e-Catalyst

# Catalogue de FORMATIONS

e-Catalyst.fr

**Edito du Président** 2

**Les modalités de financements** 3

**CONDITIONS GÉNÉRALES DE VENTE** 4

**Tarifs** 5

**Formulaire d'inscription** 6

**Formations tout public** 7
Utiliser les outils numériques dans le cadre de l'emploi (réf. NumEmp) 7
Sensibilisation au RGPD dans ma pratique professionnelle (réf. RGPD) 9
Initiation / perfectionnement en informatique ( réf. IniINFO ) 11
Cybersécurité des TPE/PME (réf. CybPME) 13
Certified Data Protection Officer (réf. DPO) 15
ISO 27001 Lead Implementer (réf. ISO01) 16
Après avis favorable du jury d'évaluation, d'un certificat de compétences 17
ISO 27005 Risk Manager (réf. ISO05) 18
EBIOS Risk Manager 2018 (réf. ERM18) 20
Certified Ethical Hacker (réf. CEH) 22
Sauveteur Secouriste du Travail: Formation Initiale (réf. SST) 24
Sauveteur Secouriste du Travail: MAC (réf. MACSST) 26
Sécurité Incendie (Réf : SécInc) 28
Habilitation Électrique BE manœuvre / BS / BR (Ref : HE-BO/BS/BR) 29
Gestes et Postures (réf. GesPos) 31
Chaîne de survie ALERTER / MASSER / DÉFIBRILLER (réf. ChainS) 32

**Certification Délégué à la protection des données (réf. CDPD)** 34
MODULE 1 : Bases techniques (réf. CDPD1) 35
MODULE 1 : Bases juridiques (réf. CDPD1) 36
MODULE 2 : La gestion des risques (réf. CDPD2) 37
MODULE 3 : Sécurisation du Système d'information (réf. CDPD3) 38
MODULE 4 : Pilotage de projet et la communication à 360° (réf. CDPD4) 39
MODULE 5 : Connaissance des outils, l'environnement de travail (réf. CDPD5) 40

**Community manager MAKER (réf. COMM)** 41
MODULE 1 : les fondamentaux du marketing, de la communication et du webmarketing (réf. COM1) 42
MODULE 2 : le réseau social, blog, l'e-réputation et écrire pour le web (réf. COM2) 43
MODULE 3 : Builder : création graphique, vidéo, un site internet la VR (réf. COM3) 44
MODULE 4 : Créer une campagne publicitaire social média, et la suivre (réf. COM4) 45
MODULE 5 : Communication 360° et le mode projet (réf. COM5) 46

**Spécialiste défense des systèmes d'information (réf. SDSI)** 47
MODULE 1 : Les bases du réseau (réf. SDSI1) 48
MODULE 2 : Reconnaissance (réf. SDSI2) 49
MODULE 3 : Attaque (réf. SDSI3) 50
MODULE 4 : Attaque déportée (réf. SDSI4) 51
MODULE 5 : gouvernance et certification CEH (réf. SDSI5) 52

# Edito du Président

e-Catalyst

Au cœur de vos attentes. En réponse à vos besoins

**Depuis plus de 20 ans, les outils numériques bouleversent le monde de l'entreprise : échanges d'informations, nouveaux débouchés commerciaux, gains d'efficacité, nouvelles méthodes de travail… Les opportunités sont nombreuses pour toutes les entreprises, à commencer par les TPE et PME. Les métiers d'hier évoluent par leur digitalisation et les métiers du numériques apparaissent. Tous sont vecteurs de développement économique.**

**23 600 c'est le nombre de salariés recensés dans la branche numérique dans les Hauts-de-France en septembre 2018, selon une étude Syntec numérique (contre 19 700 en 2015). Ce n'est plus un secret, la digitalisation des métiers génère de l'emploi et c'est du côté de la Data et de la sécurité qu'il faudra se tourner dans les années à venir.**

**La fracture numérique est trop souvent utilisée dans un discours dominant simplificateur et superficiel qui tend à gommer les véritables enjeux sociétaux et à focaliser le débat sur le thème des accès, au sens restrictif du thème.**

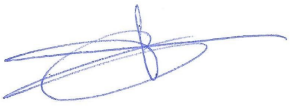
**La première réponse d'e-Catalyst est d'être un appui pour la compétitivité des salariés et des entreprises locales. Cela passe par le renforcement de l'esprit d'innovation et la formation.**
**La transition digitale est une opportunité pour tout salarié ou toute entreprise qui souhaite évoluer.**

**Mais cela nécessite de s'engager dans la démarche. C'est pourquoi e-Catalyst vous accompagne dans ce processus de changement. Certes, par de la formation aux nouveaux outils digitalisés, mais aussi en travaillant avec vous vos freins. De manière co construite, avec le dirigeant si besoin, nous savons adopter la posture managériale adaptée aux situations de stress.**

**Vous trouverez dans ce catalogue un ensemble de formations, réparties en modules, qui vous permettront, certes, de maintenir votre employabilité, ou l'employabilité de vos salariés, mais aussi de développer de nouvelles compétences nécessaires à votre entreprise ou à votre parcours professionnel.**

**L'équipe d'e-Catalyst vous remercie pour l'attention que vous porterez à nos offres et reste à votre service.**

**Julien WALBERT, Président d'e-Catalyst**



# Les modalités de financements

Le financement de la formation professionnelle peut s'avérer complexe car de nombreux financeurs y contribuent. En fonction de votre statut et de la formation envisagée, vous pourrez faire appel aux formations financées par :

- votre compte personnel d'activité : *https://www.moncompteactivite.gouv.fr/cpa-prive/html/#/connexion*
- votre employeur
- l'OPCO dont vous dépendez
- votre Conseil Régional
- Pôle emploi
- la Mission Locale ou un PLIE
- l'AGEFIPH ....

Il existe plus d'une dizaine de financements possibles. Pourtant, clarifier vos droits est une étape cruciale dans la mise en œuvre de votre parcours de formation.

**N'hésitez pas à nous contacter par le biais de *contact@e-catalyst.fr* afin de trouver avec vous l'interlocuteur privilégié qui vous guidera dans votre projet.**

**<u>Zoom sur les obligations des entreprises</u>**

A partir du 1er janvier 2019, les obligations des entreprises en matière de formation évoluent quelque peu.

Elles sont désormais soumises à deux obligations principales :

- Le maintien de l'employabilité : cela passe par l'adaptation du poste de travail et le devoir de fournir au salarié les compétences nécessaires pour accomplir ses missions.
- L'organisation d'entretiens professionnels (qui s'effectue désormais en deux temps) :
  - un entretien obligatoire devra être organisé tous les 2 ans
  - mais aussi l'entreprise devra délivrer une formation non obligatoire au moins tous les 6 ans, c'est-à-dire une formation qui ne découle pas d'un texte normatif (loi, décret, accord collectif notamment)

***e-Catalyst*** est à la disposition des dirigeants souhaitant être accompagnés dans la création de leur plan de développement des compétences.

# CONDITIONS GÉNÉRALES DE VENTE

Les inscriptions aux formations sont soumises aux présentes conditions, sauf dérogation écrite et expresse d'e-Catalyst. Une inscription implique l'adhésion pleine et entière du responsable de l'inscription et du stagiaire à ces conditions générales de participation.

- **Article 1- Inscription**

Les inscriptions se font par mail via contact@e-catalyst.fr

En cas de prise en charge du paiement d'une formation par un organisme extérieur (OPCO), il appartient, au responsable de l'inscription, de communiquer à e-Catalyst les coordonnées complètes de celui-ci et de communiquer à cet organisme extérieur tous les éléments qui lui sont indispensables pour assurer ce paiement. En cas de prise en charge partielle par cet OPCO, la différence de coût vous est facturée directement. Si votre OPCO ne confirme pas la prise en charge de votre stage avant son démarrage, le coût de ce stage sera facturé dans sa totalité à votre entreprise.

- **Article 2- Confirmation d'inscription, convocations et attestation**

Dès réception d'une demande d'inscription, une confirmation d'inscription et une convention de formation sont adressées au responsable de cette inscription.
7 jours avant le début de la formation, une convocation qui précise la date, le lieu et les horaires de la formation est adressée au responsable de l'inscription et / ou au participant.
À l'issue de chaque formation relevant du champ de la formation professionnelle continue, une attestation d'assiduité ainsi qu'une facture de formation professionnelle est adressée au responsable de l'inscription.

- **Article 3- Tarifs**

Les prix sont indiqués en euros hors taxes, sur chaque programme, en inter-entreprises. Tout stage commencé est dû dans sa totalité. Les prix n'incluent pas les forfaits repas. Toutefois, pour davantage de confort pour vos stagiaires, et une facilité de gestion pour vous, cet aspect peut être pris en charge et inclus dans le prix de la prestation.

- **Article 4- La garantie de maintien des stages inter-entreprises**

Le nombre de participants aux stages inter-entreprises est limité à une douzaine de personnes environ – sauf cas particuliers. e-Catalyst annule le minimum de stagiaires inter-entreprises et maintient ses formations même avec un nombre réduit de participants, lorsque le thème s'y prête et si les conditions sont réunies. Dans le cas d'un stage inter-entreprises maintenu à effectif réduit, e-Catalyst propose à l'entreprise de nouvelles conditions de réalisation de la formation

- **Article 5- Annulation et abandon**

Toute demande d'annulation d'une inscription à l'initiative du stagiaire ou du responsable de l'inscription doit être notifiée par écrit à e-Catalyst et parvenir au moins 15 jours avant le début du stage par A/R. Pour toute annulation parvenue moins de 2 semaines avant le début du stage concerné ou en cas d'absence du stagiaire, e-Catalyst facturera à l'entreprise inscrite la totalité du prix de la formation. Sous réserve des pré-requis, le remplacement par une autre personne est accepté. Par ailleurs, e-Catalyst se réserve le droit d'ajourner à titre exceptionnel une session au plus tard 7 jours avant le début de celle-ci, si le nombre de participants prévu est jugé insuffisant pour garantir une qualité pédagogique satisfaisante. Dans ce cas, e-Catalyst s'engage à prévenir immédiatement chaque participant, par écrit, et à lui proposer une inscription prioritaire sur la prochaine session de la formation concernée.

- **Article 6- Paiement**

Les factures sont payables comptant sans escompte, au plus tard à la date d'échéance figurant sur celle-ci, par virement. Toute facture non payée à l'échéance porte intérêt, de plein droit et sans mise en demeure préalable, à un taux égal à une fois et demi le taux de l'intérêt légal, calculé par mensualité. En cas de prise en charge du paiement d'une facture par un organisme payeur extérieur, il appartient, au responsable de l'inscription, de communiquer à cet organisme tous les éléments qui lui sont indispensables pour assurer ce paiement. Si celui-ci n'était pas effectué, e-Catalyst serait fondé à réclamer le montant de ce paiement à l'entreprise inscrite, solidairement débitrice à son égard.

- **Article 7- RGPD**

Les informations à caractère personnel communiquées par le client à e-Catalyst en application et dans l'exécution des commandes et / ou ventes pourront également être communiquées aux partenaires contractuels de e-Catalyst pour les besoins desdites commandes. Elles font l'objet d'un traitement et d'une conservation conformes au règlement (UE) 2016/679

du Parlement européen et du Conseil du 27 avril 2016 (RGPD).

# Tarifs

**Tarif dégressif dès le minimum de personnes atteintes.** **DÉLAI : Minimum 4 semaines.**

Un devis personnalisé sera étudié pour toute entreprise en faisant la demande. Demandez les dates de formations.

e-Catalyst est exonéré de TVA en application de l'art. 261-4-4 du CGI pour la formation continue qu'elle met en œuvre.

| Formations tout public | Durée | Conditions particulières | Réf. | Prix |
|---|---|---|---|---|
| Utiliser les outils numériques dans le cadre de l'emploi | 2 jours | par personne | *NumEmp.* | **250€** |
| Sensibilisation au RGPD dans ma pratique professionnelle | 1 jour | par personne | *RGPD* | **250€** |
| Initiation / perfectionnement en informatique | 5 jours | par personne | *COMPT1* | **1500€** |
| Cybersécurité des TPE/PME | 5 jours | par personne | *CybPME* | **1500€** |
| Sauveteur Secouriste du Travail: Formation Initiale | 2 jours | par personne | SST | **190€** |
| | 2 jours | tarif groupe | SSTgr | **980€** |
| Sauveteur Secouriste du Travail: MAC | 1 jour | par personne | MACSST | **120€** |
| | 1 jour | tarif groupe | MACSSTg | **750€** |
| Sécurité Incendie : EPI | 1 jour | tarif groupe | SécInc | **500€** |
| évacuation / Gestes et Postures | 1 jour | tarif groupe | SécEvac | **600€** |
| Habilitation Électrique BE manœuvre / BS / BR | 1 jour | tarif groupe | HEBO/BM | **980€** |
| Habilitation Électrique BR | 1 jour | tarif groupe | HE-BR | **1500€** |
| Gestes et Postures | 1 jour | tarif groupe | GesPos | **500€** |
| Formation « Chaîne de Survie » | 0.5 jour | tarif groupe | ChainS | **500€** |

| Certifications | durée | condition particulière | réf. | prix |
|---|---|---|---|---|
| DPO Certified (by PECB) | 5 jours | par personne | *DPO* | **2850€** |
| ISO 27001 | 5 jours | par personne | *ISO01* | **3000€** |
| ISO 27005 RM | 3 jours | par personne | *ISO05* | **2100€** |
| EBIOS/Risk Manager 2018 | 2,5 jours | par personne | *ERM18* | **1750€** |
| Certified Ethical Hacker | 5 jours | par personne | *CEH* | **3200€** |
| Certification Délégué à la Protection des Données | 75 jours | par personne | *CDPD* | **5000€** |
| Community Manager maker | 65 jours | par personne | *COMcert* | **4500€** |
| Spécialiste en défense des systèmes d'information | 85 jours | par personne | *SDSIcert* | **5500€** |

## Formations certifiantes par module

| | | | | |
|---|---|---|---|---|
| **CERTIFICATION DÉLÉGUÉ À LA PROTECTION DES DONNÉES** | | | | |
| MODULE 1 : Bases techniques et juridiques | 21 jours | par personne | CDPD 1 | **2100€** |
| MODULE 2 : La gestion des risques | 18 jours | par personne | CDPD 2 | **1800€** |
| MODULE 3 : Sécurisation du Système d'information | 21 jours | par personne | CDPD 3 | **2100€** |
| MODULE 4 : Pilotage de projet et communication | 18 jours | par personne | CDPD 4 | **1800€** |
| MODULE 5 : Connaissance des outils, l'environnement de travail | 23 jours | par personne | CDPD 5 | **2300€** |
| **COMMUNITY MANAGER MAKER** | | | | |
| MODULE 1 : Les fondamentaux : marketing, communication, webmarketing | 13 jours | par personne | COM1 | **2200€** |
| MODULE 2 : Gérer un réseau social, blog, l'e-réputation et écrire pour le web | 14 jours | par personne | COM2 | **1500€** |
| MODULE 3 : Builder : création graphique, vidéo, un site internet la VR | 13 jours | par personne | COM3 | **1500€** |
| MODULE 4 : Créer une campagne publicitaire social média, et la suivre | 16 jours | par personne | COM4 | **1500€** |
| MODULE 5 : Pilotage de projet, l'audit et la communication à 360° | 9 jours | par personne | COM5 | **2200€** |
| **SPÉCIALISTE DÉFENSE DES SYSTÈMES D'INFORMATION** | | | | |
| MODULE 1 : Les bases du réseau | 20 jours | par personne | SDSI1 | **2500€** |
| MODULE 2 : Reconnaissance | 15 jours | par personne | SDSI2 | **1600€** |
| MODULE 3 : Attaque | 15 jours | par personne | SDSI3 | **1600€** |
| MODULE 4 : Attaque déportée | 20 jours | par personne | SDSI4 | **2000€** |
| MODULE 5 : Gouvernance et certification CEH | 5 jours | par personne | SDSI5 | **1500€** |

e-Catalyst SAS
49 rue de l'égalité 59600 MAUBEUGE
N° SIRET 84501436400010
Formation : enregistré sous le numéro 32590993659
Présentation détaillée d'e-Catalyst, CV des intervenants,
Catalogue détaillé des stages 2020 sont disponibles sur : www.e-Catalyst.fr

# Formulaire d'inscription

Pour vous inscrire à l'un de nos stages inter-entreprises, merci de nous renvoyer ce formulaire complété par courrier ou par courriel : contact@e-catalyst.fr

**Tarifs :** le prix, net de taxe, comprend les frais de formation, les supports de cours remis à chaque participant pour les sessions organisées dans nos locaux à Maubeuge. Les sessions en entreprise sont personnalisables et établies sur devis.

**Moyens de paiement :** virement ou chèque à l'ordre de e-Catalyst. La facture sera adressée à l'issue du stage.
**Annulation :** voir article 5 du CGV
**Organisation :** dès la validation de l'inscription, chaque stagiaire reçoit un livret d'accueil comprenant la convocation, le programme détaillé, les horaires (de 9h30 à 12h30 et de 13h30 à 17h), etc.
Une fiche de suivi et une attestation de présence seront fournies en fin de stage. Le stagiaire et le prescripteur seront amenés à remplir deux fiches d'évaluation de la formation dispensée dans le cadre de notre démarche d'amélioration de la qualité.

## Sessions retenues

Références :
Dates souhaitées : _____ Nombre de participants : _____ Prix H.T : _____ €
Moyen de règlements : ▢ chèque (joint) ▢ virement (un RIB vous sera envoyé)
▢ à la réception de la facture (bon de commande joint)
Convention de formation à établir : ▢ Oui ▢ Non

## Participants (- 10% du prix global à partir de 2 stagiaires d'une même entreprise aux mêmes sessions)

| | | | | |
|---|---|---|---|---|
| ▢ Mme ▢ M. | Nom : | Prénom : | Tél : | Courriel : |
| ▢ Mme ▢ M. | Nom : | Prénom : | Tél : | Courriel : |
| ▢ Mme ▢ M. | Nom : | Prénom : | Tél : | Courriel : |

## Entreprise

Société : Adresse :

Demandeur : ▢ Mme ▢ M. Nom : Prénom :

Signature : Cachet de l'entreprise :

# Formations tout public

## Utiliser les outils numériques dans le cadre de l'emploi (réf. NumEmp)

**Objectifs :**

Identifier les compétences acquises dans les pratiques numériques
Développer des compétences de base sur l'utilisation des outils numériques dans le cadre professionnel (recherche d'emploi, exercice du métier)
Identifier les conséquences de l'utilisation du numérique dans les pratiques professionnelles (employabilité) comme les opportunités d'emploi et de formation liées aux activités numériques.

***Nombre de jours*** **:** 2 jours (14h)
***Nombre de stagiaires*** **:** 10 à 12
***Outils mis à disposition*** **:** 4 PC portables, 4 tablettes, 4 smartphones, accès à internet
***Prérequis*** **: aucun**
***Codes des fiches ROME les plus proches*** **:**

**Contenus :**

**Journée 1**
**9h-9h30 :** phase d'inclusion : accueil sous la forme de café

- obligation administrative (émargement, explication de l'action et du mode de financement si fonds européens)
- présentation des deux jours et de la méthode pédagogique qui sera utilisée (voir la mallette du formateur)

**9h30-10h :** passage du test diagnostic

**10-12h30 :** module " Créer son adresse mail et sa boite mail et la gérer "

- Création de boite mail GMAIL
- Savoir faire des recherches pertinentes sur internet (utilisation mots clés, savoir sélectionner le bon site)
- Apprentissage des connaissances spécifiques telles que : transfert de mail, gestion de signatures, formulations, archivages, groupes de contacts, etc.
- Exercices de transmission d'informations (j'envoie mon CV, je réponds à une annonce, je fais une relance etc.)

**13h30-14h :** phase d'inclusion : quiz culture générale sur le numérique par le biais d'un KAHOOT

**14h-16h** : module "consulter seul les contenus et effectuer des démarches de recherche d'emploi"

- Créer/modifier un compte sur les réseaux sociaux (Facebook, Twitter, Snapchat) et sur les applications Travail (LinkedIn, Monster, Pôle Emploi)
- Se connecter sur les applications mobiles des réseaux sociaux, des applications travail
- Créer son espace Compte Personnel Formation et faire des recherches de formation en lien avec son projet professionnel

- Utiliser Google Agenda pour synchroniser ses rendez-vous et placer des rappels

**16h30-17h :** phase de déclusion : retour sur la journée, et évocation de métiers en lien avec le numérique ou leur parcours

**Journée 2**
**9h-10h :** phase d'inclusion : accueil sous la forme de café

- obligation administrative (émargement)
- Kahoot permettant de lancer les deux modules de la journée

**10 -12h30 :** module " j'ai mon CV en ligne, je sais me valoriser sur les réseaux"

- Inciter et initier les publics à dématérialiser leur CV
- Initier, former les publics à savoir modifier et mettre à jour leur CV
- Accompagner les publics à la création d'un compte Facebook, Twitter afin d'interagir avec les partenaires de l'emploi (RESA, Pôle Emploi…)

**13h30-14h :** phase d'inclusion : quiz culture générale sur le numérique par le biais d'un KAHOOT

**14h-16h** : module "Découvrir la digitalisation des métiers et connaître les nouveaux métiers autour du numérique."

- Sous forme de minis groupes : faire rechercher les jeunes sur la place du numérique dans tous les métiers (ex : en quoi un vendeur chez Décathlon doit maîtriser le numérique, une fleuriste, un opérateur sur machine pour les rapports numériques ?)
- Leur proposer des dessins, des vidéos, des posters décrivant des métiers et les faire réfléchir/réagir dessus
- Synthèse des groupes et animation des débats entre participants
- Présentation des métiers spécifiques au numérique : Webmaster, modérateur, community manager

**16h-17h :** Questionnaire final pour évaluation et correction en collectif par le biais d'un *Google Forms* afin d'avoir des éléments statistiques à la fois individuels mais aussi collectifs pour le bilan

**Méthodes et outils de réalisation de l'action**
Phase d'évaluation :
Questionnaire sous la forme d'un Google Forms.
Ce questionnaire permettra de confirmer les acquis des participants sur les thèmes des modules vus durant les deux jours.

Nature de la validation: La formation dispensée sera sanctionnée, à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,
-

# Sensibilisation au RGPD dans ma pratique professionnelle *(réf. RGPD)*

**Objectifs**

- Maîtriser le nouveau cadre sur la règlementation des données personnelles (RGPD) et, notamment, la loi informatique et libertés
- Sécuriser les données personnelles au sein de votre entreprise
- Aménager ses contrats aux nouvelles règles sur les données personnelles
- Appréhender les risques en matière d'atteinte aux données personnelles

***Nombre de jours*** **:** 1 jour (7h)
***Nombre de stagiaires*** **:** 10 à 12
***Outils mis à disposition*** **:**
***Prérequis*** **:**
***Codes des fiches ROME les plus proches*** **:**

**Organisation type**

**1ere demi-journée**

**9h-9h30 :** phase d'inclusion : accueil sous forme de café

- Obligation administrative (émargement, explication de l'action et du mode de financement si fonds européens.)
- Mise en situation professionnelle sous forme d'une vidéo afin de comprendre les enjeux liés à la protection des données personnelles

**9h30-12h30 :** module "information et sensibilisation sur le RGPD"

**Qu'est-ce qu'un traitement des données personnelles ?**

- Visualiser les catégories de données visées dans le cadre de la réglementation
- Faire le point sur les types de traitement des données personnelles

**Quelles sont les obligations du responsable du traitement des données ?**

- Appréhender les notions de loyauté, de proportionnalité et de finalité
- Appréhender le principe de durée de conservation et recours à une autorisation

**Quelles sont les obligations en matière de sécurité et de confidentialité ?**

- Qui est responsable - notion de co-responsabilité
- Contrats avec vos sous-traitants

**Comment transférer des données à l'étranger en toute légalité ?**

- Identifier les pays présentant un niveau de protection adéquat
- Dans quel cas dois-je implémenter des Binding Corporate Rules
- Qu'est-ce que le Privacy Shield ?

**Quelles sont les sanctions en cas d'abus sur le traitement des données personnelles ?**

- Mise au point sur le contrôle, à priori, de la CNIL
- Panorama des voies de recours des personnes concernées
- Panorama des sanctions encourues en cas de plainte

**Dans quel cas un délégué à la protection est requis ?**

- Identifier le rôle et les responsabilités du délégué à la protection. Mettre en place une analyse des risques

**2ème demi-journée**

**13h30-14h :** phase d'inclusion : quiz culture générale sur le RGPD par le biais d'un KAHOOT

**14h-17h** : module "comment intégrer les bonnes pratiques dans ma pratique professionnelle ?"

**Quelles sont les droits des personnes dont les données personnelles sont traitées ?**

- Gérer l'organisation du recueil de consentement (*opt in* et *opt out*, *cookie*, *profilage..)*
- Assimiler les principes de droit d'accès et droit d'opposition
- Comment exercer son droit à l'oubli et au déréférencement ? Assimiler la notion de droit à la portabilité

**Quelles sont les nouvelles formalités à respecter ?**

- Comment intégrer le Privacy by Design ?
- Appréhender le registre des activités
- Gérer la notification des failles de sécurité

**16h30-17h :** phase de déclusion : retour sur la journée et évaluation

**Public cible**

- Salarié en contact avec du public, manipulant des données personnelles.
- Juriste
- Webmaster
- Responsable ou chef d'entreprise

**Méthodes pédagogiques**

- Définition des objectifs et des pratiques des participants
- Courte période magistrale intégrant les problématiques des participants
- Pédagogie interactive à partir de QCM et d'exercices pratiques
- Support de cours formation RGPD - protection des données personnelles

Nature de la validation: La formation dispensée sera sanctionnée, à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,
- Après avis favorable du jury d'évaluation, d'un certificat de compétences précisant la nature de la formation reçue.

# Initiation / perfectionnement en informatique *( réf. IniINFO )*

**Contenu**

Cette formation permettra au stagiaire d'être autonome et plus performant sur son poste de travail.
A l'issue de la formation, le participant sera capable de :

- Comprendre le fonctionnement matériel d'un PC
- Maîtriser l'environnement Windows,
- Gérer ses fichiers et les arborescences,
- Utiliser Internet et sa messagerie.

**Passage de la certification ICDL**

***Nombre de jours*** **:** 4 jours (28h)
***Nombre de stagiaires*** **:** à partir de 6 stagiaires
***Outils mis à disposition*** **:**
***Prérequis*** **:** *sans prérequis*
***Codes des fiches ROME les plus proches*** **:**

**Organisation type**

**Notions sur le matériel**

- Les composants d'un ordinateur (disque dur, processeur, mémoire, etc.)
- Le stockage externe Clé USB, DVD, SSD

**L'environnement Windows**

Le vocabulaire de base
Les unités de mesures en informatique
Allumer/éteindre l'ordinateur proprement
Le bureau, les icônes et les raccourcis, la corbeille
Les barres d'outils de défilement.
Les boîtes de dialogue

**L'arborescence des fichiers et dossiers**

Différence entre un dossier et un fichier
Comprendre une arborescence
Créer, nommer, enregistrer un dossier
Créer, modifier, supprimer une arborescence, les niveaux de l'arborescence
Copier et déplacer des fichiers et des répertoires
Rechercher des fichiers ou des répertoires

**Utiliser l'Internet**

L'Internet, une histoire pas comme les autres
Utilité d'internet au quotidien
Les annuaires et moteurs de recherche
La légalité, les risques légaux et sécuritaires
Notion de taille de fichier et de temps de téléchargement
Reconnaître les formats (xls, doc, zip, jpg, avi, pdf...)

**Notion sur les messageries**

Les différents types de messagerie
Composition d'une adresse de messagerie
Interfaces classiques des messageries
Actions et dossiers de la messagerie
Joindre des fichiers (images, documents...)

**Présentation des outils Office**
**Microsoft Word**

Changer les modes de vue du document : page, plan, normal.
Créer et insérer du texte.
Insérer un caractère spécial, un symbole, une date.
Afficher les caractères cachés du document (espaces, sauts).
Sélectionner une lettre, un mot, un paragraphe, le document entier, une suite de mots, une ligne, un ensemble de lignes.
Écrire le texte (supprimer un mot, une lettre, remplacer une sélection par la frappe).
Rechercher un texte (mot, expression simple).
Copier, déplacer du texte dans le document ou entre documents ouverts (via le Presse-papier).
Naviguer dans le document (page, début, fin) et comprendre la barre d'état (numéro de page, de ligne, langue).
Utiliser les fonctions Annuler et Répéter.
Changer la police, la taille (corps) de la police.
Changer l'apparence d'un texte : gras, italique, souligné.
Insérer un saut de ligne.
Connaître les bonnes pratiques d'alignement des textes (alignement et les tabulations).
Utiliser les alignements, les retraits de paragraphe.
Savoir ajuster l'espacement avant et après, ajuster l'interligne.
Utiliser des puces ou des numéros à une liste, choisir le style des puces

**Microsoft Excel : gérer une base de donnée**

Changer les modes de vue du document : page, plan, normal.
Contenu des cellules.
Copier une cellule (ou une plage de cellules) dans une feuille.
Utiliser la poignée de recopie, connaître les incréments standards.
Déplacer des cellules ou plages de cellules.
Supprimer du contenu ou des formats de cellules.
Mise en forme manuelle et conditionnelle.
Mathématiques, Priorisation des opérations, Rappels sur les pourcentages.
Utilisation des formules
Connaître les bonnes pratiques pour la création de formules
Utiliser les formules simples utilisant des cellules, des opérateurs arithmétiques, parenthèses.
Comprendre les codes erreurs usuels dans les formules erronées : #NOM, #DIV/0, #REF.
Utiliser des fonctions standards simples

**Méthodes pédagogiques**

- Apports théoriques et pratiques
- Réflexions de groupe guidées par l'animateur
- Questionnaires-tests avec autocorrection
- Mises en situation (training) analysées en groupe

**Nature de la validation:** La formation dispensée sera sanctionnée, à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,
- Après avis favorable du jury d'évaluation, d'un certificat de compétences précisant la nature de la formation reçue.

SecNumedu
Formation continue
ANSSI

# Cybersécurité des TPE/PME *(réf. CybPME)*

**Contenu**

La formation a pour objectif d'apporter des connaissances sur l'environnement cyber. Afin de mieux piloter leur entreprise, les dirigeants et salariés se doivent de prendre en considération cet aspect. Il faut aussi connaître les aspects juridiques et assurantiels afin de se prémunir des actes criminels. La question n'est plus de savoir si nous allons subir une attaque, ni même quand nous allons subir, mais bien de connaître les dispositions à prendre pour minimiser ce risque ou son impact.

***Nombre de jours*** **:** 5 jours (35h)
***Nombre de stagiaires*** **:** en fonction de la demande.
***outils mis à disposition*** **:**
***prérequis*** **:** aucun
***Codes des fiches ROME les plus proches*** **:**
**Organisation type**

- **Cybersécurité : notions de bases, enjeux et droit commun**
  - Définitions
  - Les enjeux de la sécurité
  - Formation et défense
  - Savoir repérer ce qu'il faut protéger
  - Juridique et assurances
  - Les relais et garants de la cybersécurité
- **L'hygiène informatique pour les utilisateurs**
  - Le système d'information et ses employés
  - Les actifs essentiels et supports
  - Les préconisations de l'Anssi
  - La gestion des logs
  - La gestion des backup
  - Utiliser son matériel professionnel hors de l'entreprise
- **Gestion et organisation de la cybersécurité**
  - Les institutions et leurs recommandations
  - Les métiers de l'informatique
  - Comment parler cyber suivant son interlocuteur
  - La cybersécurité et la communication
  - Gestion des incidents et réactions
- **Protection de l'innovation et cybersécurité**
  - Protéger son entreprise
  - Droits intellectuels liés à l'entreprise
  - Assurances
  - RGPD

- **Administration sécurisée du système d'information (SI) interne d'une entreprise**
  - Analyse de risques suivant la méthode Ebios & Ebios RM
  - Défense en profondeur
  - Détection d'incident
  - Gestion de crise
  - Résilience
  - Traitement et recyclage

- **La cybersécurité des entreprises ayant externalisé tout ou partie de leur SI**
  - Les différentes formes d'externalisation
  - Les règles à suivre pour évaluer son prestataire
  - Aspects contractuels et garanties

- **Sécurité des sites internet gérés en interne**
  - Les différents types de site
  - Avantages et inconvénients de tout automatiser
  - Sécurité des bases de données numériques et autres
  - Configurer ses serveurs et les services associés
  - Les accès aux utilisateurs et administrateurs

**Public cible**

La formation à la cybersécurité peut toucher un public hétérogène parmi les salariés des entreprises :
- Direction : Dirigeant, Cadre, RSSI
- Opérationnels : DSI, DPO, experts techniques

Tous les salariés représentent des cibles potentielles et doivent donc être formés à de bonnes pratiques cyber.

**Méthodes pédagogiques**

- Cours théorique téléprésentiel
- Etude d'un cas d'actualité
- Mises en situation
- Exercices pratiques : mise en application des concepts préalablement enseignés
- Déroulement de la méthode sur un cas d'étude

**Nature de la validation**: La formation dispensée sera sanctionnée, à son issue, par la remise :
- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,
- Après avis favorable du jury d'évaluation, d'un certificat de compétences précisant la nature de la formation reçue.

# Certified Data Protection Officer (*réf. DPO)*

**Objectifs :** Le cours de formation Certified Data Protection Officer vous permettra de développer les connaissances, aptitudes et compétences nécessaires pour mettre en œuvre et gérer efficacement un cadre de conformité en matière de protection des données personnelles.

**Pré requis** : aucun

**Contenu :**

**Programme de la formation**

**Jour 1 :** Introduction au RGPD et initialisation de la conformité au RGPD
**Jour 2 :** Planifier la mise en œuvre du RGPD
**Jour 3 :** Déployer le RGPD
**Jour 4 :** Suivi et amélioration continue de la conformité au RGPD
**Jour 5 :** Examen de certification

L'examen «PECB Certified Data Protection Officer» répond entièrement aux exigences relatives au programme d'examen et de certification de PECB. L'examen couvre les domaines de compétences suivants:
**Domaine 1 :** Concepts de protection des données et exercice des droits par la personne concernée
**Domaine 2 :** Le responsable du traitement des données, le sous-traitant, et le Délégué à la protection des données
**Domaine 3 :** Planification du projet de conformité RGPD
**Domaine 4 :** Analyse d'impact relative à la protection des données et étude d'impact sur la vie privée
**Domaine 5 :** Mesures et approches de la protection des données
**Domaine 6 :** Évaluation des performances, suivi et mesure du projet de conformité RGPD

**Nature de la validation**: **Certification**
Après avoir réussi l'examen, vous pouvez demander l'une des qualifications mentionnées sur le tableau ci-dessous. Un certificat vous sera délivré si vous remplissez toutes les exigences relatives à la qualification sélectionnée.

**Les exigences de PECB pour les certifications en protection des données sont :**

| Qualification | Examen | Expérience professionnelle | Expérience projet du SM | Autres exigences |
|---|---|---|---|---|
| **PECB Certified Provisional Data Protection Officer** | Examen PECB Certified Data Protection Officer | Aucune | Aucune | Signer le Code de déontologie de PECB |
| **PECB Certified Data Protection Officer** | Examen PECB Certified Data Protection Officer ou équivalent | Cinq années: Deux années d'expérience professionnelle en protection des données | Activités de protection des données: 300 heures au total | Signer le Code de déontologie de PECB |

**Pour être considérées comme valides, ces activités de mise en œuvre doivent suivre les meilleures pratiques de mise en œuvre et inclure les activités suivantes**

1. Rédaction d'un plan de protection des données
2. Initialisation de la mise en œuvre de la protection des données
3. Mise en œuvre d'une politique de protection des données
4. Suivi et gestion de la mise en œuvre de la protection des données
5. Effectuer des mesures relatives à l'amélioration continue

La formation dispensée sera sanctionnée également , à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement

# ISO 27001 Lead Implementer (réf. ISO01)

**Objectifs :** La norme internationale de maîtrise du risque ISO/CEI 27001 liée à la sécurité de l'information décrit, sous forme d'exigences, les bonnes pratiques à mettre en place pour qu'une organisation puisse maîtriser efficacement les risques liés à l'information. Ce module vous présentera dans un premier temps l'ensemble des normes ISO traitant de la sécurité du système d'information puis vous apportera les éléments nécessaires pour mettre en place un système de management (SMSI) du risque de la sécurité de l'information.

**Contenu**

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.

***Nombre de jours*** **:** 5 jours (35h)
***Nombre de stagiaires*** **:** en fonction de la demande
***Outils mis à disposition*** **:**
***Prérequis*** **:** 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.)
***Codes des fiches ROME les plus proches*** **:**

**Organisation type**

Jour 1 : introduction à la norme ISO/CEI 27001 et initialisation d'un SMSI

- SMSI
- Principes fondamentaux de la sécurité de l'information
- Initialisation de mise en oeuvre du SMSI
- Compréhension de l'organisme et clarification des objectifs de sécurité de l'information
- Analyse du système de management existant

Jour 2 : planification de la mise en œuvre d'un SMSI

- Leadership et approbation du projet SMSI
- Domaine d'application du SMSI
- Politiques de sécurité de l'information
- Evaluation du risque
- Déclaration d'applicabilité et autorisation par la direction de mise en oeuvre du SMSI
- Définition de la structure organisationnelle de la sécurité de l'information

Jour 3 : mise en œuvre d'un SMSI

- Conception des mesures de sécurité et rédaction des procédures et des politiques spécifiques
- Mise en oeuvre des mesures de sécurité
- Définition du processus de gestion de la documentation
- Plan de communication

- Plan de formation et de sensibilisation
- Gestion des opérations
- Gestion des incidents

Jour 4 : surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI

- Surveillance, mesure, analyse et évaluation
- Audit interne
- Revue de direction
- Traitement des problèmes et des non-conformités
- Amélioration continue
- Préparation à l'audit de certification
- Compétence et évaluation d'un implémenteur

Jour 5 : examen de certification

- Révisions
- Questions/réponses
- Passage de l'examen

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 dissertation pendant une durée de 3 heures a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification ISO 27001 Lead Implementer après validation de l'expérience professionnelle du stagiaire auprès de l'organisme de certification.

**Public cible**

Personne souhaitant découvrir, comprendre ou mettre en pratique l'ISO 27001. RSSI, consultants en sécurité, y compris ceux connaissant d'autres méthodes comme ISO 27005 ou EBIOS 2010/RM.

**Méthodes pédagogiques**

- 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.
- 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

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

**Nature de la validation:**

La formation dispensée sera sanctionnée, à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,
- Après avis favorable du jury d'évaluation, d'un certificat de compétences

# ISO 27005 Risk Manager (réf. ISO05)

**Objectifs :** Cette formation, basée en partie sur la norme ISO/CEI 27005, permet aux participants d'acquérir les bases théoriques et pratiques de la gestion des risques liés à la sécurité de l'information. Elle prépare efficacement les candidats à la certification ISO 27005 Risk Manager à partir d'études de cas. Vous verrez également comment mettre en place la méthode EBIOS afin de pouvoir apprécier et traiter les risques relatifs à la sécurité des SI. Cette nouvelle méthode combine une démarche de 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.

**Contenu**

Comprendre le concept de risque lié à la sécurité de l'information, utiliser l'ISO 27005 pour l'analyse de risques, connaître d'autres méthodes (EBIOS, MEHARI), faire un choix rationnel de méthode d'analyse de risques. Fournir aux participants l'ensemble des éléments pour pouvoir, par la suite être autonome dans la réalisation d'une analyse des risques selon l'ISO 27005 avec la méthode EBIOS RM. Présenter le vocabulaire et les différents ateliers qui composent la méthode.

***Nombre de jours* :** 3 jours (21h)
***Nombre de stagiaires* :** en fonction de la demande
***outils mis à disposition* :**
***Prérequis* :** 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.)
***Codes des fiches ROME les plus proches* :**

**Organisation type**

Jour 1 : introduction à la norme ISO/CEI 27005 et mise en oeuvre d'un programme de gestion des risques

- Cadre normatif et réglementaire
- Concepts et définition des risques
- Programme de gestion des risques
- Etablissement du contexte

Jour 2 : planification de la mise en œuvre d'un SMSI

- Identification du risque
- Analyse du risque
- Evaluation du risque
- Appréciation des risques avec une méthode quantitative
- Traitement du risque
- Acceptation du risque en sécurité de l'information

Jour 3 : mise en œuvre d'un SMSI

- Communication et consultation sur les risques liés à la sécurité de l'information
- Suivi et examen des risques liés à la sécurité de l'information
- Méthodes OCTAVE
- Méthode MEHARI
- Méthodes EBIOS
- Méthodologie harmonisée d'évaluation des menaces et des risques (TRA)
- Examen

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 dissertation pendant une durée de 3 heures a lieu durant la dernière après-midi de formation. La réussite à l'examen donne droit à la certification ISO 27005 Risk Manager après validation de l'expérience professionnelle du stagiaire auprès de l'organisme de certification.

**Public cible**

RSSI ou correspondants Sécurité, architectes de sécurité, directeurs ou responsables informatiques, ingénieurs, chefs de projets (MOE, MOA) devant intégrer des exigences de sécurité.

**Méthodes pédagogiques**

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
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

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

**Nature de la validation:** La formation dispensée sera sanctionnée, à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,
- Après avis favorable du jury d'évaluation, d'un certificat de compétences précisant la nature de la formation reçue.

# EBIOS Risk Manager 2018 (réf. ERM18)

**Objectifs :** EBIOS RM ou EBIOS Risk Manager est une méthode de gestion des risques conçue par l'ANSSI et publiée en octobre 2018. Cette nouvelle méthode combine une démarche de 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.

**Contenu :**

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 Risk Manager 2018. Présenter le vocabulaire et les différents ateliers qui composent la méthode.

***Nombre de jours* :** 2,5 jours (17h)
***Nombre de stagiaires* :** en fonction de la demande
***outils mis à disposition* :**
***Prérequis* :** 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.)
***Codes des fiches ROME les plus proches* :**

**Organisation type**

Les bases de la gestion de risques
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

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.

**Public cible**

Personne souhaitant découvrir, comprendre ou mettre en pratique la méthode EBIOS 2018, RSSI, consultants en sécurité, y compris ceux connaissant d'autres méthodes comme ISO 27005 ou EBIOS 2010

**Méthodes pédagogiques**
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
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

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

**Nature de la validation:** La formation dispensée sera sanctionnée, à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,
- Après avis favorable du jury d'évaluation, d'un certificat de compétences précisant la nature de la formation reçue.

# Certified Ethical Hacker *(réf. CEH)*

**Contenu**

- Réussir la certification CEH Certified Ethical Hacker et devenir Certifié CEH
- Maîtriser une méthodologie de piratage éthique
- Découvrir comment scanner, tester et hacker son propre système
- Comprendre comment fonctionne la défense périmétrique
- Acquérir les privilèges et les actions mises en oeuvre pour sécuriser un système
- Comprendre les tests d'intrusions ou les situation de piratage éthique
- Détecter les intrusions
- Mettre en place une politique de création de : ingénierie sociale, gestion des incidents et interprétation des logs
- Avoir des compétences d'auditeur technique en sécurité informatique
- Préparer, réviser et acquérir les trucs et astuces pour réussir l'examen officiel CEH Certified Ethical Hacker

***Nombre de jours*** **:** 5 jours (35h)
***Nombre de stagiaires*** **:** minimum 2 personnes
***Outils mis à disposition*** **:**
***Prérequis*** **:** Connaissance basique de TCP/ IP, Linux et Windows Server
***Codes des fiches ROME les plus proches*** **:** *M1802 - Expertise et support en systèmes d'information*
*M1801 - Administration de systèmes d'information*

**Public cible**

- Responsables sécurité
- Auditeurs
- Professionnels de la sécurité
- Administrateurs de site
- Toute personne concernée par la stabilité des systèmes d'information

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

**Nature de la validation**: La formation dispensée sera sanctionnée, à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,
- Après avis favorable du jury d'évaluation, d'un certificat de compétences précisant la nature de la formation reçue.

# E-CATALYST

## PRÉVENTION SANTÉ SÉCURITÉ

**Protéger ses salariés c'est garantir à l'entreprise sa force et ses valeurs.**

Chez nous, sécuriser l'entreprise c'est préserver certes ses hardware et ses données, mais avant tout ses équipes.

Ecoute, réactivité et proximité sont dans notre ADN.

**CONTACTEZ-NOUS**

Laurence OURDOUILLIE
Responsable Prévention/Santé/Sécurité
06.61.82.88.37 laurence.ourdouillie@e-catalyst.fr
www.e-catalyst.fr

e-catalyst — Carsat Hauts-de-France — INRS

numéro d'habilitation
1487076/2020/SST-01/O/04

# Sauveteur Secouriste du Travail: Formation Initiale

**(réf. SST)**

**Objectifs**

Le SST, sauveteur secouriste du travail, sera capable :

- D'identifier les situations dangereuses au sein de l'entreprise
- De proposer des mesures de prévention
- D'intervenir efficacement sur un accident du travail
- D'alerter les secours compétents

***Nombre de jours*** **:** *2* jours (14h)
***Nombre de stagiaires*** **:** 4 à 10
***Outils mis à disposition*** **:**
***Prérequis*** **:** aucun
**Organisation type**

**Séquence 1 : démarche globale de la prévention**
Objectif : situer le rôle du Sauveteur Secouriste du Travail dans la santé, la sécurité au travail / cadre juridique
Etre capable de définir le rôle du Sauveteur Secouriste du Travail dans l'organisation de la prévention dans l'entreprise (le SST est
acteur de la prévention) :
- Situer son rôle de SST dans l'organisation des secours dans l'entreprise
- Situer son rôle de SST dans l'organisation de la prévention de l'entreprise
- Caractériser les risques professionnels dans une situation de travail
- Participer à la maîtrise des risques professionnels par des actions de prévention

**Séquence 2 : protéger**
Objectif : Etre capable de réaliser une protection adaptée (première action du SST)
Protéger de façon adaptée :
- Connaître l'alerte aux populations
- Reconnaître sans s'exposer soi-même, les dangers persistants éventuels qui menacent la victime et/ou son environnement
- Supprimer ou isoler le danger, ou soustraire la victime au danger sans s'exposer soi-même

**Séquence 3 : examiner**
Objectif : Etre capable de collecter les informations en examinant la victime, afin de choisir les actions à mettre en oeuvre
- Examiner la ou les victimes avant et pour la mise en oeuvre de l'action choisie en vue du résultat à obtenir

**Séquence 4 : alerter ou faire alerter**
Objectif : Etre capable de transmettre correctement les informations nécessaires à une intervention efficace
- Garantir une alerte favorisant l'arrivée de secours adaptés au plus près de la victime

**Séquence 5 : secourir**
- Victime saigne abondamment : Objectif à atteindre : arrêter le saignement
- Victime s'étouffe : Objectif à atteindre : lui permettre de respirer
- Victime se plaint d'un malaise : Objectif à atteindre : éviter l'aggravation et prendre un avis médical
- Victime se plaint de brûlures : Objectif à atteindre : éviter l'aggravation de la brûlure
- Victime se plaint de douleur empêchant certains mouvements : Objectif à atteindre : éviter l'aggravation du traumatisme supposé
- Victime se plaint d'une plaie qui ne saigne pas abondamment : Objectif à atteindre : éviter l'aggravation de la plaie
- Victime ne répond pas, mais elle respire : Objectif à atteindre : lui permettre de continuer à respirer
- Victime ne répond pas, elle ne respire pas : Objectif à atteindre : assurer une respiration et une circulation artificielles

**Séquence 6 : épreuves certificatives**

Les critères d'évaluation utilisés sont ceux définis par l'INRS, l'outil utilisé est la grille d'évaluation nationale (document INRS version
03/2020). La validation s'obtient lorsque les indicateurs incontournables référencés sont acquis.
Epreuve 1 : pour la validation des compétences C2-C3-C4-C5
Lors d'un accident de travail simulé, le stagiaire devra montrer ses capacités à mettre en oeuvre l'ensemble de ses compétences
pour intervenir efficacement.
Epreuve 2 : pour la validation des compétences C1-C6-C7-C8
Connaissance du cadre réglementaire de l'activité SST et compétences en matière de prévention

**Méthodes pédagogiques**

- Outils pédagogiques du formateur :
- - Support de l'entreprise (exemple organigramme)
- - Le plan d'intervention + les pictogrammes de l'INRS
- - Le PAP SST + les pictogrammes de l'INRS
- - Les supports Tuto Prév de l'INRS ( ED4439 / ED4461/ ED4463/ ED4464/ ED4337/ ED4455)
- - 3 mannequins de formation (adulte, enfant, nourrisson)
- - Un défibrillateur de formation
- - Une mallette de maquillage, fausses plaies (brûlures), flaque de sang, outils en plastique, gants, garrot, coussin
- hémostatique, compresses, couverture de survie…, pour la réalisation des cas concrets et des ateliers d'apprentissage

**Nature de la validation**:
La formation est certifiée selon les critères d'évaluation définis par l'INRS.
Elle comporte une évaluation réalisée tout au long de la formation et une certification finale.
Les critères d'évaluation utilisés pour cette validation sont ceux définis par l'INRS dans le référentiel de certification des SST et
transcrits dans une grille de certification individuelle (documents INRS).
A l'issue de cette évaluation certificative, un certificat de Sauveteur Secouriste du Travail sera délivré au candidat et sera valable 24
mois.
Les candidats n'ayant pas suivi l'intégralité de la formation ne pourront être admis et obtenir leur certificat.
Une session de rattrapage est envisageable (dans les 6 mois suivant la 1 ère session), suivant les modalités du document de référence
SST (V7-01/2020) pour un candidat n'ayant pas validé la totalité des compétences demandées.

**CLÔTURE DE LA FORMATION**
Evaluation à chaud (qualité globale de la formation / atteinte des objectifs / impact)
Tour de table et retour des stagiaires
Remise à chaque stagiaire :
- attestation individuelle de fin de formation
- aide-mémoire SST (Edition INRS ED 4085)
- autocollant SST
- couverture de survie et masque d'insufflation

# Sauveteur Secouriste du Travail: MAC (réf. MACSST)

**PUBLIC CIBLE :** Tout Sauveteur Secouriste du Travail

**NOMBRE DE STAGIAIRES PAR SESSION :** Minimum 4 et maximum 10 stagiaires par session

**PRÉ-REQUIS :** Être titulaire du certificat de Sauveteur Secouriste du Travail en cours de validité
Les titulaires d'un certificat APS (Acteur Prévention Secours)

**ORGANISATION / MODALITES DE DEROULEMENT DES FORMATIONS**
En entreprise ou dans les locaux de l'Organisme de Formation
Formation en groupe (en présentiel), dans une salle équipée (PC portable, vidéoprojecteur, paperboard)

**DURÉE DE LA FORMATION:** 7 heures (soit 1 jour)

**OBJECTIFS DE LA FORMATION**
Maintenir et actualiser ses compétences de Sauveteur Secouriste du Travail définies dans le dernier référentiel national de l'INRS, afin de prolonger la validité du certificat SST.
Intervenir efficacement face à une situation d'accident du travail.
Mettre en application, dans le respect de l'organisation de l'entreprise et des procédures spécifiques, ses compétences en matière de prévention, au profit de la santé et de la sécurité au travail.

**MODALITÉS D'ANIMATION**
***Outils pédagogiques du formateur :***
- Support de l'entreprise (exemple organigramme)
- Le plan d'intervention + les pictogrammes de l'INRS
- Le PAP SST + les pictogrammes de l'INRS
- Supports TutoPrév de l'INRS (ED4439/ED4461/ED4463/ED4464/ED4337/ED4455)
- 3 mannequins de formation (adulte, enfant, nourrisson)
- Un défibrillateur de formation
- Une mallette de maquillage, fausses plaies (brûlures), flaque de sang, outils en plastique, gants, garrot, coussin hémostatique, compresses, couverture de survie..., pour la réalisation des cas concrets et des ateliers d'apprentissage

***Ressources du formateur :***
- document de référence (V7-01/2020)
- guide des données techniques et conduites à tenir (V3.06/2019)
- aides mémoire SST (édition INRS ED 4085)

***Dossier du formateur :***
- grilles de certification des compétences (MAC) de l'INRS
- fiches de suivi individuel de l'OF
- feuille collective d'émargement de l'OF
- attestation individuelle de fin de formation de l'OF

**ENCADREMENT**
Les formations sont dispensées par des formateurs certifiés par le réseau Assurance maladie risques professionnels / INRS et rattachés à un organisme de formation habilité par ce même réseau.

**CONTENU DE LA FORMATION**
***Séquence 1 : démarche globale de la prévention***
Objectif : situer le rôle du Sauveteur Secouriste du Travail dans la santé, la sécurité au travail / cadre juridique
Etre capable de définir le rôle du Sauveteur Secouriste du Travail dans l'organisation de la prévention dans l'entreprise (le SST est acteur de la prévention) :
- Situer son rôle de SST dans l'organisation des secours dans l'entreprise
- Situer son rôle de SST dans l'organisation de la prévention de l'entreprise
- Caractériser les risques professionnels dans une situation de travail
- Participer à la maîtrise des risques professionnels par des actions de prévention

***Séquence 2 : protéger***

Objectif :

- Etre capable de réaliser une protection adaptée (première action du SST)

Protéger de façon adaptée :

- Connaître l'alerte aux populations
- Reconnaître sans s'exposer soi-même, les dangers persistants éventuels qui menacent la victime et/ou son environnement
- Supprimer ou isoler le danger, ou soustraire la victime au danger sans s'exposer soi-même

***Séquence 3 : examiner***

Objectif :

- Etre capable de collecter les informations en examinant la victime, afin de choisir les actions à mettre en œuvre
- Examiner la ou les victimes avant et pour la mise en œuvre de l'action choisie en vue du résultat à obtenir

***Séquence 4 : alerter ou faire alerter***

Objectif :

- Etre capable de transmettre correctement les informations nécessaires à une intervention efficace
- Garantir une alerte favorisant l'arrivée de secours adaptés au plus près de la victime

***Séquence 5 : secourir***

- Victime saigne abondamment. Objectif à atteindre : arrêter le saignement
- Victime s'étouffe. Objectif à atteindre : lui permettre de respirer
- Victime se plaint d'un malaise. Objectif à atteindre : éviter l'aggravation et prendre un avis médical
- Victime se plaint de brûlures. Objectif à atteindre : éviter l'aggravation de la brûlure
- Victime se plaint de douleur empêchant certains mouvements. Objectif à atteindre : éviter l'aggravation du traumatisme supposé
- Victime se plaint d'une plaie qui ne saigne pas abondamment. Objectif à atteindre : éviter l'aggravation de la plaie
- Victime ne répond pas, mais elle respire. Objectif à atteindre : lui permettre de continuer à respirer
- Victime ne répond pas, elle ne respire pas. Objectif à atteindre : assurer une respiration et une circulation artificielles

***Séquence 6 : épreuves certificatives***

Les critères d'évaluation utilisés sont ceux définis par l'INRS, l'outil utilisé est la grille d'évaluation nationale (document INRS version mars 2020). La validation s'obtient lorsque les indicateurs incontournables référencés sont acquis.
Epreuve 1 : pour la validation des compétences C2-C3-C4-C5
Lors d'un accident de travail simulé, le stagiaire devra montrer ses compétences pour intervenir efficacement face à la situation proposée.
Epreuve 2 : pour la validation des compétences C6-C7-C8
Validation des compétences en matière de prévention

## MODALITES D'EVALUATION

La formation est certifiée selon les critères d'évaluation définis par l'INRS.

Elle comporte une évaluation réalisée tout au long de la formation et une certification finale.
Les critères d'évaluation utilisés pour cette validation sont ceux définis par l'INRS dans le référentiel de certification des SST et transcrits dans une grille de certification individuelle (documents INRS).
A l'issue de cette évaluation certificative, un nouveau certificat de Sauveteur Secouriste du Travail sera délivré au candidat et sera valable 24 mois.
Les candidats n'ayant pas suivi l'intégralité de la formation et/ou non aptes à mettre en œuvre l'ensemble des compétences attendues du SST, ne pourront obtenir le renouvellement de leur certificat.
Dans le cas où ce maintien-actualisation des compétences ferait défaut, le SST perd sa « certification de Sauveteur Secouriste du Travail » à la date de fin de validité de sa carte de SST. A partir de cette date, il n'est plus autorisé à exercer en tant que SST, mais il conservera son obligation d'intervenir pour porter secours à une personne en danger (art 223-6 du code pénal).
Afin d'être de nouveau certifié SST, il devra valider ses compétences lors d'une nouvelle session de MAC.

## CLÔTURE DE LA FORMATION

Evaluation à chaud (qualité globale de la formation / atteinte des objectifs / impact)
Tour de table et retour des stagiaires
Remise à chaque stagiaire :

- attestation individuelle de fin de formation
- aide-mémoire SST (édition INRS ED 4085)

- autocollant SST

# Sécurité Incendie (Réf : SécInc)

**Objectifs :** Répondre à la législation du code du travail (articles R4227-28 / R4227-39) imposant la formation du personnel à la sécurité incendie
**Montée en compétences de salariés par le biais de nos formations personnalisées et adaptées à votre environnement et à vos besoins.**

**Contenu :**
**1 / FORMATION EPI (équipier de première intervention) / MANIPULATION EXTINCTEURS**

**Module théorique :**
- Règles de prévention
- Les causes d'incendie
- L'organisation de la lutte contre l'incendie et les principes d'évacuation
- Les différents types d'extincteurs et les agents extincteurs

**Module pratique :**
- Exercice de manipulation d'extincteurs (eau pulvérisée et CO2) sur feu réel (bacs à flammes)

**Durée :** 2h30 (peut varier en fonction du nombre de stagiaires)
**Public visé :** Ensemble du personnel de l'entreprise
**Validation de la formation :** elle donnera lieu à la remise d'une attestation de présence

**2 / FORMATION GF&SF (guide file & serre file) / Exercices d'évacuation**

**Module théorique :**
- Règles de prévention
- Les causes d'incendie et propagation du feu
- L'organisation de la lutte contre l'incendie et les principes d'évacuation
- Comportement des personnes en cas de situation de danger
- Fonction des GF&SF

**Module pratique :**
- Application des consignes de sécurité
- Déclenchement d'un boîtier manuel
- Réalisation d'un exercice d'évacuation (tour du site et des organes de sécurité)

**Durée :** une demi-journée (peut varier en fonction du nombre de stagiaires)
**Public visé :** Ensemble du personnel de l'entreprise
**Validation de la formation :** elle donnera lieu à la remise d'une attestation de présence

**Modalité du déroulement des formations :**
- Autoriser les déplacements sur le site pour la réalisation de l'exercice d'évacuation
- Remise d'une fiche d'observation sur demande de la direction

<u>Nature de la validation</u>: La formation dispensée sera sanctionnée, à son issue, par la remise :
- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,

# Habilitation Électrique BE manœuvre / BS / BR (Ref : HE-BO/BS/BR)

**Habilitation BE manœuvre / BS**

La formation aux habilitations BE manœuvre / BS s'adresse au personnel non électricien devant effectuer des opérations d'ordre électrique élémentaires (BS) ou manœuvrer de l'appareillage électrique en basse tension (BE manœuvre).

**RÉGLEMENTATION :**
L'employeur est dans l'obligation de remettre une habilitation électrique à tout son personnel non électricien devant intervenir à proximité d'une installation électrique.

**OBJECTIFS :**
Savoir exécuter des travaux de remplacement, de raccordement et de manœuvres simples, en toute sécurité.
Permettre à l'employeur de délivrer les titres d'habilitation.

**DURÉE** :
Formation initiale : 1 journée
Recyclage : 4 heures / Pré-requis : Etre titulaire d'un titre d'habilitation en limite de validité, à présenter au formateur en début de stage.

**CONTENU::**
- La réglementation et les habilitations
- Notions élémentaires d'électricité
- Sensibilisation aux risques électriques
- Prévention des risques électriques
- Opérations dans l'environnement
- Appareillage électrique (BT/HT)
- Travailler en toute sécurité
- Application lors des travaux électriques
- Evaluation des connaissances

**MÉTHODE PÉDAGOGIQUE :**
Apports théoriques et exercices pratiques

**EVALUATION DE LA FORMATION :**
Les stagiaires seront évalués avec un questionnaire écrit, sur les acquis théoriques et pratiques.
A l'issue de l'évaluation des acquis un titre pré-rédigé sera remis à l'employeur, qui délivrera au salarié un titre d'habilitation électrique.
**RECYCLAGE :**
Le recyclage est obligatoire, la durée de validité recommandée selon la norme NF C 18-510 est de 3 ans.
Au cours de la période triennale, l'employeur peut suspendre ou supprimer l'habilitation électrique.

*Ce que dit la loi à propos de l'habilitation électrique*
*Article R4544-10*
*Un travailleur est habilité dans les limites des attributions qui lui sont confiées.*
*L'habilitation, délivrée par l'employeur, spécifie la nature des opérations qu'il est autorisé à effectuer. Avant de délivrer l'habilitation, l'employeur s'assure que le travailleur a reçu la formation théorique et pratique qui lui confère la connaissance des risques liés à l'électricité et des mesures à prendre pour intervenir en sécurité lors de l'exécution des opérations qui lui sont confiées. L'employeur délivre, maintient ou renouvelle l'habilitation selon les modalités contenues dans les normes mentionnées à l'article R. 4544-3.*
*Norme NF C18-510*
*Tous les personnels, qui dans le cadre de leur travail ont accès ou s'approchent des installations électriques, doivent bénéficier d'une formation adaptée aux tâches confiées et leur environnement. Cette formation est destinée à leur faire connaître les dangers de l'électricité ainsi qu'à leur apprendre à s'en prémunir. Les électriciens sont bien sûr les premiers concernés, mais aussi tous ceux que leur travail amène à côtoyer de près les installations électriques.*

## 2) Habilitation BR

Le personnel d'intervention BR assure des prestations de dépannage, de connexion électrique, d'essais et de mesurages sur un réseau électrique de basse tension. Et doit présenter à son employeur une attestation prouvant sa formation habilitation électrique BR.

**OBJECTIFS :**
-Permettre aux électriciens de mettre en application les prescriptions de sécurité de la publication UTE C 18-510 lors des opérations relatives à la consignation sur les ouvrages électriques BT.
-S'assurer de leur aptitude à adapter ces prescriptions dans les domaines et les situations propres à leurs établissements.
-Obtenir l'habilitation électrique BR
**PUBLIC CONCERNÉ:**
Personnel électricien appelé à intervenir sur des ouvrages électriques, pour réaliser des interventions d'entretien et/ou de dépannage d'ordre électrique

**DURÉE :** 3 jours (peut varier selon le nombre de stagiaires)

**CONTENUS :**
Apports théoriques et ateliers pratiques (exercices)

**PROGRAMME :**
***Connaissances générales :***
Les zones d'environnement / les effets du courant / les symboles d'habilitations / la mise en sécurité d'un circuit / le matériel / les EPI / la conduite à tenir en cas d'accident
***Travaux d'ordre électrique :***
L'identification des ouvrages BT / les fonctions des matériels électriques BT / les mesures de prévention / les niveaux d'habilitation nécessaires / les différentes consignations / l'analyse des risques / la préparation des travaux / les travaux hors tension / les respect des consignes du chargé d'exploitation et instructions de sécurité / la rédaction des documents
***Entretien et dépannage :***
Les risques spécifiques aux interventions BT / les mesures de prévention / la préparation d'intervention / les différentes interventions / la consignation / les consignes et instructions de sécurité
***Exercices pratiques :***
Repérage des environnements / analyse préalable d'une intervention / préparation des EPI et consignes de sécurité / le balisage de la zone de travaux / la réalisations de connexions et de déconnexions / la pose d'une nappe et d'un EPC / la rédaction des documents et compte rendu de son activité.
**EVALUATION :**
L'évaluation des acquis théoriques et pratiques selon le référentiel et les modalités d'évaluation de la norme NF C 18-510 est réalisés en fin de formation en vue de la remise d'un titre pré-rédigé à l'employeur, qui remettra le titre d'habilitation électrique au salarié.

**RECYCLAGE :**
Le renouvellement de l'habilitation électrique est obligatoire avec une périodicité recommandée de 3 ans.
L'objectif du recyclage est de mettre à jour la pratique pour réaliser en toute sécurité les travaux et interventions sur les installations électriques.
Durée de la formation : 1,5 jours

La formation dispensée sera sanctionnée, à son issue, par la remise :
- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,

# Gestes et Postures (réf. GesPos)

**Module 1 : Prévention des Risques & Gestes et postures**

**Public concerné** :

Responsable de service, chef de groupe, responsable de chantier, manager…, toute personne ayant sous sa responsabilité des collaborateurs astreints à des manutentions manuelles ou/et opérations répétitives

**Durée** : 1 journée

**Objectif** :

Etre capable d'appliquer les connaissances acquises pour prévenir des accidents et maladies professionnelles dans l'entreprise

**Programme** :

**Module théorique :**

- La démarche globale de la Prévention
- Découvrir les bases de l'anatomie pour mieux comprendre les problèmes de santé liés aux gestes et postures
- Méthode d'analyse de postes, de situations de travail (manutention/ bureautique)
- Vous avez dit TMS (Troubles Musculo-Squelettiques) ?

**Module pratique** :

- Exercices de soulagement articulaire et musculaire

Cette formation est sanctionnée par une attestation individuelle de fin de formation

**Module 2 : Gestes et Postures**

**Public concerné** :

Tout salarié astreint à des manutentions manuelles ou/et opérations répétitives

**Durée** : une demi-journée

- Découvrir les bases de l'anatomie pour mieux comprendre les problèmes de santé liés aux gestes et postures
- Vous avez dit TMS (Troubles Musculo-Squelettiques) ?
- Identifier les risques liés aux postures de travail
- Exercices de soulagement articulaire et musculaire

**Nature de la validation**: La formation dispensée sera sanctionnée, à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,

# Chaîne de survie (réf. ChainS)
# ALERTER / MASSER / DÉFIBRILLER

**Objectif visé**

Identifier les signes permettant de reconnaître un arrêt cardiaque

Réaliser les gestes permettant d'augmenter les chances de survie d'une victime

**Durée**

Une demi-journée (peut varier en fonction du nombre de stagiaires)

**Déroulement de la formation**

En présentiel, un groupe de 10 stagiaires maximum

**Méthodologie**

Alternance de théorie et d'exercices pratiques avec mannequins et défibrillateur de formation

**Programme :**

Pratiquer l'examen d'une victime

Alerter ou faire alerter les secours

Savoir réaliser une réanimation cardio-pulmonaire (RCP)

Savoir utiliser un défibrillateur

**Nature de la validation**:

La formation dispensée sera sanctionnée, à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,


TAKE-OFF
L'école 100 % numérique !
Apprenez de chez vous un métier digital avec un formateur à distance !
Financement possible par CPF, OPCO, Pôle Emploi ou tous les autres types de financement.
CONTACTEZ-NOUS
Téléphone : 09 72 17 65 25
07 85 88 71 33
E-mail : contact@take-off.tech
Site : www.take-off.tech/
Facebook : @TakeOfficiel
Instagram : @takeoff_officiel

# Certification Délégué à la protection des données (réf. CDPD)


*Conforme à l'annexe de la Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données*

***Objectif :*** *maîtriser les compétences du DPD qui a pour mission d'assurer une veille et un conseil interne auprès de l'employeur sur les obligations de protection des données personnelles. Il est également le référent de la CNIL.*

*3.5 mois = 525h*
*Principaux domaines couverts:*

- *Organisation des entreprises et collectivités.*
- *Juridique*
- *Gestion des risques*
- *Sécurisation du SI*
- *Pilotage de projet*
- *Connaissances des outils et de l'environnement de travail*

***Certification PECB CDPO et PCIE : Sécurité des TIC, MS Project, Présentation***

**En terme de pratique professionnelle :**

- Le stagiaire devra avoir au minimum 2 ans d'expérience professionnelle pour prétendre passer la certification
- La formation laisse une place prépondérante à la pratique puis très rapidement à des mise en situations professionnelles

# Certification délégué à la protection des données

## MODULE 1 : Bases techniques (*réf. CDPD1)*

### Contenu

**Socle de base des connaissances de la vie privée**

1. Introduction :
    a. premières définitions de la vie privée
    b. un peu d'histoire
    c. Les réglementations sur les données personnelles dans le monde (CCPA, LGPD, KvKK, PDPA …)
2. Le Règlement Général sur la Protection des données.
3. Le Délégué à la protection des données.
4. Cadre réglementaire.
5. Principes fondamentaux de la protection des renseignements personnels.
6. Législation : cadre juridique, consentement, catégories spéciales des données personnelles.
7. Le Contrôleur européen de la protection des données (CEPD) , groupe Berlin , Groupe article "29"

**L'organisation des entreprises**

1. La notion d'organisation
2. Les types d'organisations : pyramidale, cellulaire. personnalisée, cellulaire.
3. Mode d'emploi des organisations
4. Les leviers d'actions
    - Structuration RH
    - Les outils de pilotage
    - Les indicateurs
    - Les responsabilités (Chief Compliance Officer, les responsables de la conformité aux réglementations d'autres domaines (ISO, sapin 2 et?))
    - la communication interne
    - Stratégie et plan d'actions
    - le management

**Socle de base des connaissances Techniques :**

1. Les fondamentaux : évolutions techniques et technologiques impactant la vie privée
2. Bases techniques
3. Focus sur la Biométrie
4. Applications pratiques

**NTIC : définitions et impacts :**

1. Définitions
2. Les Réseaux Sociaux
3. Cybermarketing
4. Traces numériques
5. Profiling
6. Archivage électronique
7. Le vote électronique

**Sécurité des données personnelles :**

8. Approche par les risques
9. Sécurité des données personnelles
10. Sécurité : retours d'expériences
11. Notification des violations aux traitements de données à caractère personnel
12. Anonymisation de données personnelles
13. Forens

***Nombre de jours*** **:** 10 jours (70h)
***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.
***Outils mis à disposition*** **:** PC , casque avec micro, clavier et souris, logiciels métiers
***Prérequis*** **:** au minimum 2 ans d'expérience professionnelle pour prétendre passer la certification
***Codes des fiches ROME les plus proches*** **:** *K1903 - Défense et conseil juridique*

### Public cible

- aux responsables, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser.

### Méthodes pédagogiques

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours
- Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# CERTIFICATION DÉLÉGUÉ À LA PROTECTION DES DONNÉES

## MODULE 1 : Bases juridiques (*réf. CDPD1)*

### Contenu

**Introduction aux règles de Droit :**

**Définitions, sources et preuves**

1. Méthodologie juridique générale
2. Définition et caractères du droit objectif
3. Les sources du droit objectif
4. La preuve des droits subjectifs
5. L'organisation judiciaire et le règlement des conflits

**Les personnes physiques civiles et commerçantes**

1. La personnalité juridique - Les personnes juridiques
2. Les principes généraux du droit commercial français
3. Les activités civiles.

**Introduction au droit, européen et international :**

1. Définitions
2. La vision Européenne du Règlement général sur la protection des données
3. La certification (Art 42) et le programme EuroPrivacy
4. Art 27. du RGPD

**Cadre légal du métier de DPD :**

**«Informatique et libertés » :**

1. Genèse de la loi Informatique et Libertés, fondements philosophiques
2. Historique et perspectives "informatique et libertés" en France, en Europe et dans le monde
3. La loi Informatique et Libertés – lecture du droit et cas pratiques
4. Autres textes (Code du travail, LCEN, Hadopi, Loppsi, Santé Publique, loi CADA, Archives…)

**La protection des données personnelles : enjeux et risques**

1. La CNIL
2. Droits des personnes
3. La base légale et juridique
4. La gouvernance du projet
5. Le Responsable de traitement

i. Les spécificités par secteur d'activité,
ii. L'écosystème juridique du DPD

6. Identification du Responsable de traitement, des responsables conjoints et des sous-traitants
7. Le travail en mode collaboratif
8. La gestion du plan de mise en conformité
9. Le maintien de la conformité
10. Impacts des évolutions légales et juridiques
11. La certification (Art 42 du RGPD)
12. Interaction entre CNIL, Responsable de traitement et CSE (Conseil Social et Économique)
13. L'Archivage des données
14. Echanges de données entre pays de l'UE et hors UE.
15. Cybersurveillance

***Nombre de jours*** **:** 5 jours (35h)
***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.
***Outils mis à disposition*** **:** PC , casque avec micro, clavier et souris, logiciels métiers
***Prérequis*** **:** au minimum 2 ans d'expérience professionnelle pour prétendre passer la certification
***Codes des fiches ROME les plus proches*** **:** *K1903 - Défense et conseil juridique*

**Public cible**

- aux responsables, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# CERTIFICATION DÉLÉGUÉ À LA PROTECTION DES DONNÉES

## MODULE 2 : La gestion des risques (*réf. CDPD2)*

**Contenu**

**1 - Bases de la gestion des risques et de la sécurité de l'information**

1. Gestion des risques : Définitions, analyse, méthodologies et standards, surveillance.
2. Systèmes d'Information et sécurité : fonctions et responsabilités, formation et sensibilisation, classification.
3. Accès, exposition, cryptographie et signatures numériques.
4. Sécurité mobile et la Big Data.
5. Internet des objets : concepts, modèles et principes, applications, menaces.
6. Nouvelles technologies, nouvelles menaces.

**Incidents et protection**

1. Gestion : incident de sécurité de l'information, évènement.
2. Continuité des activités : récupération, temps, stratégie.
3. Évaluation de l'impact sur la protection des données.
4. Cycle de vie des données personnelles.

**2 - Ebios RM**

**introduction à la norme ISO/CEI 27005 et initiation à la mise en oeuvre d'un programme de gestion des risques**

1. Cadre normatif et réglementaire
2. Concepts et définition des risques
3. Programme de gestion des risques
4. Etablissement du contexte

**3- Le PIA**

1. Les textes juridiques encadrant le PIA
2. Les traitements concernés par le PIA
3. Définition du risque sur la vie privée justifiant la conduite d'un PIA
4. La démarche globale de conformité
5. Quels sont les référentiels juridiques et éthiques à prendre en compte ?

**La mise en place d'un PIA**

**méthodologies :**

1. Les points clés des PIA facultatifs, obligatoires ou adossés à des normes de la CNIL
2. La boîte à outils : méthodes, outillage, catalogue de mesures
3. schématiser les risques, menaces et évènements en fonction de la gravité et de la vraisemblance.
4. Le rapport d'analyse de risque PIA

**Mise en opérationnalité du PIA**

1. Les outils pour l'étude des mesures, les études des risques, la validation de l'analyse de risque PIA
2. Les impacts génériques, corporels, matériels, moraux
3. Valider le PIA en évaluant les mesures de nature juridique et les risques résiduels en fonction des risques qui peuvent être acceptés pour
4. Agir sur les impacts, les sources des risques, au niveau transversal de l'organisation

***Nombre de jours*** **:** 10 jours (70h)
***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.
***Outils mis à disposition*** **:**
***Prérequis*** **:** au minimum 2 ans d'expérience professionnelle pour prétendre passer la certification
***Codes des fiches ROME les plus proches*** **:** *K1903 - Défense et conseil juridique*

**Public cible**

- aux responsables, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# CERTIFICATION DÉLÉGUÉ À LA PROTECTION DES DONNÉES

## MODULE 3 : Sécurisation du Système d'information (*réf. CDPD3)*

**Contenu**

**Socles de connaissances :**

**1- Cybersécurité :**

1. Définitions et les enjeux de la sécurité
2. Savoir repérer ce qu'il faut protéger
3. Juridique et assurances
4. Les relais et garants de la cybersécurité

**2 - L'hygiène informatique pour les utilisateurs**

1. Le système d'information et ses employés
2. Les actifs essentiels et supports
3. Les préconisations de l'Anssi
4. La gestion des logs
5. La gestion des backup
6. Utiliser son matériel professionnel hors de l'entreprise

**3- Gestion et organisation de la cybersécurité**

1. Les institutions et leurs recommandations
2. Les métiers de l'informatique
3. Comment parler cyber suivant son interlocuteur
4. La cybersécurité et la communication
5. Gestion des incidents et réactions

**4- Protection de l'innovation et cybersécurité**

1. Protéger son entreprise
2. Droits intellectuels liés à l'entreprise

**5 - Administration sécurisée du système d'information interne d'une entreprise**

1. Analyse de risques ; Ebios & Ebios RM
2. Défense en profondeur
3. Détection d'incident
4. Gestion de crise
5. Résilience
6. Traitement et recyclage

**6- La cybersécurité des entreprises ayant externalisé tout ou partie de leur SI**

1. Les différentes formes d'externalisation
2. Les règles à suivre pour évaluer son prestataire
3. Aspects contractuels et garanties

**7 - Sécurité des sites internet gérés en interne**

1. Les différents types de site
2. Avantages et inconvénients de tout automatiser
3. Sécurité des bases de données numériques et autres
4. Configurer ses serveurs et les services associés
5. Les accès aux utilisateurs et administrateurs

**Système de Management de la Sécurité de l'Information (27001)**

**1 - Initialisation d'un SMSI et norme ISO/CEI 27001**

1. Définition et principes fondamentaux
2. Initialisation de mise en oeuvre du SMSI
3. Compréhension de l'organisme et clarification des objectifs de sécurité de l'information
4. Analyse du système de management existant

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

1. Leadership et approbation du projet SMSI
2. Domaine d'application du SMSI
3. Politiques de sécurité de l'information
4. Evaluation du risque
5. Déclaration d'applicabilité et autorisation par la direction de mise en oeuvre du SMSI
6. Définition de la structure organisationnelle de la sécurité de l'information

**3 - Mise en œuvre d'un SMSI**

1. Conception des mesures de sécurité et rédaction des procédures et des politiques spécifiques
2. Mise en oeuvre des mesures de sécurité
3. Définition du processus de gestion de la documentation
4. Plan de communication, de formation et de sensibilisation
5. Gestion des opérations et des incidents

**4 - Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI**

1. Surveillance, mesure, analyse et évaluation
2. Audit interne
3. Revue de direction
4. Traitement des problèmes et des non-conformités
5. Amélioration continue
6. Préparation à l'audit de certification
7. Compétence et évaluation d'un implémenteur

***Nombre de jours*** **:** 10 jours (70h)
***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.
***Outils mis à disposition*** **:** PC , casque avec micro, clavier et souris, logiciels métiers
***Prérequis*** **:** au minimum 2 ans d'expérience professionnelle pour prétendre passer la certification
***Codes des fiches ROME les plus proches*** **:** *K1903 - Défense et conseil juridique*

**Public cible**

- aux responsables, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# CERTIFICATION DÉLÉGUÉ À LA PROTECTION DES DONNÉES

## MODULE 4 : Pilotage de projet et la communication à 360° (*réf. CDPD4)*

### Contenu

**Méthode AGILE :**

**1 - Les principales spécificités des méthodes AGILE :**

1. les fondamentaux, le management par la valeur.
2. Le manifeste AGILE.
3. Les acteurs : product owner, scrum master, chef de projet, équipe etc.
4. Management des parties prenantes : le client au cœur de la démarche.

**2 - Les étapes permettant de comprendre et prioriser les besoins des clients utilisateurs :**

1. Users story, note de cadrage.
2. Story mapping, backlog produit, check-list, management visuel.

**3 - La planification et le pilotage d'un projet en mode AGILE :**

1. Planification organisationnelle et temporelle. Release et Iteration planning.
2. Sprint, planning poker, management visuel.
3. Scrum, sprint review et retrospective, pilotage motivant et efficace.
4. Animation efficace de réunion, tableaux de bord. Le burndown chart, management visuel.

**4 - Le management des risques et les critères d'efficacité de mon équipe en mode AGILE**

1. Risques et opportunités : check-list sur les risques.
2. Caractéristiques de l'équipe AGILE.

**5 -Les étapes de la mise en place d'un projet en mode projet AGILE :**

1. Les changements requis, les facteurs clés de succès, les pièges à éviter.
2. Plan d'action de mise en oeuvre

**La Communication**

**1 - Comprendre les concepts de base de la Communication**

1. Distinguer le processus de communication (la manière de dire) de son contenu (ce qui est dit).
2. Comprendre la structure de personnalité.

**2 - Identifier les caractéristiques des diverses personnalités**

1. Utiliser une grille de lecture systémique pour chaque type de personnalité
2. Repérer les caractéristiques des types de personnalité et leurs modes de communication
3. Prendre en compte les aspects intergénérationnels

**3 - Repérer l'environnement humain adapté à chaque type de personnalité**

1. Comprendre les différentes manières d'entrer en relation avec les autres
2. Repérer la zone de confort relationnelle de chaque type de personnalité.

**4 - Développer une communication positive**

1. Comprendre la règle de la communication, et les modes de perception de chaque type de personnalité.
2. Accroître son impact en adaptant sa communication et son style de management à la personnalité de chacun.

**5 - Déclencher et entretenir sa motivation**

1. Identifier et nourrir les besoins psychologiques qui conditionnent la motivation et les choix de chacun.

**6 - Prévenir et gérer les comportements de stress**

1. Comprendre les effets du stress dans la communication et ce qui génère du stress
2. Identifier les comportements associés aux trois degrés de stress chez l'autre
3. Savoir revenir à une communication positive.
4. Gérer les situations d'incompréhension, inefficacité, conflits

***Nombre de jours*** **:** 10 jours (70h)
***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.
***Outils mis à disposition*** **:** PC , casque avec micro, clavier et souris, logiciels métiers
***Prérequis*** **:** au minimum 2 ans d'expérience professionnelle pour prétendre passer la certification
***Codes des fiches ROME les plus proches*** **:** *K1903 - Défense et conseil juridique*

**Public cible**

- aux responsables, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# CERTIFICATION DÉLÉGUÉ À LA PROTECTION DES DONNÉES

## MODULE 5 : Connaissance des outils, l'environnement de travail (*réf. CDPD5)*

**Contenu**

**1 - Le métier de Délégué à la Protection des données :**

1. Les fondamentaux : statut, missions, cartographie, relations avec la CNIL, positionnement interne, diffusion de l'information, constat d'usage, référentiel
2. Désignation d'un DPO dans une organisation
3. La mission de veille du DPO

**2 - Savoir-être et Éthique du DPO**

1. Déontologie et Éthique du DPO au regard de la compliance des organisations
2. Communiquer, sensibiliser, convaincre sur son champ d'expertise.
3. Organiser ses missions
4. Surmonter et gérer les crises
5. Gérer une équipe

**3 - Compléments**

1. Le triptyque Plaintes-Contrôles-Sanctions
2. Alertes professionnelles et alertes éthiques
3. Conformité Informatique et Libertés du périmètre Ressources Humaines
4. Synergies entre DPO et Responsable Qualité
5. Synergies entre DPO et Archiviste/Documentaliste

**1 - Mes outils numériques**

1. pour ma gestion au quotidien
2. pour ma gestion administrative partagée
3. pour mes réunions d'équipes
4. pour communiquer avec mes équipes
5. pour communiquer vers l'extérieur

**2a - Mes outils RGPD**

1. pour la collecte
2. pour l'analyse des écarts
3. pour les préconisations
4. pour le registre des traitements
5. pour le registre d'incidents
6. pour le registre des demandes
7. pour mes audits
8. pour mes tableaux de bord

**2b - Outil de gestion spécifique**

1. Définition de la gouvernance
2. Inventaire des traitements
3. Evaluation de la conformité
4. Analyse d'écart et plan de remédiation
5. Gestion des sous-traitants
6. Maintien de la conformité
7. Certification
8. La possibilité d'utiliser ou de créer d'autres référentiels

**3 - Mes outils pour communiquer**

1. pour ma gestion au quotidien
2. pour mes échanges avec les autorités de contrôle
3. pour la presse en cas de fuite de données

**4 - Mes outils pour les spécialités :**

1. Santé
2. Social
3. Réutilisation des données publiques
4. Collectivités territoriales et locales
5. Vente à distance et e-Commerce
6. Banque & Finance
7. Assurance
8. Prospective

***Nombre de jours*** **:** 15 jours (105h)
***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.
***Outils mis à disposition*** **:** PC , casque avec micro, clavier et souris, logiciels métiers
***Prérequis*** **:** au minimum 2 ans d'expérience professionnelle pour prétendre passer la certification
***Codes des fiches ROME les plus proches*** **:** *K1903 - Défense et conseil juridique*

**Public cible**

- aux responsables, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# *Community manager* MAKER *(réf. COMM)*

**Objectifs :** La formation complète d'un Community manager couplée à des compétences de création de sites internet, sites vitrine, dynamique, e-commerce et de la visite virtuelle ! Un community manager avec une boîte à outils renforcée pour se démarquer et démarquer les entreprises !

*3 mois = 455h*
*Principaux domaines couverts :*

- *Les fondamentaux : marketing, communication, webmarketing*
- *Le réseau social, blog, l'e-réputation et écrire pour le web*
- *Maker : création graphique, vidéo, un site internet la VR*
- *Créer une campagne publicitaire social média, et la suivre*
- *Pilotage de projet, l'audit et la communication à 360°*

***Certification PCIE : Gimp, Photoshop CC, Illustrator CC, Marketing numérique, Wordpress, Dreamweaver, MS Project, Présentation***

**En terme de pratique professionnelle :** la formation laisse une place prépondérante à la pratique puis très rapidement à des mises en situation professionnelles.

Nature de la validation: La formation dispensée sera sanctionnée, à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,
- Après avis favorable du jury d'évaluation, d'un certificat de compétences précisant la nature de la formation reçue.

# Community manager maker *(réf. COMcert)*

## MODULE 1 : les fondamentaux du marketing, de la communication et du webmarketing (réf. COM1)

**Contenu**

Savoir intégrer une réflexion de stratégie marketing et communication à ma pratique du métier de community manager
Je comprends l'importance du marketing dans l'entreprise, je m'initie à ses outils et à l'analyse structurée pour proposer des recommandations :

- Typologie des besoins, freins et motivations, facteurs d'influence du consommateur
- Étude de marché et concurrence
- Diagnostic SWOT
- Mix marketing

Je comprends les étapes clés d'une stratégie de communication :

- Acteurs et typologies de la communication
- Stratégie de communication, brief et diagnostic
- Positionnement et publics cible (persona)
- Moyens média (ex : médias sociaux) et hors média

J'identifie les techniques marketing et publicitaires utilisées dans un environnement internet pour créer du trafic, fidéliser les clients et analyser les performances :

- Réseaux sociaux
- E-mailing
- Affiliation
- Référencement
- UI et UX design

***Nombre de jours*** **:** 15 jours (105h)

***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.

***Outils mis à disposition*** **:** PC, caméra 360°, casque avec micro, clavier et souris, logiciels

***Prérequis*** **:** maîtrise de la langue française à l'écrit et à l'oral

***Codes des fiches ROME les plus proches*** **:**
E1101 - Animation de site multimédia, E1103 - Communication, M1702 - Analyse des tendances

**Public cible**

- aux responsables, aux dirigeants voulant se former dans la communication, le marketing numérique, le webmarketing,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser ou se réorienter dans des métiers en tension.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# COMMUNITY MANAGER MAKER

## MODULE 2 : le réseau social, blog, l'e-réputation et écrire pour le web (*réf. COM2)*

**Contenu**

Découvrir l'ensemble des réseaux sociaux, en connaître les usages publics et privés, être en capacité de créer et animer différents profils en adéquation avec sa stratégie de communication et le public cible. Configurer et paramétrer de manière avancée et automatisée ses réseaux en fonction d'objectifs professionnels.

- Panorama des différents réseaux sociaux (avantages, inconvénients, cibles…)
- Comment choisir les bons réseaux ? (cibles,stratégie marketing…)
- Création des comptes professionnels sur l'ensemble des réseaux sociaux
- Découvertes des options avancées, personnalisation des réseaux sociaux

Le community manager maîtrise les codes de la lecture et de l'écriture pour le web. Il est capable d'optimiser son contenu en fonction des normes et des notions de référencement naturel (SEO). Il utilise les mots-clés pour une indexation optimale de son site. Vous apprendrez à rédiger une news, condenser et synthétiser une information, concevoir et publier une newsletter.

- Connaître les techniques d'écriture pour le Web
- Les astuces pour rédiger sur le Web
- Optimisation des pages, des mots-clés et liens
- Le principe de référencement naturel (SEO)
- Adapter un style rédactionnel
- Synthétiser une information
- Faire du storytelling
- Rédaction et mise en page d'une newsletter / emailing (Sendinblue, mailchimp)

La veille est indispensable dans les métiers du numérique. Ce module apportera les outils indispensables à une bonne curation ainsi que la méthodologie pour assimiler et restituer de manière efficace sa veille. Le module aborde également le principe d'e-réputation d'une entreprise, d'une marque et même d'une personne.

- Les enjeux de la veille
- Découverte des outils de curation
- Résumer, synthétiser et restituer sa veille à l'oral
- Connaître mes objectifs
- Anticiper les besoins de veille
- Connaître les principes d'e-réputation
- Anticiper les risques
- Communication de crise
- Comment améliorer sa e-réputation

***Nombre de jours*** **:** 10 jours (70 h)

***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.

***Outils mis à disposition*** **:** PC , caméra 360°, casque avec micro, clavier et souris, logiciels

***Prérequis*** **:** maîtrise de la langue française à l'écrit et à l'oral

***Codes des fiches ROME les plus proches :***

E1101 - Animation de site multimédia, E1103 - Communication, M1702 - Analyse des tendances

**Public cible**

- aux responsables, aux dirigeants voulant se former dans la communication, le marketing numérique, le webmarketing
- aux salariés et demandeurs d'emploi souhaitant se spécialiser ou se réorienter dans des métiers en tension.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# COMMUNITY MANAGER MAKER

## MODULE 3 : Builder : création graphique, vidéo, un site internet la VR (*réf. COM3)*

**Contenu**

Le community manager est en capacité de retoucher, recadrer, dynamiser une image avant publication sur les réseaux sociaux. Il est également en mesure de réaliser une affiche, un flyer, un logo pour promouvoir une marque ou un événement. La vidéo étant un vecteur de communication important, le community manager possède les connaissances nécessaires à la réalisation d'une vidéo (interview, clip…) avec les compétences techniques (gestion de la lumière, du son…) et artistiques (retouche, effets…).

- Retoucher rapidement une image avec les outils en ligne (Canva…)
- Retouche chromatique et cadrage d'une photo/image
- Découverte des outils Adobe (Photoshop, adobe XD…)
- Les notions de UX et UI Design
- Savoir exporter ses fichiers avec le bon format
- Filmer une séquence vidéo avec différents périphériques
- Réaliser un montage simple avec des outils en ligne
- Exporter, compresser et mettre en ligne une vidéo (les formats, l'encodage…)

Découverte des outils liés à la VR et les utiliser dans un contexte d'inclusion sociale. Prise en main d'une caméra 360° et réalisation de photos et vidéos avec différentes configurations (Rendu HDR, ISO…) en fonction des lieux de tournage et de la luminosité. Réaliser le montage des éléments dans une interface Web via les langages HTML et CSS.

Intégration de la formation dans la réalisation de plusieurs vidéos métiers réalisées

- Comprendre les enjeux de la formation en VR
- Panorama des outils VR
- Réaliser les photos 360°
- Mener une interview vidéo en 360°
- Réaliser une vidéo de présentation d'un métier
- Retouche des photos 360°
- Retouche des vidéos 360°
- Découverte des langages HTML et CSS
- Création d'une interface Web
- Organisation de la Visite VR
- Mise en ligne sur le Web

***Nombre de jours*** **:** 10 jours (70 h)

***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.

***Outils mis à disposition*** **:** PC , caméra 360°, casque avec micro, clavier et souris, logiciels

***Prérequis*** **:** maîtrise de la langue française à l'écrit et à l'oral

***Codes des fiches ROME les plus proches*** **:**
E1101 - Animation de site multimédia, E1103 - Communication, M1702 - Analyse des tendances

**Public cible**

- aux responsables, aux dirigeants voulant se former dans la communication, le marketing numérique, le webmarketing
- aux salariés et demandeurs d'emploi souhaitant se spécialiser ou se réorienter dans des métiers en tension.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# COMMUNITY MANAGER MAKER

## MODULE 4 : Créer une campagne publicitaire social média, et la suivre (réf. COM4)

**Contenu**

Mettre en place une campagne publicitaire en ligne en utilisant les différentes plateformes de médias sociaux. Se fixer des objectifs, planifier, et budgéter une campagne social Ads. Analyser les performances.

- Les différents formats publicitaires
- Le SEA Search Engine Marketing (Adwords)
- Mettre en place une campagne adwords via Google et les réseaux sociaux
- Les outils d'analyse de performance
- Identifier des influenceurs et organiser des opérations d'influence

Google Analytics est un outil indispensable pour analyser et comprendre votre audience. Ce module vous apprendra à mesurer l'efficacité de vos stratégies de communication et adapter vos actions en temps réel. Apprenez à définir vos propres indicateurs de performance (KPI) et réaliser des tableaux de suivi.

- Comment établir et analyser des statistiques ?
- Les outils Google Search Console et Google Analytics
- Les indicateurs de performance (KPI)
- Les outils indispensables pour les réseaux sociaux
- Méthodologie pour le reporting

***Nombre de jours*** **:** 10 jours (70 h)

***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.

***Outils mis à disposition*** **:** PC , caméra 360°, casque avec micro, clavier et souris, logiciels

***Prérequis*** **:** maîtrise de la langue française à l'écrit et à l'oral

***Codes des fiches ROME les plus proches :***
E1101 - Animation de site multimédia, E1103 - Communication, M1702 - Analyse des tendances

**Public cible**

- aux responsables, aux dirigeants voulant se former dans la communication, le marketing numérique, le webmarketing
- aux salariés et demandeurs d'emploi souhaitant se spécialiser ou se réorienter dans des métiers en tension.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# COMMUNITY MANAGER MAKER

## MODULE 5 : Communication 360° et le mode projet (*réf. COM5)*

**Contenu**

**1 - Le métier de Délégué à la Protection des données :**

4. Les fondamentaux : statut, missions, cartographie, relations avec la CNIL, positionnement interne, diffusion de l'information, constat d'usage, référentiel
5. Désignation d'un DPO dans une organisation
6. La mission de veille du DPO

**2 - Savoir-être et Éthique du DPO**

6. Déontologie et Éthique du DPO au regard de la compliance des organisations
7. Communiquer, sensibiliser, convaincre sur son champ d'expertise.
8. Organiser ses missions
9. Surmonter et gérer les crises
10. Gérer une équipe

**3 - Compléments**

6. Le triptyque Plaintes-Contrôles-Sanctions
7. Alertes professionnelles et alertes éthiques
8. Conformité Informatique et Libertés du périmètre Ressources Humaines
9. Synergies entre DPO et Responsable Qualité
10. Synergies entre DPO et Archiviste/Documentaliste

**1 - Mes outils numériques**

6. pour ma gestion au quotidien
7. pour ma gestion administrative partagée
8. pour mes réunions d'équipes
9. pour communiquer avec mes équipes
10. pour communiquer vers l'extérieur

**2a - Mes outils RGPD**

9. pour la collecte
10. pour l'analyse des écarts
11. pour les préconisations
12. pour le registre des traitements
13. pour le registre d'incidents
14. pour le registre des demandes
15. pour mes audits
16. pour mes tableaux de bord

**2b - Outil de gestion spécifique**

9. Définition de la gouvernance
10. Inventaire des traitements
11. Evaluation de la conformité
12. Analyse d'écart et plan de remédiation
13. Gestion des sous-traitants
14. Maintien de la conformité
15. Certification
16. La possibilité d'utiliser ou de créer d'autres référentiels

**3 - Mes outils pour communiquer**

4. pour ma gestion au quotidien
5. pour mes échanges avec les autorités de contrôle
6. pour la presse en cas de fuite de données

**4 - Mes outils pour les spécialités :**

9. Santé
10. Social
11. Réutilisation des données publiques
12. Collectivités territoriales et locales
13. Vente à distance et e-Commerce
14. Banque & Finance
15. Assurance
16. Prospective

***Nombre de jours*** **:** 15 jours (105h)
***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.
***Outils mis à disposition*** **:** PC , casque avec micro, clavier et souris, logiciels métiers
***Prérequis*** **:** au minimum 2 ans d'expérience professionnelle pour prétendre passer la certification
***Codes des fiches ROME les plus proches*** **:** *K1903 - Défense et conseil juridique*

**Public cible**

- aux responsables, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# Spécialiste défense des systèmes d'information (*réf. SDSI)*

**Objectifs : Très convoités, les experts en cybersécurité sont chargés de protéger les informations confidentielles des entreprises. Cette appellation regroupe en réalité une myriade de métiers, dont celui de consultant en sécurité des systèmes d'information (SSI).**

*4,5 mois = 630h*
*Principaux domaines couverts :*

- *Les fondamentaux : Le socle des connaissances*
- *Reconnaissance (Scan, prise d'empreintes, recherche d'informations, ingénierie sociale)*
- *Attaque (Attaques sur les systèmes, sans fil et mobile, sniffing)*
- *Attaque déportée (Attaques sur les serveurs, cloud, Firewall et cryptographie, malware)*
- *PSSI / ISO / RGPD et certification CEH*

***Certification PCIE : Sécurité des TIC, MS Project, Présentation***
***Certification CEH by EC- Council : Certified Ethical Hacker***

**En terme de pratique professionnelle :** la formation laisse une place prépondérante à la pratique puis très rapidement à des mises en situation professionnelles.

Nature de la validation: La formation dispensée sera sanctionnée, à son issue, par la remise :

- D'une attestation de fin de formation précisant la nature, les dates, la durée, les objectifs et les résultats des acquis de la formation reçue,
- D'une feuille d'émargement,
- Après avis favorable du jury d'évaluation, d'un certificat de compétences précisant la nature de la formation reçue.

# Spécialiste défense des systèmes d'information

## MODULE 1 : Les bases du réseau (réf. SDSI1)

**Contenu**

L'apprenant aura une vue complète de la configuration des **Réseaux**, il sera en mesure de :

- Connaître les différents équipements réseaux
- Comprendre l'importance du protocole TCP/IP dans l'élaboration d'un réseau
- Installer un réseau physique : poste de travail, routeur, commutateur, dns, dhcp
- Appréhender les principaux services et protocoles : tcp/ip, udp, arp, http, https

Installer et administrer le nouveau système d'exploitation Microsoft **Windows Server** 2016. Vous apprendrez à installer et paramétrer ses déclinaisons, réaliser les tâches d'administration courantes et mettre des ressources sécurisées en environnement Active Directory.
Installer et administrer **Linux** au quotidien. Vous verrez notamment la gestion des utilisateurs, des disques et des périphériques, les sauvegardes, la configuration du réseau et des principaux services.
Découvrir les bases algorithmiques du scripting bash et la logique des conditions/boucles. Connaître les commandes de bases du shell Linux. Être capable d'analyser un besoin et de réaliser un script répondant à ce besoin.
Acquérir tous les éléments principaux pour programmer en **Python.**
Être capable de réaliser des programmes avec les conditions, les boucles, les fonctions en Python.
Connaître la programmation orientée objet.

***Nombre de jours*** **:** 20 jours (140h)
***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.
***Outils mis à disposition*** **:** PC , casque avec micro, clavier et souris, logiciels métiers
***Prérequis*** **:** maîtrise de la langue française à l'écrit et à l'oral
***Codes des fiches ROME les plus proches*** **:** *M1802 - Expertise et support en systèmes d'information*
*M1801 - Administration de systèmes d'information*

**Public cible**

- aux responsables informatiques, aux administrateurs de réseaux, aux responsables de la sécurité des systèmes d'information, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser ou se réorienter dans des métiers en tension.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# SPÉCIALISTE DÉFENSE DES SYSTÈMES D'INFORMATION

## MODULE 2 : Reconnaissance (*réf. SDSI2)*

**Contenu**

Etre capable de comprendre les enjeux de **l'ingénierie sociale**. Pouvoir utiliser les outils de prise d'empreintes pour créer une fiche identité de la cible en cas d'attaque pour mieux la défendre.

- Comment effectuer une prise d'empreintes
- Utiliser les sources libres et ouvertes à disposition

Être capable de **scanner des réseaux** afin de trouver des artefacts. Trouver des failles dans les réseaux. Exploiter ces failles. Combler les failles.

- Comment lister les réseaux d'une cible
- Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques
- Mesurer le niveau de sécurité de votre Système d'Information
- Réaliser un test de pénétration
- Définir l'impact et la portée d'une vulnérabilité

Savoir comprendre les aspect de **l'ingénierie sociale**. Les attaques en face à face, par email, téléphone. Savoir identifier les tentatives d'escroquerie.

- Les techniques utilisées par les attaquants via ingénierie sociale
- Comment se protéger contre ces attaques
- Mener mon pentest en utilisant ces techniques

Afin de faire de la reconnaissance, il faut pouvoir énumérer les services et protocoles des hôtes du réseau. Il est donc nécessaire d'avoir un listing précis du réseau grâce aux différentes techniques **d'énumération.**

- Comment aller chercher de l'information via les protocoles réseaux
- Comment et quels sont les protocoles utilisés

***Nombre de jours*** **:** 15 jours (105h)

***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.

***Outils mis à disposition*** **:** PC , casque avec micro, clavier et souris, logiciels métiers

***Prérequis*** **:** maîtrise de la langue française à l'écrit et à l'oral

***Codes des fiches ROME les plus proches*** **:** *M1802 - Expertise et support en systèmes d'information*
*M1801 - Administration de systèmes d'information*

**Public cible**

- aux responsables informatiques, aux administrateurs de réseaux, aux responsables de la sécurité des systèmes d'information, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser ou se réorienter dans des métiers en tension.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# SPÉCIALISTE DÉFENSE DES SYSTÈMES D'INFORMATION

## MODULE 3 : Attaque (*réf. SDSI3)*

**Contenu**

L'apprenant comprendra les possibilités qui lui seront données lors d'une attaque sur les systèmes cible. Il parcourra les différentes techniques employées par les pirates informatique. Il comprendra enfin comment placer des barrières pour éviter d'être exposé à ces risques.

- Tester la sécurité des systèmes cible
- Couvrir ses traces après l'attaque
- Adapter ses rapports de pentest

L'apprenant comprendra les techniques indispensables pour réaliser une analyse a posteriori (aussi appelée inforensic) d'incidents de sécurité informatique. Suite à des simulations d'attaques, il apprendra à collecter et préserver les preuves, les analyser et améliorer la sécurité du SI après l'intrusion.

- Maîtriser les bons réflexes en cas d'intrusion sur une machine
- Collecter et préserver l'intégrité des preuves électroniques
- Analyser l'intrusion a posteriori
- Améliorer sa sécurité après une intrusion

L'apprenant parcourra les différentes phases du Sniffing : interception, analyse, injection réseau.

- Les méthodes de **sniffing**
- Les failles potentielles
- Les contre-mesures
- J'adapte mon pentest au sniffing

Mettre en place une cellule de détection ou de protection contre les attaques est primordial. Encore faut-il comprendre comment se déroulent les attaques pour pouvoir paramétrer au plus juste notre protection.

- Comment fonctionne un **IDS/IPS**
- Comment paramétrer un **firewall**
- Comment adapter mon pentest à ces détections

L'apprenant découvrira les techniques indispensables pour mesurer le niveau de sécurité de votre SGBD (base de données). A la suite de ces attaques, vous apprendrez à déclencher la riposte appropriée et à en élever le niveau de sécurité.

- Définir l'impact et la portée d'une vulnérabilité
- Comprendre les techniques des pirates informatiques et pouvoir contrer leurs attaques
- Mesurer le niveau de sécurité de votre base de données
- Réaliser un test de pénétration

***Nombre de jours*** **:** 15 jours (105h)

***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.

***Outils mis à disposition*** **:** PC , casque avec micro, clavier et souris, logiciels métiers

***Prérequis*** **:** maîtrise de la langue française à l'écrit et à l'oral

***Codes des fiches ROME les plus proches*** **:** *M1802 - Expertise et support en systèmes d'information*
*M1801 - Administration de systèmes d'information*

**Public cible**

- aux responsables informatiques, aux administrateurs de réseaux, aux responsables de la sécurité des systèmes d'information, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser ou se réorienter dans des métiers en tension.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# SPÉCIALISTE DÉFENSE DES SYSTÈMES D'INFORMATION

## MODULE 4 : Attaque déportée (*réf. SDSI4)*

**Contenu**

La puissance de calcul des ordinateurs permet aujourd'hui de lancer simultanément des attaques distribuées contre des services en ligne. Il est important de comprendre comment se déroulent ces attaques afin de mieux s'en protéger.

- Comment mener une attaque de type DoS et DDoS, comment me prémunir contre ces attaques

**Vol de session** : Il s'agit d'une technique consistant à intercepter une session TCP initiée entre deux machines afin de la détourner. Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session. Il convient donc de comprendre comment se forge une attaque afin de mieux s'en prémunir.

- Les différentes attaques possibles, Comment se prémunir de ces attaques
- Mener mon Pentest via le vol de session

L'intrusion sur les serveurs de l'entreprise représente un risque majeur. Il est essentiel de comprendre et d'appliquer les technologies et les produits permettant d'apporter le niveau de sécurité suffisant aux applications déployées et plus particulièrement aux applications à risque comme les services extranet et la messagerie.

- Identifier les vulnérabilités les plus courantes des applications Web, comprendre le déroulement d'une attaque, tester la sécurité de ses applications Web
- Configurer un serveur Web pour chiffrer le trafic Web avec HTTPS
- Mettre en place des mesures de sécurisation simples pour les applications Web

L'intrusion sur les serveurs de l'entreprise représente un risque majeur. Il est essentiel de comprendre et d'appliquer les technologies et les produits permettant d'apporter le niveau de sécurité suffisant aux applications déployées et plus particulièrement aux applications à risque comme les services extranet et la messagerie.

- Identifier les vulnérabilités les plus courantes des applications Web
- Comprendre le déroulement d'une attaque. Tester la sécurité de ses applications Web

L'apprenant aura connaissance des techniques indispensables pour mesurer le niveau de sécurité de son réseau sans fil. A la suite de ces attaques, vous apprendrez à déclencher la riposte appropriée et à en élever le niveau de sécurité.

- Les différents protocoles liés au sans fil, les failles connues des modules sans fil
- Adapter mon pentest au sans fil

Les terminaux mobiles s'intègrent de plus en plus dans notre environnement de travail et dans nos projets, et engendrent de nouveaux défis en termes de sécurité. Ce module propose une synthèse des problématiques de sécurité posées par ces appareils : communication, stockage de données, publication d'applications.

- Identifier les services de sécurité des systèmes d'exploitation mobiles
- Définir les règles de sécurité dans une conduite de projet mobile
- Différencier les solutions de sécurité selon le terminal, identifier les impacts du BYOD sur la sécurité

Comment peut-on assurer la sécurité des informations dispersées dans "le nuage" ? Ce module dresse un panorama complet de ce problème majeur du cloud.

- Découvrir les bases du cloud, ses différents modes de déploiement, évaluer les principales menaces et vulnérabilités du cloud, comprendre les trente-cinq risques identifiés par l'ENISA
- Découvrir les principes d'audit de la sécurité dans le cloud

Ce module présente les différentes techniques cryptographiques ainsi que les principales applications. Les chiffrements symétriques et asymétriques, le hachage, les algorithmes les plus utilisés ainsi que les méthodes de gestion des clés seront expliqués en détail.

***Nombre de jours*** **:** 20 jours (140h)

***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.

***Outils mis à disposition*** **:** PC , casque avec micro, clavier et souris, logiciels métiers

***Prérequis*** **:** maîtrise de la langue française à l'écrit et à l'oral

***Codes des fiches ROME les plus proches*** **:** *M1802 - Expertise et support en systèmes d'information*
*M1801 - Administration de systèmes d'information*

**Public cible**

- aux responsables informatiques, aux administrateurs de réseaux, aux responsables de la sécurité des systèmes d'information, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser ou se réorienter dans des métiers en tension.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

# SPÉCIALISTE DÉFENSE DES SYSTÈMES D'INFORMATION

## MODULE 5 : gouvernance et certification CEH (*réf. SDSI5)*

**Contenu**

Il convient de ne pas maîtriser que la technique. Lors de pentests, il y a des obligations et des devoirs. Les possibilités offertes par les attaques cyber sont multiples et peuvent être dévastatrices. Il convient d'en maîtriser les textes de lois et les règles organisationnelles.

- Je sais analyser les besoins en législation
- Comment me conformer au RGPD
- Comment me conformer aux normes ISO 27001 et ISO 27005
- Comment rédiger une PSSI

Un Hacker Éthique certifié est un professionnel qualifié qui comprend et sait comment rechercher les faiblesses et les vulnérabilités des systèmes cibles et utilise les mêmes connaissances et outils qu'un hacker malveillant, mais d'une manière légale et légitime pour évaluer la sécurité d'un système cible. L'accréditation HEC certifie les individus dans la discipline spécifique de la sécurité des réseaux du piratage éthique d'un point de vue neutre vis-à-vis des fournisseurs.

- Établir et régir des normes minimales pour l'accréditation des spécialistes professionnels de la sécurité de l'information en matière de mesures de piratage éthique
- Informer le public que les personnes accréditées satisfont aux normes minimales ou les dépassent
- Renforcer le piratage éthique en tant que profession unique et auto réglementée

***Nombre de jours*** **:** 5 jours (35h)

***Nombre de stagiaires*** **:** minimum 4 en modulaire, 20 pour une session entière.

***Outils mis à disposition*** **:** PC , casque avec micro, clavier et souris, logiciels métiers

***Prérequis*** **:** maîtrise de la langue française à l'écrit et à l'oral

***Codes des fiches ROME les plus proches*** **:** *M1802 - Expertise et support en systèmes d'information*
*M1801 - Administration de systèmes d'information*

**Public cible**

- aux responsables informatiques, aux administrateurs de réseaux, aux responsables de la sécurité des systèmes d'information, aux dirigeants voulant se former en fonction de leur infrastructure réseau,
- aux salariés et demandeurs d'emploi souhaitant se spécialiser ou se réorienter dans des métiers en tension.

**Méthodes pédagogiques**

- en présentiel ou en téléprésentiel avec un formateur pour la théorie et un assistant pour un suivi supplémentaire pour les exercices et mises en situation.
- Apports théoriques et pratiques
- Utilisation de matériel informatique adéquat (matériel de la box)
- Support de cours

Une fiche d'évaluation est remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration.

e-catalyst

Au cœur de vos attentes. En réponse à vos besoins

**49 rue de l'égalité 59600 MAUBEUGE**
**N° SIRET 84501436400010**
**Organisme de Formation : enregistré sous le numéro 32590993659**
**Cet enregistrement ne vaut pas agrément de l'État.**
**La présentation détaillée d'e-Catalyst, CV des intervenants, catalogue détaillé des formations 2020 sont disponibles sur :**

# www.e-Catalyst.fr

**Version du Catalogue au 21-11-2020**