MS CORE
TECHNOLOGIES

CATALOGUE DE FORMATION MS CORE

FORMATIONS

01 SÉCURITÉ MICROSOFT – OUTILS, BONNES PRATIQUES ET ATELIERS PRATIQUES (ATELIERS)

02 MESURES DE SÉCURITÉ ISO/IEC 27001:2022 (ANNEXE A)

03 PRÉPARATION À LA CERTIFICATION ISO 27001 LEAD IMPLEMENTER

04 FORMATION ET SENSIBILISATION À LA SÉCURITÉ DE L’INFORMATION

FORMATION MSC 01

Sécurité Microsoft

OUTILS, BONNES PRATIQUES ET ATELIERS PRATIQUES (ATELIERS)

OBJECTIFS DE LA FORMATION :

- Comprendre l'écosystème de sécurité Microsoft
- Mettre en œuvre concrètement les contrôles de sécurité clés
- Réduire les risques liés aux identités, données, postes et cloud
- Développer l'autonomie des équipes TI et Sécurité
- Aligner la sécurité avec les besoins métiers et réglementaire

PRÉREQUIS :

- Aucun pour modules introductifs
- Notions IT recommandées pour modules avec ateliers techniques

FORMATS PÉDAGOGIQUES

- Présentiel | Virtuel | Hybride
- Théorie + démonstrations + ateliers guidés
- Cas réels inspirés de situations en entreprise
- Supports fournis

FORMATION MSC 01

MODULE 1

INTRODUCTION À LA SÉCURITÉ MICROSOFT

Objectif : Comprendre la vision globale de la sécurité Microsoft.

Contenu :
- Écosystème Microsoft Security
- Modèle Zero Trust
- Responsabilité partagée
- Vue d'ensemble des outils

Durée : 4h
Prix : 100 000 FCFA / personne

MODULE 2

MICROSOFT ENTRA ID – SÉCURITÉ DES IDENTITÉS

Objectif : Protéger les comptes et les accès critiques.

Contenu :
- Identités et authentification
- MFA et accès conditionnel
- Gestion des rôles et privilèges
- Protection contre le vol d'identifiants

ateliers pratiques
- Activation et configuration du MFA
- Création d'une politique d'accès conditionnel
- Simulation d'une connexion bloquée / autorisée
- Analyse des journaux de connexion à risque

Durée : 5h
Prix :150 000 FCFA / personne

MODULE 3

MICROSOFT DEFENDER FOR ENDPOINT

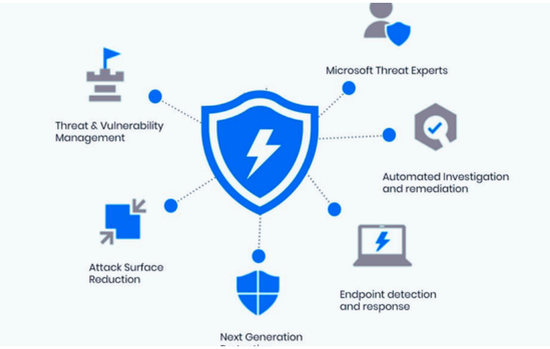
Objectif : Détecter et répondre aux menaces sur les postes.

Contenu :
- Protection anti-malware et ransomware
- Détection comportementale
- Réponse aux incidents

ateliers pratiques
- Onboarding d'un poste dans Defender
- Simulation d'une alerte de sécurité
- Investigation d'un incident
- Isolement d'un poste compromis

Durée : 5h
Prix : 180 000 FCFA/personne

FORMATION MSC 01



MODULE 4

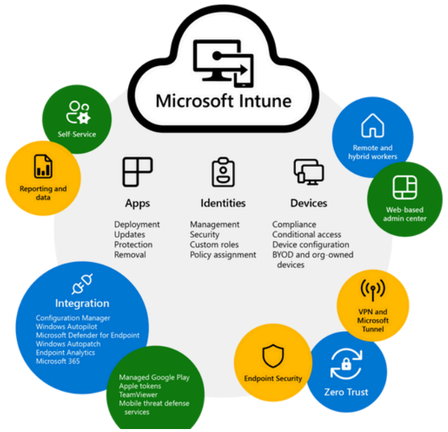
MICROSOFT DEFENDER FOR OFFICE 365

Objectif : Réduire les risques liés aux emails et à la collaboration.

Contenu :
- Hameçonnages, liens et pièces jointes
- Sécurité de SharePoint et Teams

ateliers pratiques
- Configuration des politiques anti-phishing
- Analyse d'un email malveillant
- Simulation d'un clic sur lien suspect
- Consultation des rapports de sécurité

Durée : 5h
Prix : 180 000 FCFA/personne



MODULE 5

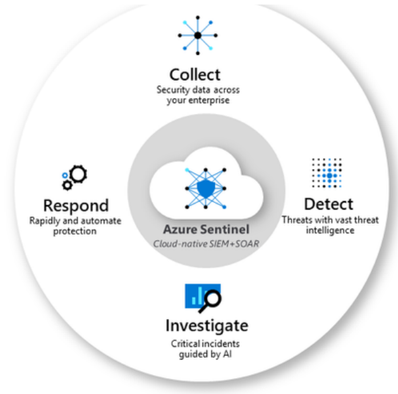
MICROSOFT INTUNE – GESTION ET SÉCURITÉ DES APPAREILS

Objectif : Sécuriser les appareils et le télétravail.

Contenu :
- Gestion des appareils
- Politiques de conformité
- Sécurité BYOD

ateliers pratiques
- Enrôlement d'un appareil
- Création d'une politique de conformité
- Blocage d'un appareil non conforme
- Séparation données professionnelles et personnelles

Durée : 5h
Prix : 180 000 FCFA/personne



MODULE 6

MICROSOFT SENTINEL (SIEM & SOC)

Objectif : Mettre en place une surveillance de sécurité centralisée.

Contenu :
- Fonctionnement d'un SOC
- Collecte des journaux
- Détection et réponse

ateliers pratiques
- Connexion d'une source de logs
- Déploiement d'une règle d'alerte
- Investigation d'un incident
- Création d'un playbook de réponse

Durée : 6h
Prix : 200 000 FCFA/personne

MODULE 7

SÉCURITÉ DES DONNÉES AVEC MICROSOFT PURVIEW

Objectif : Protéger les données sensibles et prévenir les fuites.

Contenu :
- Classification et étiquetage
- DLP et protection de l'information
- Gouvernance des données

ateliers pratiques
- Création d'étiquettes de sensibilité
- Application automatique d'une règle DLP
- Blocage d'un partage non autorisé
- Analyse d'un incident de fuite de données

Durée : 6h
Prix : 250 000 FCFA/personne

MODULE 5

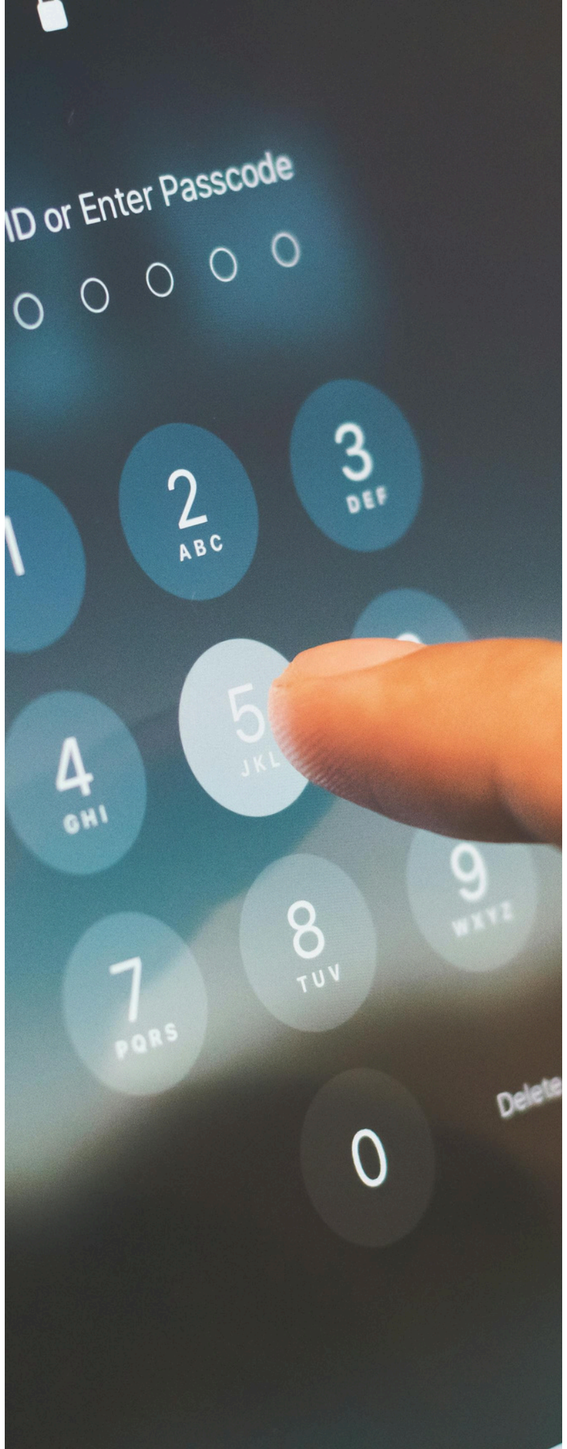
GESTION DE LA POSTURE DE SÉCURITÉ (DEFENDER & SECURE SCORE)

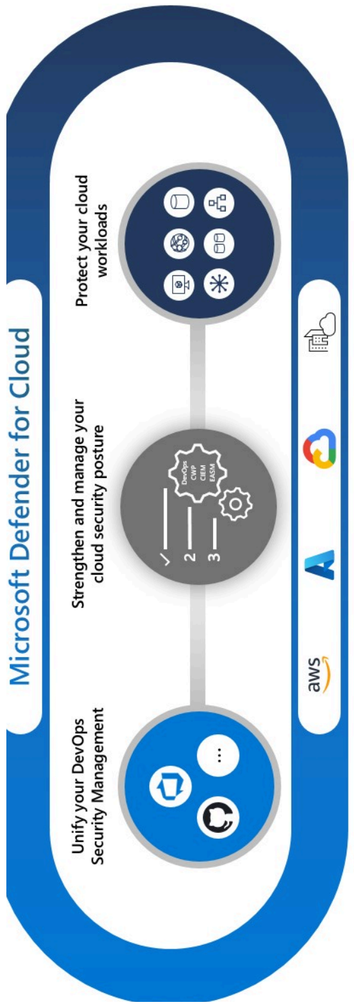
Objectif : Améliorer la posture globale de sécurité.

Contenu :
- Secure Score
- Gestion des vulnérabilités
- Priorisation des risques

ateliers pratiques
- Lecture et analyse du Secure Score
- Application de recommandations
- Suivi de l'amélioration de la posture

Durée : 5h
Prix : 180 000 FCFA/personne





MODULE 9

MICROSOFT DEFENDER FOR CLOUD

Objectif : Renforcer la sécurité des environnements Azure, multicloud et hybrides.

Contenu

- Modèle de responsabilité partagée en environnement Cloud
- Présentation de Defender for Cloud (CSPM & protection des workloads)
- Évaluation continue de la posture de sécurité (Secure Score Cloud)
- Recommandations de sécurité et priorisation des risques
- Protection des ressources :
  - Machines virtuelles
  - Bases de données
  - Conteneurs & Kubernetes
  - Stockage et services PaaS
- Gestion des vulnérabilités et alertes de sécurité

ateliers pratiques

- Activation et configuration de Defender for Cloud
- Analyse du Secure Score Cloud
- Application de recommandations de sécurité
- Détection d'une configuration à risque

Durée : 5h
Prix : 150 000 FCFA/personne

FORFAITS

Économisez jusqu'à 30 % par rapport aux modules individuels

PACK - BASE SÉCURITÉ MICROSOFT

- Module 1 + 2
- Total 9h

200 000 FCFA

PACK-GOUVERNANCE ET CONFORMITÉ

- Module 7 + 8+ 9
- Total 16h

450 000 FCFA

PACK - SÉCURITÉ ET OPÉRATIONS

- Module 3+4+ 5+6
- Total 21h

590 000 FCFA

PACK-ALL-IN SÉCURITÉ MICROSOFT

- Module 1 à 9
- Total 46h

1 150 000 FCFA

Les packs sont fortement recommandés pour une montée en compétence complète et un meilleur retour sur investissement.

FORMATION MSC 02

Mesures de sécurité ISO/IEC 27001:2022 (Annexe A)

OBJECTIFS DE LA FORMATION :
Comprendre et d'appliquer les mesures de sécurité de l'Annexe A de la norme ISO/IEC 27001:2022, en les reliant aux enjeux organisationnels, humains, physiques et technologiques de la sécurité de l'information.
À l'issue de la formation, les participants seront capables de :

- Comprendre la logique et la structure des contrôles ISO/IEC 27001:2022
- Identifier les mesures de sécurité applicables à leur organisation
- Contribuer efficacement à la mise en œuvre d'un SMSI conforme à la norme
- Soutenir les démarches de conformité et de certification ISO 27001

PUBLIC CIBLE

- Directeurs des systèmes d'information (DSI)
- Responsables sécurité de l'information (RSSI)
- Responsables IT et infrastructures
- Auditeurs internes et responsables conformité
- Consultants en cybersécurité

TARIF TOTAL (4 MODULES) :

300 000 FCFA / personne

ÉLÉMENTS INCLUS

- Supports de cours
- Matrice des contrôles ISO/IEC 27001:2022 – Annexe A
- Modèles d'outils (Statement of Applicability – SoA, registre des risques)
- Attestation de formation

MODULE 1

MESURES ORGANISATIONNELLES

Objectif : Ce module aborde les mesures de sécurité liées à la gouvernance de la sécurité de l'information. Il couvre la définition des politiques, la répartition des rôles et responsabilités, la gestion des actifs informationnels, la conformité réglementaire ainsi que la continuité des activités.
L'objectif est d'assurer que la sécurité de l'information est structurée, pilotée et intégrée dans l'ensemble des processus organisationnels.

Prix : Inclus dans le forfait global

MODULE 2

MESURES APPLICABLES AUX PERSONNES

Objectif : Ce module se concentre sur la gestion des risques humains. Il traite des pratiques de recrutement, des obligations contractuelles, de la sensibilisation à la sécurité, des responsabilités des employés et du travail à distance.
Il vise à réduire les risques liés aux erreurs humaines, à la négligence ou aux actes malveillants internes.

Prix : Inclus dans le forfait global

MODULE 3

MESURES DE SÉCURITÉ PHYSIQUES

Objectif : Ce module couvre la protection des locaux, équipements et supports physiques contre les accès non autorisés, les pertes, les vols ou les incidents environnementaux.
Il permet de comprendre comment sécuriser les infrastructures physiques essentielles au traitement et à la conservation de l'information.

Prix : Inclus dans le forfait global

MODULE 4

MESURES TECHNOLOGIQUES

Objectif : Ce module traite des mesures de sécurité appliquées aux systèmes d'information et aux technologies. Il aborde la gestion des accès, l'authentification, la sécurité des postes de travail et serveurs, la protection contre les logiciels malveillants, la gestion des vulnérabilités, la journalisation, la surveillance et les sauvegardes.
L'objectif est de garantir la confidentialité, l'intégrité et la disponibilité des informations.

Prix : Inclus dans le forfait global

FORMATION MSC 03

Préparation à la Certification ISO 27001 Lead Implementer

OBJECTIFS DE LA FORMATION :
Acquisition des connaissances et compétences nécessaires pour planifier, mettre en œuvre, exploiter, surveiller et améliorer un Système de Management de la Sécurité de l'Information (SMSI) conformément aux exigences de la norme ISO/IEC 27001.

PUBLIC CIBLE

- Responsables sécurité de l'information (RSSI)
- Directeurs des systèmes d'information (DSI)
- Responsables conformité, risques et audit
- Chefs de projets SMSI
- Consultants en cybersécurité
- Toute personne impliquée dans la mise en œuvre d'un SMSI

ÉLÉMENTS INCLUS

- Supports de cours
- Attestation de formation

TARIF TOTAL (4 MODULES) :

450 000 FCFA / personne

MODULE 1

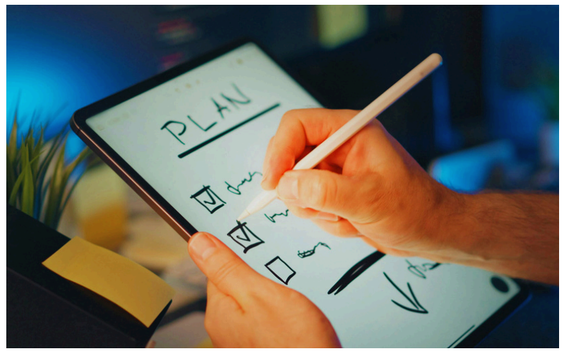
INTRODUCTION À ISO/IEC 27001 ET INITIATION D'UN SMSI

Objectif : Ce module introduit les fondamentaux de la norme ISO/IEC 27001 et les principes clés de la sécurité de l'information. Il permet de comprendre le concept de SMSI, son rôle stratégique et son intégration dans l'organisation.

Contenu :

- Objectifs et structure de la formation
- Normes et cadres réglementaires de la famille ISO 27000
- Concepts et principes fondamentaux de la sécurité de l'information
- Système de management de la sécurité de l'information (SMSI)
- Compréhension de l'organisme et de son contexte
- Analyse du système existant

Prix : Inclus dans le forfait global



MODULE 2

PLANIFICATION DE LA MISE EN ŒUVRE D'UN SMSI

Objectif : Ce module est dédié à la phase de planification du SMSI, en mettant l'accent sur le leadership, la gouvernance et la gestion des risques.

.

Contenu :

- Leadership et engagement de la direction
- Définition du périmètre du SMSI
- Politique de sécurité de l'information
- Processus de gestion des risques de sécurité de l'information
- Structure organisationnelle de la sécurité de l'information
- Déclaration d'applicabilité (SoA) et décision de la direction

Prix : Inclus dans le forfait global

MODULE 3

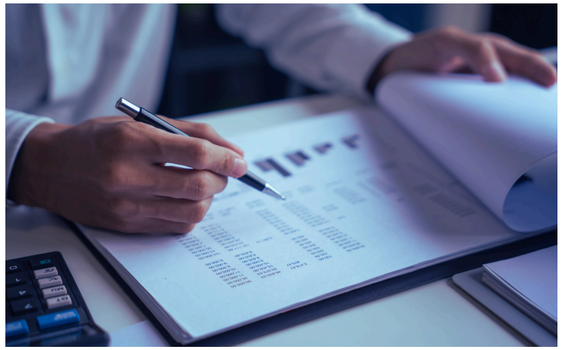
MISE EN ŒUVRE DU SMSI

Objectif : Ce module couvre la mise en œuvre opérationnelle du SMSI, en traduisant les exigences de la norme en actions concrètes.

Contenu :

- Conception des mesures de sécurité
- Rédaction des politiques spécifiques et procédures
- Mise en œuvre des mesures de sécurité
- Gestion des documents et informations documentées
- Plan de communication
- Plan de formation et de sensibilisation
- Gestion des opérations
- Gestion des incidents de sécurité de l'information

Prix : Inclus dans le forfait global



MODULE 4

SURVEILLANCE, AMÉLIORATION CONTINUE ET PRÉPARATION À L'AUDIT

Objectif : Ce module se concentre sur le pilotage du SMSI, la surveillance des performances et la préparation à l'audit de certification.

Contenu :

- Surveillance et mesure du SMSI
- Audit interne du SMSI
- Revue de direction
- Traitement des non-conformités et des problèmes
- Amélioration continue
- Préparation à l'audit de certification
- Processus de certification ISO/IEC 27001

Prix : Inclus dans le forfait global

FORMATION MSC 04

Formation et Sensibilisation à la Sécurité de l'information

OBJECTIFS DE LA FORMATION :

- Réduire les incidents liés au facteur humain
- Développer une culture de cybersécurité
- Améliorer la conformité et la vigilance des employés
- Protéger les données de l'organisation et des clients

PUBLIC CIBLE
Employés, cadres, gestionnaires, équipes administratives, financières, RH, commerciales

AUDIENCE : 1 à 15 employés

TARIF TOTAL (10 MODULES) :
Prix : 400 000 FCFA
Durée : 7 h

FORMAT DES FORMATIONS

- Présentiel | Virtuel | Hybride
- Sessions courtes et interactives
- Cas concrets et scénarios réels
- Langage simple, non technique

FORMATION MSC 04

MODULE 1

SENSIBILISATION GÉNÉRALE À LA SÉCURITÉ DE L'INFORMATION

Objectif : Comprendre les risques et les responsabilités de chacun.

Contenu :

- Pourquoi la cybersécurité concerne tous les employés
- Menaces courantes (hameçonnage, fraude, fuite de données)
- Responsabilités individuelles
- Bonnes pratiques au quotidien

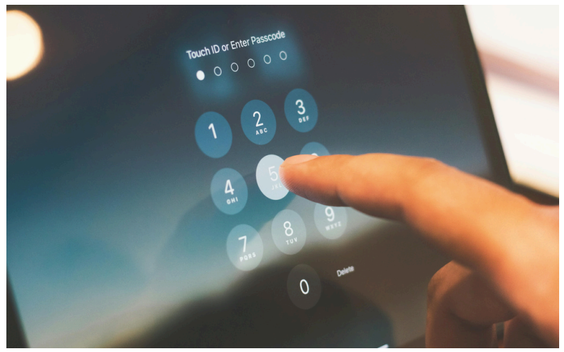
MODULE 2

HAMEÇONNAGE ET INGÉNIERIE SOCIALE

Objectif : Reconnaître et éviter les tentatives de fraude

Contenu :

- Qu'est-ce que l'hameçonnage?
- Emails, SMS, appels frauduleux
- Signes d'alerte concrets
- Que faire en cas de doute ?
- Exercices pratiques et exemples réels



MODULE 3

ÉVITER LES COMPROMISSIONS DE COMPTES

Objectif : Détecter et répondre aux menaces sur les postes.

Contenu :

- Bonnes pratiques de mots de passe
- MFA expliqué simplement
- Risques du partage d'identifiants
- Sécurité des accès professionnels

MODULE 4

PROTECTION DES DONNÉES ET CONFIDENTIALITÉ

Objectif : Prévenir les fuites de données

Contenu :

- Données sensibles : lesquelles et pourquoi
- Bonnes pratiques de manipulation des documents
- Partage interne et externe sécurisé
- Risques liés au cloud et aux emails

MODULE 5

SÉCURITÉ DU POSTE DE TRAVAIL ET DU TÉLÉTRAVAIL

Objectif : Sécuriser l'environnement de travail

Contenu :

- Sécurité du poste informatique
- Télétravail et Wi-Fi public
- Clés USB, imprimantes, documents papier
- Bonnes pratiques au bureau et à domicile

MODULE 6

RÉACTION FACE À UN INCIDENT DE SÉCURITÉ

Objectif : Savoir réagir rapidement et correctement

Contenu :

- Qu'est-ce qu'un incident de sécurité ?
- Que faire (et ne pas faire)
- Qui contacter ?
- Importance du signalement rapide

MODULE 7

SENSIBILISATION DES GESTIONNAIRES ET CADRES

Objectif : Responsabiliser les décideurs non techniques

Contenu :

- Risques cyber pour l'organisation
- Responsabilités légales et managériales
- Décisions à risque
- Rôle des gestionnaires dans la sécurité

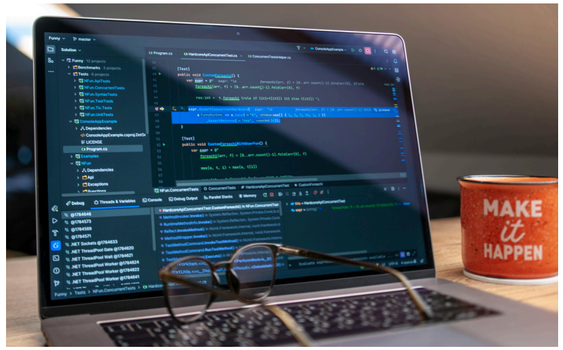
MODULE 8

RISQUES LIÉS À L'INTELLIGENCE ARTIFICIELLE (IA)

Objectif : Sensibiliser les employés aux risques liés à l'utilisation de l'IA

Contenu :

- Qu'est-ce que l'IA générative (en termes simples)
- Exemples d'outils couramment utilisés (chatbots, assistants, générateurs de texte)
- Risques majeurs pour l'organisation :
- Partage involontaire d'informations sensibles
- Perte de confidentialité des données clients
- Utilisation d'outils IA non autorisés
- Dépendance excessive aux réponses de l'IA
- Faux contenus (hallucinations, erreurs)
- Bonnes pratiques d'utilisation responsable de l'IA
- Rôle des employés dans la protection des données face à l'IA



MODULE 9

SENSIBILISATION AUX RANÇONGICIELS (RANSOMWARE)

Objectif : Comprendre ce qu'est un rançongiciel, comment il se propage et comment chaque employé peut contribuer à prévenir une attaque majeure pouvant paralyser l'organisation.

Contenu :

- Qu'est-ce qu'un rançongiciel
- Comment une attaque ransomware démarre
- Conséquences d'une attaque :
- Signes avant-coureurs d'une infection
- Que faire immédiatement en cas de soupçon de ransomware :
- Bonnes pratiques de prévention au quotidien
- Rôle de chaque employé dans la lutte contre les rançongiciels

MODULE 10

PROTECTION DES RENSEIGNEMENTS PERSONNELS

Objectif : Sensibiliser les employés à l'importance de la protection des renseignements personnels afin de prévenir les violations de confidentialité et de respecter les obligations légales et organisationnelles.

Contenu :

- Qu'est-ce qu'un renseignement personnel ? (exemples concrets)
- Différence entre données personnelles, sensibles et confidentielles
- Pourquoi la protection des renseignements personnels est critique
- Situations à risque au quotidien
- Bonnes pratiques de protection
- Rôle de chaque employé dans la protection des renseignements personnels
- Que faire en cas de perte, d'erreur ou de fuite d'informations ?

MS CORE
TECHNOLOGIES

Telephone : +225 05 04 44 01 78

Site web : www.techmscore.com

Mail: info@techmscore.com

Addresse: Abidjan, Port-Bouët, Zone Industrielle de Vridi