ICT Berufsbildung
Formation professionnelle
Formazione professionale

Profil de qualification pour la profession de Cyber Security Specialist avec brevet fédéral

Mandant	ICT-Formation professionnelle Suisse
Direction de projet	eduxept AG
Auteurs	Stephan Leiser, Jörg Aebischer
Classification	aucune
Statut	validé

Modifications			
Date	Version	Modifications	Qui?
25.09.2018	0.1	Version initiale sur la base d'un workshop	S. Leiser
27.09.2018	0.2	Lectorat et feedbacks au niveau du contenu	J. Aebischer
12.10.2018	0.3	Adaptations sur la base des feedbacks du comité de pilotage et du groupe de travail	S. Leiser
15.10.2018	0.9	Remise au SEFRI	ICT-FPCH, J. Aebischer
23.10.2018	1.0	Validation par le SEFRI	SEFRI, S. Ryan
30.10.2018	1.0	Publication de la page Internet du projet	ICT-FPCH
27.02.2019	1.1	Numérotation des critères de performance	S. Leiser

Table des matières

1 Introduction

Le présent profil de qualification pour la profession de Cyber Security Specialist avec brevet fédéral a été élaboré sur mandat d'ICT-Formation professionnelle Suisse par un groupe de travail constitué de représentants du monde économique et de l'administration, sous la conduite méthodique de la société eduxept AG.

Le document décrit le profil de la profession, les compétences opérationnelles et le profil d'exigences au moyen de critères de performance. Ces bases servent à l'élaboration du règlement d'examen, des directives sur le règlement d'examen et des descriptions de modules pour le plan modulaire.

Le document a été approuvé dans le cadre d'une procédure de décision par voie de circulation le 8 octobre 2018 par le comité de pilotage du projet et le 23 octobre 2018 par le Secrétariat d'Etat à la formation, à la recherche et à l'innovation (SEFRI).

2 Profil de la profession

2.1 Domaine d'activité

Les Cyber Security Specialists (CSS) constituent une main-d'œuvre hautement spécialisée opérant dans le domaine de la cybersécurité. Ils travaillent généralement au sein de moyennes ou grandes entreprises privées ou dans des institutions publiques. Leurs principales tâches consistent en la protection préventive des systèmes d'information et de communication d'une organisation contre les attaques dans le cyberespace et en la gestion réactive des incidents de sécurité.

Les Cyber Security Specialists peuvent diriger de petites équipes constituées de professionnels chargés de l'exploitation opérationnelle ou engagées dans des projets spécifiques. Dans le cadre de projets, ils endossent la responsabilité pour des lots de travaux individuels ou des sous-projets.

2.2 Principales compétences opérationnelles

Les Cyber Security Specialists

- analysent en continu les cybermenaces actuelles et anticipent les menaces pertinentes pour leur organisation;
- examinent la sécurité des systèmes, détectent les vulnérabilités et prennent des mesures de protection préventives pour y remédier;
- surveillent les systèmes en cours d'exploitation et, ce faisant, identifient les incidents de sécurité pertinents et les non-conformités par rapport aux directives de sécurité d'une organisation;
- analysent les causes et les répercussions des incidents de sécurité et y répondent avec des mesures de protection réactives;
- planifient des projets dans le domaine de la cybersécurité et les concrétisent;
- conseillent et forment sur le plan technique les parties prenantes concernées.

2.3 Exercice de la profession

La cybersécurité constitue un domaine d'activités spécifique de la gestion des technologies de l'information et de la communication (ICT). L'intégration de la cybersécurité dans l'organisation fonctionnelle et structurelle d'une entreprise ou d'une administration varie en fonction de la taille et de l'orientation de celle-ci. En règle générale, les Cyber Security Specialists collaborent avec d'autres spécialistes de la sécurité ICT d'une organisation (Security Operations Center [SOC]). Les procédures

et règles de la stratégie de sécurité du management et les directives de sécurité y afférentes (politique de sécurité de l'information) forment le cadre de travail des Cyber Security Specialists.

Outre de solides connaissances techniques, l'exercice de la profession de Cyber Security Specialist requiert une grande vivacité d'esprit, une capacité de réflexion analytique et systémique développée, la faculté de raisonner en processus, le sens des responsabilités, la tolérance à la frustration, une aisance à communiquer et un très bon esprit d'équipe sans oublier discrétion, intégrité et persévérance.

2.4 Importance de la profession pour la société, l'économie, la nature et la culture

L'utilisation des technologies de l'information et de la communication progresse dans tous les domaines de la vie. La place croissante qu'occupent les informations et les technologies entraîne dans son sillage une augmentation des risques d'abus susceptibles d'occasionner de sérieux dommages à l'économie et à la société. Les Cyber Security Specialists contribuent à protéger les systèmes, les applications et les données contre les utilisations illicites des technologies et, partant, à réduire les dommages patrimoniaux et matériels, les préjudices portés aux personnes ainsi que les atteintes au savoir. Ils contribuent par ailleurs à l'image de la Suisse en tant que place économique sûre et partenaire politique et commercial fiable.

3 Compétences opérationnelles et critères de performance

3.1 Vue d'ensemble des compétences opérationnelles

↓ Domaines de compétences opérationnelles DCO		Compétences opérationnelles →						
A	**Protection préventive des systèmes**	A1: suivre en continu l'évolution des menaces	A2: analyser les menaces et traiter les informations	A3: détecter les vulnérabilités	A4: remédier aux vulnérabilités	A5: utiliser des procédures de leurre	A6: donner des conseils techniques aux parties prenantes	A7: former les parties prenantes
B	**Détection des incidents de sécurité**	B1: surveiller les systèmes en exploitation	B2: analyser et interpréter les données	B3: trier les incidents de sécurité	B4: documenter les incidents de sécurité	B5: surveiller le traitement d'un incident de sécurité		
C	**Maîtrise des incidents de sécurité**	C1: mettre en œuvre des mesures immédiates	C2: assurer la conservation des preuves	C3: analyser les causes et les répercussions	C4: définir et mettre en œuvre des mesures de protection	C5: soutenir la restauration des systèmes		
D	**Planification et mise en œuvre des solutions de sécurité**	D1: délimiter les systèmes et spécifier les exigences	D2: vérifier la faisabilité et l'efficacité	D3: déterminer l'investissement en ressources et le budgéter	D4: procéder à une évaluation	D5: mettre en œuvre un projet	D6: diriger une équipe	

3.2 DCO A: protection préventive des systèmes

Description du domaine de compétences opérationnelles (DCO)		
Le DCO A englobe les compétences opérationnelles exercées par les Cyber Security Specialists (CSS) dans les domaines **Anticipation** et **Prévention**. Les activités entrant dans ces domaines visent à la détection précoce de menaces potentielles et à la réduction des possibilités d'attaques par la mise en place de mesures de protection préventives. S'appuyant sur différentes sources d'informations et sur des échanges d'expériences, les CSS suivent et analysent en continu l'évolution actuelle des menaces dont ils tirent des constats et des informations sur les plans tactique, opérationnel et technique à l'attention des décideurs. Au moyen de procédures et d'outils sélectionnés, les CSS détectent les vulnérabilités des réseaux, des applications et des solutions de stockage ainsi que des appareils terminaux et périphériques. Pour déterminer s'il convient de remédier à une vulnérabilité, les CSS tiennent compte du rapport charges/bénéfices ainsi que des directives et processus de l'organisation. Si nécessaire, les CSS utilisent des procédures techniques et des outils en vue de leurrer les attaquants. Les CSS forment et conseillent différentes parties prenantes sur les aspects techniques et contribuent ainsi à les sensibiliser à la cybersécurité, ce qui constitue un élément essentiel d'une prévention efficace.		
Contexte		
L'appétence au risque du management et son évaluation des risques déterminent dans une large mesure le type de prévention et son étendue. Les mesures préventives sont efficaces et judicieuses du point de vue économique pour autant qu'elles soient conformes à la gestion des risques définie dans la stratégie de sécurité globale. L'utilisation de procédures et d'outils de détection des vulnérabilités doit tenir compte des dispositions du droit pénal (p. ex. soustraction de données, accès indu à un système informatique) et de la protection des données. Les menaces et scénarios d'attaque évoluent et changent de façon extrêmement dynamique dans le cyberespace. Outre des compétences personnelles décisives, l'acquisition effective d'informations et de connaissances requiert également un solide réseau de relations et de communication avec les parties prenantes déterminantes. Rapport avec le DCO D: dans les domaines Anticipation et Prévention, des besoins en solutions de sécurité plus étendues ou plus complexes peuvent se faire jour dans la pratique. Ces besoins sont généralement traités dans le cadre de projets dédiés, en-dehors de l'exploitation opérationnelle normale. Les compétences opérationnelles des CSS liées à des projets sont décrites dans le DCO D.		
Compétence opérationnelle	**Précisions sur le contenu et terminologie spécifique**	**Critères de performance (CP)**
A1: suivre en continu l'évolution des menaces	- Sources d'informations telles que catalogues des menaces MELANI, BSI, rapports de sécurité de fabricants, forums, organes spécialisés, etc.	Les CSS sont en mesure: CP-A-1: de différencier les diverses sources d'informations sur les menaces CP-A-2: d'évaluer la crédibilité des sources et des informations
A2: analyser les menaces et traiter les informations	- Concept et niveaux de la Cyber Threat Intelligence (CTI) (stratégique, tactique, opérationnel et technique)	

A3: détecter les vulnérabilités	- Audits et types d'audits (audit des systèmes, audit des processus, audit de la performance et audit de conformité) - Procédures et outils pour les tests de pénétration, les scans de vulnérabilité et les scans de conformité - Indicateurs de compromission (IoC) et indicateurs d'attaques (IoA) - Threat hunting proactif - Cadre légal régissant le piratage informatique	CP-A-3: d'élargir leurs connaissances sur les menaces de façon continue, proactive et autodirigée CP-A-4: d'expliquer le concept de Cyber Threat Intelligence CP-A-5: d'identifier la pertinence des menaces pour leur propre organisation CP-A-6: de préparer, de réaliser et d'évaluer des audits CP-A-7: de sélectionner et d'utiliser des procédures et des outils pour détecter les vulnérabilités en fonction du contexte et des systèmes CP-A-8: de définir et de mettre en œuvre des mesures de protection techniques ou organisationnelles appropriées CP-A-9: de sélectionner et d'utiliser des procédures et des outils appropriés pour leurrer les attaquants CP-A-10: d'évaluer la conformité légale et réglementaire de toutes les mesures prises dans les domaines Anticipation et Prévention CP-A-11: de conseiller les parties prenantes sur le plan technique selon une approche orientée besoins et solutions CP-A-12: de préparer des contenus spécialisés de façon méthodologique et didactique CP-A-13: de planifier, de réaliser et d'évaluer des formations
A4: remédier aux vulnérabilités	- Directives de la stratégie de sécurité de l'information (police de sécurité de l'information [PSI]) - Mesures de protection techniques et organisationnelles (MTO) spécifiques aux systèmes, solutions de sécurité et meilleures pratiques - Méthodes de durcissement des systèmes (hardening)	
A5: utiliser des procédures de leurre	- Procédures et outils visant à leurrer les attaquants (p. ex. honeypot, pièges, leurres ou outils servant à se masquer)	
A6: donner des conseils techniques aux parties prenantes	- Principes du conseil systémique orienté solutions - Modèles et règles de communication	
A7: former les parties prenantes	- Principes méthodologiques et didactiques - Planification et réalisation de formations	
Compétences personnelles et sociales		
- Curiosité et disposition à apprendre - Capacité de changer de perspective (penser comme un attaquant) - Sens des responsabilités dans l'utilisation de procédures sensibles visant à détecter les vulnérabilités ou à leurrer les attaquants - Confidentialité et intégrité dans le traitement des données et des informations sensibles - Aisance à communiquer dans le cadre des activités de conseil et de formation		

3.3 DCO B: détection des incidents de sécurité

Description du domaine de compétences opérationnelles (DCO)		
Le DCO B englobe les compétences opérationnelles exercées par les Cyber Security Specialists (CSS) dans le domaine **Détection.** Les activités entrant dans ce domaine concourent à la détection des incidents de sécurité dans l'exploitation opérationnelle. Les CSS enregistrent au moyen d'outils sélectionnés les données pertinentes dans les réseaux, les applications et les solutions de stockage ainsi que lors de l'utilisation d'appareils terminaux et périphériques. Les données enregistrées font l'objet d'une évaluation et d'une analyse manuelle ou automatisée en temps réel ou avec un décalage temporel en vue de détecter des anomalies ou des non-conformités. Au moyen d'un tri systématique, les CSS priorisent les incidents de sécurité identifiés et documentent les informations pertinentes nécessaires au traitement d'un incident par le service compétent.		
Contexte		
La détection des incidents de sécurité au sein d'une organisation s'effectue généralement selon des processus définis et des procédures précises que les CSS doivent respecter dans l'exécution de leurs tâches. L'utilisation de procédures et d'outils à des fins de surveillance des systèmes doit tenir compte des dispositions de la protection de la personnalité et de la protection des données. Rapport avec le DCO C: le traitement des incidents de sécurité identifiés est décrit dans le DCO C. Rapport avec le DCO D: la détection d'incidents de sécurité peut engendrer dans la pratique des besoins en solutions de sécurité plus étendues ou plus complexes. Ces besoins sont généralement traités dans le cadre de projets dédiés, en-dehors de l'exploitation opérationnelle normale. Les compétences opérationnelles des CSS liées à des projets sont décrites dans le DCO D.		
Compétence opérationnelle	**Précisions sur le contenu et terminologie spécifique**	**Critères de performance (CP)**
B1: surveiller les systèmes en exploitation	- Procédures et outils pour surveiller (monitoring) les réseaux, applications, services serveur, solutions de stockage, appareils terminaux et périphériques - Solutions techniques (appliance) pour détecter des attaques telles que pare-feux, systèmes de détection d'intrusion (IDS) systèmes de prévention d'intrusion (IPS) ou pare-feux applicatifs web (WAF) - Gestion des événements et des informations de sécurité (SIEM)	Les CSS sont en mesure: CP-B-1: d'expliquer les structures, les processus et les interdépendances au sein de l'organisation qui sont pertinents pour leur propre activité CP-B-2: d'expliquer l'organisation structurelle et fonctionnelle spécifique à la gestion des incidents CP-B-3: de sélectionner et d'utiliser des procédures et des outils de surveillance des systèmes CP-B-4: d'expliquer les solutions techniques permettant de détecter des attaques et d'en assurer le fonctionnement
B2: analyser et interpréter les données	- Evaluation automatisée ou manuelle des fichiers journal (log files) - Détection de faux positifs - Langages de script pour l'évaluation des données - Méthodes d'analyse des données	

	- Techniques de représentation en vue de synthétiser les informations	CP-B-5: d'évaluer et d'interpréter les journaux de différents systèmes dans divers formats CP-B-6: de programmer, au moyen de langages de scripts, des fonctions pour l'évaluation des données CP-B-7: d'analyser et/ou de comparer le contenu des ensembles de données ainsi que de synthétiser et de représenter les informations obtenues CP-B-8: de classer les incidents de sécurité identifiés, de les prioriser et de les attribuer aux services compétents CP-B-9: d'utiliser les logiciels de suivi des problèmes et de documenter les incidents de sécurité sur tout leur cycle de vie CP-B-10: d'évaluer si les dispositions des OLA ou des SLA sont respectées et, si nécessaire, de procéder à une escalade CP-B-11: d'évaluer la conformité légale et réglementaire de toutes les mesures engagées dans le domaine de la détection
B3: trier les incidents de sécurité	- Respect des directives et processus internes - Classification et priorisation des incidents - Attribution (dispatching) des incidents	
B4: documenter les incidents de sécurité	- Logiciels de suivi des problèmes ou issue tracking systems (ITS) pour la gestion des incidents sur tout le cycle de vie - Eléments informatifs sur un incident resp. ticket	
B5: surveiller le traitement d'un incident de sécurité	- Accord sur les niveaux opérationnels (OLA), accord sur les niveaux de service (SLA) pour le traitement des incidents - Niveaux d'escalade selon OLA resp. SLA	
Compétences personnelles et sociales		
- Capacité de raisonner en processus, pensée systémique - Discipline, persévérance et sens des responsabilités lors de la détection des incidents - Faculté d'analyse et pensée en réseau lors de l'analyse et du tri des données - Sens de la précision et bonne expression écrite pour la documentation des incidents - Aisance à communiquer et intelligence émotionnelle dans le cadre du travail en équipe et des échanges avec les parties prenantes		

3.4 DCO C: maîtrise des incidents de sécurité

Description du domaine de compétences opérationnelles (DCO)		
Le DCO C englobe les compétences opérationnelles exercées par les Cyber Security Specialists (CSS) dans le domaine **Réponse**. Les activités entrant dans ce domaine comprennent le traitement des incidents de sécurité survenant en cours d'exploitation normale et le soutien technique apporté lors de la gestion de situations d'urgence ou de crises dans le cadre du Business Continuity Managements (BCM) d'une organisation. En cas de graves incidents de sécurité, les CSS implémentent des mesures techniques immédiates en vue de réduire les répercussions directes et les dommages d'un incident. Dans ce contexte, il est essentiel d'assurer la conservation des éléments de preuve qui serviront de base à l'analyse des incidents de sécurité et aux éventuelles enquêtes pénales et aux investigations forensiques numériques. Les CSS examinent les causes et les répercussions des incidents de sécurité. Sur la base de leur analyse et conformément au plan de réponse aux incidents de l'organisation, les CSS implémentent des mesures de protection réactives ou recommandent des mesures correctives ou d'amélioration aux décideurs. A la suite d'une panne de système, les CSS soutiennent les services compétents dans la restauration sécurisée de l'exploitation.		
Contexte		
La gestion des incidents de sécurité au sein d'une organisation s'effectue généralement selon des processus définis et des procédures précises que les CSS doivent respecter dans l'exécution de leurs tâches. La mise en œuvre de mesures immédiates ou de protection doit tenir compte des interdépendances avec les autres unités organisationnelles et processus (p. ex. transition des services ICT et fonctionnement des services, conformité, organisation d'urgence et de crise). Raison pour laquelle les CSS doivent impérativement disposer de connaissances approfondies de l'organisation structurelle et fonctionnelle propre à leur entreprise ou administration. S'agissant de la disponibilité et de la conservation des preuves, les méthodes et principes appliqués en vue de garantir l'utilisation juridique de moyens de preuve doivent respecter les dispositions légales applicables en l'espèce. Rapport avec le DCO D: l'analyse des causes d'un incident de sécurité peut engendrer dans la pratique des besoins en solutions de sécurité plus étendues ou plus complexes. Ces besoins sont généralement traités dans le cadre de projets dédiés, en-dehors de l'exploitation opérationnelle normale. Les compétences opérationnelles des CSS liées à des projets sont décrites dans le DCO D.		
Compétence opérationnelle	**Précisions sur le contenu et terminologie spécifique**	**Critères de performance (CP)**
C1: mettre en œuvre des mesures immédiates	- Directives du plan de réponse aux incidents - Mesures techniques immédiates, p. ex. isolation, désactivation ou arrêt des systèmes et services	Les CSS sont en mesure: CP-C-1: d'expliquer les structures, les processus et les interdépendances au sein de leur organisation qui sont pertinents pour leur propre activité CP-C-2: d'expliquer l'organisation structurelle et fonctionnelle spécifique à la gestion des incidents
C2: assurer la conservation des preuves	- Bases et principes forensiques - Conformité légale - Méthodes de conservation des preuves (post mortem, live response)	

C3: analyser les causes et les répercussions	- Analyse des attaques - Analyse statique et dynamique des logiciels malveillants - Forensique des systèmes, réseaux et mémoires - Méthodes et technique d'analyse structurée des causes	CP-C-3: d'interpréter et d'appliquer les directives du plan de réponse aux incidents de l'organisation CP-C-4: de sélectionner et d'implémenter des mesures techniques immédiates adaptées à la situation et au contexte et de vérifier leur efficacité CP-C-5: d'assurer la conservation des preuves conformément aux principes régissant leur utilisation juridique CP-C-6: d'analyser les causes et les répercussions des attaques au moyen de méthodes et de procédures appropriées CP-C-7: d'expliquer des méthodes et des procédures d'analyse des logiciels malveillants CP-C-8: d'utiliser des outils pour effectuer des analyses forensiques numériques des systèmes, réseaux et mémoires CP-C-9: de définir des mesures de protection réactives appropriées CP-C-10: de formuler et de présenter aux décideurs des recommandations dans un langage adapté à leurs interlocuteurs CP-C-11: d'implémenter des mesures de protection réactives en tenant compte des parties prenantes concernées et de vérifier leur efficacité CP-C-12: de conseiller une organisation de crise et d'urgence en matière de cybersécurité avec une approche orientée besoins et solutions CP-C-13: d'évaluer la conformité légale et réglementaire de toutes les mesures entrant dans le domaine Réponse
C4: définir et mettre en œuvre des mesures de protection	- Mesures de protection techniques et organisationnelles (MTO) - Interfaces avec les autres parties prenantes et processus	
C5: soutenir la restauration des systèmes	- Business Continuity Management (BCM) - Mesures de reprise après sinistre (desaster recovery)	
Compétences personnelles et sociales		
- Capacité de raisonner en processus, pensée systémique - Faculté d'analyse et pensée en réseau lors de l'examen des causes et des répercussions - Extrême précision, soin et rigueur lors de la collecte et conservation des moyens de preuve et de leur analyse - Confidentialité et intégrité dans le traitement des moyens de preuve - Créativité et capacité d'innovation lors du développement de solutions - Aisance à communiquer et intelligence émotionnelle dans le cadre du travail en équipe et des échanges avec les parties prenantes		

3.5 DCO D: planification et mise en œuvre des solutions de sécurité

Description du domaine de compétences opérationnelles (DCO)		
Le DCO D englobe les compétences opérationnelles exercées par les Cyber Security Specialists (CSS) dans les domaines **Business Engineering, Gestion de projets** et **Direction.** Ces compétences sont pertinentes lorsqu'il s'agit de traiter, sous forme de projet, des besoins nouveaux ou des changements de besoins en solutions de sécurité. Les CSS spécifient, en tenant compte des parties prenantes concernées, des exigences fonctionnelles et non fonctionnelles mesurables, qui doivent être remplies par les solutions de sécurité, et analysent leur intégration dans le système global ainsi que leurs interfaces avec celui-ci. Si nécessaire, ils vérifient la faisabilité et l'efficacité de la solution de sécurité dans un contexte spécifique. Les CSS déterminent et budgétisent, à l'attention des décideurs, le personnel et les moyens d'exploitation requis par la solution de sécurité. Sur la base des exigences définies, ils procèdent à l'évaluation des offres et de variantes et soutiennent les services concernés dans l'acquisition des solutions de sécurité. Dans le cadre de projets, les CSS sont responsables de lots de travail ou de sous-projets. Ils établissent la planification de projet, assurent la communication avec toutes les parties prenantes lors de la mise en œuvre du projet, vérifient la réalisation des objectifs et prennent, si nécessaire, des mesures de pilotage ou des mesures correctives. En tant que chef d'équipe d'une unité organisationnelle ou de responsable d'un sous-projet, les CSS peuvent diriger de petits groupes d'experts.		
Contexte		
Les projets dans le domaine de la cybersécurité se déroulent dans un contexte de travail caractérisé par des problèmes complexes, des exigences interdisciplinaires et des changements fréquents. Outre de vastes connaissances spécialisées de divers domaines d'activités et méthodes, les CSS doivent aussi disposer de compétences sociales et personnelles afin de faire face à la complexité des tâches qui leur incombent.		
Compétence opérationnelle	**Précisions sur le contenu et terminologie spécifique**	**Critères de performance (CP)**
D1: délimiter les systèmes et spécifier les exigences	- Modélisation de systèmes, de sous-systèmes et des limites du système - Description des interfaces - Spécification d'exigences mesurables	Les CSS sont en mesure: CP-D-1: d'analyser et d'évaluer des systèmes et processus CP-D-2: de définir et de décrire les interfaces CP-D-3: de spécifier les exigences des systèmes dans des environnements complexes CP-D-4: de vérifier et d'évaluer la faisabilité des solutions de sécurité CP-D-5: de calculer les coûts engendrés par les solutions de sécurité CP-D-6: de développer des critères d'évaluation des solutions de sécurité CP-D-7: de comparer et d'évaluer des variantes
D2: vérifier la faisabilité et l'efficacité	- Méthodes de vérification de la faisabilité (p. ex. proof of concept, étude de faisabilité, prototypage, projets pilotes)	
D3: déterminer l'investissement en ressources et le budgéter	- Méthodes d'estimation des coûts - Planification et calcul des coûts - Controlling de projet et reporting	
D4: procéder à une évaluation	- Elaboration de critères d'évaluation - Cahier des charges et cahier des charges avec spécification des exigences - Comparaison de variantes	

	- Soutien lors des processus de négociation et d'acquisition	CP-D-8: de conseiller les services concernés quant aux solutions de sécurité et de soutenir leur acquisition CP-D-9: de planifier des sous-projets au niveau du contenu et des ressources CP-D-10: de surveiller des sous-projets et d'évaluer leur état d'avancement CP-D-11: de définir et de mettre en œuvre des mesures de pilotage et correctives adaptées au contexte et à la situation dans le cadre des sous-projets CP-D-12: de conduire et de développer une équipe tant sur le plan technique que social CP-D-13: de gérer de façon proactive les conflits au sein de groupes et de développer des solutions constructives
D5: mettre en œuvre un projet	- Planification de projets ou de sous-projets - Gestion des risques et communication - Assurance qualité - Controlling financier et reporting	
D6: diriger une équipe	- Comportement managérial adapté au contexte et à la situation - Modèles et règles de communication - Team building et motivation - Gestion des conflits	
Compétences personnelles et sociales		
- Capacité à communiquer et orientation clientèle lors du recensement des exigences - Pensée systémique et bonne expression écrite lors de la spécification des exigences - Créativité et capacité d'innovation lors du développement de solutions - Capacité d'analyse d'interdépendances complexes dans le cadre de projets interdisciplinaires - Sens des responsabilités, conscience des coûts et de la qualité dans le cadre des projets - Compétences décisionnelles dans le cadre des projets - Esprit d'équipe, aisance à communiquer et capacité à motiver les autres dans la conduite d'un groupe - Capacité de gérer des conflits et force de persuasion dans la conduite d'un groupe		