Domaine : Informatique - **Thématique(s) :** Cloud, réseaux et sécurité

STAGES COURTS

CYBERSÉCURITÉ : ANALYSTE CYBERSÉCURITÉ

Les tâches d'un analyste de cybersécurité sont multiples et très techniques. La complexité des composants des SI ne permet plus à un administrateur systèmes et réseaux de surmonter les problèmes provoqués par les alertes de ces composants. La sécurité des opérations, des transactions et des données critiques demande des compétences spécifiques. La formation donnera à ces professionnels la possibilité d'analyser les vulnérabilités, de détecter les incidents et de garantir la sécurité des infrastructures des SI en utilisant les méthodes et les outils dédiés aux analystes.

Durée de la formation : 35 heures
Dates : Voir le calendrier
Lieu : Campus Pierre et Marie Curie – Paris (Jussieu)
Tarif : 3300 €

Modalité : Présentiel

OBJECTIFS ET COMPÉTENCES VISÉES

- Maitriser la surveillance de sécurité des SI
- Détecter et analyser d'incidents de sécurité
- Mettre en œuvre les principes de sécurisation SSI
- Participer à l'intégration d'infrastructures SIEM
- Participer à la restauration de la sécurité du SI après attaque
- Maîtriser les dictionnaires de vulnérabilité des applications
- Maîtriser la détection d'intrusion et savoir lire une alerte
- Effectuer une veille technologique sur les nouvelles vulnérabilités, menaces desécurité et techniques de sécurisation.
- Anticiper les menaces
- Être force de proposition sur l'amélioration la sécurisation des SI

PUBLIC VISÉ ET PRÉ-REQUIS

Public :
Formation destinée à des informaticiens ayant une expérience professionnelle d'au moins 5 ans dans les domaines des systèmes d'exploitation et des réseaux ainsi qu'en systèmes d'information (SI). Les compétences en administration des systèmes et réseaux sont nécessaires.

Pré-requis :
Avoir des compétences techniques sur l'ensemble de l'infrastructure d'un SI
Avoir des connaissances de bases en solutions de sécurité

PROGRAMME

- Outils de sécurité
- Méthodes et outils de tests d'intrusion d'un réseau ou d'applications Web
- Outils de forensics
- Outils de surveillance des réseaux
- Méthodologie des tâches de l'analyste
- Attaques classiques sur les couches basses et la couche applicative
- Les SIM, SIEM, SEM

INFORMATIONS

Catégorie de l'action de développement des compétences:
(Article L6313-1 du Code du Travail)
Action de formation
Effectifs : Min 4 pers. / Max 15 pers.
Possibilité de sessions sur-mesure

CONTACT

ingenierie-fc@sorbonne-universite.fr

- Détection, analyse et corrélation des différentes alertes
- Qualification des évènements, levée de doute, élimination des faux positifs
- Les attaques DoS, DDoS
- Les attaques sur TCP/IP et leurs solutions.
- Sécuriser une infrastructure de réseau et de télécommunication
- Système de gestion des identités, des accès, des vulnérabilités et des anomalies comportementales des utilisateurs
- Les investigations et la documentation liées aux incidents de sécurité
- Élaboration des reporting et des fiches d'incident.
- Sécurité périmétrique (Filtrage et proxifiation , Architectures, VPN
- Sécurité des réseaux internes (Antivirus, sécurité VLAN, 802.1X, Systèmes de quarantaine, Wifi)
- Authentification et chiffrement des données

MÉTHODES

- Cours théoriques suivis des séances pratiques pour une assimilation parfaite des concepts abordés.
- Méthodes pédagogiques adaptables suivant le niveau et les expériences professionnelles du groupe.
- Equipe pédagogique composée des enseignant–chercheurs et des spécialistes professionnels.
- Supports pédagogiques sous plusieurs formes (papier, électronique, internet
- Évaluation des connaissances acquises.

Documents : Supports de cours PDF

MODALITÉS D'ÉVALUATION

Attestation de fin de formation

ET APRÈS

Cette formation permet aux individus de sécuriser leur parcours professionnel en leur donnant les compétences nécessaires pour accompagner les entreprises dans les enjeux liés à leur secteur d'activité et s'adapter aux évolutions technologiques associées.

LES + DE LA FORMATION

- Une salle cours équipée d'un video-projecteur, d'un tableau numérique, du WiFi et une salle machine de 24 postes de travail avec OS virtualisés sont dédiées à la formation.
- Une plateforme dédiée et un simulateur de cas pratique pour illustrer des attaques internes et externes