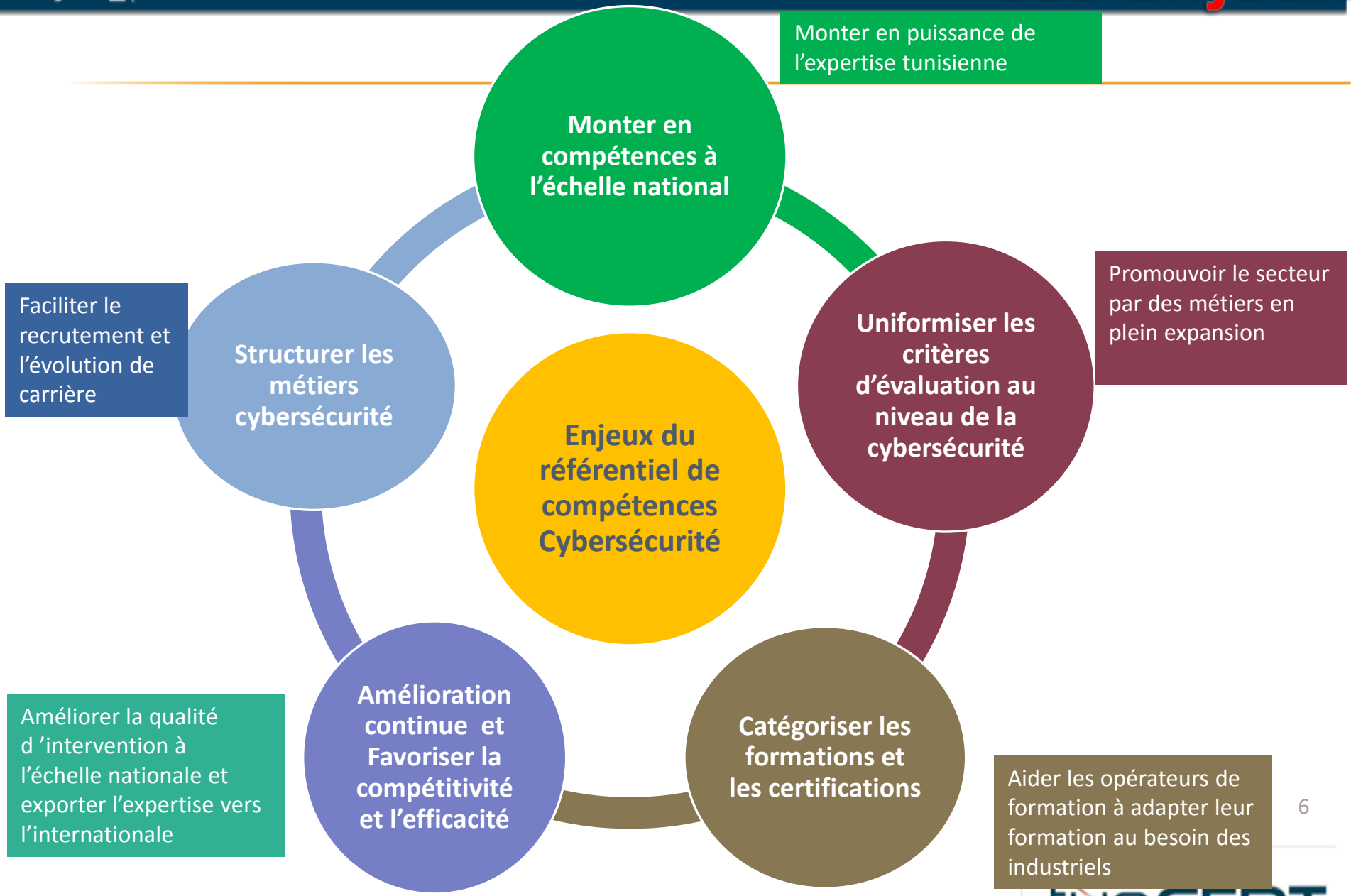
- **Department of Labor's Employment and Training Administration (US) :** « The capability of applying or using knowledge, skills, abilities, behaviors and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position »

Problématique

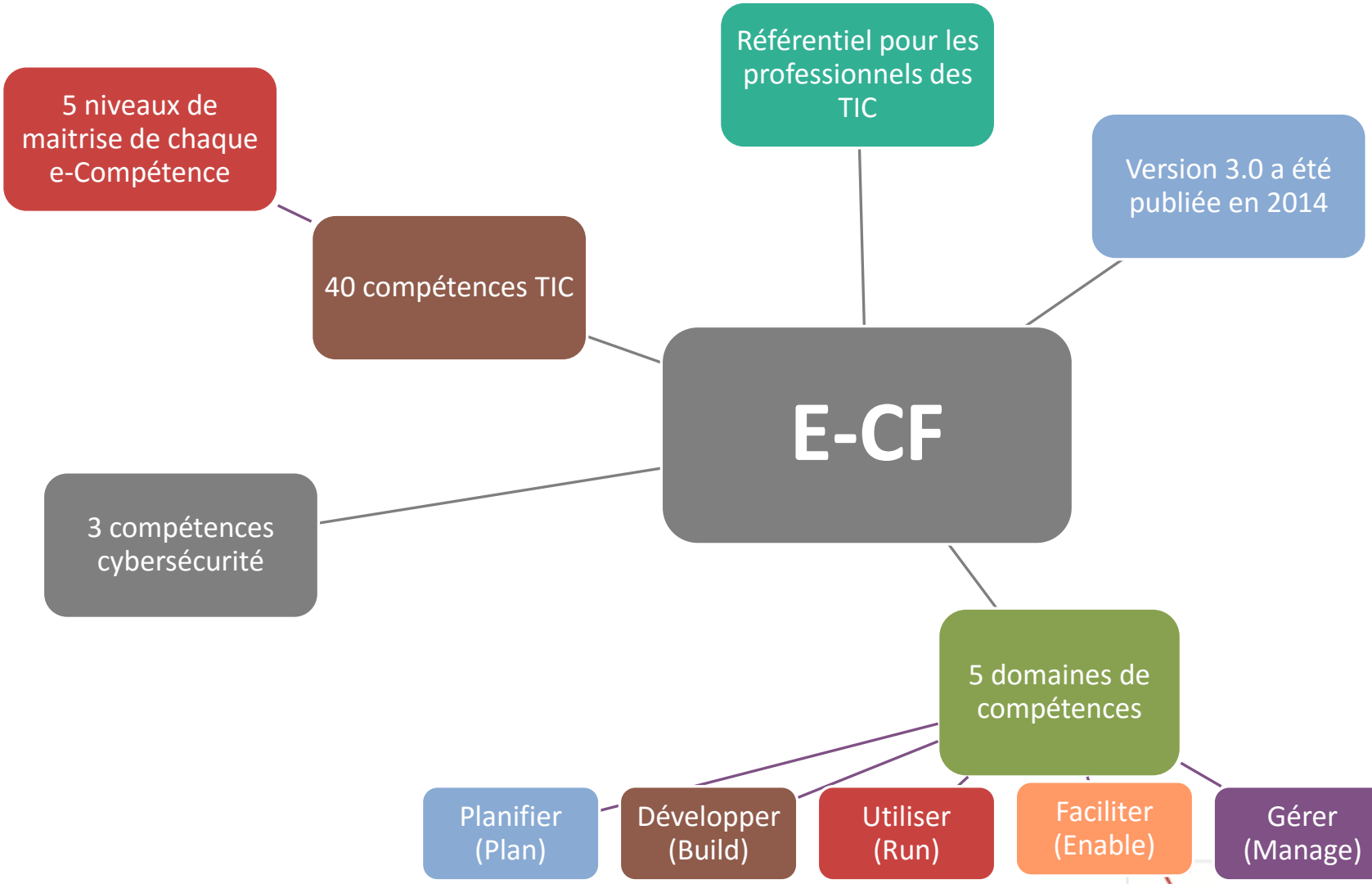
» **Absence de référentiel de compétence cybersécurité** adapté à l'échelle national permettant le **renforcement** des compétences cybersécurité



Les Enjeux


Monter en puissance de l'expertise tunisienne
Monter en compétences à l'échelle national
Promouvoir le secteur par des métiers en plein expansion
Uniformiser les critères d'évaluation au niveau de la cybersécurité
Faciliter le recrutement et l'évolution de carrière
Structurer les métiers cybersécurité
Enjeux du référentiel de compétences Cybersécurité
Améliorer la qualité d 'intervention à l'échelle nationale et exporter l'expertise vers l'internationale
Amélioration continue et Favoriser la compétitivité et l'efficacité
Catégoriser les formations et les certifications
Aider les opérateurs de formation à adapter leur formation au besoin des industriels

Etat de l'art: référentiel compétence en cybersécurité


Référentiel pour les professionnels des TIC
5 niveaux de maitrise de chaque e-Compétence
Version 3.0 a été publiée en 2014
40 compétences TIC
E-CF
3 compétences cybersécurité
5 domaines de compétences
Planifier (Plan)
Développer (Build)
Utiliser (Run)
Faciliter (Enable)
Gérer (Manage)

e-CF: 3 Compétences Cybersécurité

- **Développement d'une stratégie de sécurité de l'information:**
  - **e4**: Met en œuvre un niveau élevé d'expertise et exploite au mieux les normes et les bonnes pratiques reconnues
  - **e5**: conduit la stratégie pour ancrer la sécurité de l'information dans la culture de de l'organisation

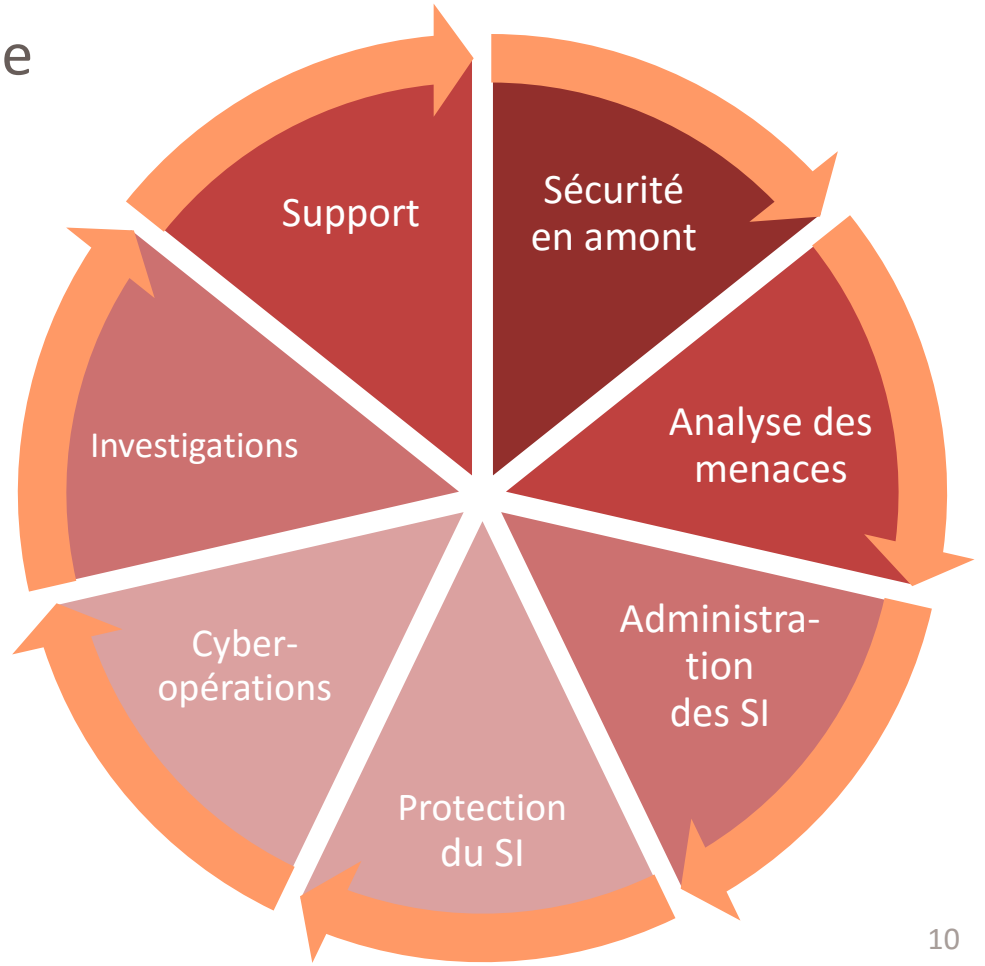
- **Gestion des risques:**
  - **e2**: Comprend et applique les principes de gestion des risques et recherche des solutions informatiques permettant de limiter les risques identifiés.
  - **e3**: Décide des actions nécessaires pour adapter la sécurité et gérer l'exposition au risque. Evalue, gère et garantit le traitement des exceptions. Audite les processus et l'environnement informatique.
  - **e4**: Définit et fait appliquer une politique de gestion des risques en tenant compte de toutes les contraintes potentielles, y compris techniques, économiques et politiques. Délègue les responsabilités.

- **Gestion de la sécurité de l'information :**
  - **e2**: Analyse de manière systématique l'environnement pour identifier et définir les failles et les menaces. Consigne et fait remonter à ses supérieurs les non-conformités.
  - **e3**:Evalue les mesures et indicateurs de gestion de la sécurité et décide s'ils sont conformes à la politique de sécurité de l'information de l'entreprise. Etudie et suscite des mesures correctives destinées à répondre à toute atteinte à la sécurité.
  - **e4**:Est responsable de l'intégrité, de la confidentialité et de la disponibilité des données stockées dans le système d'information et répond à toutes les obligations juridiques.

Référentiel des Métiers et Compétences Cybersécurité : CEIS(*)

» Etude réalisée en 2013 pour le compte de la Délégation aux Affaires Stratégiques DAS (Ministère de la Défense Française)

- Ce référentiel classifie les métiers cybersécurité selon 7 grandes fonctions cybersécurité:



(*) CEIS : la Compagnie Européenne d'Intélligence Stratégique

- A chaque fonction des métiers cybersécurité est associée une liste des métiers liées.

- **60 fiches métiers** liés au domaine **cybersécurité et IT**

- Ce référentiel **ne cite pas** les **compétences** nécessaires associées à chaque fiche métiers.

Référentiel des Métiers et Compétences Cybersécurité : CEIS

Fonction	Détail	N°	Emplois types
1. Sécurité en amont	a) R&D	E1	Ingénieur R&D
	b) Assurances, audit et compliance	E2	Assureur qualité
		E3	Auditeur organisationnel
		E4	Auditeur conformité
		E5	Professionnel qualité
		E6	Auditeur technique
	c) Anticipation du risque	E7	Consultant / expert gestion du risque
		E8	Gestionnaire de Risques
		E9	Consultant gestion de crise
	d) Architecte des infrastructures et systèmes d'information	E10	Architecte système
		E11	Architecte réseau
		E12	Architecte application
		E13	Développeur
		E14	Architecte sécurité
		E15	Référent sécurité projet
		E16	cryptologue

Référentiel NCWF (NICE Cybersecurity Workforce Framework) US

Le référentiel NCWF identifie :

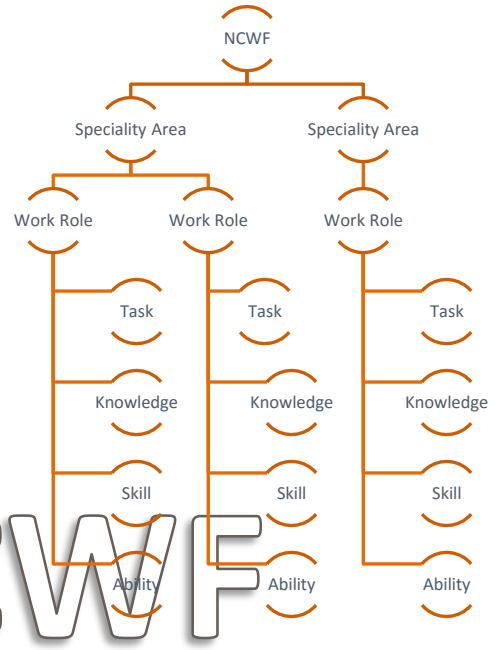
Les fonctions haut niveau communs en cybersécurité sont regroupées en catégories

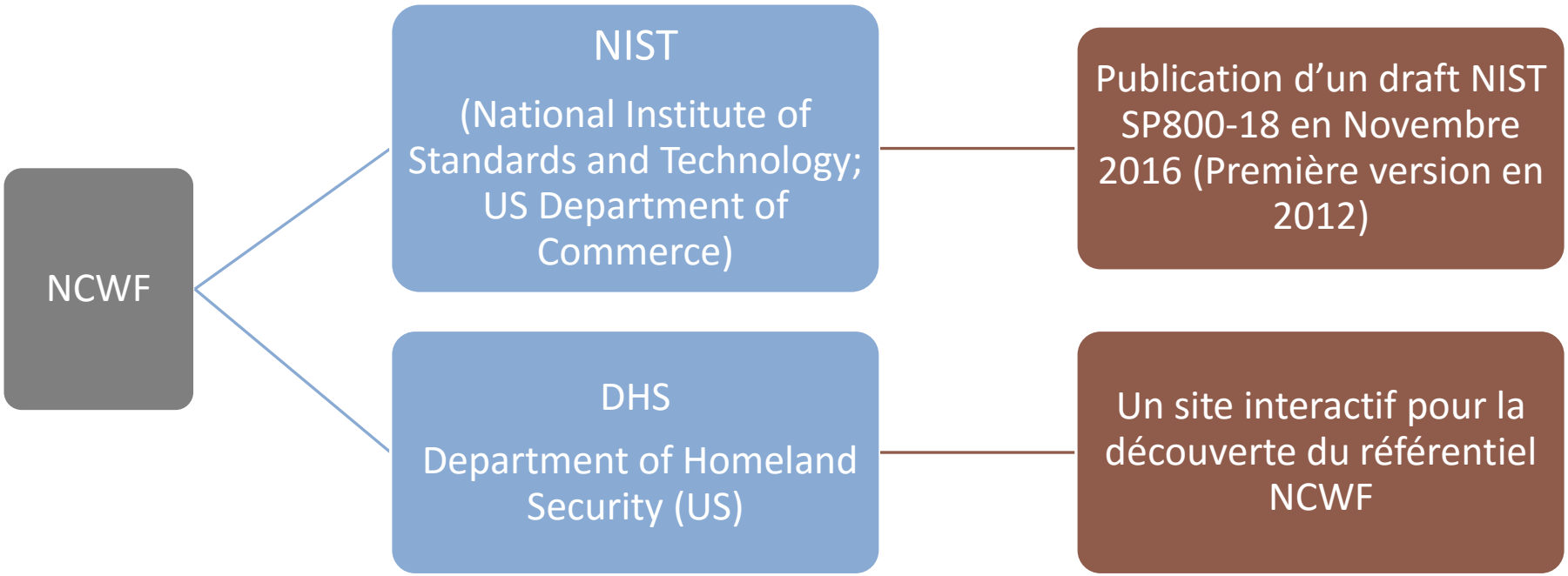
(**7 catégories**)

A chaque catégorie, des domaines de spécialité sont associés

(**31 domaines de spécialité**)

Pour chaque domaines de spécialité, NCWF associe : une description des **tâches**, des **connaissances**, **savoir-faire** et **aptitudes**




NCWF
NIST
(National Institute of Standards and Technology; US Department of Commerce)
Publication d'un draft NIST SP800-18 en Novembre 2016 (Première version en 2012)
DHS
Department of Homeland Security (US)
Un site interactif pour la découverte du référentiel NCWF

Référentiel NCWF (US)

» Les sept catégories de la cybersécurité proposé par le référentiel NCWF sont :

Securely Provision	• Concevoir et construire des systèmes IT sécurisées (c'est-à-dire, responsable d'un certain aspect de développement de systèmes)
Operate and Maintain	• Assistance, administration et maintenance nécessaire pour assurer la performance et la sécurité des systèmes IT
Protect and Defend	• Identification, analyse et réduction des menaces des systèmes IT ou des réseaux l'information
Investigate	• Enquêter sur les évènements et/ou les crimes cybernétiques dans les systèmes IT, réseaux et preuves numériques
Collect and Operate	• Les opérations spéciales de déni et d'escroquerie, et la collection des informations de la cybersécurité qui peuvent être utilisées pour le développement de l'intelligence
Analyze	• La revue très spécialisée et l'évaluation des informations entrantes de la cybersécurité afin de déterminer son utilité pour l'intelligence
Oversee and Govern	• Le leadership, la gestion, la direction, le développement et la défense des intérêts pour que les individus et les organisations puissent efficacement conduire le travail de cybersécurité

» Exemple NIST: « NCWF Work Role »

Work Role ID	PR-IR-001
Category	Protect and Defend (PR)
Speciality Area	Incident Response (IR)
Work Role Name	Cyber Defense Incident Responder (531)
Work Role Description	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Tasks	T0041, T0047, T0161, T0163, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0333, T0395, T0503, T0510
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0225, K0230, K0259, K0287, K0332
Skills	S0003, S0047, S0077, S0078, S0079, S0080, S0173
Abilities	[None specified]

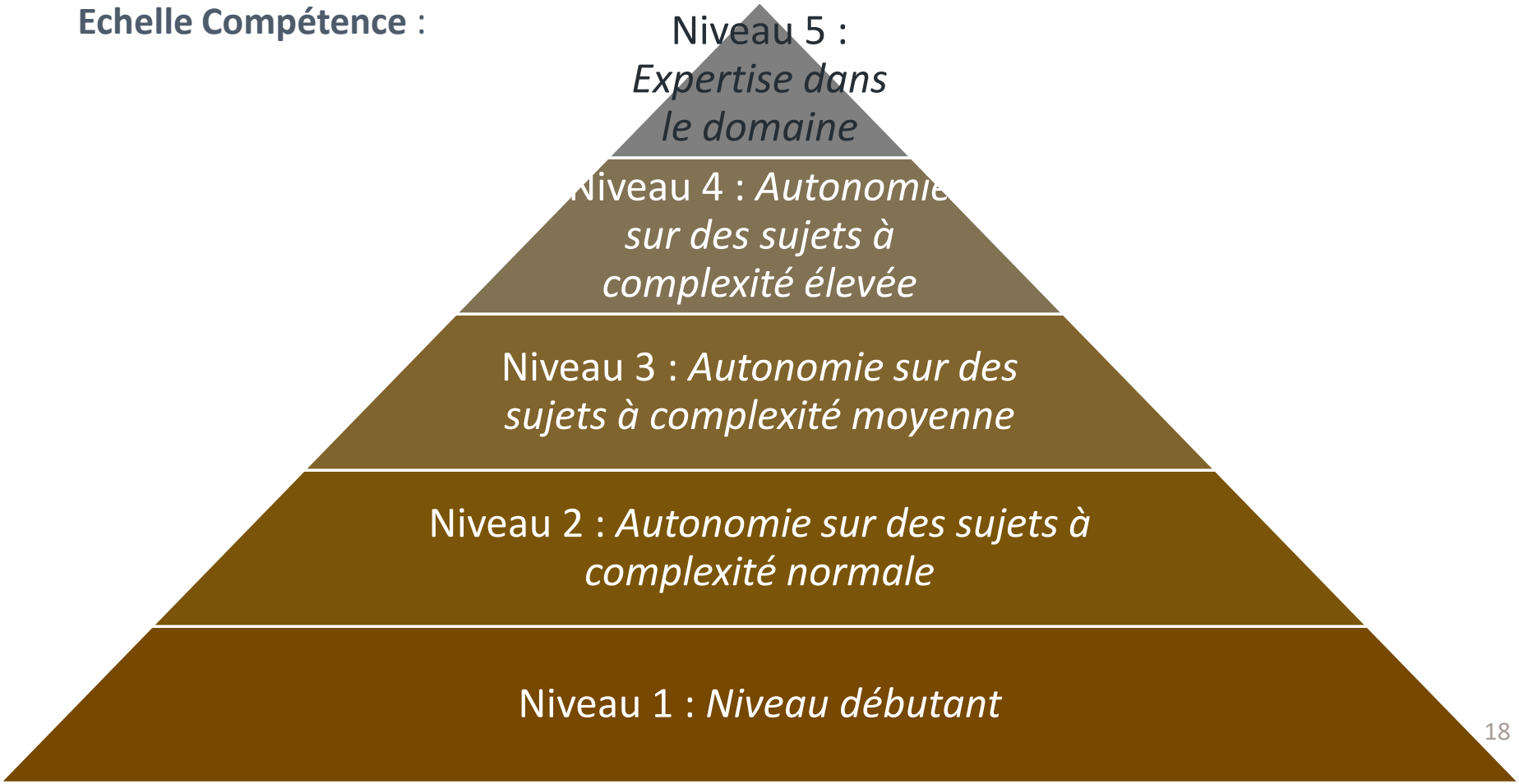
» Exemple NIST: « NCWF Work Role »

Work Role ID	PR-IR-001
Category	Protect and Defend (PR)
Speciality Area	Incident Response (IR)
Work Role Name	Cyber Defense Incident Responder (531)
Work Role Description	Investigates, analyzes, and responds to cyber incidents within the network environment or enclave.
Tasks	T0041, T0047, T0161, T0163, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0333, T0395, T0503, T0510
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0225, K0230, K0259, K0287, K0332
Skills	S0003, S0047, S0077, S0078, S0079, S0080, S0173
Abilities	[None specified]

T0041	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.
K0026	Knowledge of disaster recovery continuity of operations plans.
S0003	Skill of identifying, capturing, containing, and reporting malware

Le projet « Référentiel de compétences cybersécurité

Echelle Compétence :



» Le projet référentiel de compétence cybersécurité définit :

- ❖ 5 niveaux de compétences (N1 ..N5)
- ❖ Grille d'évaluation de chaque niveau
- ❖ Passage d'un niveau à un autre

Moyennant :

- ➢ Formations universitaires / professionnelles
- ➢ Certifications
- ➢ Expériences

Exemple Fiche compétence cybersécurité

Fiche Compétence Cybersécurité					
Nom de la compétence	G1: Gestion de l'incident				
Description générique	Gérer les incidents de sécurité à temps en prenant connaissance de leur cycle de vie.				
Niveau de la compétence De N1 à N5	N1	N2	N3	N4	N5
		Analyse l'environnement d'une manière systématique pour identifier les incidents	Évalue et surveille les incidents de sécurité survenus au sein de l'entreprise	Est responsable de la surveillance et la gestion des incidents de sécurité survenus au sein de l'entreprise	
Connaissance	C1: continuité des opérations et la reprise après sinistre C2: la réponse aux incidents et les procédures de gestion de l'incident				
Savoir-faire	S1: récupération des serveurs défaillants S2: l'analyse de la racine de l'incident				