Certification Microsoft Power BI (PL-300) – Formation de préparation professionnelle

Introduction à Power BI et à la certification PL-300

- Introduction à la formation Power BI
- Rappel sur les fondamentaux Power BI
- Principes et cycle de travail Power BI Desktop
- Comprendre la certification PL-300 et les compétences évaluées
- Identifier les avantages de la certification pour sa carrière
- Connaître le déroulement de la certification
- Se préparer à la certification pour maximiser ses chances de réussite

Préparation et transformation des données

- Se connecter aux données avec Power BI
- Explorer et se connecter aux différentes sources de données
- Choisir le mode de connexion adapté
- Préparer les données dans l'éditeur Power Query
- Transformations dans l'éditeur Power Query
- Créer et utiliser des paramètres dynamiques
- Appliquer des filtres pour cibler les données
- Utiliser le profilage pour vérifier la qualité des données
- Détecter et corriger les erreurs
- Assigner les bons types de données
- Créer des dossiers et organiser les données
- Gérer, fusionner et combiner plusieurs requêtes
- Choisir entre référence ou duplication
- Importer les données préparées dans Power BI
- Atelier pratique : Transformation des données importées
- Supprimer les totaux dans un TCD
- Fusionner les cellules dans un TCD
- Dépivoter les colonnes dans un TCD
- Quiz sur la préparation et la transformation des données

Modélisation des données

- Ajuster les propriétés des tables et colonnes
- Créer un schéma en étoile
- Comprendre les relations et la cardinalité
- Configurer les options de relations
- Gérer un modèle relationnel
- Créer une disposition logique des tables

- Atelier : Créer un modèle en étoile à partir d'un fichier Excel
- Atelier : Gérer un modèle relationnel dans Power BI
- Quiz sur la modélisation des données

Table de temps (Calendrier)

- Pourquoi ajouter une table de temps
- Créer une table de temps en DAX
- Configurer et marquer la table de temps
- Trier les colonnes de date
- Gérer plusieurs colonnes de dates

Langage DAX

- Présentation du DAX
- Différencier mesures et colonnes
- Créer des mesures DAX
- Utiliser la fonction CALCULATE
- Appliquer les fonctions Time Intelligence
- Générer des mesures rapides
- Comprendre les mesures implicites et explicites

Visualisation et analyse

- Principes de la visualisation Power BI
- Créer des visuels : histogrammes, courbes, secteurs, tableaux
- Mise en forme conditionnelle
- Créer une matrice (tableau croisé)
- Créer un rapport : ergonomie et mise en place
- Ajouter des info-bulles personnalisées
- Contrôler les interactions entre les visuels
- Appliquer et personnaliser le tri
- Maîtriser le drill-down avec une hiérarchie temporelle
- Optimiser les rapports pour mobile
- Assurer l'accessibilité des rapports
- Grouper (ajouter des compartiments sur des colonnes)
- Intégrer la fonctionnalité Q&A
- Utiliser les visuels IA
- Détecter les valeurs aberrantes et anomalies
- Interaction entre visuels et personnalisation
- Quiz sur la visualisation et l'analyse des données

Déploiement – Gérer son espace de travail

- Publier ses rapports dans le service Power BI
- Différencier un espace personnel et un espace partagé
- Gérer et attribuer des rôles dans les espaces de travail
- Créer et gérer une application d'espace de travail
- Construire et personnaliser des tableaux de bord

- Abonner des utilisateurs à un rapport
- Mettre en place des alertes
- Promouvoir et certifier du contenu
- Automatiser la mise à jour des modèles sémantiques
- Gérer la sécurité au niveau des lignes avec des groupes d'utilisateurs
- Quiz sur le déploiement et la gestion des ressources

Conclusion

- Synthèse de la formation
- Conseils pour réussir l'examen PL-300
- Quiz final de révision générale

Formation Sentinel : Configurer les opérations de sécurité SIEM avec Microsoft

Introduction à Microsoft Sentinel

- Présentation de Microsoft Sentinel comme solution SIEM
- Architecture et intégration dans Azure

Création et gestion des espaces de travail Sentinel

- Création d'un espace de travail Log Analytics
- Activation de Microsoft Sentinel
- Gestion des autorisations et des ressources

Connexion des services Microsoft

- Connecteurs de données intégrés (Microsoft 365, Azure AD, etc.)
- Configuration des permissions et intégration fluide

Connexion des hôtes Windows

- Collecte des journaux d'événements de sécurité
- Installation et configuration des agents sur les hôtes

Détection des menaces avec Microsoft Sentinel

- Utilisation des règles d'analyse programmées
- Création de requêtes KQL personnalisées
- Gestion des incidents et alertes

Automatisation de la réponse aux incidents

- Création de playbooks avec Logic Apps
- Déclencheurs et actions automatisées
- Cas pratiques de réponses automatisées

Bonnes pratiques et supervision continue

- Surveillance proactive et tableaux de bord
- Optimisation de la détection et réduction des faux positifs
- Intégration avec d'autres outils de sécurité

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 Lead Cybersecurity Manager (certification)

Jour 1 : Concepts fondamentaux de la cybersécurité

- Introduction à la cybersécurité et à son importance dans le contexte actuel.
- Terminologie et concepts clés.
- Cadres et normes internationaux en cybersécurité.

Jour 2 : Gouvernance de la cybersécurité et gestion des risques

- Établissement d’un programme de cybersécurité.
- Gouvernance et leadership en cybersécurité.
- Identification et évaluation des risques liés à la cybersécurité.

Jour 3 : Sélection et mise en œuvre des contrôles de cybersécurité

- Définition des contrôles de sécurité appropriés.
- Mise en œuvre des mesures de sécurité techniques et organisationnelles.
- Intégration des contrôles de sécurité dans les processus métier.

Jour 4 : Communication, formation et gestion des incidents

- Élaboration de programmes de sensibilisation et de formation à la cybersécurité.
- Communication efficace des politiques et procédures de sécurité.
- Gestion des incidents de cybersécurité et planification de la continuité des activités.

Jour 5 : Amélioration continue et examen de certification

- Surveillance et mesure de la performance du programme de cybersécurité.
- Processus d'amélioration continue.
- Préparation à l'examen et passage de l'examen de certification « PECB Certified Lead Cybersecurity Manager ».

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 27002 Lead Manager(certification)

Jour 1 : Introduction à la norme ISO/IEC 27002

- Présentation des concepts fondamentaux de la sécurité de l'information.
- Vue d'ensemble de la norme ISO/IEC 27002 et de ses objectifs.
- Compréhension de la structure et des domaines couverts par la norme.

Jour 2 : Rôles et responsabilités en matière de sécurité de

l’information, mesures relatives aux personnes et mesures physiques

- Définition des rôles et responsabilités en matière de sécurité de l’information.
- Mesures de sécurité liées aux ressources humaines.
- Mesures de sécurité physique pour la protection des actifs informationnels.

Jour 3 : Actifs de sécurité de l’information, contrôles d’accès et protection des systèmes et réseaux d’information

- Identification et classification des actifs informationnels.
- Implémentation des contrôles d’accès adaptés.
- Mesures de protection pour les systèmes et réseaux d’information.

Jour 4 : Gestion des incidents de sécurité de l’information et test et surveillance des mesures de sécurité de l’information

- Processus de gestion des incidents de sécurité de l’information.
- Techniques de test et de surveillance des mesures de sécurité.
- Approches pour l’amélioration continue des mesures de sécurité.

Jour 5 : Examen de certification

- Révision des concepts clés abordés durant la formation.
- Passage de l’examen de certification « PECB Certified ISO/IEC 27002 Lead Manager ».