Template - Multiple failed login attempts

Link to alert

**Description**

This detection identifies users that failed multiple login attempts in a single session with respect to the baseline learned, which could indicate on a breach attempt.

**Classification**: Incident

**How to investigate**

<https://docs.microsoft.com/en-us/cloud-app-security/investigate-anomaly-alerts>

User details

User:

Country or region:

Office:

**Alert details**

Activity:

Date:

Application:

Device:

IP address:

Location:

Authentication detail:

* Authentication method:
* Authentication method detail:
* Succeeded:
* Result detail:

ISP:

Severity:

**Remediation**

Confirm that MFA is enabled

Clear MS application sign-ins (revoke sessions)

Confirm that the password is reset to a strong password

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