Template - Compromised account

Link to alert

**Description**

The account has marked as compromised and revoked all refresh tokens and session cookies issued to applications

**Classification**: Incident

**Alert detail**

User:

Date:

Actor IP address:

Protocol:

Severity:

**Remediation**

Investigate the user’s device for an authorised tools

Remove saved passwords

Perform full scan on the device

Disable AD account on-prem

reset the password to a strong password

Setup MFA with two authentication methods (ensure the user does not user her Premier email address)

Use klist.exe purge to delete all the tickets of the specified logon session and prevent future usage of the tickets on the device

***NB: PROVIDE A SCREESNHOT OF THE WORK DONE***