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

Formation intensive : se défendre seul !

Formation réalisée en présentiel et en distanciel.

Lors de cette formation, nous vous expliquerons les enjeux de la cyber sécurité, mais aussi comment détecter, surveiller un système d'information avec des technologies et des processus de cyber sécurité.

A l'issue de cette formation, vous serez capable de :
- maîtriser ses activités pour limiter ou annuler une cyber attaque.
- comprendre les différences entre des incidents et des événements de sécurité.
- analyser des vrais et faux négatifs avec un outil de SIEM.
- détecter des cyber attaques et comment les arrêter.
- utiliser un outil de détection (SPLUNK, QRADAR ou ZIWIT)
- création d'un tableau de bord et amélioration continue

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).

Travaux pratiques
- cyber vigilance : Analyse d'un évènement et d'un incident de sécurité.
- identifier les faux négatifs et comment faire baisser leur volumétrie.

Délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel à distance).

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

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

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: 21.00 heures (3.00 jours)

Profils des apprenants

- Technicien et administrateur
- Ingénieur réseau
- Responsable informatique
- Architecte

Prérequis

- Bonne connaissance informatique
- Bonne connaissance en système et réseau
- 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

- Maîtriser ses activités pour limiter ou annuler une cyber attaque.
- Comprendre les différences entre des incidents et des événements de sécurité.
- Analyser des vrais et faux négatifs avec un outil de SIEM.
- Détecter des cyber attaques et comment les arrêter.
- Utiliser un outil de détection (SPLUNK, QRADAR ou ZIWIT)
- Création d'un tableau de bord et amélioration continue

Contenu de la formation

- Jour 1
    - Initiation à la cyber sécurité et à la cyber défense
    - Comprendre la gestion des risques et la mise en place de mesures de sécurité
    - Identifier les incidents et les évènements de sécurité et la surveillance des flux(s).
    - Comprendre les différences entre un incident et un événement de sécurité.
    - Comprendre les activités d'une analyse d'un incident et d'un évènement.
- Jour 2
    - Installation & configuration d'un SIEM + exercices pratiques.

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

- Méthodologie de remédiation et rôle des règles de sécurité.
- Gestion de la crise et résilience.
- Le PRA et le PCA

- Jour 3
  - Identifier les principales problématiques à travers des cas d'usage.
  - Apprendre à détecter des faux négatifs et comment faire baisser leur volumétrie.
  - Comprendre les engagements (les S.L.A)
  - Optimiser la sécurité d'un système d'information.

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 : 2900.00 €