

Gagner en souveraineté numérique et renforcer sa cybersécurité

Date et durée
Code formation : GSI006FR Durée : 2 jours Nombre d'heures : 14 heures
Description
<p>Dans un contexte géopolitique instable où la cybercriminalité se professionnalise, la maîtrise de vos données ne dépend plus seulement de vos outils, mais de leur origine. Cette formation intensive de 2 jours vous apprend à dessiner une stratégie de souveraineté numérique qui vous immunise contre les dépendances technologiques et les ingérences juridiques extraterritoriales.</p> <p>Au programme : choix de fournisseurs de confiance, déploiement d'Open Source, architecture de cloud souverain, protection juridique des données. Des ateliers pratiques vous font inventorier vos données critiques, évaluer la maturité de vos fournisseurs et prioriser vos actions sans bloquer l'innovation.</p> <p>À la fin de cette formation, vous repartirez avec une feuille de route validée : calendrier, budget rapide, indicateurs de résilience et scénario de continuité. Résultat : vous alliez IA, blockchain et innovation tout en garantissant l'indépendance numérique de votre organisation.</p>
Objectifs
<p>À l'issue de cette formation, vous atteindrez les objectifs de compétences suivants :</p> <ul style="list-style-type: none">• maîtriser les enjeux géopolitiques et économiques de la souveraineté numérique ;• diagnostiquer le niveau de dépendance technologique de son organisation ;• naviguer entre les réglementations locales et les lois extraterritoriales impactant les données ;• élaborer une stratégie d'achat et de partenariat favorisant l'indépendance (Open Source, Cloud souverain) ;• mettre en œuvre les bonnes pratiques de cybersécurité pour garantir la résilience du SI.
Points forts
<ul style="list-style-type: none">• Double vision : vous aborderez la cybersécurité sous l'angle technique, mais aussi géopolitique et juridique.• Pragmatisme : vous repartirez avec des modèles de documents (registre, contrats types) directement exploitables.• Innovation : vous explorerez les technologies de rupture (Blockchain, IA) comme vecteurs de souveraineté.• Mise en situation : vous testerez votre réactivité via un exercice de gestion de crise spécifique aux enjeux d'indépendance.
Modalités d'évaluation
Travaux Pratiques

Pré-requis

Suivre cette formation ne nécessite aucun prérequis technique spécifique.

Public

Cette formation s'adresse aux dirigeants et responsables de la stratégie IT. Le public inclut notamment :

- **les RSSI et DSI** qui doivent aligner les choix technologiques avec les impératifs de sécurité ;
- **les dirigeants et managers** souhaitant renforcer la résilience et l'autonomie stratégique de leur structure ;
- **les responsables et équipes SSI** chargés de la mise en œuvre opérationnelle de la protection des données.

Programme

Module 1 : comprendre les enjeux de la souveraineté numérique

- L'analyse du contexte géopolitique et des nouveaux marchés de la cybercriminalité.
- La définition de l'indépendance numérique et ses implications pour l'entreprise.
- L'état des lieux d'Internet : données, chiffres clés et infrastructures.

Module 2 : protéger les données face aux lois extraterritoriales

- Les principes fondamentaux de la protection des données (DICP/T).
- Le décryptage des réglementations clés et l'impact des lois extraterritoriales.
- La sécurisation des données propres à l'entité.

Travaux pratiques

- Identifier et classer les données critiques de son organisation à protéger.

Module 3 : construire une stratégie d'indépendance technologique

- L'analyse de la dépendance vis-à-vis des fournisseurs actuels.
- La mise en place d'un Plan Assurance Sécurité (PAS).
- L'évaluation de l'opportunité et des cas d'usage de l'Open Source.
- La définition d'une stratégie d'achat orientée vers l'indépendance numérique.

Module 4 : allier cybersécurité opérationnelle et souveraineté

- Le panorama de l'évolution des menaces ciblant l'indépendance.
- L'application des bonnes pratiques d'hygiène numérique.
- La gestion des incidents et la garantie de la continuité d'activité (PCA).

Travaux pratiques

- Simuler une gestion de crise liée à une perte d'indépendance numérique.

Module 5 : maîtriser les technologies clés de la souveraineté

- La mise en place et l'intérêt d'un cloud souverain.
- Le rôle de l'intelligence artificielle et de la blockchain dans la souveraineté.
- L'innovation comme levier stratégique de succès et d'autonomie.

Module 6 : synthétiser et pérenniser la démarche

- Le récapitulatif des mesures clés pour l'indépendance numérique.
- La présentation des ressources, sites web de référence et outils de veille.