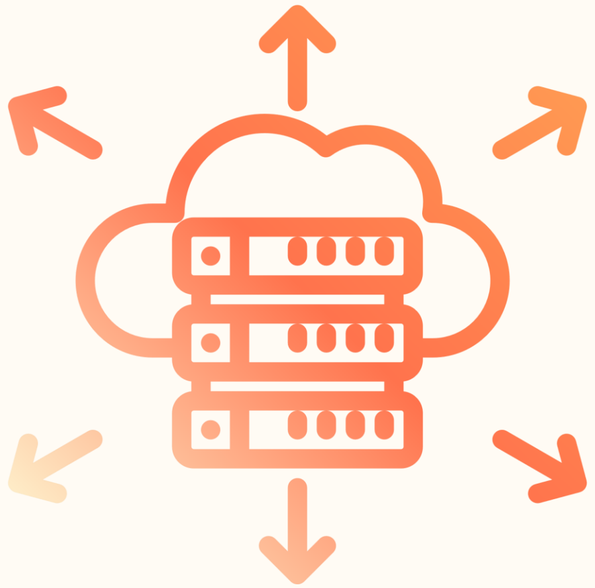
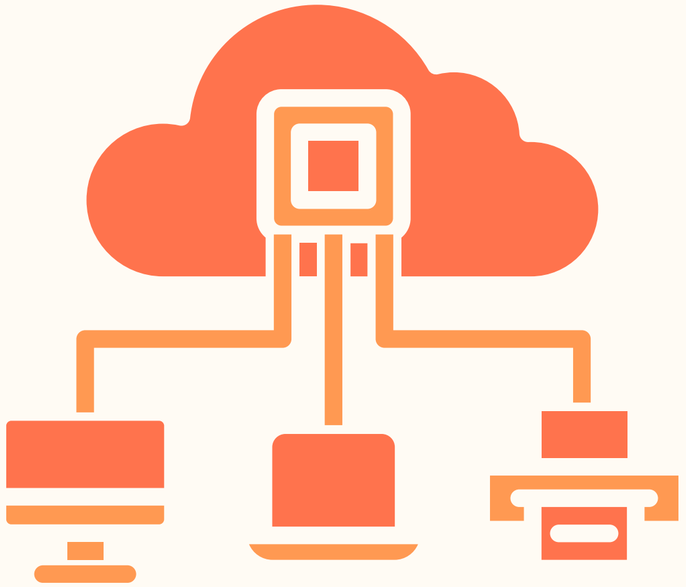
ARCHITECTURE
CLOUD ET HYBRIDES

Intervenant : Nathan VIDAL FAGES

PRÉSENTATION DU MODULE

- Chapitre 1 : Introduction aux architectures Cloud et hybrides
- Chapitre 2 : Gestion des risques liés aux architectures Cloud et hybrides
- Chapitre 3 : Stratégies de protection des données en environnement Cloud
- Chapitre 4 : Stratégies de protection des applications en environnement Cloud
- Chapitre 5 : Mise en pratique à travers des études de cas





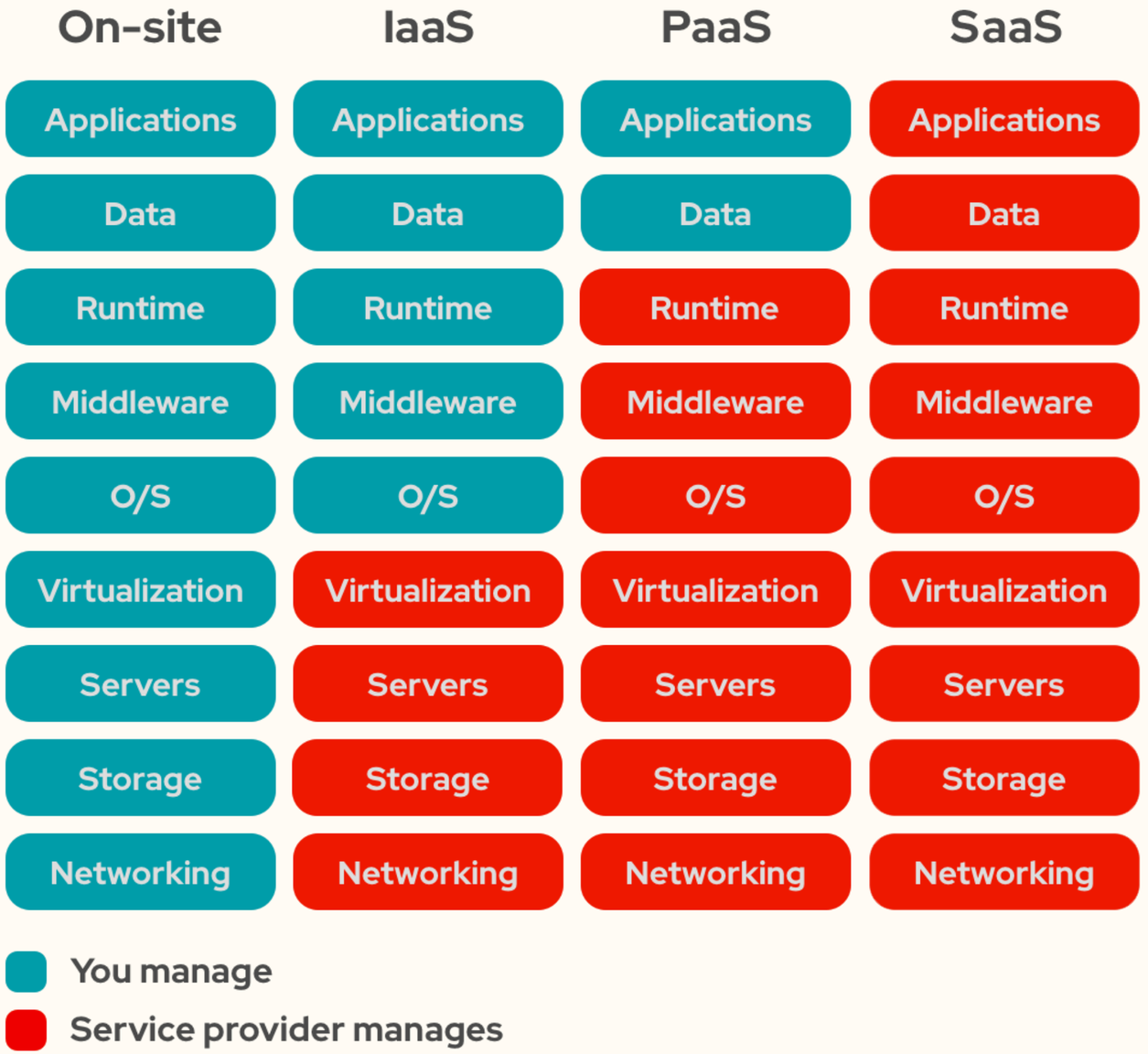
CHAPITRE 1 :

INTRODUCTION AUX ARCHITECTURES CLOUD ET HYBRIDES

DÉFINITION DU CLOUD COMPUTING

MODÈLES DE SERVICES

DÉFINITION DU CLOUD COMPUTING



EVERYTHING AS A SERVICE (XAAS)

MODÈLES DE SERVICES

- **DESKTOP AS A SERVICE (DaaS)**
  Externalisation d'une solution VDI (Virtual Desktop Infrastructure) dans le Cloud, où l'utilisateur peut accéder directement à un bureau virtuel à distance (une session sur un système d'exploitation).

- **COMMUNICATIONS AS A SERVICE (CAAS)**
  Modèle qui fait référence aux services de communication basés sur Internet (téléphonie par Internet, visioconférence, etc.)

- **DATABASE AS A SERVICE (DBAAS)**
  Référence à la mise à disposition d'un système de bases de données via le Cloud

- **VPN AS A SERVICE (VPNAAS)**
  Lorsque le VPN est proposé sous la forme d'un service

- **RANSOMWARE AS A SERVICE (RAAS)**
  Référence à un modèle utilisé par les cybercriminels qui offrent la possibilité de louer un logiciel malveillant de type ransomware et toute l'infrastructure associée.

MODÈLES DE DÉPLOIEMENT

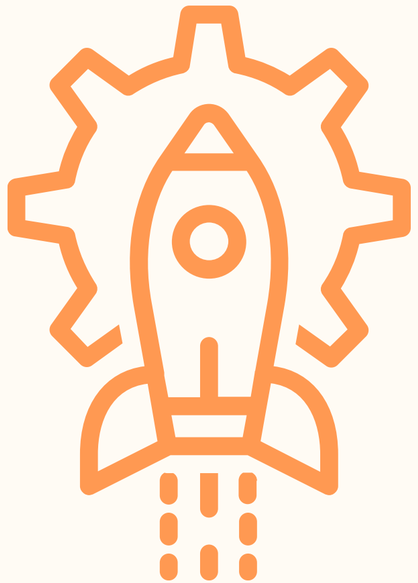
MODÈLES DE SERVICES

- **CLOUD PUBLIC**
  Ressources partagées, opérées par un fournisseur tiers (AWS, Azure, OVH).

- **CLOUD PRIVÉ**
  Infrastructure dédiée, interne ou hébergée (VMware, OpenStack).

- **CLOUD HYBRIDE**
  Combinaison des deux, permettant flexibilité et optimisation.

- **MULTICLOUD**
  Utilisation de plusieurs fournisseurs pour éviter le verrouillage et augmenter la résilience.



CAS PRATIQUE

CARTE MENTALE AVANTAGES / DÉFIS

OBJECTIF

IDENTIFIER COLLECTIVEMENT LES AVANTAGES/DÉFIS DU CLOUD.

DÉROULÉ - GROUPES DE 5 ÉTUDIANTS

- SUR UNE FEUILLE / TABLEAU COLLABORATIF, DESSINER UNE CARTE AVEC DEUX BRANCHES :

  AVANTAGES DU CLOUD

  DÉFIS / RISQUES DU CLOUD

CHAQUE GROUPE DOIT TROUVER AU MOINS 5 AVANTAGES ET 5 DÉFIS.

20 MIN

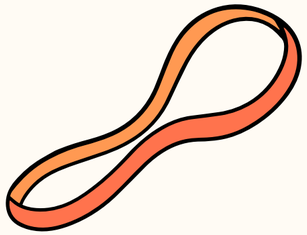
ANALYSE EN GROUPE

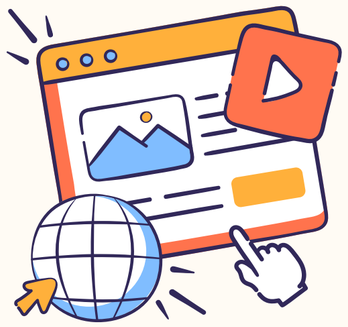
CHAQUE GROUPE PARTAGE 2 AVANTAGES + 2 DÉFIS → COMPILATION EN TABLEAU COMMUN

AVANTAGES ET DÉFIS DU CLOUD

1

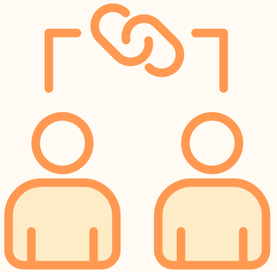
AVANTAGES





2

DÉFIS



LES GRANDS ACTEURS DU MARCHÉ

ENJEUX DE SÉCURITÉ SPÉCIFIQUES

MODÈLE DE RESPONSABILITÉ PARTAGÉE

- FOURNISSEUR CLOUD
- CLIENT

PRINCIPAUX ENJEUX

- PROTECTION DES DONNÉES
- GESTION DES IDENTITÉS ET DES ACCÈS
- SURVEILLANCE ET DÉTECTION
- PLAN DE CONTINUITÉ ET REPRISE D'ACTIVITÉ

QUIZZ

VRAI / FAUX

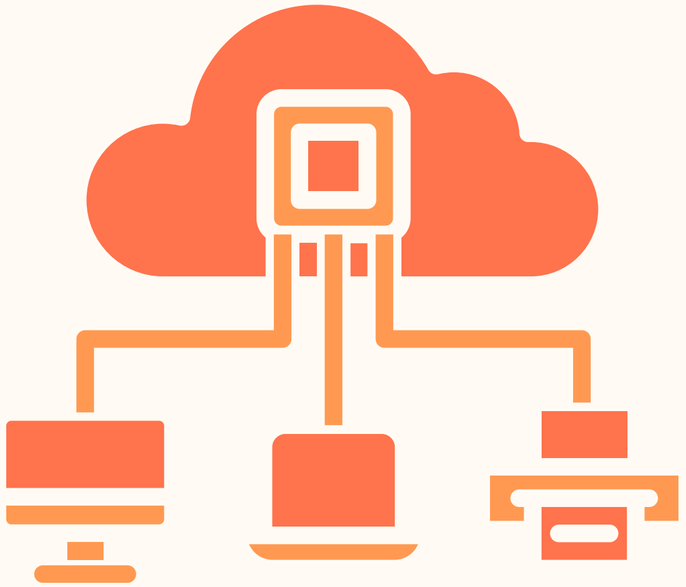
- ✓ GOOGLE DRIVE EST UN SERVICE SAAS
- ✗ AMAZON EC2 EST UN SERVICE PAAS.
- ✓ LE CLOUD HYBRIDE COMBINE CLOUD PRIVÉ ET CLOUD PUBLIC.
- ✓ NETFLIX REPOSE SUR AWS.
- ✗ DROPBOX EST UN SERVICE IAAS.
- ✗ UN CLOUD PRIVÉ EST TOUJOURS PLUS SÉCURISÉ QU'UN CLOUD PUBLIC.
- ✗ AVEC LE CLOUD, LA SÉCURITÉ EST 100% GÉRÉE PAR LE FOURNISSEUR.
- ✓ MICROSOFT AZURE EST SURTOUT UTILISÉ POUR LES ENVIRONNEMENTS HYBRIDES.
- ✗ LE CLOUD SUPPRIME TOTALEMENT LE RISQUE DE PERTE DE DONNÉES.
- ✓ SPOTIFY EST UN EXEMPLE DE SAAS.
- ✓ LE MULTICLOUD CONSISTE À UTILISER PLUSIEURS FOURNISSEURS CLOUD POUR UN MÊME SI.
- ✗ SALESFORCE EST UN EXEMPLE DE PAAS

CONCLUSION

- LE CLOUD OFFRE DE NOMBREUX AVANTAGES MAIS NÉCESSITE UNE MAÎTRISE DES MODÈLES DE SERVICE ET DE DÉPLOIEMENT.

- LA **SÉCURITÉ N'EST PAS EXTERNALISÉE** : LE CLIENT CONSERVE DES RESPONSABILITÉS CLÉS.

- LA COMPRÉHENSION DE CES ENJEUX EST ESSENTIELLE AVANT D'ABORDER LA **GESTION PROACTIVE DES RISQUES**.



CHAPITRE 2 :

GESTION DES RISQUES LIÉS AUX ARCHITECTURES CLOUD ET HYBRIDES

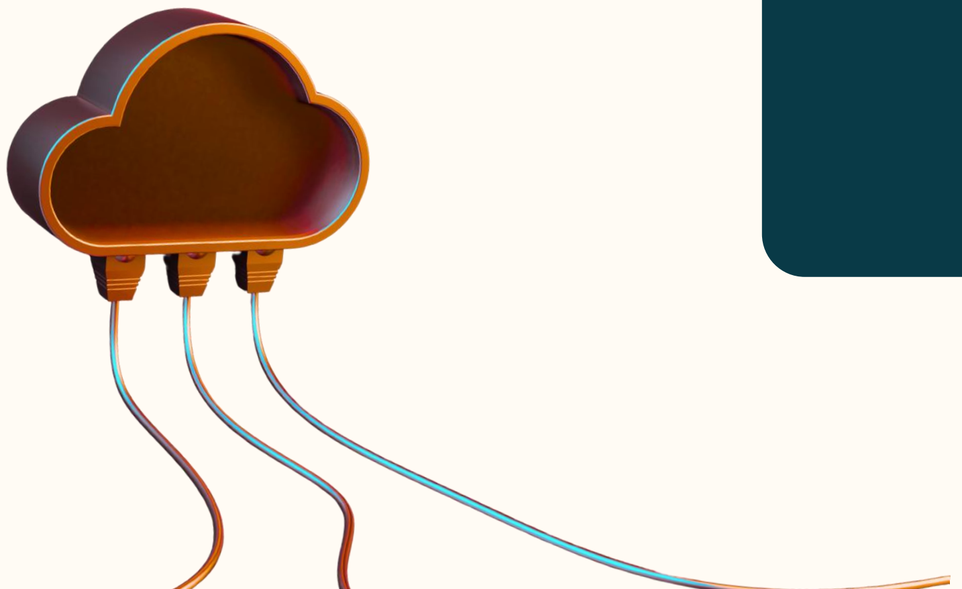
1.INTRODUCTION À LA GESTION DES RISQUES (CONCEPTS CLÉS)

DÉFINITION DU RISQUE

DIFFÉRENCES ENTRE SI CLASSIQUE ET SI CLOUD

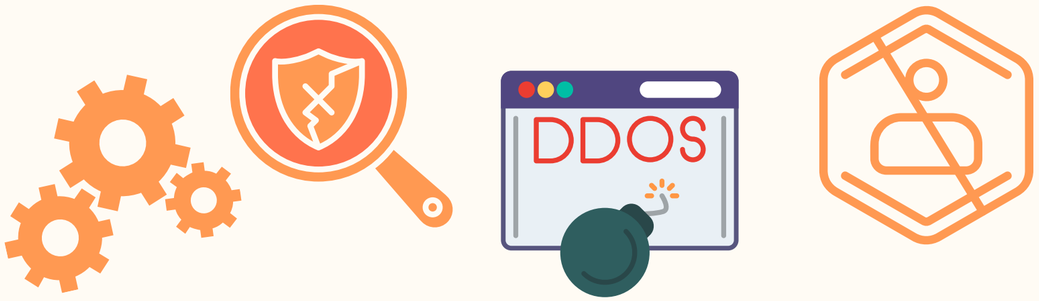
DÉFINITION DU RISQUE

DIFFÉRENCES ENTRE SI CLASSIQUE ET SI CLOUD



2. TYPOLOGIE DES RISQUES SPÉCIFIQUES AU CLOUD

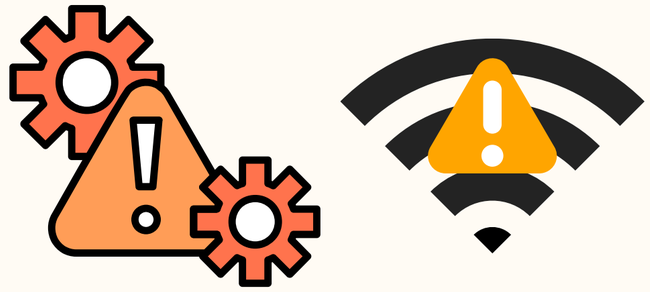
1 TECHNIQUES



2 ORGANISATIONNEL

3 CONTRACTUELS / JURIDIQUE

4 OPÉRATIONNELS



3. ÉVALUATION DE L'IMPACT DES RISQUES

MÉTHODOLOGIE SIMPLE (UTILISABLE EN COURS)

- IDENTIFIER LES RISQUES.
- DÉTERMINER LEUR PROBABILITÉ (FAIBLE, MOYENNE, FORTE).
- DÉTERMINER LEUR IMPACT (FAIBLE, MOYEN, FORT).
- COMBINER POUR OBTENIR UN NIVEAU DE CRITICITÉ.

MÉTHODES AVANCÉES

- EBIOS RISK MANAGER (ANSSI) / ISO 27005 / FAIR

EXERCICE

40 MIN

ANALYSE EN GROUPE

MATRICE DE CRITICITÉ

OBJECTIF

- LISTE DE RISQUES : FUITE S3, PANNE AZURE RÉGIONALE, PIRATAGE COMPTE ADMIN, SHADOW IT, DDOS
- CHAQUE GROUPE DOIT PLACER CES RISQUES DANS UNE MATRICE 2×2 (PROBABILITÉ FAIBLE/FORTE × IMPACT FAIBLE/FORT).
- EXPLIQUER UN CHOIX “CRITIQUE” ET COMMENT Y RÉPONDRE.

LIVRABLE ATTENDU

- MATRICE DES RISQUES SUR FEUILLE / MAIL : esn@vidalfages.fr

4. MESURES DE PRÉVENTION ET DE DÉTECTION

PRÉVENTION

DÉTECTION

CORRECTION
ET RÉPONSE

5. GOUVERNANCE ET CONFORMITÉ

RÈGLEMENTATIONS

SecNumCloud

NORMES & CERTIFICATIONS

Information Security Management System ISO 27001 Certified

Information Security Management ISO 27017 Certified

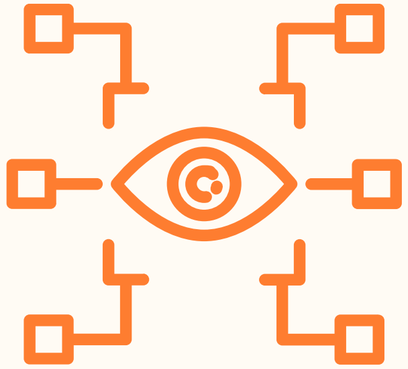
Information Security Management System ISO 27018 Certified

SOC 2

ENJEUX DE SÉCURITÉ SPÉCIFIQUES

- MODÈLE DE RESPONSABILITÉ PARTAGÉE
- PRINCIPAUX ENJEUX

6. APPROCHE PROACTIVE



45 MIN

ANALYSE EN GROUPE

CAS PRATIQUE 1

SCÉNARIO

UNE ENTREPRISE A MIGRÉ UNE PARTIE DE SON SI VERS AZURE (CRM + ERP). ELLE CONSERVE UN DATACENTER INTERNE (HYBRIDE).

- UN BUCKET DE STOCKAGE CONTIENT DES DONNÉES INTERNES SENSIBLES.

TRAVAIL DEMANDÉ (EN SOUS-GROUPES)

- IDENTIFIER LES RISQUES CONCRETS LIÉS À CETTE APPLICATION.
- ÉVALUER LEUR CRITICITÉ
- PROPOSER UNE MESURE DE PRÉVENTION
- PROPOSER UNE MESURE DE DÉTECTION
- DÉCRIRE UNE RÉPONSE EN CAS DE FUITE CONFIRMÉE.

RESTITUTION SUR FEUILLE / MAIL : esn@vidalfages.fr

45 MIN

ANALYSE DE GROUPE

CAS PRATIQUE 2

“LA BASE DE DONNÉE ACCESSIBLE EN PUBLIQUE”

SCÉNARIO

UNE START-UP UTILISE UNE BASE DE DONNEE SAAS POUR SON SITE E-COMMERCE AVEC COMME DONNEES:

- IMAGES PRODUITS (NON SENSIBLES).
- LOGS CLIENTS (EMAILS, NUMÉROS DE CARTE PARTIELS).

TRAVAIL DEMANDÉ (EN SOUS-GROUPES)

- IDENTIFIER LES RISQUES CONCRETS LIÉS À CETTE APPLICATION.
- ÉVALUER LEUR CRITICITÉ
- PROPOSER UNE MESURE DE PRÉVENTION
- PROPOSER UNE MESURE DE DÉTECTION
- DÉCRIRE UNE RÉPONSE EN CAS DE FUITE CONFIRMÉE.

RESTITUTION SUR FEUILLE / MAIL : esn@vidalfages.fr

CONCLUSION

- LA GESTION DES RISQUES CLOUD EST MULTIDIMENSIONNELLE (TECHNIQUE, ORGANISATIONNELLE, JURIDIQUE).
- PRÉVENTION, DÉTECTION ET CORRECTION DOIVENT ÊTRE INTÉGRÉES EN CONTINU.
- LA GOUVERNANCE ET LA CONFORMITÉ (RGPD, ISO, SECNUMCLOUD) SONT DES PILIERS INDISPENSABLES.