# Threat Model (Light)

**People First / Itrent Integration**

Date Assessed: 19/08/2025

Prepared by: David Biayna Neal

Reviewed by: Will North, Charlie Harris, Trefor Walters

### Background

This is an existing functionality where PF has an option to integrate with iTrent, this involves the PF team making API calls to iTrent using a credential. It appears that the credential, which is used to access pay data, is passed as a URL parameter and this is logged out to App Insights where it is widely visible to MHR staff. There are some security concerns that have been listed in the table below.

### Scope

PF, Itrent and APP Insights.

### Threat Assessment

The following key threats were identified and assessed.

|  |  |  |
| --- | --- | --- |
| **Threat** | **Mitigation** | **Mitigated** |
| Malicious actor with App Insights access replays a logged sessionId before expiry to fetch payslip data. | Stop logging query strings; rotate/shorten token TTL; Move secret out of URL; Add nonce timestamp with server-side single-use enforcement. | No |
| Malicious actor replays after a failed call (token not redeemed by iTrent due to timeout/network error) while it’s still valid. | Reject tokens that were presented but not fully authenticated (spent on first use); Tie token validity to a signed request containing nonce timestamp; Very short TTL. | No |
| Malicious actor on an allowed corporate/VPN IP spoofs the user agent and reuses the stolen sessionId, bypassing weak IP/UA checks. | Do not rely on User Agent; Bind requests cryptographically (HMAC over method+path+query+body+timestamp+nonce) or with mTLS/DPoP; Scope token to tenant/resource. | No |

### Conclusion

The current People First / iTrent implementation presents a material insider-misuse and replay risk because a payslip access credential/sessionId is passed in the URL and logged to Application Insights.

Itrent’s multi metric fingerprinting provides a mechanism to ensure only correctly authenticated users can perform critical operations within the system. The fingerprinting depends on the session ID, Ip and user agent which reduces the risk and requires an advantageous position. Nevertheless, this fingerprinting does not deliver cryptographic proof-of-possession and based on observed “bad data”.

User-Agent is trivially spoofed, insiders often originate from approved egress IPs, and logging the sessionId in full URL form materially widens who can obtain and replay it, especially in failure paths where the token is not redeemed.

As a result, the residual insider-misuse and replay risk remains until the above recommended controls are implemented. These controls will reduce the attack surface from “anyone who can read logs” to “only a client holding the private key/secret within a narrow time window,”.