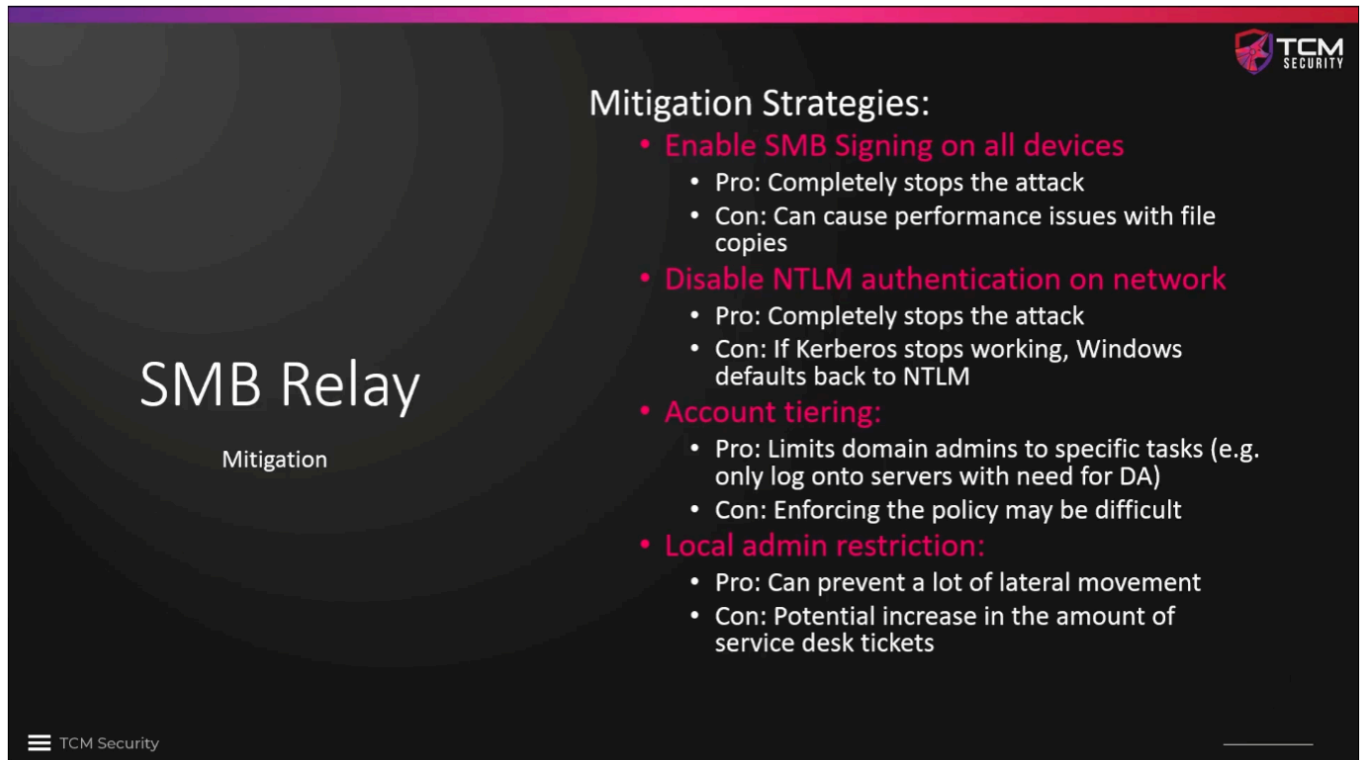


90.07 - SMB Relay Mitigations

The slide features a dark background with a purple-to-pink gradient at the top. On the left, the text 'SMB Relay' is displayed in a large, white, sans-serif font, with the word 'Mitigation' in a smaller font directly below it. On the right side, the title 'Mitigation Strategies:' is followed by a bulleted list of four strategies, each with its own 'Pro' and 'Con' points. The TCM Security logo is positioned in the top right corner, and a small menu icon with the text 'TCM Security' is in the bottom left corner.

SMB Relay
Mitigation

Mitigation Strategies:

- **Enable SMB Signing on all devices**
 - Pro: Completely stops the attack
 - Con: Can cause performance issues with file copies
- **Disable NTLM authentication on network**
 - Pro: Completely stops the attack
 - Con: If Kerberos stops working, Windows defaults back to NTLM
- **Account tiering:**
 - Pro: Limits domain admins to specific tasks (e.g. only log onto servers with need for DA)
 - Con: Enforcing the policy may be difficult
- **Local admin restriction:**
 - Pro: Can prevent a lot of lateral movement
 - Con: Potential increase in the amount of service desk tickets

TCM Security