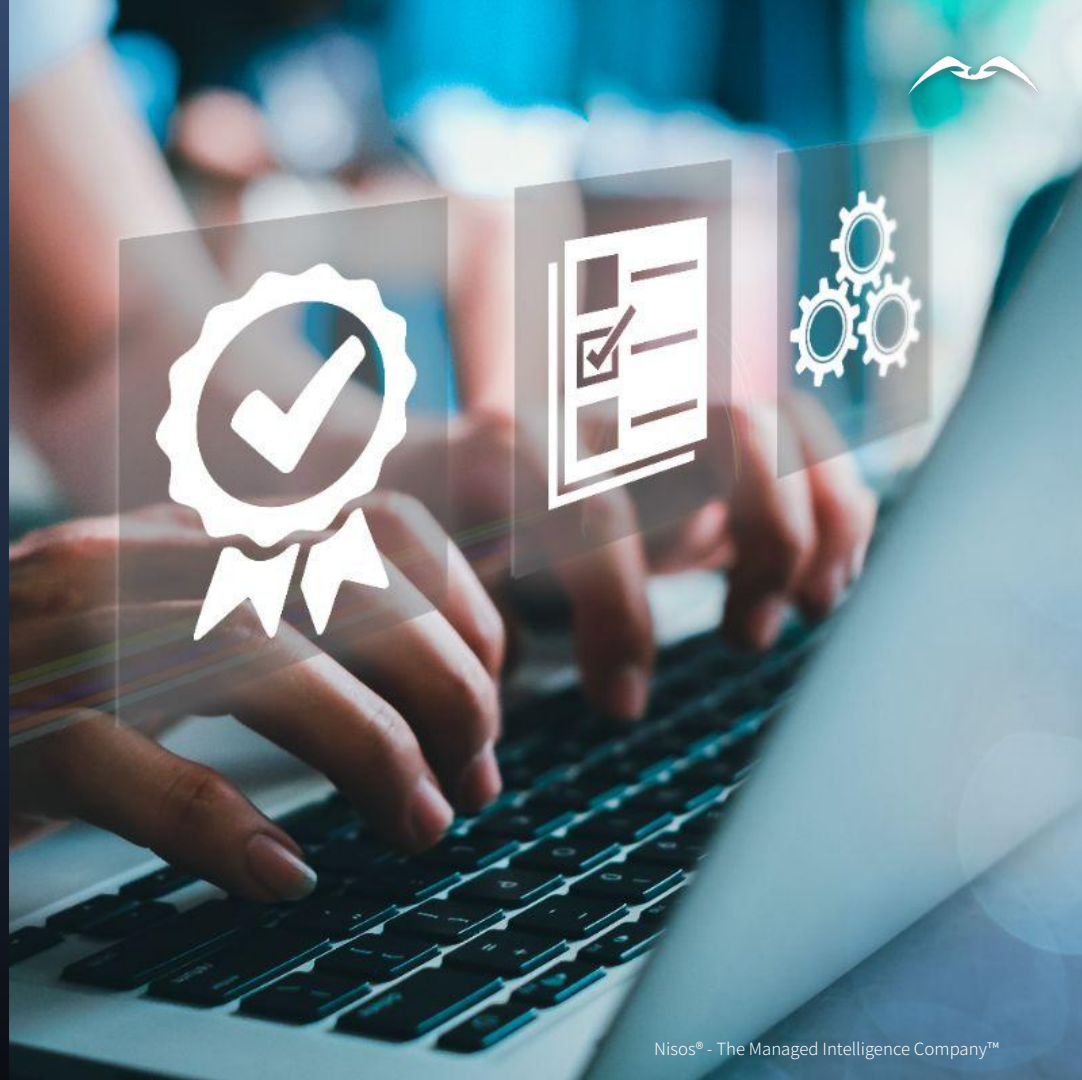
eBook

Trust & Safety Case Studies

Protecting Online Platforms

How Nisos helps **protect, and preserve safe, open, profitable environments where users thrive**



Trusted Digital Investigators

Online platforms must defend against determined, non-traditional attacks targeting your service and users. Confidently shutting down a threat requires diligence and know-how. Whether you face organized crime, nation-state campaigns, or individual actors, Nisos can unmask and attribute the threats targeting your platform.

Nisos provides an unparalleled digital investigations capability for:

- Unmasking threat actors
- Monitoring extremism
- Countering disinformation
- Adhering to global regulations
- Enabling real-world consequences

Maintaining trust in your platform and staying one step ahead of adversaries has never been more challenging. Nisos empowers your teams with insight and disrupts threat actors who use your systems for monetary gain.

In this eBook, we explore three examples of how Nisos has helped large online platforms overcome security challenges and protect their users.

Case Studies:

- Engaging Threat Actors Behind Targeted Fraud
- Investigating Extremist Groups
- Monitoring for Threats of Harm
- Unmasking a Short and Distort Campaign

“Nisos has an amazing team… Their ability to adapt to our needs as we mature has made them a key and critical partner for us.”

Dan Williams
Uber Technologies, Inc

Case Study

Trust & Safety

Engaging Threat Actors Behind Targeted Fraud

Nisos unmasks actors publishing content stolen from a **top educational technology brand**

SITUATION

Fraud and IP theft is an ongoing problem for educational vendors who offer digital courses and content. Using scraping tools, and other techniques, fraudsters steal content and offer it for sale in the dark corners of the internet.

When an leading platform for Online Education discovered a website offering free content taken from their digital products, they contacted Nisos to investigate who was behind the theft. The fraudulent websites allowed users to access the stolen content, without requiring a subscription, impacting the Client's revenue potential.

The fraudulent website allowed users to post questions to query data scraped from the Client's services. Users were required to complete a simple Captcha and provide a verifiable email address, to access to the final site hosting the content.

Nisos discovered the provided domain URL was hijacked from a legitimate news source, and changes randomly as a means to obfuscate the infrastructure behind the scheme.

INVESTIGATION

Anticipating legal action, Nisos was asked to engage with the actors behind the scheme to uncover any details that could be useful to the Client's case.

Using aged personas, burner devices, and other techniques to operate in anonymity, Nisos investigators engaged with threat actors inside of various Telegram channels offering 'free' solutions related to the Client's products.

- Nisos analysts actively **monitored four closed Telegram channels**, and **made direct contact with five threat actors** related to the scheme.
- Nisos investigators **exchanged direct messages with the primary threat actor** suspected to be behind the scheme, and were **able to confirm the owners likely identity**.
- Nisos **confirmed that the primary threat actor worked for the Client**, and also had **access to a compromised account** that allowed them to scrape content from the Client's products and services undetected.

IMPACT

Uncovering that the source of the stolen content allowed Nisos to further investigate the individuals behind the scheme. Nisos had direct conversations via Telegram with the actors to validate our findings and uncover additional details.

As a result of our work:

- Our investigation resulted in the **unmasking of three individuals** who either owned or operated the domains used to host stolen content and facilitate ad revenue.
- Nisos provided a **full profile of the actors** behind the fraudulent websites, including correlated social media accounts, emails, domains and more.
- The Client was able to confidently **pursue legal action against a current employee** who was helping to exfiltrate the stolen content.

Case Study

Trust & Safety

Investigating Extremist Groups

Nisos does a deep dive into an anti-government militia recruiting on a **a global social media platform**

SITUATION

The rise of extremisms and anti government movements is often amplified by Online platforms who struggle to balance content restriction from their ethos of free speech. Understanding the degree to which these groups manifest in online spaces, and staying ahead of escalating violent rhetoric is a challenge for every social media brand.

A major social media company requested information the Three Percenters, a loosely affiliated anti-government militia movement in the United States and Canada, after detecting a rise in content related to the movement on their platform. The Client was specifically concerned with their platform being used to facilitate recruitment efforts or prompt violence to their customers.

Nisos investigators analyzed on-platform and off-platform content and communications to understand the ecosystem behind the Three Percenters movement online.

INVESTIGATION

As part of their effort to prevent extremism and violent content on their platform, the Client requested Nisos provide a full accounting of relevant Three Percenters activity.

Nisos operator used our advanced toolset, and aged personas to anonymously detect and monitor Three Percenter content on, and off the Client's social media platform.

- Nisos **discovered users posting content supporting Three Percenters**, and including a variation of "Three Percent" in their user bios, usernames, display names, and as hashtags.
- We identified Three Percenter content **associated with Oath Keepers, Boogaloo Boys, and QAnon,** and seeking to connect with like-minded users and post content expressing their interest in **joining "patriot groups."**
- **Content referencing violence and rebellion** directed at the government in general terms, including comments saying they are ready to "fight" suggesting the **messaging may border on incitement**.

IMPACT

Nisos investigation resulted in a Deep RFI outlining ongoing on-platform and off-platform efforts by the Three Percenters to recruit new members, spread their message, connect with like minded groups, and share violent ideation.

As a result of our work:

- The **Client received a baseline of Three Percenter saturation** on their platform, and an assessment of the activity of the group.
- Nisos identified the **ongoing intersection** between the Three Percenters and other extremist groups.
- Nisos provided a detailed list of **common evasion techniques** used by the group to evade content detection, allowing the Client to tune their detection methods and refine their policies.

Case Study

Trust & Safety

Monitoring for Threats of Harm

Nisos provides overwatch for **a major gig economy platform** whose CEO was the target of planned protests

SITUATION

Executives and key personnel of controversial brands may find themselves targets of protests and harassment, online and in person, that are fomented and organized in behind digital closed doors.

When a Client was alerted to ongoing chatter on social media channels organizing a protest at their CEO's residence, they were concerned that the event could turn violent, and contacted Nisos to assess the risk.

Nisos discovered social media pages created by a fringe political organization that was promoting events targeting the Client and their executives. In addition to the one flagged by the Client, additional events were being organized by the group also targeting the Client's people.

INVESTIGATION

Nisos monitored the social media pages of several fringe political organizations targeting the Client. No mentions of the organizations were discovered on the deep or dark web, suggesting the accounts were new, and not part of public leaks.

Although the threat actors posts about the protest event received little interaction, the organizers hosted a public video meeting several days before the event to prepare potential participants.

- Nisos analysts **attended the video conference anonymously** to understand how the event was being characterized to potential attendees.
- Nisos **assessed that the event was unlikely to turn violent** given the lack of violent rhetoric, and minimal interaction with the social media posts themselves.
- A deeper look at the **individuals behind the social media pages uncovered that most shared a common nationality**, and attended universities in California.

IMPACT

As a result of our work:

- The Client and their CEO had a full understanding of the planned protest, and confidence that it was unlikely to cause any physical risk to themselves or their family.
- The Client was made aware of other political organizations generating chatter about the Client, and their relationship to the initial organization.
- Nisos was asked to continue to monitor social media, and the deep and dark web for evidence of similar threats.

Case Study

Trust & Safety

Unmasking a Short and Distort Campaign

Nisos investigates threat actors behind targeted campaign against **global Healthcare technology brand**

SITUATION

A global healthcare technology company faced a sophisticated 'short and distort' stock market manipulation campaign, costing the company billions in market cap. They uncovered various virtual, anonymous personas publishing false information about the company's leadership on social media and investing platforms – apparently in a coordinated fashion.

These activities negatively influenced public perception of the company's corporate governance and damaged the stock price, allowing those holding short positions to profit. While the Client had a firm understanding of the anonymous personas targeting it, their security team wasn't able to attribute the true identity of the fraudsters.

INVESTIGATION

The Client required a partner to confidently attribute the individual behind the "short and distort" scheme so they could assuage the concerns of investors and industry stakeholders. Our expertise in threat actor attribution and disinformation and curated open-source and commercial toolset enabled Nisos to connect the dots and develop finished intelligence with the context the Client needed to prove the nefarious origin of the disinformation.

After a thorough investigation, Nisos delivered a report attributing the online personas responsible for publishing false information. Nisos positively identified five individuals, each of which was found to hold a short position (or be affiliated with other investors who held short positions) against the pharmaceutical company's stock.

Nisos provided evidence that the fraudsters, via their hedge fund and pseudonymous social media accounts, fostered relationships with other like-minded short sellers, who helped to spread and amplify the same disinformation about the Client.

IMPACT

With Nisos report as the basis, the Client provided evidence to key institutional investors and stakeholders that confirmed the disinformation campaign was a fraudulent, coordinated effort to drive down the company stock price.

By addressing the issue head-on, and working with an expert like Nisos, the Client was able to reinforce confidence in corporate governance and secure continued investment from these key stakeholders at a time when further capital flight may have represented an existential risk to the business.

Let's **Connect**

Nisos is The Managed Intelligence Company®. Our analyst-led intel investigations, assessments, and monitoring services empower your security, intelligence and trust and safety teams. We provide accurate, customized intelligence that guides your security and risk decisions – protecting your organization, assets, and people. Learn more at nisos.com.

For more information:

visit: www.nisos.com
email: info@nisos.com
call: +1-703-382-8400
follow: LinkedIn, Twitter, Facebook, Instagram