Cybersécurité - Gouvernance

Gouvernance en Cybersécurité

Cette formation de 2 jours « **Gouvernance en cybersécurité** » est spécifiquement conçue pour les directeurs et responsables de la sécurité des systèmes, et toute personne impliquée dans la gestion stratégique de la cybersécurité.

Elle vise à **renforcer vos compétences en cybersécurité**, en mettant l'accent sur la **les cadres législatifs et normatifs**, la **gestion des risques, la gestion de crise et la continuité d'activité, la stratégie de sécurité** et le **leadership** face à des menaces variées.

L'objectif est de **renforcer les connaissances** et le **développement de stratégies holistiques** pour **anticiper les menaces futures**.

Objectifs

Acquérir une compréhension approfondie des vulnérabilités multiplateformes	Maîtriser l'utilisation avancée de l'intelligence artificielle dans le contexte de la cybersécurité	Acquérir des compétences avancées en détection, exploitation de vulnérabilités et gestion d'incidents	Élaborer des stratégies de cybersécurité holistiques et anticiper les menaces futures	Faciliter le partage d'expertise et résoudre des défis multiplateformes lors d'ateliers et de discussions

Publics cibles

Ce parcours est ouvert aux directeurs, responsables de la sécurité des systèmes d'information et toutes personnes initiées à la cybersécurité, souhaitant renforcer leurs connaissances.

Pré-requis et objectifs pédagogiques

Cette formation exige une expérience professionnelle d'au moins 2 ans dans le domaine des services informatiques, accompagnée d'une connaissance en cybersécurité et d'une utilisation régulière d'outils avancés dans ce domaine, afin d'atteindre les objectifs suivants :

- Explorer les vulnérabilités 5G, Cloud, IoT et appliquer des solutions de patching avancées
- Maîtriser l'utilisation de l'intelligence artificielle pour anticiper et contrôler les menaces
- Perfectionner les compétences en détection, exploitation de vulnérabilités et simulations de crises
- Élaborer des stratégies holistiques face aux menaces, anticiper les évolutions technologiques pour un leadership solide en cybersécurité

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 intersectorielle.

1. Cadre législatif et normatif

> Normes clés et leur impact

> Cadres légaux, réglementaires et normatifs
(RGPD, NIS Directive, ISO/IEC 27001...)

> Application pratique

> Conformités et réglementations complémentaires

2. Gestion des risques

> Gestion des vulnérabilités multiplateformes
Approfondissement des vulnérabilités 5G, Cloud, IoT, et des solutions avancées de patching

> Méthodes d'évaluation

> Intelligence artificielle dans la cybersécurité
Utilisation avancée de l'IA pour anticiper les menaces sur diverses plateformes

> Mise en pratique avancée de détection et d'exploitation de vulnérabilité
Exercices avancés de détection et d'exploitation de vulnérabilités pour affiner les compétences

2. Gestion de crises et de continuité d'activité

> Elaboration et mise en oeuvre de plans de continuité d'activité et de réponses aux incidents

> Stratégie de sécurité
Développement de stratégies de cybersécurité

> Objectifs d'affaires et de réglementations

3. Leadership en cybersécurité

> Renforcement des compétences
Leadership face à des menaces diversifiées

> Communication pour promouvoir une culture de sécurité

> Anticipation des évolutions technologiques pour un leadership solide

5. Elaborer des stratégies holistiques face aux menaces

> Analyse de l'écosystème des menaces
Exploration approfondie de scénarios spécifiques aux participants, incluant les défis multiplateformes

> Approche intégrée de la sécurité
Adoption d'une approche globale qui intègre la technologie, les processus et les personnes pour contrer les menaces de manière holistique

> Adaptabilité et évolutivité
Capacité à s'adapter aux nouvelles menaces et à évoluer dans un environnement en constante évolution en ajustant continuellement les stratégies de sécurité.

Compétences ciblées

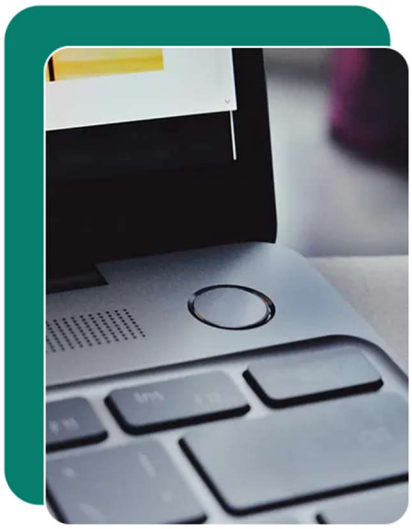
- Gestion des vulnérabilités multiplateformes
- Utilisation avancée de l'intelligence artificielle en cybersécurité
- Exercices pratiques de détection et d'exploitation de vulnérabilités
- Simulation de crises et gestion d'incidents complexes
- Leadership en cybersécurité et élaboration de stratégies holistiques

Moyens pédagogiques

Cette formation s'appuie sur **approche immersive et pratique** pour plonger les candidats dans des **scénarios réalistes afin de renforcer la réactivité**.

Parallèlement, elle offre une **analyse approfondie des vulnérabilités** multiplateformes ainsi qu'un volet **leadership** afin d'encourager les **échanges en situation d'urgence**.

Elle vise à renforcer la **posture de sécurité organisationnelle** et à fournir des **solutions immédiatement applicables** face 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

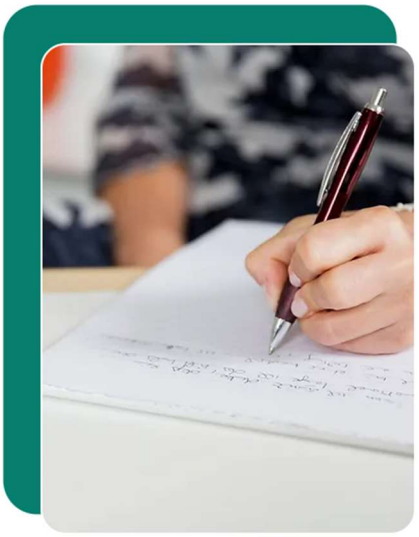
Les évaluations se dérouleront à travers des simulations d'attaques pour tester les réactions face à des scénarios réalistes.

Le dispositif d’évaluation est composé de :

- Exercices pratiques : Évaluation des compétences pratiques à travers des exercices ciblés
- Quiz : Évaluation des connaissances théoriques sur des sujets avancés

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 2100€

Innov8learn
98 rue du Château - 92100 Boulogne-Billancourt