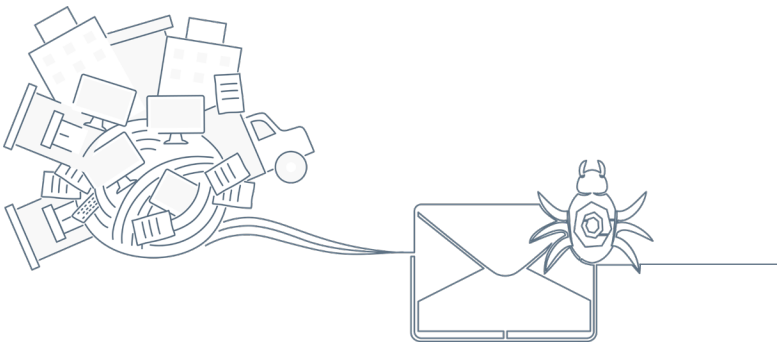
Service Brief

TPRM Zero Touch Diligence℠

Subscription assessment of external network hygiene, key personnel, and non-traditional business risks

Nisos helps you meet challenges that exceed typical Third-Party Risk Management (TPRM) capabilities by contextualizing the risk of third parties.



Third-party vendors and supply chains are one of the fastest growing risks to enterprise organizations. Ponemon Institute estimates that poor outsourcing decisions are responsible for 63% of data breaches. Security analysts responsible for vendor management are faced with complex human and technical challenges.

Common "Solutions"

Organizations typically rely on **questionnaires** as a standard baseline tool, but they recognize their shortcomings when it comes to visibility, deep dive analysis, and bad information. In addition, they fail to provide critical, time-sensitive, and actionable information.

Questionnaires offer point-in-time visibility and are affected by false positives and human reporting errors. They lack context making it challenging to validate information quickly and often cannot inform TPRM teams of data leaks or a breach until they are public knowledge.

Ratings and risk management tools aggregate useful insights, in real time, offering risk managers data about their third-party suppliers, but the information **isn't tuned to specific business risks with unique parties.**

Also, typical ratings companies fail to include an organizations extended supply chain as part of their assessment.

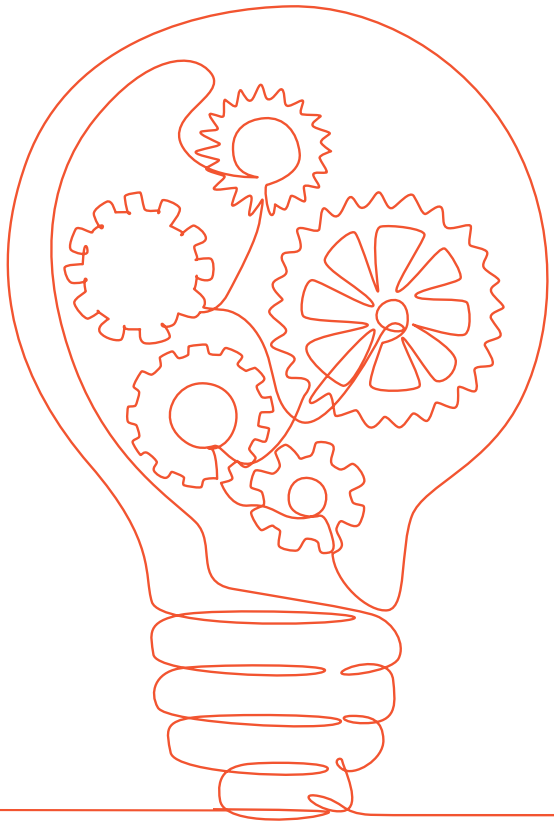
It's also unlikely that risk managers will have the access required to evaluate third party's networks in a reasonable timeframe.

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 about third-party risk.

How it Works:

Zero Touch Diligence℠ combines cybersecurity and OSINT (Open Source Intelligence) expertise to provide deep, current, and comprehensive insight within the context of your specific needs. By fusing robust analytic methodology with a suite of tools Nisos facilitates tailored monitoring and professional analysis of complex data sources. These tools collect, store, enrich, and integrate data from a wide variety of sources, which translates into more accurate, validated, and actionable insights delivered to you.



Why it's Better:

The information delivered through Zero Touch Diligence is curated and prepared by trained experts who contextualize and triage the findings for you. When used at scale, Zero Touch helps TPRM teams save time and money typically lost to nebulous or unorganized findings.

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

Network Infrastructure & Analysis

Analyzes information collected from a wide range of data sources to identify specific vulnerabilities in the network and infrastructure of a target company. 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

Deep/Dark/Surface Web Threat Discovery

Assesses the extent of a third party'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.

Historical Actions Investigation

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 third parties. 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 boardroom-ready with triaged, actionable findings that augment your internal analyses. For each vendor 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 vendor 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

While conducting a zero touch diligence assessment, we were able to uncover IP addresses directly associated with a vendor's physical office on the public Internet. This led to the identification of specific infrastructure which would likely be targeted by an advanced attacker.

Additionally, this led to the identification of a VPN server which provided remote access to the vendor's corporate network. We also discovered a third-party Docker instance publicly accessible with default credentials.

This particular instance did not belong to the vendor, but it could be leveraged by an attacker to gain control over a customer. It could also be used as an access vector leading to a potential breach of someone using the third-party's software; ultimately affecting their brand reputation and ability to generate new clients.

These discoveries are important for a TPRM analyst to use in the context of their own risk matrices.

In this case, a TPRM team might only want to notify the vendor to take remediations in a given 60-90 time window if no critical access of the third-party is required.

On the other hand, if the vendor requires critical access, perhaps the TPRM team might need to take more aggressive action and request in depth on-network measures like a penetration test or compromise assessment.