synetis

Pourquoi et comment durcir son annuaire Active Directory ?

JoSy Sécurisation Active Directory - RESINFO

25/06/2024

TLP:GREEN

INTERVENANT

synetis

Camille JOUDRIER
Consultante sécurité
Opérationnelle

06 58 43 36 37
camille.joudrier@synetis.com

SOMMAIRE

TLP:GREEN


01
SYNETIS
SYNETIS

SYNETIS TOURNÉES VERS LA SÉCURITÉ ACTIVE DIRECTORY

Gouvernance, Risques et Conformité :
Identifier les risques

Identité Numérique :
Cycle de vie des comptes Microsoft et qualité des données

CERT :
Réponse à incidents en cas de compromission du SI

Sécurité Opérationnelle :
Durcissement des solutions Microsoft, détection des attaques et Services Managés Microsoft

Audits SSI :
Test d'intrusion / Red team

Formation :
Qualiopi sur la sécurité des solutions Microsoft

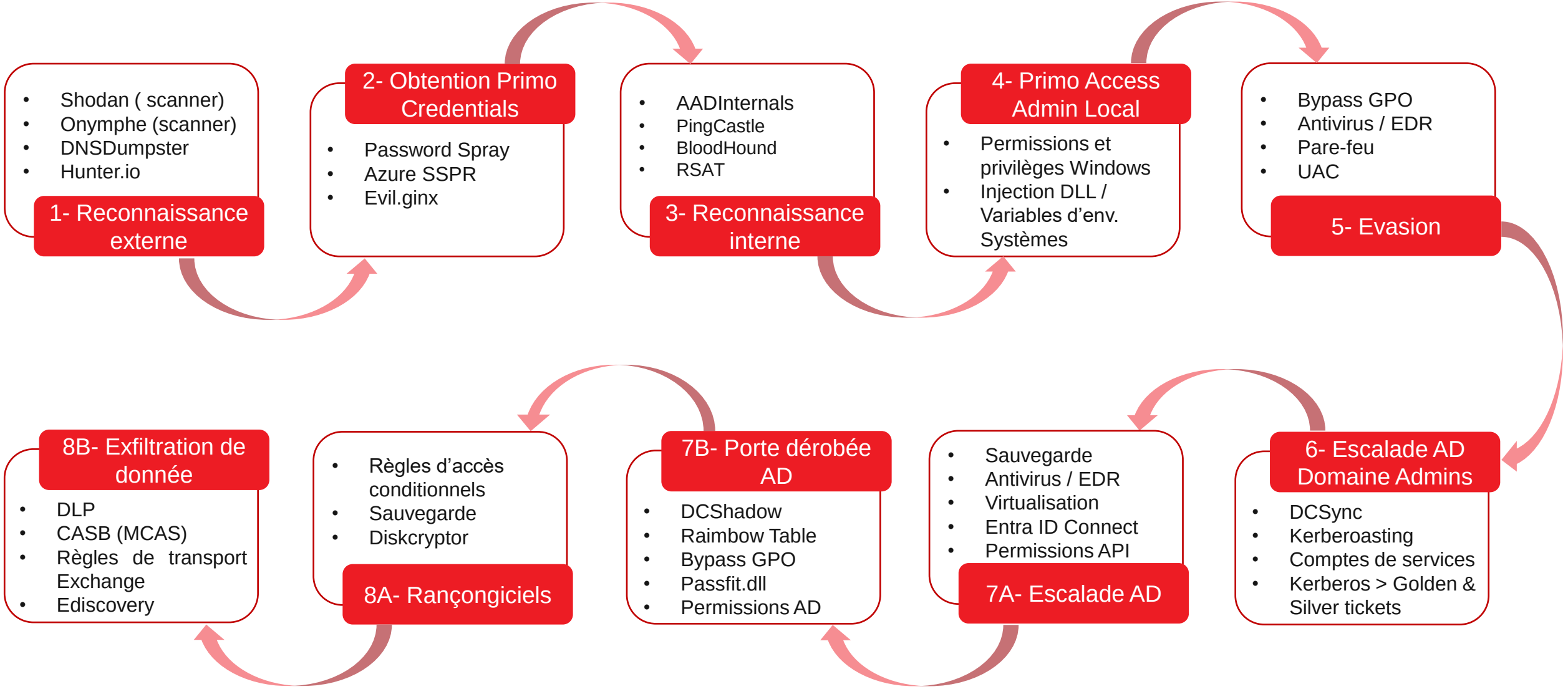
Auditer → Conseiller → Construire → Opérer → Réagir


02
SYNETIS
POURQUOI DURCIR SON
ANNUAIRE ACTIVE DIRECTORY ?

Pourquoi durcir Active Directory ?

- La majorité des attaques ciblent l'annuaire AD.
- Si l'annuaire est compromis, tout le SI est compromis.

EXEMPLE DE KILLCHAIN SUR L'ACTIVE DIRECTORY

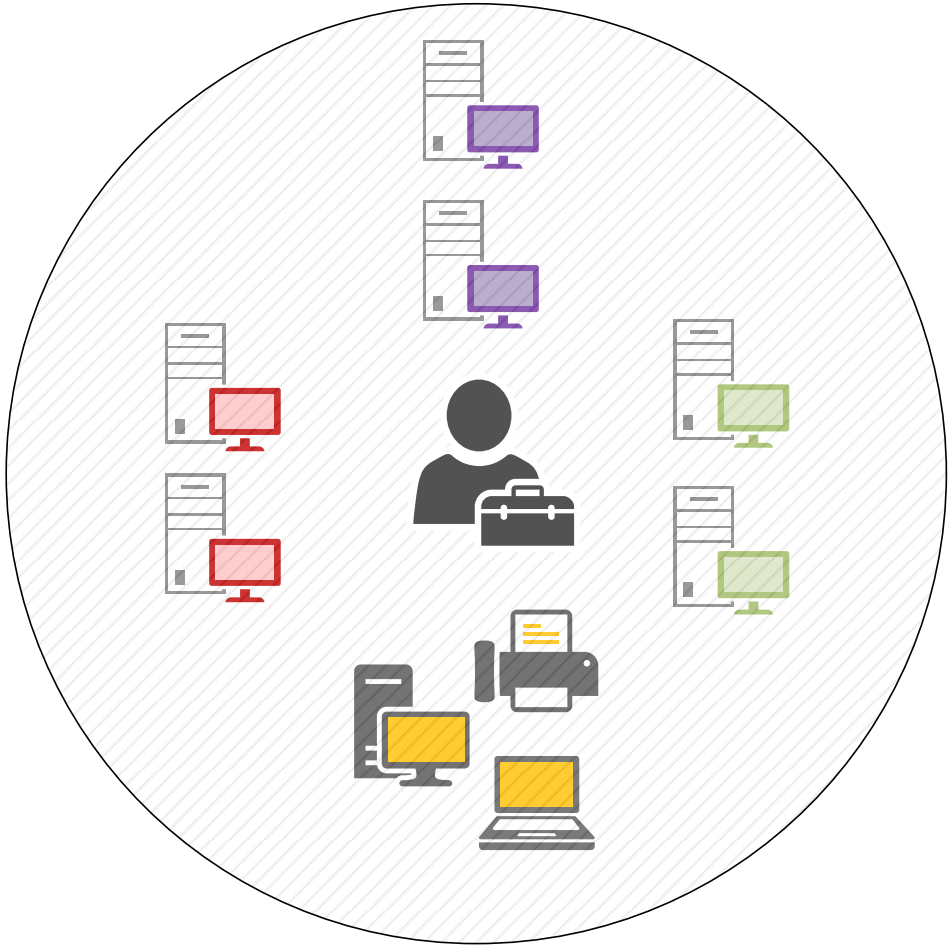


PROPAGATION D'UNE ATTAQUE

Un parc informatique est composé de différents type de point d'accès :

- DC, PKI, DNS, … (en violet)
- Serveur d'application ou d'infrastructure (en vert)
- Station de travail, MFP, … (en jaune)
- Système hérité (en rouge)

Problème : sans une configuration spécifique, n'importe-qui est à même de se connecter sur n'importe-quel système avec un compte à privilège.



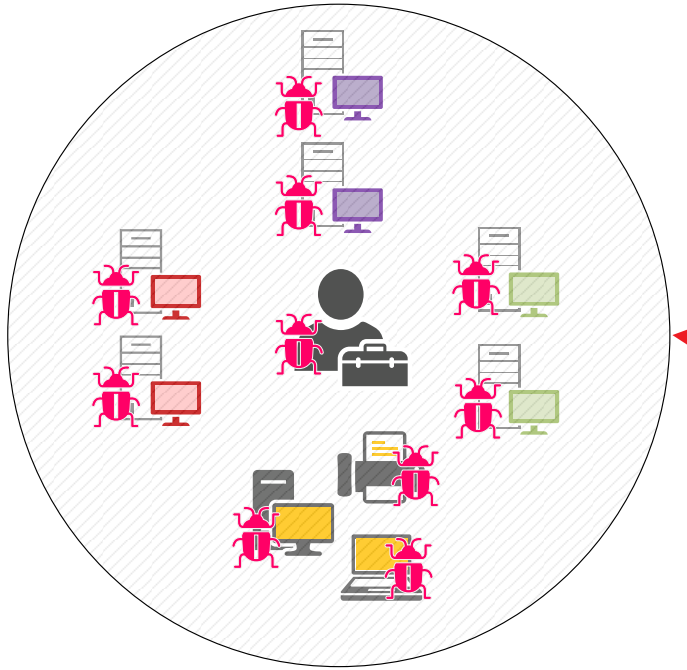
Un compte unique peut gérer tout les types de système

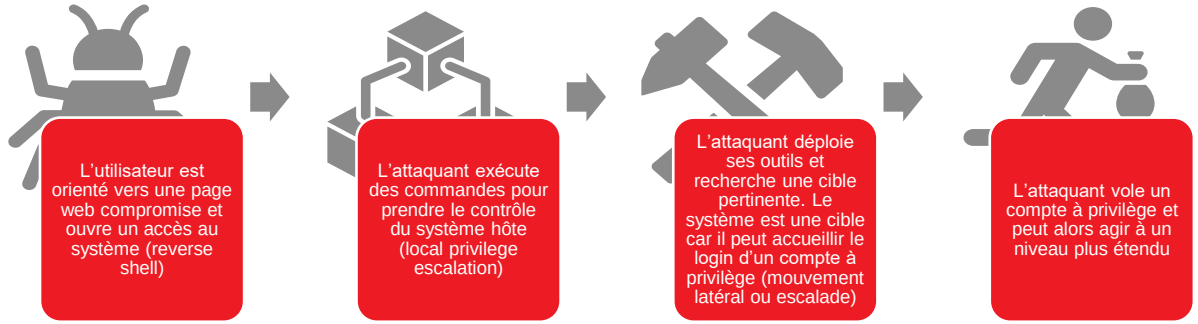
PROPAGATION D'UNE ATTAQUE

Un attaquant chercher à prendre le contrôle du domaine AD, le groupe Domain Admins est par défaut membre du groupe Administrateurs de la base SAM de chaque machine membre du domaine.

Scénarios possibles :

- Compromission de l'accès au réseau de l'entreprise.
- Compromission d'une machine.
- Vol d'une identité privilégiée et escalade sur plusieurs machines.
- Prise de contrôle de l'ensemble du domaine AD via des mouvements latéraux et des escalades de privilèges.
- Obtention d'un accès Domain Admins et donc prise de contrôle de toutes les machines membres du domaine AD.





03

SYNETIS

COMMENT SÉCURISER SON ANNUAIRE ACTIVE DIRECTORY (THÉORIE)

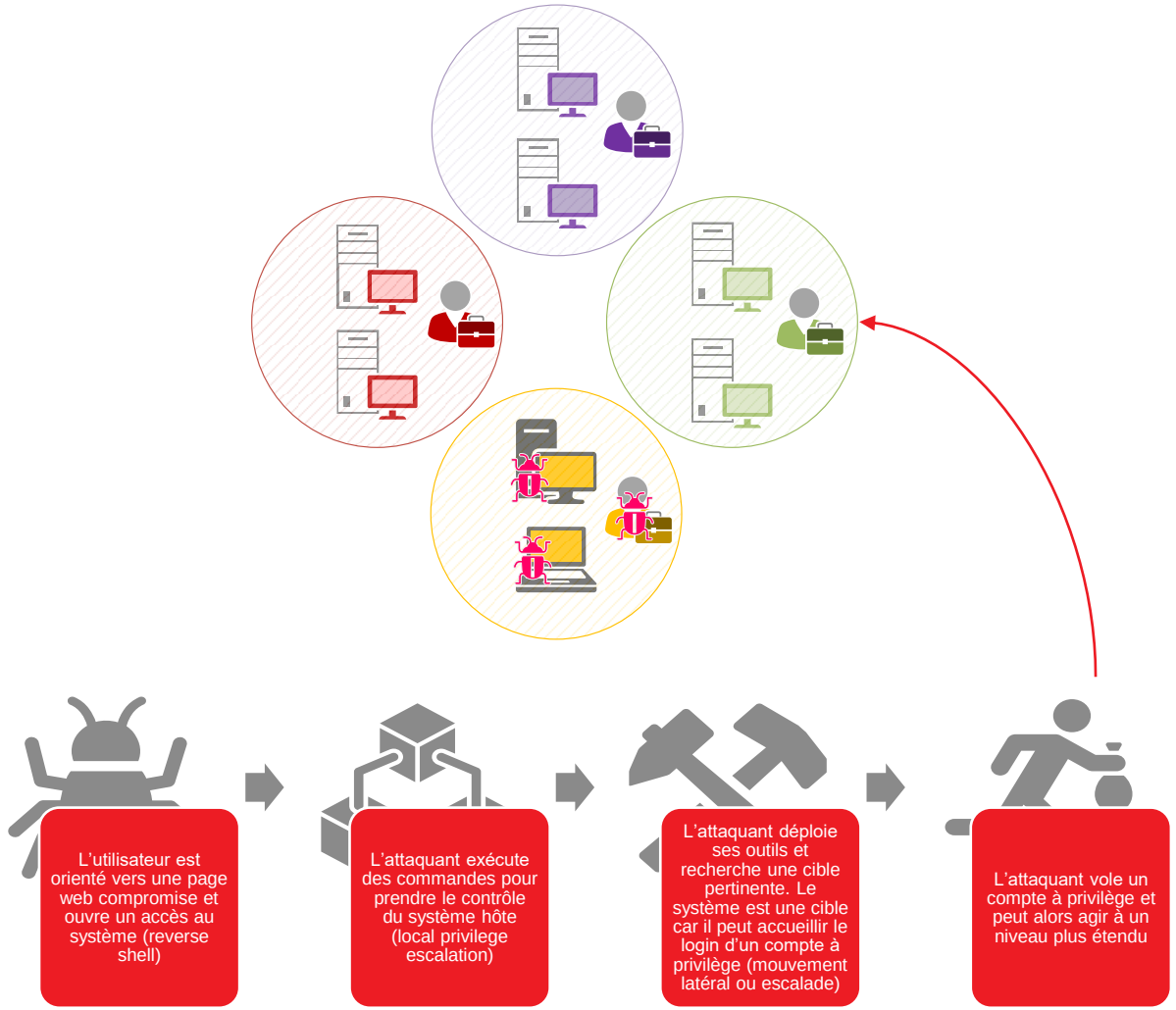
MISE EN PLACE DE ZONES D'ADMINISTRATIONS

En isolant les systèmes en fonction du risque qu'ils représentent pour l'entreprise, il est possible de limiter la portée d'une attaque.

Scénarios :

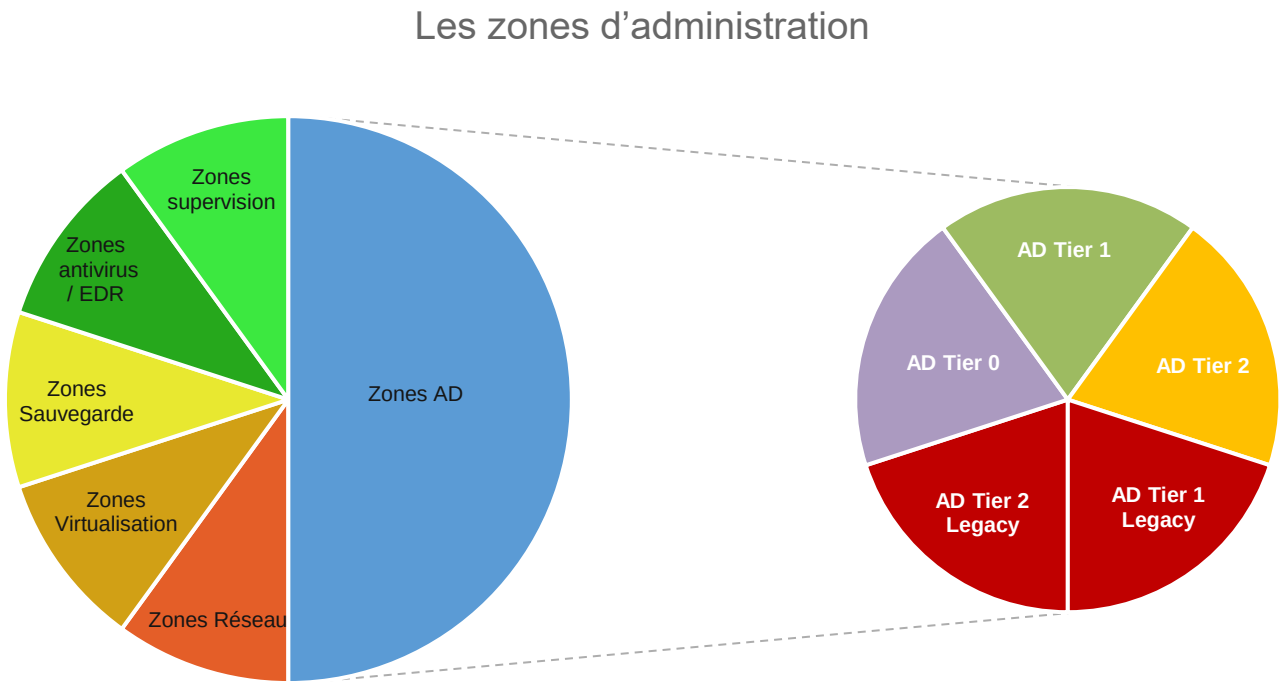
- Compromission de l'accès au réseau de l'entreprise.
- Compromission d'une machine.
- Vol d'une identité à privilège et escalade sur les autres machines du même Tier. L'attaquant ne peut pas escalader vers d'autres Tier AD car les secrets des comptes AD d'administration des autres Tiers AD ne sont pas présents sur les machines compromis.
- L'attaquant est bloqué au niveau du Tier qu'il a compromis initialement.

Pour prendre le contrôle du SI, l'attaquant doit prendre le contrôle du Tier 0 AD pour désactiver/contourner le modèle de tiering.



LE TIERING A L'ECHELLE DU SI

L'ANSSI préconise de découper le SI administrer en zones de confiance. A une zone de confiance correspond une zone d'administration.



Les recommandations Synetis :

- Réduire au maximum les dépendances entre l'annuaire AD et les autres composants du SI :
  - Infrastructure de virtualisation dédiée pour héberger les machines Tier 0 AD.
  - Protéger les sauvegardes AD contre les accès non autorisés
- **1 zone d'administration = 1 Tier**
- **1 Tier = 1 comptes d'administration dédié**
- Déployer des serveurs d'administration (PAW) dédié pour administrer les équipements Tier 0 AD et les autres équipements critiques du SI (hyperviseurs, sauvegarde, antivirus, etc.)
- Déployer des serveurs d'administration pour gérer les autres Tiers AD et reste du SI.

LE MODÈLE DE SÉCURITÉ AD

Tier 0 – Authentification, centre de données et sauvegarde

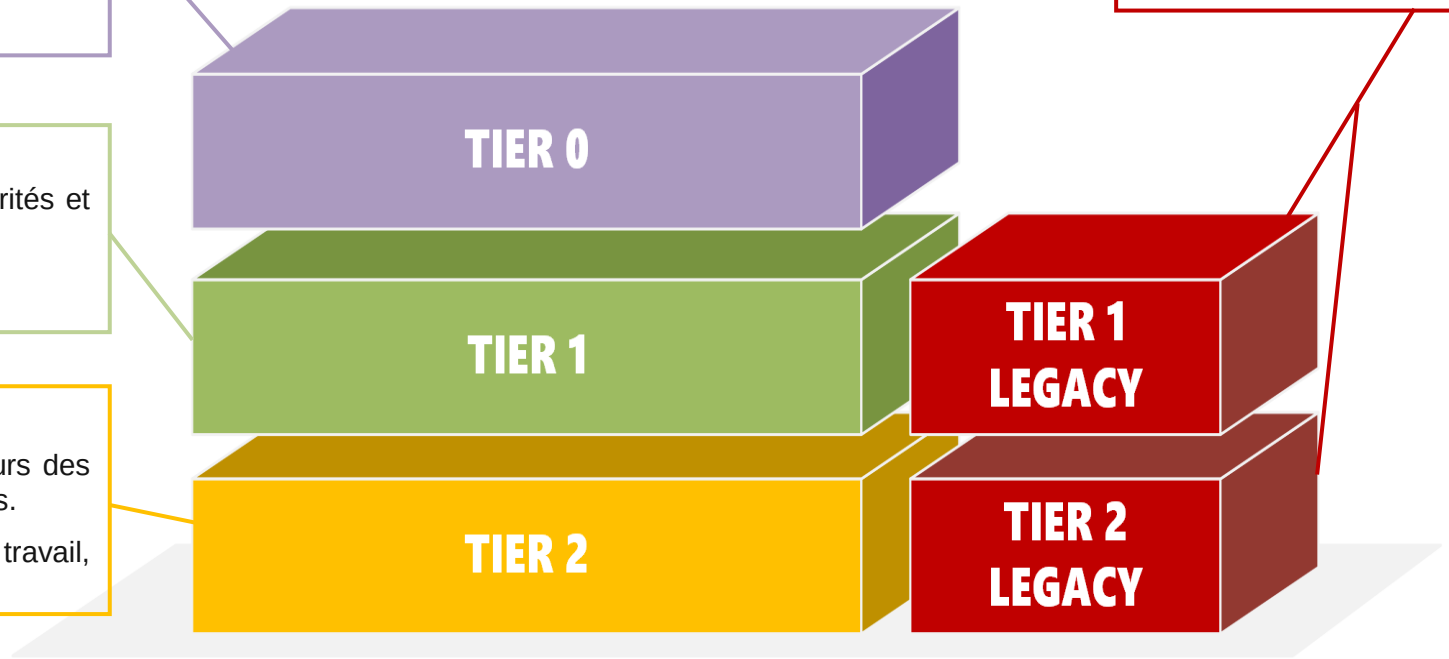
- Contrôleurs de domaine
- Serveurs d'autorité de certification (PKI - AD CS)
- Serveurs d'authentifications ou d'infrastructure (Radius, ADFS, DHCP, …)
- Serveurs de synchronisation (Entra ID Connect)

Tier 1 – Serveurs et applications métiers

- Gestion des comptes de services, groupes de sécurités et des comptes ordinateurs des serveurs.
- Accès administrateur local sur les serveurs tier 1.

Tier 2 – Comptes utilisateurs et station de travail

- Gestion des comptes utilisateurs, comptes ordinateurs des stations de travails et des appartenances aux groupes.
- Accès administrateur local sur les stations de travail, terminaux mobiles et imprimantes.



Tier Legacy – Serveurs et stations de travail avec un OS non supporté

- Accès avec un compte administrateur local.

04

SYNETIS

COMMENT SÉCURISER SON ANNUAIRE ACTIVE DIRECTORY (PRATIQUE)

LE MODELE HARDEN AD

- La **communauté Harden** a été cofondée par Guillaume MATHIEU manager de l'équipe sécurité opérationnelle chez **Synetis**.
- L'objectif de la communauté est d'accompagner les entreprises de toutes tailles dans l'amélioration de la sécurité de leurs en commençant par l'Active Directory.
- La solution Harden AD permet de facilité la sécurisation AD pour les équipes techniques.

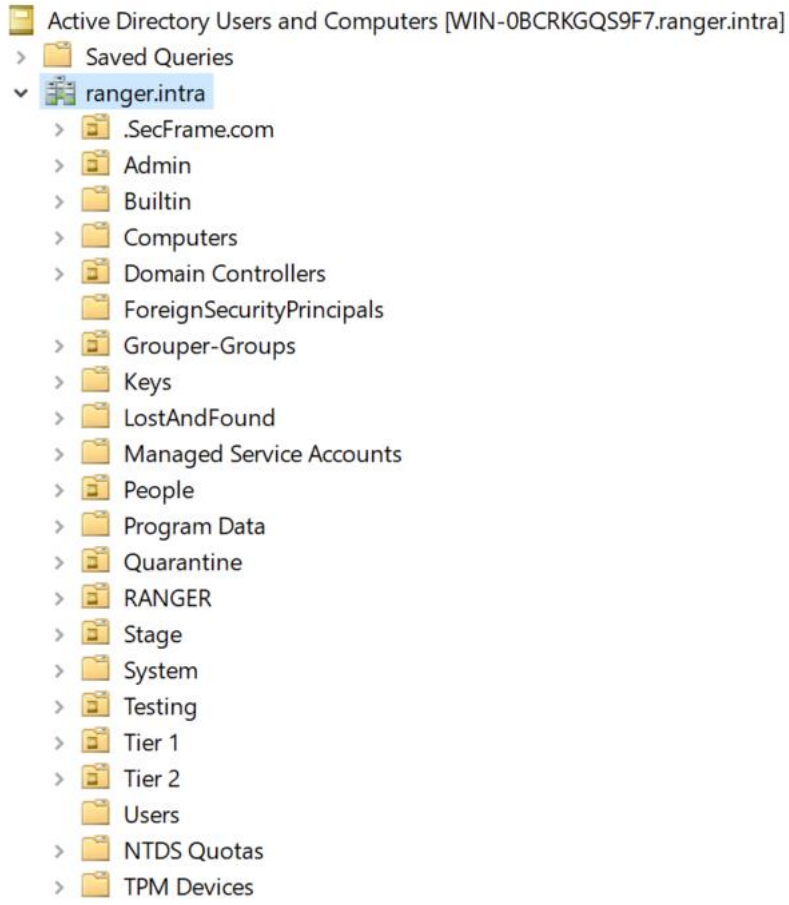
Des scripts PowerShell et un fichier de configuration xml.

Une solution personnalisable pour s'adapter aux besoins et à l'infrastructure client.

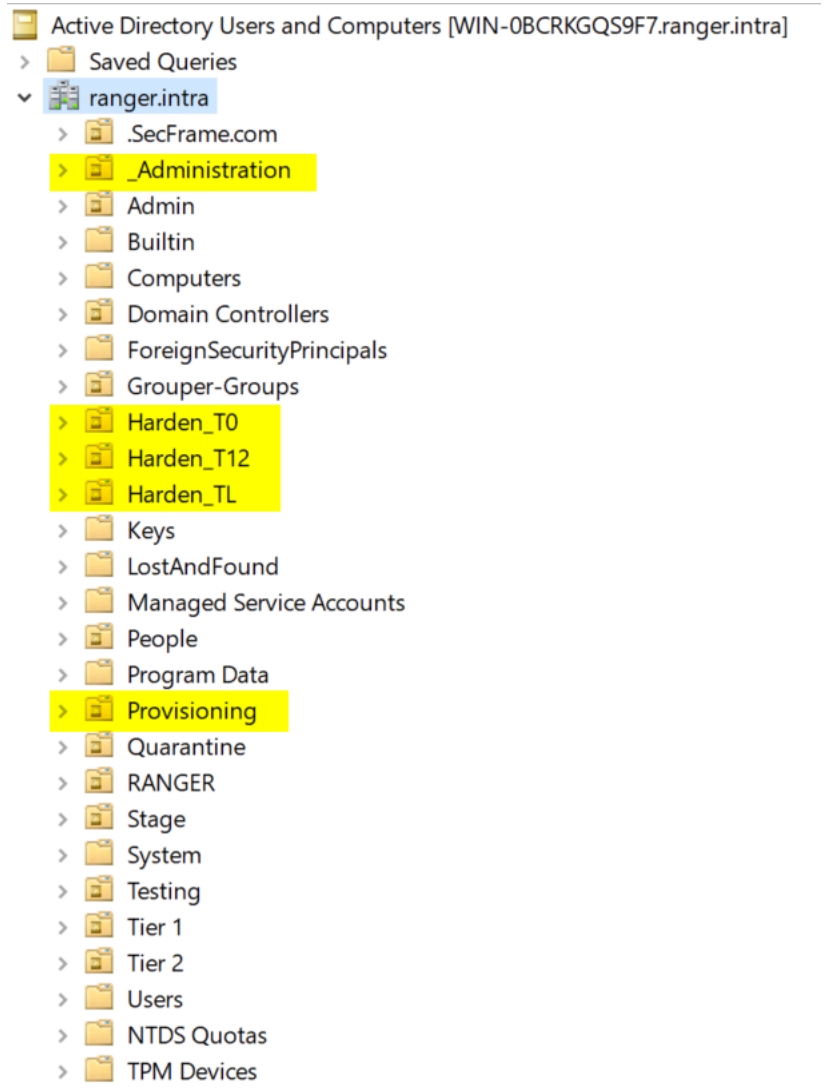
Une solution Open Source

Les experts de la communauté pour vous accompagner sur le modèle.

ADAPTATION DE L'ARCHITECTURE AD



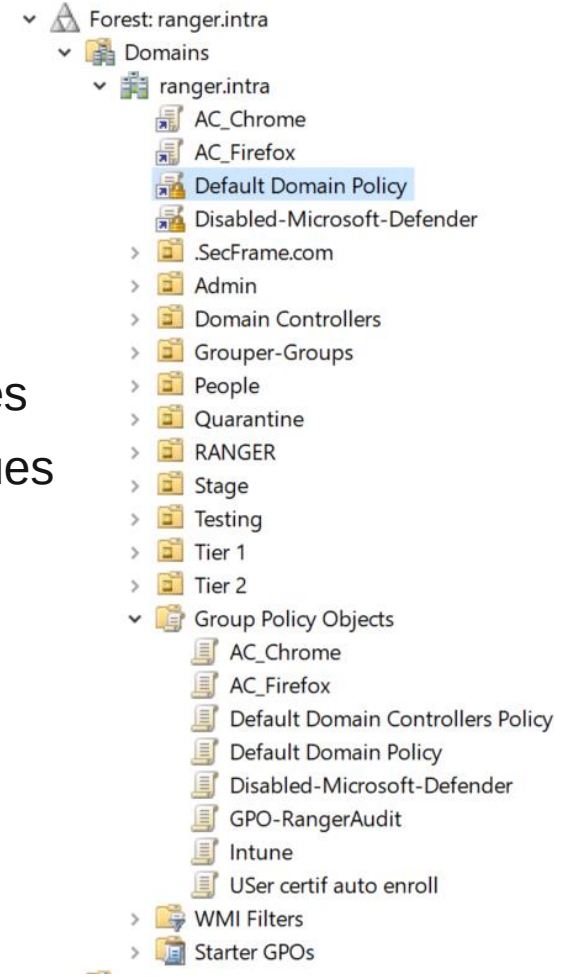
Déploiement du modèle de sécurité AD.



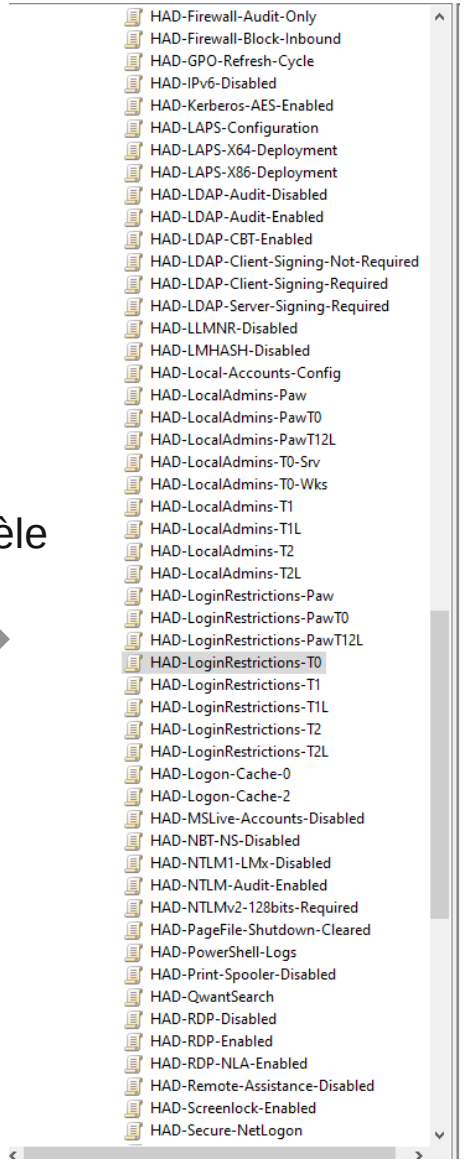
DURCISSEMENT GRACE AUX GPO

Plus de 80 GPO :

- Désactivation de protocoles à risques
- Implémentations des bonnes pratiques
- Restriction de login
- Patching

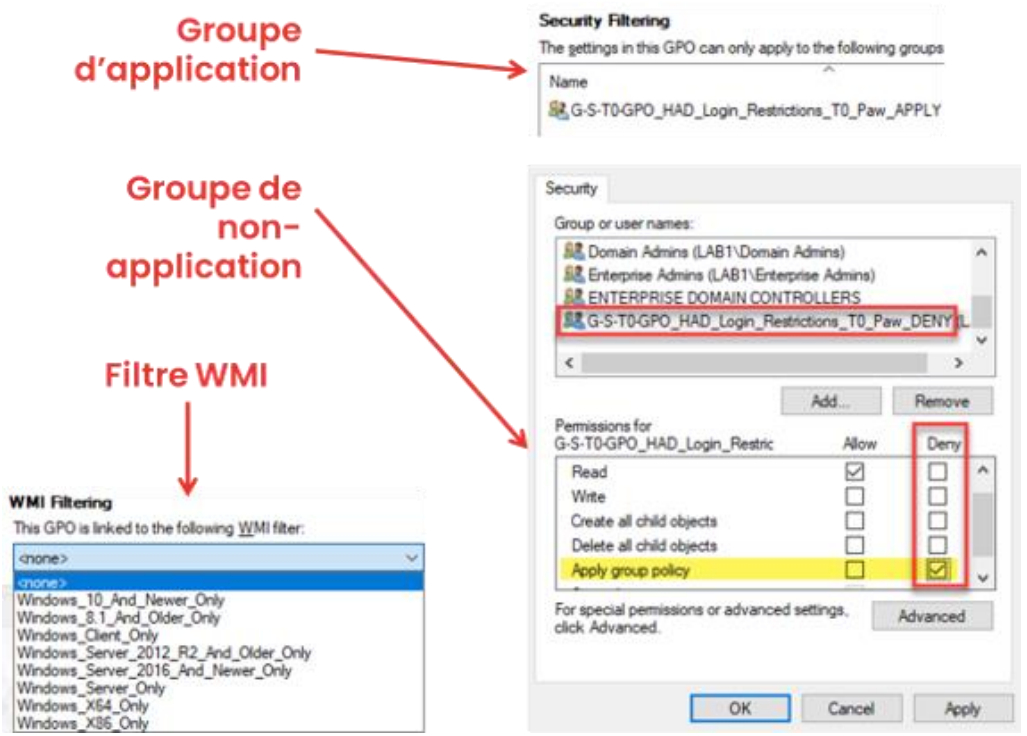


Déploiement du modèle de sécurité AD.



COMMENT METTRE EN PLACE LE MODELE ?

- Définition de l'architecture cible :
  - Topologie d'OU
  - Analyse des GPO à appliquer
  - Analyse des conflits potentiels avec les GPO existantes
  - Personnalisation du modèle
- Déploiement sans impact
- Mise en pilote :
  - Activation des GPO pour les machines du pilote
  - Recette
- Généralisation du modèle



Déploiement sans impact


?
DISCUSSION OUVERTE

contact@synetis.com
+33 1 47 64 48 66

www.synetis.com
19 rue du Général Foy, 75008 Paris
2 rue Claude Chappe, 35510 Cesson-Sévigné