Third-Party Intelligence Solutions

Third-party threat assessments, investigations, and monitoring

NISOS.

Nisos Third-Party Intelligence Solutions give you ready access to a team of expert intelligence practitioners focused on identifying, investigating, and countering human risks to your organization. As an analyst-led service Third-Party Intelligence Solutions help enterprise teams lift the veil on threat actors, and potential partners, clients, and investors to identify risk indicators. These insights empower you to make informed decisions.

Threat Assessments	Investigations	Monitoring
Understand risk posture to inform critical decisions.	Unmask threats. Understand techniques & motivations.	Post-investigation monitoring for critical threats.

Unmask and Identify a Threat Actor Threatening Your Company or People

Identify a specific individual, group, or organization to a threat or security incident. Understand who is responsible for the attack, their motives, methods, and whether they are part of a larger network or acting independently.

Assess Third-Party Risks

Investigate and understand whether your partner, investor, or client has undisclosed ties that could pose a risk. Assessments identify hidden relationships, affiliations, or connections that may negatively impact your business or brand. These undisclosed ties could involve associations with individuals, organizations, or activities that are unethical, illegal, or controversial, resulting in company risk.

Stay on Top of Identified Risks and be Alerted to any Critical Threats

Monitoring and analysis delivers finished, actionable intelligence that helps your security team cut through the noise, identify critical threats, and respond confidently to reduce risk. Nisos works as an extension of your team to track and uncover targeted threats, disruptions, and other areas of concern that could impact your organization.

Threat Ecosystem Assessments	Social Network Analysis	Threat Actor Assessment
Threat Monitoring & Analysis	**Individual Due Diligence**	**Attribution & Enrichment**

For more information visit: **www.nisos.com**
email: **info@nisos.com**

call: **+1-703-382-8400**
follow: **LinkedIn**

Third-Party Intelligence Solutions

Nisos Assessments are Different

Unlike the traditional threat intelligence approach of delivering standard datasets with generic insights, Nisos uses our vast multi-source collection and analysis capability to uncover critical insights and tailored recommendations for your unique human risk threats. Nisos' threat assessments provide visibility beyond the perimeter of your internal firewalls and security. Our insights provide actionable intelligence and prioritized threat mitigation recommendations to help you reduce human risk.

Driving Impact

Third-Party Risk Investigations Maximize our Visibility

"Nisos' analyst-led Third-Party Risk Investigations maximize our visibility into relevant, traditional, AND non-traditional business risks within our ecosystem ensuring we are able to properly analyze exposure and take proper action."
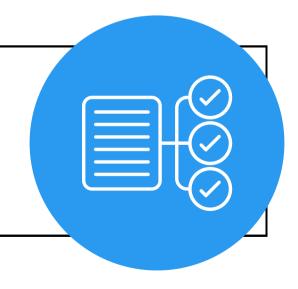
Global Chief Security and Resiliency Officer - Vice President - Boston Scientific

Elevating the Power of Human Tradecraft

Nisos derives finished intelligence from the chaos of the open, deep, and dark web using tradecraft and advanced tools. Our proprietary human intelligence platform empowers Nisos' team of expert analysts to rapidly query a vast, curated collection of data sources, collection tools, and lawfully obtained breach records.

Deliverables Include

- One comprehensive threat ecosystem assessment report
- Intelligence briefings with Nisos analysts
- Monitoring & analysis
- Individual investigations & assessments scoped to your requirements

About Nisos®

Nisos is the human risk management company specializing in unmasking threats before they escalate. We are a trusted advisor who operates as an extension of security, intelligence, legal, and human resource teams to protect their people and business. Our intelligence-led solutions help enterprises make critical decisions, manage human risk, and drive real world consequences for digital threats.