Cybersécurité - Maîtrise

Maîtrise de la cybersécurité : Evoluer avec assurance

Cette formation de 2 jours « **Maîtrise de la cybersécurité** » est conçue pour les **TPE / PME et collectivités**, afin de vous aider à **faire face aux défis croissants de la cybercriminalité**.

Elle vise à **renforcer les connaissances existantes** tout en vous fournissant les outils nécessaires pour adapter et **actualiser vos compétences** dans le paysage complexe de la **cybersécurité actuelle**.

L'objectif est d'approfondir les **connaissances en techniques d'attaque/défense**, de se mettre à jour face aux **menaces émergentes**, et d'approfondir les compétences en **sécurité réseau**.

Objectifs

Analyser les menaces émergentes et leurs impacts

(Identifier et différencier les techniques d'attaques sophistiquées)

Appliquer des stratégies de sécurisation avancées

(Configurer et tester des défenses multicouches pour protéger les réseaux)

Élaborer des plans de réponse adaptés

(Actualiser les procédures de réponse aux incidents en intégrant des scénarios de crises complexes)

Publics cibles

Ce parcours est ouvert aux professionnels des petites et moyennes entreprises (PME), gestionnaires, responsables informatique et toute personne souhaitant approfondir leurs connaissances techniques.

Pré-requis

Des connaissances en informatique, notamment les techniques de sécurisation des réseaux ainsi qu'une compréhension générale des systèmes et des risques de sécurité liés aux données sont nécessaires.

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 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

1. Actualisation des techniques d'attaque et de défense

> Techniques d'attaques avancées
Vulnérabilités 5G, mais aussi attaques spécifiques à l'IoT, ransomware sophistiqué, etc…

> Défenses avancées
Utilisation de l'IA pour la détection de menaces multiplateformes

> Pratique
Scénarios d'attaques simulées pour tester la réactivité face aux menaces avancée

2. Évolution des menaces et adaptation

> Analyse de menaces émergentes
Focus sur les menaces émergentes telles que l'IA malveillante, les attaques par détour de l'IA, etc.

> Stratégies d'adaptation :
Intégration de stratégies de défense multicouche adaptatives

> Pratique
Simulation de scénarios d'attaques évoluées pour tester les réponses adaptatives.

3. Renforcement de la sécurité réseau

> Sécurisation avancée des réseaux
Approfondissement des techniques de sécurisation des réseaux 5G, Cloud, IoT, etc.

> Analyse comportementale et IA
Utilisation avancée de l'IA pour l'analyse comportementale dans des environnements diversifiés

> Pratique
Exercices de configuration avancée des réseaux pour mettre en œuvre des techniques de sécurisation avancées.

4. Gestion des crises et actualisation des plans de réponse

> Actualisation des plans de réponse aux incident
Actualisation des plans de réponse aux incidents

> Simulation de crise avancée
Exercices de gestion de crises cybernétiques complexes pour affiner la réactivité et les procédures d'intervention

> Pratique
Simulation de cybercrises multiplateformes pour une gestion holistique des incidents

Compétences ciblées

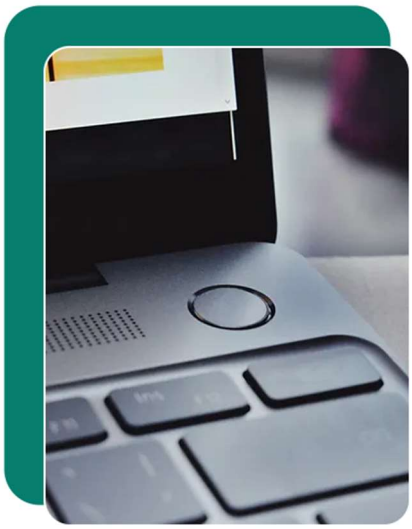
- Identification et évaluation des menaces
- Détection proactive des cyberattaques
- Mise en œuvre de solutions de sécurisation
- Gestion holistique des crises
- Amélioration continue des plans de réponse

Moyens pédagogiques

Cette formation repose sur des **présentations didactiques**, des exercices pratiques, des **plateformes virtuelles**, et **des discussions interactives** pour offrir une expérience d'apprentissage complète, et explorer les aspects concrets des cyberattaques sophistiquées.

Elle fournit une **compréhension** approfondie des **défis pratiques de la cybersécurité**, une maîtrise des **compétences avancées en sécurité réseau**, et une **expertise opérationnelle** dans l'analyse comportementale.

Cette formation vise à habiliter les participants à **faire face aux défis complexes de 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 d'animation.

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 :

- Tests pratiques évaluant la capacité à utiliser des outils ou à appliquer des concepts sur des cas concrets
- Quiz : Évaluation des connaissances théoriques par des questions à choix multiples

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 1900€

Cette formation est accessible aux personnes en situation de handicap, n'hésitez pas à nous contacter pour toute demande ou à vous adresser à notre référent handicape dont vous trouverez les coordonnées dans nos informations légales / accessibilité

Innov8learn
98 rue du Château - 92100 Boulogne-Billancourt