Onboard Azure Identity Protection

1. Prerequisites

- Representative with Security Administrator or Conditional Access Administrator role access
- Entra ID P2 License
- Break the glass accounts to prevent lockout
- Routines in place for unlocking accounts

2. Tasks

2.1. Enable user risk policy

Azure identity protection enables a feature that gives Truesec SOC the ability to confirm users as compromised. A user marked as compromised will have its user risk elevated to the highest level and the preset user risk policies will kick in. Truesec recommends that increased user risk should result in block to all cloud applications.

Add the role “Cloud App Security Administrator” to the group “Truesec SOC Operators” to enable response actions in M365 Defender, this is a work around due to privilege changes done by Microsoft that is currently being investigated.

Confirm setup by going through this guide: Risk policies - Azure Active Directory Identity Protection - Microsoft Entra | Microsoft Learn