

Cybersécurité supply chain : protéger les systèmes logistiques contre les cybermenaces

Lien : https://innov-maroc.com/formation/cybersecurite-supply-chain-proteger-les-systemes-logistiques-contre-les-cybermenaces

DURÉE
5 jours (35h)

RÉFÉRENCE
LTSC65

CATÉGORIE
Résilience et Gestion des Risques Supply Chain

INNOV MAROC

🎯 OBJECTIFS DE LA FORMATION

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

- Comprendre les enjeux et spécificités de la cybersécurité appliquée à la Supply Chain et à la logistique.
- Savoir identifier et cartographier les actifs, systèmes, données et surfaces d’attaque de l’écosystème logistique.
- Maîtriser les méthodes d’évaluation et de gestion des risques cyber affectant les opérations Supply Chain.
- Sécuriser les principaux systèmes logistiques : ERP, WMS, TMS, plateformes digitales et interfaces interentreprises.
- Comprendre les risques liés aux IoT, équipements connectés, robots et environnements industriels OT.
- Savoir identifier les cybermenaces et mettre en place des mécanismes efficaces de détection et de monitoring.
- Évaluer et maîtriser les risques cyber liés aux fournisseurs, transporteurs et prestataires logistiques.
- Protéger les données et les flux d’information critiques contre les accès non autorisés, fuites et manipulations.
- Concevoir un dispositif efficace d’Incident Response, de continuité et de résilience face aux cyberattaques.
- Être capable de déployer une gouvernance et une stratégie de cybersécurité Supply Chain permettant de protéger durablement les opérations et l’écosystème de partenaires.

👥 POUR QUI ?

- Directeurs Supply Chain, Chief Supply Chain Officers et responsables de la performance logistique.
- Responsables cybersécurité, RSSI, Security Managers et responsables IT.
- Responsables logistique, transport, entreposage et opérations Supply Chain.
- Responsables systèmes d’information, ERP, WMS, TMS et plateformes digitales.
- Ingénieurs réseaux, systèmes, cloud, IoT et infrastructures technologiques.
- Responsables OT, automatisation, robotique et systèmes industriels.
- Responsables achats, procurement et gestion des risques fournisseurs.
- Responsables Third-Party Risk Management, conformité et contrôle interne.
- Chefs de projets Supply Chain 4.0, transformation digitale et cybersécurité.
- Consultants, managers et dirigeants souhaitant renforcer la cybersécurité et la résilience de leur Supply Chain.

INNOV MAROC



Programme détaillé

1 / FONDAMENTAUX DE LA CYBERSÉCURITÉ SUPPLY CHAIN

- Comprendre les enjeux de cybersécurité propres aux chaînes d'approvisionnement et aux opérations logistiques.
- Identifier les principales surfaces d'attaque liées aux ERP, WMS, TMS, IoT, plateformes fournisseurs et systèmes industriels.
- Évaluer l'impact potentiel d'une cyberattaque sur les flux, les stocks, les transports et la continuité des opérations.

2 / CARTOGRAPHIE DES ACTIFS ET DES SURFACES D'ATTAQUE

- Identifier les systèmes, équipements, applications, données et infrastructures critiques de la Supply Chain.
- Cartographier les interconnexions entre entreprises, fournisseurs, transporteurs, prestataires logistiques et systèmes d'information.
- Identifier les points d'entrée, dépendances critiques et vulnérabilités susceptibles d'être exploitées.

3 / GESTION DES RISQUES CYBER DE LA SUPPLY CHAIN

- Construire une cartographie des risques cyber couvrant les dimensions technologiques, humaines et organisationnelles.
- Évaluer la probabilité, l'impact et la criticité des cybermenaces affectant les opérations logistiques.
- Définir des mesures de réduction des risques adaptées aux processus et actifs critiques.

4 / SÉCURISATION DES ERP, WMS, TMS ET PLATEFORMES LOGISTIQUES

- Identifier les vulnérabilités spécifiques aux systèmes de gestion des commandes, stocks, entrepôts et transports.

INNOV MAROC

- Renforcer les contrôles d’accès, l’authentification, la segmentation réseau et la protection des interfaces.
- Sécuriser les échanges de données entre les applications internes et les plateformes des partenaires.

5 / CYBERSÉCURITÉ DES OBJETS CONNECTÉS ET SYSTÈMES INDUSTRIELS

- Identifier les risques liés aux capteurs IoT, RFID, GPS, robots, automates et équipements connectés.
- Protéger les environnements OT et les infrastructures industrielles contre les intrusions et manipulations.
- Mettre en place une segmentation IT/OT et des mécanismes de supervision adaptés aux environnements logistiques.

6 / MENACES, ATTAQUES ET DÉTECTION DES INCIDENTS

- Comprendre les principales menaces : ransomware, phishing, compromission de comptes, malware, DDoS et attaques par la chaîne fournisseur.
- Identifier les indicateurs de compromission et les comportements anormaux dans les systèmes logistiques.
- Mettre en place des mécanismes de Security Monitoring et d’alerte pour détecter rapidement les incidents.

7 / CYBERSÉCURITÉ DES FOURNISSEURS ET PARTENAIRES LOGISTIQUES

- Évaluer la maturité cyber des fournisseurs, transporteurs, 3PL, 4PL et prestataires technologiques.
- Intégrer des exigences de cybersécurité dans les contrats, appels d’offres et processus de référencement fournisseurs.
- Mettre en place un dispositif de Third-Party Risk Management pour surveiller les risques cyber externes.

8 / PROTECTION DES DONNÉES ET DES FLUX LOGISTIQUES

- Identifier les données critiques : commandes, stocks, clients, itinéraires, tarifs, contrats et informations fournisseurs.
- Mettre en œuvre des mécanismes de chiffrement, contrôle d’accès, sauvegarde et traçabilité des données.
- Prévenir les fuites de données, altérations d’informations et manipulations susceptibles de perturber les opérations.

INOV MAROC

9 / INCIDENT RESPONSE, CONTINUITÉ ET RÉSILIENCE SUPPLY CHAIN

- Construire un plan de réponse aux incidents adapté aux systèmes et processus logistiques.
- Définir les procédures de confinement, investigation, restauration et reprise des opérations après une cyberattaque.
- Tester régulièrement les plans de continuité, de reprise informatique et de résilience Supply Chain.

10 / GOUVERNANCE ET INDUSTRIALISATION DE LA CYBERSÉCURITÉ SUPPLY CHAIN

- Définir une gouvernance cyber intégrant les responsabilités des équipes IT, OT, Supply Chain et partenaires externes.
- Mettre en place des KPI, audits, contrôles et indicateurs de maturité permettant de piloter la sécurité.
- Construire une stratégie de cybersécurité durable permettant de protéger et renforcer la résilience de l'écosystème Supply Chain.

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Mises en Situation pour faciliter l'assimilation
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

15 au 19 Fév. 2027	Présentiel - Casablanca
12 au 16 Avr. 2027	Présentiel - Casablanca
07 au 11 Juin 2027	Présentiel - Casablanca
02 au 06 Août 2027	Présentiel - Casablanca
27 Sep. au 01 Oct. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

INOV MAROC

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-maroc.com
Web : https//www.innov-maroc.com

INNOV MAROC — Tous droits réservés

INNOV MAROC