ICT Berufsbildung
Formation professionnelle
Formazione professionale

ICT-Formation professionnelle Suisse

RÈGLEMENT

concernant

l'examen professionnel de Cyber Security Specialist*

du 06 mai 2019

Vu l'art. 28, al. 2, de la loi fédérale du 13 décembre 2002 sur la formation professionnelle, l'organe responsable au sens du ch. 1.3 arrête le règlement d'examen suivant:

1. DISPOSITIONS GÉNÉRALES

1.1 But de l'examen

L'examen professionnel fédéral a pour but de vérifier de manière exhaustive si les candidats ont acquis les compétences opérationnelles nécessaires pour exercer la profession de Cyber Security Specialist.

1.2 Profil de la profession

1.21 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 de 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.

1.22 Principales compétences opérationnelles

Les Cyber Security Specialists

* Pour faciliter la lecture du document, le masculin est utilisé pour désigner les deux sexes.

- 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.

1.23 Exercice de la profession

La cybersécurité constitue un domaine d'activité 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 la discrétion, l'intégrité et la persévérance.

1.24 Apport de la profession à la société, à l'économie, à la nature et à 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.

1.3 Organe responsable

1.31 L'organisation du monde du travail suivante constitue l'organe responsable:

Association ICT-Formation professionnelle Suisse

1.32 L'organe responsable est compétent pour toute la Suisse.

2. ORGANISATION

2.1 Composition de la commission d'examen

2.11 Toutes les tâches liées à l'octroi du brevet sont confiées à une commission d'examen. Celle-ci est composée de 7 membres au moins, nommés par l'organe responsable pour une période administrative de 2 ans.

2.12 La commission d'examen se constitue elle-même. Le quorum est atteint lorsque la majorité des membres sont présents. Les décisions se prennent à la majorité des membres présents. Le président tranche en cas d'égalité des voix.

2.2 Tâches de la commission d'examen

2.21 La commission d'examen:

a) arrête les directives relatives au présent règlement et les met à jour périodiquement;
b) fixe la taxe d'examen;
c) fixe la date et le lieu de l'examen;
d) définit le programme d'examen;
e) donne l'ordre de préparer les énoncés de l'examen et organise l'examen;
f) nomme et engage les experts, et les forme pour accomplir leurs tâches;
g) décide de l'admission à l'examen ainsi que d'une éventuelle exclusion de l'examen;
h) décide de l'octroi du brevet;
i) traite les requêtes et les recours;
j) s'occupe de la comptabilité et de la correspondance;
k) décide de la reconnaissance ou de la prise en compte d'autres diplômes et d'autres prestations;
l) rend compte de ses activités aux instances supérieures et au Secrétariat d'État à la formation, à la recherche et à l'innovation (SEFRI);
m) veille au développement et à l'assurance de la qualité, et en particulier à l'actualisation régulière du profil de qualification en fonction des besoins du marché du travail.

2.22 La commission d'examen délègue les tâches administratives et la gestion des affaires à ICT-Formation professionnelle Suisse.

2.3 Publicité et surveillance

2.31 L'examen est placé sous la surveillance de la Confédération. Il n'est pas public. Dans des cas particuliers, la commission d'examen peut autoriser des dérogations à cette règle.

2.32 Le SEFRI est invité suffisamment tôt à assister à l'examen et reçoit les dossiers d'examen.

3. PUBLICATION, INSCRIPTION, ADMISSION, FRAIS D'EXAMEN

3.1 Publication

3.11 L'examen est annoncé publiquement dans les trois langues officielles cinq mois au moins avant le début des épreuves.

3.12 La publication informe sur:

a) les dates des épreuves;
n) la taxe d'examen;
o) l'adresse d'inscription;
p) le délai d'inscription;
q) le déroulement de l'examen.

3.2 Inscription

L'inscription doit comporter:

a) un résumé de la formation et des activités professionnelles du candidat;
b) les copies des titres et des certificats de travail requis pour l'admission;
c) la mention de la langue d'examen;
d) la copie d'une pièce d'identité officielle munie d'une photo;
a) la mention du numéro d'assurance sociale (n° AVS)[1].

3.3 Admission

3.31 Sont admis à l'examen les candidats qui:

a) possèdent un certificat fédéral de capacité dans le domaine des technologies de l'information et de la communication (ICT) et peuvent justifier d'au moins deux ans de pratique professionnelle dans le domaine de la sécurité de l'information ou de la cybersécurité;

ou

b) possèdent un certificat fédéral de capacité, un titre d'une école supérieure d'enseignement général ou un titre équivalent et peuvent justifier d'au moins quatre ans de pratique professionnelle dans le domaine des technologies de l'information et de la communication (ICT), dont au moins deux ans dans le domaine de la sécurité de l'information ou de la cybersécurité;

ou

c) peuvent attester d'au moins six ans de pratique professionnelle dans le domaine des technologies de l'information et de la communication (ICT), dont au moins deux ans dans le domaine de la sécurité de l'information ou de la cybersécurité;

[1] La base juridique de ce relevé est l'ordonnance sur les relevés statistiques (RS **431.012.1**; n° 70 de l'annexe). La commission d'examen ou le SEFRI relève, sur mandat de l'Office fédéral de la statistique, les numéros AVS utiles à des fins purement statistiques.

ou

d) ont suivi avec succès la cyberformation au sein de l'armée et peuvent attester d'au moins une année de pratique professionnelle dans le domaine de la sécurité de l'information ou de la cybersécurité.

Le jour de référence pour la preuve de la pratique professionnelle est le premier jour de l'examen.

L'admission à l'examen reste subordonnée à l'acquittement dans les délais de la taxe d'examen conformément au ch. 3.41.

3.32 Les décisions concernant l'admission à l'examen sont communiquées par écrit aux candidats au moins trois mois avant le début de l'examen. Les décisions négatives indiquent les motifs et les voies de droit.

3.4 Frais

3.41 Après avoir reçu confirmation de son admission, le candidat acquitte la taxe d'examen. Les taxes pour l'établissement du brevet et pour l'inscription de son titulaire dans le registre officiel des titulaires de brevets, ainsi qu'une éventuelle contribution pour frais de matériel sont perçues séparément. Ces frais sont à la charge du candidat.

3.42 Le candidat qui, conformément au ch. 4.2, se retire dans le délai autorisé ou pour des raisons valables, a droit au remboursement du montant payé, déduction faite des frais occasionnés.

3.43 L'échec à l'examen ne donne droit à aucun remboursement.

3.44 Pour le candidat qui répète l'examen, la taxe d'examen est fixée dans chaque cas par la commission d'examen, compte tenu du nombre d'épreuves répétées.

3.45 Les frais de déplacement, de logement, de subsistance et d'assurance pendant la durée de l'examen sont à la charge du candidat.

4. ORGANISATION DE L'EXAMEN

4.1 Convocation

4.11 L'examen a lieu une fois par année. Il est organisé

a) en allemand, dans la mesure où 25 candidats au moins
b) en français, dans la mesure où 8 candidats au moins
c) en italien, dans la mesure où 3 candidats au moins

remplissent les conditions d'admission après la publication, mais tous les deux ans au moins.

4.12 Les candidats peuvent choisir de passer l'examen dans l'une des trois langues officielles: le français, l'allemand ou l'italien.

La première épreuve peut avoir lieu en anglais.

4.13 Les candidats sont convoqués quatre semaines au moins avant le début de l'examen. La convocation comprend:

a) le programme d'examen, avec l'indication du lieu, de la date, de l'heure des épreuves et des moyens auxiliaires dont les candidats sont autorisés ou invités à se munir;
b) la liste des experts.

4.14 Toute demande de récusation d'un expert doit être motivée et adressée à la commission d'examen 14 jours au moins avant le début de l'examen. La commission prend les mesures qui s'imposent.

4.2 Retrait

4.21 Les candidats ont la possibilité d'annuler leur inscription jusqu'à six semaines avant le début de l'examen.

4.22 Passé ce délai, le retrait n'est possible que si une raison valable le justifie. Sont notamment réputées raisons valables:

a) la maternité;
b) la maladie et l'accident;
c) le décès d'un proche;
r) le service militaire, le service de protection civile ou le service civil imprévu.

4.23 Le retrait doit être communiqué sans délai et par écrit à la commission d'examen, assorti de pièces justificatives.

4.3 Non-admission et exclusion

4.31 Le candidat qui, en rapport avec les conditions d'admission, donne sciemment de fausses informations ou tente de tromper la commission d'examen d'une autre manière n'est pas admis à l'examen.

4.32 Est exclu de l'examen quiconque:

a) utilise du matériel ou des documents non autorisés;
b) enfreint gravement la discipline de l'examen;
c) tente de tromper les experts.

4.33 La décision d'exclure un candidat de l'examen incombe à la commission d'examen. Le candidat a le droit de passer l'examen sous réserve, jusqu'à ce que la commission d'examen ait arrêté une décision formelle.

4.4 Surveillance de l'examen et experts

4.41 Au moins une personne compétente surveille l'exécution des travaux d'examen écrits et pratiques. Elle consigne ses observations par écrit.

4.42 Deux experts au moins évaluent les travaux écrits et les travaux pratiques. Ils s'entendent sur la note à attribuer.

4.43 Deux experts au moins procèdent aux examens oraux, prennent des notes sur l'entretien d'examen et sur le déroulement de l'examen, apprécient les prestations fournies et fixent en commun la note.

4.44 Les enseignants aux cours préparatoires, les personnes ayant des liens de parenté avec le candidat ainsi que les supérieurs hiérarchiques présents ou passés du candidat ou ses collaborateurs se récusent en tant qu'experts.

4.5 Séance d'attribution des notes

4.51 La commission d'examen décide de la réussite ou de l'échec des candidats lors d'une séance mise sur pied après l'examen. La personne représentant le SEFRI est invitée suffisamment tôt à cette séance.

4.52 Les enseignants aux cours préparatoires, les personnes ayant des liens de parenté avec le candidat ainsi que les supérieurs hiérarchiques présents ou passés du candidat ou ses collaborateurs se récusent lors de la prise de décision sur l'octroi du brevet.

5. EXAMEN

5.1 Épreuves d'examen

5.11 L'examen est organisé selon les épreuves et durées suivantes:

Épreuve		Forme d'examen	Durée	Pondération
1	Cybersécurité	Traitement de cas pratique	5 h	60%
2	Projets et économie d'entreprise	Traitement de cas écrit	2 h	20%
3	Direction et communication	Traitement de cas oral et entretien professionnel	¾ h	20%
		Total	7 ¾ h	

La forme d'examen varie selon qu'il s'agit d'évaluer les compétences opérationnelles, les prestations de transfert ou l'application pratique.

Épreuve 1: cybersécurité

Cette partie de l'examen sert à évaluer les compétences opérationnelles inhérentes à la profession. Les candidats doivent traiter des cas en rapport direct avec le travail quotidien d'un Cyber Security Specialist en assurant le transfert de connaissances, de capacités et d'aptitudes dans le cadre d'une situation pratique simulée. Les énoncés sont formulés en anglais pour tous les candidats.

Épreuve 2: projets et économie d'entreprise

Cette partie de l'examen sert à évaluer les compétences opérationnelles dans le domaine de la gestion de projets ainsi que les aspects relevant de l'économie

d’entreprise inhérents à la profession. Les candidats doivent traiter par écrit des situations pratiques proches de la réalité.

Épreuve 3: direction et communication

Cette partie de l’examen sert à évaluer les compétences personnelles et sociales exigées des Cyber Security Specialists, en particulier dans les domaines de la conduite d’équipe et de la communication. Les compétences opérationnelles sont examinées dans le cadre d’une analyse de cas orale et d’un entretien professionnel.

5.12 Chaque épreuve peut être subdivisée en points d’appréciation. La commission d’examen fixe cette subdivision et la pondération des points d’appréciation dans les directives relatives au présent règlement.

5.2 Exigences

5.21 La commission d’examen arrête les dispositions détaillées concernant l’examen final figurant dans les directives relatives au règlement d’examen (au sens du ch. 2.21, let. a.).

5.22 La commission d’examen décide de l’équivalence des épreuves ou des modules effectués dans le cadre d’autres examens du degré tertiaire ainsi que de la dispense éventuelle des épreuves correspondantes du présent règlement d’examen. Les candidats ne peuvent être dispensés de l’épreuve 1.

6. ÉVALUATION ET ATTRIBUTION DES NOTES

6.1 Généralités

L’évaluation des épreuves et de l’examen est basée sur des notes. Les dispositions des ch. 6.2 et 6.3 du règlement d’examen sont applicables.

6.2 Évaluation

6.21 Une note entière ou une demi-note est attribuée pour les points d’appréciation, conformément au ch. 6.3.

6.22 La note d’une épreuve est la moyenne des notes des points d’appréciation correspondants. Elle est arrondie à la première décimale. Si le mode d’appréciation permet de déterminer directement la note de l’épreuve sans faire usage de points d’appréciation, la note de l’épreuve est attribuée conformément au ch. 6.3.

6.23 La note globale de l’examen correspond à la moyenne pondérée des notes des épreuves. Elle est arrondie à la première décimale.

6.3 Notation

Les prestations des candidats sont évaluées au moyen de notes échelonnées de 6 à 1. Les notes supérieures ou égales à 4,0 désignent des prestations suffisantes. Seules les demi-notes sont admises comme notes intermédiaires.

6.4 Conditions de réussite de l'examen et de l'octroi du brevet

6.41 L'examen est réussi si:

c) la note générale est égale ou supérieure à 4,0;
d) la note de l'épreuve 1 n'est pas inférieure à 4,0;
e) les notes des épreuves 2 et 3 ne sont pas inférieures à 3,0.

6.42 L'examen est considéré comme non réussi si le candidat:

a) ne se désiste pas à temps;
b) ne se présente pas à l'examen ou à une épreuve, et ne donne pas de raison valable;
c) se retire après le début de l'examen sans raison valable;
d) est exclu de l'examen.

6.43 La commission d'examen décide de la réussite de l'examen uniquement sur la base des prestations fournies par le candidat. Le brevet fédéral est décerné aux candidats qui ont réussi l'examen.

6.44 La commission d'examen établit un certificat d'examen pour chaque candidat. Le certificat doit contenir au moins les données suivantes:

a) les notes des différentes épreuves d'examen et la note globale de l'examen;
b) la mention de réussite ou d'échec à l'examen;
c) les voies de droit, si le brevet est refusé.

6.5 Répétition

6.51 Le candidat qui échoue à l'examen est autorisé à le repasser à deux reprises.

6.52 Les examens répétés ne portent que sur les épreuves dans lesquelles le candidat a fourni une prestation insuffisante.

6.53 Les conditions d'inscription et d'admission au premier examen s'appliquent également aux examens répétés.

7. BREVET, TITRE ET PROCÉDURE

7.1 Titre et publication

7.11 Le brevet fédéral est délivré par le SEFRI à la demande de la commission d'examen et porte la signature de la direction du SEFRI et du président de la commission d'examen.

7.12 Les titulaires du brevet sont autorisés à porter le titre protégé de:

- **Cyber Security Specialist avec brevet fédéral**
- **Cyber Security Specialist mit eidgenössischem Fachausweis**
- **Cyber Security Specialist con attestato professionale federale**

Traduction du titre en anglais:

- **Cyber Security Specialist, Federal Diploma of Higher Education**

7.13 Les noms des titulaires de brevet sont inscrits dans un registre tenu par le SEFRI.

7.2 Retrait du brevet

7.21 Le SEFRI peut retirer tout brevet obtenu de manière illicite. La poursuite pénale est réservée.

7.22 La décision du SEFRI peut être déférée dans les 30 jours suivant sa notification au Tribunal administratif fédéral.

7.3 Voies de droit

7.31 Les décisions de la commission d'examen concernant la non-admission à l'examen ou le refus du brevet peuvent faire l'objet d'un recours auprès du SEFRI dans les 30 jours suivant leur notification. Le recours doit mentionner les conclusions et les motifs du recourant.

7.32 Le SEFRI statue en première instance sur les recours. Sa décision peut être déférée dans les 30 jours suivant la notification au Tribunal administratif fédéral.

8. COUVERTURE DES FRAIS D'EXAMEN

8.1 Sur proposition de la commission d'examen, l'organe responsable fixe le montant des indemnités versées aux membres de la commission d'examen et aux experts.

8.2 L'organe responsable assume les frais d'examen qui ne sont pas couverts par la taxe d'examen, la subvention fédérale ou d'autres ressources.

8.3 Conformément aux directives en la matière[2], la commission d'examen remet au SEFRI un compte de résultats détaillé au terme de l'examen. Sur cette base, le SEFRI définit le montant de la subvention fédérale accordée pour l'organisation de l'examen.

9. DISPOSITIONS FINALES

9.1 Entrée en vigueur

Le présent règlement d'examen entre en vigueur à la date de son approbation par le SEFRI.

[2] Directives du SEFRI concernant l'octroi de subventions fédérales pour l'organisation d'examens professionnels fédéraux et d'examens professionnels fédéraux supérieurs selon les art. 56 LFPr et 65 OFPr

10. ÉDICTION

Berne, le

ICT-Formation professionnelle Suisse

Andreas Kaelin Président	Serge Frech Directeur

Le présent règlement d'examen est approuvé.

Berne, le 06 mai 2019

Secrétariat d'État à la formation,
à la recherche et à l'innovation SEFRI

Rémy Hübschi
Chef de division Formation professionnelle et continue

ICT Berufsbildung
Formation professionnelle
Formazione professionale

ICT-Formation professionnelle Suisse

DIRECTIVES

relatives au

règlement concernant

l'examen professionnel de Cyber Security Specialist*

du 20 mai 2019

Vu le ch. 2.21, let. a du règlement concernant l'examen professionnel de Cyber Security Specialist du 6.5.2019, la commission d'examen arrête les directives suivantes:

1. INTRODUCTION

1.1 But des directives

Les directives complètent et précisent les dispositions du règlement d'examen. Elles sont édictées, contrôlées périodiquement et, si nécessaire, adaptées par la commission d'examen.

1.2 Bases légales

- Loi fédérale sur la formation professionnelle (LFPr)
- Ordonnance sur la formation professionnelle (OFPr)

1.3 Secrétariat d'examen

Le secrétariat assure les tâches administratives en relation avec l'examen professionnel pour l'ensemble des régions linguistiques et est l'interlocuteur pour toutes les questions qui s'y rapportent.

Adresse du secrétariat d'examen:

ICT-Formation professionnelle Suisse
Aarbergergasse 30, 3011 Berne
Tél.: +41 58 360 55 50
E-mail: info@ict-berufsbildung.ch
Site Internet: www.ict-berufsbildung.ch

* Pour faciliter la lecture du document, le masculin est utilisé pour désigner les deux sexes.

2. PROFIL DE LA PROFESSION

Le profil de la profession est décrit au ch. 1.2 du règlement d'examen sur la base des principales compétences opérationnelles. Dans le profil de qualification, il est défini de manière détaillée, précisé et complété par des critères de performance.

Le profil de qualification, joint en annexe, fait partie intégrante des présentes directives.

3. CONDITIONS D'ADMISSION

3.1 Généralités

Les conditions d'admission sont réglées au ch. 4.3 du règlement d'examen.

3.2 Pratique professionnelle

La durée de la pratique professionnelle exigée est calculée sur la base d'un plein temps. En cas d'occupation à temps partiel, la durée requise est prolongée en conséquence.

3.3 Documents et attestations à fournir

Les conditions à remplir sont énoncées dans la publication de l'examen, qui décrit aussi le processus d'inscription.

Doivent obligatoirement être joints à l'inscription les documents et attestations ci-dessous:

- curriculum vitae,
- certificats de travail attestant la pratique professionnelle requise,
- titre (certificat, diplôme, etc.) le plus élevé obtenu.

4. EXAMEN

4.1 Généralités

L'examen professionnel fédéral a pour but de vérifier de manière exhaustive si les candidats ont acquis les compétences opérationnelles nécessaires pour exercer la profession de Cyber Security Specialist. La forme d'examen varie selon qu'il s'agit d'évaluer les compétences opérationnelles, les prestations de transfert ou l'application pratique.

4.2 Épreuves d'examen

L'examen est organisé selon les épreuves et durées suivantes:

Épreuve		Forme d'examen	Durée	Pondération
1	Cybersécurité	Traitement de cas pratique	5 h	60%
2	Projets et économie d'entreprise	Traitement de cas écrit	2 h	20%
3	Direction et communication	Traitement de cas oral et entretien professionnel	¾ h	20%
		Total	7 ¾ h	

4.3 Épreuve 1: cybersécurité

4.31 Évaluation et attribution des notes

L'évaluation se fonde sur les critères de performance du profil de qualification en annexe. Pour l'épreuve cybersécurité, les points d'appréciation pondérés suivants sont attribués:

Point d'appréciation		Domaine de compétences op. (DCO x) Critères de performance (CP-x-x)	Pondération
a	Anticipation et prévention	*DCO A*: CP-A-1 à CP-A-13 *DCO D*: CP-D-1 à CP-D-4	30%
b	Détection	*DCO B*: CP-B-1 à CP-B-11 *DCO D*: CP-D-1 à CP-D-4	30%
c	Réponse	*DCO C*: CP-C-1 à CP-C-13 *DCO D*: CP-D-1 à CP-D-4, CP-D-6	40%

4.4 Épreuve 2: projets et économie d'entreprise

4.41 Évaluation et attribution des notes

L'évaluation se fonde sur les critères de performance du profil de qualification en annexe. Pour l'épreuve projets et économie d'entreprise, les points d'appréciation pondérés suivants sont attribués:

Point d'appréciation		Domaine de compétences op. (DCO x) Critères de performance (CP-x-x)	Pondération
a	Projets	*DCO D*: CP-D-9 à CP-D-11	50%
b	Economie d'entreprise	*DCO D*: CP-D-5 à CP-D-8	50%

4.5 Épreuve 3: direction et communication

4.51 Évaluation et attribution des notes

L'évaluation se fonde sur les critères de performance et sur les compétences personnelles et sociales définies dans le profil de qualification en annexe. Pour l'épreuve direction et communication, les points d'appréciation pondérés suivants sont attribués:

Point d'appréciation		Domaine de compétences op. (DCO x) Critères de performance (CP-x-x)	Pondération
a	Direction	*DCO A*: CP-A-6 *DCO D*: CP-D-11 à CP-D-13	50%
b	Communication	*DCO A*: CP-A-11 à CP-A-13 *DCO B*: CP-B-9 *DCO C*: CP-C-10, CP-C-12 *DCO D*: CP-D-8, CP-D-12, CP-D-13	50%

4.6 Moyens auxiliaires

Les moyens auxiliaires autorisés à l'examen sont les suivants:

a) Traitement de cas pratique ou écrit
Est autorisé tout ce qui reflète de manière la plus réaliste possible le travail quotidien d'un Cyber Security Specialist, à l'exception de la collaboration ou de l'aide de tiers, sous quelque forme que ce soit.

b) Traitement de cas oral et entretien professionnel
Est autorisé tout ce qui reflète de manière la plus réaliste possible le travail quotidien d'un Cyber Security Specialist pour la préparation d'un entretien, d'une présentation, etc., à l'exception de la collaboration ou de l'aide de tiers, sous quelque forme que ce soit.

4.7 Plan modulaire ICT

ICT-Formation professionnelle Suisse précise et complète dans le plan modulaire ICT les directives contraignantes du profil de qualification relatif au Cyber Security Specialist (cf. annexe) sous forme de modules. Chaque module ou description de module place une ou plusieurs compétences opérationnelles du profil de qualification dans le contexte technique orienté processus correspondant. Les compétences sont décomposées en plusieurs sous-compétences appelées "objectifs opérationnels". Sont aussi définis pour chaque objectif opérationnel les éléments de connaissance déterminants, c'est-à-dire les "connaissances opérationnelles nécessaires". La description de l'objet fournie dans la description du module renseigne également sur le contexte et la complexité, constituant ainsi un indicateur du niveau d'exigence.

Lien vers le plan modulaire ICT: www.ict-berufsbildung.ch

4.8 Informations complémentaires

Sur le site Internet du Secrétariat d'État à la formation, à la recherche et à l'innovation, les candidats trouveront des informations complémentaires, par exemple sur:

- les contributions pour cours préparatoires de la Confédération,
- la compensation des inégalités frappant les personnes avec handicap,
- les procédures de recours.

Source: https://www.sbfi.admin.ch/sbfi/fr/home/formation/fps/examens-federaux/candidats-et-diplomes.html

5. ORGANISATION DE L'EXAMEN

5.1 Publication

L'examen professionnel est annoncé cinq mois au moins avant le début des épreuves. La publication se fait sur www.ict-berufsbildung.ch et est communiquée directement aux prestataires de formation connus.

5.2 Inscription

L'inscription se fait par voie électronique conformément aux indications dans la publication de l'examen.

5.3 Délais

- 4 mois avant l'examen: clôture des inscriptions
- 3 mois avant l'examen: décision sur l'admissibilité
- 6 semaines avant l'examen: convocation à l'examen
- Dates de l'examen selon publication
- 5 semaines après l'examen: communication des résultats

5.4 Retrait

Une éventuelle annulation de l'inscription avant l'examen doit être annoncée conformément au ch. 4.2 du règlement d'examen. Pour couvrir les coûts occasionnés par un retrait, l'organisation des examens facture les frais suivants:

a) CHF 300 en cas de retrait jusqu'à six semaines avant le début de l'examen;
b) CHF 400 en cas de retrait après ce délai pour une des raisons valables selon le ch. 4.22 du règlement d'examen;
c) taxe d'examen complète en cas de retrait après ce délai pour une autre raison que celles valables selon le ch. 4.22 du règlement d'examen.

5.5 Lieux de l'examen et logistique

Les lieux de l'examen sont précisés dans la publication. Les frais de déplacement, de logement et de restauration sont à la charge des candidats.

5.6 Taxe d'examen

L'admission à l'examen ne devient définitive qu'avec le paiement de la taxe d'examen. Le montant de celle-ci figure dans la publication

La taxe d'examen doit être acquittée selon les modalités prévues par l'organisation des examens. Suivant le mode de paiement, l'organisation des examens facture des coûts supplémentaires pour couvrir les frais occasionnés.

5.7 Assurance

Il appartient aux candidats de veiller à leur couverture d'assurance accident, maladie, responsabilité civile, etc.

6. DISPOSITIONS FINALES

6.1 Entrée en vigueur

Les présentes directives ont été adoptées par la commission d'examen le 20 mai 2019

7. ÉDICTION

Berne, le 20 mai 2019

ICT-Formation professionnelle Suisse
Commission d'examen

Daniel Jäggli	Serge Frech
Président	Directeur

8. ANNEXE

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

Identification du module

Numéro de module	674	
Titre	Diriger et soutenir une équipe	
Compétence	Diriger et soutenir une équipe sur le plan professionnel et social en adoptant un comportement de conduite et de communication adapté à la situation.	
Objectifs opérationnels	1	Mener une réflexion sur son propre comportement en vue de conduire une équipe de manière efficace et efficiente.
	2	Définir son propre comportement de conduite de manière consciente et l'adapter en fonction du contexte.
	3	Définir son propre comportement de communication de manière consciente et en fonction de la situation et instaurer au sein de l'équipe une culture de communication basée sur l'estime.
	4	Promouvoir activement le développement de l'esprit d'équipe et clarifier les rôles au sein de l'équipe.
	5	Créer les conditions cadres pour qu'une équipe puisse travailler avec motivation.
	6	Identifier les potentiels de conflit et les conflits au sein de l'équipe et prendre des mesures appropriées pour les éviter, les désamorcer ou les résoudre.
	7	Planifier des processus de changement et soutenir les personnes concernées lors du règlement de différends et de la gestion du changement.
	8	Identifier le besoin de formation continue au sein de l'équipe, développer avec les collaborateurs des objectifs de développement individuels et planifier des mesures correspondantes de formation continue ou de soutien.
Domaine de compétence	Project Management	
Objet	Responsabilité de conduite d'équipes de projet ou d'unités organisationnelles avec des spécialistes et 10 à 12 collaborateurs au maximum.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	674
Titre	Diriger et soutenir une équipe
Compétence	Diriger et soutenir une équipe sur le plan professionnel et social en adoptant un comportement de conduite et de communication adapté à la situation.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître des modèles simples de perception des traits de la personnalité et des caractéristiques comportementales (p.ex. fenêtre de Johari, modèle de l'iceberg) et pouvoir expliquer les différences entre la perception de soi et la perception d'autrui.
	1.2	Connaître des modèles fondamentaux de la gestion du temps et de soi (p.ex. principe d'Eisenhower, principe de Pareto).
	1.3	Connaître l'importance du devoir d'exemplarité dans la conduite.
2	2.1	Connaître les différents styles de conduite et leurs caractéristiques et pouvoir expliquer l'adéquation d'un style en fonction de la situation.
	2.2	Connaître les différentes formes d'organisation et leurs caractéristiques (p.ex. organisation hiérarchique et organisation fonctionnelle, organisation hiérarchique avec état-major, organisation matricielle, organisation de projet pure avec Task Force) et pouvoir expliquer l'adéquation d'une forme d'organisation en fonction de la situation.
3	3.1	Connaître des modèles de communication fondamentaux (p.ex. le modèle des quatre oreilles de Schultz von Thun, la communication non violente selon B. Rosenberg) et pouvoir expliquer leur importance par rapport à son propre comportement de communication.
	3.2	Connaître les règles pour la transmission et la réception de feedbacks.
4	4.1	Connaître la différence entre un groupe et une équipe.
	4.2	Connaître les cinq étapes du développement de l'esprit d'équipe selon Tuckman (Forming, Storming, Norming, Performing et Adjourning) et pouvoir expliquer les caractéristiques de chaque étape.
	4.3	Connaître des modèles de rôles au sein d'une équipe (p.ex. rôles en équipe selon Belbin), connaître la différence entre la construction d'un rôle (role making) et la prise active d'un rôle (role taking) et pouvoir expliquer l'importance de la composition des rôles pour les performance au sein d'une équipe.
5	5.1	Connaître des modèles fondamentaux de la théorie de la motivation (p.ex. Maslow, Herzberg) et pouvoir expliquer leur importance dans la pratique.
	5.2	Connaître la différence entre la motivation intrinsèque et la motivation extrinsèque.
6	6.1	Connaître les caractéristiques et la dynamique des conflits.
	6.2	Connaître des mesures pour éviter et résoudre des conflits.

Connaissances opérationnelles nécessaires

7	7.1	Connaître les phases typiques des processus de changement et pouvoir expliquer les caractéristiques des différentes phases.
	7.2	Connaître les facteurs de succès (p.ex. perception de l'urgence, succès rapides, communication) et les risques liés aux processus de changement.
	7.3	Connaître les signes typiques des peurs et des oppositions et pouvoir expliquer des procédures adaptées pour les gérer.
8	8.1	Connaître des mesures de soutien (p.ex. formation, coaching, développement de l'équipe) et pouvoir expliquer leurs caractéristiques et leur adéquation en fonction de la situation.
	8.2	Connaître les exigences à remplir pour de bonnes conventions d'objectifs et des entretiens constructifs basés sur l'estime en vue d'une convention d'objectifs communs.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	679	
Titre	Collecter des informations sur les menaces et les traiter	
Compétence	Dans le cadre de la Cyber Threat Intelligence (CTI) d'une organisation, collecter et analyser en continu les informations sur les menaces potentielles du cyberespace et consigner les résultats sous forme adéquate, conformément à leur finalité et aux groupes cibles.	
Objectifs opérationnels	1	Collecter de façon continue, proactive et autodirigée des informations sur les menaces actuelles du cyberespace.
	2	Vérifier et évaluer la crédibilité des informations.
	3	Evaluer le potentiel de risque des menaces en tenant compte de la stratégie de sécurité de l'information et de l'infrastructure informatique d'une organisation.
	4	Analyser les informations sur les menaces et documenter les résultats sur les plans tactique et opérationnel de la CTI.
	5	Traiter les résultats issus de la CTI et les communiquer aux parties prenantes internes ou externes sous forme adéquate, conformément aux groupes cibles et aux niveaux concernés.
Domaine de compétence	Security/Risk Management	
Objet	Organisation avec une infrastructure informatique complexe, une stratégie de sécurité de l'information donnée et une organisation structurelle et fonctionnelle définie en termes de Cyber Threat Intelligence (CTI).	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	679
Titre	Collecter des informations sur les menaces et les traiter
Compétence	Dans le cadre de la Cyber Threat Intelligence (CTI) d'une organisation, collecter et analyser en continu les informations sur les menaces potentielles du cyberespace et consigner les résultats sous forme adéquate, conformément à leur finalité et aux groupes cibles.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître la finalité de la Cyber Threat Intelligence (CTI) et ses différents niveaux (p.ex. stratégique, tactique et opérationnel).
	1.2	Connaître diverses causes de menace (p.ex. acte délibéré, vulnérabilités, défaillance technique, com-portement humain inadéquat, cas de force majeure) et pouvoir en expliquer la pertinence quant à la sécurité de l'information et à la cybersécurité.
	1.3	Connaître des sources d'informations internes et externes sur les menaces (p.ex. organisations CERT, catalogue des menaces MELANI, ENISA et BSI, listes d'adresses électroniques, avis et rapports de sécu-rité de fabricants et de prestataires tiers, rapports sandbox, échange d'expériences au sein du réseau de relations, OWASP Top 10, SANS Top 20).
	1.4	Connaître diverses formes de menace et de vecteurs d'attaque (p.ex. maliciels, menace persistante avancée [APT], rançongiciel, attaques DDoS, spoofing, phishing, attaques DNS, bots et réseaux de bots, injection de script, vol de session [session hijacking], ingénierie sociale, courriers indésirables) et pouvoir les expliquer sous l'angle de la voie d'attaque, de la technique d'attaque et de l'objectif de l'attaque (p. ex. panne du système, utilisation abusive du système, vol, fraude, chantage).
2	2.1	Connaître des indicateurs pour évaluer la crédibilité des informations (p.ex. auteur, éditeur, format, indication des sources, actualité, vérifiabilité, reproductibilité) et pouvoir en expliquer la pertinence pour différentes sources.
3	3.1	Connaître les directives et les éléments déterminants de la stratégie de sécurité de l'information d'une organisation (p.ex. appétence au risque, tolérance au risque, objectifs de sécurité stratégiques, inven-taire et classification des valeurs [assets]).
	3.2	Connaître l'infrastructure informatique et le paysage système d'une organisation et pouvoir expliquer la pertinence d'une menace pour les systèmes, réseaux et applications spécifiques à une organisation.
	3.3	Connaître des modèles courants d'évaluation des risques et des menaces (p.ex. matrice des risques, méthodologie d'évaluation des risques de l'OWASP, système d'évaluation standardisé de la criticité des vulnérabilités [CVSS]).

Connaissances opérationnelles nécessaires

4	4.1	Connaître l'importance des descriptions de tactiques, techniques et procédures (TTP) et pouvoir en expliquer l'utilité pour la cybersécurité d'une organisation.
	4.2	Connaître l'importance des indicateurs d'attaque (IoA) et pouvoir citer des exemples typiques (p.ex. anomalies dans le trafic réseau, anomalies dans les heures d'utilisation, requêtes DNS suspectes, redirection des utilisateurs).
	4.3	Connaître l'importance des indicateurs de compromission (IoC) et pouvoir citer des exemples typiques (p.ex. valeurs de hachage, signatures numériques, noms de domaine, adresses IP, URL, adresses e-mail, X-Mailer, HTTP User Agent).
	4.4	Connaître des normes et des modèles courants de classification des menaces (p.ex. taxonomie CERT, taxonomie MISP, taxonomie eCSIRT, Europol Common Taxonomy for Law Enforcement and CSIRTs).
5	5.1	Connaître les parties prenantes internes ou externes déterminantes de la CTI (p.ex. management, CISO, analystes SOC, incident response team [CERT/CIRT], gestion des vulnérabilités et des correctifs, architectes système, administrateurs système, autorités en charge des poursuites pénales) et pouvoir expliquer leurs besoins spécifiques en informations.
	5.2	Connaître divers canaux de communication (p.ex. rapports écrits ou verbaux, collecticiel [groupware], wiki, base de connaissances, forums, médias sociaux) et pouvoir expliquer leurs différences quant à leur impact, fiabilité et sécurité.
	5.3	Connaître des plateformes et des cadres d'échange d'informations courants dans le domaine de la CTI (p.ex. Malware Information Sharing Platform [MISP], Collective Intelligence Framework [CIF], Collaborative Research Into Threats [CRITs], Open Threat Exchange [OTX]).
	5.4	Connaître des formats usuels d'informations CTI (p.ex. STIX, OpenIOC, Intrusion Detection Message Exchange Format [IDMEF], Incident Object Description Exchange Format [IODEF]) et des standards pour l'échange de données CTI lisible par machine (p.ex. TAXII).

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	680	
Titre	Contrôler la sécurité de l'infrastructure informatique	
Compétence	Contrôler, dans le cadre d'un mandat, la sécurité des systèmes, des réseaux et des applications d'une organisation au moyen de méthodes et d'outils appropriés, consigner et présenter les résultats des tests de façon concluante et recommander des mesures pour corriger les failles identifiées.	
Objectifs opérationnels	1	Clarifier et définir avec le mandant les objectifs, le périmètre et les conditions cadres de l'audit de sécurité de tout ou partie de l'infrastructure informatique.
	2	Sélectionner des méthodes de tests de sécurité appropriées en fonction des objectifs et du rapport coûts/utilité.
	3	Vérifier la conformité légale et contractuelle des tests de sécurité planifiés et engager, si nécessaire, des mesures correctives.
	4	Choisir, en tenant compte des objectifs et de la méthodologie de test, des techniques et des outils appropriés pour procéder aux tests et aux audits de sécurité.
	5	Exécuter les tests de sécurité et consigner la procédure et les résultats des tests de façon continue et exhaustive.
	6	Analyser et évaluer les résultats des tests et rédiger un rapport d'audit avec des mesures pour corriger les vulnérabilités.
Domaine de compétence	Security/Risk Management	
Objet	Mandat d'audit de sécurité portant sur l'infrastructure ICT d'une organisation dotée de systèmes, de réseaux et d'applications.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	680
Titre	Contrôler la sécurité de l'infrastructure informatique
Compétence	Contrôler, dans le cadre d'un mandat, la sécurité des systèmes, des réseaux et des applications d'une organisation au moyen de méthodes et d'outils appropriés, consigner et présenter les résultats des tests de façon concluante et recommander des mesures pour corriger les failles identifiées.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître des méthodologies et des standards pertinents pour procéder à des contrôles de sécurité (p.ex. OSSTMM, normes BSI pour les tests d'intrusion [BSI Leitfaden für Penetrationstests], Penetration Testing Execution Standard [PTES], méthodologie de l'OWASP pour la réalisation de tests de pénétration d'applications WEB, Technical Guide to Information Security Testing and Assessment du NIST, CIS Controls, ISO/CEI 2700x).
	1.2	Connaître l'infrastructure informatique et le paysage système du mandant et pouvoir expliquer les possibilités de limitation du périmètre d'un audit de sécurité (p.ex. complet, limité, ciblé).
	1.3	Connaître les conditions cadres organisationnelles et techniques pertinentes applicables aux audits de sécurité (p.ex. identification de tous les systèmes et collaborateurs concernés, durée d'exécution, risques relevant de la responsabilité en cas de pannes et de dommages, accès aux réseaux et à l'infrastructure).
	1.4	Connaître des aspects éthiques pertinents dans le cadre des audits de sécurité (p.ex. utilisation de techniques d'ingénierie sociale, exploitation de vulnérabilités identifiées).
2	2.1	Connaître les possibilités et les limites des scans de vulnérabilité et de l'exploitation (exploiting).
	2.2	Connaître les possibilités et les limites des tests d'intrusion et pouvoir expliquer leurs caractéristiques quant à la perspective (en mode boîte noire, boîte grise ou boîte blanche), au système cible, à la procédure (visible, invisible), à la position de l'attaquant (interne, externe) et à l'agressivité.
	2.3	Connaître les possibilités et les limites des audits et revues techniques (p.ex. audit de sécurité, audit de processus, audit de conformité) et pouvoir expliquer l'objet de l'audit en tant qu'élément de différenciation.
	2.4	Connaître les possibilités et les limites des techniques d'ingénierie sociale.
	2.5	Connaître le modèle et le but des simulations par équipe rouge (red teaming) et par équipe bleue (blue teaming) dans le contexte des tests de sécurité.
3	3.1	Connaître les aspects de droit pénal pertinents en matière de tests de sécurité (p.ex. soustraction de données, accès indu à un système informatique, détérioration de données, utilisation frauduleuse d'un ordinateur) et l'importance du consentement contractuel du mandant.

Connaissances opérationnelles nécessaires

	3.2	Connaître les dispositions légales relatives à la protection des données et au droit d'auteur (licences) dans le contexte des tests de sécurité (p.ex. traitement de données à caractère personnel, modifications non autorisées du code de programme) et pouvoir expliquer les possibilités permettant de garan-tir le respect des prescriptions en la matière.
	3.3	Connaître les risques juridiques civils pertinents dans le contexte des tests de sécurité (p.ex. pannes et endommagements de systèmes, perte et détérioration de données) et pouvoir expliquer les possibilités permettant de prévenir les dommages, les coûts consécutifs ainsi que les demandes de dommages et intérêts.
	3.4	Connaître les principaux contenus d'un contrat de service portant sur des tests de sécurité (p.ex. but, type de tests et technique utilisée, obligation de confidentialité, devoir de diligence, protection des données, demande de dommages et intérêts et exclusion de la responsabilité, notification aux personnes concernées) et pouvoir expliquer leur finalité.
4	4.1	Connaître des techniques manuelles de vérification de la sécurité (p.ex. étude de documents, enquêtes et entretiens, renseignement de sources ouvertes ou Open Source Intelligence [OSINT], piratage manuel et vérification manuelle des exploits, audit physique des contrôles d'accès).
	4.2	Connaître des outils appropriés pour procéder à un audit de sécurité assisté par ordinateur et pouvoir expliquer la finalité de leur utilisation (p.ex. test de stress, scan de vulnérabilités, exploitation, déverrouillage, sniffing, spoofing, rétro-ingénierie).
5	5.1	Connaître les principaux contenus d'un protocole de test compréhensible et traçable (p.ex. identification, timbre horodateur et calendrier, activité, motivation, outils et paramètres, résultats, pièces justificatives).
	5.2	Connaître des possibilités de sauvegarde des pièces justificatives issues des tests de sécurité (p.ex. enregistrement du trafic réseau, captures d'écran, photographies, fichiers log et fichiers journaux des outils).
6	6.1	Connaître diverses causes de vulnérabilités (p.ex. directives de sécurité lacunaires ou non appliquées, failles dans l'architecture de sécurité ou dans la configuration, failles dans la gestion des incidents ou des correctifs).
	6.2	Connaître des modèles courants d'évaluation de la criticité des vulnérabilités (p.ex. Common Vulnera-bility Scoring System [CVSS], OWASP Risk Rating Methodology, schéma de classification des vulnérabilités selon le BSI)
	6.3	Connaître les principaux contenus d'un catalogue de mesures structuré (p.ex. mesure, évaluation, priorité, compétences, évaluation des ressources et estimation des coûts, vérification).
	6.4	Connaître les principaux contenus d'un rapport d'audit (p.ex. synthèse, contexte, objet d'investigation, méthodes, résultats, constats, catalogue des mesures, recommandation avec justification).

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	681	
Titre	Détecter et contrer les attaques ciblant l'infrastructure informatique	
Compétence	Choisir des solutions techniques de surveillance et de protection en vue de détecter et de contrer les attaques ciblant les systèmes, les réseaux et les applications d'une organisation et les mettre en service.	
Objectifs opérationnels	1	Définir, en tenant compte de la situation des menaces, les indicateurs, signatures et motifs pertinents pour détecter des attaques contre l'infrastructure informatique d'une organisation.
	2	Choisir des solutions de surveillance et de protection pour la détection d'attaques basée réseau et leur blocage et mettre celles-ci en service.
	3	Choisir des solutions de protection et de durcissement appropriées pour la détection d'attaques basée hôte et application et leur blocage et mettre celles-ci en service.
	4	Choisir, au regard des directives de l'organisation relatives à la classification des informations, des solutions appropriées de protection des données sensibles contre leur diffusion non autorisée et mettre celles-ci en service.
	5	Choisir, si nécessaire, des solutions appropriées pour leurrer les attaquants et mettre celles-ci en service.
	6	Configurer, en tenant compte des dispositions légales en matière de protection de la personnalité et des données, la journalisation des données concernées dans les solutions de surveillance et de protection.
	7	Tester régulièrement le fonctionnement et l'efficacité des solutions de surveillance et de protection et corriger, si nécessaire, la configuration.
	8	Intégrer les solutions de surveillance et de protection dans un système supérieur de gestion des événements et des informations de sécurité (SIEM).
Domaine de compétence	System Management	
Objet	Organisation dotée d'une infrastructure informatique complexe.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module		681
Titre		Détecter et contrer les attaques ciblant l'infrastructure informatique
Compétence		Choisir des solutions techniques de surveillance et de protection en vue de détecter et de contrer les attaques ciblant les systèmes, les réseaux et les applications d'une organisation et les mettre en service.
Objectifs opérationnels et connaissances opérationnelles nécessaires		
1	1.1	Connaître diverses formes de menace et de vecteurs d'attaque (p.ex. maliciels, menace persistante avancée [APT], rançongiciel, attaques DDoS, spoofing, phishing, attaques DNS, bots et réseaux de bots, injection de script, vol de session [session hijacking], ingénierie sociale, pourriels) et pouvoir les expliquer sous l'angle de la voie d'attaque, de la technique d'attaque et de l'objectif de l'attaque (p.ex. panne du système, utilisation abusive du système, vol, fraude, chantage).
	1.2	Connaître des concepts fondamentaux de détection d'attaques (p.ex. recherche basée sur des motifs ou des règles, détection d'anomalies, inspection de paquets et du contenu, vérification de l'intégrité des fichiers, surveillance des processus, contrôle des journaux).
	1.3	Connaître l'importance des tactiques, techniques et procédures (TTP), des indicateurs d'attaque (IoA) et des indicateurs de compromission (IoC) pour la détection des attaques.
2	2.1	Connaître des normes de réseau courantes (IEEE 802) pour les réseaux locaux (LAN), les réseaux locaux sans fil (WLAN), les réseaux personnels ainsi que les réseaux personnels sans fil (PAN, WPAN) et pouvoir expliquer leurs caractéristiques.
	2.2	Connaître des protocoles d'application courants dans les réseaux TCP/IP (p.ex. HTTP, protocoles de messagerie, DHCP, DNS, annuaires, protocoles de transfert de fichiers, protocoles de gestion des réseaux).
	2.3	Connaître des protocoles de réseau et de transport courants en termes de sécurité cryptographique (p.ex. IPSec, TLS) et leur champ d'application pour un transfert sécurisé des données (p.ex. HTTPS, SMTPS, SIPS, FTPS, SFTP, LDAPS).
	2.4	Connaître des concepts de séparation physique ou logique des réseaux sur différentes couches OSI (p.ex. Spanning Tree Protocol [STP], commutateur de couche 2 et de couche 3, subnetting, VLAN, pare-feu, zone démilitarisée [DMZ], proxy inverse, serveur d'entrée Web [WES], pare-feux applicatifs Web [WAF], répartition de charge [load balancing] et pouvoir expliquer leur fonction.
	2.5	Connaître des outils appropriés pour surveiller le trafic réseau (p.ex. analyseur de paquets Wireshark, MRTG, Nmap, Nagios, lignes de commande pertinentes).

Connaissances opérationnelles nécessaires

	2.6	Connaître les fonctions, les possibilités et les limites des systèmes de détection et de prévention d'intrusion basés réseau (NIDS/NIPS) et pouvoir citer des outils courants (p.ex. Snort, Suricata).
	2.7	Connaître l'importance et le principe de fonctionnement des tarpits pour lutter contre les spams et les vers et pouvoir citer des outils usuels (p.ex. LaBrea, Netfilter).
3	3.1	Connaître des concepts fondamentaux de durcissement des systèmes (p.ex. administration des utilisateurs et authentification, contrôle des accès, désactivation ou limitation des services, chiffrement du disque dur) et pouvoir citer des sources relatives aux meilleures pratiques en matière du durcissement de systèmes d'exploitation courants (p.ex. Windows, Unix/Linux, Mac OS, iOS, Android).
	3.2	Connaître des sources de guides, de directives et de standards courants en matière de durcissement de systèmes et d'applications spécifiques (p.ex. CIS Benchmarks, OpenSCAP, Microsoft Security Baselines, STIG de la DISA, guides de durcissement de la sécurité propres à des produits).
	3.3	Connaître les fonctions, les possibilités et les limites de systèmes de détection et de prévention d'intrusion basés hôte (HIDS/HIPS) et pouvoir citer des outils courants (p.ex. Open Source Tripwire, IDDS, Botshield, Samhain, armes cybernétiques).
	3.4	Connaître les fonctions, les possibilités et les limites de solutions de protection pertinentes basées application (p.ex. WAF basé hôte, filtre anti-spam) et pouvoir citer des outils courants (p.ex. ModSecurity, Fortinet, SpamAssassin, RSPAMD).
4	4.1	Connaître les lignes directrices de l'organisation sur la classification des données quant à leur confidentialité (p.ex. secret, confidentiel, diffusion restreinte, interne et public) et à leur intégrité (p.ex. vital, important, normal) et pouvoir expliquer leur pertinence en ce qui concerne la protection des données sensibles.
	4.2	Connaître des possibilités techniques de protection des données en mouvement (data in motion) sur différents canaux (p.ex. Web, courrier électronique, partages).
	4.3	Connaître des possibilités techniques de protection des données traitées (data at use).
	4.4	Connaître des possibilités techniques de protection des données stockées (data at rest) sur différents supports de stockage (magnétique, optique ou électronique) et dans diverses architectures de stockage (p.ex. NAS, SAN, cloud).
	4.5	Connaître différentes architectures et des fonctions typiques des solutions de protection dans le domaine de la prévention de la perte ou fuite de données (DLP).
5	5.1	Connaître l'importance des honeypots et des honeynets pour leurrer les attaquants et analyser les attaques et pouvoir expliquer leurs caractéristiques en termes d'architecture (client/serveur, physique/virtuelle) et d'interaction (basse/élevée).
	5.2	Connaître des outils courants pour les serveurs honey (p.ex. Honeyd, HoneyTrap, Argos) et les honey clients (p.ex. PhoneyC, mapWOC).
	5.3	Connaître la finalité des honey links dans les applications Web et pouvoir expliquer leur traitement dans les pare-feux applicatifs Web (WAF).

Connaissances opérationnelles nécessaires

6	6.1	Connaître les dispositions régissant la surveillance du comportement personnel issues de la loi sur le travail et de la loi sur la protection des données.
	6.2	Connaître les dispositions de la protection des données en termes de pseudonymisation et d'anonymisation des données à caractère personnel et pouvoir expliquer comment observer les principes de licéité, de proportionnalité, de finalité et de transparence à l'aide d'exemples types d'application.
7	7.1	Connaître des techniques et des outils appropriés de simulation d'attaques (p.ex. scanner de ports, scripts d'exploit, générateurs de charge utile, générateurs SYN flood, générateurs de tests de stress et générateurs de faux positifs).
	7.2	Connaître l'importance des faux positifs dans les solutions de surveillance et de protection et pouvoir expliquer par quels moyens les détecter et les réduire.
	7.3	Connaître les principaux éléments de description des cas de test (p.ex. identification, conditions, consignes d'exécution, procédures et outils, comportement attendu) et établir un protocole de test clair et compréhensible (p.ex. responsabilité, horodatation de l'exécution des tests, résultats des tests, traitement des anomalies et mesures).
8	8.1	Connaître les principales fonctions des systèmes SIEM (collecte et agrégation des données au moyen de collecteurs/agents, présentation des résultats, alarme, application des règles, archivage des données) et pouvoir citer des outils courants (p.ex. ELK Stack, Apache Metron, OSSEC, AlienVault OSSIM, Splunk).
	8.2	Connaître des formats courants d'échange de données lisible par machine entre divers clients et le SIEM (p.ex. Interface for Metadata Access Points [IF-MAP], Common Event Format [CEF], formats Syslog, CSV, XML, valeur-clé).

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	682	
Titre	Gérer les incidents de sécurité	
Compétence	Piloter et surveiller le traitement des incidents de sécurité identifiés tout au long de leur cycle de vie conformément aux structures et aux processus définis dans le cadre de la gestion des incidents de sécurité d'une organisation.	
Objectifs opérationnels	1	Analyser, catégoriser et prioriser les incidents de sécurité dans le cadre du fonctionnement opérationnel et définir, selon le plan de réponse aux incidents, la future marche à suivre pour traiter les différents incidents.
	2	Engager des mesures immédiates appropriées et efficaces en vue de réduire les répercussions d'un incident de sécurité.
	3	Coordonner avec les divisions spécialisées compétentes les mesures techniques requises pour un retour à la normale.
	4	Garantir, si nécessaire, la préservation des éléments de preuve et communiquer les incidents de sécurité pertinents aux divisions ou organes compétents en vue de procéder à des analyses forensiques numériques détaillées.
	5	Soutenir et conseiller de façon ciblée et conformément aux besoins l'organisation d'urgence ou de crise en cas de graves incidents de sécurité.
	6	Documenter et surveiller le traitement d'un incident de sécurité tout au long du cycle de vie et, si nécessaire, procéder à une escalade.
	7	Evaluer périodiquement les incidents de sécurité et faire en sorte que les enseignements tirés soient intégrés dans l'organisation.
Domaine de compétence	Service Management	
Objet	Organisation dotée de structures et de processus définis en vue de détecter et de traiter les incidents de sécurité (Security Incident Management).	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	682
Titre	Gérer les incidents de sécurité
Compétence	Piloter et surveiller le traitement des incidents de sécurité identifiés tout au long de leur cycle de vie conformément aux structures et aux processus définis dans le cadre de la gestion des incidents de sécurité d'une organisation.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître l'importance et le contenu d'un plan de réponse aux incidents pour le traitement des incidents de sécurité.
	1.2	Connaître des facteurs d'influence pour l'analyse et le tri des incidents de sécurité (p. ex. degré de gravité des répercussions, niveau d'urgence de la réponse, ampleur, personnes et services touchés).
	1.3	Connaître des concepts de catégorisation et de priorisation des incidents de sécurité.
	1.4	Connaître des outils permettant d'administrer les incidents de sécurité de l'information (p. ex. système de gestion des incidents de sécurité, système de suivi de problèmes [issue tracking system], banque de données répertoriant les problèmes).
2	2.1	Connaître des mesures techniques immédiates de blocage des vecteurs d'attaque (p. ex. séparation, isolation, désactivation, déconnexion, sinkholding).
	2.2	Connaître des critères d'évaluation de l'adéquation des mesures immédiates (p. ex. danger potentiel, complexité et chances de réussite, temps requis, niveau de gravité des préjudices, ampleur de l'impact).
3	3.1	Connaître les divisions ICT spécialisées et les processus concernés au sein de l'organisation et pouvoir expliquer leurs compétences et besoins pour un retour à la normale (p. ex. Service Operations, Service Continuity Management, Release and Deployment Management, Service Asset and Configuration Management, Service Level Management).
	3.2	Connaître les différences entre style de direction directif et participatif, entre procédure orientée structures, orientée processus et orientée personnes ainsi qu'entre une communication formelle et informelle et pouvoir expliquer leur adéquation situationnelle respective lors de la coordination des parties prenantes.
	3.3	Connaître les directives de l'entreprise relatives à la reprise d'activité (business recovery) et pouvoir expliquer les objectifs déterminants dans le cadre du retour à la normale (p. ex. recovery time objective [RTO], recovery point objective [RPO]).
	3.4	Connaître les directives de l'entreprise en termes de Business Continuity Management (BCM) et pouvoir expliquer la pertinence des mesures BCM planifiées pour le retour à la normale.

Connaissances opérationnelles nécessaires

4	4.1	Connaître les principes des investigations numériques (p. ex. intégrité, crédibilité, reproductibilité, documentation).
	4.2	Connaître les exigences en termes de recevabilité légale des éléments de preuve (p. ex. duplication forensique, principe des quatre yeux, journalisation exhaustive).
	4.3	Connaître les directives de l'entreprise et les compétences en matière d'analyses forensiques numériques (p. ex. Incident Response Team [CERT/CIRT], spécialistes externes, autorités de poursuites pénales).
5	5.1	Connaître les caractéristiques des situations d'urgence et des crises et pouvoir expliquer les différences par rapport à un fonctionnement opérationnel normal.
	5.2	Connaître les compétences et les processus d'une organisation dans le cadre de la maîtrise des crises et des situations d'urgence.
	5.3	Connaître les principes de base de la communication de crise (rapidité, véracité, langage compréhensible, cohérence) et les différents groupes cibles (p. ex. personnes concernées, autorités, médias, parties impliquées) et pouvoir expliquer l'importance d'une communication adaptée au public cible.
6	6.1	Connaître les éléments de contenu d'une documentation claire et compréhensible relative aux incidents de sécurité (rapport d'incident [incident record]).
	6.2	Connaître des standards et des modèles permettant une description et une classification structurée des incidents de sécurité (p. ex. taxonomie CERT, taxonomie MISP, taxonomie eCSIRT, Europol Common Taxonomy for Law Enforcement and CSIRTs).
	6.3	Connaître des éléments déclencheurs d'un processus d'escalade (p. ex. liés à la quantité dans le temps, à la qualité du contenu, à des personnes) et pouvoir expliquer des exemples typiques de la gestion des incidents de sécurité (p. ex. priorité de l'incident de sécurité, niveaux de service issus des SLA et niveaux opérationnels issus des OLA, RTO et RPO en ce qui concerne la reprise après sinistre [disaster recovery]).
	6.4	Connaître le processus d'escalade et la hiérarchie d'escalade d'une organisation dans le cadre de la gestion des incidents de sécurité.
7	7.1	Connaître des valeurs statistiques et des indicateurs clés de performance (ICP) dans le contexte de la gestion des incidents de sécurité.
	7.2	Connaître des méthodes et des techniques appropriées pour synthétiser et représenter les informations (p. ex. tableaux de fréquence et histogrammes, agrégation au moyen de tableaux croisés et de tableaux croisés dynamiques, diagramme de corrélation, analyse de séries temporelles et analyse des tendances).
	7.3	Connaître les directives de l'entreprise en matière d'amélioration continue et pouvoir expliquer les besoins en informations spécifiques et les compétences des parties prenantes concernées (p. ex. management, CISO, CTI, gestion des changements, compliance, ressources humaines, divisions ICT, collaborateurs).

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	683	
Titre	Analyser et interpréter des ensembles de données	
Compétence	Inspecter des données brutes et des ensembles de données quant à la présence d'informations critiques et déterminantes pour la sécurité, plausibiliser les résultats et les exploiter de façon probante en adéquation avec le public cible.	
Objectifs opérationnels	1	Collecter des données brutes non structurées, semi-structurées ou structurées qui sont pertinentes pour la sécurité à partir des systèmes, des applications, des solutions de surveillance et de protection d'une organisation.
	2	Masquer, pseudonymiser ou anonymiser des données brutes sensibles si nécessaire et conformément à la protection des données.
	3	Programmer des scripts et des outils pour évaluer, traiter et représenter de grands ensembles de données.
	4	Interroger des bases de données et mettre en forme les résultats obtenus.
	5	Inspecter les données quant à la présence d'anomalies, d'indicateurs ou de motifs spécifiques à des incidents de sécurité potentiels.
	6	Plausibiliser les données obtenues, identifier et filtrer les faux positifs et étoffer le contenu informatif des résultats en enrichissant les données brutes avec des informations complémentaires lisibles.
	7	Evaluer l'analyse des données, consigner les résultats dans un rapport final probant et présenter les résultats aux décideurs en adéquation avec le groupe cible.
Domaine de compétence	Security/Risk Management	
Objet	Données brutes et ensembles de données relevant de la sécurité et issus de systèmes, d'applications, de solutions de surveillance et de protection d'une organisation.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	683
Titre	Analyser et interpréter des ensembles de données
Compétence	Inspecter des données brutes et des ensembles de données quant à la présence d'informations critiques et déterminantes pour la sécurité, plausibiliser les résultats et les exploiter de façon probante en adéquation avec le public cible.

Objectifs opérationnels et connaissances opérationnelles nécessaires		
1	1.1	Connaître des exemples typiques de données non structurées, semi-structurées ou structurées et pouvoir expliquer leurs différences et leurs spécificités au regard de l'analyse des données.
	1.2	Connaître des sources usuelles de données pertinentes pour la sécurité dans l'infrastructure informatique d'une organisation (p. ex. SIEM, fichiers log et fichiers journaux d'appareils et d'applications, e-mail, messages instantanés, bases de données d'applications).
	1.3	Connaître des formats de données texte et binaires pour l'échange et la sérialisation des données (p. ex. CSV, XML, JSON, BSON, YAML, HDF) et pouvoir expliquer leurs spécificités, leurs différences et leur pertinence pour les analyses de données.
	1.4	Connaître divers standards et formats de fichiers journaux (p. ex. Syslog, journal des événements Windows, fichiers log de serveurs Web).
	1.5	Connaître des outils appropriés pour la gestion des logs (p. ex. Splunk, Papertrail, Loggly, GrayLog, Logstash) et pouvoir expliquer leurs fonctionnalités (p. ex. collecte, indexation, analyse, visualisation).
2	2.1	Connaître l'importance du masquage, de la pseudonymisation et de l'anonymisation statiques et dynamiques des données et pouvoir expliquer leurs différences ainsi que les défis à relever lors de leur mise en œuvre.
	2.2	Connaître diverses méthodes de masquage, de pseudonymisation et d'anonymisation des données (p. ex. suppression, substitution, hachage, réarrangement de données [shuffling], méthode de variance, méthodes de chiffrement) et pouvoir expliquer leur principe de fonctionnement.
	2.3	Connaître diverses procédures d'anonymisation (p. ex. k-anonymité, l-diversité, confidentialité différentielle, Diffix) et pouvoir expliquer leur niveau de sécurisation face à la désanonymisation ou réidentification et leur influence sur la qualité et la valeur informative des données brutes.
	2.4	Connaître les dispositions légales de la protection des données en matière de pseudonymisation et d'anonymisation des données à caractère personnel et pouvoir expliquer comment respecter les principes de licéité, de proportionnalité, de finalité et de transparence à l'aide d'exemples d'application typiques.

Connaissances opérationnelles nécessaires

	2.5	Connaître des outils appropriés de masquage, de pseudonymisation et d'anonymisation d'ensembles de données (p. ex. Amnesia, Anonimatron, ARX).
3	3.1	Connaître des expressions régulières et pouvoir expliquer leur pertinence dans les analyses de données.
	3.2	Connaître des commandes et des concepts pertinents (p. ex. entrées et sorties, filtres, tubes [pipes], redirection) des interpréteurs de commande des systèmes d'exploitation Windows (cmd, PowerShell) et Unix/Linux (p. ex. bash, ksh, zsh) et pouvoir expliquer leurs possibilités et leurs limites dans le contexte de l'analyse des données.
	3.3	Connaître la syntaxe du langage de programmation Python, les bibliothèques de référence (p. ex. NumPy, SciPy, Pandas, Matplotlib) et les outils usuels (p. ex. IPython, Jupyter Notebooks) pour l'analyse et la représentation des données.
	3.4	Connaître des langages de programmation alternatifs à Python (p. ex. R, Scala, Julia, MATLAB) et pouvoir expliquer leur pertinence dans le contexte de l'analyse des données.
4	4.1	Connaître le concept de base de données relationnelle et SQL, pouvoir citer des exemples d'application et des technologies typiques (p. ex. MySQL, serveur SQL, PostgreSQL) et expliquer leurs avantages et leurs inconvénients dans le traitement de grandes quantités de données.
	4.2	Connaître des technologies courantes de bases de données non relationnelles NoSQL (p. ex. Cassandra, BigTable, MongoDB, CouchDB, Riak) et pouvoir expliquer leur modèle de données (orienté colonne, orienté document, orienté graphe, valeur-clé), les possibilités d'effectuer des requêtes (p. ex. UnQL, méthodes objet) ainsi que leurs avantages et leurs inconvénients pour le traitement de grandes quantités de données.
5	5.1	Connaître des techniques et des concepts pertinents pour l'analyse de grandes quantités de données (p. ex. reconnaissance de motifs, A/B testing, analyse de séries temporelles, corrélation statistique et régression, apprentissage automatique [machine learning].
	5.2	Connaître des indicateurs typiques de compromission (IoC), p. ex. valeurs de hachage, signatures, noms de domaine, adresses IP, URL, adresses e-mail, X-Mailer, HTTP User Agent).
	5.3	Connaître des anomalies typiques relatives à la sécurité (p. ex. écarts dans l'utilisation de la bande passante, anomalies au niveau des protocoles/ports).
6	6.1	Connaître l'importance des faux positifs pour l'évaluation des ensembles de données et pouvoir expliquer des exemples typiques.
	6.2	Connaître des sources usuelles d'informations complémentaires en vue d'enrichir les données (p. ex. DHCP, AD, inventaire, base de données de configuration).
	6.3	Connaître des commandes pertinentes pour recueillir des informations complémentaires (p. ex. nslookup, whois, trace/tracert) et pouvoir expliquer le contenu de ces informations.
7	7.1	Connaître des méthodes et des techniques appropriées de synthèse et de présentation des informations (p. ex. réduction des données, création de ratios, tableaux de fréquence et histogrammes, agrégation au moyen de tableaux croisés et de tableaux croisés dynamiques, diagramme de corrélation, analyse de séries temporelles et analyse des tendances).

Connaissances opérationnelles nécessaires

	7.2	Connaître les principaux contenus d'un rapport final d'analyse (p. ex. synthèse, contexte, objet de l'analyse, méthodes, résultats, constats, options d'action, recommandation avec justification) et pouvoir expliquer leur contribution à la prise de décisions.
	7.3	Connaître les contenus et la structure d'une bonne présentation et pouvoir expliquer en quoi ses propres compétences en termes d'expression et de comportement influencent le travail de persuasion.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	684	
Titre	Procéder à une investigation numérique des systèmes	
Compétence	Inspecter les données persistantes, temporaires ou volatiles des systèmes quant à la présence de maliciels ou de traces numériques suspectes, exploiter et présenter les résultats de l'investigation de façon probante et en adéquation avec le groupe cible.	
Objectifs opérationnels	1	Clarifier et définir avec le mandant l'objet de suspicion, les objectifs et les conditions cadres d'une investigation numérique.
	2	Définir, en tenant compte des objectifs et des conditions cadres, la méthode et la procédure de l'investigation numérique.
	3	Vérifier la conformité légale d'une investigation numérique et engager, si nécessaire, des mesures correctives.
	4	Acquérir les systèmes à inspecter et sauvegarder les données persistantes, temporaires ou volatiles.
	5	Inspecter les données préservées quant à la présence de traces suspicieuses ou d'indicateurs de maliciels et procéder à l'enregistrement continu et exhaustif des étapes de l'investigation numérique.
	6	Analyser les fichiers suspects à des fins de détection de fonctions nuisibles ou indésirables et décrire les indicateurs relatifs aux maliciels identifiés.
	7	Evaluer l'investigation, consigner les résultats dans un rapport final probant et présenter les résultats aux décideurs en adéquation avec le groupe cible.
Domaine de compétence	Security/Risk Management	
Objet	Données persistantes, temporaires ou volatiles sur des serveurs, des terminaux et périphériques fixes ou mobiles, des solutions de stockage et des applications.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	684
Titre	Procéder à une investigation numérique des systèmes
Compétence	Inspecter les données persistantes, temporaires ou volatiles des systèmes quant à la présence de maliciels ou de traces numériques suspectes, exploiter et présenter les résultats de l'investigation de façon probante et en adéquation avec le groupe cible.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître les phases et activités usuelles d'une investigation numérique (p. ex. identification de l'objet d'investigation, collecte et conservation des données, investigation, rapport) et pouvoir citer des normes ou standards établis (p. ex. guides NIST, Guide to IT Forensics du BSI).
	1.2	Connaître les sous-domaines typiques de la forensique numérique (p. ex. analyse forensique des disques durs, des systèmes d'exploitation, des réseaux) et pouvoir expliquer leur pertinence dans l'inspection de serveurs, de terminaux et de périphériques fixes ou mobiles, de solutions de stockage et d'applications.
	1.3	Connaître des types de données pertinents pour les investigations numériques (p. ex. données de configuration, données de processus, données d'application, données de session, données de protocole de communication, métadonnées) et pouvoir expliquer des exemples et les différences entre les types de données.
	1.4	Connaître des conditions cadres organisationnelles et techniques pertinentes pour les investigations numériques (p. ex. identification de tous les systèmes et collaborateurs concernés, temps requis et dilemme par rapport au rétablissement rapide du fonctionnement normal, risques relevant de la responsabilité, accès à l'infrastructure et aux réseaux, proportionnalité).
2	2.1	Connaître les conditions, les possibilités et les limites des analyses post mortem (dead box, hors ligne) et des analyses live (live box, en ligne) et pouvoir expliquer les différences entre ces deux approches.
	2.2	Connaître les différences entre une procédure orientée données et une procédure orientée incidents dans le cadre des investigations numériques et pouvoir expliquer la pertinence de la chronologie dans leur exécution.
	2.3	Connaître les conditions, les possibilités et les limites des analyses statiques et dynamiques de maliciels et pouvoir expliquer les différences entre ces deux approches.
3	3.1	Connaître les dispositions pertinentes de la protection des données dans le cadre d'investigations numériques effectuées par des organisations privées (p. ex. ordonnance d'investigation, communication et annonce, protection de la personnalité).
	3.2	Connaître les dispositions et les limites pénales pertinentes relatives aux investigations numériques effectuées par des organisations privées (p. ex. li-

Connaissances opérationnelles nécessaires

		mitation à la propre infrastructure, soustraction de données, accès indu à un système informatique, détérioration des données).
	3.3	Connaître les conditions applicables aux investigations numériques effectuées par les autorités d'instruction pénale et pouvoir citer les possibilités étendues qu'elles détiennent (p. ex. accès aux données de tiers par décision de justice ou par demande d'entraide judiciaire).
	3.4	Connaître les exigences à remplir par un processus d'investigation numérique (p. ex. intégrité des données, admissibilité et crédibilité des méthodes, reproductibilité, documentation) et pouvoir expliquer leur pertinence pour une chaîne de traçabilité solide (chain of custody) et la recevabilité juridique des éléments de preuve.
4	4.1	Connaître les exigences à remplir par la sauvegarde forensique de supports de données physiques avec des données persistantes (p. ex. copie de travail et copie d'archive, exhaustivité, traitement des erreurs, intégrité) et pouvoir expliquer avec quelles mesures ces exigences peuvent être remplies (p. ex. utilisation de bloqueurs d'écriture matériels ou logiciels, copie bit par bit, somme de contrôle cryptographique).
	4.2	Connaître les exigences à remplir par la sauvegarde forensique de mémoire volatile et de fichiers d'échange (swap files) temporaires et pouvoir expliquer quelles informations doivent être préservées en sus pour l'analyse d'une copie-image (p. ex. date et heure système, liste des applications et des processus actifs, connexions réseau actives).
	4.3	Connaître des outils appropriés pour créer des copies forensiques de supports de données et regrouper des supports de données (systèmes RAID).
	4.4	Connaître des outils appropriés pour créer des images mémoire (p. ex. Volatility, Autopsy, The Sleuth Kit).
	4.5	Connaître des possibilités, des techniques et des outils pour la sauvegarde de systèmes virtualisés (p. ex. copies de fichiers RAM ou de fichiers HDD, instantané de stockage [snapshot]).
5	5.1	Connaître les caractéristiques déterminantes de l'architecture des appareils fixes ou mobiles (p. ex. processeur, mémoire, interfaces) et pouvoir expliquer leurs différences et leur pertinence pour des analyses forensiques numériques.
	5.2	Connaître des systèmes d'exploitation courants d'appareils fixes ou mobiles (p. ex. Windows, Unix/Linux, Mac OS, iOS, Android) et pouvoir expliquer leurs caractéristiques et différences au regard des analyses forensiques numériques (p. ex. noyau, appels système, gestion des processus, formats de fichiers exécutables, processus de démarrage, emplacement de stockage des données de configuration).
	5.3	Connaître des concepts courants de partitionnement des supports de données (p. ex. DOS/MBR, partition Apple, partition BSD, table de partitionnement GUID [GPT]) et de regroupement ou de concaténation de supports de données (p. ex. RAID, disk spanning, JBOD, NRAID) et pouvoir expliquer leurs caractéristiques, leurs différences et leur pertinence pour des analyses forensiques numériques.
	5.4	Connaître des systèmes de fichiers courants (p. ex. FAT, NTFS, ExtX, UFS) et pouvoir expliquer leurs caractéristiques, leurs différences et leur pertinence pour des analyses forensiques numériques (p. ex. structure des données, noms de fichiers et de répertoires, journalisation, récupération de données [carving]).

Connaissances opérationnelles nécessaires

	5.5	Connaître des procédures cryptographiques courantes pour le chiffrement des données (p. ex. RSA, ECDHE, ECDSA, SHA, 3DES, AES) et pouvoir expliquer leurs fonctions (échange de clés, authentification, fonction de hachage et chiffrement) ainsi que leur influence sur les analyses forensiques numériques.
	5.6	Connaître des indicateurs typiques de détection de maliciels (p. ex. valeurs de hachage, noms de fichiers, clé de registre, règles YARA) et des sources pertinentes pour de tels indicateurs (p. ex. OpenIOC, YARA Repository, CTI de l'organisation).
	5.7	Connaître des outils appropriés pour l'analyse des fichiers et de leur contenu.
	5.8	Connaître les principaux contenus d'un rapport d'investigation probant et compréhensible (p. ex. identification, chronologie et horodatage, activité, outils et paramètres, résultats, justificatifs, preuves).
6	6.1	Connaître des outils appropriés pour l'analyse statique de maliciels et pouvoir expliquer la finalité de leur utilisation (p. ex. détermination des propriétés des fichiers et des métadonnées, éditeurs Hex, identification de motifs, désassemblage, rétro-ingénierie).
	6.2	Connaître les défis typiques à relever dans le cadre de l'analyse statique de maliciels (p. ex. compression, chiffrement, déguisement ou camouflage de maliciels au moyen de run time packers, de crypteurs et de méthodes d'obfuscation du code source) et pouvoir expliquer des procédures alternatives.
	6.3	Connaître des outils appropriés pour l'analyse dynamique de maliciels et pouvoir expliquer la finalité de leur utilisation (p. ex. isolation/sandboxing, simulation, débogage).
	6.4	Connaître les défis typiques à relever dans le cadre de l'analyse dynamique de maliciels (p. ex. différences au niveau du langage, de l'architecture système ou du système d'exploitation; détection de machines virtuelles ou de sandboxes par le maliciel, mesures anti-débogage du maliciel par chiffrement ou camouflage) et pouvoir expliquer des procédures ou méthodes alternatives.
	6.5	Connaître des formats courants pour décrire les indicateurs de maliciels (p. ex. STIX, format OpenIOC, Intrusion Detection Message Exchange Format [IDMEF], Incident Object Description Exchange Format [IODEF], règles YARA).
7	7.1	Connaître des méthodes et des techniques appropriées de synthèse et de présentation des informations (p. ex. réduction des données, création de ratios, tableaux de fréquence et histogrammes, agrégation au moyen de tableaux croisés et de tableaux croisés dynamiques, diagramme de corrélation, analyse de séries temporelles et analyse des tendances).
	7.2	Connaître les principaux contenus d'un rapport final d'investigation (p. ex. synthèse, contexte, objet de l'analyse, méthodes, résultats, constats, options d'action, recommandation avec justification) et pouvoir expliquer leur contribution à la prise de décisions.
	7.3	Connaître le contenu et la structure d'une bonne présentation et pouvoir expliquer en quoi ses propres compétences en termes d'expression et de comportement en public influencent le travail de persuasion.

Version du module	1.0

Connaissances opérationnelles nécessaires

Créé le	11.02.2021

Identification du module

Numéro de module	685	
Titre	Assurer la gestion des vulnérabilités et des correctifs	
Compétence	Identifier et prioriser les failles des systèmes, des réseaux et des applications d'une organisation et les traiter dans le cadre de la gestion des vulnérabilités et des correctifs.	
Objectifs opérationnels	1	Surveiller en continu les développements actuels concernant les vulnérabilités dans le fonctionnement opérationnel.
	2	Vérifier de façon proactive la sécurité de l'infrastructure informatique d'une organisation quant aux vulnérabilités devenues connues.
	3	Evaluer la criticité des vulnérabilités identifiées et fixer les priorités dans leur traitement.
	4	Vérifier la disponibilité d'un correctif afin de supprimer une vulnérabilité et définir, si nécessaire, des mesures alternatives.
	5	Vérifier au moyen de tests appropriés la fonction et l'efficacité des correctifs avant la mise en production.
	6	Planifier et coordonner avec les divisions ICT la distribution des correctifs de sécurité sur l'environnement productif et garantir l'actualisation des informations de configuration.
	7	Vérifier et évaluer périodiquement la performance et l'efficacité de la gestion des vulnérabilités et des correctifs et proposer, si nécessaire, des mesures d'amélioration.
Domaine de compétence	Service Management	
Objet	Organisation dotée d'une infrastructure informatique complexe ainsi que de structures et de processus définis pour la gestion des vulnérabilités et des correctifs.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	685
Titre	Assurer la gestion des vulnérabilités et des correctifs
Compétence	Identifier et prioriser les failles des systèmes, des réseaux et des applications d'une organisation et les traiter dans le cadre de la gestion des vulnérabilités et des correctifs.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître des déclencheurs possibles (triggers) pour la détection des vulnérabilités dans le fonctionnement opérationnel d'une organisation (gestion des incidents de sécurité, tests de sécurité périodiques, Cyber Threat Intelligence [CTI], avis et rapports de sécurité des fabricants).
	1.2	Connaître diverses sources contenant des informations actuelles sur les vulnérabilités (p. ex. Common Vulnerabilities and Exposures [CVE], avis et rapports de sécurité de fabricants et de prestataires tiers, listes d'adresses électroniques, organisations CERT, catalogue des menaces MELANI, ENISA et BSI).
2	2.1	Connaître l'infrastructure informatique et le paysage système d'une organisation et pouvoir expliquer la pertinence des interdépendances entre les systèmes dans le contexte de la gestion des vulnérabilités et des correctifs.
	2.2	Connaître des normes et directives courantes en matière de durcissement des systèmes, des réseaux et des applications (p. ex. CIS Benchmarks, Microsoft Security Baselines, STIG de la DISA, guides de durcissement de la sécurité spécifiques à des produits) et pouvoir expliquer en quoi le durcissement des systèmes est important dans le cadre de la gestion des vulnérabilités.
	2.3	Connaître des outils appropriés pour détecter des vulnérabilités dans les systèmes, les réseaux et les applications (p. ex. OpenVAS, Nessus, Metasploit, IronWASP, outils spécifiques à des fabricants).
3	3.1	Connaître des modèles courants d'évaluation de la criticité des vulnérabilités (p. ex. Common Vulnerability Scoring System [CVSS], schéma de classification des vulnérabilités selon le BSI).
	3.2	Connaître des facteurs d'influence déterminants dans la priorisation des vulnérabilités (p. ex. inventaire et classification des valeurs [assets], exposition des systèmes menacés, répercussions possibles d'une vulnérabilité, disponibilité d'exploits).
4	4.1	Connaître divers types de releases logiciels (p. ex. mise à niveau, mise à jour, service pack, correctif, hotfix) et pouvoir expliquer leurs différences en termes de portée, de finalité, de degré de maturité, de versionnage (numéros de version) et de déploiement.
	4.2	Connaître l'importance d'une réaction en temps réel dans la gestion des correctifs et pouvoir expliquer les caractéristiques d'exploits zero-day et d'attaques zero-day ainsi que les menaces que ceux-ci représentent.

Connaissances opérationnelles nécessaires

	4.3	Connaître des mesures alternatives aux correctifs afin de réduire le potentiel de menace d'une vulnérabilité (p. ex. renoncement à un produit ou produit alternatif, déplacement d'un système menacé dans un segment de réseau avec un besoin de protection plus élevé, séparation temporaire ou déconnexion).
5	5.1	Connaître des raisons de tester des mises à jour et des correctifs avant le déploiement (p. ex. dépendances dans la suite des correctifs, temps requis et interruptions éventuelles, dépendances résultant de la configuration système, interdépendances avec d'autres systèmes, preuve de l'efficacité).
	5.2	Connaître les exigences à remplir par un environnement de test idéal (p. ex. séparation de l'environnement productif, image exacte [miroir] de l'environnement productif en ce qui concerne les conditions système, les logiciels, la configuration et les données) et pouvoir expliquer d'autres procédures en cas d'indisponibilité d'un environnement de test.
	5.3	Connaître des méthodes et des techniques pour tester des correctifs (p. ex. tests de fonctionnement manuels, contrôle des fichiers log ou fichiers journaux, tests de régression automatisés, vérification de l'efficacité au moyen de scripts d'exploits).
6	6.1	Connaître les divisions ICT et les processus d'une organisation et pouvoir indiquer leurs compétences et leurs besoins lors du déploiement des mises à jour et des correctifs (p. ex. Change Management, Release and Deployment Management, Service Asset and Configuration Management, Service Operations, Service Level Management).
	6.2	Connaître diverses stratégies de distribution des mises à jour et des correctifs (p. ex. séquentielle, parallèle, big bang) et pouvoir expliquer les facteurs déterminants dans le choix d'une stratégie.
	6.3	Connaître des aspects déterminants de la planification des mises à jour et des correctifs (p. ex. temps requis, interruptions, annonce, sauvegarde des données, scénario d'urgence et scénario de retour en arrière [fallback]).
	6.4	Connaître les possibilités et les limites des outils servant à la distribution automatisée des mises à jour et des correctifs.
	6.5	Connaître l'importance de la gestion de configuration et l'utilité d'une base de données de gestion de configuration (CMDB) et pouvoir expliquer les principaux éléments d'information d'un configuration item (CI) dans la CMDB.
7	7.1	Connaître des valeurs statistiques et des indicateurs clés de performance (CPI) pertinents dans le contexte de la gestion des vulnérabilités et des correctifs.
	7.2	Connaître des méthodes et des techniques appropriées de synthèse et de présentation des informations (p. ex. tableaux de fréquence et histogrammes, agrégation au moyen de tableaux croisés et de tableaux croisés dynamiques, diagrammes de corrélation, analyse de séries temporelles et analyse des tendances).
	7.3	Connaître les directives de l'entreprise en matière d'amélioration continue et pouvoir expliquer les besoins en informations relatifs à la gestion des vulnérabilités et des correctifs spécifiques aux parties prenantes concernées (p. ex. management, CISO, SOC, CERT, divisions ICT, fournisseurs et fabricants).

Connaissances opérationnelles nécessaires

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	686	
Titre	Fournir des conseils techniques aux clients et les former	
Compétence	Fournir aux clients internes ou externes des conseils techniques orientés besoins et solutions, planifier et dispenser des formations adaptées aux groupes cibles.	
Objectifs opérationnels	1	Clarifier et définir avec le client les attentes, les objectifs et les conditions cadres du conseil technique.
	2	Discuter avec le client de l'espace de problème du conseil technique et l'analyser avec lui.
	3	Concevoir et animer avec le client le développement d'options d'actions et de solutions.
	4	Conseiller le client lors de l'évaluation des options de solutions et de la formulation des objectifs de changement.
	5	Clarifier et définir en accord avec le client les objectifs d'apprentissage et les conditions cadres de la formation.
	6	Planifier une formation adaptée au groupe cible en tenant compte des objectifs d'apprentissage et préparer les contenus de façon didactique.
	7	Dispenser une formation, vérifier la réalisation des objectifs d'apprentissage, évaluer la formation et identifier des possibilités d'amélioration.
Domaine de compétence	Service Management	
Objet	Fournir aux clients internes ou externes des conseils techniques orientés besoins et solutions, planifier et dispenser des formations adaptées aux groupes cibles.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module		686
Titre		Fournir des conseils techniques aux clients et les former
Compétence		Fournir aux clients internes ou externes des conseils techniques orientés besoins et solutions, planifier et dispenser des formations adaptées aux groupes cibles.
Objectifs opérationnels et connaissances opérationnelles nécessaires		
1	1.1	Connaître les caractéristiques spécifiques à un conseil technique (p. ex. transmission du savoir et des compétences, réflexion sur les relations de cause à effet, démarche orientée résultats et responsabilité en matière de résultat, propres position et avis).
	1.2	Connaître d'autres formes de conseil (p. ex. conseil en processus ou en organisation, médiation, coaching, supervision) et pouvoir expliquer les différences par rapport au conseil technique.
	1.3	Connaître les champs de tension en matière de conseil (p. ex. impartialité vs partialité, caractère facultatif vs obligatoire, indépendance vs dépendance, relation d'égal à égal vs hiérarchie, absence de jugement de valeur vs orientation de valeurs, confidentialité vs transparence, neutralité vs responsabilité quant à la solution).
	1.4	Connaître les différents niveaux du conseil systémique orienté solutions (espace de réalités, espace de possibilités, espace d'objectifs) et pouvoir expliquer leurs caractéristiques et leur finalité dans le cadre d'un processus de conseil.
2	2.1	Connaître des principes de communication et d'entretien importants dans le cadre d'un conseil (p. ex. écoute active, messages-je et messages-tu, refléter, paraphraser, recadrer).
	2.2	Connaître des modèles permettant une analyse structurée de l'espace de problème (p. ex. modèle SCORE de Dilts et Epstein, modèle GROW).
	2.3	Connaître différentes techniques de questionnement (p. ex. questions circulaires, questions échelle, questions de l'exception, questions associatives ou dissociatives) et pouvoir expliquer leur utilisation et leur intérêt dans le cadre du conseil.
	2.4	Connaître des méthodes et des techniques appropriées pour structurer et visualiser des contenus d'entretien (p. ex. diagramme de système et d'interaction, méthode KJ ou diagramme des affinités et clustering, mind mapping, représentations chronologiques, diagramme de causes et d'effets).
3	3.1	Connaître des méthodes appropriées visant à développer des options de solutions (p. ex. Design Thinking, méthode SPALTEN).
	3.2	Connaître des techniques de créativité visant à développer des options de solutions (p. ex. brainstorming, méthode 635, méthode des six chapeaux d'Edward de Bono, méthode Walt Disney, Creative Problem Solving [CPS], workshop pre-morten).

Connaissances opérationnelles nécessaires

	3.3	Connaître des techniques d'intervention couramment utilisées dans le cadre du conseil en vue de développer des options d'actions et de solutions (p. ex. changement de perspective, formation d'hypothèses, intervention paradoxale).
4	4.1	Connaître le principe de l'orientation sur les ressources et son importance dans la réalisation des objectifs.
	4.2	Connaître des méthodes et des techniques appropriées pour évaluer et sélectionner des options de solutions (p. ex. vote à main levée ou vote secret, procédure d'exclusion, questions échelle, méthode du signal lumineux).
	4.3	Connaître des méthodes et des critères pour bien formuler des objectifs et pouvoir expliquer des modèles établis (p. ex. SMART, PURE, CLEAR).
5	5.1	Connaître les facteurs d'influence déterminants pour planifier une formation (p. ex. public cible, taille du groupe, temps disponible, infrastructure, niveau d'exigence).
	5.2	Connaître les principaux éléments pour formuler les objectifs d'apprentissage (comportement final attendu, conditions, critères de performance).
	5.3	Connaître les niveaux de taxonomie du domaine cognitif (selon Bloom) et pouvoir expliquer leur importance lors de la formulation des objectifs d'apprentissage.
6	6.1	Connaître le concept de l'éducation complète «tête, cœur et mains».
	6.2	Connaître les éléments essentiels du triangle didactique et pouvoir expliquer les interrelations entre le savoir, l'apprenant et l'enseignant.
	6.3	Connaître le modèle PAITÉ comme modèle didactique axé sur les compétences pour la préparation de la formation.
	6.4	Connaître divers concepts de formation (p. ex. formation en classe, e-learning, apprentissage mixte [blended learning], auto-apprentissage) et pouvoir expliquer leurs différences en termes de didactique, de forme sociale et de forme de travail.
	6.5	Connaître différentes méthodes de formation (p. ex. exposé, démonstration en direct, jeux, jeux de rôle, discussions, exercices pratiques) et pouvoir expliquer leur adéquation et l'importance du mix des méthodes pour un apprentissage global.
7	7.1	Connaître les compétences et comportements clés d'un formateur ou coach (p. ex. compétence professionnelle, capacité de communication, fonction d'exemplarité, authenticité, motivation, curiosité, ouverture d'esprit) et pouvoir expliquer leur pertinence pour la réussite des formations.
	7.2	Connaître diverses techniques de présentation et d'animation.
	7.3	Connaître diverses formes de vérification des objectifs de formation (p. ex. tests, quiz, auto-évaluation, travail pratique, portefeuille).
	7.4	Connaître des critères de qualité applicables aux formations (p. ex. degré de satisfaction des participants, réussite de l'apprentissage, transfert dans la pratique, intérêt) et diverses méthodes d'évaluation d'une formation (p. ex. questionnaire, enquête orale, baromètre d'opinion).

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	687	
Titre	Délimiter les systèmes et spécifier les exigences	
Compétence	Faire le relevé des prestations qu'un système doit fournir, décrire le contexte du système et les interfaces et spécifier les exigences dans un catalogue d'exigences structuré.	
Objectifs opérationnels	1	Faire avec les parties prenantes déterminantes le relevé des prestations qu'un système doit fournir et de ses propriétés.
	2	Identifier les systèmes périphériques déterminants et leurs relations dans le contexte du système et définir les frontières du système.
	3	Décomposer un système en sous-systèmes ou en systèmes partiels et décrire les interactions.
	4	Définir et décrire des interfaces entre des systèmes périphériques ou des systèmes partiels.
	5	Spécifier dans le cadre d'un dialogue avec les parties prenantes des exigences précises et vérifiables envers les prestations à fournir par le système.
	6	Classer et décrire les exigences dans un catalogue d'exigences structuré.
Domaine de compétence	Business Engineering	
Objet	Analyse d'exigences pour le développement, l'exploitation ou la maintenance de systèmes, processus et services techniques et organisationnels.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	687	
Titre	Délimiter les systèmes et spécifier les exigences	
Compétence	Faire le relevé des prestations qu'un système doit fournir, décrire le contexte du système et les interfaces et spécifier les exigences dans un catalogue d'exigences structuré.	
Objectifs opérationnels et connaissances opérationnelles nécessaires		
1	1.1	Connaître les phases du cycle de vie d'une solution informatique (introduction, croissance, maturité, saturation, déclin et fin de vie) et pouvoir expliquer les prestations typiques des différentes phases.
	1.2	Connaître différentes techniques de relevés (p. ex. entretien, questionnaire, observation, étude de documents, méthode de rapport, atelier) et pouvoir expliquer leurs avantages et leurs inconvénients.
2	2.1	Connaître différentes caractéristiques de systèmes périphériques susceptibles d'influer sur un système (p. ex. acteurs, systèmes de tiers, processus, événements, lois, réglementations, normes).
	2.2	Connaître le but d'une analyse contextuelle du système et son utilité pour le développement du système.
	2.3	Connaître des techniques adaptées pour décrire et représenter des systèmes et leurs relations (p. ex. diagramme de contexte, schéma conceptuel, diagramme de cas d'utilisation UML, diagramme de composants UML, diagramme de flèche).
3	3.1	Connaître la méthode de l'analyse structurée (AS) et ses éléments pour une description formelle du système (p. ex. représentation hiérarchique, diagramme de flux de données, organigramme de programme, structogramme, tableaux et arbres de décision).
	3.2	Connaître la méthode de l'analyse orientée objet (AOO) et ses éléments pour une description formelle de la structure (p. ex. diagrammes de structure UML, modèle entité-relation ERM) et du comportement d'un système (p. ex. diagramme de comportement UML).
	3.3	Connaître la conception pilotée par domaine (Domain Driven Design [DDD]) et ses éléments fondamentaux (p. ex. langage ubiquitaire, modèle de domaine avec entités, objets de valeur et événements de domaine, schéma conceptuel, contexte délimité [bounded context]).
4	4.1	Connaître différents types d'interfaces (p. ex. interfaces matérielles ou logicielles, interfaces utilisateurs [UI], interfaces de programmation [API]) et pouvoir citer des standards courants.
	4.2	Connaître des formes adaptées de description syntaxique et sémantique d'interfaces de données (dictionnaire de données, forme étendue de Backus Naur [EBNF], XML avec DTD ou XMD, JSON, OpenAPI).
5	5.1	Connaître le but et les principaux contenus d'un cahier des charges et d'un cahier des charges avec spécification des exigences.

Connaissances opérationnelles nécessaires

	5.2	Connaître les critères de qualité applicables à la description des exigences (p. ex. concision, compréhensibilité, consistance, mesurabilité et testabilité, clarté, conformité légale).
	5.3	Connaître les éléments du relevé agile des exigences (p. ex. épopées [epics], fonctionnalités, récits utilisateurs [user stories], tâches) et pouvoir expliquer leur but et leur degré de détail.
6	6.1	Connaître les éléments typiques d'une description d'exigences (p. ex. identification, description, priorité, critère d'acceptation, statut).
	6.2	Connaître la différence entre exigences fonctionnelles et exigences non fonctionnelles.
	6.3	Connaître des exigences non fonctionnelles typiques (p. ex. fiabilité, sécurité, utilisabilité, performance, maintenabilité, portabilité, évolutivité) et pouvoir expliquer leur influence sur la qualité d'un système.
	6.4	Connaître l'importance et le but du carnet de produit [product backlog], du carnet de sprint [sprint backlog] et d'un incrément produit pour la gestion agile des exigences.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	688	
Titre	Déterminer les ressources à allouer à des projets ICT et les budgéter	
Compétence	Déterminer les coûts d'un projet ICT, établir une planification des coûts et un budget et contrôler les coûts pendant la réalisation.	
Objectifs opérationnels	1	Déterminer et structurer les ressources nécessaires pour un projet ICT.
	2	Définir les coûts sur la base de la planification des ressources et établir une planification des coûts structurée.
	3	Soutenir les divisions compétentes lors du calcul de l'offre pour le projet ICT.
	4	Etablir sur la base du processus de budgétisation d'une organisation et du plan de financement un budget pour la réalisation du projet ICT.
	5	Contrôler pendant la réalisation du projet ICT les coûts effectifs par rapport au budget et proposer des mesures adéquates de réaction aux écarts.
Domaine de compétence	Business Management	
Objet	Projet ICT (projet, développement du produit ou des services) avec un plan de financement donné.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	688
Titre	Déterminer les ressources à allouer à des projets ICT et les budgéter
Compétence	Déterminer les coûts d'un projet ICT, établir une planification des coûts et un budget et contrôler les coûts pendant la réalisation.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître des éléments de structure typiques de projets ICT orientés en phases (p. ex. phases de projet, projets partiels, lots de travail, procédures, étapes de travail) et de projets ICT agiles (p. ex. backlogs, itérations/sprints, timeboxing).
	1.2	Connaître des positions typiques de la planification des ressources dans des projets ICT (p. ex. personnel, matériel, outils d'exploitation, prestations externes).
	1.3	Connaître des méthodes adaptées de calcul ou d'estimation des coûts (p. ex. méthodes analogiques, cercle d'experts, estimation à 3 points, méthode PERT).
	1.4	Connaître des facteurs d'influence déterminants lors de la planification des coûts des ressources humaines (p. ex. disponibilité, qualification, heures d'inactivité et heures perdues).
2	2.1	Connaître la différence entre coûts d'investissement, coûts de réalisation de projet et coûts d'exploitation.
	2.2	Connaître différents taux de frais pour des projets ICT et pouvoir citer des tarifs conformes au marché et aux branches.
	2.3	Connaître des modèles de calcul simples des coûts.
	2.4	Connaître l'approche de gestion des coûts de projets ICT agiles (enveloppe de coûts fixes, délais fixes et périmètre [scope] ajustable) et l'importance d'un code de collaboration clairement défini (valeurs, principes et pratiques).
3	3.1	Connaître la différence entre frais fixes et frais variables et pouvoir citer des exemples typiques issus de projets ICT.
	3.2	Connaître la différence entre frais individuels et frais généraux (frais overhead) et pouvoir expliquer leur importance pour le calcul des coûts totaux et le taux de couverture.
	3.3	Connaître le seuil de rentabilité (break even) et pouvoir expliquer son importance pour le calcul du prix ou le volume des ventes.
4	4.1	Connaître les exigences de base à l'égard d'un budget (p. ex. rapport à l'avenir, référence à la période, harmonisation temporelle, caractère contraignant, traçabilité) et pouvoir expliquer les incidences sur la trésorerie.

Connaissances opérationnelles nécessaires

	4.2	Connaître le processus de budgétisation au niveau supérieur de l'organisation et pouvoir expliquer ses conséquences sur la budgétisation dans son propre domaine de responsabilité.
5	5.1	Connaître les paramètres fondamentaux d'un contrôle de coûts (p. ex. coûts prévisionnels, coûts effectifs, coûts résiduels prévus).
	5.2	Connaître des méthodes et des instruments adaptés pour l'analyse et la représentation des coûts (p. ex. comparaison entre l'état actuel et l'état projeté, analyse de la tendance des coûts, analyse de la valeur acquise [earned value], coûts de retard [costs of delay]).
	5.3	Connaître des conventions contractuelles typiques pour le contrôle de l'avancement dans le cadre des projets ICT agiles avec un budget et des délais fixes (p. ex. points de contrôle [checkpoints], critères d'acceptation, modèle de partage des risques [riskshare] entre le client et le fournisseur, bonus d'efficience, sorties [exits]).
	5.4	Connaître les paramètres du triangle magique et du carré diabolique et pouvoir expliquer la pertinence de ces modèles pour le développement de mesures en cas d'écarts.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	689	
Titre	Évaluer des solutions informatiques	
Compétence	Procéder à l'évaluation d'une solution informatique sur la base d'un mandat donné et d'exigences définies et formuler une recommandation pour l'acquisition.	
Objectifs opérationnels	1	Évaluer les exigences définies auxquelles la solution informatique doit répondre dans le contexte spécifique et vérifier, si nécessaire, la faisabilité technique et l'efficacité de la solution en question.
	2	Définir, sur la base du mandat de projet ou d'acquisition, la procédure pour l'évaluation d'une solution informatique et établir un calendrier.
	3	Déterminer, sur la base du mandat et des exigences définies, les critères pertinents du catalogue des critères pour évaluer les offres.
	4	Établir un cahier des charges servant de base à l'appel d'offres.
	5	Établir des documents d'évaluation permettant d'apprécier les offres de manière objective et transparente.
	6	Soutenir les départements et organes compétents dans la sélection des prestataires appropriés pour l'appel d'offres.
	7	Contrôler l'exhaustivité et la qualité des offres reçues, demander si nécessaire des modifications et procéder à une première sélection des offres en tenant compte des critères d'exclusion définis.
	8	Évaluer et comparer les offres retenues sur la base des documents d'évaluation et formuler une recommandation d'acquisition à l'attention des décideurs.
Domaine de compétence	Business Engineering	
Objet	Mandat de projet ou d'acquisition pour une solution informatique assorti d'exigences clairement spécifiées.	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module	689
Titre	Évaluer des solutions informatiques
Compétence	Procéder à l'évaluation d'une solution informatique sur la base d'un mandat donné et d'exigences définies et formuler une recommandation pour l'acquisition.

Objectifs opérationnels et connaissances opérationnelles nécessaires

1	1.1	Connaître l'importance et le but des contrôles de faisabilité techniques et leurs différences par rapport à des études de faisabilité ou de projet plus complètes (p. ex. pas de contrôle ou d'évaluation de la rentabilité, de la conformité au droit, du temps à disposition/nécessaire, des risques).
	1.2	Connaître des méthodes pour vérifier la faisabilité technique et la rentabilité de projets ICT (p. ex. projets pilotes, prototypage, simulations, consultation d'experts, objets de référence).
2	2.1	Connaître les raisons typiques d'une évaluation des outils informatiques avant leur acquisition.
	2.2	Connaître les phases, activités et livrables typiques d'un processus d'évaluation et pouvoir en expliquer les interdépendances temporelles et de contenu.
	2.3	Connaître des modèles de procédure pour des acquisitions agiles (p. ex. agile.agreement) et l'importance d'un code de collaboration clairement défini (valeurs, principes et pratiques).
3	3.1	Connaître la différence entre objectifs et exigences.
	3.2	Connaître des possibilités de classifier les objectifs (p. ex. objectifs en termes de performances, de délais, de coûts).
	3.3	Connaître des possibilités de prioriser les objectifs (p. ex. objectifs impératifs, souhaités ou facultatifs, analyse ABC selon Pareto, objectifs de performance, priorisation par catégories d'objectifs, carnets [backlogs] prioritaires).
	3.4	Connaître différents types de critères (p. ex. critères d'exclusion ou KO, critères d'évaluation qualitatifs et quantitatifs, critères de sélection) et la structure de base d'un catalogue de critères.
4	4.1	Connaître les contenus d'un cahier des charges pour un appel d'offres (p. ex. situation de départ, état actuel, objectifs, budget, calendrier, exigences à remplir par l'objet à acquérir ou épopées [epics] de référence et récits utilisateurs [user stories] dans la procédure agile, critères à remplir par les offres, principaux points d'évaluation, critères d'évaluation) et pouvoir expliquer l'utilité des divers éléments pour un soumissionnaire.
	4.2	Connaître les prescriptions légales et les directives de l'entreprise pour les appels d'offres publics ou privés et pouvoir expliquer leur but (p. ex. concurrence, égalité des chances, prévention de la corruption).

Connaissances opérationnelles nécessaires

5	5.1	Connaître les exigences de base auxquelles doivent satisfaire les documents d'évaluation (p. ex. objectivité, clarté, transparence, aide à la décision).
	5.2	Connaître les différentes méthodes d'évaluation pour comparer des offres (p. ex. pondération par paire de facteurs, matrice préférentielle, analyse de la valeur utile, méthode de classement hiérarchique) et pouvoir expliquer leur adéquation, leurs avantages et leurs inconvénients.
6	6.1	Connaître les exigences de base auxquelles les prestataires et les fournisseurs doivent satisfaire (p. ex. compétences, projets de référence, disponibilité, certifications, respect des normes, contrats ou coopérations existants) et pouvoir les expliquer dans le contexte de l'acquisition prévue.
	6.2	Connaître différentes sources pour collecter des informations sur les prestataires (p. ex. recherche documentaire dans différents médias, salons professionnels, projets de référence, sondage auprès des prestataires) et pouvoir expliquer leur adéquation, leurs avantages et leurs inconvénients.
7	7.1	Connaître les critères typiques de la présélection des offres (p. ex. exhaustivité, respect de tous les critères d'exclusion, degré de réalisation des critères principaux, respect du budget).
8	8.1	Connaître des techniques et des représentations appropriées pour synthétiser les résultats de la comparaison des offres (p. ex. histogramme, diagramme de corrélation, analyse des tendances, tables).
	8.2	Connaître les contenus fondamentaux d'un sommaire de gestion [Management Summary] (p. ex. contexte, raison et portée de la décision à prendre, objectifs, options d'action possibles, évaluation des options, recommandation avec motivation) et pouvoir expliquer leur contribution à la prise de décision.

Version du module	1.0
Créé le	11.02.2021

Identification du module

Numéro de module	690	
Titre	Planifier, conduire et superviser des projets	
Compétence	Structurer et planifier un projet conformément au mandat de projet défini, conduire et superviser le projet pendant sa réalisation et informer périodiquement les décideurs sur l'avancement du projet.	
Objectifs opérationnels	1	Analyser et vérifier conjointement avec le mandant le mandat de projet et définir une procédure appropriée ainsi que l'organisation du projet.
	2	Structurer les prestations exigées selon le mandat de projet en sous-projets et lots de travaux et définir leurs objectifs en termes de contenu, de qualité et de délai.
	3	Planifier la réalisation du projet sur la base des ressources définies.
	4	Identifier les parties prenantes déterminantes internes et externes du projet et assurer la communication du projet pendant sa réalisation.
	5	Connaître les responsables appropriés pour des sous-projets et des lots de travaux et attribuer des mandats de travail.
	6	Assurer, sur la base des directives de l'entreprise, la gestion du changement pendant la réalisation du projet.
	7	Identifier et analyser les risques du projet en continu et proposer aux décideurs des mesures pour les traiter.
	8	Surveiller l'avancement du projet en continu et proposer aux décideurs des mesures de pilotage efficaces en cas d'écarts.
	9	Etablir des rapports périodiques sur l'avancement du projet et les présenter aux décideurs compétents.
Domaine de compétence	Project Management	
Objet	Projets de complexité moyenne assortis d'objectifs et de ressources prédéfinis (phase d'initialisation terminée, mandat de projet existant).	
Version du module	1.0	
Créé le	11.02.2021	

Connaissances opérationnelles nécessaires

Les connaissances opérationnelles nécessaires décrivent les savoirs qui contribuent à l'exécution compétente des actions d'un module. La définition de ces connaissances est fournie à titre indicatif et n'est pas exhaustive. La concrétisation des objectifs de formation et la définition du chemin d'apprentissage en vue d'acquérir ces compétences incombent aux prestataires de formation.

Numéro de module		690
Titre		Planifier, conduire et superviser des projets
Compétence		Structurer et planifier un projet conformément au mandat de projet défini, conduire et superviser le projet pendant sa réalisation et informer périodiquement les décideurs sur l'avancement du projet.
Objectifs opérationnels et connaissances opérationnelles nécessaires		
1	1.1	Connaître les caractéristiques typiques d'un projet (p. ex. ressources limitées, objectifs fixés, forme d'organisation spécifique, nouveauté concernant le contenu) et pouvoir expliquer les différences entre un projet et les tâches courantes.
	1.2	Connaître des modèles de procédures séquentielles et itératives pour des projets (p. ex. modèle en cascade [waterfall], cycle en V, méthode RUP, méthode HERMES) et pouvoir expliquer leurs caractéristiques (p. ex. phases, rôles, livrables) et ce qui les différencie.
	1.3	Connaître des modèles de procédures agiles pour des projets (p. ex. Scrum, Kanban, XP, DAD, SAFe) et pouvoir expliquer leurs caractéristiques typiques (p. ex. principes agiles, itérations/sprints, rôles) et ce qui les différencie.
	1.4	Connaître différentes formes d'organisation des projets (p. ex. organisation de projet pure, task force, organisation hiérarchique avec état-major, organisation hiérarchique, organisation matricielle) et pouvoir expliquer leurs caractéristiques et ce qui les différencie.
	1.5	Connaître les principaux facteurs déterminants pour le choix de la procédure et de la forme d'organisation des projets (p. ex. directives du mandant, taille du projet, complexité, standards de la branche).
2	2.1	Connaître le but d'une structure de découpage du projet (SDP) et différentes possibilités de classifier les sous-tâches dans la SDP (p. ex. fonction, objet du projet, calendrier).
	2.2	Connaître les principaux éléments pour la définition de lots de travaux (p. ex. objectifs de résultats et livrables, estimation des coûts et du travail nécessaire, informations sur les délais, exigences en matière de ressources en personnel) et pouvoir en expliquer l'importance pour la planification et la supervision de projets.
	2.3	Connaître le but des carnets (backlogs), de la définition du fini (Definition of Done; DoD), des épopées (epics), fonctionnalités, récits utilisateurs (user stories) et tâches dans les projets agiles et pouvoir en expliquer les différences en termes de granularité et d'exactitude.
3	3.1	Connaître des méthodes et des techniques de planification de projets séquentiels et itératifs (p. ex. diagramme de Gantt, plan de réseau).
	3.2	Connaître les cérémonies dans la planification de projets agiles (p. ex. planification des versions dans le carnet de produit [product backlog], planification du sprint dans le carnet de sprint [sprint backlog], revue de sprint [sprint

Connaissances opérationnelles nécessaires

		review], rétrospective de sprint [sprint retrospective], mêlée quotidienne [daily scrum]).
4	4.1	Connaître les parties prenantes déterminantes internes et externes ainsi que leurs rôles dans le cadre d'un projet (p. ex. mandant, direction du projet, comité du projet ou comité de pilotage, équipe du projet, propriétaire du produit [product owner], maître de mêlée [scrum master]) et pouvoir expliquer leurs besoins en informations spécifiques.
	4.2	Connaître des méthodes et des techniques appropriées pour gérer les parties prenantes dans le cadre d'un projet (p. ex. liste des parties prenantes, cartographie des parties prenantes, analyse du champ de force, réunion des 3 amigos).
	4.3	Connaître les contenus d'un plan de communication d'un projet comprenant des mesures de communication (p. ex. cercle des destinataires, but, canal ou média, responsabilité, délai, planification, revues).
5	5.1	Connaître les critères de délai, qualitatifs, écologiques et économiques pertinents pour l'attribution de sous-projets.
	5.2	Connaître les principaux contenus d'un mandat de sous-projet et pouvoir expliquer les prescriptions légales et spécifiques à l'entreprise déterminantes pour l'attribution.
	5.3	Connaître les principaux facteurs d'influence lors du choix des ressources en personnel pour les projets (p. ex. disponibilité, qualification, charge de travail).
	5.4	Connaître les exigences fondamentales à remplir par un mandat de travail ciblé et adapté à son destinataire (p. ex. cohérence, délimitation, adéquation avec les objectifs du projet) et pouvoir citer les contenus d'un mandat de travail complet (p. ex. tâches, livrables, exigences de qualité, délais à tenir, conditions cadres).
6	6.1	Connaître le processus et les directives de l'entreprise relatives à la gestion du changement et pouvoir expliquer leur importance pour le projet.
	6.2	Connaître les raisons typiques des changements dans un projet (p. ex. modification des objectifs, de l'étendue, des exigences, des conditions cadres).
	6.3	Connaître les principaux contenus d'une demande de modification (change request) (p. ex. description de la modification, raison et motivation, estimation des coûts, priorité).
	6.4	Connaître l'influence des modifications sur la documentation du projet.
7	7.1	Connaître les causes typiques des risques dans les projets (p. ex. conflits d'intérêts, ressources temporelles et personnelles, charges supplémentaires, environnement du projet, facteurs psycho-sociaux).
	7.2	Connaître des méthodes et des techniques d'évaluation et de représentation des risques appropriées (p. ex. matrice des risques, cartographie des risques).
	7.3	Connaître les différentes options d'actions pour traiter les risques (réduction, refus/évitement, acceptation/maintien, externalisation) et pouvoir en expliquer les caractéristiques.
8	8.1	Connaître des instruments appropriés pour suivre l'avancement du projet en continu (p. ex. rapports de situation, système de signalisation, rapports, revues, messages sur l'état d'avancement).
	8.2	Connaître des méthodes et des instruments appropriés pour surveiller l'avancement du projet (p. ex. planification des jalons, analyse de tendance des jalons, comparaison état actuel/visé, analyse de la valeur acquise [ear-

Connaissances opérationnelles nécessaires

		ned value analyse], analyse de tendance des coûts, graphiques d'avancement [burndown charts]).
	8.3	Connaître les accords contractuels typiques servant à contrôler l'avancement des projets agiles avec un budget ainsi que des délais et des cycles itératifs fixes (p. ex. points de contrôle, critères d'acceptation, modèle de partage du risque entre le client et le fournisseur, bonus d'efficience, critères de sortie [exits]).
	8.4	Connaître les paramètres du triangle magique et du carré diabolique et pouvoir expliquer l'importance de ces modèles pour l'élaboration de mesures de pilotage en cas d'écarts.
9	9.1	Connaître les caractéristiques et les contenus d'un rapport sur l'avancement du projet (p. ex. état du projet, degré d'atteinte des objectifs en termes de coûts, de délais et de but concret, analyse du risque, propositions, planification).
	9.2	Connaître les contenus et la structure d'une présentation de l'état du projet et pouvoir expliquer en quoi ses propres compétences en termes d'expression et de comportement influencent le travail de persuasion.

Version du module	1.0
Créé le	11.02.2021