

FICHE 6 – APPORTS THÉORIQUES

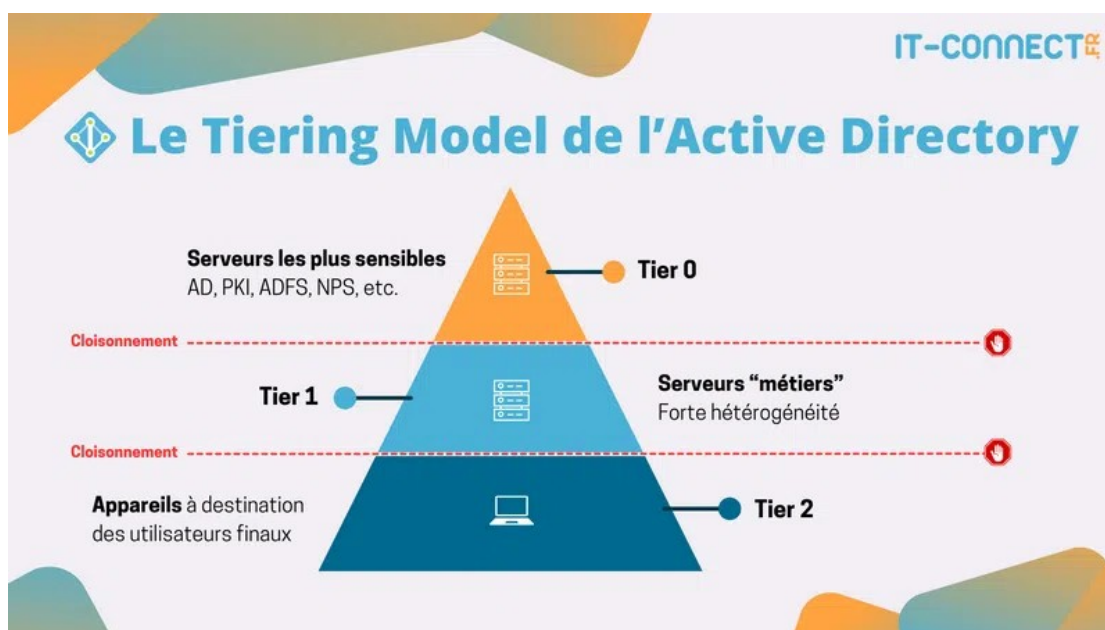
LA NOTION DE TIERING DANS UN ENVIRONNEMENT MICROSOFT (SOURCE : FLORIAN BURNEL SUR LE SITE IT CONNECT)

A. INTRODUCTION

Dans un environnement Active Directory, la sécurité des comptes à privilèges et leur cloisonnement représente un enjeu majeur. La compromission d'un seul compte administrateur membre du groupe "Admins du domaine" peut avoir d'énormes conséquences sur l'ensemble du système d'information d'une entreprise. En effet, comme nous le verrons, l'attaquant détient alors les clés du royaume.

Pour répondre à cette problématique, le modèle en couches, que l'on appelle aussi Tiering Model, propose une segmentation stricte des comptes afin de limiter l'impact d'une intrusion ou d'une compromission de compte. Ce modèle, recommandé par Microsoft, l'ANSSI et de nombreux experts en Active Directory, repose sur un découpage en plusieurs niveaux (couches).

B. NOTION DE TIERS

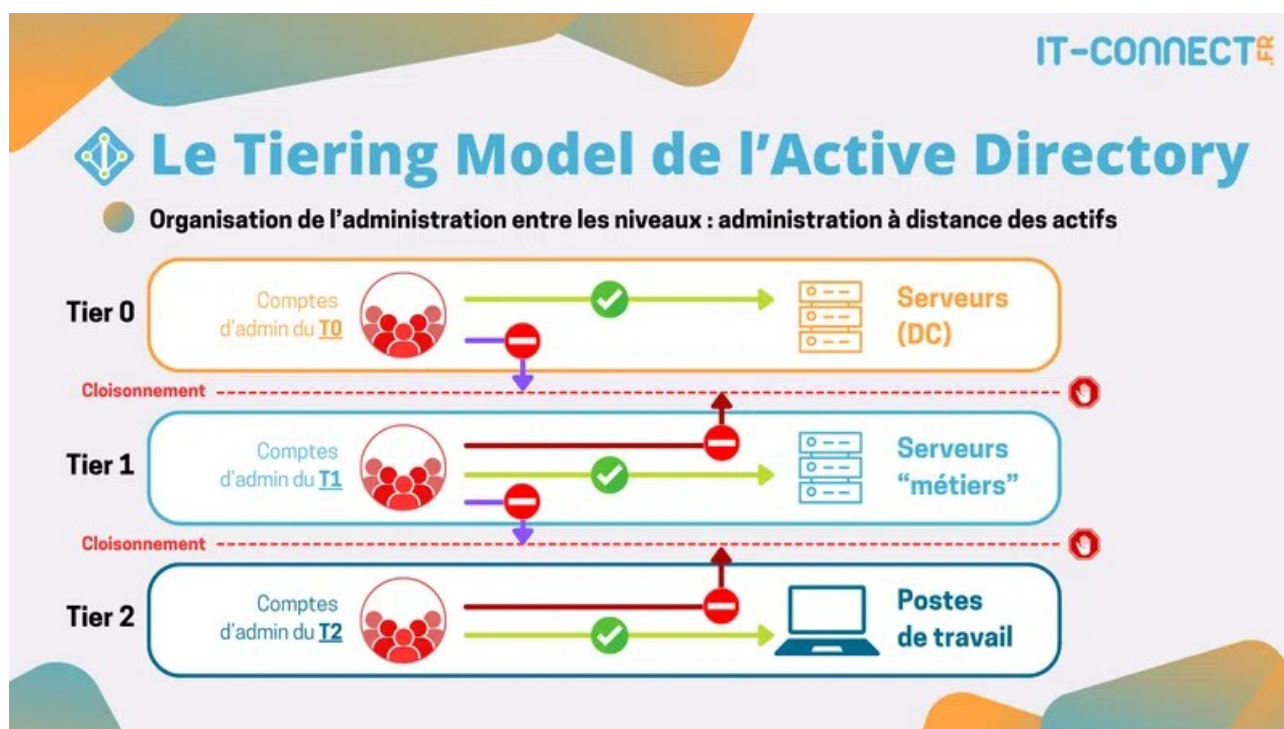


Le Tier 0 comprend les actifs les plus sensibles du système d'information (hyperviseurs, pki, contrôleurs de domaine, etc), à savoir ceux liés à la gestion des identités. Il représente le haut de la pyramide ! Les privilèges d'administration de ce Tier sont les plus élevés puisqu'ils offrent un contrôle sur l'annuaire Active Directory, ainsi que la possibilité de reprendre la main sur les autres Tier.

Le Tier 1 correspond au niveau intermédiaire de notre pyramide. Il concerne les serveurs, notamment ceux liés à l'activité de l'entreprise et qui ont une dimension « métier ». Nous n'irons pas jusqu'à dire que ce Tier est un « fourre-tout » pour les serveurs, mais il y a une grande hétérogénéité. Il accueillera notamment les serveurs qui n'ont pas leur place dans le Tier 0.

Le Tier 2 correspond au troisième niveau, c'est-à-dire le plus bas de notre pyramide. Ce Tier contient les appareils et périphériques des utilisateurs

C. PRINCIPE DE FONCTIONNEMENT



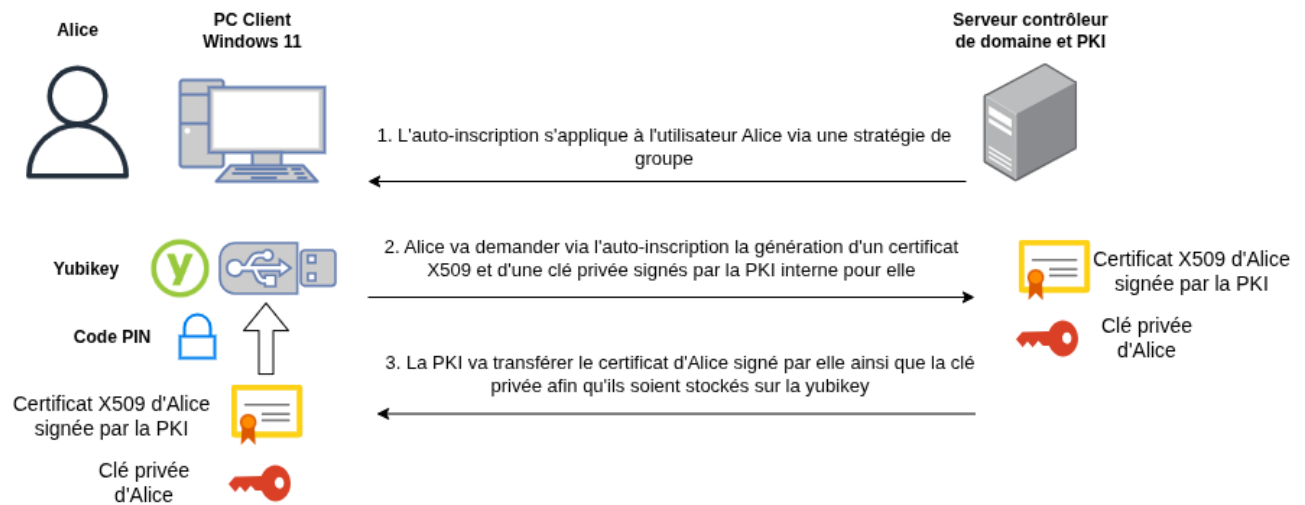
Les comptes d'administration du Tier 0 pourront être utilisés pour effectuer l'administration à distance des serveurs du Tier 0 (et c'est tout !). Cette logique se répète pour les deux autres niveaux. Ainsi, un compte T0 ne pourra pas administrer un poste de travail : il n'a pas ce privilège ! À l'inverse, un compte T2 permettra à l'administrateur système d'agir sur un poste de travail dans le cadre d'un dépannage, mais ne lui permettra de se connecter sur un serveur du T1 ou du T0.

L'AUTHENTIFICATION PAR CERTIFICAT ET CARTE À PUCE (SMARTCARD / PIV)

L'authentification SmartCard / PIV est une authentification forte dont l'implémentation a été proposée par le NIST (National Institute of Standards and Technology), un institut américain. Elle consiste à générer des certificats X509 signés par une PKI interne et des clés privées pour les utilisateurs. Ces certificats et ces clés privées ont la particularité d'être stockés dans une carte à puce (ou des clés de sécurité matérielles) protégés par un code PIN.

Elle a permis de renforcer nettement les processus d'authentification dans des environnements sensibles dont les domaines Windows non externalisés.

A. SCHÉMA DE PRINCIPE DE LA GÉNÉRATION D'UN CERTIFICAT ET D'UNE CLÉ PRIVÉE POUR UN UTILISATEUR



B. SCHÉMA DE PRINCIPE DE L'AUTHENTIFICATION SMARTCARD PIV SUR UN CONTRÔLEUR DE DOMAINE UTILISANT LE PROTOCOLE KERBEROS

