

Know the cyber risk before you sign

A white-box technical and code assessment of the target, delivered in time to inform the decision rather than explain it afterwards.

In M&A, the risk you miss becomes the liability you own

A target can look healthy on paper and still carry vulnerabilities that turn into financial and reputational damage the day after close. Technical debt, unsupported components, and unreviewed code do not appear in a data room.

We assess the technology stack and codebase from an attacker's perspective, then hand you a clear picture of the cyber risk so you can price it, plan for it, or walk away.

5 to 10 days.

Most assessments, start to finish, scoped to your deal timeline.

What you are actually signing up for

Turnaround. 5 to 10 days for most deals, agreed against your timeline at scoping.

Access required. This is a white-box assessment, so we need source code and infrastructure access. We agree exactly what is needed before we start.

What you receive. An executive summary, scope and limitations, findings rated from critical to informational, and remediation recommendations.

Buy-side or sell-side. Assess a target before you commit, or have your own environment assessed before buyers scrutinise it.

Scoped to the deal. We align on your investment objectives first, so findings are framed against valuation rather than against a generic checklist.

What we assess

- 01 White-box code assessment.** Full access to source code, with manual and automated analysis of the codebase and technology stack.
- 02 OWASP Top 10 focus.** Critical issues such as injection, cross-site scripting, and broken authentication, identified and rated.
- 03 Infrastructure and stack review.** Technical assets reviewed for the weaknesses that change what the deal is worth.
- 04 Investor-ready reporting.** Risks and recommendations with an executive summary and clear severity levels.

Who it is for

Private equity and investors.

Price cyber risk into the deal before you commit.

Strategic acquirers.

Understand what you are integrating before you own it.

Companies being acquired.

Go to market with cyber risk already understood and evidenced.

Corporate development teams.

A repeatable technical assessment across targets, on deal timelines.

From investment objectives to a decision-ready report

01 Scope and preparation.
Align on your investment objectives and the target's infrastructure, then agree access and timeline.

02 Security assessment.
Review the technical assets and codebase, and identify the cyber risks that matter to the transaction.

03 Comprehensive reporting.
Actionable findings, severity levels, and remediation guidance, in time to inform the decision.

Why Syndis

Based in Iceland, Sweden, and Poland. Serving clients globally.

The assessment is run by our offensive team, the same people who spend the rest of their time breaking into production environments. They are looking at the target the way an attacker would after the deal closes, not working through a compliance checklist.

OSWA

OSWE

OSCP

OSCP+

Assess before you acquire

Tell us about the target and your timeline. We come back with scope, access needs, and a delivery date that fits the deal. We respond to most inquiries within one business day.

■ syndis@syndis.com

