

PARCOURS DE CYBER SÉCURITÉ

Fondamentaux et Pratiques Avancées

Durée : 3 jours (soit 21h)

Organisée en intra

Maximum 8 participants par session



À QUI S'ADRESSE LA FORMATION

- **Public concerné** : Tous les utilisateurs souhaitant se former aux fondamentaux de la sécurité informatique
- **Prérequis** : aucun
- Toutes nos formations et bilans de compétences sont accessibles aux personnes en situation de handicap



LES OBJECTIFS DE LA FORMATION

À l'issue de la formation les stagiaires seront capables de :

- Comprendre les Enjeux de la Cybersécurité : identifier les menaces courantes et distinguer les principaux acteurs du domaine
- Protéger efficacement leur Environnement Informatique : mettre en œuvre les meilleures pratiques et outils pour assurer la sécurité des systèmes et des communications
- Gérer et répondre aux incidents avec efficacité : se préparer à des incidents de sécurité, intervenir rapidement et connaître les aspects légaux associés



AVANT LA FORMATION

- Auto-évaluation réalisée en amont



MÉTHODE PÉDAGOGIQUE

Méthode participative qui alternera des moments :

- D'apports théoriques amenés par le consultant sous forme de tuto simples, pratiques
- D'échanges entre les participants
- De mise en situation et jeux de rôle

Durant les journées de formation, la pédagogie s'appuiera sur les contextes professionnels des participants (un tour de table est réalisé). Ce fil conducteur permettra aux participants d'utiliser et de s'approprier l'ensemble des connaissances et des savoir-faire transmis



Jour 1 : Introduction à la cybersécurité

Matinée

- Accueil des participants
- Objectifs et enjeux de la formation
- Définition et importance de la cybersécurité
- Principaux risques et menaces (phishing, ransomware, attaques DDoS, etc.)

Après-midi

- Les fondamentaux des réseaux
- Protocoles, services et infrastructure
- Concepts de ports, VPN, pare-feu
- Les acteurs de la cybersécurité (hackers, hacktivistes, cybercriminels, etc.)
- Exercice pratique : Identifier une tentative de phishing

Jour 2 : Protéger son environnement

Matinée

- Bonnes pratiques de la sécurité informatique
- Mise à jour régulière des logiciels et systèmes
- Utilisation de mots de passe forts et gestionnaires de mots de passe
- Double authentification
- Sécurisation des communications
- HTTPS, SSL/TLS
- VPN et réseaux privés

Après-midi

- Sécurité des systèmes d'information
- Patch management
- Principe du moindre privilège
- Surveillance et détection des incidents
- Exercice pratique : Configuration sécurisée d'un poste de travail
- Présentation et utilisation d'outils de scan (ex: Nmap, Wireshark)

Jour 3 : Réponse aux incidents et prévention

Matinée

- Planification et réponse aux incidents
- Identifier et classer les incidents
- Processus de réponse aux incidents
- Aspects légaux de la cybersécurité
- Règlementations et normes (ex: RGPD)
- Signalement et gestion des violations de données

Après-midi

- Sensibilisation et formation du personnel
- Importance de la formation continue
- Rôles et responsabilités de chacun
- Exercice pratique : Simulation d'une attaque et réponse à l'incident
- Conclusion et perspectives : évolutions de la cybersécurité, Intelligence Artificielle en sécurité, etc.
- Evaluation de la formation et feedback des participants

Outils et Supports:

- Diaporamas et vidéos illustratives
- Exercices pratiques à réaliser sur ordinateurs
- Documentation remise à chaque participant
- Quizz et tests pour évaluer la compréhension



SUIVI ET ÉVALUATION

- Une fiche d'évaluation à chaud sera complétée par chaque participant à l'issue de la formation



VALIDATION

- Attestation de suivi de la formation remise à la fin de la formation, précisant la nature, les acquis et la durée de la formation



CONTACT

Nous contacter pour obtenir un devis dans le cadre de votre projet :
contact@hubconseil.fr

Pour plus de détails :

Référente pédagogique : Julia Langlade - **j.langlade@hubconseil.fr** – 06 29 60 46 96

Référente handicap : France Dupont - **f.dupont@hubconseil.fr** - 06 85 59 47 79

Référente technique : Marie Thouret - **m.thouret@hubconseil.fr** - 06 25 77 09 74

Hub conseil

Siège & bureaux 6 rue Emile Zola 69002 Lyon – France

contact@hubconseil.fr

SIRET 844 820 175 000 66 - SAS au capital de 20 000€ - RCS Lyon 844 820 175

Déclaration d'activité 84691725669