SERVICE DATASHEET

M&A-Related Due Diligence

Get a clear view of an organization's cyber exposure before you invest.

Cye's due diligence security assessments provide the buyer side an evidence-based view of an organization's security posture and potential exposure. Cye combines organizational and product security assessments, threat hunting, penetration testing, and threat intelligence to uncover vulnerabilities, active threats, exposed data, and other issues that could affect the value of the acquired organization.

With Cye, deal teams can assess cyber risk, understand its potential impact, and make informed decisions before and after close.

TRUSTED BY

Cyber Exposure Can Impact Valuation

An organization may look healthy on paper while carrying vulnerabilities, compromised assets, exposed credentials, or security gaps that only emerge through deeper diligence.

Those findings can affect valuation, deal terms, closing conditions, and post-close investment requirements. Identifying them before signing gives the deal team evidence to negotiate with — and a clearer view of the cyber risk being acquired.

Treating cybersecurity merely as an IT checkbox can result in unwanted costly surprises after deal closure.

1 in 4 PE firms

reported reduced valuation or exit price due to an incident.

Source: Kroll, 2026

Get a Defensible View of Cyber Exposure Before You Invest

1

Assess

Understand the organization's maturity, controls, products, assets, and external exposure

→

2

Validate

Use threat intelligence-led threat hunting to determine what is actually vulnerable, exploitable, or already compromised.

→

3

Quantify

Prioritize findings and understand their potential financial, remediation, and transactional impact.

A Comprehensive View of Cyber Exposure

01 Organizational Assessment

Assess maturity and controls

Evaluate the organization's security maturity, practices, and controls through internal and external threat scenarios.

02 Product Security Assessment

Assess the security of the product

Test the product's security posture using grey-box testing and, where required, source-code review to identify high-risk vulnerabilities.

03 Threat Hunting

Look for signs of active compromise

Proactively search the organization's networks and assets for evidence of breaches, malicious activity, or other threats.

04 Threat Intelligence Investigation

Find what's already exposed

Search the clear, deep, and dark web for exposed credentials, leaked data, breaches, and other evidence of malicious activity affecting the organization.

What You Get from the Assessments

Cye translates assessment findings into a prioritized view of cyber exposure and its potential impact on the investment.

▸ Prioritized Exposure
Identify the vulnerabilities, threats, and security gaps that could affect the investment.

▸ Plan Remediation
Understand what needs to be addressed, how urgently, and where post-close investment may be required.

▸ Inform the Deal
Use defensible findings to inform valuation, negotiations, and closing conditions.

▸ Avoid Post-Close Surprises
Start with a clear understanding of cyber exposure rather than discovering issues after close.

Why Cye

Due diligence should connect cyber exposure to the investment decision. Cye combines hands-on cybersecurity expertise with an AI-native exposure management platform to provide an evidence-based view of cyber exposure — from security controls and product vulnerabilities to active compromise and external threats that could affect the value of the acquired organization.

Cye translates cyber exposure into clear priorities for the transaction, from valuation and negotiations to remediation requirements after close.

Assess the Risk Before You Sign →

About Cye Cye combines an AI-native exposure management platform with world-class cyber expertise to help organizations understand their cyber exposure, prioritize risk mitigation, and automate remediation. Cye's 500+ customers gain the clarity to make smart, defensible decisions across the investment lifecycle.