Programme de formation

Introduction à la cybersécurité : architecture, techniques et meilleures pratiques pour protéger le SI

Objectifs

Pierre angulaire de toute organisation, le Système d'Information doit faire l'objet d'une surveillance constante, tant du point de vue matériel que logiciel. Lors de cette formation d'initiation aux grands principes qui fondent la cybersécurité, les stagiaires apprendront à mettre en œuvre les meilleures techniques pour se prémunir des intrusions et répondre aux menaces qui pèsent sur le SI. A l'issue des 3 jours de formation, ils connaîtront les différents facteurs et typologies de risques pouvant porter atteinte à la performance d'une organisation. Les acquis théoriques seront mis en application au travers de nombreux cas pratiques sur une entreprise fictive.

Pré requis

Des connaissances générales en informatique

Durée

3 jours

Public

Administrateurs, architectes, développeurs, DSI, responsables sécurité

Plan de formation

Introduction : les principes et concepts fondamentaux de la sécurité informatique
Présentation générale et objectifs de cette formation
Vue d'ensemble de la sécurité du Système d'Information
Définitions et concepts fondamentaux : confidentialité, intégrité, disponibilité…
Les composants de la cybersécurité : que faut-il protéger ?
Défense en profondeur et politique de sécurité
Principales méthodes et normes pour l'analyse des risques (EBIOS, Mehari, ISO 27001…)
Qu'est-ce que la cybercriminalité ? Les grandes familles de virus et malwares
Quelles sont les menaces physiques ?
Cas pratiques

Sécurité du réseau : protéger les systèmes et équipements
Rappels sur le protocole TCP/IP
Différents types de réseaux : VPN SSL, VPN IPsec, MPLS, VLANs, Wifi…
Equipements : NAT, pare-feux, proxies, UTM…
Systèmes de détection et de prévention des intrusions
Méthodes et outils pour l'identification, l'authentification et les contrôles d'opérations (SAML, LDAP, AD, Kerberos…)
Utilisation des technologies Big Data et de l'intelligence artificielle (détection des anomalies, stockage et analyse des logs…)
Eléments de cryptographie : cryptage symétrique et asymétrique, certificats et PKIs
Les protocoles SSL (Secure Sockets Layer), TLS (Transport Layer Security) et HTTPS (HyperText Transfer Protocol Secure)
Les meilleures pratiques pour superviser le réseau
Cas pratiques

Technologies Cloud et datacenters : la sécurité dans le nuage
Quel plan d'infrastructure technique pour les centres de données ?
DMZ, quartiers techniques, VLANs et appliances next génération
Plan de Continuité d'Activité (PCA) et Plan de Reprise d'Activité (PRA)
Sauvegarder et archiver les données : établir une stratégie
Critères d'externalisation pour virtualiser serveurs, réseaux et applications
Composant de la sécurité du Cloud : VPC, CASB, VPN…
Analyse de risque avec la Cloud Control Matrix
Contrats et certifications d'hébergement
Cas pratiques

Sécurité des logiciels et applications
Différents types de logiciels : systèmes d'exploitation, bases de données, utilitaires…
Les bonnes pratiques de développement
Les architectures pour sécuriser applications et données
Sécurité des services et référentiels de données
Inforensic, pentests et mise en place du SIEM
Sécurité des postes de travail, serveurs, périphériques, terminaux mobiles et objets connectés
Intégrité des données
Supervision logicielle avec les technologies Big Data
Objectifs d'un DAT (Dossier Architecture Technique)
Auditer la sécurité d'un point de vue technique et organisationnel
Cas pratiques

Aspects organisationnels et gouvernance
Considérations pour l'organisation : rôles, comité directeur, reporting, supervision, formation, documentation…
L'importance d'effectuer une bonne veille technologique
Gouvernance centralisée
Quel avenir pour la sécurité informatique ?
Cas pratiques