appsecure security.

PENETRATION TEST

Attestation of Security Assessment

Matillion Ltd Security Assessment

PREPARED FOR
Matillion Ltd

PREPARED BY
AppSecure Security

ENGAGEMENT TYPE
Penetration Testing as a Service (PTaaS)

ASSESSMENT TIMELINE
START Apr 14, 2026
END Apr 24, 2026

REPORT DATE
June 12, 2026

DOCUMENT VERSION
v1.0 — Final

To Whom It May Concern,

In April 2026, the AppSecure team conducted a security assessment for Matillion Ltd of their Matillion DPC web application to identify security vulnerabilities within the application. For detailed information on the products and scope, please see **Appendix A**.

The engagement objective was to identify the security vulnerabilities within the shared scope. The AppSecure team has completed an application security assessment, including thorough testing to identify security weaknesses. For more information on AppSecure's testing approach, please see **Appendix B**.

This letter confirms that the security assessment of the Matillion DPC web application has been completed, and the identified security vulnerabilities have been reported to the team.

Sincerely,

Sandeep H.

Sandeep Hodkasia

Founder & CEO

AppSecure Security

FINDINGS AT A GLANCE

Vulnerabilities summary

CRITICAL	HIGH	MEDIUM	LOW
0	0	1	8
No critical findings	No high findings	Remediation in progress	Remediation in progress

APPENDIX A

Scope

Prior to commencing the assessment, Matillion Ltd shared the scope with AppSecure Security as detailed below. Within the overall scope, this report has been articulated, focusing on the assets enumerated here.

APPLICATION NAME / URL	ASSET	TYPE
`https://app-preprod.matillion.com`	DPC Web Application	Web

APPENDIX B

Web Application with AI Capabilities

The security assessment combined real-world attack simulation with automated discovery and manual validation. The activities below describe the techniques AppSecure Security performed against the in-scope assets.

05

Web Application with AI Capabilities

Includes OWASP Top 10 — Web, API, and LLM.

- **Standard web & API testing**
  Full web and API assessment of the surrounding application.
- **Prompt injection**
  Direct and indirect injection, jailbreaks, and instruction override.
- **Sensitive information disclosure**
  System-prompt leakage and exposure of context or training data.
- **Data & model integrity**
  Data poisoning, model manipulation, and improper output handling.
- **Adversarial & abuse testing**
  Adversarial inputs, misinformation, and unsafe output generation.
- **Resource & availability**
  Model denial-of-service via resource exhaustion and cost abuse.

ALIGNED WITH

OWASP Top 10 — Web | OWASP API Security Top 10 | OWASP LLM Top 10 | NIST AI RMF | MITRE ATLAS