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

Mise en place d'un SOC

Formation réalisée en présentiel et en distanciel.

Lors de cette formation, nous vous expliquerons comment détecter des événements et des incidents de sécurité, et plus globalement, comment 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 les activités dans un SOC
- comprendre les différences entre des incidents et des événements de sécurité
- analyser des vrais et faux négatifs
- détecter des cyber attaques et comment les arrêter.
- utiliser un outil de détection (SPLUNK ou QRADAR)
- 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
- analyse d'un évènement et d'un incident avec SPLUNK ou QRADAR
- 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

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

— 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: 21.00 heures (3.00 jours)

Profils des apprenants

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

Prérequis

- Bonne connaissance informatique
- Bonne connaissance en cyber sécurité
- Bonne connaissance en système et réseau
- Certification ANSSI
- 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 les activités dans un SOC
- Comprendre les différences entre des incidents et des événements de sécurité
- Analyser des vrais et faux négatifs
- Détecter des cyber attaques et comment les arrêter.
- Utiliser un outil de détection (SPLUNK ou QRADAR)
- Création d'un tableau de bord et amélioration continue

Contenu de la formation

- Jour 1
    - Connaître l'organisation d'un SOC
    - Comprendre les différences entre un incident et un événement de sécurité
    - Comprendre les activités d'une analyse d'un incident et d'un évènement

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

- Jour 2
    - Identifier les outils utilisés par les analystes SOC (SPLUNK et QRADAR)
    - Identifier les principales problématiques à travers des cas d'usage
    - Apprendre à détecter des faux négatifs et comment faire baisser leur volumétrie
- Jour 3
    - 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 €