Cybersécurité - Initiation

Initiation à la cybersécurité pour ETI et PME Prévention et Réaction

Cette formation de 2 jours en « **Initiation à la cybersécurité** » est conçue **pour les ETI et PME** afin de les **sensibiliser aux risques cybernétiques**.

Elle vise à **explorer les vecteurs d'attaque**, les vulnérabilités et les **conséquences financières et opérationnelles** des cyberattaques.

L'objectif est de **renforcer les pratiques de sécurité**, en mettant l'accent sur le **développement de stratégies défensives adaptées aux ETI et PME**, la gestion des incidents et **optimiser la réactivité des équipes de sécurité**.

Objectifs

Identifier et évaluer les risques uniques pour les petites et moyennes entreprises	Appliquer des principes de sécurité avancés adaptés aux PME	Élaborer des plans préventifs et réagir efficacement aux menaces	Réagir promptement face aux cyberattaques	Maîtriser les techniques pour renforcer la sécurité informatique

Publics cibles

Ce parcours est ouvert aux professionnels des petites et moyennes entreprises (ETI et PME), gestionnaires, responsables informatiques et toute personne souhaitant renforcer leurs connaissances.

Pré-requis et objectifs pédagogiques

Des connaissances de base en informatique et une compréhension générale des risques de sécurité liés aux données. Aucune expertise avancée n'est nécessaire, mais une familiarité avec les concepts informatiques de base serait bénéfique.

- Comprendre les menaces des ETI et PME
- Évaluer et défendre les vulnérabilités
- Appliquer des principes de cybersécurité adaptés
- Détecter et réagir aux attaques
- Renforcer les pratiques de sécurité

Programme

Cette formation se démarque par son approche pratique et opérationnelle.

Elle est proposée en présentiel, dure 14 heures, et est déployée sur deux journées consécutives.

Axée sur les enjeux spécifiques des ETI et PME, elle combine des présentations interactives et des études de cas concrets pour offrir une vision approfondie des risques cybernétiques.

Ce programme débutera par une contextualisation de la cybersécurité et son importance dans l'environnement numérique actuel, puis sera fait un aperçu rapide des normes majeures avec une brève mention de leur application, ainsi qu'une présentation succincte sur l'importance de la conformité intersectorielle.

1. Risques cybernétiques spécifiques aux ETI et PME

> Analyse des menaces et des risques pour les ETI et PME
Méthodes d'analyse de risques, cartographie de l'existant, définition des référentiels, actions d'audit ponctuelles

> Évaluation des vulnérabilités
Identification des faiblesses courantes dans les infrastructures des ETI et PME

> Impact financier et opérationnelles
Illustration des conséquences financières et opérationnelles des cyberattaques

2. Sensibilisation aux attaques courantes des ETi et PME

> Techniques d'attaque fréquentes
Découverte des méthodes et analyse

> Études de cas : Scénarios d'illustration des méthodes d'attaque et impacts potentiels

> Mécanismes de propagation des menaces
Compréhension des mécanismes par lesquels les menaces se propagent dans les ETI et PME

3. Principes fondamentaux de cybersécurité pour ETI et PME :

> Concepts fondamentaux de sécurité
Explication des concepts de confidentialité, d'intégrité et de disponibilité des données dans le contexte des ETI et PME

> Normes et meilleures pratiques
Normes de sécurité et meilleures pratiques adaptées aux ressources et aux contraintes des ETI et PME

> Stratégies de défense adaptées ETI et PME
Développement de stratégies de défense alignées sur les besoins spécifiques des PME, avec des conseils pratiques pour leur mise en œuvre

4. Renforcement des pratiques de sécurité pour ETI et PME :

> Approfondissement des bonnes pratiques
Bonnes pratiques sur l'ensemble de la chaine du SI

> Élaboration de plans de protection
Plans proactifs pour prévenir les cybermenaces courantes et protéger les ETI et PME

> Mesures proactives
Mise en place de mesures pour contrer les attaques courantes

5. Gestion des incidents et réponse aux cybermenaces pour les ETI et PME :

> Détection précoce des cyberattaques
Techniques de détection dans les environnements ETI et PME

> Formation à la réponse aux incidents
Entraînement pratique pour répondre efficacement

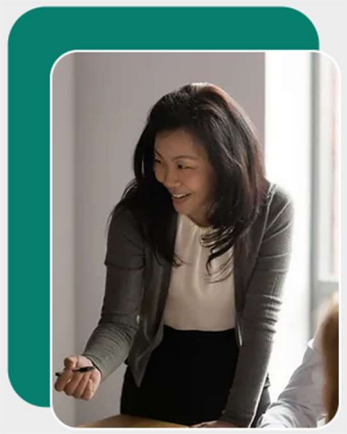
> Gestion des incidents spécifiques
Approche adaptée à la taille des ETI et PME

6. Exercices pratiques de simulation pour les ETI et PME :

> Simulation d'attaques d'incidents
Démonstrations pratiques pour renforcer la réactivité des équipes de sécurité

> Analyse des réponses et débriefing
Analyse des réponses lors des simulations afin d'améliorer les stratégies de défense et le processus de réponse aux incidents

Compétences ciblées



- Identifier et évaluer les risques uniques pour les petites entreprises
- Appliquer des principes de sécurité avancés adaptés aux ETI et PME
- Élaborer des plans préventifs et réagir efficacement aux menaces
- Réagir promptement face aux cyberattaques
- Maîtriser les techniques pour renforcer la sécurité informatique

Moyens pédagogiques

Cette formation repose sur des **ateliers interactifs**, des **débats approfondis**, des **études de cas réels**, et des **simulations d'attaques pratiques**, offrant ainsi une **approche immersive** pour explorer les spécificités des risques cybernétiques.

Elle fournit une **compréhension approfondie des menaces spécifiques aux ETI et PME**, des techniques d'attaque courantes, ainsi que **des concepts fondamentaux de cybersécurité** adaptés aux entreprises de taille moyenne.

Cette formation vise à habiliter les participants à **renforcer activement les pratiques de sécurité** de leur organisation en développant des **compétences proactives et réactives**, tout en visant à **améliorer la détection précoce** et la **gestion des incidents** liés à la cybersécurité.

Moyens d'encadrement

La formation est assurée par un formateur.rice expert.e en cybersécurité, disposant d'une expérience professionnelle significative sur la thématique et une expérience en techniques

Modalités d'évaluation

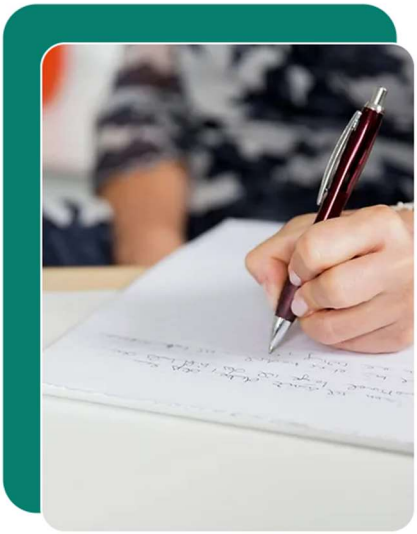
Les évaluations se dérouleront à travers des simulations d'attaques pour tester les réactions face à des scénarios réalistes.

Le dispositif d'évaluation est composé de :

- Quiz interactifs afin d'évaluer la compréhension des risques et techniques d'attaque
- Des exercices pratiques afin d'évaluer la mise en place concrète des mesures de sécurité

Ces méthodes d'évaluation permettront de mesurer la réactivité, la compréhension et l'application des connaissances acquises lors de la formation.

Une attestation de réalisation est remise à chaque participant à l'issue de la formation. Une attestation de réussite est remise aux participants satisfaisant les critères de réussite de la formation.



Prix et modalités d'accès

La formation est commercialisée en inter-entreprise et en intra-entreprise pour des groupes de 6 à 12 personnes.

Prix HT : à partir de 1750€

Innov8learn
98 rue du Château - 92100 Boulogne-Billancourt