Formation: Migration vers le Cloud des Infrastructures de Télécommunications

Module 1 : Introduction à la migration vers le cloud

- Tendances et enjeux dans les télécommunications
- Différences entre cloud public, privé et hybride
- Concepts clés : virtualisation, conteneurs, microservices
- Rôle du cloud dans la 5G et les télécoms de nouvelle génération

Module 2 : Architectures cloud pour les télécommunications

- NFV (Network Function Virtualization)
- SDN (Software Defined Networking)
- MEC (Multi-Access Edge Computing)
- Étude des principaux fournisseurs (AWS, Azure, GCP, OpenStack)

Module 3 : Étapes et méthodologie de migration

- Analyse des infrastructures existantes
- Évaluation des charges de travail et dépendances
- Modèles de migration (lift & shift, re-platforming, refactoring)
- Planification et gouvernance de projet

Module 4 : Sécurité, conformité et SLA

- Gestion de la cybersécurité dans le cloud
- Normes et réglementations (ISO, GDPR, CRTC, etc.)
- Continuité des opérations et reprise après sinistre
- Gestion de la qualité de service et SLA

Module 5 : Intégration et interopérabilité

- Connectivité entre réseaux traditionnels et cloud
- API, orchestration et automatisation
- Gestion multi-cloud et interopérabilité

Module 6 : Études de cas et ateliers pratiques

- Exemple de migration d’un core réseau vers le cloud
- Déploiement d’une fonction réseau virtualisée (ex. VoIP, pare-feu)
- Simulation d’un plan de migration
- Analyse de cas réels de migration réussie

Module 7 : Gestion du changement et adoption

- Accompagnement des équipes techniques
- Optimisation des coûts et du modèle économique
- Bonnes pratiques de monitoring et gestion post-migration

Crystal Reports ou Power BI : quelle solution pour votre reporting structuré ?

Depuis plus de deux décennies, **Crystal Reports** s'est imposé comme une solution puissante pour produire des rapports d'entreprise précis, détaillés et personnalisables. Utilisé dans de nombreux secteurs, il reste aujourd'hui une référence solide pour le **reporting structuré basé sur des données fiables**.

Mais avec l'évolution des outils de visualisation et l'arrivée de solutions cloud, de nouvelles options émergent pour répondre aux besoins actuels des entreprises, notamment en matière d'analyse dynamique, de collaboration et de mobilité.

Pourquoi envisager une solution complémentaire ou alternative ?

Crystal Reports excelle dans la génération de documents structurés, tels que :

- États financiers
- Rapports d’exploitation
- Documents réglementaires

Toutefois, certaines organisations recherchent aujourd’hui des outils offrant :

- Un partage rapide dans le cloud
- Des tableaux de bord interactifs
- Une analyse visuelle en temps réel

C’est dans ce contexte que des solutions comme **Microsoft Power BI** s’imposent comme **une alternative moderne et complémentaire**.

Power BI : une réponse aux nouveaux besoins d’analyse

Développé par Microsoft, Power BI est une solution de **Business Intelligence** conçue pour rendre les données accessibles et compréhensibles, tant pour les analystes que pour les décideurs.

Avantages de Power BI :

- Interface intuitive avec glisser-déposer
- Tableaux de bord dynamiques et interactifs
- Connectivité native avec Excel, SharePoint, SQL Server, etc.
- Partage facile en ligne via Power BI Service
- Modélisation de données avec Power Query et DAX

Crystal Reports + Power BI : une combinaison gagnante

Plutôt que d'opposer les deux outils, de nombreuses entreprises choisissent de les **utiliser de façon complémentaire** :

- Crystal Reports pour les rapports imprimables et normés
- Power BI pour la visualisation en temps réel et le pilotage interactif

Cette synergie permet de tirer le meilleur parti de vos données, selon les besoins métier.

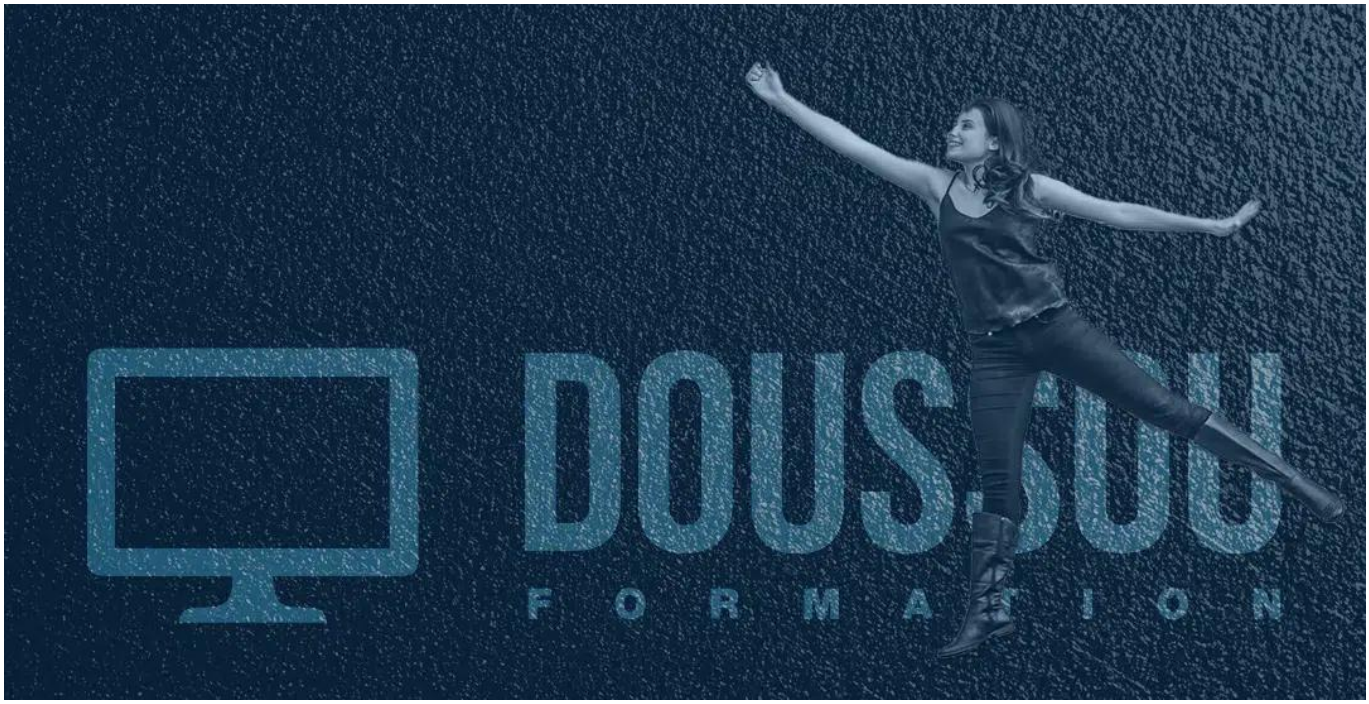
Formation et accompagnement

Chez **Doussou Formation**, nous proposons des formations professionnelles adaptées :

- **Crystal Reports** : pour maîtriser la conception de rapports structurés
- **Power BI** : pour créer des tableaux de bord modernes et interactifs

Nos formations sont offertes en ligne ou en présentiel, et adaptées aux besoins des professionnels de la donnée.

Conclusion



Crystal Reports reste un pilier du reporting structuré. Pour les entreprises qui souhaitent enrichir leurs capacités d'analyse et collaborer plus efficacement, **Power BI représente une alternative moderne, complémentaire et puissante**.

En combinant les deux outils, vous optimisez vos processus de décision et exploitez vos données à leur plein potentiel.

Formation Python: la plus complète

Introduction à Python

- Installer Python et un éditeur (VS Code, Jupyter…)
- Découvrir la console interactive et les scripts
- Créer son premier script Python

Syntaxe et fondamentaux

- Types de données (int, float, str, bool)
- Variables et typage dynamique
- Opérations arithmétiques et logiques
- Conditions (if, elif, else)
- Boucles (for, while) et itérations
- Fonctions (définition, paramètres, retour)
- Introduction au typage statique avec type hints

Manipulation de chaînes de caractères et de fichiers

- Opérations sur les chaînes de caractères
- Lecture et écriture de fichiers avec with open()
- Manipulation de fichiers CSV
- Introduction au format JSON

Structures de données

- Listes, tuples, ensembles, dictionnaires
- Parcours et filtrage avec list comprehension
- Fonctions lambda, map, filter, zip
- Tri et recherche dans les structures

Gestion des erreurs et exceptions

- Comprendre les types d'erreurs (SyntaxError, ValueError…)
- Utiliser try / except / finally
- Lever des exceptions personnalisées
- Bonnes pratiques de gestion d'erreurs

Programmation modulaire

- Créer et utiliser des modules
- Importer avec import et from
- Découverte des modules standards utiles (os, datetime, pathlib, etc.)

Programmation orientée objet (POO)

- Créer une classe, instancier des objets
- Encapsulation, héritage, polymorphisme
- Constructeurs et méthodes spéciales (__init__, __str__…)
- Introduction aux dataclasses

Interaction avec des bases de données

- Connexion à SQLite avec sqlite3
- Lire, insérer, mettre à jour et supprimer des données
- Introduction à SQLAlchemy (ORM moderne)

Travailler avec des API Web

- Requêtes HTTP avec requests
- Consommer une API REST (GET, POST…)
- Analyse des réponses JSON

Développement Web avec Flask

- Principes de base de Flask
- Création d'un serveur REST simple
- Routage et gestion des requêtes

- Tester une API avec Postman ou curl

Tests automatisés avec Pytest

- Écrire des tests unitaires avec pytest
- Asserts, organisation des fichiers de test
- Exécuter les tests et interpréter les résultats

Initiation à la manipulation de données

- Introduction à NumPy et Pandas
- Lire des fichiers CSV avec Pandas
- Filtrer, grouper et résumer des données
- Création de DataFrames à partir de données JSON ou SQL

Rétro-Ingénierie des Logiciels Malveillants

Introduction

- Rappels sur les bonnes pratiques d'investigation numérique
- Présentation des différentes familles de malwares
- Vecteurs d'infection
- Mécanismes de persistance et de propagation

Laboratoire d'Analyse

- Laboratoire virtuel vs. physique
  - Avantages de la virtualisation
  - Solutions de virtualisation
- Ségrégation des réseaux
  - Réseaux virtuels et réseaux partagés
  - Confinement des machines virtuelles
  - Précautions et bonnes pratiques

Supervision de l'Activité d'une Machine

- Réseau
- Système de fichiers
- Registre
- Services

Initiation à l'Analyse Comportementale

- Variété des systèmes

Mise en Place d'un Écosystème d'Analyse Comportementale

- Configuration de l'écosystème
- Définition des configurations types
- Virtualisation des machines invitées
  - VMware
  - VirtualBox
- Installation de CAPEv2 et VirtualBox

Mise en Pratique

- Soumission d'un malware
- Déroulement de l'analyse
- Analyse des résultats et mise en forme

Amélioration via API

- Possibilités de développement et d'améliorations

Analyse Dynamique de Logiciels Malveillants

- Précautions
  - Intervention en machine virtuelle
  - Configuration réseau
- Outils d'analyse
  - OllyDbg
  - Immunity Debugger
- Analyse sous débogueur
  - Step into / Step over
  - Points d'arrêt logiciels et matériels
  - Fonctions systèmes à surveiller
  - Génération pseudo-aléatoire de noms de domaines (C&C)
  - Bonnes pratiques d'analyse
- Mécanismes d'anti-analyse
  - Détection de débogueur
  - Détection d'outils de rétro-ingénierie
  - Exploitation de failles système

Analyse de Documents Malveillants

- Fichiers PDF
  - Introduction au format PDF
  - Spécificités
  - Intégration de JavaScript et possibilités
  - Exemples de PDF malveillants
  - Outils d'analyse : OLE Tools, éditeur hexadécimal

    - Extraction et analyse de la charge
- Fichiers Office (DOC/DOCX)
    - Introduction aux formats DOC/DOCX
    - Spécificités
    - Macros
    - Objets Linking and Embedding (OLE)
    - Outils d’analyse : OLE Tools, éditeur hexadécimal
    - Extraction de code malveillant et analyse
- Fichiers APK
    - Introduction au format APK
    - Outils d’analyse : jadx, Frida, Genymotion, MobSF
    - Contournement des protections d’émulation
    - Compréhension du fonctionnement des applications

Découvrez aussi nos autres formations en cybersécurité et en informatique :

- Formation Cybersécurité – Sécurité informatique
- Formation Ethical Hacking et Tests d’intrusion
- Toutes nos formations en informatique

Pour en savoir plus sur la rétro-ingénierie, consultez la ressource suivante :

Qu’est-ce que la rétro-ingénierie ? – Wikipédia

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 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 ».