Capability Brief

Social Media Monitoring & Analysis

Broad and Customized Monitoring of Social Media Data to Enable Actionable Intelligence for Nisos Clients

Nisos customizes social media analysis to enable managed intelligence operations for physical security, cybersecurity, fraud, trust and safety, and executive protection teams within an enterprise.

Nisos maintains a robust social media analysis capability which informs brand reputation, disinformation, and adversary attribution research.

Social Media Data We Analyze

Adversaries don't just use the best known and most widely trafficked platforms - they use more obscure channels. Nisos investigates those less-trafficked platforms to ensure you are more fully informed about your risks. Contact us for a full list.

Our Differentiator

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.**

Virtual Research Environment

We conduct all social media 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.

Broad-Based Collection

Using 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.

Customized Monitoring Against 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.

Managed Intelligence™ Solutions

Adversary Research

Discovering the methods, motives and identity of threat actors to disrupt attacks

Reputation Defense

Technical guidance for countering disinformation and slanderous attacks

Outside Intel

"Tier 3" as a service providing outside the firewall intelligence and external threat hunting

Executive Shield

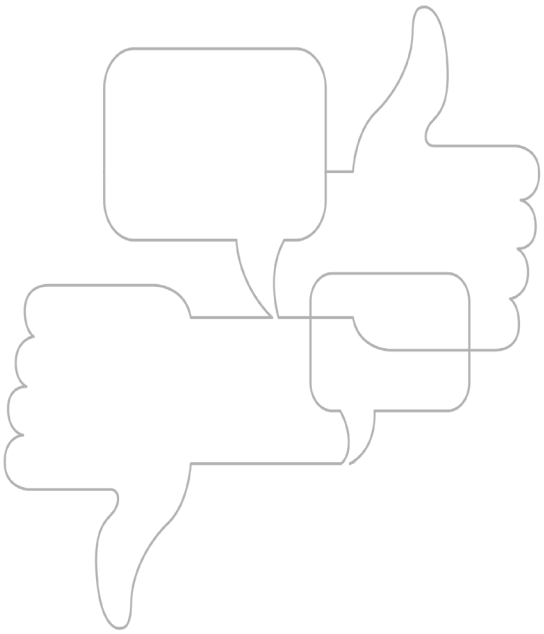
Assessment of threats to key personnel with attribution and PII takedown

Trust & Safety

Intelligence to secure business operations and defend against fraud, abuse, and e-crime

Third Party Risk Management Exposure

Adversary-centric intelligence to address supplier, M&A and investment risks



Social Media Analysis

Specific to Managed Intelligence™ Solutions

Brand Reputation, Executive Protection, M&A Diligence, and Third Party Risk Management

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. We use the collection for indicators and warnings, or to alert on negative information about a brand.

If warranted, we also gain access to closed groups and perform network and geopolitical analysis for long term monitoring engagements. Using the same methodologies, we conduct merger and acquisition diligence on executives and potential risks to the business.

Social Media Analysis

Specific to Managed Intelligence™ Solutions

Disinformation

We use third party tools that allow us to watchlist, alert, and analyze the narratives, outlets, accounts, and signatures of disinformation campaigns to uncover coordinated inauthentic behavior. This includes the examination of domain and web registrations as well as social network analysis.

Narrative:
What's being said

Account:
Which social media accounts are spreading the original disinformation

Outlet:
Where it's being said

Signature:
Technical indicators that enable attribution of the actor(s) responsible for genesis and spread

Trust and Safety

Malicious actors regularly target platforms for e-crime, fraud, and abuse and post their activity on social media where broad based collection is needed. Actors defraud an enterprise platform to cause losses to the company while they abuse the platform (potentially even as a paying customer) to defraud others.

Activity generally starts on a closed channel like Telegram or sub-Reddit forum. After engagement with an actor, we collect information on different protocols and tokens used as well as actors selling this type of information on the company. Bitcoin and crypto analysis can be deployed if we need to facilitate a time-sensitive purchase of information for a client.

Adversary Research and Attribution

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.

Social Media Collection and Analysis is a critical component of an enterprise's capabilities. Whether empowering intelligence operations for physical security, cyber, fraud, trust and safety, or executive protection, without being able to effectively collect, digest and draw connections from social media data, opportunities to identify adversaries are lost in the ether. Our unique collection and collection capabilities allow for ongoing and customized threat assessments that can stop adversaries in their tracks.