OSINT | Auto Risk Assessment

For When "Good" Is Good Enough

Effortlessly track vendors by reviewing a concise overview of their risk standing. This basic assessment uses publicly available open-source intelligence to provide a high-level indication of risk.

We refer to this data as "good" since, despite being less reliable than a comprehensive assessment, it still holds value. OSINT | Auto automatically updates scores on a weekly basis, ensuring uninterrupted monitoring of third-party risk.

What Does OSINT | Auto Assess?

Cyber Hygeine
Evaluates misconfigurations and inadequate cyber hygiene. Identifies vulnerabilities, SSL certificate status, email configurations, and more.

News & Reputation
Searches public reports, breach notifications, and third-party associations for evidence of prior breaches or security issues.

User Behavior
Analyzes users' data security practices. Investigates data leakage, DNS typo-squatting, and technical data disclosures in RFPs, RFQs, and other publications. Includes a Dark Web scan for compromised credentials.

Cost & Time Effiecient

OSINT | Auto collects and scores risk data in its automated digital dashboard within seconds, requiring little input or cost from an organization.

Automated processes gather data on a target company using its primary domain name. Because OSINT data is historical and publicly available, OSINT | Auto is capable of rapidly assessing thousands of vendors.

OSINT is best suited for evaluating risk related to new business ventures, non-critical vendors, or vendors with restricted access to sensitive data.

When to Choose OSINT | Auto

QUALIFY vendors prior to onboarding

SELECT vendors and conduct evaluations

VALIDATE vendor compliance

myCYPR™

6315 Hillside Court, Ste J
Columbia, MD 21046
United States

410-292-7601
info@anchortechnologies.com
www.mycypr.com