

SCHOOL FOR MATE

LIVRET PÉDAGOGIQUE

Sensibilisation cyber : zéro phishing, zéro ransomware en TPE/PME

CT06 · Module de spécialisation

Ce module donne aux TPE et PME les moyens concrets d'atteindre un objectif ambitieux : zéro phishing réussi, zéro ransomware subi. De l'identification des menaces à la gestion de crise, il prépare aux certifications RS5568 et RS6986 à travers un fil rouge réaliste qui suit une PME pas à pas dans la construction de sa démarche de cybersécurité.

VOLUME HORAIRE	COURS	BLOCS
21 h	6	3

01 · PRÉSENTATION

La formation en bref

Intitulé	Sensibilisation cyber : zéro phishing, zéro ransomware en TPE/PME
Code	CT06
Type	Module de spécialisation
Certificateur	Hors répertoire
Durée	21 h, 6 cours
Modalité	Formation à distance (e-learning), tutorat assuré par l'organisme de formation
Formats	SCORM 1.2 / 2004, xAPI, sources éditables
Mise à jour	Novembre 2026

Le métier et les compétences visées

Le référent cybersécurité en TPE/PME est le professionnel qui, sans être forcément spécialiste à temps plein, porte la démarche de sécurité numérique de l'entreprise. Chef d'entreprise, responsable informatique, directeur technique ou consultant externe, il identifie les enjeux et les menaces qui pèsent sur l'activité, évalue les vulnérabilités du système d'information et vérifie le respect des obligations réglementaires. Il définit une politique de sécurité adaptée à la taille et au budget de la structure : sauvegardes, mises à jour, gestion des accès, surveillance. Il diffuse une culture de l'hygiène numérique auprès de tous les collaborateurs, suit leurs comportements et coordonne la réponse lorsqu'un incident survient, de l'alerte des autorités jusqu'à la reprise de l'activité.

Public visé

- Chefs d'entreprise et dirigeants de TPE/PME
- Référents ou responsables informatiques au sein d'une TPE/PME
- Directeurs techniques (CTO) de PME
- Consultants en systèmes informatiques et techniciens support d'entreprises de services numériques ayant des TPE/PME en portefeuille
- Collaborateurs désignés pour porter la démarche de cybersécurité de leur structure

Prérequis

- Justifier d'un titre ou diplôme de niveau 5, ou, à titre dérogatoire, d'une expérience professionnelle d'au moins 3 ans (prérequis de la certification RS5568)
- Disposer des connaissances de base concernant l'informatique (poste de travail, messagerie, réseau, logiciels courants)
- Avoir accès à un ordinateur connecté à Internet pour suivre le parcours en ligne
- Pour la certification, vérifier auprès de votre organisme de formation les conditions d'accès définies par chaque certificateur

Objectifs pédagogiques

À l'issue du parcours, l'apprenant est capable de :

- Identifier les enjeux d'intelligence économique et de cybersécurité qui touchent l'activité d'une TPE/PME
- Reconnaître les principales menaces (phishing, ransomware, fraude au président, attaques de la chaîne d'approvisionnement) et leurs modes opératoires
- Identifier les responsabilités juridiques de l'entreprise en matière de cybersécurité et de protection des données personnelles
- Réaliser un inventaire du système d'information et analyser ses vulnérabilités à l'aide d'une démarche d'analyse de risques inspirée d'EBIOS RM et d'ISO 27005
- Établir un état des lieux du niveau de sécurité et un plan de sécurisation priorisé
- Définir une politique de sécurité couvrant les mises à jour, les sauvegardes, la surveillance et la gestion des identités et des accès
- Concevoir et animer un programme de sensibilisation accessible à tous les collaborateurs, y compris en situation de handicap
- Mesurer et suivre les comportements et usages des collaborateurs en matière de cybersécurité
- Coordonner la gestion d'une crise cyber : alerte, cellule de crise, communication hors système attaqué, plan de continuité
- Conduire une réponse à incident sans destruction de traces et rédiger un rapport d'incident exploitable

02 · FIL ROUGE PÉDAGOGIQUE

Transports Brévan

NF

Nadia Ferrand

Responsable informatique, désignée référente cybersécurité

Transport routier de marchandises et logistique régionale

Transports Brévan est une PME familiale de 48 salariés installée près d'Angers. Elle gère une flotte de poids lourds, un entrepôt et un logiciel de gestion des tournées connecté aux systèmes de plusieurs clients industriels. Ses chauffeurs utilisent des tablettes, la comptabilité est partiellement externalisée et la messagerie est hébergée dans le cloud. Un lundi matin, la comptable reçoit un courriel imitant parfaitement un fournisseur de carburant et demandant un changement de coordonnées bancaires. Le virement est bloqué de justesse. Le dirigeant, Laurent Brévan, prend conscience de l'exposition de son entreprise et confie à Nadia Ferrand, responsable informatique depuis quatre ans, la mission de bâtir une véritable démarche de cybersécurité, avec un budget limité et sans recrutement supplémentaire.

Chaque cours se termine par une mise en situation dans cette entreprise : l'apprenant accompagne Nadia dans des situations professionnelles réalistes, de plus en plus complexes, jusqu'à la préparation des épreuves.

La progression

1. Bloc M1 : Nadia analyse la tentative de fraude, cartographie les menaces qui visent un transporteur et présente au dirigeant les responsabilités juridiques de l'entreprise.
2. Bloc M2 : Nadia inventorie le système d'information, mène une analyse de risques, dresse l'état des lieux et rédige la politique de sécurité de Transports Brévan.
3. Bloc M3 : Nadia déploie un programme de sensibilisation pour les bureaux, l'entrepôt et les chauffeurs, puis pilote la réponse à une attaque par ransomware sur le serveur de l'entrepôt.

03 · ARCHITECTURE

Organisation du parcours

Le parcours est construit sur les compétences visées : chaque bloc regroupe les cours qui préparent à son évaluation.

N°	Bloc et cours	Durée
M1 · Comprendre les enjeux, les menaces et le cadre juridique de la cybersécurité		**7 h**
1	Enjeux de cybersécurité et d'intelligence économique en TPE/PME	3 h
2	Menaces cyber, veille et responsabilités juridiques de l'entreprise	4 h
M2 · Diagnostiquer et sécuriser le système d'information		**7 h**
3	Inventaire du SI, analyse de risques et état des lieux de sécurité	3 h 30
4	Politique de sécurité, sauvegardes et gestion des identités et des accès	3 h 30
M3 · Sensibiliser les collaborateurs et gérer les incidents cyber		**7 h**
5	Déployer et suivre une culture de cybersécurité dans l'entreprise	3 h 30
6	Gérer une crise cyber et conduire la réponse à incident	3 h 30
Total du parcours		**21 h**

Répartition des modalités pédagogiques

Chaque sous-chapitre s'ouvre sur une vidéo de 3 à 5 minutes. La vidéo représente 30 % du volume horaire, complétée par du cours texte enrichi, des infographies, des études de cas, des mises en situation et des QCM.



- Vidéos : 6 h 30
- Cours texte et infographies : 6 h 30
- Études de cas et mises en situation : 5 h
- QCM et évaluations : 3 h

04 · PROGRAMME DÉTAILLÉ

Contenu des cours

M1 · 7 h

Comprendre les enjeux, les menaces et le cadre juridique de la cybersécurité

Cours 1 · Enjeux de cybersécurité et d'intelligence économique en TPE/PME

3 h

OBJECTIFS

- Identifier les actifs stratégiques et le patrimoine immatériel d'une TPE/PME
- Relier les enjeux de cybersécurité aux enjeux économiques, réputationnels et concurrentiels de l'entreprise

ÉVALUATION FORMATIVE

QCM de compréhension et étude de cas courte : identification des actifs critiques d'une PME

CONTENUS

- Pourquoi les TPE/PME sont devenues des cibles privilégiées
- Intelligence économique : protéger l'information stratégique de l'entreprise
- Patrimoine immatériel : données clients, savoir-faire, fichiers, accès partenaires
- Les conséquences d'une cyberattaque : financières, opérationnelles, juridiques, réputationnelles
- Le rôle et le positionnement du référent cybersécurité
- Panorama des acteurs ressources : ANSSI, Cybermalveillance.gouv.fr, CNIL

Fil rouge · Après la tentative de fraude au fournisseur, Nadia recense avec Laurent Brévan les informations et activités les plus critiques de l'entreprise (planning des tournées, fichier clients, accès aux portails des donneurs d'ordre) afin de mesurer ce qu'une attaque réussie aurait coûté.

Cours 2 · Menaces cyber, veille et responsabilités juridiques de l'entreprise

4 h

OBJECTIFS

- Reconnaître les principales menaces et leurs modes opératoires, dont le phishing, le ransomware et les attaques de la chaîne d'approvisionnement
- Mettre en place une politique de veille sur les menaces internes et externes
- Identifier les obligations et responsabilités juridiques de l'entreprise en matière de cybersécurité et de données personnelles

ÉVALUATION FORMATIVE

Exercice d'analyse de courriels suspects et QCM sur le cadre juridique

CONTENUS

- Hameçonnage, harponnage et fraude au président : anatomie d'une attaque par ingénierie sociale
- Ransomware : modes d'infection, chiffrement, double extorsion
- Attaques de la chaîne d'approvisionnement : altération de code, diffusion massive de code malveillant, détournement d'applications légitimes
- Menaces internes : erreurs humaines, malveillance, départs de collaborateurs
- Organiser une veille sur les menaces : sources, fréquence, diffusion
- Responsabilités juridiques : RGPD, obligation de sécurité des données, notification des violations à la CNIL
- Responsabilité du dirigeant, contrats fournisseurs et clauses de sécurité, évolutions réglementaires européennes (directive NIS 2)

Fil rouge · Nadia décortique le faux courriel du fournisseur de carburant pour en extraire les indices d'alerte, puis rédige une note au dirigeant précisant ce que la loi aurait imposé à Transports Brévan si des données de clients avaient été dérobées.

M2 · 7 h
Diagnostiquer et sécuriser le système d'information

Cours 3 · Inventaire du SI, analyse de risques et état des lieux de sécurité

3 h 30

OBJECTIFS

- Analyser l'organisation interne et réaliser l'inventaire des équipements, logiciels et interconnexions
- Évaluer les vulnérabilités et les risques associés en mobilisant les principes d'EBIOS RM et d'ISO 27005
- Établir un état des lieux du niveau de sécurité et un plan de sécurisation priorisé

ÉVALUATION FORMATIVE

Étude de cas : réalisation d'une matrice des risques et d'un état des lieux à partir d'un dossier d'entreprise

CONTENUS

- Cartographier l'organisation : acteurs, rôles, flux d'information, prestataires
- Inventorier équipements, logiciels, comptes et interconnexions avec l'extérieur
- Identifier les vulnérabilités techniques et organisationnelles
- Les méthodes d'analyse de risques : principes d'EBIOS RM et d'ISO 27005 adaptés à une TPE/PME
- Évaluer la conformité aux obligations réglementaires
- Construire l'état des lieux et le plan de sécurisation du SI
- Présenter les résultats à la direction et obtenir les arbitrages

Fil rouge · Nadia inventorie les postes, les tablettes des chauffeurs, le serveur de l'entrepôt et les connexions aux portails clients, puis présente à Laurent Brévan une matrice des risques et un plan de sécurisation en trois priorités.

Cours 4 · Politique de sécurité, sauvegardes et gestion des identités et des accès

3 h 30

OBJECTIFS

- Définir les règles de sécurité relatives à l'usage du SI, aux mises à jour, aux antivirus et aux sauvegardes
- Préconiser une solution de surveillance adaptée à la taille de l'entreprise (EDR, SIEM)
- Définir les modalités de gestion des identités et des contrôles d'accès

ÉVALUATION FORMATIVE

Mise en situation : rédaction d'extraits de politique de sécurité et QCM sur les mesures techniques

CONTENUS

- Structurer une politique de sécurité du système d'information proportionnée
- Mises à jour des appareils, des logiciels et des antivirus : organiser et contrôler
- Stratégie de sauvegarde : sauvegardes déconnectées, tests de restauration
- Solutions de surveillance : rôles respectifs de l'EDR et du SIEM, critères de choix pour une PME
- Gestion des identités : création, revue et suppression des comptes, comptes à privilèges
- Authentification multifacteur et politique de mots de passe
- Contrôler les équipements et les prestataires ayant un accès technique au SI

Fil rouge · Nadia rédige la politique de sécurité de Transports Brévan : sauvegarde hors ligne du logiciel de tournées, authentification multifacteur sur la messagerie, revue trimestrielle des accès du prestataire comptable et choix argumenté d'une solution de surveillance des postes.

M3 · 7 h
Sensibiliser les collaborateurs et gérer les incidents cyber

Cours 5 · Déployer et suivre une culture de cybersécurité dans l'entreprise

3 h 30

OBJECTIFS

- Établir un code de bonne conduite et diffuser les règles d'hygiène fondamentales de la cybersécurité
- Concevoir un programme de sensibilisation accessible à tous les publics, y compris les collaborateurs en situation de handicap
- Mesurer et suivre les comportements et usages des collaborateurs

ÉVALUATION FORMATIVE

Projet guidé : conception d'un plan de sensibilisation avec indicateurs de suivi, et QCM

CONTENUS

- Les règles d'hygiène informatique fondamentales pour l'organisation et les individus
- Rédiger une charte informatique et un code de bonne conduite : précautions techniques et juridiques
- Choisir les supports de sensibilisation : affiches, capsules courtes, ateliers, quiz
- Organiser des campagnes de simulation d'hameçonnage dans un cadre éthique et transparent
- Rendre la sensibilisation accessible aux collaborateurs en situation de handicap
- Vérifier la compréhension des enjeux : risques, réputation, conséquences financières
- Indicateurs de suivi des comportements et amélioration continue

Fil rouge · Nadia conçoit un programme adapté à trois publics (bureaux, entrepôt, chauffeurs sur tablette), lance une première campagne de simulation d'hameçonnage et adapte les supports pour un préparateur de commandes malentendant.

Cours 6 · Gérer une crise cyber et conduire la réponse à incident

3 h 30

OBJECTIFS

- Organiser l'alerte, la cellule de crise et la communication indépendante du système attaqué
- Conduire une réponse à incident sans destruction de données ni de traces
- Rédiger un rapport d'incident et capitaliser pour éviter la récidive

ÉVALUATION FORMATIVE

Simulation de crise interactive avec chronologie de décisions à prendre et rapport d'incident à compléter

CONTENUS

- Les premiers réflexes : sécuriser les personnes, les lieux et les équipements
- Alerter les bons interlocuteurs : autorités, banque, CNIL, personnes concernées, assureur
- Mettre en place une cellule de crise et des moyens de communication hors SI
- Identifier les indicateurs de compromission et évaluer l'étendue de l'incident
- Isoler l'élément compromis en préservant les traces, puis restaurer l'activité
- Déclencher et ajuster le plan de continuité d'activité
- Rédiger le rapport d'incident et diffuser les enseignements aux collaborateurs

Fil rouge · Un vendredi soir, le serveur de l'entrepôt affiche une demande de rançon : Nadia isole la machine sans l'éteindre, réunit la cellule de crise par téléphone, organise les livraisons du lundi en mode dégradé et rédige le rapport d'incident présenté à la direction.

05 · CONFORMITÉ AU RÉFÉRENTIEL

Couverture des compétences

Correspondance entre les compétences visées et les cours du parcours.

Compétence	Bloc	Cours
RS5568 C1 : Identifier les enjeux d'intelligence économique et de cybersécurité touchant l'activité	M1	1
RS5568 C2 : Identifier les risques et menaces pour le SI et le patrimoine immatériel	M1	1, 2
RS5568 C3 : Identifier les responsabilités juridiques en cybersécurité et protection des données	M1	2
RS5568 C4 : Analyser l'organisation interne et le système d'information	M2	3
RS5568 C5 : Évaluer les vulnérabilités et le niveau de sécurisation	M2	3
RS5568 C6 : Établir un état des lieux de la sécurité et du respect des obligations réglementaires	M2	3
RS5568 C7 : Déterminer les actions à mettre en œuvre et les supports à déployer	M2, M3	4, 5
RS5568 C8 : Diffuser les bonnes pratiques et règles d'hygiène fondamentales	M3	5
RS5568 C9 : Systématiser l'application des règles d'hygiène pour l'organisation et les individus	M2, M3	4, 5
RS5568 C10 : Opérer le suivi des comportements et usages en cybersécurité	M3	5
RS6986 C1 : Analyser la vulnérabilité de l'entreprise (inventaire, veille, analyse de risques EBIOS RM / ISO 27005)	M1, M2	2, 3
RS6986 C2 : Établir un état des lieux, un plan de sécurisation et sensibiliser la direction	M1, M2, M3	2, 3, 6
RS6986 C3 : Définir une politique de sécurité (surveillance, mises à jour, sauvegardes)	M2	4
RS6986 C4 : Gérer les identités et contrôles d'accès	M2	4
RS6986 C5 : Sensibiliser les collaborateurs et infuser une culture de la cybersécurité	M3	5
RS6986 C6 : Gérer une situation d'urgence par l'alerte et la sécurisation	M3	6
RS6986 C7 : Réaliser les opérations de réponse à incident sans destruction de traces	M3	6

Évaluations formatives

Chaque cours se conclut par une évaluation formative adaptée à la compétence travaillée : QCM de compréhension, analyse de courriels suspects, études de cas, rédaction de livrables (matrice des risques, extraits de politique de sécurité, plan de sensibilisation, rapport d'incident) et simulation de crise interactive. Les QCM sont corrigés automatiquement avec des explications détaillées pour chaque réponse. Les livrables s'appuient sur des modèles et des corrigés types qui permettent à l'apprenant de s'autoévaluer et au formateur de l'organisme de formation d'assurer un suivi individualisé. Les résultats sont tracés sur la plateforme, ce qui fournit à l'organisme les preuves de suivi et d'acquisition attendues dans le cadre de Qualiopi.

Modalités de certification

Bloc	Modalité d'évaluation
RS5568 (couverte par M1, M2 et M3)	Les modalités d'évaluation ne sont pas détaillées dans les données du référentiel transmises. Elles sont définies par le certificateur CCI France et doivent être vérifiées dans la fiche RS5568 en vigueur sur le site de France Compétences. L'organisme de formation reste seul responsable de l'inscription et de l'organisation de la certification.
RS6986 (couverte par M1, M2 et M3)	Les modalités d'évaluation ne sont pas détaillées dans les données du référentiel transmises. Elles sont définies par le certificateur ECOLE SUP INFORM COMMERCE et doivent être vérifiées dans la fiche RS6986 en vigueur sur le site de France Compétences. L'organisme de formation reste seul responsable de l'inscription et de l'organisation de la certification.

Le parcours reprend une à une les capacités attestées des deux certifications, comme le montre la matrice de couverture. Les livrables produits dans le fil rouge Transports Brévan (cartographie des menaces, inventaire du SI, matrice des risques, état des lieux, politique de sécurité, plan de sensibilisation, rapport d'incident) correspondent aux productions qu'un référent cybersécurité doit savoir réaliser et constituent une base solide pour préparer les épreuves, quelle que soit leur forme. L'apprenant peut les transposer à sa propre entreprise ou à un cas fourni par l'organisme de formation. Nous vous recommandons de compléter le parcours par une séance de préparation spécifique aux modalités du certificateur choisi, animée par vos formateurs.

06 · MOYENS ET PERSPECTIVES

Moyens pédagogiques et débouchés

Moyens pédagogiques et techniques

- Plateforme e-learning en marque blanche, accessible 24 h/24 sur ordinateur, tablette et smartphone, avec suivi de progression et traçabilité des connexions
- Une vidéo de 3 à 5 minutes par sous-chapitre, représentant 30 % du volume horaire du parcours
- Cours texte enrichi, infographies et fiches réflexes téléchargeables (hygiène informatique, premiers gestes en cas d'incident)
- Fil rouge Transports Brévan avec mises en situation et études de cas dans chaque cours
- Modèles de livrables : grille d'inventaire, matrice des risques, trame de politique de sécurité, charte informatique, modèle de rapport d'incident
- QCM corrigés automatiquement et simulation de crise interactive
- Ressources de référence publiques citées et commentées (guides de l'ANSSI, Cybermalveillance.gouv.fr, CNIL)

Débouchés et évolutions

- Référent cybersécurité en TPE/PME
- Responsable informatique en TPE ou PME intégrant le pilotage de la cybersécurité
- Directeur technique (CTO) de PME
- Consultant en systèmes informatiques accompagnant des TPE/PME sur leur démarche de cybersécurité
- Technicien support informatique chargé de comptes TPE/PME
- Chef d'entreprise pilotant lui-même la sécurité numérique de sa structure

Accessibilité

Contenus sous-titrés en français, contrastes conformes WCAG AA, navigation au clavier sur les écrans interactifs. L'organisme de formation qui diffuse le parcours adapte les modalités d'accompagnement aux personnes en situation de handicap avec son référent handicap.

Livrables fournis à l'organisme de formation

- Package SCORM 1.2 / 2004 et xAPI, compatible avec les principaux LMS
- Sources éditables des cours, scripts vidéo et banques de QCM
- Livret apprenant et grilles d'évaluation
- Licence marque blanche à vie, stagiaires illimités, maintenance 24 mois

School For Mate
On crée vos formations, vous n'avez plus qu'à les diffuser.

contact@schoolformate.com · catalogue-2026-sfm.netlify.app

La délivrance de la certification relève exclusivement du certificateur et de l'organisme de formation habilité. Document non contractuel, susceptible d'évoluer avec le référentiel.