Template - Suspicious application consent for offline access

Link to alert

**Description**

This will alert when a user consents to provide a previously unknown Azure application with offline access via OAuth. Offline access will provide the Azure App with access to the listed resources without requiring two-factor authentication. Consent to applications with offline access and read capabilities should be rare, especially as the known Applications list is expanded.

**Classification**: Incident

**How to investigate**

<https://docs.microsoft.com/en-us/security/compass/incident-response-playbook-app-consent>

**Alert detail**

User:

Time Generated [UTC]:

Grant Consent Type:

Grant Scope:

Grant Initiated By:

App Display Name:

Grant User Agent:

Grant Authentication:

Operation Name:

Grant Operation:

**Remediation**

Confirm with the user if the application consent is valid