



Third Party Memorandum

iWize – Aqopi

September 1, 2020

Confidential



WhiteHats
ethical hackers

Third Party Memorandum

Introduction

WhiteHats has performed a security assessment for iWize. The goal of this project was to identify potential weaknesses in the solution Aqopi; a solution that processes personal information that it retrieves from several sources (the solution does not store any personal information on iWize systems).

Remark: the solution has been previously assessed in February 2019.

Project information

- Initial assessment executed in week 31 - 34, 2020
- Reassessment executed in week 35, 2020
- Total hours spent: 35
- No social engineering- or DDoS-attacks executed.
- Source code and a testing environment were provided by iWize.

Result

The solution was thoroughly assessed in two phases using both code reviewing and testing techniques.

During the first phase, no critical weaknesses or vulnerabilities were identified and the total number of realistic attack scenarios was low. The findings were discussed with the development team which promptly implemented several additional security measures.

The second phase confirmed the effectiveness of the improvements and revealed no new practical attack scenarios. WhiteHats therefore considers the solution to be adequately protected and suitable for the processing of sensitive personal information.