INNOV8LEARN
FORME AUX ENJEUX DE DEMAIN

fait partie du groupe

GROUPE EDU FORM' ACTION

CYBERSÉCURITÉ 2024 : POURQUOI VOTRE PME EST LA PROCHAINE CIBLE DES HACKERS ?

Dirigeants d'entreprises,
comment mettre en place une stratégie
en cybersécurité efficace pour votre structure ?

SOMMAIRE

INTRODUCTION

Qu’est-ce que la Cybersécurité ?

Sécuriser un système d’information est essentiel pour garantir la pérennité d’une entreprise, mais aussi pour accroître sa compétitivité. Dans un contexte où les menaces internationales ne cessent de croître, la cybersécurité concerne toutes les entreprises, indépendamment de leur taille. Que ce soit pour une TPE, une PME ou une ETI, la sécurisation des systèmes d’information est une priorité pour tous les **acteurs économiques.** La menace cyber est bien réelle et peut frapper n’importe quelle entreprise.

Définition de la Cybersécurité

La cybersécurité englobe l’ensemble des technologies, processus et pratiques conçus pour protéger les réseaux, ordinateurs, programmes et données contre les attaques, dommages ou accès non autorisés. Dans un monde où les technologies numériques sont omniprésentes, assurer la sécurité de ces systèmes est devenu une priorité absolue pour les entreprises de toutes tailles et quel que soit leur secteur d’activité.

Pour vous faire accompagner dans votre démarche CYBER, contactez Innov8Learn à : contact@innov8learn.fr

L’importance de la cybersécurité pour les ETI, TPE et PME

Selon une étude de l’Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI), paru début 2024, 40 % des attaques par rançon logiciels visent les entreprises de petites et moyennes tailles.

La cybersécurité est un enjeu crucial pour les entreprises de toutes tailles, et plus particulièrement pour les ETI, TPE et PME. Dans un environnement numérique en constante évolution, ces entreprises sont souvent perçues comme des cibles privilégiées pour les cybercriminels, en raison de leur faible niveau de **protection des donnée**s et d’une **vigilance parfois insuffisante** en matière de sécurité informatique.

Dans un environnement où les crises sont inévitables, il est crucial de s’y préparer et de s’en protéger pour assurer une continuité d’activité sans interruption, garantir la **confiance des collaborateurs** et des partenaires, maintenir sa **compétitivité** et éviter des pertes financières qui peuvent être considérables.. Pour ce faire, **sensibilisation**, **anticipation et protection doivent être au cœur de toute démarche de cybersécurité**, intégrée de manière indissociable à la stratégie globale de l’entreprise.

Objectifs du Livre Blanc

Ce livre blanc vise à sensibiliser les ETI, TPE et PME aux risques liés à la cybersécurité, à vous éclairer sur les **grands enjeux de la cybersécurité en 2024** et sur son **importance pour les années à venir** et à fournir les bonnes pratiques et les **solutions** pour protéger leurs infrastructures. Nous aborderons les principales menaces, les conséquences d’une mauvaise gestion de la cybersécurité, et les **mesures de prévention et de protection** nécessaires. Enfin, nous présenterons les solutions de formation d’Innov8Learn pour renforcer la cybersécurité de votre entreprise.

Dans ce Livre Blanc “Cybersécurité : ETI, TPE & PME, quelles mesures pour votre structure ?”

- Approfondissez vos connaissances sur les cybermenaces, leurs enjeux et spécificités pour votre structure.
- Découvrez l’état des lieux des bonnes pratiques de la cybersécurité en 2023 et 2024 pour connaître les grandes tendances cyber à venir.
- Visualisez l’importance de la formation de vos équipes et collaborateurs pour se faire accompagner par des experts cybersécurité afin d’assurer la pérennité et la croissance de votre entreprise.

1- QUELS SONT LES RISQUES & ENJEUX DE LA CYBERSÉCURITÉ POUR LES ENTREPRISES ?

INNOV8 LEARN
FORME AUX ENJEUX DE DEMAIN

COMPRENDRE LES RISQUES & LES ENJEUX DE LA CYBERSÉCURITÉ

1- Quelles sont les principales cybermenaces pour votre structure ?

Les entreprises, quelle que soit leur taille, sont exposées à diverses cybermenaces, dont les plus courantes incluent :

- **Exploitation de vulnérabilités** : Utilisation de failles de sécurité dans les logiciels ou les systèmes pour accéder à des informations sensibles ou prendre le contrôle des systèmes.
- **Ransomware (rançongiciel)** : Logiciels malveillants qui chiffrent les données de l'entreprise et exigent une rançon pour les déchiffrer.
- **Phishing (hameçonnage)** : Attaque où les cybercriminels se font passer pour des institutions de confiance pour inciter les victimes à révéler des informations sensibles.
- **Malware (logiciel malveillant)** : Programmes malveillants conçus pour infiltrer, endommager ou désactiver les systèmes informatiques.
- **Attaques par déni de service (DDoS)** : Attaques visant à rendre un service indisponible en le submergeant de trafic.

2- Les conséquences d'une mauvaise gestion de la cybersécurité de votre entreprise

Les conséquences d'une mauvaise gestion de la cybersécurité peuvent être importantes pour les PME :

- **Perte financière** : Les attaques peuvent entraîner des coûts élevés en termes de rançons, de réparations et de pertes de revenus.
- **Atteinte à la réputation** : Une violation de données peut nuire gravement à la confiance des clients et des partenaires.
- **Perturbation des activités** : Les attaques peuvent paralyser les opérations quotidiennes, entraînant des interruptions de service.
- **Amendes réglementaires** : Le non-respect des normes de protection des données peut entraîner des sanctions juridiques et financières.

En 2022, les organisations ont subi en moyenne 1,8 cyberattaques. 43 % d'entre elles en ont même subi en moyenne 4,3.

La formation de vos équipes en cybersécurité est un levier indispensable pour assurer le bien-être de votre structure et prévenir le risque de cyber-attaques.

Selon le **PwC 2024 Global Digital Trust Insights*,** les disparités entre les structures en matière de cybersécurité représentent un volume important.

Selon ce rapport, **parmi le top 5 % des répondants, 96 % d'entre eux répondent que leurs équipes cyber réagissent rapidement dans 80 à 100 % des cas de cyber attaques**. Mais ce n'est pas le cas pour l'ensemble des organisations, dont certaines sous-estiment à coup sûr les risques cyber.

Les défis spécifiques des PME concernant la cybermenace

Les **PME (Petites et Moyennes Entreprises) et TPE** sont les cibles premières des cyber attaques. Toujours selon ce rapport, seulement 23 % des dirigeants d'entreprises interrogés considérent la cybersécurité comme l'une des menaces majeures des entreprises. En 2024, la cyberrésilience représente ainsi l'un des enjeux majeurs : les organisations vont devoir se prémunir contre ces menaces de façon très sérieuse.

Le nombre de cyberattaques est en constante augmentation en France et dans le monde. Il est toutefois possible de diminuer leur coût moyen grâce à une **protection informatique efficace** et à des **pratiques de cybersécurité** rigoureuses. Les coûts élevés des cyberattaques sont souvent liés à des **interruptions de production** ou au **vol de données**.

Avec la **digitalisation massive des entreprises**, la quantité de **données sensibles** ne cesse de croître, offrant davantage de cibles aux cybercriminels, notamment dans les attaques par **ransomware**. Par conséquent, il est essentiel de renforcer la **protection des données** pour éviter des coûts conséquents et assurer la continuité des activités..

POUR DÉCOUVRIR LA FORMATION CYBER GOUVERNANCE D'INNOV8LEARN, CLIQUEZ ICI.

*https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights/report-download.html

3- Les tendances de la cybersécurité 2024

Le **rapport SoSafe, "Les tendances en cybercriminalité en 2023"*** met en évidence **4 grandes tendances de la cybersécurité pour 2024** que les organisations devront anticiper.

Pour en savoir plus sur l'offre de formations en cybersécurité d'Innov8Learn, découvrez l'article exclusif de Silicon en partenariat avec Innov8Learn

1- L'essor de l'IA

L'intelligence artificielle (IA) jouera un rôle crucial dans la cybersécurité des années à venir. Il est important de distinguer entre l'IA défensive et l'IA offensive. L'IA défensive, intégrée dans des solutions comme les pare-feu et les antivirus, permet de renforcer et d'optimiser ces outils. En revanche, l'IA offensive est utilisée par les hackers pour analyser de vastes quantités de données et détecter des failles informatiques ou des vulnérabilités de sites web.

2- Le phishing

Le phishing reste un des principaux vecteurs d'attaque pour les cybercriminels, qui utilisent la manipulation psychologique pour tromper les employés des entreprises ciblées. En gagnant leur confiance, les hackers incitent les victimes à cliquer sur des liens frauduleux et à divulguer des informations sensibles (identifiants de comptes Office, LinkedIn, etc.). Ces attaques peuvent engendrer le vol de données de millions de personnes, exposées sur le dark net.

3- Le risque de burn-out des équipes de sécurité

Les experts en cybersécurité sont des ressources précieuses pour les entreprises. Avec la montée de la cybercriminalité, leur travail demande une expertise et une vigilance accrues, augmentant la pression sur ces professionnels. Il est crucial de soutenir ces équipes en les formant.

4- Les crises géopolitiques

Les cybercriminels exploitent les crises géopolitiques, comme la guerre en Ukraine, pour accroître l'anxiété et infiltrer des systèmes informatiques bien protégés. Les attaques contre des personnalités politiques et les systèmes de surveillance massifs illustrent bien cette tendance.

*https://sosafe-awareness.com/fr/ressources/rapports/tendances-en-cybercriminalite/

2- PRÉVENTION & PROTECTION : QUELLES SOLUTIONS POUR GARDER UNE LONGUEUR D'AVANCE ?

1- L'évaluation des vulnérabilités

Sans stratégie cyber, les conséquences sont potentiellement graves pour les entreprises. Une attaque a des répercussions importantes sur l'activité d'une organisation. Les données volées ne sont parfois jamais restituées dans leur intégralité, causant une détérioration de l'image de l'entreprise.

"Dans 94 % des cas, les cyberattaques conduisent l'entreprise à devoir reconstruire totalement ou partiellement son système d'information" (Source : ANSSI)

L'étape de l'évaluation des vulnérabilités qui consiste à identifier et à analyser les faiblesses de votre infrastructure informatique est ainsi cruciale :

- Détecter les points faibles avant que les attaquants ne le fassent.
- Prioriser les correctifs et les améliorations de sécurité.
- Développer une stratégie de cybersécurité adaptée aux besoins spécifiques de votre entreprise.

Les politiques de sécurité établissent les règles et les procédures à suivre pour protéger les actifs informationnels de l'entreprise.

Nos 4 conseils pour renforcer la cybersécurité de votre entreprise :

- **Contrôle d'accès : Limitation de l'accès aux informations sensibles uniquement aux personnes autorisées.**
- **Gestion des mots de passe : Utilisation de mots de passe forts et mise en place de mécanismes de gestion de mots de passe.**
- **Surveillance et audit : Surveillance continue des systèmes pour détecter toute activité suspecte et audit régulier des politiques de sécurité.**
- **Plans de réponse aux incidents : Élaboration de plans détaillés pour répondre rapidement et efficacement aux incidents de sécurité.**

3 bonnes pratiques à appliquer en cybersécurité

- **Sensibilisez tous vos collaborateurs à la cybersécurité et aux bonnes pratiques.**

75 % des cyberattaques résultent d'erreurs humaines. Proposer des formations sur les risques cyber et numériques est un enjeu clé pour les PME et ETI, pour renforcer leur niveau de sécurité.

La sensibilisation des collaborateurs peut être abordée de plusieurs manières : en rendant obligatoire une formation sur les bases de la cybersécurité ou au travers de simulations de campagnes de phishing.

Ces mesures permettent d'accroître la vigilance des employés et de réduire les risques d'incidents cyber.

- **Investissez dans l'installation de systèmes technologiques de défense**

Les systèmes de défense comme les antivirus, antispam, etc. sont la première ligne de défense automatique en situation de cyberattaque.

- **Réalisez régulièrement une sauvegarde des données hors ligne**

Assurez-vous que les procédures de récupérations sont efficientes et qu'elles permettent une bonne reprise de l'activité de l'entreprise après une cyber attaque.

2- La mise en place de politiques de sécurité

Mettre en place une bonne stratégie cybersécurité à tous les niveaux de votre organisation est un levier indispensable à la pérennité de l'entreprise. Elle implique à la fois un enjeu de compétitivité, une garantie de croissance du groupe et un levier de confiance pour vos partenaires.

Stratégie cybersécurité : par quoi commencer ?

Pour vous protéger efficacement, votre stratégie cybersécurité doit reposer sur trois grands principes :

- La disponibilité en assurant en permanence l'accès aux services et données.
- L'intégrité en s'assurant que les données ne peuvent être ni modifiées, ni supprimées.
- La confidentialité en veillant à la traçabilité des accès aux données (collaborateurs, fournisseurs, etc) et à la protection des données sans fuite.

Pour une stratégie optimale, il est nécessaire d'avoir, au préalable, déterminé le contexte de la structure et le périmètre à protéger grâce à une feuille de route.

Dans 60 % des attaques*, celles-ci "impactent fortement le business de l'entreprise concernée, avec pour conséquence une perturbation significative de la production, pour 24 % des dirigeants interrogés. Dans 7 % des situations, on constate une baisse du CA (chiffres d'affaires).

*8e édition du baromètre annuel du CESIN

Pour lire l'article d'Innov8Learn et de Silicon sur les enjeux de la cybersécurité pour les TPE et PME en 2024, cliquez ici.

TOP 5 DES CYBERATTAQUES À PRÉVOIR POUR 2024

1. Les attaques relatives aux cloud services
2. Les attaques sur les objets connectés
3. Les violations et vols de données
4. Les piratages de comptes d'entreprises
5. Les rançongiciels (ransomwares)

Consultez notre catalogue de formations en CYBERSECURITE en toute simplicité !

Pour renforcer la stratégie Cybersécurité de votre structure, RENDEZ-VOUS ICI.

INNOV8LEARN
FORME AUX ENJEUX DE DEMAIN

LES CHIFFRES CLÉS DE LA CYBERSÉCURITÉ EN ENTREPRISE

2 milliards € |

coût des cyberattaques sur l'année 2022.

2 sur 3 |

nombre d'entreprises ne disposant pas de solution de protection sur ses applications web.

25 à 29 jours |

durée moyenne de reconstruction des SI pour les TPE et PME victimes d'une cyber-attaque;

La formation & la sensibilisation des collaborateurs

Dans un monde dans lequel les menaces cybernétiques sont en constante évolution, la formation et la sensibilisation des collaborateurs est l'un des piliers essentiels d'une stratégie de cybersécurité efficace pour les ETI, TPE et PME. Les technologies et les systèmes de sécurité, bien que cruciaux, ne suffisent pas à eux seuls pour protéger une entreprise contre les cyberattaques. Les collaborateurs, souvent considérés comme le maillon faible de la chaîne de sécurité, peuvent devenir la première ligne de défense lorsqu'ils sont bien formés et sensibilisés.

L'importance de la formation continue

La cybersécurité n'est pas une discipline statique, elle évolue rapidement en réponse aux nouvelles menaces et aux avancées technologiques. Par conséquent, il est impératif que la formation en cybersécurité soit un processus continu et non une simple initiative ponctuelle.

1. Mise à jour des connaissances : Les cyberattaques deviennent de plus en plus sophistiquées. Les collaborateurs doivent être régulièrement informés des nouvelles méthodes de **phishing**, de **ransomware** et autres menaces. Une formation continue permet de maintenir un niveau de vigilance élevé.

2. Pratiques sécuritaires : Une formation régulière inculque des pratiques sécuritaires quotidiennes, telles que l'utilisation de mots de passe forts, la reconnaissance des emails suspects et l'importance de maintenir les logiciels à jour. Ces pratiques doivent devenir des réflexes pour chaque employé.

3. Simulations et exercices : La théorie seule ne suffit pas. Des simulations d'attaques et des exercices pratiques aident les employés à réagir de manière appropriée en cas de véritable incident. Ces exercices peuvent inclure des simulations de phishing, des tests de réponse à des violations de données et des scénarios de récupération après sinistre.

FOCUS SUR LE PHISING

Selon la CNIL, le phishing, également connu sous le nom d'hameçonnage, est une escroquerie en ligne où l'attaquant se fait passer pour un organisme officiel (banque, CAF, Sécurité sociale, service des impôts, etc.). Ces messages, envoyés par SMS ou email, imitent si bien les communications légitimes qu'il est souvent difficile de distinguer le vrai du faux. Ils demandent généralement la mise à jour de vos informations personnelles (coordonnées bancaires,...). En milieu professionnel, les fraudeurs ne se contentent pas de détourner des fonds, ils visent aussi à voler des informations sensibles (attaque contre Sony Pictures Entertainment). D'après le rapport "Analyse du risque humain 2023" de Sosafe, le phishing est la deuxième méthode d'attaque la plus efficace en entreprise. Un utilisateur sur trois clique sur des emails de phishing malveillants, et parmi eux, un sur deux divulgue des données sensibles.

Intérêt de la sensibilisation : créer une culture de la sécurité

Au-delà de la formation technique, la sensibilisation à la cybersécurité vise à instaurer une culture de la sécurité au sein de l'organisation. Cette culture doit être soutenue par l'ensemble de l'entreprise, de la direction aux employés.

1. Engagement de la direction : En tant que dirigeant, vous êtes garant de la mise à niveau des connaissances et des bonnes conduites à adopter. En vous formant, vous montrer votre engagement sur les pratiques sécuritaires, et encouragez vos collaborateurs à se sensibiliser et à adhérer à cette culture de la sécurité.

2. Communication continue : Des campagnes de sensibilisation régulières, via des newsletters, des affichages dans les bureaux, et des réunions d'information, aident à garder la cybersécurité à l'esprit des employés. Ces communications doivent inclure des conseils pratiques, des mises à jour sur les nouvelles menaces et des rappels sur les politiques de sécurité de l'entreprise.

3. Reconnaissance et récompenses : Encourager et récompenser les comportements sécuritaires peut renforcer l'engagement des employés. Par exemple, reconnaître publiquement ceux qui signalent des incidents ou qui démontrent une vigilance particulière peut inciter les autres à adopter des comportements similaires.

Impact de la formation et de la sensibilisation sur la cybersécurité

La sensibilisation et la formation des collaborateurs de votre structure ont un impact global sur la croissance de votre entreprise. Selon les chiffres, **85% des violations de données sont causées par une erreur humaine, et en particulier l'entrée de logiciels malveillants dans les systèmes d'information.** Voici pourquoi il est essentiel d' investir dans la formation des salariés en cybersécurité.

Pourquoi former ses équipes à la cybersécurité ?

1. Réduction des risques : Une main-d'œuvre bien formée et sensibilisée est moins susceptible de commettre des erreurs qui pourraient conduire à une violation de la sécurité. Cela inclut éviter les clics sur des liens de phishing, utiliser des mots de passe forts et uniques, et signaler des activités suspectes.

2. Détection précoce des menaces : Les employés formés à reconnaître les signes d'une cyberattaque potentielle peuvent agir rapidement pour prévenir ou limiter les dommages. Une détection précoce est souvent cruciale pour minimiser l'impact d'une attaque.

3. Réponse efficace aux incidents : En cas de cyberincident, des employés formés et sensibilisés peuvent suivre les protocoles de sécurité établis, ce qui permet une réponse rapide et coordonnée. Une réponse efficace peut contenir l'incident, réduire les temps d'arrêt et limiter les pertes financières.

Innov8Learn, un partenaire de confiance

Innov8Learn propose une gamme de formations cyber courtes et opérationnelles, disponibles en format inter-entreprise pour une expérience collective enrichissante, ou en intra-entreprise pour une adaptation totale à vos besoins spécifiques.

Pour en savoir plus, rendez-vous sur : https://www.innov8learn.fr/

Pour les ETI, TPE et PME, la formation et la sensibilisation des collaborateurs en matière de cybersécurité ne sont pas simplement des options, mais des nécessités. En investissant dans une formation continue et en cultivant une culture de la sécurité, ces entreprises peuvent se doter d'une défense robuste contre les cybermenaces. Une main-d'œuvre informée et vigilante est l'un des atouts les plus puissants dans la lutte contre les cyberattaques. La cybersécurité devient alors une responsabilité partagée, où chaque employé joue un rôle crucial dans la protection de l'entreprise.

3- L’ACCOMPAGNEMENT CYBERSÉCURITÉ D’INNOV8LEARN

INNOV8LEARN EN QUELQUES MOTS

“Développer les compétences de vos équipes pour préparer la réussite de demain.”

Des formations adaptables à vos besoins sur 4 thématiques :

- IA (Intelligence Artificielle)
- Cybersécurité
- RSE (Responsabilité Sociétale & Environnementale des entreprises)
- Communication Digitale

2024
date de création

25
intervenants

4
thématiques de formations

48H
temps de maitrise de l’IA

Nous plaçons l’innovation, l’adaptabilité et la créativité au cœur de notre engagement à offrir une formation dynamique et évolutive, visant l’excellence. Ces valeurs fondamentales façonnent notre mission et notre engagement envers nos apprenants, partenaires et réseau.

Voici comment nous intégrons ces valeurs dans notre approche éducative :

- Perspective et évolution : Promouvoir une vision dynamique de la formation, favorisant une évolution continue et une adaptation aux changements.

- Innovation et créativité : Encourager des approches novatrices pour relever les défis de l’apprentissage et du développement professionnel.

- Développement de compétences : Se concentrer sur l’acquisition de compétences essentielles pour un épanouissement professionnel.

- Adaptation et flexibilité : Encourager l’adaptabilité face aux évolutions du marché du travail pour s’ajuster rapidement aux nouvelles tendances.

- Carrière et réalisation : Soutenir le développement du potentiel professionnel pour préparer à une carrière épanouissante.

Pour en savoir plus sur Innov8Learn, rendez-vous sur : innov8learn.fr

LES FORMATIONS EN CYBERSÉCURITÉ D'INNOV8LEARN

INNOV8LEARN du groupe EDUFORM'ACTION vous propose de découvrir son offre de formations pour vous aider à apporter une réponse aux enjeux de CYBERSÉCURITÉ :

Sensibilisation réglementaire (6-12 personnes, 2 jours)

Cette formation est ouverte aux **dirigeants d'ETI, de PME, TPE, startups et collectivités** pour une vue d'ensemble sur les normes clés de cybersécurité, les réglementations complémentaires tels que IA Act et l'implication de la RGPD.

Notions abordées :

- Les normes majeures de cyber
- Les différentes réglementations cyber (ISO 27001, NIS2, DORA)
- NIST Framework pour la **sécurisation des données** et les **réglementations complémentaires (AI Act, HIPAA, PCI-DSS)**

Découverte de la cybersécurité (6-12 personnes, 2 jours)

Destinée aux dirigeants, gestionnaires et employés des petites structures et collectivités ayant peu de connaissances préalables en cybersécurité, cette formation vise à sensibiliser sur les menaces, comprendre le fonctionnement, mais surtout à adopter des pratiques de sécurité de base et à réagir efficacement en cas d'incidents.

Notions abordées :

- Panorama des menaces et risques cybernétiques
- Sensibilisation aux attaques les plus répandues (phising, ...).
- Bonnes pratiques de sécurité de base pour les TPE/PME

Initiation à la Cybersécurité pour PME Prévention et réaction (6-12 personnes, 2 jours)

Cette formation, spécialement conçue pour les ETI et PME, vise à sensibiliser les participants aux risques cybernétiques. Les participants exploreront les différents vecteurs d'attaque, identifieront les vulnérabilités et comprendront les conséquences financières et opérationnelles des cyberattaques pour développer des stratégies défensives adaptées aux besoins de leur PME.

Notions abordées :

- Identification et évaluation des risques uniques pour les PME
- Les principes de sécurité avancés adaptés aux PME
- Les plans préventifs pour réagir efficacement aux menaces

Maitrise de la Cybersécurité : Évoluer avec assurance (6-12 personnes, 2 jours)

Cette formation intensive de 2 jours est spécialement conçue pour les **TPE, PME et collectivités**, afin de leur permettre de **relever les défis croissants posés par la cybercriminalité.**

Elle a pour objectif de renforcer vos connaissances existantes tout en vous dotant des outils nécessaires pour adapter et actualiser vos compétences..

Notions abordées :

- Renforcement des compétences face aux nouvelles menaces plus sophistiquées,
- Stratégies de défense adaptatives
- Simulation de situations de crise pour améliorer leur gestion.

Gouvernance en cybersécurité (6-12 personnes, 2 jours)

Cette formation de 2 jours, destinée aux directeurs et responsables de la sécurité des systèmes et à toute personne impliquée dans la gestion stratégique de la cybersécurité, couvre les **cadres législatifs et normatifs, la gestion des risques, la gestion de crise et la continuité d'activité, ainsi que la stratégie de sécurité et le leadership face à des menaces variées.**

Notions abordées :

- Acquisition approfondie des **vulnérabilités multiplateformes**
- **Utilisation avancée de l'intelligence artificielle** dans le contexte de la cybersécurité
- **Stratégies de cybersécurité holistiques** pour l'anticipation des menaces futures

Expertise technique avancée en cybersécurité (6-12 personnes, 2 jours)

Cette formation de 2 jours Expertise technique avancée en cybersécurité est spécifiquement conçue pour les professionnels techniques, Architecte SI, DSI et RSSI ayant un rôle technique actif, et techniciens souhaitant approfondir leurs compétences techniques en cybersécurité. Elle nécessite une solide expérience technique dans le domaine des services informatiques ou de la cybersécurité.

Notions abordées :

- Étude des scénarios cyberavancés, vulnérabilités zéro-day, attaques physiques/logiques
- Utilisation des outils spécialisés pour des attaques ciblées avancées
- Développer les compétences détection/réaction, réponse rapide, contre-mesures immédiates

4- LE GROUPE EDUFORM'ACTION : QUI SOMMES-NOUS ?

LE GROUPE EDUFORM'ACTION EN QUELQUES MOTS

+ 57 000
apprenants formés

300
produits de formation

DES FORMATIONS DE POINTE DANS 3 PÔLES D'EXPERTISE

11
sites partout en France

SANTÉ & SÉCURITÉ

DIGITAL & TECH

IMPACT & ÉNERGIE

+ 100
collaborateurs

Des locaux maillés sur le territoire et un déploiement des formations partout en France.

GROUPE EDU FORM' ACTION

A l'échelle nationale, contribuer à l'essor économique en favorisant l'employabilité des individus aujourd'hui et en formant les talents pour demain.

Eduform'Action, groupe entrepreneurial fondé en 2022, regroupe un réseau étendu d'écoles, d'organismes de formation professionnelle et de Centres de Formation d'Apprentis (CFA).

Eduform'Action forme les jeunes à des métiers d'avenir pour les accompagner vers leur premier emploi, développe les **compétences professionnelles**, facilite les reconversions pour les salariés et propose des parcours adaptés aux demandeurs d'emploi et aux personnes en situation de handicap. Eduform'Action est un partenaire de confiance pour les entreprises privées comme les organismes publics dans leurs plans de développement des compétences en proposant un panel complet de parcours de formation.

Nos formations couvrent trois thématiques majeures : **Digital et Tech**, **Impact et Énergie**, **Santé et Sécurité au Travail**. Chacune est portée par des entités spécialisées offrant une expertise reconnue. L'excellence pédagogique est au cœur des priorités du groupe, favorisant l'apprentissage par la pratique avec des ateliers techniques, des outils de simulation et l'utilisation d'outils de réalité virtuelle. Toutes nos entités sont certifiées **Qualiopi,** ce qui leur permet de travailler avec des acteurs institutionnels comme privés.

Avec une présence nationale assurée par ses **11 sites stratégiquement répartis**, le groupe Eduform'Action assure une accessibilité optimale à ses services, garantissant ainsi une réponse rapide et efficace aux besoins de ses clients. En 2023, le groupe a accompagné et formé 57 000 apprenants sur l'ensemble du territoire.

Plus récemment, l'avènement et la démocratisation de l'IA générative, notamment avec l'apparition de ChatGPT, nous a amené à concevoir des formations en IA pour exploiter pleinement les opportunités, risques et questions soulevées par cette nouvelle révolution digitale.

NOUS CONTACTEZ

INNOV8LEARN

innov8learn.fr

Innov8Learn

contact@innov8learn.fr

06 86 66 76 44

EDUFORM'ACTION

eduformaction.fr

Eduform'Action

hello@eduformaction.fr