



Bridging the Gap 8th session

2800 DT

HT / personne*

Session de Préparation Approfondie à la Certification CISSP®

Du 06 au 10 Mai 2013

Le Formateur



L'animateur, **Hafedh BEN HAMIDA**, Tunisien résident en France, ingénieur certifié CISSP®, est Expert Senior en sécurité des systèmes d'information. Il a plus de 10 ans d'expérience en conseil stratégique, tactique et opérationnel en sécurité pour des grands groupes et de nombreuses PME/PMI. Outre son activité de développement de l'offre et de management des équipes, l'instructeur a effectué et dirigé des missions de gouvernance de sécurité, d'analyses et de gestion des risques, de définition de politique de sécurité, d'intégration de la sécurité dans les grands projets et d'organisation de la fonction sécurité. Il a animé de nombreux séminaires et formations de haut niveau dans le domaine de la sécurité et des réseaux à l'échelle internationale (France, Tunisie, KSA, Algérie, HongKong, Maroc, Vietnam, Soudan, Chine, Canada...etc). Il est titulaire d'un diplôme de Mastère en Sécurité des systèmes d'information et est le **Premier Tunisien**, certifié CEH et CHFI. Il est, par ailleurs, Expert Auditeur certifié de l'Agence Nationale de la Sécurité Informatique (ANSI), certifié MSCE 2003 Security, LPIC-1, CCNA, ISO/IEC 27001 accrédité IRCA, ITIL et CompTIA Security+.

Objectifs de la Formation

L'international Information Systems Security Certification Consortium – l'(ISC)²[®] a développé la certification CISSP[®], certification internationale reconnue mondialement par les experts sécurité, dans le but de valider les connaissances des experts et d'assurer qu'ils continuent leur formation. L'(ISC)²[®] définit un tronc commun de connaissances en sécurité (CBK = Common Body of Knowledge) qui représente les savoirs spécifiques que tous les professionnels du domaine ont en commun et qu'ils utilisent couramment dans l'exercice de leurs tâches. La certification CISSP[®] permet d'étalonner son niveau de compétences tant au niveau des connaissances techniques qu'au niveau analyse des risques et audit des systèmes dans une optique gouvernance des systèmes d'informations. Ainsi, cette formation permettra aux participants de :

- Approfondir les domaines de la sécurité déjà connus
- Acquérir des connaissances plus poussées dans des domaines moins connus
- Acquérir le vocabulaire commun relatif au CISSP[®]
- Mieux comprendre les questions de l'examen
- Discuter des meilleures pratiques avec vos collègues
- Acquérir des aptitudes en gestion de la sécurité et des risques
- Développer une vision globale et pas seulement technologique des besoins en sécurité de l'entreprise

Pré-requis

Il est recommandé d'avoir une expérience en administration de systèmes, une bonne compréhension des systèmes d'exploitation (*Unix, Linux* ou *Windows*) et d'avoir des notions des concepts de base de la sécurité de l'information.

Public visé

Cette formation s'adresse aux administrateurs de réseaux, consultants, conseillers en gouvernance, gestionnaires, responsable de la protection des actifs informationnels et tout autre professionnel dont le développement de carrière nécessite la certification CISSP[®].

Informations Générales sur la Formation

- La formation est donnée en français
- 3 supports de cours en anglais (langue recommandée pour le passage de l'examen) seront remis à chaque participant
- Chaque session est limitée à un maximum de **12 personnes**

Programme détaillé de la Formation (5 jours)

Chapitre 1

Gouvernance de la Sécurité de l'information et Gestion des Risques

- Gestion de la Sécurité
- Administration de la Sécurité et Contrôles associés
- Modèle de Sécurité Organisationnel
- Gestion des Risques informationnels
- Analyse des Risques
- Politique, Standards, Baselines, Guides et Procédures
- Classification des Informations
- Niveaux de Responsabilités
- Formation de Sensibilisation en Sécurité Informatique
- Conclusion

Chapitre 2

Contrôle des Accès

- Introduction sur le Contrôle des Accès
- Piliers de la Sécurité
- Identification, Authentification, Autorisation et Journalisation
- Modèles de Contrôle d'Accès
- Technologies et Techniques de Contrôle d'Accès
- Administration de Contrôle d'Accès
- Méthodes de Contrôles d'Accès
- Types de Contrôles des Accès
- Journalisation
- Pratiques des Contrôles d'Accès
- Monitoring
- Quelques Menaces
- Conclusion

Chapitre 3

Architecture de Sécurité et Conception

- Architecture des Ordinateurs
- Architecture des Systèmes
- Modèles de Sécurité
- Modes des Opérations de la Sécurité
- Méthodes d'Evaluation des Systèmes
- Le Livre Orange et les Livres d'Arc-en-ciel
- Critères d'Evaluation de la Sécurité
- Les Critères Communs
- Certification et Accréditation
- Systèmes Ouverts et Systèmes Fermés
- Architecture des Entreprises
- Quelques Menaces

Chapitre 4

Sécurité Physique et Environnementale

- Introduction à la Sécurité Physique
- Le Processus de Planification
- Protection des Biens
- Sécurité Frontalière
- Conclusion

Chapitre 5

Sécurité des Réseaux et des Télécommunications

- Le Modèle OSI
- TCP/IP
- Types de Transmission
- Réseaux LAN
- Protocoles de Routage
- Périphériques Réseaux
- Protocoles et Services Réseaux
- Intranet et Extranet
- MAN et WAN
- Accès distants
- Les réseaux Sans Fil
- Rootkits
- Conclusion

Chapitre 6

Cryptographie

- Histoire de la Cryptographie
- Concepts et Définition de la Cryptographie
- Implication des Gouvernements dans la Cryptographie
- Types d'Algorithmes Cryptographiques
- Méthodes de Cryptage
- Différents Types des Systèmes Symétriques
- Différents Types des Systèmes Asymétriques
- Intégrité des Messages
- PKI
- Gestion des Clés
- Cryptage des Liens et Cryptage de Bout-en-Bout
- Les Standards d'Emails
- Sécurité Internet
- Attaques Cryptographiques
- Conclusion

Chapitre 7

Continuité des Services et Reprise après Désastre

- Introduction aux BCP/DRP
- Exigences de la Planification
- BIA
- Les Backups
- Le CyberInsurance
- Les Tests et les Révisions des Plans
- Conclusion

Chapitre 8

Lois, Régulations, Conformité et Investigations

- Problématiques des Lois Cybernétiques
- Complexité des Crimes Cybernétiques
- La Propriété Intellectuelle
- Les Informations à Caractère Personnel
- Investigations Cybercriminelles
- La Collecte des Preuves
- Ethiques
- Conclusion

Chapitre 9

Développement de Logiciels Sécurisés

- Importance de la Sécurité des Applications
- Complexité des Fonctionnalités
- Implémentation
- Gestion des Bases des Données
- SDLC
- Méthodologies de Développement des Applications
- Informatique distribuée
- Systèmes Experts
- ANN
- Sécurité WEB
- Code Mobile
- Gestion des Patches
- Conclusion

Chapitre 10

Sécurité des Opérations

- Rôle du Département des Opérations
- Gestion Administrative
- Les Niveaux d'Assurance
- Les Responsabilités Opérationnelles
- La Gestion des Configurations
- Contrôle des Supports de Stockage
- Fuite des Informations
- Disponibilité des Ressources et des Réseaux
- Les Mainframes
- Sécurité des Emails
- Tests de Vulnérabilités
- Conclusion

Chapitre 11

Préparation à l'Examen CISSP®

- Examen Blanc

CISSP® is a registered trademark of (ISC)²®
Our classes are not endorsed, sponsored or delivered by (ISC)²®.

Disclaimer:

CISSP® is a registered trademark of (ISC)²® Inc (International Information Systems Security Certification Consortium) Inc. The materials have been developed specifically for this session and are not endorsed, sponsored or delivered by (ISC)²®. The goal of the course is to prepare security professionals for the CISSP® exam by covering the ten domains defined by (ISC)²®.

Quelques Témoignages Post-Formation

« La préparation que le formateur nous a donné ma beaucoup aidé et je pense qu'elle ma permis de bien comprendre tous les domaines abordés dans la CISSP. Je pense que cette préparation m'a aussi permis de me mettre plus en confiance pour l'examen et de le réussir »

Mr. Alexis Ravel, France

« I followed the CISSP training with Mr. Ben Hamida in June 2009. Hafedh taught us the Common Body of Knowledge with a great sense of pedagogy and a contagious enthusiasm thanks to his leadership and his incredible knowledge and experience in the security area!

As a great coach, he helped us focusing on the key aspects of the training in order to get certified and the key factors of success to become a CISSP as well. He trained us, not only technical knowledge but also, psychological and physical conditions to pass this difficult exam. »

Mr. Nicolas ROUSSET, France

« J'ai suivi avec Mr. BEN HAMIDA une formation CISSP. J'ai trouvé la formation très complète et aussi j'ai acquis un savoir-faire très riche. Cette formation m'a été très utile dans le cadre de mon poste de Responsable sécurité informatique. J'ai particulièrement apprécié le professionnalisme et la disponibilité du formateur et aussi son expérience. Je vous le recommande pour son sérieux et son efficacité »

Mr. Anis GHARBI, Tunisia

« J'ai beaucoup apprécié la préparation CISSP avec un énorme travail de synthèse des points importants des deux ouvrages de références CISSP, permettant de traiter efficacement tout le périmètre des 10 CBK et de faire gagner beaucoup de temps de révision.

Le petit groupe a permit beaucoup d'interactivité et d'échanges et, malgré un programme très dense, nous avons réussi à tout traiter dans une bonne ambiance »

Mr. Julien STENO, France

« Le volume d'informations à intégrer lors de la formation CISSP est grandement facilité par le travail en amont du formateur (support de cours au top!). Les explications sont claires et le formateur n'hésites pas à revenir sur les points qui pourraient éventuellement laisser quelques personnes sur le bord du chemin et ceci malgré l'emploi du temps séré.

J'ai apprécié la pédagogie du formateur, son enthousiasme, sa sympathie et sa passion pour la sécurité. C'était une super semaine! Merci »

Mr. Jean-Yann RIVIERE, France

« Cela était un grand privilège pour moi d'avoir assisté à la formation CISSP organisée au MAROC.

C'est une formation très consistante et très variée qui englobe de manière générale tout ce qui est relatif à la sécurité. Assister à la formation m'a été d'un grand secours pour pouvoir assimiler plus facilement les 10 modules CBK et préparer plus aisément le test de certification CISSP. Les modules sont assez volumineux et riches d'informations et de vocabulaires »

Mr. Yahya LAKLALECH, Morocco

« I attended Hafedh's CISSP training with the hope to get the best preparation in the shortest time, and wasn't disappointed!! His great security expertise and knowledge, and the comprehensive way he delivers it to its students was really what one would expect for this kind of bootcamp.

If you want to quickly get the CISSP cert, I would definitely recommend Hafedh as a trainer »

Mr. Sami GHOURABI, Tunisia

« Hafedh was a great teacher during my CISSP study. He is very involved in his missions and has a huge knowledge & experience in Security. It is a pleasure to recommend him »

Mr. Emmanuel ORLANDO, France

« I know Hafedh since December 2009 when he leads a CISSP training course for the first time in Morocco. He is very pedagogical. He can transmit the right information to everyone in the group even if they don't have the same profiles. He also has the faculty to use all his skills and his talents (CISSP, ISO 27001, LA, CEH, Security+, etc.) to permit to the entire group to benefit from his experience. He's a very skilled person with a high capacity to lead people and gather them around the right goals. He has a prominent sense of organization and a valuable know-how. Available and easy to contact, he's a results oriented person too. He acts for long term projects and achieves his goals with determination and perseverance. Very high recommended »

Mr. Mohamed LAHLOU, Morocco

« Je suis très satisfait de la semaine de formation. Cela m'a permis de travailler très efficacement. Le groupe a été très stimulant.

Par ailleurs, pour garder le rythme acquis au cours de cette formation intense, je me suis d'emblée inscrit au test CISSP. À la fin de la formation, je fais le constat que, plonger seul dans les 10 CBK, le soir en rentrant à la maison, aurait très certainement été hors de portée pour moi »

Mr. Pierre MACHARD, France

Nous ont fait confiance au cours de nos précédentes sessions CISSP en **TUNISIE**



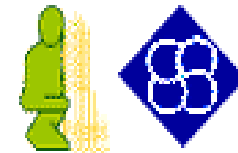
بنك تونس العربي الدولي
BANQUE INTERNATIONALE ARABE DE TUNISIE



بنك الأمان
AMEN BANK



TÜVRheinland®
Precisely Right.



Groupe Chimique Tunisien



إدارة الملكية العقارية
Conservation de la Propriété Foncière
Land Property Register



Société Tunisienne de l'Electricité et du Gaz

Le monde change, la STEG évolue

France: +33 (0) 6 48 62 71 01 / Fax: +33 (0) 1 70 24 77 12

Tunisie: +216 97 97 11 21 / Fax : +216 70 73 13 09

Page 9/13

Emails: hafedh.benhamida@gmail.com - bhafedh@iscsp.org - Web: <http://www.iscsp.org>



STONESOFT



Teleperformance

Nous ont fait confiance au cours de nos précédentes sessions CISSP à l'**International**





Demande d'inscription
à la formation de préparation à la certification CISSP®
du 06 au 10 Mai 2013
à remplir et renvoyer par email

M./Mme	Prénom Nom	Fonction	E-mail / GSM

Entreprise :

Adresse :

Code postal :

Ville :

Téléphone :

Fax :

Les frais d'inscription sont à **2800 DT** HT par personne*.

Soit pour un montant total de : DT / HT pour personne(s).

Montant total TTC (TVA 12%) : DT (TTC)

Tunis, le

Signature et Cachet

***Conditions générales d'inscription**

Votre inscription sera définitive après réception de ce formulaire dûment rempli ainsi que du règlement du montant total de la formation **au plus tard une semaine avant le début de la session**. Elle sera prise en compte dans la limite des places disponibles.

Pour discuter d'une offre de groupe ou pour plus d'amples détails sur la formation, merci de nous consulter par:

Email : bhhafedh@iscsp.org – hafedh.benhamida@gmail.com
Phone # : +33 6 48 62 71 01 - +216 97 97 11 21

Nous nous tenons à votre disposition pour toute information complémentaire.

Calcul des coûts:

Le prix inclue :

- La participation à la formation.
- Les supports de cours + 1 DVD par participant
- Les collations et déjeuners
- L'assistance téléphonique post-formation d'une durée de 3 mois.

Annulation de session:

Nous nous réservons le droit d'annuler une session lorsque le nombre de participants est insuffisant.

Annulation d'inscription:

Tout désistement devra nous être notifié au moins une semaine avant le début de la session (annulation avec remboursement sans frais). Au delà de ce délai, le montant prévu pour la session vous sera intégralement facturé.