# Formation : Protection des informations avec Microsoft Purview

### Introduction à Microsoft Purview

- Vue d’ensemble de Microsoft Purview
- Rôle dans la gouvernance et la conformité des données

### Concepts de sécurité et gouvernance des données

- Définitions clés : confidentialité, intégrité, disponibilité
- Normes de sécurité et exigences de conformité

### Classification et étiquetage des données

- Création de types d’informations sensibles personnalisés
- Création et gestion des étiquettes de sensibilité
- Application manuelle et automatique des étiquettes

### Stratégies de prévention des pertes de données (DLP)

- Comprendre les DLP dans Microsoft 365
- Créer et appliquer des stratégies DLP efficaces
- Surveillance et rapports des violations de données

### Politiques de conservation et de suppression

- Cycle de vie des données
- Création de politiques de rétention
- Gestion des enregistrements

### Gestion des données dans différents environnements

- Environnements cloud (Microsoft 365)
- Intégration sur site et hybrides
- Gestion des données dans les applications SaaS

---

# Formation Certification CISSP –

# Certified Information Systems Security Professional

## Module 1 : Gestion de la sécurité et des risques

- Compréhension des concepts fondamentaux de sécurité
- Gouvernance de la sécurité de l'information
- Conformité légale et réglementaire
- Gestion des risques de sécurité
- Politiques de sécurité, normes et procédures
- Éthique professionnelle (Code de conduite ISC²)

## Module 2 : Sécurité des actifs

- Identification et classification des actifs
- Propriété de l'information et de la responsabilité
- Conservation, protection et gestion des ressources
- Traitement sécurisé des données sensibles

## Module 3 : Architecture et ingénierie de la sécurité

- Concepts de sécurité des systèmes
- Modèles de sécurité et principes de conception
- Sécurité des composants matériels et logiciels
- Mesures de protection contre les vulnérabilités matérielles et logicielles
- Chiffrement et cryptographie appliquée

## Module 4 : Sécurité des réseaux et des communications

- Conception et sécurisation de l'architecture réseau
- Protocoles sécurisés et vulnérabilités réseau
- Dispositifs de sécurité (pare-feux, IDS/IPS, VPN)
- Contrôle de la sécurité des canaux de communication

## Module 5 : Gestion des identités et des accès (IAM)

- Contrôles d'accès physiques et logiques
- Gestion des identités et du cycle de vie des accès
- Mécanismes d'authentification et d'autorisation
- Gestion des privilèges et séparation des tâches

## Module 6 : Évaluation et tests de sécurité

- Conception d'un programme de tests de sécurité
- Tests de vulnérabilités et scans réguliers
- Audits de sécurité internes et externes

- Analyse des résultats et recommandations

### Module 7 : Opérations de sécurité

- Gestion des événements de sécurité
- Réponse aux incidents et gestion de crise
- Plan de continuité des activités et reprise après sinistre
- Gestion des ressources humaines en contexte opérationnel

### Module 8 : Sécurité du développement logiciel

- Intégration de la sécurité dans le SDLC (cycle de vie du développement logiciel)
- Environnements de développement sécurisé
- Contrôles de sécurité applicative
- Tests d'applications et revue de code sécurisée

---

# Formation Lead Pen Test Professional

### Module 1 : Introduction aux tests d'intrusion et planification

- Principes fondamentaux des tests d'intrusion
- Éthique, légalité et conformité dans le pen testing
- Définition du périmètre et des objectifs du test
- Collecte d'informations préliminaires et reconnaissance
- Élaboration du plan de test d'intrusion

### Module 2 : Connaissances techniques fondamentales

- Fonctionnement des réseaux et protocoles
- Systèmes d'exploitation (Linux, Windows)
- Concepts de sécurité et points d'entrée typiques
- Outils essentiels pour les tests (Nmap, Wireshark, Metasploit…)
- Environnement de test : préparation et configuration

### Module 3 : Réalisation pratique du test d'intrusion

- Scanning et analyse des vulnérabilités
- Exploitation des failles (privilege escalation, accès non autorisé, injections…)
- Tests sur les applications Web, infrastructures réseaux, et systèmes
- Attaques sur les services, applications mobiles et IoT

- Techniques d’ingénierie sociale (phishing, pretexting…)

### Module 4 : Analyse, rapport et recommandations

- Organisation et interprétation des résultats
- Rédaction de rapports professionnels de tests d’intrusion
- Proposition de recommandations concrètes
- Présentation des résultats à différents types d’interlocuteurs
- Gestion des actions correctives et suivi post-audit

### Module 5 : Examen de certification

- Révision des modules et questions de mise en situation
- Préparation à l’examen PECB Lead Pen Test Professional
- Passage de l’examen

---

# Formation Certified Ethical Hacker (CEH)

### Module 1 : Introduction à l’éthique du hacking

- Définitions clés et concepts
- Phases du hacking éthique
- Cadres juridiques et conformité

### Module 2 : Reconnaissance passive et active

- Gathering d’information
- OSINT et footprinting
- Utilisation de WHOIS, Google hacking, Maltego, etc.

### Module 3 : Scan et énumération

- Scanning de ports et de vulnérabilités
- Analyse avec Nmap, Netcat, etc.
- Énumération des services et utilisateurs

### Module 4 : Vulnérabilités et hacking système

- Exploitation des systèmes d’exploitation
- Escalade de privilèges
- Rootkits, backdoors et trojans

## Module 5 : Malware et stéganographie

- Types de malwares
- Techniques de dissimulation de données

## Module 6 : Sniffing et attaques réseau

- Analyse de paquets réseau (Wireshark, TCPDump)
- ARP poisoning, MITM
- Contre-mesures

## Module 7 : Hacking Web & Applications

- Failles XSS, CSRF, SQL Injection
- Traversal de répertoire, manipulation d'URL
- Tests avec Burp Suite, OWASP ZAP

## Module 8 : Sécurité mobile et IoT

- Attaques sur Android et iOS
- Sécurité des objets connectés

## Module 9 : Cloud computing & piratage de serveurs

- Vulnérabilités spécifiques au cloud
- Audit de sécurité dans AWS, Azure

## Module 10 : Cryptographie & attaques sur le chiffrement

- Concepts de base : symétrique, asymétrique
- Attaques par force brute, rainbow tables
- Certificats, SSL, TLS

## Module 11 : Ingénierie sociale & techniques de phishing

- Prétexting, baiting, spear phishing
- Techniques d'usurpation d'identité

## Module 12 : Contremesures, logs et couverture de traces

- Effacement des logs système
- Techniques d'obfuscation
- Contre-hacking et prévention

## Module 13 : Préparation à l'examen CEH

- Révisions des modules clés
- Simulations de QCM
- Exercices pratiques

# Formation ISO 31000 Risk Manager – certification

### Jour 1 : Introduction aux concepts et principes du management du risque selon ISO 31000

- Présentation générale de la formation.
- Principes et cadre du management du risque selon ISO 31000.
- Établissement du contexte organisationnel pour le management du risque.

### Jour 2 : Processus de management du risque selon ISO 31000

- Identification, analyse et évaluation des risques.
- Traitement, communication et consultation liés aux risques.
- Surveillance et revue du risque.

### Jour 3 : Techniques d'appréciation du risque et examen de certification

- Présentation des techniques d'appréciation du risque selon ISO/IEC 31010.
- Préparation à l'examen de certification.
- Passage de l'examen de certification « PECB Certified ISO 31000 Risk Manager ».

# Formation ISO/IEC 27005 Risk Manager ( certification)

### Jour 1 : Introduction à la norme ISO/IEC 27005 et à la gestion des risques

- Objectifs et structure de la formation.
- Cadres normatifs et réglementaires.
- Principes et concepts fondamentaux de la gestion des risques liés à la sécurité de l'information.
- Programme de gestion des risques.

- Établissement du contexte.

### Jour 2 : Appréciation des risques, traitement des risques, communication et concertation selon ISO/IEC 27005

- Identification des risques.
- Analyse du risque.
- Évaluation du risque.
- Traitement du risque.
- Évaluation des risques liés à la sécurité de l'information.
- Communication et concertation relatives aux risques liés à la sécurité de l'information.

### Jour 3 : Surveillance, revue et examen de certification

- Surveillance et revue du risque.
- Examen de certification « ISO/IEC 27005 Risk Manager ».

---

# Formation ISO/IEC 27001 Lead Implementer( certification)

### Module 1 : Introduction à ISO/IEC 27001 et initiation de la mise en œuvre d'un SMSI

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Fondements de la sécurité de l'information
- Initiation de la mise en œuvre du SMSI
- Compréhension de l'organisation et de son contexte
- Définition du périmètre du SMSI

### Module 2 : Planification de la mise en œuvre d'un SMSI

- Leadership et approbation du projet
- Structure organisationnelle
- Analyse du système existant
- Politique de sécurité de l'information
- Gestion des risques
- Déclaration d'applicabilité

### Module 3 : Mise en œuvre d'un SMSI

- Sélection et conception des mesures de sécurité

- Mise en œuvre des mesures
- Gestion de l'information documentée
- Tendances et technologies
- Communication
- Compétence et sensibilisation
- Gestion des opérations de sécurité

### Module 4 : Surveillance, amélioration continue et préparation à l'audit de certification du SMSI

- Surveillance, mesure, analyse et évaluation
- Audit interne
- Revue de direction
- Traitement des non-conformités
- Amélioration continue
- Préparation à l'audit de certification
- Clôture de la formation

### Module 5 : Examen de certification

- Test final basé sur les connaissances acquises durant la formation
- Questions à choix multiples
- Préparation à la réussite de l'examen ISO/IEC 27001 Lead Implementer

---

# Formation : ITIL v4 – Gestion des Problèmes

### Module 1 : Introduction à la Gestion des Problèmes selon ITIL® 4

- Définition et rôle stratégique de la gestion des problèmes
- Différence entre incident et problème
- Intégration dans le Système de Valeur des Services (SVS)
- Relations avec les autres pratiques ITIL (Gestion des incidents, Gestion des changements, Gestion de la configuration)

### Module 2 : Fondements et Objectifs de la Gestion des Problèmes

- Comprendre les causes profondes des dysfonctionnements IT
- Importance de la gestion proactive et réactive des problèmes
- Effets sur la qualité des services et la satisfaction des utilisateurs
- Automatisation et innovation dans l'identification des problèmes

## Module 3 : Structurer un Processus Efficace de Gestion des Problèmes

- Étapes clés du cycle de vie d'un problème :
  - Détection et enregistrement
  - Analyse et diagnostic
  - Élaboration d'une solution de contournement
  - Mise en œuvre d'une solution définitive
  - Vérification et clôture
- Utilisation des techniques d'analyse des causes racines (RCA)
- Documentation et gestion des bases de connaissances

## Module 4 : Rôles et Responsabilités des Acteurs Clés

- Rôles impliqués dans la gestion des problèmes :
  - Équipes de support et exploitation
  - Responsable de la gestion des problèmes
  - Experts techniques et architectes IT
  - Fournisseurs et partenaires
- Compétences requises pour gérer efficacement un problème
- Meilleures pratiques pour coordonner les équipes et optimiser la communication

## Module 5 : Apports des Outils et Technologies pour une Meilleure Gestion

- Utilisation des solutions ITSM pour suivre et documenter les problèmes
- Intelligence artificielle et machine learning pour identifier les tendances
- Automatisation de la gestion des problèmes pour réduire les délais de résolution
- Exploitation des bases de connaissances et du partage d'informations

## Module 6 : Collaboration avec les Partenaires et Fournisseurs

- Rôle des partenaires dans la résolution des problèmes complexes
- Intégration des fournisseurs dans le processus de gestion des problèmes
- Alignement des engagements contractuels avec les objectifs de gestion des problèmes
- Responsabilisation et coordination avec un modèle RACI

## Module 7 : Améliorer la Maturité de la Pratique avec ITIL

- Application des quatre dimensions de la gestion des services
- Utilisation du modèle de capacités ITIL pour structurer et faire évoluer la gestion des problèmes
- Identification des écarts entre les processus actuels et les bonnes pratiques ITIL

### Module 8 : Stratégies pour une Gestion des Problèmes Efficace et Pérenne

- Facteurs de succès et meilleures pratiques pour une gestion optimisée
- Méthodes d'amélioration continue et de révision des processus
- Alignement des objectifs de gestion des problèmes avec la stratégie IT globale
- Suivi des indicateurs de performance (KPI) et retour sur expérience

---

# Formation : ITIL v4 – Gestion des Incidents

### Module 1 : Comprendre les Fondamentaux de la Gestion des Incidents

- Définition et importance stratégique de la gestion des incidents
- Différence entre un incident, un problème et une demande de service
- Place de la gestion des incidents dans le Système de Valeur des Services (SVS)
- Interactions avec d'autres pratiques ITIL (Gestion des problèmes, Gestion des changements, Gestion des niveaux de service)

### Module 2 : Objectifs et Défis de la Gestion des Incidents

- Réduction de l'impact des incidents sur la continuité des activités
- Accélération du rétablissement des services impactés
- Amélioration de l'expérience utilisateur et satisfaction des clients internes
- Automatisation et standardisation pour optimiser le traitement des incidents

### Module 3 : Structurer un Processus de Gestion des Incidents Performant

- Étapes clés du cycle de vie d'un incident :
  - Détection et enregistrement
  - Classification et évaluation de la priorité
  - Diagnostic et résolution
  - Clôture et analyse post-incident
- Mise en place de modèles d'incidents standardisés
- Définition des SLA (Service Level Agreements) et engagements de service

## Module 4 : Responsabilités et Rôles Clés dans la Gestion des Incidents

- Acteurs impliqués :
  - Utilisateurs et demandeurs
  - Équipes du Service Desk et support technique
  - Experts techniques et gestionnaires IT
  - Partenaires et fournisseurs
- Compétences requises pour une gestion efficace des incidents
- Bonnes pratiques de coordination et de communication

## Module 5 : Technologies et Outils au Service de la Gestion des Incidents

- Utilisation des solutions ITSM pour le suivi et la gestion des incidents (ServiceNow, BMC, Jira, etc.)
- Apport de l'automatisation et de l'intelligence artificielle pour la détection et la résolution rapide
- Intégration d'un portail utilisateur et d'une base de connaissances
- Analyse des performances avec des tableaux de bord et indicateurs clés (KPIs)

## Module 6 : Gestion des Incidents en Collaboration avec les Partenaires et Fournisseurs

- Intégration des fournisseurs dans le processus de gestion des incidents
- Gestion des escalades et responsabilités contractuelles
- Suivi des engagements externes pour une meilleure continuité de service
- Clarification des responsabilités à travers le modèle RACI

## Module 7 : Renforcer la Maturité de la Gestion des Incidents

- Application des quatre dimensions de la gestion des services ITIL
- Utilisation du modèle de capacités ITIL pour structurer et optimiser la gestion des incidents
- Identification des écarts entre les processus actuels et les bonnes pratiques ITIL
- Intégration d'une approche proactive pour réduire le nombre d'incidents récurrents

## Module 8 : Bonnes Pratiques pour une Gestion des Incidents Durable et Améliorée

- Facteurs clés de succès pour une gestion des incidents optimisée
- Méthodes d'amélioration continue et revue des processus
- Alignement de la gestion des incidents avec les objectifs IT et métier
- Suivi et analyse des KPIs pour assurer une amélioration continue

# Formation ITIL v4 – Centre de Services

## Module 1 : Comprendre le Rôle et les Enjeux du Centre de Services

- Définition et mission d'un Centre de Services selon ITIL 4
- Différences entre Service Desk, Help Desk et Centre d'Assistance
- Place du Centre de Services dans le Système de Valeur des Services (SVS)
- Connexions avec d'autres pratiques ITIL (Gestion des incidents, Gestion des demandes, Gestion des problèmes)

## Module 2 : Objectifs et Stratégies d'un Centre de Services Performant

- Amélioration de l'expérience utilisateur et de la satisfaction client
- Réduction des délais de traitement des tickets et optimisation des ressources
- Passage d'une approche réactive à proactive pour anticiper les besoins des utilisateurs
- Intégration de l'automatisation et du self-service

## Module 3 : Structuration et Déploiement d'un Processus Efficace

- Cycle de vie d'un ticket dans un Centre de Services :
  - Accueil et enregistrement
  - Classification et priorisation
  - Diagnostic et résolution initiale
  - Escalade vers un niveau supérieur si nécessaire
  - Clôture et suivi de la satisfaction utilisateur
- Développement de modèles de tickets standardisés
- Définition des SLA (Service Level Agreements) et attentes des utilisateurs

## Module 4 : Rôles et Responsabilités au sein du Centre de Services

- Acteurs clés et missions :
  - Techniciens et agents du Service Desk
  - Responsable du Centre de Services
  - Experts IT et support de niveau supérieur
  - Gestionnaires ITSM et fournisseurs externes
- Compétences essentielles pour un support efficace
- Bonnes pratiques pour la gestion des interactions avec les utilisateurs

## Module 5 : Outils et Technologies pour Optimiser le Centre de Services

- Présentation des outils ITSM et solutions de gestion des tickets (ServiceNow, BMC Remedy, Freshdesk, etc.)
- Automatisation des réponses avec chatbots et intelligence artificielle
- Déploiement d'un portail utilisateur et base de connaissances pour encourager le self-service
- Analyse des performances avec des tableaux de bord et KPIs

## Module 6 : Gestion de la Collaboration avec les Partenaires et Fournisseurs

- Intégration des partenaires dans le processus de support et d'escalade
- Alignement des engagements contractuels avec les objectifs de gestion des tickets
- Optimisation de la communication entre le Centre de Services et les fournisseurs
- Utilisation du modèle RACI pour clarifier les rôles et responsabilités

## Module 7 : Développer la Maturité du Centre de Services

- Application des quatre dimensions de la gestion des services ITIL
- Utilisation du modèle de capacités ITIL pour structurer et améliorer la gestion du Centre de Services
- Adoption d'une approche centrée sur l'amélioration continue
- Suivi des performances et analyse des retours utilisateurs pour affiner les processus

## Module 8 : Bonnes Pratiques pour une Gestion Durable et Performante

- Facteurs clés de succès pour un Centre de Services efficace
- Développement d'une culture du service et de l'excellence opérationnelle
- Automatisation et intelligence artificielle pour une gestion plus fluide
- Alignement avec la stratégie IT pour maximiser la valeur apportée aux utilisateurs