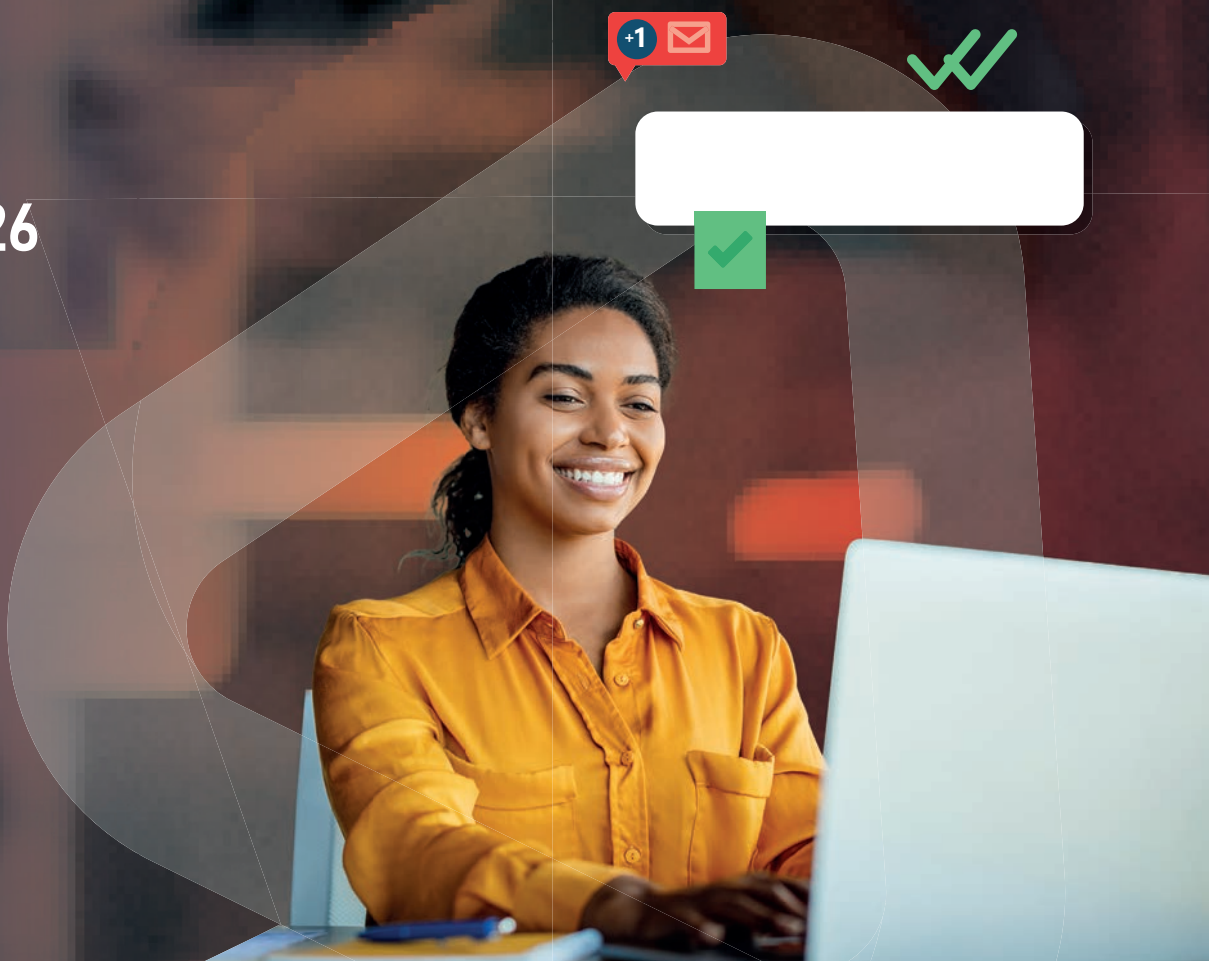
phosforea
by june factory

Catalogue de contenus

Mars 2026



June Factory
Nos contenus
Nos formations présentielles

SOMMAIRE

JUNE FACTORY

Softwares de pilotage des conformités et des compétences.

Nous développons des solutions logicielles pour piloter la mise en conformité et le développement des compétences en dans une logique d'amélioration continue.
June Factory est à la fois éditeur de solutions SAAS, de contenus et de base de connaissance.

Nous vous accompagnons de la sensibilisation jusqu'aux formations expertes pour accroitre la maturité de votre organisation. Au service de nos clients, nous développons également des formations et services 100 % sur-mesure ou adaptés à leurs secteurs et à leurs processus internes.

Nos deux produits phares, Auditool (dédié au pilotage des conformités) et Phosforea (spécialisé dans la sensibilisation et la formation E-learning) offrent une suite de solutions globales permettant le pilotage de la

NOTRE ÉQUIPE

La formation pour les professionnels par des professionnels.

PÔLE WEB

Lead Dev
Developpeur web
Développeur full stack
Infra

PÔLE COMMERCE

Commerce
Marketing

PÔLE PROJET

Customer success
Product Owner

PÔLE PÉDAGOGIQUE

Directrice pédagogique
Ingénieures pédagogiques
Infographistes

PHOSFOREA

Des contenus adaptés à tous les niveaux de connaissance.

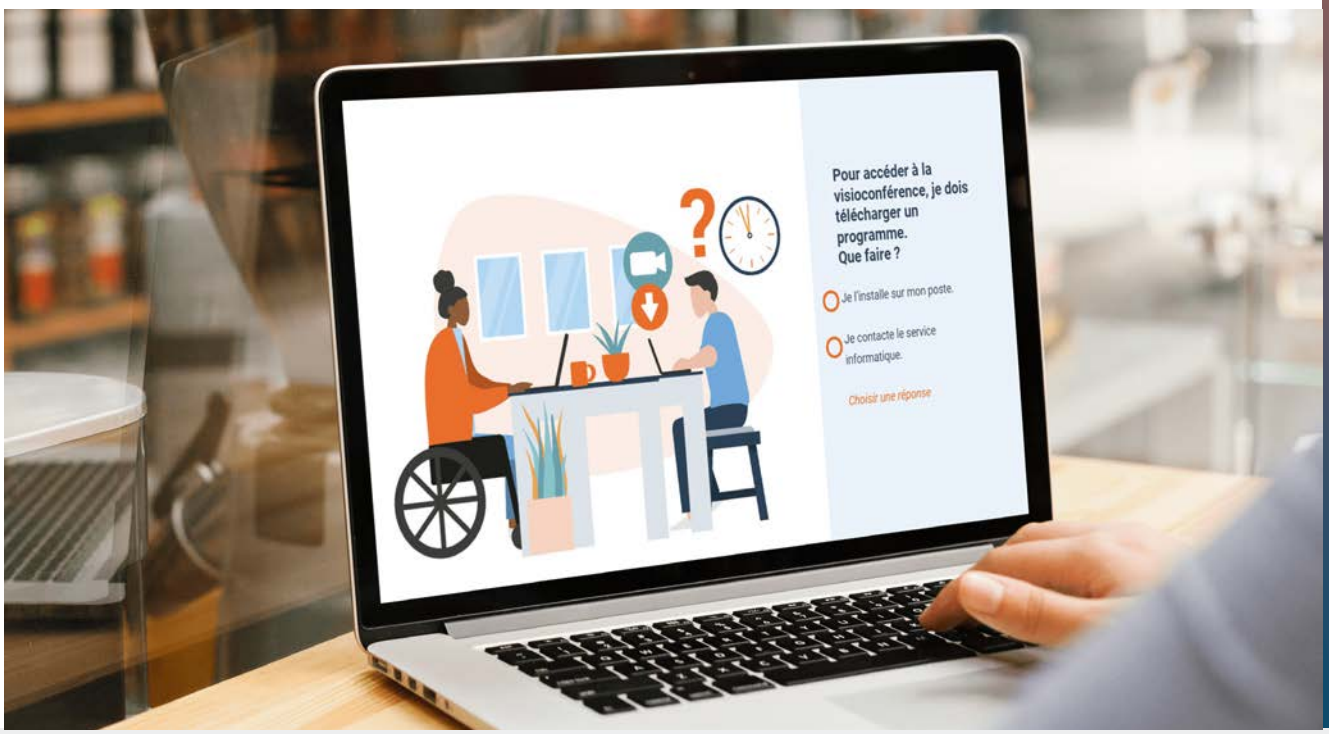
DES CONTENUS

Phosforea, c'est avant tout plus de 120 contenus classées par thématique. 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 adressons tous les profils d'apprenant, quel que soient leurs niveaux de connaissances, du novice à l'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 de contenus, gestion des compétences de vos collaborateurs, campagnes de communication interne pour promouvoir une action de sensibilisation, parcours de formation sur-mesure selon les profils de vos collaborateurs…

N'hésitez pas à nous solliciter !



UNE PLATEFORME

Une plateforme e-learning clé-en-main !

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 mesurez rapidement les résultats avec des rapports et analyses simplifiés.

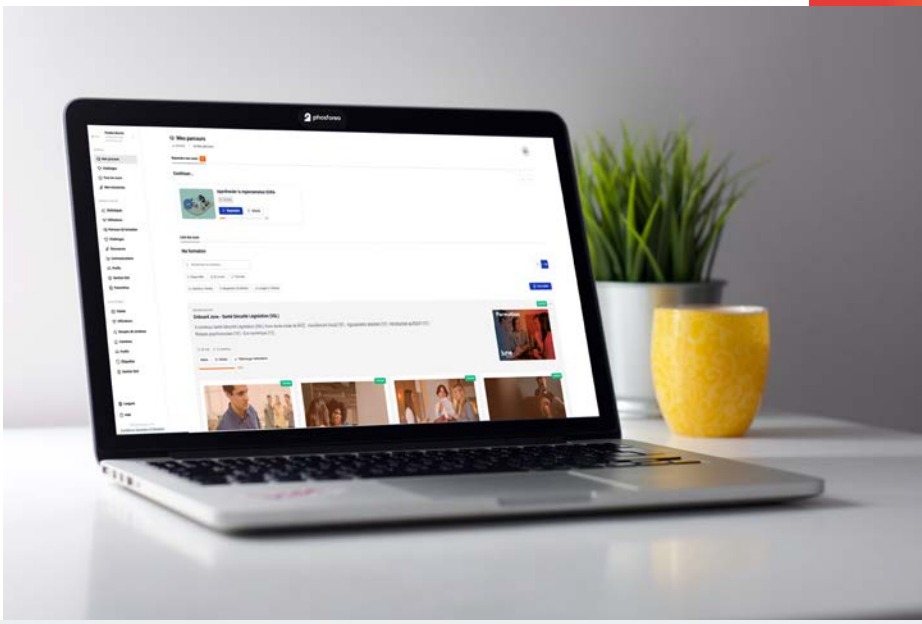
Déploiement rapide des campagnes e-learning sur notre plateforme LMS.

Mode SaaS : accès web, nous assurons la maintenance et la disponibilité hébergés en France.

Accès aux cours : **24h/24**

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

N'ATTENDEZ PLUS ET DEMANDEZ UNE DÉMO !



NOUS FAIRE CONFIANCE

1

DE LA SENSIBILISATION À LA CERTIFICATION

Phosforea accompagne l'ensemble de vos apprenants en proposant une approche pédagogique basée sur 4 niveaux de compétences : de la sensibilisation à la certification.

2

LA MESURE DE LA COMPÉTENCE EN TEMPS RÉEL

Grâce à son LMS, Phosforea permet à chaque apprenant de suivre un parcours de formation adapté à son besoin. Le manager peut piloter la montée en compétence de son équipe et le risque humain de son organisation via des tableaux de bord consolidés.

3

SPÉCIALISTE DU E-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 via notre outil LMS (ou la plateforme interne du client).

4

DES CONTENUS ADAPTÉS

Chez Phosforea, nous savons que chaque entreprise est unique, nos contenus sont disponibles sur catalogue, personnalisés ou crées sur-mesure avec notre équipe pédagogique pour s'adapter à vos besoins.

5

UNE ÉQUIPE À VOTRE ÉCOUTE

Une équipe proche de vous et des interlocuteurs disponibles pour vous accompagner tout au long de votre projet (avant-vente, cadrage projet, onboarding, suivi et analyse des campagnes).

NOS CONTENUS

FORMATS

7 MÉTHODES PÉDAGOGIQUES

1 CAPSULE – Durée 4 à 6 min

CARACTÉRISTIQUES

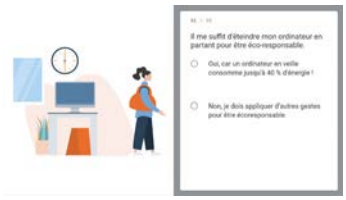
- Navigation verticale (similaire à une page web)
- Un contenu responsif non sonorisé basé sur les codes du web
- Une approche pédagogique micro-learning (quiz, cartes à retourner, cherche-et-trouve, etc.)
- Un quiz de validation des connaissances en fin de contenu
- Une fiche de synthèse téléchargeable en fin de contenu

2 VIDÉO – Durée 1 à 2 min

CARACTÉRISTIQUES

- Une notion par vidéo
- Une musique d'ambiance, pas de voix-off
- Des contenus illustrés avec des exemples issus du terrain

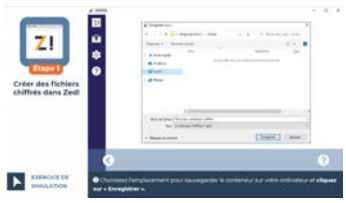
3 ACTIV'LEARNING – Durée 10 à 12 min



CARACTÉRISTIQUES

- 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)
- Un quiz de validation des connaissances en fin de contenu
- Fiche de synthèse téléchargeable en fin de contenu
- Traduction et personnalisation rapide grâce à un contenu non sonorisé

4 SIMULATION – Durée 5 min



CARACTÉRISTIQUES

- Apprentissage par l'action pour découvrir de manière interactive comment paramétrer la confidentialité d'outils et/ou de matériel quotidien
- Ancrage mémoriel facilité : apprentissage par l'action (learning by doing)
- Traduction et personnalisation rapide grâce à un contenu non sonorisé

FORMATS

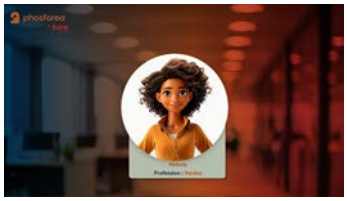
7 MÉTHODES PÉDAGOGIQUES

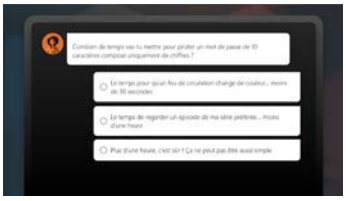
5 BANDE DESSINÉE - Durée 2 à 5 min

CARACTÉRISTIQUES

- Contenu court et scénarisé sous forme de bande dessinée
- Compatible LMS ou PDF
- Des contenus illustrés avec des exemples issus du terrain
- Navigation verticale (similaire à une page web)

6 DARK SIDE - Durée 5 min





CARACTÉRISTIQUES

L'apprenant devient un apprenti pirate informatique :

- Prise de conscience facilitée
- Meilleure compréhension des bonnes pratiques pour se protéger
- Traduction rapide grâce à l'IA

7 AUTRES - Durée variable selon support

CARACTÉRISTIQUES

- Jeux présentiels
- Escape game
- Challenge cyber
- Podcasts
- Communication (newsletters, affiches, teasing...)
- ...

THÉMATIQUE 1

SÉCURITÉ DE LA MESSAGERIE

CAPSULE - (4 à 6 min)
VIDÉO - (1 à 2 min)
ACTIV'LEARNING - (10 à 12 min)
DARK SIDE - (5 min)

DÉTECTER UNE TENTATIVE DE PHISHING

Détecter un message malveillant pour ne pas se faire hameçonner

PROTÉGER SA MESSAGERIE

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

RANSOMWARE

Empêcher la contamination de son entreprise par un cryptovirus

PHISHING

Éviter de se faire hameçonner

J'IDENTIFIE LES TENTATIVES D'HAMEÇONNAGE

Identifier les messages malveillants

PHISHING À L'ÈRE DE L'IA

Comprendre les techniques d'hameçonnage et appliquer les bonnes pratiques pour les contrer

OBJECTIF

Reconnaître les principales menaces sur la messagerie et adopter les précautions de base.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 2

SÉCURITÉ DES INFORMATIONS

- **CAPSULE** - (4 à 6 min)
- **VIDÉO** - (1 à 2 min)
- **ACTIV'LEARNING** - (10 à 12 min)
- **SIMULATION** - (5 min)
- **DARK SIDE** - (5 min)

ENVOYER UN DOCUMENT CONFIDENTIEL

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

PROTÉGER MES DONNÉES DURANT LEUR CYCLE DE VIE

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

CHIFFREMENT

Chiffrer les informations pour les manipuler et les transmettre

CLOUD

Utiliser le cloud en sécurité

JE SÉCURISE MES DONNÉES

Identifier les différents types de données, les niveaux de sensibilité et les modalités d'accès

ZED

Chiffrer mes données avec Zed!

7ZIP

Chiffrer mes données avec 7Zip

ANDROID

Paramétrer la confidentialité sur Android

IOS

Paramétrer la confidentialité sur iOS

SHAREPOINT

Utiliser Sharepoint en sécurité

GOOGLE DRIVE

Utiliser Google Drive en sécurité

ENVOI DE DONNÉES

Découvrir les risques d'envoi de données et appliquer les bonnes pratiques de sécurité

OBJECTIF

Mettre en œuvre les principes de stockages, d'envoi et de suppression sécurisée des données.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 3

SÉCURITÉ DE L'AUTHENTIFICATION

VIDÉO - (1 à 2 min)
ACTIV'LEARNING - (10 à 12 min)
SIMULATION - (5 min)
DARK SIDE - (5 min)

MOT DE PASSE

Créer un mot de passe sécurisé

JE M'AUTHENTIFIE

Mettre en œuvre les principes de l'authentification

KEEPASS

Gérer mes mots de passe avec Keepass

VAULTWARDEN

Gérer ses mots de passe avec Vaultwarden

MOTS DE PASSE

Découvrir la vulnérabilité des mots de passe et appliquer les bonnes pratiques pour les rendre inviolables

OBJECTIF

Identifier les menaces et mettre en œuvre les principes de l'authentification pour contrer les risques associés.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 4

SÉCURITÉ EN DÉPLACEMENT

CAPSULE - (4 à 6 min)
VIDÉO - (1 à 2 min)
ACTIV'LEARNING - (10 à 12 min)
DARK SIDE - (5 min)

TÉLÉTRAVAILLER EN SÉCURITÉ

Respecter les règles de cybersécurité en situation de télétravail

WI-FI

Utiliser les réseaux Wi-Fi en sécurité

TÉLÉTRAVAIL

Travailler en sécurité de son domilice comme au bureau

JE TÉLÉTRAVAILLE ET JE SUIS MOBILE

Sécuriser mes données sur l'ensemble de mes matériels en mobilité

DÉPLACEMENTS

Analyser les risques de vol ou d'espionnage opportunistes lors des déplacements et appliquer les bonnes pratiques pour s'en protéger

CONNEXIONS WI-FI

Analyser les techniques d'attaques pour exploiter les connexions Wi-Fi et appliquer les bonnes pratiques pour se connecter.

ÉQUIPEMENTS MOBILES

Comprendre les vulnérabilités des appareils mobiles et appliquer les bonnes pratiques de sécurité

OBJECTIF

Adopter des gestes simples de sécurité lors des déplacements.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 5

SÉCURITÉ PHYSIQUE

VIDÉO - (1 à 2 min)

ACTIV'LEARNING - (10 à 12 min)

DARK SIDE - (5 min)

BUREAU PROPRE

Ranger son bureau pour protéger ses informations

VACANCES

Partir en vacances en sécurité

JE PROTÈGE MON ESPACE DE TRAVAIL

Respecter les mesures de protection physiques

SÉCURITÉ PHYSIQUE

Découvrir les failles de sécurité physique et appliquer les bonnes pratiques pour protéger les locaux, le matériel et les informations

OBJECTIF

Mettre en œuvre les principes de sécurité physique et respecter les protections en place.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 6

SÉCURITÉ DES ÉQUIPEMENTS MOBILES

CAPSULE - (4 à 6 min)
VIDÉO - (1 à 2 min)
ACTIV'LEARNING - (10 à 12 min)

PROTÉGER SES OBJETS CONNECTÉS

Assurer la sécurité de l'entreprise lorsque tout est interconnecté

SMISHING

Se protéger des SMS malveillants

QUISHING

Se protéger des QR Codes malveillants

SMARTPHONE

Utiliser ses appareils nomades en sécurité

JE SUIS HYPERCONNECTÉ(E)

Identifier les risques de mes connexions matérielles

OBJECTIF

Identifier les menaces sur les appareils mobiles et leurs connexions.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 7

SÉCURITÉ DU POSTE DE TRAVAIL

CAPSULE - (4 à 6 min)

ACTIV'LEARNING - (10 à 12 min)

EVITER LE SHADOW IT

Protéger l'entreprise de l'utilisation de ressources externes

JE PROTÈGE MON MATÉRIEL INFORMATIQUE

Adopter les bonnes pratiques pour protéger mon poste de travail

OBJECTIF

Respecter les usages et configurations des matériels et outils pour préserver la sécurité de son poste.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 8

SÉCURITÉ EN LIGNE

CAPSULE - (4 à 6 min)
VIDÉO - (1 à 2 min)
ACTIV'LEARNING - (10 à 12 min)
SIMULATION - (5 min)
DARK SIDE - (5 min)

DÉTECTER LES FAKE NEWS

Distinguer le vrai du faux sur Internet

ACHATS EN LIGNE

Effectuer ses achats en ligne en toute sécurité

JE NAVIGUE SUR INTERNET

Identifier les pratiques à risques sur Internet

CONFIGURER LE NAVIGATEUR GOOGLE CHROME

Paramétrer la confidentialité de mon navigateur Chrome

CONFIGURER LE NAVIGATEUR MICROSOFT EDGE

Paramétrer la confidentialité de mon navigateur Edge

CONFIGURER LE NAVIGATEUR SAFARI

Paramétrer la confidentialité de mon navigateur Safari

CONFIGURER LE NAVIGATEUR FIREFOX

Paramétrer la confidentialité de mon navigateur Firefox

NAVIGATION SUR INTERNET

Analyser les techniques pour piéger les internautes et appliquer les bonnes pratiques pour éviter les attaques.

OBJECTIF

Mettre en œuvre les principes de navigation sécurisée.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 9

SÉCURITÉ DES COMMUNICATIONS

- **CAPSULE** - (4 à 6 min)
- **VIDÉO** - (1 à 2 min)
- **ACTIV'LEARNING** - (10 à 12 min)
- **SIMULATION** - (5 min)
- **DARK SIDE** - (5 min)

COMMUNIQUER SUR LES RÉSEAUX SOCIAUX

Communiquer de manière responsable sur les réseaux sociaux

PROTÉGER SA E-RÉPUTATION

Préserver sa réputation sur Internet

DONNÉES PRIVÉES

Découvrir qui exploite les données privées sur le Web

INGÉNIERIE SOCIALE

Reconnaître les techniques de manipulation des pirates

JE VOYAGE À L'ÉTRANGER

Préparer la sécurisation de son déplacement

SÉCURISER SON PROFIL LINKEDIN

Paramétrer mon profil LinkedIn

RÉSEAUX SOCIAUX

Découvrir comment les pirates informatiques collectent les informations sensibles et les bonnes pratiques pour les protéger

OBJECTIF

Mettre en œuvre les principes de sécurité des communications lors de déplacements ou dans les échanges.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 10

SÉCURITÉ GÉNÉRALE

CAPSULE - (4 à 6 min)
VIDÉO - (1 à 2 min)
ACTIV'LEARNING - (10 à 12 min)

DEVENIR CYBER-RESPONSABLE

S'impliquer efficacement dans la cybersécurité de l'entreprise

CIBLE

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

MENACES INFORMATIQUES

Reconnaître les menaces informatiques

L'ESSENTIEL DE LA CYBER

Devenir cyber-responsable : identifier les tentatives d'hameçonnage, protéger ses données, sa messagerie, son matériel et réagir en cas d'attaque

JE SUIS «ÉCO-NUMÉRIQUE»

Identifier les risques écologiques liés au numérique

MA JOURNÉE CYBER

Vivre une journée de bureau en étant acteur de la cybersécurité

OBJECTIF

Appliquer les règles de sécurité de l'entreprise.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 11

INTELLIGENCE ARTIFICIELLE

VIDÉO - (1 à 2 min)
ACTIV'LEARNING - (10 à 12 min)
DARK SIDE - (5 min)

COMPRENDRE CE QU'EST UNE IA ET SES LIMITES

Comprendre ce qu'est une IA, ses principes de fonctionnement et identifier ses limites

RISQUES DE L'IA ET BONNES PRATIQUES POUR UN USAGE SÉCURISÉ

Connaître les risques associés aux IA, les actions à mettre en œuvre pour s'en protéger et utiliser l'IA de manière critique

PANORAMA DE L'IA EN ENTREPRISE : OUTILS, USAGES ET ACTEURS

Identifier les principaux outils d'IA utilisés et adopter un usage responsable et pertinent de l'IA en contexte professionnel

IA : ATTENTION À VOS DONNÉES !

Comprendre pourquoi on ne peut pas saisir n'importe quelle donnée dans une IA et connaître les règles de protection

L'ART DU PROMPT : FORMULER DES DEMANDES EFFICACES

Formuler un prompt clair et structuré pour obtenir une réponse exploitable dans un contexte professionnel

L'IA DANS LES OUTILS MÉTIER ET LES WORKFLOWS

Comprendre comment l'IA s'intègre dans les outils utilisés au quotidien

JE SÉCURISE MON UTILISATION DES IA

Sécuriser son utilisation des intelligences artificielles

DEEPFAKE

Lutter contre les deepfakes

CONTENUS FALSIFIÉS PAR IA (DEEPFAKES)

Analyser les techniques de deepfake et appliquer les bonnes pratiques pour ne pas être victime de contenus falsifiés

OBJECTIF

Comprendre, utiliser et intégrer l'IA de manière efficace, sécurisée, et responsable, en adoptant de bonnes pratiques de protection des données, de formulation de prompts et de vérification des résultats.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 12

SÉCURITÉ DEV : TOP 10 OWASP

BANDE DESSINÉE - (2 à 5 min)

BIENVENUE CHEZ ACME LABS

Présenter les personnages récurrents et l'environnement de travail de cette bande dessinée

A01: BROKEN ACCESS CONTROL

Identifier les failles de contrôle d'accès et comprendre comment des accès indirects ou mal contrôlés peuvent être exploités

A02: SECURITY MISCONFIGURATION

Reconnaître les erreurs de configuration courantes (environnements, APIs, cloud) et leurs impacts sur la sécurité

A03: SOFTWARE SUPPLY CHAIN FAILURES (NOUVEAUTÉ 2025)

Comprendre les risques des dépendances tierces aux outils et adopter les bons réflexes de contrôle de la chaîne logicielle

A04: CRYPTOGRAPHIC FAILURES

Identifier les mauvaises pratiques cryptographiques et comprendre leurs conséquences sur la protection des données

A05: INJECTION

Comprendre les mécanismes d'injection et savoir les prévenir par de bonnes pratiques de développement

A06: INSECURE DESIGN

Intégrer la sécurité dès la conception et identifier les failles liées à des hypothèses métier ou techniques non sécurisées

A07: AUTHENTICATION FAILURE

Reconnaître les faiblesses des mécanismes d'authentification et les erreurs de mise en oeuvre courantes

A08: SOFTWARE & DATA INTEGRITY FAILURES

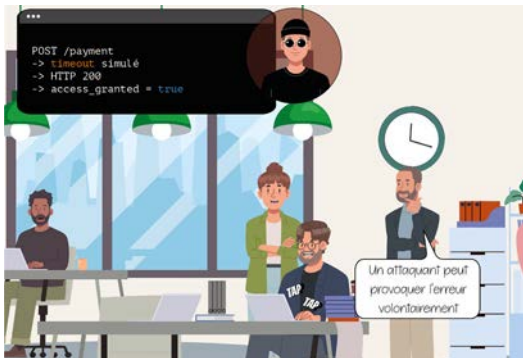
Comprendre les risques liés à l'intégrité du code et des données tout au long du cycle de vie applicatif

A09: SECURITY LOGGING & MONITORING FAILURES

Mesurer l'importance de la journalisation et de la détection pour identifier et réagir aux incidents de sécurité

A10: MISHANDLING OF EXCEPTIONAL CONDITIONS (NOUVEAUTÉ 2025)

Comprendre comment une mauvaise gestion des erreurs et des situations imprévues peut devenir exploitable, et adopter une approche fail-safe



OBJECTIF

Permettre aux développeurs de comprendre, identifier et prévenir les principales vulnérabilités applicatives décrites dans le Top 10 OWASP – édition 2025.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Développeurs web

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 13

SANTÉ, SÉCURITÉ, LÉGISLATION

VIDÉO - (1 à 2 min)

ACTIV'LEARNING - (10 à 12 min)

RISQUES PSYCHOSOCIAUX

Identifier les risques psychosociaux (RPS), prévenir et maîtriser ces risques et agir sur la qualité de vie au travail

AGISSEMENTS SEXISTES

Définir et caractériser le harcèlement sexuel, mettre en œuvre les dispositifs et outils de prévention et réagir en cas de harcèlement sexuel

HARCÈLEMENT MORAL

Définir et caractériser le harcèlement moral, mettre en place des dispositifs et outils de prévention et agir en cas de harcèlement déclaré

ETHIQUE ET CORRUPTION

Comprendre les enjeux d'une politique anti-corruption et respecter les règles éthiques

INTRODUCTION AU RGPD

Expliquer les objectifs du RGPD, identifier les principes du règlement et les obligations pour les responsables des traitements

MANAGEMENT INCLUSIF

Un enjeu collectif : identifier et signaler les biais et comportements discriminatoires, agir pour un environnement de travail inclusif

LA MINUTE RGPD

Introduire les principes et enjeux du RGPD

AUTRES CONTENUS SUR DEMANDE

IDENTITÉ NUMÉRIQUE

Protéger son identité numérique

PROPRIÉTÉ INTELLECTUELLE DES DONNÉES SUR INTERNET

Comprendre les droits sur les données et éviter la fuite de données via des outils en ligne.

CYBER HARCÈLEMENT

Comprendre les mécanismes de cyber harcèlement, le signaler et agir pour se protéger

DROIT SOCIAL

Définir le cadre juridique, les enjeux de prévention et identifier les risques sociaux de l'entreprise pour les gérer

OBJECTIF

Permettre aux RH et managers de renforcer leurs connaissances et de faire adhérer l'ensemble des collaborateurs aux règles et enjeux de l'éthique et du bien-être au travail afin de prévenir les risques dans le respect de la réglementation française.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 14

ACTIV'LEARNING - (10 à 12 min)

SÉCURITÉ DES SYSTÈMES D'INFORMATION*

ENJEUX DE LA CYBERSÉCURITÉ

Identifier les sources de menaces et connaître les mesures de protection à suivre pour s'impliquer dans la démarche de protection des systèmes

INTÉGRATION DE LA CYBER DANS LA GOUVERNANCE DE L'ENTREPRISE

Identifier les acteurs de la cybersécurité et leur rôle ainsi que les documents utiles et les mesures organisationnelles et techniques

PROTECTION DES DONNÉES

Gérer les identités et l'accès aux données en fonction du besoin d'en connaître et du moindre privilège

INTÉGRATION DE LA SÉCURITÉ DANS LES PROJETS

Intégrer la sécurité tout au long des projets pour fournir des produits sécurisés

SÉCURITÉ ET GESTION DES TIERS

Acquérir les compétences nécessaires pour évaluer, sécuriser et contrôler les accords avec les tiers

CYBERSÉCURITÉ DANS LE DÉVELOPPEMENT LOGICIEL

Intégrer la sécurité dans le cycle de développement, corriger les vulnérabilités et maintenir le niveau de sécurité des applications

SÉCURITÉ DES INFRASTRUCTURES

Définir une infrastructure sécurisée, surveiller l'infrastructure et pérenniser la sécurité

SÉCURITÉ DES RÉSEAUX

Identifier les mesures pour sécuriser les connexions réseau

SÉCURITÉ DES POSTES ET ÉQUIPEMENTS - ENDPOINT

Connaitre les principales mesures pour sécuriser les postes et équipements individuels et maîtriser les mesures de protection locales

MAINTIEN EN CONDITION DE SÉCURITÉ

Maintenir la sécurité dans un environnement de production : sécuriser les actifs, identifier les vulnérabilités et réaliser des tests périodiques

CYBER INCIDENT : SURVEILLANCE ET RÉPONSE

Surveiller, identifier, gérer et résoudre les incidents de sécurité informatique : analyser et réagir rapidement en maîtrisant sa communication

GESTION DE CRISE ET CONTINUITÉ D'ACTIVITÉ : LA RÉSILIENCE

Lier la gestion de crise et continuité d'activité pour répondre aux situations exceptionnelles et comprendre le concept de résilience opérationnelle

*A noter : contenus techniques et organisationnels SSI conformes aux attentes de l'ISO 27001, NIS2, DORA...

OBJECTIF

Permettre aux personnels d'identifier les principales mesures de sécurité, techniques et organisationnelles à intégrer sur un système d'information.

PRÉREQUIS

Connaissances générales de la SSI

PUBLIC CIBLE

Personnels informatiques, techniques, chef de projet et gouvernance.

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 15

DORA

ACTIV'LEARNING - (10 à 12 min)

1 - APPRÉHENDER LA RÈGLEMENTATION DORA

Appréhender sa terminologie, son contexte, ses objectifs et les enjeux de la résilience opérationnelle numérique pour les institutions financières

2 - DEVENIR CYBER-RESPONSABLE

Identifier les tentatives d'hameçonnage, protéger ses données durant leur cycle de vie, protéger son matériel informatique et réagir en cas d'attaque

3 - LES ENJEUX DE LA CYBERSÉCURITÉ

S'impliquer dans la cybersécurité de l'entreprise et comprendre les enjeux de sa mise en œuvre

4 - GESTION DE CRISE ET CONTINUITÉ D'ACTIVITÉ : LA RÉSILIENCE

Définir les notions d'incident de sécurité, gestion de crise et continuité d'activité. Comprendre le concept de résilience opérationnelle

OBJECTIF

Comprendre les fondamentaux de la réglementation DORA, son vocabulaire, ses objectifs et les enjeux de la résilience opérationnelle numérique pour devenir cyber-responsables et réagir de manière appropriée en cas d'incident.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public non IT et équipes transverses.

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

THÉMATIQUE 16

NIS2

ACTIV'LEARNING - (10 à 12 min)

APPRÉHENDER LA RÈGLEMENTATION NIS2

Sa terminologie, son contexte, ses objectifs et les enjeux de la résilience opérationnelle numérique pour les entités essentiels et importantes

DEVENIR CYBER-RESPONSABLE

Identifier les tentatives d'hameçonnage, protéger ses données durant leur cycle de vie, protéger son matériel informatique et réagir en cas d'attaque.

GESTION DE CRISE ET CONTINUITÉ D'ACTIVITÉ : LA RÉSILIENCE

Définir les notions d'incident de sécurité, gestion de crise et continuité d'activité. Comprendre le concept de résilience opérationnelle

LES ENJEUX DE LA CYBERSÉCURITÉ

S'impliquer dans la cybersécurité de l'entreprise et comprendre les enjeux de sa mise en œuvre

OBJECTIF

Comprendre les fondamentaux de la réglementation NIS2, son vocabulaire, ses objectifs et les enjeux de la résilience opérationnelle numérique. Saisir les enjeux de la cybersécurité en entreprise et le rôle de chacun dans sa mise en œuvre.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public non IT et équipes transverses.

MODALITÉ ET DÉLAIS D'ACCÈS :
12 mois d'accès sur la plateforme Phosforea dès validation de l'inscription.

MÉTHODES MOBILISÉES :
Contenus interactifs en ligne sur plateforme LMS ou SCORM seuls.

MODALITÉ D'ÉVALUATION :
Questionnaires inclus dans chaque contenu.

ACCESSIBILITÉ :
Tout public (conforme au RGAA ou en cours de conformité), n'hésitez pas à nous faire part de toutes demandes spécifiques afin d'adapter au mieux nos modalités de formation.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

FORMATIONS PRÉSENTIELLES

LES FONDAMENTAUX DE LA SSI

BONNES PRATIQUES DE CYBERSÉCURITÉ

Quelle que soit notre fonction dans l'entreprise, nous avons tous un rôle à jour en matière de cybersécurité. Cette formation constitue une approche générale de la cybersécurite.

Aperçu du programme :

- Appréhender les différents aspects de la SSI (origine, évolution des systèmes et des menaces dans un monde ultra connecté ; types d'attaques et enjeux pour les entreprises).
- Identifier les différentes menaces informatiques et les impacts de ces cyberattaques.
- Détecter les problèmes de sécurité.
- Découvrir les moyens de protection, leurs limites et les bonnes pratiques.
- Passer en revue les différents problèmes de sécurité régulièrement rencontrés en entreprise.

OBJECTIFS

- Découvrir les techniques utilisées par les pirates pour accéder aux systèmes et les méthodes de protection et/ou bonnes pratiques permettant de s'en prémunir au quotidien.
- Amorcer une démarche cyber-responsable.

PRÉREQUIS

Aucun

PUBLIC CIBLE

Tout public

En savoir plus

PRÉSENTIEL

DURÉE : 1 JOUR (7H)

REF : BP-SSI

TARIF : 825€ HT

MODALITÉ ET DÉLAIS D'ACCÈS :
Accès sur inscription préalable au minimum 15 jours avant la date prévue. Pour être maintenue, une session doit rassembler un minimum de 3 participants.

MÉTHODES MOBILISÉES :
Projection de support de cours et démonstrations

MODALITÉ D'ÉVALUATION :
Quiz collectif avec correction commune

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.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

GOUVERNANCE & CONFORMITÉ SSI

SMSI - ISO 27001 FONDAMENTAUX

Cette formation s'adresse à tous les personnels impliqués dans le management de la sécurité de l'information ou souhaitant acquérir des connaissances relatives aux principaux processus du système de management de la sécurité de l'information.

Aperçu du programme :

- Jour 1 : introduction aux concepts du système de management de la sécurité de l'information (SMSI), tels que définis par la norme ISO/CEI 27001
- Jour 2 : exigences relatives au système de management de la sécurité de l'information et examen de certification.

Détails de la certification :

Cette formation inclut le passage de l'examen « PECB Certified ISO/CEI 27001 Foundation » (1h).
Cette certification délivrée par notre partenaire PECB atteste que vous avez compris les méthodes et exigences ainsi que le cadre et l'approche de management relatifs à la norme.
Cet examen est disponible en français et dans plusieurs autres langues.
Les candidats qui n'obtiennent pas un score suffisant ont la possibilité de le repasser dans les 12 mois qui suivent sans frais supplémentaires.

OBJECTIFS

- Comprendre les éléments et le fonctionnement d'un système de management de la sécurité de l'information
- Comprendre la corrélation entre la norme ISO/CEI 27001 et ISO/CEI 27002 ainsi qu'avec d'autres normes et cadres règlementaires
- Connaître les approches, les méthodes et les techniques permettant de mettre en oeuvre et de gérer un système de management de la sécurité de l'information

PRÉREQUIS

Notions relatives aux Systèmes d'Information

PUBLIC CIBLE

Consultant
RSSI
Chef de projet
Ingénieur SSI
Toute personne impliquée dans le management de la sécurité de l'information

En savoir plus

PRÉSENTIEL

DURÉE : 2 JOURS (14H)

REF : ISO27001-FDX

TARIF : 1690€ HT

PECB AUTHORIZED PARTNER

FORMATION CERTIFIANTE

MODALITÉ ET DÉLAIS D'ACCÈS :
Accès sur inscription préalable au minimum 15 jours avant la date prévue. Pour être maintenue, une session doit rassembler un minimum de 3 participants

MÉTHODES MOBILISÉES :
Support de cours et norme papier illustrés par des exemples basés sur une étude de cas et des jeux de rôles.

MODALITÉ D'ÉVALUATION :
Examen de certification

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.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

GOUVERNANCE & CONFORMITÉ SSI

SMSI - ISO 27001 LEAD IMPLEMENTOR

Cette formation s'adresse à tous les personnels impliqués dans le management de la sécurité de l'information ou responsables du maintien de la conformité aux exigences du SMSI.

Aperçu du programme :

- Jour 1 : introduction à la norme ISO/CEI 27001 et initialisation d'un SMSI
- Jour 2 : planification de la mise en œuvre d'un SMSI
- Jour 3 : mise en œuvre d'un SMSI
- Jour 4 : surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI
- Jour 5 : examen de certification

Détails de la certification :

Cette formation inclut le passage de l'examen « PECB Certified ISO/CEI 27001 Lead Implementer » (3h).
Cette certification délivrée par notre partenaire PECB atteste que vous maîtrisez les 7 domaines de compétences de la norme.
Cet examen est disponible en français et dans plusieurs autres langues.
Les candidats qui n'obtiennent pas un score suffisant ont la possibilité de le repasser dans les 12 mois qui suivent sans frais supplémentaires.

OBJECTIFS

- Maîtriser les concepts, approches, méthodes et techniques nécessaires pour mettre en œuvre et gérer efficacement un SMSI.
- Interpréter les exigences de la norme ISO/CEI 27001 dans un contexte spécifique à l'organisation
- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques relatives au SMSI

PRÉREQUIS

Connaissance de base des systèmes d'information, des principes de sécurité des SI et de gestion de projet

PUBLIC CIBLE

Consultant
RSSI
Chef de projet
Ingénieur SSI
Toute personne impliquée dans le management de la sécurité de l'information ou responsable du maintien de la conformité aux exigences du SMSI

En savoir plus

PRÉSENTIEL

DURÉE : 4.5 JOURS (31H)

REF : ISO27001-LI

TARIF : 3750€ HT

PECB AUTHORIZED PARTNER

FORMATION CERTIFIANTE

MODALITÉ ET DÉLAIS D'ACCÈS :
Accès sur inscription préalable au minimum 15 jours avant la date prévue. Pour être maintenue, une session doit rassembler un minimum de 3 participants

MÉTHODES MOBILISÉES :
Support de cours et norme papier illustrés par des exemples basés sur une étude de cas et des jeux de rôles.

MODALITÉ D'ÉVALUATION :
Examen de certification

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.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

GOUVERNANCE & CONFORMITÉ SSI

SMSI - ISO 27001 LEAD AUDITOR

Cette formation s'adresse à tous les personnels impliqués dans les audits de certification du système de management de la sécurité de l'information ou responsables du maintien de la conformité aux exigences du SMSI.

Aperçu du programme :

- Jour 1 : introduction au système de management de la sécurité de l'information et à la norme ISO/CEI 27001
- Jour 2 : principes, préparation et déclenchement de l'audit
- Jour 3 : activités d'audit sur site
- Jour 4 : clôture de l'audit
- Jour 5 : examen de certification

Détails de la certification :

Cette formation inclut le passage de l'examen « PECB Certified ISO/CEI 27001 Lead Auditor » (3h).
Cette certification délivrée par notre partenaire PECB atteste que vous maîtrisez les 7 domaines de compétences de la norme.
Cet examen est disponible en français et dans plusieurs autres langues.
Les candidats qui n'obtiennent pas un score suffisant ont la possibilité de le repasser dans les 12 mois qui suivent sans frais supplémentaires.

OBJECTIFS

- Comprendre le fonctionnement d'un système de management de la sécurité de l'information (SMSI) conforme à la norme ISO /CEI 27001.
- Diriger un audit et une équipe d'audit.
- Interpréter les exigences d'ISO/CEI 27001 dans le contexte d'un audit du SMSI.
- Acquérir les compétences d'un auditeur : planifier, diriger, suivre un audit et rédiger des rapports en conformité avec la norme ISO 19011.

PRÉREQUIS

Connaissance de base des systèmes d'information, des principes de sécurité des SI, d'audit et de gestion de projet.

PUBLIC CIBLE

Consultant
RSSI
Chef de projet
Ingénieur SSI
Auditeurs
Toute personne souhaitant réaliser et diriger des audits de certification du Système de management de la sécurité de l'information

En savoir plus

PRÉSENTIEL

DURÉE : 4.5 JOURS (31H)

REF : ISO27001-LA

TARIF : 3750€ HT

FORMATION CERTIFIANTE

MODALITÉ ET DÉLAIS D'ACCÈS :
Accès sur inscription préalable au minimum 15 jours avant la date prévue. Pour être maintenue, une session doit rassembler un minimum de 3 participants

MÉTHODES MOBILISÉES :
Support de cours et norme papier illustrés par des exemples basés sur une étude de cas et des jeux de rôles.

MODALITÉ D'ÉVALUATION :
Examen de certification

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.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

GOUVERNANCE & CONFORMITÉ SSI

ANALYSE DE RISQUES - ISO 27005 RISK MANAGER

Cette formation s'adresse à tous les personnels impliqués dans un programme de management du risque.
Elle peut être couplée avec la formation EBIOS RM.

Aperçu du programme :

- Jour 1 : introduction au programme de gestion des risques conforme à ISO/IEC 27005
- Jour 2 : mise en œuvre d'un processus de gestion des risques conforme à ISO/IEC 27005
- Jour 3 : aperçu des autres méthodes d'appréciation des risques liés à la sécurité de l'information et examen de certification

Détails de la certification :

Cette formation inclut le passage de l'examen « PECB Certified ISO/CEI 27005 Risk Manager » (2h).
Cette certification délivrée par notre partenaire PECB atteste que vous maîtrisez les 4 domaines de compétences de la norme.
Cet examen est disponible en français et dans plusieurs autres langues.
Les candidats qui n'obtiennent pas un score suffisant ont la possibilité de le repasser dans les 12 mois qui suivent sans frais supplémentaires.

OBJECTIFS

- Comprendre la relation entre la gestion des risques de sécurité de l'information et les mesures de sécurité.
- Comprendre les concepts, approches, méthodes et techniques du processus de gestion des risques ISO/IEC 27005.
- Acquérir les compétences pour conseiller efficacement les organisations sur les meilleures pratiques en matière de management du risque lié à la sécurité de l'information.

PRÉREQUIS

Connaissances approfondies de l'évaluation des risques et de la sécurité de l'information.

PUBLIC CIBLE

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

En savoir plus

PRÉSENTIEL

DURÉE : 3 JOURS (21H)

REF : ISO27005-RM

TARIF : 2150€ HT

PECB AUTHORIZED PARTNER

FORMATION CERTIFIANTE

MODALITÉ ET DÉLAIS D'ACCÈS :
Accès sur inscription préalable au minimum 15 jours avant la date prévue. Pour être maintenue, une session doit rassembler un minimum de 3 participants

MÉTHODES MOBILISÉES :
Support de cours et norme papier illustrés par des exemples basés sur une étude de cas et des jeux de rôles.

MODALITÉ D'ÉVALUATION :
Examen de certification

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.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

GOUVERNANCE & CONFORMITÉ SSI

EBIOS RISK MANAGER

Cette formation permet de mener une analyse de risques avec la méthode EBIOS développée par l'ANSSI et s'adresse à tous les personnels impliqués dans un programme de management du risque.
Elle peut être couplée avec la formation ISO 27005 RM.

Aperçu du programme :

- Jour 1 : mener une analyse de risques avec EBIOS RM
- Jour 2 : achever une analyse de risques avec EBIOS RM
- Jour 3 : étude de cas & examen de certification

Détails de la certification :

Cette formation inclut le passage de l'examen « PECB Certified EBIOS Risk Manager » (2h).
Cette certification délivrée par notre partenaire PECB atteste que vous maîtrisez l'application de la méthode EBIOS.
Cet examen est disponible en français et dans plusieurs autres langues.
Les candidats qui n'obtiennent pas un score suffisant ont la possibilité de le repasser dans les 12 mois qui suivent sans frais supplémentaires.

OBJECTIFS

- Développer les compétences et connaissances nécessaires pour mener une analyse de risques avec la méthode EBIOS ;
- Maîtriser les étapes de réalisation d'une analyse de risques avec la méthode EBIOS ;
- Comprendre les concepts, approches, méthodes et techniques permettant une gestion du risque en accord avec l'ISO 27005.

PRÉREQUIS

Connaissances approfondies de l'évaluation des risques et de la sécurité de l'information.

PUBLIC CIBLE

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

En savoir plus

- PRÉSENTIEL
- DURÉE : 3 JOURS (21H)
- REF : EBIOS
- TARIF : 2150€ HT

PECB AUTHORIZED PARTNER

FORMATION CERTIFIANTE

MODALITÉ ET DÉLAIS D'ACCÈS :
Accès sur inscription préalable au minimum 15 jours avant la date prévue. Pour être maintenue, une session doit rassembler un minimum de 3 participants

MÉTHODES MOBILISÉES :
Support de cours et norme papier illustrés par des exemples basés sur une étude de cas et des jeux de rôles.

MODALITÉ D'ÉVALUATION :
Examen de certification

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.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

AUTRES FORMATIONS

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. Cursus 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, 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.

En savoir plus

BLENDED

DURÉE : 3H30 E-LEARNING + 3 JOURNÉES (21H)

REF : BL-21434

TARIF : DEMANDEZ UN DEVIS

MODALITÉ ET DÉLAIS D'ACCÈS :
Accès sur inscription préalable au minimum 15 jours avant la date prévue. Pour être maintenue, une session doit rassembler un minimum de 3 participants

MÉTHODES MOBILISÉES :
Support e-learning sonorisés et sous-titrés. 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.

contact@june-factory.com | 05.61.14.03.28
Mars 2026

phosforea
by june factory

209 rue Jean Bart - Bât. Agora 1
31670 Labège

SIRET : 825 216 328 00013
Organisme de formation : 76 31 08704 31

contact@june-factory.com

+33 (0)5 61 14 03 28

Qualiopi processus certifié
RÉPUBLIQUE FRANÇAISE
La certification qualité a été délivrée au titre de la catégorie d'action suivante :
- Actions de formation

www.june-factory.com