Alliance Cyber Technologies
229 rue de Solferino
59000 Lille
Email : d.corgiat@alliancecybertech.com
Tel : +33134908677

Parcours introductif à la cybersécurité - Collectivités territoriales

Formation réalisée en présentiel et en distanciel.

A l'issue de cette formation, vous serez capable de :
- identifier les grands enjeux de la cybersécurité
- détenir une vision globale de la cybersécurité et son environnement
- connaître les différents référentiels, normes et outils de la cybersécurité
- connaître les obligations juridiques liées à la cybersécurité
- comprendre les principaux risques et menaces ainsi que les mesures de protection
- identifir les bonnes pratiques en matière de sécurité informatique
- préparer la mise en œuvre des mesures prioritaires en cas de crise

Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par Alliance Cyber Technologies.

Le formateur alterne entre méthode démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Cette formation bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Modalités d'évaluation des acquis :
— en cours de formation, par des études de cas ou des travaux pratiques
— et, en fin de formation, par une certification éditeur, et/ou un questionnaire d'auto-évaluation

Modalités d'inscription :
– par email : contact@alliancecybertech.com ;
– par téléphone : 01 34 90 86 77
– depuis le catalogue en ligne : https://alliancecybertech.catalogueformpro.com/

Durée: 35.00 heures (5.00 jours)

Profils des apprenants

Alliance Cyber Technologies
229 rue de Solferino
59000 Lille
Email : d.corgiat@alliancecybertech.com
Tel : +33134908677

- Étudiants en sécurité informatique
- Administrateurs système
- Développeurs
- Chefs de projets

Prérequis

- Il n'y a pas de conditions préalables pour participer à cette formation.
- En cas de formation intra sur site externe à Alliance Cyber Technologies, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

Accessibilité et délais d'accès

Alliance Cyber Technologies met tout en oeuvre pour rendre accessible ses formations aux personnes en situation de handicap. Contactez notre référent handicap à contact@alliancecybertech.com pour nous faire part de vos besoins.
48 heures

Qualité et indicateurs de résultats

Objectifs pédagogiques

- Identifier les grands enjeux de la cybersécurité
- Détenir une vision globale de la cybersécurité et son environnement
- Connaître les différents référentiels, normes et outils de la cybersécurité
- Connaître les obligations juridiques liées à la cybersécurité
- Comprendre les principaux risques et menaces ainsi que les mesures de protection
- Identifir les bonnes pratiques en matière de sécurité informatique
- Préparer la mise en œuvre des mesures prioritaires en cas de crise

Contenu de la formation

- Jour 1
    - Les menaces et les risques : - Qu'est-ce la sécurité informatique ? - Comment une négligence peut-elle créer une catastrophe ? - Les responsabilités de chacun. - L'architecture d'un SI et leurs vulnérabilités potentielles. - Les réseaux d'entreprise (locaux, distantes, Internet). - Les réseaux sans Ljl et mobilité. - Les applications à risques : Web, messagerie... - La base de données et système de Ljchiers. Menaces et risques. - Accompagnement sécurité dans les projets
    - Sécurité informatique et réseaux : - Réseaux d'entreprise (locaux, site à site, accès par Internet). - Réseaux sans Ljl et mobilité. Les applications à risques : Web, messagerie... - Base de données et système de Ljchiers. Menaces et risques. - Typologie des risques. La cybercriminalité en France. Vocabulaire (sniffing, spooffing, smurfing, hijacking, ..)
    - Focus sur la cybermenace : - Quelles sont les principales menaces cyber auxquelles les collectivités sont exposées ?Quels sont principaux chemins d'aljaques ? - Quelles mesures de sécurité meljre en œuvre dans votre collectivité territoriale ? - Matrice MITRE Attack
- Jour 2
    - La sécurité du poste de travail : - La confidentialité, la disponibilité et l'intégrité. Les avantages liés au chiffrement. - Gestion des données sensibles & personnelles. La problématique des ordinateurs portables et téléphones. - Les différentes menaces sur le poste client ? Comprendre ce qu'est un code malveillant. Comment gérer les failles de sécurité ? - Les ports USB. Le rôle du firewall client.
    - Le cadre juridique et les bons réflexes à avoir : - Quelles sont les contraintes réglementaires et juridiques. - Pourquoi on doit respecter ces exigences de sécurité ? - Le RGS (Référentiel Général de Sécurité) - Agir pour une meilleure sécurité : les aspects sociaux et juridiques. - La CNIL (Commission Nationale de l'Informatique et des Libertés) et la législation. - La cybersurveillance et la protection de la vie privée. - La charte d'utilisation des ressources informatiques. - La sécurité au quotidien et les bons réflexes à avoir.

Alliance Cyber Technologies
229 rue de Solferino
59000 Lille
Email : d.corgiat@alliancecybertech.com
Tel : +33134908677

- L’analyse des risques informatiques : - Qu’est-ce qu’une analyse des risques, des vulnérabilités et des menaces ? - Comment mettre en place une démarche d'identification et de classification des risques.Risques opérationnels, physiques, logiques. - Comment constituer sa propre base de connaissances des menaces et vulnérabilités ?Méthodes et référentiels : EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)/FEROS, MEHARI. - La démarche d’analyse de risques dans le cadre de l’ISO 27001, l’approche PDCA (Plan, Do, Check, Act). - De l’appréciation des risques au plan de traitement des risques : les bonnes pratiques

- Jour 3
  - Découvrir les normes, référentiels… utiles aux collectivités : - ISO 27001 : la norme de référence en matière de cybersécurité - Focus sur les normes complémentaires : ISO 27005, 27018, 20 000, RGPD - Le Référentiel Général de Sécurité (RGS)
  - Le processus d’un audit de sécurité : - Processus continu et complet. - Les catégories d’audits, de l’audit organisationnel au test d’intrusion. Audits RGS. - Comment créer son programme d’audit interne ? Comment qualiLjer ses auditeurs ?Apports comparés, démarche récursive, les implications humaines. - Sensibilisation à la sécurité : qui ? Quoi ? Comment ? - La charte de sécurité, son existence légale, son contenu, sa validation.
  - Les bonnes pratiques : - Protection des données à caractère personnel & sanctions prévues en cas de non-respect. - L’usage de la biométrie en France. - La cybersurveillance des salariés : limites et contraintes légales. - Le droit des salariés et les sanctions encourues par l’employeur. - Le choix d’un prestataire dans le cadre d’une collectivité locale - L'authentiLjcation de l'utilisateur et les accès depuis l'extérieur - Contrôles d'accès : authentiLjcation et autorisation. - Pourquoi l'authentiLjcation est-elle primordiale ? - Le mot de passe traditionnel. - Authentification par certiLjcats et token - Accès distant via Internet : comprendre les VPN. - De l'intérêt de l'authentiLjcation renforcée.
- Jour 4
  - Comment s'impliquer dans la sécurité du SI ? - Agir pour une meilleure sécurité : les aspects sociaux et juridiques. La CNIL, la législation. - Pourquoi mon organisme doit respecter ces exigences de sécurité ? - La cybersurveillance et la protection de la vie privée. - La charte d'utilisation des ressources informatiques - La Politique de sécurité du système d'information de l’Etat (PSSIE)
  - Gestion de crise et des incidents : - Cybercriminalité moderne : Types de criminalité - Cadre de gestion d'un incident de sécurité - Typologie des crises informatiques. - La capacité à réagir : Premières erreurs à éviter pour la DSI. - Se préparer au danger. Réduire la gravité de l'événement quand et s'il se produit. - Potentiels de crises et scénarios.
- Jour 5
  - Les audits de sécurité : - Le métier de l'auditeur sécurité. - Identifier le contexte de la mission. - La préparation de la mission, l'analyse du référentiel. - La classification des écarts, déterminer les critères de risques retenus. - Revue documentaire & préparation des interviews. - L'audit sur site : ce qu'il faut faire (et ne pas faire).
  - Les indicateurs et instruments de mesures : - La présentation des indicateurs et tableaux de bord, exemples de formats. - Une typologie d'indicateurs. A quoi sert mon indicateur ? - Le nombre et le choix des indicateurs en fonction du domaine d'application choisi. - L'inscription dans une démarche SMSI. - Les exemples de la norme sur des contrôles 27001 et mesures Annexe A.
  - Les tableaux de bord et le pilotage de la sécurité : - Le suivi de la PSSIE dans un cadre PDCA. - Les tableaux de bord : pour qui, pour quoi ? - Suivi des actions et de la conformité PSSIE - Suivi des niveaux de risques acceptables pour les directions opérationnelles.
  - Conclusion

Organisation de la formation

Équipe pédagogique

Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par Alliance Cyber Technologies.

Ressources pédagogiques et techniques

- Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont : — Ordinateurs Mac ou PC, connexion internet, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel) — Environnements de formation installés sur les postes de travail ou en ligne — Supports de cours et exercices En cas de formation intra sur site externe à Alliance Cyber Technologies, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation

- Fiches d'évaluations et / ou quizz

Prix : 3500.00 €

Alliance Cyber Technologies
229 rue de Solferino
59000 Lille
Email : d.corgiat@alliancecybertech.com
Tel : +33134908677