Mise à jour : 01/03/2026

FORMATION : Cybersécurité Supply Chain

PUBLIC	Cette formation est à destination des RSSI, de la Direction des Achats, du Juridique, de la DSI, et du Risk Management.
PRÉREQUIS	Prérequis : ▪ Avoir les connaissances de base en cybersécurité et supply chain. ▪ Aucune expertise technique approfondie requise. Matériel requis : ▪ Ordinateur portable avec accès Internet, accès administrateur pour les ateliers.
MODALITÉS ET DÉLAIS D'ACCÈS	En présentiel : ⇨ Formation en présentiel : lieu de formation communiqué en amont de la formation. ⇨ Inscription à réaliser 1 mois avant le démarrage de la formation. En distanciel : ⇨ Formation individuelle ou collective à distance sous la forme de visioconférence participative. ⇨ Inscription à réaliser 1 mois avant le démarrage de la formation.
DURÉE	14H pour une période de 2 jours
DATES	À définir avec l'organisme de formation
HORAIRES	⇨ Les horaires de formation sont : 9H à 12H et de 13H à 17H ⇨ Le monitoring et l'assistance pédagogique sont disponibles du lundi au vendredi de 9H à 18H.
LIEU	En présentiel : ⇨ Sur site ⇨ Au siège de Tricolor Expertise ⇨ Autre adresse En distanciel : ⇨ Formation à distance – visioconférence **Pour les personnes en situation de handicap : Nous adaptons nos formations en fonction de votre handicap et nous mettrons tout en œuvre pour vous accueillir ou pour vous réorienter si besoin.** **Vous pouvez nous contacter au 06 34 31 28 65**
TARIF	2 200€ par personne
NOMBRE DE PARTICIPANTS	En présentiel : Jusqu'à 12 personnes En distanciel : Jusqu'à 5 personnes
OBJECTIF DE LA FORMATION ET COMPÉTENCES VISÉES	À l'issue de la formation, le participant sera capable de mettre en œuvre les compétences suivantes : ▪ Poser le cadre conceptuel et identifier les enjeux spécifiques à la chaîne d'approvisionnement. ▪ Connaître les obligations légales et les référentiels applicables à la sécurité de la supply chain. ▪ Construire un registre des tiers et évaluer leur criticité. ▪ Mettre en œuvre une démarche d'évaluation structurée et continue. ▪ Traduire les exigences de sécurité en obligations contractuelles opposables. ▪ Être prêt à détecter et gérer un incident impliquant un tiers. ▪ Intégrer la sécurité de la supply chain dans la gouvernance globale de l'organisation.
MODALITÉS D'ÉVALUATION D'ATTEINTE DES OBJECTIFS DE LA FORMATION	⇨ Évaluation individuelle du profil, des attentes et des besoins du participant avant le démarrage de la formation ⇨ Évaluation des connaissances & compétences en début et en fin de formation via un QCM ⇨ Tests de contrôle de connaissances et validation des acquis à chaque étape ⇨ Travaux pratiques et mises en situation ⇨ Echange avec le formateur ou la formatrice par visioconférence (webinar), téléphone et mail ⇨ Questionnaire d'évaluation de la satisfaction en fin de formation
CONTENU	Dans cette formation, le participant aura accès au programme suivant :

MODULE 1	**Comprendre la supply chain numérique et ses risques (2h)** 1. Définition de la supply chain numérique : fournisseurs de logiciels, matériels, services cloud, sous-traitants, intégrateurs 2. Pourquoi la supply chain est devenue un vecteur d'attaque privilégié 3. Incidents marquants : SolarWinds, Kaseya, XZ Utils, 3CX, MOVEit 4. Typologies d'attaques : compromission de code source, backdoors matérielles, détournement de mises à jour, attaques par rebond 5. Les effets de cascade : de la PME sous-traitante à l'entité critique 6. Cartographie des interdépendances numériques dans une organisation type
MODULE 2	**Cadre réglementaire et normatif (2h)** 1. Réglementations européennes : NIS2 (article sur les tiers), DORA (risque tiers TIC), CRA (Cyber Resilience Act) 2. Réglementations sectorielles : défense (IGI 1300), industrie critique, spatial 3. Normes et référentiels internationaux : ISO 27001/27036, NIST SP 800-161, C-SCRM 4. Référentiels sectoriels : CMMC (défense US), IEC 62443 (industrie), SOC 2 5. Recommandations ANSSI sur la sécurité des prestataires 6. Cartographie des obligations selon le secteur et la taille de l'organisation
MODULE 3	**Identification et classification des tiers (2h)** 1. Typologie des tiers : fournisseurs logiciels, hébergeurs, ESN, éditeurs, intégrateurs, sous-traitants 2. Critères de criticité : accès aux données sensibles, accès réseau, dépendance opérationnelle, concentration 3. Construction et tenue d'un registre des tiers (format, contenu, fréquence de mise à jour) 4. Méthode de scoring et de priorisation des tiers à risque 5. Notion de quatrième partie (sous-traitants des sous-traitants) et de risque de concentration Atelier pratique : qualification et scoring d'un portefeuille de fournisseurs fictifs
MODULE 4	**Évaluation et audit de la sécurité des fournisseurs (2h)** 1. Due diligence initiale : questionnaires de sécurité, analyse documentaire, certifications 2. Référentiels d'évaluation : CAIQ (CSA), SIG (Shared Assessments), questionnaires ANSSI 3. Audits de sécurité : droit d'audit contractuel, tests d'intrusion ciblés, revues de code 4. Évaluation continue : surveillance de la surface d'attaque externe (ASM), threat intelligence sur les tiers 5. Gestion des résultats : plans d'action, suivi des remédiations, réévaluation périodique Atelier pratique : analyse d'un questionnaire fournisseur et identification des points de risque
MODULE 5	**Sécurisation contractuelle et exigences fournisseurs (2h)** 1. Les clauses de sécurité incontournables : exigences minimales, droit d'audit, notification d'incident 2. Niveaux de service sécurité (SLA sécurité) : délais de patch, disponibilité, temps de réponse incide 3. Gestion de la chaîne de sous-traitance : clause de flux descendant (flow-down) 4. Exigences sur le cycle de développement sécurisé (SSDLC) pour les éditeurs logiciels 5. Software Bill of Materials (SBOM) : définition, formats (SPDX, CycloneDX), cas d'usage 6. Le format VEX 7. Plans de sortie et de réversibilité : portabilité des données, continuité de service Atelier pratique : Génération de SBOM et analyse des vulnérabilités
MODULE 6	**Détection, réponse aux incidents et continuité (2h)** 1. Signaux d'alerte d'une compromission via un tiers : indicateurs techniques et comportementaux 2. Surveillance des tiers : monitoring des flux, détection d'anomalies, threat intelligence externe 3. Processus de gestion d'incident impliquant un fournisseur : rôles, communication, coordination 4. Obligations de notification : vers les autorités, vers les clients, vers les partenaires 5. Plan de continuité d'activité (PCA) intégrant les défaillances fournisseurs 6. Stratégie de sortie d'urgence et fournisseurs de substitution Atelier pratique : simulation de crise — compromission d'un prestataire disposant d'accès distants
MODULE 7	**Gouvernance, pilotage et amélioration continue (2h)** 1. Intégration dans la PSSI et le système de management de la sécurité (SMSI)

	2. Rôles et responsabilités : RSSI, Direction des Achats, Juridique, DSI, Risk Management 3. Tableaux de bord et indicateurs de suivi : couverture des évaluations, taux de conformité, délais de remédiation 4. Sensibilisation et formation des équipes achats et métiers 5. Gestion du cycle de vie fournisseur : entrée, vie du contrat, sortie Retours d'expérience et tendances : évolution des menaces, IA et supply chain, open source
MOYENS PERMETTANT LE SUIVI ET L'APPRÉCIATION DES RÉSULTATS	Suivi de l'exécution : ⇨ Feuilles de présences signées par les participants et le formateur ou la formatrice par demi-journée ⇨ Attestation de fin de formation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation. Appréciation des résultats : ▪ Recueil individuel des attentes du stagiaire ▪ Questionnaire d'auto-évaluation des acquis en début et en fin de formation ▪ Évaluation continue durant la session ▪ Remise d'une attestation de fin de formation ▪ Questionnaire d'évaluation de la satisfaction en fin de formation
MOYENS PÉDAGOGIQUES ET TECHNIQUES D'ENCADREMENT DES FORMATIONS	Modalités pédagogiques : ▪ Évaluation des besoins et du profil du participant ▪ Apport théorique et méthodologique : séquences pédagogiques regroupées en différents modules ▪ Contenus des programmes adaptés en fonction des besoins identifiés pendant la formation ▪ Réflexion et échanges sur cas pratiques ▪ Questionnaires, exercices, ateliers et étude de cas ▪ Tests de contrôle de connaissances et validation des acquis à chaque étape ▪ Retours d'expériences Éléments matériels : ▪ Mise à disposition de tout le matériel pédagogique nécessaire (pour les formations en présentiel) ▪ Support de cours au format numérique projeté sur écran et transmis au participant par mail à la fin de la formation Référent pédagogique et formateur/formatrice : Chaque formation est sous la responsabilité de la directrice pédagogique de l'organisme de formation ; le bon déroulement est assuré par le formateur ou la formatrice désigné(e) par l'organisme de formation.