Template - Impossible travel activity

Link to alert

**Description**

This risk detection type identifies two sign-ins originating from geographically distant locations, where at least one of the locations may also be atypical for the user, given past behavior. Among several other factors, this machine learning algorithm takes into account the time between the two sign-ins and the time it would have taken for the user to travel from the first location to the second, indicating that a different user is using the same credentials.

**Classification**: Incident

**How to investigate**

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

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***