NISOS

A Buyer's Guide for CISOs

Elevating Your Cybersecurity with Threat Intelligence

Introduction

As a CISO, you are responsible for providing strategic guidance to align the organization's cybersecurity program and business objectives. The organization is looking to you as a trusted advisor and resident cybersecurity expert who can help address threats and anticipate risks.

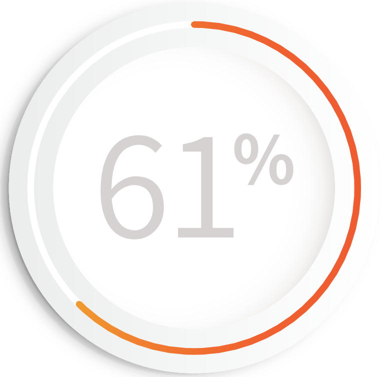
The job has never been bigger. Your environment must constantly evolve to keep pace with digital transformation, threat actors are more sophisticated and capable than ever, and the growth of the dark web has lowered the barrier to entry for cyber criminality.

Threat intelligence makes it possible to better understand your organization's unique threat ecosystem, with the goal of helping your team prevent and mitigate attacks more 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.

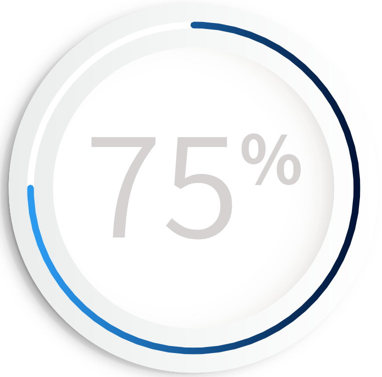
Actionable threat intelligence can help your organization be proactive in preventing breaches, inform decision-making, and enable better use of scarce security resources.

But threat intelligence isn't a product, it's a process. In this guide, we'll explore what it takes to build and mature a cyber threat intelligence program to support your enterprise.

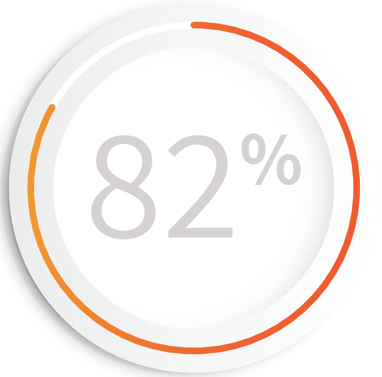
State of Threat Intelligence According to Security Leaders[1]



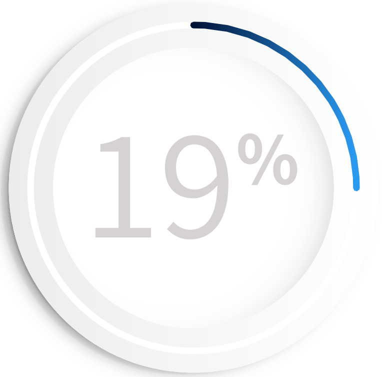
report difficulty deriving actionable insight from their threat data



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

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 threat actors in cyberspace to anticipate their intended target, motivation, behavior, and likely objective.

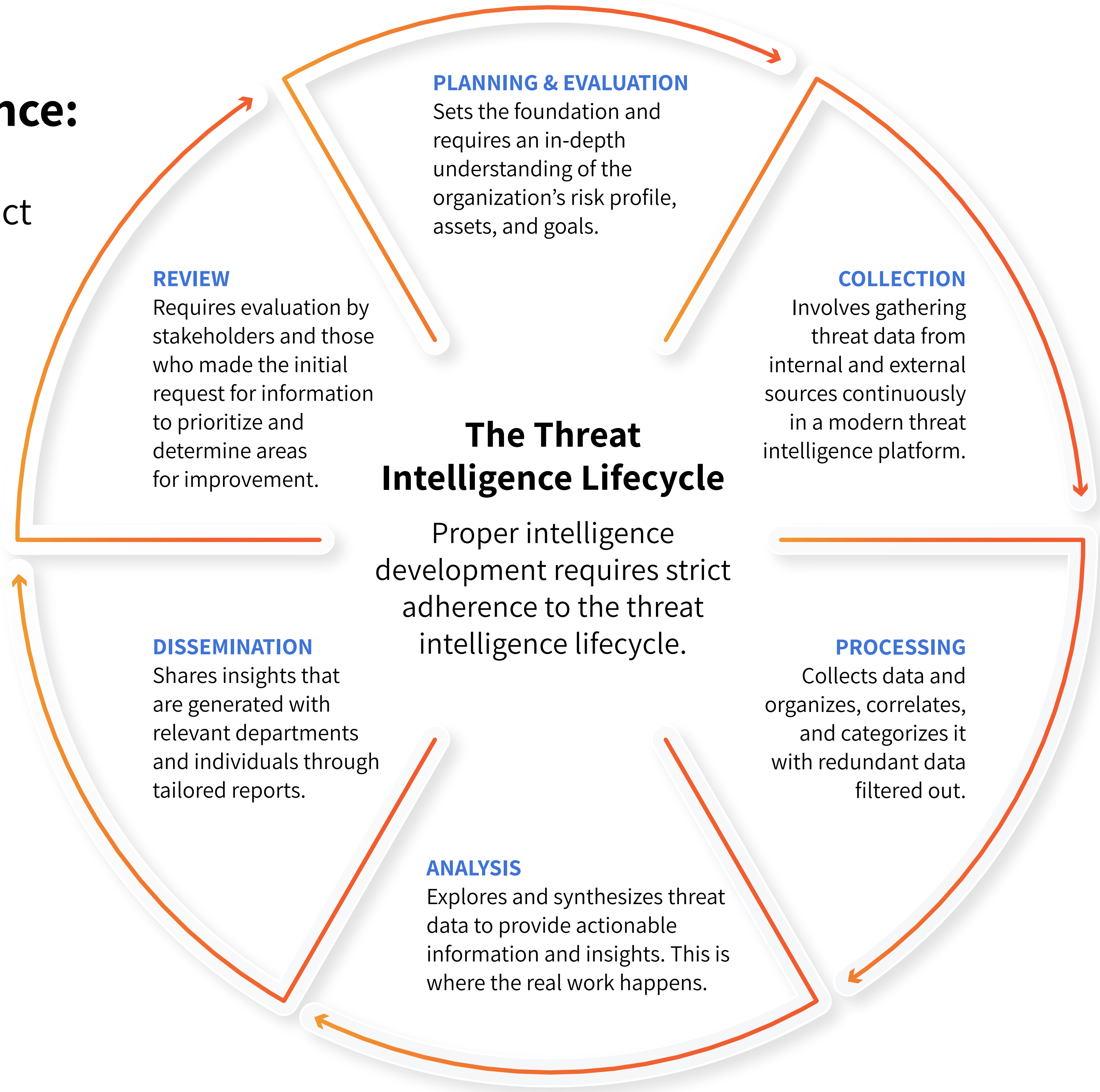
When the outcome of a single cybersecurity event can spell disaster for your organization, access to intelligence that enables a proactive approach to risks is imperative.

Your Threat Intelligence should help you answer:

1. Is there an active threat against my organization, our assets, or key personnel?
2. Who are the people or organizations targeting us?
3. What do those threat actors want?
4. Why do they want to attack us?
5. Which parts of our ecosystem are the most vulnerable?
6. How can we disrupt or mitigate risks based on what we know?
7. Who / what talent do we need to maintain our resilience against attacks?

Threat Intelligence:

A Process,
not a Product



The Threat Intelligence Lifecycle

Proper intelligence development requires strict adherence to the threat intelligence lifecycle.

PLANNING & EVALUATION
Sets the foundation and requires an in-depth understanding of the organization’s risk profile, assets, and goals.

COLLECTION
Involves gathering threat data from internal and external sources continuously in a modern threat intelligence platform.

PROCESSING
Collects data and organizes, correlates, and categorizes it with redundant data filtered out.

ANALYSIS
Explores and synthesizes threat data to provide actionable information and insights. This is where the real work happens.

DISSEMINATION
Shares insights that are generated with relevant departments and individuals through tailored reports.

REVIEW
Requires evaluation by stakeholders and those who made the initial request for information to prioritize and determine areas for improvement.

How is Threat Intelligence Delivered?

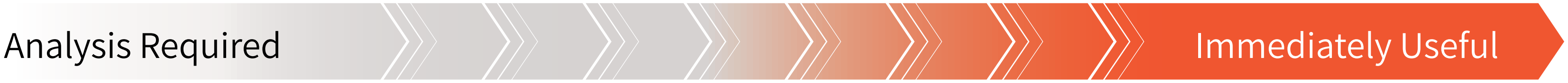
The purpose of intelligence is to help inform a decision or action, but the market is saturated with products that inundate and confuse even experienced security teams with unspecific threat data that isn't always relevant to their environment. What these cyber vendors call "threat intelligence" is mere "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. 61% of SOC staff members believe having too many tools is the primary cause of inefficiency for their team, demonstrating that too much tech can be encumbering.

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

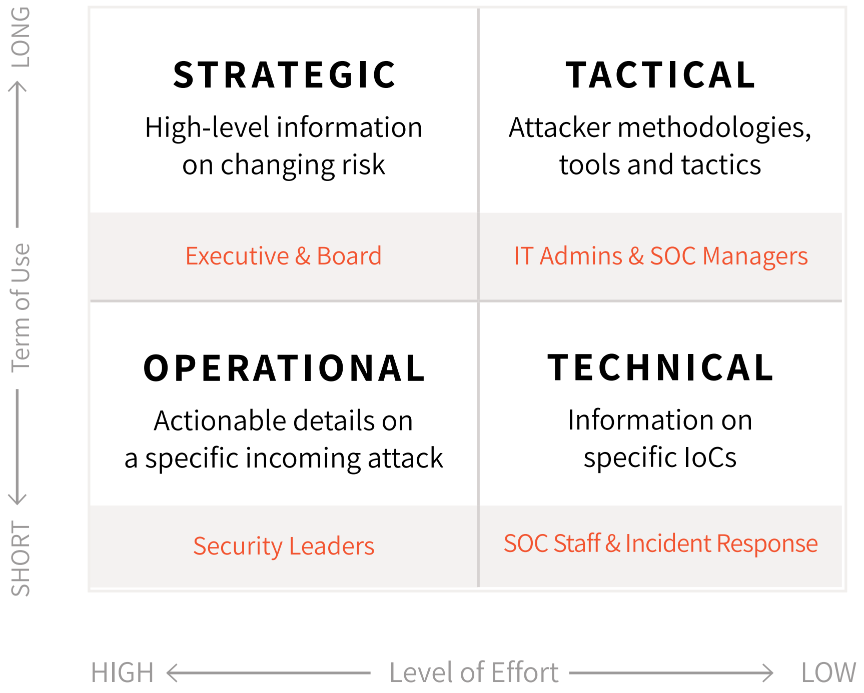
	Threat Feeds	Threat Intelligence Platform	Intelligence Reports	Managed Intelligence Services
	Threat Feeds provide a continuous stream of data related to specific threats, enabling automated information sharing for improved situational awareness, real-time network defense, and threat analysis.	Threat 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	■ Machine-readable ■ Easy to integrate ■ Fast delivery	■ 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	



Building a Threat Intelligence Program for Cybersecurity

Building and maturing an in-house cyber threat intelligence function is a worthwhile endeavor but requires a significant investment. The goal of threat intelligence is to achieve a knowledge advantage against threat actors targeting your organization, but nearly a quarter of intelligence functions are not created until after a crisis.

A well-resourced threat intelligence program makes it possible to break away from the reactive security posture imposed by technology-first threat intelligence products that dominate the CTI market and achieve a state of proactivity. Threat intelligence that provides not just a historical view of threat actors' activities but also provides clues about what they will do next is invaluable.



STRATEGIC High-level information on changing risk Executive & Board	**TACTICAL** Attacker methodologies, tools and tactics IT Admins & SOC Managers
OPERATIONAL Actionable details on a specific incoming attack Security Leaders	**TECHNICAL** Information on specific IoCs SOC Staff & Incident Response

Taking an outside-in view, these teams are able to bring context to their internal intelligence and achieve a more holistic view of the organization's risk. With this newfound proactivity, you can more effectively disrupt targeted attacks, identify breaches sooner, and reign in your organization's digital exposure.

The right cyber threat intelligence program can ensure your security team is focused on the most important threats to the organization, inform security prioritization, and quickly understand the who, what, when, how, and why of your organization's threat landscape.

5 Challenges to Building a Cyber Threat Intelligence Program

1. **Rapidly Evolving Threats**
   From ransomware and phishing to third-party exposure and configuration mistakes, keeping pace with your rapidly evolving threat picture can feel like a marathon with no end in sight.

2. **Staffing Shortages and Churn**
   Intelligence analysis requires hard-to-hire skills that fall outside the scope of traditional cybersecurity. Finding the right expertise at the right salary is difficult, and keeping them on staff is even more challenging.

3. **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.

4. **Supply Chain Sprawl**
   A decade of digital transformation has made our environments more complex than ever. It's no longer enough to focus solely on the security of your business, now you need visibility into your vendor's cyber hygiene to understand the full picture of your risk.

5. **Executive Visibility and Support**
   30% of security leaders[2] 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

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 with regard to cybersecurity, incident response, reputational attacks, vulnerability management, 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 a means to establish a plan that meets the needs of stakeholders.

5 Questions you must answer in your initial planning include:

1. What are your core revenue drivers?
2. What technologies are foundational to your business, and what processes drive those technologies?
3. Has your organization been a target of intellectual property theft?
4. Which executives or key personnel may be targeted by a cyber attack?
5. What are your business's strategic objectives, and how do threat and risk management play into their fulfillment?

Threat = **Intent** + **Capability** + **Opportunity**

Threat	=	Intent	+	Capability	+	Opportunity
		Your adversaries' goals		The means, in both skills and tools, to achieve their goals		Timing and knowledge of your environment[4]

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	Organizational leadership is more cyber aware than ever but still requires straightforward explanations of risk and impact. Executives and security-savvy boards are also asking tougher questions that require information sourced through the intelligence process.
Security Operations Centre (SOC)	The SOC ultimately holds the responsibility for processing threat intelligence and using it to add context to internal sources of data. Intelligence that can help the SOC reprioritize a threat avoids wasting cycles on false positives and frees up resources to handle real threats.
IT Security Management	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 get controls in place before an issue arises.
Vulnerability Management	Even security teams with sophisticated vulnerability management capabilities will benefit from threat intelligence. These teams often rely on public disclosures and updated feeds. Intel helps vulnerability teams prioritize according to the likelihood and potential impact of exploitation.
Investigation and Response	Understanding the intent and capability of threat actors allows responders to react appropriately in the event of a breach and mitigate its impact, giving insight into whether ransomware payment will result in the date being returned, for example.

Build Your Team

A top-notch threat intelligence team must have expertise in various disciplines. 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 manage technical intelligence as a liaison to the Security Operations Team.

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 cybersecurity roles reached over 750,000 in the United States alone[5].

Hiring and nurturing personnel with the necessary skill set is both costly and challenging. As a result, organizations that lack sophisticated operations teams must often take a basic 'block and tackle' approach to information security.

This can result in numerous organization-wide problems:

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 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.

Establishing Your Threat Intelligence Workflow

Assess, Monitor, and Investigate

Risk Assessments and Diligence | Set the baseline

The foundation of a successful cyber 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.

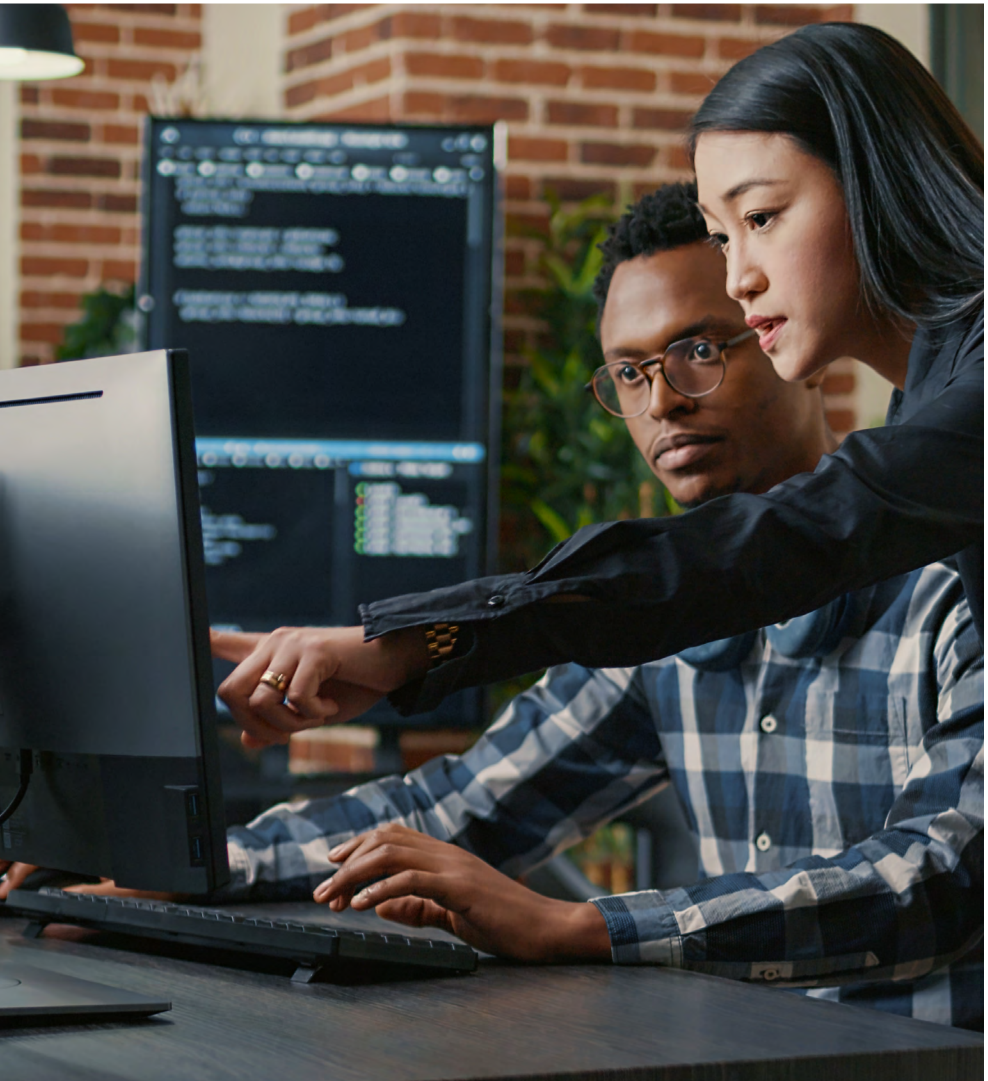
Select Your Intelligence Sources

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[6] 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 ubiquity of social media has made it a popular tool for threat actors who use it to select targets, recruit malicious insiders, and more.
Deep Web Forums	Cybercriminals frequently offer their services, seek advice and assistance, and share best practices in forums that require a membership to access.
Dark Web	Includes marketplaces and shops that are hosted on anonymity-focused networks such as Tor or I2P, which criminals use to purchase goods and services.
Code Repositories	Code repositories offer both a means to traffic in stolen intellectual property and share exploits among threat actors.
Paste Sites	Paste sites are public forums frequently used by hackers to anonymously share critical and sensitive information such as password files stolen during a breach.
Closed Groups	Sophisticated threat actors avoid using semi-public forms for communications, instead preferring to communicate using restricted access messaging platforms like Telegram.

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, 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 baseline assessment of your organization's threat profile	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 Cyber 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. 2021 Devo SOC Performance Report

3. https://www.ciisec.org

4. CISA-Cybersecurity-Briefing.pdf

5. https://www.cyberseek.org/heatmap.html

6. Nisos and Vanson Bourne

7. Nisos and Vanson Bourne

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