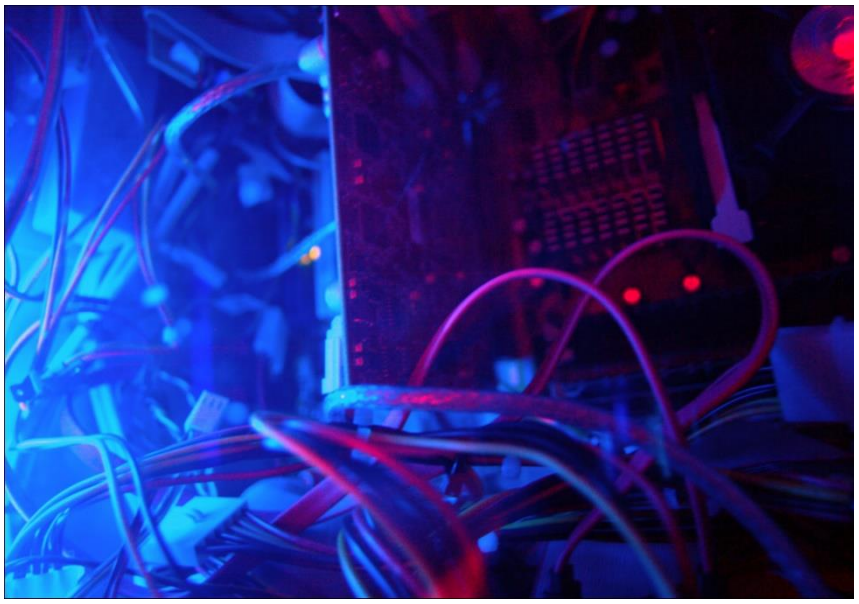
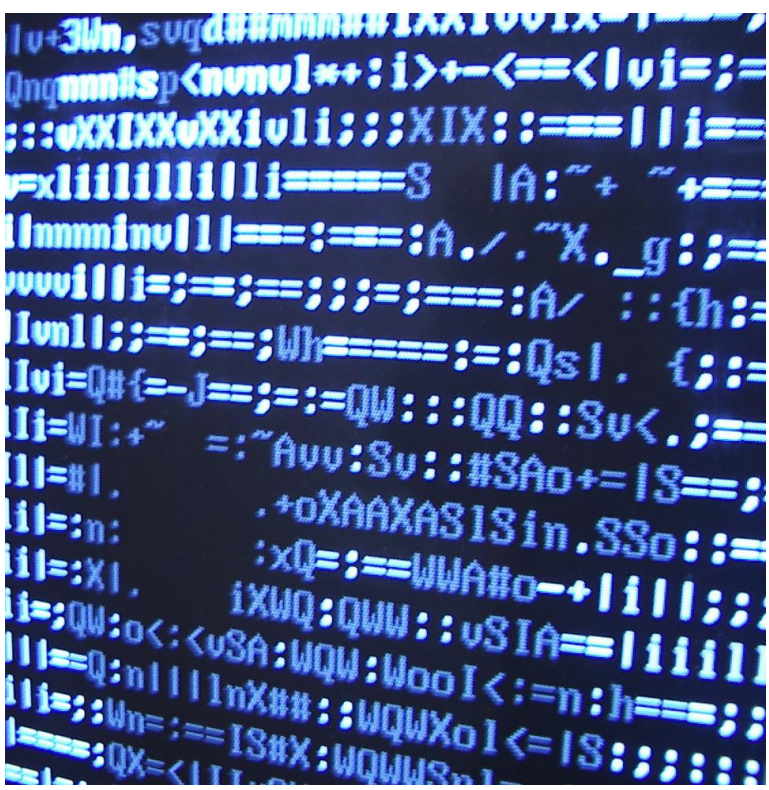


Cyber Security Specialist
avec brevet fédéral

ISEIG
Institut Suisse d'Enseignement de l'Informatique de Gestion



ISEIG - Institut Suisse d'Enseignement de l'Informatique de Gestion
Avenue des Boveresses 52, CH - 1010 Lausanne
Tél. +41 (0)21 654 40 60, E-mail : info@iseig.ch, URL : www.iseig.ch

Cyber Security Specialist

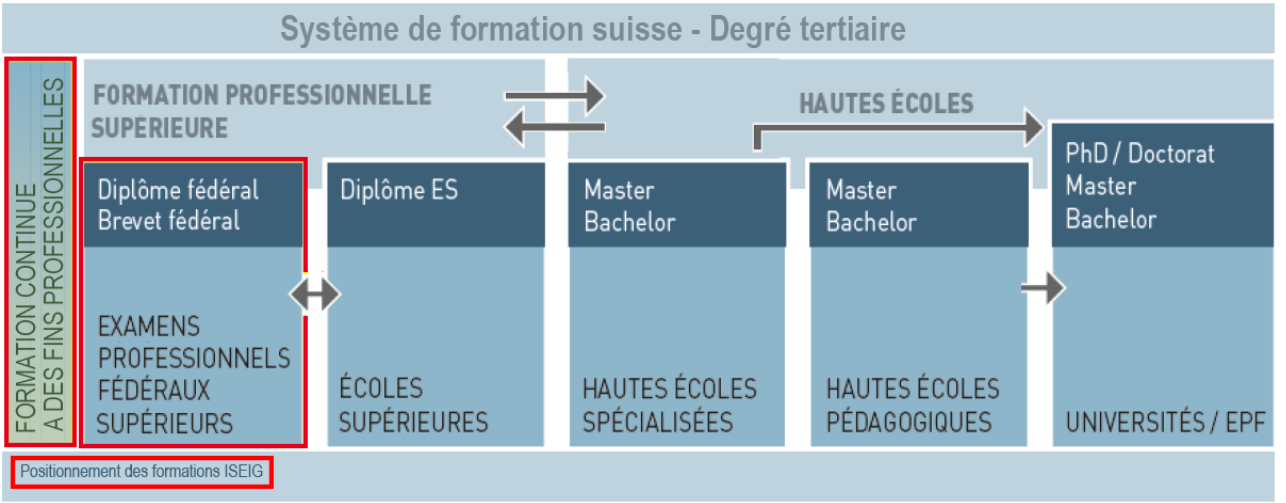
avec brevet fédéral

Introduction

Les principales tâches du Cyber Security Specialist 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. Il constitue une main-d'œuvre hautement spécialisée opérant dans le domaine de la cybersécurité. Il travaille généralement au sein de moyennes ou grandes entreprises privées ou dans des institutions publiques.

Le Cyber Security Specialist peut diriger de petites équipes constituées de professionnels chargés de l'exploitation opérationnelle. Il peut être engagé dans des projets spécifiques liés à la sécurité. Dans le cadre de projets, il endosse la responsabilité pour des lots de travaux individuels ou des sous-projets.

Les exigences de l'examen pour l'obtention du titre « Cyber Security Specialist » avec brevet fédéral sont définies par « ICT-Formation professionnelle Suisse », l'organisation nationale du travail (OrTra) pour les métiers de l'informatique (www.ict-formationprofessionnelle.ch), en collaboration avec l'Unité de pilotage informatique de la Confédération (UPIC) et des représentants de l'économie. « ICT-Formation professionnelle Suisse » est également responsable de la définition et de l'organisation des examens.



Le **Cyber Security Specialist est positionné au niveau 6 du CNC – Cadre National de Certification** qui comprend 8 niveaux.

Le brevet fédéral est le 1er diplôme de la formation professionnelle supérieure. Il s'agit de formation continue qui permet l'obtention d'une reconnaissance officielle des connaissances et compétences sans recommencer une longue formation de base déjà acquise. Il peut être complété par le diplôme fédéral de ICT Security Expert qui est le plus haut diplôme de la formation professionnelle supérieure. Le diplôme fédéral permet à son tour d'accéder aux études HES ou universités en vue de l'obtention d'un MAS (Master of Advanced Studies), d'un CAS (Certificate of Advanced Studies) ou d'un MBA (Master of Business Administration).

Pour qui

La filière du brevet fédéral de Cyber Security Specialist s'adresse à des informaticien(ne)s spécialisé(e)s[1] dans la protection préventive des systèmes d'information et de communication contre les attaques dans le cyberespace et en la gestion réactive des incidents de sécurité.

Compétences opérationnelles principales

Le Cyber Security Specialist est en mesure d'effectuer les missions suivantes :

- **Protection préventive des systèmes**
  - suivre en continu l'évolution des menaces
  - analyser les menaces et traiter les informations
  - détecter les vulnérabilités
  - remédier aux vulnérabilités
  - utiliser des procédures de leurre
  - donner des conseils techniques aux parties prenantes
  - former les parties prenantes
- **Détection des incidents de sécurité**
  - surveiller les systèmes en exploitation
  - analyser et interpréter les données
  - trier les incidents de sécurité
  - documenter les incidents de sécurité
  - surveiller le traitement d'un incident de sécurité
- **Maîtrise des incidents de sécurité**
  - mettre en oeuvre des mesures immédiates
  - assurer la conservation des preuves
  - analyser les causes et les répercussions
  - définir et mettre en oeuvre des mesures de protection
  - soutenir la restauration des systèmes
- **Planification et mise en oeuvre des solutions de sécurité**
  - délimiter les systèmes et spécifier les exigences
  - vérifier la faisabilité et l'efficacité
  - déterminer l'investissement en ressources et le budgéter
  - procéder à une évaluation
  - mettre en oeuvre un projet
  - diriger une équipe

[1] Afin de faciliter la lecture, par la suite, seul le masculin est utilisé pour désigner les deux genres.

Exercice de la profession

La cybersécurité constitue un domaine d'activités spécifique de la gestion des technologies de l'information et de la communication (ICT). L'intégration de la cybersécurité dans l'organisation fonctionnelle et structurelle d'une entreprise ou d'une administration varie en fonction de la taille et de l'orientation de celle-ci. En règle générale, le Cyber Security Specialist collabore 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 du Cyber Security Specialist.

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 résistance au stress, une aisance à communiquer et un très bon esprit d'équipe sans oublier discrétion, intégrité et persévérance.

Plan de formation et compétences à acquérir

Le programme de la formation se base sur les modules suivants :

- **Gestion des services ICT**
  - 682 - **Gérer les incidents de sécurité**
    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.
  - 685 - **Assurer la gestion des vulnérabilités et des correctifs**
    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.
  - 686 - **Fournir des conseils techniques aux clients et les former**
    Fournir aux clients internes ou externes des conseils techniques orientés besoins et solutions, planifier et dispenser des formations adaptées aux groupes cibles.
- **Gestion des systèmes**
  - 681 - **Détecter et contrer les attaques ciblant l'infrastructure informatique**
    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.
- **Sécurité ICT**
  - 679 - **Collecter des informations sur les menaces et les traiter**
    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.
  - 680 - **Contrôler la sécurité de l'infrastructure informatique**
    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.

- 683 - **Analyser et interpréter des ensembles de données**
  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.
- 684 - **Procéder à une investigation numérique des systèmes**
  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.

- **Gestion de projet ICT**
  - 674 - **Diriger et soutenir une équipe**
    Diriger et soutenir une équipe sur le plan professionnel et social en adoptant un comportement de conduite et de communication adapté à la situation.
  - 690 - **Planifier, conduire et superviser des projets**
    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.
- **Ingénierie des procédures**
  - 687 - **Délimiter les systèmes et spécifier les exigences**
    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. Analyse d'exigences pour le développement, l'exploitation ou la maintenance de systèmes, processus et services techniques et organisationnels.
  - 689 - **Évaluer des solutions informatiques**
    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.
- **Economie d'entreprise**
  - 688 - **Déterminer les ressources à allouer à des projets ICT et les budgéter**
    Déterminer les coûts d'un projet ICT, établir une planification des coûts et un budget et contrôler les coûts pendant la réalisation.

Conditions d'admission aux examens

Est admis à l'examen final, celui qui remplit 1 des 4 conditions suivantes :

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

- peut attester d'au moins six ans de pratique professionnelle dans le domaine des technologies de l'information et de la communication (TIC), dont au moins deux ans dans le domaine de la sécurité de l'information ou de la cybersécurité; **ou**
- a suivi avec succès la cyberformation au sein de l'armée et peut attester d'au moins une année de pratique professionnelle dans le domaine de la sécurité de l'information ou de la cybersécurité.

Prérequis professionnels recommandés pour la formation

En plus des conditions d'admission aux examens, les connaissances suivantes sont recommandées pour assimiler la matière de la formation :

- **Anglais technique** écrit : le matériel pédagogique étant majoritairement en anglais et une partie des examens formulée en anglais.
- **Gestion des systèmes**
  - solides connaissances de l'architecture des systèmes d'exploitation courants d'appareils fixes ou mobiles (p. ex. gestion des processus, des ressources et des utilisateurs)
  - expérience pratique dans l'administration des systèmes Windows et Linux
  - bonnes connaissances de la programmation shell (ligne de commande)
  - solides connaissances des différents supports de stockage et des systèmes de fichiers
  - solides connaissances des technologies Microsoft que sont les annuaires actifs (Azure, Federation)
  - solides connaissances des protocoles et services DHCP, DNS, VPN, IPSec, HTTP, HTTPS
- **Gestion des réseaux**
  - solides connaissances des normes 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)
  - solides connaissances des protocoles d'application usuels dans les réseaux TCP/IP (p. ex. HTTP, protocoles de messagerie électronique, DHCP, DNS, services d'annuaires, protocoles de transfert des données)
  - solides connaissances des protocoles de réseau et de transport usuels pour le cryptage (p. ex. IPSec, TLS)
  - solides connaissances 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])
  - expérience pratique dans l'enregistrement et l'analyse du trafic réseau
- **Sécurité ICT**
  - connaissances des procédures cryptographiques courantes pour le chiffrement des données
  - connaissances de base dans les domaines de la sécurité des systèmes, des réseaux et des applications (par ex. menaces et risques courants, solutions de protection répandues telles que scanners de virus, pare-feu, WAF)

- connaissances de l'encodage, du décodage, de la transformation de données, par ex. conversion hexadécimale, binaire, base64, et de transformations similaires

- **Ingénierie d'applications et gestion de données**
  - connaissances de base d'au moins un langage de script et/ou de programmation
  - connaissances des concepts fondamentaux de bases de données

Titre obtenu

Le diplôme est délivré par le SEFRI - Secrétariat d'Etat à la formation, à la recherche et à l'innovation.

La ou le titulaire du diplôme fédéral est autorisé(e) à porter le titre protégé de :

- **Cyber Security Specialist avec brevet fédéral**
- Cyber Security Specialist mit eidgenössischem Fachausweis
- Cyber Security Specialist con brevetto federale.

La traduction anglaise recommandée est :

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

Confédération suisse

BREVET

Leonhard EULER

né le 20 janvier 1985, originaire de Fribourg

a prouvé qu'il satisfait aux exigences requises pour l'obtention du diplôme en vertu de la loi du 13 décembre 2002 sur la formation professionnelle et conformément au règlement du 1 mars 2012 approuvé par le Département fédéral de l'économie.

Le présent diplôme autorise le titulaire à porter la dénomination légalement protégée de

ICT Cyber Security Specialist

Berne, le 24 novembre 2019

Secrétariat d'Etat à la formation, à la recherche et à l'innovation

La directrice

Pour l'organe responsable de l'examen

Le président de la Commission d'examen

Spécimen

Et la suite ...

Le brevet fédéral est le premier diplôme de la formation professionnelle supérieure. Il est suivi par le diplôme fédéral qui est le plus haut diplôme de la formation professionnelle supérieure. Il s'agit de formation continue qui permet l'obtention d'une reconnaissance officielle des connaissances et compétences sans recommencer une longue formation de base déjà acquise. Les 2 filières du diplôme fédéral sont :

- ICT Security Expert diplômé
- ICT-Manager diplômé

Pour plus d'informations : www.iseig.ch .

Durée et prix

Dates	Formation	Durée	Prix	Prix/j
Voir détail sur www.iseig.ch	Cyber Security Specialist avec brevet fédéral **Prix avec le subventionnement CHF 7'500.- ou CHF 3'750.-, soit CHF 150.- ou 75.- par jour**	50 jours	15'000.-*	300.-*

selon conditions générales. Le prix comprend toute la doc. distribuée.

* Le prix du cours n'inclut pas la taxe d'examens de CHF 3'200.- (tarif 2021), non soumis à la TVA, montant facturé par ICT-FP Suisse.

Les cours se déroulent en journée de 09:00 à 12:00 et 13:00 à 16:30

Subventions jusqu'à CHF 11'250.- avec la subvention de la Confédération de CHF 7'500.- et, dans le canton de Vaud, la subvention de la fondation FONPRO de CHF 3'750.- pour la formation et 3'000.- pour l'examen.

Modalités de paiement : sur demande, le paiement de la formation peut être réglé par acomptes.

Cinq bonnes raisons :

- **de se perfectionner à l'ISEIG et**
- **de profiter de plus de 30 ans d'expérience ...**

... vos avantages :

1. Restez compétitif et toujours au top

- Vous apprendrez des contenus basés sur les meilleures pratiques développées par des experts au niveau international. Les méthodes et techniques sont éprouvées et évoluent constamment pour répondre aux besoins en constante évolution. Par vos nouvelles connaissances et compétences, vous vous différencierez sur le marché et serez plus attractif.

2. Garantissez votre investissement formation

- La majorité des formations aboutissent à des certifications qui prouvent vos acquis à votre employeur, partenaires et clients. Vous vous différenciez ainsi positivement et restez attractif sur le marché du travail.
- Votre réussite est optimisée par notre soutien. Si vous considérez que la matière n'a pas été assimilée, nous vous offrons généralement la possibilité de refaire gratuitement tout ou partie de la formation dans les 6 mois, dans une session organisée. Vous ne payerez que les éventuels nouveaux documents pédagogiques ou taxes d'examen. Le reste est à notre charge.

3. Gagnez de l'argent

- Vos nouvelles compétences vous permettront d'être plus productif et d'obtenir une promotion.
- ISEIG, fondation à but non lucratif, offre des formations au meilleur prix. Pour un montant donné, vous obtenez plus.
- Investissez sur vos compétences pour assurer votre rendement, il ne s'agit pas d'une loterie au gain des plus illusoires.

4. Gagnez du temps

- Mettez immédiatement en pratique vos nouvelles compétences. Les ateliers pratiques basés sur des cas réels assurent un transfert de connaissances aisé et l'utilisation des acquis dans votre environnement professionnel.

5. Evitez les mauvaises surprises

- Tout est inclus dans le prix de la formation : supports pédagogiques, énoncés de travaux pratiques avec corrigés, examens à blanc avec corrigés.
- Vous choisissez votre formation sur la base de programmes d'actualité clairement définis.