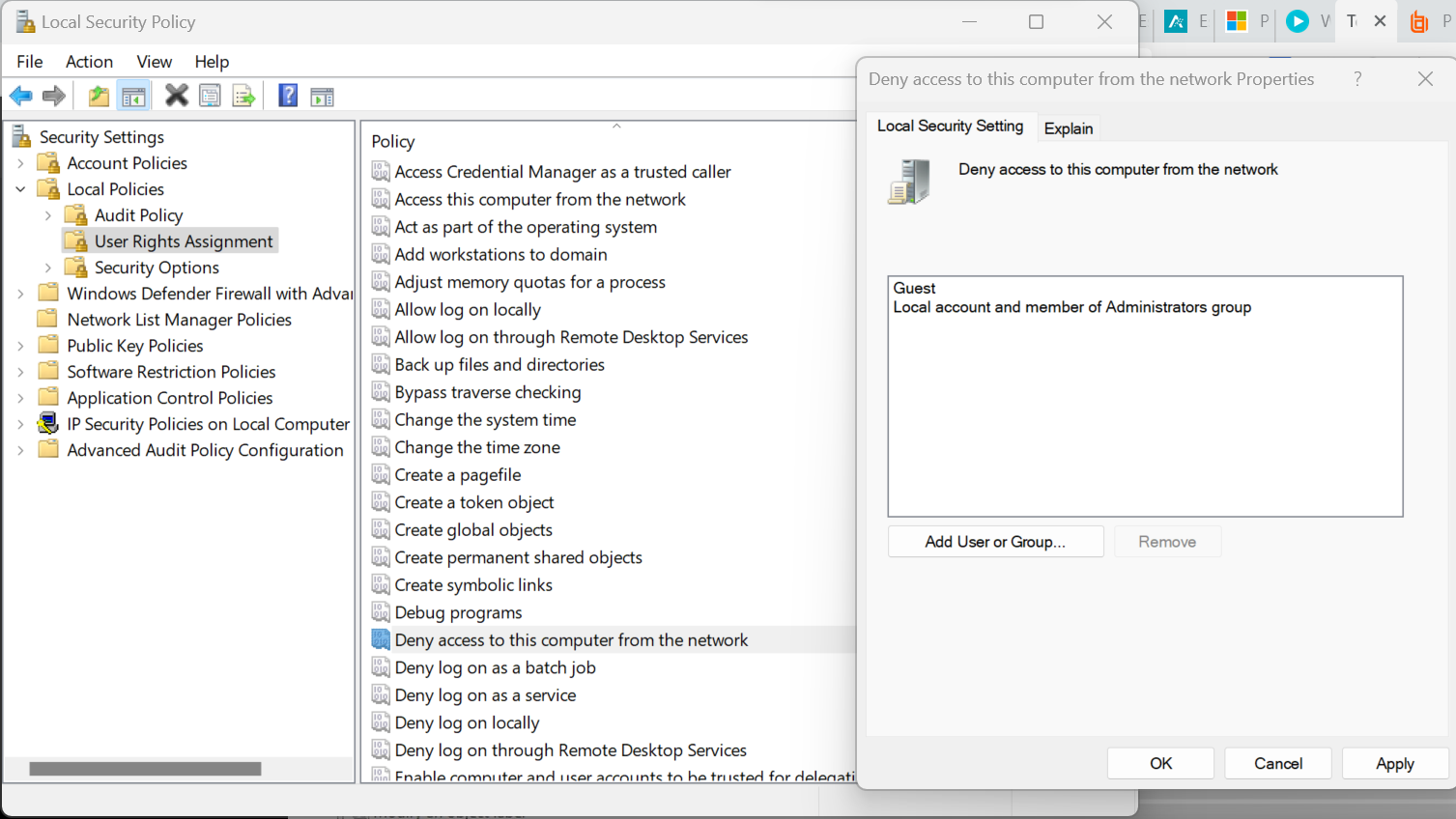
Windows Audit

Source: <https://www.youtube.com/watch?v=AlOrfCjy69U>

1. Hard disk Encryption: Bitlocker
2. No Admin User. Must use non privilege user account on machine
3. Tier0 must not be the able to access client machines (tiering model)
4. Schema Admin and Enterprise Admin group should not contain any member. Always leave them empty. Only add Tier0 admin to this group when needed to extend schema, to add another DC member, adding DHCP server, adding Exchange server etc. But after that remove the admin member and leave it empty.
5. LAPS (intended for Pass the Hash attack -> best solution):

Stop Pass the Hash attack quick fix:

1. 
2. Use Biometric to logon logoff
3. Password Policy: minimum 15 characters. If you use 15 characters then windows cannot create LAN Manager hash. LAN manager hash is saved this way: if it 11 characters password then it saves first 7 chars in a block of hash then the rest 4 in a block without hashed. Someone can break hash of first 7 chars in a few minutes and then use dictionary attack for the next 4 chars. 15 chars password prevent LAN manager to save the password. LAN manager only supports till 14 chars.
4. Service Accounts: Use group managed service accounts or managed service accounts. (need to study how to do that)
5. Whitelisting: -> watch the whitelist session:
6. Applocker:
7. Use Microsoft Security Baselines for Win10
8. PAW implementation
9. Use: <https://www.beyondtrust.com/products>
10. EMET or Windows defender exploit guard should be enabled
11. Disallow Powershell on client machines\*\*\* or create Firewall rule to disallow powershell to connect to internet.