Sensitive accounts like Break Glass accounts which are not protected by Conditonal Access or MFA, need additional monitoring to be setup to ensure right usage. This alert rule will trigger on any sign-ins from the identified break glass accounts.

Pre-Requisites:

* Log Analytic Workspace
  + Create Log Analytic Workspace

Graphical user interface, text, application

Description automatically generated

* Azure AD Sign In logs must be enabled and configured to be exported into an Azure Log Analytic Workspace
  + For exporting Sign-In logs, Azure AD P1 or P2 license is required
  + Configure Azure AD Diagnostic Logs

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Alert Configuration:

* Check if the Azure AD logs are returning results as expected by running the below query in Log Analytic Workspace:
  + SigninLogs | where ResultType == 0 and (UserPrincipalName == "your-id@your-tenant.com")
  + If this query returns more than one results, the configuration is working

Graphical user interface, text, application

Description automatically generated

* Create New Alert

Graphical user interface, text, application, email

Description automatically generated

* + Log Query to be used:
    - SigninLogs | where ResultType == 0 and (UserPrincipalName == "admin-1@your-domain.com" or UserPrincipalName == "admin-2@your-domain.com")

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

* + Create Action Group if there isn’t one already:

Graphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

* This marks completion of steps and the alert rule should now be created