RED CITADEL
CYBER SECURITY

Letter of Attestation



CREST MEMBER

Client: GRW Halo Ltd T/A Halo Benefits
Classification: Public
Issue Date: 20.11.2026

Summary

This letter confirms that, on the 12 November 2026, Red Citadel Limited conducted a half-day engagement comprising a CREST black box external infrastructure penetration test for GRW Halo Ltd T/A Halo Benefits.

The purpose of the assessment was to provide an independent, point-in-time review of the security posture of the in-scope external infrastructure and to identify security weaknesses that could affect its confidentiality, integrity or availability, or that of the data it stores and/or processes.

Scope of Engagement

The scope of the assessment was broken down into the following components:

- External Infrastructure: Internet-facing infrastructure associated with Halo Benefits' systems.

No exclusions were agreed for this assessment.

Findings

An external infrastructure penetration test was performed against the in-scope public IP addresses to evaluate the organisation's exposure to unauthenticated attacks originating from the internet. The assessment included service discovery, enumeration, vulnerability identification, and validation of publicly exposed services. No security vulnerabilities, misconfigurations, or exploitable conditions were identified during the assessment.

Based on the testing performed, no findings were identified. The assessment did not identify any unauthenticated attack paths that could enable compromise of the assessed infrastructure, and no critical, high, medium, or low-risk vulnerabilities were identified. Overall, the results indicate that the externally accessible infrastructure was appropriately secured, with effective security controls in place to protect internet facing services.

Testing Methodology

Red Citadel carried out a black box penetration test against the client's internet-facing infrastructure and services. An external black box approach assesses the environment from the perspective of an unauthenticated external attacker, with limited prior knowledge of the organisation's infrastructure, internal architecture, security controls, or supporting documentation. This approach is designed to replicate the level of visibility and access that would typically be available to an external threat actor attempting to identify and exploit weaknesses from the internet.

The assessment included reconnaissance and security testing of the in-scope public IP addresses, with the objective of identifying externally accessible services, potential vulnerabilities, misconfigurations, and other weaknesses that could increase the organisation's exposure to internet-based threats.

Our methodology is based on industry-standard Penetration Test frameworks and security best practices and includes:

- External attack surface enumeration and service identification
- Manual and automated testing techniques
- Vulnerability identification and validation
- Safe and controlled exploitation
- Risk-based prioritisation of findings
- Cross-referencing against CVSS and industry best practice guidance
- Manual review and analysis

Limitations

The following limitations apply:

- Penetration Test was conducted against a specific version of the systems within a defined environment and agreed testing window.
- The results reflect the security posture only at the time of assessment.
- Changes made after the test, including software updates, code changes, infrastructure changes, configuration changes, or newly introduced functionality, fall outside the scope of this letter.
- This attestation does not confirm that all vulnerabilities were identified or that the system is free from weaknesses.
- The engagement did not include remediation or verification of fixes unless explicitly stated.

Red Citadel Limited | **Registered Address:** 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ | **Company Number:** 16554117

About Red Citadel

Red Citadel is a CREST Penetration Test company delivering expert security assurance across Penetration Test, cloud security audits, vulnerability assessments and IASME certification services.

Our CREST accreditation provides independent assurance that our Penetration Test services are delivered in line with recognised technical, ethical and quality standards. Testing is carried out by experienced consultants using structured methodologies, agreed Rules of Engagement and a clear focus on genuine risk, business impact and practical remediation.

As an IASME Certification Body, we are also authorised to deliver Cyber Essentials, Cyber Essentials Plus and IASME Cyber Assurance Level 1 and Level 2 certifications.

Our team brings more than 20 years of combined IT and cyber security experience. We work closely with clients throughout each engagement, sharing clear findings, practical guidance and support that helps them strengthen their defences and make informed security decisions.