HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Certification en sécurité

des individus

Hervé Schauer
<Herve.Schauer@hsc.fr>

Plan

- Certification des individus
  - Rôle
  - Obtention
  - Formation continue
  - Norme ISO17024
- CISM / CISA
- BS7799 Lead Auditor
- CEH / CHFI
- SCNP / SCNA
- OPSA / OPST / OPSE
- GIAC
- CISSP
- ProCSSI
- Autres certifications
- Conclusion
- Remerciements
- *Note : liste de certifications non-exhaustive*

Certification : rôle

- Un diplôme professionnel
- Titre décerné par un organisme privé
  - A caractère commercial ou associatif
  - Qui assure la promotion de la certification
  - Qui devient propriétaire et responsable d'une base de données très détaillée (avec CV) de tous les professionnels du secteur
- Permet de d'obtenir une reconnaissance de tiers
- Permet de démontrer une compétance, un acquis, un savoir-faire
- Participe à l'établissement de la confiance et aux choix entre clients et fournisseurs
- Etre certifié est un atout et deviendra un pré-requis

Certification : obtention

- Questionnaire à choix multiples (QCM)
- Dossier présenté par le candidat
- Travaux pratiques
- Rédaction de mémoire
- Soutenance
- Expérience professionnelle du candidat
- *Honoris causa*
- Maintien
  - Respect d'un code d'éthique
  - Repassage de l'examen
  - Poursuite dans le métier
  - Formation continue

Certification : formation continue

- Formation continue ou CPE (*Continuing Professional Education*) en anglais
- Obligatoire dans de nombreuses certifications pour le maintien de la certification
- Les formations dans le domaine concernés donnent droit à des points de CPE ou des heures de CPE
- Obtention de CPE variable suivant les certifications
  - Certaines conférences en sécurité délivrent également des certificats de CPE
  - Dans certains cas toute conférence en sécurité apportera des CPE
  - Dans certains cas donner des cours en sécurité apporte également des CPE

Certification : ISO17024

- ISO17024:2003 : Norme du processus de certification des individus
- *Awareness Training*
- *Accreditation of Certification Bodies for Certification of Persons*
- Egalement EN45013 en Europe
- Normes ISO1702x / EN450xx : normalisation des obligations dans l'accréditation des centres de certification
  - ISO17024/EN45013 pour les centres de certification des individus
- Impose la séparation de la formation et de la certification
- Certains schémas de certification sont propriétaires, d'autre conformes à la norme

CISM / CISA (1/3)

- CISM *: Certified Information Security Manager*, pour manager
- CISA : *Certified Information System Auditor*, pour auditeur
  - Auditeurs internes ou externes en informatique
- Editeur : ISACA (USA) : www.isaca.org
  - *Information Systems Audit and Control Association*
  - Chapitre de l'ISACA en France : AFAI : www.afai.asso.fr
  - Association à but non-lucratif
- Non-conformes à l'ISO17024
  - Formation et certification liées
- Création en 1978 du CISA, en 2003 du CISM

CISM / CISA (2/3)

- Environ 3000 CISM et 34000 auditeurs certifiés CISA
  - Dont environ 20000 CISSP ayant obtenu une équivalence du CISSP vers le CISA
- Examen
  - 500$
  - Une fois par an
  - CISM : Anglais, CISA : 11 langues
  - QCM de 200 questions en 4h
  - 8 ans d'expérience professionnelle dans la sécurité ou diplôme de niveau BAC+5
- Maintien
  - 20$ par an à l'ISACA
  - Minimum de crédit CPE de 20h par an et 120h sur 3 ans

CISM / CISA (3/3)

- Formation
  - Langue locale
  - AFAI (France) : 700 € pour 2 jours
  - APVCSI (Canada) : 475 $CAN pour 5 jours
  - Pas de sociétés de formation
- Modèle économique
  - Formation, examen et promotion réalisés par l'ISACA et ses affiliés, uniquement des structures associatives

BS7799 Lead Auditor (1/3)

- BS7799 Lead Auditor
- Mise en place de SMSI (Système de Management de la Sécurité de l'Information) et audit de sécurité
  - Application du modèle PDCA
- Editeur : BSI (UK), www.bsi.org.uk et www.bsi-global.com
  - Société privée
  - Etre l'agence de normalisation brittannique est juste une de ses activités
- Création fin années 90 ?
- Nombre de certifiés inconnu
- Certification non-conforme à l'ISO17024
  - Formation et certification liées

BS7799 Lead Auditor (2/3)

- Examen
  - Prix inclu dans le prix de la formation
  - Anglais
  - QCM + rédaction en 2h
- Pas de maintien

BS7799 Lead Auditor (3/3)

- Formation
  - A priori toujours réalisée par un formateur du BSI, même quand la formation est organisée par une société locale
  - Anglais
  - BSI
    - http://www.bsi-global.com/Training/Infosec/it04.xalter
  - Infoguard (Suisse)
    - 4500 CHF pour 5 jours (environ 3000 €)
    - http://www.infoguard.com/index.php?nav=5,56,111
- Modèle économique
  - Promotion, formation, examen et certification réalisés par le BSI

CEH / CHFI (1/4)

- Certified Ethical Hacker
  - 1- Certified ethical hacker
  - 2- Advanced hacking techniques
  - 3- Open Source Intrusion Detection Systems Training
- Computer Hacking Forensics Investigator
- Certifications à profil technique
- Editeur : EC-Council (USA) : www.eccouncil.org
  - International Council of E-Commerce Consultants
  - Non-profit organization/company
- Date de création inconnue
- Nombre de personnes certifiées non-publié

CEH / CHFI (2/4)

- Certification non-conforme à l'ISO17024, affirme suivre un schéma NIST antérieur et similaire
  - Mais liens privilégiés entre EC-Council et Mile2
- Examen CEH
  - 150 $ + suivi de la formation auprès d'une société agréée par EC-Council
  - 250 $ + 2 ans d'expérience à justifier sur dossier sans suivi de formation
  - En ligne, sous-traité à Prometric (www.prometric.com), à passer dans un centre de formation agréé
  - Anglais
    - Projets de traduction en français
  - 125 questions en 3h
    - http://www.eccouncil.org/312-50.htm

CEH / CHFI (3/4)

- Maintien
  - Respect du code d'éthique
  - Certification valable à vie
- Formation
  - Formateurs certifiés CEH + certification à confirmer
  - Support fourni par EC-Council
    - Information non-affichée chez EC-Council mais fournie par MILE2 qui argumente que leur laboratoire et leur expérience sont supérieurs à la concurrence
  - Travaux pratiques
  - Langue locale

CEH / CHFI (4/4)

- Formation (suite)
  - Sociétés de formation
    - MILE2 (USA, Australie, Israel, etc) : www.mile2.com
      - Plan du cours en 5 jours : http://www.mile2.com/certified_ethical_hacker_training_v3.html
    - Trainfargo (USA)
      - Cours CEH en 6 jours, 2300$: http://www.trainfargo.com/training/networking/enterprisehacking.htm
    - Vigilar (USA)
      - http://www.vigilar.com/services_ed1_habc.html
    - Axioma Technologies (Canada)
      - http://www.profex.qc.ca/axioma/
      - Cours CEH : 2700 CAN$ pour 5 jours
      - Cours CHFI : 2700 CAN$ pour 3 jours
- Modèle économique
  - Profit pour les sociétés de formation

SCNP / SCNA (1/6)

Security Certified Network Professional / Architect

- Certifications à profil techniques
  - Domaines couverts par le SCNP
    - Advanced TCP/IP
    - IPSec
    - Securing Linux Computers
    - Securing Windows Computers
    - Securing Routers and Access Control Lists
    - Contingency Planning
    - Security on the Internet and the World Wide Web
    - Attack Techniques
    - Network Defense Fundamentals
    - Designing Firewall Systems
    - Configuring Firewalls
    - Configuring VPNs
    - Designing an IDS
    - Configuring an IDS
    - Analyzing Intrusion Signatures
    - Performing a Risk Analysis
    - Creating a Security Policy

SCNP / SCNA (2/6)

Certifications à profil techniques (suite)

- Domaines couverts par le SCNA
  - Introduction to Trusted Networks
  - Cryptography and Data Security
  - Computer Forensics
  - Law and Legislation
  - Biometrics
  - Strong Authentication
  - Digital Certificates
  - Digital Signatures
  - Trusted Network Implementation
  - Plan and Design a Trusted Network
  - Microsoft Trusted Networks
  - Linux Trusted Networks
  - Managing Certificates
  - Local Resource Security
  - Wireless Security
  - Securing Email
  - Building Trusted Solutions

SCNP / SCNA (3/6)

- Editeur : Ascendant Learning (www.securitycertified.net)
  - Société privée (USA), nom commercial SecurityCertified
  - Fondée et dirigée par Uday O. Ali Pabrai
  - Financée par du capital-risque ?
    - Bluemoon ventures (pas de web)
  - La certification est vu comme tout autre produit commercial prêt-à-l'emploi
- Création en 2002
- Sans doute encore peu de certifiés SCNP
  - Examen SCNA ne semble pas encore ouvert
- Certification non-conforme à l'ISO17024

SCNP / SCNA (4/6)

- Examen
  - 150$ pour le SNCP, 180$ pour le SCNA
  - En ligne, sous-traité à Prometric (www.prometric.com) et Pearson Vue (www.vue.com), à passer dans un centre de formation agréé
  - SCNP : Deux QCM de 60 questions chacun, en 1h30 chacun
  - SCNA : QCM de 60 question en 1h30 + un exercice rédigé à partir d'un scénario en 1h
- Maintien
  - Re-certification tous les deux ans de la moitié de l'examen

SCNP / SCNA (5/7)

- Formation
  - Formateur certifié SCNP / SCNA + SCPCI
    - SCPCI : certification spéciale Security Certified Program Certified Instructor
    - CV et expérience à l'approbation d'Ascendant learning
    - Suivi d'une formation Train-the-Trainer à Chicago pour ?? $
    - QCM (pas de détails)
  - Supports fourni par SecurityCertified
    - Anglais
    - Transparents pour 4 formations de 5 jours chacune
    - Support écrit pour les stagiaires
  - Langue locale
  - Payement d'une redevance annuelle en $ de la société de formation à SecurityCertified pour être dans le programme

SCNP / SCNA (6/7)

- Deux formations de 5 jours par certification
  - SCNP
    - Hardening the Infrastructure (HTI)
    - Network Defense and Countermeasures (NDC)
  - SCNA
    - Advanced Security Implementation (ASI)
    - Enterprise Security Solutions (ESS)
- Sociétés de formation, plutot issues des formations produits
  - IDSA (Suisse)
    - www.idsa.ch
  - Roman (Suisse)
    - 2760 € pour 5 jours
    - www.roman.ch/documents/
  - GFN (Allemagne)
    - www.gfn.de

SCNP / SCNA (7/7)

- Modèle économique
  - Transparents des formations réalisés par SecurityCertified
  - Contenu de l'examen réalisé par SecurityCertified
  - Promotion de la certification par SecurityCertified et les sociétés de formation
  - Revente de la certification par les sociétés de formation
  - Profit pour SecurityCertified
  - Profit pour les sociétés de formation

OPSA / OPST / OPSE (1/5)

- OSSTMM Professionnal Security Analyst / Tester / Expert
- Certifications orientées techniques et pratiques
- Editeur : ISECOM (USA) : www.isecom.org
  - Institute for Security and Open Methodologies
    - ... Security Examination, Certification, and ...
  - Non-profit organization
  - Fondé et contrôlé par Pete Herzog
- Création en 2004
- Sans doute encore peu de certifiés OPSA & OPST
  - OPSE pas encore ouvert
- Certification non-conforme à l'ISO17024

OPSA / OPST / OPSE (2/5)

- Examen
  - 350 $ pour chaque niveau
  - A l'issue de chaque formation dans le site de la société de formation agrée
  - Anglais
  - QCM
  - Lié à l'Université de Barcelone (La Salle Universitat Ramon Llull), www.salleurl.edu
- Maintien
  - Le certificat est lié à la version d'OSSTMM sur laquelle il a été passé : actuellement 2.1
  - Pour être certifié sur OSSTMM 3.0 il faut repasser l'examen

OPSA / OPST / OPSE (3/5)

- Formation
  - Formateur certifié OPSA / OPST / OPSE + ISECOM TtT
    - TfT : certification spéciale Train-the-Trainer
    - CV à l'approbation de Pete Herzog
    - Suivi d'une formation à Barcelone pour ?? $
    - 3 ans d'expérience dans la sécurité
    - QCM de 50 questions en 2h
  - Support fourni par ISECOM
    - Anglais
    - 40h de transparents
    - 20h de support écrit
  - Travaux pratiques
  - Langue locale

OPSA / OPST / OPSE (4/5)

- Formation (suite)
  - Obligation de planifier au moins un cours ou examen tous les 2 mois
  - Payement d'une redevance en $ de la société de formationà ISECOM (montant non-public)
    - Une partie annuelle pour le droit de délivrer une formation donnant accès à une cerftification ISECOM
    - Une partie trimestrielle pour les frais de marketing d'ISECOM
  - Obligation pour tous les stagiaires de passer et payer l'examen de la certification ISECOM
  - Sociétés de formation
    - Dreamlab (Suisse), Mediaservice (Italie), S21sec (Espagne), Nyxtec (Uk), etc
      - http://www.isecom.org/partners/training.shtml
    - Entre $400 et $1000 par jour et par stagiaire suivant la zone géographique d'implantation de la société

OPSA / OPST / OPSE (5/5)

- Modèle économique
  - Transparents des formations réalisés par ISECOM
  - Contenu de l'examen réalisé par ISECOM
  - Promotion de la certification par ISECOM et les sociétés de formation
  - Revente de la certification par les sociétés de formation
  - Profit pour ISECOM
  - Profit pour les sociétés de formation
    - Exclusivité de l'accord entre ISECOM et la société de formation pour une zone géographique donnée

GIAC (1/4)

- Global Information Assurance Certifications
  - GIAC Security Essentials Certification (GSEC)
  - GIAC Certified Firewall Analyst (GCFW)
  - GIAC Certified Intrusion Analyst (GCIA)
  - GIAC Certified Incident Handler (GCIH)
  - GIAC Certified Windows Security Administrator (GCWN)
  - GIAC Certified UNIX Security Administrator (GCUX)
  - GIAC Systems and Network Auditor (GSNA)
  - GIAC Certified Forensic Analyst (GCFA)
  - GIAC Information Security Fundamentals (GISF)
  - GIAC IT Security Audit Essentials (GSAE)
  - GIAC Certified ISO17799 Specialist (G7799)
  - GIAC Security Leadership Certification (GSLC)
  - GIAC Certified Security Consultant (GCSC)

GIAC (2/4)

- Certifications à profil technique couvrant l'ensemble des aspects de la sécurité
- Editeur : SANS (USA) : www.sans.org
  - Non-profit organization
  - Fondé et contrôlé par Alan Paller
- Certification GIAC créée en 2000
- Environ 6400 personnes certifiées
- Certification non-conforme ISO17024
  - Formation et certification liées

GIAC (3/4)

- Examen
  - 250 $ par certification + suivi de la formation chez SANS
    - 3000 $ pour 12 certifications
  - Possibilité de passer l'examen en candidat libre pour certaines certifications, dans ce cas examen à 450 $
  - En ligne
  - Anglais
  - QCM
  - Rédaction d'un mémoire noté par un jury
    - Possibilité de demander pour pouvoir le rédiger dans sa langue natale
- Maintien
  - Re-certification tous les 2 ans ou 4 ans suivant la certification

GIAC (4/4)

- Formation
  - Exclusivement réalisées par SANS
    - $450 par jour à $800 par jour suivant le niveau de la certification
    - En moyenne 5 jours de cours par certification
  - Formateurs certifiés aux certifications GIAC + membres du SANS Institute et co-optés par leurs pairs
  - Anglais
  - Pas de sociétés de formation
- Modèle économique
  - Formations, contenus des examens et promotion réalisés par SANS
  - Formateurs rémunérés en fonction du nombre de participants
  - Profit pour SANS

CISSP (1/5)

- Certified Information System Security Professionnal
- Connaissance complète de tous les sujets en sécurité informatique
  - Access Control Systems & Methodology
  - Applications & Systems Development
  - Business Continuity Planning
  - Cryptography
  - Law, Investigation & Ethics
  - Operations Security
  - Physical Security
  - Security Architecture & Models
  - Security Management Practices
  - Telecommunications, Network & Internet Security

CISSP (2/5)

- Editeur : ISC2 (USA) : www.isc2.org
  - Non-profit organization
- ISC2 propose égalelement une certification deux fois plus petite :
  - SSCP : System Security Certified Practitioner
- Création en 1995 (à confirmer)
- Environ 25000 personnes certifiées
  - 60 en France, + 40 en un an
- Certification non-conforme à l'ISO17024
  - Travail nécessaire pour être conforme en cours d'étude
- ISSA (www.issa.org, www.issafrance.org)
  - Association à laquelle les CISSP adhèrent souvent

CISSP (3/5)

- Examen
  - Europe : 660 €, UK : 370 £, USA : 600$, si réservé à l'avance : 460 €, 310 £ ou 500$
  - Anglais, japonais, coréen
    - Français prévu en 2005, puis allemand, puis espagnol
  - A dates fixes plusieurs fois par an
    - Les samedis à Paris
  - QCM de 250 questions en 6h
  - 4 ans d'expérience professionnelle dans la sécurité ou diplôme de niveau BAC+2 (*college degree*) et 3 ans d'expérience professionnelle dans la sécurité

CISSP (4/5)

- Maintien
  - 85 $ par an à ISC2
  - Re-certification tous les 3 ans ?
    - Obsolescence de l'examen
    - Pas le cas dans la réalité
  - Crédit CPE de 120h pour trois ans
  - Respect du code d'éthique
  - Rester dans le métier de la sécurité

CISSP (5/5)

- Formation
  - Formateur certifié CISSP + certifié comme formateur auprès de l'ISC2
    - Modalités inconnues
    - Nouveau formateur accompagné par un ancien au début
  - Supports officiels en anglais réalisés par ISC2
  - Langue locale
  - Sociétés de formation :
    - Auditware (France) www.auditware.fr
      - Cours inter-entreprises : 2595 € pour 5 jours de cours
      - Cours intra : 30000 € pour 16 personnes, par instructeur certifié ISC2
    - Axioma technologies (Canada) www.profex.qc.ca/axioma
      - Cours intra : prix similaire pour 15 personnes, par instructeur certifié ISC2
- Modèle économique
  - Formation, contenu de l'examen et promotion du CISSP financés par ISC2
  - Profit pour ISC2
  - Profit pour les sociétés de formation

ProCSSI (1/6)

- Professionnel Certifié de la Sécurité des Systèmes d'Information
  - Nom provisoire devant être confirmé
- Contenu prévisionnel
  - Un tronc commun + une spécialisation au choix :
  - Domaine A. Sécurité des systèmes et des réseaux
  - Domaine B. Sécurité des applications et des transactions
  - Domaine C. Sécurité des informations et contenus numériques
  - Domaine D. Sécurité physique des sites informatiques et plan de continuité
- Garantit une connaissance et expérience globale de la sécurité et une connaissance approfondie dans au moins un domaine spécifique

ProCSSI (2/6)

- Editeur : INSECA (France), serveur web à venir en septembre
  - Institut Européen de Certification et d'Audit
  - Société privée
    - Fondée et dirigée par Marc Janiaud
    - Filiale du pôle universitaire Léonard de Vinci
      - Lui-même financé par le conseil général des hauts-de-seine
  - Edite et gère 8 certifications dans d'autres domaines
- Création en 2004, démarrage prévu fin 2004
- Seule certification française
- Certification conforme à l'ISO17024 / EN45013, agrément COFRAC en cours

ProCSSI (3/6)

- Examen
  - 1300 € avec un domaine, 350 € par domaine supplémentaire
    - Réduction de 150 € pour les membres d'une association
  - ½ journée à dates fixes plusieurs fois par an
  - Français
    - Le seul
  - Dossier de candidature détaillé
  - QCM de 40 questions en 1h pour le tronc commun
    - Idem pour chaque domaine
  - 5 ans d'expérience professionelle en sécurité

ProCSSI (4/6)

- Examen (suite)
  - Soutenance devant un jury
    - Le jury passe 4 à 6 candidats par jour
    - Durée maximum de chaque entretien de 1h30
    - Membres du jury certifiés ProCSSI et co-optés par leurs pairs
    - Président du jury : Pierre-Luc Refalo
    - Le jury conseille le candidat sur ses lacunes
    - Le jury rédige un rapport pour le comité de certification qui décidera
  - Membres du comité de certification en cours de constitution
    - 10 ans d'expérience en sécurité
    - Représentants de l'administration
      - Par exemple : DCSSI, ADAE, Minefi, ...
    - Représentants des associations professionelles en sécurité qui apportent leur crédibilité
      - Par exemple : Cercle Européen de la Sécurité, Cigref, Clusif, Ossir, ...

ProCSSI (5/6)

- Maintien
  - Entretien annuel devant le jury : 350 €
  - Re-certification tous les 3 ans : 1000 €
- Formation
  - Formateurs certifiés ProCSSI
  - Français
  - Société privées
    - Le référentiel étant en cours de réalisation, il n'y a pas encore de sociétés de formation déclarées

ProCSSI (6/6)

- Modèle économique
  - Examen réalisé par les membres du jury et des bénévoles
  - Membres du jury rémunérés quand ils sont jury
  - Promotion réalisée par des associations professionnelles
  - Profit pour INSECA
  - Profit pour les sociétés de formation

Autres certifications

- TICSA
  - TrueSecure ICSA Certified Security Associate
  - https://ticsa.trusecure.com/

Conclusion

- Certification des individus en sécurité en plein développement
- Offre diversifiée
- Chacun doit sélectionner ce qui correspond à ses compétences et ses ambitions
- Etre certifié est un atout et deviendra un pré-requis

Questions ?

www.hsc.fr

Remerciements

- CISM / CISA
  - Frederic Huynh, Ernst & Young
- BS7799 Lead Auditor
  - Alexandre Fernandez, HSC
  - Nicolas Jombart, HSC
- CEH / CHFI
  - Michael Roberts, Mile2
  - Dominique Melançon, Axioma
- SCNP / SCNA
  - Tracy Andrews, SecurityCertified
  - Suzanne O'Rourke, Bluemoon Ventures
- OPSA / OPST / OPSE
  - Pete Herzog, Isecom
  - Nicolas Mayencourt, Dreamlab
  - Raoul Chiesa, Mediaservice
- GIAC
  - Garrett Anderson, Consultant
  - Debbie Taylor, SANS
  - Zoe Dias, Consultant
- CISSP
  - James E. Duffy, ISC2
  - Patrick Morrissey, Auditware
  - Christian Simatos, Savoir-Faire
- ProCSSI
  - Marc Janiaud, Pôle universitaire Léonard de Vinci
  - Pierre-Luc Réfalo, Comprendre & Réussir

Avertissement

- Je m'excuse auprès de ceux qui n'ont pas été cités
  - Remarques / erreurs / oublis : Herve.Schauer@hsc.fr
- Les informations fournies peuvent être erronées
  - Les recoupements ont souvent donné des résultats contradictoires
  - Les sources sont parfois les vendeurs, parfois les individus certifiés
- Les listes de sociétés sont purement indicatives
  - Pas d'exhaustivité
  - Pas de d'endossement d'HSC ni d'Hervé Schauer pour l'une ou l'autre des sociétés citées
- Formations
  - Même quand les formations sont dispensées dans la langue locale, les supports des formations sont toujours en anglais, sauf pour le ProCSSI franco-français.