

**INTITULE : FORMATION CYBERSÉCURITÉ - HYGIÈNE INFORMATIQUE QUOTIDIENNE**Astrée Solution est un organisme de formation **DATADOCK** ID : 0060332Astrée Solution est **labelisé ExpertCyber** par le GIP ACYMAAstrée Solution est partenaire **référéncé sur le dispositif national** : [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)**Public concerné** : Dirigeant·e, responsables & managers, salarié·e, création d'entreprise**Prérequis** : Aucun**Durée** : 7 heures sur 1 journée**Type de formation et lieu** : Formation en présentiel dans les locaux du client ou en visio**Formateurs** : Jean-François & Emmanuelle Bobo**Tarifs** : 400 € net de taxes**Mode de formation** : inter ou intra entreprise**Modalités d'accès** : La formation est accessible sous condition d'un accord de financement par un financeur ou du paiement en tout ou partie par ses propres moyens.**Délais d'accès** : Notre accompagnement est personnalisé, ainsi nous nous adapterons à vos contraintes, un délai de 15 jours minimum est nécessaire à l'établissement des documents administratifs, 1 mois en cas de financement par un OPCO.**Réfèrent handicap - Réfèrent égalité professionnelle - Réfèrent suivi en entreprise** : Emmanuelle Bobo.**Notre objectif** : rendre nos formations accessibles à tous ! Formation accessible aux personnes en situation de handicap avec adaptation sur mesure des moyens de la prestation.**OBJECTIFS**

Connaître le contexte cyber actuel mondial dans lequel évoluent les sociétés françaises.

Savoir reconnaître les menaces.

Connaître les techniques simples se prémunir de la cyberdélinquance.

Obtenir un savoir-faire et un savoir-être numérique pour éviter la contamination.

**INTRODUCTION - CONTEXTE**

Renforcer les connaissances et les compétences des professionnels en matière de cybersécurité pour mieux appréhender et protéger leurs sociétés face aux nouveaux risques liés à la cybercriminalité.

Le but de cette formation est aussi de les amener à mieux appréhender une crise cyber si cela leur arrive et ayant acquis notamment des actes réflexes permettant de protéger leur société d'une menace cyber mais tout en préservant les preuves numériques afin de permettre un éventuel dépôt de plainte ultérieur.

**MODALITE D'ENCADREMENT – METHODE PEDAGOGIQUE – SUIVI**

- Formation associant aspects théoriques et exemples concrets, cas pratiques avec mise en situation, échanges d'expériences (liste exhaustive des méthodes pédagogiques utilisées dans document « séquences et méthodes de dialogue pédagogique »)
- Remise d'un support technique
- Session personnalisée en fonction des participants afin d'apporter des cas concrets percutants
- Formation encadrée par directeur pédagogique et technique.
- Pour formation à distance, participants aidés techniquement par encadrant technique par tous moyens : mails, téléphone, prise en main à distance du terminal avec accord préalable du participant. Plateforme sécurisée de visio propriété d'Astrée Solution.
- Suivi des stagiaires après la formation

**MODALITES D'EVALUATION - NATURE DES TRAVAUX DEMANDES - TEMPS IMPARTI - SANCTION**

4 évaluations intermédiaires de type QCM de 10mn après séquence + 1 évaluation finale de 20mn sanctionnant l'action de formation.

Documents délivrés en fin de formation : Un certificat de réalisation - une attestation individuelle de formation - une attestation des compétences d'acquis de fin de formation à insérer dans votre portefeuille de compétences.

**PROGRAMME**

- ✚ Savoir quels sont les risques cyber aujourd'hui – Panorama de la menace cyber pour les sociétés françaises
- ✚ Connaître les techniques d'attaque, les motivations de la cyberdélinquance, leurs méthodes
- ✚ Avoir des notions sur la judiciairisation - préservation des preuves numériques
- ✚ Prendre conscience du type de données détenues dans son service
- ✚ Connaître les recommandations à appliquer en tout temps : choisir et stocker ses mots de passe, mises à jour, sauvegardes...
- ✚ Se prémunir des actes malveillants pouvant intervenir via une messagerie internet ou intranet.
- ✚ Savoir identifier un acte malveillant et savoir faire remonter l'information par le bon canal
- ✚ Connaître les premiers gestes à avoir en cas de suspicion d'acte malveillant sur son environnement de travail
- ✚ Visualiser les risques lors de déplacements professionnels
- ✚ Maîtriser les informations publiées sur les réseaux sociaux
- ✚ Ne pas mélanger usage personnel & usage professionnel et connaître les dangers du nomadisme (BYOD)
- ✚ Identifier les risques liés aux Faux Ordres de Virement (FOVI)
- ✚ Connaître les nouvelles obligations juridiques (RGPD)
- ✚ Questions libres sur les risques liés au numérique et retours d'expériences

**Contact unique pour tous renseignements : Astrée Solution 07.70.41.04.31 ou [contact@astree-solution.com](mailto:contact@astree-solution.com)****Personne chargée des relations pédagogiques et techniques avec les stagiaires et les financeurs : Emmanuelle Bobo**Déclaration d'activité prestataire de formation : *Enregistré sous le numéro 76660214066 cet enregistrement ne vaut pas agrément de l'Etat - art. R6351-6 du code du travail. Astrée Solution est exonéré de TVA dans le cadre des formations professionnelles continues. N° DATADOCK : 0060332*