Docebo Flow

**Report Reference: CYSEC-SECREP-04**

**Version**: 1.0

**Prepared by**: David Biayna Neal

**Report Date**: 13th August 2025

**Classification**: Sensitive

**Document Control**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version No. | Date of Issue | Authors | Status | Comments |
| 0.1 | 13th August 2025 | David Biayna Neal | Initial Draft |  |

Contents

[1 Introduction 4](#_Toc205994659)

[2 Executive Summary 5](#_Toc205994660)

[3 Scope 6](#_Toc205994661)

[4 Background 7](#_Toc205994662)

[5 Limitations and Constraints 12](#_Toc205994663)

[6 Results of Assessment 13](#_Toc205994664)

# Introduction

MHR Cyber Security conducted a security assessment Docebo’s Flow or also known as Embedded/ Headless Learning, which allows to fully customize and integrate learning experiences within existing MHR systems such as Itrent. The assessment began on the 12th of August 2025 and concluded on the 15th of August 2025. The assessment was carried out by David Biayna Neal.

# Executive Summary

Docebo’s Headless/Embedded learning can be integrated into iTrent to surface courses while Docebo continues to own content, tracking, and reporting. The platform provides mature security setup with OAuth2 with scoped tokens, SSO, granular RBAC across comprehensive REST APIs, event webhooks (HTTP and AWS SQS/EventBridge), and a segregated sandbox, consistent with industry practice. The primary risks are integration-centric: server-side token issuance and storage, strict origin/CSP control for embedded widgets, robust webhook authentication and least-privilege segregation of API clients and admin roles.

# Scope

The subject of this report is the Docebo’s flow / known also as Embedded learning. Headless components include (Embedded Launchers and Building Blocks), REST APIs, Webhooks, and Docebo Connect; authentication/authorisation flows for API access using OAuth2 and bearer tokens. Further information is available below.

* Building Blocks Example: [https://codepen.io/alejandro318/pen/RwYjqKv](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcodepen.io%2Falejandro318%2Fpen%2FRwYjqKv&data=05%7C02%7CDavid.BiaynaNeal%40mhrglobal.com%7C6b216edb28634bda26cb08ddd9a8c74d%7C75b02e0d90d143e5b5db20eaaddbfac6%7C0%7C0%7C638906041483101132%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=K%2BtVhlUlcjHFmcZiXAQMggpiY9VL0dKbBbZtNF6G%2B68%3D&reserved=0)
* Authentication Token Example: [https://codepen.io/alejandro318/pen/mdzYxZY](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcodepen.io%2Falejandro318%2Fpen%2FmdzYxZY&data=05%7C02%7CDavid.BiaynaNeal%40mhrglobal.com%7C6b216edb28634bda26cb08ddd9a8c74d%7C75b02e0d90d143e5b5db20eaaddbfac6%7C0%7C0%7C638906041483144989%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=SAwHcLygEHj7M0C2UlDcEohBUITMn4AAjnGG16rvo7g%3D&reserved=0)
* Launcher example [https://codepen.io/alejandro318/pen/MWPxbZj](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcodepen.io%2Falejandro318%2Fpen%2FMWPxbZj&data=05%7C02%7CDavid.BiaynaNeal%40mhrglobal.com%7C6b216edb28634bda26cb08ddd9a8c74d%7C75b02e0d90d143e5b5db20eaaddbfac6%7C0%7C0%7C638906041483185213%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=5nLZKK6MB8nNGS7RYfoB53Z0RvB3sM9mTgMAHXWIKL4%3D&reserved=0)

# Background

The focused on the integration of Docebo's Flow, now known as Embedded Learning, within MHR's iTrent system. It was emphasized by the Docebo team the need for Flow to avoid poor performance with iFrames., including launchers and building blocks for content integration.

**Launcher**: The launcher starts the experience as it’s been set upon the Docebo platform. The

launcher and gives the authenticated learner the appropriate content. It must be configured from the Docebo backend.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Building Blocks:** AllowS customers to start a single widget presenting the content of their Docebo platform as part of the composition of their external web page which is Implemented via HTML + Tag/Attributes. An example code of Building blocks is demonstrated below.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Authentication**

To be able to request the content from Docebo, iTrent backend requests a Docebo OAuth2 access token (e.g., JWT-bearer or client-credentials) via an API call. These will provide a user-permission-scopedaccess token (bearer) that can be used to authenticate and authorize API requests. Various OAuth2 grant types are available and can be configured separately on each API client. The authentication flow diagram is demonstrated below.

A screenshot of a computer

AI-generated content may be incorrect.

Example access token is demonstrated below.  
  
A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Once the user opens the “Learning” area/page in iTrent (web or mobile), the page makes a call to the backend i.e. learning/Docebo/session to download the content either using a reverse proxy or signed launch links.​ While the learner consumes content, Docebo records progress/completion and sends back to Itrent via a webhook.

A screenshot of a webbook

AI-generated content may be incorrect.

# Limitations and Constraints

# Results of Assessment

No findings were raised as a result of this assessment.