LIACOM SYSTEMS LTD.

PENETRATION TEST REPORT FOR CYBEREADY

DECEMBER 2023

5 Hatzoref St., Holon 5885633, Israel

+972-3-5573400

info@liacom.co.il

www.liacom.co.il

During November 2023, Liacom Systems conducted comprehensive penetration testing on the Cybeready platform to assess security resilience, identify security risks, address hardening gaps in line with best practices, and uncover other vulnerabilities that might compromise the overall security of Cybeready's business and its customers.

The security team at Liacom Systems conducted a penetration testing engagement utilizing a proven, proprietary methodology that combines manual testing with industry-standard tools. This approach aims to comprehensively cover the attack surface informed by Cybeready's technology stack, thereby offering a thorough insight into the existing security posture of the web application. Specifically, the application-level testing adheres to the OWASP10 standard.

After conducting the initial test, the Cybeready team addressed the primary issues identified. In December 2023, the team revisited the Cybeready platform to ensure that the previously identified gaps had been resolved. During the time of the retest, no critical, high, or medium findings were reported. The customer addressed all major issues in accordance with the recommendations provided by the Liacom Systems team, implementing the suggested security countermeasures or alternative measures where necessary.

Purpose Rules of Engagement (RoE)

The PT engagement scope is defined in the following content:

Asset Name	Category	IP / Host
Marketing website	Web App	https://cybeready.com
BackOffice	Web App	https://manage.cybeready.com
Customer's dashboard	Web App	https://dashboard.cybeready.com

We conducted tests using a dedicated account for the customer's dashboard and a separate, lower-privileged account for the management portal, which operates behind a Perimeter81 VPN.

Security Objectives

The security objectives for the PT project have been established with the following:

- Identify any security risks that could potentially compromise the privacy of company personnel, customers, and users.
- Detect risks to the organization's reputation stemming from potential abuse of the application by malicious actors, whether internal or external; and to assess the adequacy of the existing security controls.
- Evaluate security risks that may emerge from misconfigurations and implementation flaws within the application's technology stack and its associated infrastructure.