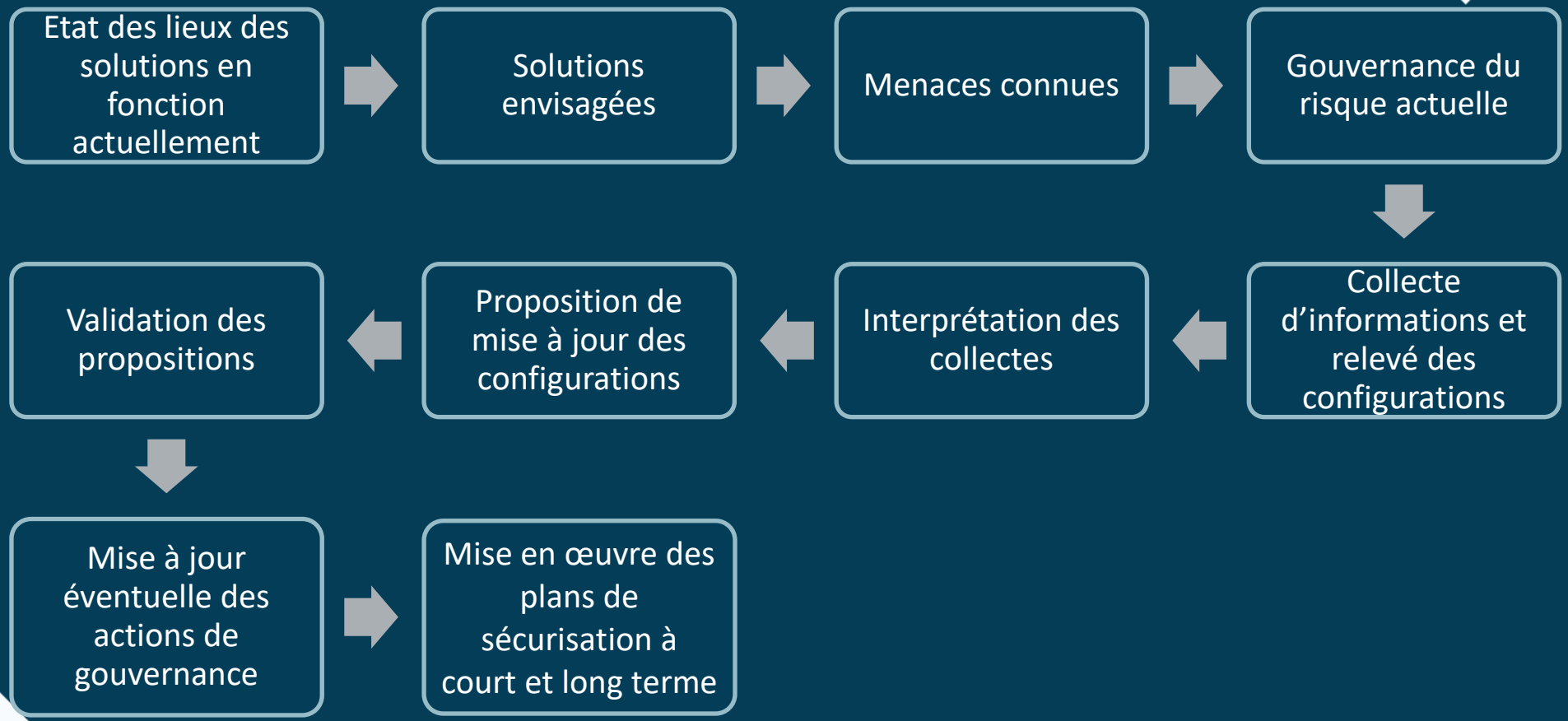
SÉCURISER OFFICE 365 EN CAPITALISANT AU MAXIMUM LES FONCTIONNALITÉS NATIVES

YANN KERNANEC - ELIADE

QUELLE APPROCHE ?



OBJECTIFS ET ENJEUX

- Capitaliser au maximum les services détenus
- Définir les usages souhaités
- Paramétrer les différentes solutions au sein des différentes consoles d'administration
- Automatiser les collectes d'informations
- Acter et diffuser les règles d'utilisations
- Faciliter les actions de gouvernance

PLAN DE SÉCURISATION GÉNÉRIQUE D'OFFICE 365

CLUSIF

✔ LA SÉCURISATION D'UN TENANT OFFICE 365 DOIT ADRESSER PLUSIEURS PANS :

La configuration globale du tenant

La protection de la messagerie

La protection des identités

La configuration des espaces collaboratifs

Les accès invités et la stratégie de partage externe

La protection des périphériques

La gouvernance

- ✓ Des identités
- ✓ Des données
- ✓ Des périphériques
- ✓ Des espaces collaboratifs

✔CONFIGURATION GLOBALE DU TENANT :

Personnaliser la mire de connexion

Acter la liste des services Office 365 qui sont (vont être) activés

S’astreindre à la réalisation des audits des vulnérabilité de façon régulière

Réaliser des campagnes de sensibilisation des utilisateurs

Acter un process d’entrée/sortie des personnels robuste

Acter un process d’entrée/sortie des partenaires / invités / externes

Projeter un cycle de vie des données

Projeter un cycle de vie des périphériques

Acter et diffuser une matrice d’utilisation des outils en fonction des usages souhaitées (quel outil pour quel usage ?)

✔PROTECTION DE LA MESSAGERIE :

Application des recommendations ORCA

- ✓ Office 365 Advanced Threat Protection Recommended Configuration Analyzer (ORCA) a une portée EOP et pas ATP uniquement, ce qui permet de mettre en place les best practices de configuration

Sécuriser ses domaines de messagerie avec les configurations SPF / DKIM et DMARC

Acter la liste des domaines de messagerie en whitelist

Acter la pertinence des expéditeurs autorisés dans chacune des boites aux lettres

Délégations et transferts ?

Règles de traitement automatisées ?

✔PROTECTION DES IDENTITÉS:

Les items identités à sécuriser, sur AD comme sur Azure AD :

- ✓ Les comptes utilisateurs
- ✓ Les comptes à privilèges
- ✓ Les comptes invités

Plan d'action

- ✓ Identifier les scénarios d'accès légitimes
- ✓ Bloquer les authentifications basiques
- ✓ Exiger le MFA pour l'ensemble des comptes à privilèges
- ✓ Créer et sécuriser plusieurs comptes à privilèges nominatifs (cloud only et non pas synchronisés)
- ✓ Désactiver (supprimer dans l'idéal) les comptes inactifs depuis plus de 90 jours

Si Azure AD Premium :

- Accès conditionnels
- PIM
- Azure Identity Protection

✔LA CONFIGURATION DES ESPACES COLLABORATIFS :

Les items à sécuriser :

- ✓ Azure AD
- ✓ Microsoft 365
- ✓ SharePoint
- ✓ Teams
- ✓ OneDrive

Plan d'action :

Partage externe

- ✓ SharePoint
- ✓ OneDrive

Teams

- ✓ Fédération ?
- ✓ Stratégie de configuration
- ✓ Stratégie d'application
- ✓ Stratégie de réunion

Si Azure AD Premium :

- Groupe Dynamique
- Expiration
- Convention de nommage
- Restriction de création

LES ACCÈS INVITÉS ET LE PARTAGE EXTERNE :

Il faut différencier l'accès externe et l'accès invité

Par exemple, sur Teams :

External Acces

- ✓ chat / appels avec des domaines externes
- ✓ on autorise ou l'on bloque un domaine complet
- ✓ par défaut c'est sur ON sur le tenant

Guest Access

- ✓ invitation d'utilisateur externe et ajout au sein d'Azure AD
- ✓ il y a beaucoup plus d'usage associé (ex MFA, partage de fichier…)
- ✓ par défaut c'est sur OFF sur le tenant

C'est le guest access qui joue sur le licensing (50 000 si Azure AD Premium...)

✓PROTECTION DES PÉRIPHÉRIQUES :

Les sujets à prendre en compte afin de sécuriser ses périphériques :

- Le traditionnel Antivirus
- Windows 10 et sa gestion particulière des mises à jour
  (le patch management en général)
- La gestion des périphériques mobiles
  - ✓ MDM
  - ✓ MAM
- Le provisionnement automatique (AutoPilot)
- BYOD & CORP

Quels enjeux ?

- Sécurisation de l'accès aux données (et par extension des données)
- Contrôle de l'interaction des données professionnelles avec les données à caractère personnel
- Maitrise du cycle de vie de l'espace professionnel de l'utilisateur

✔GOUVERNANCE OFFICE 365 :

Des identités

- ✓ Gestion des entrées / sorties

Des périphériques

Des données

Des espaces collaboratifs

- ✓ Diffusion des règles d'utilisation
- ✓ Vérification du respect de ces règles
- ✓ Promotion de telle ou telle solution
- ✓ Suivi des partages / des invitations
- ✓ Application des conventions de nommage
- ✓ Archivage des espaces non utilisés

LA ROADMAP MICROSOFT