Security review brief — Olyteck Cyber

For the person who has to approve the scan. A two-minute read. Everything here is verifiable in your own tenant without contacting us.

Product	Olyteck Cyber — Microsoft 365 security posture scanner
Version	1.0 · 18 August 2026
Access model	Microsoft Graph, read-only, via Entra ID app consent
Agents to install	None
Data exported from your tenant	Aggregate findings only — no file contents
Hosting	European Union
Time to first report	Under 15 minutes on a 50–200 seat tenant

1. The three questions a review usually turns on

Can it change anything in our tenant?

No. The application that runs the scans holds **19 Microsoft Graph permissions, every one of them a `.Read.*`**. There is no write permission of any kind on it, so there is no code path — ours or anyone else's — by which a scheduled scan can modify your tenant. This is not a policy we promise to follow; it is a property of the permission grant, and you can read that grant yourself (§3).

Can it read our documents and email?

No. We read **metadata and permissions** — site names, folder paths, who has access, whether a link is anonymous, whether a mailbox forwards externally. We do not download file contents, message bodies, or attachments, and none are stored in our systems. Over-exposure is a property of permissions, not of content, so reading content would add risk without adding findings.

What happens if we want to end it?

Microsoft Entra admin center → Enterprise applications → the app → Delete. That is the whole procedure. It takes effect immediately, from your side, and requires no notice to us and no cooperation from us.

2. Remediation is a separate, optional application

Most scanners stop at telling you what is wrong. We can also fix some of it — revoke a sharing link, remove someone from a group. **That capability lives in a different Entra application, and you do not have to enable it.**

	Scanner	Remediation
Required to use the product	**Yes**	**No**
Consent	Once, by an administrator	Separate, explicit, optional
Acts as	Itself, unattended, on a schedule	**The person clicking**, never alone
Can it write?	**No**	Yes — only what you consented to
Revoke independently	Yes	Yes

If you never enable it, the product has no ability to modify your tenant, and every fix button refuses, states which permission it would need, and records the refusal in your audit trail. Nothing silently fails and nothing is retried.

If you do enable it, it uses **delegated** permissions — it acts as the signed-in operator, with that operator's own rights. It cannot remove anything they could not remove themselves in the Microsoft admin portal, and the action is attributed to **them**, in **your own** Microsoft audit log, not only in ours. Scheduled scans continue to run under the read-only scanner identity, so **nothing on a timer can ever change your tenant.**

A reasonable way to run a first engagement: **scan only.** Decide about remediation later, once the findings have shown you whether you want it.

3. How to verify this yourself, in about a minute

Do not take our word for any of it. Two independent checks:

In your own tenant — *Microsoft Entra admin center → Enterprise applications → Olyteck Cyber Scanner → Permissions*. Every row should read `.Read.`. That list is authoritative: if it disagrees with anything we have told you, **your tenant is right and we are wrong**, and we want to know.

In the product — *Security Console → Apps & consent*. This panel reads the live grant from Microsoft every time it loads. It is not a stored setting and not marketing copy. It shows all three applications, every permission each one holds, and an action-by-action list of what the product can and cannot change in your tenant. If a write permission were present, that panel would say so — it is not capable of rendering the read-only claim when the claim is untrue.

4. Data handling, in four lines

- **Stored:** counts, flags, severities, and the identifiers needed to show you which site or account a finding refers to.
- **Not stored:** file contents, message bodies, attachments, access tokens.
- **Where:** European Union. GDPR-aligned. Sub-processor list published.
- **Retention:** configurable; 30 days during a trial.

Full detail: Trust Center (**https://olyteck.com/trust/cyber**) and the DPA.

5. Documents available for a review pack

Document	What it covers
Microsoft Graph permissions statement	Every permission, why, and what we deliberately do not request. Offered for counter-signature
Data Processing Agreement (DPA)	GDPR Article 28 terms
Sub-processor list	Every third party, with location
Information Security Policy — executive summary	Signed, 2 pages
Latest production DAST scan	OWASP ZAP, current result
CAIQ v4.0.3	Completed Consensus Assessments Initiative Questionnaire
GDPR one-pager	For DPO review

All at **https://olyteck.com/trust/cyber**.

6. One thing we disclose without being asked

A permissions statement that lists only the flattering facts is not worth relying on, so:

`SecurityEvents.Read.All` **is broader than our use of it.** The permission also permits reading the legacy `/security/alerts` collection. We call only the two Secure Score endpoints — `/security/secureScores` and `/security/secureScoreControlProfiles`. Microsoft publishes no narrower permission for Secure Score; we would use one if it existed.

We would rather you heard that from us than found it in the Graph documentation.

Olyteck · security@olyteck.com · https://olyteck.com/trust/cyber