L’essentiel du cloud souverain

Prix : 750 €HT

Durée : 1 jour

Code de Référence : CSESS

Catalogue Cloud Native et DevOps

La souveraineté numérique est devenue un enjeu stratégique majeur pour les organisations publiques et privées. Face à la montée en puissance des législations extraterritoriales, telles que le Cloud Act ou le FISA, et aux exigences croissantes du RGPD et des réglementations européennes, choisir et piloter des solutions Cloud en toute maîtrise est devenu incontournable.

En une journée, cette formation donne aux participants les clés pour comprendre les risques juridiques et géopolitiques liés au Cloud, identifier les solutions souveraines disponibles sur le marché français et poser les bases d’une stratégie d’hébergement souveraine, maîtrisée et durable.

Objectifs de la formation

A l’issue de cette formation, vous serez capable de :

- Identifier les enjeux juridiques et géopolitiques de la souveraineté numérique dans le Cloud.
- Analyser les impacts des législations extra-européennes, notamment le Cloud Act et le FISA, sur les données de son organisation.
- Distinguer les principaux acteurs et labels du Cloud souverain en France.
- Sélectionner des solutions Cloud compatibles avec les exigences de souveraineté numérique.
- Esquisser les bases d’une stratégie de gouvernance souveraine adaptée à son organisation.

Public

Cette formation s’adresse aux décideurs IT, RSSI, DPO, architectes cloud, responsables de projets numériques, juristes IT et consultants en transformation digitale.

Prérequis

Connaissances générales en systèmes d'information et en solutions Cloud : IaaS, PaaS, SaaS. Une expérience dans la gestion, l'administration ou le pilotage d'environnements numériques est un plus.

Programme de la formation

Les démonstrations, exemples et travaux pratiques sont donnés à titre indicatif et pourront être adaptés selon les besoins et le contexte de la session.

Jour 1
Matinée – Fondements de la souveraineté numérique et cadres réglementaires
Chapitre 1 – Définir la souveraineté numérique

- Définition et dimensions de la souveraineté numérique : juridique, technique, politique
- Notions de localisation des données, d'indépendance stratégique et de contrôle des infrastructures
- Typologies de Cloud : public, privé, hybride, communautaire, multicloud
- Cloud souverain vs Cloud de confiance : distinctions et enjeux

Exemples et travaux pratiques :

- Étude de cas : exemples d'atteintes à la souveraineté via le Cloud
- Identification des enjeux de maîtrise des données, des accès et des infrastructures

Chapitre 2 – Cadres réglementaires européens et français

- RGPD : obligations, implications en matière d'hébergement et de transferts internationaux de données
- Grandes réglementations sectorielles et cadres de référence : HDS, NIS2, DORA
- SecNumCloud : objectifs, portée et acteurs qualifiés
- Cas concrets de non-conformité et sanctions

Exemples et travaux pratiques :

- Identification des types de données sensibles à protéger selon le RGPD dans un contexte Cloud
- Analyse des impacts d'une contrainte réglementaire sur le choix d'une solution d'hébergement

Chapitre 3 – Lois extraterritoriales et risques géopolitiques

- Cloud Act, FISA, Patriot Act : portée extraterritoriale des lois américaines et implications pratiques
- Contradictions entre législations américaines et européennes : arbitrages possibles
- Cartographie des fournisseurs mondiaux et risques de dépendance technologique
- Initiatives européennes et françaises : Gaia-X, EUCS, SecNumCloud, doctrine « Cloud au centre », offres Cloud de confiance et recommandations ANSSI pour l'hébergement cloud des systèmes d'information sensibles

Exemples et travaux pratiques :

- Analyse critique des clauses à risque d'un contrat Cloud type
- Identification des points de vigilance liés à l'accès aux données, aux sous-traitants et aux juridictions applicables

Après-midi – Solutions souveraines, gouvernance et stratégie
Chapitre 4 – Identifier et qualifier les solutions de Cloud souverain

- Principaux acteurs français et européens : Bleu, S3NS, NumSpot, Outscale, OVHcloud, Scaleway
- Offres des hyperscalers à dimension souveraine : AWS European Sovereign Cloud, Microsoft Cloud for Sovereignty
- Offres hybrides et Cloud de proximité : AWS Outposts, Azure Local, OVHcloud Hosted Private Cloud
- Labels et certifications : analyse comparative de SecNumCloud, HDS, ISO 27001 et EUCS
- Place de l'open source dans une démarche de souveraineté numérique

Exemples et travaux pratiques :

- Construction d'une grille d'analyse pour auditer un fournisseur Cloud sur les critères de souveraineté
- Comparaison de plusieurs offres selon des critères juridiques, techniques, opérationnels et contractuels

Chapitre 5 – Gouvernance des données et pilotage souverain

- Classification des données selon leur sensibilité, leur criticité et leurs exigences réglementaires
- Chiffrement, cloisonnement et maîtrise des accès aux données sensibles
- Sécurisation des contrats et des accès : gestion des clés, zero trust, IAM
- Indicateurs de suivi, sensibilisation des équipes et veille réglementaire
- Retour d'expérience sur la migration vers une solution Cloud souveraine ou de confiance

Exemples et travaux pratiques :

- Élaboration d'une matrice simple de classification des données
- Identification des mesures de gouvernance à appliquer selon le niveau de sensibilité des données

Chapitre 6 – Élaborer une stratégie souveraine

- Grille d'évaluation des fournisseurs Cloud : souveraineté, conformité, sécurité, coût, performance et réversibilité
- Arbitrages entre exigences de souveraineté, contraintes budgétaires et continuité opérationnelle
- Définition des premières étapes d'une trajectoire d'hébergement souveraine
- Formalisation d'une feuille de route adaptée aux contraintes de l'organisation

Étude de cas et mise en pratique :

- Étude de cas finale en groupe : simuler une décision stratégique de migration vers un Cloud souverain
- Analyse du contexte, des contraintes et des risques
- Choix argumenté d'une solution ou d'une trajectoire cible

- Élaboration d’une feuille de route synthétique
- Restitution collective et discussion sur les conditions de mise en œuvre

Méthodes pédagogiques

- Accompagnement théorique et pratique alliant apports conceptuels, analyses de cas réels et mises en situation guidées.

- Le formateur s’appuie sur les expériences et le contexte des participants pour nourrir les échanges de cas concrets et de retours d’expérience ciblés.

- Le format d’une journée privilégie les notions essentielles, les analyses comparatives, les exercices guidés et les cas d’usage directement exploitables.

Les supports de formation seront fournis aux participants au cours de la formation au format PDF.

Méthodes d’évaluation des acquis

Avant la formation :

- Recueil éventuel des attentes et du contexte des participants en amont de la session.

En cours de formation :

- Points d’étapes réguliers du formateur sur la compréhension des stagiaires.
- Vérification des résultats lors des travaux pratiques ou exercices guidés.
- Analyse collective de cas d’usage liés à la souveraineté numérique et au Cloud.

Après la formation « à chaud » :

- Questionnaire d’auto-évaluation des compétences complété individuellement par chaque stagiaire en fin de session.
- Questionnaire de satisfaction complété individuellement en fin de session.
- Le compte rendu formateur complété par le formateur.

Après la formation « à froid » :

- Questionnaire de satisfaction complété individuellement quelques semaines après la session.

Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.