Template - Sign-ins from IPs that attempt sign-ins to disabled accounts

Link to alert

**Description**

Identifies IPs with failed attempts to sign in to one or more disabled accounts signed in successfully to another account.

**Classification**: Incident

**How to investigate**

<https://docs.microsoft.com/en-us/cloud-app-security/investigate-anomaly-alerts>

**Alert details**

User:

Date:

Location:

Device name:

IP address:

Application:

Error code:

Failure reason:

Severity:

**Remediation**

Confirm with the user’s manager if the account should be disabled.

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