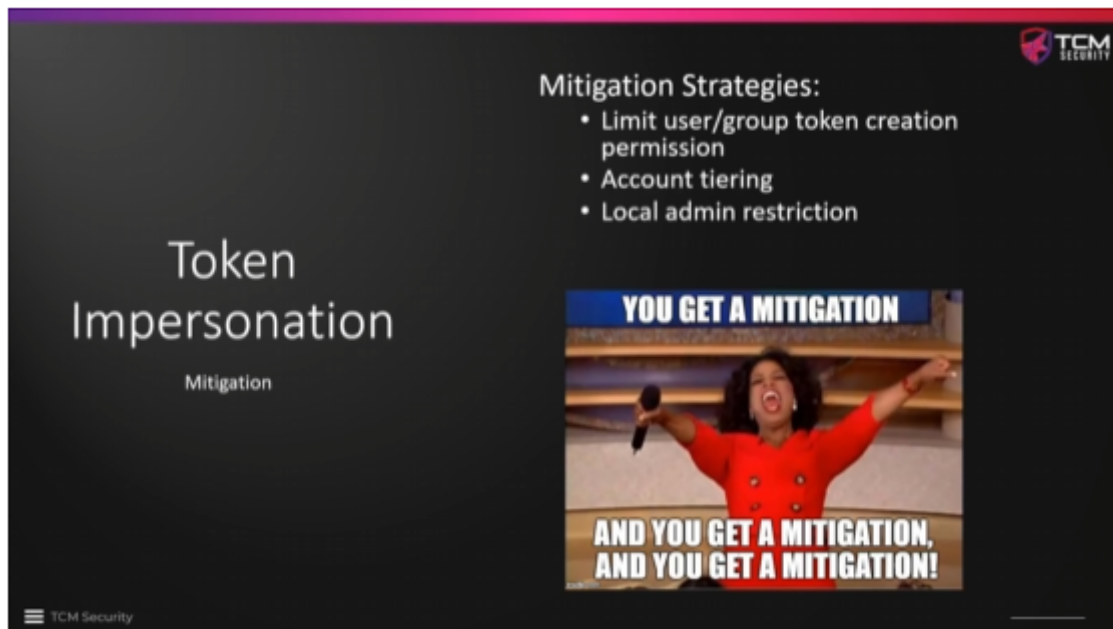


10 - Token Impersonation - Mitigations



The slide features a dark background with a purple and red gradient at the top. On the left, the text 'Token Impersonation' is displayed in a large, white, sans-serif font, with 'Mitigation' in a smaller font below it. In the top right corner, there is a logo for 'TCM SECURITY' consisting of a red shield icon and the text 'TCM SECURITY'. To the right of the title, under the heading 'Mitigation Strategies:', there is a bulleted list of three items: 'Limit user/group token creation permission', 'Account tiering', and 'Local admin restriction'. Below the list is a meme image of a woman in a red dress with her arms raised in a celebratory gesture. The meme has a blue banner at the top that reads 'YOU GET A MITIGATION' and a white banner at the bottom that reads 'AND YOU GET A MITIGATION, AND YOU GET A MITIGATION!'. In the bottom left corner, there is a small logo for 'TCM Security'.

Token Impersonation

Mitigation

Mitigation Strategies:

- Limit user/group token creation permission
- Account tiering
- Local admin restriction

YOU GET A MITIGATION

AND YOU GET A MITIGATION, AND YOU GET A MITIGATION!

TCM Security

Best practices. Focus on that. Domain Admins should not be logging in with their accounts in other machines. They can set up other accounts which allow them to do whatever they need to do in other machines, but they are not supposed to use their domain admin accounts to do daily routine tasks in other computers.