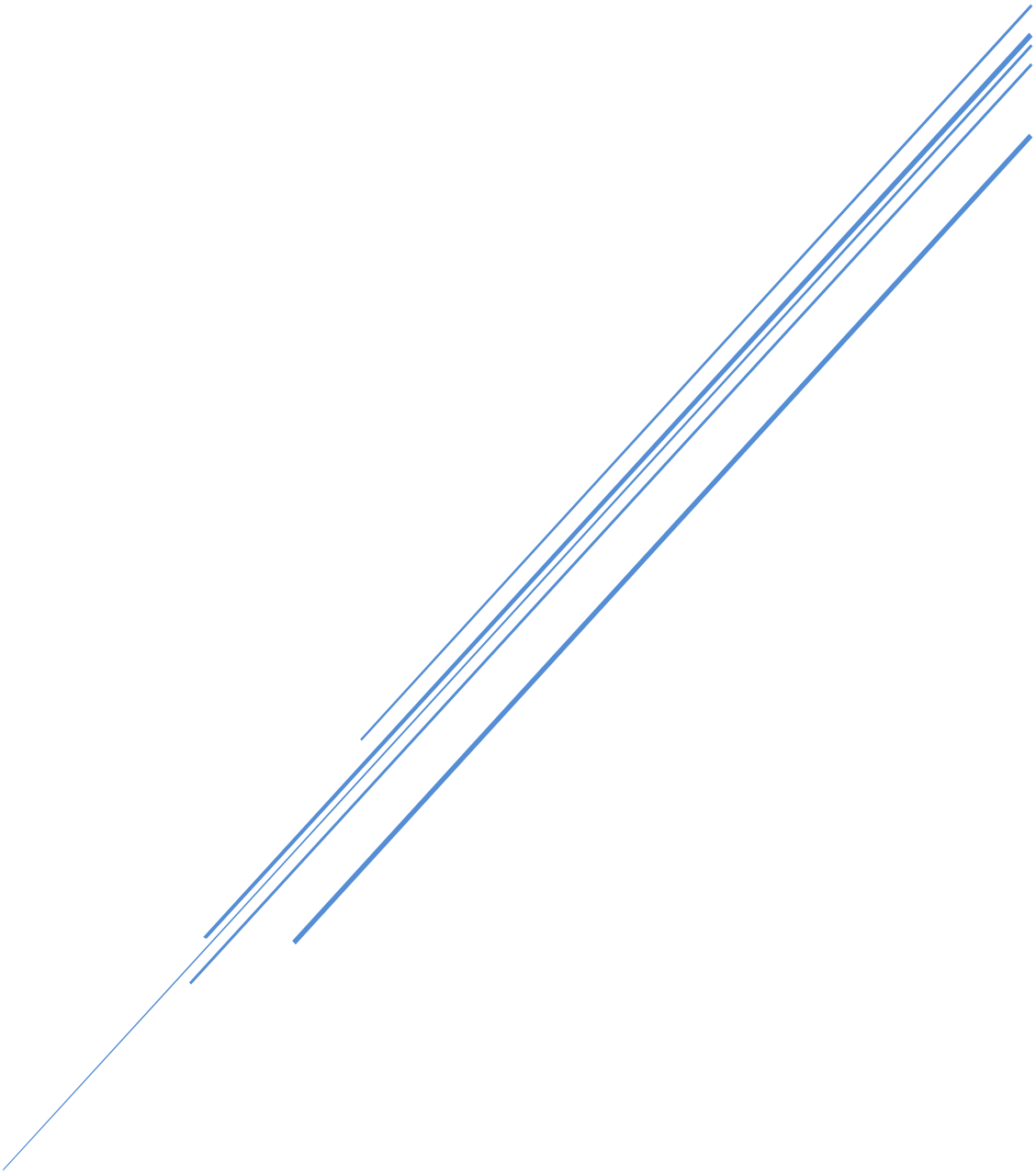
CATALOGUE DE FORMATION

CyberSécurité



Collaboration entre : INFORMICA - école de formation professionnelle agréée par l'État &
Aicha Amina LAKEHAL | Cybersécurité & Transformation Digitale Consultante Advisor

EFP INFORMICA
Agréée par l'Etat
Agrément N° 307/2020

Introduction

Toutes les organisations sont confrontées aux menaces informatiques externes comme internes. Chacune se doit de protéger et sécuriser ses données et ses systèmes, d'assurer la continuité d'activité en cas de panne, de respecter les exigences de la loi 18-07, de recourir aux référentiels ISO pour définir et mettre en œuvre une politique de sécurité, de simuler des cas critiques et d'effectuer des tests de sécurité.

En interne, la sensibilisation et la formation des utilisateurs à la conduite à adopter contribuent activement à la sécurité du système d'information.

Les formations proposées dans ce catalogue ont été élaborées et sont assurées par Aicha Amina LAKEHAL, Cybersecurity & IT Digitalization Architect Advisor, experte dans la mise en œuvre de solutions de sécurité adaptées aux besoins des entreprises.

Le programme couvre l'ensemble des volets nécessaires pour accompagner votre entreprise dans sa démarche de Cybersécurité. Il est défini selon une approche progressive, en fonction des objectifs, des attentes et du niveau de maturité du public concerné en matière de sécurité des systèmes d'information.

Les formations proposées se déclinent comme suit :

Vous trouverez ci-après le descriptif détaillé et la fiche technique de chacune des formations proposées.

Formation
Sensibilisation à la Cybersécurité

Description de la Formation
Cette formation vise à fournir aux participants une **compréhension globale de la sécurité informatique** et de son impact crucial sur l'entreprise.
Le cours permet d'identifier et de comprendre les **cybermenaces, les risques** et les **conséquences potentielles** qu'une action d'un employé peut avoir sur la sécurité des informations de l'entreprise. Il clarifie également le **rôle et la responsabilité** des employés dans la prévention des risques et la protection de leur organisation.
La formation propose des **conseils pratiques** et des **bonnes pratiques** pour renforcer la vigilance des employés et développer une **cyberculture solide** au sein de l'entreprise.

Objectifs
- **Sensibiliser** les utilisateurs à l'importance de la sécurité informatique en entreprise.
- **Comprendre** les risques et menaces pesant sur le système d'information et leurs impacts.
- **Expliquer** le rôle et la responsabilité de l'utilisateur pour la sécurité du SI.
- **Favoriser** l'application de la politique de sécurité des SI de l'entreprise.
- **Acquérir** les bons réflexes pour la sécurité des données et promouvoir une culture de sécurité.

DURÉE	PUBLIC CONCERNÉ	PRÉREQUIS
5 jours	- Tous les utilisateurs du système d'information. - Tout le personnel (employés) de l'entreprise.	Aucune connaissance particulière n'est attendue.

Programme de la formation

Module 1 : Introduction à la Cybersécurité
- Enjeux de la Cybersécurité (notamment dans le journalisme)
- Risques des cyberattaques
- Responsabilités en matière de protection des données

Module 2 : L'importance de la Sensibilisation en Entreprise

- Pourquoi sensibiliser à la Cybersécurité ?

Module 3 : Profils et Motivations des Cybercriminels

- Hackers éthiques
- Hacktivistes
- Espionnage politique

Module 4 : Types et Vecteurs d'Attaques Informatiques

- Attaques par messagerie électronique
- Logiciels malveillants
- Usurpation et piratage de comptes
- Erreurs et mauvaises manipulations d'appareils digitaux
- Arnaques et escroqueries en ligne (téléphoniques, etc.)

Module 5 : Les Cyberattaques Majeures

- Phishing (Hameçonnage)
- Ransomware
- Ingénierie Sociale
- Sites malveillants (crack, vidéo, etc.)

Module 6 : Stratégies de Protection

- Sécurité de la messagerie
- Authentification et mots de passe forts
- Sécurité des connexions (réseaux sans fil, mobiles)
- Sécurité du Cloud
- Sécurité des appareils digitaux (postes de travail, téléphones)
- Utilisation sécurisée d'Internet (e-paiement, sites de confiance, téléchargement)
- Utilisation des médias sociaux
- Sécurité des données personnelles (Loi 18-07)

Module 7 : Bonnes Pratiques en Entreprise

Module 8 : Évaluation des Connaissances

- Test final

Formation

La Loi 18-07 Relative à la Protection des Données à Caractère Personnel

Objectifs de la Formation

À l'issue de cette formation, les participants seront capables de :

- **Maîtriser le nouveau cadre réglementaire** sur la protection des données personnelles : la **Loi 18-07**.
- **Évaluer la situation de leur organisation** vis-à-vis de cette réglementation.
- **Sécuriser les données personnelles** au sein de leur entreprise.
- **Comprendre les missions** spécifiques assignées au DPO (Délégué à la Protection des Données).
- **Identifier les actions concrètes** à mettre en œuvre pour assurer la mise en conformité de leur organisation.

DURÉE	PUBLIC CONCERNÉ	PRÉREQUIS
3 jours	- **Responsables informatiques, Responsables juridiques, Directeurs, Administratifs**. - **DSI, RSSI, Juristes**. - Toute personne concernée par la **protection des données à caractère personnel**.	Aucun prérequis spécifique n'est mentionné.

Programme de la Formation

Module 1 : Aperçu Général de la Loi 18-07

- État de la protection des données à caractère personnel dans le monde.
- L'importance de protéger les données personnelles.
- Base juridique de la loi 18-07.
- Historique de la réglementation de protection des données personnelles en Algérie.
- Structure : Chapitres et Sections de la loi 18-07.

Module 2 : Notions et Terminologie Clés de la Protection des Données

- Définition des données à caractère personnel.

- Compréhension du terme "personne concernée".
- Le traitement des données à caractère personnel.
- Le consentement de la personne concernée.
- Rôle et responsabilité du responsable du traitement.
- Distinction des données sensibles.

Module 3 : L'Autorité Nationale de la Protection des Données à Caractère Personnel

- Mise en place de l'autorité.
- Objectifs et principales missions de l'autorité.

Module 4 : Principes Fondamentaux de la Protection des Données à Caractère Personnel

- Le consentement de la personne concernée.
- Principes de licéité et de loyauté.
- Principe de finalité.
- Principe de pertinence.
- Durée de conservation des données.
- Déclaration et autorisation.

Module 5 : Droits des Personnes Concernées

- Droit d'information.
- Droit d'accès.
- Droit d'opposition.
- Droit de rectification.
- Droit d'interdiction de prospection.

Module 6 : Obligations du Responsable du Traitement

- Confidentialité et sécurité du traitement.
- Traitement lié aux certifications et signature électronique.
- Notification d'une violation de données.
- Transfert des données à l'étranger.

Module 7 : Sanctions

- Dispositions administratives.
- Dispositions pénales.

Module 8 : Mise en Conformité à la Loi 18-07

- L'obligation de la mise en conformité à la loi.
- Désignation du représentant de la protection des données personnelles (DPO).

Module 9 : Plan d'Actions de la Mise en Conformité à la Loi 18-07

- Démarche de la mise en conformité technique et réglementaire.
- **Phase 01 : Audit et Diagnostic** (Audit des données personnelles et traitements, et de la sécurité informatique).
- **Phase 02 : Correction des Non-Conformités** réglementaires et techniques (mise en place de mesures de sécurité de l'information).

Formation
Sécurité des Réseaux et Systèmes

Description de la Formation
Ce stage pratique vous guidera dans la mise en œuvre des principaux moyens de **sécurisation des systèmes et des réseaux**. Après une étude des menaces pesant sur le Système d'Information, vous découvrirez le rôle essentiel des divers équipements de sécurité pour la protection de l'entreprise. L'objectif est de vous rendre capable de **concevoir une architecture de sécurité robuste** et d'en assurer la mise en œuvre.

Objectifs
À l'issue de cette formation, les participants seront capables de :

- **Identifier** les failles et les menaces des systèmes d'information.
- **Maîtriser** le rôle des divers équipements de sécurité.
- **Concevoir et réaliser** une architecture de sécurité adaptée.
- **Mettre en œuvre** les principaux moyens de sécurisation des réseaux.
- **Sécuriser** un système Windows et Linux.

DURÉE	PUBLIC VISÉ	PRÉREQUIS
5 jours	- **Responsables informatiques**. - **Administrateurs réseaux**. - **Responsables de la sécurité informatique (RSSI, DSI)**.	Une **bonne connaissance générale des réseaux et des systèmes d'exploitation courants** est nécessaire.

Programme de la formation

Module 1 : L'Environnement de la Sécurité

- Le périmètre (réseaux, systèmes d'exploitation, applications).
- Les acteurs (hackers, responsables sécurité, auditeurs, vendeurs et éditeurs).
- La veille technologique.
- Les organismes officiels.

Module 2 : Les Méthodes des Attaquants

- Les scénarios d'attaques : intrusion, DDoS, etc.

- Les attaques sur les protocoles réseaux.
- Les faiblesses des services : Web, VoIP, Messagerie.
- Le code vandale : virus, vers et chevaux de Troie.

Module 3 : La Sécurité des Accès (Firewall, WAF, Proxy, NAC)

- L'accès des stations aux réseaux d'entreprise et son organisation (802.1X, NAC).
- Les différents types de firewalls.
- Les règles de filtrage.
- Les règles de la translation d'adresse (NAT).
- La mise en œuvre d'une zone démilitarisée (DMZ).
- La détection et surveillance avec les IDS (Intrusion Detection Systems).
- L'intégration d'un firewall dans le réseau d'entreprise et son organisation.
- La gestion et l'analyse des fichiers log.

Module 4 : La Sécurité des Systèmes d'Exploitation

- Le hardening de Windows.
- Le hardening d'Unix/Linux.
- Le hardening des nomades : iOS / Android.

Module 5 : Sécurité des Applications et Architectures

- Les serveurs et clients Web.
- La messagerie électronique.
- La VoIP (IPBX et téléphones).

Module 6 : La Sécurité des Échanges et la Cryptographie

- L'objectif du cryptage et les fonctions de base.
- Les algorithmes symétriques et asymétriques.
- Les algorithmes de hashing.
- Les méthodes d'authentification (PAP, CHAP, Kerberos).
- Le HMAC et la signature électronique.
- Les certificats et la PKI (Public Key Infrastructure).
- Les protocoles SSL, IPsec, S/MIME.
- Les VPN (réseau privé virtuel) : site à site et nomade.

Formation
ISO 27001 Lead Implementer

Objectifs de la Formation
Cette formation vous permettra de :

- **Acquérir les compétences** nécessaires pour appliquer efficacement les meilleures pratiques en **management de la sécurité de l'information (MSI)**.
- **Maîtriser les approches, méthodes et techniques** pour mettre en œuvre, gérer, surveiller et réviser un **Système de Management de la Sécurité de l'Information (SMSI)**, en totale conformité avec la **norme ISO/IEC 27001**.
- **Comprendre la corrélation** entre l'**ISO 27001 et l'ISO 27002**, ainsi qu'avec d'autres normes et cadres réglementaires.
- **Savoir conseiller et accompagner** une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la mise à jour de son SMSI.
- **Appréhender la relation** entre un SMSI (incluant la gestion des risques et des contrôles) et la conformité aux exigences des différentes parties prenantes d'une organisation.

DURÉE	PUBLIC CONCERNÉ	PRÉREQUIS
5 jours	- Toute personne impliquée dans le **management de la sécurité de l'information**. - Toute personne souhaitant acquérir des connaissances sur les principaux processus de mise en place d'un système de management de la sécurité. - **Consultants, chefs de projet, RSSI, DSI**, ou ingénieurs sécurité souhaitant accompagner une organisation dans l'implémentation de son SMSI.	- Connaissances de base de la sécurité des systèmes d'information. - Connaissances en réseau et système.

Programme de la formation

Module 1 : Introduction aux Concepts du SMSI selon ISO/IEC 27001

- Introduction aux systèmes de management et à l'approche processus.
- Présentation de la suite des normes ISO 27000, ainsi que du cadre normatif, légal et réglementaire.

- Principes fondamentaux de la sécurité de l'information.
- Analyse préliminaire et détermination du niveau de maturité d'un SMSI existant.
- Rédaction d'une étude de faisabilité et d'un plan projet pour la mise en œuvre d'un SMSI.

Module 2 : Planification de la Mise en Œuvre d'un SMSI basé sur l'ISO 27001

- Définition du périmètre (domaine d'application) du SMSI.
- Développement de la politique et des objectifs du SMSI.
- Sélection de l'approche et de la méthode d'évaluation des risques.
- Gestion des risques : identification et traitement du risque (selon ISO 27005).
- Rédaction de la Déclaration d'Applicabilité.

Module 3 : Mise en Œuvre d'un SMSI basé sur la norme ISO 27001

- Mise en place d'un processus de gestion de la documentation.
- Conception et implémentation des mesures de sécurité.
- Développement d'un plan de formation, de sensibilisation et de communication sur la sécurité de l'information.
- Gestion des incidents.
- Gestion des opérations d'un SMSI.

Module 4 : Contrôle, Surveillance, Mesure et Amélioration d'un SMSI selon ISO 27001

- Surveillance, mesure, analyse et évaluation.
- Audit interne.
- Revue de direction.
- Traitement des non-conformités.

Formation

ISO 27005 Risk Manager

Gestion des Risques de Sécurité de l'Information

Objectifs de la Formation

Cette formation vous permettra de :

- **Comprendre** les concepts, approches, méthodes et techniques pour un processus de **gestion des risques efficace et conforme à ISO/IEC 27005**.
- **Savoir interpréter** les exigences de la norme **ISO/IEC 27001** dans le cadre du management du risque de la sécurité de l'information.
- **Acquérir les compétences** pour conseiller efficacement les organisations sur les meilleures pratiques en matière de **management du risque lié à la sécurité**.
- **Comprendre le concept de risque** lié à la sécurité de l'information, savoir l'apprécier, le traiter et le présenter au propriétaire du risque.

DURÉE	PUBLIC VISÉ	PRÉREQUIS
3 jours	- Tout individu **responsable de la sécurité de l'information, de la conformité et du risque** dans un organisme. - Tout individu mettant en œuvre **ISO/IEC 27001**, désirant s'y conformer ou impliqué dans un programme de management du risque. - **Gestionnaires du risque (Risk Managers), consultants, chefs de projet, RSSI, DSI**, ou ingénieurs sécurité amenés à réaliser une analyse de risques de la sécurité de l'information.	- Connaissances de base de la **sécurité des systèmes d'information**. - Connaissances en **réseau et système**.

Programme de la formation

Module 1 : Introduction au Programme de Gestion des Risques Conforme à ISO/IEC 27005

- Objectifs et structure de la formation.
- Concepts et définitions du risque.

- Cadres normatifs et réglementaires.
- Mise en œuvre d'un programme de gestion des risques.
- Compréhension de l'organisation et de son contexte.

Module 2 : Mise en Œuvre d'un Processus de Gestion des Risques Conforme à ISO/IEC 27005

- Identification des risques.
- Analyse et évaluation des risques.
- Appréciation du risque avec une méthode quantitative.
- Traitement des risques.
- Acceptation des risques et gestion des risques résiduels.

Module 3 : Communication et Surveillance du Risque

- Communication et concertation relatives aux risques en sécurité de l'information.
- Surveillance et revue du risque.

Formation
Certified Ethical Hacker v13 (CEH v13)

Description de la Formation
Le programme de certification "**Hacker Éthique**" est une formation complète qui explore les diverses facettes de la sécurité. Son principe fondamental est de se **mettre dans la peau d'un hacker** pour comprendre leurs méthodes d'attaque et ainsi mieux s'en prémunir.
Ce cours accrédité fournit les **outils et techniques de piratage informatique avancés** que les hackers et les professionnels de la sécurité de l'information utilisent pour pénétrer les systèmes d'information des organisations. La devise de la formation est claire : "**Pour battre un hacker, il faut réfléchir comme un hacker**".
Vous explorerez les **cinq phases du piratage éthique** : reconnaissance, obtention d'accès, dénombrement, maintien d'accès et couverture des traces. Vous apprendrez concrètement comment **scanner, tester, hacker et sécuriser un système**.

Objectifs
À l'issue de cette formation, les participants seront capables de :

- **Maîtriser une méthodologie de Hacking Éthique** rigoureuse.
- **Découvrir comment scanner, tester et hacker** leur propre système de manière sécurisée.
- **Acquérir des compétences techniques** d'auditeur en sécurité informatique.
- **Obtenir des compétences** en piratage éthique hautement recherchées sur le marché.

DURÉE	PUBLIC CONCERNÉ	PRÉ-REQUIS
5 jours	- **Responsables sécurité** - **Auditeurs** - **Professionnels de la sécurité** - **Administrateurs de site** - Toute personne concernée par la **stabilité des systèmes d'information**	Connaissances de **TCP/IP, Linux et Windows Server**.

Programme de la formation

Module 1 : Introduction au Hacking Éthique

Module 2 : Footprinting et Reconnaissance

Module 3 : Scanning de Réseaux

Module 4 : Énumération

Module 5 : Analyse de Vulnérabilité

Module 6 : Hacking de Système

Module 7 : Menaces Liées aux Logiciels Malveillants

Module 8 : Sniffing

Module 9 : Ingénierie Sociale

Module 10 : Attaques par Déni de Service (DoS/DDoS)

Module 11 : Hijacking de Sessions

Module 12 : Éviter les IDS, les Pare-feu et les Pots de Miel (Honeypots)

Module 13 : Piratage de Serveurs Web

Module 14 : Piratage d'Applications Web

Module 15 : Injection SQL

Module 16 : Piratage de Réseaux Sans Fil

Module 17 : Piratage de Plates-formes Mobiles

Module 18 : Piratage d'Équipements IoT (Internet des Objets)

Module 19 : Cloud Computing

Module 20 : Cryptographie

Formation

CISA (Certified Information Systems Auditor)

Auditeur de Sécurité Informatique

Description de la Formation

La certification **CISA (Certified Information Systems Auditor)** est une référence mondiale reconnue pour l'**audit, le contrôle et l'assurance des systèmes d'information**. Les professionnels certifiés CISA apportent une crédibilité essentielle pour interpréter les normes, gérer les vulnérabilités, assurer la conformité, proposer des solutions, mettre en place des contrôles et générer de la valeur pour les organisations.

Cette certification atteste de la **maîtrise de la gouvernance, du management et du suivi des risques informatiques**. C'est souvent une qualification indispensable pour exercer la fonction d'auditeur informatique.

Objectifs

À l'issue de cette formation, les participants seront capables de :

- **Approfondir** leurs connaissances et compétences en **audit des systèmes d'information**.
- **Comprendre et appliquer** les **normes ISACA**.
- **Acquérir les connaissances et compétences** nécessaires pour devenir des auditeurs de systèmes d'information compétents, capables de mener des audits conformes aux normes ISACA.
- **Conseiller les entreprises** sur la gestion des risques et la gouvernance IT.
- **Valider leurs compétences** sur leur capacité à évaluer les vulnérabilités, à rédiger des rapports de conformité et à mettre en œuvre des contrôles au sein d'une entreprise.

DURÉE	PUBLIC VISÉ	PRÉREQUIS
5 jours	- **Responsables et dirigeants** impliqués dans la gestion de la cybersécurité. - **Professionnels de la cybersécurité**. - **RSSI, DSI, Ingénieurs, Chefs de projet sécurité**. - **Chefs de projet et consultants en sécurité IT**.	- Connaissances de base de la **sécurité des systèmes d'information**. - Connaissances en **réseau et système**.

Programme de la formation

Module 1 : Processus d'Audit des Systèmes d'Information

- Les standards d'audit.
- L'analyse de risque et le contrôle interne.
- La pratique d'un audit SI.

Module 2 : Gouvernance et Gestion des Systèmes d'Information

- La stratégie de la gouvernance du SI.
- Les procédures et le Risk Management.
- La pratique de la gouvernance des SI.
- L'audit d'une structure de gouvernance.

Module 3 : Acquisition, Conception, Implantation des SI

- La gestion de projet : pratique et audit.
- Les pratiques de développement.
- L'audit de la maintenance applicative et des systèmes.
- Les contrôles applicatifs.

Module 4 : Exploitation, Entretien et Soutien des Systèmes d'Information

- L'audit de l'exploitation des SI.
- L'audit des aspects matériels du SI.
- L'audit des architectures SI et réseaux.

Module 5 : Protection des Actifs Informationnels

- La gestion de la sécurité : politique et gouvernance.
- L'audit et la sécurité logique et physique.
- L'audit de la sécurité des réseaux.
- L'audit des dispositifs nomades.

Formation

Responsable de la Sécurité des Systèmes d'Information (RSSI)

Description de la Formation

À l'ère du digital, la fonction de **RSSI** est devenue éminemment stratégique. Le RSSI doit non seulement posséder une solide culture technique, mais aussi définir des **politiques de sécurité**, assurer la **conformité du système d'information** aux référentiels en vigueur, et prendre des **décisions éclairées** en cas d'incident. Il est le pont entre les problèmes techniques complexes et la communication avec la direction et le personnel.

En somme, le RSSI est le garant de l'équilibre entre les **orientations stratégiques** et les **décisions opérationnelles** quotidiennes. Il doit être capable de dialoguer avec le management tout en pilotant des projets et en résolvant des problématiques purement techniques.

Cette formation est précisément conçue pour apporter au RSSI tous les éléments et les **compétences indispensables** à l'exercice efficace de ses fonctions.

Objectifs

À l'issue de cette formation, les participants seront capables de :

- **Définir et comprendre** les enjeux de sécurité des SI dans les organisations.
- **Posséder** les connaissances techniques essentielles.
- **Mettre en œuvre** l'organisation de la sécurité et la norme **ISO 27001**.
- **Maîtriser** la politique de sécurité, savoir auditer la sécurité et les indicateurs.
- **Appréhender** les méthodes d'appréciation des risques.
- **Connaître** les aspects juridiques de la sécurité des SI.
- **Être sensibilisé** à la sécurité des SI et à la gestion des incidents.

DURÉE	PUBLIC CONCERNÉ	PRÉREQUIS
5 jours	- Toute personne amenée à exercer la fonction de **Responsable Sécurité des Systèmes d'Information (RSSI)**, ou futur RSSI. - **Responsables informatiques, DSI, Ingénieurs et chefs de projet Sécurité des systèmes d'information.**	Des connaissances en **réseau et système**.

Programme de la formation

Module 1 : Enjeux de la Sécurité des Systèmes d'Information

- Introduction à la Cybersécurité
- Objectifs de la cybersécurité
- Alignement stratégique organisation / cybersécurité
- Sécurité des SI, de l'information, informatique et cybersécurité
- Principes et Critères de sécurité informatique

Module 2 : Activités du RSSI

- Le métier de RSSI
- Missions et responsabilités du RSSI
- Le RSSI dans les projets
- Relations DSI - RSSI - DSSI
- Conformité et réglementation - La Loi 18-07 relative à la protection des données à caractère personnel

Module 3 : Sécurité Défensive et Opérationnelle

A. Sécurité Réseau

- Principes de base du réseau
- Attaques et mesures de protection
- Pare-feu et proxy
- Architecture sécurisée

B. Sécurité Applicative

- Vulnérabilités mémoire
- Vulnérabilités web
- Développement sécurisé

C. Sécurité Système

- Principes de sécurité système
- Contrôle d'accès
- Veille sécurité
- Gestion des mises à jour
- Stratégies de sauvegarde
- Journalisation des événements
- Protection du poste de travail
- Sécurité des équipements mobiles

Module 4 : Système de Management de la Sécurité de l'Information (SMSI)

- Introduction à ISO 27001 (et la suite ISO 2700x)
- Systèmes de management et SMSI
- Processus du SMSI
- Introduction à ISO 27002
- Mise en place du SMSI

Module 5 : Politiques de Sécurité

- Définition des politiques de sécurité
- Politiques spécifiques déclinées
- Rédaction, élaboration et validation des politiques
- Révision des politiques
- Mise en œuvre de la PSSI (Politique de Sécurité des Systèmes d'Information) et des politiques spécifiques

Module 6 : Audit de Sécurité des Systèmes d'Information

- Types d'audits (technique, organisationnel, de conformité, de certification)
- Démarche d'audit (selon ISO 19011)
- Livrables d'audit
- Actions correctives et suivi

Module 7 : Gestion des Risques

- Méthodologies d'appréciation des risques
- Menaces, sources de risques, vulnérabilités
- Identification et valorisation des actifs
- Analyse des risques
- Évaluation du risque
- Traitement des risques (réduction, partage, maintien, refus)

Module 8 : Gestion des Incidents en Sécurité des SI

- Définition d'un incident de sécurité
- Objectifs de la gestion des incidents liés à la SSI
- Démarche de gestion d'un incident

Module 9 : Sensibilisation à la Sécurité des SI

- Objectifs de la sensibilisation
- Programme de sensibilisation
- Moyens de sensibilisation et vecteurs de communication

Formation
Lead Cybersecurity Manager

Description de la Formation
Cette formation vous permettra d'acquérir les **concepts, stratégies, méthodologies et techniques fondamentaux de la cybersécurité**. L'objectif est d'établir et de gérer efficacement un **programme de cybersécurité** solide, basé sur les directives des normes internationales de cybersécurité, notamment la **norme ISO/IEC 27032** et le **cadre de cybersécurité du NIST**.

Objectifs
À l'issue de cette formation, les participants seront capables de :

- **Acquérir des connaissances approfondies** sur les composantes et les opérations d'un programme de Cybersécurité, en conformité avec l'**ISO/IEC 27032** et le cadre de Cybersécurité **NIST**.
- **Expliquer les concepts, stratégies, méthodologies et techniques** nécessaires pour mettre en œuvre et gérer un programme de Cybersécurité.
- **Comprendre la corrélation** entre la norme ISO 27032, le cadre du NIST, ainsi que d'autres normes et cadres pertinents.
- **Soutenir un organisme** dans l'exploitation, la maintenance et l'amélioration continue de son programme de Cybersécurité.
- **Acquérir les compétences** pour conseiller un organisme sur les bonnes pratiques de management de la Cybersécurité.

DURÉE	PUBLIC CONCERNÉ	PRÉREQUIS
5 jours	- **Responsables et dirigeants** impliqués dans la gestion de la cybersécurité. - **Professionnels de la cybersécurité**. - **RSSI, DSI, Ingénieurs, Chefs de projet sécurité**. - **Chefs de projet et consultants en sécurité IT**.	- Connaissances de base de la **sécurité des systèmes d'information**. - Connaissances en **réseau et système**.

Programme de la formation

Module 1 : Initiation à l'Implémentation d'un Programme de Cybersécurité

- Objectifs et structure de la formation.
- Normes et cadres réglementaires.
- Concepts fondamentaux de la Cybersécurité.
- Le programme de Cybersécurité.
- L'organisme et son contexte.
- Gouvernance de la Cybersécurité.

Module 2 : Rôles et Responsabilités en Matière de Cybersécurité

- Définition des rôles et responsabilités en cybersécurité.
- Gestion des biens (assets).

Module 3 : Gestion des Risques, Conception et Architecture de la Sécurité

- Gestion des risques.
- Conception et architecture de la sécurité.
- Les mécanismes d'attaque.

Module 4 : Mesures de Sécurité, Communication, Sensibilisation et Formation

- Mesures de Cybersécurité.
- Communication relative à la Cybersécurité.
- Sensibilisation et formation.

Module 5 : Management des Incidents, Surveillance et Amélioration Continue

- Plan de la continuité d'activité.
- Management des incidents de sécurité de l'information.
- Tests de Cybersécurité.
- Mesure et surveillance des performances et des paramètres en matière de Cybersécurité.
- Amélioration continue.

Formation
CISSP (Certified Information Systems Security Professional)

Description de la Formation
Cette formation prépare à la **Certification CISSP**, couvrant l'intégralité du **CBK (Common Body of Knowledge)**, le tronc commun de connaissances en sécurité défini par ISC2®.
Le CBK englobe les connaissances essentielles en sécurité de l'information, réparties sur **huit domaines clés** :

- Sécurité et Management des Risques
- Sécurité des Assets
- Ingénierie de la Sécurité
- Sécurité des Réseaux et des Communications
- Management des Identités et des Accès
- Évaluation de la Sécurité et Tests
- Sécurité des Opérations
- Sécurité du Développement Logiciel

Objectifs
À l'issue de cette formation, les participants seront capables de :

- **Conseiller une organisation** sur les meilleures pratiques en management de la sécurité de l'information.
- **Maîtriser** les connaissances en sécurité de l'information à travers les huit domaines du CBK.
- **Comprendre** les besoins en sécurité de l'information pour l'ensemble de l'organisation.
- **Acquérir** les compétences nécessaires pour guider une organisation vers l'excellence en management de la sécurité de l'information.
- **Obtenir une reconnaissance internationale** de leurs compétences en sécurité de l'information.
- **Dialoguer efficacement** avec le management pour la mise en œuvre des mesures de sécurité.
- **Appréhender le rôle crucial** du RSSI (Responsable de la Sécurité des Systèmes d'Information) dans l'organisation.

DURÉE	PUBLIC CONCERNÉ	PRÉREQUIS
5 jours	- **DSI, RSSI, Managers, Ingénieurs, Experts Consultants**. - **Auditeurs confirmés, Informaticiens**.	- Expérience dans le domaine des **réseaux et de la sécurité**. - La **compréhension de l'anglais technique** est nécessaire, le support de cours étant en anglais.

Programme de la formation

Module 1 : Sécurité et Management des Risques

- Comprendre et appliquer les concepts de confidentialité, intégrité et disponibilité.
- Appliquer les principes de gouvernance de la sécurité et conformité.
- Comprendre les questions légales et réglementaires globales liées à la sécurité de l'information.
- Comprendre l'éthique professionnelle.
- Développer et implémenter des politiques de sécurité, standards, procédures et directives.
- Comprendre les exigences de continuité d'activité.
- Contribuer aux politiques de sécurité du personnel.
- Comprendre et appliquer les concepts de management des risques et le modèle de menace.
- Intégrer les considérations de risque de sécurité dans la stratégie d'acquisition.
- Établir et gérer la sensibilisation, la formation et l'éducation à la sécurité de l'information.

Module 2 : Sécurité des Assets

- Classification de l'information et support des assets.
- Déterminer et maintenir la propriété.
- Protéger la confidentialité.
- Assurer une rétention appropriée.
- Déterminer les mesures de sécurité des données et établir les exigences de manipulation.

Module 3 : Ingénierie de la Sécurité

- Implémenter et gérer les processus d'ingénierie en utilisant les principes de conception sécurisée.

- Comprendre les concepts fondamentaux des modèles de sécurité.
- Sélectionner les mesures et contre-mesures basées sur les modèles d'évaluation de la sécurité des systèmes.
- Comprendre les capacités de sécurité offertes par les systèmes d'information.
- Évaluer et réduire les vulnérabilités de sécurité des architectures, des conceptions et des solutions.
- Évaluer et réduire les vulnérabilités de sécurité des systèmes web, mobiles et embarqués.
- Appliquer la cryptographie.
- Appliquer les principes de sécurité au site et à la conception de l'installation.
- Concevoir et implémenter la sécurité physique.

Module 4 : Sécurité des Réseaux et des Communications

- Appliquer les principes de conception sécurisée aux architectures réseau.
- Sécuriser les composants réseau.
- Concevoir et établir des canaux de communication sécurisés.
- Prévenir ou limiter les attaques réseau.

Module 5 : Management des Identités et des Accès

- Contrôle d'accès physique et logique aux Assets.
- Gérer l'identification et l'authentification des personnes et des équipements.
- Intégrer l'identité en tant que service et des services d'identité tiers.
- Intégrer et gérer les mécanismes d'autorisation.
- Prévenir ou réduire les attaques au contrôle d'accès.
- Gérer le cycle de vie des identités et le provisioning des accès.

Module 6 : Évaluation de la Sécurité et Tests

- Concevoir et valider les stratégies d'évaluation et de test de sécurité.
- Conduire des tests de mesures de sécurité.
- Collecter les données des processus de sécurité.
- Analyser et reporter les résultats des tests.
- Conduire ou faciliter les audits internes ou tiers.

Module 7 : Sécurité des Opérations

- Comprendre et supporter les investigations ; comprendre les exigences des types d'investigations.
- Réaliser les activités de monitoring et de logging.
- Sécuriser le provisioning des ressources.

- Comprendre et appliquer les concepts fondamentaux de sécurité des opérations.
- Utiliser les techniques de protection de ressources.
- Gérer les incidents.
- Opérer et maintenir des mesures de sécurité préventives.
- Implémenter et supporter le management des patchs et vulnérabilités.
- Comprendre et participer aux processus de gestion des changements.
- Implémenter des stratégies de reprise (continuité d'activité et reprise après sinistre).
- Tester les plans de reprise après sinistre.
- Participer au Plan de Continuité d'Activité et aux exercices.
- Implémenter et manager la sécurité physique.
- Aborder les problèmes de sécurité du personnel.

Module 8 : Sécurité du Développement Logiciel

- Comprendre et appliquer la sécurité dans le cycle de vie de développement logiciel.
- Appliquer les mesures de sécurité dans les environnements de développement.
- Évaluer l'efficacité de la sécurité du logiciel et l'impact de la sécurité du logiciel acquis.