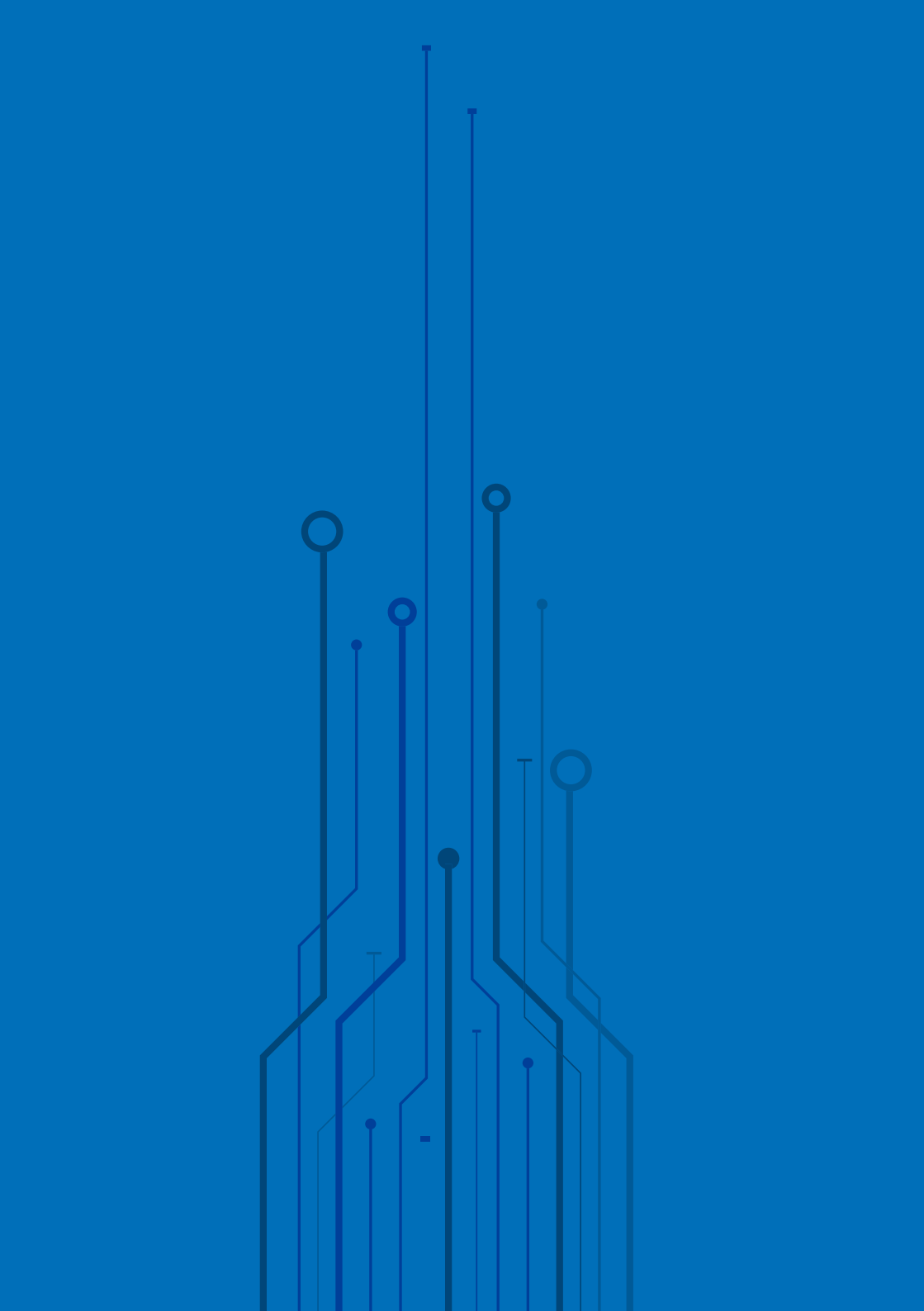
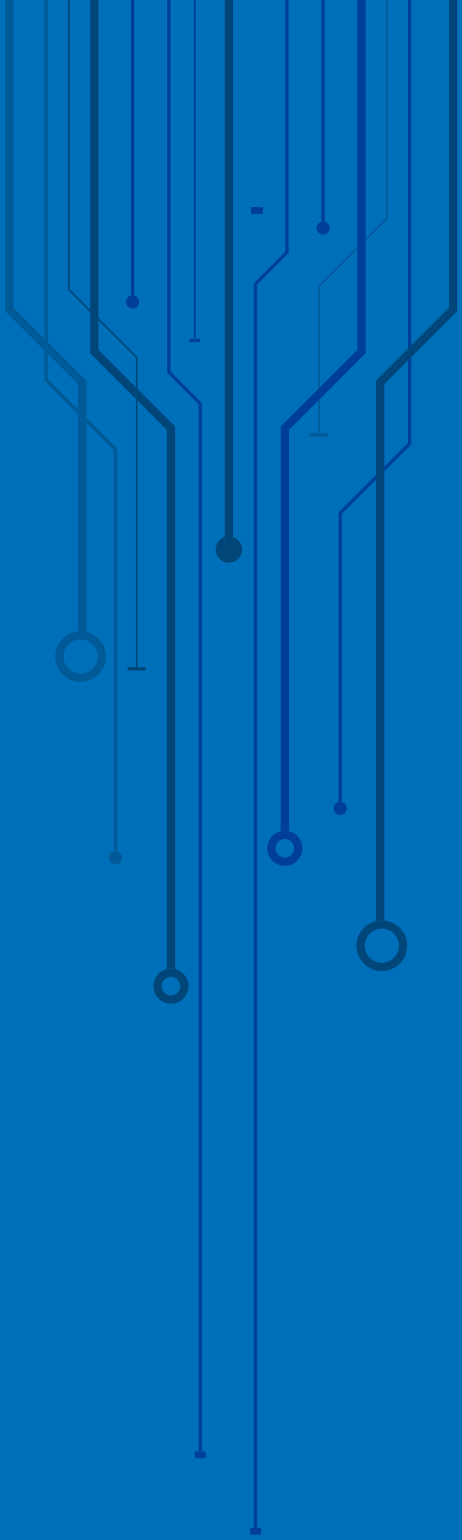
Techno.bel
Centre de Compétence

CYBER SÉCURITÉ
FORMATIONS
ATELIERS PRATIQUES
CAUSERIES





À PROPOS

La sécurité informatique doit aujourd'hui être au cœur des préoccupations de tout le monde, entreprises comme particuliers. Plus une semaine ne se passe sans que la presse ne révèle de nouvelles cyber attaques ou tentatives d'escroqueries via des canaux numériques. La cyber sécurité nous concerne et garantit une protection efficace des données que nous produisons et traitons au quotidien. Il s'agit aussi pour les entreprises de s'assurer certains avantages concurrentiels en protégeant leurs process et systèmes d'information. Ce sont les raisons pour lesquelles Technobel a décidé de vous aider, en compilant au sein de ce catalogue non exhaustif, une offre de formations mais aussi des ateliers pratiques et des causeries entièrement dédiés à la cyber sécurité.

Les thématiques abordées par les **formations** reprises dans ce catalogue sont regroupées parmi cinq catégories interdépendantes (voir schéma p.2). La première s'intéresse aux questions liées aux périphériques et à tous les appareils désormais utilisés au quotidien (PC, smartphones, tablettes…) mais aussi à tous les objets connectés (montres, capteurs, boîtiers de mesures…) qui produisent et émettent des données. Le chapitre consacré à la sécurisation des réseaux informatiques constitue la seconde catégories de ce catalogue. Tous les types de communications (filaires, hertziennes…) y sont reprises. Une fois produites et véhiculées au travers de réseaux sécurisés, les données sont sauvegardées. C'est la troisième thématique de cet ouvrage : les environnements de stockage. Ensuite, c'est au tour des applications d'entrer sur la piste. Celles-ci exploitent les données jusqu'ici produites, émises et stockées de manière fiable. Notons, qu'à leur tour, ces applications produiront de nouvelles données auxquelles une politique de sécurité devra également être appliquée. Enfin, afin de garantir le fonctionnement global des sécurités informatiques mises en place, il est indispensable d'en orchestrer les différentes étapes, de sécuriser l'ensemble des processus et d'y intégrer les concepts de protection des données à caractère personnel. Ce sont les points abordés dans la thématique de la gouvernance.

Les **ateliers pratiques** présentés dans cette brochure proposent par ailleurs une forme nouvelle d'apprentissage. L'approche par la pratique, ou comment « mettre les mains dans le cambouis », est en effet une méthodologie régulièrement promue et activée dans les différentes actions du Centre Technobel. Grâce à un matériel de pointe mis à votre disposition et à l'accompagnement d'un coach, vous pourrez vous exercer à la mise en œuvre de politiques de cyber sécurité fiables.

Enfin des conférences, reprises sous le nom de **causeries** et abordant des thématiques précises, vous sont proposées au sein de ce catalogue. Animés par des experts du secteur, ces moments sont des occasions uniques de démystifier les thématiques qu'ils abordent mais aussi de provoquer quantité de débats des plus intéressants.

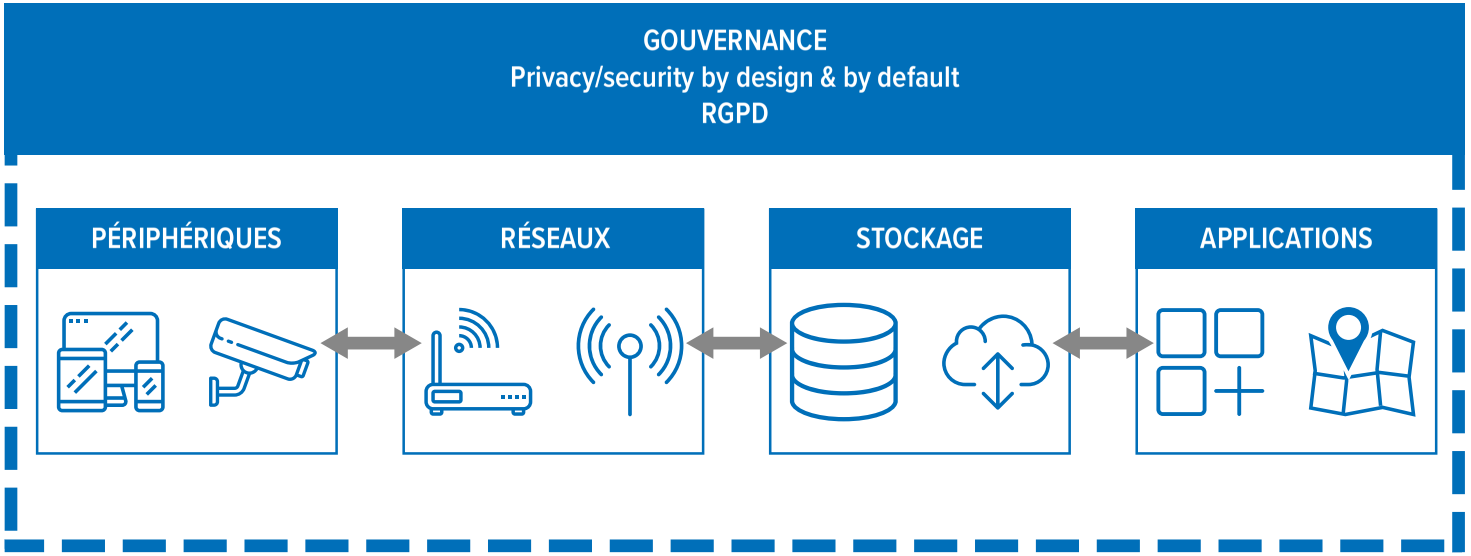

GOUVERNANCE
Privacy/security by design & by default
RGPD
PÉRIPHÉRIQUES
RÉSEAUX
STOCKAGE
APPLICATIONS

TABLE DES MATIÈRES

STOCKAGE

APPLICATIONS

GOUVERNANCE - PRIVACY/SECURITY BY DESIGN & BY DEFAULT

NOS ATELIERS, NOS CAUSERIES 35

NOS FORMATIONS

Le catalogue des formations que vous trouverez dans les pages qui suivent aborde les technologies identifiées par le Centre de compétence Technobel, avec l'aide de nombreux experts, comme ayant un impact important dans la gestion d'une politique de cyber sécurité efficace.

L'information partout, tout le temps, sur tous les supports, la multiplication des objets connectés, le cloud computing, le Big Data et l'omniprésence des technologies dans nos vies nous exposent chaque jour un peu plus aux dangers des cyber attaques ! Toutes ces menaces entachent d'une part le développement des technologies mais aussi la croissance économique de nombreuses structures qui subissent, au quotidien, des attaques informatiques pour lesquelles elles n'étaient pas préparées.

Plus qu'un simple défi d'informaticiens, la sécurité informatique doit aujourd'hui être une priorité pour les entreprises !

PÉRIPHÉRIQUES

RÉSEAUX

STOCKAGE

APPLICATIONS

GOUVERNANCE

PRIVACY/SECURITY BY DESIGN & BY DEFAULT

PC, TABLETTES, SMARTPHONES ? LES BONNES PRATIQUES DE SÉCURITÉ

Description :

Comprendre les risques encourus d'une mauvaise utilisation de ses outils numériques (PC, tablettes, smartphones...) mais aussi anticiper les dangers qui y sont liés ne sont pas choses évidentes. Cette formation d'une demi-journée vous donnera toutes les astuces pour travailler au quotidien dans un environnement de travail numérique sécurisé.

Objectifs :

- Acquérir les bons réflexes d'utilisation de son environnement informatique
- Être conscient des risques encourus
- Se prémunir contre les attaques IT
- Comprendre le vocabulaire IT lié aux cyber attaques et aux outils de protection

Prérequis :

- Avoir une connaissance des outils informatiques de base

Contenus :

1. Sécuriser son environnement informatique : les enjeux ?
2. Choisir avec soin ses mots de passe
3. Mettre à jour régulièrement ses logiciels
4. Connaître ses utilisateurs et prestataires
5. Effectuer des sauvegardes régulières
6. Sécuriser l'accès Wifi de son entreprise
7. Être aussi prudent avec un smartphone ou une tablette qu'avec un ordinateur
8. Protéger les données lors de ses déplacements
9. Être prudent lors de l'utilisation d'une messagerie
10. Télécharger ses programmes sur les sites officiels des éditeurs
11. Être vigilant lors d'un paiement sur Internet
12. Différencier les usages privés des usages professionnels
13. Maîtriser son identité numérique

0,5 jour | **60 € / ttc**

SÉCURISER SON POSTE DE TRAVAIL

Description :

De nombreux employés, parfois par méconnaissance et plus souvent encore par peur des outils informatiques, développent des habitudes pouvant mettre à mal la sécurité de leurs différents postes de travail. Cette formation d'une demi-journée vous permettra de structurer vos différents outils et d'en vérifier le niveau de sécurité, de configurer un antivirus adéquat ou encore d'établir une stratégie de sauvegarde.

Objectifs :

- Être conscient des menaces existantes
- Se prémunir contre des attaques potentielles
- Disposer d'outils de vérification pour garantir le bon fonctionnement de vos outils
- Se préparer à une reprise après sinistre

Prérequis :

- Avoir une connaissance des outils informatiques de base

Contenus :

1. Identifier les dangers potentiels
2. Identifier les modes de contamination
3. Identifier les mesures de protection adéquates à votre poste de travail
   - Les mesures préventives
   - Les mesures effectives
4. Exercices

60 € / ttc

0,5 jour

SE PRÉPARER À LA CERTIFICATION COMPTIA SECURITY+

Description :

CompTIA Security+ est la certification reconnue mondialement qui valide les connaissances et les compétences de base en matière de sécurité informatique. Vue comme une référence dans le domaine de la sécurité informatique, cette certification couvre les principes essentiels de la sécurité des réseaux et de la gestion des risques. La certification *CompTIA Security+* est le tremplin pour votre carrière dans la sécurité informatique. Cette formation de quatre jours vous préparera au passage de la certification *CompTIA Security+*.

Objectifs :

- Mettre en œuvre des protocoles de sécurité
- Réagir efficacement aux problèmes de sécurité
- Identifier les menaces et risques en matière de sécurité des systèmes d'information
- Découvrir les solutions logicielles et matérielles nécessaires à la mise en place d'une infrastructure sécurisée
- Mettre en place un système de gestion d'identités et de droits
- Superviser la sécurité de son infrastructure
- Appréhender la notion de sécurité offensive

Prérequis :

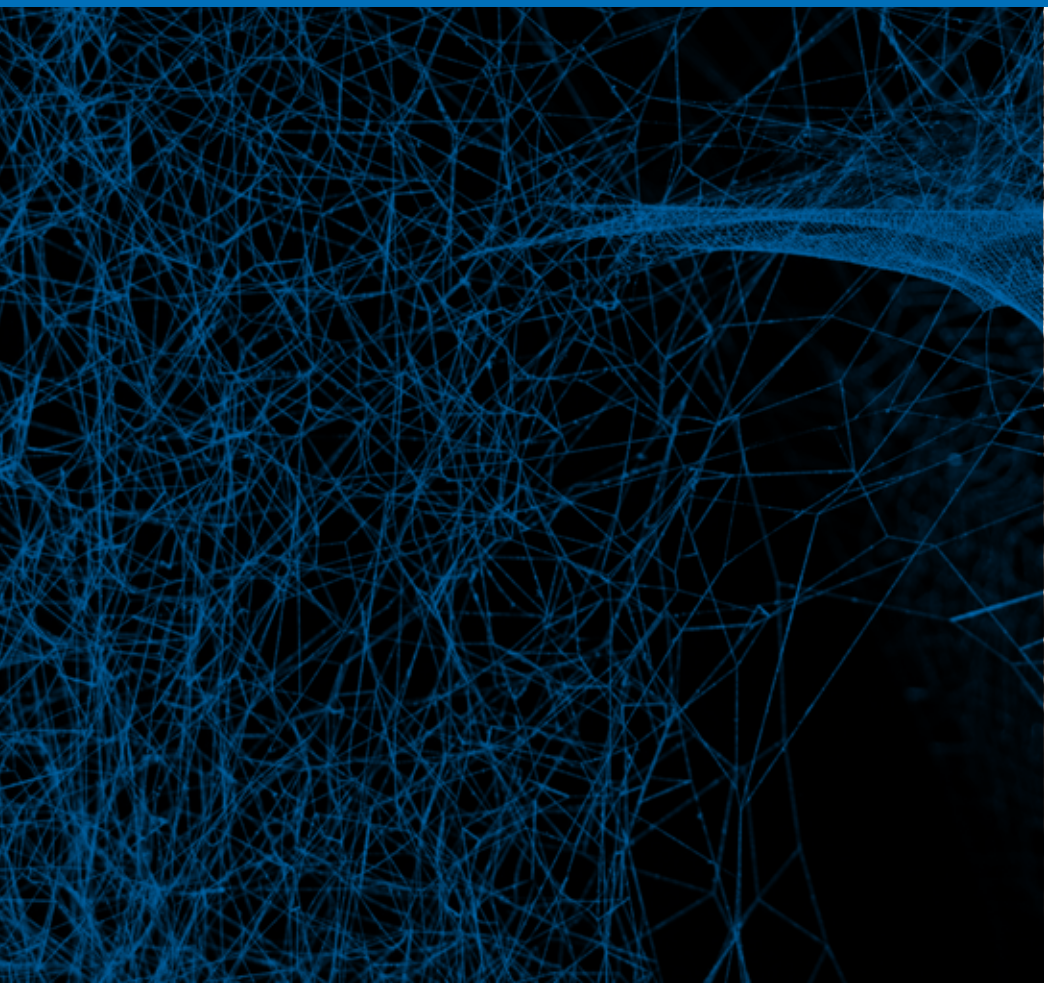
- Avoir une connaissance de base de la pile TCP/IP
- Avoir une connaissance de la configuration et du paramétrage d'un ordinateur
- Avoir une connaissance de base du domaine IT

Contenus :

1. Gérer efficacement les risques potentiels
2. Diagnostiquer et superviser les réseaux informatiques
3. Comprendre le fonctionnement des périphériques et des infrastructures
4. Gérer les identités et les accès
5. Prévenir les menaces sur les réseaux wireless
6. Sécuriser un environnement Cloud
7. Sécuriser des hôtes, des données et des applications
8. Comprendre les techniques de cryptographie
9. Comprendre les menaces, les attaques et les points vulnérables
10. Se prémunir contre le « Social Engineering » et autres ennemis
11. Administrer la cyber sécurité d'un environnement de travail professionnel
12. Ateliers pratiques

4 jours | **1000 € / ttc**

RÉSEAUX



SÉCURISER UN RÉSEAU INFORMATIQUE

Description :

Cette formation aborde les notions essentielles permettant de sécuriser un réseau informatique. Bon nombre d'attaques utilisent des failles décelées depuis plusieurs années car elles n'ont pas encore été corrigées. En suivant cette formation de trois jours, vous serez à même d'optimiser la sécurité de votre réseau.

Objectifs :

- Comprendre les différentes menaces
- Découvrir et utiliser les outils de sécurisation
- Mettre en œuvre des mesures de prévention et de détection

Prérequis :

- Avoir une connaissance des réseaux informatiques
- Avoir une connaissance des systèmes d'exploitation client

Contenus :

1. Comprendre les différentes menaces
   - Les attaques Dos, Ddos, spoofing...
   - Les autres menaces et points de vulnérabilité
   - La standardisation et la gradation des risques
   - La détection des risques, menaces et points de vulnérabilité
2. Identifier et paramétrer les outils existants dans les unités du réseau
   - Les commutateurs
   - Les routeurs
3. Mettre en œuvre efficacement les outils existants : exemples concrets
4. Comprendre et paramétrer les technologies du firewall
5. Positionner correctement un firewall dans un environnement de travail en réseau
6. Mettre en place des mesures de prévention et de détection (IPS/IDS)
7. Comprendre les signatures, les bases de données et les mises à jour
8. Configurer et exploiter des signatures
9. Analyser les corrélations d'une cyber attaque et étude « Forensic »
10. Implémenter la sécurité dès la conception des réseaux (SDB)

3 jours | **750 € / ttc**

SÉCURISER SON ENVIRONNEMENT IOT ET IIOT

Description :

Si l'Internet des Objets (IoT) a déjà bouleversé nos relations avec les technologies, l'Internet des Objets Industriel (IIoT-Industrial Internet of Things) va encore un pas plus loin en forçant la rencontre entre des solutions web et des capteurs électroniques capables de recueillir mais aussi d'interpréter les données qui constituent notre environnement. Cette formation de trois jours vous soulignera tous les points d'attention à mettre en œuvre dans une politique de sécurité dans un environnement connecté industriel ou non.

Objectifs :

- Comprendre les problématiques de sécurité liés à l'IoT et à l'IIoT
- Appliquer une sécurité sur une environnement IoT
- Appliquer une sécurité sur un environnement industriel utilisant l'IoT (IIoT)

Prérequis :

- Avoir une connaissances pointues des réseaux informatiques
- Avoir une compréhension d'un environnement de type IoT
- Avoir une connaissance élémentaire du monde industriel

Contenus :

1. Comprendre les 6 piliers de l'IoT
   - La connectivité réseau
   - Le Fog Computing
   - La sécurité (cyber et physique)
   - Le traitement analytique des données
   - La gestion et l'automatisation
   - La plate-forme d'activation d'applications
2. Définir la sécurité (cyber vs. physique)
3. Comprendre les problèmes de sécurité lié à l'IoT et à l'IIoT
4. Différencier du point de vue de la sécurité l'IoT et l'IIoT
   - La sécurité des technologies opérationnelles (OT)
   - La sécurité du réseau (IoT/IIoT)
   - La sécurité physique de l'IoT
5. Utiliser les différents protocoles
   - Le niveau physique
   - Les transmissions locales des données
   - Les transmissions distantes des données
6. Définir les niveaux et les outils de la sécurité

750 € / ttc | **3** jours

SÉCURISER UN RÉSEAU WIFI EN ENTREPRISE

Description :

L'usage des réseaux sans fil (Wifi) dans nos entreprises est aujourd'hui monnaie courante. Nombreuses d'entre elles donnent en effet la possibilité à leurs employés mais aussi à toutes les personnes qui les visitent de bénéficier d'une connexion Internet Wifi. Malheureusement, tous ces réseaux sans fil ne sont pas sécurisés correctement ou ne disposent que d'une sécurité minimale, laissant portes ouvertes aux attaques et autres actions malveillantes. Cette formation d'un jour vous donnera toutes les clés pour sécuriser vos différents réseaux Wifi.

Objectifs :

- Connaître les bonnes pratiques de sécurité
- Sécuriser un réseau Wifi

Prérequis :

- Avoir des connaissances élémentaires des réseaux informatiques
- Avoir des notions théoriques des réseaux sans fil

Contenus :

1. Comprendre les composants de la sécurité dans un environnement Wifi
2. Gérer les authentifications
3. Assurer l'intégrité d'un réseau Wifi
4. Comprendre les principes de confidentialité : méthode de cryptage
5. Identifier les moyens disponibles et créer sa boîte à outils
6. Comparer WEP et WPA(2)
7. Mettre en place la norme 802.11i
8. Mettre en place une logique de sécurité et établir des recommandations

1 jour	250 € / ttc

CONFIGURER ET ADMINISTRER DES FIREWALLS CHECKPOINT «NEXT GEN»

Description :

L'omniprésence actuelle d'Internet dans le fonctionnement des entreprises ouvre la porte à de nombreux dangers auxquels elles ne sont pas toujours préparées. Les défis actuels en termes de *firewalling* se sont par ailleurs complexifiés et les besoins des entreprises sont aujourd'hui orientés vers les firewalls de type *Next Generation*. Cette formation de quatre jours vous permettra de configurer et d'administrer les firewalls *Checkpoint Next Gen* considérés comme des leaders depuis de très nombreuses années.

Objectifs :

- Définir une politique de sécurité de connexion Internet
- Sécuriser le trafic entrant et sortant
- Intégrer les fonctionnalités firewall L4 et L7
- Intégrer les firewalls et les VPN

Prérequis :

- Avoir une connaissance des réseaux informatiques (OSI, TCP/IPv4)
- Avoir une connaissance des systèmes d'exploitation client/serveur

Contenus :

1. Comprendre la sécurité des connexions Internet et les firewalls Checkpoint
2. Installer et déployer des firewalls Checkpoint
3. Administrer des firewalls Checkpoint
4. Gérer les flux sortants et entrants
5. Gérer les fonctions avancées de Layer 7 (partie Next Gen)
6. Mettre en place des VPN avec les firewalls Checkpoint

1000 € / ttc

4 jours

CONFIGURER ET ADMINISTRER DES FIREWALLS JUNIPER : INITIATION

Description :

Les firewalls sont des pièces fondamentales dans une architecture informatique sécurisée. En effet, s'ils n'assurent pas à eux seuls la sécurité d'un réseau, elle ne pourrait néanmoins pas exister sans eux. Les enjeux liés au dessin, à la gestion et à la maintenance d'une architecture sécurisée de firewalls sont donc conséquents. Cette formation de quatre jours vous permettra de mettre en place des firewalls de type *Juniper*, constructeur et leader mondial incontesté du domaine pour les PMEs mais aussi pour les plus grands comptes grâce à une gamme complète de solutions.

Objectifs :

- Comprendre les approches possibles d'une architecture sécurisée
- Installer et configurer des firewalls de type Juniper

Prérequis :

- Avoir une connaissance élémentaire des réseaux informatiques (modèles OSI, TCP/IPv4)

Contenus :

1. Découvrir les firewalls Juniper
   - Les fondamentaux
   - Les systèmes
   - Les produits et solutions Juniper
2. Comprendre les concepts de la sécurité chez Juniper
   - Les exigences pour un design de sécurité
   - L'architecture de sécurité Juniper
   - La séquence de traitement de paquets
   - Les scénarii de déploiement
3. Administrer les firewalls Juniper
   - Les composants systèmes
   - L'établissement de la connectivité
   - Les paramétrages et les options
   - Les clés de licence
   - La configuration et les fichiers d'images
   - Le « Disaster Recovery »
4. Opérer en couche 3
   - Le routage
   - Les routes statiques et les routes par défaut
   - Le « Virtual Router »
   - Le « Inter-V routing »
   - L'interface « Loopback »
   - Le « NAT »
5. Développer une « Basic policy »
   - La présentation d'une politique de sécurité
   - La configuration d'une politique de sécurité
   - Les problèmes rencontrés
6. Ateliers pratiques

3 jours | **750 € / ttc**

CONFIGURER ET ADMINISTRER DES FIREWALLS JUNIPER : PERFECTIONNEMENT

Description :

Cette formation aborde les concepts avancés liés à la configuration de firewalls *Juniper* et fait suite à la l'initiation de trois jours reprise également dans ce catalogue (p.15). Les ateliers pratiques de cette formation de quatre jours vous permettront de mieux maîtriser les matières relatives à l'univers *Juniper*.

Objectif :

- Comprendre les mécanismes des firewalls Juniper et des concepts qui y sont liés

Prérequis :

- Avoir suivi la formation « Configurer et administrer des firewalls Juniper : initiation » ou disposer des compétences équivalentes

Contenus :

1. Rappel des fondamentaux des firewalls Juniper
2. Détecter les attaques et mettre en place des mécanismes de défense
3. Comprendre la translation d'adresses (modes simples et modes avancés)
4. Gérer les authentifications simples et avancées
5. Configurer un VPN (« client to gateway » et « gateway to gateway »)
6. Paramétrer les autres fonctionnalités avancées (systèmes virtuels, haute disponibilité…)

1000 € / ttc

4 jours

ETHICAL HACKING : INITIATION

Description :

Si, aujourd'hui, les *hackers* font régulièrement la une des journaux, le *ethical hacking* est, quant à lui, peu souvent mis en lumière. Il s'agit pourtant d'une discipline essentielle aux politiques de sécurité mises en place par les organismes qui vise à identifier les failles de sécurité d'un réseau à des fins de prévention et d'anticipation. Cette formation de trois jours répartis en 18 modules vous permettra de comprendre ce qu'est le *ethical hacking*. Il vous sera également possible par la suite de suivre un module de perfectionnement qui reprendra cette structure de cours de manière plus approfondie.

Objectifs :

- Se familiariser avec l'ethical hacking
- Comprendre les méthodes et modes opératoires employés par les hackers lors d'une attaque informatique
- Identifier et utiliser les outils permettant de tester les protections d'un système d'information d'entreprise

Prérequis :

- Avoir une connaissance des réseaux informatiques
- Avoir une connaissance des systèmes d'exploitation (client/serveur)

Contenus :

1. Introduction au Ethical Hacking : profil d'un Ethical Hacker, motivations d'un pirate…
2. Footprinting et reconnaissance : analyse périmétrique, collecte d'éléments techniques…
3. Scanning de réseaux : analyse de réseaux et d'infrastructures, systèmes…
4. Enumération : collecte d'éléments SNMP, NTP, Netbios, DNS…
5. Hacking de système : cassage de mots de passe, attaque des hash…
6. Analyse de Malwares : chevaux de Troie, backdoors, virus, vers…
7. Sniffing réseau : analyse de trames réseau, injection de données…
8. Ingénierie sociale : attaques non techniques SE, attaques numériques…
9. Attaques par Déni de Service : attaques de type DOS, DDOS, par réflexion…
10. Hijacking de sessions : détournement d'identifiants de sessions…
11. Hacking de serveurs Web : modes d'attaque de serveurs web…
12. Hacking d'applications Web : vecteurs d'attaque d'applications Web, LDAP…
13. Injection SQL : modes d'attaque SQL, injection SQL en aveugle…
14. Hacking de réseaux sans fil : infrastructures WiFi WEP/WPA/WPA2, attaques WiFi…
15. Hacking plateformes mobiles : Android, Windows 8, iOS, rooter les smartphones…
16. Evasions d'IDS : firewalls & Honey Pots, comment échapper aux IDS/IPS…
17. Cloud Computing : sécurité dans le Cloud, risques, vulnérabilités…
18. Cryptographie : évolution des chiffrements AES/DES/3DES, RSA, PKI…

3 jours | **750 € / ttc**

ETHICAL HACKING : PERFECTIONNEMENT

Description :

Discipline aujourd'hui devenue incontournable parmi les spécialistes de la cyber sécurité, le *ethical hacking* vise, avant toute chose, à identifier les failles et à prévenir les menaces en amont de leurs réalisations. Cette formation de trois jours vous permettra d'approfondir en détail les matières vues dans la formation « Ethical Hacking : initiation » (p.17).

Objectifs :

- Approfondir ses connaissances en sécurité informatique
- Mieux maîtriser les concepts de la sécurité
- Avoir une approche complète en matière de sécurité

Prérequis :

- Avoir suivi la formation Ethical Hacking : initiation (p.17) ou disposer d'une expérience équivalente

Contenus :

1. Comprendre les techniques avancées de reconnaissance
2. Comprendre les techniques avancées des attaques système et réseau
3. Appliquer une sécurité accrue sur un environnement Cloud Computing, Wifi, bases de données, applications...
4. Comprendre les techniques avancées de cryptographie
5. Labo complet regroupant :
   L'ensemble des aspects sécuritaires visant à surveiller, détecter une anomalie, permettre de la contrer tout en assurant la continuité du/des service(s)
   Les techniques de hacking permettant d'anticiper les failles d'un système
   Les bonnes pratiques à mettre en œuvre

750 € / ttc | **3** jours

COMPRENDRE LA CYBER SÉCURITÉ CISCO

Description :

Cette formation fournit un premier pas précieux pour acquérir les connaissances et les compétences nécessaires pour travailler avec une équipe « SOC » (Security Operations Center). Vous y parcourrez tous les outils modernes (SIEM) dans le domaine excitant et croissant de la cyber sécurité. Avec cette formation de quatre jours, vous apprendrez à mettre en place une « base line » pour la réalisation de la corrélation et du forensic.

Objectifs :

- Comprendre le fonctionnement d'un SOC
- Répondre à un incident technique de sécurité
- Établir une fiche de corrélation

Prérequis :

- Avoir une connaissance des réseaux informatiques (niveau Cisco CCENT) ou disposer d'une expérience équivalente

Contenus :

1. Identifier les vecteurs d'attaque
2. Comprendre la méthodologie du hacker
3. Développer la méthodologie de défense
4. Identifier les « outils » du hacker
5. Utiliser le CVSS 3.0
   - Les vecteurs
   - La complexité
   - Les privilèges
   - L'interaction avec l'utilisateur
   - Le champ d'application
   - Exemples pratiques d'utilisation
6. Définir un SOC et ses procédures
7. Utiliser le « SIEM » : exemples concrets
8. Réaliser une analyse de corrélation et forensic
9. Répondre à un incident
10. Investigations complémentaires

4 jours | **1000 € / ttc**

CISCO CCNA SECURITY

Description :

Parmi les constructeurs IT, *Cisco* n'est certainement plus à présenter. Leader mondial dans le matériel et les solutions télécom, on le retrouve en effet dans de nombreuses architectures informatiques d'entreprises. Cette formation de quatre jours vous permettra de maîtriser les technologies de sécurité de base de type *Cisco* mais aussi de gérer l'installation, le dépannage et la surveillance des périphériques réseaux afin de maintenir l'intégrité, la confidentialité et la disponibilité des données et des dispositifs mis en place.

Objectifs :

- Sélectionner les bons dispositifs réseaux sécurisés en fonction des besoins de l'infrastructure
- Configurer les accès et la sécurité des dispositifs sélectionnés
- Connaître les méthodes d'adressage IP
- Configurer un IPS Cisco
- Maîtriser les ACL
- Utiliser Cisco SDM

Prérequis :

- Avoir suivi et terminé les quatre modules du cursus Cisco Netacad CCNA ou disposer d'une expérience équivalente

Contenus :

1. Comprendre les concepts de sécurité
2. Comprendre les menaces et leurs principes
3. Découvrir la cryptographie
4. Sécuriser les différents accès
5. Comprendre et mettre en œuvre le modèle AAA
6. Implémenter l'authentification 802.1X
7. Implémenter l'authentification de type RADIUS
8. Comprendre la sécurité dans une architecture BYOD
9. Comprendre l'architecture d'une infrastructure LAN en 3 couches
10. Sécuriser la couche d'accès
    - Les attaques possibles
    - La réduction des risques
11. Sécuriser les protocoles de routages
12. Sécuriser le management des unités
13. Comprendre le principe du VPN
    - Le « remote » VPN
    - Le « site à site » VPN
    - Le framework IPSec
14. Comprendre le principe du firewall
    - La mise en œuvre d'un firewall
15. Comprendre le principe de IPS/IDS
    - Les signatures et les catégories
    - Le filtre URL
16. Mettre en œuvre de la fonction IPS/IDS dans un router
17. Découvrir le Cisco ASA
    - Le context-base (CBAC)
    - La zone-base firewall (ZBF)

1000 € / ttc | **4** jours

STOCKAGE

SÉCURISER DES BASES DE DONNÉES

Description :

L'Internet des Objets (IoT) et le *Big Data* nous noient aujourd'hui littéralement dans des quantités astronomiques de données. Ces productions et consommations quotidiennes de données nécessitent des bases de données de plus en plus fonctionnelles et accessibles. Cette formation d'un jour vous donnera toutes les clés pour sécuriser vos bases de données devenues si cruciales.

Objectifs :

- Comprendre une approche 360° de la sécurité autour des bases de données
- Sécuriser des données sensibles (chiffrement)
- Gérer efficacement des comptes utilisateurs (identification et authentification)
- Gérer des correctifs de sécurité

Prérequis :

- Connaissances élémentaires relatives aux bases de données
- Connaissances élémentaires des systèmes d'information

Contenus :

1. Mettre en œuvre une sécurité efficace : méthodologie
2. Sécuriser les accès
3. Créer des rôles et des autorisations (identification et authentification)
4. Chiffrer des données
5. Protéger les accès aux données sensibles
6. Partager les données
7. Configurer les outils d'audits pour monitorer les tentatives d'intrusions

1 jour	250 € / ttc

WINDOWS SERVER SECURITY

Description :

La solution *Windows Server* de *Microsoft* compte parmi les plus répandues dans les systèmes d'exploitation pour serveurs en entreprise. Cette formation de trois jours vous permettra de sécuriser des environnements *Microsoft* (clients/serveurs). Vous serez capable d'identifier les problèmes potentiels et de mettre en œuvre les solutions pour garantir un environnement fonctionnel et pérenne.

Objectifs :

- Sécuriser l'ensemble des plateformes Windows Server dans un réseau
- Sécuriser l'environnement Windows Server
- Sécuriser les communications entre les différentes machines Windows
- Contrôler et maintenir un environnement pérenne

Prérequis :

- Maîtriser l'administration de réseaux « Windows »
- Avoir des connaissances des réseaux informatiques

Contenus :

1. Découvrir la sécurité
2. Comprendre le modèle de sécurité Windows
3. Sécuriser l'authentification et le logon (Kerberos, NTLM...)
4. Sécuriser des fichiers et partager des ressources
5. Sécuriser l'Active Directory
6. Group Policies (Distributed Security Services)
7. Cryptographie et Microsoft PKI
8. Implémenter la sécurité du réseau Windows (VPN...)
9. Techniques de contrôle

750 € / ttc

3 jours

SÉCURISER LES SERVEURS LINUX

Description :

Les systèmes et technologies *Open Source* se répandent de plus en plus dans l'univers des entreprises mais aussi au sein des administrations publiques. Cette formation de trois jours vous permettra de sécuriser de manière optimale des serveurs de type *Linux*.

Objectifs :

- Comprendre la cryptographie sous Linux
- Sécuriser des serveurs informatiques
- Effectuer des audits

Prérequis :

- Avoir des connaissances élémentaires des environnements Open Source
- Avoir des connaissances élémentaires des réseaux informatiques
- Être familiarisé avec l'utilisation d'une interface en ligne de commande (CLI)

Contenus :

1. Découvrir la sécurité informatique
2. Comprendre la cryptographie sous Linux
3. Implémenter une sécurité locale
   - Les utilisateurs
   - Le système de fichiers
   - Les ACL
4. PAM (Pluggable Authentication Module)
5. Découvrir Selinux
6. Comprendre le protocole SSH sous Linux
7. Comprendre les PKI et les SSL
8. Implémenter l'authentification de type Kerberos
9. Implémenter l'authentification de type RADIUS
10. Mettre en place les firewalls
    - Le Kernel
    - Les firewalls externes
11. Sécuriser les services serveurs et réseaux
12. Effectuer des audits de sécurité
13. Exemple avec un serveur LAMP

3 jours | **750 € / ttc**

APPLICATIONS

SÉCURISER DES APPLICATIONS WEB

Description :

Si la sécurité informatique s'applique au monde des réseaux et de l'infrastructure, elle intervient également dans le développement des applications. Cette formation de trois jours vous permettra de manière pragmatique de sécuriser, dès sa conception, une application web afin de garantir son bon fonctionnement lors de son utilisation.

Objectifs :

- Aborder les bonnes pratiques liées au développement sécurisé d'applications
- Connaître les menaces et vulnérabilités existantes pour mieux y faire face

Prérequis :

- Avoir des connaissances dans un langage de programmation

Contenus :

1. Tour d'horizon des menaces et vulnérabilités liées aux applications web
2. Renforcer la sécurité
   - Les firewalls
   - Les filtres
   - L'empreinte
   - La signature
   - Le chiffrement
   - Les SSL et PKLI
   - L'authentification http et le certificat
3. Sécuriser des applications web
4. Contrôler la sécurité mise en place
5. Gérer la sécurité mobile
6. Laboratoires, travaux pratiques

3 jours	750 € / ttc

SÉCURISER DES APPLICATIONS .NET

Description :

Le langage de programmation *.NET* permet de rendre des applications facilement portables sur Internet. Cette formation de trois jours vous enseignera de manière pragmatique les techniques pour sécuriser, dès sa conception, une application *.NET*.

Objectifs :

- Utiliser les fonctionnalités des sécurités intégrées au framework .NET
- Mettre en œuvre le chiffrement et la signature des données

Prérequis :

- Avoir des connaissances en développement .NET
- Avoir une expérience dans le domaine du développement

Contenus :

1. Cryptographier : rappel de base
2. Comprendre le chiffrements, le hash et la signature des données en .NET
3. Comprendre l'infrastructure PKI
4. Définir les certificats
5. Sécuriser des services Web
6. Implémenter les certificats de serveurs SSL
7. Comprendre l'API « Data Protection »
8. Découvrir les outils de sécurité et d'audit
9. Laboratoires, travaux pratiques

750 € / ttc

3 jours

GOUVERNANCE

PRIVACY/SECURITY BY DESIGN & BY DEFAULT

RGPD/GDPR, CONCRÈTEMENT ON COMMENCE PAR QUOI ?

Description :

L'entrée en vigueur en mai 2018 du nouveau « Règlement Général sur la Protection de Données » (RGPD) impacte toutes les entreprises. Chacune d'entre elles doit se mettre en conformité face à leurs nouvelles obligations européennes. Mais par où commencer ? Cette formation d'un jour démystifiera les principes du RGPD/GPDR et vous aidera à établir un plan simple de mise en œuvre avec lequel vous repartirez en fin de journée. Divisée en deux temps, théorie en matinée et pratique l'après-midi, cette formation vous donnera toutes les clés pour vous faciliter la tâche !

Objectifs :

- Comprendre ce qu'est le RGPD/GDPR et quels en sont les impacts
- Élaborer une feuille de route pour démarrer la mise en conformité d'une entreprise
- Échanger sur les bonnes pratiques et les modèles de documents fournis

Contenus :

1. Mettre en contexte le RGPD/GDPR
   - L'historique et son évolution
   - Les définitions et le cadre
   - Les enjeux
   - Les droits de la personne
   - Les obligations pour les organisations
2. Découvrir le règlement RGPD/GDPR
   - Les principes
   - L'applicabilité
   - Le droit des personnes concernées
   - Le consentement
   - Le droit à l'oubli
   - La portabilité des données
   - La licéité du traitement
   - La conservation des données
3. Identifier un Délégué à la Protection des Données (DPD)
4. Comprendre les 6 principes de protection des données
5. Comprendre les impacts sur la vie privée
6. Gérer des risques
7. Appliquer le « Privacy by design »
8. Que faire en cas d'incident ?
9. Exemples concrets liés à l'activité d'une PME
10. Ateliers pratiques et foire aux questions

GOUVERNANCE

1 jour	250 € / ttc

FONDAMENTAUX DE LA CYBER SÉCURITÉ

Description :

La sécurité fait partie intégrante de l'environnement de travail d'un administrateur réseaux et systèmes. Celle-ci doit être pensée et intégrée dans les premières phases de la conception des réseaux et des systèmes, et ce, bien avant leurs mises en œuvre. Pour ce faire, il est impératif de comprendre les concepts de base et avancés de la sécurité. Cette formation de deux jours vous permettra d'évaluer la pertinence des protections ou des contre-mesures mises en place.

Objectifs :

- Analyser et mieux comprendre ce qu'est l' « IT Security »
- Comprendre la méthodologie « risk approach » et les méthodes d'évaluation de celui-ci (ex. Octave, Cobit, ISO2700x...)
- Cerner les menaces qui nous environnent et les attaques subies continuellement par les réseaux et les systèmes
- Mettre en œuvre une approche sécurité efficace et appropriée dans un environnement réseau et système (CSP, Security wheel...)

Contenus :

1. Construire un « Security from scratch »
   - La définition de la sécurité
   - Les trois « A » de la sécurité
   - L'évaluation des risques (ISO2700x, Cobit, Mehari, NIST...)
   - Les menaces
   - Les politiques de sécurité
   - Les méthodes générales d'attaque
   - Les contre-mesures de sécurité
2. Découvrir la cryptographie
   - Son historique
   - Les algorithmes de cryptographie
   - Les PKI
3. Les autres aspects de la sécurité
   - La sécurité Hardware
   - La sécurité Infrastructure
   - Le boot process
   - Les backups
   - Le plan de reprise d'activité (DRP & BCP)
   - Les programmes anti-virus/anti-malware
   - Les procédures de sécurité

500 € / ttc | **2** jours

ISO 2700x : COMPRENDRE LES NORMES

Description :

La famille de normes ISO 2700x aide les organisations à assurer la sécurité de leurs informations. Elles facilitent notamment la sécurisation des données financières, des documents soumis à la propriété intellectuelle, des informations relatives au personnel ou des données qui vous sont confiées par des tiers.
La norme ISO/IEC 27001, qui expose les exigences relatives aux systèmes de management de la sécurité des informations (SMSI), est la norme la plus célèbre de cette famille. Il existe plus d'une douzaine dans la famille ISO/IEC 27000. Cette formation de trois jours vous en donnera une grille de lecture précise et efficace.

Objectifs :

- Comprendre le Système de Management de la Sécurité de l'Information (SMSI)
- Comprendre toutes les normes (vue d'ensemble) de la famille ISO 2700x

Contenus :

1. Découvrir les normes ISO 2700x
   - Qu'est-ce qu'une norme ?
   - La finalité d'une norme
   - ISO/IEC 27000 – liste des normes
2. Comprendre la famille des normes ISO 2700x
3. Identifier les points clé de la sécurité des systèmes d'informations
4. S'habituer aux bonnes pratiques
5. Atelier récapitulatif

3 jours | **750 € / ttc**

ÉVALUATION ET GESTION DES RISQUES

Description :

Une politique de cyber sécurité efficace repose sur une évaluation des risques informatiques réalisée en amont de son implémentation. Cette formation de trois jours vous donnera toutes les clés pour maîtriser les méthodes et outils qui vous permettront de mener à bien votre analyse des risques.

Objectifs :

- Maîtriser les éléments fondamentaux relatifs à la gestion des risques informatiques
- Sensibiliser à la gestion des risques pour les systèmes d'information
- Comprendre et maîtriser les différents outils et méthodes utilisés dans les entreprises

Prérequis

- Avoir des connaissances de base dans la gestion des risques informatiques

Contenus :

1. Découvrir la gestion des risques
   - Le concept de gestion des risques
   - Le gestion des risques définie par ISO17799
   - La sécurisation des systèmes informatiques
   - Le budget alloué à la sécurisation
   - La crédibilité du système
   - La multiplicité des méthodes de calcul (plus de 200 méthodes)
2. Comprendre les fondements de la gestion des risques
   - Les concepts de la gestion des risques
   - Les processus de la gestion des risques
   - Les différentes zones de risque
3. Choisir la méthode de gestion de risques
   - Rapide panorama des 200 méthodes
   - Le CIGREF et le Club de la Sécurité de l'Information français (CLUSIF)
   - Les méthodes européennes
   - La méthode EBIOS
   - La méthode MEHARI
   - La méthode OCTAVE
4. Comparer trois méthodes de gestion des risques
   - La démarche globale EBOIS (ISO 15408 – 17799)
   - Les trois phases de la méthode OCTAVE
   - Organisationnelle
   - Technologique
   - Développement de la stratégie
   - La méthode MEHARI
   - La classification des méthodes
   - L'analyse des enjeux
   - L'audit de la sécurité
   - L'analyse des situations
   - Le plan d'action
5. Comprendre la vue des constructeurs (Cisco)
   - Le SAFE Network Security Fundation (NSF)
   - Le concept SAFE
   - Le Sans Institute - Spunk
   - Le Top 20 Critical Security Control (CSC)
6. Étude d'un cas pratique simple et utilisation des « top 20 CSC »

750 € / ttc | **3** jours

NOS ATELIERS
NOS CAUSERIES

Le Centre de compétence Technobel propose de nombreuses méthodes d'acquisition de nouvelles compétences. Outre une offre de formation dite traditionnelle, Technobel propose en effet des ateliers pratiques et des causeries qui, sous des formes interactives, vous permettent de comprendre, maîtriser et appliquer directement de nouveaux concepts, de nouvelles théories et technologies.

Les ateliers pratiques ont ainsi pour objectif de recréer, lors de laboratoires d'exercices, des situations concrètes susceptibles d'être rencontrées sur le terrain. Ces laboratoires fournis d'équipements de pointe sont aussi des possibilités pour les professionnels de se mettre à niveau et d'augmenter leurs compétences techniques.

Les causeries proposées dans ce catalogue, quant à elle, visent à dresser le portrait de thématiques particulières et variées. Le ton de ces causeries, volontairement décontracté, n'enlève rien à la qualité et à l'expertise des propos qui y sont tenus. Sorte de « mini-conférences » interactives, elles sont également l'occasion pour les participants de poser leurs questions et d'entretenir des débats réfléchis avec de nombreux experts.

Découvrez dans les pages qui suivent une liste non exhaustive de thématiques qui peuvent être abordées dans nos ateliers pratiques et dans nos causeries.


3m

NOS ATELIERS

Mettre en œuvre un Security Operation Center (SOC)	3 jours
Comprendre l'Ethical Hacking par la pratique	3 jours
Mettre en place une solution de protection (firewall/proxy) Linux	3 jours
Construire un outil Pentest gratuit sur Raspberry Pi	2 jours

NOS CAUSERIES

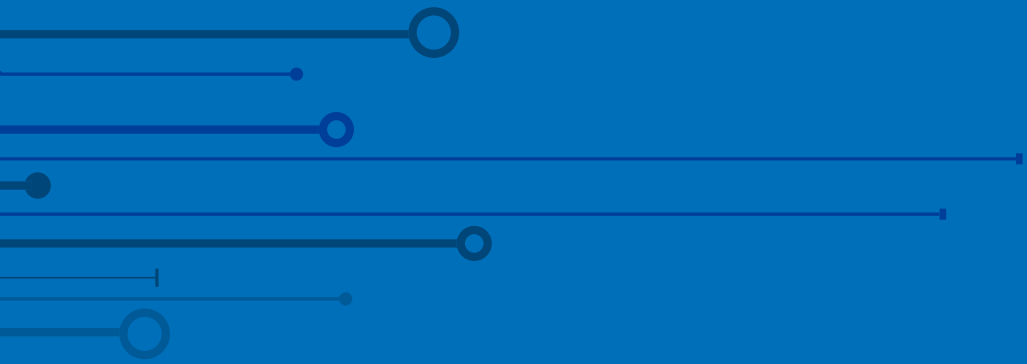
Comprendre le RGPD/GDPR	15 min.
RGPD/GDPR – Un levier pour votre transformation numérique ?	30 min.
La cyber criminalité, quelles conséquences pour les PME ?	30 min.
Pensez votre cyber sécurité Agile, non intrusive et au service de vos utilisateurs	30 min.
La sécurité du Blockchain : évolution ou révolution ?	30 min.

Les listes reprises précédemment ne sont que quelques exemples de thématiques pouvant être abordées au cours d'ateliers et de causeries. L'expertise développée et reconnue de Technobel permet en effet d'élargir facilement les champs d'intervention.

Des solutions crées « sur mesure » pour votre organisation sont également envisageables afin de répondre au mieux à vos attentes et besoins.

N'hésitez pas à nous contacter via le n° gratuit **0800 188 22** ou via l'adresse mail **entreprises@technobel.be**.

www.enmieux.be
FEDER–FSE
L'UNION EUROPÉENNE ET LA WALLONIE
INVESTISSENT DANS VOTRE AVENIR
Wallonie
proximus
LE FOREM
Techn.bel
Centre de Compétence



Techno.bel

Allée des Artisans 19
5590 CINEY
0800 188 22
entreprises@technobel.be
www.technobel.be