

## Souveraineté numérique et cybersécurité

Référence : **SECSOUV**

Durée : **1 jour (7 heures)**

Certification : **Aucune**

**Opcommerce**

### CONNAISSANCES PRÉALABLE

- Aucun prérequis

### PROFIL DES STAGIAIRES

- RSSI / CISO
- Fonction SSI
- Direction Générale
- DSI

### OBJECTIFS

- Comprendre les enjeux de la souveraineté numérique
- Identifier les enjeux de l'indépendance numérique de son organisation
- Comprendre les législations actuelles
- Identifier des ressources adaptées à son organisation
- Préparer l'indépendance numérique de son organisation

### CERTIFICATION PRÉPARÉE

- Aucune

### MÉTHODES PÉDAGOGIQUES

- Pédagogie active et participative : Alternance d'apports conceptuels et d'activités pratiques ; Études de cas concrets ; Travaux collaboratifs ; Évaluation continues et interactives
- Formats et adaptation selon le contexte de formation : Présentiel (inter Paris, Lyon, Nantes, Rennes, Toulouse, Pau/ intra partout en France) ; Évaluation de prestataires numériques selon des critères de souveraineté ; Construction d'un plan d'indépendance numérique ; Distanciel synchrone ; Distanciel asynchrone
- Dimension innovante et engageante : Serious game Le Choix Souverain ; Auto-diagnostic de souveraineté numérique ; Atelier fil rouge ; Suivi post-formation
- Moyens pédagogiques et techniques mobilisés : Plateforme Internet pour héberger les supports, quiz, ressources et capsule de révision ; Supports de formation numériques
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

### FORMATEUR

- Consultant-formateur expert en cybersécurité et gouvernance numérique, garantissant des apports à jour et un accompagnement individualisé

### MÉTHODES D'ÉVALUATION DES ACQUIS

- Avant la formation : test de positionnement ou de validation des prérequis
- Pendant la formation : Évaluations formatives sous diverses formes (exercices, quiz...)
- Fin de formation : Évaluation sommative ; Évaluation satisfaction
- Après la formation : Évaluation à froid, un mois après la session de formation
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

### CONTENU DU COURS

#### 1. Matinée (3h30) – Comprendre et cadrer la souveraineté numérique

#### 2. Définition et enjeux de la souveraineté numérique (1h45)

- Définitions clés : souveraineté, autonomie stratégique, indépendance numérique
- Les trois dimensions de la souveraineté : technologique, économique et politique
- Enjeux pour les entreprises : dépendance logicielle, maîtrise des données, sécurité des infrastructures
- État de l'art en France et en Europe : stratégie européenne du cloud, programmes Gaia-X, SecNumCloud, et Data Spaces
- 💡 *Étude de cas : analyse d'une dépendance critique (ex : migration forcée vers une plateforme étrangère)*

### 3. Protection des données et cadre réglementaire (1h45)

- Réglementations clés : RGPD, Data Governance Act, NIS2, LPM, DORA
- Impact du Cloud Act et des transferts internationaux de données
- Hébergement souverain, certification SecNumCloud, exigences de localisation
- 💡 *Exercice : cartographier les données sensibles de son organisation et leurs flux (hébergement, traitement, transfert)*

### 4. Après-midi (3h30) – Construire l'indépendance numérique de son organisation

#### 5. Indépendance numérique et choix des fournisseurs (1h15)

- Identifier les dépendances critiques : cloud, messagerie, cybersécurité, logiciels métiers
- Analyse des risques liés à la dépendance technologique
- Critères de choix d'un fournisseur souverain ou conforme aux exigences européennes
- 💡 *Atelier collaboratif : grille d'évaluation de la souveraineté d'un prestataire (juridique, technique, contractuel)*

#### 6. Cybersécurité et technologies clés (1h15)

- Lien entre souveraineté et cybersécurité : sécurité des infrastructures, gestion des identités, cryptographie, résilience
- Technologies clés : cloud souverain, chiffrement de confiance, blockchain, edge computing, IA éthique, open source sécurisé
- Panorama des acteurs français et européens de la cybersécurité
- 💡 *Exercice pratique : construction d'un plan d'action "Cybersécurité & indépendance numérique" pour son organisation*

#### 7. Conclusion – Préparer l'indépendance numérique (1h)

- Synthèse des enjeux stratégiques et leviers opérationnels
- Élaboration d'une feuille de route personnalisée : priorités à 3, 6 et 12 mois
- Ressources et accompagnements disponibles : ANSSI, DINUM, Bpifrance, France Num, Hub France IA
- 💡 *Quiz final / auto-évaluation des acquis*

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel:01.71.19.70.30) ou par mail à [referent.handicap@edugroupe.com](mailto:referent.handicap@edugroupe.com) pour vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible .