Formation Maîtriser la Sécurité Systèmes et Réseaux

Durée :	5.0 jour(s)
Objectifs :	• Connaître les enjeux de la **sécurité des systèmes d'information** • Sécuriser le trafic **réseau** • Sécuriser une **architecture hybride** • Déployer et gérer des modèles de **sécurité informatique** • Découvrir les différents algorithmes de cryptographie
Public :	• Responsables informatiques • Techniciens et administrateurs réseaux • Responsable de la sécurité informatique
Prérequis :	• Connaissance des protocoles réseaux et des systèmes d'exploitation • Forte sensibilisation aux enjeux liés à la sécurité.
Modalités et moyens pédagogiques	Démonstrations visuelles et pratiques à travers des exercices d'application et/ou des cas concrets des stagiaires. Salle de formation équipée d'un poste PC par personne et de dispositif vidéo Grand Ecran. Portail web: maformation.vaelia.fr
Modalités d'évaluation	Auto évaluation des acquis, exercices pratiques et/ou échanges avec le formateur.
Moyens d'encadrement	Un formateur expert spécialisé en Systèmes et Réseaux dont les compétences ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou Vaelia.
Satisfaction globale :	4.20/5 *Calculée à partir des évaluations stagiaires sur les 12 derniers mois.*

Jour 1 - Introduction à la cybersécurité

Comprendre les principes fondamentaux de la cybersécurité (CIAD)

- Identifier les principes de Confidentialité
- Identifier les principes d'Intégrité
- Identifier les principes de Authenticité
- Identifier les principes de Disponibilité

Reconnaître les acteurs de la cybersécurité

- Acteurs publiques (ANSSI, COMCYBER, …)
- Acteurs privés (ESN, Formations professionnels, écoles, Assurances...)

Acquérir les bases des réseaux informatiques

- Différencier les WAN, LAN, …
- Identifier et configurer les EAR (routeurs, switch, pare-feu, …)
- Expliquer TCP/IP, DNS, DHCP

Explorer la cryptographie

- Connaître l'histoire de la cryptographie
- Comprendre les chiffrements symétriques et asymétriques, les signatures, le contrôle (SHA), ...

Jour 2 - La sécurisation des réseaux

Comprendre son réseau

- Différencier les ressources métiers
- Différencier les données en transit

Segmenter son réseau

- Mettre en place la segmentation physique (pare-feu, fibre optique,...)
- Concevoir la segmentation logique (VPN, VLAN, ...)

Atelier “Séparer mes réseaux”

- Mise en pratique de la séparation des réseaux en fonctions des données

Jour 3 - La sécurisation des SI

Gérer l'identité et l'accès IAM (Identity and Access Management)

- Configurer l'annuaire pour l'identification et la gestion des identités
- Appliquer le RBAC pour la gestion des droits et des permissions
- Etablir les politiques de gestion des mots de passe et d'authentification externe (SSO)

Les architectures hybrides

- Intégration de service CLOUD dans son architecture

Atelier “Sécurisation de son SI”

- Mise en place d’une architecture hybride (contrôle d’accès, sauvegardes, chiffrements, SSO, …)

Jour 4 - Se préparer

Gestion de la continuité d’activité

- Définir et Appliquer le PCA (Plan de Continuité d'Activité)
- Définir et Appliquer le PRA (Plan de Reprise d'Activité)
- Établir et simuler une cellule de crise

Gestion des incidents de sécurité

- Développer des procédures de gestion des incidents

Appréciation des risques

- Évaluer les risques liés à la cybersécurité

Outils et méthodes d'attaques

- Connaître les méthodes telles que le phishing, le ransomware, le man-in-the-middle, ...
- Comprendre les outils d'attaques associés

Détection d'intrusions

- Utiliser des outils de supervision
- Mettre en œuvre des outils de détection
- Analyser l'utilisation des pots de miel et comprendre sa mise en place

Jour 5 - Se défendre

Sécurité opérationnelle

- Élaborer des procédures opérationnelles
- Établir les exigences cyber
- Participer à des exercices de défense
- Mettre en œuvre des programmes de formation et de sensibilisation

La veille

- Analyser les sources telles que OWASP, ANSSI (CERT),…

Intégrer et sécuriser l'IA

- Appliquer des mesures de sécurité pour l'intégration de l'IA

Les approches de la cybersécurité

- Évaluer les approches "métiers"
- Évaluer les approches "légales"
- Mettre en œuvre les approches "restrictive/permissive"

Bilan

- Évaluer les connaissances acquises au cours de la formation
- Recommander des actions futures pour renforcer la sécurité

Pour aller plus loin : Formation Hacking et Sécurité avancée - Gestion des procédures et des attaques , Formation Ethical Hacking - Les fondamentaux de la sécurité informatique