# Penetration Testing Certificate

RM Information Security have conducted manual application penetration testing of the following:

Client: PlayoutONE Ltd

Test Completion Date: 08/01/2021

## Key objectives

This document provides a summary of the penetration testing carried out against the target system above. The key objectives of the testing were to:

- Provide an independent security assessment.
- Conduct full manual penetration testing in-line with industry good practice.
- Cover all applicable vulnerability classes using the output from organisation such as CWE, OWASP, OSSTMM, SANS and WASC as a baseline.
- Identify any weaknesses that an attacker may exploit to compromise the confidentiality, integrity or availability.
- Use open source reconnaissance to identify and interrogate data sources that may be used to gain information about the target systems and users as part of a targeted attack.
- Provide assurance that security standards and good practice are being met.
- Quantify and present any vulnerabilities in a manner which enables risks to be mitigated appropriately utilising CVSS.

Lead test consultant:

Mark Wityszyn

RM Technical Director

# RM – Information Security Application testing methodology

The target system was manually tested using the RM Information Security penetration testing methodology, which is built on years of knowledge and experience delivering manual penetration testing. We provide assurance of industry good practice as a minimum whilst utilising the output from organization such as OWASP, OSSTMM, PTES, WASC and SANS as fundamental baselines. A more detailed description of our methodology and approach is available online at https://www.rminfosec.co.uk.

An outline of the key areas covered and applicability to the target system are shown below with any outstanding issues and ratings.

| Host Infrastructure Testing | | |
|---|---|---|
| **No.** | **Test Category Name** | **Assessed** |
| 1 | Authentication | Yes |
| 2 | Authorisation | Yes |
| 3 | Configuration | Yes |
| 4 | Cryptography | Yes |
| 5 | Information disclosure | Yes |

| Application Testing | | |
|---|---|---|
| **No.** | **Test Category Name** | **Assessed** |
| 1 | Authentication | Yes |
| 2 | Authorisation | Yes |
| 3 | Business logic | Yes |
| 4 | Configuration | Yes |
| 5 | Cryptography | Yes |
| 6 | Information disclosure | Yes |
| 7 | Input validation | Yes |
| 8 | Insecure functionality | Yes |
| 9 | Session management | Yes |

TIGERSCHEME
Providing excellence in penetration testing

**Disclaimer** This document does not confirm the solution is completely secure. Vulnerabilities in operating systems, infrastructure services and applications are discovered on a daily basis. It has been recommended that a holistic security program should be implemented to ensure any vendor security patches or configuration changes are applied to mitigate these risks. In addition, it is accepted industry good practice that a regular schedule of penetration testing is carried out (e.g. annually) and after any significant change.





`