# Threat Model (Light)

**Integration update Klue – Salesforce**

Date Assessed: 17/06/2025

Prepared by: David Biayna Neal

Reviewed by: Will North, Charlie Harris, Trefor Walters

### Background

MHR is updating its integration with Klue, a platform used for managing competitive intelligence. Previously, Klue accessed MHR’s Salesforce data through a third-party service. This setup is now being replaced with a direct connection between Klue and Salesforce. This change uses OAuth 2.0 for access and data sharing. Klue will continue to collect CRM data via a Connected App, such as sales opportunities and user information, which supports their services like performance tracking and win-loss analysis. Currently, Klue accesses Salesforce using a highly privileged admin account, which poses unnecessary security risk. To reduce this, MHR plans to introduce a new dedicated user account for the integration that has read-only access and is restricted to only the necessary data.

### Scope

The scope of this assessment covers the security implications of Klue’s direct integration with Salesforce using OAuth 2.0, including access permissions, data exposure, and user account controls.

### Threat Assessment

The following key threats were identified and assessed.

|  |  |  |
| --- | --- | --- |
| **Threat** | **Mitigation** | **Mitigated** |
| A malicious actor who compromises the high-privilege BIS Admin user could exfiltrate or alter all Salesforce records. | Replacing the admin user with a read-only integration user that has object-level access controls. | Yes. The account will only be able to access account, contact, opportunity, user information. |
| A malicious actor who gains access to Klue’s access or refresh tokens could extract Salesforce data. | Tokens are stored encrypted, tenant-scoped, and isolated to Klue’s internal network. | Yes |
| A malicious actor causes excessive API calls, leading to service degradation. | Klue is internally rate limited to 1 request / 2 seconds with exponential backoff, preventing abuse. | Yes |
| A malicious actor uses long-lived refresh tokens after deprovisioning. | Token rotation and revocation is controlled by the customer (MHR) and can be enforced via Connected App settings. | Yes |
| A malicious actor who obtains valid OAuth2 tokens (e.g., via phishing, token leak, or compromised client system) could use them from any geographic location or unauthorized IP address to access MHR’s Salesforce environment via Klue's integration. | MHR can configure IP range restrictions in the Salesforce Connected App settings. Klue has confirmed they can supply static IP ranges for this purpose. Restricting token usage to trusted IPs would block access attempts from unrecognized sources. | Yes, configurable |

### Conclusion

MHR’s use of a dedicated, minimally privileged integration account, together with encrypted token handling, request rate limits, and IP-based access control, substantially reduces the chance of unauthorized data exposure. When these settings are correctly applied, the residual risk remains low: the integration only ever has the minimal access it needs, and any attempts at misuse are constrained.