Datadocké

# Catalogue de formation

Edition 2022

SECURELAND Security

## Cyber Sécurité

Formations certifiantes

*« Dis moi et j'oublierai;*

*Enseigne moi et je m'en souviendrai;*

*Implique moi et j'apprendrai.»*

***Benjamin Franklin***

# Nos engagements

## Expertise

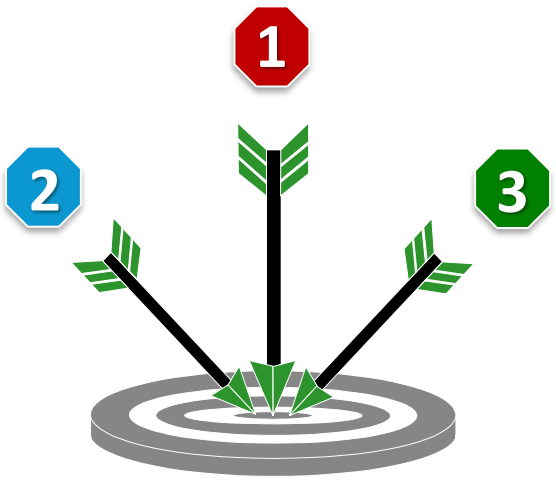
Nos formateurs apportent de fortes compétences IT, tant techniques que fonctionnelles. Ils mettent en œuvre leur expérience avec méthodologie et vont au bout de leur démarche qui se veut pragmatique et exhaustive.

## Plus value

Nous veillons à apporter une plus value à nos clients sur toutes nos formations. Nos formateurs mettent en situation pratiquement réelle les notions théoriques qu'ils enseignent afin de vous rapprocher des situations professionnelles auxquelles vous serez confrontés.

## Motivation

La motivation de nos formateurs constitue un réel moteur pour SecureLand. Nos formateurs sont tous des professionnels qui exercent le métier enseigné lors de leur formation. Ils aiment leur métier et souhaitent transmettre leur savoir-faire aux autres.



# Nos références

SECURELAND
Security

# Nos formations en Cybersécurité

# Nos formations

## Cybersécurité



# Sécurité des Systèmes d'Information

SecureLand vous propose cette formation en sécurité informatique, afin de découvrir globalement ce monde en plein expansion. C'est une bonne sensibilisation aux acteurs des entreprises à la sécurité.
Il s'agit de découvrir toutes les bases de la sécurité informatiques à la fois organisationnelles et techniques.
Plusieurs démonstration techniques des attaques sécurité sont proposées tout au long de la formation.

## Jour 1

**Introduction à la cyber-sécurité**
- ❑ Notions de bases
- ❑ Les besoins de la sécurité des systèmes d'information
- ❑ Politiques et procédures de sécurité
- ❑ Notions de vulnérabilité, menace, attaque
- ❑ Aspects légaux de la cybersécurité en France

**Management de la sécurité**
- ❑ Intégrer la sécurité au sein d'une organisation
- ❑ Intégrer la sécurité dans les projets
- ❑ Normes ISO 27001,
- ❑ Gestion des risques (ISO 27005, EBIOS,..)
- ❑ Difficultés liées à la prise en compte de la sécurité
- ❑ Métiers liés à la cybersécurité

## Jour 2

**Sécurité opérationnelle**
- ❑ Connaitre le Système d'Information
- ❑ Maitriser le réseau
- ❑ Sécuriser les terminaux
- ❑ Gérer les utilisateurs
- ❑ Les types d'attaques de sécurité informatique
- ❑ Sécurisation des infrastructures, du SI, du réseau et des applications
- ❑ Continuité d'activité
- ❑ Sécuriser physiquement les sites et les Datacenter
- ❑ Contrôler la sécurité du S.I.

## Jour 3

**Sécurité technique**
- ❑ La sécurité du protocole IP
- ❑ Sécurisation d'un réseau
- ❑ Les bases de la cryptographie
- ❑ La sécurité des applications web
- ❑ Audit de sécurité d'un application Web

**Dans la peau d'un « ethical Hacker »**
- ❑ Démonstration du déroulement d'un test d'intrusion web
- ❑ Préparation de l'attaque (Périmètre, objectif, etc.)
- ❑ Collecte d'information et scanning
- ❑ Exploitation des résultats
- ❑ Etude et synthèse (QCM + rédaction par les élèves)

**Evaluation des connaissances**
- ❑ Test des connaissances acquises

## Objectifs opérationnels

- Présenter globalement le domaine de la sécurité informatique
- Présenter les différents métiers de la sécurité informatique
- Sensibiliser aux risques de cybersécurité
- Former à l'identification des menaces et à la protection des attaques

## Informations générales

- **Code de la formation :** SECU
- **Langues** : Français
- **Durée** : 3 jours
- **Public visé** : Toute personne intéressée par la sécurité informatique,
- **Tarif** :

## Pré-requis

- Support de formation
- Un PC avec une connexion internet

## Mode d'enseignement

- Support sous forme de diapositifs
- Exercices pendant la formation
- Démonstrations techniques

# Dans la peau d'un Ethical hacker

SecureLand vous propose une formation de 3 jours totalement orientée vers la réalisation des attaques sécurité comme si vous étiez un Ethical Hacker ou un auditeur sécurité.
Les notions théoriques sont brièvement évoquée pendant les 3 jours durant lesquels vous serez en face d'une cible vulnérable afin d'exploiter ses failles.
Durant la dernière demi-journée, vous participerez à un concours amical dit CTF (capture the flag) afin de consolider vos compétences !


## Jour 1

**Introduction au technique du hacking**
- ❑ Introduction à la cyber-sécurité
- ❑ Gouvernance de la sécurité de l'information (SMSI)
- ❑ Management des risques
- ❑ Phases d'un audit sécurité
- ❑ Présentation de l'environnement technique

**Phase de découverte**
- ❑ Prise de main sur la machine d'attaque
- ❑ Découverte et tests de quelques outils
- ❑ Prise d'information passive
- ❑ Utilisation des moteurs de recherche
- ❑ Recherche avec terminal
- ❑ Prise d'information active
- ❑ TP de recherche d'information

## Jour 2

**Phase de reconnaissance**
- ❑ Revue de la journée 1
- ❑ Présentation du modèle OSI
- ❑ Présentation des protocoles et l'adressage IP
- ❑ Présentation des failles réseaux et systèmes
- ❑ Prise d'information active sur les cibles
- ❑ Découverte des hôtes
- ❑ Scan des ports et des services
- ❑ Empreintes des OS
- ❑ Enumération
- ❑ Scan des vulnérabilités
- ❑ TP : ARP cache Poisonning
- ❑ TP: metasploitable2

## Jour 3

**Phase d'exploitation**
- ❑ Revue de la journée 2
- ❑ Attaque GRUB
- ❑ Attaque Windows
- ❑ Cracker un mot de passe
- ❑ Ecoute réseau et vol de données
- ❑ Attaque par Déni de service
- ❑ Introduction à Metasploit
- ❑ Attaque Web
- ❑ Attaque Android
- ❑ Attaques cryptographiques

**Attaques web**
- ❑ Brute force avec cookie
- ❑ Cross Site Scripting (XSS)
- ❑ Injection SQL
- ❑ File uploadInjection de commande
- ❑ Local File inclusion (LFI)
- ❑ Bonnes pratiques de sécurité
- ❑ TP : devenir root sur un serveur web grâce aux injection SQL

**Concours « Capture the Flag - CTF »**
- ❑ Challenge sur une cible vulnérable
- ❑ Scoring et classement sur un outils web développé pour cette formation

## Objectifs opérationnels

- Compréhension des aspects de la sécurité techniques des réseaux et des systèmes informatiques
- Compréhension des notions de risques et de vulnérabilités ainsi que leurs impacts
- Exploitation des failles de sécurité
- Sensibilisation aux risques de sécurité informatique

## Informations générales

- **Code de la formation :** HACK
- **Langues** : Anglais ou Français
- **Durée** : 3 jours
- **Public visé** : Consultant en sécurité information, chef de projet sécurité, toute personne intéressée par les tests d'intrusion

## Pré-requis

- Un PC avec une connexion internet
- Logiciel Virtual Box installé
- Notions informatiques, développements et réseaux (linux principalement)

## Mode d'enseignement

- Support sous forme de diapositifs
- Manipulation technique de toutes les attaques présentées

PECB

# Certification ISO 27001 Lead implementor

La formation ISO/CEI 27001 Lead Implementer vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation lors de l'établissement, la mise en œuvre, la gestion et la tenue à jour d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO/CEI 27001. Cette formation est conçue de manière à vous doter d'une maîtrise des meilleures pratiques en matière de Systèmes de management de la sécurité de l'information pour sécuriser les informations sensibles, améliorer l'efficacité et la performance globale de l'organisation.

ISO 27001 Lead Implementer

## Jour 1

**Introduction à ISO/IEC 27001 et initiation d'un SMSI**

- ❑ Objectifs et structure de la formation
- ❑ Normes et cadres réglementaires
- ❑ Système de management de la sécurité de l'information (SMSI)
- ❑ Concepts et principes fondamentaux de la sécurité de l'information
- ❑ Initiation de la mise en œuvre du SMSI
- ❑ Compréhension de l'organisme et de son contexte
- ❑ Périmètre du SMSI

## Jour 2

**Planification de la mise en œuvre d'un SMSI**

- ❑ Leadership et approbation du projet
- ❑ Structure organisationnelle
- ❑ Analyse du système existant
- ❑ Politique de sécurité de l'information
- ❑ Gestion des risques
- ❑ Déclaration d'applicabilité

## Jour 3

**Mise en œuvre d'un SMSI**

- ❑ Gestion de l'information documentée
- ❑ Sélection et conception des mesures de sécurité
- ❑ Mise en œuvre des mesures de sécurité
- ❑ Tendances et technologies
- ❑ Communication
- ❑ Compétence et sensibilisation
- ❑ Gestion des opérations de sécurité

## Jour 4

**Surveillance du SMSI, amélioration continue et préparation à l'audit de certification**

- ❑ Surveillance, mesure, analyse et évaluation
- ❑ Audit interne
- ❑ Revue de direction
- ❑ Traitement des non-conformités
- ❑ Amélioration continue
- ❑ Préparation à l'audit de certification
- ❑ Processus de certification et clôture de la formation

## Jour 5

**Examen de certification**

- ❑ L'examen « PECB Certified ISO/CEI 27001 Lead Implementer » remplit les exigences relatives au programme d'examen et de certification de PECB.
- ❑ Examen en ligne
- ❑ QCM en Français (3h)
- ❑ Les frais d'examen et de certification sont inclus dans le prix de la session de formation.

## Objectifs opérationnels

- Expliquer les concepts et principes fondamentaux d'un système de management SMSI basé sur ISO/IEC 27001
- Interpréter les exigences d'ISO/IEC 27001 pour un SMSI du point de vue d'un responsable de la mise en œuvre
- Initier et planifier la mise en œuvre d'un SMSI basé sur ISO/IEC 27001, en utilisant la méthodologie IMS2 de PECB et d'autres bonnes pratiques

## Informations générales

- **Code de la formation :** 27001LI
- **Langues** : Français
- **Durée** : 5 jours
- **Public visé** : Responsables ou consultants sécurité, toute personne intéressée par la sécurité

## Pré-requis

- Une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies des principes de mise en œuvre

## Mode d'enseignement

- Support sous forme de diapositifs
- Exercices et TD
- Travaux dirigés interactifs en groupe

PECB

# Certification ISO 27002 Lead Manager

La formation ISO/CEI 27002 Lead Manager vous permettra d'acquérir l'expertise nécessaire pour accompagner une organisation dans la mise en œuvre et la gestion des mesures de sécurité de l'information conformes à la norme ISO/CEI 27002. Durant cette formation, vous acquerrez des connaissances approfondies sur les meilleures pratiques en matière de mesures de sécurité de l'information et vous serez apte à améliorer la sécurité de l'information dans une organisation.

## Jour 1

**Introduction aux mesures de sécurité de l'information conformes à la norme l'ISO/CEI 27002**

- ❑ Objectifs et structure de la formation
- ❑ Cadres normatifs et réglementaires
- ❑ Principes fondamentaux de la sécurité de l'information
- ❑ Système de mangement de la sécurité de l'information
- ❑ Politiques de sécurité de l'information
- ❑ Management de la sécurité de l'information

## Jour 2

**Exigences et objectifs de la sécurité de l'information conforme à la norme ISO/CEI 27002**

- ❑ Sécurité des ressources humaines
- ❑ Gestion des actifs
- ❑ Contrôle d'accès

## Jour 3

**Surveiller, mesurer, analyser et évaluer les mesures de la sécurité de l'information**

- ❑ Cryptographie
- ❑ Sécurité physique et environnementale
- ❑ Sécurité liée à l'exploitation
- ❑ Sécurité des communications

## Jour 4

**Amélioration continue de la performance du Système de management de la sécurité de l'information de l'organisation**

- ❑ Acquisition, développement et maintenance des systèmes d'information
- ❑ Relations avec les fournisseurs
- ❑ Gestion des incidents liés à la sécurité de l'information
- ❑ Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- ❑ Conformité
- ❑ Compétences et évaluation des gestionnaires
- ❑ Clôture de la formation

## Jour 5

**Examen de certification**

- ❑ L'examen « PECB Certified ISO/CEI 27002 Lead Manager » remplit les exigences relatives au programme d'examen et de certification de PECB
- ❑ Examen en ligne Open Book
- ❑ Question rédactionnelle en Français (3h)
- ❑ Les frais d'examen et de certification sont inclus dans le prix de la session de formation.

## Objectifs opérationnels

- Maîtriser la mise en œuvre des mesures de sécurité de l'information en respectant le cadre et les principes de la norme ISO/CEI 27002
- Maîtriser les concepts, les approches, les normes et les techniques nécessaires pour la mise en œuvre et la gestion efficace des mesures de la sécurité de l'information
- Maîtriser la mise en œuvre des processus de la sécurité de l'information

## Informations générales

- **Code de la formation :** 27002
- **Langues** : Français
- **Durée** : 5 jours
- **Public visé** : Responsables ou consultants sécurité, toute personne intéressée par la sécurité

## Pré-requis

- Des connaissances fondamentales de la norme ISO/CEI 27002 et des connaissances approfondies sur la sécurité de l'information.

## Mode d'enseignement

- Support sous forme de diapositifs
- Supports officiels fournis
- Exercices et TD
- Travaux dirigés interactifs en groupe

PECB

# Certification ISO 27001 Lead Auditor

Au cours de cette formation, vous acquerrez les connaissances et les compétences nécessaires pour planifier et réaliser des audits conformément aux processus de certification ISO 19011 et ISO/IEC 17021-1. À l'aide d'exercices pratiques, vous serez en mesure d'acquérir des connaissances sur la protection de la vie privée dans le contexte du traitement des informations d'identification personnelle (IIP), et de maîtriser des techniques d'audit afin de devenir compétent pour gérer un programme et une équipe d'audit, communiquer avec des clients et résoudre des conflits potentiels.

## Jour 1

**Introduction au système de management de la sécurité de l'information (SMSI) et à ISO/IEC 27001**

- ❑ Objectifs et structure de la formation
- ❑ Normes et cadres réglementaires
- ❑ Processus de certification
- ❑ Concepts et principes fondamentaux de la sécurité de l'information
- ❑ Système de management de la sécurité de l'information (SMSI)

## Jour 2

**Principes d'audit, préparation et initiation d'un audit**

- ❑ Concepts et principes fondamentaux de l'audit
- ❑ Impact des tendances et de la technologie en audit
- ❑ Audit basé sur les preuves
- ❑ Audit basé sur les risques
- ❑ Initiation du processus d'audit
- ❑ Étape 1 de l'audit

## Jour 3

**On-site audit activities**

- ❑ Préparation de l'étape 2 de l'audit
- ❑ Étape 2 de l'audit
- ❑ Communication pendant l'audit
- ❑ Procédures d'audit
- ❑ Création de plans d'échantillonnage d'audit

## Jour 4

**Closing the audit**

- ❑ Rédaction des rapports de constatations d'audit et de non-conformité
- ❑ Documentation d'audit et revue de la qualité
- ❑ Clôture de l'audit
- ❑ Évaluation des plans d'action par l'auditeur
- ❑ Après l'audit initial
- ❑ Gestion d'un programme d'audit interne
- ❑ Clôture de la formation

## Jour 5

**Examen de certification**

- ❑ L'examen « PECB Certified ISO/CEI 27001 Lead Auditor » remplit les exigences relatives au programme d'examen et de certification de PECB
- ❑ Examen en ligne
- ❑ QCM en Français (3h)
- ❑ Les frais d'examen et de certification sont inclus dans le prix de la session de formation.

## Objectifs opérationnels

- Expliquer les concepts et principes fondamentaux d'un système de management de la continuité d'activité (SMCA) basé sur ISO 22301
- Interpréter les exigences d'ISO 22301 pour un SMCA du point de vue d'un auditeur
- Évaluer la conformité du SMCA aux exigences d'ISO 22301, en accord avec les concepts et principes fondamentaux d'audit
- Planifier, conduire et clore un audit de conformité à ISO 22301.

## Informations générales

- **Code de la formation :** 27001LA
- **Langues** : Français
- **Durée** : 5 jours
- **Public visé** : Responsables ou consultants sécurité, Auditeurs, Experts techniques sécurité.

## Pré-requis

- Une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies des principes de mise en œuvre

## Mode d'enseignement

- Support sous forme de diapositifs
- Supports officiels fournis
- Exercices et TD
- Travaux dirigés interactifs en groupe

PECB

# Certification ISO 27005 *Risk Manager*

La formation « ISO/IEC 27005 Risk Manager » vous permettra de développer les compétences nécessaires pour maîtriser les processus liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la norme ISO/IEC 27005 comme cadre de référence. Au cours de cette formation, nous présenterons également d'autres méthodes d'appréciation des risques telles qu'OCTAVE, EBIOS, MEHARI et la méthodologie harmonisée EMR. Cette formation s'inscrit parfaitement dans le processus de mise en œuvre du cadre SMSI selon la norme ISO/IEC 27001.

## Jour 1

**Introduction au programme de gestion des risques conforme à ISO/IEC 27005**

- ❑ Objectifs et structure de la formation
- ❑ Cadres normatifs et règlementaires
- ❑ Concepts et définitions du risque
- ❑ Programme de gestion des risques
- ❑ Établissement du contexte

## Jour 2

**Mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005**

- ❑ Identification des risques
- ❑ Analyse et évaluation des risques
- ❑ Appréciation du risque avec une méthode quantitative
- ❑ Traitement des risques
- ❑ Acceptation des risques et gestion des risques résiduels
- ❑ Communication relative aux risques
- ❑ Surveillance et réexamen des risques

## Jour 3

**Aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification**

- ❑ Méthode OCTAVE
- ❑ Méthode MEHARI
- ❑ Méthode EBIOS
- ❑ Méthodologie harmonisée d'EMR
- ❑ Clôture de la formation

**Examen de certification**

- ❑ L'examen « PECB Certified ISO/IEC 27005 Risk Manager » remplit les exigences relatives au programme d'examen et de certification de PECB
- ❑ Examen en ligne Open Book
  - ❑ Question rédactionnelle en Français (2h)
  - ❑ QCM en Anglais (2h)
- ❑ Les frais d'examen et de certification sont inclus dans le prix de la session de formation.

## Objectifs opérationnels

- Comprendre la relation entre la gestion des risques de la sécurité de l'information et les mesures de sécurité
- Comprendre les concepts, approches, méthodes et techniques permettant un processus de gestion des risques efficace et conforme à ISO/IEC 27005
- Savoir interpréter les exigences de la norme ISO/IEC 27001 dans le cadre de la gestion des risques de la sécurité de l'information

## Informations générales

- **Code de la formation :** 27005RM
- **Langues** : Français
- **Durée** : 3 jours
- **Public visé** : Responsables ou consultants sécurité, toute personne intéressée par la sécurité

## Pré-requis

- Une compréhension fondamentale de la norme ISO/IEC 27005 et une connaissance approfondie de l'évaluation des risques et de la sécurité de l'information.

## Mode d'enseignement

- Support sous forme de diapositifs
- Supports officiels fournis
- Exercices et TD
- Travaux dirigés interactifs en groupe

PECB

# Certification EBIOS Risk Manager

La formation EBIOS vous permettra d'acquérir les connaissances et développer les compétences nécessaires pour maîtriser les concepts et les éléments de management des risques liés à tous les actifs pertinents pour la sécurité de l'information en utilisant la méthode EBIOS. Grâce aux exercices pratiques et aux études de cas, vous acquerrez les connaissances et les compétences nécessaires pour réaliser une appréciation optimale des risques liés à la sécurité de l'information et pour gérer les risques dans les temps par la connaissance de leur cycle de vie.

## Jour 1

**Introduction à la gestion des risques et déroulement de la méthode EBIOS**

- ❑ Objectifs et structure du cours
- ❑ Introduction à la méthode EBIOS
- ❑ Atelier 1 « Cadrage et socle de sécurité »
- ❑ Atelier 2 « Sources de risques »

## Jour 2

**Déroulement de la méthode EBIOS (suite)**

- ❑ Atelier 3 « Scénarios stratégiques »
- ❑ Atelier 4 « Scénarios opérationnels »
- ❑ Atelier 5 « Traitement du risque »
- ❑ Processus de certification et clôture de la formation

## Jour 3

**Examen de certification**

- ❑ L'examen « PECB Certified EBIOS Risk Manager » remplit les exigences relatives au programme d'examen et de certification de PECB.
- ❑ Examen en ligne Open Book
- ❑ Question rédactionnelle en Français (3h)
- ❑ Les frais d'examen et de certification sont inclus dans le prix de la session de formation.

## Objectifs opérationnels

- Comprendre les concepts et les principes fondamentaux relatifs à la gestion du risque selon la méthode EBIOS
- Comprendre les étapes de la méthode EBIOS afin de poursuivre l'achèvement des études (pilote, contrôle, reframe) en tant que maître de travail
- Comprendre et expliquer les résultats d'une étude EBIOS et ses objectifs clés
- Acquérir les compétences nécessaires afin de mener une étude EBIOS

## Informations générales

- **Code de la formation :** EBIOS
- **Langues** : Français
- **Durée** : 3 jours
- **Public visé** : Responsables ou consultants sécurité, toute personne intéressée par la sécurité

## Pré-requis

- Une connaissance en gestion du risque est recommandée.

## Mode d'enseignement

- Support sous forme de diapositifs
- Supports officiels fournis
- Exercices et TD
- Travaux dirigés interactifs en groupe

PECB

# Certification Tests d'intrusion PECB

La formation « Lead Pen Test Professional » vous permettra d'acquérir l'expertise nécessaire pour mener un test d'intrusion professionnelle en utilisant un ensemble de techniques pratiques et de compétences de gestion. Le cours est conçu par des experts de l'industrie avec une expérience approfondie dans le domaine du test d'intrusion.
Contrairement à d'autres certifications, ce cours se concentre spécifiquement sur les connaissances et les compétences requises par les professionnels qui cherchent à diriger ou à participer à un test d'intrusion.


## Jour 1

**Introduction aux tests d'intrusions, à l'éthique, à la planification et au domaine d'application**

- ❑ Objectifs et structure de la formation
- ❑ Principes relatifs au test d'intrusion
- ❑ Questions légales et éthiques
- ❑ Approches de test d'intrusion
- ❑ Principes fondamentaux de la sécurité de l'information et de la gestion des risques
- ❑ Phases de test d'intrusion
- ❑ Gestion d'un test d'intrusion

## Jour 2

**Connaissances techniques fondamentales et techniques**

- ❑ Connaissances techniques de base
- ❑ Exercices pratiques dans tous les domaines

## Jour 3

**Réalisation d'un test d'intrusion (à l'aide d'outils et de techniques) et revue du domaine du test**

- ❑ Réalisation d'un test d'intrusion - Tester l'infrastructure
- ❑ Réalisation d'un test d'intrusion - Tests d'intrusion sur les applications Web
- ❑ Réalisation d'un test d'intrusion - Test mobile
- ❑ Réalisation d'un test d'intrusion - Tests d'ingénierie sociale
- ❑ Réalisation d'un test d'intrusion - Tests de sécurité physique

## Jour 4

**Analyse des résultats des tests, rapports et suivi**

- ❑ Documentation de la revue de la qualité du test et du rapport
- ❑ Plans d'action et suivi
- ❑ Gestion d'un programme de test
- ❑ Compétence et évaluation des testeurs d'intrusion
- ❑ Exercices Capture the Flag CTF
- ❑ Clôture de la formation

## Jour 5

**Examen de certification**

- ❑ L'examen « PECB Certified Lead Pen Test Professional » remplit les exigences relatives au programme d'examen et de certification de PECB
- ❑ Examen en ligne Open Book
- ❑ QCM en Français (3h)
- ❑ Les frais d'examen et de certification sont inclus dans le prix de la session de formation.

## Objectifs opérationnels

- Savoir interpréter et illustrer les principaux concepts et principes relatifs au test d'intrusion
- Comprendre les connaissances techniques de base nécessaires pour organiser et mener à bien un ensemble efficace de tests d'intrusion
- Apprendre comment planifier efficacement un test d'intrusion et identifier un domaine d'application approprié et adapté en fonction du risque

## Informations générales

- **Code de la formation :** PENTEST
- **Langues** : Français
- **Durée** : 5 jours
- **Public visé** : Responsables ou consultants sécurité, pentesters, auditeurs, gestionnaires d'incidents.

## Pré-requis

- Une compréhension fondamentale des tests d'intrusion et une connaissance approfondie de la cybersécurité.

## Mode d'enseignement

- Support sous forme de diapositifs
- Supports officiels fournis
- Exercices et TD
- Travaux dirigés interactifs en groupe
- Tests techniques pratiques

PECB

# Certification Ethical Hacking PECB

La certification PECB Certified Lead Ethical Hacker vous aidera à démontrer votre capacité à évaluer légalement la sécurité des systèmes et à découvrir leurs vulnérabilités. Le cours offre des informations sur les dernières méthodes et outils de piratage éthique. Il fournit également une méthodologie pour effectuer des tests d'intrusion conformément aux normes et aux bonnes pratiques, telles que le Penetration Testing Execution Standard (PTES) et l'Open Source Security Testing Methodology (OSSTMM).


## Jour 1

**Introduction au piratage éthique**

- ❑ Objectifs et structure de la formation
- ❑ Normes, méthodologies et cadres de tests d'intrusion
- ❑ Aperçu du laboratoire
- ❑ Concepts fondamentaux du piratage éthique
- ❑ Principes de base des réseaux
- ❑ Comprendre la cryptographie
- ❑ Tendances et technologies pertinentes
- ❑ Principes fondamentaux de Kali Linux
- ❑ Initiation du test d'intrusion
- ❑ Analyse de la portée du test d'intrusion
- ❑ Implications juridiques et accord contractuel

## Jour 2

**Lancement de la phase de reconnaissance**

- ❑ Reconnaissance passive
- ❑ Reconnaissance active
- ❑ Identification des vulnérabilités

## Jour 3

**Lancement de la phase d'exploitation**

- ❑ Modèle de menace et plan d'attaque
- ❑ Éviter les systèmes de détection d'intrusion
- ❑ Attaques côté serveur
- ❑ Attaques côté client
- ❑ Attaques des applications Web
- ❑ Attaques Wi-Fi
- ❑ Escalade des droits
- ❑ Pivotement Transferts des fichiers
- ❑ Conservation de l'accès

## Jour 4

**Post-exploitation et rapports**

- ❑ Nettoyage et destruction des artefacts
- ❑ Production d'un rapport des résultats
- ❑ Recommandations sur l'atténuation des vulnérabilités identifiées
- ❑ Clôture de la formation

## Jour 5

**Examen de certification**

- ❑ L'examen « PECB Certified Lead Ethical Hacker » répond pleinement aux exigences du Programme d'examen et de certification (PEC) de PECB
- ❑ Examen en ligne Open Book
- ❑ Examen pratique en Français (6h)
- ❑ Les frais d'examen et de certification sont inclus dans le prix de la session de formation.

## Objectifs opérationnels

- Maîtriser les concepts, méthodes et techniques utilisés par les organisations de cybersécurité et les hackers éthiques pour réaliser des tests d'intrusion
- Reconnaître la corrélation entre les méthodologies de tests d'intrusion, les cadres réglementaires et les normes
- Acquérir une connaissance approfondie des composantes et des opérations du piratage éthique

## Informations générales

- **Code de la formation :** ETH-HACK
- **Langues** : Français
- **Durée** : 5 jours
- **Public visé** : Responsables ou consultants sécurité, pentesters, auditeurs, gestionnaires d'incidents.

## Pré-requis

- Connaissance des concepts et principes de sécurité de l'information et des compétences avancées en matière de systèmes d'exploitation.
- Connaissance des réseaux informatiques et des concepts de programmation.

## Mode d'enseignement

- Support sous forme de diapositifs
- Supports officiels fournis
- Exercices et TD
- Travaux dirigés interactifs en groupe
- Accès au laboratoire
- Tests techniques pratiques

PECB

# Certification Cloud Security

Cette formation est conçue pour aider les participants à acquérir les connaissances et les compétences nécessaires pour aider un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un programme de sécurité du cloud basé sur ISO/IEC 27017 et ISO/IEC 27018. Elle fournit une élaboration complète des concepts et principes du cloud computing, de la gestion des risques de sécurité du cloud computing, des mesures spécifiques au cloud, de la gestion des incidents de sécurité du cloud et des tests de sécurité du cloud.

## Jour 1

**Introduction aux normes ISO/IEC 27017 et ISO/IEC 27018 et à l'initiation d'un programme de sécurité du cloud**

- ❑ Objectifs et structure de la formation
- ❑ Normes et cadres réglementaires
- ❑ Concepts et principes fondamentaux du cloud computing
- ❑ Comprendre l'architecture du cloud computing de l'organisme
- ❑ Rôles et responsabilités en matière de sécurité de l'information liés au cloud computing
- ❑ Politique de sécurité de l'information pour le cloud computing

## Jour 2

**Gestion des risques de sécurité du cloud computing et mesures spécifiques au cloud**

- ❑ Gestion des risques de sécurité du cloud computing
- ❑ Sélection et conception de mesures spécifiques au cloud
- ❑ Mise en œuvre de mesures spécifiques au cloud (partie 1)

## Jour 3

**Gestion de l'information documentée et sensibilisation et formation à la sécurité du cloud**

- ❑ Mise en œuvre de mesures spécifiques au cloud (partie 2)
- ❑ Gestion de l'information documentée dans le cloud
- ❑ Sensibilisation et formation à la sécurité du cloud

## Jour 4

**Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue**

- ❑ Gestion des incidents de sécurité du cloud
- ❑ Tests de sécurité du cloud
- ❑ Surveillance, mesure, analyse et évaluation
- ❑ Amélioration continue
- ❑ Clôture de la formation

## Jour 5

**Examen de certification**

- ❑ L'examen « PECB Certified Lead Cloud Security Manager » répond pleinement aux exigences du Programme d'examen et de certification (PEC) de PECB.
- ❑ Examen en ligne Open Book
- ❑ QCM en Anglais (3h)
- ❑ Les frais d'examen et de certification sont inclus dans le prix de la session de formation.

## Objectifs opérationnels

- Acquérir une compréhension complète des concepts, approches, méthodes et techniques utilisés pour la mise en œuvre et la gestion efficace d'un programme de sécurité du cloud.
- Comprendre la corrélation entre ISO/IEC 27017, ISO/IEC 27018 et d'autres normes et cadres réglementaires
- Apprendre à interpréter les lignes directrices des normes ISO/IEC 27017 et ISO/IEC 27018 dans le contexte spécifique d'un organisme

## Informations générales

- **Code de la formation :** CLOUDSEC
- **Langues** : Français
- **Durée** : 5 jours
- **Public visé** : Responsables ou consultants sécurité, experts cloud, Managers ou consultants cloud.

## Pré-requis

- La principale exigence pour participer à cette formation est d'avoir une compréhension fondamentale des normes ISO/IEC 27017 et ISO/IEC 27018 et une connaissance générale des concepts du cloud computing.

## Mode d'enseignement

- Support sous forme de diapositifs
- Supports officiels fournis
- Exercices et TD
- Travaux dirigés interactifs en groupe

SECURELAND
Security

# Votre partenaire de formation par excellence

# Exemple de CV de nos formateurs

## M. STA

Auditeur en sécurité des systèmes d'information, Formateur agréé en Sécurité des SI et tests d'intrusion

### FORMATION

- ❑ Ingénieur sécurité des systèmes et des réseau – Télécom SUD Paris
- ❑ Certifié ISO 27005 « Risk manager » et
- ❑ Certifié ISO 27001 « Lead implementor »
- ❑ Certifié Cloud security professional « CSSP »
- ❑ Certifié ISO 27001 « Lead auditor »

### EXPERIENCE

Plus de 10 ans d'intervention au sein de grandes entreprises

- ❑ Architecte sécurité,
- ❑ Consultant en sécurité
- ❑ Formation
- ❑ Audit de conformité
- ❑ Audit fournisseurs
- ❑ Tests d'intrusions

### COMPETENCES CLES

- ❑ Compétences techniques dans le domaine de la sécurité des réseaux et des systèmes
- ❑ Capacité à analyser des systèmes et des réseaux et en donner un avis sur leur niveau de sécurité
- ❑ Ingénierie et création de solutions et architectures sécurisées

Soufiane est ingénieur en sécurité informatique depuis 10 ans, et passionné par ce domaine.
Il intervient depuis de très nombreuses années au sein de grandes entreprises sur des sujets IT très diversifiés. Il a une capacité à analyser les systèmes et les réseaux sans relâche afin d'identifier leurs vulnérabilités et proposer des solutions de sécurité pour les couvrir. Il a pu travailler sur plusieurs métiers liés à la sécurité durant sa carrière, en passant par un consultant généraliste, puis un risque manager, ensuite un architecte sécurité des solutions réseaux, avant d'arriver à l'audit organisationnel et technique (pentester).

orange

Auditeur en sécurité informatique

- ❑ Evaluation de la sécurité informatique de tous les fournisseurs IT d'Orange France
- ❑ Tests d'intrusion technique en interne et en externe sur les solutions déployées par le groupe

Architecte sécurité des systèmes et des réseaux

- ❑ Conception d'architectures sécurisées pour l'accès des partenaires d'Orange au SI interne
- ❑ Analyses de risques sécurité sur plusieurs services d'orange mobile

eFrei PARIS

- ❑ Formateur en sécurité des SI et en audit (Sécurité des systèmes et réseaux, Authentification,…)

General Electric

Auditeur organisationnel et fonctionnel de la conformité du Système d'information GE aux politiques de sécurité du groupe : applications et infrastructures

- ❑ Audit et contrôle de conformité sur le périmètre de l'IT
- ❑ Pilotage de la gestion des risques et accompagnement IT leader dans le traitement de leurs risques sur les applications et les infrastructures les plus critiques

# SecureLand en 4 mots


## Expertise

Nos collaborateurs apportent de fortes compétences IT, tant techniques que fonctionnelles. Ils mettent en œuvre leurs tâches avec méthodologie et vont au bout de leur démarche qui se veut pragmatique et exhaustive.

## Motivation

La motivation de nos collaborateurs constitue un réel moteur pour SecureLand.
Dans la mise en œuvre, nos ressources sont agiles et pertinentes; aller droit au but afin de délivrer résultats et livrables dans les délais.

## Plus value

Nous veillons à apporter une plus value à nos clients sur toutes nos interventions. Nos collaborateurs ont une vision global sur les projets gérés, et une vision client pour les différentes maitrises d'ouvrage.

## Client

Nous apportons une grande importance à la satisfaction client car notre premier objectif est de construire une relation durable avec nos clients.

# Nos Valeurs

Nos valeurs, qui sont également nos engagements, sont :

**1** **Client**
Avec lequel nous sommes très proches pour faire de son point de vue le nôtre

**2** **Fiabilité**
Nous annonçons ce que nous ferons et nous faisons ce que nous avions annoncé

**3** **Transparence**
Tant avec nos clients qu'avec nos ressources humaines

**4** **Excellence**
Délivrer une forte Valeur Ajoutée est notre raison d'être

# Contact

M. Rabah HAMIANE
+33 (0)1 84 17 78 95
+33 (0)6 21 95 78 41
Rabah.hamiane@rhgroup.fr

M. Soufiane TAZARINE
+33 (0)6 02 14 03 54
Soufiane.tazarine@Secureland.fr

40 Rue de Châteaudun, 75009 Paris

https://secureland.fr