Template - Impossible travel activity

Link to alert

**Description**

Activity from the same user in different locations within a time period that is shorter than the expected travel time between the two locations. This can indicate a credential breach, however, it's also possible that the user's actual location is masked, for example, by using a VPN.

**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:

Severity: Medium

**Remediation**

Confirm if the user performed the activity.

If the user did not perform the activity, then assist the user to reverse the activity if applicable and reset the password to a strong password.

Ensure that MFA is enabled with two authentication methods.

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