Rentrée en toute (cyber)sécurité : les nouveautés Microsoft

Mardi 3 octobre 2023

Sommaire

Romaric MAHUT
Chef de projets Marketing

Antoine Loreau
Consultant avant-vente

Nicolas BOUILLON
Consultant avant-vente

Estelle FLAUJAT
Team Leader Projet & Change Management

01.
Les changements de l'été côté Microsoft

Les nouveautés côté Microsoft sur la sécurité

Microsoft 365 Backup

Microsoft 365 Archive

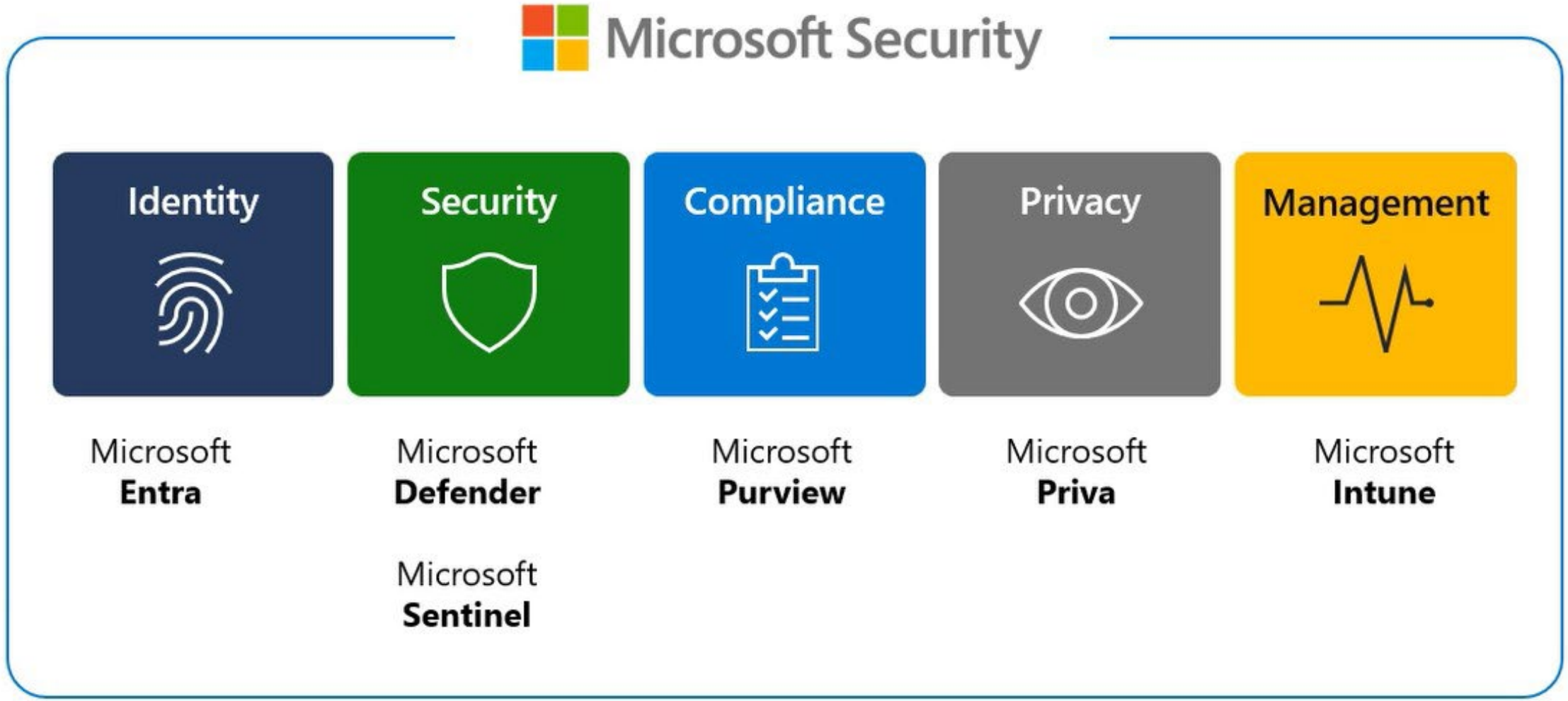
Microsoft Security Copilot

Famille Entra ID

Microsoft Priva

Microsoft Purview

blue soft Empower


Microsoft Security
Identity
Security
Compliance
Privacy
Management
Microsoft Entra
Microsoft Defender
Microsoft Sentinel
Microsoft Purview
Microsoft Priva
Microsoft Intune

Microsoft Entra

Accès sécurisé

Gestion des identités et des accès dans l'ensemble de votre environnement numérique

Visibilité et contrôle

Gouvernance de toutes les identités et de toutes les ressources avec des autorisations sur plusieurs clouds

Vérification des identités

Vérification des informations d'identification en fonction de normes d'identité décentralisées

Microsoft Priva

Gestion de la confidentialité

Protéger les informations personnelles et gérer les risques liés à la confidentialité des données

Subject Rights Requests

Gérer à grande échelle, répondre en toute confiance

Microsoft Purview

Comprendre et gouverner les données

Gérez la visibilité et la gouvernance des ressources de données dans votre environnement

Protéger les données, où qu'elles se trouvent

Protégez les données sensibles sur les différents clouds, applications et appareils

Améliorer la position en matière de risques et de conformité

Identifiez les risques liés aux données et gérez les exigences de conformité réglementaire

02.
La Kill Chain et ses produits

Protection contre les menaces et services à mettre en oeuvre (à l'état de l'art)

Cloud App Security

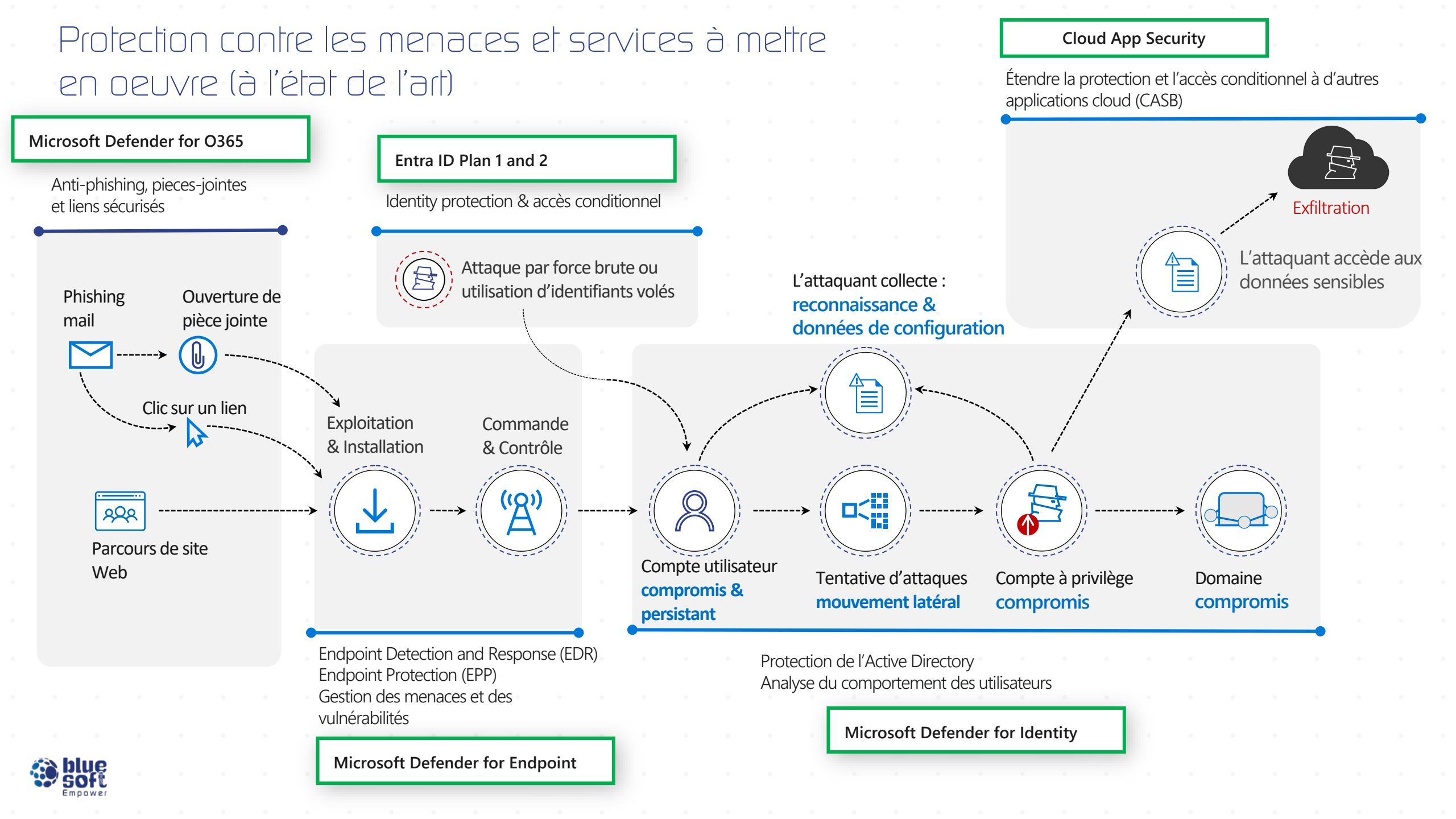
Étendre la protection et l'accès conditionnel à d'autres applications cloud (CASB)

Microsoft Defender for O365

Anti-phishing, pieces-jointes et liens sécurisés

Entra ID Plan 1 and 2

Identity protection & accès conditionnel



Endpoint Detection and Response (EDR)
Endpoint Protection (EPP)
Gestion des menaces et des vulnérabilités

Microsoft Defender for Endpoint

Protection de l'Active Directory
Analyse du comportement des utilisateurs

Microsoft Defender for Identity

Identités

Gérez les identités et les stratégies d'accès conditionnel pour connecter les utilisateurs à leurs applications.

Produits

- **Entra ID P1/P2**

Matériel

- **Token TOTP**
- **Authenticator**

Prestations

- **Mise en œuvre du MFA et de l'accès conditionnel**
- **Mise en œuvre de SSO avec Entra ID**
- **Fusion des identités**
  - Fusion d'annuaire
  - Agrégation des identités avec Entra ID
- **Mise en œuvre du principe de moins privilège avec JIT**
- **Mise en œuvre du tiering**

Endpoints

Endpoints ou « points de terminaison » sont des dispositifs physiques qui se connectent à un réseau informatique et échangent des informations avec celui-ci.

Produits

- Intune
- MECM
- Microsoft Defender for Endpoint

Prestations

- Analyse de la posture de sécurité des périphériques (CIS, ANSSI, Microsoft)
- Déploiement de stratégie de sécurité pour Intune et/ou Microsoft Defender for Endpoint
- Déploiement d'un politique de conformité
- Mise en œuvre de Microsoft Defender for Endpoint
- Mise en oeuvre d'Intune sur le périmètre des périphériques mobiles (tablette, téléphone, ordinateur nomade)
- Gestion du cycle de vie des endpoints

Applications

Une application ne application est un programme ou ensemble de logiciels destinés à réaliser une tâche ou un ensemble de tâches élémentaires d'un même domaine.

Produits

- Entra ID P1/P2
- Intune
- Defender for Cloud App

Prestations

- Déploiement de stratégie de configuration des applications pour Intune
- Déploiement de stratégie de protection des applications
- Déploiement de l'accès conditionnel

Datas

Toutes les données sont à prendre en considération (données client, à caractère personne, administrateur, de paiement, etc).

Produits

- Microsoft Purview
- Intune / MECM
- Microsoft Defender for Cloud Apps

Prestations

- Mise en œuvre du chiffrement des disques bitlocker
- Accompagnement à la définition des données sensibles
- Mise en œuvre de stratégie d'étiquetage manuel ou automatique des données sensibles
- Mise en œuvre d'un politique de DLP
- Mise en œuvre de Microsoft Defender for Cloud Apps

Infrastructure

Une infrastructure comprend les composants nécessaires au fonctionnement et à la gestion des environnements informatiques d'entreprise.

Produits

- Microsoft Defender for Identity, Office 365, Endpoint, Cloud App
- Solutions de sécurité Azure
- Ping Castle / ORADAD
- PKI / MECM

Prestations

- Déploiement des briques Microsoft Defender for X
- Déploiement du SIEM Azure Sentinel
- Accompagnement à la personnalisation d'Azure Sentinel
- Audit Ping Castle / ORADAD et accompagnement à la remédiation
- Mise en œuvre d'une infrastructure de PKI
- Passage en HTTPS de l'infrastructure MECM
- Audit de sécurité de la configuration de MECM et remédiation
- Formations Microsoft Defender, Microsoft PurView, Azure sécurité

03.
REX Clients

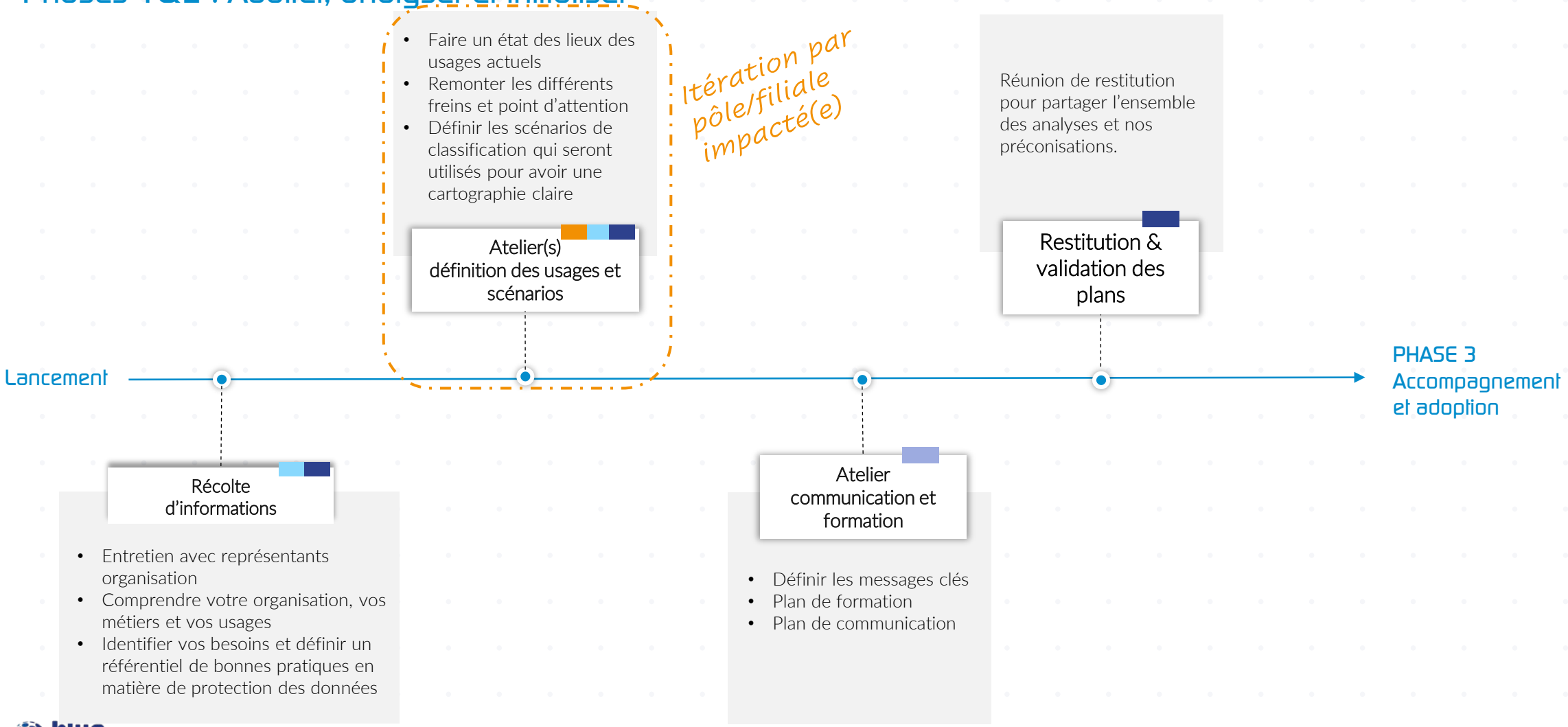
blue soft
Empower

Démarche d'accompagnement au changement Protection des données

Phases 1&2 : Auditer, analyser et initialiser

INTERVENANTS

- Administrateurs Technique DLP&AIP
- Equipe projet client
- Représentants de la communication/ formation
- Représentants métiers (10 utilisateurs max.)



Démarche d'accompagnement au changement Protection des données

Phase 3 : plan d'adoption

EQUIPE CONDUITE DU CHANGEMENT

Exemple de feuille de route adoption DLP&MIP

Embarquer l'ensemble des utilisateurs

Volet 1

Brique 1

- Les fondamentaux de la MIP

Brique 2

- Bonnes pratiques

- Expliquer la philosophie générale de la protection des données
- Comprendre les enjeux et le contexte
- Savoir utiliser la MIP & DLP à mon niveau au sein de mon organisation

Adopter la MIP & DLP au sein des pôles/filiales impacté(e)s

Volet 2

- Identifier les scénarios d'usage
- Déterminer les labels de confidentialités appropriés

Brique 3

- Comprendre et utiliser les labels de confidentialité de mon organisation

Itération par pôle/filiale impacté(e) :
- Faire un état des lieux des usages actuels
- Remonter les différents freins et point d'attention
- Définir les scénarios et labels de classification qui seront utilisés

Formation :
- Savoir utiliser les labels au sein de mon pôle
- Adopter les process adéquats et les bonnes pratiques

Onboarding :
- Feuille de route d'onboarding MIP/DLP par pôle
- Communiquer du contenu « sur étagère »
- Intégrer la MIP/DLP à la session d'accueil RH/métier

Le HUB : un espace d'échange privilégié avec nos clients

LE HUB

LA 1ère COMMUNAUTÉ

« M365 - Adoptons les usages »

Une communauté autour des usages et de l'adoption des solutions Microsoft 365.

2ème COMMUNAUTÉ

« M365 EDUC Adoptons les usages »

Une communauté autour des usages et de l'adoption des solutions Microsoft 365 Education.

Un accès à une multitude de communautés portées sur différentes thématiques

- Un espace d'échanges, de retours d'expériences
- De l'informations autour de l'actualité et des nouveautés Microsoft
- Des évènements exclusifs !

Enquête sur la sensibilisation des utilisateurs à la cybersécurité

Cette enquête couvre :

- la stratégie de sécurité déployée
- les types de cyberattaques subies et la période
- le rôle des utilisateurs dans la lutte contre les cyberattaques
- les actions de sensibilisation menées
- les statistiques par secteur (privé, public, santé)
- les tendances et les conclusions

04. Questions & Réponses

blue soft
Empower

Merci !

www.bluesoft-group.com