

A background image showing a desk setup with a laptop, a keyboard, two pens, and a cup of coffee with latte art. The image is partially framed by a white border and an orange border.

FORMATION ET SENSIBILISATION À LA CYBERSÉCURITÉ

2023

A decorative graphic consisting of a grid of orange dots of varying sizes, arranged in a pattern that tapers to the right.

Catalogue de formation
Distanciel

WWW.PHOSFOREA.COM





Laurent PELUD

*Président de SCASSI,
PHOSFOREA et JUNE Factory*

SCASSI est depuis plus de 18 ans un expert reconnu du monde de la cybersécurité. Basés à Toulouse, Paris et Madrid, nous assurons la gestion des risques pour nos clients, grands comptes des secteurs industriel, bancaire et public.

Pour mener à bien notre mission, nous concilions expertise technique et approche du facteur humain afin d'apporter des réponses sur-mesure aux besoins de nos clients.

Parce que la sécurité des systèmes d'information n'est pas qu'une question d'outils et d'antivirus, nous avons développé au cours des années une solide offre de formation et de sensibilisation.

Afin de donner à chacun les connaissances et le savoir-faire nécessaires à la protection du SI dans son ensemble.

Phosforea® est la filiale dédiée à la formation. Elle propose une offre pensée pour vous, qui êtes sur le terrain tous les jours. Pragmatique et orientée métier, elle saura s'adapter à vos problématiques et répondre à votre besoin de montée en compétences.

Chez Phosforea, nous croyons que l'humain sera demain le maillon fort de la sécurité de votre entreprise. Vous découvrirez à travers les pages de ce catalogue une offre riche et adaptée à tous les niveaux de connaissance : depuis le collaborateur novice sur les sujets cyber, qu'il vous faut motiver et impliquer, jusqu'à l'expert SSI dont vous souhaitez valoriser les compétences à travers une certification reconnue.



Thomas ROBERT

*Directeur des Opérations
et du Développement
PHOSFOREA*

Bonne lecture !



SOMMAIRE



PRÉAMBULE.....7

Présentation de Phosforea.....	9
Une plateforme.....	10
6 bonnes raisons de choisir Phosforea.....	11
L'équipe Phosforea.....	12

CAMPAGNES DE SENSIBILISATION SSI.....13

Notre offre essentielle.....	15
Notre Ligne pédagogique.....	16
Modules.....	17
Vidéos.....	19
Capsules.....	21
Activ'Learning.....	23
Notre offres professionnelle.....	25
Notre solution sur-mesure.....	26
Sensibilisation métier.....	27
Campagne de faux-phishing.....	28
L'accompagnement marketing.....	30
Kit de communication.....	31

FORMATIONS & CERTIFICATIONS.....32

— Métier développeur.....	34
— RGPD et métier DPO.....	35
— Métier IT.....	37
— Métier chef de projet.....	43
— Autres formations.....	45

A CHAQUE MÉTIER SA FORMATION



		Admin / Commerce / Utilisateurs	Administrateurs Système, Réseau et Sécurité	Architecte Applicatif	Ingénieur Sécurité
Les fondamentaux de la SSI	Bonnes pratiques de cybersécurité	✓	✓	✓	✓
	Introduction à la sécurité des systèmes critiques	✓	✓	✓	✓
	Fondamentaux de la sécurité de l'information	✓	✓		✓
RGPD et métier DPO	RGPD	✓	✓	✓	✓
	RGPD - santé	✓	✓	✓	✓
	Fondamentaux du RGPD - Mettre l'entreprise en conformité				
Métier IT	Référent cybersécurité		✓		✓
	Gestion de crise	✓	✓		✓
	Management d'un programme d'audit		✓		✓
	Management de la sécurité dans les développements		✓		✓
Métier développeur	Sécurité dans les développements - Intermédiaire		✓	✓	✓
	Sécurité dans les développements - Avancé		✓	✓	✓
	Sécurité dans les développements (expertise)			✓	
	Certified Ethical Hacker - CEH		✓	✓	✓
Métier chef de projet	Sécurité dans les projets		✓	✓	✓
	Critères Communs		✓		✓
	Analyse de risques : principes et utilisation	✓	✓		✓
	Management de la sécurité dans les développements		✓	✓	✓
Gouvernance et conformité SSI	SMSI - ISO 27001 Fondamentaux		✓		✓
	SMSI - ISO 27001 Lead Auditor				✓
	SMSI - ISO 27001 Lead Implementor				✓
	Recommandations HDS pour le SMSI				✓
	Analyse de risques - ISO 27005 Risk Manager		✓	✓	✓
	Analyse de risques -EBIOS		✓	✓	✓
Sécurité des systèmes critiques	Introduction à la sécurité des systèmes critiques		✓	✓	✓



PRÉAMBULE

Présentation de Phosforea.....	9
Une plateforme.....	10
6 bonnes raisons de choisir Phosforea.....	11
L'équipe Phosforea.....	12



PRÉSENTATION

Sensibiliser et former à la sécurité informatique n'a jamais été aussi simple.

DES CONTENUS

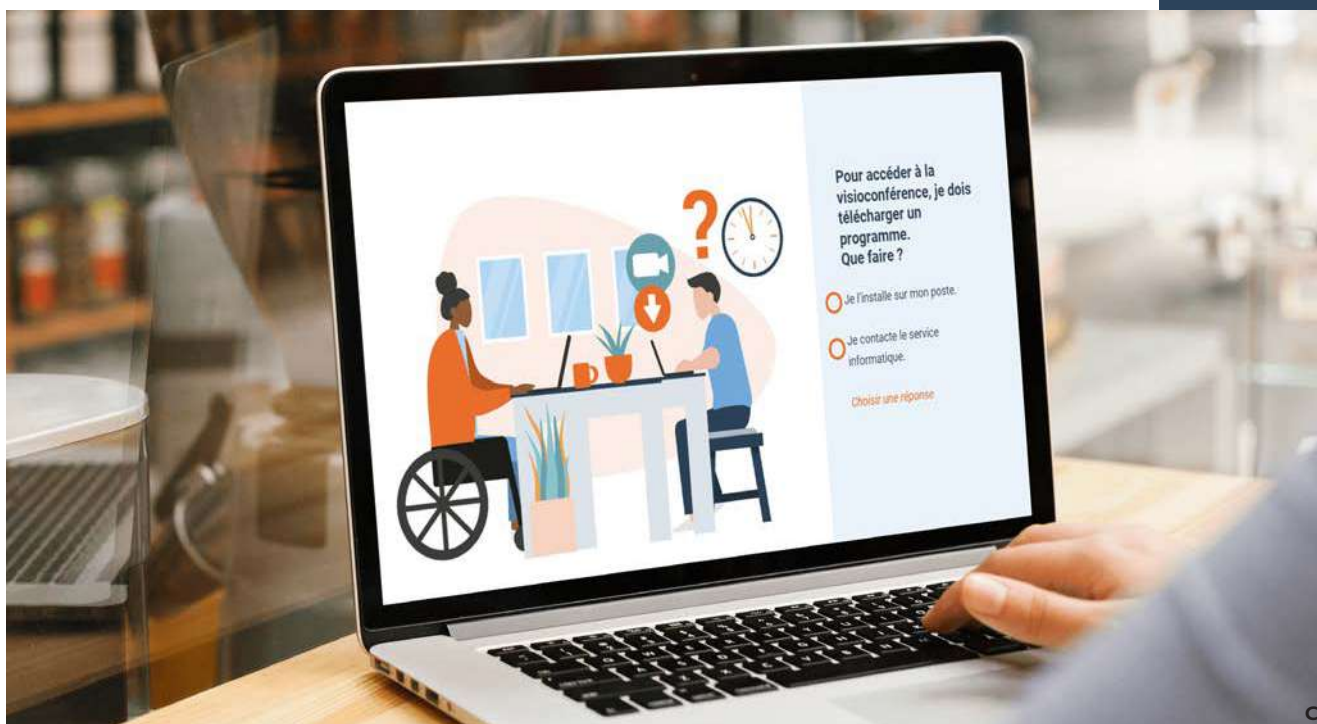
Phosforea, c'est avant tout plus de 120 contenus de sensibilisation et de formation en cybersécurité.

Notre approche « Work based learning » permet à chaque apprenant de se plonger rapidement dans le sujet, quel que soit son niveau de technicité, grâce à une mise en situation professionnelle illustrée par des cas concrets. Nous travaillons sur 4 niveaux de connaissance : de novice à expert !

DES SERVICES

Parce que nous croyons qu'une bonne formation est une formation qui répond à vos besoins en termes de compétences et de supports, nous avons développé divers services : personnalisation des modules de sensibilisation, gestion des compétences de vos collaborateurs, campagnes de communication interne pour promouvoir une action de sensibilisation, parcours de formation e-learning sur-mesure selon les profils de vos collaborateurs...

N'hésitez pas à nous solliciter !



UNE PLATEFORME

Une plateforme e-learning clé-en-main !

Pour les RSSI/DSI et les apprenants :

Avec Phosforea, vous choisissez la formule qui vous convient le mieux pour mettre à disposition vos formations : notre plateforme e-learning s'adapte à vos besoins.

Nous pouvons la personnaliser à votre image, afin de la rendre plus proche de vos collaborateurs.

Vous gérez vos campagnes de formation directement depuis votre tableau de bord administrateur et vous en mesurez les résultats en deux clics, grâce aux rapports et analyses simplifiés.



Déploiement rapide des campagnes e-learning sur notre plateforme LMS.



Mode SaaS : accès web, nous assurons la maintenance et la disponibilité



Accès aux cours : **24h/24**



Suivi individualisé des apprenants, relances et édition des attestations de suivi



**N'ATTENDEZ PLUS ET
DEMANDEZ UNE DÉMO !**



6 RAISONS DE CHOISIR PHOSFOREA



La certification qualité a été délivrée au titre de la catégorie d'action suivante : **ACTIONS DE FORMATION**

1

DE LA SENSIBILISATION À LA CERTIFICATION

Phosforea accompagne l'ensemble de vos apprenants en proposant un programme complet.

2

DES NIVEAUX DE FORMATION

Phosforea permet à chaque apprenant de suivre un parcours de formation adapté à son besoin tout en prenant en compte ses acquis.

3

UNE APPROCHE EN BLENDED-LEARNING

Cette approche permet d'optimiser le temps de formation de tous les collaborateurs et de limiter les déplacements en formation, tout en garantissant un parcours de formation de qualité.

4

RÉFÉRENCÉ QUALIOPi

C'est un gage de qualité pour Phosforea car nos formations sont prises en charge par les organismes financeurs.

5

DES CONTENUS «SUR-MESURE»

Chez Phosforea nous savons que chaque entreprise est unique, c'est pour cela que nos contenus s'adaptent à vos besoins.

6

UNE ÉQUIPE À VOTRE ÉCOUTE

Une équipe proche de vous et des interlocuteurs disponibles pour vous accompagner tout au long de votre projet : voilà la force de notre proposition !



NOTRE ÉQUIPE

La formation en cybersécurité,
pour les professionnels par des
professionnels



ÉQUIPE PÉDAGOGIQUE



Caroline BARREAU
*Directrice Pédagogique & Chef
de projet*



Morgane MADEC
*Ingénieure et Conceptrice
Pédagogique*



Céline ROUVRAIS
*Ingénieure et Conceptrice
Pédagogique*

DESIGN & MULTIMÉDIA



Pauline BERRIOT
Infographiste



Maria PAGAN GUTIERREZ
Infographiste

ÉQUIPE TECHNIQUE WEB/LMS



Paco CERVANTES
*Directeur Technique & Chef de
projet*



Ludovic HUGENOT
Lead Dev



Jonathan DELHOUX
Développeur Web



Dirk-Dominik DOLLE
Développeur Web

CHEFFERIE DE PROJET



Vincent FEUILLERAT
Chef de projet

NOS FORMATEURS

Notre équipe technique formateurs
experts cybersécurité



Jean-Philippe POMIES

Ingénieur Sécurité
Sécurité des applications
Responsable du pôle
Evaluation technique



Emmanuel WILDEMANN

Ingénieur Sécurité
ISO 27001 / 27005 / EBIOS
Directeur Technique



Sylvain DAUMAS

Ingénieur Sécurité
Sécurité des applications
Responsable du pôle
Gouvernance & Conformité



Ludovic BOMBAIL

Ingénieur Sécurité
Co-Responsable du pôle
Gouvernance & Conformité



Julien CHEZEAUX

Ingénieur Sécurité
CEH



CAMPAGNES DE SENSIBILISATION SSI



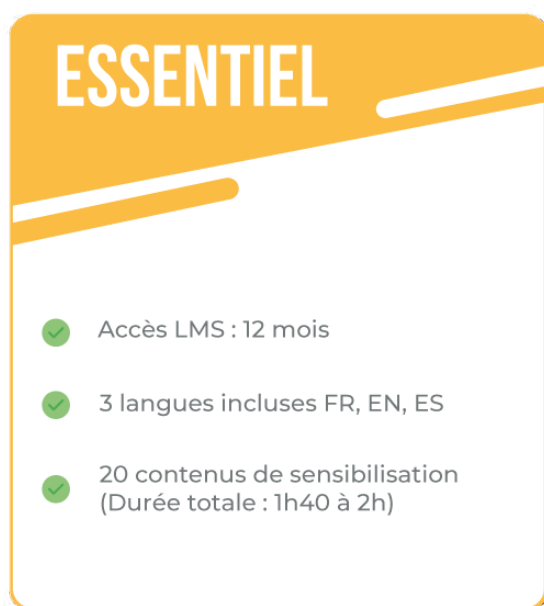
Notre offre essentielle.....	15
Notre Ligne pédagogique.....	16
Modules.....	17
Vidéos.....	19
Capsules.....	21
Activ'Learning.....	23
Notre offres professionnelle.....	25
Notre solution sur-mesure.....	26
Sensibilisation métier.....	27
Campagne de faux-phishing.....	28
L'accompagnement marketing.....	30
Kit de communication.....	31



NOTRE OFFRE ESSENTIELLE



Afin de répondre à votre besoin, nous vous proposons **une campagne de sensibilisation clé-en-main** composée des éléments suivants :



DES CONTENUS DE SENSIBILISATION À LA CYBERSÉCURITÉ

Mise à disposition de 20 contenus e-learning sur un ensemble de thématiques SSL.

UNE PLATEFORME E-LEARNING

- Diffusion pendant **12 mois** sur la **plateforme LMS Phosforea®** (www.phosforea.com)
- Inscription des **apprenants** et des **administrateurs**
- **Formation des administrateurs** pour inscrire les apprenants, suivre leur progression et relancer les retardataires
- Génération de statistiques de participation de suivi.

UN DÉPLOIEMENT DU PROJET RAPIDE

peu consommateur de temps pour le client et un suivi optimal par un **chef de projet** Phosforea

Prenez contact avec notre équipe et échangez sur la meilleure formule pour répondre à votre besoin

LIGNE PÉDAGOGIQUE



L'offre essentielle se décline en 2 gammes graphiques :

MENTOR ou **ACTIVE**



GAMME MENTOR - 2H (ESSENTIEL 1)

8 MODULES : Mot de passe, USB, E-mail, Ingénierie sociale, Sécurité sur Internet, Sécurité Physique, Mobilité Professionnelle, Cybersécurité tous concernés

9 VIDEOS : Cible, Ransomware, Données Privées, Bureau propre, Menaces informatiques, RGPD, Ingénierie Sociale, Wi-Fi, Smartphone

3 CAPSULES : Phishing, Shadow It, Télétravail

GAMME ACTIVE - 1H40 (ESSENTIEL 2)

10 ACTIV'LEARNING : J'identifie les tentatives d'hameçonnage, Je m'authentifie, Je sécurise mes données, Je navigue sur internet, Je télétravaille et suis mobile, Je protège mon matériel informatique, Je protège mon espace de travail, Je suis hyper connecté(e), Je voyage à l'étranger, Je suis « Éconumérique »

10 VIDEOS : Mot de passe, Cible, Ransomware, Données Privées, Bureau propre, Menaces informatiques, RGPD, Ingénierie Sociale, Wi-Fi, Smartphone

MODULES DE SENSIBILISATION

13 modules interactifs et ludiques entièrement sonorisés et sous-titrés pour faire passer les messages auprès de l'ensemble de votre personnel

LES CONTENUS



MOT DE PASSE

Créer un mot de passe complexe et comprendre son utilité



PÉRIPHÉRIQUES USB

Utiliser les périphériques USB en sécurité



ACCÈS AUX DONNÉES

Savoir ce qu'est une donnée, comment y accéder et les moyens de la protéger



BYOD

Comprendre les bonnes pratiques d'utilisation des équipements personnels en contexte professionnel



E-MAIL

Différencier les e-mails malveillants des e-mails légitimes



INGÉNIERIE SOCIALE

Comprendre les mécanismes d'acquisition déloyale d'information



SÉCURITÉ SUR INTERNET

Naviguer sur Internet en toute sécurité



SÉCURITÉ PHYSIQUE

Comprendre pourquoi et comment être vigilant avec la sécurité physique



MOBILITÉ PROFESSIONNELLE

Respecter les règles de sécurité lors d'un déplacement professionnel



RÉAGIR À UN INCIDENT

Développer les bons réflexes face à un incident de sécurité

**10 - 15
MINUTES**



**SONORISÉ ET
SOUS-TITRÉ**

MULTILANGUES



DISPONIBLE

GAMME MENTOR



AUTHENTIFICATION

Mettre en œuvre les principes de l'authentification



CYBERSÉCURITÉ, TOUS CONCERNÉS

Identifier les risques cyber et comprendre les enjeux de la cybersécurité



RGPD

Expliquer les objectifs et enjeux de la réglementation RGPD

VIDÉOS DE SENSIBILISATION

17 «minutes sécurité» ludiques de 1 à 2 minutes qui permettent de se familiariser avec un vocabulaire simple sur un sujet de cybersécurité.

LES CONTENUS



CIBLE

Comprendre les intérêts des pirates et être capable de protéger ses données



MOT DE PASSE

Créer un mot de passe sécurisé



PHISHING

Eviter de se faire hameçonner



INGÉNIERIE SOCIALE

Reconnaître les techniques de manipulation des pirates



RGPD

Identifier les enjeux de la Réglementation Générale sur la protection des Données Personnelles



RANSOMWARE

Empêcher la contamination de son entreprise par un cryptovirus



VACANCES

Partir en vacances en sécurité



CHIFFREMENT

Chiffrer les informations pour les manipuler et les transmettre



BUREAU PROPRE

Ranger son bureau pour protéger ses informations



WI-FI

Utiliser les réseaux Wi-Fi en sécurité

2
MINUTES



MULTILANGUES



DISPONIBLE

GAMME MENTOR

GAMME ACTIVE



CLOUD

Utiliser le cloud en sécurité



MENACES INFORMATIQUES

Reconnaître les menaces informatiques



TÉLÉTRAVAIL

Travailler en sécurité de son domicile comme au bureau



SMARTPHONE

Utiliser ses appareils nomades en sécurité



DONNÉES PRIVÉES

Découvrir qui exploite les données privées sur le Web



ACHATS EN LIGNE

Effectuer ses achats en ligne en toute sécurité



SMISHING

Se protéger des SMS malveillants

CAPSULES DE SENSIBILISATION

11 capsules de formation réparties en micro séquences d'information.



Pour réaliser ces contenus, nous avons effectué les choix scénaristiques suivants :

- Un style graphique One Page et une dimension ludique apportée par une mascotte d'accompagnement.
- Navigation en « scrollant » (déroulement vertical similaire à une page web)
- Un contenu responsive basé sur les codes du web et non sonorisé.
- Une approche pédagogique micro-learning, très proche du jeu (quiz, cartes à retourner, cherche-et-trouve, etc.)
- Une fiche de synthèse téléchargeable en fin de contenu

LES CONTENUS



ENVOI

Diffuser un document confidentiel à un client ou un collaborateur en toute sécurité



PHISHING

Détecter un message malveillant pour ne pas se faire hameçonner



DONNÉES

Appliquer les bonnes pratiques de protection des données tout au long de leur cycle de vie



RÉSEAUX SOCIAUX

Communiquer de manière responsable sur les réseaux sociaux

5
MINUTES



8 LANGUES



DISPONIBLE

GAMME MENTOR

GAMME ACTIVE



CYBER-RESPONSABLE

S'impliquer efficacement dans la cybersécurité de l'entreprise



SHADOW-IT

Protéger l'entreprise de l'utilisation de ressources externes



FAKE NEWS

Distinguer le vrai du faux sur Internet



IoT

Assurer la sécurité de l'entreprise lorsque tout est interconnecté



MESSAGERIE

S'assurer que l'accès à sa boîte mail reste un secret bien gardé



E-RÉPUTATION

Préserver sa réputation sur Internet



TÉLÉTRAVAIL

RESPECTER LES RÈGLES DE CYBERSÉCURITÉ EN SITUATION DE TÉLÉTRAVAIL

ACTIV'LEARNING

10 sujets différents pour sensibiliser vos collaborateurs



Pour réaliser cette ligne, nous avons effectué les choix scénaristiques suivants :

- Un style graphique épuré, flat design et responsive
- Apprentissage par le jeu et l'action avec des situations réalistes et implication de l'apprenant grâce à une scénarisation dont il est le héros.
- Ancrage mémoriel facilité : apprentissage par l'action (learning by doing)
- Fiche de synthèse téléchargeable en fin de contenu.
- Traduction et personnalisation rapide grâce à un contenu non sonorisé

LES CONTENUS



J'IDENTIFIE LES TENTATIVES D'HAMEÇONNAGE

Identifier les messages malveillants
Adopter les bonnes pratiques
Savoir réagir si j'ai été piégé



JE M'AUTHENTIFIE

Mettre en œuvre les principes de l'authentification pour contrer les risques associés.
Créer et mémoriser des mots de passe complexes.
Appliquer les bonnes pratiques pour utiliser et gérer mes mots de passe de façon sécurisée.



JE SÉCURISE MES DONNÉES

Identifier les différents types de données, les niveaux de sensibilité et les modalités d'accès
Adopter les bonnes pratiques de stockage, protection, suppression
Réagir en cas d'incident



JE NAVIGUE SUR INTERNET

Identifier les pratiques à risques
Adopter les bons réflexes pour naviguer sur Internet en sécurité
Réagir en cas d'incident

8 - 10
MINUTES



8 LANGUES



DISPONIBLE

GAMME ACTIVE



JE TÉLÉTRAVAILLE ET SUIS MOBILE

Sécuriser mes données sur l'ensemble de mes matériels pendant mes déplacements professionnels en France
Respecter les règles de sécurité en télétravail
Réagir en cas d'incident



JE PROTÈGE MON MATÉRIEL INFORMATIQUE

Adopter les bonnes pratiques pour protéger mon poste de travail et les données auxquelles il donne accès
Identifier les risques sur mon matériel et mes données
Réagir en cas d'incident



JE PROTÈGE MON ESPACE DE TRAVAIL

Respecter les mesures de protection physiques
Ranger pour préserver le patrimoine informationnel de l'entreprise
Réagir en cas d'incident



JE SUIS HYPER CONNECTÉ(E)

Identifier les risques de mes connexions matérielles
Sécuriser mes équipements et protéger mes informations
Réagir en cas d'incident



JE VOYAGE À L'ÉTRANGER

Préparer la sécurisation de son déplacement
Adopter les bons réflexes durant le déplacement
Réagir en cas d'incident



JE SUIS «ÉCONUMÉRIQUE»

Identifier les risques écologiques liés au numérique pour utiliser les ressources de manière responsable

NOTRE OFFRE PROFESSIONNELLE



Validez les compétences.
Pas les heures de formation.

Les approches classiques de sensibilisation à la cybersécurité sont insuffisantes pour protéger votre entreprise des cybermenaces.

PROFESSIONNEL

- ✓ Evaluation d'entrée *radar de maturité*
- ✓ Parcours de sensibilisation personnalisé
- ✓ Accès LMS : 12 mois
- ✓ 3 langues incluses FR, EN, ES
- ✓ Contenus : tout le catalogue, *affectation automatique des contenus selon résultats de l'évaluation*

AVEC LE CUSTOM LEARNING, PERSONNALISEZ LA SENSIBILISATION

- Quiz d'évaluation individuel des compétences et calcul d'un cyberscore
- Création automatisée de parcours personnalisés de sensibilisation
- Des parcours compris entre 25 et 140 minutes de sensibilisation : notre plateforme affecte automatiquement les contenus de sensibilisation nécessaires à vos apprenants !

CRÉEZ UN RADAR DE MATURITÉ DES COMPÉTENCES SSI DE VOS COLLABORATEURS



Evaluez les compétences



Identifiez les risques



Améliorez les compétences



NOTRE SOLUTION SUR-MESURE



Besoin de personnaliser vos contenus de sensibilisation ou de formation ?

Faites de votre campagne un outil 100% corporate et aux couleurs de votre entreprise.

Nos chefs de projet sont là pour construire avec vous la campagne qui vous correspond le mieux :

- 1 Création à façon
- 2 Flexibilité
- 3 Accompagnement tout au long du processus de création et en post-production.
- 4 Proximité entre notre équipe et la vôtre
- 5 Plateforme LMS indépendante, personnalisée et aux couleurs de votre entreprise.
- 6 Contenus sur-mesure et dans les langues de votre choix (même hors catalogue).



À LA CARTE

- ✓ Plateforme LMS personnalisée
- ✓ Suivi par un chef de projet
- ✓ Contenus sur mesure
- ✓ Langues à la demande

**NOUS CRÉONS AVEC VOUS VOTRE
CAMPAGNE !**

**N'hésitez plus et contactez notre
équipe pour échanger sur vos
besoins et vos attentes.**

SENSIBILISATIONS MÉTIERS

Parce que la cybersécurité touche tous les secteurs, nos experts ont mis au point des modules de sensibilisation spécifiques, adaptés aux problématiques et aux enjeux de votre métier.



LES CONTENUS



INFRASTRUCTURE RÉSEAU

Connaître les enjeux de la cybersécurité relatifs à la fonction d'administrateur IT.

Notions abordées :

- Comprendre son rôle en matière de cybersécurité
- Assurer la protection des éléments liés à sa fonction
- Protéger le système et gérer les incidents



DÉVELOPPEUR

Connaître les enjeux de la cybersécurité relatifs à la fonction de développeur.

Notions abordées :

- Comprendre son rôle en matière de cybersécurité
- Appréhender les principes de sécurité dans les développements
- Tester la sécurité des développements et maintenir son programme en condition opérationnelle



CHEF DE PROJET

Être capable de communiquer les règles et les bonnes pratiques de cybersécurité à ses équipes.

Notions abordées :

- Comprendre son rôle en matière de cybersécurité
- Avoir une attitude cyber-responsable exemplaire
- Appliquer et faire appliquer les règles générales de cybersécurité



CAMPAGNE DE FAUX PHISHING

Un outil clé-en-main pour préparer, envoyer et suivre (en temps réels) le nombre de clics sur des faux e-mails piégés.

- Un seul outil intégré à votre plateforme elearning
- Ergonomique et facile d'usage : prise en main en 30 min
- Accompagnement par nos chefs de projets : bénéficiez de toute notre expérience pour réussir votre campagne
- Protection des données personnelles et hébergement en France.



- 3 ÉTAPES :**
- 1 PRÉPAREZ LES E-MAILS**
 - 2 ENVOYEZ SUR LA CIBLE**
 - 3 MESUREZ LES RÉSULTATS**

VOTRE PROJET CLÉ-EN-MAIN



Des modèles d'e-mails frauduleux



Personnalisation de campagne



Envoi pilote et test



Suivi statistique avancé

NOTRE OFFRE

Afin de mesurer le niveau de risque initial ou l'efficacité de votre sensibilisation, Phosforea vous propose des campagnes de faux-phishing clé-en-main.



Bibliothèque d'emails

- Grand choix de modèles d'emails personnalisables
- Différents sujets et niveaux



Statistiques de clics

- Suivi des clics en temps réel sur notre interface web
- Edition de rapports et analyses



Pilotage

- Chef de projet dédié
- Faible charge de travail pour le client
- Cadre contractuel maîtrisé (RGPD...)
- Fiabilité des résultats



Vous avez un projet ?

Nous avons forcément une offre qui vous correspond !



ABONNÉ

- ✓ Entre 12 et 48 campagnes annuelles
- ✓ Entre 5 000 et 10 000 cibles
- ✓ Modèles d'emails et de landing page B2B

FLEXI

- ✓ Facturation à la campagne
- ✓ De 100 à 10 000 cibles
- ✓ Modèles d'emails et de landing page B2B

**Lancez une campagne de Faux Phishing en moins de 30 minutes ?
Demandez un essai gratuit !**

ACCOMPAGNEMENT MARKETING

Des outils pour réussir votre campagne de sensibilisation à la cybersécurité

CAMPAGNE DE COMMUNICATION - NEWSLETTER

Pendant 4 semaines, envoi d'un mail hebdomadaire à l'ensemble du public « cible ».

SÉMINAIRE CODIR

Animation d'un atelier de sensibilisation en mode présentiel, à destination de l'équipe dirigeante (entre 10 et 30 personnes).

ANIMATION PRÉSENTIELLE

Jeu en salle pour comprendre pourquoi et comment être vigilant par rapport à la cybersécurité sur son lieu de travail ou ses déplacements (entre 5 et 10 participants).

CRÉATION D'UNE VIDÉO DE PROMOTION

Outil de promotion de la campagne, la vidéo sera diffusée en interne auprès des collaborateurs.

CAMPAGNE D'AFFICHAGE INTERNE

Mise en œuvre d'une campagne de promotion : 5 affiches et 1 triptyque.

JEU CONCOURS

Organisation d'un jeu concours interne.



KIT DE COMMUNICATION

Des ressources pédagogiques pour acculturer chaque collaborateur de l'entreprise aux cyber-risques.

Parce qu'il s'agit de travailler sur l'humain et de changer profondément des réflexes, préparez le terrain avec des affiches, gifs animées ou autres petits jeux-sérieux en ligne qui stimuleront leur curiosité.

CE KIT DE COMMUNICATION COUVRE TROIS RISQUES RÉCURRENTS

Authentification, Phishing, Mobilité et déplacements.

Mettez entre les mains de vos collègues des outils qui vont leur servir au quotidien :

- un fond d'écran sympa pour se rappeler les bons messages,
- un gif animé qu'ils peuvent poster en un clic sur le réseau social interne de l'entreprise quand ils voient une communication qui déborde des limites de la confidentialité,
- des affiches pour décorer leurs salles de restauration,
- un jeu de plateau pour accompagner leur pause-déjeuner...



FORMATIONS



Métier développeur.....	35
RGPD et métier DPO.....	36
Métier IT.....	38
Métier chef de projet.....	44
Autres formations.....	46



MÉTIER DÉVELOPPEUR



E-LEARNING



**Durée : 10 modules +
1 évaluation (5h30)**



SÉCURITÉ DANS LES DÉVELOPPEMENTS - NIVEAU INTERMÉDIAIRE

Cette formation en ligne permet de comprendre comment intégrer la sécurité dans les développements quel que soit le langage.

Notions abordées dans les différents modules :

- concepts du développement sécurisé.
- vulnérabilités et référentiel OWASP
- objectif des attaquants et impacts sur le système
- guides et référentiels
- principes génériques de la sécurité dans les développements (authentification, session, protection des données)
- logique applicative
- cycle de développement, processus (tests, recette, livraison, sécurité de l'exploitation).



OBJECTIFS

Intégrer la cybersécurité dans les développements à tous les niveaux et quel que soit le langage utilisé.



PRÉREQUIS

Maîtriser les langages et outils de développements



PUBLIC CIBLE

Développeur Web
Administrateur réseau et système
Architecte applicatif
Ingénieur sécurité

DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.

MÉTHODES MOBILISÉES :

Supports de cours en ligne illustrés par des études de cas

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne pour chaque module et questionnaire d'évaluation final de 25 questions



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.



Ref : SEC-DEV-SECU-I



Demandez un devis

contact@phosforea.com | 05.61.17.08.54
Janvier 2023
Siret : 825 216 328 00013

RGPD ET METIER DPO



E-LEARNING

Durée : 7 modules (3h30)

RGPD

Cette formation en ligne permet de mesurer les enjeux du RGPD et d'évaluer les impacts pour son activité.

Notions abordées dans les différents modules :

- objectifs et enjeux de la réglementation européenne
- principes fondamentaux du RGPD
- rôle et responsabilités du DPO
- plan d'actions de mise en conformité
- impacts de la non-conformité au RGPD
- transfert de données personnelles hors UE



OBJECTIFS

- Expliquer les objectifs et enjeux du RGPD, identifier les bonnes pratiques de mise en œuvre, les principes fondamentaux du RGPD et le rôle et les responsabilités du DPO
- Contribuer à la mise en œuvre du RGPD au sein de son organisation et évaluer les impacts de la non-conformité à cette réglementation
- Elaborer le plan d'actions à mettre en œuvre pour se conformer aux obligations du RGPD



PRÉREQUIS

Aucun



PUBLIC CIBLE

Manager
RSSI
Directeur de fonctions
DPO
Responsable des traitements,
Réfèrent RGPD
Tout opérationnel traitant des données personnelles

MODALITÉ ET DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.

MÉTHODES MOBILISÉES :

Support de cours en ligne illustré par des études de cas

MODALITÉ D'ÉVALUATION :

Questionnaire en ligne



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

Ref : LT-RGPD



Demandez un devis

contact@phosforea.com | 05.61.17.08.54
Janvier 2023
Siret : 825 216 328 00013

RGPD ET MÉTIER DPO



E-LEARNING



Durée : 8 modules (4h)



RGPD - SANTÉ

Cette formation en ligne permet de mesurer les enjeux du RGPD dans le secteur de la santé et d'évaluer les impacts pour son activité.

Notions abordées dans les différents modules :

- objectifs et enjeux de la réglementation européenne
- principes fondamentaux du RGPD
- rôle et responsabilités du DPO
- plan d'actions de mise en conformité
- impacts de la non-conformité au RGPD
- transfert de données personnelles hors UE
- spécificités et enjeux liés au traitement de données de santé à grande échelle



OBJECTIFS

- Expliquer les objectifs et enjeux du RGPD, identifier les bonnes pratiques de mise en œuvre, les principes fondamentaux du RGPD et le rôle et les responsabilités du DPO
- Contribuer à la mise en œuvre du RGPD au sein de son organisation et évaluer les impacts de la non-conformité à cette réglementation dans le traitement des données de santé
- Elaborer le plan d'actions à mettre en œuvre pour se conformer aux obligations du RGPD



PRÉREQUIS

Aucun



PUBLIC CIBLE

Managers
RSSI
Directeur de fonctions
DPO
Responsable des traitements
Réfèrent RGPD
Tout opérationnel traitant des données personnelles

MODALITÉ ET DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.

MÉTHODES MOBILISÉES :

Support de cours en ligne illustré par des études de cas

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.



Ref : LT-RGPD-SANTE



Demandez un devis

contact@phosforea.com | 05.61.17.08.54
Janvier 2023
Siret : 825 216 328 00013



MANAGEMENT D'UN PROGRAMME D'AUDIT

Cette formation en ligne donne les clés aux organismes devant être audités afin de mobiliser les ressources nécessaires au passage d'un auditeur.
Elle prépare également les auditeurs pour réaliser l'ensemble des étapes du processus d'audit.

Notions abordées dans les différents modules :

- comprendre les intérêts et enjeux d'un audit pour une organisation
- anticiper l'arrivée d'un auditeur
- gérer un programme d'audit
- découvrir le plan d'audit et les référentiels
- piloter le plan d'action de mise en conformité
- se préparer à auditer un organisme
- mobiliser les ressources nécessaires à un audit
- communiquer avec l'équipe d'audit
- rédiger un rapport d'audit et le diffuser



OBJECTIFS

- Mesurer les enjeux d'un audit pour une organisation.
- Répondre aux questions de l'auditeur et mobiliser les ressources nécessaires à un audit.
- Piloter un audit.
- Réaliser un audit : de sa préparation à la rédaction du rapport



PRÉREQUIS

Aucun



PUBLIC CIBLE

Consultant
RSSI
Chef de projet
Ingénieur SSI
Auditeurs

MODALITÉ ET DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.

MÉTHODES MOBILISÉES :

Support de cours en ligne illustré par des études de cas

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.



MÉTIER IT

“



E-LEARNING



Durée : 5 modules (2h30)

”



GESTION DE CRISE

Cette formation en ligne permet de développer les bons réflexes face à un incident de sécurité et d'acquérir les méthodes pour suivre et traiter les incidents de sécurité.

Notions abordées dans les différents modules :

- types d'incidents de sécurité et définition.
- gestion des incidents de sécurité.
- concepts de PKI et PDCA
- méthodologie de gestion des incidents et plan d'action suite à un incident de sécurité
- évaluation de la criticité d'un incident et mise en œuvre des solutions techniques adaptées.
- définition de mesures de sécurité adaptées au processus de gestion des incidents de sécurité



OBJECTIFS

- Développer les bons réflexes face à un incident de sécurité.
- Suivre les incidents et coordonner les différents acteurs impliqués.
- Traiter les incidents de sécurité.
- Mettre en place des mesures de sécurité pour maîtriser le processus de gestion des incidents de sécurité.



PRÉREQUIS

Connaissances générales de la SSI



PUBLIC CIBLE

Consultant
RSSI
Chef de projet
Spécialiste en gestion de crise
Ingénieur SSI

MODALITÉ ET DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.

MÉTHODES MOBILISÉES :

Support de cours en ligne illustré par des études de cas

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

“



Ref : LT-REACT



Demandez un devis

”

contact@phosforea.com | 05.61.17.08.54
Janvier 2023
Siret : 825 216 328 00013

MÉTIER IT

“



E-LEARNING



Durée : 1 module +
1 évaluation (10 min)

”

MANAGEMENT DE LA SÉCURITÉ DANS LES DÉVELOPPEMENTS

Cette formation en ligne permet d'appréhender la notion de développement sécurisé.

Notions abordées :

- les différents types de vulnérabilités existantes
- les bases de la programmation sécurisée
- la sécurité dans les méthodes et processus de développement



OBJECTIFS

Comprendre les risques liés aux développements non-sécurisés et les principes génériques de développement sécurisé.



PRÉREQUIS

Connaissances des principes de développements.



PUBLIC CIBLE

Chef de projet
Développeur
Toute personne impliquée dans un projet de développement

MODALITÉ ET DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.

MÉTHODES MOBILISÉES :

Support de cours en ligne illustré par une étude de cas

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

“



Ref : SEC-DEV-SECU-001



Demandez un devis

”

contact@phosforea.com | 05.61.17.08.54
Janvier 2023
Siret : 825 216 328 00013

MÉTIER IT

“

**E-LEARNING****Durée : 5 modules +
1 évaluation (2h50)**

”



ADMINISTRATION RÉSEAUX ET SYSTÈMES

Cette formation en ligne transmet les bonnes pratiques de sécurité à appliquer dans les activités liées à l'administration et à l'exploitation des systèmes et des réseaux.

Notions abordées dans les différents modules :

- Principes fondamentaux de la sécurité de l'information (critères DIC, gestion des risques, ressources humaines, contrôles d'accès, politiques de sécurité)
- Sécurité des réseaux et des télécommunications (réseaux, accès distants, terminaux mobiles, antivirus, postes de travail, serveurs, menaces réseau, mesures de sécurité)
- Sécurité des applications (journalisation, méthodologies de développement, gestion des tiers, tests de sécurité)
- Sécurité opérationnelle (gestion des tiers, identités et droits d'accès, mots de passe, juridique, sécurité physique et logique)
- Gestion du plan de continuité d'activité (continuité d'activité et exigences légales ou réglementaires, sauvegardes et restaurations, ressources, tests, maintien du PCA)



OBJECTIFS

- Connaître les fondamentaux de la gestion des risques de sécurité, les éléments du contrôle et les politiques de sécurité de l'information.
- Identifier les menaces réseaux et les mesures de sécurité.
- Connaître les méthodologies de développement, gérer la sécurité des applications et tester la sécurité.
- Définir le périmètre de la sécurité physique et logique.
- Identifier les rôles et les responsabilités des équipes de travail et résoudre les incidents.



PRÉREQUIS

Connaissances générales de la SSI



PUBLIC CIBLE

Administrateur réseau et système
Consultant
Tout intervenant ayant des droits élevés sur le SI

MODALITÉ ET DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.

MÉTHODES MOBILISÉES :

Support de cours en ligne illustré par des études de cas

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne pour chaque module et questionnaire d'évaluation final de 25 questions



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

“

**Ref : SEC-ARS****Demandez un devis**

”

contact@phosforea.com | 05.61.17.08.54
Janvier 2023
Siret : 825 216 328 00013

MÉTIER IT

“



E-LEARNING



Durée : 5 modules +
1 évaluation (2h50)

”

SENSIBILISATION DES PERSONNELS IT

Cette formation en ligne permet aux personnels informatiques et techniques d'identifier les principales mesures de sécurité à intégrer sur un système d'information.

Notions abordées dans les différents modules :

- Concepts de la Sécurité des Systèmes d'Information (vocabulaire, critères DIC)
- Mesures de sécurité organisationnelle (organisation de la sécurité, sécurité des RH, relations fournisseurs, lois et réglementation)
- Mesures d'exploitation du SI (contrôle d'accès, sécurité physique et environnementale, actifs et cryptographie)
- Mesures de sécurité des développements et support (tests et recette, assistance, exploitation, communication et maintenance des SI)
- Mesures de gestion des incidents et de continuité (processus de gestion des incidents, mesures de sécurité, PCA)



OBJECTIFS

- Définir les concepts de la Sécurité des Systèmes d'Information et utiliser son vocabulaire.
- Intégrer la sécurité dans les processus organisationnels de l'entreprise.
- Intégrer la sécurité dans les processus d'exploitation du SI.
- Prendre en compte la sécurité dans les développements et dans les processus de support (assistance technique).
- Reconnaître un incident de sécurité et assurer la continuité d'activité.



PRÉREQUIS

Connaissances générales de la SSI



PUBLIC CIBLE

Personnels informatiques et techniques ayant des connaissances avancées en cybersécurité.

MODALITÉ ET DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.

MÉTHODES MOBILISÉES :

Support de cours en ligne sonorisé et illustré par une étude de cas

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne pour chaque module et questionnaire d'évaluation final de 25 questions



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

“



Ref : SEC-PIT



Demandez un devis

”

contact@phosforea.com | 05.61.17.08.54
Janvier 2023
Siret : 825 216 328 00013



SÉCURITÉ DES INFRASTRUCTURES IT : ANTICIPER ET GÉRER LES INCIDENTS DE SÉCURITÉ

Cette formation mixte, alliant théorie et mise en pratique, permet à toute personne qui travaille et héberge des données, logiciels ou systèmes d'information sur une infrastructure (virtualisée ou non) d'anticiper et de gérer des incidents de sécurité.

Notions abordées dans les différents modules :

Cours distanciels - 5 modules de e-learning de 30 minutes non sonorisés et une évaluation de 20 minutes (2h50)

Thématiques abordées : bonnes pratiques de sécurité pour les activités liées à l'administration et à l'exploitation.

- Principes fondamentaux de la sécurité de l'information
- Sécurité des réseaux et des télécommunications
- Sécurité des applications
- Sécurité opérationnelle
- Gestion du plan de continuité d'activité

Atelier présentiel - « Gestion des incidents sur le SI » 1 jour en salle (7h)

Démonstrations d'attaques, notions et travaux pratiques de gestion d'incidents de sécurité.

Thématiques abordées : démonstrations de scan de port et pare-feu, exécution de commande à distance, webshell et reverse-shell, exploitation de configuration non sécurisée, exfiltration de données via DNS, etc.



OBJECTIFS

- Anticiper les risques qui pèsent sur une infrastructure et réagir à un incident le cas échéant.
- Identifier, monter une équipe de gestion des incidents et faire dialoguer les différents acteurs.
- Tracer et recueillir les preuves en cas d'incident.



PRÉREQUIS

Connaissances de base en systèmes, réseaux et internet
Connaissances générales de la sécurité des systèmes d'information



PUBLIC CIBLE

Chefs de projets
Responsables infrastructure IT
DevOps
Administrateurs système

MODALITÉ ET DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea. Session présentielle définie selon les disponibilités des participants.

MÉTHODES MOBILISÉES :

Support de cours en ligne illustré par des études de cas

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne pour chaque module et questionnaire d'évaluation final de 25 questions



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.



MÉTIER CHEF DE PROJET

“

**E-LEARNING****Durée : 10 modules (5h)**

”

ANALYSE DE RISQUES : PRINCIPES ET UTILISATION

Cette formation en ligne se base sur la norme ISO27005 et permet d'identifier et évaluer les risques en sécurité de l'information dans le cadre d'un projet.

Notions abordées dans les différents modules :

- définition du risque et bénéfices d'une analyse de risques au regard du cadre de référence de l'ISO27005.
- les différents critères utilisés dans une analyse de risques et la classification des actifs.
- l'identification, l'estimation, le traitement et l'acceptation des risques.
- les principes de gouvernance et de gestion : surveillance, amélioration continue et communication.
- l'application de la norme ISO27005 à des méthodes d'analyse de risques à travers l'exemple EBIOS.



OBJECTIFS

- Identifier et évaluer les risques en sécurité de l'information dans le cadre d'un projet.
- Présenter son analyse de risques à sa direction.
- Communiquer sur les risques et améliorer sa gestion du risque.



PRÉREQUIS

Notions relatives aux systèmes d'information



PUBLIC CIBLE

Consultant
RSSI
Chef de projet
Ingénieur SSI
Toute personne impliquée dans un programme de management du risque

MODALITÉ ET DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.

MÉTHODES MOBILISÉES :

Support de cours en ligne illustré par des études de cas

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

“

**Ref : SEC-RISK-27005****Demandez un devis**

”

contact@phosforea.com | 05.61.17.08.54
Janvier 2023
Siret : 825 216 328 00013

MÉTIER CHEF DE PROJET

“

**E-LEARNING****Durée : 5 modules (2h30)**

”



SÉCURITÉ DANS LES PROJETS

Cette formation en ligne permet de découvrir les principes généraux de la sécurité dans le cycle de vie d'un projet.

Notions abordées dans les différents modules :

- fondamentaux de la sécurité de l'information.
- notion de risque projet
- exigences de sécurité
- notion de test de sécurité et de traitement du risque
- gestion du dossier sécurité et maintien en condition de sécurité



OBJECTIFS

- Comprendre la notion de risque et d'exigences de sécurité dans les phases de développement d'un projet.
- Découvrir les fondamentaux des tests de sécurité et comprendre leur nécessité dans un projet.
- Maintenir un projet en condition de sécurité.



PRÉREQUIS

Connaissances générales sur la gestion de projet



PUBLIC CIBLE

Consultant
RSSI
Chef de projet
Ingénieur SSI

MODALITÉ ET DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.

MÉTHODES MOBILISÉES :

Support de cours en ligne illustré par des études de cas

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

“

**Ref : SEC PROJ GEN****Demandez un devis**

”

contact@phosforea.com | 05.61.17.08.54
Janvier 2023
Siret : 825 216 328 00013

AUTRES FORMATIONS

“

 **BLENDED**

 **Durée : 3h30 e-learning + 3 jours (21h)**

”

ISO 21434

Cette formation mixte, alliant théorie et mise en pratique, permet à l'ensemble des collaborateurs de découvrir les objectifs et enjeux de la norme ISO 21434.

Elle permet à des collaborateurs plus ciblés de définir et faire respecter des exigences pour la gestion des risques de cybersécurité durant le cycle de vie des équipements des véhicules routiers. Cours basé sur les recommandations de la norme ISO 21434.

Cours distanciels - 7 modules de e-learning de 30 minutes environ (3h30)

Thématiques abordées : Enjeux de la norme ISO 21434, gouvernance d'entreprise, organisation projet, exigences de sécurité, intégration et maintien de la sécurité, analyse de risque et notion de TARA, amélioration continue, monitoring et maintenance

Cours présentiels - 3 jours en salle

- Discussions ouvertes et interactives avec les apprenants sur le support ISO21434
- Travaux dirigés sur l'utilisation des annexes et la réalisation de TARA



OBJECTIFS

- Déchiffrer les objectifs et enjeux de la norme ISO 21434.
- Définir des exigences pour sécuriser les produits et processus durant le cycle de vie du produit.
- Gérer la mise en place d'un CSMS et mettre en œuvre les activités nécessaires à la mise en place d'un plan de cybersécurité et partager les rôles et responsabilités entre les parties prenantes.



PRÉREQUIS

Notions relatives aux systèmes d'information



PUBLIC CIBLE

Administrateurs et architectes Système, Réseau, Ingénieur Sécurité, Responsable Technique, Responsable de la Sécurité des Systèmes d'Information, RSSI, DSI, Chef de projet, Responsable d'équipe, Responsable métiers cybersécurité, Responsable métiers développement système embarqué, Auditeur, contrôleur, évaluateur, Juriste spécialisé et tout public spécialisé dans les systèmes embarqués.

MODALITÉ ET DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.
Session présentielle définie selon les disponibilités des participants.

MÉTHODES MOBILISÉES :

Support e-learning sonorisé et sous-titré.
Support de cours et norme papier avec réalisation de travaux dirigés sur les annexes

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne et examen sur table



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

“

 **Ref : BL-21434**

 **Demandez un devis**

”

contact@phosforea.com | 05.61.17.08.54
Janvier 2023
Siret : 825 216 328 00013

LES FONDAMENTAUX DE LA SSI

“

 **E-LEARNING**

 **Durée : 1 module (10 min)**

”

INTRODUCTION À LA SÉCURITÉ DES SYSTÈMES CRITIQUES

Cette formation en ligne donne une vision générale de la cybersécurité des systèmes critiques.

Notions abordées :

- Présentation des ICS (définition, exemples d'utilisation, fonctionnement).
- Contexte, enjeux et exigences de sécurité (DICA, évolution des technologies et des menaces).
- Attitude en cas d'incident suite à de mauvais comportements sur les ICS (étude de divers cas d'incident et scénarios de réaction).



OBJECTIFS

Comprendre les enjeux d'un système industriel et l'impact du comportement de chacun sur celui-ci.



PRÉREQUIS

Aucun



PUBLIC CIBLE

Tout public

DÉLAIS D'ACCÈS :

Accès de 3 mois suite à l'inscription sur la plateforme Phosforea.

MÉTHODES MOBILISÉES :

Support de cours en ligne illustré par une étude de cas

MODALITÉ D'ÉVALUATION :

Questionnaires en ligne



ACCESSIBILITÉ :

Notre offre de formation est accessible à tout public, n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.



Ref : LT-SCADA



Demandez un devis

contact@phosforea.com | 05.61.17.08.54
Janvier 2023
Siret : 825 216 328 00013





CyberPlay ▲

Un jeu de carte directement inspiré du célèbre jeu français 1000 Bornes®.

Une approche ludique et pédagogique pour introduire les menaces cyber qui pèsent sur les collaborateurs au quotidien, et découvrir les bonnes pratiques associées.

Soyez le premier à atteindre les 500 points « cyber-responsable ».

Jouez en équipe lors de sessions présentielles ou autour d'un café !



209 rue Jean Bart - Bât. Agora 1
31670 Labège
SIRET : 825 216 328 00013
Organisme de formation : 76 31 08704 31



+33 (0)5 61 17 08 54



contact@phosforea.com

WWW.PHOSFOREA.COM



Toulouse



Paris



Madrid