# Signature LDAP non requise sur les contrôleurs de domaine

ID METSYS : 23  
ID PurplKnight : [LDAP signing is not required on Domain Controllers](https://www.purple-knight.com/fr/security-indicators/)

Charge de travail : 2 jours  
Difficulté : 4 - Requière des connaissances avancées sur l'infrastructure et de l'anomalie qu'elle contient

****Description****

Le trafic réseau non signé est exposé aux attaques MiTM (Man-in-the-Middle), où les attaquants modifient les paquets et les transmettent au serveur LDAP, ce qui amène le serveur à prendre des décisions basées sur des demandes falsifiées provenant du client LDAP.

****Recommandation****

Les modifications requises par cet indicateur dans l'AD sont très délicates et peuvent entraîner des problèmes dans votre domaine si elles ne sont pas suivies correctement. Il y a trois étapes qui doivent être suivies dans l'ordre, en utilisant des stratégies de groupe :

* Configurer les clients pour demander la signature LDAP - Nom de la stratégie de groupe : Sécurité réseau : Exigences de signature du client LDAP -> sélectionnez « Demander la signature » dans la boîte de dialogue.
* Lorsque tous les clients demandent la signature, vous pouvez continuer et configurer les contrôleurs de domaine pour exiger la signature - Nom de la stratégie de groupe : Contrôleur de domaine : Exigences de signature du serveur LDAP -> sélectionnez « Exiger la signature ».
* Configurer les clients pour exiger la signature - Nom de la stratégie de groupe : Sécurité réseau : Exigences de signature du client LDAP -> sélectionnez « Exiger la signature » dans la boîte de dialogue.

En suivant ces étapes, vous vous assurerez qu'aucun client ne cessera de fonctionner pendant la transition.