Agence Nationale de la Sécurité Informatique

Référentiels des Compétences en Cybersécurité

Date : Septembre 2017

Sommaire

Introduction

Aujourd'hui, l'utilisation des TIC s'est multipliée dans tous les domaines (éducation, e-commerce, industrie, santé, services publiques, banques …), et la connexion des objets qu'on utilise quotidiennement à Internet est devenu une tendance (contrôle à distance des équipements industrielles et domotiques, voiture connectée …), surtout avec l'avènement de l'Internet des Objet (Internet of Things). Cette révolution technologique a augmenté aussi le nombre et la complexité des menaces cybernétiques. Par conséquent, la cybersécurité est devenu un vrai défi.

Sur ce, la Tunisie doit se munir des moyens pour monter en compétences au niveau national dans le domaine de la sécurité de l'information puisque les demandes des profils spécifiques des experts en cybersécurité vont être multipliées ces prochaines années.

Consciente de l'enjeu et de la criticité de cet axe, l'Agence Nationale de la Sécurité Informatique (ANSI) a préparé un référentiel des compétences en cybersécurité. L'objectif de ce référentiel est de structurer et promouvoir les métiers de la cybersécurité, et favoriser la montée en puissance de l'expertise tunisienne. Ce référentiel permet aussi aux opérateurs de formations d'adopter leurs formations au besoin du marché.

Ce référentiel a été élaboré suite à un benchmark réalisé par l'ANSI sur les référentiels des compétences et métiers dans le domaine des TIC et cybersécurité.

Les enjeux :

Ce référentiel est un outil qualitatif afin d'ajuster les compétences aux exigences.

Il permet de :

- structurer les métiers cybersécurité et faciliter le recrutement et l'évolution de carrière
- monter en compétences à l'échelle national ; et monter en puissance de l'expertise tunisienne
- uniformiser les critères d'évaluation au niveau de la cybersécurité afin de promouvoir le secteur par des métiers en plein expansion
- catégoriser les formations académiques et professionnelles pour aider les opérateurs de formation à adapter leur formation au besoin des industriels
- catégoriser les certifications professionnelles en relation avec les organismes de certification
- amélioration continue et favoriser la compétitivité et l'efficacité (améliorer la qualité d'intervention à l'échelle nationale et exporter l'expertise vers l'internationale

Les domaines :

Ce référentiel classifie les grandes fonctions de la cybersécurité en huit domaines :

1. Gouvernance
2. Gestion des risques, audit, conformité et continuité d'activités
3. Sécurité des réseaux
4. Sécurité des applications
5. Sécurité des systèmes et architecture de sécurité
6. Sécurité des données
7. Les opérations de sécurité
8. Aspect juridique et règlementaire

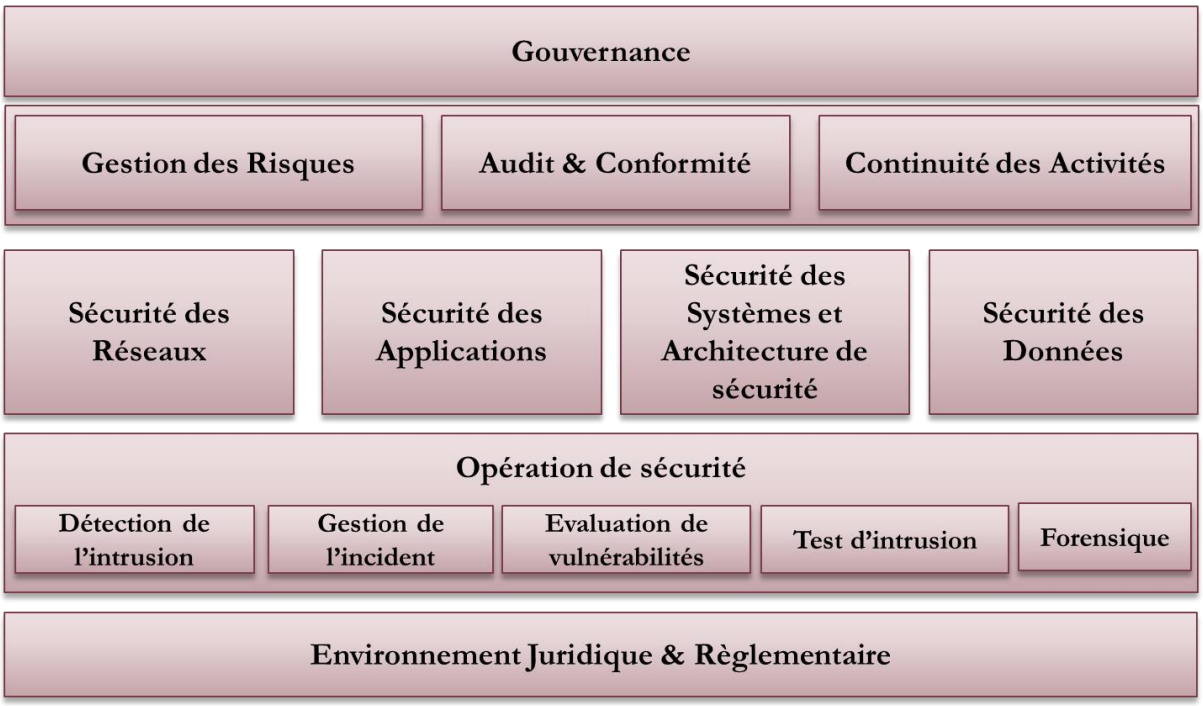

Figure 1: Les domaines

Les compétences :

Définition d'une compétence :

Le Référentiel Européen des e-Compétences (e-CF) définit une compétence de la façon suivante :

> « Une compétence est une capacité démontrée à appliquer des connaissances, des savoir-faire et des savoirs-être en vue d'obtenir des résultats observables »

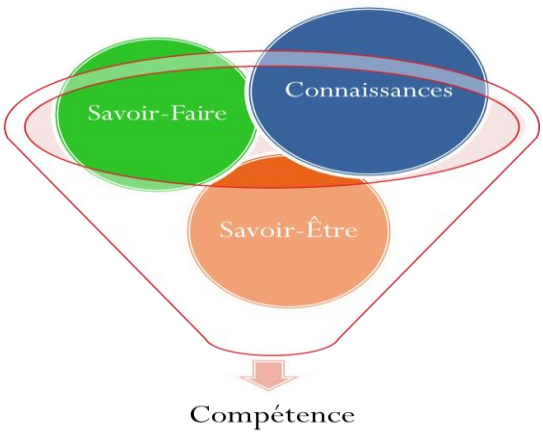

Figure 2 : Compétence

1. Domaine : Gouvernance

Gouvernance	**Les Connaissances**
	- Les concepts fondamentaux de la gouvernance de la sécurité de l'information - Les rôles et les responsabilités exigées pour la sécurité de l'information dans l'entreprise - Les méthodes pour mettre en œuvre des politiques de gouvernance de la sécurité de l'information - Les exigences légales et réglementaires concernant la sécurité de l'information - Les normes, les cadres et les bonnes pratiques internationalement reconnues liées à la gouvernance de la sécurité de l'information et au développement de stratégie
	Les Savoir-Faire
	- Définir les métriques applicables à la sécurité de l'information - Développer des modèles de gouvernance de la sécurité de l'information - Définir les indicateurs de performance de la sécurité de l'information - Développer le business case justifiant des investissements dans la sécurité de l'information

2. Domaine : Gestion des risques, audit et conformité, continuité des activités :

Gestion de risque (Risk management)	**Les Connaissances**
	- Approches et méthodes de gestion des risques - Critères d'évaluation des risques et d'impacts, et critères d'acceptation des risques - Les cadres et les modèles de risque, quantification des risques, enregistrement et rapport des risque - Les standards industriels de la sécurité de l'information (NIST, Payment Card Industry PCI)
	Les Savoir-Faire
	- Identifier les risques, les actifs, les menaces, les mesures de sécurité existants, les vulnérabilités et les conséquences - Analyser les risques : méthodologies d'analyse des risques, appréciation des conséquences, appréciation de la vraisemblance d'un incident, estimation du niveau des risques - Evaluer et apprécier les risques - Traiter les risques : réduction du risque, maintien des risques, refus des risques, partage des risques - Surveiller et examiner les risques : revu des facteurs de risques, amélioration de la gestion des risques

Audit, assurances et conformité (Audit, assurance and compliance)	**Les Connaissances**
	- Les standards, directives et les bonnes pratiques de l'audit de la sécurité de l'information - La planification d'audit et les techniques de gestion de projet d'audit - Les standards industriels de la sécurité de l'information (ISO/IEC 27000 series, ISF, NIST, Payment Card Industry PCI) - Les exigences légales et réglementaires concernant la

	sécurité de l'information - Les approches et les techniques d'audit
	Les Savoir-Faire
	- Elaborer, mettre en œuvre et maintenir des plans d'audits, des procédures, des méthodologies, des outils et des techniques appropriés afin de répondre aux exigences de la sécurité de l'information - Réaliser des missions d'audit périodiques pour vérifier la conformité aux politiques, normes et standards de sécurité, ainsi que les exigences juridiques et règlementaires - Documenter et déclarer les résultats d'audit et de conformité - Définir les objectifs de l'audit et les tests adéquats

Plan de Continuité d'Activité (Business Continuity Planning)	**Les Connaissances**
	- Les systèmes de gestion de la continuité des activités (SGCA) (Business Continuity Management System [BCMS]) conformément aux normes et standards : ISO 22301, ISO 27031, ISO/PAS 22399, BS 25999 ….) - Les méthodes, les techniques, les concepts, les approches et les standards requis pour l'efficacité des systèmes de gestion de la continuité des activités - Gestion des incidents et gestion des crises - L'analyse de l'impact des incidents sur les activités (Business Impact Analysis [BIA]) et évaluation des risques - Mise en œuvre, gestion et maintenance d'un système de gestion de la continuité des activités (SGCA)

	- Les indicateurs de performances, les matrices et le les tableaux de bord pour contrôler et surveiller un d'un système de gestion de la continuité des activités (SGCA) - La revue de gestion d'un d'un système de gestion de la continuité des activités (SGCA)
	Les Savoir-Faire
	- Elaborer un système de gestion de la continuité des activités (SGCA) et les politiques de continuités des activités - Elaborer les procédures d'un système de gestion de la continuité des activités (SGCA) - Implémenter d'un référentiel de gestion des documents - Concevoir une procédure de continuité d'actrivité - Développer et communiquer un programme de formation et de sensibilisation concernant le système de gestion de la continuité des activités (SGCA) - Conseiller les entreprises sur les bonnes pratiques de gestion des continuités des activités

3. Domaine : sécurité des réseaux :

Sécurité des réseaux (Telecommunication and network security)	**Connaissances**
	- Les concepts de sécurité réseau, les protocoles, architecture et mitigation (par exemple : firewall, chiffrement et cryptographie, zone démilitarisées …) - Les protocoles et l'architecture de sécurités des réseaux sans fils - Les systèmes de détection de l'intrusion (IDS) et les systèmes de prévention des intrusions (IPS) : logiciels, outils, méthodologies, techniques, …

	- Les canaux de communication sécurisée - Les redondances des données et les procédures de récupération des systèmes - L'évaluation des performances des technologies de l'information (par exemple : indicateur de performance des systèmes, capacité, disponibilité …) - Les différentes catégories des attaques réseaux (passif, actif, interne, distribué, common attacks vectors) - La sécurité des réseaux virtuels privés (VPN) - Gestion des identités et gestion des accès au réseau - Les technologies de filtrage web - Les outils de diagnostic des serveurs et les techniques d'identification des failles
	Les Savoir-Faire
	- Sécuriser les communications réseau - Protéger les réseaux contre les malwares - Installer, configurer, surveiller et maintenir les composants de protection réseau (IDS, IPS, VPN, firewalls, DMZ, anti-virus software, anti-spyware, chiffrement, …) - Etablir et documenter les politiques et les procédures d'utilisation de réseau local conformément à la politique de l'entreprise - Gérer les comptes, les droits d'accès réseau au système et aux équipements - Identifier les vulnérabilités réseaux moyennant les outils d'analyse réseau

4. Domaine : Sécurité des applications

Sécurité des applications (Application security)	**Connaissances**
	- Les modèles de cycle de vie de développement sécurisé : MS Security Development Life Cycle (MS

	SDL), NIST 800 – 64, OWASP CLASP - Les méthodologies de développement des logiciels (Waterfall, Agile, …) - Les politiques, les techniques et les standards de codage sécurisé - Les pratiques générales de codage (modularisation, structuration en couche, abstraction, masquage de donnée, …) - Les outils de test de sécurité (Secure Assist, AppScan Source, …) - Gestion d'authentification et de mot de passe (traitement sécurisé des identifiants par des scripts et des services externes …) - La gestion des identités et des contrôles d'accès des réseaux - La gestion des sessions - Les algorithmes de chiffrement et de cryptage (AES, 3DES, MD5, SHA, IPSEC, …) - Les concepts et les principes de protection des données - Les techniques et les principes de sécurité des communications - Les bonnes pratiques, les techniques et les outils de sécurité des bases de données - Les techniques de gestion des configurations de la sécurité - Les vulnérabilités et les menaces de sécurité des applications et des systèmes - Les méthodes d'évaluation et de test de sécurité des systèmes
	Savoir-Faire
	- Vérifier le niveau de sécurité des applications en utilisant des scanners de vulnérabilités ou des outils de revue de code - Rechercher les codes malveillants au sein des applications (recherche de virus, portes dérobées,

	…) - Modéliser les menaces et les vulnérabilités - Développer et mettre en œuvre des contrôles d'accès de sécurité et d'authentification aux applications - Mise en œuvre et gestion des configurations de sécurité des systèmes - Evaluer et vérifier la conception de sécurité - Elaborer un guide de maturité de la sécurité d'une application

5. Domaine : Sécurité des Systèmes et Architecture de Sécurité

Sécurité des systèmes (system security)	**Connaissances**
	- Les méthodes communes d'attaques et des menaces et les stratégies d'atténuation - La sécurité des systèmes d'exploitation (Linux, Unix, Windows, Mac OS, …) - La sécurité des systèmes d'information - La sécurité des systèmes distribués - La sécurité des services cloud - La sécurité des systèmes Big Data - La sécurité des systèmes embarqués - La sécurité de l'Internet des Objet (Internet of Things) - La sécurité des appareils mobiles
	Savoir-Faire

	- Configuration les systèmes d'une manière sécurisée et revue des fichiers de configuration afin de détecter les failles de sécurité - Analyser et évaluer des fichiers logs pour localiser les éventuelles anomalies - Gérer les privilèges - Sécuriser les démons réseaux

Architecture de Sécurité (Security Architecture)	**Connaissances**
	- Compréhension des architectures de sécurité de l'information et les normes existantes - Plateforme de l'architecture de sécurité de l'information (Sherwood Applied Business Security Architecture SABSA, The Open Group Architecture Framework TOGAF, …) - Les méthodes de vérification et de validation des architectures de sécurité de l'information - Autorité de certification (CA), signatures digitales, infrastructure à clés publique - Gestion de l'identité et authentification
	Savoir-Faire
	- Analyser les besoins et concevoir des modèles de sécurité de l'information - Concevoir des architectures de sécurité robustes tout au long du cycle de vie des projets TIC - Evaluer et analyser les risques de sécurité - Développer des exigences de sécurité réseaux : LAN (Local Area Network), WAN (Wide Area Network, VPN (Virtual Private Network), routeurs, firewalls, et les équipements réseaux … - Concevoir des infrastructures à clés publiques (Public Key Infrastructure PKI) - Estimer les coûts et identifier les problèmes

	d'intégrations - Valider l'installation des IDS, IPS, firewall, VPN, routeurs, serveur … - Définir et implémenter les politiques et les procédures de sécurité de l'entreprise - Recommander les mise-à-jour de sécurité nécessaire pour sécuriser les systèmes - Vérifier et valider les architectures de sécurité de l'information

6. Domaine : Sécurité des données

Sécurité des données (Data security)	**Connaissances**
	- Les principes et les techniques de sécurité des données : confidentialité, disponibilité, intégrité, non répudiation, confiance, données privées... - Les lois, règlements et politique nationaux et internationaux liés à la protection des données - Les politiques de conservation des données, suppression et archivage - Concept et types des certificats numériques, signature numérique, infrastructure à clé publique (Public Key Infrastructure [PKI]) … - Cryptographie (cryptographie quantum, chiffrement, cryptographie à clé publique/ privé, les fonctions de hachage …) - Les stratégies et les techniques de sécurisation des données dans les Clouds, ainsi que la classification des données et la découverte des données - Les principes et les techniques de sécurité des Big Data - Les principes et les techniques de sécurité des données ouvertes (Open Data)

	Savoir-Faire
	- Identification des risques liés à la protection des données - Définition des règles de sécurité des données - Gestion des risques liés à la sécurité des bases de données - La vérification de l'intégrité des données (vérification quantum, checksum, hash)

7. Domaine : Opération de sécurité (Security Operation)

Détection de l'intrusion **(Intrusion detection)**	**Connaissances**
	- Les techniques d'intrusion (basé sur les empreintes ou artefacts …), les outils et les boites à outils d'intrusion - Les types d'attaques et les risques associés, les méthodes de prévention, de mitigation et de récupération
	Savoir-Faire
	- Analyser les rapports d'incidents et les données collectées afin d'identifier les intrusions - Identifier les nouvelles vulnérabilités - Reconnaitre les nouvelles techniques d'intrusion - Rédiger les documents d'analyse des intrusions détectées - Rédiger les directives sur l'identification des empreintes, les risques associés et les méthodes de prévention

Gestion de l'incident **(incident management)**	**Connaissances**
	- Les procédures, les processus et les bonnes pratiques de gestion des incidents (par exemple ITIL, ISO 20000 …) - Les procédures, les processus et les bonnes pratiques de réponse aux incidents (contenir, éradiquer et récupérer)
	Savoir-Faire
	- Identifier l'origine de l'incident - Communiquer les incidents de la sécurité de l'information - Evaluer les incidents et déterminer les moyens de les aborder - Elaborer et mise en place d'une politique de gestion des incidents - Mettre à jour les politique de sécurité de l'information et de gestion des risques suite à un incident

Evaluation des vulnérabilités (Vulnerability Assessment)	**Connaissances**
	- Les menaces et les vulnérabilités cybernétiques (les menaces de sécurité des systèmes et des applications) - Les attaques de types code malveillant et les risques et dommages associés - Les concepts et les techniques de l'ingénierie inverse (ingénierie inverse logicielle et matérielles) - Les concepts, les méthodes et les outils d'analyse des logiciels malveillants (Ida Pro, Oily Debug …) - Les méthodes de prévention et de mitigation, les processus de détection et de suppression, et les techniques de récupération

	Savoir-Faire
	- Effectuer des scans de vulnérabilités et les identifier - Reconnaitre et catégoriser les différents types de vulnérabilités et les attaques possibles (les failles de configuration, débordement de mémoire tampon, code malveillant, attaque de mystification, attaque de l'homme au milieu, …

Test d'intrusion (Penetration testing)	**Connaissances**
	- Les outils et les techniques de piratage éthique - Les outils et les techniques de test d'intrusion des applications - Les outils et les techniques de test d'intrusion des réseaux - Les outils et les techniques de test d'intrusion Web - Les outils et les techniques de test d'intrusion des appareils mobiles - Les différents types de vulnérabilités et les attaques possibles (débordement de mémoire tampon, attaques d'ingénierie sociale, … - Les attaques des applications Web (cross Site Scripting XSS, SQL injection, …) - les attaques de mot de passe (key-space Brute Force, online password attacks, password hash attacks, …)
	Savoir-Faire

	- Effectuer les scans de vulnérabilités et détecter les failles (Nmap, OpenVAS …) - Collecter les informations d'une manière passive (collecte des informations du Web, collecte d'adresses électroniques, …) - Collecter les informations d'une manière active (énumération DNS, énumération SMB, …)

Investigation numérique légale **Forensique** **(Digital Forensics)**	**Connaissances**
	- Analyse forensique des systèmes de fichiers (identification des fichiers systèmes : fichiers journaux, fichiers de registre, fichier de configuration, extraction des données de différents support numériques, …) - Ensemble d'outils forensiques (forensic Tool Kit (FTK), EnCase, DD, Sleuthkit…) - Ingénierie inverse et revue de code - Analyse et décryptage des données collectées - Les outils et les techniques d'analyse de données brutes : data carving (Foremost, …) - Les tactiques, techniques, et procédures anti forensique d'une cyber-attaque - Les différents environnements des systèmes d'exploitation - Les outils et les techniques d'analyse forensique des matériels (Hardware), des réseaux, des bases de données, des logiciels malveillants, des Cloud, … - Les outils et les techniques d'analyse forensique des réseaux sociaux
	Savoir-Faire

	- Collecter et analyser les preuves numériques - Collecter et analyser les données persistantes et volatiles - Analyser les rapports d'incidents et identifier les informations critiques - Déterminer les outils et les méthodes utilisés lors d'une cyber-attaque - Evaluer les dégâts suite à une cyber-attaque (le niveau d'accès, les machines / sites impliqués, …) - Analyser approfondi des outils, scripts, et autres artefacts collectés durant la réponse au incident, …) - Conserver les preuves digitales : collecter, traiter, transporter, et enregistrer les preuves numériques afin d'éviter les modifications, la perte, l'endommagement physique ou la destruction des données …

Sensibilisation (Awareness)	**Connaissances**
	- Les techniques de communications et de présentations - Les nouvelles et les émergentes technologies de cybersécurité - Les nouveaux problèmes de sécurité de l'information, les risques et les vulnérabilités
	Savoir-Faire
	- Developppper des arguments convaincants - Defendre une thèse - Rédiger les rapports, bulletin d'information, présentations sur site, … - Créer une présentation de qualité supérieure - Parler et présenter à un public

	- Développer la connexion avec le public et maintenir l'intérêt

8. Domaine : Aspect juridique et règlementaire

Aspect juridique et règlementaire **(Legal aspect and regulation)**	**Connaissances**
	- Les exigences légales et réglementaires concernant la sécurité de l'information - Les lois, procédures et législations, nationaux et internationaux, relatifs aux cybercriminalités, cybersécurité et vie privée
	Savoir-faire
	- Analyser et suivre les actualités techniques et juridiques en relation avec la cybersécurité - Evaluer l'impact des tendances technologiques sur les politiques, règlementations et les lois

L'échelle des compétences

Ce référentiel des compétences définit trois niveaux de compétence :

- **Niveaux débutant** : ayant des connaissances basiques
- **Niveau confirmé** : ayant des connaissances approfondies et une capacité à résoudre les problèmes avec une autonomie limitée
- **Niveau expert** : ayant des connaissances plus approfondies et une capacité à résoudre les problèmes avec une autonomie élevée

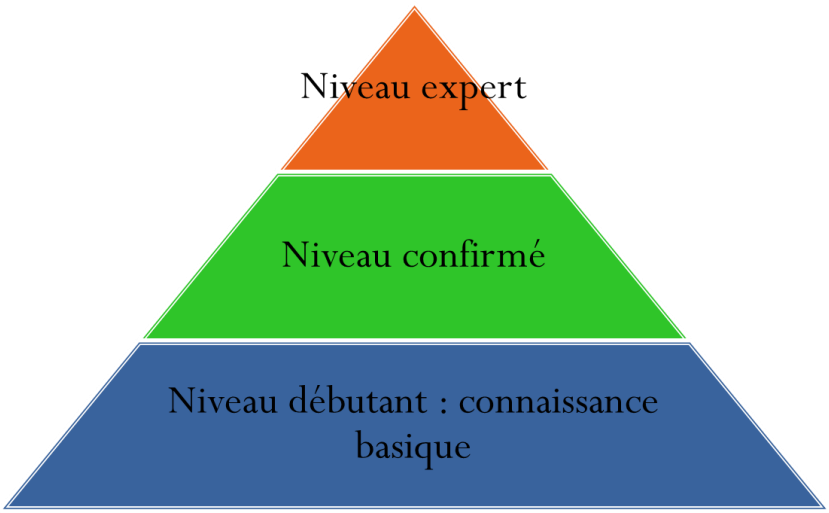

Figure 3: Niveau des compétences

Conclusion

Pour conclure, l'ANSI a élaboré un **référentiel de compétence** dans le domaine de la cybersécurité, ce dernier va servir comme un outil pour la préparation des fiches métiers en cybersécurité qui inclura les compétences issues du référentiel de compétences en cybersécurité. Le référentiel des métiers en cybersécurité permettra de structurer les métiers de la cybersécurité à l'échelle nationale.