Catalogue de formations 2023

Vie privée,
Droit de la cybersécurité

Continuité d'activité

Cybersécurité organisationnelle

Cybersécurité technique

HS2
Hervé Schauer Sécurité

SOMMAIRE ET CALENDRIER

Vie privée, droit de la cybersécurité

Continuité d'activité

***Examen de certification HS2 inclus**
***Examen de certification AFNOR certification inclus**
***Examen de certification Certi-Trust inclus**

Cybersécurité organisationnelle				
Réf.	Formations	Durée	Sessions	Pages
RSSI*	Formation RSSI	**5 j**	• 20 au 24 mars 2023 • 22 au 26 mai 2023 • 3 au 7 juillet 2023 • 25 au 29 septembre 2023 • 6 au 10 novembre 2023 • 11 au 15 décembre 2023	**31-34**
SECUPROJET	Security by Design	**2 j**	• 26 au 27 juin2023 • 5 au 6 octobre 2023	**35-36**
CISSP*	Préparation au CISSP	**5 j**	• 6 au 10 mars 2023 • 26 au 30 juin 2023 • 2 au 6 octobre 2023 • 4 au 8 décembre 2023	**37-38**
CCSP*	Préparation au CCSP	**5 j**	• 6 au 10 février 2023 • 20 au 24 novembre 2023	**39-40**
CISA	Préparation au CISA	**5 j**	• 13 au 17 mars 2023 • 13 au 17 novembre 2023	**41-42**
SECUHOMOL	Homologation de la SSI	**1 j**	• 10 mai 2023 • 10 novembre 2023	**43-44**
SECUCRISE	Gestion de crise cyber	**2 J**	• 1 au 2 juin 2023 • 19 au 20 octobre 2023	**45-46**
EBIOS2018*	EBIOS RM 2018 Risk Manager		• 6 au 8 Févier 2023 • 17 au 19 avril 2023 • 10 au 12 mai 2023 • 26 au 28 juin 2023 • 16 au 18 octobre 2023 • 4 au 6 décembre 2023	**47-48**
ESS27	Essentiels ISO27001 & ISO27002	**2 J**	• 30 au 31 mai 2023 • 30 au 31 octobre 2023	**49-50**
MAJ27	Mise à jour ISO 27001 & ISO 27002	**1 J**	• 3 avril 2023 • 30 juin 2023 • 8 septembre 2023	**51-52**
ISO27LA*	ISO 27001 Lead Auditor	**5 J**	• 19 au 23 juin 2023 • 20 au 24 novembre 2023	**53-54**
ISO27LI*	ISO 27001 Lead Implementer	**5 J**	• 6 au 10 mars 2023 • 12 au 16 juin 2023 • 18 au 22 septembre 2023 • 13 au 17 novembre 2023 • 18 au 22 décembre 2023	**55-56**
IS027RM*	ISO 27005 Risk Manager	**3 J**	• 1er au 3 février 2023 • 12 au 14 avril 2023 • 31 mai au 2 juin 2023 • 11 au 13 septembre 2023 • 6 au 8 novembre 2023 • 27 au 29 novembre 2023	**57-58**
ISO27004	ISO27004 / Indicateurs et tableaux de bord cybersécurité	**1 J**	• 5 juin 2023 • 2 novembre 2023	**59-60**

ISO27035	ISO27035 / Gestion des incidents de sécurité	**1 J**	• 6 juin 2023 • 3 novembre 2023	**61-62**

***Examen de certification HS2 inclus** ***Examen de certification AFNOR certification inclus** ***Examen de certification Certi-Trust inclus**

Cybersécurité technique

Réf.	Formations	Durée	Sessions	Pages
ESSCYBER	Essentiels techniques de la cybersécurité	**2 j**	• 2 au 3 février 2023 • 15 au 16 mai 2023 • 7 au 8 septembre 2023 • 9 au 10 novembre 2023	**63-64**
SECUCYBER*	Fondamentaux techniques de la cybersécurité	**5 j**	• 27 au 31 mars 2023 • 5 au 9 juin 2023 • 11 au 15 septembre 2023 • 13 au 17 novembre 2023	**65-66**
SECUINDUS*	Cybersécurité des systèmes industriels	**4 j**	• 27 février au 2 mars 2023 • 30 mai au 2 juin 2023 • 18 au 21 septembre 2023 • 20 au 23 novembre 2023	**67-68**
SECUOBJ*	Sécurité des objets connectés	**3 J**	• 15 au 17 mai 2023 • 23 au 25 octobre 2023	**69-70**
DNSSEC	DNSSEC	**2 J**	• 2 au 3 novembre 2023	**71-72**
SECUMOBILE*	Audit sécurité d'applications mobiles Android et iOS	**3 J**	• 9 au 11 octobre 2023	**73-75**
SECUPKI*	Infrastructures de clés publiques		• 19 au 21 juin 2023	**76-78**
SECUPKIWIN*	Infrastructures de clés publiques Windows	**3 J**	• 18 au 20 septembre 2023	**79-80**
SECUWEB*	Sécurité des serveurs et des applications Web	**5 J**	• 22 au 26 mai 2023 • 25 au 29 septembre 2023	**81-83**
SECUWIN*	Sécurisation des infrastructures Windows	**5 J**	• 19 au 23 juin 2023 • 9 au 13 octobre 2023 • 18 au 22 décembre 2023	**84-85**
SECULIN*	Sécurité Linux	**5 J**	• 11 au 15 décembre 2023	**86-87**
SELINUX	Comprendre SELinux et savoir modifier la politique de sécurité	**2 J**	• 3 au 4 avril 2023 • 26 au 27 octobre 2023	**88-89**
SECUARCH*	Conception d'architectures sécurisées	**5 J**	• 24 au 28 avril 2023 • 25 au 29 septembre 2023 • 6 au 10 novembre 2023	**90-91**
PENTESTWIFI	Sécurité et Red Team Wi-Fi moderne	**2 J**	• 10 au 11 mai 2023	**92-93**
OSINT	OSINT/CTI	**3 J**	• 10 au 12 mai 2023	**94-95**
SECUBLUE1*	Surveillance, détection et réponse aux incidents de sécurité	**5 J**	• 22 au 26 mai 2023 • 16 au 20 octobre 2023	**96-97**
SECUSOC*	Détection des incidents de sécurité	**5 J**	• 20 au 24 mars 2023 • 27 nov. au 1er déc. 2023	**98-99**
FORENSIC1*	Analyse inforensique Windows	**5 J**	• 17 au 21 avril 2023 • 18 au 22 septembre 2023	**100-101**
FORENSIC2*	Analyse inforensique avancée	**5 J**	• 2 au 6 octobre 2023	**102-103**
REVERSE1*	Rétroingénierie de logiciels malfaisants	**5 J**	• 23 au 27 novembre 2023	**104-106**

PENTEST1*	Tests d'intrusion	**5 J**	• 13 au 17 mars 2023 • 16 au 20 octobre 2023	**107-109**
PENTEST2*	Tests d'intrusion et développement d'exploits	**5 J**	• 23 au 27 novembre 2023	**110-111**
PENTESTINDUS*	Tests d'intrusion des systèmes industriels	**3 J**	• 4 au 8 décembre 2023	**112-113**
PENTESTWEB*	Test d'intrusion des serveurs et des applications Web	**5 J**	• 9 au 13 octobre 2023	**115-117**
SPLUNK*	SPLUNK	**3 J**	• 27 au 29 mars 2023 • 27 au 29 novembre 2023	**118-120**
Nos intervenants				**121-125**
Bulletin d'inscription				**126**

***Examen de certification HS2 inclus**

Formation
« RGPD : les fondamentaux de la protection des données »

Réf : RGPD

Le mot « RGPD » est sur toutes les lèvres depuis l'entrée en application, il y a plus d'un an, du règlement général n°2016/679 sur la protection des données. Les principes directeurs de la conformité et les principaux points d'achoppement du texte apparaissent aujourd'hui. Projet transversal et pluridisciplinaire qui implique tous les collaborateurs de l'entreprise, le RGPD est difficile de lecture et d'application. L'objectif de cette formation courte est d'en donner une vision d'ensemble et de livrer ses notions clés. Elle délivre la base de connaissance nécessaire pour traiter les questions récurrentes et prendre part aux projets comprenant des données personnelles.

Objectifs

- Connaître le règlement et les évolutions apportées par celui-ci
- Avoir une vision d'ensemble de la protection des données personnelles
- Maîtriser les notions clés du RGPD et comprendre ses implications opérationnelles

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

- Chef de projet
- RSSI, DSI
- Directions
- Juriste
- Consultant en protection des données
- DPO, DRPO et futur DPO

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
- Certificat de réussite de l'examen final

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 RGPD 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 « Métier de DPO »

Pratiques et Échanges entre professionnels

Réf : MDPO

La formation Métier de DPO est dédiée aux DPO (ou délégués à la protection des données) et à toute personne en charge de la protection de la vie privée.
L'objectif de la formation est de permettre aux professionnels de la protection des données d'échanger entre eux et d'adresser leurs questions tant juridiques et pratiques aux formateurs.
L'approche de cette formation se veut opérationnelle et pragmatique. Ainsi, son programme prend la forme d'un plan d'action du DPO.

Objectifs

- **Connaître le métier de DPO : ses missions, ses responsabilités et son positionnement**
- **Créer un espace d'échanges entre professionnels de la protection des données**
- **Présenter un plan d'action pour un DPO fraîchement nommé**
- **Réaliser des focus sur les sujets complexes régulièrement rencontrés par les DPO**

Durée & horaires

- **5 jours, soit 35h00**
- **Horaires : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.**

Nombre de participant

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

Public visé

- **DPO**
- **Adjoints au DPO**
- **Relais ou référents informatique et libertés**
- **Consultants conseils en protection des données**
- **Et plus généralement toute personnes ayant une expérience en matière de protection des données et souhaitant approfondir ses connaissances métier**

Pré-requis

- **Avoir une bonne expérience professionnelle dans le secteur de la protection des données**
- **Connaître les exigences légales et réglementaires applicables en la matière**

Méthode pédagogique

- **Une formation construite sous l'angle d'un plan d'action du DPO**
- **Une présentation des exigences légales et réglementaires, des enjeux opérationnels qui en découlent et des retours d'expérience des formateurs ainsi que des participants**
- **Des focus sur les sujets de droit complexes régulièrement rencontrés par les DPO**
- **Des exercices pratiques individuels ou en groupe effectués par les stagiaires, basés sur des études de cas, permettant de se confronter à des situations réelles**
- **La création d'un espace d'échange entre professionnels de la protection des données**

Supports

- **Support de cours au format papier en français ;**
- **Cahier d'exercices et corrections des exercices ;**
- **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 n'est pas certifiante.**

Programme

0 – Introduction

1 – Je décroche un poste de DPO

1.1 – Mon statut
1.2 – Mes compétences
1.3 – Mon positionnement
1.4 – Mes missions
1.5 – Ma prise de fonctions

2 – Je prends mes fonctions, j'identifie l'existant

2.1 – Identifier l'existant et Définir le contexte
2.2 – Gérer un projet

3 – Je pilote la cartographie des traitements

3.1 - Dresser le registre des activités de traitement
3.2 - Identifier les traitements critiques et comprendre leur écosystème

4- Je me présente et j'instaure les bons réflexes

4.1 – Former, sensibiliser et communiquer
4.2 – Déployer les premiers processus prioritaires

5 – J'attaque la mise en conformité de l'existant, je priorise les actions

5.1 - Priorisation et plan d'action
5.2 - Mise en conformité des traitements
5.3 - Gérer les droits des personnes et les réclamations
5.4 - Gérer les partenaires

6 - Je gère les risques sur la vie privée et les mesures de sécurité associées

6.1 - Réaliser les PIA
6.2 - Assurer la sécurité des données
6.2.1 La sécurité, une approche par le risque
6.2.2 Gestion des incidents
6.2.3 Surveillance et amélioration continue

7 – La gouvernance de la protection des données

7.1 - Politiques et procédures
7.2 - Suivi et communication des chantiers
7.3 - Management de la protection des données
7.4 - Opportunité de la certification ?

8 - Je me prépare à un contrôle de la CNIL

Formation « DPO »

Réf : DPO

La formation certifiante par excellence pour devenir Data Protection Officer (DPO) ou confirmer ses compétences de DPO.
Notre formation est enregistrée par AFNOR Certification comme prérequis à la certification de compétences des DPO.
AFNOR Certification est historiquement le 1er organisme certificateur agréé par la CNIL pour certifier les compétences des délégués à la protection des données / data protection officer (DPO), sur la base des référentiels du 20 septembre 2018 adoptés par la CNIL.

Objectifs

- **Connaître les missions du Data Protection Officer (DPO) ;**
- **Acquérir les connaissances juridiques, technique et organisationnelles nécessaires à l'exercice de ces fonctions ;**
- **S'approprier les démarches et outils nécessaires au maniement des règles en matière de protection des données ;**
- **Disposer de l'ensemble des connaissances utiles à la réussite à l'examen de certification.**

Durée & horaires

- **5 jours, soit 37h heures réparties en 35h00 de cours (dont 2h de travail personnel) et 2h 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 16h00/16h30.**

Nombre de participant

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

Public visé

- **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 et souhaitant disposer de la certification DPO :**
  - **DPO, DRPO**
  - **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

- **Avoir au minimum relu les principaux textes applicables, notamment le RGPD.**
- **Avoir des bases informatiques ou juridiques est un vrai plus.**
- **Passer le MOOC de l'ANSSI est également un vrai plus.**

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**
- **Enrichi de cas pratiques et d'exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2, avocats ou juristes spécialistes reconnus de ces questions ou implémenteurs des normes**
- **Un cours construit de manière à favoriser l'interactivité entre les participants, qui peuvent à tout moment poser des questions,**
- **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). Formation enregistrée par AFNOR Certification comme prérequis à la certification de compétences des DPO**
- **A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 2h en français. L'examen est constitué d'un QCM. Cet exercice valide les compétences et les savoir-faire présentés dans la catégorie 2 de la délibération n°2018-318 du 20 septembre 2018. Les questions couvrent tous les domaines du programme figurant en annexe de la délibération n°2018-317 du 20 septembre 2018.**

Programme

1 - Les principes de la protection des données à caractère personnel

- **1.1 Les sources**
  - Évolution et mise en perspective des principes généraux applicables (loi informatique et Libertés, textes européens, genèse RGPD, droit comparé US)
  - Qu'est-ce que la CNIL ? Qu'est-ce que le CEPD ?
- **1.2 Les définitions essentielles**
  - De quoi parle-t-on ? Notions de donnée à caractère personnel, traitement, responsable de traitement/sous-traitant, etc.
- **1.3 Le champ d'application**
  - Champ d'application matériel du RGPD (la Directive 2016/680 dite Directive « Police », le secteur des télécom/commerce électronique)
  - Champ d'application territorial (l'autorité de contrôle « chef de file », les transferts de données hors UE/EEE, certifications/codes de conduite)
- **1.4 Les grands principes**
  - L'architecture complexe du RGPD

Les principes essentiels du RGPD (licéité, loyauté, transparence, limitation des finalités, minimisation des données, exactitude, etc.)
- Conformité de l'écosystème (la qualification de responsable de traitement/sous-traitant ; accords contractuels)
- Le registre de traitements

➢ **1.5 Les régimes spéciaux**
- Les données à caractère hautement personnel, les données relatives aux condamnations pénales ou infractions, catégories particulières de données, etc.
- Le profilage
- Les référentiels de la CNIL

➢ **1.6 Les droits des personnes**
- Droit à l'information, droit d'accès, droit de rectification, droit à l'effacement, droit d'opposition, etc.

2 - L'approche par les risques

➢ **2.1 Intégrer les principes de Privacy by design et by default**
- Les 7 piliers du Privacy by design
- À quoi servent ces principes ?
- Les outils de mise en œuvre

➢ **2.2 Se donner les moyens d'assurer la sécurité**
- Les violations de données personnelles : notion d'intégrité, de disponibilité, de confidentialité… et d'accountability
- Les sanctions en cas de manquement à la sécurité
- Notions de mesures de sécurité et d'adéquation aux risques
- Exemples de mesures de sécurité et de contre-mesures pour chaque type de violation
- Les bonnes pratiques, etc.

➢ **2.3 Évaluer les risques et analyser l'impact de vos traitements sur les droits et libertés fondamentales (AIPD)**
- Qu'est-ce qu'une analyse d'impact ? Position de la CNIL
- Contenu de l'AIPD
- Appréciation du risque
- Notion d'AIPD flash

➢ **2.4 Savoir notifier les violations de données personnelles**
- Genèse de l'obligation de notification
- Modalités de la notification (qui, quand, comment ?)
- Modalités de la communication aux personnes concernées

➢ **2.5 Anticiper les recours et préparer un contrôle par les autorités**
- Réclamations, recours, responsabilités
- L'action collective, le droit à réparation
- Se préparer à un contrôle de la CNIL (modalités, pouvoirs de la CNIL, sanctions)

3 - Mettre en œuvre la conformité

➢ **3.1 Nommer un DPO dans l'entreprise**
- Qualités, profil, statut

➢ **3.2 Mettre en place et/ou gérer la gouvernance de protection des données**
- DPO, contrôleur ou faiseur ?
- Comité de pilotage, groupe de travail, etc.

➢ **3.3 Déployer une culture « Protection des données » dans l'entreprise**
- Notion, intérêt et structuration du Dossier de conformité
- Sensibilisation des personnels

- **3.4 Recenser parallèlement les outils et livrables de gouvernance**
  - Analyse de l'existant, veille globale
  - Accountability
- **3.5 Connaître son environnement et son écosystème**
  - Cartographies

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

- **Avoir suivi en amont soit une formation sur le RGPD, soit une formation DPO.**

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

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 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUSANTE par HS2.**

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

Formation « Droit de la cybersécurité »

Réf : SECUDROIT

La cybersécurité ne se gère pas qu'avec une organisation adaptée et des savoir-faire techniques, le droit en est un des piliers incontournables, et tout professionnel de la sécurité des systèmes d'information doit en connaître les bases.

Le cours aborde les principaux aspects juridiques de la sécurité informatique, de façon pratique, concrète et pragmatique. La formation est conçue conjointement par des juristes ou avocats et des ingénieurs en informatiques.

Objectifs

- **Apprendre les règles juridiques encadrant la sécurité informatique**
- **Permettre à des personnes n'étant pas juristes de comprendre les règles de droit s'appliquant à la sécurité informatique**
- **Savoir comment assurer le respect du droit de manière efficace et opérationnelle**
- **Pouvoir améliorer le niveau de conformité de son organisme ou de ses clients**

Durée & horaires

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

Nombre de participant

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

Public visé

- **RSSI, DSI**
- **Administrateurs systèmes et réseaux, astreintes opérationnelles**
- **Maîtrises d'œuvre de la SSI, chefs de projet, responsables de compte**
- **Consultants en sécurité**
- **Juristes amenés à intervenir dans le domaine de la cybersécurité**
- **Toute personne impliquée dans la sécurité informatique**

Pré-requis

- **Aucun pré-requis n'est demandé. Il n'est pas nécessaire de disposer de connaissances en droit ou en sécurité informatique pour suivre cette formation. Cependant, une connaissance générale de l'informatique est souhaitable.**

Méthode pédagogique

- **Le cours se veut avant tout pratique. Chaque thème est abordé en partant des dispositions juridiques, qui sont expliquées en langage courant. Le formateur conseille les stagiaires sur le comportement qu'il estime le plus pertinent en pratique, en prenant en compte l'ensemble des aspects (coûts, image, risques, etc.).**
- **Le cours est conçu pour être totalement interactif : les stagiaires peuvent constamment poser des questions, et le formateur soumet souvent des cas pratiques aux stagiaires, afin qu'ils réfléchissent au comportement le plus adapté.**

Supports

- **Support de cours au format papier en français**
- **Extraits de documents pratiques : charte informatique, fiches de traitement, etc.**
- **Certificat attestant de la participation à la formation**

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

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 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUDROIT par HS2.**

Programme

1 - Introduction
- Présentation de la formation
- Présentation du cadre juridique français
- Articulation du droit national avec les droits étrangers

2 - Les atteintes à la sécurité du SI
- Notion essentielle : responsabilité pénale et civile / infractions
- Les infractions d'atteintes au SI
- La collecte des preuves
- Le dépôt de plainte
- Les services spécialisés
- Les obligations de signalement des atteintes au SI

3 - Les obligations de sécurité
- Les obligations légales de sécurité : sécurité des données personnelles, des données de santé, des données bancaires, etc.
- Les obligations contractuelles : disponibilité du service, confidentialité des données, etc.
- Les responsabilités de chacun :
  - de l'organisme
  - de l'employeur
  - des salariés
  - du RSSI, du DSI, de l'administrateur système

4 – La protection des données personnelles
- Le cadre légal : les textes, les principes fondamentaux, les risques associés aux manquements
- Les principales notions : données à caractère personnel, traitement, responsable de traitement, sous-traitant, personnes concernées, DPO, CNIL.
- Les obligations :
  - La cartographie des traitements
  - La conformité des traitements
  - La responsabilité des acteurs : responsable de traitement, co-responsable, sous-traitant, DPO
  - Les études d'impact (PIA)
  - La sécurité des données
  - Les prestataires et sous-traitants
  - Les transferts internationaux
  - Les droits des personnes concernées
- Les contrôles de la CNIL
- Pour aller plus loin : Gouvernance, Code de conduite, Certifications

5 - Les obligations de conservation des traces
- Données relatives au trafic
- Données d'identification des créateurs de contenus
- Accès administratif aux données de connexion
- Autres traces

6 - Surveillance des salariés
- Le pouvoir et devoir de contrôle de l'employeur
- Le respect de la vie privée des salariés
- L'accès au poste et aux données des salariés
- Les règles encadrant l'usage du SI
- La responsabilité du salarié
- La Charte informatique :
  - son rôle
  - son contenu
  - son entrée en vigueur
  - sa valeur contraignante

7 - Conclusion
- Conclusion
- Démarche documentaire
- Outils de veille

Examen

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

Formation « ISO 27701 (ex. 27552) – Privacy Information Management System (PIMS) »

Réf : ISO27701LI

Avec l'entrée en application du RGPD, les exigences en matière de protection des données personnelles se sont renforcées. Le principe d'accountability est au cœur de la réglementation. Pourtant il n'existe pas encore de certification ni de label permettant aux organismes de démontrer leur conformité au RGPD.
La norme ISO 27701 est une étape importante vers la création d'une certification relative à la protection des données personnelles. Extension des référentiels ISO 27001 et ISO 27002, elle définit un cadre et énumère les mesures nécessaires à la mise en œuvre d'un PIMS (Privacy Information Management System) ou Système de management des données personnelles.
La formation ISO 27701 – Privacy Information Management System (PIMS) d'HS2 est dédiée à cette nouvelle norme. Son objectif est de présenter les apports de l'ISO 27701 aux référentiels ISO 27001 et ISO 27002 afin de permettre aux stagiaires d'implémenter et d'auditer un processus PIMS, notamment dans un contexte RGPD.

Objectifs

- **Présenter le RGPD, les principes et les enjeux de la protection des données personnelles**
- **Présenter l'articulation de la norme ISO 27701 avec les référentiels ISO 27001 et ISO 27002**
- **Présenter les apports de la norme ISO 27701 en matière de protection des données personnelles, notamment dans un contexte RGPD**
- **Présenter les différentes étapes d'implémentation d'un PIMS (Système de management des données personnelles)**
- **Présenter les éléments utiles pour auditer un PIMS**

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

- **RSSI**
- **DPO**
- **Responsable conformité**
- **Consultants cybersécurité**
- **Consultants RGPD**

Pré-requis

- **Connaître les normes ISO27001 et ISO27002 est indispensable.**
- **Connaître le RGPD est un véritable plus.**
- **Pour information, la norme ISO 27701 n'existe actuellement qu'en anglais.**

Méthode pédagogique

La méthode pédagogique se base sur les quatre points suivants :

- **Cours magistral basé sur les normes ISO 27701, ISO 27001, ISO 27002 et ISO 29100.**
- **Exercices de contrôle des connaissances sur les concepts à connaître et sur les normes.**
- **Exercices pratiques individuels et collectifs effectués par les stagiaires.**
- **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 Certi-Trust ISO 27701 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

1 - Introduction : Rappel du cadre général

- 1.1 - Protection des données personnelles et RGPD
- 1.2 - SMSI – Système de management de la sécurité de l'information
- 1.3 – Panorama des normes ISO dédiées à la protection de la vie privée
- 1.4 – Présentation générale de la norme ISO27701

2 – Processus PIMS – Privacy Information Management System

- 2.1 - Présentation des briques du processus PIMS
- 2.2 – Notion de protection des données personnelles (protection of privacy)
- 2.3 – La protection des données personnelles intégrée au système de management
  - -> Intégration de la protection des données personnelles aux différentes briques du processus

3 – Mesures de protection des données personnelles

- 3.1 – Présentation générale des mesures
- 3.2 – Focus sur les mesures clefs de la protection des données personnelles
  - -> Présentation des mesures essentielles de sécurité des données personnelles

4 – Mesures de protection des droits à la vie privée

- 4.1 – Au-delà de la sécurité, la conformité aux autres principes du RGPD
- 4.2 – Conditions de collecte des données
- 4.3 – PIA – Privacy impact assessment
- 4.4. – Droits des personnes concernées
- 4.5 – Concepts de Privacy by design and by default
- 4.6 – Transferts de données
- 4.7 – Sous-traitance

5 – Boîte à outils

-> Documentation du PIMS, Indicateurs, Veille et documents tiers utiles

6 - Focus sur l'audit

- 6.1 – Rappel de la méthodologie d'audit
- 6.2 - Grille d'audit et Documentation

7 – Conclusion

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

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.

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

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

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

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 35 heures dont 2h30 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.

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

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 Certi-Trust 22301 Lead Auditor. Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

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 Certi-Trust

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

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 35 heures dont 2h30 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.

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

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 Certi-Trust (ISO 22301 Lead Implementer). Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

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 Certi-Trust

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

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 et les connaissances indispensables à sa prise de fonction. Un retour d'expérience sur les chantiers et la démarche à mettre en œuvre dans le rôle sont détaillés par des 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 :**
  - **Enjeux de sécurité des SI dans les organisations**
  - **Connaissances techniques essentielles**
  - **Organisation de la sécurité et normes ISO27001**
  - **Politiques de sécurité, audit de sécurité et indicateurs**
  - **Méthodes d'appréciation des risques**
  - **Aspects juridiques de la sécurité des SI**
  - **Sensibilisation à la sécurité des SI et gestion des incidents**

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, RSSI adjoint, responsables sécurité opérationnelle à la production, correspondant local de sécurité des systèmes d'information**
- **Techniciens devenus RSSI, souhaitant acquérir des notions en gouvernance et management de la sécurité des SI**
- **Spécialistes de domaines transverses des systèmes d'information (qualité, audit, gestion de projets) devant compléter leurs compétences dans le domaine de la sécurité des systèmes d'information**

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

- **Cette formation est proposée en mode présentiel et peut être accessible en mode distanciel via ZOOM pour les personnes qui ne peuvent ou ne veulent pas se déplacer**
- **Cours magistral dispensé à chaque fois par des experts de chaque module**

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

- **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 en français au format papier pour le présentiel et au format numérique pour le distanciel (sous réserve du règlement intérieur signé)**
- **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

- **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 RSSI par HS2.**

Programme

Accueil des participants et tour de table

Enjeux de la sécurité des systèmes d'information (1 jour)

- Introduction
  - Objectifs de la cybersécurité
  - Objectifs des organisations
  - Alignement stratégique organisation / cybersécurité
  - Objectifs et organisation de la formation
- Enjeux de la cybersécurité
  - Sécurité des SI, de l'information, informatique et cybersécurité
  - Vocabulaire : critères et objectifs
  - Le critère de preuve
  - Vocabulaire : incident et risque
- Activités du RSSI
  - Le RSSI, polyvalent face aux enjeux
  - La politique de sécurité
  - Le programme de sécurité
  - Les mesures de sécurité
  - Le RSSI dans les projets
  - Le RSSI et les associations professionnelles
- Introduction à la menace cyber
  - Gérer le risque
  - Dans la peau d'un attaquant
  - Sécurité - Règles de base

Aspects techniques de la cybersécurité (1 jour)

- Introduction à la cryptographie
- Sécurité réseau
  - Principes de base du réseau
  - Attaques et mesures
  - Pare-feu et proxy
  - Architecture sécurisée
- Sécurité applicative
  - Vulnérabilités mémoire
  - Vulnérabilités web
  - Développement sécurisé
- Sécurité système
  - Principes
  - Contrôle d'accès
  - Veille sécurité
  - Mise à jour
  - Sauvegarde
  - Journalisation
  - Protection du poste de travail
  - Équipements mobiles
  - Auditer son SI

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

Système de Management de la Sécurité de l'Information (normes ISO 2700x) (1/4 journée)

- Introduction à ISO 27001
- Systèmes de management et SMSI
  - Exemples de systèmes de management
  - Propriétés des systèmes de management
  - Processus du SMSI
- Introduction à ISO 27002
- Comment utiliser les normes
- Conclusion et bienfaits du SMSI ISO 27001

Politiques de sécurité (1/4 journée)

- Définitions
- Hiérarchie et utilité des politiques de sécurité
- Politiques spécifiques, organisation et exemples
- Rédaction, élaboration et mise en œuvre des politiques
- Révision des politiques
- Synthèse et éléments indispensables des politiques

Indicateurs en sécurité des SI (1/4 journée)

- Introduction et règles d'or
- Sources de collecte des indicateurs
- Spécification des indicateurs et exemples
- Indicateurs dérivés et exemples
- Risques sur les indicateurs, questions pratiques et erreurs à éviter

Audit (1/4 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 (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
- Évaluation du risque
- Traitement des risques (réduction, partage, maintien, refus)
- Notion de risque résiduel
- Acceptation du risque

Aspects juridiques de la SSI (1/2 journée)

- Focus sur 3 obligations générales de protection du SI
  - Un bref panorama des obligations de SSI
  - LPM et OIV
  - NIS, OSE et FSN
  - RGPD
- Synthèse des principales règles de la SSI au sein des organisations
  - Détecter les incidents
  - Journaliser les activités
  - Encadrer les usages dans les organisations
  - Contractualiser avec les prestataires
- Le volet pénal : réagir aux atteintes à la sécurité des systèmes d'information
  - L'importance de la gestion de crise
  - La qualification des faits de cybercriminalité

Sensibilisation à la sécurité des SI (1h)

- Mesure de sécurité
- Programme de sensibilisation
- Objectif de la sensibilisation
- Moyens de sensibilisation et vecteurs de communication
- Sources d'information
- Conseils
- Rappel des objectifs
- Coûts
- Évaluation

Gestion des incidents en sécurité des SI (1h)

- Définitions
- Exemples d'incidents liés à la sécurité

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

- Objectifs de la gestion des incidents liés à la SSI
- Étapes de la gestion d'un incident
  - Préparation, identification et analyse, confinement, endiguement, éradication, recouvrement, retour d'expérience
- Erreurs à éviter
- Outils
- Ressources

Acheter des prestations en sécurité des SI (1h)

- Contexte et objectifs
- Acheter la SSI
  - Définition
  - Le service achats
  - Le processus achats
  - Avant / pendant
  - Après
  - Augmentez votre pouvoir d'achat

Examen (1h30)

Témoignage et retour d'expérience d'un RSSI (1h30)

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

Formation « Security by Design »

Réf : SECUBYDESIGN

La maîtrise de la gestion de projet informatique associée aux risques numériques est une dimension essentielle aux systèmes d'information. Ainsi l'intégration réussie de la cybersécurité est une étape clef afin de mener à bien les projets informatiques. Cela amène à mettre en perspectives les enjeux classiques de la gestion de projet notamment en termes de coût/délai/performance, au service d'un métier, avec un contexte où il est souvent nécessaire de composer avec une infogérance, le cloud, la règlementation et les bonnes pratiques en matière de sécurité des systèmes d'information.

La présente formation apporte une vision pragmatique de la sécurité applicable aux projets informatiques. Le retour d'expérience proposé en matière de sécurité et de gestion de projet donnera des clés facilitant le pilotage du projet et la conception d'une sécurité intégrée.

Objectifs

- **Faciliter la prise en compte de la sécurité dans vos projets informatiques**
- **Fiabiliser votre gestion de projets informatiques**
- **Contribuer à niveau de confiance acceptable du SI**
- **Maîtriser les risques liés à la sous-traitance et à l'externalisation**

Durée & horaires

- **2 jours soit 14 heures**
- **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 mener un projet informatique**
- **DSI, RSSI, chef de projet, responsable opérationnel**
- **Responsable métier, gestionnaire de contrat, gestionnaire de risque**
- **Consultant**

Pré-requis

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

Méthode pédagogique

- **Cours magistral avec de nombreux exemples anonymisés**
- **Exercices de mise en œuvre**
- **Mises en situation**
- **Support de cours au format papier en français**
- **Certificat attestant de la participation à la formation**

Supports

- **Support de cours au format papier en français**
- **Extraits de documents pratiques : charte informatique, fiches de traitement, etc.**
- **Certificat attestant de la participation à la formation**

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

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

Module 1 : Introduction à la sécurité des systèmes d'information

- Le contexte
- Une étude de cas
- Un quizz

Module 2 : Principes de sécurité des systèmes d'information

- Des architectures sécurisées
- Une administration sécurisée des SI
- La sécurité de l'infrastructure
- La sécurisation des développements logiciels et applicatifs : DevSecOps, SDLC, OWASP, CWE, etc
- Les fondamentaux de la cryptographie

Module 3 : Sécurité des systèmes d'information et projet informatique

- Pourquoi intégrer la sécurité dans vos projets ?
- Les rôles et les responsabilités SSI dans les projets
- Les étapes SSI dans les projets : approche Agile intégrée, ISO 27034, etc
- Quelques aspects juridiques et règlementaires : NIS, LPM, RGPD, etc
- La maîtrise des risques : EBIOS RM, MEHARI, etc
- Une étude de cas
- Une sous-traitance maîtrisée : maintien en conditions opérationnelles et de sécurité (MCO-MCS), plan d'assurance sécurité (PAS), référentiel Cloud, etc
- La documentation SSI
- Les audits de sécurité : infrastructure et applications

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

« 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**

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

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

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

« Préparation au CCSP »

Réf : CCSP

La certification CCSP, créée en 2015 par l'(ISC)² en partenariat avec le CSA (Cloud Security Alliance), est l'une des certifications les plus reconnues dans le domaine du cloud computing. C'est la certification "soeur" du CISSP, entièrement focalisée sur les problématiques liées à l'infonuagique. Elle s'appuie sur le CCSP CBK (Common Body of Knowledge), tronc commun de connaissances composé de 6 domaines couvrant tous les aspects de la sécurité du Cloud.

La formation CCSP d'HS2 est au format "boot camp" : c'est un entrainement intensif dont l'objectif est de préparer à l'examen de certification CCSP de l'(ISC)². 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 (ISC)² Guide to the CSSP CBK », Sybex). La formation s'articule autour des 6 domaines du CCSP : 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'une application en ligne similaire à celle de l'examen réel. Les résultats de chaque question sont ensuite analysés avec les formateurs. Cette méthode permet au stagiaire de « s'imprégner » de l'esprit CCSP et de maximiser ses chances de réussite.

Objectifs

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

- **Architecte**
- **Administrateur**
- **Manager sécurité**
- **Ingénieur sécurité**
- **Chef de projet**
- **Consultant en sécurité**
- **Toute personne souhaitant valoriser ses expériences dans le domaine du Cloud**

Pré-requis

- **Avoir lu le CBK ("Official (ISC)² Guide to the CCSP CBK" - Sybex).**

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**

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

Supports

- **Support de cours au format papier en anglais**
- **Diapositives en anglais à l'écran, avec explications en français par les formateurs**
- **Livre CCSP 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**
- **Ordinateur mise à disposition pendant la formation pour répondre aux questions**

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 CCSP 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 CCSP dans ces deux pays.**

Programme

Accueil et introduction au CCSP

Domaine 1. Architectural Concepts & Design Requirements :
- Rappel des fondamentaux
- Test d'entrainement

Domaine 2. Cloud Data Security
- Rappel des fondamentaux
- Test d'entrainement

Domaine 3. Cloud Platform & Infrastructure Security
- Rappel des fondamentaux
- Test d'entrainement

Domaine 4. Cloud Application Security
- Rappel des fondamentaux
- Test d'entrainement

Domaine 5. Operations
- Rappel des fondamentaux
- Test d'entrainement

Domaine 6. Legal and Compliance
- Rappel des fondamentaux
- Test d'entrainement

Entrainement final

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

« 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**
- **Certificat attestant de la participation à la formation**

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

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 suivies d'une revue des réponses des stagiaires.

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

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 cyber »

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

- 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

- 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

Module 1 : Gestion de crise cyber

- Exemple de crises cyber
- Cas concret détaillé d'une crise cyber "rançongiciel"
  - Pourquoi est-ce la principale crainte des organisations ?
  - Quel est l'état d'un système d'information et d'une organisation après le déclenchement d'un rançongiciel ?
  - Description d'une chronologie classique : l'attaque, le constat, la réaction, le suivi et la sortie de crise

Module 2 : Dispositif de crise et les spécificités d'une cyber-attaque

- Vocabulaire : Investigation/Inforensic, Plan de défense, Assainissement, Durcissement, Reconstruction, Main courante, etc.
- Les spécificités d'une crise cyber
- Qu'est-ce qu'un dispositif de gestion de crise cyber ?
- Organisations types
- Processus de la crise : la montée en crise, le lancement, les points de situation, la sortie de crise
- Outillage
- Facteurs humains et gestion du stress
- Logistique et communication
- Cyber-assurance
- Mise en situation : qualification et premier plan d'actions

Module 3 : Observation & Investigation

- Comprendre pour mieux agir
- Plan d'investigation : vecteurs d'intrusion/patient 0, de propagation, mécanismes de persistance
- Responsabilité de l'investigation
- Posture d'observation
- Actions clefs de l'investigation
- Outillage du plan d'investigation
- Interactions inter et intra cellules de crise
- Mises en situations : définir une posture, mobiliser les ressources, établir un plan d'investigation

Module 4 : Défense & Surveillance

- Plan de défense
- Responsabilité de la défense
- Remédiation
- Reconstruction
- Durcissement
- Surveillance de circonstance et surveillance long terme
- Mises en situation : évaluer les impacts, établir un plan de défense, construire l'organisation nécessaire

Module 5 : Sortie de crise… et l'après crise

- Critères de sortie de crise
- Analyse de la cause primaire ("root cause analysis")
- Construction du RETEX
- Plan d'actions post-crise
- Retour en mode projet et en "RUN"
- S'entraîner / exercices de crise
- Mises en situation : construction un plan d'actions post-crise, acter une sortie de crise, établir un RETEX

Synthèse : les clefs de la gestion de crise cyber

Mise en situation complète

Formation « EBIOS 2018 Risk Manager »

Réf : EBIOS2018

EBIOS Risk Manager est une méthode de gestion des risques conçue par l'ANSSI et publiée en octobre 2018 (nous appellerons cette méthode EBIOS RM ou EBIOS2018 pour éviter de la confondre avec EBIOS2010). 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 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.**

Durée & horaires

- **3 jours soit 21 heures**
- **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 20 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

- **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 EBIOS 2018 Risk Manager par HS2.**

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

Examen

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 « Mise à jour ISO27001 & ISO27002 »

Réf : MAJ27

La norme ISO27001 est la référence internationale en termes de système de management de la sécurité de l'information (SMSI). 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.

2022 est l'année de la publication d'une importante mise à jour de la norme ISO27002 et donc en conséquence de l'Annexe A de la norme ISO 27001. Les changements contenus dans ces nouvelles versions impactent forcément un SMSI existant mais également toute démarche de gestion de la Cybersécurité.

Objectifs

- **Découvrir les mises à jour 27001 & 27002**
- **Se préparer à la migration du SMSI en 2022**
- **Comprendre les apports des nouvelles versions des normes pour lancer un projet de SMSI**
- **Appréhender l'usage de la nouvelle 27702 pour vos audits ou vos politiques de sécurité**

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

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

Pré-requis

- **Avoir suivi une formation Lead Implementer ou Lead Auditor 27001 ou maîtriser les normes 27001-27002 en version 2013/2017**

Méthode pédagogique

Cours magistral basé sur les normes, exercices de mises en situation.

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, éligible au CP2 d'ISC2**

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

Les nouveautés :

- Amendements de la norme ISO27001 : l'Annexe A
- Une nouvelle vision « processus » de l'ISO27002:2022
  - La nouvelle organisation des 93 mesures
  - Les attributs : intérêt et usages
  - Les nouvelles mesures
- L'impact sur la documentation SSI
  - PSSI et les politiques associées
  - Déclaration d'applicabilité
  - Gestion du SMSI : suivi de projets, manuel, modèles documentaires.
  - Points de contrôle : Indicateurs, activité de surveillance, programme d'audit interne
- Evolution des processus du SMSI
  - Appréciation des risques
  - Plan de traitement des risques
  - Audit Interne
  - Surveillance
- Stratégies de migration d'un SMSI
  - Approche par la DdA
  - Approche par Processus
- Etudes de cas :
  - Faire évoluer les mesures de sécurité existantes
  - Communiquer sur ces évolutions
    - Acteurs du SMSI
    - Clients et partenaires
- Gestion de la relation avec l'organisme de certification
  - Gérer les audits intermédiaires
  - Bascule sur les nouvelles versions
- Evolutions des autres normes 27x
  - ISO 27005
  - ISO 27006
  - ISO 27701

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 35 heures réparties en 31h30 de cours, 3h30 de travail individuel sur les exercices le soir et 3h00 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 Certi-Trust 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 Certi-Trust

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 35 heures réparties en 31h30 de cours, 3h30 de travail individuel sur les exercices le soir et 3h00 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

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

- **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 Certi-Trust 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 Certi-Trust

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**

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

- **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 Certi-Trust ISO 27005 Risk Manager. Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation.**

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 Certi-Trust

Formation
« ISO27004 / Indicateurs et tableaux de bord cybersécurité »

Réf : ISO27004

Que ce soit un avion ou un organisme, il est toujours possible de conduire celui-ci avec peu d'informations, mais cela sera moins efficace, voire dangereux. Dans le cas de la gestion de la sécurité de l'information, le pilotage d'une telle activité consiste à prendre des décisions et ce à plusieurs niveaux. Ce peut être la décision de modifier une fréquence de scan antivirus ou encore, à un niveau plus stratégique, l'arbitrage en faveur d'une redistribution des budgets.

Si elles ne relèvent pas du même niveau d'arbitrage, ces décisions ont ceci en commun qu'elles se font de façon plus éclairée si elles sont prises en fonction d'informations fiables et pertinentes. La prise de décision est d'autant meilleure qu'elle peut s'appuyer sur des indicateurs concrets et pertinents.

Les indicateurs stratégiques, regroupés en tableaux de bord, permettent de répondre à ce besoin d'information. Pour ce faire ils doivent être adaptés au profil du lecteur et aux décisions qui sont attendues de lui. En ce sens, les tableaux de bord sont à rapprocher des principes de communication dont la finalité est d'obtenir une action de la cible de cette communication.

Un tableau de bord pertinent se doit également d'être réaliste, ce qui implique que son coût soit maitrisé et en rapport avec les enjeux qu'il permet d'arbitrer. L'objectif étant, non pas de construire des indicateurs trop complexes et coûteux à produire, ce qui contribuerait à consommer de la valeur plutôt qu'à sécuriser celle-ci…

Objectifs

- Comprendre ce qu'est un indicateur, ce en quoi il est nécessaire à une gestion efficace de la sécurité de l'information, comment en faire un outil de communication vis-à-vis de toutes les parties prenantes, comment mettre en place des tableaux de bord adaptés à un contexte
- Savoir concevoir des indicateurs pertinents et réalistes dans le contexte de son organisme
- Savoir concevoir des indicateurs conformes aux exigences de la norme ou du référentiel suivi
- Savoir tirer des informations utiles des indicateurs en produisant des tableaux de bord pour surveiller et améliorer un SMSI, pour prouver sa conformité et améliorer la SSI, et pour communiquer

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

- Personnes chargées de concevoir des indicateurs sécurité, de les produire, ou de présenter des tableaux de bord.
- Personnes chargées de déployer des indicateurs sécurité
  - RSSI et équipes du RSSI
  - Consultants en sécurité
  - Ingénieurs sécurité.
- Personnes chargées de produire des indicateurs de sécurité
  - Ingénieur de production informatique
  - Chef de projet métier

Pré-requis

- **Avoir suivi la formation "Essentiels ISO27001/ISO27002" ou la formation "RSSI"**
- **ou avoir suivi une formation plus complète à l'ISO27001 comme "ISO27001 Lead Implementer"**
- **ou avoir une connaissance de la SSI et une maîtrise de l'ISO27001 ou des systèmes de management en général**
- **ou être déjà RSSI ou consultant sécurité avec une expérience**

Méthode pédagogique

- **Cours magistral avec des exemples pratiques issus de l'expérience des formateurs.**
- **Exercices pratiques individuels de mise en œuvre d'indicateurs.**

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 n'est pas certifiante.**

Programme

- Introduction
  - Qu'est-ce qu'un indicateur ?
  - Vocabulaire
- Indicateurs : pourquoi mesurer une activité ?
  - Peut-on piloter sans instruments ?
  - Quelle valeur ajoutée
- Points à mesurer dans le domaine de la SSI
  - Efficience de la sécurité
  - Coût de la sécurité, ou de l'absence de sécurité
  - Conformité aux normes, référentiels, exigences, réglementations
- Approches pour gérer les indicateurs :
  - Travaux issus du monde de la sécurité : ANSSI, ISO, CLUSIF, CIGREF
  - Techniques de communication au service des indicateurs
  - Coût des indicateurs
- Démarche de mise en œuvre
  - Vue d'ensemble
  - Concevoir ses indicateurs
    - Définir ses besoins et ses finalités
    - Définir les moyens de production
  - Produire ses indicateurs
  - Communiquer ses indicateurs
  - Auditer ses indicateurs
- Conseils pratiques
  - Principaux indicateurs à mettre en place
    - Pour un Système d'Information
    - Pour un SMSI
  - Exemples
  - Erreurs à éviter
  - Identifier les solutions simples et efficaces (« quick wins »)
- Présentation de la norme ISO 27004
  - Raison d'être de la norme
  - Processus de mise en œuvre
  - Quels indicateurs pour quel usage
- Exercices

Formation « Gestion des incidents de sécurité / ISO27035 »

Réf : ISO27035

La gestion des incidents de sécurité dans un délai court et leur prise en compte dans la gestion des risques et l'amélioration continue sont imposés par l'ISO 27001. Le processus de gestion des incidents de sécurité est un processus fondamental pour le succès d'une bonne organisation de la sécurité des systèmes d'information. Un guide, la norme ISO27035, explicite en détail comme organiser ce processus.

Objectifs

- **Comprendre et savoir mettre en œuvre concrètement dans son SMSI le processus de gestion des incidents de sécurité et une équipe de réponse aux incidents de sécurité (Information Security Incident Response Team : ISIRT)**
- **Comprendre et savoir gérer les interactions du processus de gestion des incidents de sécurité avec les autres processus dans son organisme, par exemple savoir différencier incident informatique et incident de sécurité.**
- **Apprendre à organiser son processus de gestion des incidents de sécurité.**

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

- **DSI**
- **Personnes chargées de gérer les incidents de sécurité ;**
- **Personnes chargées de gérer les incidents au sens ITIL/ISO 20000 ;**
- **Responsables de la mise en place d'un SMSI.**

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

- Introduction
  - Contexte, Enjeux et ISO27001, Vocabulaire
- Norme ISO 27035
  - Concepts
  - Objectifs
  - Bienfaits de l'approche structurée
  - Phases de la gestion d'incident
- Planification et préparatifs (Planning and preparation)
  - Principales activités d'une équipe de réponse aux incidents de sécurité (ISIRT)
  - Politique de gestion des incidents de sécurité
  - Interactions avec d'autres éférentiels ou d'autres politiques
  - Modélisation du système de gestion des incidents de sécurité
  - Procédures
  - Mise en œuvre de son ISIRT
  - Support technique et opérationnel
  - Formation et sensibilisation
  - Test de sons système de gestion des incidents de sécurité)
- Détection et rapport d'activité (Detection and reporting)
  - Activités de l'équipe opérationnelle de détection des incidents de sécurité de l'information
  - Détection d'évènements
  - Rapport d'activité sur les événements
- Appréciation et prise de décision (Assessment and decision)
  - Activités de l'équipe opérationnelle d'analyse des incidents de sécurité
  - Analyse immédiate et décision initiale
  - Appréciation et confirmation de l'incident
- Réponses (Responses)
  - Principales activités d'une équipe opérationnelle de réponse aux incidents de sécurité
  - Réponse immédiate
  - Réponse à posteriori
  - Situation de crise
  - Analyse Inforensique
  - Communication
  - Escalade
  - Journalisation de l'activité et changement
- Mise à profit de l'expérience ('Lessons Learnt')
  - Principales activités d'amélioration de l'ISIRT
  - Analyse Inforensique approfondie
  - Retours d'expérience
  - Identification et amélioration
- Mise en pratique
  - Documentation
  - Exemple d'incidents de sécurité de l'information
  - Catégories d'incidents de sécurité
  - Méthodes de classement ou de typologie d'incidents de sécurité
  - Enregistrement des évènements de sécurité
  - Fiche de déclaration des évènements de sécurité
- Aspects légaux et réglementaires de la gestion d'incidents

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 base
- Gestion du risque : vulnérabilité, menace, impacts métiers
- Dans la peau d'un attaquant
- Principes de base : connaître son SI, moindre privilège, défense en profondeur

Cryptographie

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

Sécurité des réseaux

- Principes de base
- Attaques
- Contrôle d'accès
- Filtrage et relayage
- Architecture sécurisée
- WiFi

Sécurité des applications

- Vulnérabilités web : le TOP 10 de l'OWASP
- Vulnérabilités mémoire
- Attaques et défenses
- Processus de développement

Sécurité des systèmes

- Contrôle d'accès
- Minimisation et durcissement
- Veille sécurité
- Mise à jour
- Sauvegarde
- Journalisation
- Protection du poste de travail
- Equipements mobiles

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

- 4 jours soit 28 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 « Sécurité des objets connectés »

Réf : SECUOBJ

Objectifs

- Fournir suffisamment d'éléments techniques et de langage afin de permettre aux développeurs et aux intégrateurs de solutions communicantes de comprendre l'aspect multi vectoriel de la sécurité des systèmes embarqués avec notamment une approche de défense vis à vis d'une vision attaquante.
- Être en mesure d'évaluer une solution IoT en prenant en compte l'ensemble de la chaine de données, depuis sa production jusqu'à sa consommation. Sur l'ensemble de la formation, le profil type attaquant est un attaquant opportuniste.

Durée & horaires

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

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Le profil type ciblé est un industriel (développeur ou intégrateur)

Pré-requis

- Avoir une bonne connaissance générale en environnement linux nécessaire, ainsi que des notions en système.

Méthode pédagogique

- Cours magistral avec échanges interactifs
- Travaux pratiques ayant pour objectif de réaliser un audit global d'une solution IoT en mode matriochka Plusieurs challenges sont imbriqués avec une construction en plusieurs niveaux. Chacun d'entre eux seront étudier tout au long du cours A chaque découverte d'une vulnérabilité, une fiche détail composée d'une description, d'un score (CVSSv3) et d'une recommandation sera réalisée. Les travaux pratiques seront basés sur la plateforme Microbit (https://microbit.org/) et sur les puces STM32 (STM32F103C8T6)

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- 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 certifiante. L'évaluation de la formation se fera sous la forme d'un Quizz.

Programme

Qu'est-ce que l'Iot ?

- Au cœur de la révolution industrielle et sociétale
- L'environnement IoT
- Cadre légal
- Analyse de risque
- Référentiels (ANSSI / GSMA / GIE / norme ISO / Internationale / NIST / CIS)
- Méthodologie test d'intrusion
  - MITRE ATT&CK ICS
  - PTES
  - OSTMM
  - OWASP

Caractéristiques spécifiques

- Contraintes spécifiques / contraintes d'encombrement
- Microcontrôleur vs CPU
- Notion d'architecture
- Système temps-réel
- Protocoles
- Attaque

Récupération d'information

- Lecture de documentation technique (ex. : DataSheet et cartographie)
- Suivi des pistes physiques (ex.: Gerber)
- Voyage dans le temps (ex. : Gitlog / timemachine)
- Fiches d'identité

Couche matérielle

- Liaison série (Synchrone et Asynchrone)
- Accès au microcode (port débogage / lecture mémoire)
- Accès indirect / Injection de fautes (DMA/DPA)
- Introduction aux radio fréquences (SDR)

Couche microcode

- Rétro-ingénierie ARM (ex. : R2 et Ghidra)
- Exploitation ARM (Emulateur, Debogueur, Montage des partitions de fichiers)
- Développement sécurisé
- Simulation d'une carte “alpha” (version de développement)

Couche concentrateurs

- Passerelles
  - Modèle souscription/publication
  - Modèle ad-hoc
  - Gestion par événements
- Android
  - Architecture
  - Décompilation d'une archive applicative (APK)
  - Interaction avec la pile d'exécution
  - Analyse légale post-incident (Forensic)

Couche Internet

- Terminaison API / fonctions lambda
- Application Web
- Gestion des réseaux d'énergie / villes intelligentes

Défense

- Protection du matériel
- Développement sécurité par construction (Secure design)
- Sécurité périmétrique et surveillance (Parefeu, IDS/IPS, Gestion de journaux VS SIEM)

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
« Audit sécurité d'applications mobiles Android et iOS »

Réf : SECUMOBILE

Vous souhaitez acquérir des compétences dans l'audit des applications mobiles Android et iOS ? Ou vous voulez approfondir vos connaissances sur les vulnérabilités propres à ces plateformes ? Ou bien vous souhaitez connaitre la démarche à adopter pour auditer une application mobile ? Cette formation vous permettra de passer en revue les techniques nécessaires pour auditer une application mobile, ainsi que les vulnérabilités les plus courantes sur ce type d'applications.

Objectifs

- Appréhender les problématiques sécurité des applications mobiles
- Savoir effectuer une analyse statique
- Utiliser Frida pour réaliser une analyse dynamique
- Intercepter le trafic d'une application mobile

Durée & horaires

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

Nombre de participant

- Minimum 6 participants – Maximum 20 participants

Public visé

- Administrateurs système ou réseau
- Développeurs
- Consultant en sécurité souhaitant acquérir des compétences en audit d'applications mobiles

Pré-requis

- Bonne connaissance en informatique
- Connaissances en réseau (TCP/IP et HTTP) et Linux (savoir utiliser le terminal)
- Connaissances de base en sécurité

Méthode pédagogique

- Cours magistral
- Travaux pratiques

Supports

- Support de cours au format papier en français pour les sessions en présentiel
- Ordinateur portable mis à disposition du stagiaire

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 SECUMOBILE par HS2.**

Programme

Jour 1

iOS

Présentation de l'écosystème iOS

- Architecture iOS et fonctionnalités de sécurité
- OWASP MSTG et MASVS
- Techniques utilisées pour auditer une application
- Jailbreak : histoire, types et évolution
- Mise en place d'un environnement de test
- Signature d'applications
- Présentation de Corellium

Analyse statique d'applications iOS

- Analyse des méta-données liées aux applications
- Déchiffrement d'une application
- Décompilation avec Hopper
  - Travaux Pratiques
    - Automatisation de l'analyse statique avec MobSF
    - Déchiffrement d'une application récupérée de l'AppStore
    - Décompilation et retro-ingénierie d'une application

Android

Présentation de l'écosystème Android

- Architecture d'Android (Composants et Sandboxing)
- Structure et contenu d'un APK
- Présentation de l'Android Manifest
- Mise en place d'un environnement de test
  - Travaux Pratiques : Développement d'une application Android

Analyse statique et modification d'applications Android

- Décompilation d'une application avec JADX
- Analyse statique avec apktool
- Modification d'une application Android avec apktool
- Signature d'une application Android
  - Travaux Pratiques
    - Recherche et identification de secrets au sein d'une application
    - Modification d'une application Android

Jour 2

iOS

Analyse des données d'applications iOS

- Les données sauvegardées par iTunes
  - Travaux Pratiques : Récupération d'informations sensibles à partir d'une sauvegarde
- Les données stockées sur le terminal
  - Travaux Pratiques : Récupération d'informations sensibles / via les journaux

Analyse dynamique d'applications iOS

- Interfaces et implémentations en Objective-C
- Rétro-ingénierie d'une application pour contourner des fonctions de sécurité
  - Travaux Pratiques : Décompilation, retro-ingénierie puis modification en mémoire d'une application avec Frida pour contourner une fonction de sécurité

Android

Analyse dynamique d'applications Android

- Revue des différentes méthodes de stockage de données
  - Shared Preferences
  - Bases de données (SQLite)
  - Stockage interne et externe
  - Travaux Pratiques : Exploitation des faiblesses de chaque méthode
- Comparaison de l'utilisation d'un émulateur ou d'un terminal physique
- Techniques de détection d'un émulateur ou d'un équipement "rooté"
- Revue des contrôles d'accès des composants Android
  - Activities
  - Content Providers
  - Travaux Pratiques : Exploitation des faiblesses de contrôle d'accès
  - Travaux Pratiques : Décompilation, rétro-ingénierie puis modification en mémoire d'une application avec Objection pour contourner une fonction de sécurité

Jour 3

iOS

Sécurité des communications des applications iOS

- Interception du trafic réseau
- Fonctionnement et implémentation du Certificate Pinning
- Techniques de contournement du Certificate Pinning
  - Travaux Pratiques
    - Interception de trafic non chiffré
    - Interception de trafic chiffré
    - Contournement du Certificate Pinning

Que faire sans terminal iOS jailbreaké ?

- Analyse des sauvegardes et des journaux
- Interception du trafic réseau
- Side-loading d'application pour embarquer un framework d'analyse (Frida/Cycript/Objection)

Android

Sécurité des communications des applications

- Revue des faiblesses courantes
- Interception du trafic réseau
- Fonctionnement et implémentation du Certificate Pinning
- Techniques de contournement du Certificate Pinning
  - Travaux Pratiques : Inteception de trafic chiffré et contournement du Certificate Pinning

Instrumentation d'applications Android avec Frida

- Présentation de Frida
- Création de scripts Frida pour instrumenter du code Java
- Utilisation de Frida pour instrumenter du code natif
  - Travaux Pratiques : Utilisation de Frida pour contourner des routines de détection de "root"

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 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

- 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

- **Éduquer vos équipes de développement aux risques et aux enjeux de la sécurité applicative en mettant en application l'ensemble des points clés du standard OWASP**
- **Être en mesure d'augmenter rapidement la qualité et la sécurité de leurs développements de façon pertinente et efficace.**

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 ayant un profil technique souhaitant acquérir les connaissances suffisantes pour sécuriser leurs développements Web :**
- **DevSecOps**
- **Programmeurs,**
- **Développeurs**
- **Architectes**
- **Chefs de projet**
- **Consultants cybersécurité**

Pré-requis

- **Expérience en programmation, idéalement en développement Web**
- **Connaissance de base en cybersécurité, par exemple suivi de la formation SECUCYBER est un plus**

Méthode pédagogique

- **Cours magistral illustré par des exercices guidés pas à pas**
- **Résolution de challenges de sécurité réaliste de type Capture The Flag (CTF)**

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

Introduction aux risques et aux enjeux de la sécurité applicative

- Quelques idées reçues
- La couche applicative – Une surface d'attaque de choix
- Prise en main de l'environnement de travaux pratiques

Rappels sur les technologies web

- Encodages (URL, HTML, Base64)
- HTTP / HTTPS
- Utilisation d'un proxy Web pour intercepter, analyser et modifier les échanges HTTP(S)

Introduction aux techniques d'attaque et aux mécanismes de défense

- Présentation de l'OWASP (guides, outils et TOP 10 de l'OWASP Web)
- Attaques et mécanismes de défense
- Utilisation du scanner de vulnérabilité OWASP ZAP

La phase de reconnaissance utilisée avant d'attaquer une application

- Axes de fuite d'informations techniques
- Utilisation d'outils de "Crawling" et d'outils de collecte d'information

Le mécanisme de gestion de l'authentification (attaque et défense)

- Mécanismes d'authentification les plus rencontrés
- Failles / Attaques qui ciblent le mécanisme d'authentification
- Moyens de défense permettant de sécuriser le mécanisme d'authentification
- "Brute-force" d'un mécanisme d'authentification
- Interception de données en transit (Sniffing)

Le mécanisme de gestion de la session (attaque et défense)

- Rappel autour des sessions
- Failles / Attaques qui ciblent le mécanisme de gestion de la session
- Moyens de défense permettant de sécuriser le mécanisme de gestion de la session
- Exploitation de la faille permettant la fixation de session

Le mécanisme de gestion des autorisations (attaque et défense)

- Droits horizontaux et droits verticaux
- Failles / Attaques qui ciblent le mécanisme de gestion des autorisations
- Attaques de type Cross-Site Request Forgery (CSRF)
- Attaques de type File Inclusion (RFI / LFI) et Path Traversal
- Moyens de défense permettant de sécuriser le mécanisme de gestion des autorisations
- Exploitation d'une faille de type Path Traversal

La gestion des entrées utilisateurs (injection de code)

- Les différents types d'attaques permettant l'injection de code (SQL, HQL, LDAP, commandes, etc.) et le principe général de ce type d'attaque
- Moyens de défense permettant de sécuriser vos entrées utilisateurs
- Exploitation de failles de type Injection SQL manuellement et de façon automatique (via l'utilisation d'un outil)

Les attaques ciblant les autres utilisateurs (attaque de type cross-site)

- Attaques de type Cross-Site Scripting (XSS)
- Le cas des clients riches JavaScript (AngularJS, Backbone, Ember, NodeJS, ReactJS, etc.)
- Moyens de défense permettant de sécuriser la navigation de vos utilisateurs et de se protéger contre l'injection de code HTML / JavaScript
- Mise en œuvre de différents scénarios d'attaques reposant sur l'exploitation d'une faille de type Cross-Site Scripting (modification de l'affichage, vol de session, redirection arbitraire, etc.)

Sécurité de la journalisation, de la gestion des erreurs et des exceptions

- Principe et enjeux de la journalisation des évènements de sécurité
- Stockage d'informations sensibles dans les journaux et attaques de type injection de "logs"
- Principe et enjeux de la gestion des erreurs et des exceptions
- Axes de prévention et bonnes pratiques dans le domaine

Sécurité des services web (Front end JavaScript, API SOAP & REST)

- Front-end à base de clients riches JavaScript
- Les failles des clients riches JavaScript
- Services Web SOAP et REST
- Failles des Services Web SOAP et des Services REST
- Axes de prévention et bonnes pratiques dans le domaine

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 « Comprendre SELinux et savoir modifier la politique de sécurité »

Réf : SELinux

SELinux vise à renforcer la sécurité d'un système Linux en mettant en œuvre une politique de contrôle d'accès obligatoire. SELinux est intégré en standard au noyau Linux depuis 2003 et certaines distributions (Fedora depuis 2004, Red Hat Enterprise Linux et CentOS depuis 2005) l'activent par défaut.

On constate en pratique que beaucoup d'administrateurs de systèmes Linux sur lesquels SELinux est activé par défaut le désactivent parce qu'ils ne comprennent pas son fonctionnement et que SELinux les empêche de travailler. S'il est gênant pour les administrateurs, il est également gênant pour les intrus et c'est son intérêt.

Objectifs

- Gérer en profondeur les problèmes de sécurité liés aux systèmes Linux
- Comprendre les mécanismes du fonctionnement de SELinux
- Analyser les problèmes pratiques liés à SELinux
- Savoir adapter les contextes de sécurité des fichiers et les booléens
- Savoir personnaliser la politique de sécurité

Durée & horaires

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

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 exercices pratiques et échanges interactifs

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- 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

- Contexte de sécurité
- L'option `-Z` (ou `--context`)
- Mise en évidence des problèmes pratiques posés par SELinux
- États de fonctionnement
- La commande `sestatus`
- Les commandes `getenforce` et `setenforce`
- La commande `selinuxenabled`

Les booléens SELinux

- La commande `getsebool`
- La commande `setsebool`

Gestion de la politique de sécurité

- La commande `setfiles`
- La commande `restorecon`
- La commande `fixfiles`
- La commande `chcon`
- La commande `newrole`
- La commande `runcon`
- La commande `seinfo`
- La commande `semanage`
- La commande `apol`
- Les commandes `audit2why` et `audit2allow`

Modification de la politique de sécurité

- Types de fichiers permettant d'étendre la politique de sécurité
- Procédure d'extension de la politique de sécurité
- Exemple de module simple
- Exemple de module de politique
- Cas pratiques

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

- 5 jours soit 35 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 et connaissances de base en sécurité, par exemple une certification SECUCYBER d'HS2 ou GSEC de GIAC ou CISSP d'(ISC)2 ou équivalent.
- Très bonnes connaissances en réseaux (VLAN, pare-feux, etc), par exemple une certification CCNA+CCNP de Cisco ou NSE4 de Forninet ou CCSA de Checkpoint ou CSNA de Stormshield ou équivalent.

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 / risque / persona
- Lien avec d'autres domaines
  - Administration
  - Urbanisation
  - Gestion des risques
- Dessine-moi un schéma d'architecture

Notions de réseaux

- Modèles théoriques
- Quiz introductif
- Couche 2 - Liaison
  - Domaine de collision / domaine de diffusion
  - Composants de base et adressage
  - Segmentation - LAN / VLAN / PVLAN
  - Sécuriser le lien local
- Couche 3 - Réseau
  - Composants de base et adressage
  - Segmentation
- Échanges d'informations
- Composants spécifiques
  - Diode / WDM / sonde

Flux

- Filtrage
- Modes de connexion
- Chiffrement
- Authentification

Architecture de base : risques, points d'attention, contraintes et solutions

- Notion de bulle et niveaux : tiers-{0,2}
- Séparation des environnements
  - Production vs. hors-production
- Authentification et autorisation
- Administration
  - Zones d'administration
  - Spécificités de Windows et Active
  - Postes d'administration
- Composants d'infrastructure et de sécurité
  - Services d'infrastructure
  - Cas pratiques : DNS / supervision / sauvegarde / accès Internet / VPN
- Applications, 2-tiers / 3-tiers
- Continuité
  - Redondance et haute disponibilité
  - Dépendance circulaire

Architectures spécifiques

- Virtualisation de l'infrastructure
- Cloud
- Sous-traitants
- Architectures industrielles & SCADA
- Gestion technique des bâtiments
- Divers
  - ToIP / Wi-Fi / Grid / virtualisation et infrastructures "agiles" / IoT

Formation « Sécurité et Red Team Wi-Fi moderne »

Réf : SECUWIFI

Objectifs

- Comprendre la sécurité Wi-Fi dans sa globalité
- Apprendre à attaquer, à détecter et à défendre un réseau Wifi
- Identifier les points faibles et erreurs courantes sur les architectures existantes

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 intéressée par la compréhension de la sécurité Wi-Fi dans sa globalité.

Pré-requis

- Connaissances de base en Linux (lignes de commande, compilation, etc.)
- Base en réseaux et manipulation d'outils de visualisation tels que Wireshark, Scapy est un plus
- Connaissances en sécurité offensive ou défensive
- Des connaissances en Wi-Fi sont un plus

Méthode pédagogique

- Cours magistral avec échanges interactifs
- Travaux pratiques

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- 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

1. IEEE 802.11

2. Réseaux sans-fil
- Les différents modes
- Sécurité actuelle suivant les modes

3. Choix du matériel
- Cartes d'acquisition
- Antenne
- Optimisation de la transmission
- Amplificateurs et connecteurs
- Problèmes courants

4. Linux et module noyaux
- Introduction
- Pile protocolaire et modules
- Différences SoftMAC et HardMAC
- Chargement de module
- Problèmes courants

5. Inspection réseau
- Monitoring et identification de réseaux
- Analyse de paquets
- Manipulation de paquets
- Interactions avec un point d'accès
- Analyse de « probe requests »

6. Attaques
- Modes:
  - Réseaux ouverts
  - WEP – WPA/WPA2
  - WPA/WPA2 entreprise – WPS
  - WPA3
- Relais
- Vulnérabilités publiques
- Méthodes Red Team et retour d'expérience
- Procédures d'attaques adaptées aux conditions
- etc.

7. Aller plus loin
- Recherche de vulnérabilités
- Attaque de la pile protocolaire
- Débogage avec Nexmon
- Outillage discret et minimalisation
- etc.

Formation « OSINT / CTI »

Réf : OSINT

Objectifs

- Réaliser des recherches avancées en source ouverte
- Rédiger des fiches opérationnelless du mode opératoire de l'attaquant
- Lier des identifiants à une ou des personnes physiques
- Mettre en place une stratégie de veille afin de suivre des attaquants ou de protéger une entreprise

Durée & horaires

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

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Analyste SOC
- Enquêteur
- Analyste Threat Intel (CTI)
- Pentesteur

Pré-requis

- Cette formation n'impose pas de prérequis particulier. La maîtrise des outils informatiques de base est nécessaire.
- Avoir une connexion internet

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs
- Immersion dans le rôle d'un enquêteur suite à une compromission
- Apprentissage par application concrète tout en laissant une grande autonomie dans la démarche d'investigation

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- 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 OSINT1 par HS2.

Programme

Jour 1

- Méthodologie d'enquête (timeline, prise de note)
- Relevé d'Indice de Compromission (IoC)
- Pivot vers de nouveaux IoCs
- Recherche avancée : expression régulière (regexp)

Jour 2

- Moteur de recherche DeepWeb
- Dorking
- Cartographie réseau
- Renseignement sur protocoles variés (hors Web)
- Exploitation des métadonnées fichiers et protocoles

Jour 3

- Recherche et analyse de code
- Reverse image
- Utilisation outil open-source
- Reconnaissance réseau
- Outil d'investigation d'adresse courriel
- Cartographie d'information

Formation « Détection et réponse aux incidents de sécurité »

Réf : SECUBLUE1

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
- 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
- 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
- Renseignement sur la menace
  - CTI et renseignement
  - Cyber Kill Chain
  - MITRE ATT&CK / SHIELD
- Principes de défense

Module 2 : Comprendre l'attaque

- Objectifs de l'attaquant
- Phases d'une attaque
- Différents champs de bataille
  - Réseau
  - Systèmes d'exploitation Applications
  - Active Directory
  - Cloud

Module 3 : Mettre en place notre architecture de détection

- Détection : les classiques
  - SIEM
  - IDS/IPS, WAF, CASB
  - SandBox, Capture réseau
  - Honeypots et autres Honey-*
- Valoriser les "endpoints"
  - Parefeu, antivirus
  - Whitelisting: Application Control, AppLocker
  - Sysmon
  - AppArmor, SELinux
- Journalisation
  - Windows : configuration, choix des événements, Powershell
  - Linux : auditd
  - Centralisation: WEF, syslog-NG...
  - Focus : Journalisation
- Bonus : Données DNS

Module 4 : Détecter les différentes phases d'une attaque

- Outils & techniques
  - Wireshark/Tshark, Bro/Zeek
  - Recherche d'entropie
- Reconnaissance
  - Fuites d'information
  - scans réseau et applicatifs
- Exploitation
  - Man-in-the-Middle : ARP spoofing, Rogue DHCP...
  - Protocoles obsolètes & Responder
  - Kerberoas
  - Attaques mémoire
  - Attaques web : WAF et "Self-defense" applicative
- Mouvement latéral
  - Exécution de commandes distantes
  - Pass-The-Hash / Pass-the-Ticket
  - Attaques Powershell
- Élévation de privilège
  - Vol de secrets : Mimikatz, Impacket...
  - Recherche de chemins d'attaque : Bloodhound / SharpHound
- Persistance
  - Persistance Linux et Windows
  - Golden Ticket, Silver Ticket, SID History...
- Exfiltration et C&C
  - Tunnelling: ICMP, DNS...
  - C&C HTTP/HTTPS

Module 5 : Réponse à incident et Hunting

- SOC & CSIRT
- Triage
- Analyse de binaires
- Recherche d'IOC, Yara
- Outils de réponse : Kansa, GRR, DFIR-ORC...
- Remédiation Linux & Windows
- Partons à la chasse : Hunting

Formation « Détection des incidents de sécurité »

Réf : SECUSOC

Tous les attaquants laissent des traces ! Le SOC est la brique indispensable pour les détecter et limiter les impacts d'une compromission. Détecter est impératif face au niveau de menace actuel et ce sont l'efficacité des analystes et l'intelligence des règles qui font la différence. Vous disposez d'un SOC, ce SOC dispose d'une vision unique sur le Si grâce aux sources d'information qu'il collecte, il est en première ligne pour détecter. De nouvelles techniques de recherche d'attaquant, dont la chasse aux menaces (hunting), doivent également être mis en place pour être proactif vis à vis des nouvelles techniques et outils d'attaque.

Objectifs

- **Former les analystes SOC à la détection et aux spécificités de la détection système, en abordant les aspects méthodologiques, théoriques et pratiques de la création d'alertes et de leur investigation, en s'appuyant principalement sur l'environnement Windows.Appliquer la notion de "prévention détective"**

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

- **Analystes SOC N2 et N3**

Pré-requis

- **Avoir de bonnes bases en cybersécurité ou avoir suivi la formation SECUCYBER**
- **Connaissance d'un SIEM (ELK, Logpoint, Prelude, Qradar, Splunk, etc) ou avoir suivi une formation SPLUNK ou ELASTICSEARCH**
- **Avoir un SOC dans son organisation**

Méthode pédagogique

- **Cours magistral illustré par des travaux pratiques à chaque module**

Supports

- **Support de cours en français au format papier en présentiel et au format numérique en distanciel**
- **Machine virtuelle contenant l'ensemble des exercices**
- **Ordinateur portable mis à disposition des stagiaires qui ne disposerait pas du leur**
- **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 de savoir-faire, pas un simple test de connaissance, dure 1h30 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification SECUSOC par HS2.**

Programme

Panorama de la détection système

- Chaîne de détection et terminologie
- Organisation des équipes
- Sources de données
- Quoi collecter ?
- Normalisation et standardisation des données
- Connaissance du SI supervisé et des pratiques d'administration
- Cycle de vie des signatures
- Tableaux de bord
- Environnement, contexte de détection, interaction avec les autres acteurs de la sécurité opérationnelle

Méthodologies

- Kill chain / Mitre attack
- "Pyramide of pain" et détection de menace connue vs inconnue
- Démarche de création et de hiérarchisation des nouvelles alertes
- Compréhension des apports de l'apprentissage automatique (machine learning)
  - Notions clés
  - Comment travailler avec les experts en mégadonnées (data scientists)

Techniques de détection pour Windows

- Détection grâce aux journaux d'authentification :
  - ActiveDirectory, Kerberos, NTLM, lsass, ntds, sam
  - Moyens de détection des outils et techniques de vol d'authentifiant dont mimikatz
- Techniques d'attaque et de détection Powershell
- Pré-requis et création de règles Sysmon
- Détection des techniques de latéralisation : RDP, SMB, PSRemoting, WMI
- Détection de la persistance : création de services, tâches planifiées, clés de registres, dossiers startup
- Repérage des traces générées par les outils communément utilisés par les attaquants : Cobalt Strike, Empire, Lolbins
- Fonctionnement et détection des élévations de privilège : SID, Niveau d'intégrité, token
- Détection en amont la reconnaissance faite par l'attaquant au sein du SI : adfind, bloodhoud, LOLBins

Techniques de détection de compromission d'autres environnements

- Linux : auditd, wazuh, ossec
- Réseau : scans, flux, beaconning, trafic HTTP/HTTPS sortant, trafic DNS
- Infonuagique (Cloud) : API et services
- OT (systèmes industriels, objets connectés)

Processus métier des analystes

- Processus d'investigation d'une alerte
- Processus de chasse (hunting)
- SOAR (ochestration, automatisation et réponse aux incidents de sécurité)

Examen de certification

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

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

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

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

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

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

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

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

- 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

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
  - Technique de contournement de flux d'exécution (ie: detour)
- Shellcode
  - Techniques et outils d'analyses
  - Miasm2
  - Unicorn Engine

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

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

- **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

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

- 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***

Formation « Tests d'intrusion et développement d'exploits »

Réf : PENTEST2

Pour tester des vulnérabilités complexes, les outils et exploits grand public rencontrent parfois leurs limites. Maitrisez les concepts derrière ces outils et apprenez à concevoir des attaques vous permettant de tirer profit de toutes les situations.

Objectifs

- Maîtriser les vulnérabilités complexes
- Comprendre le fonctionnement des exploits
- Développer des outils d'attaque
- Contourner les protections système
- Élargir la surface d'attaque

Attention, cette formation ne traite pas des bases des tests d'intrusion ni de l'utilisation de Metasploit, elle va exclusivement au-delà.

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 16h00/16h30.

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Pentesters expérimentés
- Développeurs expérimentés

Pré-requis

- Avoir suivi PENTEST1 ou posséder une bonne expérience des tests d'intrusion

Méthode pédagogique

- Cours magistral avec travaux pratiques et échanges interactifs
- 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 tests d'intrusions
- Un réseau vulnérable fidèle à la réalité sert de plateforme pour les tests
- Tous les outils utilisés sont issus du monde libre et peuvent être réutilisés lors des missions
- Les techniques et outils classiques ainsi que modernes sont utilisés tout au long de la formation

Supports

- Support de cours en Français imprimé
- Cahier d'exercices
- Cahier de corrections
- Ordinateur portable prêté 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

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

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 PENTEST2 par HS2.**

Programme

WEB AVANCE
- Injections SQL en aveugle
- Injections SQL basées sur le temps
- Attaques de désérialisation
- Attaques avancées BDD
- Attaques XXE

ATTAQUES RESEAU
- Scan furtif
- Scapy
- TCP-highjack
- Network Access control (NAC)
  - Contourner un portail captif
  - Contourner le 802.1X
- VLAN-Hopping
- Rerouter le trafic
  - ARP cache poisoning
  - DNS spoofing
  - Exploitation des protocoles de routing
- Attaque PXE

LES OUTILS DE L'EXPLOITATION AVANCEE
- Python
- Assembleur
- Désassembleurs et debuggers
  - GDB/Peda, Radare2
  - Ollydbg, Immnunity, EDB

LES BASES DU DEVELOPPEMENT D'EXPLOIT
- structure basique d'un exploit (python/perl)
- Win32 shellcoding
- Exploits Metasploit
- Fuzzing
  - Sulley/Boofuzz

DEVELOPPEMENT EXPLOITS
- String Format
  - Lire à des adresses
  - Ecrire à des adresses
  - dtor
  - Ecraser la GOT
- Double free
- Off by one
- Integer Overflow

VULNERABILITES APPLICATIVES
- String Format
  - Lire à des adresses
  - Écrire à des adresses
  - dtor
  - Ecraser la GOT
- Double free
- Off by one
- Integer Overflow

BUFFER OVERFLOW
- Stack based
  - Ecraser EIP
  - Sauter vers le shellcode
    - Jump (or call)
    - Pop return
    - Push return
    - Jmp [reg + offset]
    - blind return
    - SEH
    - popadd
    - short jumps et conditionnal jumps
    - stack pivot
  - SEH Exploits
  - Egg Hunting
- Heap based
  - Heap spraying
- Encodage
  - MSFVenom
  - code polymorphique (veniatian encoding)
- Unicode Exploit

CONTOURNEMENT DES PROTECTIONS
- * NX/DEP et ASLR
  - ret2libc
  - retour dans system()
  - ROP
  - écrasement partiel d'EIP
  - NOP spray
- Stack cookies (canaries)
- SafeSEH
- SEHOP
- Outils divers
  - Mona
  - Peda
  - Pwntools

WIFI
- WEP
- WPA/WPA2
- WPS

PHISHING
- Pieces jointes vérolées
  - SCRIPT
  - DDE
- Créer une porte dérobée dans un exécutable
  - Utiliser les code cave
- Échapper aux antivirus
- Assurer la persistance
  - Le Command & Control

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

Formation « Tests d'intrusion des systèmes industriels »

Réf : PENTESTINDUS

La vérification de la cybersécurité par les tests d'intrusion est une mesure de sécurité courante (Redteam, Bug Bounty), et qui est dans l'arsenal des bonnes pratiques. Dans le cas des systèmes industriels, le matériel cible est spécifique, le contexte et sa sureté de fonctionnement et sa criticité souvent hors des contextes de tests habituels. Il est donc indispensable de comprendre cet environnement et ces composants pour pouvoir en évaluer le niveau de sécurité.

Objectifs

- Comprendre le fonctionnement des SI industriels et leurs spécificités
- Découvrir les outils et les méthodologies pour les tests d'intrusion sur SI industriel
- Mettre en pratique ses connaissances sur un environnement industriel représentatif

Durée & horaires

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

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- Ingénieur en charge de la sécurité ou du contrôle de SI industriels
- Consultants, auditeurs et pentesteurs voulant monter en compétence sur les SI industriels
- Automaticien voulant se former à la sécurité d'un point de vue attaque et par la pratique

Pré-requis

- Bonne connaissance générale en informatique et en réseaux, par exemple une certification SECUCYBER d'HS2 ou CISSP d'(ISC)².
- Maîtrise d'un interpréteur de commande (Bash, Powershell, etc)
- Utilisation de machines virtuelles
- Une expérience en test d'intrusion est un plus
- Aucune connaissance des systèmes industriels n'est nécessaire

Méthode pédagogique

- Cours magistral
- Démonstrations
- Travaux pratiques avec un ordinateur par stagiaire, avec mise en œuvre sur plusieurs automates et exercice sous forme de concours (CTF)

Supports

- Support de cours au format papier en français
- Ordinateur portable mis à disposition du stagiaire
- Clé USB contenant les machines virtuelles, les outils utilisés, ainsi que de la documentation complémentaire
- 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 PENTESTINDUS par HS2.**

Programme

Module 1 : Introduction aux SI industriels

- Historique des SI industriels et de l'automatisme
- Vocabulaire
- Modèle CIM
- Architectures classiques
- Composants des SI industriels (PLC,HMI,SCADA,DCS,capteurs,effecteurs, RTU...)

Module 2 : Tests d'intrusion : principes & outillage

- Tests d'intrusion et autres méthodologies d'évaluation de la sécurité des SI industriels
- Différentes étapes et outil d'un test d'intrusion classique (notamment reconnaissance, exploitation, post-exploitation)
- Travaux pratiques : scans nmap, exploitation simple avec Metasploit

Module 3 : Sécurité des systèmes Windows et Active Directory

- Introduction aux environnements Windows et AD
- Méthodes d'authentifications, format et stockage des mots de passe et secrets
- Faiblesses classiques de ces environnements
- Travaux pratiques : recherche d'informations dans un AD avec Powerview, utilisation de mots de passe et condensats avec crackmapexec…

Module 4 : Vulnérabilités courantes en environnement industriel

- Segmentation réseau
- Sécurité dans les protocoles
- Supervision Sécurité
- Sensibilisation
- Gestion des tiers
- Correctifs de sécurité

Module 5 : Protocoles de communication industriels

- Présentation des protocoles les plus courants (modbus tcp, S7, OPC...)
- Travaux pratiques : analyse de capture réseau Modbus/TCP, S7 et OPC-UA

Module 6 : Introduction à la sureté de fonctionnement

- Présentation du concept
- Méthodologies d'analyse de sureté fonctionnelle
- Différentes couches de sureté
- Travaux pratiques : ébauche d'analyse HAZOP sur un exemple simple

Module 7 : Programmation d'automates programmables industriels (API)

- Présentation des différents langages
- Travaux pratiques : Exercices de programmation en ladder logic sur simulateur Schneider TM221 et SCADA Schneider IGSS

Module 8 : Tests d'intrusion sur API

- Outils de communication pour les protocoles industriels
- Surface d'attaque des automates (web, ftp, http)
- Présentation d'attaques avancées sur les API (protocoles propriétaires, ...)
- Travaux pratiques : Utilisation de mbtget pour envoi de requêtes modbus sur simulateur Schneider, bibliothèque Snap 7 pour échanger avec simulateur Siemens, opcua-gui pour échanger avec SCADA Schneider IGSS

Module 9 : Principes de sécurisation des SI industriels

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

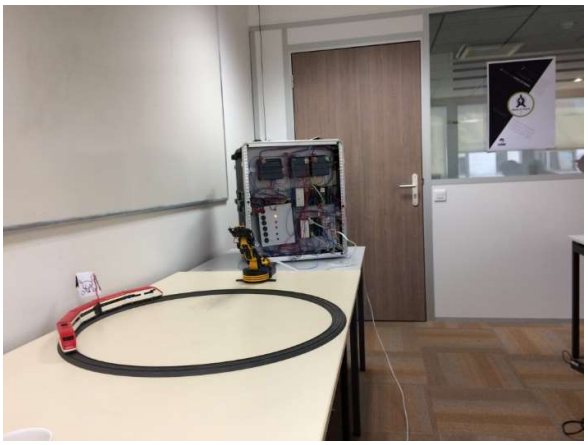
- Panel normatif
- Architectures et technologies de cloisonnement réseau
- Focus sur les diodes réseau
- Autres points d'attention particuliers

Module 10 : Étude de cas

- Analyse d'une Étude de cas présentant une description d'une société fictive, des schémas réseau, ainsi que des règles de pare-feu.
- Travail collaboratif pour identifier vulnérabilités, risques, et élaboration de plan d'action

Module 11 : Exercice sous forme de CTF (Capture The Flag)

- Mise en pratique des acquis par la réalisation d'un test d'intrusion sur un environnement représentatif :
  - Compromission d'un environnement bureautique
  - Découverte de liens réseau et rebond vers le SI industriel
  - Attaques sur les automates et la supervision pour impacter un processus physique (train miniature et bras robotisés)
  - Visuels de la maquette :



Formation « Tests d'intrusion des serveurs et des applications Web»

Réf : PENTESTWEB

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

Objectifs

- Anticiper les besoins des tests d'intrusion
- Comprendre les principales vulnérabilités du web
- Analyser les risques encourus
- Détecter les failles de sécurité
- Exploiter les vulnérabilités pour prendre le contrôle de l'infrastructure

Durée & horaires

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

Nombre de participant

- Minimum 8 participants – Maximum 24 participants

Public visé

- Quiconque souhaite comprendre et pratiquer les techniques utilisées par les attaquants pour compromettre un système d'information depuis Internet :
  - Pentesters
  - RSSI
  - Chefs de projets
  - 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 interactifs. La formation est proposée en mode présentiel et accessible en mode distanciel via ZOOM pour ceux qui ne veulent pas se déplacer

Supports

- Support de cours numérique en Français projeté
- Support de cours en Français imprimé en présentiel / au format numérique en distanciel après signature du règlement intérieur
- Cahier d'exercices
- Cahier de corrections
- Ordinateur portable prêté pour la réalisation des exercices

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

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 PENTESTWEB par HS2.**

Programme

Le test d'intrusion
- Méthodologie et type de tests
- Équipement et outils
- Législation
- Déroulement de l'audit
- Gestion des informations et des notes
- Clôture de l'audit
- Pour aller plus loin

Le proxy applicatif
- Usages
- Burpsuite, Zap...

Les mécanismes du Web
- Le protocole HTTP (méthodes, entêtes, codes de retours, encodage...)
- Les risques du modèle client/serveur

La sécurité du client
- La SOP
- Les communications "cross-domain"
- Contournements CORS
- Contournements CSP
- Open Redirect

Cryptographie
- SSL/TLS
- Les suites cryptographiques
- Renegociation non sécurisée
- Audits et contrôles
- La PKI
- Le cassage de condensats

Reconnaissance et fuite d'informations
- Introduction et objectifs
- Découverte passive
  - Résolutions DNS et registres
  - Détournement de sous-domaine
  - OSINT
  - Les Googles Dorks
  - Les fuites
- Découverte active
  - Le transfert de zone
  - Le balayage de ports
  - Découverte de serveurs web
  - Prévisualisation des applications
  - Crawling et Spidering
  - Le WAF
- Le scan de vulnérabilités

Les processus d'authentification
- Gestion de l'identité
- Les attaques sur l'authentification
  - XML Signature Wrapping
  - Détournement d'Oauth

La gestion des sessions
- Les jetons de session
- Les cookies
- Jetons JWT
- Forge de requêtes inter-sites (CSRF)
- Fixation de session
- Forge de jetons de session
- Le cloisonnement des sessions
- Référence directe à des objets non sécurisés (IDOR)

Les injections
- Les injections coté client
  - L'injection XSS
- Les injections côté serveur
  - L'attaque CRLF (et response splitting)
  - Les injections de commandes
  - L'injection XXE
  - L'injection SQL
  - Quelques injections moins fréquentes (XPath, LDAP, NoSQL)
  - Les injections via sérialisation/dé-sérialisation
  - Forge de requête côté client (SSRF)

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

Les Webservices et API

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

- Le fonctionnement des Webservices (XML-RPC, SOAP, REST)
- Les websockets
- Méthodologie d'intrusion
- Les applications mobiles

Le Cloud

- Méthodologies et spécificités
- Quelques outils
- Vulnérabilités

Les vulnérabilités plus complexes

- Tour d'horizon (Buffer Overflow...)
- Méthodologie d'exploitation

Tout au long de la semaine, vous pratiquerez les attaques présentées durant le cours sur notre infrastructure web réaliste simulé : de simple visiteur sur un site web, terminez root d'un serveur ! (Tous les outils utilisés durant les exercices sont accessibles gratuitement en dehors de la formation)

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

Formation « SPLUNK »

Réf : SPLUNK

Splunk permet à de très nombreuses équipes opérationnelles, SOC, CSIRT de réaliser efficacement leurs investigations numériques, détection d'attaques ou chasse, en facilitant les opérations de recherche & manipulation des journaux quelques soient le volume de données. Cette formation vous permettra d'apprendre à utiliser Splunk pour les cas d'usage de la sécurité informatique, elle complète bien les formations SECUBLUE et SECUSOC en vous fournissant les clés pour exploiter au mieux cet outil puissant.

Cette formation n'est pas une présentation exhaustive des capacités de Splunk, elle a été construite pour pouvoir être efficace et pertinente dans l'utilisation de Splunk.

Objectifs

- **Découvrir le fonctionnement et les capacités de Splunk**
- **Apprendre le langage SPL pour requêter les données efficacement**
- **Enrichir les données opérationnelles à partir de sources externes**
- **Créer des tableaux de bord dynamiques pour l'aide à la décision et la synthèse d'informations**
- **Créer des requêtes matures pour la détection d'attaque**

Durée & horaires

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

Nombre de participant

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

Public visé

- **Analystes en détection (SOC)**
- **Analyste en conception (SOC, CSIRT)**
- **Analystes forensique (CSIRT)**
- **Auditeurs**
- **Opérationnels en sécurité**
- **Responsables sécurité opérationnelle**

Pré-requis

- **Connaissances informatiques générales (qu'est-ce qu'une adresse IP, une authentification, etc.)**
- **Compréhension des enjeux généraux en sécurité informatique (qu'est-ce qu'une attaque par bruteforce, une exfiltration de données, etc.)**

Méthode pédagogique

La formation est délivrée à travers un mélange de cours magistral et démonstrations sur le produit. Les apprenants ont tous accès à un Splunk pendant toute la durée de la formation leur permettant de reproduire les exemples fournis en cours. Des travaux pratiques de mise en œuvre sont fournis aux apprenants sur les concepts clés. Les travaux pratiques possèdent tous un énoncé et une solution détaillée, permettant aux apprenants de valider leurs exercices. Les formateurs supervisent la réalisation des travaux pratiques et accompagnent les apprenants ayant besoin d'aide. Pour les apprenants venant en salle de formation, le déjeuner est offert et est un moment privilégié de partage entre apprenants et formateurs.

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

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 1h00 et a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification Splunk par HS2.**

Programme

Introduction à Splunk

- Produits de la marque Splunk
- Fonctions de Splunk Enterprise
- Architecture
- Flux de données

Ajouter des données

- Processus d'indexation
- Téléversement à travers l'interface graphique
- Organisation de la donnée dans les indexes
- Envoi à travers un Universal Forwarder
- Envoi à travers un collecteur syslog
- Supervision de modifications dans des fichiers
- Envoi par API
- Extraction de champs
- Normalisation des champs

Requêter

- - Accès aux données indexées
- - Filtre temporel
- - Paramètres des tâches de recherche
- - Exploration des résultats
- - Modes de recherche
- - Différences entre les événements et les statistiques
- - Commandes
  - Search
  - Fieldsummary
  - Where
  - fields
  - rename
  - rex
  - eval
    - Fonctions d'évaluation
  - dedup
  - sort
  - head
  - tail
  - fillnull
  - table
- - Calculs statistiques
  - Commande stats
  - Fonctions d'agrégations
  - Agrégats multiples
  - Combinaison des fonctions d'agrégation et des fonctions d'évaluation
- Manipulation des JSON
- Enrichissement de données
  - Types de lookups
  - Manipulation des lookups
  - Recoupement des données
  - Utilisation des lookups pour faire une chasse de marqueurs
    - Jointures
  - Macros de recherche
  - Sous-recherches

Configurer

- Fichiers de configuration
- Précédence des configurations
- Périmètres et gestion des droits
- Objets de connaissance
- Partage d'objets
- Installation d'une application

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

Tableaux de bord

- Utilisation des tableaux de bord Studio
- Forces et limitations du moteur
- Sélecteurs et filtres
- Commande timechart
- Requêtes chaînées
- Utilisation des tokens
- Interactivité des tableaux de bord

Requêtes avancées

- Commandes bin et transaction
- Requêtes pour l'investigation numérique
- Requêtes pour la détection
- Détection par seuil
- Création d'alertes pour un SOC

Conclusion

- Ressources pertinentes pour l'apprentissage continu

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

Nos Intervenants
Formations en vie privée, droit de la cybersécurité

François Coupez dispense la formation :
DPO

Erik Boucher de Crèvecoeur dispense la formation :
ISO27701LI

Amélie Deleuze dispense la formation :
SECUDROIT

Pierre Desmarais dispense les formations :
SECUSANTE - ISO27701LI

Hadi Elkhoury dispense la formation :
PIA

Olivier Iteanu dispense les formations :
SECUCLOUD

Alexandre Magloire dispense la formation :
SECUSANTE

Elisabeth MANCA dispense la formation :
SECUCOUD

Amélie Paget dispense les formations :
RGPD - SECUDROIT - ISO27701LI

Géraldine Péronne dispense les formations :
DPO - RGPD

Diane Rambaldini dispense les formations :
DPO - PIA

Hervé Schauer dispense la formation :
SECUCLOUD

Nos Intervenants
Formations en continuité d'activité et cybersécurité organisationnelle

Yuksel Aydin dispense la formation : IS027035

Jean-Luc Austin dispense la formation : CISA

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

Pierre-Antoine Bonifacio dispense la formation : CISSP

William Bourgeois dispense les formations : ISO27LA - ISO27LI

Matthieu Caron dispense les formations : CISSP - CCSP

Lucien Caumartin dispense la formation : ISO27LA

Thierry Chiofalo dispense la formation : ISO27004

François Coupez dispense la formation : RSSI

Sabine Dacruz Mangeot dispense la formation : SECUPROJET

Amélie Deleuze dispense la formation : RSSI

Laurent Doublein dispense les formations : RPCA - ISO22LA - ISO22LI

Alexandre Fernandez-Toro dispense les formations : ISO27LA - ISO27LI

Etienne Gérain dispense les formations : EBIOS2018 - ISO27RM

Jordan Hordé dispense les formations :
ISO27LA - ISO27LI - ISO27RM - EBIOS2018

Mathieu Couturier dispense la formation : SECUCRISE

Béatrice Joucreau dispense les formations :
ISO27LA - ISO27LI - ISO27RM

Anthony Hubbard dispense la formation :
RSSI - ISO27LA - ISO27LI - ISO27035

Giuliano IPPOLITI dispense la formation :
CCSP

Thomas Le Poëtvin dispense les formations :
RSSI - EBIOS2018 - ISO27LA - ISO27LI - ISO27RM

Julien Levrard dispense la formation :
ISO27LI

Alexandre Magloire dispense les formations :
SECUHOMOL- EBIOS2018 - ISO27LI

Elisabeth Manca dispense les formations :
RSSI - ISO27LI

Lionel Mourer dispense les formations :
RPCA - ISO22LA - ISO22LI

Vincent Nguyen dispense les formations :
SECUCRISE - ISO27035

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

Matthieu Renard dispense la formation :
EBIOS2018

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 :
EBIOS2018 - ISO27RM - ISO27LI

Alphonsine Yacoubou-Djima dispense les formations :
ESS27 - ISO27LA - ISO27LI

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 - SELINUX

Danil Bazin dispense les formations :
ESSCYBER - FORENSIC1 - FORENSIC2

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

Rémi Chauchat dispense les formations :
SECUINDUS - PENTEST1

Sébastien Dudek dIspense la formation :
SECUWIFI

Tarik El Aouadi dIspense la formation :
SECUWEB

Azziz ERRIME dIspense la formation :
SECUWEB

Jordan Hordé dispense la formation :
SECUARCH

Olivier Houssenbay dispense la formation :
ESSCYBER - SECUCYBER - SECUWIN

Baptiste Dolbeau dispense la formation :
FORENSIC1

Romain Bentz dispense la formation :
PENTEST1 - PENTEST2

Olivier Caillault dispense la formation :
SPLUNK

Cyrille De Pardieu dispense les formations :
SECUBLUE1 - SECUWIN

Igor Hermann dispense la formation :
SPLUNK

Anthony Hubbard dispense la formation :
SECUBLUE1

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

Jérôme Naucelle dispense la formation :
SECUWEB

Christophe Renard dispense les formations :
SECUINDUS

Julien Reveret dispense la formation :
FORENSIC1

Jérémy Richard dispense la formation :
SECUBLUE1

Inês Ribeiro dispense la formation :
PENTEST1

Matthieu Schipman dispense les formations :
ESSCYBER - SECUCYBER - SECUBLUE1 - 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 :
PENTESTINDUS

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 OPCO* : oui ❍ non ❍
*Dans le cas d'une subrogation de paiement via votre OPCO, l'inscription sera confirmée uniquement à réception du contrat ou de l'accord de prise en charge de votre OPCO 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 :

Lynda Benchikh / Elisa Keller / Estelle Dubois

☎ +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

Qualiopi processus certifié

RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre de la catégorie d'action suivante : **ACTIONS DE FORMATIONS**