# Threat Model (Light)

## iSM SSO

Date Assessed: February 2025

Prepared by: David Biayna Neal

Reviewed by: Will North, Trefor Walters

### Background

The IBM TM1 and Planning Analytics Workspace (PAW) applications underpins the MHR iTrent Salary Modelling (iSM) product. To allow customers to login to iSM via their own Identify Providers (IDP), Single Sign On (SSO) is being enabled. This is achieved through implementing the Cognos Access Manager (CAM) to broker the SSO.

### Scope

This threat model assesses if the new threats introduced by enabling SSO are sufficiently mitigated.

### Threat Assessment

The following key threats were identified and assessed.

|  |  |  |
| --- | --- | --- |
| **Threat** | **Mitigation** | **Mitigated** |
| **High:** A malicious actor spoofs an ID token and gains unauthorized access. | The professional services team have configured authentication to use the industry-standard OIDC protocol, which use public key cryptography to validate that the token received is legitimate and has not been tampered with. | **Yes** |

### Conclusion

The Cyber Security team conclude that this change design is approved for implementation as all key threats are sufficiently mitigated.