Template - Data exfiltration to an app that is not sanctioned

Link to alert

**Description**

This policy is automatically enabled to alert you when a user or IP address uses an app that is not sanctioned to perform an activity that resembles an attempt to exfiltrate information from your organization.

**Classification**: Incident

**How to investigate**

[Create anomaly detection policies in Cloud App Security | Microsoft Docs](https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy)

**Alert detail**

User:

Application:

IP Address:

Data downloaded:

Date:

Severity:

**Remediation**

Inform the user that the application in use is not sanctioned

Confirm if the user initiated the usage of data on the application

If the user did not initiate the usage of data then reset the password to a strong password and ensure that MFA is enabled.

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