Template - Perform failed sign in activities from remote locations

Link to alert

**Description**

Failed login attempts could indicate on an attempt to breach an account. However, failed logins can also be normal behaviour.

**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 user is trying to log into **Application x** because there are multiple sign-ins from IP address in a remote location.

If the user is trying to log into **Application x**, assist the user to sign-in

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