thecamp
enabling humans for tomorrow

Accompagner les entreprises dans leur *transformation digitale*

Formation inter-entreprises

10-11 juin 2024

« CYBERSECURITE, REGLEMENTATION, NORMES ET BONNES PRATIQUES »

thecamp
enabling humans for tomorrow

Transformation digitale

PUBLIC VISE

Membres de la Direction Générale, dirigeants, managers, professionnels se questionnant sur la cybersécurité : sa réglementation, ses normes et ses bonnes pratiques.

PREREQUIS

Cette formation ne nécessite pas de prérequis.

DUREE

2 jours
14,00 heures

COÛT

1650 € HT par personne (1970 € TTC)

Ce budget comprend :
La formation sur 2 journées
Le forfait restauration sur place
(Pauses gourmandes matins et après-midis + 2 déjeuners)

Optionnel
Forfait restauration
+ hébergement 1 nuit
+ 1 diner
250 € HT par personne (TVA 10%)

CONTACT

Francis PAPAZIAN
thecamptraining@thecamp.fr

Objectifs stratégiques

- **Acquérir une connaissance approfondie des normes de cybersécurité.**
- **Favoriser une compréhension pratique des risques et des solutions concrètes**

Objectifs opérationnels et pédagogiques

A l'issue de cette formation, vous serez en mesure de :

Objectifs pédagogiques **:**

- **Explorer les normes majeures de cybersécurité**
- **Appliquer les principes de l'ISO 27001 et de la directive NIS2 dans des contextes réels**
- **Mettre en pratique le NIST Framework pour renforcer la sécurité des données**
- **Examiner et comprendre les réglementations complémentaires telles que IA Act, HIPAA et PCI-DSS**
- **Développer les compétences pratiques par le biais d'ateliers**

Objectifs opérationnels :

- **Comprendre et appliquer les normes majeures de cybersécurité pour assurer la conformité et réduire les risques**
- **Évaluer les risques spécifiques à son organisation, définir des stratégies de gestion des risques efficaces et mettre en œuvre des mesures de mitigation adaptées**
- **Comprendre et respecter les réglementations complémentaires telles que HIPAA et PCI-DSS, et les intégrer à sa politique de cybersécurité**
- **Sensibiliser et former les collaborateurs aux bonnes pratiques de sécurité, instaurer une culture de sécurité continue et réagir efficacement en cas d'incident**
- **Sélectionner et déployer des outils de protection adaptés**

★ Contenu

Présentation des objectifs des 2 jours avec un accent sur l'approche proactive en cybersécurité.
Mise en avant de l'importance d'une approche orientée projet face aux normes.

Jour 1- matinée

Module 1 **: Découverte des Menaces et Renforcement des Pratiques Sécuritaires**

- Exploration interactive des menaces courantes (avec des scénarios concrets) avec une focalisation sur la sensibilisation des équipes.
- Analyse approfondie et identification des risques spécifiques aux TPE, intégrant des pratiques dérisquantes, pour renforcer la posture de sécurité de votre organisation, en mettant l'accent sur la projection vers un futur sécurisé.
- Discussion approfondie sur les conséquences financières et opérationnelles des attaques.
- Exploration interactive des techniques d'attaque, incluant le phishing, les ransomwares, etc.
- Études de cas approfondies avec identification de signaux précurseurs, mettant l'accent sur la détection précoce.
- Conseils détaillés sur les bonnes pratiques de sécurité, avec une orientation dérisquante.

Jour 1 – Après-midi

Module 2 **- Techniques d'Attaque et Pratiques Préventives**

- Développement interactif d'un plan d'action en cas d'incident cybernétique.
- Méthodologie interactive pour identifier, isoler et résoudre rapidement les incidents, minimisant les pertes.
- Sensibilisation interactive à la communication et à la notification des incidents, intégrant des stratégies de dérisquage.

Solutions de Protection Accessibles aux TPE

- Présentation interactive des outils et logiciels abordables pour renforcer la sécurité.
- Sélection interactive de solutions en fonction des besoins et des budgets des TPE.
- Démo interactive d'antivirus efficaces basée sur des cas d'utilisation réels.

Développement d'une Culture de Sécurité au sein des Petites Entreprises

- Sensibiliser et former votre personnel aux bonnes pratiques de sécurité.
- Mise en place de processus internes favorisant une culture de sécurité continue, orientée vers un avenir résilient face aux défis cybernétiques.
- Illustration interactive de la mise en place de processus internes pour signaler les incidents de sécurité et y réagir rapidement.

Jour 2 – matinée

Module 3 **- Exploration des Normes et Concrétisation des Pratiques**

- Introduction approfondie aux normes majeures : ISO 27001, NIST, RGPD, NIS2, DORA.
- Analyse des mécanismes de conformité, en mettant l'accent sur la réduction des risques.
- Exemples concrets tirés de cas réels, illustrant la conformité et les conséquences en cas de non-conformité.
- Atelier interactif sur la mise en œuvre de l'ISO 27001 et des directives NIS2
- Approfondissement des principes de gestion des risques et de classification des informations pour minimiser les vulnérabilités.
- Retours d'expérience concrets et partage des meilleures pratiques pour optimiser les processus et systèmes.

Jour 2 – après-midi

Module 4 - **Mise en Lumière du NIST Framework et de la RGPD**

- Session interactive sur l'application concrète du NIST Framework avec une perspective sur les projets de conformité.
- Discussions approfondies sur les implications de la RGPD, mettant en avant les opportunités de dérisquage des pratiques.
- Scénarios interactifs détaillant la conformité avec la RGPD, en soulignant les bonnes pratiques de protection des données.
- Régulation de l'intelligence artificielle (AI Act) et des plateformes numériques (DMA/DSA)
- Vue d'ensemble interactive d'autres réglementations telles que HIPAA et PCI-DSS.
- Discussions approfondies en groupe sur les exigences spécifiques de ces réglementations.

Modalités

Modalités pédagogiques

La formation est fondée sur des principes de pédagogie active, participative, concrète et ludique et alterné :

- apports de connaissances théoriques,
- brainstorming questions/réponses,
- mise en pratique par des exercices et applications,
- échanges de bonnes pratiques,
- vidéos…

Moyens et supports pédagogiques

Outils
Les salles sont équipées d'écrans multimédia et de tous les outils et matériel nécessaires au bon déroulement de la formation.

Support
Le support pédagogique sera envoyé à chaque participant sous format digital.

Modalités d'évaluation et de suivi

Avant la formation
Le stagiaire reçoit en amont de la formation (par mail) un questionnaire permettant de recueillir ses besoins et de préciser ses attentes individuelles.

Pendant la formation
Une évaluation formative sera réalisée par l'intervenant pour s'adapter au mieux aux besoins des participants.
En début et fin de formation, un quizz ou un QCM sera proposé afin d'évaluer l'acquisition des compétences liées à la formation.

Après la formation
Une attestation de « fin de formation » sera adressée à chaque participant.

Modalités d'évaluation de la satisfaction des participants
A l'issue de la formation, un questionnaire de satisfaction *(*dit *«à chaud »)* est adressé à chaque participant pour évaluer son niveau de satisfaction sur le contenu, les méthodes pédagogiques, le formateur,…
Dans un délai de 3 mois après la formation, le participant recevra un nouveau questionnaire de satisfaction (dit *« à froid »)* pour appréhender la mise en œuvre opérationnelle de la formation.

Admission et Accessibilité

Information sur l’admission

Admission sans disposition particulière.

Délai d’accès à la formation

Entre 1 et 6 mois

Conditions d’accès au site

Bus depuis la gare TGV et taxis.

Conditions d'hébergement et de restauration

Restauration sur place (« forfait restauration » cf conditions financières)
Hébergement sur place à thecamp Hôtel & Lodge, possible sur demande

Informations sur l'accessibilité

Nos locaux sont accessibles aux personnes à mobilité réduite (*)

(*) Si l'un ou plusieurs des participants présentent une situation de handicap, un entretien avec le formateur, en amont de la formation, nous permettra de confirmer la possibilité d'adapter les moyens de la prestation.