Template - Unfamiliar sign-in properties

Link to alert

**Description**

This risk detection type considers past sign-in history (IP, Latitude / Longitude and ASN) to look for anomalous sign-ins. The system stores information about previous locations used by a user and considers these "familiar" locations. The risk detection is triggered when the sign-in occurs from a location that is not already in the list of familiar locations.

**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:

ISP:

Severity:

**Remediation**

Confirm if the user is in the location and operating on the specific device,

Otherwise, reset the password to a strong password and confirm if MFA is setup with two authentication methods

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