Olyteck Cyber
Cybersecurity for Microsoft 365

PRODUCTION DAST · PUBLIC EVIDENCE

Production Security Scan Summary

Result of the latest automated Dynamic Application Security Testing (DAST) scan against the live Olyteck Cyber production environment. Performed with OWASP ZAP.

Scan date	1 June 2026
Scanner	OWASP ZAP 2.17.0 (industry-standard, open source)
Plan	Production baseline — passive rules, no attack payloads
Target	https://cyber.olyteck.com (and crawled paths)
URLs scanned	76 (traditional spider + AJAX spider)
Methodology	Spider crawl, then OWASP ZAP passive ruleset across the full discovered surface
Frequency	On every staging deploy; production scan re-run quarterly and on material change

Result

Zero risk findings

0 High, 0 Medium, 0 Low. All risk-level alerts are resolved. The 7 informational alerts are technology-detection observations only (Google Analytics, Google Tag Manager, Google Fonts, Nginx, PHP, HSTS, Open Graph) and are not security findings.

Risk	Count	Interpretation
High	0	No critical risk identified.
Medium	0	No moderate risk identified.
Low	0	No low-severity finding identified.

Risk	Count	Interpretation
Informational	7	Technology-stack disclosures expected by design (analytics, fonts, web server).

Controls verified by this scan

- HTTP Strict Transport Security (HSTS) enforced — max-age 2 years, includeSubDomains, preload.
- Content Security Policy (CSP) in place — restricts script, style, image, font, and form-action sources.
- X-Frame-Options: DENY — clickjacking protection (also via CSP frame-ancestors).
- X-Content-Type-Options: nosniff — MIME-sniffing protection.
- Referrer-Policy: strict-origin-when-cross-origin — minimal cross-origin referrer leakage.
- Permissions-Policy — restricts use of powerful browser features (camera, mic, geolocation, payment, fullscreen).
- Server signature suppressed (X-Powered-By, Server headers removed).
- Internal partial files denied direct access via Apache (FilesMatch + per-file PHP guard).
- TLS 1.2 / 1.3 with modern cipher suites enforced on the edge.

Methodology details

OWASP ZAP, an open-source project maintained by the OWASP Foundation, is the industry-standard DAST scanner for web applications. The baseline plan used here runs the full passive ruleset across the discovered surface without injecting attack payloads — making it safe to run against production.

The plan crawls the public application using both a traditional link-following spider and an AJAX (browser-driven) spider, then evaluates every response against the passive ruleset. Findings are categorised by ZAP's standard risk ratings: High, Medium, Low, Informational.

Active scanning (attack-pass testing for SQL injection, cross-site scripting, command injection, and similar) is performed against a separate staging environment with synthetic data, never against production. A summary of the latest active scan is available under non-disclosure agreement.

Scope and limitations

- Public, unauthenticated surface only. Authenticated areas (the tenant administrator dashboard) are scanned in staging, not production.
- Passive checks only on production. SQLi / XSS / command-injection probes run on staging.
- Microsoft Graph integration is exercised end-to-end on staging against a synthetic Microsoft 365 tenant, not from this production scan.

Re-running this scan

Sales and security teams can re-run this scan on demand by following the operator runbook at /zap/README.md in our internal documentation. The scan plan is open and reproducible; the report below is an output of the same plan a customer can re-execute under our coordination.

This summary is updated after each scheduled scan. The most recent raw report (JSON) is available alongside this PDF on the Trust Center for technical reviewers who want to verify line-by-line.