esup portail

utt TROYES — MEMBER OF — EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

17 NOVEMBRE 2026 @Distance

ESUP-DAYS 42

MFA À L'UTT : RETOUR D'EXPÉRIENCE

MULTI-FACTOR AUTHENTICATION

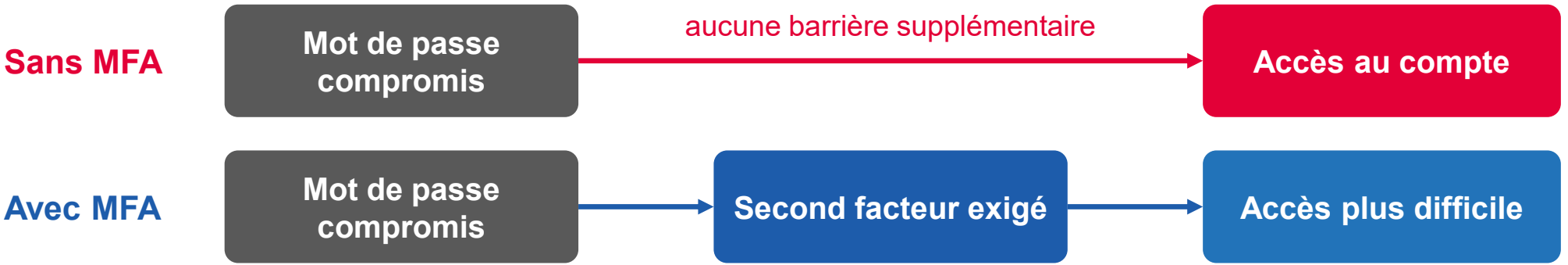
Charles Tournemeule -- Université de technologie de Troyes (UTT)

CONTEXTE ET OBJECTIFS

- École d'ingénieur :
  - 3000 étudiants
  - 500 personnels
- Un mot de passe seul ne suffit plus
- Trois objectifs :
  - Sécurité
  - Intégration
  - sobriété

CONTEXTE ET OBJECTIFS

École d'ingénieur · 3000 étudiants



Causes fréquentes : réutilisation, divulgation, hameçonnage

Trois objectifs du projet

Sécurité
renforcer l'authentification

Intégration
s'appuyer sur les briques en place (CAS, LDAP)

Sobriété
solution gratuite, sans matériel à fournir

CHOIX DE LA SOLUTION

- JRES 2024 : plusieurs solutions comparées
- Concertation avec le groupe UT et Compiègne
- ESUP-OTP : gratuit, compatible avec l'existant
- Pas de YubiKey : trop chère, mauvaise pour la planète

CHOIX DE LA SOLUTION

JRES 2024 → **Comparaison de solutions** → **Concertation UT + Compiègne** → **Test d'ESUP-OTP**

JRES 2024	Comparaison de solutions	Concertation UT + Compiègne	Test d'ESUP-OTP
veille et échanges	plusieurs solutions regardées	Compiègne déjà avancée sur ESUP-OTP	décision de tester

Critères retenus

- **Gratuit**
- **Compatible avec les briques en place**

Écartée : clé physique (YubiKey)

- **Trop chère**
- **Mauvaise pour la planète**

Mieux vaut de l'OTP que rien

DIMENSIONNEMENT ET CHARGE DE TRAVAIL

- Chef de projet technique
- Dimensionnement :
  - 1 serveur CAS
  - 1 serveur Esup-OTP
    - API
    - Manager
- Charge (hors support) :
  - 230 heures (environ 0,3 ETP) du 20/01/2026 au 29/06/2026
- Toujours en cours :
  - Accompagnement Etudiants + Personnels : 60h
  - Support : 30h

DIMENSIONNEMENT ET CHARGE DE TRAVAIL

Direction
préparation en amont

Chef de projet technique
pilotage + mise en œuvre

Support
utilisateurs et incidents

Dimensionnement et charge de travail

Dimensionnement
1 serveur CAS, 1 serveur Esup-OTP (API + Manager)

Charge de travail
230 heures · env. 0,262 ETP

Séparation des environnements

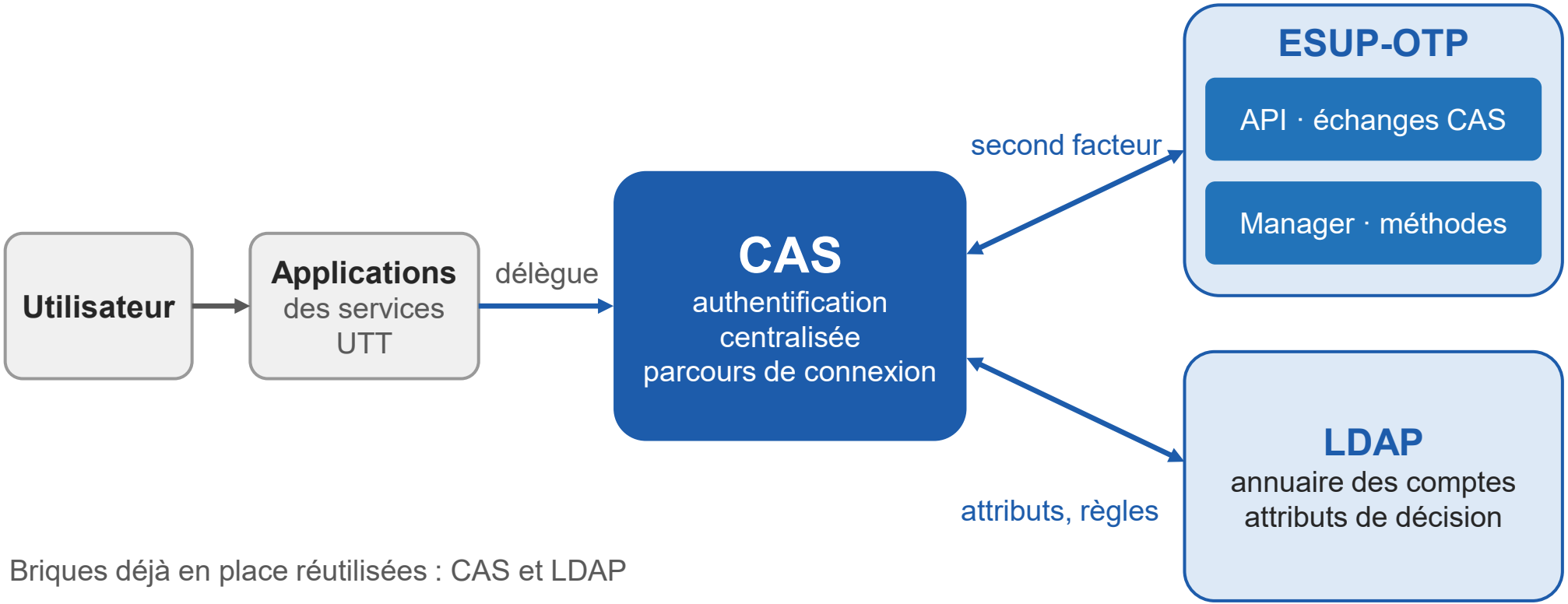
Préproduction
tester sans impact utilisateur

Production
rester stable pour les services

ARCHITECTURE : CAS, ESUP-OTP, LDAP

- CAS :
  - authentification centralisée
- ESUP-OTP :
  - API
  - Manager
- LDAP :
  - attributs qui pilotent les règles

ARCHITECTURE : CAS, ESUP-OTP, LDAP

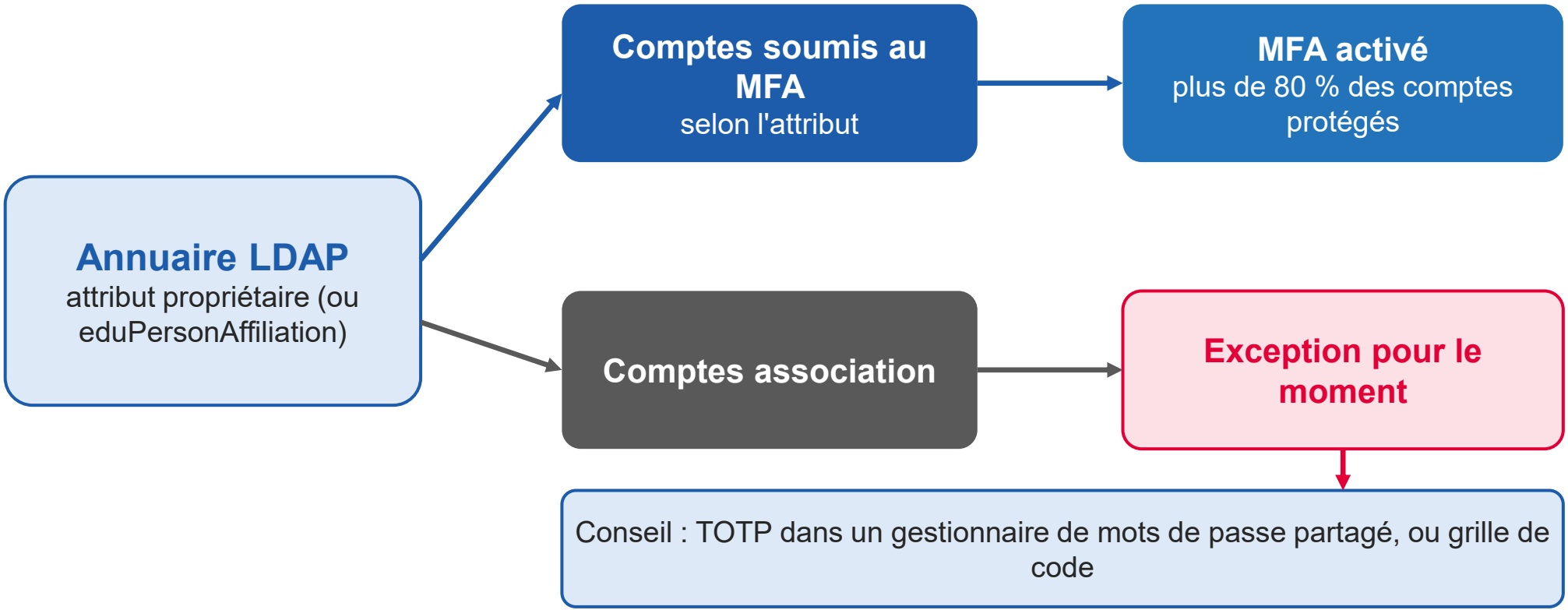


Briques déjà en place réutilisées : CAS et LDAP

QUI DOIT UTILISER LE MFA ?

- Attribut propriétaire (ou eduPersonAffiliation)
- Plus de 80 % des comptes protégés
- Comptes association : exception pour le moment

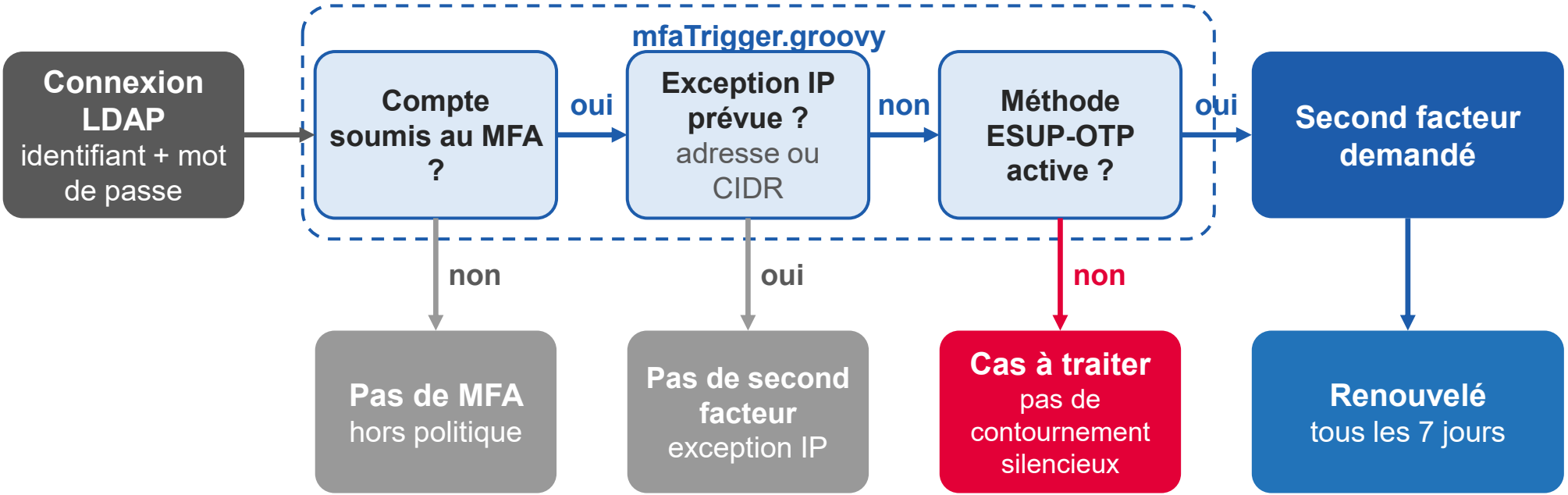
QUI DOIT UTILISER LE MFA ?



RÈGLES DE DÉCLENCHEMENT DU MFA

- Deux scripts Groovy :
  - mfaTrigger
  - interrupt
- Exceptions IP centralisées
- Second facteur renouvelé tous les 7 jours

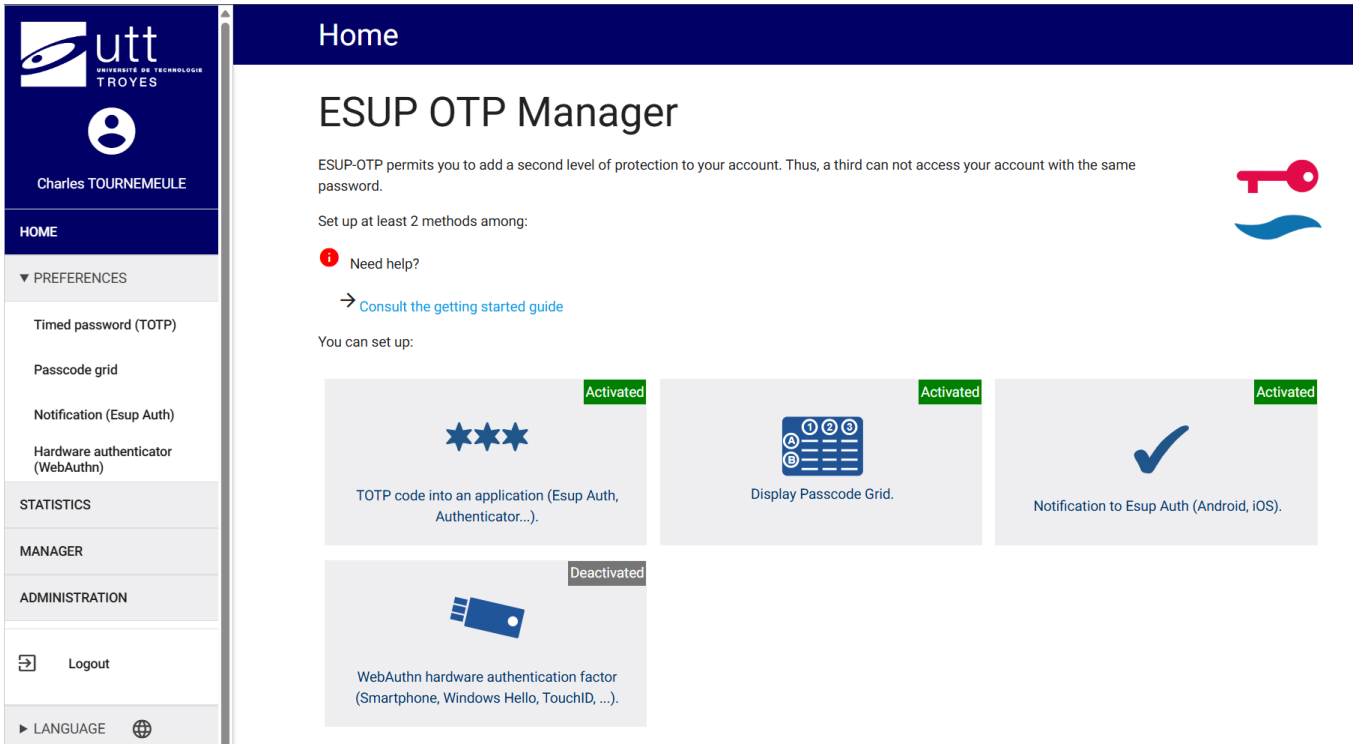
RÈGLES DE DÉCLENCHEMENT DU MFA



interrupt.groovy : contrôle du parcours, cas particuliers non interrompus
(callbacks applicatifs, portail MFA)

ESUP-OTP MANAGER : FONCTIONNEMENT

- Gestion des méthodes par l'utilisateur
- TOTP et grille de code



ESUP-OTP MANAGER : FONCTIONNEMENT

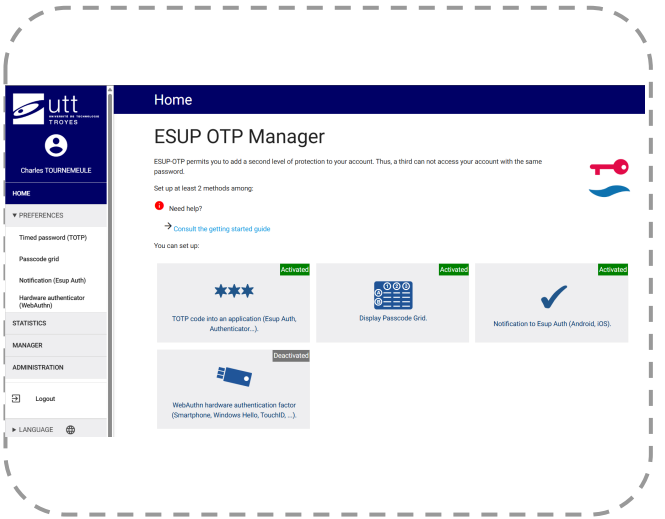
Utilisateur → **ESUP-OTP Manager** active et gère ses méthodes → **API ESUP-OTP** enregistre les méthodes ↔ **CAS** demande le second facteur

Méthodes proposées

TOTP
application d'authentification

Grille de code
alternative au TOTP

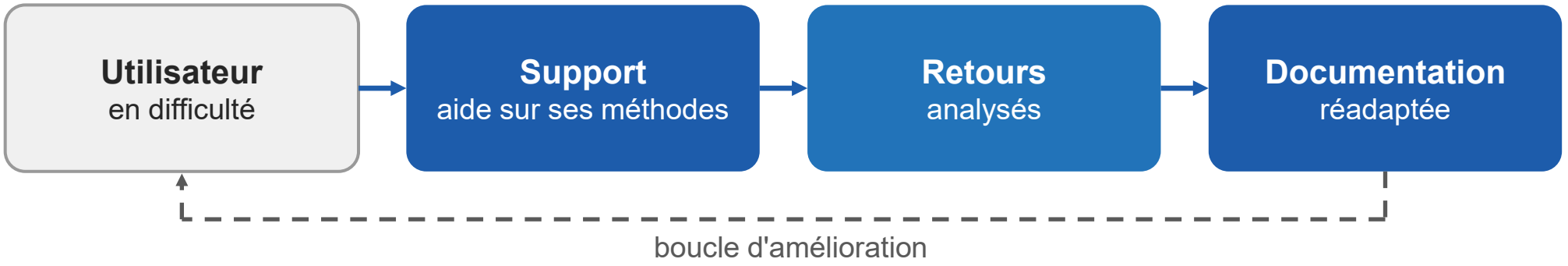
Gestion en autonomie par l'utilisateur



ESUP-OTP MANAGER : SUPPORT ET USAGES

- Support : aide aux utilisateurs pour leurs méthodes
  - Cas fréquents : Grille de code, perte du smartphone
- Retours des utilisateurs
  - Documentation réadaptée en conséquence
- Grille de code : nombreux soucis rencontrés
  - Réflexion en cours pour possiblement la retirer

ESUP-OTP MANAGER : SUPPORT ET USAGES



Points de vigilance

Cas fréquents
Grille de code, perte du smartphone

Grille de code
nombreux soucis rencontrés

Comptes association
gestionnaire de mots de passe partagé (TOTP) ou grille de code

DÉPLOIEMENT ET ACCOMPAGNEMENT

- Préparation en amont avec la direction
- Sensibilisation dans différents comités (RSSI)
- Personnels DNUM volontaires : ateliers d'1 h par jour pendant 1 semaine
- Étudiants : 2 semaines d'accompagnement
  - Avec l'aide d'étudiants en contrat étudiant
- Documentation réadaptée suivant les retours

DÉPLOIEMENT ET ACCOMPAGNEMENT

Préparation	Sensibilisation	Personnel	Étudiants
en amont avec la direction	dans différents comités	ateliers d'1 h par jour pendant 1 semaine	2 semaines, avec des étudiants en contrat étudiant

Documentation réadaptée suivant les retours

Plus de 80 % des comptes protégés

DIFFICULTÉS, BILAN ET PERSPECTIVES

Difficultés

Scripts Groovy
partie la plus complexe

Support
aux utilisateurs

Grille de code
nombreux soucis

Bilan

Plus de 80 %
des comptes protégés

Perspectives

Comptes association
sortir de l'exception

Amélioration continue
règles et documentation

« L'ÊTRE HUMAIN EST LE MAILLON LE PLUS FAIBLE ; LE PLUS GRAND RISQUE EST L'IGNORANCE. »

KEVIN MITNICK (EXPERT EN SÉCURITÉ INFORMATIQUE)

-- Retour d'expérience MFA

ESUP-DAYS 42

MERCI DE VOTRE ATTENTION

QUESTIONS ?

esup portail