NISOS

A Buyers' Guide for CSOs

Elevating Your Corporate Security with Threat Intelligence

Introduction

As a CSO, you are responsible for directing all efforts concerned with the security of the organization, including overseeing the identification, assessment, and prioritization of risks. The organization is looking to you as a security problem solver to translate strategic goals into tactical objectives to secure the organization holistically. The job has never been bigger.

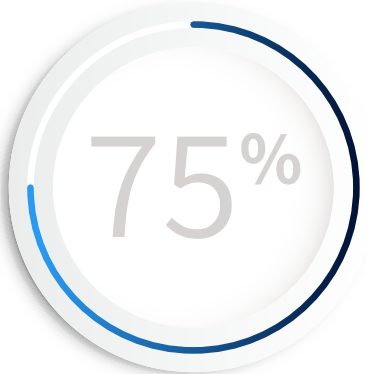
Your team must constantly evolve to address a multitude of risks to organizational continuity, including threats to people, property, and places.

Threat intelligence makes it possible to stay ahead of your organization's potential risks, accurately assess their probability and impact, and respond more quickly and effectively. Developing the threat intelligence needed to stay ahead of your ever-evolving threat landscape requires a combination of people, processes, and technology capable of delivering clear answers and recommending courses of action.

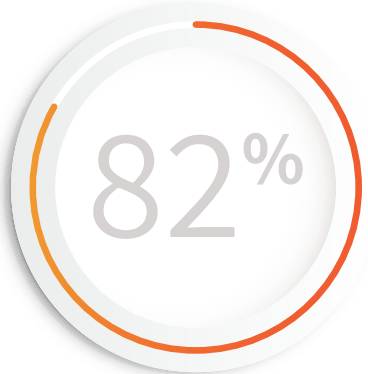
Actionable threat intelligence can help your organization be more proactive in securing personnel, as well as sensitive physical and digital assets, helping to inform decision-making and enable better use of scarce security resources. In this guide, we'll explore what it takes to build and mature an intelligence program to support corporate security for your enterprise.

State of Threat Intelligence According to Security Leaders[1]

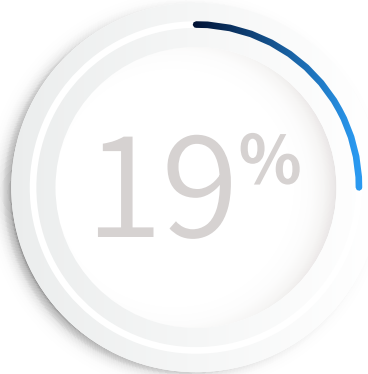
feel their organization needs to focus more on threat intelligence rather than just cybersecurity



admit struggling to stay ahead of an ever-changing threat landscape



feel their organization's approach to threat intelligence is too reactive



find it impossible to act on their intel at their organization

Convergence of Cyber and Physical Risk Challenges Cyber-first Security Approaches

While cyber risk constitutes a significant portion of your organization's threat landscape, it only makes up part of the broader threat environment. 56% of security leaders admit their organization doesn't have a full picture of all threats they face, with 77% percent expressing concern that new, interconnected risks are emerging faster than ever[2]. Today, 96% of security leaders feel cybersecurity and physical security must be integrated or else both cyber and physical threats will be missed.

According to the 2020 IBM Cost of a Data Breach Report, 10% of malicious data breaches can be traced to an initial physical security compromise.

Understanding the implications of a physical compromise on your cybersecurity posture, and conversely, the impact of a cyber breach on your physical security is critical to protecting the health of your organization:

- A cyber attack on your business could result in a physical security breach, such as theft or damage to equipment.
- A physical security breach, such as unauthorized access to your facilities, could result in a cyber attack if the perpetrator gains access to your computer systems or data

The convergence of cyber and physical risks means intelligence must support organizational privacy, safety, and trust, with as much rigor as cybersecurity goals of confidentiality, integrity, and availability.

What is Threat Intelligence?

"Intelligence is not a data feed, nor is it something that comes from a tool. Intelligence is actionable information that answers a key knowledge gap, pain point, or requirement of an organization. This collection, classification, and exploitation of knowledge about adversaries give defenders an upper hand and forces defenders to learn and evolve with each subsequent intrusion they face."

SANS Institute

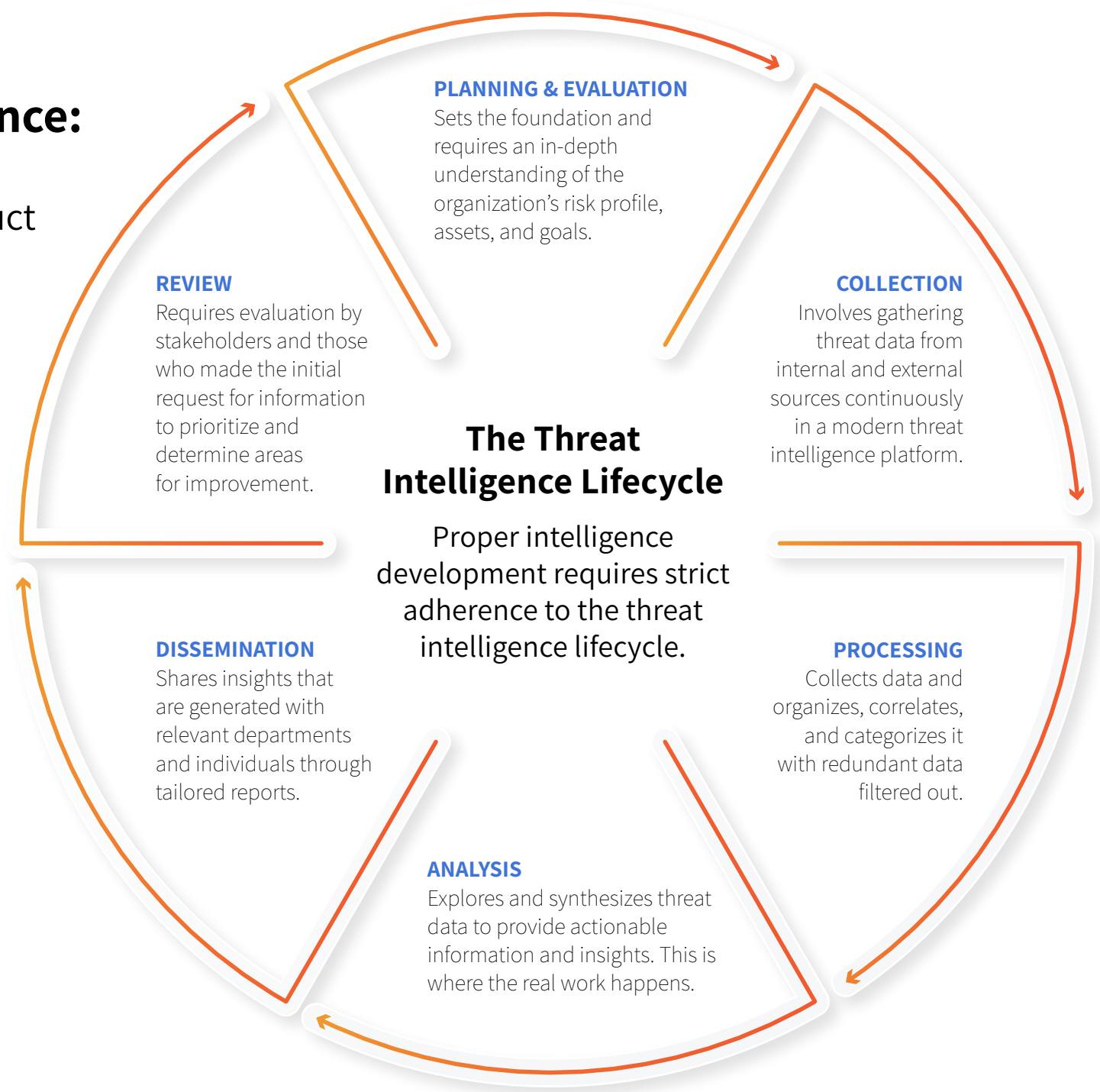
Threat intelligence is the process of developing knowledge and supporting data that can help prevent or respond to a specific threat. Developing threat intelligence involves collecting, correlating, processing, analyzing, and refining information about emerging risks to improve defenses, accelerate detection, guide response, and improve prioritization.

In your role as head of corporate security, you are responsible for identifying and managing all events that could threaten the organization's sustainability and continued existence, necessitating a holistic and proactive approach that takes into account the evolving threat landscape and the need for effective coordination among stakeholders.

Threat intelligence makes it possible to elevate your security program through:

- Proactive identification of emerging risks by monitoring and analyzing emerging threats and trends, so you can take pre-emptive action.
- Deeper assessment of risk probability and impact, so you can prioritize and allocate resources accordingly.
- Faster and more effective response to risk using real-time information.
- Risk trend and pattern identification to guide risk management strategies, so you can adjust accordingly.

Threat Intelligence:
A Process,
not a Product



How is Threat Intelligence Delivered?

The purpose of intelligence is to help inform a decision or action, but the market is saturated with products that inundate and confuse even experienced security teams with unspecific threat data that isn't always relevant to their environment. What these vendors call "threat intelligence" is mere "data" refined by proprietary artificial intelligence engines to make it more relevant.

Even with advanced intelligence platforms, threat data quickly becomes a wall of noise, leaving organizations overwhelmed by the amount of information they need to sift through to avert a crisis. Lack of organizational relevance is the top shortcoming of threat intelligence solutions, according to security leaders. [3]

What *doesn't* qualify as intelligence?

- A feed of broad or industry-focused threat indicators
- Anomaly detection or artificial intelligence
- Web, social media, or dark web scanning/scraping
- A visualization platform for all your telemetry

	Free/ Freemium Tools	Threat Intelligence Platform	Intelligence Reports	Managed Intelligence Services
	A host of free and freemium tools for social media monitoring, sentiment analysis, and news aggregation are available to support corporate security use cases.	Threat Intelligence Platforms consolidate threat data across different sources, apply a standard format, remove duplicates, and help with the validation and scoring of IoCs.	Narrative reports written on behalf of a client by a threat intelligence vendor that mirrors the outputs of intelligence operations in the public sector.	Managed Intelligence providers perform the entire intelligence lifecycle for you, from collection to production and dissemination, delivering regular reports, providing overwatch, and handling complex investigations.
PROS	■ Free/low cost	■ User-friendly ■ API availability ■ AI & Automation	■ Easy to consume ■ Topical and timely ■ Thought leadership	■ No noise - Hyper-relevant ■ Deliver finished intel ■ Partner with you
CONS	× Data, not intel × Noisy × No context	× Info, not intel × Limited dataset × Limited context	× Broad focus × Not actionable × Goal = Marketing	× No DIY

Building a Threat Intelligence Program for Corporate Security

Building and maturing an in-house threat intelligence function is a worthwhile endeavor but requires a significant investment. The goal of threat intelligence is to understand the motivations and methods threat actors are using so you can anticipate risks and provide guidance to security stakeholders. Unfortunately for most organizations, nearly a quarter of intel functions aren't created until after a crisis has occurred.

Security leaders responsible for physical security are the most likely to feel their organization's approach to threat intelligence is very reactive (89%).[4]

Top Responsibilities of Corporate Security Teams:

Physical Security	Protecting physical assets of the company, such as buildings, equipment, and inventory through access control measures, surveillance systems, and security guards.
Information Security	Defending the company's information assets, such as data and intellectual property. It involves implementing cybersecurity measures such as firewalls, encryption, and access controls.
Crisis Management	Preparing for and responding to crisis situations, such as natural disasters, cyber-attacks, and other security incidents by developing emergency response plans, conducting drills and exercises, and coordinating with other departments and external stakeholders.
Investigations	Investigating security incidents, such as theft, fraud, and cyber-attacks by collecting and analyzing evidence, interviewing witnesses, and working with law enforcement and legal counsel.

5 Challenges to Building a Threat Intelligence Program to Support Corporate Security

Rapidly Evolving Threats
From insider threats, protests, and harassment of your executives, to keeping pace with your rapidly evolving threat picture can feel like a marathon with no end in sight.

Staffing Shortages and Churn
Intelligence analysis requires hard-to-hire skills that fall outside the scope of traditional corporate security, including digital and cybersecurity. Finding the right expertise at the right salary is difficult, and keeping them on staff is even more challenging. Worse still, 54%[5] of security teams are already reaching burnout.

Budget Constraints
Fighting for the budget to get the tools, team, and training you need can feel like a never-ending cycle, and there never seems to be enough to invest in everything required.

Data Overload
A decade of digital transformation has made our environments more complex than ever. 59%[6] of corporate security leaders admit they are completely overwhelmed by their threat intelligence data

Executive Visibility and Support
30%[7] of security leaders now meet with the board of directors at least once a week. Executive leadership is more in-tune with security issues than ever. Maintaining a positive relationship with these stakeholders requires anticipating their concerns and having answers when they ask questions.

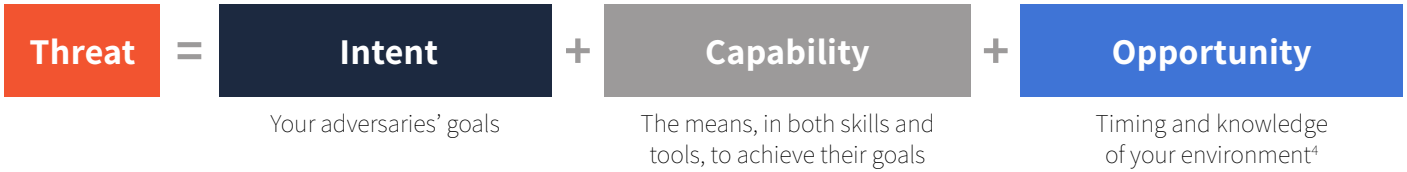
Scope and Document Your Intelligence Requirements

Overseeing an ecosystem of interconnected risks poses a significant challenge. The impact of an attack where sensitive information is stolen, for example, may increase the risk of identity theft or fraud for your personnel or customers. Security incidents also increasingly impact the organization's reputation, a critical indicator of success for every organization. Understanding the scope of the risks requires working with stakeholders throughout the organization.

The requirements of different departments and stakeholders — both internal and external — are likely to vary significantly, particularly in a larger organization. In some cases, these requirements may clash with one another for priority or even seem to be in direct opposition. It's important that you set clear expectations and outline the challenges. In the process, you'll be able to form a framework for how each risk, threat, and requirement should be prioritized and a means to establish a plan that meets the needs of stakeholders.

6 Questions you must answer in your initial planning include:

1. Who do we need to protect, and where?
2. What are our critical assets?
3. How do we maintain awareness of threats to our brand and reputation?
4. What laws, regulations, or compliance mandates are we subject to?
5. What is our risk tolerance and how do we prioritize?
6. What are your business's strategic objectives, and how do threat and risk management play into their fulfillment?



Consult with Key Stakeholders

Intelligence programs thrive when they are aligned with the actions a stakeholder could take based on the intelligence they receive. When your intelligence analysts understand the purpose of a request, and how a stakeholder intends to use the intelligence they provide, they have a better shot at finding the correct information and doing an analysis that will enable decisions and actions.

Executive Leadership and the Board	Executives and security-savvy boards are asking tougher questions that require information sourced through the intelligence process.
Information Technology	Threat intelligence can help IT security departments prioritize the adoption of appropriate controls throughout an organization. Keeping these teams abreast of changes in the threat picture ensures they can improve defenses before an issue arises.
Human Resources	Human Resources (HR) is charged with helping to manage the risks associated with employees and their activities. They play a critical role in ensuring the organization's policies and procedures are communicated and understood by everyone.
Finance	Your finance team ensures that your corporate security program is adequately resourced, aids in due diligence, and translates risks into financial forecasting.
Facilities	Facilities teams provide physical infrastructure to support security initiatives, including managing access control, maintaining secure environments, and taking point on emergency response procedures.
Legal	Your legal team is instrumental in ensuring your program's goals and initiatives are in compliance and that the organization is properly protected against the legal risks associated with security incidents.

Build Your Team

A top-notch threat intelligence team must have expertise in various disciplines to support the needs of the entire corporate security apparatus. Building the right team requires a mix of analysts able to set strategy and guide organizational leadership, analyze and bring context to external intel sources, and disseminate actionable intelligence to teams responsible for security design and monitoring, access control, emergency response, and investigations, as well as executive protection and travel security.

Once you know the skills required for your program, you need to determine which skills your organization already possesses and which ones are missing. From there, you can choose to hire new talent, provide cross-training, or opt instead for Managed Intelligence.

An effective team also considers the personalities of its members, ensuring a balance of risk-averse and risk-taking, as well as strategic and technical individuals. The ability to view risk from an adversarial perspective is also crucial to success. Sourcing expertise from outside the organization is an option, but increasingly difficult, as the number of unfilled security roles reached over 750,000 in the United States alone[9].

Organizational Challenges with Building Out Your Intelligence Program:

1. Security controls that are either too broad or too narrow in scope.

2. Ineffective and/or untested incident response plans.

3. Inaccurate attribution of attacks to threat actors.

4. A security team relegated to testing, auditing, and managing rudimentary security solutions.

5. Cyber incidents that may cause significantly more damage or be considerably more disruptive — sometimes both.

6. Slower response to user incidents and issues with existing systems/infrastructure.

This is not a simple problem to address. Between the ongoing technology talent shortage and the considerable cost of hiring, training, and retaining seasoned intelligence professionals, most businesses find themselves held back by budget and staffing issues. Threat intelligence thus becomes yet another item foisted onto an already-overloaded security team.

Select Your Intelligence Sources

Getting the coverage you need to ensure a holistic view of your organization's threats requires multiple, disparate threat sources. To build a successful intelligence function, you'll need to curate a list of data feeds that align with the goals of the program. 98% of security leaders report[10] significant shortcomings in the threat intelligence solutions available to them on the market. The lack of direct organizational relevance of most intelligence data is among the leading failures of current solutions.

Surface Web	Staying up-to-date on what's going on in your industry or region beats the news cycle and improves relationships with organizational leadership.
Social Media	The first signs of risk increasingly occur on social media as individuals share information and opinions which can provide insight into an impending problem, and details about adversaries to contextualize risk.
Deep Web Forums	Adversaries frequently offer their services, seek advice and assistance, and share best practices in forums that require a membership to access.
Dark Web	The dark web is where criminals increasingly set up shop and monetize their attacks. Keeping tabs on the dark web ensures your organization is protected against the latest tactics and techniques used by threat actors and helps defend against supply chain risk.
Closed Groups	Sophisticated threat actors avoid using semi-public forms for communications, instead preferring to communicate using restricted access messaging platforms like Telegram.

Establishing Your Threat Intelligence Workflow

Assess, Monitor, and Investigate

Risk Assessments and Diligence | Set the baseline

The foundation of a successful threat intelligence program starts with a comprehensive, repeatable evaluation of your organization's threat landscape. To get a clear picture of your key threats, vulnerabilities, and exposure, a thorough assessment should focus on the actors with the capability and intention to attack your organization. This will provide an intimate understanding of your organization by pinpointing critical assets and connecting them to specific threats and scenarios. This way, you can align your resources with the right risks and avoid wasting time and resources on low-priority threats.

Threat / Issue Monitoring | Monitor for changes and new threats

With a threat landscape assessment serving as a baseline, monitoring the surface, deep, and dark web ensures you have eyes on where threat actors set up shop, hang out, and master their craft. Establishing a monitoring capacity doesn't stop with tool selection. Developing and refining feeds, integrating them into your systems, and establishing the scope of monitoring takes time.

Investigations and Requests for Information | Investigate at any level or scope

Mature organizations understand that the more they learn, the more questions they have that require further investigation and analysis. Driven by Requests for Information (RFIs), investigations are arguably the most crucial process in the threat intelligence lifecycle as they allow a deeper look into specific threats or concerns and questions from key stakeholders.

Intelligence: A Natural Fit for Managed Services

Developing threat data into actionable intelligence takes time, skill, experience, as well as the right tools. Enterprise security teams spend the majority of their cycles dealing with raw data and reviewing pre-populated threat dashboards[11], which keep them from effectively and proactively investigating risks to their organization. Investigations, as a result, end up being shallow, as intel teams simply lack the time to properly evaluate and analyze each critical alert they receive.

While these threat data feeds and platforms provide value, they fail to meet the business's unique needs and deliver intelligence. 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.

Managed Intelligence providers fill a crucial gap by combining people, processes, and technology to deliver threat intelligence as a service.

What to Look for in a Managed Intelligence™ Provider

Threat intelligence is a critical element of any serious security strategy, but few security teams have the expertise or resources to tackle all the threats they face. Managed Intelligence providers fill a crucial gap by combining people, processes, and technology to deliver threat intelligence as a service.

A Managed Intelligence Provider allows organizations to offload resource-intensive threat intelligence tasks to an experienced partner provider.

7 Things Managed Intel Providers Should Do

1. Generate intelligence specific to your organization
2. Deliver analyst-led finished intelligence with access to the analysts
3. Utilize multi-source collection and analysis capabilities
4. Leverage multilingual data sources and analysis
5. Discover and understand the adversarial mindset (motivations and intended outcomes)
6. Attribute and unmask adversaries based on relevance and need
7. Provide intel advice and threat actor engagement guidance

Nisos: The Managed Intelligence Company™

For enterprise security teams with tight budgets, limited time, and expertise in short supply, Nisos fills a crucial gap by combining people, processes, and technology to deliver threat intelligence as a managed service. Nisos experts monitor, identify, analyze, and investigate risks to provide client-specific intelligence that is necessary to stop threats.

Unlimited Access, Unlimited Questions

The Nisos Managed Intelligence™ Suite allows you to offload complex threat intelligence efforts to an expert analyst team focused on your needs. Nisos analysts have the tools and experience to efficiently reveal critical open-source intelligence from the surface, deep, and dark web to identify threats in your security shadows.

Threat Landscape Assessment	Managed OSINT Monitoring	Adversary Insights® Investigations	Executive Shield Digital
Comprehensive assessment of risks to your people, assets, and locations	External threat monitoring, investigation, and critical threat alerting	Analyst expertise to identify and investigate risks and counter adversary threats	Digital risk assessment, monitoring, plus PII identification and removal

A Partner Focused on Your Intelligence Needs

Working as an extension of your team, Nisos provides intelligence focused on real-world threats specific to your organization. With Nisos as a partner, you can be confident in your ability to respond to advanced threats, even as your team evolves. You benefit from our broad experience and extensive toolset, so you'll always have the resources to fill knowledge gaps and address unique stakeholders' needs. Nisos analysts work with your team to respond to Requests for Information (RFIs) on your most pressing security concerns and support ongoing security operations with monitoring and alerts.

Reasons to Partner with Nisos for Corporate Threat Intelligence

1. **Unmatched Collection Capabilities**
   Using an integrated toolset of over 30 third-party and proprietary tools, Nisos collects and maintains a vast collection of content to query evidence of exposure and keep tabs on your threats.

2. **Team Pandion®**
   Pandion, our team of elite intelligence analysts, average 10+ years of US Intelligence Ops and Fortune 500 experience. They provide unmatched cross-functional expertise and insights into adversarial challenges.

3. **Extension of Your Team**
   With Nisos, you work with named technical operators and analysts who contextualize their findings. Engagement is scoped to your needs.

4. **Closed Forums**
   Using appropriate tradecraft and following legal guidance, Nisos is uniquely able to access closed cybercriminal forums, and connect with persons of interest, including threat actors, to obtain insights important to you.

5. **No Noise**
   Nisos doesn't provide a feed or stream of alerts you'll have to silence. We only alert you to issues you should address.

6. **Analyst Engagement and Client Success**
   Nisos experts are at the center of each engagement. As a Nisos client, you have access to a Lead Analyst and a Client Success Director who are focused on your ongoing intelligence needs.

7. **Right-Sized Reporting**
   Detailed reports with recommendations that include prioritized actions, next steps, and key considerations specific to each client.

8. **Immediately Useful Intelligence**
   Nisos delivers finished intelligence, not just a statement of facts. A report from Nisos provides real answers, to quickly understand the who, what, when, and how behind everything we uncover.

Sources:

1. Vanson Bourne
2. Accenture 2021 Global Risk Management Study
3. Vanson Bourne
4. Vanson Bourne 2022
5. Vanson Bourne 2022
6. Vanson Bourne 2022
7. https://www.ciisec.org/
8. ISA-Cybersecurity-Briefing.pdf
9. https://www.cyberseek.org/heatmap.html
10. Nisos and Vanson Bourne - The State of Threat Intelligence: Eliminating Noise and Creating Actionable Insight
11. Nisos and Vanson Bourne - The State of Threat Intelligence: Eliminating Noise and Creating Actionable Insight

Explore Nisos

Analyst-Led Threat Intelligence

Nisos is The Managed Intelligence Company™.

Our services enable security, intelligence, and trust & 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 cyberattacks, disinformation and abuse of digital platforms.

For more information visit www.nisos.com or email info@nisos.com