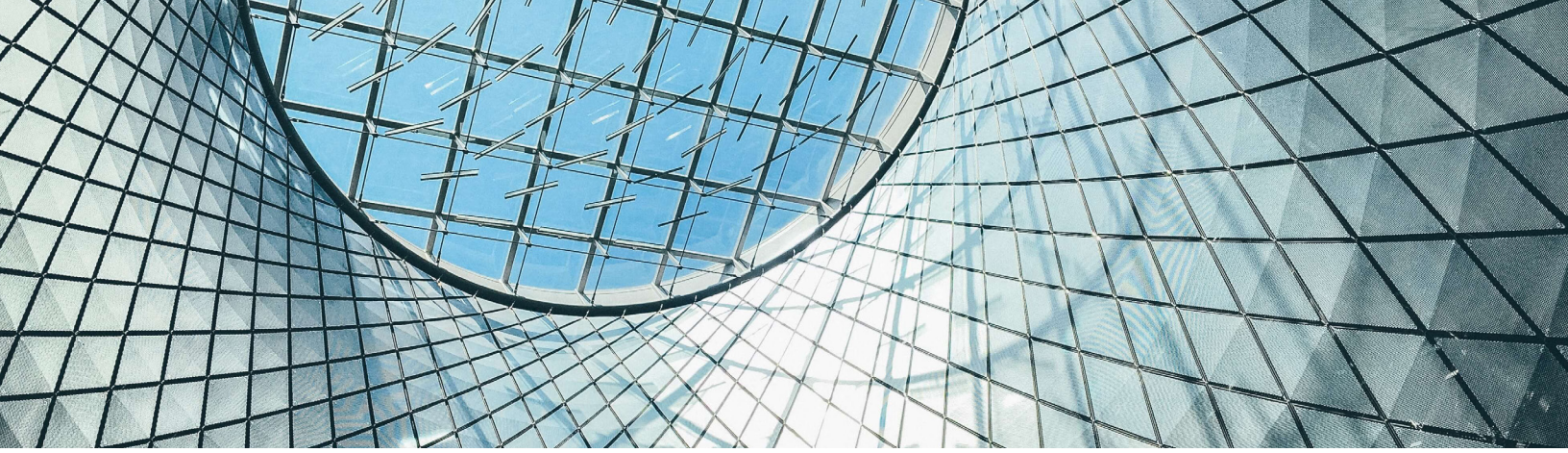

Market Insight Report Reprint

Coverage Initiation: Nisos combines breadth and depth to deliver managed intelligence services

August 24 2021

Aaron Sherrill

As the number of cybercrimes continues to rise, threat intelligence is becoming an increasingly critical component to building and maintaining a resilient security posture. Nisos is aiming to fill a growing gap in security operations, and to provide tailored contextual and actionable intelligence to mitigate significant risks across cybersecurity, disinformation, fraud and physical security.

451 Research

S&P Global
Market Intelligence

Introduction

As the number of cybercrimes, threats, breaches and sophisticated attacks continues to rise, threat intelligence is becoming an increasingly critical component to building and maintaining a resilient security posture. Having in-depth knowledge about existing, emerging and evolving hazards to an enterprise's IT ecosystem and assets can help organizations make informed decisions about threats and risks. However, having breadth and depth of intelligence to also counter disinformation, fraud, platform abuse and threats to key personnel and corporate reputation requires data and expertise that is often beyond the scope of most traditional cyber threat intelligence providers.

Seeking to establish its differentiated offering, Nisos is positioning itself as a custom alternative to traditional, generalized threat intelligence feeds. The company's managed intelligence services approach aims to fill a growing gap in security operations by fulfilling client-directed intelligence requests, and providing monitoring with expert analysis tailored to client-specific risks. Delivered at scale, this contextual and actionable intelligence is designed to mitigate significant risks across cybersecurity, disinformation, fraud and physical security.

THE 451 TAKE

An ongoing parade of high-profile attacks in recent months has underscored the extent to which organizations are demanding more actionable insight into malicious activity. Data from 451 Research's recent Voice of the Enterprise: Information Security, Workloads and Key Projects survey shows that 40% of respondents have implemented threat intelligence in their security operations, with another 36% either in the process of deploying threat intelligence or planning to do so within the next 24 months. Of those that have deployed threat intelligence, 24% plan to increase their spending on threat intelligence in the coming year.

Nisos is positioning its service offerings to capitalize on this growing market trend, primarily targeting organizations that have already invested in building enterprise intelligence programs. Its tailored managed intelligence approach stands in contrast to the 'speeds and feeds' focus of traditional cyber threat intelligence, aiming to provide actionable information that can help organizations drive critical decisions.

Context

Nisos was founded in 2015 by a group of former US special forces officers and cyber operators in the intelligence community. This group included current president Justin Zeefe, as well as Landon Winkelvoss and former CEO James Bourie. David Etue, former global head of managed security services at BlueVoyant, was appointed CEO in July 2020. To date, the company has raised $17m in funding, including a $6m round in January led by global cyber investor Paladin Capital Group, along with participation from existing investors Columbia Capital and Skylab Capital. The company indicated the investment will be leveraged to expand marketing and operations and extend its international footprint.

Headquartered in Alexandria, Virginia, Nisos offers managed intelligence services aimed at helping enterprises find, investigate, attribute, and expose adversaries that are targeting their organizations, personnel, vendors and platforms. LogMeIn, Mars and Uber Technologies are among the company's notable clients that span large internet platform providers, financial service providers, private equity firms, consumer brands, and technology and security companies.

Nisos believes that, despite vendor promises and significant spending, security and intelligence teams are saddled with an abundance of threat data, but possess little actual intelligence – leaving them ill-equipped to combat motivated and sophisticated adversaries. Turning data into client-specific intelligence requires expertise that is not present in many enterprises. Designed for mature and maturing corporate security and intelligence teams, Nisos says its platform approach to managed intelligence delivers a unique blend of skillsets and cross-functional expertise spanning cybersecurity, analytical, investigative and technical domains, providing the insights and finished intelligence needed to disrupt adversary operations.

Managed intelligence

According to Nisos, most security and intelligence teams think of intelligence services as noisy data feeds focused on indicators that often lack organizational context, and require additional analysis to determine relevance. Nisos agrees, stating that many intelligence products or feeds available in the market provide unfinished intelligence, only providing organizations with a generalized piece of the picture, and failing to deliver business-specific actionable outcomes.

Nisos' proprietary intelligence platform, coupled with its multifaceted collection of intelligence data spanning network and telephony, web and social, human, media, adversarial, breach and business domains, is the foundation to its portfolio of managed intelligence services.

The company's services, intended to meet a variety of use cases and security challenges, are composed of offerings that are designed to inform cybersecurity operations, disrupt fraud and attacks, attribute actions to actors, and improve cyber and physical defenses. Nisos covers six domains to help its clients manage risk: cyber threat intelligence, fraud intelligence, platform intelligence, protective intelligence, reputation intelligence, and third-party intelligence.

With its Adversary Insights custom response subscriptions, Nisos delivers rapid-response research to client-driven inquiries, providing insights into threat actor behaviors, methods, motivations and identity to help organizations prepare and defend against sophisticated attackers. Nisos Intel Team-as-a-Service, a threat monitoring and assessment subscription, delivers client-directed monitoring that combines automation with expert human analysis to provide actionable and customized intelligence based on threat actors and their associated activity covering OSINT (open source intelligence), attack surface and technical indicator monitoring.

The company also offers risk discovery and assessment for investments, IPOs, mergers and acquisitions through its Investment Zero Touch Diligence service. Nisos TPRM Zero Touch Diligence service offers similar capabilities, which include project and subscription-based assessment of nontraditional business risks, including external network vendor cyber hygiene for key supply chain partners and vendors.

Nisos Executive Shield tracks and identifies threat actors on social media, extremist forums and within the dark web that are targeting an organization's executives and key personnel, providing intelligence on threats, vulnerabilities and publicly accessible PII. The company also offers rapid response to security events that require immediate attention and expert analysis with its Event-Driven Intelligence Investigation services.

In addition to helping organizations better understand the methods and motives of attacks, Nisos says it provides specific and detailed attribution data on attackers, a key component to combating fraud, abuse and disinformation. The company also empowers reputation defense, helping enterprises fight slander and disinformation that could damage the organization's sales, stock price and trustworthiness.

Competition

The demand for threat intelligence has led to an increasingly crowded market space. However, threat intelligence varies vastly between providers, ranging from feeds based on generalized signatures and reputations to custom analysis of threats, actors, methods and motives customized to each organization.

Nisos' primary competition is from other firms with a focus on threat intelligence services, including Intel 471, Cyveillance (recently acquired by ZeroFOX from LookingGlass), Cybersixgill, Anomali, Group-IB, Cognyte, Flashpoint and Recorded Future. The company also squares off against a broad range of competitors that offer a variety of intelligence services as part of a larger portfolio of services. This group of competition includes firms like FireEye, Palo Alto, Cisco, IBM, ThreatQuotient, Secureworks, Rapid7, Webroot, Fortinet, Proofpoint, Kaspersky and Optiv. Consulting companies including Accenture, EY and Booze Allen Hamilton have also made investments in a variety of intelligence offerings.

SWOT Analysis

STRENGTHS

With its focus on client-specific, tailored, multisourced intelligence that delivers broad cross-functional expertise and insights, Nisos has carved out a distinctive position for itself as a managed intelligence provider.

WEAKNESSES

Nisos' capabilities and offerings should appeal to organizations with a threat intelligence function or strategy that ranges from maturing to mature. However, the advanced nature of the company's offering could limit its appeal to a broader field of prospects with no objective to have an advanced threat intelligence capability. Even so, this limitation is likely offset by the advantages and the tools it offers to organizations with the resources and investments to build robust intelligence capabilities.

OPPORTUNITIES

Expanding partnerships with consultants and security service providers, especially with managed detection and response and extended detection and response providers, could help broaden the company's market reach, and be a force multiplier in its customer expansion efforts.

THREATS

Threat intelligence is a highly crowded and competitive field, with many recognized names, including those that have combined with strategic security and IT vendors.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence