Template - Multiple Password Reset by user

Link to alert

**Description**

This query will determine multiple password resets by user across multiple data sources. Account manipulation including password reset may aid adversaries in maintaining access to credentials and certain permission levels within an environment.

**Classification**: Incident

**Information on alert**

<https://www.managedsentinel.com/ms-a195>

**Alert detail**

User:

Application:

Start Time [UTC]:

End Time [UTC]:

Total:

Device name:

IP address:

Location

Error:

Severity:

**Remediation**

Confirm if the user was trying to reset their password, if not then reset the password to a strong password

Ensure that MFA is setup

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