

Souveraineté et sécurité de la Supply Chain

2 jours (14 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

1 470 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

Objectifs

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

- Décrire les enjeux de souveraineté numérique et de dépendance fournisseurs
- Identifier les menaces majeures pesant sur la Supply Chain logicielle et matérielle
- Cartographier et évaluer les risques de sa propre chaîne d'approvisionnement IT
- Concevoir des exigences de sécurité et de souveraineté pour les fournisseurs
- Mettre en oeuvre des contrôles techniques et organisationnels de sécurisation
- Mettre en place un plan d'amélioration continue et de mise en conformité (NIS2, réglementations européennes...).

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Ingénieurs systèmes, réseaux, Cloud, DevOps et SecOps, architectes IT / Cloud / sécurité, RSSI, responsables sécurité IT et responsables risques numériques ainsi que les chefs de projets techniques impliqués dans la gestion de fournisseurs IT.

Prérequis

Avoir des connaissances de base en architectures systèmes, réseaux et/ou Cloud ainsi qu'une bonne compréhension des concepts fondamentaux de cybersécurité. Avoir une expérience dans des projets IT, DevOps ou Cloud est conseillé.

Programme

1 Pendant votre formation

Souveraineté et sécurité de la Supply Chain

Jour 1 – Matin

Enjeux de souveraineté numérique et de sécurité de la Supply Chain

- Contexte géopolitique et économique
 - Fragmentation numérique et dépendances critiques
 - Tensions réglementaires, extraterritorialité et accès aux données
- Notions clés de souveraineté numérique
 - Données, infrastructures, Cloud et logiciels
 - Localisation, juridictions, contrôle et autonomie
- Spécificités de la Supply Chain numérique
 - Supply Chain logicielle (Open Source, CI/CD et SaaS)
 - Supply Chain matérielle (composants, firmware et IoT)
- Typologie des risques et impacts métier
 - Risques de compromission, fuite et indisponibilité
 - Impacts opérationnels, financiers, réglementaires et réputationnels

Cadre réglementaire et référentiels

- Cadre européen et national
 - NIS2 et obligations sur la Supply Chain
 - Cybersecurity Act, certification et directives sectorielles
- Réglementation sur les données et la souveraineté
 - RGPD, transferts internationaux et localisation des données
 - Initiatives et stratégies de souveraineté Cloud et données
- Standards, normes et bonnes pratiques
 - ISO 27001/27036, frameworks de gestion des risques fournisseurs
 - Référentiels sectoriels et guides de bonnes pratiques

Jour 1 – Après-midi

Cartographie et analyse de la Supply Chain IT

- Identification des actifs critiques et dépendances
 - Services métiers, applications, données et infrastructures
 - Fournisseurs directs, sous-traitants et dépendances en cascade

- Cartographie de la Supply Chain numérique
 - Flux techniques (accès, API et interconnexions)
 - Flux de données (localisation, transfert et traitement)
- Analyse de criticité et de risques
 - Matrice criticité / dépendance / exposition
 - Approche par scénarios de menace
- Indicateurs de souveraineté et de résilience
 - Indicateurs de dépendance technologique
 - Indicateurs de maîtrise et de diversification

Exemples de travaux pratiques (à titre indicatif)

- *Exercice de cartographie d'une chaîne d'approvisionnement IT (cas fourni ou environnement des participants)*
- *Identification des fournisseurs critiques et points de concentration*
- *Construction d'une grille de criticité et premiers scénarios de risque*

Gouvernance, rôles et processus

- Gouvernance de la Supply Chain numérique
 - Rôles (DSI, RSSI, achats, juridique et métiers)
 - Comités, responsabilités et sponsorship
- Intégration dans les processus internes
 - Intégration dans les processus d'achats et de sourcing
 - Intégration dans les processus projet (cycle de vie)
- Gestion du risque fournisseur
 - Segmentation des fournisseurs par niveau de risque
 - Cycle de vie du fournisseur (onboarding, suivi et offboarding)
- Pilotage et reporting
 - Indicateurs de performance (KPI) et de risque (KRI)
 - Tableaux de bord, reporting à la direction

Exemples de travaux pratiques (à titre indicatif)

- *Définition d'un schéma de gouvernance cible pour la Supply Chain numérique*
- *Formalisation d'un workflow simplifié d'onboarding / suivi / offboarding fournisseur*

Jour 2 – Matin

Exigences de sécurité et de souveraineté pour les fournisseurs

- Politique de sécurité de la Supply Chain
 - Principes directeurs, périmètre et objectifs
 - Alignement avec les politiques sécurité et conformité existantes

- Critères de sélection et de qualification des fournisseurs
 - Critères techniques, sécurité, souveraineté et conformité
 - Exigences de localisation, juridiction et certifications
- Clauses contractuelles et SLA de sécurité
 - Clauses sécurité, confidentialité et réversibilité
 - SLA sécurité, supervision et notifications d'incident
- Contrôle, audits et revue périodique
 - Droit d'audit, questionnaires et preuves
 - Gestion des écarts, plans de remédiation et suivi

Exemples de travaux pratiques (à titre indicatif)

- *Elaboration d'une grille d'évaluation sécurité / souveraineté pour les fournisseurs*
- *Rédaction de clauses-clés à intégrer dans les contrats et SLA*

Sécurité de la Supply Chain logicielle

- Menaces sur la Supply Chain logicielle
 - Compromission de dépendances Open Source
 - Attaques sur les pipelines CI/CD et les registres
- Pratiques de développement et de build sécurisés
 - Signature, intégrité et provenance des artefacts
 - Gestion des dépendances, SBOM et revue de composants
- Intégration de la sécurité dans la chaîne DevOps
 - Contrôles dans les pipelines CI/CD
 - Intégration avec la supervision et l'observabilité
- Gestion des vulnérabilités et mises à jour
 - Processus de correction sur composants tiers
 - Critères de priorisation et fenêtres de maintenance

Exemples de travaux pratiques (à titre indicatif)

- *Analyse d'un cas d'attaque sur la Supply Chain logicielle*
- *Définition de mesures techniques à déployer dans un pipeline CI/CD*
- *Elaboration d'une liste de contrôles à imposer à un éditeur logiciel ou fournisseur SaaS*

Sécurité de la Supply Chain matérielle, Cloud et services managés

- Risques matériels, IoT et firmware
 - Provenance des composants et chaînes de fabrication
 - Risques de firmware malveillants ou non maîtrisés
- Cloud, services managés et souveraineté

- Choix de modèles de déploiement (Cloud public, privé et souverain)
- Gestion des dépendances à des hyperscalers et solutions souveraines
- Contrôles techniques pour les fournisseurs d'infrastructure
 - Segmentation, filtrage et accès privilégiés
 - Journalisation, supervision, sauvegardes et PRA / PCA
- Continuité d'activité et scénarios de rupture fournisseur
 - Stratégies de multi-Cloud, multi fournisseur et réversibilité
 - Exercices de tests et de bascule

Exemples de travaux pratiques (à titre indicatif)

- Construction d'un scénario de rupture critique d'un fournisseur Cloud ou d'infrastructure
- Définition de mesures de mitigation et d'un plan de continuité

Jour 2 – Après-midi

Feuille de route et plan d'action Supply Chain sécurité et souveraineté

- Diagnostic rapide de maturité
 - Evaluation du niveau actuel (organisation, technique et contrat)
 - Identification des gaps principaux
- Priorisation des actions
 - Actions rapides et chantiers structurels
 - Alignement avec les obligations réglementaires
- Roadmap 12-24 mois
 - Séquencement des projets et jalons
 - Ressources nécessaires et dépendances internes
- Communication, acculturation et formation continue
 - Sensibilisation des équipes IT, achats, juridiques et métiers
 - Intégration dans les plans de formation et d'onboarding

Exemples de travaux pratiques (à titre indicatif)

- Construction d'une feuille de route adaptée au contexte de l'organisation ou d'un cas d'étude
- Définition d'un premier jeu de livrables (politique, procédures, modèles de contrats et tableaux de bord)

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

[Accessibilité aux personnes en situation de handicap](#)

Détails de la session

Du 7 décembre 2027 au 8 décembre 2027 (2 jours / 14 heures)

À distance

Du 7 décembre 2027 au 8 décembre 2027 **À distance**

- 7 décembre 2027 9h00 – 16h30
- 8 décembre 2027 9h00 – 16h30