Mighty Guides

Sponsored by NISOS

Building a World-Class Threat Intelligence Operation

Table of Contents

NISOS

Nisos® Managed Intelligence Infrastructure
Visit nisos.com

ANALYST-LED

Nisos Experts | Team Pandion™

Pandion™ Monitoring and Analysis

Expert-first, curated, and triaged threat intelligence

Open Source Intelligence

A combination of intelligence domains curated to meet client-specific needs

Attack Surface

Outside-in intelligence to defend the client's digital perimeter and internal environment

Adversary Insights℠

Client-specific, credible, and accurate intelligence

RFI Subscription

A client-driven set of reports - from indicator research to deep threat analysis and attribution

Assessments

- Threat Landscape Assessment
- Zero Touch Diligence®

Threat Response

- Event-Driven Intel Investigation

Nisos Intelligence Platform

NISOS INTEL DOMAINS

Cyber

Intelligence analysis using outside the firewall telemetry to bring context to your network security.

Fraud

Gain insight and disrupt threat actors who illegally leverage corporate systems for monetary gain.

Platform

Stop abuse of your platform and the negative impact on customer experience and brand safety.

Protective

Identify, assess, and mitigate threats to your company's people, assets, and properties.

Reputation

Technical guidance for defending your reputation against threats, negative sentiment, disinformation, and slander.

Third Party

Adversary-centric intelligence to address cyber and non-traditional supply chain and investment risk.

OSINT **Intelligence Collection and Database** **Cyber**

The Threat Landscape Has Changed

Years ago, before the advent of smartphones and social media, threat management was relatively simple. Organizations had well-defined security perimeters that could be tightly controlled. Cybercrime was relatively nascent.

In the modern era, the perimeter has effectively dissolved. Cybercriminals are increasingly sophisticated and endless in number, with state sponsored threat actors and large illegal organizations among their ranks. In this climate, threat intelligence has never been more important.

Organizations now face an ever-evolving ecosystem of targeted threats that challenge their safety, security, and in some cases the viability of their business. The traditional threat intelligence approach of providing voluminous “data lakes” of generalized threat information is not effective in this environment.

Modern threat intelligence requires organization-specific insights. A clear understanding of which threats are active and most relevant to your unique landscape is essential to identifying and responding to material risks. This approach requires a new threat model—one which actively collects and analyzes threat intelligence across the entire ecosystem and results in the following:

- More relevant data
- Actionable threat insights
- More effective remediation efforts
- Maximized utilization of security and intelligence resources
- Empowered security and intelligence personnel

This eBook explores how the threat landscape has evolved and why this necessitates a new approach to threat intelligence. With an emphasis on the value of timely, relevant, actionable, and organization-specific insights, it explains the processes, technology, and skills required to keep pace.

Finally, it examines how the threat intelligence market has transitioned from collecting and distributing broad data sets to an emerging, analyst-led managed intelligence approach that exists as an alternative to, and resource for, in-house teams.

Chapter One

Threats and the Evolution of the Threat Intelligence Market

Today, much of the public conversation about threats in the private sector centers around cybersecurity and the prevention of cyberattacks against digital assets and data. Driven by public breaches and emerging compliance mandates, the focus on cybersecurity-only mitigation gives a false perception that threats are exclusively technical. The reality is that cyber threats and real-world threats are two sides of the same coin.

The attack against Colonial Pipeline, attributed to the Russia-based criminal gang known as DarkSide, snared the largest fuel pipeline in the United States with ransomware. The pipeline remained offline for six days, threatening shortages, causing panic buying, and driving up fuel costs. Despite the threat actors themselves claiming the attack was not politically motivated, the impact in the United States went far beyond the relatively small amount of ransom demanded. Attacks like that on Colonial Pipeline demonstrate that while the goals may appear purely financial, the motivations—and impact—are often more complex.

The traditional threat intelligence market emerged over a decade ago, growing out of a shared responsibility among the intelligence community, law enforcement, and the private sector. Since then, it has grown into a $12 billion market as business leaders have begun to recognize that threat intelligence is essential. Today, organizations understand that the right intelligence can help them better protect their reputation, assets, infrastructure, and personnel.

"The threat landscape has evolved significantly, particularly over the past two years. Risk-based intelligence that addresses client-specific requirements is more critical than ever. At the same time, the market faces a worldwide talent shortage making it increasingly difficult to hire and retain the necessary resources."

Thom VanHorn

VP of Marketing, Nisos

Unfortunately, we now face an entirely new problem. Because most vendors focus only on the cyber component of intelligence, the market is saturated with similar players that aggregate and recycle large, generic data sets, contributing no independent analysis or insight beyond what is performed by their AI and machine learning engines. Perhaps this was sufficient when the only area of risk a business needed to concern itself with was cyber, but the realities of the modern threat landscape require expanding the scope of threat intelligence programs.

Modern threat intelligence must address a broad set of domains, including many that are external to the organization such as dark web monitoring. Threat intelligence therefore can no longer focus solely on the confidentiality, integrity, and availability of data systems and networks. It must also encompass the broader threat environment, including geopolitical threats, disinformation, fraud, identity, physical security, trust and safety, and platform abuse.

The challenge is that generalized threat data and broad observations do very little to prepare a company for potential incidents or threats to their specific business. No two businesses are the same, and no two threat intelligence strategies should be identical, either.

In a world where the outcome of an incident can be the difference between a business's success and failure, a proactive approach to risk management is crucial. Forward-thinking organizations need to understand the "how," "why," and "who" behind potential threats. More importantly, they must be able to determine if a particular threat or vulnerability is material and requires remediation.

As has been established, addressing today's complex threat intelligence challenges requires scalable, customizable technology. It also requires expertise. Even the best analytics platform requires human intelligence to guide it—expert analysts to follow the data trail and put together the pieces.

"The majority of threat intelligence companies follow an editor-in-chief model. They gather a large amount of data that matters to a broad set of organizations, package it, and sell it. But none of that makes it effective in resolving the highly specific challenges of individual organizations."

David Etue

CEO, Nisos

The Evolution of the Threat Intelligence Market

The threat intelligence market has been defined by technology platform data feeds and the sale of data for integrations into internal tools such as SIEMs, TIPs, and ticketing systems. This is a flawed approach, built on generic data and threat models that do not address the specific threats targeting individual organizations. To offer value, aggregated data must be properly contextualized, its insights tailored to organization-specific problems. Because of this, we are seeing the threat intelligence market evolve to cover a set of products and services.

Product

Holistic, modular platforms tailored to the buyer. This tends to create information silos but can help deliver data at a low cost. Those platforms that do not simply aggregate generic data generally cover one or more of the following domains:

- **Cyber security**, aka cyber threat intelligence (security operations, third-party intelligence, vulnerability management, identity)
- **Physical security** (executive protection, Global Security Operations Center (GSOC) safety, brand reputation)
- **Trust and safety** aka platform abuse
- **Legal** (investigative)
- **Global investigations** and/or threat management
- **Fraud**

Services

The threat intelligence service market is evolving to provide tangible answers rather than just aggregated data. At a high level, this typically comes in four forms:

- **Monitoring**, which consists of:
  1) Open source Intelliggence (OSINT) based on social media, the dark web, and other publicly addressable data sources. Clients typically have to hire internal resources and pay for the product feeds.
  2) Attack surface intelligence, which focuses on more traditional network monitoring and cyber threats.
- **Analysis**, typically available as a managed service to contextualize the data gathered through monitoring and apply client-tailored insights in the process.
- A **request for information** (RFI) service that addresses client-specific requirements.
- **Routine dark web/OSINT** or external attack surface management monitoring services outsourced to experts and not sold as a product.

One-size-fits-all threat feeds fail to offer either customizability or expertise. Rather than approaching a business's threat landscape with precision, they simply generate noise. As one might expect, this rarely delivers a justifiable return on investment for enterprise security teams.

Drawing quality insights and actionable intelligence from threat data requires careful strategic planning. An organization must first identify its objectives. It must also develop a program focused on the intentional curation, correlation, analysis, and dissemination of threat data. Too often, businesses jump straight to collection and skip this essential planning phase. And because they don't have the right strategy in place, they fail to achieve meaningful results.

The Core Challenges of Threat Intelligence

"Data is cheap. Client-specific intelligence is much harder to produce but far more valuable."

Modern businesses face a number of significant challenges in the development of effective threat intelligence, including:

- Access to meaningful threat data
- Lack of expertise for evaluation and contextualization of threat intelligence
- Insufficient industry data due to lack of sources in the deep and dark web
- Tailoring intelligence to organizational pain points
- Dealing with the signal-to-noise ratio

"Scalable managed intelligence is essential to combating increasingly sophisticated threat actors, and threat insights don't exist in a single dataset. Expert analysis is needed to correlate and understand the implications of a business's threat posture—true intelligence comes from a tailored approach rather than recycled news or a one-size-fits-all strategy."

Robert Raines

VP of Engineering, Nisos

Key Points

- The threat intelligence sector is experiencing a period of intense evolution.
- Traditional threat models are no longer sufficient in a modern context.
- An effective approach to threat management requires the following:
  - A strategy for gathering the right data to achieve high-quality outcomes.
  - Multisource intelligence contextualized by expert analysis.
  - Relevant, client-specific insights.
  - Up-to-date intelligence that focuses on current, real threats instead of vague observations or generalized third-party feeds.
  - A scalable, repeatable delivery process.
  - Stakeholder engagement to drive business priorities.

Chapter Two

Intelligence Must be Timely, Relevant, Actionable, and Client-Specific

To manage the complicated flow of information that defines modern threat intelligence, businesses must ensure they have access to the right mix of skills, experience, and analytics expertise, and that these skills are augmented and enabled by the right tools and technology—particularly in terms of automation.

In most cases, security and intelligence teams lack finished intelligence, leaving them ill-prepared to combat the motivated, sophisticated adversaries targeting their organization. Information feeds from so-called threat intelligence organizations are of little help. This is because monitoring and alerts do not represent a complete approach to threat intelligence.

Although threat feeds often contain meaningful and relevant information, they frequently fail to define how that information actually applies to a specific scenario. Intelligence requires the timely application of analytics. Moreover, it demands context.

An organization must be capable of determining the relevance of collected threat data in order to extract any real value. Understanding which threats are active and how attacks may be carried out is essential to effective response and remediation. Businesses cannot afford to squander time and resources chasing hypotheticals with little to no impact.

"Enterprises have realized that a prevention-only strategy is no longer effective. Modern threats are largely driven by threat actors and in many cases have never been seen before. It's impossible to prevent something if you don't know what form it will take, which is precisely why understanding the threat actors, their motivations, and their technical signatures is critical."

Justin Zeefe

President and Co-Founder, Nisos

Unfortunately, given that even a small- to mid-sized organization may have to manage millions of data points, achieving this level of insight is often easier said than done.

Real-time curation of threat information is valuable in this regard. Once data has been collected, it must be correlated and reviewed quickly enough to pull out salient insights before they become stale. Then, once risks, threats, and vulnerabilities have been identified through those insights, each must be put under a lens to determine their relevance to the business and whether they exceed the business's risk tolerance.

Even if all this is accomplished, the result is a single snapshot of the organization's threat landscape. It must be continually refreshed and updated as the landscape shifts and actors modify their tactics and processes. And all the while, it must be reviewed and analyzed by skilled experts. Expert analysis is critical in connecting threats to technical signatures, to threat actors, to motivations, and to intended outcomes.

In the absence of that expertise, even the most powerful threat intelligence solution will likely fall short.

"Most threat intelligence organizations focus on platforms and feeds of generic threat information, but information is not intelligence. The key to positive outcomes lies in the correlation and deep investigation and analysis of client-specific data."

Julian Matossian

VP of Product Management, Nisos

Key Points

Organizations seeking to advance their threat intelligence and response with a third party must ask the following questions:

- What systems are in place to ensure that I will receive threat information in a timely way with the insights I require?
- What is my role in identifying risk, managing business continuity, and directing threat/incident investigations?
- How is the team enhancing data sets and other information about threat actors and the threatscape that affects my organization?
- Is the team looking at the tactics, techniques, and procedures with an adversarial mindset?
- How will my threat intelligence partner track how actors are adjusting their tactics, techniques, and procedures in response to company defenses?
- Can my partner identify the motivations and objectives of adversaries?
- How actionable is the data I receive?
- If a legal or civil action is required, to what extent can adversaries be identified and unmasked?

Achieving the full potential of threat intelligence requires more than software and strategy; it also demands data analysis by skilled experts.

Chapter Three

Experts Are the Foundation of Finished Intelligence

Effective threat intelligence requires deep expertise across several broad categories, including engineering, IT systems, regulatory compliance, physical security, trust and safety, business continuity, and cyber forensics. Hiring and nurturing personnel with the necessary skill sets is both costly and challenging. As a result, organizations that lack sophisticated operations teams must often take an incredibly basic "block and tackle" approach to information security.

This can result in numerous organization-wide problems, including the following:

- Security controls that are either too broad or too narrow in scope
- Ineffective and/or untested incident response plans
- Inaccurate attribution of attacks to threat actors
- A security team relegated to testing, auditing, and managing rudimentary security solutions
- Cyber incidents that cause significantly more damage or are considerably more disruptive—sometimes both
- Slower response to user incidents, and issues with existing systems/infrastructure

"Finished Intelligence is defined by the threat intelligence market as researching, analyzing, and disseminating threat data based on industry-specific concerns. This definition is outdated. For threat intelligence to have value today, it cannot simply be sector-specific, it needs to be organization-specific. And it must be credible and accurate."

Landon Winkelvoss

Co-Founder, Nisos

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 and cybersecurity 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.

Threat actors, meanwhile, can dedicate as much time as necessary to cracking a target's ecosystem.

Managed threat intelligence has emerged as a solution to this problem, providing businesses with access to actionable, meaningful threat data at a significantly lower cost. Instead of having to worry about attracting and retaining talent, an organization collaborates with an experienced third party that not only approaches threats from an adversarial mindset to provide insights on risk and remediation, but also monitors the business's assets and infrastructure, responds to requests for information, and tears down data silos.

Yet even the most seasoned threat intelligence team is ill-equipped for real-time management of an entire corporate or public sector ecosystem. The sheer volume of data that must be collected, orchestrated, and digested is simply beyond the capacity of the human mind. Threat experts must be equipped with the monitoring, management, and analytics tools needed to do their job. The key to success lies in enabling and enhancing the skills of expert analysts via technology.

"Threat intelligence is more than identifying known TTPs and associating them with known threat actors. Actionable intelligence requires the identification and correlation of new threats with the responsible threat actor, their technical signatures, their motivations, and their intended outcomes. Achieving that level of understanding requires an adversarial mindset, a broad range of tools, and a diverse set of investigative and analysis capabilities."

Johnny Calhoun

Chief Operating Officer, Nisos

Key Points

- Threat intelligence is deceptively complex and requires expertise across a range of categories and disciplines.
- Most organizations lack personnel with the necessary skill sets to manage threat intelligence internally.
- The absence of threat expertise means threat intelligence becomes another task for general security or IT, significantly degrading an organization's risk posture.
- An ongoing talent shortage only exacerbates issues with talent acquisition.
- Managed threat intelligence represents a compelling alternative, allowing businesses access to seasoned expertise at a fraction of what it would cost to develop internally.
- Threat experts require the right tools to reach their full potential.

Chapter Four

Data and Technology Empower Experts to Succeed

The job of a threat expert is to transform information into insights, to contextualize threat data in a way that not only makes sense but also addresses organization-specific needs and pain points. To accomplish this, they require access to a wide range of unique and tailored data sets.

They must then select relevant data, assess it, correlate it, and disseminate their findings in an organized and timely fashion. This is a daunting task without help from enabling technology and tools—perhaps an impossible one. In order for threat experts to successfully deliver finished intelligence to their clients, they require a toolkit with the following functionality:

- **Orchestration:** Gather data from relevant threat intelligence sources and then store it in a central repository in real time.
- **Attack Surface Monitoring:** Working from a complete map of an organization's combined internal and partner ecosystem, monitor for both external-facing risks such as shadow IT and external risks such as vulnerable services and unauthorized access.
- **OSINT Monitoring:** Monitor and collate both publicly available threat information and intelligence gathered from sources such as the dark web and closed forums.
- **Forensics:** Automate logging and reporting during critical incidents to streamline post-incident evaluation.

"True threat intelligence is the intersection of critical data with an analysis platform and humans analyzing and delivering information in a timely, relevant, and actionable way. To build a successful Intelligence source, an organization must first curate a list of data feeds by evaluating dozens of vendors and selecting those with the most relevant and timely data."

Robert Raines

VP of Engineering, Nisos

- **Analytics:** Categorize risks and threats based on predefined criteria, provide insights into a business's historical threat intelligence and risk profile, and apply performance metrics to remediation and incident response actions.
- **Reporting:** Disseminate credible and accurate reports to key stakeholders securely.

Artificial intelligence and machine learning can be—and frequently are—applied to all the above functions to streamline threat intelligence even further. This must be done judiciously. AI is by no means a replacement for human expertise. Those who claim otherwise are basing their belief on a fundamental misunderstanding of the technology. Artificial intelligence is at its best when supported by human intelligence, and vice versa. Each achieves something that the other cannot—digesting and analyzing massive data feeds for the former, identifying and understanding contextual information for the latter.

A machine, for instance, does not inherently understand what constitutes critical data. It can be taught that information from a particular source applies to a certain department within a business. But it cannot effectively respond to client-specific requests for information, nor can it readily adapt to scenarios for which there is no training data. And ultimately, without human guidance, it cannot refine collected information into actionable intelligence. Data and AI alone cannot connect threats with threat actors, motivations, and tactics. To achieve this, your organization needs to embrace analyst-led intelligence.

To put it another way, it's only through human intelligence that artificial intelligence and threat data truly provide value. Without human expertise, even the best threat intelligence solutions in the world will be of little help. And without the necessary enablement tools, experts cannot work to their full potential. But there's a third category to consider here, the glue that binds people and technology together: processes.

Key Functionality For An Intelligence Toolkit:

- Orchestration
- Attack Surface Monitoring
- OSINT Monitoring
- Forensics
- Analytics
- Reporting

Key Points

- Threat intelligence almost inevitably requires the management of an overwhelming volume of data.
- Even the most seasoned experts need access to enabling technology and tools if they're to be effective in their work.
- Required functionality includes data orchestration, internal and external monitoring, analytics, reporting, and logging.
- Artificial intelligence should be used to augment expertise; machines lack the capacity to replace human intelligence and analysis.
- Processes represent another cornerstone of threat intelligence and are what bring people and technology together.

Chapter Five

Process Makes Intelligence Scalable and Repeatable

Ultimately, threat intelligence is a collaborative pursuit. It requires multiple business units to come together and express their unique pain points, risks, and concerns. Particularly in larger organizations, this can present a considerable challenge.

Every business segment likely has its own processes and frameworks, its own standards, solutions, and data silos. Aligning all of these disparate elements behind a common initiative is a daunting prospect, to say the least.

The solution lies in standardization. By defining clear processes for threat intelligence, you greatly improve the quality of threat data collected and considerably reduce risk. More importantly, you ensure that your organization's approach to threat intelligence is both scalable and repeatable, characteristics that are critical in today's digital ecosystem.

"When planning your organization's threat intelligence program, it's crucial that you first establish the processes by which you'll evaluate data feeds; identify, analyze, and remediate risks; respond to incidents; disseminate information; and review the program."

Johnny Calhoun

Chief Operating Officer, Nisos

Throughout this eBook, we've touched on the various stages of the threat intelligence life cycle. It's important to understand each of those stages before discussing some of the more critical processes involved.

1. **Planning and Evaluation:** This phase lays the groundwork. It requires a thorough understanding of the organization's unique risk profile, assets, and strategic objectives. Many of the processes used to evaluate one's own organization at this stage will be revisited based on the assessment of vendors, partners, and new solutions.
2. **Collection:** Threat data is collected from both internal and external sources and consolidated. In a modern threat intelligence platform, this happens continuously.
3. **Processing:** Collected threat data is organized, correlated, and categorized. Redundant data is filtered out. This stage is typically highly automated, with the automation overseen by threat intelligence experts.
4. **Analysis:** This is where effective threat intelligence teams do the bulk of their work, examining and contextualizing threat data to provide actionable information and insights.
5. **Dissemination:** The insights generated in the analysis stage are sent to the relevant departments and individuals via tailored reports. Reports typically include advice and responsibilities for remediation, overlapping slightly with risk management. The report should quantify risk and may recommend avenues for further investigation. These reports must be focused, consumable, credible, and trustworthy. Reports must also be easy to understand and backed up by concrete data, something which is often the exception in threat intelligence rather than the rule.
6. **Review:** The stakeholders who received the threat intelligence in the previous stage and whoever made the initial request for information meet to document, discuss, and evaluate in an effort to determine where improvements might be made.

Stages of the Threat Intelligence Lifecycle:

- Planning and Evaluation
- Collection
- Processing
- Analysis
- Dissemination
- Review

A Process-Based Approach to Threat Intelligence

Mature organizations understand that the more they learn, the more that is unknown and requires further investigation and analysis. Arguably the most crucial process in the threat intelligence life cycle, and the one likeliest to be revisited, involves the management of RFIs, and answers the following questions:

- What intelligence is required?
- What questions need to be asked in order to collect the required intelligence?
- What data is needed to answer each question?
- Where does this data reside? Is it internal or external? Attack-surface focused or adversary focused?
- Who is responsible for collecting and evaluating this data?

In addition to RFIs, analysis and integration are also pivotal. Having the right data with the right analysts, equipping those analysts with the right tools, and defining appropriate success criteria and requirements are critical first steps. To that end, there must be standardized processes in place for the following use cases:

- Determining the value of a data feed as it pertains to your threat intelligence objectives
- Assessing threat intelligence vendors and service providers
- Testing, deploying, and integrating new software and systems
- Onboarding new vendors and/or threat analysts
- Defining strategic objectives and goals and determining progress towards those goals
- Applying threat intelligence to other departments and disciplines, such as risk management, cybersecurity, and governance, risk, and compliance (GRC)

The first step is to ask yourself the following questions:

- What intelligence is required?
- What questions need to be asked in order to collect the required intelligence?
- What data is needed to answer each question?
- Where does this data reside? Is it internal or external? Attack-surface focused or adversary focused?
- Who is responsible for collecting and evaluating this data?

Key Points

- The best way to address the complexity of threat intelligence is to break it into more manageable processes.
- The development of standardized, streamlined, and repeatable processes is crucial.
- Management and assessment of RFIs is one of the most important considerations for any threat intelligence program.
- Clear processes for analysis and integration of data feeds, vendors, and platforms are also a must.

Chapter Six

Putting It All Together: Tips for Building a World-Class Threat Intelligence Operation

We've established what goes into effective threat intelligence. We've covered the importance of strategic planning, identifying the right datasets, finding threat experts, and standardizing processes. Now, there's only one final question—how does one unify all of this into a cohesive whole?

The following best practices will help guide you as you work to establish your own threat intelligence program.

Understand Your Business Requirements

There are a number of questions you must answer in your initial planning, including the following:

- What are your core revenue drivers?
- What technologies are foundational to your business, and what processes drive those technologies?
- Has your organization been a target of intellectual property theft?
- What executives or key personnel may be targeted by reputational or physical attacks?

"Intelligence operations continually evolve. New questions and gaps in knowledge are identified, new datasets are incorporated, new tools are added, and processes are refined and improved. Effective intelligence programs are committed to continually learning, expanding, and becoming more effective."

Johnny Calhoun

Chief Operating Officer, Nisos

- What are your business's strategic objectives, and how does threat and risk management play into their fulfillment?
- Is your company vulnerable to misinformation or disinformation attacks?
- Is your business dependent on platforms that are subject to acts of fraud or abuse?
- Are there any legislative or regulatory restrictions you must consider?

Consult with Every Stakeholder

The requirements of different departments and stakeholders—both internal and external—are likely to vary significantly, particularly in a large organization. In some cases, these requirements may clash with one another in priority, or even seem to be in direct opposition. It's important that you set clear expectations and outline the challenges with regard to cybersecurity, incident response, reputational attacks, vulnerability management, fraud prevention, physical threats, and supply-chain risk.

In the process, you'll be able to form an idea of how each risk, threat, and requirement should be prioritized, and establish a plan that meets the needs of stakeholders.

Identify Skill Sets and Skill Gaps

An effective threat intelligence team requires deep expertise across a broad spectrum of disciplines. Once you've determined the skills necessary to fulfill the goals of your threat intelligence program, you must next identify what skills your organization has internally, and what skills it lacks. From there, your options include talent acquisition, cross-training, or managed intelligence.

Successful intelligence teams are also formed with consideration for the personalities of those involved, ensuring a mix of risk averse/risk-taking and strategic/technical individuals. The ability to view risk with an adversarial mindset is also critical to success.

Best Practices for Establishing Your Own Threat Intelligence Program:

- Understand Your Business Requirements
- Consult with Every Stakeholder
- Identify Skill Sets and Skill Gaps
- Buy or Build?
- Map Your Infrastructure and Break Down Silos
- Evaluate Your Data Options
- Avoid Common Mistakes

Buy or Build?

Choosing whether to purchase a threat intelligence solution or create your own in-house is largely a question of speed, expertise, and return on investment. Does your business have the capital and expertise to create its own unique, secure threat intelligence program, including expert operators, analysts, data feeds, and technology?

Or would it be better in the long term to seek out a tuned, tested, and tailored solution from a managed intelligence provider?

The answer to these questions largely depends on your business's threat landscape, the resources you have available to your program, and whether you have the capacity to staff and retain the necessary personnel.

Map Your Infrastructure and Break Down Silos

Effective threat intelligence is timely, relevant, actionable, and client-specific. It is also both credible and accurate. These characteristics are impossible to achieve if your business's ecosystem is laden with blind spots and siloed data.

Visibility, network monitoring, data orchestration, and tech enablement are all non-negotiable—and not solely from a threat intelligence standpoint. Governance, risk and compliance, business continuity, and cybersecurity initiatives all demand full visibility.

Evaluate Your Data Options

What datasets are necessary to meet your specific intelligence needs? Once you've answered this question, these datasets must be correlated, orchestrated, analyzed, and categorized then augmented with internal and external telemetry. Is one internally managed tool sufficient or is it beneficial to partner with a service provider that utilizes numerous tools across a range of intelligence domains?

Your business may have its own unique data categories, but the following are broadly applicable across all risks and threats:

- Business data
- Network and telephony data
- People and groups
- Web and social data

Avoid Common Mistakes

The most critical mistake that most businesses make with threat intelligence is a failure to plan ahead. They purchase security data feeds without understanding or even considering the business problem that needs to be solved. Other common blunders include the following:

- Not prioritizing the highest-impact risks and threats
- Failing to act on intelligence
- Not bothering to update, verify, and assess data feeds
- Not conducting regular threat assessments
- Assigning responsibility to people who lack the necessary skill sets

Key Points

When planning a threat intelligence program, consider the following:

- Know your needs and objectives.
- Take a collaborative approach.
- Determine how you'll address skill gaps.
- Decide upfront if you'll build or buy.
- Eliminate blind spots and data silos.
- Determine what datasets are required relative to your goals.
- Integrate threat intelligence with other security, compliance, and resilience initiatives.
- Plan ahead, validate, update, and most importantly, act.

In Closing

As an organization learns more about risk, it is inevitable that unknown elements will surface, and more questions will arise. Finding answers to those questions is often a complex process. Building an efficient, effective, and successful threat intelligence program is daunting, to say the least.

It's certainly something your business can take on if you're positive you have the necessary resources, people, and systems in place to support such an initiative. Otherwise, a seasoned managed intelligence provider may be your best option.

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 cyber attacks, physical threats to personnel or facilities, disinformation and reputational attacks and the abuse and fraud of digital platforms. For more information visit: www.nisos.com

Mighty Guides make you stronger. These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

Expert-Driven, Cross-Functional Research & Analysis

Analyst-Led Monitoring, Analysis and Investigation

Nisos enables cybersecurity, corporate security, and trust and safety teams with world-class intelligence capabilities tailored to meet their needs.

Fusing robust data collection and a deep understanding of the adversarial mindset we deliver smarter defense and more effective response. We address disinformation, fraud and abuse of digital platforms, reputational and physical attacks against key personal and facilities, and advanced cyber attacks.

Third Party Intelligence

Gain deep visibility into latent risks in your supply-chain or acquisition targets

Reputation Intelligence

Defend your brand and reputation from external threats and disinformation

Protective Intelligence

Identify, assess, and mitigate threats to your company's people, property, and assets

Cyber Intelligence

Reveal digital threats outside your network, unmask insiders, and threat hunt on the dark web

Platform Intelligence

Stop platform abuse that impacts your customer's experience and trust in your brand

Fraud Intelligence

Stop fraud leveraging corporate environments, services, and systems for monetary gain

Learn more about our service offerings at www.nisos.com