Catalogue de formations 2019

Vie privée,
Droit de la cybersécurité

Continuité d'activité

Cybersécurité organisationnelle

Cybersécurité technique

HS2
Hervé Schauer Sécurité

HS2
Hervé Schauer Sécurité

SOMMAIRE ET CALENDRIER

Vie privée, droit de la cybersécurité				
Réf.	Formations	Durée	Sessions	Pages
RGPD	RGPD/GDPR	2j	• 18 au 19 février 2019 • 10 au 11 octobre 2019	5-6
DPO*	Formation DPO	5 j	• 1er au 5 avril 2019 • 3 au 7 juin 2019 • 9 au 13 septembre 2019 • 25 au 29 novembre 2019	7-9
PIA*	PIA / ISO 29134	3 j	• 12 au 14 juin 2019 • 28 au 30 octobre 2019	10-12
SECUSANTE	Hébergement des données de santé et vie privée	3 j	• 13 au 15 mai 2019 • 21 au 23 octobre 2019	13-14
SECUCLOUD	Sécurité du cloud	2 j	• 27 au 28 juin 2019 • 19 au 20 décembre 2019	15-16
SECUDROIT	Droit de la cybersécurité	3 j	• 27 au 29 mai 2019 • 12 au 14 décembre 2019	17

Continuité d'activité				
Réf.	Formations	Durée	Sessions	Pages
RPCA*	Formation RPCA	5 j	• 15 au 19 avril 2019 • 30 septembre au 4 octobre 2019	18-19
ISO22LA*	ISO 22301 Lead Auditor	5 j	• 14 au 18 octobre 2019	20-21
ISO22LI*	ISO 22301 Lead Implementer	5 j	• 4 au 8 mars 2019 • 23 au 27 septembre 2019	22-23

Cybersécurité organisationnelle				
Réf.	Formations	Durée	Sessions	Pages
RSSI*	Formation RSSI	5 j	• 8 au 12 avril 2019 • 14 au 18 octobre 2019	24-26
CISSP*	Préparation au CISSP	5 j	• 11 au 15 février 2019 • 1er au 5 juillet 2019 • 25 au 29 novembre 2019	27-28
CISA	Préparation au CISA	5 j	• 25 au 29 mars 2019 • 25 au 29 novembre 2019	29-30
SECUHOMOL	Homologation de la SSI	1 j	• 10 mai 2019	31-32
SECUCRISE	Gestion de crise IT/SSI	1 J	• 20 juin 2019 • 5 décembre 2019	33-34
EBIOS2010*	EBIOS 2010 Risk Manager	3 J	• 18 au 20 mars 2019 • 21 au 23 octobre 2019	35-37

*Examen de certification HS2 inclus

*Examen de certification LSTI inclus

Cybersécurité organisationnelle (Suite)				
Réf.	Formations	Durée	Sessions	Pages
ESS27	Essentiels ISO27001 & ISO27002	2 J	• 17 au 18 juin 2019 • 2 au 3 décembre 2019	38-39
ISO27LA*	ISO 27001 Lead Auditor	5 J	• 21 au 25 janvier 2019 • 3 au 7 juin 2019 • 23 au 27 septembre 2019 • 18 au 22 novembre 2019	40-41
ISO27LI*	ISO 27001 Lead Implementer	5 J	• 20 au 24 mai 2019 • 1er au 5 juillet 2019 • 16 au 20 septembre 2019 • 4 au 8 novembre 2019 • 9 au 13 décembre 2019	42-43
IS027RM*	ISO 27005 Risk Manager	3 J	• 30 janvier au 1er février 2019 • 4 au 6 mars 2019 • 13 au 15 mai 2019 • 24 au 26 juin 2019 • 4 au 6 septembre 2019 • 12 au 14 novembre 2019 • 16 au 18 décembre 2019	44-45
EBIOS2018*	EBIOS 2018 Risk Manager		• 11 au 13 juin 2019 • 7 au 9 octobre 2019	46-47
ISO27004	ISO27004 / Indicateurs et tableaux de bord cybersécurité	1 J	• 19 juin 2019 • 4 décembre 2019	48
ISO27035	ISO27035 / Gestion des incidents de sécurité	1 J	• 21 juin 2019 • 6 décembre 2019	48

Cybersécurité technique				
Réf.	Formations	Durée	Sessions	Pages
ESSCYBER	Essentiels techniques de la cybersécurité	2 j	• 20 au 21 février 2019 • 5 au 6 septembre 2019	49-50
SECUCYBER*	Fondamentaux techniques de la cybersécurité	5 j	• 11 au 15 mars 2019 • 9 au 13 septembre 2019	51-52
SECUINDUS*	Cybersécurité des systèmes industriels	3 j	• 20 au 22 mai 2019 • 28 au 30 octobre 2019	53-54
DNSSEC	DNSSEC	2 J	• 2 au 3 décembre 2019	55-56
SECUPKI	Infrastructures de clés publiques	3 J	• 27 au 29 mai 2019	57-58
SECUPKIWIN	Infrastructures de clés publiques Windows	3 J	• 13 au 15 novembre 2019	59-60
SECUWEB*	Sécurité des serveurs et des applications Web	5 J	• 24 au 28 juin 2019 • 21 au 25 octobre 2019	61-62
SECUWIN*	Sécurisation des infrastructures Windows	5 J	• 16 au 20 décembre 2019	63-64

Cybersécurité technique (Suite)				
Réf.	Formations	Durée	Sessions	Pages
SECULIN*	Sécurité Linux	5 J	• 9 au 13 décembre 2019	65-66
SECUARCH*	Conception d'architectures sécurisées	3 J	• 14 au 16 octobre 2019	67-68
SECUBLUE*	Surveillance, détection et réponse aux incidents de sécurité	5 J	• 17 au 21 juin 2019 • 30 sept au 4 octobre 2019	69-70
FORENSIC1*	Analyse inforensique Windows	5 J	• 1er au 5 avril 2019 • 16 au 20 septembre 2019	71-72
FORENSIC2*	Analyse inforensique avancée	5 J	• 3 au 7 juin 2019	73-74
REVERSE1*	Rétroingénierie de logiciels malfaisants	5 J	• 4 au 8 novembre 2019	75-77
PENTEST1*	Tests d'intrusion	5 J	• 13 au 17 mai 2019 • 7 au 11 octobre 2019	78-80
PENTEST2*	Tests d'intrusion et développement d'exploits	5 J	• 18 au 22 novembre 2019	81
SECURSF	Sécurité des réseaux sans fil	2 j	• 5 au 6 décembre 2019	81
Nos intervenants				82-86
Bulletin d'inscription				87

*Examen de certification HS2 inclus
*Examen de certification LSTI inclus

Formation « RGPD / GDPR »

« GDPR / règlement européen sur la protection des données »

Réf : RGPD

Le règlement n° 2016/679, dit Règlement Général sur la Protection des Données (RGPD/GDPR), est le règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données au sein de l'Union européenne. Il introduit de nouvelles obligations pour les entreprises, et de nouveaux droits pour les individus. La présente formation s'efforce de proposer un plan de mise en conformité à mettre en œuvre dans votre organisme.

Objectifs

- Connaître le règlement et les évolutions apportées par celui-ci
- Maîtriser les implications opérationnelles du RGPD et sa mise en œuvre

Durée & horaires

- 2 jours soit 14 heures
- Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- DPO et futurs DPO
- Juristes
- Consultants en protection des données
- Directions
- Chef de projet
- RSSI, DSI

Pré-requis

- Aucun pré-requis n'est demandé cependant avoir des bases informatique ou juridiques est un plus.

Méthode pédagogique

- Cours magistral avec exemples et échanges interactifs.

Supports

- Support de cours au format papier en français
- Tous les documents nécessaires à la formation en français ou anglais dont le texte du règlement et certaines lignes directrices du CEPD
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **À l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PIA par HS2.**

Programme

Introduction

- Fondamentaux juridiques
- Historique et avenir du règlement européen
- Enjeux de la protection des données à caractère personnel (DCP)

Fondamentaux de la protection des données

- Champ d'application du règlement
- Principes fondamentaux
- Privacy by Design, Privacy by default
- Notions essentielles et acteurs
- Données à caractère personnel, traitement, etc.
- Autorités de protection des données
  - CNIL
    - Pouvoirs
    - Guichet unique
  - Contrôle
- Comité Européen à la Protection des Données (CEPD)
- DPO (Délégué à la Protection des Données)
- Responsabilités
  - Responsabilité du DPO
    - Responsabilité du sous-traitant
    - Responsabilité conjointe
    - Autres cas
    - Sanctions

Missions du responsable de traitement et du sous-traitant

- Désigner un DPO
- Réaliser une analyse d'impact sur les DCP (PIA : Privacy impact assessment)
- Consulter au préalable l'autorité de contrôle
- Tenir un registre des activités de traitements
- Veiller aux données particulières (données sensibles, judiciaires, protection des mineurs, santé, etc.)
- Assurer la sécurité des données
- Évaluation du niveau de sécurité
- Mesures techniques et organisationnelles
- Violations de données personnelles
- Gérer les droits des personnes concernées
- Transparence et information
- Droit d'accès
- Droit de rectification et effacement (droit à l'oubli numérique)
- Droit à la limitation du traitement
- Droit à la portabilité
- Droit d'opposition
- Veiller aux transferts de données en dehors de l'UE
- Se préparer à un contrôle
- Coopérer avec les autorités

Outils

- Certifications et labels
- Codes de conduite et chartes
- Check-list
- Veille
- Références

Formation « DPO »

Réf : DPO

La protection des données personnelles est devenue un enjeu majeur. La réglementation existante, fruit de 40 ans d'évolutions, s'incarne aujourd'hui sous la forme d'un texte majeur, que le grand public a découvert sous le nom de RGPD/GDPR. S'appliquant très largement, doté de sanctions très conséquentes, il impose de repenser le traitement des données personnelles dans les organisations : il remplace le formalisme préalable par une conformité à tout moment, assurée par des processus internes renforcés. Le CIL, remplacé par le Data Protection Officer, a un rôle tout particulier à jouer pour penser et organiser les procédures nécessaires au respect de ce texte. Cette formation a pour ambition d'apporter au DPO les connaissances nécessaires et la compréhension de ces exigences, et plus globalement à ceux qui mettront en œuvre la protection des données personnelles au sein des entités.

Objectifs

- **Connaître les missions du Data Protection Officer (DPO) ;**
- **Acquérir les compétences nécessaires à l'exercice de ces fonctions ;**
- **S'approprier les démarches et outils nécessaires au maniement des règles en matière de protection des données ;**
- **Apprendre à gérer l'organisation pour accompagner la mise à niveau et le maintien de performance de l'organisation en matière de respect de la vie privée ;**
- **Mettre en place un programme de mise en conformité et priorisation des actions par les risques.**

Durée & horaires

- **5 jours, soit 37h15 heures réparties en 35h00 de cours et 2h15 d'examen.**
- **Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants.**

Public visé

- **DPO (Délégué à la Protection des Données) ou futurs DPO, anciens CIL ;**
- **Personnes ayant à prendre en charge ou à mettre en œuvre la conformité de traitements de données personnelles à tous les niveaux, du management à l'opérationnel en passant par la conformité :**
  - **Personnes responsables de services opérationnels ;**
  - **DSI et leurs équipes ;**
  - **Responsables conformité, responsables des risques ;**
  - **Juristes et responsables juridiques.**
- **Consultants accompagnant à la mise en conformité RGPD ou assistant le DPO.**

Pré-requis

- **Une expérience professionnelle de deux ans est requise pour passer la certification.**

Méthode pédagogique

La méthode pédagogique se fonde sur les quatre axes suivants :

- **Un cours magistral sur le sujet, construit en partant des textes et documents officiels mais adapté de façon à rendre la matière compréhensible en langage courant, pour aboutir à des recommandations opérationnelles ;**
- **Enrichi de cas pratiques et d'exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous avocats spécialistes reconnus de ces questions ou implémenteurs des normes ;**
- **Un cours construit pour favoriser l'interactivité entre les participants, qui peuvent à tout moment poser des questions, et les intervenants ;**
- **Des exercices pratiques individuels effectués par les stagiaires, basés sur des études de cas, permettant de se confronter à des cas réels et de se préparer aux questions de l'examen.**

Supports

- **Support de cours au format papier en français ;**
- **Cahier d'exercices et corrections des exercices ;**
- **Tous les documents nécessaires à la formation en français ou anglais ;**
- **Feuilles d'émargement par demi-journée de formation et certificat individuel de formation attestant de la participation à l'ensemble de la formation.**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.**

Certification

- **Cette formation prépare à l'examen de certification "Délégué à la protection des données" (DPO).**

Programme

1. Vision globale : les principes de la protection des données à caractère personnel

- 1.1 Les sources
  - Histoire, évolution et mise en perspective des principes généraux applicables (loi Informatique et Libertés textes européens, genèse RGPD, droit comparé US) ;
  - Changement de paradigme :
    - du contrôle a priori au contrôle a posteriori ;
    - exception : la survivance de formalités préalables dans le domaine de la santé, dans certains cas.

- 1.2 Les définitions essentielles
  - De quoi parle-t-on ? Notions de donnée à caractère personnel, traitement, etc.
  - De quel champ d'application parle-t-on ?

- 1.3 Les grands principes
  - L'architecture complexe du RGPD
  - Les principes essentiels du RGPD
  - L'accountability et la traçabilité : le changement de paradigme
  - La sécurité
  - Les droits des personnes concernées :

- 1.4 Les acteurs

- du CIL au DPO : désignation, profil (qualités professionnelles/personnelles), fonction (rattachement, moyens, indépendance, conflits d'intérêts, etc.), missions (information, contrôle, coopération, etc.) ;
- la CNIL (statut, fonctionnement, missions, pouvoirs, etc.) ;
- le CEPD ;
- les organismes de certification ;
- les voies de recours : contre la CNIL, contre un responsable de traitement ou contre un sous-traitant.

2 Vision opérationnelle : mettre en œuvre la conformité

- 2.1 Nommer un DPO dans l'entreprise
  - Mettre en place une organisation de gestion de projet :
  - Ou gérer les organisations existantes, en les faisant évoluer, au besoin.
- 2.2 Mettre en place et/ou gérer la Gouvernance de protection des données
  - Etre nommé DPO
  - Faire un état des lieux de la situation
- 2.3 Recenser parallèlement les outils et livrables de gouvernance
  - Recenser les outils d'aide à la conformité déjà disponibles
  - Constituer ou mettre à jour un dossier des outils d'aide à la conformité
  - Établir une liste des livrables attendus
  - Les sources d'information disponibles
  - Recenser les codes de conduite, labels et certifications obtenus par l'entreprise ou intéressants, ainsi que les formations en place et les compétences déjà acquises dans la société
- 2.4 Connaître son environnement et son écosystème
  - Suivant la situation, de la réalisation d'un registre des traitements à l'état des lieux plus poussé des livrables passés (maturité de la conformité de l'entreprise, etc.)
  - Cartographier les données avec l'aide du RSSI et des Services
- 2.5 Prioriser les actions sur la base de l'état des lieux
  - Tirer les conséquences des qualifications juridiques établies
  - Clarifier la situation contractuelle de l'entreprise
- 2.6 Analyser les impacts de vos traitements sur les droits et libertés fondamentales des personnes concernées et savoir notifier
  - Piloter les traitements par le risque
  - Réaliser les analyses de risque sur la sécurité des données (en parallèle)
  - Anticiper les incidents de sécurité
- 2.7 Constituer son dossier de conformité (Accountability) et déployer une culture de « Protection des données » dans l'organisation
  - Constituer son dossier de conformité (Accountability) ;
  - Déployer une culture de « Protection des données » dans l'entreprise (Privacy by design et by Default, sensibilisation, etc.) ;
- 2.8 Se préparer à un contrôle de la CNIL et intégrer les risques juridiques
  - Se préparer à un contrôle de la CNIL
  - Intégrer les risques juridiques (voies de recours, moyens de défense, sanctions)

Examen de certification (conçu, surveillé et corrigé par LSTI).

Formation « PIA »

« Etude d'impact sur la vie privée : Quand, pourquoi, comment ? » / #EIVP #DPIA

Réf : PIA

À travers le règlement européen de protection des personnes physiques à l'égard de leurs données à caractère personnel (RGPD), s'est opéré un changement profond de paradigme. C'est toute la gouvernance des données qui se voit repenser au sein des organismes. Les responsables de traitement se retrouvent non seulement responsables de protéger ces données en adoptant des mesures adaptées mais également en charge de le prouver. L'incidence la plus directe est donc la place prépondérante que les organisations doivent donner à la gestion des risques mais également au contrôle interne. En effet, il leur revient désormais d'évaluer elles-mêmes la part de risques sur la vie privée des personnes dont elles collectent, consultent, manipulent, stockent ou encore transfèrent les données. Que les organisations soient plus ou moins favorables à cette démarche, il n'en demeure pas moins qu'elle a de fortes implications non seulement pour les personnes concernées et pour l'organisation elle-même. Reste que cela suppose qu'elle soit comprise, intégrée et réalisable par tous.

La formation ici proposée aura comme objectif fondamental de donner les clefs aux acteurs concernés pour instaurer ce changement culturel majeur dans l'organisation tant il va peser sur le futur non seulement de la responsabilité sociale de l'entreprise mais également sur son innovation et les valeurs véhiculées par elle.

La formation insistera particulièrement sur :

- **La gouvernance de la gestion des données et in fine, de la gestion des risques sur la vie privée**
- **Les enjeux de la maîtrise de son environnement, pour garantir la solidité de l'étude d'impact**
- **La nécessité de l'intégrer à tous les processus de l'entreprise comme n'importe quel autre et ainsi, d'en assurer sa prise en compte par défaut et dès le début d'un projet**

Objectifs

- **Être capable de savoir quand et pourquoi déclencher une EIVP / DPIA**
- **Déterminer un processus et une méthodologie de faisabilité d'une EIVP**
- **Connaître les prérequis indispensables à l'EIVP**

Durée & horaires

- **3 jours soit 21 heures**
- **Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Responsable de traitement / Sous-traitant**
- **Directions métiers**
- **Direction Générale**
- **DPO**
- **Comité pilotage RGPD (Juriste, Responsable marketing,…)**

Pré-requis

- **Aucun pré-requis n'est demandé. Le suivi d'une formation sur le RGPD est un avantage.**

Méthode pédagogique

La formation en présentiel, ici proposée, repose sur 3 piliers qui en font son succès :

- **Le Savoir**
- **L'échange**
- **La mise en situation**

Les participants reçoivent la matière théorique, technique et pratique pour s'assurer la maîtrise du sujet. Le savoir transmis est reconnu et basé sur des référentiels éprouvés (Guides de la CNIL, Guidelines du G29/CEPD, Lois et règlements en vigueur, Norme ISO 29134. Les sessions sont basées sur l'interactivité pour qu'au fur et à mesure les participants puissent non seulement poser leurs questions et ainsi dissiper tout doute sur les points abordés, mais également pour partager leurs retours d'expérience. Enfin, les participants sont régulièrement mis en situation pour se tester.

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PIA par HS2.**

Programme

Introduction

- Cadre légal et réglementaire
- La protection des personnes physiques à l'égard de leurs données à caractère personnel : Nouvelle contrainte ou nouvelle économie ?
- La gestion des risques au cœur de la protection des données à caractère personnel

Éléments généraux sur l'EIVP (RGPD)

- Qui déclenche une EIVP ?
- Quand et pourquoi ? (Facteurs déclencheurs)
- Eléments obligatoires d'une EIVP

Questions essentielles

- Qu'est-ce qu'un risque ? un risque élevé ?
- Qu'est qu'un traitement ? un traitement à grand échelle ? un suivi régulier ?
- Analyse de risques sur les données et Analyse des risques sur les droits et libertés fondamentales des personnes : Quelles différences et dans quel ordre ?

Méthodologie

- Déclenchement du PIA (à quel moment ?)
- Les indispensables
  - Le Registre des traitements
  - Modélisation des processus métiers
  - Cartographie d'acteurs

- Périmètre
- Parties prenantes
- Référentiels :
  - Guides CNIL
  - G29
  - Norme ISO 29134
- Présentation de l'outil PIA élaboré par la CNIL (gratuit)
- Évaluation des risques
- Documentations associées
- Suites du PIA et cycle d'amélioration continue

L'intégralité de la formation est ponctuée de quizz et d'exercices de mise en pratique.

Formation « Hébergement des données de santé et vie privée »

Réf : SECUSANTE

Le secteur de la santé et du social est encadré par des règles spécifiques c'est pourquoi HS2 propose une formation dédiée pour couvrir ce domaine.

Objectifs

- **Apprendre les exigences juridiques et de sécurité en matière de :**
  - **Protection des données personnelles de santé, y compris le RGPD et la loi Informatique & Libertés 3 dans le cadre de la santé**
  - **Hébergement des données de santé (certification HDS)**
  - **Interopérabilité des systèmes d'information de santé (CI-SIS)**
  - **Sécurité des systèmes d'information de santé (PGSSI-S, CPS, RGS, LPM, NIS)**

Durée & Horaires

- **3 jours soit 21 heures**
- **9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participants

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Personnes des secteurs santé et social :**
  - **RSSI**
  - **DPO**
  - **Juristes**
  - **Toute personne confrontée à la gestion d'un système d'information de santé.**

Pré-requis

- **Avoir une culture générale en sécurité des systèmes d'information ou en droit est un plus mais n'est pas imposé.**
- **Pour les participants souhaitant apprendre la certification HDS, il convient d'avoir suivi la formation ISO27001 Lead Implementer avant la formation SECUSANTE.**

Méthode pédagogique

- **Cours magistral avec échanges interactifs**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Programme

Module 1 : Présentation du contexte

- Cadre légal et normatif
- Notions fondamentales
- Données de santé, dossier médical partagé, systèmes d'information, etc.
- Principaux acteurs
  - Patient, Professionnel de santé et médico-social, Établissements de santé, Hébergeur, ASIP-santé, CNIL, etc.

Module 2 : Droits des patients et secret

- Droits des patients
  - Confidentialité de leurs données de santé, information et accès aux données, droit de rectification et d'opposition, etc.
- Secret
  - Secret professionnel, secret médical, secret partagé

Module 3 : Gestion des données personnelles de santé

- Licéité des traitements de données personnelles
- Recueil des données de santé
- Formalités préalables, PIA
- Élaboration et tenue du registre des activités de traitement
- Conservation, suppression, anonymisation et archivage des données
- Transferts internationaux de données
- Gestion des droits des personnes concernées

Module 4 : Sécurité du système d'information de santé

- Obligations légales de sécurité de données et systèmes d'information de santé
- Enjeux de la sécurité du SI-S : Confidentialité, Intégrité, Disponibilité, Traçabilité et imputabilité
- PGSSI-S

Module 5 : Interopérabilité du système d'information de santé

- Obligation légale d'interopérabilité
- Présentation du cadre d'interopérabilité des systèmes d'information de santé

Module 6 : Hébergement des données de santé

- Exigences légales en matière d'hébergement
- Certification HDS
- Passage de l'agrément à la certification
- Médecin de l'hébergeur de la procédure d'agrément à la certification

Module 7 : SMSI

- Présentation de la norme ISO 27001
- Organisation de la sécurité
  - Rôles et responsabilités, Politique de sécurité, SMSI
  - Médecin hébergeur
  - Responsabilités vis-à-vis du CSP
- Gestion des risques
  - Appréciation des risques
  - Plan de traitement des risques
  - Déclaration d'applicabilité étendue
  - ISO27018
  - Exigences HDS
- Processus de certification
- Mesures de sécurité opérationnelles
  - Gestion des accès, identification, authentification
  - Classification et chiffrement
  - Architecture réseau et applicative
  - Sécurité des échanges
  - Durcissement des systèmes
  - Objets connectés et accès distants
  - Cycle de vie et obsolescence des systèmes
  - Sauvegarde et archivage
  - Auditabilité (Traçabilité, Imputabilité)
- Gestion des incidents dans les contextes des données de santé
  - Notifications aux autorités
- Gestion de la continuité d'activité

Formation « Sécurité du cloud computing »

Réf : SECUCLOUD

Le cloud computing s'est imposé comme un des dernières évolutions majeures de l'informatique et quasiment aucune organisation ni aucun métier ne peut y échapper. Si la gestion des prestataires en général a toujours été un enjeu depuis les premières infogérances, avec le cloud la gestion de la sécurité de ses fournisseurs de cloud vient immédiatement à l'esprit. Les risques sont à la fois techniques, organisationnels et juridiques. Les solutions pour les maîtriser sont en premier lieu juridiques, et cette formation vise à permettre aux consommateurs d'en prendre conscience et de savoir s'en servir.

Objectifs

- Exposer, analyser et hiérarchiser les risques liés au cloud computing
- Proposer des solutions et des bonnes pratiques
- Permettre une maîtrise des clauses contractuelles d'un contrat de cloud

Durée & horaires

- 2 jours soit 14 heures
- Horaires : de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Toute personne qui est ou envisage de devenir clients de solutions de cloud computing
- DSI, RSSI, chef de projet, responsable opérationnel
- Responsable métier, gestionnaire de contrats, gestionnaire de risque
- Consultant en sécurité et en infonuagique
- Responsable juridique, juriste

Pré-requis

- Cette formation ne nécessite pas de pré-requis particulier.

Méthode pédagogique

- Cours magistral avec de nombreux exemples anonymisés

Supports

- Support de cours au format papier en français
- Tous les documents nécessaires à la formation en français ou anglais
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- Cette formation n'est pas certifiante.

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Programme

Rappels sur le cloud

Rappel sur la cybersécurité

- Risque et gestion des risques
- Menaces et vulnérabilités
- Disponibilité
- Confidentialité
- Gestion des incidents

Risques avec le cloud

- Enfermement
- Perte de gouvernance
- Gestion du projet
- Plan d'Assurance Sécurité
- Suivi de la sécurité

Contractualiser les exigences de sécurité

- Sources du droit
- Généralités sur les contrats
- Preuve

Contenu du contrat de cloud

- Comité de suivi sécurité
- Envoi des données
- Obligations du client
- Prérogatives du prestataire
- Données personnelles et les nouvelles obligations issues du RGPD
- Obligations générales de sécurité
- Confidentialité
- Convention de service attendu
- Développements applicatifs
- Audits de sécurité
- Réversibilité
- Résiliation
- Effacement des données
- Responsabilité contractuelle

Cloud et charte informatique

- La notification d'une violation de données personnelles en vertu du RGPD comment en pratique concilier l'enquête interne avec les délais imposés et la notification d'un incident à l'ANSSI

Comptes à privilèges

Panorama des normes et référentiels

- ISO27001/ISO27002
- SOC1/SOC2
- ISO27017
- ISO27018
- ISO27552

HS2 - SASU au capital de 400 000 euros – Siège social : 10 rue des Poissonniers – 92200 Neuilly-Sur-Seine – France – Code APE : 8559A
Siret : 84050153000017 - Déclaration d'activité enregistrée sous le numéro 11922236092 auprès du préfet de région d'Ile-de-France

Plan de formation bientôt disponible

Réf : SECUDROIT Formation « Droit de la cybersécurité »

- **Objectif :** La maîtrise du droit à destination des informaticiens.

Formation « RPCA »

Réf : RPCA

Objectifs

- Comprendre les fondamentaux de la Continuité d'Activité,
- Prendre en compte le contexte réglementaire et juridique,
- Connaître l'état du marché de la continuité (aspect techniques),
- Apprécier les enjeux et les risques métiers,
- Formaliser un PCA efficient,
- Évaluer le fonctionnement de mon PCA,
- Gérer une crise,
- Mettre en œuvre des stratégies de prise de fonction.

Durée & horaires

- 5 jours soit 35 heures,
- Du lundi au jeudi de 9h30 à 12h et de 13h30 à 17h30/18h00,
- Le vendredi de 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Toute personne amenée à exercer la fonction de responsable du Plan de continuité d'activité :
  - RPCA,
  - Futur RPCA,
  - RSSI,
  - Assistant DSI
  - Ingénieurs sécurité assistant un RPCA,
  - Responsables de production.
- Les techniciens devenus RPCA, souhaitant obtenir une culture de management.
- Les managers confirmés manquant de la culture technique de base en matière de continuité d'activité ou ne connaissant pas les acteurs du marché.
- Toute personne amenée à assurer une fonction de correspondant local continuité d'activité ou une fonction similaire.

Pré-requis

- Aucun prérequis n'est demandé. Toutefois avoir une expérience du contexte informatique et en gestion de projet est un plus.

Méthode pédagogique

La méthode pédagogique se base sur les 4 points suivants :

- Cours orientés sur la mise en œuvre pratique de processus de continuité d'activité dans le cadre de la norme ISO 22301,
- Exercices de contrôles de connaissance,
- Exercices pratiques individuels et collectifs illustrant les notions importantes explicitées durant le cours,
- Exemples concrets reprenant les parties importantes du cours, basés sur le retour d'expérience des consultants formateurs.

Supports

- **Support de cours au format papier et en français,**
- **Cahier d'exercices et corrections.**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. La réussite à l'examen donne droit à la certification RPCA par HS2.**

Programme

Introduction - Fondamentaux de la continuité d'activité

- Interactions : RSSI, RM, Production, Direction, métiers, Services Généraux, Conformité, Juridique, RH, etc.
- Stratégies de prise de fonction du RPCA,
- Présentation de la terminologie.

Contexte réglementaire et juridique

- Panorama des référentiels du marché (lois, règlement, normes et bonnes pratiques),
- Normalisation ISO 22300 et 27000,
- Informatique et libertés, GDPR.

Aspects techniques de la continuité

- Sauvegarde & restauration,
- Réplication ou redondance,
- Réseau et télécoms.

Apprécier les enjeux et les risques métiers

- Appréciation des risques en continuité d'activité,
- Processus critiques : Bilan d'Impact sur l'Activité (BIA)

Acteurs du marché de la continuité

- Gestion des relations avec les partenaires,
- Externaliser vers un prestataire,
- Comment choisir ?

Formaliser un PCA efficient

- Projet PCA (prérequis, gouvernance, délais, livrables, etc.),
- PGC : Plan Gestion de Crise,
- PCOM : Plan de Communication (interne et externe),
- PRM : Plan de reprise métier,
- PCIT : Plan de Continuité Informatique et Télécoms,
- PRN : Plan de Retour à la Normale.
- Mon PCA fonctionne-t-il ?
- Les exercices et tests,
- L'importance du rôle d'observateur,
- Audit du PCA,
- Maintien en Condition Opérationnelle (MCO),
- Outils de gouvernance, gestion, pilotage du PCA.

Gérer une crise

- Activer tout ou partie du PCA,
- Communiquer pendant la crise,
- Assurer le retour à la normale,
- Intégrer les retours d'expérience (RETEX).

Témoignage d'un RPCA

Examen

Formation « ISO 22301 Lead Auditor »

Réf : ISO22LA

Objectifs

- Comprendre le fonctionnement d'un SMCA selon l'ISO 22301,
- Comprendre le déroulement, les spécificités et les exigences d'un audit ISO 22301,
- Acquérir les compétences pour réaliser un audit interne ou un audit de certification ISO22301 en fonction de la norme ISO19011,
- Gérer une équipe d'auditeurs de SMCA,
- Comprendre la mise en œuvre d'un processus de certification ISO22301,
- Devenir auditeur ISO 22301 certifié.

Durée & horaires

- 5 jours soit 40 heures réparties en 31h30 de cours, 5h00 de travail individuel sur les exercices le soir et 3h30 d'examen.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- RPCA
- Consultants – Auditeurs
- Chefs de Projets
- Responsables de la conformité
- Qualiticiens
- Contrôles internes

Pré-requis

- Formation initiale minimum du second cycle ou justifier d'une expérience professionnelle d'au moins 5 ans
- Connaître les principes fondamentaux de la Continuité d'Activité
- RPCA

Méthode pédagogique

La méthode pédagogique se base sur les 6 points suivants :

- Cours magistral basé sur les normes ISO 19001, ISO 22301, ISO 22313, ISO 27031, ISO 31000,
- Exercices pratiques individuels et collectifs basés sur une étude de cas,
- Exercices de contrôles de connaissance,
- Exercices pratiques individuels et collectifs illustrant les notions importantes explicitées durant le cours,
- Exemples concrets reprenant les parties importantes du cours, basés sur le retour d'expérience des consultants formateurs,
- Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.

Supports

- **Support de cours au format papier et en français,**
- **Cahier d'exercices et corrections.**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation est suivie d'un examen LSTI 22301 Lead Auditor. Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

Reconnaissance internationale

- **La formation HS2 et l'examen LSTI sont reconnus internationalement au même niveau et au même titre que d'autres formations et examens disponibles sur le marché.**

Programme

Accueil des participants

- Présentation générale du cours
- Introduction aux systèmes de management
- Principes fondamentaux de la continuité d'activité.

Présentation détaillée de la norme ISO22301

- Notions de Système de Management de la Continuité d'Activité (SMCA)
- Modèle PDCA (Plan – Do – Check - Act)
- Les exigences :
  - Comprendre l'organisation et son contexte,
  - Engagement de la Direction,
  - Analyse des impacts Métier (BIA) et appréciation des risques
  - Définir les stratégies de continuité
  - Développer et mettre en œuvre les plans et procédures de continuité d'activité
  - Tests et exercices
  - Surveillance et réexamen du SMCA
  - Amélioration continue
  - Les enregistrements

Panorama des normes ISO complémentaires :

- ISO 19011
- ISO 22313
- ISO 27031
- ISO 31000
- Présentation de la continuité d'activité
- Procédures de continuité d'activité
- Exercices et tests
- Retours d'expérience sur l'audit de Plans de Continuité d'Activité (PCA)

Processus de certification ISO 23201

Présentation de la démarche d'un SMCA basé sur l'ISO 19011

- Norme ISO 19011
- Audit d'un SMCA
- Règlement de certification
- Exemples pratiques

Techniques de conduite d'entretien

Exercices de préparation à l'examen

Examen conçu, surveillé et corrigé par LSTI

Formation « ISO 22301 Lead Implementer »

Réf : ISO22LI

Objectifs

- Comprendre la mise en œuvre d'un SMCA suivant l'ISO 22301,
- Apprendre les concepts, approches, méthodes et techniques requises pour gérer un SMCA,
- Acquérir les compétences nécessaires pour accompagner et conseiller une organisation dans l'implémentation et la gestion d'un SMCA conformément à l'ISO 22301,
- Devenir un implémenteur certifié ISO 22301

Durée & horaires

- 5 jours soit 40 heures réparties en 31h30 de cours, 5h00 de travail individuel sur les exercices le soir et 3h30 d'examen.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Responsables en charge de la Continuité d'Activité – RPCA,
- Secrétaires généraux,
- Responsables de directions opérationnelles,
- Gestionnaires de risque,
- Chefs de projet,
- Consultants.

Pré-requis

- Formation initiale minimum du second cycle ou justifier d'une expérience professionnelle d'au moins 5 ans,
- Connaître les principes fondamentaux de la Continuité d'Activité.

Méthode pédagogique

La méthode pédagogique se base sur les 7 points suivants :

- Cours magistral basé sur les normes ISO 22301, ISO 22313, ISO 27031, ISO 31000,
- Exercices pratiques individuels et collectifs basés sur une étude de cas,
- Exercices de contrôles de connaissance,
- Exercices pratiques individuels et collectifs illustrant les notions importantes explicitées durant le cours,
- Exemples concrets reprenant les parties importantes du cours, basés sur le retour d'expérience des consultants formateurs
- Quiz pour préparation à l'examen,
- Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session

Supports

- Support de cours au format papier et en français,
- Cahier d'exercices et corrections.

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation est suivie d'un examen de certification à la norme 22301 LSTI (ISO 22301 Lead Implementer). Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

Reconnaissance internationale

- **La formation HS2 et l'examen LSTI sont reconnus internationalement au même niveau et au même titre que d'autres formations et examens disponibles sur le marché.**

Programme

Introduction

- Introduction des systèmes de management,
- Principes fondamentaux de la continuité d'activité.

Présentation détaillée de la norme ISO22301

- Notions de Système de Management de la Continuité d'activité (SMCA),
- Modèle PDCA (Plan – Do – Check - Act),
- Les processus du SMCA
  - Direction,
  - Pilotage du SMCA,
  - Gestion de la conformité,
  - Gestion des impacts sur l'activité,
  - Gestion des risques,
  - Gestion des stratégies de continuité,
  - Gestion des incidents perturbateurs
  - Documentation et enregistrements,
  - Ressources, compétences et sensibilisation,
  - Surveillance et revue,
  - Gestion des actions correctives.

Panorama des normes ISO complémentaires : ISO 22313, ISO 27031, ISO 31000

Présentation des processus de continuité d'activité

- Analyse des impacts sur l'activité ou Business Impact Analysis (BIA),
- Appréciation du risque pour un SMCA sur la base de l'ISO 31000,
- Procédures de continuité d'activité,
- Exercices et tests, Retours d'expérience sur l'implémentation de Plans de Continuité d'Activité (PCA).

Mener un projet d'implémentation d'un SMCA

Convaincre la Direction

- Les étapes du projet
- Les acteurs
- Les facteurs clés de succès
- Les risques et opportunités

Intégration de l'ISO 27031 dans le SMCA

Processus de certification ISO 22301

Gestion des indicateurs

Préparation de l'examen

Examen conçu, surveillé et corrigé par LSTI

Formation « RSSI »

Réf : RSSI

La fonction de "RSSI" est un métier transverse et multi-facettes. La formation RSSI HS2 apporte au nouveau RSSI un panorama complet des fonctions du RSSI et des attentes des organisations sur le rôle du RSSI, les connaissances indispensables à sa prise de fonction du RSSI et un retour d'expérience sur les chantiers et la démarche à mettre en œuvre dans le rôle sont détaillés par d'anciens RSSI et des consultants expérimentés.

Objectifs

- **Acquérir les compétences indispensables à l'exercice de la fonction responsable de la sécurité des systèmes d'information, à savoir :**
  - **Bases de la cybersécurité**
  - **Enjeux de la SSI au sein des organisations**
  - **Connaissances techniques de base**
  - **Sécurité organisationnelle et normes ISO27001**
  - **Méthodes d'appréciation des risques**
  - **Bases juridiques**
  - **Stratégies de prise de fonction**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Toute personne amenée à exercer la fonction de responsable sécurité des systèmes d'information : RSSI, futurs RSSI, ingénieurs sécurité assistant un RSSI, responsables sécurité à la production**
- **Toute personne amenée à assurer une fonction de correspondant local de sécurité des systèmes d'information ou une fonction similaire.**
- **Techniciens devenus RSSI, souhaitant obtenir une culture de management.**
- **Managers confirmés manquant de la culture technique de base en matière de sécurité des SI ou ne connaissant pas les acteurs du marché**
- **DSI ou auditeurs en systèmes d'information souhaitant connaître les contours de la fonction et les rôles du RSSI**

Pré-requis

- **Il est préférable d'avoir une expérience au sein d'une direction informatique en tant qu'informaticien ou bonne culture générale des systèmes d'information.**
- **Avoir des notions de base en sécurité appliquées au système d'information constitue un plus.**

Méthode pédagogique

- **Cours magistral dispensé à chaque fois par des experts de chaque module**
- **Dans les modules "gestion des risques" et "juridique", des exercices de contrôle des connaissances et dans les autres modules, des démonstrations ou de nombreux exemples pratiques basés sur les retours d'expérience des instructeurs et ceux de leurs clients**
- **Forte interaction entre les formateurs et les stagiaires permettant de rendre les échanges davantage concrets, en corrélation avec les attentes des stagiaires**
- **Animation par un RSSI en activité, présentant sa stratégie de prise de fonction et un retour d'expérience sur des cas concrets et détaillés de projets sécurité menés dans son organisation.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification RSSI par HS2.**

Programme

Accueil des participants et tour de table

Enjeux et organisation de la sécurité (environ 1,5 jour)

- Critères de sécurité (disponibilité, intégrité, confidentialité, auditabilité)
- Fonction de RSSI, rôles du RSSI
- Environnement du RSSI (production, direction, métiers, conformité, juridique, etc)
- Panorama des référentiels
- Politiques de sécurité (globales, détaillées, sectorielles, géographiques, etc)
- Conformité
- Indicateurs et tableaux de bord SSI (stratégique, tactique, opérationnel)
- Gestion des incidents de sécurité
- Sensibilisation (collaborateurs, informaticiens, direction)
- Ecosystème de la SSI (associations, conférences, etc)

Aspects techniques de la sécurité (environ 1 jour)

- Sécurité du système d'exploitation
- Minimisation et durcissement des systèmes
- Contrôle d'accès
- Gestion des utilisateurs
- Gestion des moyens d'authentification
- Sécurité des applications (sessions, injection SQL, XSS)
- Validation des données (en entrées, traitées, en sortie)
- Développement et environnements de test
- Accès au code source
- Sécurité réseau (routeurs, firewalls)
- Cloisonnement et contrôle d'accès

- Messagerie
- Sécurité du poste de travail, mobilité, télétravail
- Gestion des opérations, gestion des vulnérabilités techniques
- Surveillance, sauvegardes
- Conformité technique
- Typologie des tests d'intrusion et audits de sécurité
- Protection des outils d'audits et des données d'audits

Système de Management de la Sécurité de l'Information (normes ISO 27001) (environ 1/2 journée)

- Bases sur les systèmes de management (définitions, modèle PDCA, propriétés et objectifs)
- Panorama des normes ISO 270xx
- Bases sur ISO 27001 et ISO 27002 et utilisations possibles
- Domaine d'application
- Engagement de la direction
- Surveillance (réexamen régulier, audit interne, revue de direction)
- Amélioration continue

Audit (environ 1/2 journée)

- Typologie des audits (technique, organisationnel, de conformité, de certification)
- Conséquences (inconvénients et objectifs)
- Vocabulaire (basé sur ISO 19011)
- Préparation à l'audit
- Considérations pratiques (formation, communication, intendance, audit à blanc, préparation)
- Démarche d'audit (ISO 19011)
- Avant l'audit, pendant l'audit, après l'audit
- Livrable
- Actions correctives entreprises et suivi
- Réception des auditeurs (maison-mère, ISO27001/HDS, ISAE3401/SOC2, Cour des Comptes, Commission bancaire, etc.)

Gestion de risques (environ 1/2 journée)

- Méthodologies d'appréciation des risques (ISO27001, EBIOS, Mehari)
- Vocabulaire
- Identification et valorisation d'actifs
- Menace, source des risques, vulnérabilités
- Analyse de risque
- Estimation des risques
- Vraisemblance et conséquences d'un risque
- Evaluation du risque
- Traitement des risques (réduction, partage, maintien, refus)
- Notion de risque résiduel
- Acceptation du risque

Aspects juridiques de la SSI (environ 1/2 journée)

- RGPD et Informatique et libertés
- Communications électroniques
- Conservation des traces
- Contrôle des salariés
- Atteintes aux STAD
- Charte informatique
- Comptes à privilège
- Gestion des relations avec les partenaires (infogérance, infonuagique, prestataires en sécurité)

Témoignage d'un RSSI (après l'examen la dernière 1/2 journée)
Examen (1h30)

« Préparation au CISSP »

Réf : CISSP

Le CISSP (Certified Information Systems Security Professional) est la certification en sécurité des systèmes d'information proposée depuis 1989 par l'(ISC)² (International Information Systems Security Certification Consortium). C'est l'une des certifications professionnelles les plus reconnues dans le monde. Elle s'appuie sur le CBK (Common Body of Knowledge), tronc commun de connaissances composé de 8 domaines couvrant tous les aspects de la sécurité des systèmes d'information.

La formation CISSP d'HS2 est au format "boot camp" : c'est un entrainement intensif dont l'objectif est de préparer à l'examen de certification CISSP de l'ISC². Afin de tirer un maximum de bénéfices de cette formation, les participants devront être dans la phase finale de leur préparation, le boot camp étant la dernière ligne droite avant la certification. Ils devront notamment avoir lu le CBK officiel ("Official ISC² Guide to the CISSP Exam" (ISC)² Press). La formation s'articule autour des 8 domaines du CBK : pour chacun, les concepts fondamentaux sont d'abord brièvement expliqués, puis les stagiaires sont soumis à des séries de questions auxquelles ils répondent de façon anonyme à l'aide d'un boîtier électronique individuel. Les résultats de chaque question sont ensuite analysés avec les formateurs. Cette méthode permet au stagiaire de "s'imprégner" de l'esprit CISSP et de maximiser ses chances de réussite.

Objectifs

- **Préparer sereinement les participants à l'examen de certification CISSP de l'ISC²**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au vendredi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Professionnels de la sécurité souhaitant valoriser leurs expériences**
- **Personnes souhaitant acquérir une certification en sécurité reconnue au niveau mondial**

Pré-requis

- **Avoir lu le CBK ("Official ISC² Guide to the CISSP Exam - (ISC)² Press).**

Méthode pédagogique

- **Rappels des points clés à connaitre dans chacun des domaines**
- **Séries de questions ciblées permettant de valider les connaissances**
- **Séries de questions aléatoires visant à mettre les stagiaires en conditions d'examen**

Supports

- **Support de cours au format papier en anglais**
- **Diapositives en anglais à l'écran, avec explications en français par les formateurs**
- **Livre CBK officiel de l'(ISC)² envoyé sur demande, uniquement après réception des documents de confirmation d'inscription.**
- **Livre de révision officiel de l'(ISC)² comprenant :**
  - **Des fiches de révision**
  - **Des questions d'entrainement**
  - **Un examen blanc complet**
- **Questions d'entrainement en anglais**
- **Boîtier électronique individuel pour répondre aux questions**
- **Certificat (ISC)² attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Examen de certification CISSP de l'(ISC)² à passer dans un centre PearsonVue (www.pearsonvue.com). HS2 est partenaire officiel de l'(ISC)² en France et au Luxembourg et est autorisée à vendre l'examen CISSP dans ces deux pays.**

Programme

Lundi

- **Matin :** Accueil et introduction au CISSP
- **Après-midi :** Information Security & Risk Management

Mardi

- **Matin :** Assets Security
- **Après-midi :** Security Architecture & Engineering

Mercredi

- **Matin :** Identity & Access Management
- **Après-midi :** Security Operations

Jeudi

- **Matin :** Security Assessment and Testing
- **Après-midi :** Software Development Security

Vendredi

- **Matin :** Software Development Security + Communication & Network Security
- **Après-midi :** Communication & Network Security

« Préparation au CISA »

Réf : CISA

Le CISA (Certified Information Systems Auditor) est la certification internationale des auditeurs des systèmes d'information. Cette certification est régulièrement exigée auprès des auditeurs informatiques et sécurité. Elle est éditée par l'association internationale des auditeurs informatiques ISACA (http://www.isaca.org/).

La formation CISA d'HS2 est au format "boot camp" : c'est un entraînement intensif dont l'objectif est de réussir l'examen. La formation s'articule autour des thèmes du CISA : la pratique de l'audit SI; la gouvernance des SI; l'acquisition et l'implantation des SI; l'exploitation et la gestion des SI; l'audit de l'informatique et des opérations, l'audit des infrastructures et des réseaux, la sécurité des actifs informationnels, et le contexte de l'examen (QCM, typologie de questions).

Objectifs

- **Préparer sereinement les participants à l'examen de certification CISA de l'ISACA**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au vendredi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Consultants en organisation, consultants en systèmes d'information, consultants en sécurité.**
- **Auditeurs**
- **Informaticiens**
- **Responsables informatiques**
- **Chefs de projets, urbanistes, managers**

Pré-requis

- **Connaissance générale de l'informatique, de ses modes d'organisation et de son fonctionnement.**
- **Connaissance des principes généraux des processus SI et des principes de base de la technologie des SI et des réseaux.**
- **Avoir lu le CRM (CISA Review Manuel" ou "Manuel de préparation au CISA" officiel de l'ISACA) est un plus**

Méthode pédagogique

- **Cours magistraux par des consultants certifiés CISA**
- **Exercices pratiques par des questions à l'issue de chaque exposé**
- **Examen blanc de 100 questions et explications à chaque mauvaise réponse**

Supports

- **Support de cours en français au format papier**
- **Livre officiel de l'ISACA CRM "Cisa Review Manual" en anglais ou "Manuel de préparation au CISA" en français envoyé sur demande, uniquement après réception des documents de confirmation d'inscription.**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Examen de certification CISA de l'ISACA à passer dans un centre PearsonVue (www.pearsonvue.com). L'examen est disponible uniquement auprès de l'ISACA, il n'existe aucun revendeur autorisé.**

Programme

Le stage est organisé sur 4 journées de révision des 5 thématiques de la certification CISA associées à des séries de questions illustratives.

Les 5 domaines abordés (repris dans le CRM et le support de cours) :

- **Le processus d'audit des SI :** méthodologie d'audit, normes, référentiels, la réalisation de l'audit, les techniques d'auto-évaluation.
- **La gouvernance et la gestion des SI :** Pratique de stratégie et de gouvernance SI, politiques et procédures, pratique de la gestion des SI, organisation et comitologie, gestion de la continuité des opérations.
- **L'acquisition, la conception et l'implantation des SI :** la gestion de projet, l'audit des études et du développement, les pratiques de maintenance, contrôle applicatifs.
- **L'exploitation, l'entretien et le soutien des SI :** l'audit de la fonction information et des opérations, l'audit des infrastructures et des réseaux.
- **La protection des actifs informationnels :** audit de sécurité, gestion des accès, sécurité des réseaux, audit de management de la sécurité, sécurité physique, sécurité organisationnelle.

Le stage se termine lors de la dernière journée par un exposé de pratiques pour se préparer et passer l'examen (QCM de 4 heures).
Cet exposé est suivi d'un un examen blanc (2 heures) de 100 questions suivi d'une revue des réponses des stagiaires.

Formation « Homologation de la SSI : RGS, IGI1300, LPM, PSSIE »

Réf : SECUHOMOL

La démarche d'homologation de sécurité des systèmes d'informations s'est imposée dans de multiples référentiels gouvernementaux. Cette approche permet d'expliciter les besoins de sécurité d'un système, d'en évaluer la protection effective et de faire accepter les risques résiduels par une autorité adaptée.

C'est autour de ce cœur méthodologique, que les différents référentiels (RGS, II901, IGI1300, LPM, PSSIE) développent leurs spécificités…

Objectifs

- **Se familiariser avec les différents référentiels gouvernementaux de sécurité de l'information et leurs limites**
- **Mettre en œuvre une démarche d'homologation de sécurité**
- **Fournir les clés pour approfondir les différents cadres réglementaires**
- **Aborder la mise en place d'une organisation de gestion de la sécurité dans la durée**

Durée & Horaires

- **1 jour soit 7 heures**
- **9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participants

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Responsables de mise en conformité au RGS v2**
- **Toute personne ayant la nécessité de connaître et comprendre le Référentiel Général de Sécurité**
  - **Agents au sein des autorités administratives**
  - **Prestataires d'hébergement**
  - **Consultants accompagnant à la conformité**
  - **Fournisseurs de services aux autorités administratives**
- **Agents des ministères, rectorats/préfectures, mairies/collectivités territoriales, établissements publics...**

Pré-requis

Cette formation ne demande pas de pré-requis particuliers.

Méthode pédagogique

- **Cours magistral avec échanges interactifs**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Programme

Panorama des référentiels SSI étatiques

- Principes de certification/qualification
- Objectifs de l'homologation
- Démarche d'homologation
  - Analyse de risque
  - Mise en œuvre des mesures de sécurité
- Plan de traitement des risques
- Conformité
- IGI1300
- PSSIE
- LPM
- II901
- Cryptographie RGS
  - Audits d'homologation
  - Acte d'homologation
- Dossier d'homologation
- Comité et autorité d'homologation
- Revue et maintien dans la durée
- Stratégies de mise en œuvre
  - Pour nouveau système
  - Pour système existant

Formation « Gestion de crise IT/SSI »

Réf : SECUCRISE

Les méthodes proactives demeurent limitées et tout un chacun est confronté un jour à une crise due à des incidents informatiques ou un problème de sécurité. Il faut donc maîtriser cette réaction d'urgence et savoir y faire face.

Objectifs

- Apprendre à mettre en place une organisation adaptée pour répondre efficacement aux situations de crise
- Apprendre à élaborer une communication cohérente en période de crise
- Apprendre à éviter les pièges induits par les situations de crise
- Tester votre gestion de crise SSI.

Durée & horaires

- 1 jour soit 7 heures
- Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Directeur ou responsable des systèmes d'information
- Responsable de la sécurité des systèmes d'information
- Responsable de la gestion de crise
- Responsable des astreintes
- Responsable de la gestion des incidents

Pré-requis

- Cette formation ne demande pas de pré-requis particuliers.

Méthode pédagogique

- Cours magistral avec des exemples basés sur le retour d'expérience des formateurs.

Supports

- Support de cours au format papier en français
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- Cette formation n'est pas certifiante.

Programme

- Enjeux et Objectifs de la gestion de crise
  - Vocabulaire
  - Qu'est-ce que la gestion de crise SSI ?
- Rappel des fondamentaux sur la gestion des incidents de sécurité basée sur l'ISO 27035
- Analogies avec les autres processus
  - Gestion des incidents de sécurité
  - Continuité d'activité
  - Gestion de crise stratégique
- Analyse Forensique
- Organisation de gestion de crise SSI
  - Acteurs et instances de la crise
  - Rôles et responsabilités
  - Préparation de la logistique
  - Documentation & Canevas
  - Outils de communication
- Processus de gestion de crise SSI
  - Détection et Alerte
  - Évaluation et Décision
  - Activation
  - Réagir
  - Pilotage de la crise
  - Retour à la normale
  - Tirer les enseignements
- Facteur humain et effets du stress
- Tests et exercices de crise SSI
  - Enjeux et objectifs
  - Types d'exercices et tests
  - Scénarios de crise
  - Préparation d'un exercice de crise SSI
  - Outils et moyens
- Cas pratiques de gestion de crise SSI

Formation « EBIOS 2010 Risk Manager »

Réf : EBIOS2010

EBIOS (Etude des Besoins et Identification des Objectifs de Sécurité) s'est imposée comme la méthodologie phare en France pour apprécier les risques dans le secteur public. Elle est recommandée par l'ANSSI pour l'élaboration de PSSI et schéma directeur, pour l'homologation de téléservice dans le cadre du RGS, dans le guide GISSIP ; par la CNIL pour réaliser des analyses d'impacts sur les données nominatives (PIA ou Privacy Impact Assessment).
EBIOS possède des caractéristiques uniques qui permettent son usage dans tous les secteurs de la sécurité, bien au-delà de la SSI. EBIOS permet d'identifier les risques d'un système en construction qui n'existe pas encore, et demeure idéale pour la rédaction de cahier des charges.

Objectifs

- **Appréhender la méthode EBIOS 2010 et ses différents cas d'utilisation**
- **Maîtriser la construction d'un processus de gestion des risques**
- **Donner les moyens au stagiaire de piloter et réaliser une appréciation des risques EBIOS de l'étude des besoins à la formalisation des objectifs de sécurité**
- **Communiquer les ressources et les outils disponibles afin de réaliser une appréciation des risques optimale**
- **Préparer l'apprenant à l'examen de certification LSTI**

Durée & horaires

- **3 jours soit 21 heures réparties en 2,5 jours de cours et 0,5 d'examen.**
- **Deux premiers jours : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Dernier jour : de 09h30 à 12h et de 13h30/14h00 à 16h00/16h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Personne souhaitant maîtriser la démarche EBIOS 2010 ou visant la certification EBIOS Risk Manager**
- **Personne devant réaliser une appréciation des risques en sécurité, y comprit au-delà des risques en sécurité informatique**
- **RSSI**
- **DPO**
- **Chefs de projet SI**
- **Consultants en sécurité, ainsi qu'à ceux connaissant d'autres méthodes comme ISO27005, MEHARI ou EBIOS v2 (ancienne version d'EBIOS) et souhaitant maîtriser EBIOS 2010.**

Pré-requis

- **Il est recommandé de posséder des connaissances de base en sécurité informatique.**

Méthode pédagogique

La méthode pédagogique se base sur les cinq points suivants :

- **Cours magistral basé sur le référentiel EBIOS, des références aux normes ISO 27005, ISO31000 et ISO 31010 pourront être faites**
- **Bon usage des normes et méthodes à disposition (norme ISO 27002, méthodes d'analyse des risques ISO 27005 et MEHARI, etc.)**
- **Construction d'un tableau d'appréciation des risques exploitable à partir d'un tableur de type Excel**
- **Des exemples et études de cas tirés de cas réels**
- **Des exercices réalisés individuellement ou en groupe, y compris un exercice chaque soir à faire chez soi.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation est suivie d'un examen de cetification LSTI EBIOS 2010 Risk Manager. Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

Reconnaissance internationale

- **La formation HS2 et l'examen LSTI sont reconnus internationalement au même niveau et au même titre que d'autres formations et examens disponibles sur le marché.**

Programme

Introduction

EBIOS

Historique

Les autres méthodes

Différence entre EBIOS V2 et V2010

Activité 'Identifier les biens'

- Vocabulaire (bien essentiel / bien support)
- Cartographier le SI
- Exercice
- Cas pratique

Activité 'Apprécier les événements redoutés'

- Vocabulaire (composition d'un événement redouté)
- Identifier les événements redoutés
- Estimer la gravité
- Exercice
- Cas pratique

Activité 'Apprécier les scénarios de menaces'

- Vocabulaire (composition d'un scénario de menace)
- Identifier les scénarios de menace
- Estimer la vraisemblance
- Exercice
- Cas pratique

Activité 'Apprécier les risques'

- Vocabulaire
- Identifier les risques
- Estimer le niveau de risque

- Exercice

Activité 'Identifier les objectifs de sécurité'

- . Vocabulaire
- . Identifier les objectifs
- . Analyser les risques résiduels
- Exercice
- Cas pratique

Module 'Étude des mesures de sécurité'

- Vocabulaire
- Identifier les mesures
- Exercice
- Cas pratique

Activité 'Définir le cadre de la gestion des risques'

- Établir une déclaration d'applicabilité
- Homologuer un système
- Exercice
- Applications spécifiques

Conception d'une politique de sécurité et/ou d'un schéma directeur

Présentation de la FEROS

En vue de la rédaction d'un cahier des charges

- Cas pratique

Appréciation de risques dans le cadre de l'intégration de la sécurité dans un projet

Cas particulier du RGS

- Exercice

Activité 'Préparer les métriques'

- Définir des critères et des échelles
- Exercice

Synthèse

- Point important de la méthode
- Bases de connaissances
- L'étude de cas @rchimed
- Erreurs courantes
- Logiciels existants (CNIL, Ebios, Egerie, ...)

Exercices

Mise en situation

Réalisation d'une étude EBIOS complète en groupe

Présentation orale des résultats par chaque groupe

Préparation à l'examen

Examen de certification conçu, surveillé et corrigé par LSTI

Formation « Essentiels ISO27001 & ISO27002 »

Réf : ESS27

La norme ISO27001 est la référence internationale en termes de système de management de la sécurité de l'information (SMSI). Les projets de mise en conformité se multipliant, une connaissance des éléments fondamentaux pour la mise en œuvre et la gestion d'un SMSI est nécessaire. Par ailleurs, la norme ISO27001 décrit une approche pragmatique de la gestion de la sécurité de l'information avec le choix de mesures de sécurité découlant d'une appréciation des risques. Elle s'appuie sur le guide ISO27002 pour fournir des recommandations sur le choix et l'implémentation des mesures de sécurité.

Objectifs

- **Être capable de présenter la norme ISO27001, les processus de sécurité qui lui sont associés et le projet de mise en conformité**
- **Maîtriser la corrélation entre ISO27001 et ISO27002**
- **Savoir sélectionner les mesures de sécurité**

Durée & horaires

- **2 jours soit 14 heures**
- **Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Personne qui souhaite prendre connaissance des normes ISO 27001 et 27002, améliorer sa maîtrise des mesures de sécurité de l'information :**
  - **RSSI et à leurs équipes**
  - **Personnes responsables de services opérationnels**
  - **DSI et leurs équipes**
  - **Responsables méthodes et qualité**

Pré-requis

- **Aucun pré-requis n'est demandé. Toutefois, avoir une expérience en informatique et en sécurité est un plus.**

Méthode pédagogique

Cours magistral basé sur les normes.

Supports

- **Support de cours au format papier en français**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

Introduction aux systèmes de management

- Management de la SSI
- Historique des normes ISO27
- Panorama des normes ISO27
- Présentation détaillée de la norme ISO27001
- Gestion des risques
- Mesures de sécurité
  - Présentation de la norme ISO27002
  - Gestion des mesures de sécurité
  - Implémentation des mesures de sécurité et PDCA
  - Documentation des mesures de sécurité
  - Audit des mesures de sécurité
  - Autres référentiels de mesures de sécurité
- Certification ISO27001

Formation « ISO 27001 Lead Auditor »

Réf : ISO27LA

Objectifs

- Apprendre à auditer sur la norme ISO27001 et les guides associés
- Devenir auditeur ou responsable d'équipe d'audit pour les systèmes de management de la sécurité de l'information (SMSI)
- Disposer de la vision auditeur vis-à-vis de la norme ISO 27001,
- Intégrer le modèle PDCA lors des activités d'audits,
- Auditer les différentes catégories de mesures de sécurité (Annexe A de l'ISO27001 / ISO27002) et conduire un audit de SMSI et ses entretiens en maîtrisant les notions de non-conformités majeures ou mineures.

Durée & horaires

- 5 jours soit 40 heures réparties en 31h30 de cours, 5h00 de travail individuel sur les exercices le soir et 3h30 d'examen.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- La formation s'adresse à tous ceux amenés à conduire des audits d'un SMSI et plus généralement un audit dans le domaine de la cybersécurité, donc :
  - les membres des équipes de contrôle interne,
  - des équipes sécurité ou des équipes d'audit,
  - les auditeurs d'autres systèmes de management comme les qualiticiens,
  - les auditeurs externes réalisant des audits conseil (appelés également pré-audits ou audit à blanc) pour leurs clients,
  - ceux souhaitant devenir auditeur de conformité ISO27001, et ceux devant être audités et devant comprendre l'état d'esprit de l'auditeur.

Pré-requis

- Aucun pré-requis n'est demandé. Toutefois, la connaissance des systèmes de management dans un autre domaine, la qualité par exemple, est un plus. La notion de SMSI (ISO 27001) et la réalisation d'audits de systèmes de management (ISO 19011) seront explicitées lors de la formation. Cependant la lecture des normes ISO 27001 et ISO 19011 avant la formation est recommandée. Les 133 mesures de sécurité sont rapidement survolées et ne seront pas acquises à l'issue de cette formation, leur maîtrise demandant des bases solides en informatique.

Méthode pédagogique

La méthode pédagogique se base sur les quatre points suivants :

- Cours magistral basé sur les normes ISO27001, ISO19011, et plus succinctement les normes ISO27002, ISO17021, ISO27006 et ISO27007.
- Exercices de contrôle des connaissances sur les concepts à connaître et sur les normes.
- Exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous auditeurs de SMSI
-

- **Exercices pratiques individuels et collectifs effectués par les stagiaires, basés sur des cas réels d'audit anonymisés et un jeu de rôle auditeur / audité.**
- **Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation prépare à l'examen de certification LSTI à la norme 27001:2013 (ISO 27001 Lead Auditor). Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

Programme

Accueil des participants et tour de table

Introduction à la sécurité des systèmes d'information

Introduction au système de management

- Notion de SMSI (Système de Management de la Sécurité de l'Information)
- Modèle PDCA (Plan-Do-Check-Act)

Présentation détaillée de la norme ISO 27001 pour l'auditeur

- Contexte de l'organisation
- Leadership
- Planification
- Support
- Fonctionnement
- Évaluation des performances
- Amélioration

Relations entre les éléments structurants du SMSI

- Principaux processus d'un SMSI

Processus de certification ISO27001

- Certification et accréditation
- Autorités d'accréditation
- Organismes de certification
- Normes ISO17021 et ISO27006
- Règlement de certification

Présentation de la norme ISO 27002

- Objectifs et usage de la norme
- Exigences de l'ISO 27001
- Auditer une mesure de sécurité
- Présentation des mesures de sécurité
- Exemple d'audit de mesures de sécurité

Présentation de la démarche d'audit de la norme ISO19011

- Principes de l'audit
- Types d'audit
- Programme d'audit
- Démarche d'audit
- Avant l'audit
- Audit d'étape 1
- Audit d'étape 2
- Après l'audit
- Auditeur et Responsable d'équipe d'audit

Présentation de la démarche d'audit SMSI

- Application ISO17021, ISO27006 et ISO19001 à un SMSI
- Critères d'audit
- Déroulement d'un audit
- Constats d'audit et fiches d'écart
- Conduite d'entretiens
- Réunion de clôture
- Rapport d'audit

Examen de certification conçu, surveillé et corrigé par LSTI

Formation « ISO 27001 Lead Implementer »

Réf : ISO27LI

Objectifs

- Apprendre à mettre en œuvre la norme ISO27001 et les guides associés
- Apprendre à utiliser concrètement les normes, avec des exemples pour que chacun puisse les utiliser chez lui ou chez ses clients : les processus à mettre en place, le dimensionnement et l'organisation du projet, etc

Durée & horaires

- 5 jours soit 40 heures réparties en 31h30 de cours, 5h00 de travail individuel sur les exercices le soir et 3h30 d'examen.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Personnes devant mettre en œuvre un SMSI à tous les niveaux, du management à l'opérationnel :
  - RSSI et à leurs équipes
  - Personnes responsables de services opérationnels
  - DSI et leurs équipes
  - Responsables méthodes et qualité
  - Consultants et aux personnes en reconversion souhaitant mettre en œuvre l'ISO27001
- Personnes devant participer à l'implémentation de la norme en vue d'une certification ISO27001 ou une certification HDS (Hébergeur de Données de Santé)

Pré-requis

- Aucun pré-requis n'est demandé. Toutefois, avoir une expérience en informatique et en sécurité est un plus.

Méthode pédagogique

La méthode pédagogique se base sur les quatre points suivants :

- Cours magistral basé sur la norme ISO27001, et plus succinctement les normes ISO27002, ISO27003, ISO2004 et ISO27005.
- Exercices de contrôle des connaissances sur les concepts à connaître et sur les normes.
- Exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous implémenteurs de SMSI
- Exercices pratiques individuels et collectifs effectués par les stagiaires, basés sur des études de cas : périmètre, politique, procédures, plan projet, suivi et réunions, traitement des risques, surveillance et indicateurs. Ces exercices permettent également de se préparer à l'examen de certification.
- Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.

Supports

- Support de cours au format papier en français
- Cahier d'exercices et corrections des exercices
- Tous les documents nécessaires à la formation en français ou anglais
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation prépare à l'examen de certification LSTI à la norme 27001:2013 (ISO 27001 Lead Implementer). A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 3h30 en français. L'examen est constitué d'une partie QCM sur les notions de cours et d'une partie rédactionnelle sous forme d'étude de cas.**

Programme

Accueil des participants et tour de table

Introduction à la sécurité des systèmes d'information

Introduction au système de management
- Notion de SMSI (Système de Management de la Sécurité de l'Information)
- Modèle PDCA (Plan-Do-Check-Act)

Présentation détaillée de la norme ISO 27001
- Contexte de l'organisation
- Leadership
- Planification
- Support
- Fonctionnement
- Évaluation des performances
- Amélioration

Présentation de la norme ISO 27002
- Différentes catégories de mesures de sécurité
- Mesures d'ordre organisationnel / technique
- Implémentation d'une mesure de sécurité selon le modèle PDCA

Panorama des normes complémentaires
- ISO27017, ISO27018, ISO27025

Processus dans un SMSI
- Processus support
- Gestion des exigences légales et réglementaires
- Gestion des risques
- Implémentation et suivi des mesures de sécurité
- Gestion des incidents
- Gestion documentaire
- Évaluation de la performance

La gestion des risques et la norme ISO 27005
- Vocabulaire : risque, menace, vulnérabilité, etc.
- Critères de gestion de risque
- Appréciation des risques, acceptation du risque, communication du risque
- Déclaration d'applicabilité (DdA/SoA)
- Réexamen du processus de gestion de risques et suivi des facteurs de risques

Gestion des exigences légales et réglementaires
- Protéger les données à caractère personnelles
- Outils de veille juridique
- Gestion des engagements contractuels
- Gestion des fournisseurs et prestataires
- Contractualiser la sécurité

L'évaluation des performances
- Surveillance au quotidien
- Indicateurs et norme ISO 27004
- Audit interne
- Revue de Direction

Projet SMSI
- Conviction la direction
- Étapes du projet
- Acteurs
- Facteurs clés de réussite et d'échec
- Processus de certification ISO27001

Certification ISO27001
- Accréditation
- Normes ISO19011 et ISO27007
- Normes ISO17021 et ISO27006
- Règlement de certification

Examen de certification conçu, surveillé et corrigé par LSTI

Formation « ISO 27005 Risk Manager »

Réf : ISO27RM

Une fois que les bonnes pratiques ont été appliquées, la sécurité des systèmes d'information a besoin d'être ajustée aux besoins et au contexte de chaque organisme. Partant de ce constat, les experts en sécurité ont placé la gestion des risques au cœur des processus de gestion de la cybersécurité. Aujourd'hui, systèmes de management, homologations, et RGPD sont basés par une approche sur le risque, de même que de nombreuses certifications (ISO27001, HDS, PCI-DSS, ISO22301, etc). La gestion des risques reste pourtant une démarche parfois d'abord difficile et qui conditionne souvent la réussite du système de management ou du projet associé.
La norme ISO27005 est la méthode de gestion des risques en sécurité de l'information reconnue internationalement, et un des principaux guides de la série des normes ISO27001. ISO 27005 est pragmatique, elle vise la gestion des risques dans la durée, et elle impose la prise de responsabilité par le propriétaire du risque, généralement la direction générale. Elle est la méthode préconisée pour toute appréciation des risques dans le cadre d'un SMSI (Système de Management de la Sécurité de l'Information). Elle peut être également utilisée pour l'appréciation des risques imposée en plus du BIA (Business Impact Analysis) dans un SMCA (Système de Management de la Continuité d'Activité) et dans beaucoup d'autres cadres.

Objectifs

- **Acquérir une compréhension globale des concepts, de la norme, des méthodes et des techniques de gestion des risques**
- **Apprendre à mettre en œuvre la méthode ISO 27005 dans son contexte**
- **Appliquer la méthode ISO27005 avec efficacité là où celle-ci accorde de la liberté à l'implémenteur**
- **Maîtriser le processus de gestion des risques et son cycle de vie**
- **Savoir apprécier les risques et présenter ses propositions de traitement aux propriétaires des risques**

Durée & horaires

- **3 jours soit 21 heures réparties en 2,5 jours de cours et 0,5 d'examen.**
- **Deux premiers jours : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Dernier jour : de 09h30 à 12h et de 13h30/14h00 à 16h00/16h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Consultants**
- **RSSI**
- **Chefs d projet**
- **Toute personnes devant réaliser des appréciations des risques en cybersécurité**

Pré-requis

- **Pour assister à cette formation, il est recommandé de posséder des connaissances en informatique.**

Méthode pédagogique

La méthode pédagogique se base sur les cinq points suivants :

- **Approche du sujet de manière interactive où les stagiaires remplissent un tableur édité par l'instructeur et déroulent la méthode sans la connaître**
- **Cours magistral basé sur la norme ISO 27005**
- **Des exemples et études de cas tirés de cas réels**
- **Des exercices réalisés individuellement**

- **Mise en œuvre d'une appréciation des risques et d'un traitement des risques sur une étude de cas, en groupe, à l'aide d'un tableur**
- **Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**
- **Clef USB permettant de conserver le travail réalisé durant la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation est suivie d'un examen de certification LSTI ISO 27005 Risk Manager. Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

Reconnaissance internationale

- **La formation HS2 et l'examen LSTI sont reconnus internationalement au même niveau et au même titre que d'autres formations et examens disponibles sur le marché.**

Programme

Introduction

- Normes ISO270XX
- ISO 27005 et les autres méthodes dont Ebios, Mehari, etc
- Vocabulaire du management du risque selon l'ISO 27005

Présentation interactive du vocabulaire fondamental et de l'approche empirique du management du risque avec la participation active des stagiaires à un exemple concret

- Identification et valorisation d'actifs
- Menaces et vulnérabilités
- Identification du risque et formulation sous forme de scénarios
- Estimation des risques
- Vraisemblance et conséquences d'un risque
- Évaluation des risques
- Différents traitements du risque
- Acceptation des risques
- Notion de risque résiduel

Norme ISO 27005

- Introduction
- Gestion du processus de management du risque
- Cycle de vie du projet et amélioration continue (modèle PDCA)
- Établissement du contexte
- Identification des risques
- Estimation des risques
- Évaluation des risques
- Traitement du risque
- Acceptation du risque
- Surveillance et réexamen des facteurs de risque
- Communication du risque

Exercices

Mise en situation : étude de cas

- Réalisation d'une appréciation de risque complète sur ordinateur
- Travail de groupe
- Simulation d'entretien avec un responsable de processus métier
- Présentation orale des résultats par le meilleur groupe
- Revue des résultats présentés

Examen de certification conçu, surveillé et corrigé par LSTI

Formation « EBIOS 2018 Risk Manager »

Réf : EBIOS2018

EBIOS RM ou EBIOS Risk Manager (EBIOS2018 pour éviter de confondre avec EBIOS2010), est une méthode de gestion des risques conçue par l'ANSSI et publiée en octobre 2018. Cette nouvelle méthode combine une démarche conformité afin de se focaliser sur un panel réduit de risques, tout en approfondissant ceux-ci, et met l'accent sur les risques liés aux parties prenantes et à l'externalisation. Elle est recommandée par l'ANSSI pour les appréciations des risques orientées projet et SMSI, avec à terme l'objectif de remplacer la méthode EBIOS2010 et ses cas d'usages.

Objectifs

- **Fournir aux participants l'ensemble des éléments pour pouvoir, par la suite être autonome dans la réalisation d'une analyse des risques selon la méthodologie EBIOS 2018 Risk Manager.**
- **Présenter le vocabulaire et les différents ateliers qui composent la méthode.**
- **Préparer l'apprenant à l'examen de certification LSTI**

Durée & horaires

- **3 jours soit 21 heures réparties en 2,5 jours de cours et 0,5 d'examen.**
- **Deux premiers jours : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Dernier jour : de 09h30 à 12h et de 13h30/14h00 à 16h00/16h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Personne souhaitant découvrir, comprendre ou mettre en pratique la méthode EBIOS2018**
- **RSSI**
- **Consultants en sécurité, y compris ceux connaissant d'autres méthodes comme ISO27005 ou EBIOS2010**

Pré-requis

- **Une notion sur la gestion de risque est un plus**
- **Une base en sécurité des systèmes d'information est requise (sécurité des réseaux, sécurité des systèmes, etc.)**

Méthode pédagogique

- **Cours magistral théorique via le déroulé d'un cas fictif**
- **Exercice pratique : mise en application des concepts préalablement enseignés. Déroulement de la méthode sur un cas d'étude.**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation est suivie d'un examen de cetification LSTI EBIOS 2018 Risk Manager. Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

Reconnaissance internationale

- **La formation HS2 et l'examen LSTI sont reconnus internationalement au même niveau et au même titre que d'autres formations et examens disponibles sur le marché.**

Programme

Les bases de la gestion de risques

- Objectif de la gestion de risque
- Les principales normes en gestion de risques (ISO 27005, MEHARI, etc.)
- Présentation de la méthodologie EBIOS RM (historique, évolution, concepts)
- Les notions essentielles (risques, gravité, vraisemblance, etc.)

Atelier 1 : socle de sécurité

- Identification du cadre et périmètre de l'analyse de risque
- Étude des événements redoutés et valorisation de leur gravité
- Identification des principaux référentiels composant le socle de sécurité

Atelier 2 : sources de risque

- Identification des sources de risques et des objectifs visés
- Évaluation de la pertinence des couples SR/OV
- Sélection des couples les plus pertinents

Atelier 3 : scénarios stratégiques

- Élaboration de la cartographie de l'écosystème et sélection des parties prenantes critiques
- Élaboration des scénarios stratégiques
- Définition des mesures de sécurité existantes

Atelier 4 : scénarios opérationnels

- Élaboration des scénarios opérationnels
- Évaluation de leur vraisemblance

Atelier 5 : traitement du risque

- Réalisation de la synthèse des scénarios de risque
- Définition de la stratégie de traitement de risque et définition du Plan d'Amélioration Continue de la Sécurité (PACS)
- Évaluation des risques résiduels
- Mise en place du cadre du suivi des risques

Plans de formation bientôt disponibles

Réf : ISO27004 Formation « Indicateurs et tableaux de bord cybersécurité »

- **Objectif :** Pour savoir construire des indicateurs utiles pour suivre sa progression et communiquer à sa direction. Pour RSSI et consultants

Réf : ISO27035 Formation « Gestion des incidents de sécurité »

- **Objectif :** Pour mieux organiser sa gestion d'incidents et mieux les gérer. Pour RSSI et responsables de SOC / CSIRT / CERT.

Formation « Essentiels techniques de la cybersécurité »

Réf : ESSCYBER

La sécurité des systèmes d'information (SSI), aujourd'hui appelée cybersécurité, semble un jargon lointain pour certains. Il est important de démystifier en expliquant concrètement comment ça marche, et la meilleure des sensibilisations à la cybersécurité est la formation qui explicite. Grâce à sa vision pragmatique de la sécurité : connaitre l'attaque pour mieux se défendre, et aux différentes mises en application proposées, cette formation permet aux stagiaires de comprendre la nécessité de la SSI, d'en aborder les concepts théoriques (cryptographie, contrôle d'accès...) et d'identifier tous les domaines auxquels elle s'applique (système, réseau, applications...).

Objectifs

- Acquérir la connaissance des concepts fondamentaux de la SSI.
- Identifier les besoins en sécurité à tous les niveaux (système, réseau, applications...)
- Comprendre les différents types d'attaques
- Connaitre les mesures de sécurité permettant de les contrer

Durée & horaires

- 2 jours soit 14 heures
- De 09h00 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Toute personne souhaitant acquérir la compréhension de la cybersécurité
- Responsable de la sécurité (RSSI) de formation non technique
- Chef de projet et acteur d'un projet sécurité

Cette formation est accessible à un public plus large que la formation SECUCYBER en permettant aux personnes au profil non informaticien ou non technique d'obtenir une vision opérationnelle de la cybersécurité

Pré-requis

- Cette formation ne nécessite pas de prérequis particuliers, elle accessible à un large public.

Méthode pédagogique

- Cours magistral avec de nombreux exemples pratiques

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **Cette formation n'est pas certifiante.**

Programme

Sécurité : concepts fondamentaux
- Concepts de bases
- Gestion du risque : vulnérabilité, menace, impacts métiers
- Dans la peau d'un attaquant
- Principes de base : connaître son SI, moindre privilège, défense en profondeur, prévention et détection

Cryptographie
- Chiffrement
- Hachage
- Signature
- TLS
  - PKI/IGC

Gestion des utilisateurs et des privilèges
- Provisionnement
  - Moindre privilège
- Authentification
- Protection des administrateurs

Sécurité des réseaux
- Principes de base
- Attaques
- Contrôle d'accès
- Filtrage et relayage
- Architecture sécurisée
  . WiFi

Sécurité des systèmes
- Minimisation et durcissement
- Sauvegarde
- Veille sécurité
- Mise à jour
- Sécurisation active
  - Virtualisation

Sécurité des applications
- Vulnérabilités : le TOP 10 de l'OWASP
- Attaques et défenses
- Stockage des mots de passe
- Processus de développement

Détection et gestion d'incident
- Journalisation
- SOC et CSIRT
- Processus de gestion d'incident

Formation « Fondamentaux techniques de la cybersécurité »

Réf : SECUCYBER

Si le fait d'être sensibilisé à la sécurité est important quel que soit le poste occupé, comprendre les concepts de base de la SSI est une nécessité absolue pour le personnel technique de l'entreprise. En effet, la sécurité n'est pas seulement l'affaire du RSSI et de ses équipes : administrateurs système et réseau, architectes, développeurs ont tous leur rôle à jouer dans la protection de l'entreprise et de son patrimoine.

La formation SECUCYBER, en abordant sur 5 jours tous les aspects techniques de la sécurité informatique, vise à apporter à cette population les connaissances indispensables leur permettant de choisir, d'implémenter et de maintenir les mesures de sécurité propres à leur domaine de compétence.

Objectifs

- **Être en mesure dans tous les domaines techniques de la sécurité (système, réseau, applications, cryptographie...) de :**
  - **Maîtriser le vocabulaire et les concepts principaux du domaine**
  - **Connaître différentes techniques d'attaque**
  - **Choisir et appliquer les bonnes mesures de sécurité**

Durée & horaires

- **5 jours soit 40 heures**
- **Du lundi au jeudi : de 9h00 à 12h et de 13h30 à 19h00.**
- **Le vendredi : de 09h00 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 6 participants – Maximum 24 participants**

Public visé

- **Administrateurs système ou réseau**
- **Architectes**
- **Développeurs**
- **Personnel débutant ou souhaitant acquérir de bonnes bases techniques en SSI**

Pré-requis

- **Bonnes connaissances en informatique**

Méthode pédagogique

- **Cours magistral illustré par des travaux pratiques réguliers**

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUCYBER par HS2..**

Programme

Module 1 : SSI - principes de bases

- Pourquoi la SSI ?
- Notion de risque
- Les règles de base
- Contrôle d'accès
  - AAA
  - Gestion des utilisateurs
  - Authentification
  - Gestion des privilèges

Module 2 : Cryptographie

- Concepts fondamentaux
- Fonctions de base
  - Chiffrement
  - Hachage
  - Signature
- Protocoles
  - TLS
  - IPSec
  - SSH
- PKI / IGC

Module 3 : Réseau

- Modèles théoriques : OSI, TCP/IP
- Attaques classiques
  - Découverte de ports
  - Man-in-the-Middle
- Contrôle d'accès réseau
- Segmentation
  - Qu'est qu'une bonne architecture ?
  - Comment segmenter son réseau
  - VLAN
  - Parefeu
  - Proxy
- Réseaux sans fil
- Sécuriser le Cloud

Module 4 : Applications

- Architecture n-tiers
- Protocoles
- Authentification et sessions
- Top 10 de l'OWASP
- Buffer Overflow
- Processus de développement

Module 5 : Windows

- Installation
- Bitlocker
- Mesures Windows 10 :
  - Device Guard
  - Application Guard
  - Exploit Guard
- Gestion des administrateurs
- Éviter le Pass-The-Hash

Module 6 : Linux

- Système de fichiers
- Minimisation
- Comptes utilisateurs
- Authentification
- SELinux
- AppArmor
- SSH
- Netfilter
- Journalisation

Module 7 : Gestion d'incidents

- La base : sauvegarde et journalisation
- Veille sécurité
- SOC et CSIRT
- Gestion d'incidents
- Analyse inforensique

Formation « Cybersécurité des systèmes industriels »

Réf : SECUINDUS

Les systèmes industriels sont maintenant informatisés et connectés. Longtemps isolés, ils sont maintenant dans le cœur de cible des attaques informatiques. Généralement, trop peu d'automaticiens ont une expérience significative de l'état de l'art de la sécurité informatique, et trop peu d'experts en cybersécurité ont une bonne connaissance du monde de l'informatique industrielle. La présente formation s'efforce de proposer un état des enjeux, des méthodes et des moyens de sécurisation, et de la gestion d'incident.

Objectifs

- **Aborder la cybersécurité des systèmes industriels par une approche pragmatique et pratique**
- **Développer un plan de sécurisation des systèmes informatiques industriels**
- **Pouvoir auditer les SI industriels**
- **Initier la préparation de plans de réponse à incident sur les systèmes industriels**

Durée & horaires

- **3 jours soit 21 heures**
- **De 9h30 à 12h et de 13h30 à 17h30/18h00.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Responsables sécurité, sureté, cybersécurité, sécurité industrielle**
- **RSSI**
- **Automaticiens**
- **Consultants en sécurité**
- **Auditeurs en sécurité**

Pré-requis

- **Bonne connaissance générale en informatique et en sécurité des systèmes d'information, par exemple une certification SECUCYBER d'HS2 ou CISSP d'(ISC)2.**
- **Aucune connaissance des systèmes industriels n'est nécessaire.**

Méthode pédagogique

- **Cours magistral**
- **Démonstrations**
- **Exercices de mise en œuvre**

Supports

- **Support de cours au format papier en français**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUINDUS par HS2.**

Programme

Introduction à la cybersécurité des systèmes industriels
- Vocabulaire
- Familles de SI industriels
- Bestiaire des équipements
- Particularismes de gestion des SI industriels

Architectures des SI industriels
- Architecture ISA95
- Approches de l'ISA/IEC 62443
- Spécificité des systèmes de sureté
- Accès partenaires
- Réalité du terrain

Protocoles, applications sécurisations possibles
- Grandes familles de protocole industriels
- Exemple de ModBus
- Exemple d'OPC
- Possibilité de détection et filtrage sur les flux industriels

Incidents représentatifs et évolutions
- Principaux incidents SSI ICS publics
- Cadre des SIV LPM
- Industrial IOTs et le cloud industriel

Référentiels sur la sécurité des systèmes d'information industriels
- Guides ANSSI
- Normes IEC 62443 (ISA 99)
    - IEC 62443-2-1
    - IEC 62443-3-3
- NIST SP800-82, NERC CIP, ISO 27019, etc

Sécurisation des SI industriels
- Organisation
- Appréciation des risques
- Cartographie et inventaire
- Intégration et recette de sécurité
- Maintien en condition de sécurité
- Surveillance

Réponse à incident sur un système industriel
- Premières réactions
- Détection et marqueur de compromission
- Analyse forensique d'artefacts industriel
- Préparer sa réponse à incident

Exercices
- Audit technique
    - Analyse de traces réseaux
    - Exploitation de vulnérabilités du protocole Modbus/TCP
- Sécurité organisationnelle et architecturale du réseau industriel
    - Architecture sécurisée
    - Détermination des zones et conduites
    - Points sensibles
    - Sécurisation d'architecture
    - Détermination des niveaux de classification ANSSI
    - Analyse basée sur le guide ANSSI relatif aux réseaux industriels
- Réponse à incident
    - Recherche de compromission du système sur capture réseau
    - Analyse des projets de processus industriels

Formation « DNSSEC »

Réf : DNSSEC

Le DNS est l'infrastructure sur laquelle tous les services d'Internet se reposent. DNSSEC peut protéger contre une large classe de problèmes, comme les attaques par empoisonnement, les serveurs menteurs, les révolveurs DNS configurés par certains fournisseurs pour rediriger les fautes de frappe vers de la publicité. En revanche, c'est une technologie délicate qui nécessite une bonne compréhension.

Objectifs

- Acquérir la connaissance technique du protocole DNS et de l'extension DNSSEC
- Configurer une installation d'un résolveur (Unbound) validant les réponses avec DNSSEC
- Construire une infrastructure DNSSEC comprenant OpenDNSSEC pour gérer les clés et BIND pour servir les zones signées
- Éviter les pièges du DNS
- Déterminer l'intérêt réel d'un déploiement éventuel de DNSSEC dans leur environnement

Durée & horaires

- 2 jours soit 14 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Exploitants et administrateurs systèmes et réseaux
- Responsables opérationnels
- Architectes amenés à prendre des décisions de nature technique

Pré-requis

- Formation SECUCYBER
- ou connaissances préalables de l'administration système et des protocoles réseaux TCP/IP

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **Cette formation n'est pas certifiante.**

Programme

DNS : spécifications et principes

- Vocabulaire
- Arbres, zones...
- Resolver, cache, authoritative, fowarder...
- Organisation
- TLD, autres domaines, délégations...
- Protocole
- RRSet, entêtes, couche de transport et EDNS
- Problèmes liés aux pare-feux
- Enregistrements (RR)
- A, AAAA, PTR, SOA, NS, MX ...
- Fonctionnement interne
- Récursion et itération, fonctionnement de la résolution, ... Logiciels
- Couches logicielles
- "stub resolver", résolveur, rôle de l'application ...
- Alternatives à BIND
- Outils sur le DNS
- Zonemaster, dig, delv...

Sécurité du DNS

- Risques : modification non autorisée des données, piratage des serveurs, attaque via le routage ou autre "IP spoofing", empoisonnement de cache ... Ce qu'a apporté l'attaque Kaminsky.

Cryptographie

- Petit rappel cryptographie asymétrique, longueur des clés, sécurité de la clé privée ...

DNSSEC

- Clés : l'enregistrement DNSKEY. Méta-données des clés. Algorithmes et longueurs des clés.
- Signature des enregistrements : l'enregistrement RRSIG. Méta-données des signatures.
- Délégation sécurisée : l'enregistrement DS
- Preuve de non-existence : les enregistrements NSEC et NSEC3

DNSSEC en pratique

- Objectifs, ce que DNSSEC ne fait pas, les problèmes apportés par DNSSEC.
- Protocole
- bit DO et couche de transport (EDNS)
- Problèmes liés aux pare-feux
- Créer une zone signée à la main
- "dnssec-keygen, -signzone, named-checkzone/conf
- Configurer le résolveur Unbound pour valider
- Vérifier avec dig et delv
- Déboguage
- Délégation d'une zone. Tests avec dnsviz
- Renouvellement de clés
- Créer une zone signée avec DNSSEC

Retour d'expérience

- Zone racine
- Domaines de premier niveau (.fr, .se, .org, ...)
- Zones ordinaires signées
- Stockage des clés. Les HSM.
- Problèmes opérationnels (re-signature, supervision)

Conclusion

Formation « Principes et mise en œuvre des PKI »

Réf : SECUPKI

La cybersécurité repose sur une brique de base indispensable : la cryptographie. La cryptographie repose sur des conventions secrètes, des clés secrètes en cryptographie symétrique, des bi-clés : clé privée et clé publique en cryptographie asymétrique. La PKI est ce qui permet de gérer ces clés cryptographiques asymétriques et de leurs certificats. Les PKI sont indispensables à la construction de services de confiance comme la mise en place d'identités numériques, la signature électronique, le chiffrement des échanges, etc.

Objectifs

- Apprendre les technologies et les normes (initiation à la cryptographie)
- Apprendre les différentes architectures
- Apprendre les problématiques d'intégration (organisation d'une PKI, formats de certificats, points d'achoppement)
- Apprendre les aspects organisationnels et certifications
- Apprendre les aspects juridiques (signature électronique, clés de recouvrement, utilisation, export / usage international)

Durée & horaires

- 3 jours soit 21 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Architectes
- Chefs de projets
- Responsable sécurité/RSSI avec une orientation technique
- Développeurs séniors
- Administrateurs système et réseau senior

Pré-requis

- Formation universitaire de base ou Ingénieur en informatique
- Pas de connaissance de la cryptographie ni des certificats requis
- Constitue un plus : utilisation de la ligne de commande, notion d'API bases de réseau IP

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- Support de cours au format papier en français
- Ordinateurs portables et 'tokens' cryptographiques mis à disposition par HS2 pour les exercices
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUPKI par HS2.**

Programme

Jour 1 : Mise en contexte

- Bases de cryptographie
  - Notions de dimensionnement et vocabulaire de base
  - Mécanismes
  - Combinaisons de mécanismes
  - Problèmes de gestion de clés
  - Sources de recommandation : ANSSI, ENISA, EuroCrypt, NIST
- Implémentation de la cryptographie
  - Bibliothèques logicielles
  - Formats courants
  - Usages courants et gestion associée
  - Chiffrement de fichiers et de disques
  - Chiffrement de messagerie
  - Authentification
  - Chiffrement des flux
- Grands axes d'attaques et défenses
- Exercices OpenSSL d'utilisation des primitives cryptographiques
- Cadre général : Historique

Jour 2 : PKI et organisation

- Matériel cryptographique
  - Différents types d'implémentation matérielle
  - Certification Critères Communs
  - Certification FIPS 140-2
- Structure de PKI
  - Certificats X509
  - Rôles : sujet, vérificateur, certificateur, enregistrement, révocation
  - Architectures organisationnelles courantes
  - Cinématiques dans PKIX
  - Hiérarchies d'autorités
  - Vérification récursive d'une signature1
- Cadre légal et réglementaire
  - Droit de la cryptologie
  - Droit de la signature électronique
  - Référentiel général de sécurité
- Certification d'autorité
  - ETSI TS-102-042 et TS-101-456, certification RGS
  - Exigences pour les inclusions dans les navigateurs et logiciels courants
  - Évolution des pratiques
  - Exercice : Opération d'une infrastructure de gestion de clés avec Gnomint jusqu'à authentification TLS réciproque

Jour 3 : Implémentation de PKI et perspectives

- Suite des exercices de gestion d'IGC et ajout d'une génération de certificat sur token USB
- Mise en œuvre de PKI
  - Différents types d'implémentation d'IGC rencontrées couramment
  - Types d'acteurs du marché
  - Recommandations pour l'intégration
  - Attaques sur les PKI
  - Problème des PKI SSL/TLS
  - Remédiations mise en œuvre pour TLS
- Infrastructures de gestion de clés non X509
  - GPG
  - SSH
  - R/PKI
- Prospective
  - Évolution de la cryptographie et modes journalistiques
  - Distribution de clés par canal quantique (QKD)
  - Cryptographie homomorphique
  - Cryptographie-post quantique
  - Gestion des clés symétriques
  - Chaines de blocs (blockchain)
  - Tendances et conclusion
- Examen de certification HS2 (QCM sur ordinateur)

Formation « PKI Windows »

Réf : SECUPKIWIN

Les bases de la cryptographie aux bonnes pratiques organisationnelles, cette formation donne toutes les clés nécessaires à la gestion opérationnelle d'une IGC (PKI) dans un contexte Windows. A travers des cas concrets, les stagiaires apprendront à maîtriser les concepts de base ainsi que le développement de scripts PowerShell afin d'automatiser et de faciliter la gestion de l'IGC (PKI). Une étude de cas regroupant plusieurs cas réels permettra aux stagiaires d'évaluer leur niveau en fin de formation et de se préparer à l'examen.

Objectifs

- Apprendre les technologies et les normes (initiation à la cryptographie)
- Comprendre les besoins métier concernant les certificats
- Acquérir les connaissances et compétences nécessaire afin de fournir un support haut-niveau aux métiers
- Apprendre à créer des scripts Powershell pour gérer et améliorer l'IGC

Durée & horaires

- 3 jours soit 21 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Experts sécurité
- Responsable PKI Windows
- Administrateurs système et réseaux Windows
- Architectes Active Directory

Pré-requis

- Formation universitaire de base ou ingénieur en informatique
- Pas de connaissance de la cryptographie ni des certificats requis
- Connaissance de Windows souhaitable
- Connaissance de powershell pas nécessaire
- Chaque stagiaire doit posséder un compte Microsoft Live afin d'activer une licence temporaire Windows server

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- Support de cours au format papier en français
- Ordinateur portable avec virtualbox
- Un compte Windows Live (live.com) afin d'obtenir une licence serveur temporaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUPKIWIN par HS2.**

Programme

Cryptographie et PKI

- Rappel sur les principes cryptographiques fondamentaux
- Rappel des algorithmes cryptographiques et taille de clé conseillés
- Architecture organisationnelle et technique d'une IGC (PKI)
- Principe de création, vérification et révocation de certificat
- Création d'une autorité racine indépendante

PKI Windows

- Rappel de l'environnement Windows
- Spécificité de l'IGC (PKI) Windows
- Création d'une autorité fille liée à l'AD
- Rappel des bases Powershell
- Création de scripts simples en Powershell

PKI avancée

- Cas d'étude d'une architecture IGC
- Création de scripts Powershell avancés
- Méthodologie de résolution de problème (debugging)
- Etude de cas : les stagiaires doivent résoudre 6 problèmes utilisateurs dont la difficulté va de moyen à expert
- Examen de certification HS2 (QCM sur ordinateur)

Formation « Sécurité des serveurs et des applications Web »

Réf : SECUWEB

L'infrastructure Web expose directement votre société aux menaces externe. Renforcez vos défenses en sécurisant efficacement tous les vecteurs exploités par les attaquants !

Objectifs

- Comprendre les vulnérabilités les plus fréquentes du web
- Analyser les risques encourus
- Dresser un diagnostic complet de sa sécurité
- Appliquer les contre-mesures effectives
- Maîtriser le processus de développement

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Pentesters web
- Consultants SSI
- RSSI
- Développeurs
- Architectes
- Administrateurs systèmes

Pré-requis

- Aucun prérequis
- Des notions d'utilisation d'une distribution Linux est un plus

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges intéractifs

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUWEB par HS2.

Programme

La sécurité du web
- Les motivations des attaquants
- Analyse de risques

Architecture sécurisée
- Le cloisonnement
- Le bastion
- Le filtrage
- La détection
- Le cloud et la conteneurisation

Les mécanismes du Web
- Rappels sur HTTP
- Les méthodes HTTP

La sécurité du navigateur
- Same Origin Policy
- Communication "cross-domain"
- Les entêtes de sécurité

Reconnaissance et fuite d'informations
- Cartographie et vérification des cibles
- Le scan de ports
- L'analyse de l'environnement
- La cartographie du site
- Le back office
- Open Source Intelligence
- Le scan de vulnérabilités

Les processus d'authentification
- Les méthodes d'authentification HTTP
- uni facteur
- multi facteur
- Délégation/fédération
- Le SSO
- Les attaques sur l'authentification

La gestion des sessions
- Les jetons de session
- Les cookies
- Forge de requêtes inter-sites (CSRF)
- Fixation de session
- Forge de jetons de session
- Le cloisonnement des sessions

Les injections
- Les injections coté client
- L'injection XSS
- Les injections côté serveur
- Les injections de commandes
- La SSRF
- L'injection XXE
- L'injection SQL
- Quelques injections moins fréquentes (XPath, LDAP)
- Les injections via sérialisation/désérialisation

Les injections de fichiers
- Le téléversement de fichiers
- Les inclusions de fichiers locaux et distants

La sécurité des communications
- HTTPS, SSL, TLS
- Dissection d'une suite cryptographique
- Les vulnérabilités
- Recommandations
- Audits et contrôles
- La PKI

La sécurité des données stockées
- Le stockage sécurisé des données sensibles
- La blockchain
- Auditer la sécurité des données stockées

Les Webservices
- Le fonctionnement des Webservices
- La sécurité des Webservices

Les vulnérabilités plus complexes
- Tour d'horizon
- Attaques sur la mémoire (buffer overflow)
- Heartbleed

La sécurité du serveur
- Durcissement du socle
- Durcissement de l'applicatif web

Sécurité et processus de développement
- Secure SDLC
- Notions d'analyse de risques projet
- Développement sécurisé
- Les tests des fonctions de sécurité
- La sécurité du produit en production
- La gestion des vulnérabilités
- La gestion des patchs

Les autres mesures de sécurité
- PRA/PCA
- La gestion des acteurs tierces

Les concepts essentiels développés dans la formation sont illustrés au travers de mises en pratique sur PC permettant d'acquérir des compétences concrètes applicables en entreprise.

Formation « Sécurisation des infrastructures Windows »

Réf : SECUWIN

Système d'exploitation le plus utilisé dans l'entreprise et au dehors, et sans aucun doute l'un des plus attaqués, Windows est un composant incontournable de la majorité des systèmes d'information. Ancien "mauvais élève" de la sécurité, Microsoft a depuis quelques années mis la sécurité au centre de sa stratégie, avec pour résultat une grande diversité de mesures, parfois mal connues ou sous-utilisées, et de vraies avancées technologiques.

En vous apportant la maitrise de ces mécanismes de sécurité et la connaissance des techniques d'attaques usuelles, cette formation vous donnera les moyens de sécuriser et d'auditer votre infrastructure Windows avec un maximum d'efficacité.

Objectifs

- Durcir un serveur Windows
- Administrer de façon sécurisée
- Sécuriser vos postes de travail
- Auditer votre infrastructure

Durée & horaires

- 5 jours soit 40 heures
- Du lundi au jeudi : de 9h00 à 12h et de 13h30 à 19h00.
- Le vendredi : de 09h00 à 12h et de 13h30 à 17h00/17h30.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Administrateurs
- Architectes
- Experts en sécurité
- Responsables sécurité

Pré-requis

- Formation SECUCYBER
- (ou) Expérience d'administration d'infrastructure Windows
- (ou) Solides bases en sécurité des systèmes d'information

Méthode pédagogique

- Cours magistral illustré par des travaux pratiques réguliers

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUWIN par HS2.**

Programme

Introduction

Module 1 : Durcissement système et réseau

- Système
  - Nécessité du durcissement
  - Minimisation
  - Gestion des services
  - Journalisation
- Réseau
  - Utilité des protocoles obsolètes
  - Cloisonnement réseau
    - Parefeu et IPsec
  - Protocoles d'authentification
  - Autres points d'attention
- Desired State Configuration
- Focus : sécuriser votre cloud Microsoft

Module 2 : Administration sécurisée

- Qu'est-ce qu'un administrateur
- Administration sécurisée : pourquoi ?
  - TTP : Techniques, Tactiques et Procédures
  - Compromettre un Active Directory
    - Compromission initiale
    - Mouvement latéral : Pass-the-hash...
    - Élévation de privilèges
  - Vulnérabilités classiques
- Bonnes pratiques
  - Utilisateurs et groupes locaux
  - Délégation
    - Powershell et le JEA
    - Active Directory et les GPO
- Administration sécurisée
  - Forêt "bastion"
  - Administration en strates
    - Silos d'authentification
  - Environnement d'administration
- Focus : Golden Ticket et krbtgt

Module 3 : Sécurité du poste de travail

- Windows 10 et le VBS
  - Secure Boot
  - Device Guard
  - Application Guard
  - Exploit Guard
  - Credential Guard
- Bitlocker
  - Chiffrement de disque
  - Autres fonctionnalités
- Isolation réseau
- Mise à jour

Module 4 : Auditer son infrastructure

- Différents types d'audits
- Points à auditer
- SCM
- Pingcastle
- Recherche de chemins d'attaque
  - BloodHound et AD-Control-Path
  - Les extracteurs
  - Graphes d'attaques
  - Simulation et remédiation
- Examen

Formation « Sécurité Linux »

Réf : SECULIN

Linux est le socle des infrastructures de l'internet, de l'informatique en nuage, comme des systèmes embarqués. Son durcissement et son maintien en condition de sécurité sont au cœur de la réussite de sa politique de sécurité.

Objectifs

- Gérer en profondeur les problèmes de sécurité liés aux systèmes Linux
- Réduire ou éliminer les risques sur les systèmes Linux
- Configurer les services courant pour qu'ils soient robustes avant mise en production (Apache, BIND, ...)
- S'assurer de l'intégrité des données sur les serveurs Linux
- Maîtriser les outils permettant de répondre aux incidents de sécurité
- Améliorer ses connaissances des procédures, bonnes pratiques et outils de sécurité du monde Unix

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Professionnels de la sécurité
- Administrateurs systèmes expérimentés
- Auditeurs et gestionnaires d'incidents
- Analystes en sécurité, auditeurs et membres de CSIRT (CERT)

Pré-requis

- Avoir les bases en administration de systèmes Unix, idéalement 3 à 5 ans d'expérience

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECULIN par HS2.**

Programme

Introduction
- Panorama de l'histoire des problèmes de sécurité
  - Suivre l'actualité
  - Implication des utilisateurs
  - Discipline des administrateurs
    - Sudo

Cryptographie
- Rappels sur le vocabulaire, les principes et les algorithmes
- SSH
- GnuPG
- Certificats X.509 et infrastructures à clés publiques
  - openssl
- Certificats X.509 pour le chiffrement, la signature et l'authentification
  - application à Apache et nginx
  - application à Postfix
- Systèmes de fichiers chiffrés
  - dm-crypt
  - eCryptfs
- DNS et cryptographie
  - DNSSEC

Sécurité de l'hôte
- Durcissement de l'hôte
  - configuration de GRUB
  - configuration du système
  - bonnes pratiques de configuration des daemons
  - Détection d'intrusion sur l'hôte
  - Syslog
  - comptabilité système (accounting)
  - audit
  - détection de rootkits
  - AIDE
- Gestion des utilisateurs et authentification
  - NSS
  - PAM

Contrôle d'accès
- Contrôle d'accès discrétionnaire
  - droits d'accès
  - ACL
- Contrôle d'accès obligatoire
  - SELinux

Sécurité réseau
- Durcissement du réseau
  - nmap
  - tcpdump
  - Wireshark
- Filtrage de paquets
  - concepts et vocabulaire
  - netfilter
  - TCP Wrapper
- Réseaux privés virtuels
  - OpenVPN

Examen de certification HS2 (QCM sur ordinateur)

Formation « Sécurité des Architectures »

Réf : SECUARCH

Vous vous demandez pourquoi ne pas laisser votre infrastructure reposer sur un réseau à plat ? Vous désirez migrer votre architecture dans le cloud ? Vous cherchez comment déployer une infrastructure de supervision de manière propre ? Répondez à ces questions et bien d'autres en (ré)apprenant les composants de base d'une architecture réseau complexe, les risques associés aux mises en œuvre courantes et le déploiement de certaines architectures spécifiques. Découvrez les moyens de réduire ces risques ainsi que les points d'attention à prendre en compte lors de chaque décision d'évolution de votre architecture.

Objectifs

- Connaître les problématiques liées à l'architecture des réseaux complexes
- Connaître les solutions associées
- Savoir auditer une architecture
- Développer un plan d'évolution sécurisée d'une architecture

Durée & horaires

- 3 jours soit 21 heures
- De 9h30 à 12h et de 13h30 à 17h30/18h00.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Architectes réseaux
- Administrateurs systèmes et réseaux
- Consultants en sécurité
- Auditeurs en sécurité
- RSSI

Pré-requis

- Bonnes connaissances en informatique
- Connaissances en réseaux
- Connaissances de base en sécurité

Méthode pédagogique

- Cours magistral
- Démonstrations
- Exercices de mise en œuvre

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUARCH par HS2.**

Programme

Introduction générale
- Logistique
- Tour de table
- Objectifs de la formation
- Non-objectifs de la formation
- Signalétique

Introduction de la formation
- Principes d'architecture
  - Exposition / connectivité / attractivité
- Vocabulaire
  - Segmentation
  - Vulnérabilité
  - Risque
- Lien avec d'autres domaines
  - Sécurité logicielle
  - Appréciation des risques
  - Architecture des systèmes d'information

Rappels
- Modèle OSI
- Domaine de collision, domaine de diffusion
- LAN, VLAN, PVLAN

Composants de base : pour faire quoi, pour ne pas faire quoi et points d'attention
- Commutateur
- Répartiteur
- Routeur
- Pare-feu
- Diode
- WDM
- Sondes
- IPS / IDS
- WAF

Architectures de base : risques, points d'attention et solutions
- Applications, 2-tiers / 3-tiers
  - Partages de contenu
- Administration
  - Administration de l'administration
- Active Directory
- Composants d'infrastructure et de sécurité
  - Filtrage et détection (Pare-feu, IDS, WAF)
  - DNS
  - NTP
  - Relais et relais inverses
  - Authentification
  - Supervision
  - Journalisation
  - Anti-virus
  - Mise à jour
  - Déploiement
  - Bastion

Architectures spécifiques
- Architectures industrielles & SCADA
- IoT
- Grid
- Architectures distribuées
- Cloud

Formation « Détection et réponse aux incidents de sécurité »

Réf : SECUBLUE

Les rapports de tous les grands acteurs de la réponse à incident sont unanimes : les compromissions, qu'elles soient l'œuvre de simples malwares ou de groupes organisés, sont légions, avec bien souvent un délai effarant de plusieurs mois entre l'arrivée de l'acteur malveillant et sa détection par les défenseurs. Dans ce contexte, la question n'est plus de savoir si cela peut nous arriver, mais bien QUAND cela va-t-il nous arriver ; L'enjeu n'est plus seulement de prévenir, mais d'aller traquer l'attaquant sur nos systèmes et réseaux afin de l'empêcher d'étendre son emprise et d'atteindre ses objectifs.

En mettant l'accent sur la compréhension des techniques d'attaque et la maitrise des outils de détection, cette formation vous donnera les moyens de tirer le meilleur parti des mesures et équipements déjà en place pour répondre rapidement et efficacement aux incidents de sécurité.

Objectifs

- **Mettre en place une architecture de détection**
- **Appliquer la notion de "prévention détective"**
- **Limiter l'impact d'une compromission**
- **Prioriser les mesures de surveillance à implémenter**
- **Maitriser le processus de réponse à incident**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Membres d'un SOC ou d'un CSIRT**
- **Administrateurs**
- **Analystes**
- **Responsables sécurité**

Pré-requis

- **Formation SECUCYBER**
- **(ou) Solides bases en sécurité des systèmes d'information**

Méthode pédagogique

- **Cours magistral avec travaux pratiques et échanges interactifs**

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUBLUE par HS2.**

Programme

Module 1 : État des lieux

- Pourquoi la détection
  - Défense en profondeur
  - Tous compromis
- Évolution de l'environnement
- La "prévention détective"

Module 2 : Comprendre l'attaque

- Objectifs de l'attaquant
- Phases d'une attaque
- Plusieurs champs de bataille
  - Réseau
  - Applications
  - Active Directory
  - La dimension métier
- Portrait d'une attaque réussie

Module 3 : Architecture de détection

- La base : segmentation et moindre privilège
- Les classiques
  - Parefeu
  - IDS/IPS
  - WAF
  - SIEM
- Les outsiders
  - "Self-defense" applicative
  - Honey-*
- Valoriser les "endpoints"
  - Whitelisting
  - Sysmon
  - Protections mémoire
  - Mesures complémentaires de Windows 10
- Focus : Journalisation
- Les IOC
  - Yara
  - MISP

Module 4 : Blue Team vs. attaquant

- Gérer les priorités
- Détection et kill chain
  - Persistance
  - Post-exploitation
  - Exploitation
  - Reconnaissance
- Focus: détecter et défendre dans le Cloud

Module 5 : Réponse à incident et Hunting

- Le SOC
- Outils de réponse
  - Linux
  - Windows
  - Kansa
- Partons à la chasse
  - Principes de base
- Attaquer pour mieux se défendre
  - Audit "Purple team"
  - Focus: Bloodhound
- ISO 27035
- Aspects juridiques

Formation « Analyse inforensique Windows »

Réf : FORENSIC1

Les raisons ne manquent pas de vouloir effectuer une analyse inforensique :

- **Collaborateur indélicat ayant volé des documents interne de valeur**
- **Intrusion d'un poste suite à une erreur d'un utilisateur**
- **Compromission d'un serveur**

Quelle que soit la raison, FORENSIC 1 vous apprendra à analyser les différents artefacts inforensiques et finalement créer une frise chronologique de l'incident.

Objectifs

- **Gérer une investigation numérique sur un ordinateur Windows**
- **Avoir les bases de l'analyse numérique sur un serveur Web**
- **Acquérir les médias contenant l'information**
- **Trier les informations pertinentes et les analyser**
- **Utiliser les logiciels d'investigation numérique**
- **Maîtriser le processus de réponse à incident**

Durée & horaires

- **5 jours soit 35 heures**
- **Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.**
- **Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.**

Nombre de participant

- **Minimum 8 participants – Maximum 24 participants**

Public visé

- **Personnes souhaitant apprendre à réaliser des investigations numériques**
- **Personnes souhaitant se lancer dans l'inforensique**
- **Administrateurs système Windows**
- **Experts de justice en informatique**

Pré-requis

- **Formation SECUCYBER**
- **(ou) Solides bases en sécurité des systèmes d'information**

Méthode pédagogique

- **Cours magistral illustré par des travaux pratiques réguliers**

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Clé USB 64Go avec les données utilisées en travaux pratiques**
- **Kit d'investigation numérique**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification FORENSIC1 par HS2.**

Programme

Jour 1

- Présentation de l'inforensique
- Périmètre de l'investigation
- Trousse à outil
- Méthodologie "First Responder"
- Analyse Post-mortem
- Disques durs
- Introduction aux systèmes de fichiers
- Horodatages des fichiers
- Acquisition des données : Persistante et volatile
- Gestion des supports chiffrés
- Recherche de données supprimées
- Sauvegardes et Volume Shadow Copies
- Aléas du stockage flash
- Registres Windows
- Les structures de registres Windows
  - Utilisateurs
  - Systèmes
- Analyse des journaux
- Évènements / antivirus / autres logiciels

Jour 2 - Scénario d'investigation

- Téléchargement/Accès à des contenus confidentiels
- Exécution de programmes
- Traces de manipulation de fichiers et de dossiers
- Fichiers supprimés et espace non alloué
- Carving
- Géolocalisation
- Photographies (données Exifs)
- Points d'accès WiFi
- HTML5
- Exfiltration d'informations
- Périphérique USB
- Courriels
- Journaux SMTP
  - Acquisition coté serveur
  - Analyse client messagerie
- Utilisateurs abusés par des logiciels malveillants

Jour 3 - Interaction sur Internet

- Utilisation des Navigateurs Internet
- IE/Edge / Firefox
- Office 365
- Sharepoint
- Traces sur les AD Windows
- Présentation des principaux artefacts
- Bases de l'analyse de la RAM
  - Conversion des hyberfiles.sys
  - Bases Volatility/Rekall
  - Extraction des clés de chiffrement

Jour 4 - Inforensique Linux

- Les bases de l'inforensique sur un poste de travail Linux"
- Les bases de l'inforensique sur un serveur Linux
  - Journaux serveurs Web & Corrélations avec le système de gestion de fichiers
- Création et analyse d'une frise chronologique du système de fichier

Jour 5 - Vue d'ensemble

- Création et analyse d'une frise chronologique enrichie d'artefacts
- Exemple d'outil d'interrogation de gros volume de données
- Examen de certification HS2 (QCM sur ordinateur)

Formation « Analyse inforensique avancée »

Réf : FORENSIC2

La vraisemblance que votre entreprise ou que vos clients soient la victime d'une intrusion est importante. L'objectif de la formation est alors de vous préparer au mieux en vous présentant des techniques et des outils permettant de répondre à un incident de sécurité (du simple prestataire malveillant à des attaques plus complexes). L'ensemble de la formation sera réalisée autours d'un cas fictif d'une compromission d'une entreprise de taille intermédiaire afin de présenter les procédures et techniques à mettre en place permettant d'être scalable en fonction de la taille de votre entreprise.

Objectifs

- Appréhender la corrélation des évènements
- Retro-concevoir des protocoles de communications
- Analyser des systèmes de fichiers corrompus
- Connaître et analyser la mémoire volatile des systèmes d'exploitation

Durée & horaires

- 5 jours soit 35 heures
- Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 17h00/17h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Investigateurs numériques souhaitant progresser
- Analystes des SOC et CSIRT (CERT)
- Administrateurs système, réseau et sécurité
- Experts de justice en informatique

Pré-requis

- Avoir une bonne expérience opérationnelle en informatique
- Avoir une expérience en analyse post-mortem sous Windows et maitriser le processus d'investigation sur un poste Windows
- Ou avoir réussi la certification HS2 INFORENSIC1 ou la certification HSC INFO1 ou la certification CEH CHFI ou une des certifications GIAC GCFA ou GCFE

Méthode pédagogique

- Cours magistral illustré par des travaux pratiques réguliers

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Cahier d'exercices et corrections des exercices
- Clé USB 64Go avec les données utilisées en travaux pratiques
- Certificat attestant de la participation à la formation

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification FORENSIC2 par HS2.**

Programme

Section 1 : Introduction à l'inforensique réseau

- Incident de sécurité
  - Présentation
    - Quels sont les étapes d'une intrusion ?
    - Quels impacts de celles-ci ?
- Indices de compromission (IOC)
  - Introduction au threat intel (Misp, Yeti, etc.)
  - Quels sont les outils / ressource à disposition ?
  - Création d'IOC
- Hunting & Triage (à distance ou en local)
  - GRR
  - Kansa
  - OS Query
  - Comment analyser et automatiser l'analyse du résultat de notre hunting ?
    - NSRLDB
    - Packing/Entropie/, etc…

Section 2 : Analyse post-mortem réseau

- Analyse des journaux des principaux services réseau (DNS, HTTP, SGBD, Pare-feux, Syslog)
- Analyse de capture réseau (PCAP)
- Analyse statistique des flux (Netflow)
- Canaux de communications avec les serveurs de Command and Control
- Détection des canaux de communications cachées (ICMP, DNS)
- Détection des techniques de reconnaissances
- Création de signatures réseaux

Section 3 : Mémoire volatile

- Introduction aux principales structures mémoires
- Analyse des processus
  - Processus "cachés"
  - Traces d'injection de code et techniques utilisées
    - Process-Hollowing
- Shellcode - détection et analyse du fonctionnement
- Handles
- Communications réseaux
- Kernel : SSDT, IDT, Memory Pool
- Utilisation de Windbg
  - Création de mini-dump
  - Analyse "live" d'un système

Section 4 : FileSystem (NTFS only)

- Introduction au FS NTFS et aux différents artefacts disponibles
- Présentation de la timerules sous Windows/Linux/OSX
- Timeline filesystem
  - Timestomping + toutes les opérations pouvant entravers une timeline "only fs"

Section 5 : Trace d'exécution et mouvement latéraux

- Trace de persistances
  - Autostart (Linux/Windows/OSX)
  - Services
  - Tâches planifiées
  - WMI
- Active Directory - Détecter une compromission
  - Comment générer une timeline des objets AD ?
  - Recherche de "backdoor" dans un AD (bta, autres outils, ...)
  - Présentation des principaux EventID et relations avec les outils d'attaques (golden ticket, etc.)

Section 6 : Super-Timeline

- Présentation
  - Cas d'utilisations
    - Timesketch

Section 7 : Quizz de fin de formation

Formation « Rétroingénierie de logiciels malfaisants »

Réf : REVERSE1

Comprendre le fonctionnement des logiciels malveillants est un élément clé nécessaire auprès des entreprises afin de pouvoir répondre de manière plus efficiente à vos incidents de sécurités. L'objectif de cette information est de fournir les éléments clés permettant de comprendre le fonctionnement des logiciels afin de pouvoir créer des "Indicateurs de Compromission" ainsi que des signatures permettant de détecter des versions modifiées des outils malveillants afin de détecter les mises à jour de ceux-ci sans avoir besoin de mettre à jours vos signatures. La formation vous permettra alors de pouvoir analyser tout type de menace, du client lourd à l'application "Flash" en passant par les documents malicieux (office, PDF) en passant par les sites web malveillants et les applications mobiles.

Objectifs

- Qualifier la menace d'un logiciel malfaisant
- Savoir mettre en place d'un laboratoire d'analyse des logiciels malfaisants et préparer l'outillage d'analyse
- Analyser de manière statique et dynamique le comportement de logiciels malfaisants
- Apprendre l'architecture x86
- Savoir identifier les structures logiques (boucles, branchement...)
- Savoir identifier des motifs utilisés par les logiciels malfaisants en analysant le code
- Analyser la mémoire
- Savoir contourner les techniques d'autoprotection

Durée & horaires

- 5 jours soit 35 heures
- Horaires : de 9h30 à 12h et de 13h30 à 18h00/18h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Membres d'un SOC ou d'un CSIRT
- Équipes de réponse aux incidents
- Toute personne souhaitant réaliser des analyses avancées des menaces
- Toute personne intéressée par l'analyse des logiciels malfaisants
- Professionnel de la sécurité souhaitant acquérir des connaissances en analyse de codes malfaisants
- Analystes
- Responsables sécurité

Pré-requis

- Connaître le système Windows
- Savoir programmer
- Avoir les bases en réseau
- Connaître l'assembleur

Méthode pédagogique

- **Cours magistral illustré par des travaux pratiques réguliers**

Supports

- **Support de cours au format papier en français**
- **Ordinateur portable mis à disposition du stagiaire**
- **Cahier d'exercices et corrections des exercices**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification FORENSIC2 par HS2.**

Programme

Section 1 : Introduction aux bases de l'analyse de logiciels malveillants

- Processus et méthodologie générique
- Analyse statique :
  - Analyse des métadonnées
  - Analyse statique
- Analyse dynamique
  - Comportemental
  - Débugger
- Construire son laboratoire d'analyse
  - Simuler internet
  - Utilisation de la virtualisation
    - Contournement des mécanismes de protection anti-VM
    - Simulation d'architecture "exotique" (IOT)
    - Construction du laboratoire et boite à outils
  - Sandbox

Cas d'analyse

- Introduction au langage assembleur
  - Guide de survie des instructions de bases
  - Instruction modifiant le flux d'exécution
  - Présentation des registres
- Conventions d'appels
  - Spécificités des langages objets
- IDA Pro:
  - Introduction
  - Prise en main de l'outil (création de scripts)
- Chaine de compilation et binaires
  - Fuite d'informations possibles
  - Imports d'information dans IDA

Section 2 : Système d'exploitation

- Introduction aux systèmes d'exploitation
  - Processus vs thread
  - Scheduler
  - Syscall
  - Différence processus vs thread
- Format d'exécutable
  - Format PE
    - Présentation des informations
- Structures internes
  - SEH
  - TEB
  - PEB
  - SSDT
- Introduction au "kernel debugging"

Section 3 : Mécanismes de protection (DRM ou packer)

- Introduction aux outils de DRM/Protection de code
  - Comment les identifier ?
    - Quels sont les impacts ?

- -- Introductions aux différentes techniques de protection :
  - Anti-désassemblage
  - Anti-debogage
  - Obscurcissement du CFG
  - Machine virtuelle
  - Évasion (détection de sandbox/Virtualisation)
- Analyse de packer
  - Présentation de la méthode générique d'unpacking
  - Découverte de l'OEP
  - Reconstruction de la table d'imports
    - Miasm2 :
      - Unpacking automatique
  - Technique de contournement de flux d'exécution (ie: detour)
- Shellcode
  - Techniques et outils d'analyses
  - Miasm2
  - Unicorn Engine

Section 4 : Malwares

- Catégoriser les logiciels malveillants en fonction de leurs API
- Keyloggers
- Rootkits (userland et kerneland)
- Sniffers
- Ransomwares
- Bots et C2
- Injection de code

Section 5 : Autres types de malwares

- Malware "Web" (JavaScript/VBScript)
  - Analyse statique et dynamique
  - Limitation des navigateurs
- Malwares Flash
- Applications mobiles Android
- Documents malveillants
-
  - Suite Office
  - PDF
  - RTF
- Malwares .Net

Section 6 : Threat Intelligence

- Création de signatures Yara
- Communication et base de connaissances
  - MISP
  - Yeti

Section 7 : Avantage de l'analyse mémoire

Formation « Tests d'intrusion »

Réf : PENTEST1

Réaliser des tests d'intrusion est la méthode la plus efficace pour mettre en évidence les vulnérabilités qui seront exploitées par vos adversaires. Découvrez ces vulnérabilités par vous-même avant que celles-ci soient exploitées par d'autres !

Objectifs

- Préparer un test d'intrusion réussi
- Maîtriser toutes les phases d'un test d'intrusion (de la découverte à la post exploitation)
  - Découvrir facilement et rapidement le réseau cible
  - Exploiter en toute sécurité les vulnérabilités identifiées
  - Élever ses privilèges pour piller les ressources critiques
  - Rebondir sur le réseau compromis
- Comprendre les vulnérabilités exposées par les réseaux externes et internes
- Utiliser efficacement la trousse à outils du pentester

Durée & horaires

- 5 jours soit 35 heures
- Horaires : Du lundi au jeudi : de 9h30 à 12h et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h et de 13h30 à 16h00/16h30

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Pentesters
- Consultants SSI
- RSSI
- Architectes

Pré-requis

- Des notions en IT et/ou SSI
- Des notions d'utilisation d'une distribution Linux est un plus

Méthode pédagogique

- Cours magistral illustré par des travaux pratiques réguliers

Supports

- Support de cours numérique en Français projeté
- Support de cours en Français imprimé
- Cahier d'exercices
- Cahier de corrections
- Ordinateur portable mis à disposition pour la réalisation des exercices

Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration

Certification

- **A l'issue de cette formation, le stagiaire a la possibilité de passer un examen ayant pour but de valider les connaissances acquises. Cet examen de type QCM dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification PENTEST1 par HS2.**

Programme

Introduction aux tests d'intrusion
- Équipement et outils
- Organisation de l'audit
- Méthodologie des tests d'intrusion
- Gestion des informations et des notes
- Exemple de bon rapport d'audit
- Les meilleurs pratiques : PASSI

Rappels et bases
- Les shells Unix *sh
- Les shells Windows cmd & powershell
- Rappels sur les réseaux tcp/ip
- Rappels du protocole HTTP
- Introduction à Metasploit
  - Exploits et Payloads
  - Fonctionnalités utiles
  - Base de données
- Modules
- Customisation
- ***Mises en pratique***

Découverte d'information
- Reconnaissance de la cible
  - Open Source Intelligence
- Découverte passive du SI
  - Ecoute réseau
- Scans réseau
  - Cartographie du réseau
  - Découverte de services
  - Identification des Systèmes d'exploitation
- Scanners de vulnérabilités
  - Scanner Open Source Openvas
- ***Mises en pratique***

Mots de passe
- Attaques en ligne
  - Brute force en ligne
  - Outils Open Source
- Attaques hors ligne
  - Analyse d'empreintes
  - Méthodologies de cassage
  - Les Raibow Tables
  - Outils Open Source
- ***Mises en pratique***

Exploitation
- Identification des vulnérabilités
  - Contexte des vulnérabilités
  - Étude de divers types de vulnérabilités

- Méthodologie d'exploitation
  - Identifier le bon exploit ou le bon outil
  - Éviter les problèmes
  - Configurer son exploit
- Exploitations à distance
- Exploitations des clients
- ***Mises en pratique***

Post-exploitation
- Le shell Meterpreter et ses addons
- Élévation de privilèges
- Fiabiliser l'accès
- Pillage
  - Vol de données
  - Vol d'identifiants
- Rebond
  - Pivoter sur le réseau
  - Découvrir et exploiter de nouvelles cibles
- ***Mises en pratique***

Intrusion web
- Méthodologie d'intrusion WEB
- Utilisation d'un proxy WEB
  - Proxy Open Source ZAP
- Usurpation de privilèges
  - CSRF
- Les injections de code
  - Côté client : XSS
  - Côté serveur : SQL
- Compromission des bases de données
- Autres types d'injections
- Les inclusions de fichiers
  - Locales
  - A distance
- Les webshells
  - Précautions d'emploi
- ***Mises en pratique***

Intrusion windows
- Méthodologie d'intrusion Windows

- Découverte d'informations
  - Identification de vulnérabilités
  - Techniques de vols d'identifiants
- Réutilisation des empreintes
  - Technique de "Pass The Hash"
- Élévation de privilèges
  - Locaux
  - Sur le domaine : BloodHound
- Échapper aux anti-virus
  - Techniques diverses
  - Outil Open Source Veil
- Outillage powershell
  - Framework Open Source PowerShell Empire
- ***Mises en pratique***

Intrusion Unix/Linux

- Méthodologie d'intrusion Linux
  - Rappels sur la sécurité Unix
- Découverte d'informations
  - Identifications de vulnérabilités
- Elévation de privilèges
  - Abus de privilèges
  - Exploitation de vulnérabilités complexes
- ***Mises en pratique***

Plans de formation bientôt disponibles

Réf : SECURSF Formation « Sécurité des réseaux sans fil »

- **Objectif :** Comprendre les vulnérabilités des infrastructures sans fil et comment les sécuriser.

Réf : PENTEST2 Formation « Tests d'intrusion et développement d'exploits»

- **Objectif :** Sécurité offensive de niveau avancé pour les pentesters expérimentés.

Nos Intervenants
Formations en vie privée, droit de la cybersécurité

François Coupez dispense la formation :
DPO

Pierre Desmarais dispense les formations :
RGPD - DPO - SECUSANTE

Hadi Elkhoury dispense les formations :
RGPD - DPO - PIA

Raoul Fuentes dispense les formations :
SECUDROIT - SECUCLOUD

Olivier Iteanu dispense les formations :
SECUDROIT - SECUCLOUD

Alexandre Magloire dispense la formation :
SECUSANTE

Diane Rambaldini dispense les formations :
RGPD - DPO - PIA

Hervé Schauer dispense la formation :
SECUCLOUD

Nos Intervenants
Formations en continuité d'activité et cybersécurité organisationnelle

Jean-Luc Austin dispense la formation :
CISA

Tony Belot dispense les formations :
RSSI - ISO27LA - ISO27LI - ISO27RM

Pierre-Antoine Bonifacio dispense les formations :
CISSP

Matthieu Caron dispense la formation :
CISSP

Thierry Chiofalo dispense la formation :
ISO27004

Lucien Caumartin dispense la formation :
ISO27LA

Laurent Doublein dispense les formations :
RPCA - ISO22LA - ISO22LI

Alexandre Fernandez-Toro dispense la formation :
ISO27LA - ISO27LI

Raoul Fuentes dispense la formation :
RSSI

Jordan Hordé dispense la formation :
ISO27LA - ISO27LI - ISO27RM - EBIOS2010 - EBIOS2018

Béatrice Joucreau dispense les formations :
ISO22LA - ISO27LA - ISO27RM

Anthony Hubbard dispense la formation :
RSSI - ISO27LA - ISO27LI

Thomas Le Poëtvin dispense les formations :
SECUCRISE - EBIOS2010 - ISO27LA - ISO27LI - ISO27RM

Julien Levrard dispense la formation :
ISO27LI

Alexandre Magloire dispense les formations :
SECUHOMOL - EBIOS2010 - EBIOS2018

Lionel Mourer dispense la formation :
RPCA - ISO22LA - ISO22LI - ISO27035

Paul Pennaneac'h dispense les formations :
RSSI - SECUHOMOL - ISO27LI

Hervé Schauer dispense la formation :
RSSI - ISO22LI - ESS27 - ISO27LA - ISO27LI - ISO27RM - ISO27004

Matthieu Schipman dispense les formations :
RSSI - CISSP

Thomas Seyrat dispense la formation :
RSSI

Mikaël Smaha dispense les formations :
SECUCRISE - EBIOS2010 - EBIOS2018 - ISO27RM

Alphonsine Yacoubou-Djima dispense les formations :
ISO27LA - ISO27LI

Jamal Saad dispense la formation :
ESS27

Nos Intervenants
Formations cybersécurité technique

Pierre-Antoine Bonifacio dispense les formations :
SECUPKI - PKIWINDOWS

Stéphane Bortzmeyer dispense la formation :
DNSSEC

Johann Broudin dispense les formations :
PENTEST1 - PENTEST2

Marc Baudoin dispense la formation :
SECULIN

Danil Bazin dispense les formations :
ESSCYBER - FORENSIC1 - FORENSIC2

Matthieu Caron dispense les formations :
SECUCYBER - SECUWEB - SECUBLUE - PENTEST1 - PENTEST2

Rémi Chauchat dispense les formations :
SECUINDUS - SECURSF - PENTEST1

Romain Coltel dIspense la formation :
PENTEST2

Jordan Hordé dispense la formation :
SECUARCH

Olivier Houssenbay dispense la formation :
SECWIN

Baptiste Dolbeau dispense la formation :
FORENSIC1

Anthony Hubbard dispense la formation :
SECUBLUE

Stefan Le Berre dispense la formation :
FORENSIC1 - FORENSIC2 - REVERSE1

Jérôme Naucelle dispense la formation :
SECUWEB

Christophe Renard dispense les formations :
SECUBLUE - SECUINDUS

Julien Reveret dispense la formation :
FORENSIC1

Inês Ribeiro dispense la formation :
PENTEST1

Matthieu Schipman dispense les formations :
ESSCYBER - SECUCYBER - SECUBLUE - SECUWIN

Mikaël Smaha dispense la formation:
SECUARCH

Cyril Solomon dispense les formations :
FORENSIC1 - FORENSIC2 - REVERSE1

Hervé Schauer dispense la formation :
SECUINDUS

Arnaud Soullié dispense la formation :
SECUINDUS

HS2
Hervé Schauer Sécurité

Bulletin d'inscription

Merci de retourner ce bulletin soit par courrier à HS2 – 10, rue des Poissonniers – 92200 Neuilly-sur-Seine –
Soit par courriel à formation@hs2.fr

Responsable Formation

Nom et Prénom : .....
Fonction : ..... Société : .....
Adresse : .....
Code postal : ..... Ville : .....
Tél. : ..... E-mail : .....

Souhaite inscrire la ou les personne(s) suivante(s) au(x) stage(s) mentionné(s) :

- Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

- Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

- Nom et Prénom : .....
Fonction : .....
Tél. : ..... E-mail : .....
Intitulé de la formation choisie : .....
Date de session : .....
Pour les formations certifiantes, présentation à l'examen : oui ❍ non ❍

Adresse de facturation (si différente)

Société : ..... Adresse : .....
Code postal : ..... Ville : .....
Nom du correspondant : ..... Tél. : .....
E-mail : .....
N° de TVA intracommunautaire .....

Établissez-vous des bons de commande avec des références à reporter sur notre facture ? oui ❍ non ❍
Si oui, l'inscription sera confirmée uniquement à réception de votre bon de commande.

Demande de subrogation via votre OPCA* : oui ❍ non ❍
*Dans le cas d'une subrogation de paiement via votre OPCA, l'inscription sera confirmée uniquement à réception du contrat ou de l'accord de prise en charge de votre OPCA et de notre convention de formation signée et tamponnée

Date :
Cachet et signature de l'employeur

Convention de formation : pour chacune des sessions proposées, une convention de formation est disponible sur simple demande.
Attention, la prise en compte de votre demande d'inscription sera effective uniquement à réception d'un mail de confirmation par nos services.
Pour tout renseignement complémentaire, vous pouvez contacter le service formation par mail à formation@hs2.fr ou par téléphone au +33 974 774 390.

Retrouvez-nous sur notre site : **www.hs2.fr**

Renseignement / inscription à nos formations, n'hésitez pas à nous contacter :

Elisa Keller / Claire Monet / Olivier Dumont

☎ +33 (0)974 774 390

☞ formation@hs2.fr

Déclaration d'activité enregistrée sous le numéro 11922236092
auprès du préfet de région d'Ile-de-France

Pour nous contacter :

☎ +33 (0)974 774 390 / +33 (0)644 014 072

formation@hs2.fr

Pour nous suivre :

@HS2formation

@HS2formation

@HS2formation

Datadock
Organisme
Référencé