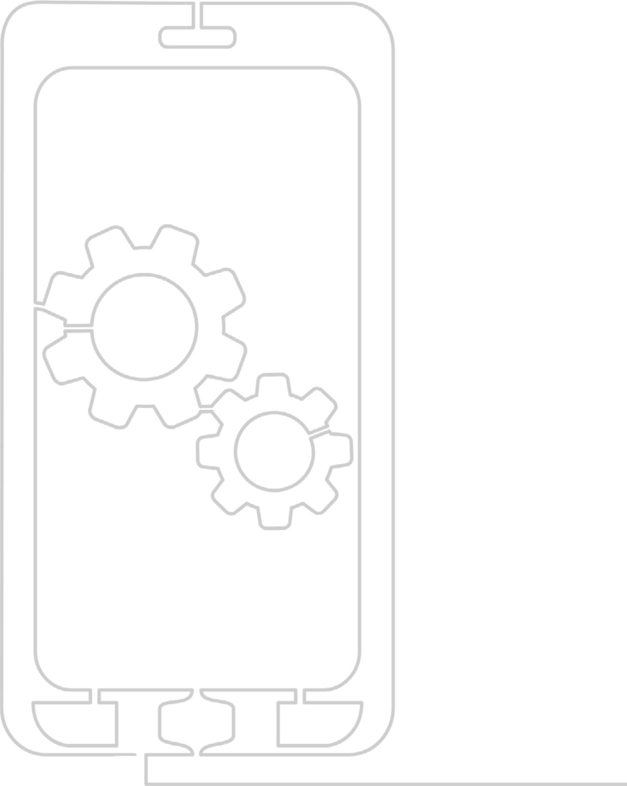
Solution Brief

Trust & Safety

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

Nisos helps businesses defend against non-traditional attacks threat actors use to target you and your customers. Attributing threat actors to crimes requires complex data aggregation and analysis.



Malicious actors regularly target external-facing platforms to commit e-crime, fraud, and abuse. Criminal actions that involve fraud across enterprise platforms and marketplaces cause financial losses to the company and breed distrust with customers and the public. Abuse of a platform, even that executed by a paying customer, in an effort to defraud others, creates deeper safety concerns.

Nisos can help, whether you're facing an organized-crime operation or an individual, we put context, including unmasking attribution (a name and face), to the people causing you or your customers damage.

Nisos Trust & Safety is Different.

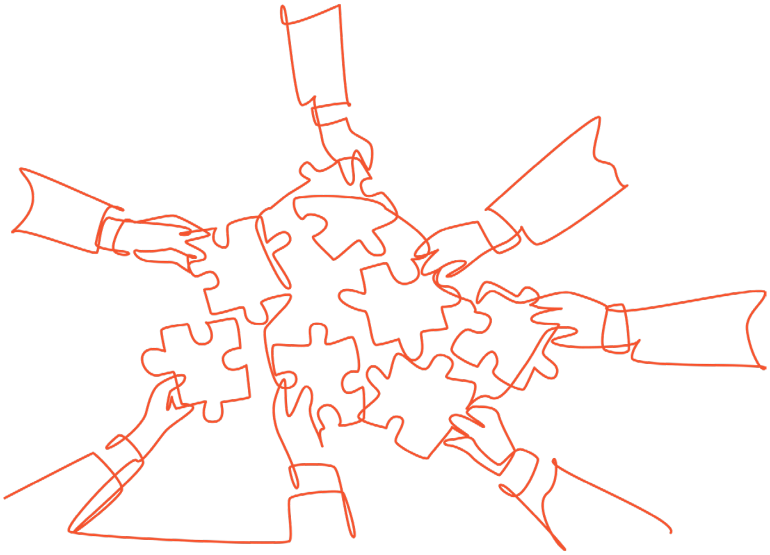
Maximize your organizational security with OSINT and technical analyst-led diligence investigations and monitoring that combine automation and digital human intelligence to deliver actionable information that is customized to your unique challenges.

Comparing Services: Trust & Safety vs Fraud and Cybersecurity

Trust and Safety is a term commonly used for defending platforms and marketplaces where people interact. Platforms are the technical foundation that enable total strangers to engage. If a platform is used to trade or sell - it is considered a marketplace, but it's important to note that not all marketplaces exchange money. For example, a dating service might require Trust & Safety to maintain a peaceful, fair, and enjoyable platform experience.

The importance of maintaining Trust & Safety cannot be overstated. Without it, people won't feel confident, comfortable, and motivated to share and interact. Without interpersonal interactions, the business may cease to thrive and issues may arise related to brand reputation that are devastating to the bottom line.

Traditional corporate security tools and collection mechanisms focus on data sources and analysis relating to a data feed. There is less emphasis on solving the problems that arise at the intersection of cybersecurity, fraud, physical security, trust, and safety. Internal teams don't typically engage with malicious actors online across the security spectrum, monitor their activities at scale across various platforms, or alert in a time-sensitive manner. This is why Nisos takes a different approach to solving the Trust & Safety Threat Actor problem.



How We Help:

Nisos collects and aggregates data across numerous social media and dark web platforms. We routinely engage with threat actors to maintain our credibility within these channels and our relevance for our clients.

In addition, we constantly curate various forms of breach data, including personally identifiable information (PII) publicly available on the internet. We also leverage information from major data brokers that aggregate PII on individuals and companies to create a more comprehensive evaluation of our client's exposure. Learn about the Nisos Intelligence Database.

Nisos has unique visibility into adversaries that goes beyond simply linking actors to previously identified and attributed tactics, techniques, and procedures (TTPs).

Capabilities

Defend and Respond to Cyber Crime, Espionage, E-Crime, and Fraud

In order to defend against espionage, e-crime, and fraud, you must detect threats with great speed, accuracy, and effectiveness. Most importantly, the intelligence must be tailored to combat global threats occurring at scale against your organization. Examples of e-crime that blend into trust and safety issues: cyber extortion, internet and platform fraud, spam and botnet activity, rogue applications, account takeovers, business email compromises, cyber espionage.

Activity generally starts outside an enterprise's perimeter in a closed channel, like Telegram. 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.

Here are a few of the things we do proactively and reactively to protect you from e-crime, trust and safety, and fraud:

Proactive & Reactive Activities

- Hosting of phishing activity on platforms or marketplaces
- Origination and amplification of DDOS attacks
- PII theft and fraud
- Phishing and spoof sites for business email compromises
- Rogue application creation and imitation
- Sensitive or Confidential information disclosure
- Financial or payment theft
- Account takeovers
- Suspicious domain registration for disinformation/brand reputation
- Command and control activity originating on platforms or in marketplaces
- Cyber espionage such as marketplace being used as a digital nation state dead drop
- Fake or spoofed accounts and apps
- Spam and botnet activity
- Virus/botnet/malicious infection or scanning in marketplace
- Selling counterfeit goods in a marketplace
- Discussions/threats observed in Dark Web/IRC/messaging networks and underground forums
- Gain access to closed forums and marketplaces
- Compromised account credentials for sale
- Malware hosting/distribution using a platform
- Attribution of PII or financial theft

Micro Case Studies

Case Study #1

Huddled around keyboards half a world away, a shadowy group of technically-savvy criminals devised techniques to hide from system administrators and run internet scams that defrauded a client out of hundreds of thousands of dollars in revenue every month. Payment fraud occurred and the merchant was a victim, probably losing both the funds and the goods, and paid the chargeback fees.

While not involved in any criminal activities of stealing credit card numbers, the platform still lost the battle of trust. Merchants, whether they like it or not, need to manage payment fraud rate, not just to reduce the financial losses, but to protect brand and reputation, and to build trust among their customers.

Read the full story >>

Case Study #2

A retail client requested our assistance to identify an individual, who was also a paying customer, who wrote a python script that scraped a backend server. The customer had also previously published a WiFi vulnerability present at the company's offices, thus threatening the safety of customers. The client was aware of closed forums where this customer and other potential threat actors exchanged ideas about denigrating the client's reputation and asked Nisos to help understand the nature of the threat.

Case Study #3

A technology company noticed a disturbing increase in malicious activity across their platform. Unknown individuals were selling bots that claimed to automate interactions with their platform and provide those that purchased the app an advantage over other users. This use of the app was a clear violation of the client's Terms of Service. In other words – the bots would "game the system" to the financial disadvantage of normal users – leading to frustration and anger directed at the client.

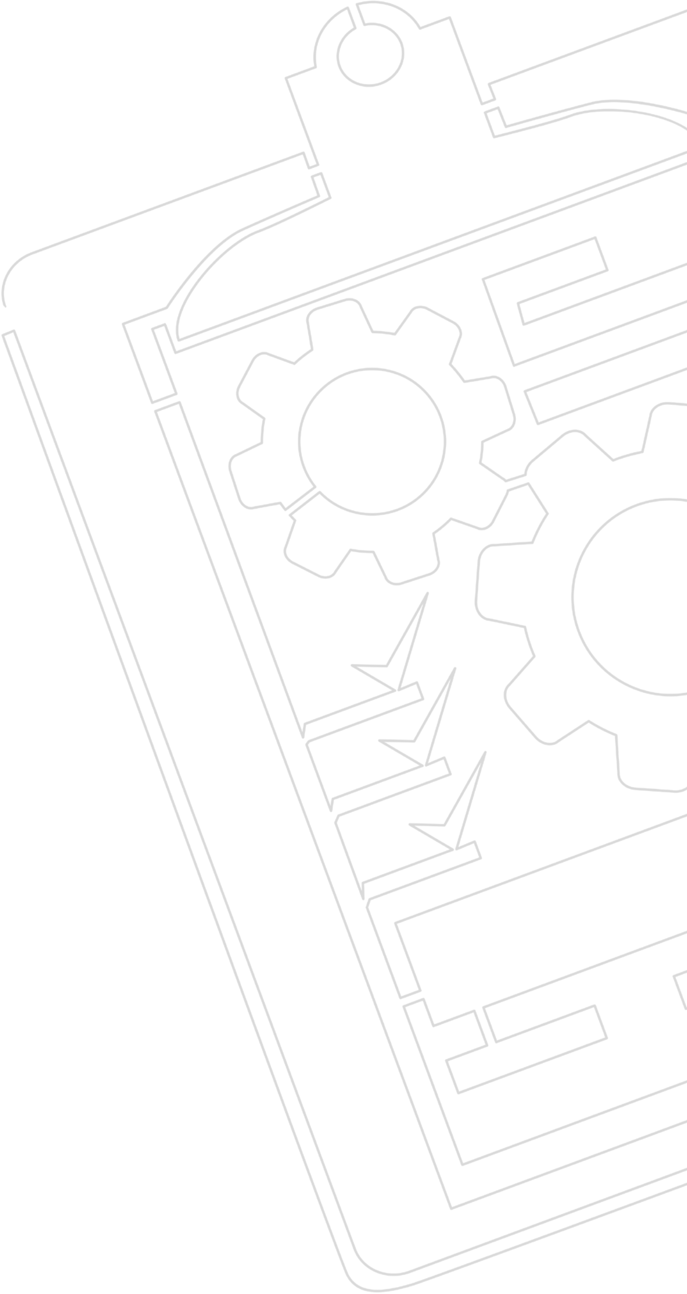
To make matters worse, the bots mirrored the legitimate client application, presenting additional security threats. While no payment fraud occurred users of the platform were taken advantage of thus reducing public trust in the platform.

Deliverables

Nisos provides subscription and retainer-based 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:

- **Fast Inquiry:** an on-demand request for information that includes a curated response to a specific intelligence question from a client
- **Situation Briefing:** an on-demand summary status report of an ongoing situation or activity monitored 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