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

- Identifier et comprendre les principales normes et réglementations applicables à leur environnement
- Évaluer et renforcer les capacités de réponse aux incidents cyber
- Développer des stratégies holistiques de cybersécurité alignées sur les objectifs de l'entreprise

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

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.

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. Introduction à la règlementation et normes

> Contextualisation de la cybersécurité : Introduction à l'importance de la cybersécurité dans l'environnement numérique actuel

> Normes clés et leurs impacts
Aperçu rapide des normes majeures telles que l'ISO 27001, le NIST, le RGPD, la directive NIS2, etc.

> Atelier application pratique des normes cyber. La démarche cyber comme principe de résilience de l'entreprise

2. Simulation de crises et la réponse à incident

> Exercices pratiques multiplateformes : Simulation de scénarios d'incidents cyber réalistes

> Stratégie de sécurité : Gestion d'incidents complexes sur différentes plateformes pour perfectionner la réactivité

> Exercices bonnes pratiques et fausses bonnes idées

> Exemples de chantiers pour renforcer sa résilience et les réponses à incident

3. Mesures et gestion de sa cyber

> Mesures de protection : basics
Mesures techniques, architectures, organisation (énumération)

> Technologies de sécurité opérationnelle
Les prestations - EDR, SIEM, SOC, Bastion, Intelligence artificielle, etc.

4. Leadership en cybersécurité et conseil stratégique

> Stratégie de cybersécurité holistique :
Leadership face à des menaces diversifiées, élaboration de stratégies.
La sécurité intégrée dans les objectifs d'entreprise.

> Anticipation des menaces futures : discussions sur les tendances émergentes et les technologies futures en cybersécurité.

> Atelier : Etablir un plan de sensibilisation efficace, mesuré, et en accord avec les objectifs de sécurités

5. Séance d'approfondissement et échange d'expertise

> Ateliers de discussion
Exploration approfondie de scénarios spécifiques aux participants, incluant les défis multiplateformes

> Partage d'expertise
Échange d'expériences pour aborder des solutions innovantes face aux menaces diversifiées sécurité

> Modules avancés pour perfectionner les compétences existantes, séances pratiques approfondies sur des sujets pointus.

Compétences ciblées

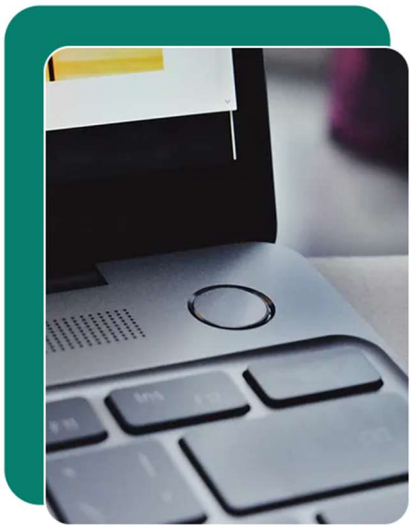
- Acquérir une compréhension approfondie des cadres légaux et réglementaires et du risque cyber
- Evaluer son niveau de maîtrise en cas de crise cyber
- Développer des stratégies de cybersécurité pour se préparer à une crise
- Déterminer les différents chantiers techniques à tenir
- Etablir un plan de sensibilisation efficace et mesuré
- Élaborer des stratégies de cybersécurité holistiques face aux menaces futures

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

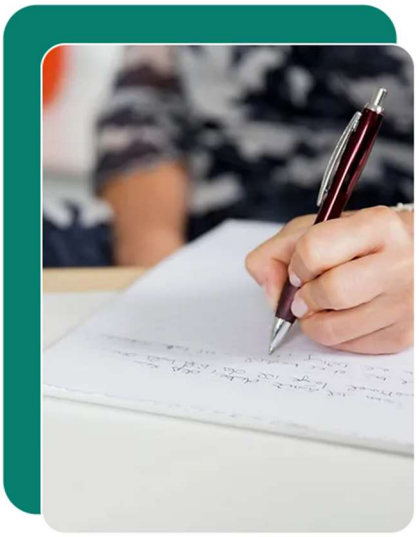
Les évaluations se dérouleront à travers des simulations d'attaques pour tester les réactions face à des scénarios réalistes.

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€

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