Cybersécurité – Expertise technique

Expertise technique avancée en Cybersécurité

Cette formation de 2 jours « **Expertise en cybersécurité** » est spécifiquement **conçue pour les DSI, RSSI** et prépare à **anticiper les défis futurs de manière holistique**.

Elle **nécessite une solide expérience technique dans le domaine des services informatiques ou de la cybersécurité**, avec **une bonne maîtrise des outils et pratiques de base en cybersécurité**.

L'objectif est la **compréhension des techniques avancées d'attaques et de défense**, explorer les vulnérabilités 5G, Cloud, IoT, **perfectionner ses compétences en détection et exploitation de vulnérabilités**, et **la prise en compte des fonctionnalités de l'Intelligence Artificielle** pour anticiper et contrôler les menaces.

Objectifs

Maîtriser les scénarios cyber avancés, vulnérabilités zero-day, attaques physiques/logiques	Employez des outils spécialisés pour des attaques ciblées avancées	Développer les compétences détection/réaction, réponse rapide, contre-mesures immédiates	Analyser les architectures SCADA, IoT, Cloud, identifier/exploiter les vulnérabilités	Gérer les cybercrises, simuler des scénarios complexes, élaborer des plans face aux attaques avancées

Publics cibles

Ce parcours est ouvert aux professionnels des services informatiques (DSI, RSSI, RSI, RISR…) évoluant au sein de TPE, PME et collectivités, souhaitant renforcer les compétences avancées en cybersécurité

Pré-requis et objectifs pédagogiques

Cette formation exige une expérience professionnelle d'au moins 5 ans dans le domaine des services informatiques avec une connaissance de la cybersécurité. Une utilisation courante et maîtrise des outils avancés de sécurité numérique ainsi qu'une pratique régulière dans la gestion de systèmes informatiques sécurisés, afin d'atteindre les objectifs suivants :

- Comprendre les techniques avancées d'attaque et de défense en cybersécurité
- Acquérir des compétences pratiques dans l'utilisation d'outils spécialisés
- Développer des capacités d'analyse forensique et de reconstruction de scénarios d'attaques complexes
- Maîtriser les techniques de sécurisation des systèmes et la gestion de crises cybernétiques

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 dirigeants, elle combine scénarios concrets et complexes, mettant ainsi l'accent sur les défis spécifiques auxquels les entreprises peuvent être confrontées.

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. Comprendre les techniques avancées d'attaque et de défense en cybersécurité

> Scénarios avancés de cyberattaques simulées en temps réel
Exploitation de vulnérabilités zero-day, attaques par injection de code, attaques physiques combinées à des attaques logiques

> Acquérir des compétences pratiques dans l'utilisation d'outils spécialisés

> Détection et réaction
Exercices pratiques de détection d'attaques sophistiquées, avec une emphase sur la réaction rapide et l'implémentation de contre-mesures immédiates

2. Analyse avancée de sécurité des systèmes

> Explorer les vulnérabilités
5G, IoT, et Cloud

> Appliquer les solutions de patching avancées

> Développer des capacités d'analyse forensique

> Développer des capacités de reconstruction de scénarios d'attaques complexes

> Maîtriser les techniques de sécurisation des systèmes de la gestion de crises cybernétiques

3. Gestion de crises et réponses aux incidents majeurs

> Perfectionner les compétences en détection, exploitation de vulnérabilités et simulation de crises

> Elaborations de stratégies holistiques face aux menaces

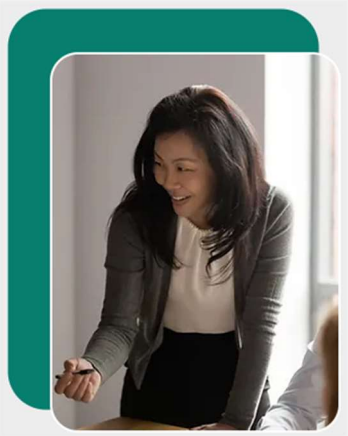
> Communication en situations d'urgence

4. Séance d'approfondissement IA

> Prise en compte des fonctionnalités de l'Intelligence Artificielle
Anticipation et contrôle des menaces

> Echange
Exploration approfondie des défis contemporains.

Compétences ciblées



- Maîtrise des simulations avancées d'attaques
- Expertise dans l'utilisation d'outils de sécurité avancés
- Analyse approfondie des architectures sécurisées
- Compétences en gestion de crises et réponses aux incidents majeurs
- Capacité à communiquer efficacement en situation d'urgence

Moyens pédagogiques

Cette formation repose sur des **scénarios avancés et des attaques ciblées**, elle offre ainsi une compréhension approfondie des cybermenaces sophistiquées et des attaques combinées. Elle fournit des **solutions pratiques et immédiatement applicables** pour contrer ces risques spécifiques.

En parallèle, elle explore les **fondamentaux avancés de la cybersécurité**, adaptés aux professionnels des services informatiques.

De la détection précoce à la mise en œuvre de contre-mesures, en passant par des simulations réalistes, cette formation permet de **renforcer la posture de sécurité de votre organisation** et faire face efficacement aux défis croissants des cybermenaces.

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 avancées, évaluant la capacité à détecter, réagir et contrer des attaques sophistiquées en temps réel.

Le dispositif d'évaluation est composé de :

- Tests pratiques la capacité à résoudre des défis complexes, tandis que des discussions approfondies évalueront les résultats obtenus et les techniques utilisées
- Quiz : Evaluation des connaissances théoriques par des questions à choix multiples

Ces méthodes d'évaluation visent à mesurer la réactivité, la compréhension et l'application des connaissances acquises pendant 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 2400€

Innov8learn
98 rue du Château - 92100 Boulogne-Billancourt