eBook

Securing the Future of AI

How Nisos helps to ensure the **safety, integrity, and success of Artificial Intelligence**

Trusted Digital Investigators

Artificial Intelligence (AI) organizations are in the crosshairs of threat actors. From engineering new platforms in a competition to be the first to general AI, while onboarding more data, navigating increasingly complex equities, getting to scale fast, enabling new business applications while minimizing harm. At the same time, your organization's success depends on driving innovation in a highly competitive environment.

Securing the future of AI is important. Protecting intellectual property (IP), preventing misuse, and staying one step ahead of adversaries has never been more challenging. Nisos empowers your team with the insights you need to protect your organization, ecosystem, and people.

Nisos provides an unparalleled intelligence capability for:

- Uncovering AI data leaks and IP exposure
- Insider and phishing threat detection
- 3rd-party risk assessments
- Violative use and policy enforcement
- Human security risks
- Business and strategic intelligence

In this eBook, we explore examples of how Nisos has helped leading AI brands overcome security challenges and stay ahead of the curve.

Case Studies:

1. Monitoring for AI Leaks
2. Unmasking Employee Imposters
3. Assessing Supply Chain Risks

“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

Artificial Intelligence

Monitoring for AI Leaks

Nisos provides dark web monitoring and investigation services, **securing a crucial AI product launch**

SITUATION

Artificial Intelligence is a competitive space. Competitors and nation-state groups will go to great lengths to steal critical intellectual property to gain the upper hand, and leaks to the media are inevitable.

When a leading AI company faced the critical challenge of leaks about its latest cutting-edge product, it turned to Nisos, recognizing the importance of our expertise in digital investigations. The company needed to stay ahead of brand reputation challenges, prevent IP secrets from leaking, and keep their team safe in the event that online rhetoric turned into in-person violence.

Nisos' expertise in open-source intelligence and digital investigations offered the client unique insight into the physical security threats, trust and safety risks, reputational threats, and cyber vulnerabilities targeting their business and executives.

INVESTIGATION

Nisos was tasked with monitoring content related to the client's AI product and any content discussing the product's launch.

Using our proprietary intelligence platform for collection and exploitation, Nisos actively monitored for exposure across the open web, social media, industry forums, the deep and dark web, and more.

- Nisos analysts actively monitored social media, focusing on imposter accounts that could damage the client's reputation.
- Nisos investigators collected mainstream media coverage of the client and its products and provided ongoing sentiment analysis.
- Nisos uncovered and monitored fraud groups targeting the client on the dark web.

Ongoing monitoring gave the client confidence that their intellectual property remained safe before the launch. Following the launch, the client tasked Nisos with continuing to monitor for physical, reputational, and technical threats to the company.

As a result of our work:

- Nisos confirmed **no specific discussion of the client's AI product launch occurred** on social media or known dark web forums.
- Nisos **identified a trend of users manipulating the AI product** to identify errors and biases within the platform and posting the results on social media.
- Nisos **uncovered users claiming limited success in jailbreaking the AI system** but found no specific prompts that enabled any violation of the client's Terms of Service.

Case Study

Artificial Intelligence

Unmasking Employee Imposters

Nisos investigates threat actors **impersonating employees of a leading AI brand**

SITUATION

Imposters are using social media to pose as employees of AI companies to gain access to data or systems. Connections risk exposing the brand to data breaches, intellectual property theft, and unauthorized access to sensitive information.

When a leading AI company received reports from its employees that they had been contacted by suspicious social media accounts claiming to be from the same company, it contacted Nisos to investigate.

INVESTIGATION

As a starting point, the client provided URLs for the offending accounts and confirmed that no employee by that name worked at their organization.

Nisos analysts utilized a combination of open-source intelligence (OSINT) tradecraft, internal and external tools, and data to investigate the suspicious accounts.

- Nisos found that the profiles were created recently. The threat actor almost certainly had two additional accounts on which the client was listed as a current or former employer.
- Investigators could not identify the person whose name matched the offending social media profiles, suggesting that they were personas created to interact with client employees and not accounts stolen from real people.

Nisos' investigation confirmed that the client had been targeted by an imposter, likely aiming to gain entry to their systems to steal data and intellectual property.

As a result of our work:

- Nisos identified additional accounts likely used by the same threat actor in a **similar attempt to infiltrate the organization.**
- Armed with an understanding of the TTPs of these threats, the **client continued to monitor for similar threats.**
- The **client alerted their employees** that they were being targeted on social media and **provided guidance on identifying fake accounts.**

Case Study

Artificial Intelligence

Assessing Supply Chain Risks

Nisos performs due diligence on the **hardware supply chain of a leading AI brand**

SITUATION

AI brands face significant supply chain risks when purchasing hardware from overseas. Assessing the dangers posed by third-party manufacturers is difficult.

When a leading AI company was considering contracting with a new hardware supplier based in China, it turned to Nisos to assess the ethical, cybersecurity, regulatory, and legal risks of working with the manufacturer.

INVESTIGATION

Nisos was tasked with performing a third-party due diligence investigation on the hardware manufacturer. As a starting point, the client provided Nisos with a framework to evaluate the risk potential of third parties on their behalf.

Nisos analysts utilized a combination of open-source intelligence (OSINT) tradecraft, internal and external tools, and data to investigate and evaluate the manufacturer's risks.

- Nisos found senior leadership at the overseas manufacturer had close personal ties to the Chinese government and the military.
- Analysts uncovered evidence that the manufacturer's products illegally collected attributable user personally identifiable information(PII) and sent it to servers in China for behavioral analysis.
- Nisos highlighted a history of alleged patent infringement by the manufacturer.

IMPACT

Nisos delivered a third-party due diligence report tailored to the client's needs and aligned with their standard framework for evaluating supply chain risks.

As a result of our work:

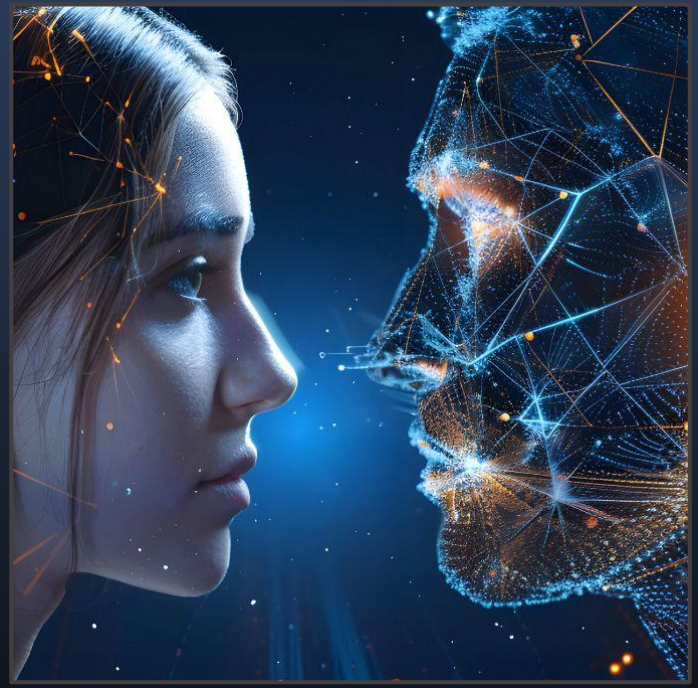
- The client thoroughly **understood the ethical, cyber, regulatory, reputational, and operational security risks** of working with the overseas supplier and used this intelligence as **a critical input to their supply chain partner selection decision.**

Safeguarding AI Innovation

As pioneers of innovation, AI organizations are constantly pushing the boundaries of what technology can achieve. Your success hinges on the ability to navigate a dynamic regulatory environment, avert platform misuse, maintain user trust, and bolster defenses against cyber attacks.

Nisos empowers leading AI organizations to continue their groundbreaking work while mitigating the risks associated with innovating in a highly competitive market. As an extension of your team, Nisos pierces the veil of anonymity to unmask threats and expose the ecosystem impacting your organization.

Our intelligence services enrich critical decision-making, enabling real-world consequences to effectively shut down threats and limit risk.



Let's **Connect**

Nisos is the Managed Intelligence Company. We are a trusted digital investigations partner specializing in unmasking threats to protect people, organizations, and their digital ecosystems in the commercial and public sectors. Our open source intelligence services help security, intelligence, legal, and trust and safety teams make critical decisions, impose real-world consequences, and increase adversary costs.

For more information, visit: https://www.nisos.com

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