Catalogue de formations Expinfo

Expinfo

\\Your Cybersecurity Expert\\

2025

La cybersécurité, plus que jamais une priorité

Véritable **problème de société**, la **cybercriminalité** est en pleine **expansion** et concerne **tout le monde** (tous types de systèmes, organisations, petites et grandes entreprises).

Que ce soit pour la **protection de vos informations** clients ou financières, la sécurité de vos opérations, la garantie de la propriété intellectuelle, ou la **sécurité** de toutes autres données sensibles, **votre système doit être protégé**. La sécurité de ces informations est **fondamentale**.

En mai 2018, les entreprises deviennent pénalement responsables.

Suite aux nouveaux textes législatifs européens RGPD, les entreprises n'ayant pas sécurisé leur infrastructure informatique s'exposent à des sanctions pouvant aller jusqu'à 4% de leur chiffre d'affaires.

58 k€	• Le coût médian d'une cyberattaque en France. [Asteres 2023]
27%	• On recense une perte moyenne de 27 % des chiffres d'affaires dans les PME suite à une cyberattaque. [CESIN 2022]
60%	• 60% des PME victimes de cyberattaques ne parviennent pas à remonter la pente et font faillite dans les 18 mois après l'attaque. [CESIN 2022]
95%	• Dans 95% des cyber-attaques, la faille vient d'une erreur humaine. L'humain reste au cœur de tout. [Étude de IBM]

Nos formations

Expinfo vous accompagne

La cybersécurité est l'affaire de chacun. Expinfo vous accompagne depuis la sensibilisation de tous vos collaborateurs, à la formation personnalisée de vos équipes techniques. Expinfo propose également l'organisation de conférences.

Expinfo
\\Votre Expert Cybersécurité\\

Liste des formations (liste non exhaustive, détails ci-dessous) :

FOR01 : L'essentiel de la sécurité informatique	5
FOR02 : Tous les fondamentaux de la sécurité informatique	6
FOR03 : Sécuriser son système d'information	7
FOR04 : Gérer la sécurité au sein d'une organisation	8
FOR05 : Formation RSSI	9
FOR06 : Test d'intrusion	10
FOR07 : Réponse sur incident et investigation numérique	11
FOR08a : Formation RGPD	12
FOR08b : Formation RGPD partie juridique	13
FOR09a : Consultant en cybersécurité	14
FOR09b : Consultant-Formateur en cybersécurité	15
FOR09c : Consultant-Formateur-Expert en cybersécurité	16
FOR09 : Atelier de travail cyberkit	17
FOR10 : Jeu sérieux sur la cybersécurité	18
FOR11 : Sensibilisation au phishing (hameçonnage) et pièges classiques	19
FOR20-CPF : Piloter la cybersécurité d'une structure	20
Conférences	21

Tarifs

Le tarif de base est de : 1500€HT/jour, quel que soit le nombre de participants, sauf pour FOR09, FOR10 et FOR11.
En fonction du nombre de jours de formation acheté, les prix à la journée sont dégressifs.
Contact commercial pour tout renseignement ou devis :

Sébastien Salito
+33 7 67 01 73 98
commercial@expinfo.fr

Modalités pédagogiques et logistiques

Notre formateur s'adaptera aux systèmes informatiques et au matériel existant pour la formation.

L'entreprise cliente garantie que le matériel est conforme en matière de sécurité. Elle se porte responsable d'établir, de diffuser et de porter à la connaissance des stagiaires, les instructions et consignes de sécurité incendie.

En cas de formation à distance, le formateur pourra interdire l'usage des vidéos ou photos prisent pendant la formation.

Les repas des stagiaires ne sont pas compris dans ce forfait.

Le client doit informer le formateur d'une adaptation éventuelle de la formation, si un stagiaire est en situation de handicap.

Voici les modalités générales applicables à toutes les formations dispensées par Expinfo :

Lieu	• Dans notre salle de formation - sur site client - en visio
Logistique et pédagogie	• Les supports seront distribués à tous les participants à l'issue de la formation
Validation	• Fiche d'émargement, attestation de fin de stage
Moyens	• Les stagiaires utilisent leur environnement de travail (PC, logiciels, etc.) • Le formateur utilise le système de projection du client • Les moyens sont étudiés avec l'entreprise cliente
Date	• A définir

Organisme de formation

Expinfo est un organisme de formation enregistré sous le N° 84730202873 auprès du préfet de région Auvergne-Rhône-Alpes. Anciennement « Datadock », **Expinfo** est maintenant **certifié QUALIOPI** par l'AFNOR. Cette certification atteste de formations de qualité, permettant d'être référencé par les organismes financeurs.
De ce fait, nos **formations** sont **finançables par votre OPCO**.

Qualiopi processus certifié

La certification qualité a été délivrée au titre des catégories d'actions suivantes :
ACTIONS DE FORMATION

Satisfaction client sur l'année 2024 :

4,8 sur 5

FOR01 : L'essentiel de la sécurité informatique

L'essentiel pour être un utilisateur averti des outils informatiques tant professionnels que personnels. Cette formation s'adresse à tous les collaborateurs d'une entreprise.

Public	• Utilisateur informatique et tout public
Durée	• 1 jour
Prérequis	• Aucun niveau minimum n'est exigé pour suivre cette formation, il est cependant recommandé d'être à l'aise avec l'outil informatique
Compétences visées	• Comprendre les grands principes de cybersécurité • Identifier les vulnérabilités d'un système d'information • Connaître les principales menaces et savoir comment s'en protéger

1) La sécurité des systèmes d'information
   - ✓ Notions et évolution de la SSI
   - ✓ Les parties prenantes
   - ✓ Focus sur les données

2) Menaces, vulnérabilités, attaques
   - ✓ Les notions
   - ✓ Panorama des attaques
   - ✓ Autres types de menaces

3) Les 10 règles d'hygiène informatique
   - ✓ Règles simples pour éviter la quasi-totalité des attaques informatique !

FOR02 : Tous les fondamentaux de la sécurité informatique

Formation très complète pour être un utilisateur averti des outils informatiques tant professionnels que personnels. Cette formation s'adresse à tous les collaborateurs d'une entreprise. Dans ce cours vous allez découvrir les techniques des pirates pour les déjouer et les éviter !

Public	• Utilisateur informatique et tout public
Durée	• 3 jours
Prérequis	• Aucun niveau minimum n'est exigé pour suivre cette formation, il est cependant recommandé d'être à l'aise avec l'outil informatique
Compétences visées	• Comprendre les grands principes de la sécurité informatique • Connaître les principales menaces, maîtriser internet et les outils • Savoir se protéger, configurer ses appareils, et adopter les bonnes pratiques

1) La sécurité des systèmes d'information
   - ✓ Notions et évolution de la SSI
   - ✓ Les parties prenantes
   - ✓ Focus sur les données

2) Menaces, vulnérabilités, attaques
   - ✓ Les notions
   - ✓ Panorama des attaques

3) Les 10 règles d'hygiène informatique
   - ✓ Règles simples pour éviter la quasi-totalité des attaques informatique !

4) L'authentification
   - ✓ Le principe de l'authentification
   - ✓ Les attaques d'authentification
   - ✓ Sécuriser et gérer ses mots de passe
   - ✓ Notions de cryptographie

5) Comprendre internet
   - ✓ Présentation d'Internet
   - ✓ La navigation web
   - ✓ La messagerie électronique et messagerie instantanée
   - ✓ Les réseaux sociaux

6) Sécurité du poste de travail et nomadisme
   - ✓ Les mises à jour
   - ✓ Configuration de base
   - ✓ Configuration complémentaire
   - ✓ Les périphériques amovibles

7) Perspectives et réflexions
   - ✓ Un domaine d'avenir
   - ✓ Exemples de challenges à venir

FOR03 : Sécuriser son système d'information

Vous voulez apprendre à sécuriser une infrastructure informatique en utilisant des méthodes simples et rapides ? Cette formation très complète vous permet d'administrer la sécurité de votre système informatique.

Public	• Technicien/responsable informatique et administrateur systèmes et réseaux
Durée	• 2 jours
Prérequis	• Expérience confirmée comme technicien informatique
Compétences visées	• Savoir sécuriser son système d'information et ses locaux • Appliquer une PSSI (Politique de Sécurité des Systèmes d'Informations) • Connaître les principales méthodes de hacking

1) La sécurité des systèmes d'information
   - ✓ Menaces, vulnérabilités, attaques
   - ✓ L'authentification
   - ✓ Sécurité du poste de travail et nomadisme
   - ✓ Sécurisation d'un réseau
   - ✓ Les bases de la cryptographie
   - ✓ La sécurité des applications web

2) Les 10 règles d'hygiène informatique pour les utilisateurs
   - ✓ Règles simples pour éviter la quasi-totalité des attaques informatique !

3) Les 42 mesures pour renforcer la sécurité de son SI
   - ✓ Sensibiliser et former
   - ✓ Connaître son système d'information
   - ✓ Authentifier et contrôler les accès
   - ✓ Sécuriser les postes
   - ✓ Sécuriser le réseau
   - ✓ Sécuriser l'administration
   - ✓ Gérer le nomadisme
   - ✓ Maintenir le système d'information à jour
   - ✓ Superviser, auditer, réagir

4) Perspectives et réflexions
   - ✓ Un domaine d'avenir
   - ✓ Exemples de challenges à venir

FOR04 : Gérer la sécurité au sein d'une organisation

Cette formation permet de donner les clés de décisions aux collaborateurs en charge de la sécurité informatique. Elle permet d'avoir une vue globale de la sécurité de son système d'information.

Public	• Professionnel IT en charge de la sécurité du système d'information
Durée	• 1 jour
Prérequis	• Connaissance des protocoles et des équipements d'un SI
Compétences visées	• Comprendre les différents niveaux de sécurité • Savoir intégrer la sécurité dans ses projets • Se préparer aux difficultés liées à la sécurisation

1) Intégrer de la sécurité au sein d'une organisation
   - ✓ Panorama des normes ISO 2700x
   - ✓ Système de Management de la Sécurité de l'Information (27001)
   - ✓ Code de bonnes pratiques pour le management de la sécurité de l'information (27002)
   - ✓ Gestion des risques (27005)
   - ✓ Classification des informations
   - ✓ Gestion des ressources humaines

2) Intégrer la sécurité dans les projets
   - ✓ Sécurité dans l'ensemble du cycle de vie d'un projet
   - ✓ Sécurité prise en compte en fin de développement
   - ✓ Approche par l'analyse et le traitement du risque
   - ✓ Plan d'action SSI

3) Difficultés liées à la prise en compte de la sécurité
   - ✓ Compréhension insuffisante des enjeux
   - ✓ Implication nécessaire de la direction
   - ✓ Difficulté pour faire des choix en toute confiance
   - ✓ Délicat arbitrage entre commodité et sécurité
   - ✓ Suivre l'évolution des technologies
   - ✓ Frontières floues entre sphères professionnelle, publique, et privée

4) Les métiers en cybersécurité
   - ✓ Positionnement des métiers au sein des organisations
   - ✓ Cartographie des métiers et compétence
   - ✓ Profils et carrières
   - ✓ Perspectives d'embauche

FOR05 : Formation RSSI

Vous devenez « Responsable de la Sécurité des Systèmes d'Information » ? Vous voulez être guidé pour gagner en efficacité ?

Cette formation personnalisée vous apportera une vision complète des fonctions de RSSI dans votre société et des attentes de votre organisation sur ce rôle. Les connaissances indispensables à la prise de fonction du poste, un retour d'expérience sur les chantiers et la démarche à mettre en œuvre seront détaillés par notre formateur expert en sécurité du SI.

Public	• RSSI, futurs RSSI, responsables sécurité à la production, correspondant local de sécurité SI, DSI, auditeurs SSI
Durée	• 5 jours
Prérequis	• Une expérience au sein d'une DSI en tant qu'informaticien ou une bonne culture générale des systèmes d'information
Compétences visées	• Acquérir les compétences indispensables à l'exercice de la fonction responsable de la sécurité des systèmes d'information • Apprendre toutes les bases de la cybersécurité

1) Intégrer de la sécurité au sein d'une organisation
   - ✓ Panorama des normes ISO 2700x
   - ✓ Système de Management de la Sécurité de l'Information (27001)
   - ✓ Code de bonnes pratiques pour le management de la sécurité de l'information (27002)
   - ✓ Gestion des risques (27005)
   - ✓ Classification des informations
   - ✓ Gestion des ressources humaines

2) Intégrer la sécurité dans les projets
   - ✓ Sécurité dans l'ensemble du cycle de vie d'un projet
   - ✓ Sécurité prise en compte en fin de développement
   - ✓ Approche par l'analyse et le traitement du risque

3) Les 42 mesures pour renforcer la sécurité de son SI
   - ✓ Sensibiliser et former
   - ✓ Connaître son système d'information
   - ✓ Authentifier et contrôler les accès
   - ✓ Sécuriser les postes
   - ✓ Sécuriser le réseau
   - ✓ Sécuriser l'administration
   - ✓ Gérer le nomadisme
   - ✓ Maintenir le système d'information à jour
   - ✓ Superviser, auditer, réagir

4) Plan d'action SSI
   - ✓ Audit cybersécurité 360° et les 80/20

FOR06 : Test d'intrusion

Vous êtes ingénieur, administrateur système et réseaux, ou responsable informatique ?

Cette formation vous permettra de maîtriser pas à pas la méthodologie de conduite d'un test d'intrusion afin de déterminer le réel potentiel d'intrusion et de destruction d'un pirate sur un système d'information.

Public	• Professionnel IT en charge de la sécurité du système d'information, administrateur système et réseaux.
Durée	• 3 jours
Prérequis	• Bonne connaissances des bases de la sécurité informatique
Compétences visées	• Maîtriser les différents types d'attaques • Réaliser un test d'intrusion • Rédaction d'un plan d'action avec les correctifs à appliquer

1) Préparez votre test d'intrusion
   - ✓ Qu'est-ce qu'un test d'intrusion (pentest) ?
   - ✓ Maîtrisez les différents types de tests
   - ✓ Découvrez les systèmes d'exploitation adaptés
   - ✓ Configurez votre environnement LAB
   - ✓ Préparez votre pentest

2) Réalisez votre test d'intrusion
   - ✓ Maîtrisez les attaques les plus courantes
   - ✓ Prévenez-vous des attaques plus complexes
   - ✓ Scannez les vulnérabilités d'un système
   - ✓ Testez le système cible avec des méthodes simples
   - ✓ Testez le système cible avec des méthodes complexes

3) Rédigez votre rapport de test d'intrusion
   - ✓ Proposez et inventoriez les mesures correctives
   - ✓ Rédigez votre rapport de test d'intrusion
   - ✓ Présentez votre rapport de test d'intrusion

FOR07 : Réponse sur incident et investigation numérique

Vous êtes expert en cybersécurité et vous souhaitez vous spécialiser en « réponse sur incident » et « Investigation numérique » ?

Cette formation vous fera plonger dans la méthodologie des enquêtes criminalistiques informatiques et la collecte de preuves.

Public	• Professionnel IT en charge de la sécurité du système d'information, administrateur système et réseaux ou experts en cybersécurité.
Durée	• 2 jours
Prérequis	• Niveau minimum de master en sécurité informatique ou expérience équivalente
Compétences visées	• Savoir réagir en cas de cyberattaque • Savoir identifier les traces laissées lors de l'intrusion dans un SI • Collecter correctement les preuves numériques

1) Réponse sur incident
   - ✓ Circonstances
   - ✓ Déroulement de l'intervention

2) La collecte
   - ✓ Arrivée sur site & Gestion de crise
   - ✓ Premiers reflexes
   - ✓ L'ordre de volatilité

3) Acquisition des données
   - ✓ Techniques d'acquisition
   - ✓ Techniques anti-forensique
   - ✓ Investigation sur l'OS (Windows, MacOS, linux, etc.)
   - ✓ Investigation sur le réseau
   - ✓ Investigation sur les Maliciels

4) Analyse en profondeur
   - ✓ Rechercher les IOCs
   - ✓ Identifier les TTPs
   - ✓ Rapport d'investigation numérique

FOR08a : Formation RGPD

Depuis le 25 mai 2018 toutes les entreprises et organismes doivent se conformer au « Règlement général sur la protection des données ». Cette formation permet de prendre en main les outils, méthodes et techniques pour se mettre en conformité.

Public	• Tout public, notamment futur délégué à la protection des données (DPO), chef d'entreprise, responsable juridique / informatique / qualité
Durée	• 2 jours
Prérequis	• Aucun niveau minimum n'est exigé pour suivre cette formation, il est cependant recommandé d'être à l'aise avec l'outil informatique
Compétences visées	• Maîtriser la réglementation et les missions du DPO • Savoir mettre en conformité son organisation • Etre capable de justifier de cette conformité

1) Comprendre la RGPD
   - ✓ Signification de RGPD
   - ✓ Objectifs et périmètre : un texte européen à portée mondiale
   - ✓ Que sont les "Données à caractère personnel"
   - ✓ A qui s'adresse cette nouvelle règlementation
   - ✓ Les risques juridiques et les sanctions
   - ✓ Les enjeux et les impacts pour votre entreprise

2) Maîtriser le traitement des données
   - ✓ Les nouveaux droits pour les résidents européens
   - ✓ Les nouvelles obligations pour le responsable du traitement et pour les sous-traitants
   - ✓ Quels changements sur votre système d'information

3) Définir un plan d'actions pour se mettre en conformité
   - ✓ DPO : rôles et responsabilités
   - ✓ Cartographier les données
   - ✓ Analyse d'impact
   - ✓ Les mesures organisationnelles et techniques
   - ✓ Préparer son plan d'actions
   - ✓ Les nouvelles règles de gestion de cybersécurité / informatiques

FOR08b : Formation RGPD partie juridique

Depuis le 25 mai 2018 toutes les entreprises et organismes doivent se conformer au « Règlement général sur la protection des données ». Cette formation permet de prendre en main les outils, méthodes et techniques pour se mettre en conformité juridique.

Public	• Tout public, notamment futur délégué à la protection des données (DPO), chef d'entreprise, responsable juridique / informatique / qualité
Durée	• 1 jour
Prérequis	• Aucun niveau minimum n'est exigé pour suivre cette formation, il est cependant recommandé d'être à l'aise avec les documents juridiques
Compétences visées	• Savoir mettre en conformité juridique son organisation • Etre capable de justifier de cette conformité juridique

1) Adaptation de la documentation contractuelle
   - ✓ Créer et adapter son registre des activités de traitement d'après la cartographie
   - ✓ Qualifier les acteurs (sous-traitant, responsable conjoint de traitement, etc.)
   - ✓ Identifier les risques au sein des contrats de ses sous-traitants
   - ✓ Mettre à jour ses propres contrats (sous-traitance, responsabilité conjointe)

2) Informer les personnes concernées
   - ✓ Rédiger sa ou ses politique(s) de confidentialité ainsi que les mentions d'information
   - ✓ Connaître les règles entourant la prospection

3) Encadrement des transferts de données
   - ✓ Définir les modalités de cession des données à des tiers
   - ✓ Encadrer les transferts de données hors UE (BCR et clauses contractuelles types)

Notre formatrice spécialisée : **Lamia EL FATH**

Titulaire d'un Master II de droit de l'innovation technique de l'Université Paris-Sud, d'un Mastère spécialisé en Droit des affaires internationales et management de l'ESSEC Business School et d'un LLM of European Law de l'Université de Nottingham (UK) ainsi que de deux diplômes universitaires de droit anglais et américain, forte de son expérience dans des départements de niche, de cabinets reconnus à Paris et Sophia-Antipolis, elle a créé son propre cabinet à Annecy exclusivement dédiée au droit du numérique et de la propriété intellectuelle.

Elle est membre de l'Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP).

Par ailleurs, elle enseigne en tant que chargée d'enseignement au sein de l'Université Catholique de Lyon.

FOR09a : Consultant en cybersécurité

Vous êtes motivé par un challenge dans l'un des domaines les plus porteurs du moment ? Vous souhaitez développer un business rentable et d'avenir ? Evoluer vers un métier passionnant et vivant ? C'est parfait ! Cette formation est faite pour vous ! Elle vous permettra de réaliser des prestations de cybersécurité !

Public	• Informaticiens motivés par la cybersécurité
Durée	• 3 jours + atelier de travail
Prérequis	• Connaisances de base des système & réseaux sur Linux, Windows client et Windows serveur
Compétences visées	• Maitriser les techniques et outils utilisés en cybersécurité • Etre capable de réaliser des prestations d'Audit Cybersécurité 360 et RGPD

1) Prise en main de la documentation
   - ✓ Administratif et juridique
   - ✓ Commercial

2) Audit Cybersécurité 360
   - ✓ Comprendre tous les points de contrôle
   - ✓ Utiliser les outils de scan
   - ✓ Générer le rapport

3) Audit RGPD et formation du DPO
   - ✓ Comprendre la méthodologie
   - ✓ Etude des documents

4) Atelier de travail
   - ✓ Mise en situation
   - ✓ Mise en pratique des prestations de cybersécurité

FOR09b : Consultant-Formateur en cybersécurité

Vous êtes motivé par un challenge dans l'un des domaines les plus porteurs du moment ? Vous souhaitez développer un business rentable et d'avenir ? Evoluer vers un métier passionnant et vivant ? C'est parfait ! Cette formation est faite pour vous ! Elle vous permettra de réaliser des prestations de cybersécurité !

Public	• Informaticiens motivés, pen-testeurs ou jeunes diplômés dans le domaine de la cybersécurité
Durée	• 4 jours + atelier de travail
Prérequis	• Connaisances de base des système & réseaux sur Linux, Windows client et Windows serveur
Compétences visées	• Maitriser les techniques et outils utilisés en cybersécurité • Etre capable de réaliser des prestations d'Audit Cybersécurité 360 et RGPD + sensibilisations + Campagnes de faux phishing

1) Prise en main de la documentation
   - ✓ Administratif et juridique
   - ✓ Commercial

2) Audit Cybersécurité 360
   - ✓ Comprendre tous les points de contrôle
   - ✓ Utiliser les outils de scan
   - ✓ Générer le rapport

3) Audit RGPD et formation du DPO
   - ✓ Comprendre la méthodologie
   - ✓ Etude des documents

4) Formation et conférence
   - ✓ Comment devenir formateur
   - ✓ Etude des supports

5) Campagnes de faux phishing
   - ✓ Créer des scénarios personnalisés
   - ✓ Utilisation des outils automatisés internes
   - ✓ Génération du rapport

6) Atelier de travail
   - ✓ Mise en situation
   - ✓ Mise en pratique des prestations de cybersécurité

FOR09c : Consultant-Formateur-Expert en cybersécurité

Vous êtes motivé par un challenge dans l'un des domaines les plus porteurs du moment ? Vous souhaitez développer un business rentable et d'avenir ? Evoluer vers un métier passionnant et vivant ? C'est parfait ! Cette formation est faite pour vous ! Elle vous permettra de réaliser des prestations de cybersécurité !

Public	• Informaticiens motivés, pen-testeurs ou jeunes diplômés dans le domaine de la cybersécurité
Durée	• 5 jours + atelier de travail
Prérequis	• Expérience en administration système & réseau sur Linux, Windows client et Windows serveur
Compétences visées	• Maitriser les techniques et outils utilisés en cybersécurité • Etre capable de réaliser des prestations d'Audit Cybersécurité 360 et RGPD + sensibilisations + Campagnes de faux phishing + tests d'intrusion + investigation • Etre capable de réaliser une expertise judiciaire selon le standard

1) Prise en main de la documentation
   - ✓ Administratif, juridique et commercial

2) Audit Cybersécurité 360
   - ✓ Comprendre tous les points de contrôle et utiliser les outils de scan
   - ✓ Générer le rapport

3) Audit RGPD et formation du DPO
   - ✓ Comprendre la méthodologie

4) Formation et conférence
   - ✓ Comment devenir formateur
   - ✓ Etude des supports
   - ✓ Réaliser des campagnes de faux phishing

5) Investigation forensique/légale
   - ✓ Préparer votre investigation numérique
   - ✓ Analyser les fichiers malveillants + dump mémoire + disque

6) Réponse suite à incidents
   - ✓ La méthodologie et utilisation des outils
   - ✓ Procédure pour traiter un incident de sécurité

7) Les Tests d'intrusion
   - ✓ Préparer un test d'intrusion et identifier les vulnérabilités
   - ✓ Utiliser les outils et applications de pentest

8) Devenir Expert judiciaire près la cour d'appel
   - ✓ Procédure et documents

9) Atelier de travail
   - ✓ Mise en situation
   - ✓ Mise en pratique des prestations de cybersécurité

FOR09 : Atelier de travail cyberkit

Public	• Informaticiens motivés par la cybersécurité
Durée	• **74 heures** d'atelier de travail
Prérequis	• Connaisances de base des système & réseaux sur Linux, Windows client et Windows serveur
Compétences visées	• Maitriser les techniques et outils utilisés en cybersécurité • Etre capable de réaliser des prestations d'Audit Cybersécurité 360 et RGPD

Ateliers pratiques et études de cas :

- ✓ La RGPD
- ✓ Réseau TCP/IP
- ✓ Configuration routage réseau
- ✓ Le modèle OSI
- ✓ Serveur DHCP
- ✓ Serveur DNS
- ✓ Windows Server (installation et configuration)
- ✓ Base Active Directory (centralisation et sécurisation de l'annuaire AD)
- ✓ Linux
  - Installation et configuration
  - Administration
- ✓ PowerShell
- ✓ Python
- ✓ Infrastructure
  - Sécurisation systèmes et application
  - La sécurité réseau et active directory
- ✓ Cybersécurité
  - Déroulement d'une attaque
  - Prévenir les cyberattaques
- ✓ Règles d'hygiène en cybersécurité

FOR10 : Jeu sérieux sur la cybersécurité

Envie de passer un moment convivial et plein de surprises ? Laissez-vous guider dans une dimension mêlant divertissement, formation, énigmes et partage. Cette formation ludique au format « jeu sérieux » s'adresse à tout un chacun afin d'apprendre les règles de base de cette nouvelle vie numérique, applicables tant au niveau professionnel que personnel. Un de nos experts sera votre maître des jeux !

Public	• Tout public - toute personne utilisant des outils numériques
Durée	• 0,5 jour
Prérequis	• Utiliser un ordinateur ou smartphone au travail
Compétences visées	• Connaître les principales règles d'hygiène informatique • Savoir reconnaître une menace • Savoir éviter les pièges des pirates
Tarif	• 2 000 € HT

1) Briefing (principes de la cybersécurité)
   - ✓ Mots de passe
   - ✓ Mises à jour
   - ✓ Session et droits
   - ✓ Sauvegarde
   - ✓ Wifi sécurisé
   - ✓ Smartphone
   - ✓ Nomadisme
   - ✓ Messagerie
   - ✓ Téléchargements
   - ✓ Paiement sur internet
   - ✓ Séparer pro et perso
   - ✓ Veiller à son identité numérique

2) Immersion pratique
   - ✓ Jeu sérieux encadré

3) Débriefing (10 règles d'hygiène informatique)
   - ✓ Règles simples pour éviter la quasi-totalité des attaques informatique !

FOR11 : Sensibilisation au phishing (hameçonnage) et pièges classiques

91% des cyberattaques commencent par un email innocent. C'est pourquoi, les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées, etc.).

Cette formation permet à tous les collaborateurs de savoir détecter ces attaques par phishing, de tester et apprendre à réagir de manière adéquate dans leur environnement habituel, et de connaître les principaux pièges des pirates.

Cette formation commence par un exercice pratique « fidèle à la réalité » de « campagne de faux phishing » sur les collaborateurs de votre entreprise. Nous nous basons entre autres sur des emails d'hameçonnage, typiques des cybercriminels, imitant les messages reçus au quotidien. Cette mise en situation permet de sensibiliser vos collaborateurs et votre équipe informatique et s'inscrit dans une démarche de formation et d'amélioration continue.

Il est important de prendre conscience que la sécurité informatique est comme une « chaîne », dont la solidité est équivalente à la solidité du plus fragile de ses maillons. Il est donc primordial que chacun puisse reconnaître et alerter ce type d'attaque.

Public	• Tout public - toute personne utilisant une messagerie
Durée	• 1 jour (Cas pratique + théorie)
Prérequis	• Aucun niveau minimum n'est exigé pour cette formation, il est cependant recommandé d'être à l'aise avec l'outil informatique.
Compétences visées	• Savoir reconnaître un email de phishing • Apprendre à réagir concrètement dans son environnement en cas d'attaque • Connaître les principaux pièges et savoir les éviter
Tarif	• 3 000€ HT

1) Cas pratique
   - ✓ Mise en situation

2) Retour d'expérience
   - ✓ Analyses statistiques
   - ✓ L'utilisation de la messagerie
   - ✓ Indices de détection de SPAM

3) Les 10 règles d'hygiène informatique
   - ✓ Règles simples pour éviter la quasi-totalité des attaques informatique !

FOR20-CPF : Piloter la cybersécurité d'une structure

Formation très complète pour piloter la cybersécurité au sein d'une structure. Dans ce cours vous allez parcourir les fondamentaux de la sécurité, comprendre comment établir un plan d'action approprié, et diffuser la notion de sécurité.

Public	• Chef d'entreprise TPE /PME, responsable de strcuture • Réfèrent cyber, responsable informatique, personne ressource,
Modalités	• 5 jours
Prérequis	• L'accès à la certification ne requiert pas d'expertise particulière. Les candidats ité un titre ou diplôme de niveau 5, ou 3 années d'expérience, ou justifier d'u niveau suffisant en informatique
Compétences visées	• Maîtriser les grands principes de la sécurité informatique • Piloter la sécurité de son système • Diffuser la sécurité au sein d'une organisation

1) Les fondamentaux de la sécurité informatique
   - ✓ La sécurité des systèmes d'information
   - ✓ Menaces, vulnérabilités, attaques
   - ✓ Les 10 règles d'hygiène informatique
   - ✓ Règles simples pour éviter la quasi-totalité des ques informatique !
   - ✓ L'authentification
   - ✓ Comprendre internet
   - ✓ Sécurité du poste de travail et noma me

1) Les 42 mesures pour renforcer la sécurité ystème
   - ✓ Connaître son système d'inf mation
   - ✓ Authentifier et contrôler les acc
   - ✓ Sécuriser les postes
   - ✓ Sécuriser le réseau
   - ✓ Sécuriser l'administration
   - ✓ Gérer le n ma
   - ✓ Maintenir le ystème nformation à jour
   - ✓ Supervis r, a liter, ré ir

2) Diffuser la sécuri sein d'une organisation
   - ✓ Se sibiliser ormer
   - ✓ Inte la sécurité au sein d'une organisation
   - ✓ écurité dans les projets
   - ✓ fficultés liées à la prise en compte de la sécurité
   - ✓ Les tiers de la cybersécurité et compétences transversales

Conférences

Les sujets touchant aux nouvelles technologies sont passionnants et en constante évolution.

Avec 20 ans d'expérience en informatique, et plus de 10 ans de travail avec le ministère de la justice en qualité d'expert judiciaire informatique auprès des tribunaux, Sébastien Salito intervient sur vos évènements pour apporter son éclairage sur les sujets d'actualité dans le numérique.

Public	• Tout public • Auditoire spécialisé
Durée	• De 30 à 90 minutes
Prérequis	• Variable selon le sujet et le public visé
Evènements	• Tables rondes et débats • Présentations et conférences

Sujets à la demande, comme par exemple :

- ✓ Le nouveau règlement NIS2
- ✓ Le RGPD, nouveau règlement européen sur la protection des données, quels changements ?
- ✓ La cybersécurité dans les TPE/PME
- ✓ 10 règles simples pour éviter les cyberattaques !
- ✓ Votre meilleur allié pour combattre la cybercriminalité : vous-même ?
- ✓ Cyberattaques, ransomware, phishing… Qu'est-ce que c'est ?
- ✓ Etes-vous bien protégés des cyberattaques ?
- ✓ Comment travailler en sécurité ?
- ✓ Protégez votre identité et vos données personnelles !
- ✓ Cybersécurité, à vous de jouer !
- ✓ Le DarkWeb
- ✓ L'intelligence artificielle
- ✓ Les Crypto-monnaies

Notes

Pourquoi travailler avec nous ?

*“ Je pense que le **sens du service**, la **confiance**, l’**éthique** et la **proximité** sont les clés pour construire une **relation pérenne** avec nos clients ”*

Expinfo s’engage à garantir une empreinte écologique minimum. Chaque année, Expinfo limite, réduit, ou compense ses émissions (achats, transports, déchets, énergie grise, énergies, etc.) pour atteindre le **zéro émission CO2 net.**

Avec un dévouement sans faille pour la sécurité des systèmes d’informations, Expinfo a fait de la **cybersécurité sa spécialité**.

Les collaborateurs de Expinfo possèdent toutes les **formations et certifications** les plus importantes dans le domaine pour mener à bien leurs missions :

PECB | ISO/IEC 27001 Lead Auditor

C|EH™ Certified Ethical Hacker

C|HFI™ Computer Hacking Forensic INVESTIGATOR

Partenaire de la Réserve Militaire Défense

EXPERT CYBER – Label Sécurité Numérique Cybermalveillance.gouv.fr – RÉPUBLIQUE FRANÇAISE

Pour toutes questions, n’hésitez pas à nous contacter

info@expinfo.fr | +33 4 58 14 08 50 | https://expinfo.fr