



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>

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Security Certified Network Professional / Architect

- x Certifications à profil techniques

- x Domaines couverts par le SCNP

- x Advanced TCP/IP
 - x IPSec
 - x Securing Linux Computers
 - x Securing Windows Computers
 - x Securing Routers and Access Control Lists
 - x Contingency Planning
 - x Security on the Internet and the World Wide Web
 - x Attack Techniques

- x Network Defense Fundamentals
 - x Designing Firewall Systems
 - x Configuring Firewalls
 - x Configuring VPNs
 - x Designing an IDS
 - x Configuring an IDS
 - x Analyzing Intrusion Signatures
 - x Performing a Risk Analysis
 - x Creating a Security Policy

Certifications à profil techniques (suite)

- x Domaines couverts par le SCNA

- x Introduction to Trusted Networks
- x Cryptography and Data Security
- x Computer Forensics
- x Law and Legislation
- x Biometrics
- x Strong Authentication
- x Digital Certificates
- x Digital Signatures

- x Trusted Network Implementation
- x Plan and Design a Trusted Network
- x Microsoft Trusted Networks
- x Linux Trusted Networks
- x Managing Certificates
- x Local Resource Security
- x Wireless Security
- x Securing Email
- x Building Trusted Solutions

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

x Examen

- x 150\$ pour le SNCP, 180\$ pour le SCNA
- x En ligne, sous-traité à Prometric (www.prometric.com) et Pearson Vue (www.vue.com), à passer dans un centre de formation agréé
- x SCNP : Deux QCM de 60 questions chacun, en 1h30 chacun
- x SCNA : QCM de 60 question en 1h30 + un exercice rédigé à partir d'un scénario en 1h

x Maintien

- x Re-certification tous les deux ans de la moitié de l'examen

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

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

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

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

x Examen

- x 350 \$ pour chaque niveau
- x A l'issue de chaque formation dans le site de la société de formation agréée
- x Anglais
- x QCM
- x Lié à l'Université de Barcelone (La Salle Universitat Ramon Llull),
www.salleurl.edu

x Maintien

- x Le certificat est lié à la version d'OSSTMM sur laquelle il a été passé :
actuellement 2.1
- x Pour être certifié sur OSSTMM 3.0 il faut repasser l'examen

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

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

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

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

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

x Examen

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

x Maintien

- x Re-certification tous les 2 ans ou 4 ans suivant la certification

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

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

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

x Examen

- x Europe : 660 €, UK : 370 £, USA : 600\$, si réservé à l'avance : 460 €, 310 £ ou 500\$
- x Anglais, japonais, coréen
 - x Français prévu en 2005, puis allemand, puis espagnol
- x A dates fixes plusieurs fois par an
 - x Les samedis à Paris
- x QCM de 250 questions en 6h
- x 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

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

x Formation

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

x Modèle économique

- x Formation, contenu de l'examen et promotion du CISSP financés par ISC2
- x Profit pour ISC2
- x Profit pour les sociétés de formation

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

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

x Examen

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

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

- x **Maintien**

- x Entretien annuel devant le jury : 350 €
 - x Re-certification tous les 3 ans : 1000 €

- x **Formation**

- x Formateurs certifiés ProCSSI
 - x Français
 - x Société privées
 - x Le référentiel étant en cours de réalisation, il n'y a pas encore de sociétés de formation déclarées

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

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

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

Questions ?

www.hsc.fr

x CISM / CISA

x Frederic Huynh, Ernst & Young

x BS7799 Lead Auditor

x Alexandre Fernandez, HSC

x Nicolas Jombart, HSC

x CEH / CHFI

x Michael Roberts, Mile2

x Dominique Melançon, Axioma

x SCNP / SCNA

x Tracy Andrews, SecurityCertified

x Suzanne O'Rourke, Bluemoon Ventures

x OPSA / OPST / OPSE

x Pete Herzog, Isecom

x Nicolas Mayencourt, Dreamlab

x Raoul Chiesa, Mediaservice

x GIAC

x Garrett Anderson, Consultant

x Debbie Taylor, SANS

x Zoe Dias, Consultant

x CISSP

x James E. Duffy, ISC2

x Patrick Morrissey, Auditware

x Christian Simatos, Savoir-Faire

x ProCSSI

x Marc Janiaud, Pôle universitaire Léonard de Vinci

x Pierre-Luc Réfalo, Comprendre & Réussir

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