Service Brief

OSINT Monitoring & Analysis

Broad and customized monitoring of social media data to enable actionable intelligence for Nisos clients

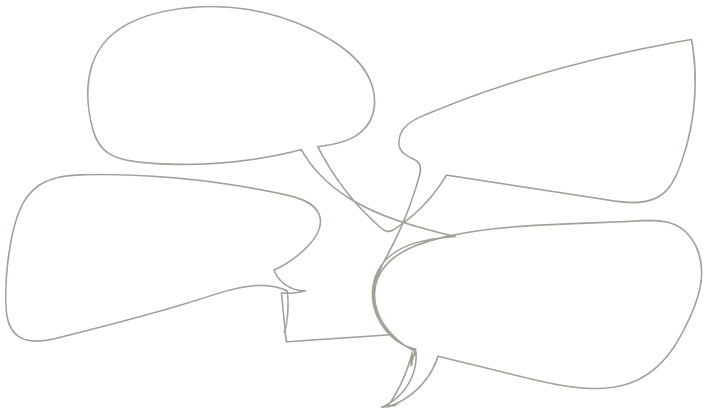
Nisos customizes social media, dark web, and open source (OSINT) analysis to enable enterprises to use Managed Intelligence™ operations for:

- **Physical security**
- **Cybersecurity**
- **Fraud**
- **Platform abuse**
- **Third-party risk**
- **Brand reputation**
- **Executive protection teams**

Nisos also maintains a robust OSINT analysis capability, which includes disinformation and actor unmasking.

Why Nisos is Different

Our highly-trained analysts use many types of technologies, providing both broad coverage of thousands of platform pages and bespoke solutions to gain access to closed forums.



Nisos Intelligence Domains

Reputation Intelligence

Threats, abuse, and risks to Client's brand and reputation. Negative sentiment and campaigns of disinformation/misinformation.

Cyber Threat Intelligence

Threats and risks to confidentiality, integrity, and availability of sensitive data including data leakage and insider threats.

Fraud Intelligence

Cybercrime, e-crime, and online fraud. Trafficking in stolen or illegal physical goods, illicit purchases of good or near money instruments (gift cards, credits), use of stolen credentials, accounts, or payment methods.

Platform Intelligence

Threats to risks to the trust and safety of an online platform. Misuse or abuse of credentials and/or accounts, platform abuse including use of counterfeit apps, malicious content syndication, API manipulation via bots.

Protective Intelligence

Threats and risks to executives, physical property, corporate assets, PII takedown capabilities in response to doxing.

Third Party Intelligence

Threats and risks by vendors, suppliers, partners, mergers, acquisitions, and investments. Data leakage of client data by vendors.

Broad-Based Collection

We use broad-based collection strategies to pool thousands of pages of content, which we then search for keyword mentions of the brand, key personnel, the company, or company products.

Using over 30 sources including third-party products and our own proprietary tools and personas, we view, store, collect, and export many social media pages and archive this data in a highly-secure and closely-maintained central storage location. We collect thousands of pages of content, which Nisos operators then review for long-term monitoring and event-driven investigations.

Dark Web Data

We maintain access to numerous dark web forums including but not limited to xss[.]is, raidforums[.]com, exploit[.]in, nulled[.]to, hackforums[.]net.

We also leverage our custom personas to collect on specific marketplaces and forums on the dark web that require credentials to access them.

Social Media Data

In addition to the best known and most widely used social media platforms, we also analyze less-trafficked platforms including:

- 4chan
- 8chan
- 8kun
- Bitchute
- Clouthub
- DailyStormer
- Discord
- Doxbin
- Element
- Freespeechtremist
- Gab
- IRC
- KiwiFarms
- MeWe
- Minds
- Parler
- Qalerts
- Reddit
- Rumble
- skidbin.org
- Telegram
- Tumblr
- VK
- Voat
- Wimkin
- Zello

Closed Forums

On many occasions, clients want detailed insights about a specified threat. Using appropriate tradecraft and following legal guidance, we gain access to closed forums on social media and connect with persons of interest, including threat actors, to gain insights important to our clients. Similarly, we export the data in a usable format for analysis.

Virtual Research Environment

We conduct all OSINT research from virtual research environments provisioned with appropriate security measures. Within these environments, through actively engaging or passively observed, our analysts move swiftly between platforms and personas to garner a better understanding of threat actors' motives and plans.

Attribution and Unmasking, if Necessary

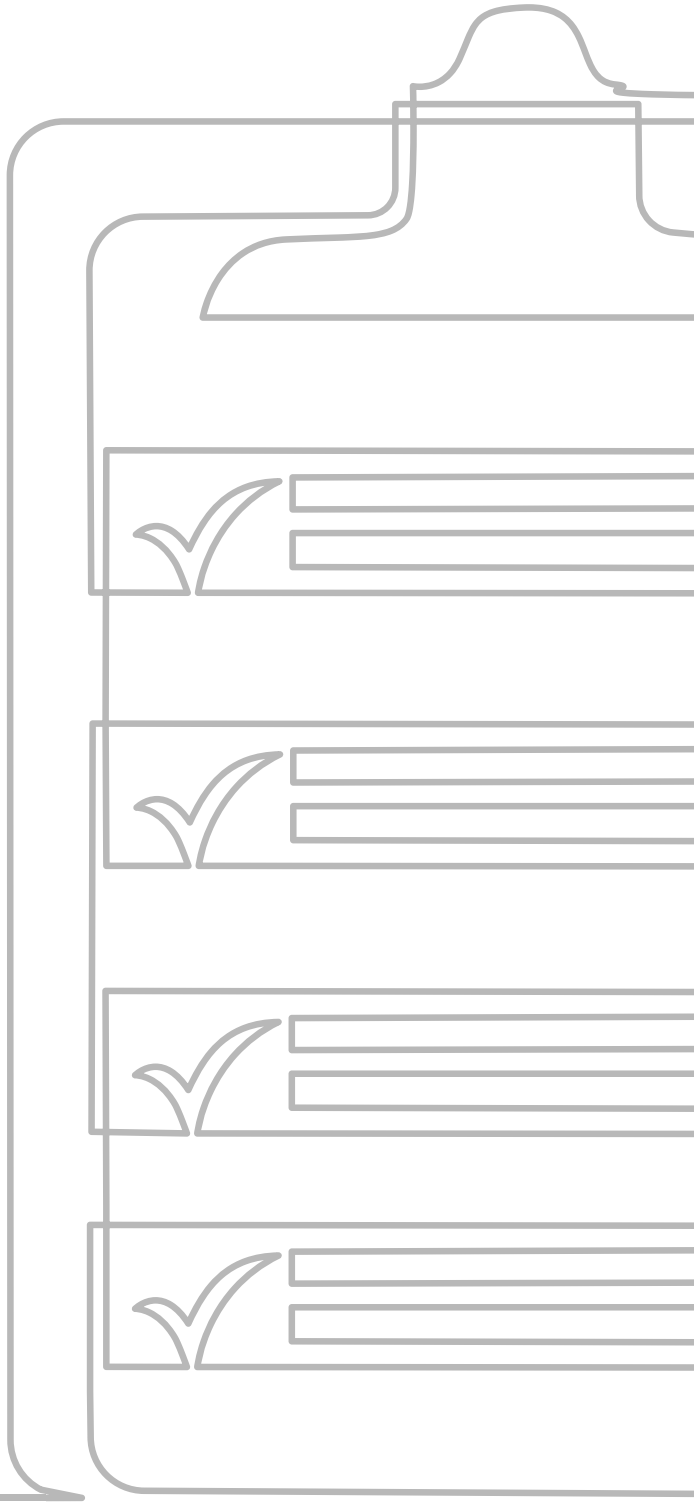
Finally, attribution is needed for various threats. Advanced adversary research attribution relies on advanced tradecraft to ensure accuracy. Our ability to correctly attribute bad actors to confirm their identity, and to do so in a manner that is unseen by the adversary, is often a critical component of our research capability.

Deliverables

Nisos provides subscription monitoring which enables you to take action and protect your people, your business, your customers, and your assets with rapid and curated responses to intelligence questions and concerns.

Reports available:

- **Situation Briefing:** Monthly summary status report of trends and activity observed by Nisos researchers and analysts
- **Spot Report:** a supplemental brief used to quickly communicate time-sensitive intelligence for significant events impacting a client



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