Club de la sécurité de l'information français

La gestion des accès au cœur du process de fabrication des JT

Alex ARNAUD – RSSI
David AUBURTIN – Chef de projet News

Charlotte FOURCROY – Consultante IAM

Plan

- Contexte
- Objectifs et Typologie des comptes
- Les cas d'usage des comptes génériques à TF1
- Les solutions mises en place en zone JT
  - Cas des salles de montage
  - Cas des régies
- Outils de pilotage
- Bilan du projet

Contexte – la sécurité informatique à TF1

- TF1 un groupe média privé français :
  - 5 chaines TNT et 4 chaines thématiques
  - Des activités dans la production audiovisuelle
  - Des diversifications dans le digital (site média, replay/vod, e_commerce)
  - Une régie publicitaire pluri-médias

Des utilisateurs métiers variés en particulier dans la production de contenu

- Journalistes, techniciens audiovisuels, intermittents techniques … avec un usage assez large des comptes génériques

- Le groupe TF1 n'est pas OIV et n'est pas soumis à SOX, mais :
  - Applique les bonnes pratiques sécurité édictées par l'audit et le contrôle interne en particulier autour de la fabrication des JTs
  - Application plus stricte des recommandations de l'ANSSI depuis les cyberattaques Sony Pictures et TV5 Monde
  - Éradication des comptes génériques via l'usage de plusieurs solutions, techniques et de workflow

Objectifs et Typologies des comptes

Vocabulaire employé lors du projet de suppression des comptes génériques :

Types de comptes	Complexité du mot de passe	Divulgation du mot de passe	Ouverture de session Windows
Compte nominatif	+	1 utilisateur	Oui
Compte générique	- -	X utilisateurs	Oui
Compte technique	+ +	Administrateurs	Oui
Compte de service	+ +	Administrateurs	Non

Configuration problématique

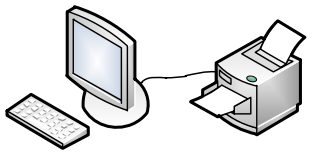
L'objectif du projet vise à **supprimer les comptes génériques** (OS), tout en **traçant** les authentifications à des fins de **dissuasion** et **d'identification** simple et sûre des auteurs de malveillance

Règle 8 du guide d'hygiène informatique de l'ANSSI :
Identifier nommément chaque personne ayant accès au système

Cas d'usage des comptes génériques à TF1

Intermittents : Population avec un turn-over important ; historiquement aucun compte nominatif ne leur était attribué

Boites email partagées : Adossés à des comptes AD obligatoirement activés



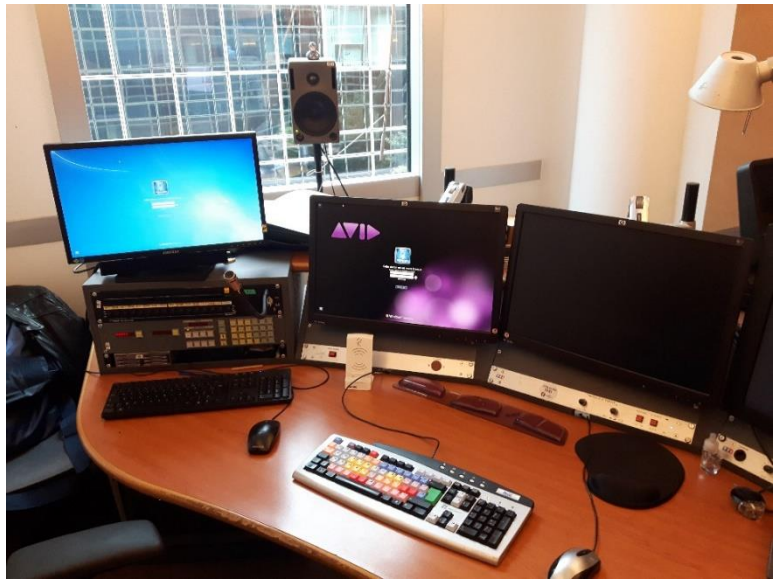
Postes partagés : Postes en libre-service. Plusieurs personnes travaillent sur 1 ou plusieurs postes. Besoin d'un accès simple et rapide. Certains de ces postes sont « critiques ».

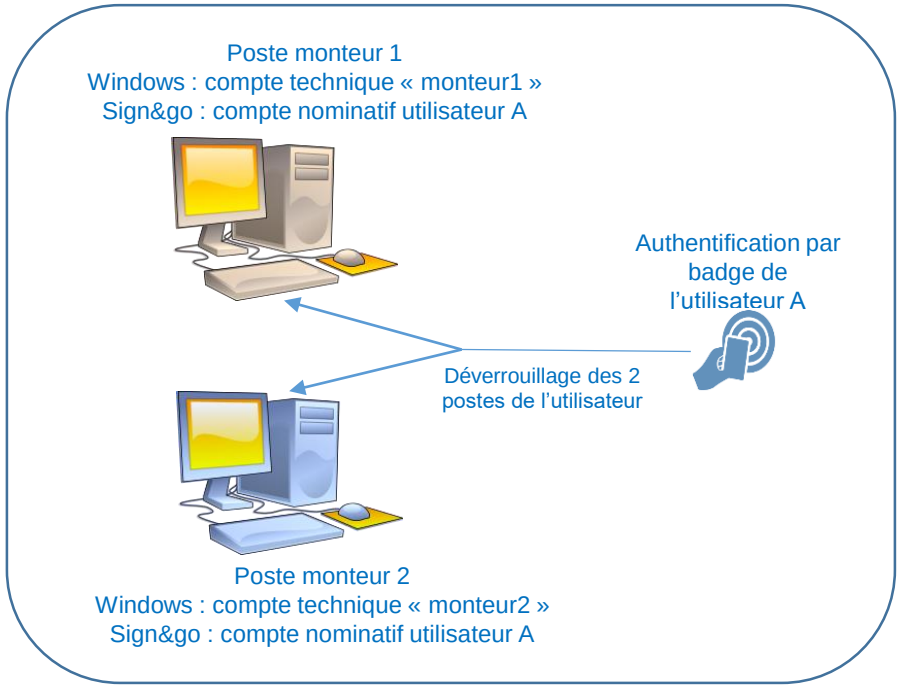
Postes d'affichage : Postes sans mise en veille, pour un affichage d'application (notamment de supervision) en continu

Postes utilisés à l'extérieur des locaux (prestataires extérieurs)

Mais aussi les salles de réunion, les comptes de tests, etc.

Focus sur les usages en zone JT
Zone de montage

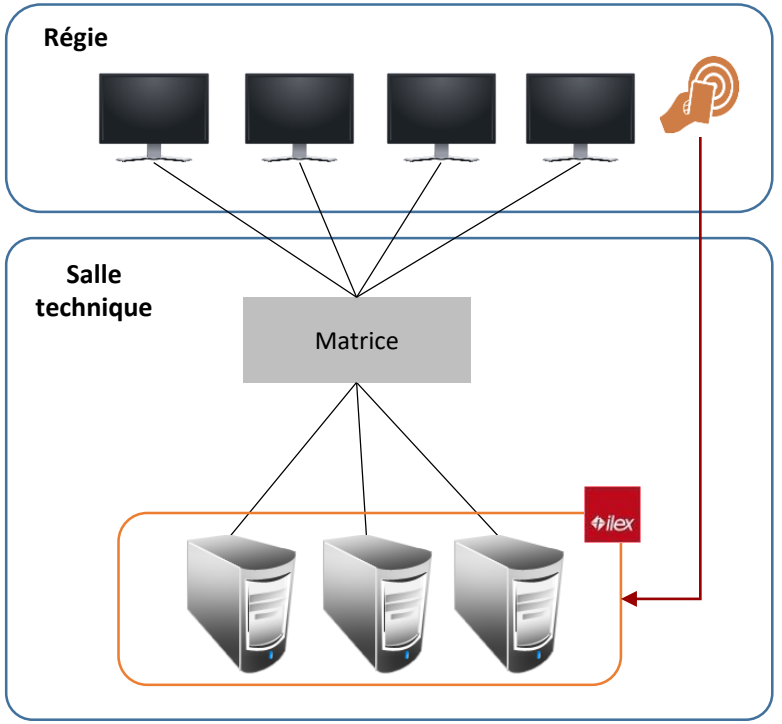




- Solution mise en place :
  - Fonctionnalité kiosque pour une authentification nominative et un profil partagé
  - Authentification par badge
  - Grappe avec les 2 postes du monteur

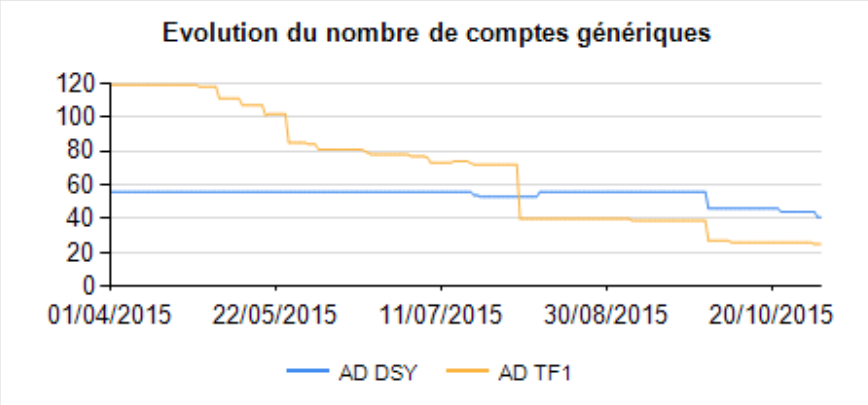
Focus sur les usages en zone JT
La régie JT

1 « clé » déverrouille tous les postes



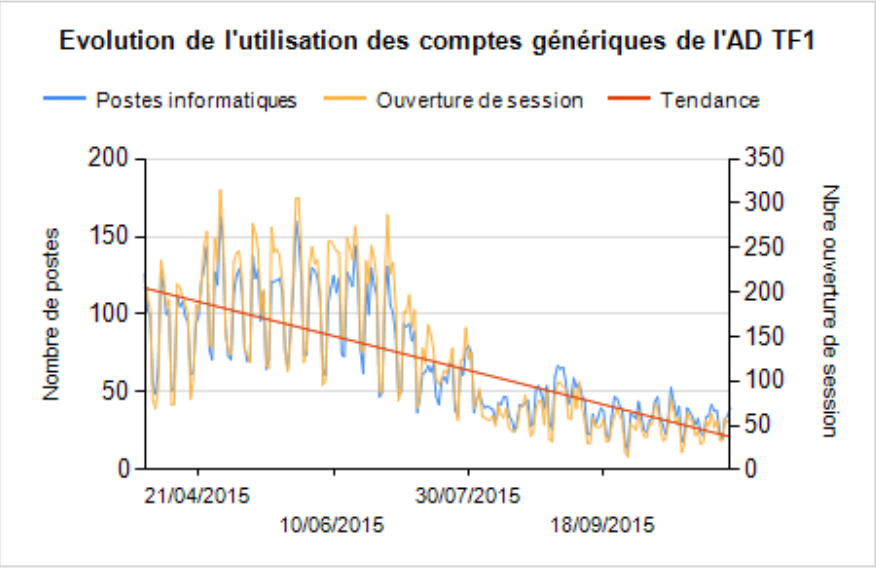
- Solution mise en place :
  - Sign&go en mode grappe
  - Architecture redondée
  - Bouton Rouge : mécanisme pour débrayer la solution en cas de problème (zone critique)

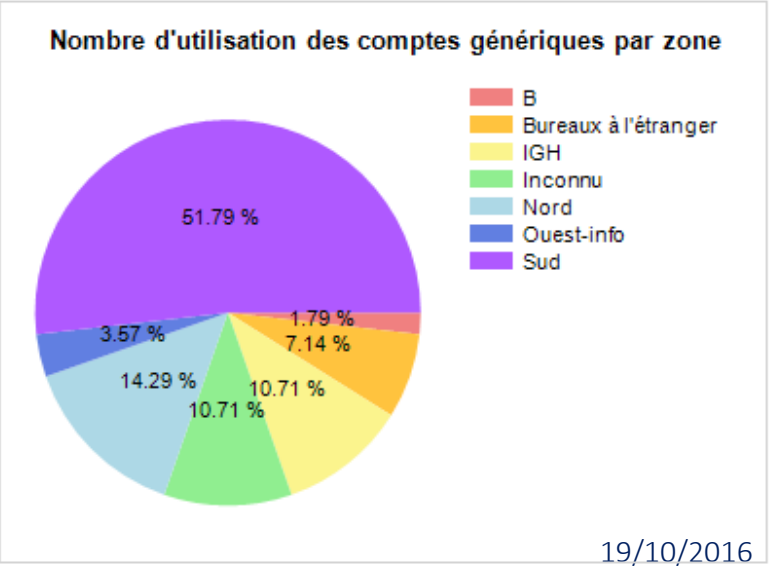
Outils de pilotage



Etat des comptes génériques au 04/11/2015

	Nombre de comptes
Comptes génériques utilisables (AD TF1)	25
Comptes génériques utilisables (AD DSY)	41
Comptes génériques neutralisés	108
Total	**174**





Bilan du projet

- Un besoin couvert par les solutions déployées
  - Tracer les authentifications dans une base facilement exploitable
  - Contraindre les utilisateurs à utiliser un compte nominatif, sans ajouter d'étapes chronophages d'exploitation
- Des difficultés rencontrées
  - Un projet au cœur de la gestion des identités : des sujets périphériques ont dû être traité pour supprimer certains comptes
    - Accélérer la création / activation des comptes
    - Enrôler le badge de 500 personnes en peu de temps
    - Organiser les profils techniques des postes Sign&Go, afin notamment de cloisonner les droits
  - Une gestion du changement difficile avec une population non technophile
    - Des « plus » comme l'usage du badge pour s'authentifier, les grappes, ont permis de faciliter l'acceptation de la solution
- A suivre…
  - Traiter les comptes génériques applicatifs
  - Fort de l'expérience sur LCI, finaliser les régies News de la chaine TF1