

Projet Administration et sécurité SI



Équipe



Philippe LUU
Ingénieur Cybersécurité



Antonin RABATEL
Ingénieur DevOps



Allan BOUHAMED
Ingénieur Systèmes & Réseaux



Alexandre RIVET
Ingénieur Data



Mathéo CARVAL
Ingénieur DevOps

Contexte

PME
multi-métiers

Déménagement
et site distant

SI vulnérable

Menace
rançongiciel

Continuité
Sécurité
Administration

Sommaire

I

**Plan
d'action**

II

Réalisation

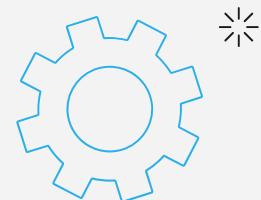
III

Résultats



Problématique

Comment concevoir et sécuriser un système d'information multi-sites pour une PME, capable de résister aux rançongiciels, tout en garantissant la continuité d'activité, la traçabilité et une administration déléguée efficace ?





Plan d'action

Plan d'action

1. Compréhension du besoin
2. Définition des politiques
3. Conceptualisation de l'infrastructure
4. Choix des solutions / matériel
5. Sensibilisation
6. Déploiement / Maquettage
7. Optimisation administrative



||

Réalisation

1. Compréhension du besoin



1. Compréhension du besoin

Type Faille	Disponibilité	Intégrité	Confidentialité	Tracabilité
HTTP ERP				
Poste admin				
Backup USB				
NAS ouvert				
Antivirus gratuit				
Drive personnel				
ERP partagé				

2. Définition des politiques



Accès & identités



Sécurité & durcissement

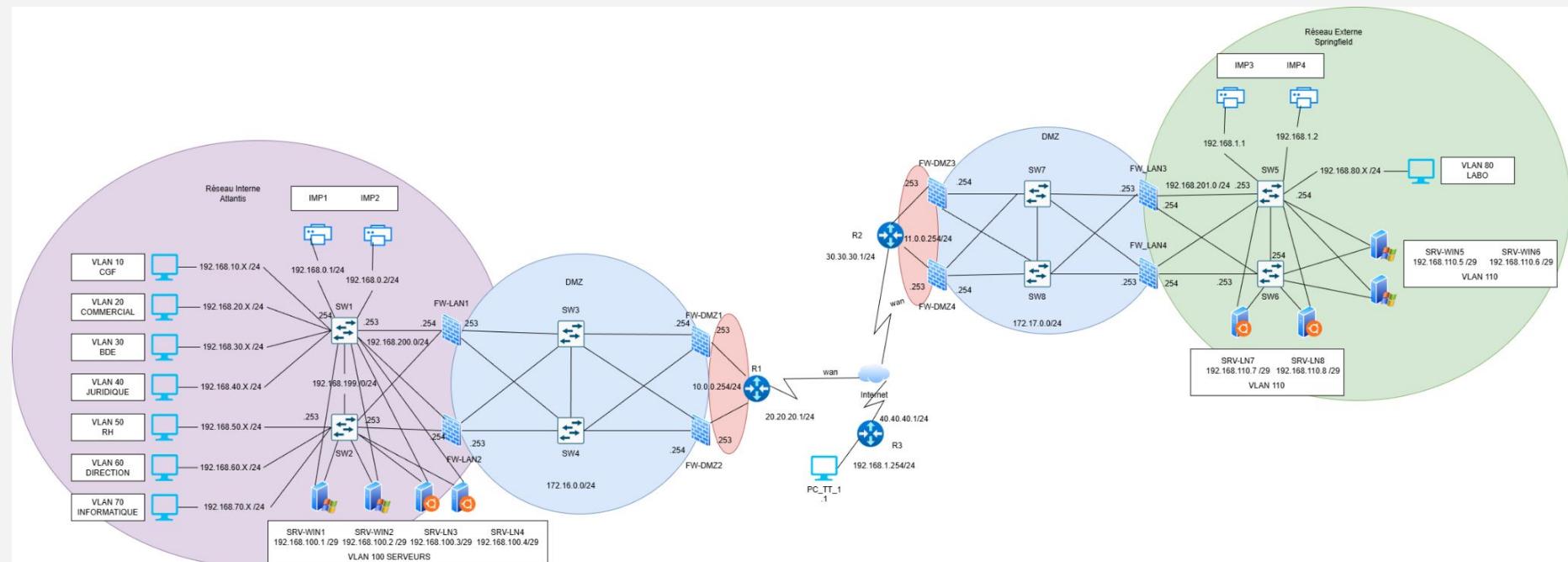


Continuité & sauvegardes

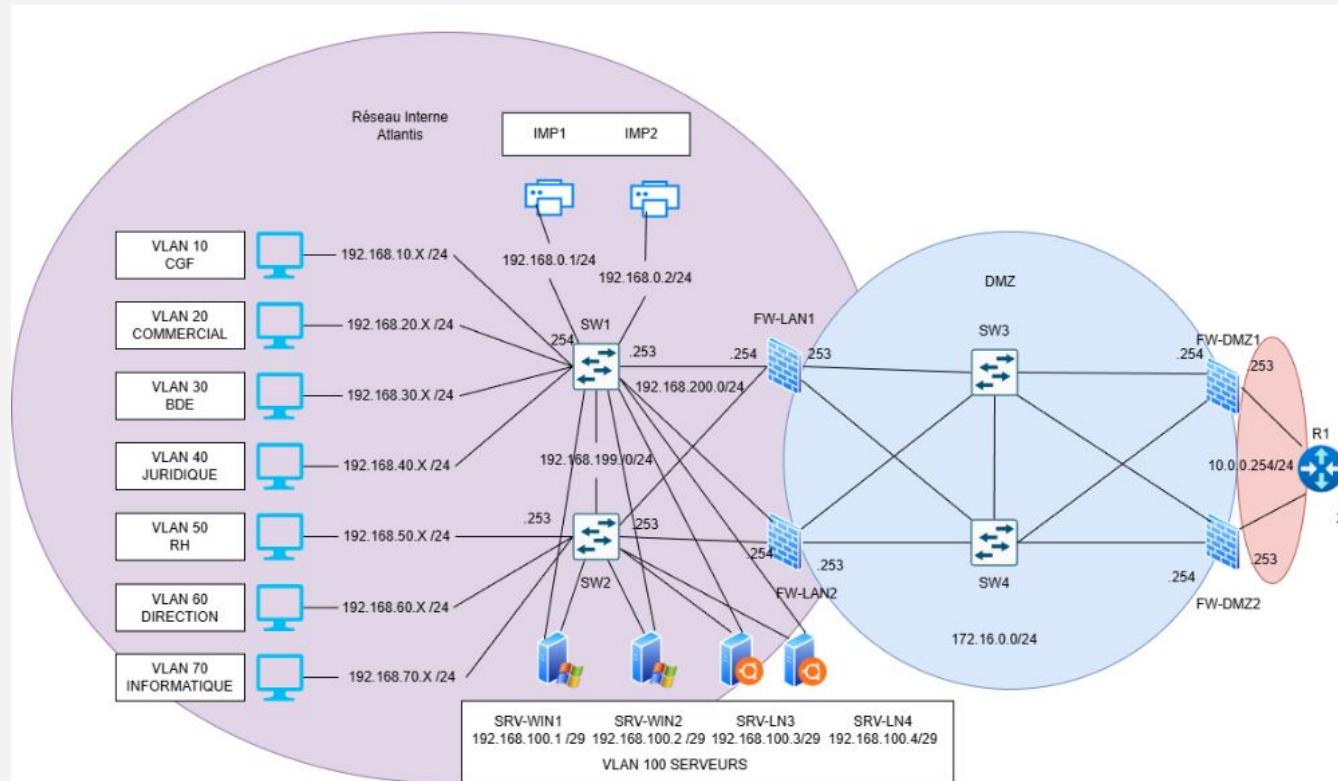


Traçabilité & supervision

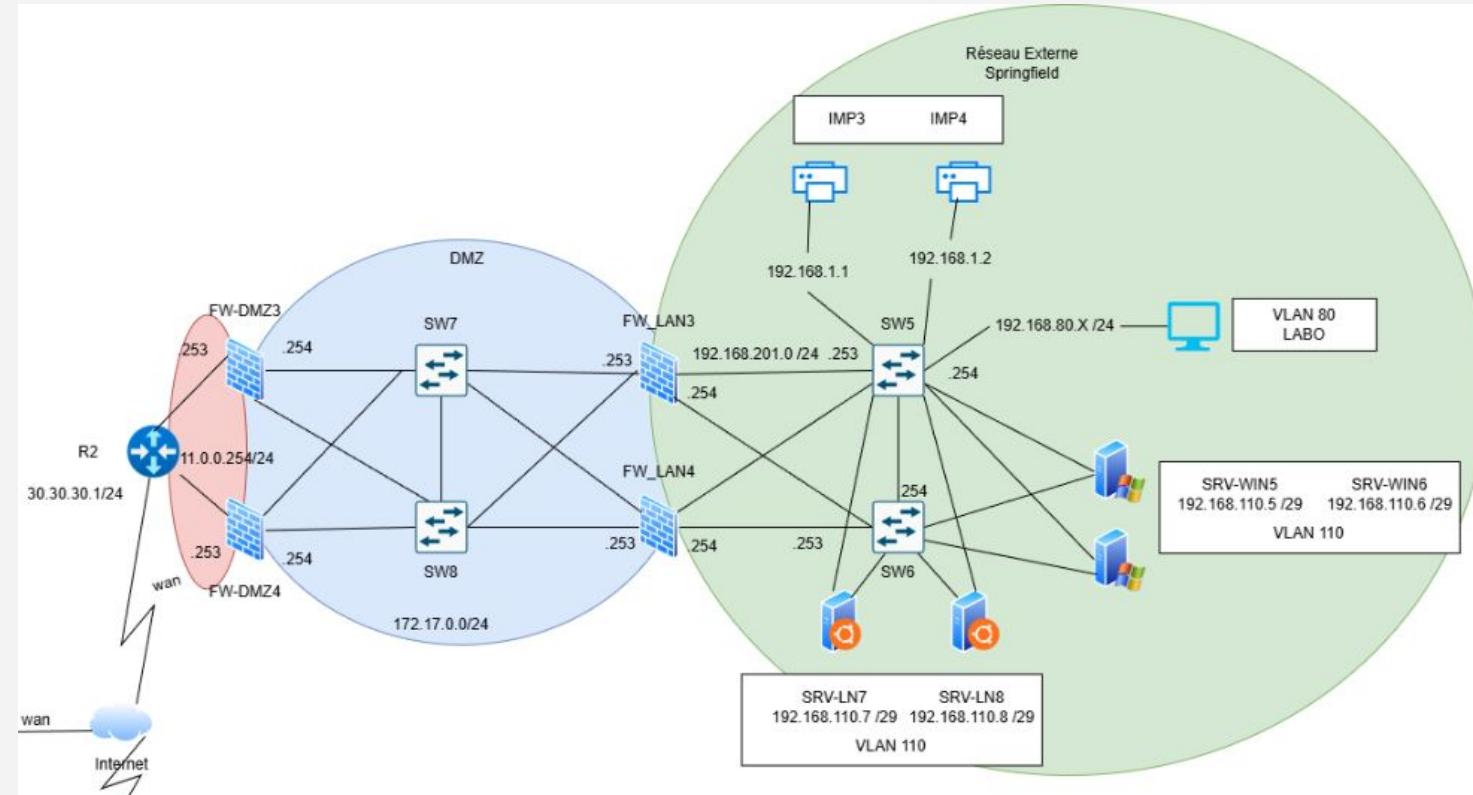
3. Conceptualisation de l'infrastructure



Conceptualisation : Site Atlantis



Conceptualisation : Site Springfield



4. Choix des solutions / matériel

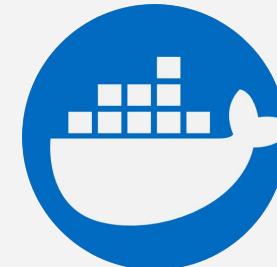


Microsoft
Active Directory



poste.io²

ZABBIX wazuh.



5. Sensibilisation

Audit de cybersécurité interne - Évaluation de la maturation

Évaluation de la posture de sécurité des systèmes d'information pour les entités Atlantis et Springfield.

1. Existe-t-il une Politique de Sécurité des Systèmes d'Information (PSSI) formalisée et validée par la direction ?

- Oui, validée et diffusée
- En cours de rédaction/validation
- Non

2. Une charte informatique a-t-elle été signée par l'ensemble des collaborateurs (Atlantis & Springfield) ?

- Oui, 100% signée et à jour
- Partiellement signée ou en cours de mise à jour
- Non

3. Où avez-vous le droit de stocker vos mots de passe ? (Une seule réponse)

choix multiples 0% moyenne du groupe

Sur un Post-it collé sous le clavier. 0%

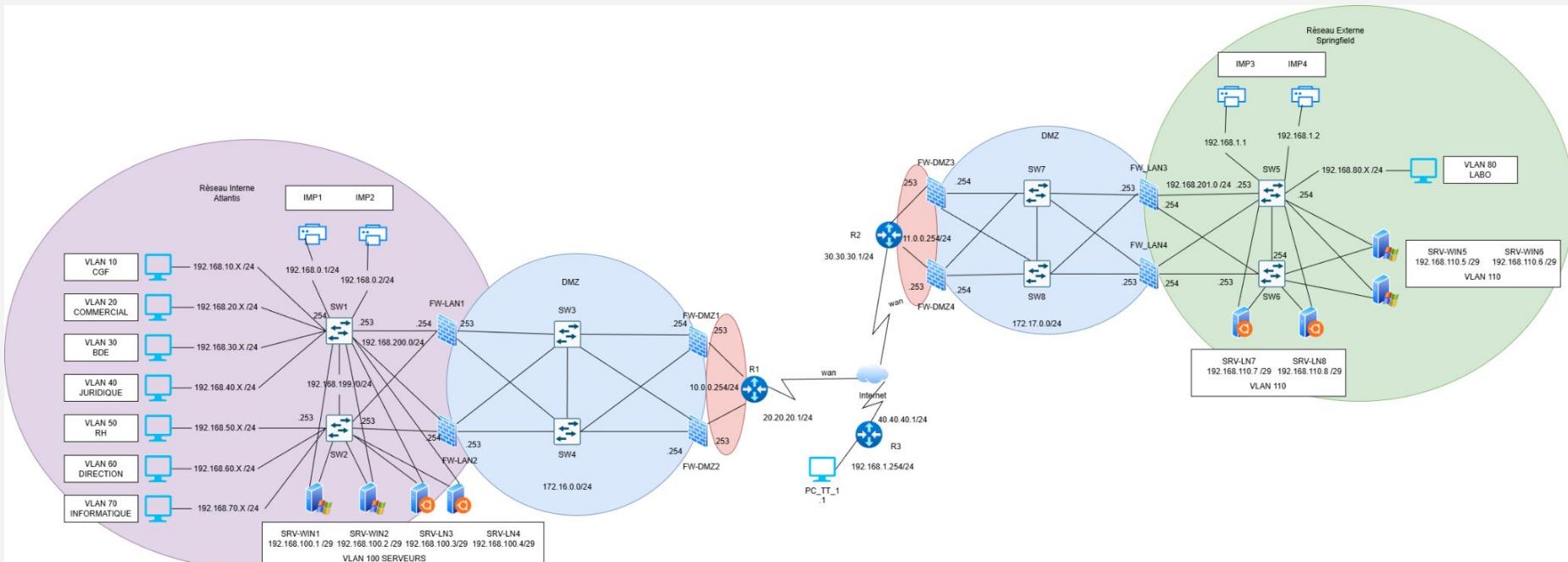
Dans un fichier Excel nommé "MotsDePasse" sur le bureau. 100%

Dans un gestionnaire de mots de passe sécurisé (ex: KeePass) validé par l'IT. 0%

Dans les brouillons de votre boîte mail. 0%

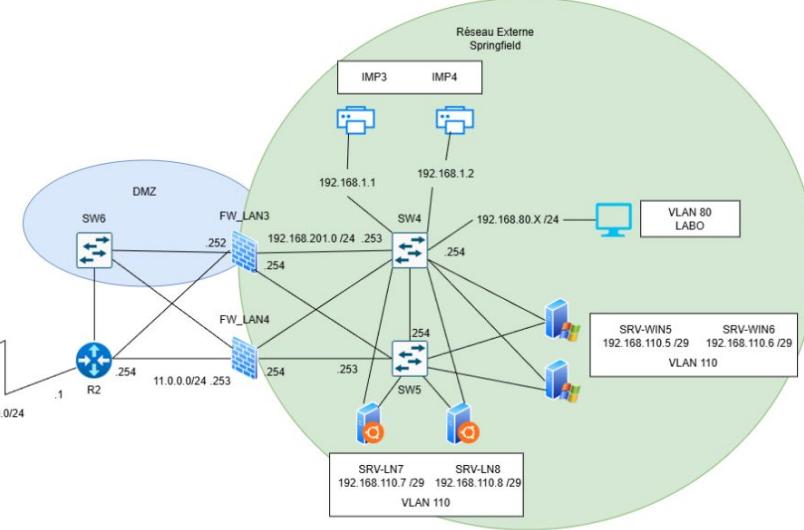
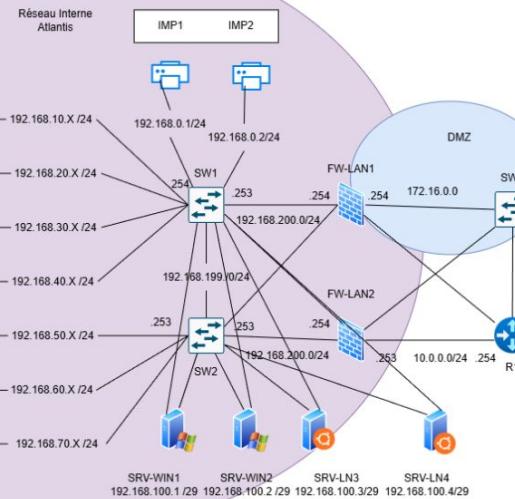
Les post-its et fichiers Excel sont lisibles par n'importe qui accédant physiquement ou logiquement à votre bureau.

6. Déploiement / Maquettage



6. Déploiement / Maquettage

Annexe 8.3



7. Optimisation administrative

- Génération automatique d'un mot de passe sécurisé (SecureString)
- Construction normalisée de l'adresse e-mail
- Création du compte Active Directory

```
2 references
function New-XanaduUser {
    param(
        [string]$FirstName,
        [string]$LastName,
        [string]$Username,
        [string]$Description,
        [string]$OUPath,
        [boolean]$isAdminAccount
    )

    # Générer un mot de passe sécurisé aléatoire
    $passwordObj = New-GenericPassword -Username $Username
    $Password = $passwordObj.SecureString      # Format SecureString pour AD
    $plainPassword = $passwordObj.PlainText     # Format texte pour affichage

    # Générer un nom complet unique (gère les homonymes automatiquement)
    $fullName = Get-UniqueFullName -FirstName $FirstName -LastName $LastName -OUPath $OUPath

    # Construire l'adresse email selon la convention @xanadu.com
    $mail = "$Username@xanadu.com"

    # Paramètres de création de l'utilisateur AD
    $userParams = @{
        Name          = $fullName                      # Nom d'affichage
        GivenName     = $firstName                     # Prénom
        Surname       = $lastName                      # Nom de famille
        SamAccountName = $username                     # Login
        AccountPassword = $password                    # Mot de passe sécurisé
        EmailAddress  = $mail                         # Email
        Description   = $description                  # Description du rôle
        Path          = $OUPath                       # OU de destination
        ChangePasswordAtLogon = $true                 # Forcer le changement de MDP
        Enabled        = $true                        # Activer le compte immédiatement
        ErrorAction    = 'Stop'                       # Arrêter en cas d'erreur
    }

    # Créer le compte utilisateur dans Active Directory
    New-ADUser @userParams

    # Retourner les informations du compte créé
    return @{
        FullName = $fullName
        Username = $Username
        Password = $plainPassword
        Email = $mail
    }
}
```

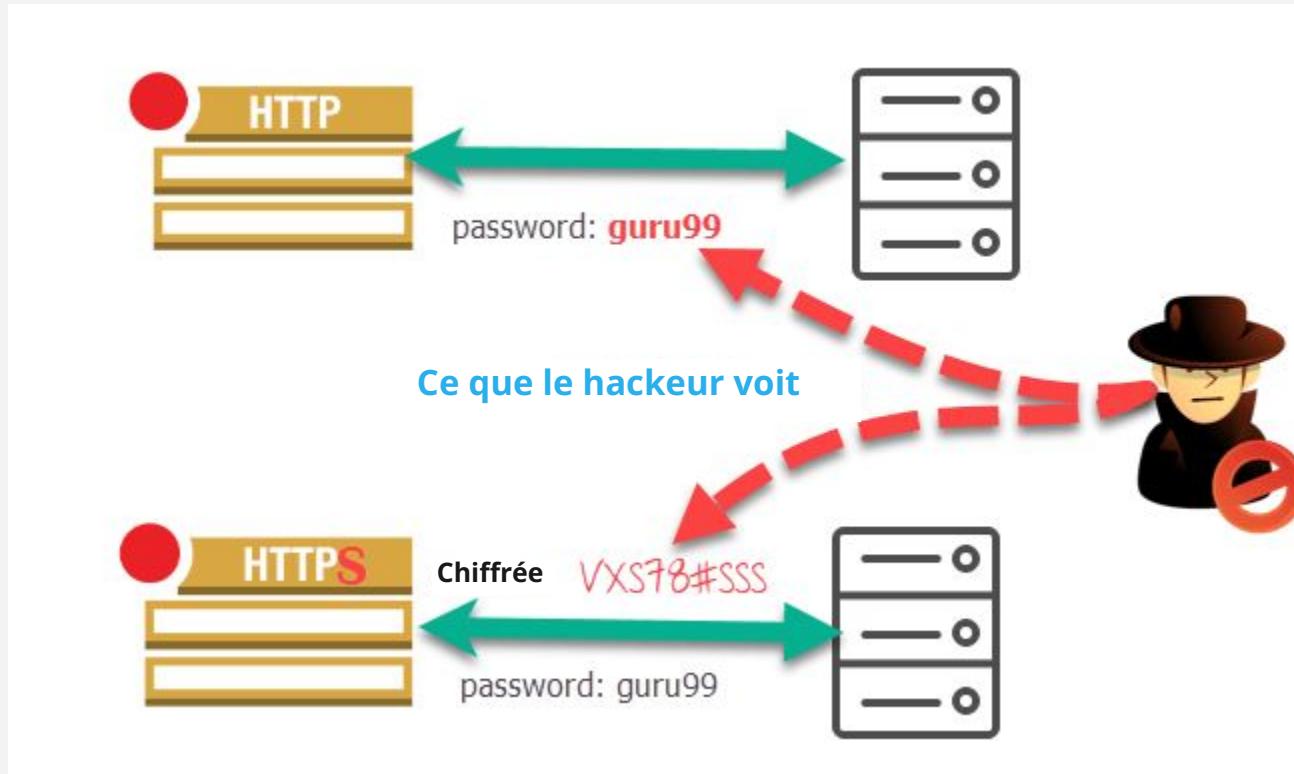
7. Optimisation administrative

```
165 #region DETERMINE_BACKUP_SCOPE
166
167 $referenceDate = $null
168
169 switch ($Type) {
170     "full" {
171         Write-Log "Sauvegarde complète : tous les fichiers seront copiés."
172     }
173     "dif" {
174         $referenceDate = [datetime]$state.LastFullDate
175         Write-Log "Sauvegarde différentielle : fichiers modifiés depuis la dernière complète du $referenceDate."
176     }
177     "inc" {
178         $referenceDate = [datetime]$state.LastBackupDate
179         Write-Log "Sauvegarde incrémentielle : fichiers modifiés depuis la dernière sauvegarde du $referenceDate."
180     }
181 }
182
183 #endregion DETERMINE_BACKUP_SCOPE
184
```



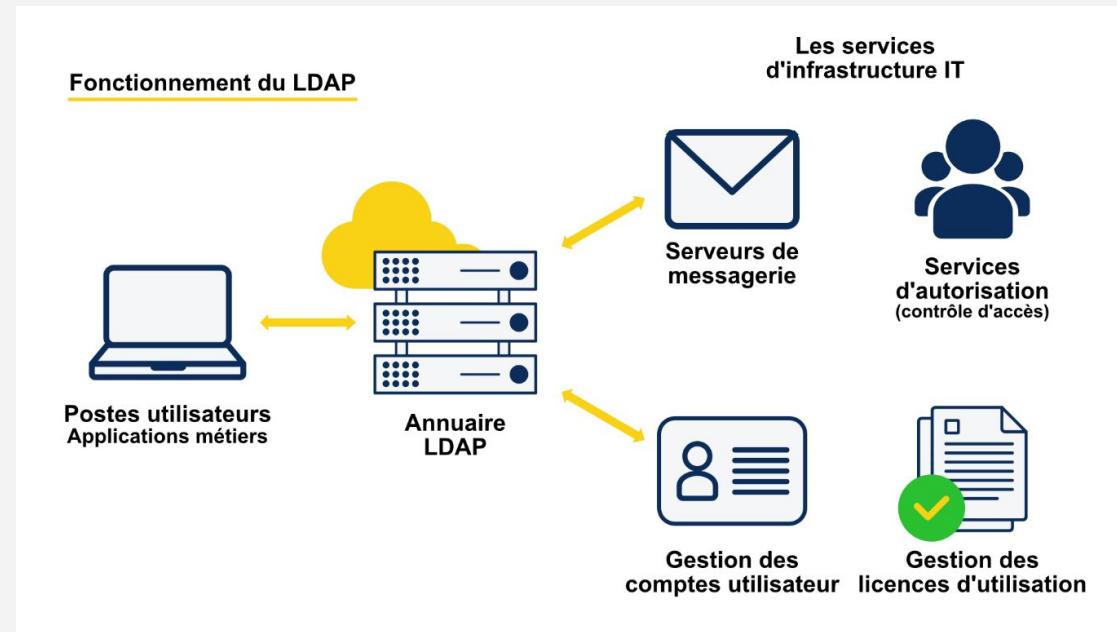
Résultats

HTTP / HTTPS

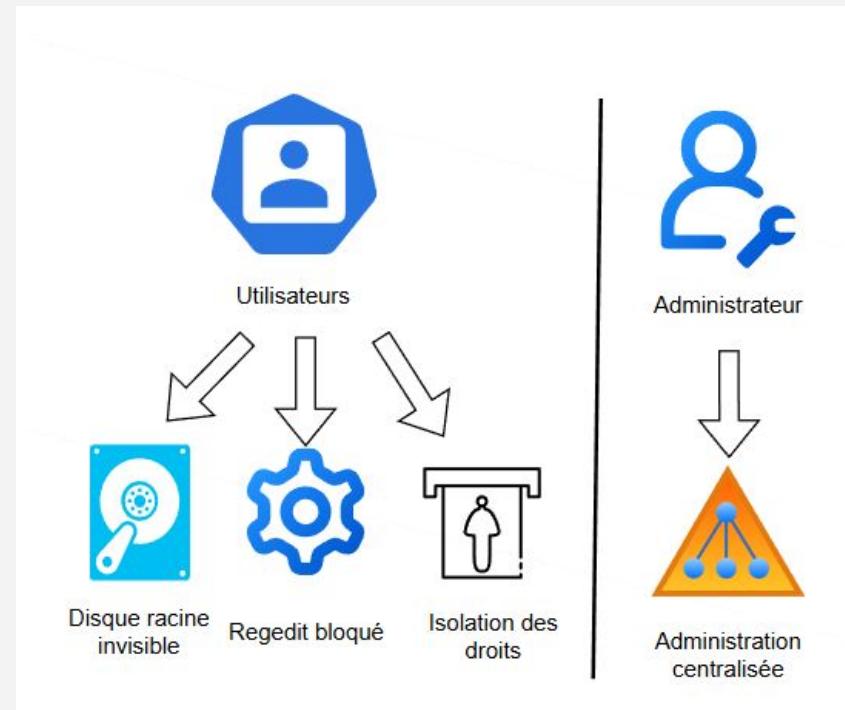
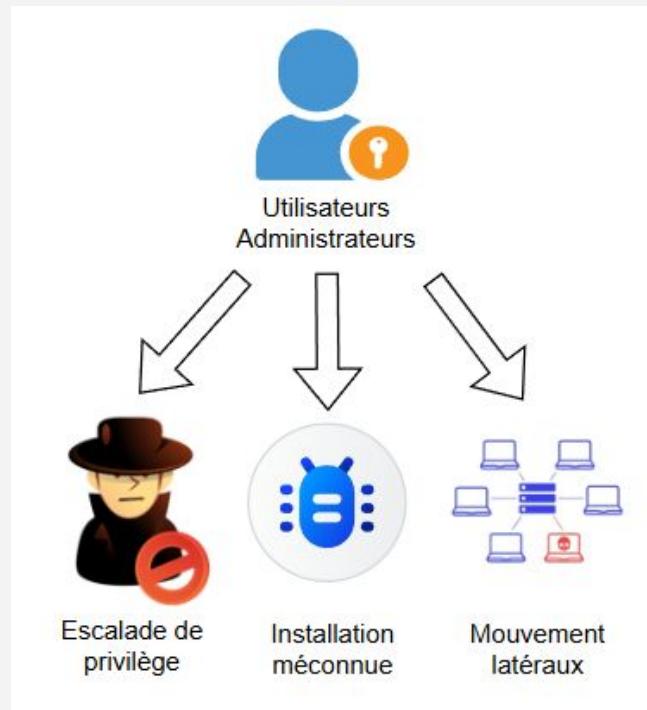


III - Résultats

ERP



Administration du poste



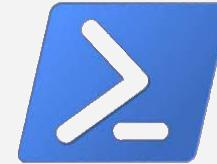
Sauvegarde

Mise en oeuvre	Bénéfices
Sauvegardes non exposées	Disponibilité (résilience ransomware)
RTO respectés (4h / 24h)	Disponibilité (continuité d'activité)
Flux & données chiffrés	Confidentialité (protection des données)
Sauvegardes automatisées et contrôlées	Intégrité & Traçabilité (Fiabilité)

Conclusion



Sécurisation renforcée et
sauvegardes (filtrage,
isolation)



Optimisation de
l'administration
(automatisation des tâches
récurrentes)



Administration centralisée
et redondance des services

Retour sur expérience

NUMÉRO	TITRE DE LA TÂCHE	PROPRIÉTAIRE DE LA TÂCHE	LIVRABLE 1					LIVRABLE 2					LIVRABLE 3									
			SEMAINE 1		SEMAINE 2			SEMAINE 3		SEMAINE 4			SEMAINE 5									
			L	M	M	J	V	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V
1	Livrable 1																					
1.1	Compréhension des tâches	Tous																				
1.2	Définition des politiques	Tous																				
1.3	Conceptualisation de l'infrastructure	Tous																				
1.4	Choix des solutions / matériel	Tous																				
2	Livrable 2																					
2.1	Sensibilisation à la cybersécurité	Philippe																				
2.2	Optimisation de l'administration	Mathéo, Antonin																				
2.3	Sauvegardes des données	Alexandre																				
3	Livrable 3																					
3.1	Déploiement de l'infrastructure	Allan, Philippe																				

Retour sur expérience

The image shows a digital dashboard with four main sections, each containing a list of items categorized by color-coded tags (Securite, Reseau, Systeme).

- Facultatif** (Grey background):
 - Securite: PENTEST
 - Securite: Audit de sécurité
 - Securite: PHISHING
 - Securite: PPTX de formation & prevention à la cyber
 - Systeme: Securite: DNSSec
- EQUIPEMENTS** (Dark grey background):
 - Reseau: Securite: OPEN VPN (ROUTE CLIENT)
 - Reseau: Securite: Anti ARP Flooding
 - Systeme: Securite: SAUVEGARDE
- Livrable 3 19/12** (Dark grey background):
 - Reseau: Systeme: Securite: DC2 (checkboxed 0/6)
 - Reseau: Systeme: Securite: DC3 (checkboxed 0/6)
 - Systeme: Securite: Droits et accès
 - Securite: FW_LAN2
 - Securite: FW_LAN3
 - Securite: FW_LAN4
- Livrable 2 18/12** (Dark grey background):
 - Securite: FW_LAN (checkboxed 0/3)
 - Reseau: Securite: Politique + règles de filtrage (firewall)

Each card has a "Ajouter une carte" (Add a card) button at the bottom right.

Merci



informatique@cesitech.com
+33 4 89 74 52 63
CESITECH.com



CESI 
ÉCOLE D'INGÉNIEURS