ceis

QUEL RÉFÉRENTIEL POUR LES MÉTIERS DE LA CYBERSÉCURITÉ ?

Décembre 2014

Les notes otratégiques

LES NOTES STRATÉGIQUES

Policy Papers – Research Papers

Cette note stratégique est tirée de l'Etude de Prospective Stratégique (EPS) n°2013-01 intitulée « quelles sont les évolutions possibles de la gestion du personnel de défense pour lutter efficacement dans le cyberespace ? » et réalisée par CEIS pour le compte de la Délégation aux Affaires Stratégiques du ministère de la Défense.

Le référentiel présenté s'inspire également les travaux réalisés dans le cadre du groupe de travail 3 du Réseau cyberdéfense de la Réserve Citoyenne.

TABLE DES MATIÈRES

INTRODUCTION

L'intérêt d'un référentiel est multiple : développer d'une vision partagée ; structurer les cursus de formation ; faciliter l'orientation des personnes intéressées ; faciliter l'émission d'offres d'emploi et donc la recherche de candidats adaptés. Disposer d'un référentiel permet en outre d'orienter le marché en fonction de ses besoins et est donc très intéressant en termes d'influence.

Attention, cependant, à éviter plusieurs écueils. Il n'existe de référentiel miracle, universel et adapté à toutes les situations. Une partie de ce référentiel sera spécifique aux organisations considérées, du fait des particularités de celles-ci et de leurs contraintes. De plus, il convient de régulièrement mettre à jour ce référentiel en fonction du marché et de l'évolution des concepts opérationnels. Il s'agit de ne pas construire un référentiel trop « globalisant » ; le terme « cyber » renvoie ainsi à des réalités très différentes et trop larges. Enfin, un référentiel n'est pas autonome au sens où les emplois et compétences qu'il catégorise et décrit ont nécessairement des liens avec d'autres activités.

L'objectif est donc de disposer d'un référentiel adapté à son organisation avec un niveau de granularité suffisant pour que l'ensemble des acteurs s'y retrouvent facilement. Ce référentiel doit être partagé et cohérent, au moins en partie, avec les autres acteurs du marché sur lequel on évolue. Il doit être ciblé sur l'ensemble des emplois liés à la sécurité et à la confiance numérique. Son scope doit cependant dépasser la cybersécurité pour prendre en compte également les aspects « métiers » de l'organisation concernée.

1. LES ÉLÉMENTS CLÉS D'UN RÉFÉRENTIEL

1.1. Les métiers

Un référentiel des métiers de la cybersécurité se doit d'être le plus opérationnel possible. Distinguer les métiers selon leur statut ne suffit pas. Une telle segmentation, prise isolément, nuit à l'efficacité en privilégiant une vision hiérarchique, souvent contre-productive, au détriment d'une vision globale mettant en avant la complémentarité des métiers.

A contrario, une classification opérationnelle des métiers permet :

- Une vision globale de la gestion de la menace ;
- Une traduction opérationnelle de la stratégie vers les métiers ;
- Une meilleure gestion des effectifs grâce à l'identification des écarts entre les besoins et la réalité ;
- Une mise à jour plus aisée et flexible, adaptable aux mutations de la cybermenace, en évolution constante ;
- Une gestion plus efficace des compétences clés, directement adaptées aux besoins métiers, besoins métiers eux-mêmes calqués sur la stratégie plus globale de cybersécurité.

La définition des métiers dépend du canevas développé dans le droit fil de la stratégie élaborée. Les fonctions suivantes peuvent être reprises afin de classer les différents métiers de la cybersécurité :

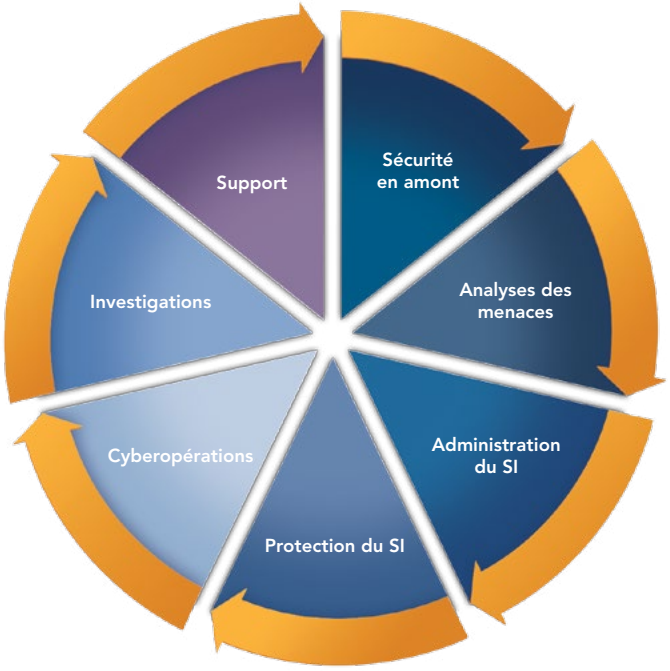
1. La sécurité en amont
2. L'analyse des risques et menaces
3. L'administration et la maintenance du SI
4. La protection du SI
5. Les opérations cyber
6. L'investigation numérique

A ces 6 fonctions de la cybersécurité, peuvent être ajoutées les fonctions support suivantes :

- Conseil et appui juridique
- Vente
- Marketing
- Entrainement et formation

Ces fonctions sont complémentaires et interdépendantes. Elles se recoupent et se superposent tout au long du cycle de gestion de la menace. A ces fonctions sont associés des emplois types.

Figure 1. Schéma récapitulatif : exemples de grandes fonctions de la cybersécurité



1.2. Les compétences et « talents » ou « appétences »

Déterminer les fonctions clés du référentiel permet de définir une vision globale des métiers de la cybersécurité. Les catégories ainsi définies reflètent une vision, une perception de la fonction cybersécurité, et une stratégie. Il est également important de référencer les compétences, talents ou appétences des personnels, afin d'orienter au mieux leur carrière en leur proposant les formations adaptées à leur profil et correspondant à leurs ambitions.

Si la matrice des compétences est le document le plus objectif à réaliser, une matrice des talents et appétences est également importante afin de mieux comprendre les profils et leurs ambitions.

Figure 2. Extraits de matrice de compétences générales

Types de compétences	Compétences
Conception	Développement
	Architecture
Intégration	Déploiement des systèmes
	Intégration des systèmes
Juridique et normatif	Régulation et législation
	Maîtrise des outils SSI (PSSI, charte, etc.)
	Normes et conformité
	Veille et intelligence juridique
	Données à caractère personnel
	Propriété intellectuelle
	Droit pénal informatique
	Règlementations sectorielles
	Droit du travail
	Export et relations internationales

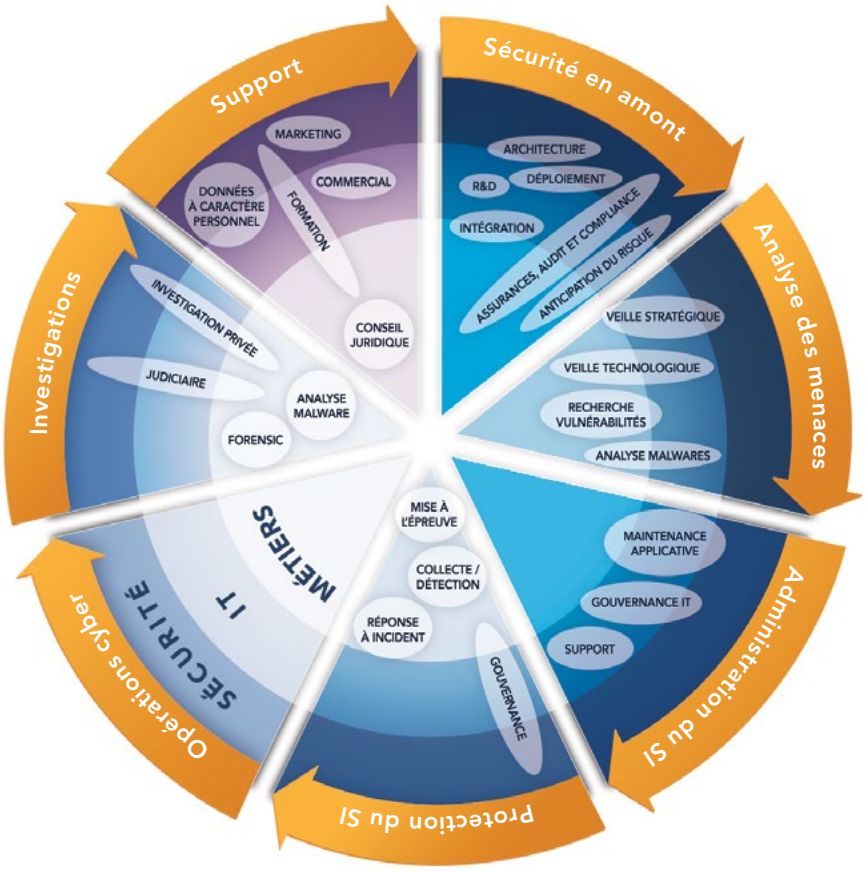
1.3. Le croisement des métiers et des compétences

Pour accompagner la mobilité, il est indispensable de flécher un parcours cohérent et réaliste. Pour ce faire, le référentiel métier peut indiquer auprès de chaque poste, à l'aide d'indicateurs, la densité métier, IT ou sécurité nécessaire.

- L'indicateur de « densité IT » traduit la part plus ou moins technique du métier ;
- L'indicateur de « densité sécurité » indique l'importance de la culture sécurité ;
- L'indicateur de « densité métier » souligne l'importance de la connaissance du secteur d'activité constituant l'environnement de travail du professionnel de la cybersécurité.

Ces indicateurs sont mis en correspondance avec les compétences et talents requis pour chacun des postes. La présence ou l'absence de telle compétence ou tel talent permettra d'évaluer, in fine, la densité IT, sécurité ou métier d'un poste en cybersécurité.

Figure 3. Récapitulatif des métiers selon leur densité



2. PROPOSITION DE RÉFÉRENTIEL

Fonctions	Détails	N°	Emplois types	Indicateurs - densité		
				IT	Sécurité	Métier
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) Architecture 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	Chef de projet (MoE/MoI)	■	■	■
		E17	Cryptologue	■	■	■
	e) Intégration	E18	Développeur / concepteur	■	■	■
		E19	Chef de projet	■	■	■
		E20	Intégrateur	■	■	■
	f) Déploiement	E21	Technicien réseau-télécoms	■	■	
		E22	Intégrateur d'exploitation	■	■	

2. Analyse des menaces	a) Veille technologique et menaces	**E23**	Consultant cybersécurité			
	b) Veille stratégique	**E24**	Veilleur cybersécurité			
	c) Recherche en vulnérabilités	**E25**	Analyste cybersécurité			
	d) Analyse de malware et modes opératoires	**E26**	Chercheur			
3. Administration et gouvernance du SI	a) Maintenance applicative	**E27**	Responsable maintenance applicative			
	b) Gouvernance IT	**E28**	Administrateur système			
		E29	Administrateur réseau			
		E30	Responsable d'exploitation			
		E31	Responsable PCA/PRA			
		E32	Administrateur data			
	c) Support utilisateurs	**E33**	Assistant fonctionnel			
		E34	Technicien IT			
4. Protection du SI	a) Gouvernance et exploitation SSI	**E35**	Ingénieur sécurité			
		E36	RSSI			
		E37	Administrateur sécurité			
		E38	Technicien sécurité			
		E39	Télé-assistant			
		E40	Expert produit/technologie (IAM, MDM, IDS, IPS, etc.			
	b) Mise à l'épreuve	**E41**	Pentesteur			
	c) Collecte et détection	**E42**	Ingénieur spécialiste collecte et analyse de log			
		E43	Ingénieur chargé d'analyse en détection d'intrusions			
	d) Réponse à incident	**E44**	Ingénieur en charge de la réponse aux incidents			

5. Cyberopérations						
6. Investigations	a) Inforensique	E45	Expert forensic			
		E46	Expert recovery			
	b) Analyse de malware et modes opératoires	E47	Ingénieur reverse			
		E48	Ingénieur analyste en vulnérabilités et codes malveillants			
	c) Acteurs judiciaires	E49	Police judiciaire			
		E50	Magistrature			
		E51	Conseil juridique			
	d) Privés	E52	Investigateurs de droit privé			
Appui juridique	a) Protection des données à caractère personnel	E53	Correspondant informatique et libertés			
	b) Conseil juridique NTIC	E54	Avocat			
		E55	Juriste d'entreprise			
		E56	Juriste cyberdéfense			
Marketing et communication		E57	Responsable Marketing et communication			
Commercial	Avant-vente	E58	Ingénieur technico-commercial			
	Vente	E59	Responsable commercial			
Formation et entrainement		E60	Formateur			

ceis

Déjà parus :

Cybercriminalité et réseaux sociaux : liaisons dangereuses
Janvier 2015 - english version available

NetMundial, un pas décisif dans l'évolution de
la gouvernance Internet ? Décembre 2014

Cybersécurité des pays émergents Décembre 2013

L'entrainement cyber, un élément clé pour améliorer
la résilience Décembre 2013

Monnaies virtuelles et cybercriminalité
Novembre 2013 – english version available

De l'Union douanière à l'Union eurasiatique, état et perspectives
d'intégration dans l'espace post-soviétique Octobre 2013

PME et marchés de défense – le SIA LAB, une initiative au service
de l'accès des PME aux marchés de défense Août 2013

La coopération technologique et industrielle de défense
et de sécurité du Brésil Mai 2013

Une nouvelle approche du terrorisme. Mieux comprendre le profil
des groupes terroristes et de leurs membres Mai 2013

Le financement de la R&D de défense
par l'Union européenne Avril 2013

Les drones et la puissance aérienne future Février 2013

Compagnie Européenne d'Intelligence Stratégique (CEIS)

Société Anonyme au capital de 150 510 € - SIRET : 414 881 821 00022 – APE : 741 G

280 boulevard Saint Germain – 75007 Paris
Tél. : 01 45 55 00 20 – Fax : 01 45 55 00 60

www.ceis.eu