Template - Mass delete

Link to alert

**Description**

Alert when a single user performs more than 50 deletes within 1 minute.

**Classification**: Incident

**How to investigate**

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

**Alert detail**

User:

Date:

IP address:

Description:

Application

Data size:

Device:

Location:

**Remediation**

Confirm if the user deleted a large amount of data from the application.

If the user did not delete the data then inform Confirm the user is compromised in Microsoft Cloud App Security.

Assist the user to retrieve the deleted data.

Thereafter, assist the user to reset the password to a strong password and ensure that MFA is setup with two authentication methods.