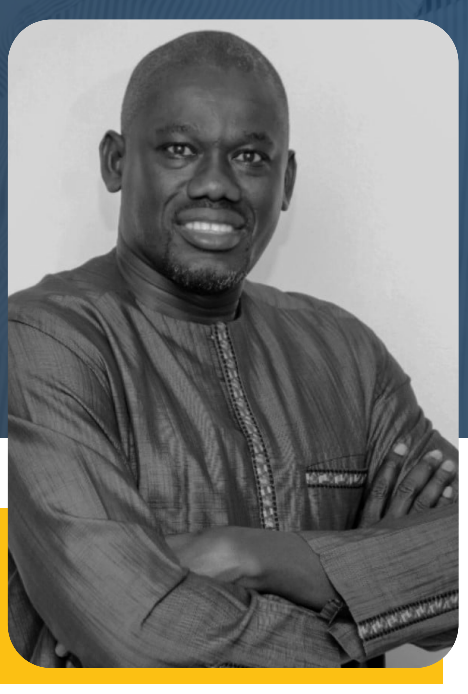
FORMATION CYBERSÉCURITÉ

Séminaire de 40 heures (15 heures théoriques et 25 heures pratiques avec des Lab)



Dr EL Hadji Modou **MBOUP**

Enseignant – chercheur
Expert en Cybersécurité
CEH
Lead Implementer 27001
+13 ans d'expérience professionnel en Cybersécurité
Fondateur du cabinet UTA (https://221uta.com)

INSCRIPTION

https://221uta.com

Formation 100 % en ligne

formations@221uta.com

+221 77 425 87 82

MODULES DE LA FORMATION

INSCRIPTION

https://221uta.com

Formation 100 % en ligne

Module 1 : Généralité à la Sécurité IT

Objectif : Ce module a pour but de présenter aux participants un ensemble de vocabulaire lié à la sécurité IT qui sera utilisé dans la suite de la formation.

Chapitre 1 : Notions fondementales de la sécurité IT

Module 2 : Sécurité réseau (VLAN, FIREWALL, VPN, IPS/IDS, PROTOCOLES, ...)

Objectif : : Ce module a pour objectif de donner aux professionnels des connaissances approndies en sécurité réseau. Il s'agit spécifiquement de permettre aux particiapants :

- o D'évaluer le niveau de sécurité d'une architecture réseau ;
- o D'affectuer des audit de sécurité dans un réseau ;
- o De disposer des connaissance pour configurer les équipements de sécurité réseau.
- o De simuler des attaques dans un réseau,
- o De mettre en œuvre des moyens de défense dans un réseau.

Chapitre 2 : Les moyens de défense techniques dans un réseau

Chapitre 3 : Les attaques réseaux

Chapitre 4 : Application des moyens de défense dans un réseau

Module 3 : Sécurité Système (Active Directory, DNS, Antivirus, IOS, ...)

Objectif : Les objectifs de ce module sont :

- o Décrire les mécanismes internes de sécurité de l'Active Directory
- o Identifier les fonctionnalités et les roles de sécurité dans l'Active Directory et dans le système de manière générale ;
- o Concevoir une architecture système (domaine) robuste ;
- o Identifier les attaques et principales exploitations dans un système existant
- o Mettre en oeuvre les contre-mesures (SSO, Authentification multifacteur, ...)..

Chapitre 5 : Sécurité Active Directory

Chapitre 6 : Sécurité des environnements (virtualisation, cloud, serveurs, ...)

Chapitre 7 : Sécurité contre les logiciels malveillant

Module 4 : Sécurité des applications (Footprinting, hacking web server, session hijacking, ...)

Objectif : Les objectifs de ce module sont de sensibiliser les développeurs, analystes, concepteurs et architectes à la sécurité applicative Web et de leur permettre d'acquérir des notions et concepts pouvant les aider à comprendre les attaques, de développer du code plus sécuritaire et déployer des applications plus vigoureuses en matière de sécurité en lien avec les pratiques définies par l'OWASP.

Chapitre 8 : Les attaques applicatves

Chapitre 9 : Les outils de protection contre les attaques applicatives

Module 5 : Cryptographie et Applications (SSL/TLS, Signature électronique, SSH, Certificat, PKI, ...)

Objectif : Ce module a pour but de permettre aux apprenants de comrendre les algorithmes cryptographiques, de déployer les protocoles de sécurité utlisant les algorithmes cryptographiques (SSL/TLS, SMIME, IPSEC, PGP, Certificat, Signature Electronique, ...) et de comprendre l'utilisation des outils professionnels de la crytographie.

Chapitre 10 : Les fondementaux de la cryptographie

Chapitre 11 : Applications de la cryptographie

Module 6 : Nouvelle Génération d'Outils de Protection (SIEM/SOC, MDM, Userlock, ...)

Objectif : Ce module a pour but de permettre aux apprenants de maitriser le déploiement des outils de sécurité de dernière gération (SIEM, Firewall NG, MDM, ...) et de comprendre leur déploiement de ces outils dans un environnement.

Chapitre 12 : Les outils NG de la sécurité IT

Chapitre 13 : Déploiement des outils de nouvelle génération