

## RENFORCER LA SECURITE NUMERIQUE ET PROTEGER LES DONNEES DE L'ENTREPRISE

<b>Durée</b>	7 heures, soit 1 jour	<b>Tarif</b>	INTER : 360 € HT /pers INTRA : 1600 € HT /groupe
<b>Public visé</b>	Toute personne amenée à améliorer ses connaissances en cybersécurité	<b>Pré-requis</b>	Maîtrise de la langue française Connaissances de base en informatique
<b>Lieu Modalité</b>	<input type="checkbox"/> ASFOREST entreprise <input type="checkbox"/> présentiel	<b>Dates</b>	Voir catalogue

### OBJECTIFS PEDAGOGIQUES

A l'issue de la formation, vous serez apte à comprendre les impacts potentiels des cyberattaques sur les opérations et la réputation de l'entreprise, identifier les données sensibles et critiques et les différents types de menaces, surveiller les systèmes pour détecter des activités suspectes et rédiger une charte informatique claire et compréhensible.

Vous serez capable d'évaluer les risques liés à la cybersécurité pour l'entreprise, de suivre les procédures de réponse en cas d'incident, d'appliquer et faire appliquer les bonnes pratiques de sécurité au quotidien telles que définies dans la charte.

### CONTENU DU PROGRAMME

**Test de positionnement** : évaluation des connaissances et compétences en amont de la formation.

#### 1- Introduction et bonnes pratiques de cybersécurité (3h30 – 2 séquences)

- Identifier les différents types de menaces en cybercriminalité et les signes d'une attaque en cours
- Maîtriser les risques et les enjeux de sécurité pour évaluer les impacts et réagir face aux menaces
- S'accoutumer aux bonnes pratiques pour prévenir les menaces

#### 2- Détection et réaction face aux menaces et mise en œuvre de la charte informatique (3h30 – 2 séquences)

- Détecter les intrusions et réagir face aux malveillances
- Maîtriser les actions à mettre en œuvre pour protéger les données importantes
- Rédiger une charte informatique pour promouvoir une culture de sécurité

**Evaluation finale** : évaluation de l'acquisition de l'ensemble des connaissances et compétences du parcours.

### SEQUENÇAGE

- **Séquence 1 (1h30) Menaces** [présentiel ou distanciel] : Cette séquence débute sur une immersion dans le programme avec le formateur qui revient sur le test de positionnement et expose les enjeux notamment sur les réactions à adopter face aux menaces et les mesures de protection efficaces à mettre en place au regard des risques non seulement opérationnel mais également sur la réputation de l'entreprise. Les stagiaires sont amenés à définir le contexte de leur entreprise et leur expérience afin d'apporter collectivement des éléments d'information sur les pratiques actuelles de leur établissement en matière de cybersécurité et de sensibilisation auprès des équipes. Le formateur synthétise les différents types de menaces (phishing, malware, ransomware, etc.) et rappelle les risques et les enjeux de sécurité non seulement pour l'opérationnel mais également pour la réputation de l'entreprise, et l'importance d'évaluer les impacts pour mieux pouvoir y réagir. Il évalue l'acquisition des compétences grâce à un questionnaire direct.

- **Séquence 2 (2h) Bonnes pratiques** [présentiel ou distanciel] : Cette séquence s'organise autour de cas pratiques réalisés individuellement ou en sous-groupes, permettant de mettre en exergue les bonnes pratiques favorisant la prévention des menaces et leur application au quotidien pour soi et l'ensemble des collaborateurs. Le formateur répond aux questions et alimente les réflexions en cours des participants, notamment sur la création et la gestion de mots de passe sécurisés, la mise à jour régulière des logiciels, l'utilisation de VPN... Les corrigés permettent aux stagiaires d'évaluer leurs productions.
- **Séquence 3 (1h30) Protection** [présentiel ou distanciel] : Cette séquence s'ouvre sur la reprise des éléments des séquences précédentes, éléments retenus, questions/réponses. Elle s'organise autour d'études de cas réalisés individuellement ou en sous-groupes, permettant aux participants d'identifier les moyens de détecter les intrusions, de réagir face aux menaces et de mettre en œuvre des actions de protection... Le formateur réalise un focus sur l'importance de la surveillance des systèmes pour prévenir, des procédures de réponse en cas d'incident, et des mesures de protection (antivirus, gestion des accès, sauvegarde régulière...). Les corrigés permettent aux stagiaires d'évaluer leurs productions.
- **Séquence 4 (2h) Charte informatique** [présentiel ou distanciel] : Dans cette séquence, le formateur propose un modèle de charte informatique permettant aux stagiaires individuellement ou en sous-groupes de rédiger la charte informatique de leur entreprise, qui servira de base pour promouvoir une culture de sécurité auprès des équipes. L'accent est notamment porté sur la communication et les moyens de développer cette culture de la cybersécurité : sensibilisation, formation, engagement, automatisation des procédures... Des outils pratiques sont transmis (modèle de charte, listes de bonnes pratiques...). Une évaluation finale permet d'évaluer les éléments de la séquence et l'acquisition des compétences du parcours.

En présentiel ou distanciel, des temps de pause réguliers sont aménagés entre les séquences et en fonction des activités pédagogiques. Ces temps de récupération favorisent l'assimilation des connaissances, le maintien de la concentration, la convivialité entre participants et la qualité globale des apprentissages.

## METHODES MOBILISEES

- **Méthodes pédagogiques variées** : alternance d'approches expositive, interrogative et active favorisant l'engagement, la créativité et la mémorisation. Les participants expérimentent des modalités adaptées à différents styles d'apprentissage : apports théoriques, travaux de groupe, études de cas, jeux de rôle, ateliers pratiques, discussions dirigées, apprentissage par projet, démonstrations, brainstorming, feedback et évaluations formatives. En distanciel, chaque séquence intègre au moins une activité pédagogique interactive (quiz, étude de cas, mise en situation, forum collaboratif) d'une durée moyenne d'environ 15 minutes, afin de garantir l'implication active des participants et la consolidation des acquis à distance.
- **Supports et ressources pédagogiques** : mise à disposition de ressources diversifiées pour créer un environnement d'apprentissage riche et stimulant : présentations, tableaux blancs, affiches, graphiques, fiches de travail, études de cas, supports imprimés et numériques, vidéos, quiz interactifs, sondages, applications web, plateformes d'apprentissage et équipements techniques adaptés (ordinateur, vidéoprojecteur, logiciels dédiés).
- **Accompagnement et assistance pédagogiques** : animation de l'ensemble des séquences par un formateur référent garantissant le suivi du groupe et l'adaptation aux besoins individuels. L'accompagnement comprend l'accueil et la mise en confiance, l'encadrement des activités, la gestion des dynamiques de groupe, les feedbacks réguliers et le suivi post-formation favorisant la transposition des acquis en situation de travail.

## MODALITES TECHNIQUES ET D'ACCES

- **Modalités d'accès et d'accompagnement** : Les participants peuvent s'inscrire auprès de nos équipes dans la limite des places disponibles, jusqu'à la veille de la session. L'employeur veille à respecter les éventuels délais imposés par un financeur tiers.  
L'assistance technique et administrative est assurée par nos équipes avant, pendant et après la formation : conventions, convocations, règlement intérieur, accueil, suivi administratif et financier, délivrance des attestations, traitement des réclamations... Nos équipes sont joignables du lundi au vendredi de 9h à 18h au 01 42 96 09 27 ou par mail [asforest@asforest.com](mailto:asforest@asforest.com). En cas d'indisponibilité, une réponse est apportée sous 48h ouvrés.
- **Lieux et moyens techniques mis à disposition** : Les espaces de formation ASFOREST, équipés d'écrans, tableaux, ordinateurs, accès Internet et outils numériques, offrent des conditions optimales d'apprentissage et d'échanges.
  - Nos locaux sont accessibles aux personnes à mobilité réduite. Dans le cadre de notre politique d'accessibilité, nous invitons tout participant à nous informer en amont de toute situation de handicap ou besoin d'adaptation afin de prévoir les aménagements nécessaires, en lien avec notre référent handicap.

- En cas de formation organisée hors du centre (en entreprise), ASFOREST s'assure en amont que les conditions matérielles et techniques sont adaptées au bon déroulement de la session. Cette vérification est réalisée en lien avec le lieu d'accueil, qui met à disposition les moyens nécessaires à la réalisation des activités prévues.
- **En distanciel, conditions techniques requises** : Chaque participant doit disposer d'un ordinateur connecté à Internet (connexion stable pour le visionnage de vidéos et l'accès à une plateforme en ligne), d'un micro et d'une caméra fonctionnels pour participer aux classes virtuelles, d'une adresse mail active, et d'une aisance suffisante dans l'utilisation des outils numériques de base (navigation web, visioconférence, téléchargement de documents).

## MODALITES D'EVALUATION ET SUIVI DE L'ACTION

**Evaluations pédagogiques** : Partie intégrante du parcours de formation, leurs coûts sont inclus dans le tarif global.

- **Positionnement** : évaluation initiale pour identifier le niveau de maîtrise du stagiaire, ses besoins et ses attentes afin d'adapter le parcours et, le cas échéant, de proposer un accompagnement individualisé.
- **Continue** : évaluations formatives pour vérifier la compréhension, l'assimilation et la mise en œuvre progressive des compétences. Ces temps d'échanges et de feedback favorisent l'ancrage des apprentissages.
- **Finale** : évaluation sommative pour mesurer l'atteinte des objectifs pédagogiques et valider les compétences acquises. Elle peut également servir à définir, le cas échéant, un plan de consolidation post-formation.

**Suivi post-formation** :

- À l'issue du parcours, chaque stagiaire reçoit une attestation de fin de formation précisant la durée, les objectifs visés et leur niveau d'atteinte évalué en fin de formation. Un certificat de réalisation est transmis au financeur et à l'employeur, en justification de la réalisation effective de l'action. Un relevé de présence peut être remis sur demande, à titre d'information complémentaire sur l'assiduité des participants.
- Une enquête de satisfaction est réalisée auprès des participants (à chaud à la fin de la formation, puis à froid trois mois après) ainsi qu'auprès des employeurs. Ces retours permettent d'évaluer la satisfaction, la transférabilité des acquis en situation de travail et la contribution de la formation à la montée en compétences.

*mise à jour : 04/07/2026*

