Service Brief

Investment Zero Touch Diligence℠

Discovery to assess risk for investments, IPOs, Mergers and Acquisitions

Nisos helps you exceed typical consultative M&A diligence capabilities by contextualizing the risk of investments in order to deliver more actionable outcomes post-acquisition.

Sophisticated investors and acquirers take robust consultative approaches to integrate networks and applications after an acquisition. However, rarely do acquiring security and intelligence teams have the resources or internal processes to perform investigative diligence on a target before an acquisition is executed.

Consultative reviews and questionnaires are a typical starting point for M&A teams, but these reviews often lack context and validation of the information provided. This leaves critical, actionable information overlooked.

Investors, auditing and consulting firms, and large company security teams generally perform interview-based cyber diligence and data reviews with the acquisition target's IT team to determine the security stack's maturity. They work to identify exposed vulnerabilities that could be or have been exploited by threat actors, typically by reviewing previous penetration tests and vulnerability scans.

However, investors and complex organizations often lack the resources to do an in-depth analysis of the incoming network. They also rarely evaluate reputation-based or negative press risks.

Typical M&A teams don't conduct intelligence analysis "outside of the firewall." This means they lack real-time insights into key-person risks, network security issues, and infrastructure vulnerabilities.

Nisos Zero Touch Diligence℠ is Different.

Maximize your external visibility with analyst-led diligence investigations that combine automation and human intelligence to deliver actionable information to assess M&A risks.

How it Works:

Nisos Zero Touch Diligence℠ is an analyst-led, external cyber diligence service that combines automation and human investigation to provide timely and accurate insight to corporate development and merger and acquisition teams.

Zero Touch Diligence combines cybersecurity and OSINT (Open Source Intelligence) expertise to provide deep, current, and comprehensive insight within the context of the client's specific needs.

Why it's Better:

Robust analytic methodology is combined with a suite of tools to collect, store, enrich, and integrate data from a wide variety of sources. When used at scale, it is capable of arming the M&A team with faster actionable insights.

Nisos Collection & Analysis Stack

Network & Telephony
- Anonymous Infrastructure
- DNS and WHOIS
- Internet Netflow (90%+ of IPV4)
- Mobile and IP Geolocation
- Threat Feeds

Web & Social
- Deep and Dark Web
- Foreign Media
- Historical Web Content
- Open Web
- Social Media

Human
- Closed Forum
- Deep and Dark Web

Media
- Domestic News
- Foreign Media

Adversaries
- Activist
- Disinformation
- E-Crime
- Nation State
- Political

Breach
- 20+ billion records of legally acquired datasets including PII, selectors, and information/credentials

Businesses
- Business Registrations
- Corporate Filings
- Corporate Profiles
- Public Records

Persons & Groups
- Biographical
- Civil and Criminal Actions
- Email and Identity
- Investigative Databases
- Public Records

Services

External Cybersecurity Posture Assessment

Analyzes information collected from a wide range of data sources to identify specific vulnerabilities in a target company's network and infrastructure. Included in our report is a criticality assessment and recommendations for additional investigation or remediation. Data analyzed includes:

- Indicators of current or past breaches
- Mapping of the target company's WAN and MPLS network infrastructure
- Network ingress and egress points
- Internal and external security products that may be in use
- Patches and security protocol maturity
- Malware infection frequency and duration
- Efficacy of malware mitigation strategies
- Geographic or business unit-based differences in security maturity across a company

Brand Reputation Threat Discovery

Assesses the extent of the acquisition target's exposure by examining key data and individuals that may have been compromised. Senior executives and network administrators are often the targets of bad actors. Using our knowledge of dark web methodologies combined with commercial and proprietary tools, we identify risk factors, such as:

- Breached credentials
- Exploitable software
- Direct network access offers
- Stolen intellectual property for sale
- Chatter related to targeting the vendor company
- Code or data in file sharing sites such as Github, Pastebin, etc.

Non-Traditional Business Risk

Non-traditional business risks can be discoverable digitally. Zero Touch Diligence includes a tailored aggregation system to gather relevant, publicly available, potentially sensitive information about the acquisition target. This may include:

- Criminal or derogatory information on key personnel or investors
- Indications of hostile control or undue influence from criminal elements or potentially hostile nation states
- Evidence of suspicious financial activity to include insider trading or embezzlement
- Allegations of intellectual property theft, unethical practices, or whistleblower complaints

Deliverables

Nisos helps you be negotiation-ready with triaged, actionable findings that augment your internal M&A analyses. For each target subject to evaluation, a comprehensive finished intelligence report will be developed that documents risk findings by type and criticality. When relevant, technical data is delivered in an ingestible format for further Client use and analysis.

Reporting will include:

- Executive overviews that outline findings and associated risks
- Detailed summaries of the risks discovered in:
  - Network and Infrastructure
  - Deep/Dark/Surface Web Threats
  - Derogatory Information and Press

About Nisos

Nisos is the Managed Intelligence™ company. Our services enable security, intelligence, and trust and safety teams to leverage a world-class intelligence capability tailored to their needs. We fuse robust data collection with a deep understanding of the adversarial mindset delivering smarter defense and more effective response against advanced cyber attacks, disinformation, and abuse of digital platforms.

For more information visit: nisos.com
email: info@nisos.com | 703-382-8400

Micro Case Study

Example 1:

While conducting a Zero Touch Diligence assessment of a company undergoing a merger, we uncovered a well-developed card-skimming attack that had been present for several months. As part of the incident response, Nisos operators identified that very early on in the breach, the attacker had posted internal source code on Pastebin.

This discovery enabled the acquiring company to prevent "passing the breach" to its much larger environment while preserving its acquisition target's value.

Example 2:

While conducting key man risk diligence against the investors and executive leadership against a foreign-owned technology company, we uncovered extensive open source press that indicated extensive connections with Russian organized crime and money laundering operations.

Our client, a US-based technology company, was in acquisition talks with the foreign-based entity and had concerns over FCPA allegations. After reviewing our diligence and postponing the deal to conduct its own investigation, the US-based technology company accepted the risk and acquired the company.