NISOS

A Practical Guide from Nisos®

Navigating Cyber Threat Intelligence in an Economic Downturn with Managed Intelligence™

In challenging economic environments, Managed Intelligence provides organizations with the ability to continue to harden their defense while containing costs and adding flexibility.

Executive Summary

In challenging economic times, all budgets get constrained. While cybersecurity has been more resilient, it hasn't escaped impact. Managed Service Providers (MSPs) have been crucial in supporting and filling operational and critical gaps during these times.

Managed Intelligence, a new sector of Managed Security Service Providers, is essential to bringing adequate security capabilities to in-house cyber and physical security teams - while providing the economic and organizational flexibility required to move forward and harden defenses during challenging economic environments.

Through customized on-going monitoring and analyst-led responses to Requests for Information (RFI taskers) - you can make your organization more robust and your operational teams more impactful.

Financial Discipline and Survival

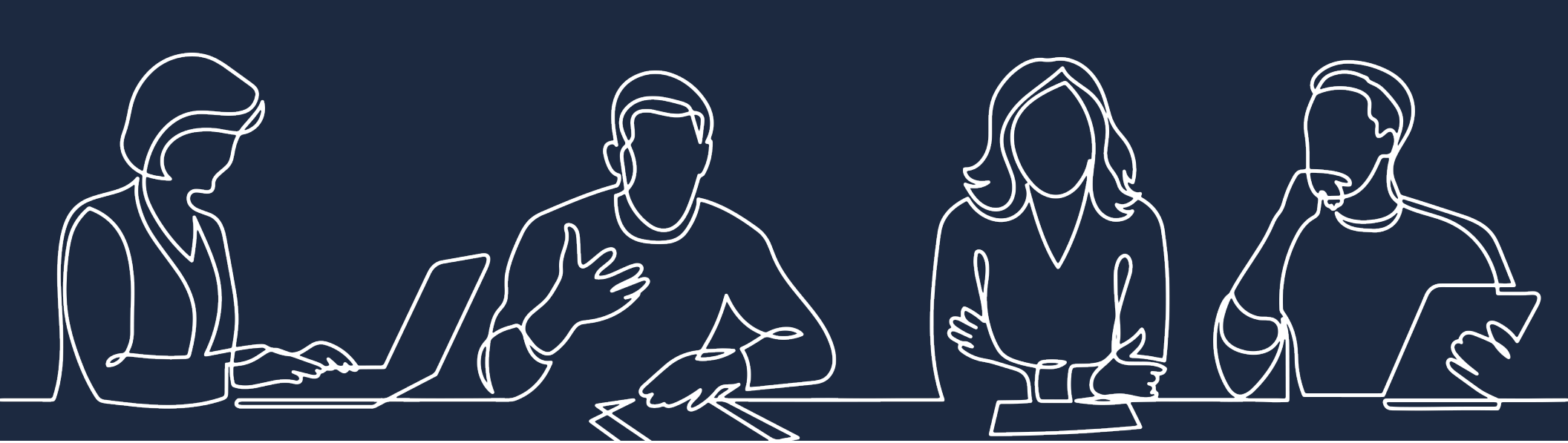
The Great Recession demonstrated the importance of financial discipline to help ensure businesses remained profitable and continued to grow - even when faced with economic uncertainty. Managed Services Providers (MSP) were vital to helping businesses stay on track.

When prosperity returned, the MSP's role evolved as their clients needed help accelerating digital transformation and combating escalating and increasingly sophisticated cyber threats.

Today's Security teams hunger for capabilities that can help avert a crisis. When it comes to threat intelligence, they are being poorly served by cyber threat feeds and platforms that require complex integrations and overwhelm analysts with too many alerts. This noise causes them to miss critical indicators of risk.

Organizations of all sizes, including large enterprises, are turning to managed intelligence services to help overcome gaps in internal skillsets, focus their efforts, and gain an outside-in view of their threat surface and risks by using world-class intelligence analysts.

In this guide, you will learn what's behind this trend, why it is successful, and when it's right to consider a managed intelligence partner.



Lessons from the Great Recession (2008-2010) through the 2010s

As the world enters a time of economic downturn and geopolitical turmoil, businesses are faced with difficult decisions. Costs are increasing, security teams are overwhelmed, and the threat landscape is more ominous than ever. The stakes are high. But this isn't new and we can learn from the past.

Driven by failures in the housing sector, the economy officially entered a recession in December 2007. Although modest at first, the rate of economic decline accelerated quickly in the Fall of 2008:

- U.S. gross domestic product fell by 4.3%, the biggest drop since WWII
- The unemployment rate more than doubled, from less than 5% to 10%

The recession lasted 18+ months, longer than any previous recession. For businesses, few were immune to the impact. Sales and profits declined for almost all industries and businesses had to make tough decisions to cut budgets and trim resources.

"If your neighbor gets laid off, it's a recession. If you get laid off, it's a depression."

Harry Truman

For over a decade, the private sector enjoyed unprecedented growth, thanks to rapid technological innovation and major societal shifts toward connectivity. The 2010s represent a transformational period in human and commercial history that saw internet connectivity become pervasive in the developed world.

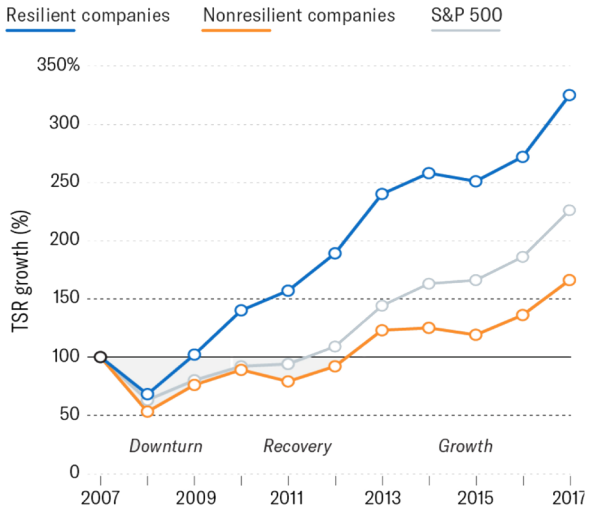
People's lives increasingly moved online. Social media adoption and influence increased, eCommerce began to dominate retail, streaming media became prevalent, and internet-enabled IoT devices delivered increased convenience. This transition to a connected world moved cybersecurity to the forefront.

"[The 2010s]...were the decade in which the last of our comfortable illusions of a free (libre), stable, and peaceful cyberspace were shattered…" according to Professor JD Work, the Bren Chair for Cyber Conflict and Security at Marine Corps University. [2]

Before the 2010s, cybersecurity responsibilities were almost exclusively the concern of the IT team. Short of a catastrophe, it rarely got a second thought from executive leadership, let alone the board of directors. That's because, before 2010, cyber-attacks were typically limited in scope and minor in impact. The 2010s changed all that.

After years of ignoring the warning signs, high-profile data breaches and complex cyber weapons became common. By the end of the decade, the world could no longer ignore the onslaught of breaches, ransomware, and digital fraud we all faced and finally began to recognize the broader impact of cybersecurity on public safety and confidence, as well as national and economic security. [3]

Now, cybersecurity is top of mind for the C-suite and is a common topic of discussion with the board as businesses strive to avoid becoming the next victim of a headline-grabbing breach.



Source: McKinsey HBR

According to McKinsey & Company, cost controls were not just key to survival; they propelled resilient organizations' growth out of the recession faster than their less disciplined peers.

At its lowest point in 2009, organizations that would weather the recession and accelerate subsequent growth had increased their EBITDA by 10%, while industry peers had lost nearly 15%. [1]

Recognizing Recession: Economic Turmoil is Here

While there is no universally accepted definition of a recession, after two consecutive quarters of negative gross domestic product (GDP), economies are generally considered to be in one. It is a dubious mark achieved by the United States in the first half of 2022.

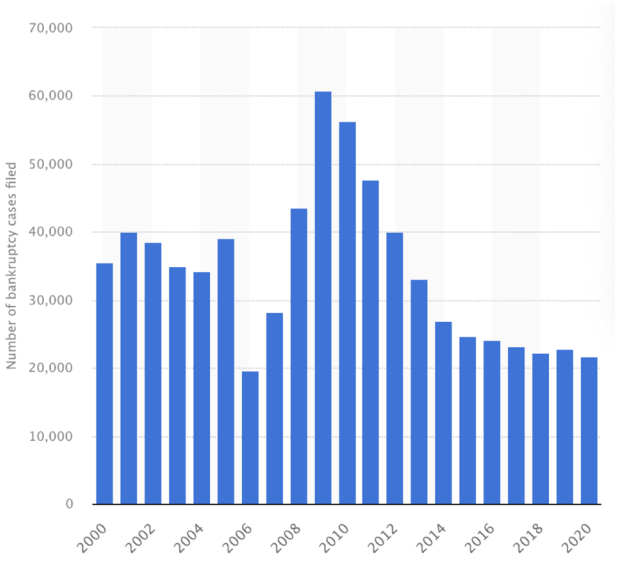
Costs are up dramatically with the Bureau of Labor Statistics reporting that the consumer price index (CPI) skyrocketed 9.1% yearly, a rise not seen in four decades.

Similarly, the Personal Consumption Expenditures (PCE) price index, was up over 5% and yields on 2-year U.S. Treasury notes jumped above the yields on 10-year Treasury notes resulting in the deepest yield curve inversion since 2007.

While there is some room for optimism (the U.S. economy is adding jobs and the unemployment rate is low), the bulk of economic indicators suggest business leaders would be wise to operate as if we are actively in recession.

Even blue-chip companies aren't immune to the economic downturn, although large companies tend to have more means to offset declining revenues and earnings.

To stay viable, companies have begun reducing hiring or imposing hiring freezes. Many will be forced to suspend pay increases and execute layoffs.



4

Studies have shown that large companies that effectively manage their costs without cutting headcount, while making long-term strategic investments, tend to outperform competitors once the downturn subsides.

Increasingly Turbulent Geopolitical Dynamics

Today, the United States and Western allies are witnessing a full-scale assault on national security, industrial, and economic base using the full spectrum of cyber, signals, and human intelligence tradecraft. Advanced Nation State adversaries are increasing cyber-attacks against the West through computer network exploitation (CNE) and active recruitment and/or compromise of insiders.

Adversaries targeting national security and economic institutions are leveraging a mixture of zero-day development, open-source and publicly available exploits, and a growing number of contractor or commercial entities. Inadequate security controls, poor configuration and patch management, and a fundamental misunderstanding of the threats and capabilities of our adversaries create a target-rich environment across all sectors of government and business.

As the geopolitical landscape heats up, nation-state actors are attacking more frequently. With the outbreak of war in Europe, thousands of threat actors have chosen sides. The result has been the most contentious cyber war the world has ever seen. Just three days after the invasion of Ukraine, Check Point Research (CPR) noted a 196% increase in cyber-attacks and a 4% increase in cyber-attacks per organization in Russia. [5]

Nation State Adversary Profiles

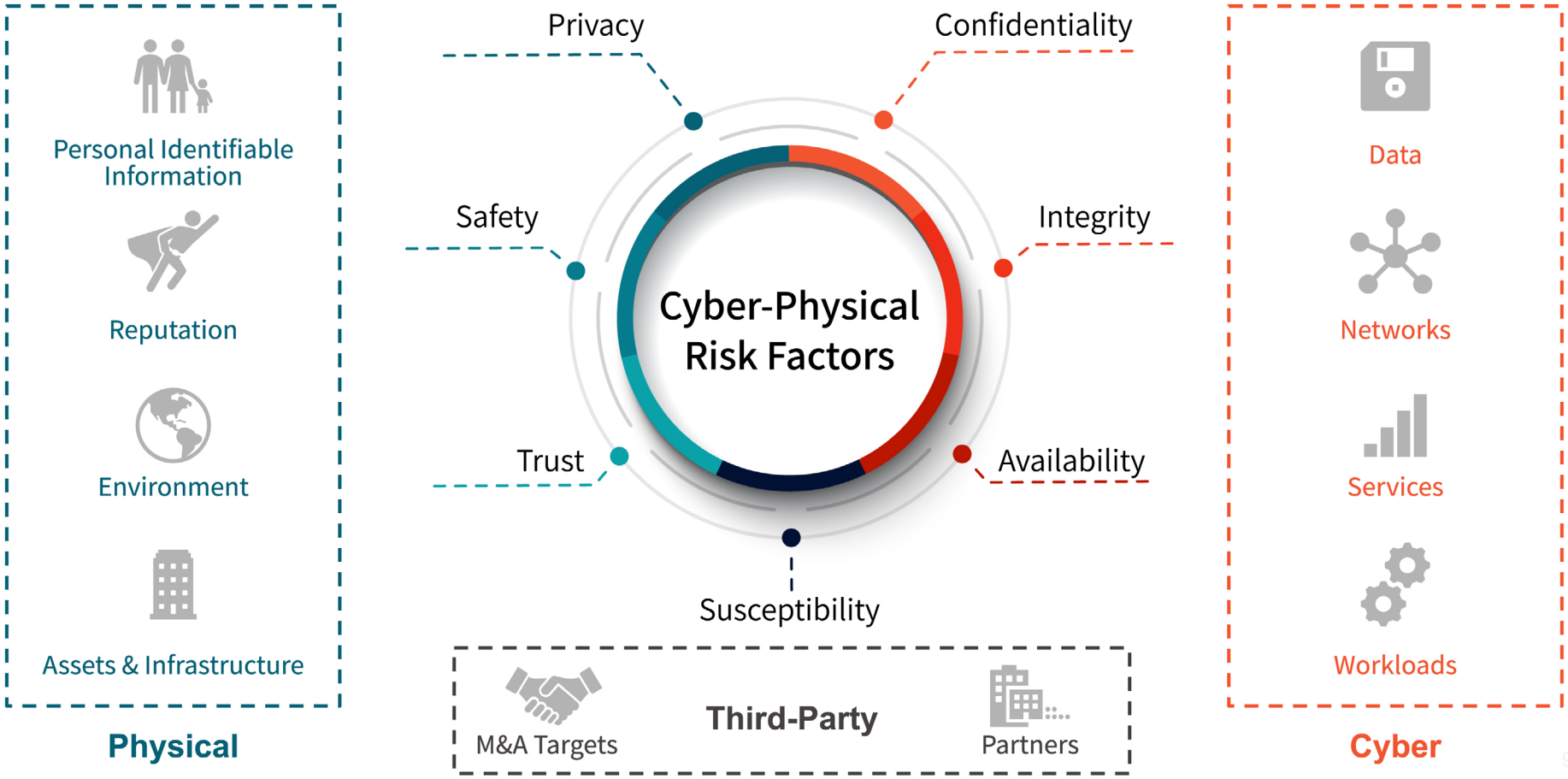
ADVERSARY	IMPACT	MODUS OPERANDI
Russia	**58% of cyber-attacks originate from Russia**	Russia demonstrates a high tolerance for collateral damage, an extensive ability to evade detection, and an impressive success rate thanks to adaptability and persistence. The attack of SolarWinds demonstrates a rare level of sophistication and capability, pushing backdoor malware to nearly 18,000 organizations. [6]
China	**8% of cyber-attacks originate from China**	China aggressively targets the U.S. political landscape, as well as those of countries in Latin America and Europe in sophisticated espionage campaigns. Targets in the U.S. included infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and more.
North Korea	**23% of cyber-attacks originate from North Korea**	North Korea shows a high level of activity relative to the country's size. The bulk of North Korea's cyber efforts center on espionage, as they seek diplomatic and geopolitical data from academia, think tanks, and diplomatic officials. During COVID-19 North Korea targeted pharmaceutical companies to steal vaccine research. They also operationalized cryptocurrency theft, targeting crypto and blockchain companies in spear-phishing campaigns.
Iran	**11% of cyber-attacks originate from Iran**	Iran's cyber focus of late has fallen on regional adversaries while mostly avoiding targets in the U.S. Iran deployed offensive cyber teams against Israel in the ongoing covert war between the countries. Iran has also escalated ransomware attacks with a series of campaigns that specifically target Israeli companies.

Escalation of Cyber-Physical Risks Factors

Today, enterprise security teams grapple with a multitude of physical threats that risk business continuity, including:

- Threats against the employees, C-suite, the board, or their families
- Threats against assets, infrastructure, and locations
- Threats against reputation
- Threats involving protests and disinformation

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, with the resulting breach costing an average of $4.36 million. This escalation is why 96% of security leaders feel cybersecurity and physical security must be integrated or else both cyber and physical threats will be missed. [7]



The Growing Importance of Threat Intelligence

Threat intelligence refers to knowledge and supporting data that can inform and assist someone in preventing or responding to a specific threat.

Threat intelligence is developed from data that is collected, correlated, processed, analyzed, and refined into an assessment of a threat actor's intended target, motivation, behavior, tactics, and likely objective.

The purpose of threat intelligence is to allow security practitioners to make informed decisions that are timely, relevant, and actionable, allowing them to protect their people and assets from dangerous threat actors.

Who Benefits from Threat Intelligence?

Any organization with sensitive or abundant digital assets will benefit from some form of threat intelligence.

Whether you are a small firm with limited resources or a large organization with vast data and a team of analysts to protect you, threat intelligence can help you defend your organization with greater accuracy, efficiency, and timeliness.

Threat intelligence is crucial because it can:

- Uncover unknowns to provide both cyber leaders and security teams with the intelligence needed to make the right decisions for the organization's safety.
- Reveal an attacker's identity, motivations, tactics, techniques, and procedures (TTPs), allowing you to understand what is going on behind the scenes in an attacker's decision-making process.

Threat intelligence will help you stay current on the latest threat actors, their methods, and targets. It will also help you to proactively address issues within your threat landscape and provide visibility to your leadership and stakeholders.

Understanding the current threats and the devastating impact that they could have on your organization is essential to proper preparedness and mitigating risks.

Seven Key Questions Intelligence Helps Answer:

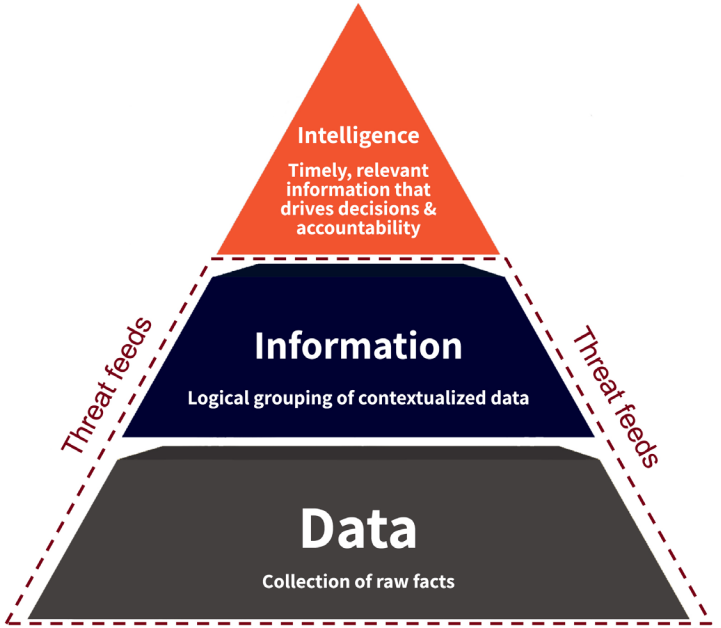
1. Is there an active threat against my organization or key personnel?
2. Who are the people or organizations targeting us?
3. What do those threat actors want?
4. Why do they want to attack us?
5. Which parts of our ecosystem are the most vulnerable?
6. How can we disrupt or mitigate risks based on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

Enterprises Need Threat Intelligence, Not Threat Data

Unfortunately, cyber threat “intelligence” (CTI) vendors have hijacked the meaning of threat intelligence, creating confusion about its real value. The CTI market, estimated to be in excess of $10 Billion, consists primarily of vendor offerings built on the idea of collecting the broadest data lakes and using AI and machine-learning to detect known threats.

What these cyber vendors call “threat intelligence” is really “data” refined by proprietary artificial intelligence engines in an attempt to make it more relevant. Proper finished intelligence must be defined as being timely, relevant, and actionable. In order to be useful, it must also be client-specific.

Developing finished intelligence requires rigid adherence to the predefined collection, processing, exploitation, and dissemination threat lifecycle and analysis by experts with an adversarial mindset.



The Difference Between Threat Intelligence and Threat Data

INTELLIGENCE

- Organization-specific, refined and correlated data points
- Triaged and actionable insights, organized for clarity and dissemination
- Timely, accurate, credible, multi-source
- Analyst-led, platform supported

DATA

- 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

True Threat Intelligence Isn't Just:

- A feed of broad, generic, 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

Security leaders are painfully aware of this fact with 53% stating the intelligence they receive from their CTI solutions is not specific enough or relevant to their organization.

Maximizing the Value of Intelligence

The information provided by threat intelligence should allow security practitioners to make timely and informed decisions to protect their people and assets. Unfortunately, 82% [8] of security leaders feel their threat intelligence is too reactive, leaving teams to respond to breaches after the event instead of before the attack. Organizations don't want to respond to attacks, they want to prevent them.

The Value of OSINT is in the Analysis

Maximizing the value of open-source information and refining it into actionable intelligence requires a rare combination of skills and experience across a wide array of intelligence domains, including HUMINT, SIGINT, GEOINT, IMINT, and FININT. For example:

- Geospatial (GEOINT) and imagery (IMINT) intelligence experts can establish a pattern of life from photos posted on social media.
- Online scams on social platforms often point victims to crypto wallet addresses. Financial intelligence (FININT) experts can track transactions to and from the address.
- Human (HUMINT) intelligence skills are now leveraged in cyber space, allowing for direct threat actor engagement, report building, and infiltration of closed forms.
- Signals intelligence (SIGINT) expertise is no longer required to track active flights, as flight data, including aircraft registration, position, altitude, and velocity, are now widely available online.

About Threat Actor Attribution

Attribution is the process of identifying the entity responsible for an incident.

While many victims simply want the actor out so they can continue to focus on normal operations, more mature security teams have a critical need to understand if an attack was targeted versus opportunistic.

Threat Analysts apply their knowledge of geopolitical context and the tactics, techniques, and procedures (TTPs) common to attackers to sift through relevant actors' actions, attributes, and infrastructure.

Three Key Challenges for Intelligence Teams

Even during prospering economies, enterprises are faced with challenges building threat intelligence programs. The financial constraints imposed by the current economic downturn have only served to increase those challenges, which can be grouped into three categories: People, Technology, and Processes.

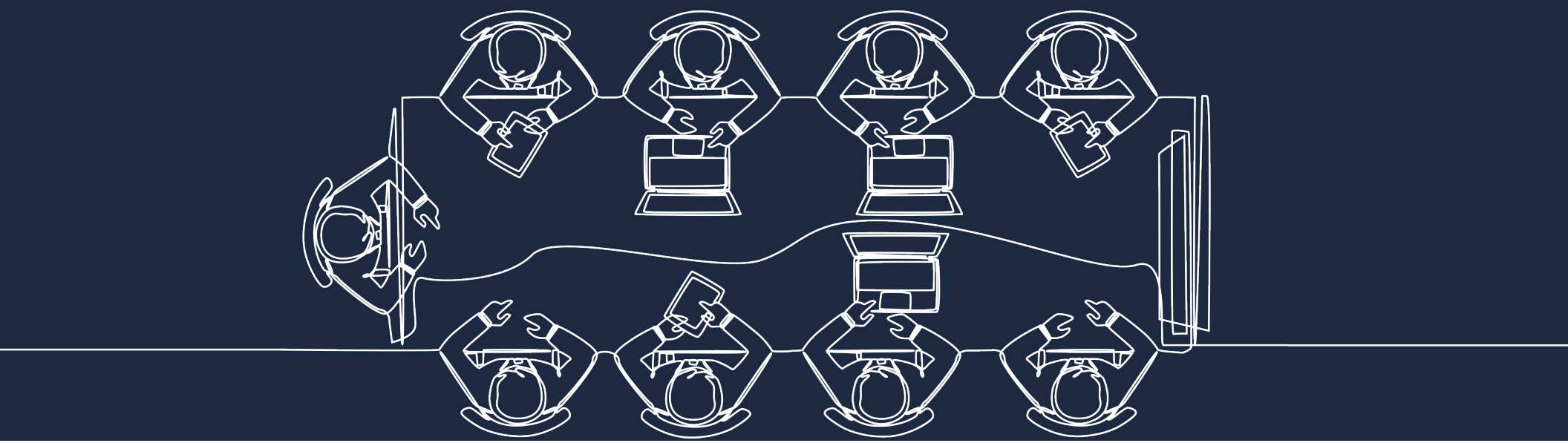
CHALLENGE #1: PEOPLE

Cyber intelligence experts are challenging to recruit, develop and retain in most environments. Workforce challenges are exceptionally high and have been getting increasingly worse due to the widely-publicized shortage of cybersecurity talent available on the market today. High demand with limited supply drives up wages, and makes it challenging to recruit and retain talent across a limited talent pool.

Cyber intelligence talent can be even more challenging. Not only do you have to illustrate core cybersecurity principles, you also have to have expertise in the intelligence cycle to be able to analyze and create finished intelligence.

Additionally, very few organizations can achieve a team size where someone can grow their career in intelligence. In a small team, there are only a few intelligence roles, sometimes even one. You have to hire generalists in these roles as they could need to support cybersecurity incident response to a network intrusion to threats to executives in social media to credentials for sale on the dark web.

This context switching makes it challenging to achieve expert level competencies. As they develop in their career, without a broad intelligence function, their career choice becomes to take on responsibilities beyond cyber intelligence, or changes companies to a larger or more specialized role. And many large financial institutions, technology platforms and ecommerce companies actively recruit from less mature organizations as training grounds to identify talent.



CHALLENGE #2: TECHNOLOGY

There is an adage in intelligence that if you don't collect it, you can't analyze it. Beyond the expertise to know what data you need to support your intelligence requirements, intelligence collection, storage, processing and analysis require significant investment in technology and integration.

The first place organizations typically leverage cyber threat intelligence is in cybersecurity operations use cases, and even their security tech indicators without actionable intelligence leaves teams exposed, as you are only able to see what your telemetry shows you. 61% of SOC staff members believe having too many tools, and the inability to effectively analyze their results and take action, is the primary cause of inefficiency for their team.

There is a massive number of options for cyber threat intelligence data - from platforms to data feeds to sharing organizations - and also, significant differences in quality across them. Knowing where to invest limited budgets is difficult. Even for more mature teams this can be a challenge because there may be key data sources that you may only use a few times a year that could be critical to a particular intelligence tasking, but impossible to justify due to their limited use.

CHALLENGE #3: PROCESSES

As mentioned above in People, the intelligence cycle is the widely accepted process for turning data into timely, actionable, and relevant intelligence. While the process is well defined, bringing it to life requires processes and discipline.

Planning, collection, processing, analysis, and dissemination are supported by unique process needs, and many of those sub-processes change based on the risk being addressed or the organization's collection capabilities. Without defined standard operating procedures (SOPs), you risk unpredictable results. And keeping processes current and the team skilled to deliver them requires constant attention, learning, and improvement.

To properly defend and proactively mitigate risks, you need a team that understands and stays current with the intelligence lifecycle and domain expertise that addresses the organization's risk. From cyber, to fraud, to trust and safety, to physical protection for key people, places, and assets - you must find a way to detect and respond to threats.

These multiple domains of expertise require multiple individuals with deeper, honed, and experienced backgrounds to know which data sources to collect, how to curate them, process and convert into finished intelligence. This isn't simply an analyst's ability to detect and respond. It's a seasoned threat intelligence team, with diverse backgrounds, working collaboratively within a defined process to extract the most relevant insights, and produce impactful intelligence.

You can see the gaps in processes today. 35% of security leaders say wasting time and money on the wrong threats is among their biggest intelligence challenges.

Managed Services

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 prepopulated threat dashboards,[9] which keep them from effectively and proactively investigating risks to the business. Investigations, as a result, end up being shallow or non-existent, as intel teams simply lack the time to properly review and investigate every critical alert they receive.

While threat data feeds and platforms provide value, they fail to address the business's unique needs and deliver actionable intelligence. Many intelligence products or feeds available in the market provide unfinished intelligence, only providing organizations with a generalized piece of the puzzle and failing to deliver business-specific actionable outcomes.

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.

Seven 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
7. Provide Intel Advice and Threat Actor Engagement Guidance

The Rise of Managed Services

With so much financial pressure falling on business leaders, cutting costs can be necessary for survival. But being understaffed and ignoring key business operations is not an option.

As they say, “you can’t cut your way to growth” - and with so much of companies’ security and intelligence dependent on expensive technology and resources, leaders know they must evaluate alternatives that give them flexibility while continuing to advance their operations.

For many years, companies have needed help supporting infrastructure while simultaneously modernizing for the future. Managed Services Providers fill that need by providing technology, IT expertise, and resources as a pay-as-you-go subscription service.

Not only can businesses upgrade and expand technology and tools, but they can also reduce or eliminate upfront costs and capital expenditures (CAPEX) in exchange for committing to a subscription contract with their MSP partner. Unsurprisingly, managed services adoption grew ~60% faster from 2008-2010 than in years prior.

Surviving the Crisis

Geopolitical conflict and economic turbulence are interconnected. Businesses of all sizes must make pragmatic decisions to survive, requiring a careful balance of economic considerations, growth plans, security needs, and workforce management.

History has shown that organizations that exercise financial discipline and cost control during times of crisis are more likely to weather the storm and recover faster than the competition.

Options to Consider to Weather Economic Instability

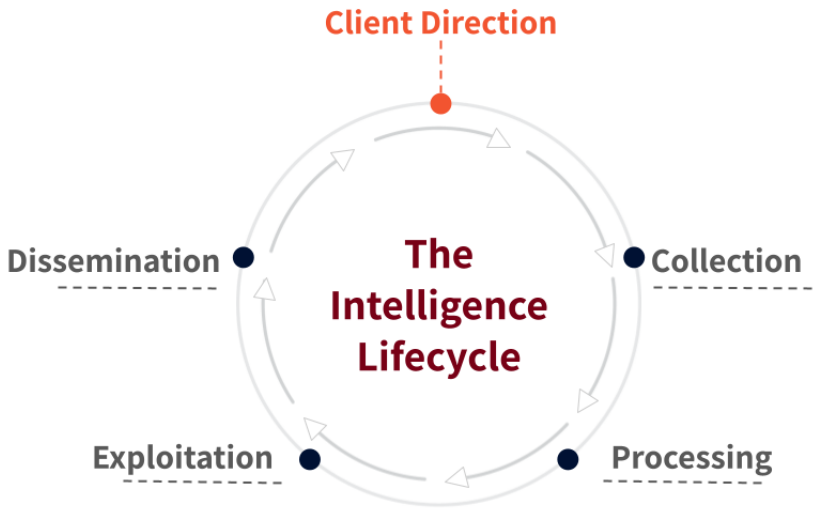
ACTION	APPROACH	QUESTIONS TO CONSIDER
Maintain Status Quo	Many businesses will opt to stay the course, trusting that their current strategic roadmap will be viable despite difficulties.	■ What, if any, new obstacles has the recession created that may risk your roadmap? ■ What elements of your business operations are critical to maintaining continuity? ■ What risk/threats should you be most concerned about?
Maintain an Agile Security Posture	Adversaries constantly innovate, and are nimble in leveraging newly discovered weaknesses; however, most budgets are static and have long planning cycles. You must be sure you are positioned to adapt to changing risks.	■ Does your organization pivot well? ■ Are you properly staffed to address multiple domains of risk? ■ Is your team able to take action quickly when confronted with changing risks and a growing threat landscape? ■ How can you modify your intelligence collection and analysis requirements as risks change?
Invest and Acquire	A few businesses will be well positioned to take advantage of the shaky foundation of acquisition targets and seize the opportunity to buy up market share at a discount.	■ How has the recession impacted your chosen investment/Merger and Acquisition targets? ■ Who is targeting your potential partner, and how? ■ How will a relationship with this third-party impact your risk profile?
Optimize Budgets	It's not easy to determine where to cut costs, especially when headcount reductions are in play. Cost-cutting and budget optimization strategies should focus on finding efficiencies in your teams' operations and ensuring continuity.	■ What tasks take up most of your team's time? ■ How can you ensure your team isn't wasting time on the wrong threats? ■ How can you ensure you don't miss threats because of budget reduction? ■ How do you maintain long-term budget flexibility while addressing current requirements?

Nisos Managed Services

Nisos Managed Intelligence™ delivers client-specific threat intelligence as an analyst-led managed service. We help businesses identify, analyze, and remediate threats across physical and cyber intelligence domains.

Our services support cybersecurity, corporate security, trust & safety, physical security, and corporate reputation teams with finished threat intelligence to enable smarter defense and informed response to threats from motivated adversaries.

We help our clients defend their organizations, preserve value, and prevent loss, as well as defeat, and attribute threats. Our in-depth understanding of the adversarial mindset helps us provide clients with in-depth insights into how someone could compromise your assets.



The Nisos Process

Using proprietary technology and datasets, Nisos delivers tailored intelligence with specific insights into targeted adversary behavior - not vague or generalized “threat data” or “feeds.” Nisos fuses intelligence with expert investigative tradecraft to identify and disrupt cyber threats before harm occurs. When necessary, Nisos investigators attribute and unmask adversaries so clients or law enforcement can pursue appropriate action.

Nisos combines the datasets, tools, and expert analysis necessary to deliver finished and actionable intelligence. With Nisos, you work with named technical operators and analysts who contextualize their findings to your specific organization.

How Nisos is Different

- We are the only analyst-led intel solution offered as a subscription service
- Each engagement is tailored to meet your specific needs
- Intelligence we provide includes recommendations, not just a statement of facts
- We don’t add noise - we identify and alert you on the material issues you need to address
- We provide you with the guidance you need - not the alerts you don’t

Nisos Case Study: How Threat Landscape Assessments Supported the Intelligence Program Roadmap of a Fortune 500 Company

A major technology company was building an intelligence program and wanted to understand the nature of threats targeting the business, as well as its competitors within the industry. They tasked Nisos with conducting a comprehensive Threat Landscape Assessment to help an internal security team level-set and prioritize ongoing intelligence requirements. Nisos was responsible for and charged with evaluating:

- Digital threats to the company
- Company sentiments and threats on social media and forums
- Company information on hacking forums
- Company information on dark web marketplaces
- Threats to C-Suite executives
- Insider threats
- Threats to subsidiaries
- Threats to developers
- Foreign influence campaigns
- Threats to the wider industry

Without placing any hardware or software, Nisos was able to gain insight into the company's threats and vulnerabilities. Through the Nisos Intelligence Database, Open-Source Intelligence gathering, and technical signature analysis of external telemetry, Nisos evaluated a wide range of social media sites, industry sites, hacking forums, domains, SSL certs, malicious IPs, threat actor profile names, and the dark web to determine the threat landscape.

The purpose of this assessment was to brief the board and senior leadership on a recommended security roadmap. Based on our findings, the company chose to: 1. Put numerous technical controls in place to reduce cyber risk, 2. Enact a subsequent executive vulnerability monitoring program to reduce executive PII proliferating on the internet, 3. Establish a broader social media and dark web monitoring program to quickly identify threats to the business.

INTELLIGENCE FOCUS	DISCOVERY
Digital Threats to Company	■ **Vulnerability discovered:** Nisos found a stale DNS entry that could allow an actor to take control of the IP. ■ **Spoofed International Domain:** An SU TLD using the company trade name was for sale on a Russian-speaking market. ■ **Past Attacks:** We discovered various SQL Injection attempts against company servers, including one anomalous attempt that we recommend be examined more closely.
Social Media and Tech Forums	■ **Negative Commentary:** Posts on Reddit and Twitter discussed the manipulation of the platform and ways to bypass security controls.
Hacking Forums and Dark Web Marketplaces	■ **Credentials:** Over 1,000+ company employee email and password combinations were found in 30 breach databases. ■ **Accounts:** Multiple instances of breached company and product line user data, accounts for sale and account checkers, cracking tools, and discussion of 2FA bypass and unban methods.
Threats to C-Suite Execs	■ **Real Injury:** The CTO was a target for hate language and death threats, some of which referred to attacking him “in real life” or for pay.
Insider Threats and Complaints	■ **Access:** A few users claimed insider access to proprietary content or tools
Subsidiaries	■ **Subsidiary 1:** Physical threats targeting tech convention and instances of a username and password database for sale. Hacker forums also referenced various bypasses, platform abuse, and hacks for sale.
Threats to Developers	■ **Harassment:** A developer who signed an exclusivity deal with the company was subjected to online abuse and death threats.
Foreign Influence Campaigns	■ **Asset Risk:** Company assets in Eastern Europe could potentially become exposed to greater Chinese influence, given a significant uptick in Chinese digital infrastructure projects in the area, spearheaded by Huawei. ■ **Theft:** Risks in Shanghai revolve around cybercrime and potential intellectual property theft and government communications monitoring.

Sources:

1. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20emerging%20resilients%20Achieving%20escape%20velocity/The-emerging-resilients-Achieving-escape-velocity-v3.pdf
2. https://www.atlanticcouncil.org/content-series/the-5x5/the-2010s-a-cyber-decade-in-review/
3. https://www.atlanticcouncil.org/content-series/the-5x5/the-2010s-a-cyber-decade-in-review/
4. https://www.statista.com/statistics/817918/number-of-business-bankruptcies-in-the-united-states/
5. https://www.checkpoint.com/downloads/resources/cyber-attack-trends-report-mid-year-2022
6. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi#page=58
7. 2022 Ontic State of Protective Intel
8. Nisos - Vanson Bourne Survey
9. Nisos - Vanson Bourne Survey

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