Template - Activity from infrequent country

Link to alert

**Description**

Activity from infrequent country Activity from a country/region that could indicate malicious activity. This policy profiles your environment and triggers alerts when activity is detected from a location that was not recently or was never visited by any user in the organization.

**Classification**: Incident

**How to investigate**

[Cloud App Security anomaly detection alerts investigation guide | Microsoft Docs](https://docs.microsoft.com/en-us/cloud-app-security/investigate-anomaly-alerts#:~:text=Activity%20from%20infrequent%20country%20Activity%20from%20a%20country%2Fregion,never%20visited%20by%20any%20user%20in%20the%20organization.)

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 performed the activity

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

Ensure that MFA is enabled with two authentication methods

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