



Guide Formateur

Sensibiliser à la cybersécurité dans les métiers du transport et de la logistique



Route



Entrepôt



Ferroviaire



Maritime



Destiné aux

Enseignants, formateurs, maîtres d'apprentissage, tuteurs en entreprise et responsables de centre de formation.

Sommaire



01

Présentation de CyberTransLog

p. 02



02

Le rôle du formateur

p. 03



03

Le dispositif en un clin d'œil

p. 04



04

Les enjeux à transmettre

p. 05



05

Idées d'animation

p. 06



06

Mini glossaire pour parler simplement

p. 07



07

Ressources, relais et accompagnement

p. 08



08

Message final et repères

p. 09

Annexes : fiches descriptives des modules

A – Module 0 : Les fondamentaux	p. 13 – 14
B – Module ferroviaire 1 : Bienvenue sur le réseau	p. 15 – 16
C – Module ferroviaire 2 : Une journée sous pression	p. 17 – 18
D – Module maritime 1 : Bienvenue au port	p. 19 – 20
E – Module maritime 2 : Escale sous tension	p. 21 – 22
F – Module transport routier	p. 23 – 24 – 25
G – Module logistique	p. 27 – 28 – 29
H – Jeu sérieux – Dans la peau d'un cyberattaquant	p. 31 – 32
Crédits et partenaires	p. 33

Présentation de CyberTransLog

CyberTransLog est un dispositif de sensibilisation à la cybersécurité dédié aux métiers du transport et de la logistique : route, ferroviaire, maritime et entrepôt. Il s'appuie sur des scénarios concrets et des personnages métiers pour parler des cyber-risques avec les mots du terrain et à partir de situations proches de la réalité professionnelle des apprenants.



Objectifs de ce guide

Ce guide a un objectif simple : aider les formateurs à intégrer facilement ces contenus dans leurs cours, même s'ils ne se sentent pas à l'aise avec l'informatique ou la cybersécurité. Il apporte des repères clairs, des exemples de séquences et des idées d'animation pour permettre une prise en main rassurante du sujet.



À retenir

Ce guide permet d'aborder la cybersécurité comme un enjeu métier et de sécurité au travail, et non comme un contenu purement technique.

Le rôle du formateur

Vous êtes le maillon qui relie le “cyber” au terrain, en traduisant les scénarios en exemples vécus et rapprochant les incidents des situations observées en stage, en atelier ou sur la route. Vous n’avez pas besoin de tout connaître sur la technique : votre valeur ajoutée réside dans votre connaissance des gestes métier et des situations à risque.

Ce que CyberTransLog apporte



Des modules scénarisés ancrés dans les métiers du transport et de la logistique.



Des formats variés, comme des capsules interactives, des vidéos, des fiches PDF et des podcasts, pour s'adapter aux profils de groupe, y compris les apprenants « dys » ou en difficulté de lecture.



Un vocabulaire volontairement déjargonné pour parler de cybersécurité sans perdre le groupe.

Ce que vous n’avez pas besoin de faire



- Devenir expert en cybersécurité.
- Répondre à toutes les questions techniques sans appui.
- Porter seul la dimension technique du sujet, alors que des relais peuvent être mobilisés.

03

CHAPITRE 03

Le dispositif en un clin d'œil

Le dispositif est structuré pour être simple à prendre en main et adaptable à différents publics.

Architecture du dispositif

Un module commun

Les fondamentaux du risque cyber : pourquoi le transport-logistique est concerné, le lien entre incident numérique et conséquences opérationnelles.



Quatre parcours sectoriels

Transport routier, logistique d'entrepôt, ferroviaire et maritime. Les apprenants suivent des personnages métiers confrontés à des incidents réalistes, comme des mails suspects, un GPS manipulé, une clé USB trouvée ou un système en panne.



Un jeu sérieux transversal

Une mission immersive qui suit le voyage d'un conteneur de Hong Kong à Bruxelles. L'apprenant observe un cyberattaquant exploiter les failles de la chaîne logistique, puis reprend le contrôle en tant que responsable cybersécurité.



Des formats complémentaires



**Capsules
interactives**



Vidéos



**Fiches de
synthèse**



**Podcasts
courts**

Intégration dans le planning

- dans des séquences de prévention des risques ou de SST ;
- en EMC ou en citoyenneté numérique ;
- en appui de travaux pratiques sur TMS, WMS, tablettes, scanners ou badges ;
- comme fil rouge d'une semaine thématique autour de la sécurité, de la cybersécurité et de la gestion des risques.

04

CHAPITRE 04

Les enjeux à transmettre

Le numérique est devenu la colonne vertébrale du métier : planning, traçabilité, guidage, accès aux sites et échanges clients passent désormais par des outils informatisés. Une erreur de clic ou une attaque peut donc ralentir, bloquer ou désorganiser une activité entière.

Message clé

Un incident cyber n'est jamais "virtuel" pour les professionnels du terrain. Il peut produire des retards de livraison, des blocages de quai, des erreurs de destination ou des situations dangereuses pour les équipes.

Exemples concrets à utiliser

1 En entrepôt



un robot autonome perturbé peut créer un risque pour les équipes sur les quais.

2 Sur la route



un GPS détourné peut envoyer un conducteur dans une zone isolée ou inadaptée, avec un risque accru de vol, d'agression ou d'accident.

3 En gare ou port



un système en panne peut bloquer les circulations, provoquer des retards et créer des tensions, voire des dangers.



Une idée forte

CyberTransLog insiste sur une idée forte : l'utilisateur n'est pas le maillon faible, mais le premier rempart grâce à ses réflexes et à sa connaissance du terrain.

05

CHAPITRE 05

Idées d'animation

Vous pouvez animer une séance autour de CyberTransLog en vous appuyant sur quelques activités simples, sans préparation technique approfondie. Ces idées peuvent être mobilisées pendant les cours pratiques, en EMC ou après le visionnage d'une capsule.

Activités possibles



Rappeler la règle « zéro branchement inconnu » : ne jamais brancher une clé USB trouvée ni un téléphone personnel sur un poste professionnel.



Faire le parallèle avec les EPI : comme pour les casques, les gants ou les chaussures de sécurité, certaines règles numériques de base ne se discutent pas.



Lancer un débat à partir d'un SMS ou d'un mail urgent piégé, en demandant quels indices devraient susciter le doute



Faire travailler les apprenants en petits groupes sur trois bonnes pratiques de mots de passe et trois mauvaises habitudes observées autour d'eux.



Organiser un débrief après chaque capsule avec trois questions simples : qu'est-ce qui semblait suspect, quand fallait-il agir autrement, et qui prévenir dans l'entreprise.



Construire une fiche réflexe collective avec trois colonnes : situation vue, mauvais réflexe, bon réflexe attendu.



Utiliser un podcast court en début ou en fin de cours pour ancrer un conseil dans une situation concrète du dépôt, de la route, du port ou de la gare.



Clôturer un parcours avec le jeu sérieux « Dans la peau d'un cyberattaquant » et débriefer : failles exploitées, failles présentes dans votre environnement, personnes à prévenir.



Les fiches descriptives en annexe permettent d'identifier les ressources mobilisables par leçon : vidéos, quiz...

Mini glossaire pour parler simplement

Ce glossaire vous aide à expliquer les notions cyber sans jargon, avec des formulations accessibles et proches du métier. Il constitue un outil pour choisir deux ou trois notions par séance et les faire reformuler par les apprenants.

Notion	Formulation simple	Exemple pédagogique
 Ingénierie sociale	Scénario du « faux client pressé » qui pousse à agir sans se méfier.	Demander quel indice aurait dû alerter.
 Phishing / hameçonnage	Faux fournisseur ou fausse administration par mail ou SMS urgent.	Comparer plusieurs messages et repérer les signaux faibles.
 Baiting	Piège de la clé USB oubliée pour pousser quelqu'un à la brancher.	Rejouer une situation trouvée sur parking ou vestiaire.
 Mise à jour / patch	Renforcement des « serrures » numériques pour corriger des failles.	Faire le parallèle avec une maintenance de sécurité.
 DDoS	« Embouteillage numérique » qui rend un système indisponible.	Illustrer par un quai saturé ou un standard bloqué.
 Ransomware	« Cadenas » qui bloque systèmes et données contre rançon.	Expliquer l'arrêt d'activité qui en découle.
 Rootkit	Double de clés invisible permettant à un intrus d'agir comme un administrateur.	Faire le lien avec un badge d'accès détourné.
 Man-in-the-Middle	Facteur invisible qui intercepte et modifie un message.	Illustrer avec un RIB changé sur une facture.

Ressources, relais et accompagnement

Vous n'êtes pas seul pour intégrer la cybersécurité dans vos séances. Voici des appuis sur lesquels vous pouvez compter.



MOOCs et guides publiés par des autorités comme l'ANSSI, dont SecNumAcadémie.



Référents numériques de l'établissement ou de l'organisme.



Collègues déjà engagés dans CyberTransLog pour mutualiser les retours d'expérience et les bonnes pratiques.



**ACCÈS
PLATEFORME**

**[https://
www.cybertranslog.movenavirpro-hdf.fr/](https://www.cybertranslog.movenavirpro-hdf.fr/)**



Accès direct à la
plateforme
CyberTransLog pour
préparer vos séances
et tester les modules.



Un Mémo Apprenant "L'essentiel à retenir" accompagne ce dispositif : remettez-le à vos apprenants en fin de parcours.

Message final et repères

En intégrant CyberTransLog dans vos séances, vous faites de la cybersécurité une composante naturelle de la sécurité au travail, au même titre que le port des EPI ou le respect des procédures de manutention.

Vous n'avez pas besoin de tout maîtriser. Chaque échange, chaque exemple concret que vous partagez avec vos apprenants contribue à renforcer la résilience numérique de la filière transport et logistique.

Repères



01

Des scénarios, supports et idées d'activités déjà prêts à l'emploi.



02

Durée, niveau et exemples adaptables à chaque groupe.



03

Des relais internes pour les questions plus complexes.



04

Faire passer des messages simples et développer des réflexes.



“ Chaque séance que vous animez renforce la protection numérique de toute la filière ”



Annexes

Fiches descriptives des modules



Module 0

Les fondamentaux de cybersécurité



Socle commun pour comprendre les risques, reconnaître les menaces et adopter les bons réflexes numériques.

En 6 leçons, complétées par une leçon de présentation, un glossaire, une évaluation finale et une page de crédits/partenaires, ce module pose les bases de la cybersécurité.

1 – Objectifs pédagogiques

- Identifier les grandes familles de cybermenaces
- Reconnaître les principales réglementations cyber
- Identifier pourquoi le facteur humain est la principale faille
- Appliquer les bons réflexes numériques au quotidien

2 – Déroulé par leçon

Leçon	Titre	Contenu	Ressources intégrées
L1	Avant de commencer	Présentation du module, consignes de navigation, accessibilité clavier.	Texte.
L2	Qu'est-ce qu'une cyberattaque ?	Définition, 3 types de cibles (individus, entreprises, infrastructures critiques), chiffres clés.	Texte, cartes interactives, quiz, PDF chiffres clés téléchargeable.
L3	Les grandes familles de menaces	Malware, Phishing, Ransomware, DDoS : définition, mécanisme et impacts.	Audios explicatifs, quiz.
L4	Les normes et réglementations	RGPD (données personnelles), NIS2 (secteurs critiques, transport), ISO 27001, NIST CSF.	Texte, audios, quiz.
L5	Le facteur humain et l'ingénierie sociale	Ingénierie sociale, témoignage expert (Damien Bancal), profils de hackers (white/black/grey hat), organisation des groupes.	1 vidéo interview expert, transcription texte, audios, quiz.
L6	Les objets connectés	IoT et surface d'attaque : caméras, capteurs, badges, terminaux. 3 risques spécifiques.	Texte, audios, quiz.

Leçon	Titre	Contenu	Ressources intégrées
L7	Les bons réflexes	5 réflexes numériques essentiels, Wi-Fi, VPN, comportements à bannir.	Process interactif, Texte, audios.
L8	Glossaire	Cyberattaque, Darknet, DDoS, Infrastructures critiques, Ingénierie sociale, IoT, ISO 27001, Malware, NIS2, NIST CSF, Phishing, Ransomware, RGPD, Script kiddie, Spyware, VPN, White hat / Black hat / Grey hat, Wi-Fi.	Glossaire interactif, PDF téléchargeable.
L9	Évaluation	5 QCM en situation professionnelle (phishing, ingénierie sociale, ransomware/NIS2, mot de passe, white hat)	5 QCM avec feedback pédagogique.

Module ferroviaire 1/2

Bienvenue sur le réseau



En 5 leçons, complétées par une leçon de présentation, une page de glossaire, une évaluation finale et une page de crédits/partenaires, ce module transpose les fondamentaux cyber dans l'univers ferroviaire. L'apprenant suit une journée à la Gare de Valmès aux côtés de Thévan, Liorah et Zorine pour adopter une lecture des risques en gare connectée.

1 – Objectifs pédagogiques

- Situer le secteur ferroviaire dans son contexte cybersécurité
- Identifier les systèmes exposés et les risques associés à chacun
- Distinguer les menaces classiques des menaces spécifiques au ferroviaire et expliquer leur mécanisme d'action
- Établir le lien entre cyberattaques et conséquences physiques sur les usagers
- Identifier les comportements numériques des usagers et les risques associés

2 – Déroulé par leçon

Leçon	Titre	Contenu	Ressources intégrées
L1	Avant de commencer	Présentation du module, consignes de navigation, accessibilité clavier.	Texte.
L2	Bienvenue à Valmès	Immersion dans la cellule SSI de la gare, identification des éléments à protéger.	Audio, transcription, quiz.
L3	Les systèmes sous tension	Distinction IT/OT ; systèmes SCADA, ERTMS, GSM-R ; exposition des protocoles et vulnérabilités.	Audios, visuels, contenus interactifs, quiz d'analyse.
L4	Quand les attaques frappent	Menaces classiques et spécifiques au ferroviaire : ransomware, DDoS, phishing, falsification de signaux, manipulation d'horaires, intrusion dans les systèmes de contrôle.	Texte, audios, quiz.

Leçon	Titre	Contenu	Ressources intégrées
L5	Cyber for Safety	Lien entre cybersécurité et sécurité physique ; convergence IT/OT ; scénario de propagation d'une attaque depuis l'IT vers l'OT.	Audio, texte, quiz, scénario en étapes, vidéo interview Nicolas Mathon – Chef de projet sensibilisation à la cybersécurité E-SNCF Solutions.
L6	L'utilisateur dans la ligne de mire	Risques numériques côté usagers : Wi-Fi public, code PIN sur borne, NFC, données de déplacement, bancaires, biométriques et de connexion.	Texte, audios, quiz, vidéo animée d'une attaque par phishing.
L7	Glossaire	Convergence IT/OT, cyber for safety, données biométriques, ERTMS, falsification de signaux, GSM-R, IT, OT, NFC, protocole, SCADA, SSI, Wi-Fi.	Glossaire interactif, PDF téléchargeable.
L8	Évaluation	3 QCM en situation professionnelle (les systèmes, les conséquences, les intrusions).	3 QCM avec feedback pédagogique.

Module ferroviaire 2/2

Une journée sous pression



En 5 leçons, complétées par une leçon de présentation, une page de glossaire, une évaluation finale et une page de crédits/partenaires, ce module plonge l'apprenant dans la gestion d'un incident cyber en gare de Valmès. Il transforme les notions de qualification, containment, résilience et Security by Design en décisions concrètes, prises au fil d'une journée sous pression. Ce module fait suite au module « La cybersécurité dans le domaine ferroviaire : Bienvenue sur le réseau, qui en est le prérequis.

1 – Objectifs pédagogiques

- Appliquer les étapes de gestion d'un incident cyber dans un contexte ferroviaire
- Analyser les conséquences d'une cyberattaque sur les systèmes et sur les usagers
- Identifier les mesures techniques et organisationnelles de résilience cyber
- Évaluer les décisions prises face à un incident en temps réel
- Situer le concept de Security by Design dans la conception des systèmes ferroviaires

2 – Déroulé par leçon

Leçon	Titre	Contenu	Ressources intégrées
L1	Avant de commencer	Présentation du module, consignes de navigation, accessibilité clavier.	Texte.
L2	L'alerte	Détection d'anomalies simultanées à 10h30 ; distinction panne technique / incident cyber ; répartition des rôles entre Liorah, Thévan et Zorine.	Image contextualisée, audio, transcription, quiz.
L3	Qualifier et contenir	Méthode de gestion d'incident : détecter, qualifier, contenir, documenter, préserver les logs et gérer l'attribution.	Audios, visuels, contenus interactifs, quiz d'analyse.

Leçon	Titre	Contenu	Ressources intégrées
L4	Résilience technique	Mesures techniques pour limiter l'impact et éviter la propagation : segmentation IT/OT, MFA, chiffrement, patch management et pentest.	Texte, audios, quiz.
L5	Résilience approche organisationnelle	Formation, plan de continuité d'activité, plan de reprise, accès, droits, audits de conformité.	Texte, audios, quiz.
L6	Retour d'expérience	Clôture de la journée : REX structuré, enseignements de l'incident, introduction de la Security by Design et de ses principes.	Audio, quiz, texte vidéo Interview Stéphane Peloux - Responsable d'équipe Cybersécurité E-SNCF Solutions.
L7	Glossaire	Containment, logs, segmentation, PCA, PRI, pentest, Security by Design...	Glossaire interactif, PDF téléchargeable.
L8	Évaluation	3 QCM en situation professionnelle (réponse à incident, reprise d'activité et décisions de conception sécurisé).	3 QCM avec feedback pédagogique.

Module maritime 1/2

Bienvenue au port



En 6 leçons, complétées par une leçon de présentation, une page de glossaire, une évaluation finale et une page de crédits/partenaires, ce module plonge l'apprenant dans la cybersécurité d'un port maritime. Le parcours articule systèmes numériques exposés, acteurs de menace, vecteurs d'attaque, conséquences physiques et comportements humains à risque autour du port fictif de Valmar.

1 – Objectifs pédagogiques

- Situer le secteur maritime dans son contexte cybersécurité
- Identifier les systèmes numériques exposés dans un port et les risques associés à chacun
- Distinguer les menaces classiques des menaces spécifiques au maritime et expliquer leur mécanisme d'action
- Établir le lien entre cyberattaques et conséquences physiques sur les navires et leurs passagers
- Identifier les comportements à risque des agents portuaires, des équipages, des prestataires et des usagers

2 – Déroulé par leçon

Leçon	Titre	Contenu	Ressources intégrées
L1	Avant de commencer	Présentation du module, consignes de navigation, accessibilité clavier.	Texte.
L2	Bienvenue au port de Valmar	Entrée dans la cellule SSI à 7h30 ; identification des systèmes numériques indispensables au fonctionnement du port.	Image contextualisée, audio, transcription, quiz.
L3	Le port et ses systèmes numériques	Distinction IT/OT, systèmes portuaires exposés, AIS, PMS, TOS, ICS/SCADA, cadres OMI/ISPS et rôle du M-CERT.	Audios, visuels, contenus interactifs, quiz, vidéo interview de Xavier Rebour – Directeur chez France Cyber Maritime.

Leçon	Titre	Contenu	Ressources intégrées
L4	Enjeux et acteurs	Secteurs maritimes les plus exposés, impacts possibles, profils d'attaquants : cybercriminels, hacktivistes, acteurs étatiques, espionnage, sabotage et désinformation.	Texte, audios, quiz.
L5	Les menaces qui ciblent le maritime	Vecteurs d'attaque : clés USB, spearphishing maritime, Business Email Compromise, câbles sous-marins, brouillage/leurage GNSS et cartes marines électroniques.	Texte, audios, quiz.
L6	Cyber for Safety	Lien entre faille numérique et conséquences physiques : propulsion, gouverne, communication, navigation, ballast et interfaces port-navire du ferry Libeccio.	Texte, audios, quiz.
L7	L'utilisateur dans la ligne de mire	Risques humains et usages : accès non tracés, mails personnels sur poste critique, partage de mots de passe, prestataires, BYOD et faux sites de ferry.	Audio, quiz, texte
L8	Glossaire	AIS, BYOD, brouillage GNSS, ICS/SCADA, PMS, TOS...	Glossaire interactif, PDF téléchargeable.
L9	Évaluation	5 QCM en situation professionnelle mobilisant l'ensemble du module : leurage GNSS, dépendances GNSS/PNT, désinformation, OT et BYOD.	5 QCM avec feedback pédagogique.

Module maritime 2/2

Escale sous tension



En 5 leçons, complétées par une leçon de présentation, une page de glossaire, une évaluation finale et une page de crédits/partenaires, ce module plonge l'apprenant dans une crise cyber maritime au Port de Valmar. Il transforme les 7 étapes de gestion de crise en décisions concrètes : détecter, contenir, communiquer, rétablir, documenter et concevoir plus sûr. Ce module fait suite au module « La cybersécurité dans le domaine maritime : Bienvenue au port, qui en est le prérequis.

1 – Objectifs pédagogiques

- Appliquer les 7 étapes de gestion d'une crise cyber maritime
- Analyser les décisions prises à chaque étape dans le contexte d'un incident réel
- Identifier les parties prenantes à contacter et dans quel ordre
- Évaluer les bénéfices d'une approche Security by Design dans le maritime
- Produire les éléments d'un retour d'expérience post-incident

2 – Déroulé par leçon

Leçon	Titre	Contenu	Ressources intégrées
L1	Avant de commencer	Présentation du module, consignes de navigation, accessibilité clavier.	Texte.
L2	L'alerte	Détection à 7h15 d'une anomalie AIS sur le Libeccio ; activation du plan de réponse ; étapes 1 et 2 : préparation, surveillance, signalement, préservation des logs.	Image contextualisée, audio, transcription, quiz.
L3	Contenir la menace	Leurrage GNSS et attaque MitM ; choix d'une isolation ciblée ; étapes 3 et 4 : réaction immédiate, containment, éradication et préservation de l'analyse forensique.	Audios, texte, quiz.

Leçon	Titre	Contenu	Ressources intégrées
L4	Communication de crise	Gestion des communications à 8h00 : 47 appels, journaliste, autorités, M-CERT, compagnie, opérateurs et communication publique maîtrisée.	Texte, audios, quiz.
L5	Rétablissement des opérations	Stabilisation à 10h30 ; audit post-incident, réintégration progressive des systèmes critiques et étape 7 : documenter, corriger, partager avec le secteur.	Texte, audios, quiz.
L6	Retour d'expérience et Security by Design maritime	Débriefing à 14h00 ; exploitation des logs, formalisation d'une action corrective, fermeture automatique de l'interface port-navire et Security by Design.	Audio, quiz, texte, vidéo interview Stéphanie Ledoux – PDG et fondatrice de la société Alcyconie.
L7	Glossaire	ANSSI, M-CERT, logs, MitM, analyse forensique, parties prenantes, audit post-incident	Glossaire interactif, PDF téléchargeable.
L8	Évaluation	6 QCM en situation professionnelle mobilisant la chronologie, la stratégie de l'attaquant, l'isolation ciblée, les systèmes OT, la Security by Design et la collaboration sectorielle.	6 QCM avec feedback pédagogique.

Module transport routier **Annexe**

La cybersécurité dans le transport routier



En 9 étapes, complétées par une leçon d'ouverture, un glossaire et une page de crédits/partenaires, ce module propose une immersion dans un parcours de transport routier réel, depuis la préparation de mission jusqu'à la livraison finale de la marchandise. L'apprenant suit différentes situations de travail du secteur transport pour comprendre les risques cyber à chaque phase, les attaques possibles et leurs conséquences concrètes sur l'activité, les données et la marchandise.

1 – Objectifs pédagogiques

- Situer le secteur du transport routier dans son contexte cybersécurité
- Identifier les risques cyber spécifiques aux différentes étapes d'un parcours de transport routier
- Reconnaître les principales attaques mobilisées dans l'environnement transport : phishing, vol de session, MITM, rootkit, attaques liées aux objets connectés, baiting, DDoS, trojan et fraude à la facturation
- Comprendre les conséquences opérationnelles, financières et commerciales d'un incident cyber dans une entreprise de transport routier
- Adopter les bons réflexes de prévention, d'alerte et de réaction face à une situation suspecte

2 – Déroulé par leçon

Leçon	Titre	Contenu	Ressources intégrées
L1	Introduction générale	Présentation du module, transformation numérique du transport routier, évolution des menaces, conséquences opérationnelles et financières, place du facteur humain.	Texte, contenus interactifs, résumé audio.
L2	Étape 1 : Demande de cotation	Risque de phishing via fausse bourse de fret ; vol d'identifiants, fraude au faux transporteur, signes d'alerte et bons réflexes.	Texte, infographie PDF, document Word, exercices pratiques, quiz, résumé audio.

Leçon	Titre	Contenu	Ressources intégrées
L3	Étape 2 : Planification & affectation du transport	Vol de session dans le TMS ; session abandonnée, détournement invisible, fonctionnement du jeton de session, protocole d'alerte et mesures de sécurité.	Texte, infographie PDF, document Word, activité avancée, quiz.
L4	Étape 3 : Déchargement des marchandises au quai	Attaque Man-in-the-Middle via faux Wi-Fi lors de la transmission d'une e-CMR ; interception des identifiants et falsification de documents.	Texte, infographie PDF, document Word, quiz.
L5	Étape 4 : Planification du transport	Compromission du TMS par keylogger et rootkit ; modification d'ordres de transport, détournement de marchandise, signes d'infection et prévention.	Texte, infographie PDF, documents Word, contenus explicatifs, quiz.
L6	Étape 5 : Stockage des marchandises	Exposition des équipements et systèmes connectés de l'environnement transport ; risques cyber liés aux usages numériques, aux accès et aux vulnérabilités sur la chaîne logistique.	Texte, contenus interactifs, quiz.
L7	Étape 6 : Le chargement du colis	Risques d'introduction de malware et de compromission via supports ou manipulations piégées ; bons réflexes de vérification et de réaction sur le terrain.	Texte, contenus interactifs, quiz.
L8	Étape 7 : Itinéraire du colis	Attaques perturbant les communications, la disponibilité des services ou le suivi du trajet ; conséquences sur la continuité du transport et les opérations.	Texte, contenus interactifs, quiz.

Leçon	Titre	Contenu	Ressources intégrées
L9	Étape 8 : Contrôle du chargement et départ du camion	Attaque de type trojan sur l'informatique embarquée et le GPS ; altération de la position, détournement d'itinéraire et risques physiques pour le conducteur et la cargaison.	Texte, infographie PDF, document Word, quiz.
L10	Étape 9 : Envoi de la facture aux clients	Interception des échanges et fraude au RIB ; modification d'une facture, détournement de paiement, contrôles à mettre en place et vigilance administrative.	Texte, contenus interactifs, quiz.
L11	Glossaire	Définitions des notions clés du module : phishing, MITM, rootkit, trojan, session hijacking, TMS, Wi-Fi, ransomware et autres termes du parcours	Glossaire

Module logistique

La cybersécurité dans le domaine de la logistique



En 11 étapes, complétées par une introduction, une leçon sur le piratage informatique en logistique, un glossaire et une page de crédits/ partenaires, ce module propose une immersion dans un parcours logistique réel, en suivant un camion, son conducteur et les opérateurs logistiques depuis l'arrivée sur site jusqu'aux opérations de facturation. L'apprenant découvre les risques cyber propres à chaque phase, les attaques possibles et leurs conséquences concrètes sur l'activité, les systèmes, les données et la sécurité physique dans l'entrepôt.

1 – Objectifs pédagogiques

- Situer le secteur de la logistique dans son contexte cybersécurité
- Identifier les principales cyberattaques ciblant les opérations de transport et de logistique, ainsi que les méthodes utilisées par les attaquants
- Identifier les risques et les dommages potentiels liés à ces menaces sur la chaîne logistique, les marchandises, les données et la sécurité physique
- Reconnaître les signes précurseurs d'une attaque en repérant rapidement les anomalies sur les outils, les interfaces, les terminaux et les systèmes de gestion
- Adopter les bonnes pratiques de prévention et la bonne réaction face à un incident cyber dans un environnement logistique

2 – Déroulé par leçon

Leçon	Titre	Contenu	Ressources intégrées
L1	Introduction générale	Enjeu stratégique de la cybersécurité dans la logistique, conséquences possibles d'une cyberattaque, objectifs du module.	Texte, visuels, contenus interactifs.
L2	Le piratage informatique en logistique	Définition du piratage informatique, modes d'intrusion sur un réseau, exemple d'attaque et sensibilisation au baiting par clé USB.	Texte, vidéo, résumé de vidéo.

Leçon	Titre	Contenu	Ressources intégrées
L3	Étape 01 : arrivée et enregistrement du camion	Phishing via fausse interface d'enregistrement transporteurs ; vol d'identifiants, accès non autorisé aux systèmes internes, signes d'alerte et bons réflexes.	Texte, contenus interactifs, résumé audio, quiz, PDF téléchargeable.
L4	Étape 02 : affectation et mise à quai	Attaque DDoS contre le logiciel de gestion ; blocage des affectations, paralysie des quais, procédure d'alerte et continuité d'activité.	Texte, contenus interactifs, résumé audio, quiz, PDF téléchargeable.
L5	Étape 03 : déchargement des marchandises	Intrusion via réseau Wi-Fi mal sécurisé et prise de contrôle d'un engin automatisé ; impact sur les opérations et la sécurité physique.	Texte, contenus interactifs, quiz.
L6	Étape 04 : contrôle qualité et quantitatif des marchandises	Détournement invisible de l'interface de contrôle par DNS spoofing ; altération des données et risque d'erreur dans la validation des marchandises.	Texte, contenus interactifs, quiz, PDF téléchargeable.
L7	Étape 05 : stockage des marchandises	Infection par malware via clé USB piégée ; propagation dans le réseau, corruption des données d'inventaire, blocage du WMS et fuite d'informations.	Texte, contenus interactifs, quiz.
L8	Étape 06 : gestion du stock et utilisation du système WMS	Risques cyber liés au système de gestion d'entrepôt, à l'accès aux données de stock et à la manipulation des opérations numériques de suivi.	Texte, contenus interactifs, quiz.

Leçon	Titre	Contenu	Ressources intégrées
L9	Étape 07 : préparation et validation des commandes	Vulnérabilités liées à la préparation de commandes, à la lecture des informations logistiques et à la fiabilité des données utilisées sur le terrain.	Texte, contenus interactifs, quiz.
L10	Étape 08 : contrôle final et validation de l'intégrité des commandes	Vérification de l'intégrité des commandes, contrôle des données et détection d'anomalies avant expédition.	Texte, contenus interactifs, quiz.
L11	Étape 09 : chargement des commandes et validation par terminaux mobiles	Risques liés aux terminaux mobiles, à la validation numérique du chargement et à la fiabilité des échanges entre terrain et système d'information.	Texte, contenus interactifs, quiz.
L12	Étape 10 : contrôle du chargement et départ du camion	Risques cyber lors du départ du camion, contrôle final des informations de transport et exposition des systèmes embarqués ou de traçabilité.	Texte, contenus interactifs, quiz.
L13	Étape 11 : facturation et opérations logistiques	Risques de fraude et d'altération des données lors des opérations administratives et de facturation en fin de chaîne logistique.	Texte, contenus interactifs, quiz.
L14	Glossaire	Définitions des principales notions du module : phishing, DDoS, malware, WMS, TMS, ERP, OT, AGV, IoT et autres termes liés à la cybersécurité logistique.	Glossaire interactif et ressources téléchargeables.

Jeu sérieux

Dans la peau d'un cyberattaquant : le voyage numérique d'un conteneur



Activité transversale de synthèse, ce jeu sérieux mobilise les acquis du module 0 à travers l'ensemble de la chaîne logistique, du port à l'entrepôt. L'apprenant suit le voyage du conteneur XJ-329 de Hong Kong à Bruxelles sur une carte animée, d'abord aux côtés d'un cyberattaquant qui exploite les failles à chaque étape, puis dans la peau d'un responsable cybersécurité chargé de reprendre le contrôle.

1 – Objectifs pédagogiques

- Identifier les failles de sécurité d'une chaîne logistique
- Expliquer comment chaque attaque compromet le système
- Appliquer les bonnes pratiques de sécurité adaptées à chaque menace

2 – Déroulé par étape

Étape	Titre	Contenu	Ressources intégrées
Briefing	Votre mission	Présentation du conteneur XJ-329 et de son dispositif IoT ; consigne : observer 5 cyberattaques puis reprendre le contrôle ; objectif de collecter les 5 badges de cybersécurité.	Narration voix off avec sous-titrage, carte animée.
1/5	Port de Hong Kong : force brute	Attaque par force brute à partir d'identifiants fuités sur le Dark Web ; détection et verrouillage automatiques ; décision de sécurisation (MFA et politique de mots de passe robustes).	Narration sous-titrée, encadré pédagogique, simulation d'attaque, question à choix avec feedback, badge Mot-de-passe.
2/5	Transit maritime : phishing	Email piégé pendant la traversée vers la Turquie ; compromission des identifiants d'une employée et accès au suivi GPS ; réponse à incident (révocation du compte, analyse des logs).	Narration sous-titrée, encadré pédagogique, simulation d'attaque, question à choix avec feedback, badge Phishing.

Étape	Titre	Contenu	Ressources intégrées
3/5	Transport ferroviaire : faille firewall	Scan des ports ouverts sur le réseau ferroviaire paneuropéen et intrusion ; reconfiguration du firewall selon le principe du moindre privilège.	Narration sous-titrée, encadré pédagogique, simulation d'attaque, défi de reconfiguration avec feedback, badge Firewall.
4/5	Transport routier : faille SSH	Connexion SSH illégitime avec privilèges root sur le serveur de gestion de flotte ; analyse des logs, révocation de la clé compromise, désactivation du root.	Narration sous-titrée, encadré pédagogique, simulation d'attaque, défi d'analyse avec feedback, badge SSH.
5/5	Hub de Bruxelles : vulnérabilité réseau	Exploitation d'une vulnérabilité (CVE) sur le hub automatisé, robots et tri IA compromis ; double défi : reprendre le contrôle, puis corriger la faille (patch, segmentation réseau).	Narration sous-titrée, encadré pédagogique, simulation d'attaque, deux défis avec feedback, badge Vulnérabilité.
Fin	Mission accomplie	Synthèse des 5 attaques et des mesures déployées ; récapitulatif des bons réflexes ; badge bonus Maître Défenseur.	Narration sous-titrée, récapitulatif des acquis, badge bonus.



Conseils d'animation

Proposez ce jeu en synthèse, après le Module 0 ou en clôture d'un parcours sectoriel. Comptez environ 45 minutes à 1 heure, débrief compris. Animez ensuite un débrief collectif à partir de trois questions : quelles failles l'attaquant a-t-il exploitées ? Lesquelles pourraient exister dans votre environnement de travail ? Qui prévenir en cas de doute ?

Astuce : les 5 badges donnent la trame du débrief, un badge égale une bonne pratique à faire reformuler par les apprenants.

Crédits et partenaires

Financier principal



BANQUE des
TERRITOIRES



Co-financeurs



TRANSPORT & LOGISTIQUE
Créativité pour l'emploi

« Opération soutenue par l'État dans le cadre de l'AMI « Compétences et Métiers d'Avenir » du Programme France 2030, opéré par la Caisse des Dépôts ». Avec le soutien d'OPCO MOBILITÉS

Partenaires du projet



Avec la participation de

Zelabo
E-SNCF Solutions
Alcyconie
France Cyber Maritime

Remerciements

Nous adressons nos sincères remerciements à :

- la DRANE ;
- l'École de la Deuxième Chance d'Amiens ;
- les établissements scolaires partenaires ;
- Euralogistic