Template - Multiple failed user logon attempts to a service

Link to alert

**Description**

Activity policy ''Multiple failed user logon attempts to a service'' was triggered.

**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 if the Service account is using the correct password to log into the device.

Confirm that the service account has a strong password, the password does not expire and the password cannot be changed.

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