5

5. Introduction à la cybersécurité de l'information

OBJECTIFS DE LA FORMATION

L' objectif de cette formation va permettre aux participants de s'informer:

- Sur les tendances actuelles des menaces et des solutions existantes
- Sur les mécanismes de gestion de la sécurité des Systèmes, réseaux et applications

Les participants sont sensibilisés :
- Sur les systèmes de management de la sécurité des systèmes d'information
- Sur la gestion opérationnelle de la sécurité
- Devenir un Data Scientist autonome et passionné!

La durée de la formation est de 3 jours.

CONTENU DE LA FORMATION

Jour 1

Séance 1 : Les concepts fondamentaux

Les différents points qui seront traités sont les suivants :

1. Les enjeux de la sécurité des SI ;
2. Les besoins de sécurité ;
3. Cybersécurité par opposition à Cyberdéfense ;
4. Les disciplines : gouvernance, sécurité opérationnelle ;
5. Cartographie des métiers de la Cybersécurité ;
6. Acquisition d'un glossaire étape 1 sur les Profils métiers de la cybersécurité.

Séance 2 : Les bonnes pratiques sur l'usage du SI

Les différents points qui seront traités sont les suivants :

1. Connaissance du SI et gestion de l'utilisateur ;
2. Identifiants et mots de passe ;
3. Gestion des documents et confidentialité ;
4. Utilisation de la messagerie.

5. Introduction à la cybersécurité de l'information

Jour 2

Séance 3 : Les références et les certifications

Les différents points qui seront traités sont les suivants :

1. Référentiels : OWASP, ISO 27000, SANS, MITRE ;
2. Les certifications pour produits : CC, CSPN ;
3. Les certifications pour entreprises ;
4. Les certifications pour les personnes : CEH, CISSP.

Séance 4 : Les références et les certifications

Les différents points qui seront traités sont les suivants :

1. Sécurisation d'un terminal ;
2. Sécurisation d'un serveur ;
3. Sécurisation physique ;
4. Sécurité périmétrique (sécurité d'un réseau) ;
5. Les principes d'une segmentation réseau.

Séance 5 : Cryptographie

Les différents points qui seront traités sont les suivants :

1. Le chiffrement : fondamentaux et méthodes (symétriques et asymétriques) ;
2. Acquisition d'un glossaire étape 2 (20 termes) ;
3. Hachage et encodage : principes fondamentaux et enjeux.

5. Introduction à la cybersécurité de l'information (Suite et fin)

Jour 3

Séance 6 : La sécurité applicative

Les différents points qui seront traités sont les suivants :

1. Intégrer la sécurité dans les projets ;
2. Les concepts de sécurité applicative (Secure-SDLC, Security by Design, Shift ;
3. Security to the Left ;
4. La sécurité des applications web ;
5. Présentation des référentiels CVE, CWE et OWASP Top10 2017 ;
6. Bonnes pratiques de développement pour éviter les vulnérabilités applicatives ;
7. Introduction au DevSecOps.

Séance 7 : Ethical hacking et audits

Les différents points qui seront traités sont les suivants :

1. Introduction au Hacking ;
2. Cybercriminalité ;
3. Contrôler la sécurité du SI ;
4. Méthodologie d'audit et boîte à outil de l'auditeur ;
5. Les différentes approches de l'audit : pentest, red team, bug bounty;
6. Acquisition d'un glossaire étape 3 (20 termes).

FORMAT

La formation se passe sous forme de présentation Powerpoint, d'interactions entre les participants et le formateur et d'ateliers pratiques entre les participants.

INTERVENANT

Amadou Moctar BA

Expert SI & Sécurité SI, Formateur agréé PECB, le Formateur participe à des missions de conseil et d'assistance, de pilotage de projets de système d'information et sécurité informatique (Implémentation SMSI, audit/diagnostic, plan stratégique SI, Schéma directeur SI, transformation digitale, etc.). Par ailleurs, le Formateur est titulaire de Lead Implementer / Auditor ISO 27001, Risk Manager ISO 27005, Lead Application Security Implementer ISO 27034 et anime des formations à la sécurité des SI, gestion des risques, sécurité des applications et cybersécurité.