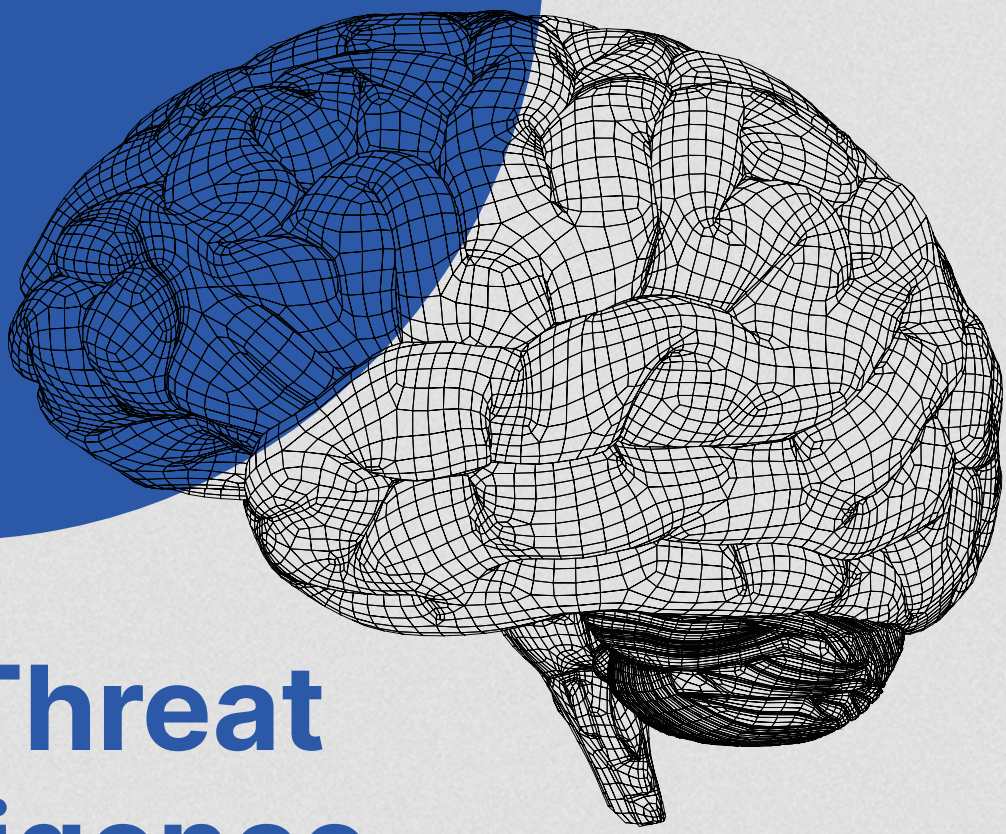
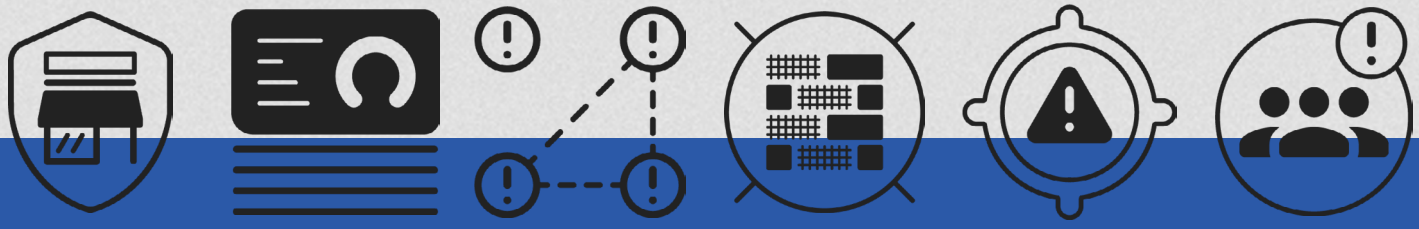
Recorded Future®



The Threat Intelligence Buyer's Guide

Everything you should know about threat intelligence before you buy

Table of Contents:



Introduction

Organizations of all sizes and from nearly every industry are facing a never ending set of challenges when trying to protect their digital assets from adversaries. This is because the modern threat landscape is vast, complex, and constantly evolving. The idea that organizations can be fully secured against any and all potential threats has become untenable and requires a shift in the tools and approaches teams need in order to stay ahead of an attack. The use and implementation of threat intelligence is a critical component of today's modern security team and when used to its full potential, it is often the difference between preventing an incident from happening vs. being a victim of a cyber incident.

Threat intelligence done right is a window into the world of your adversary. Vendors and service providers are aiming to empower organizations by alerting them to the specific threat vectors and attacks they face, as well as how they should be prioritized for protection and prevention.

As you begin the process of selecting a threat intelligence solution, you'll want to be sure you've clearly defined your needs, as well as have a good understanding of a vendor's capabilities. This short guide will pose 11 key questions and their implications to help inform your decision on selecting a solution that delivers intelligence-driven security to help protect your organization from both known or emerging threats.

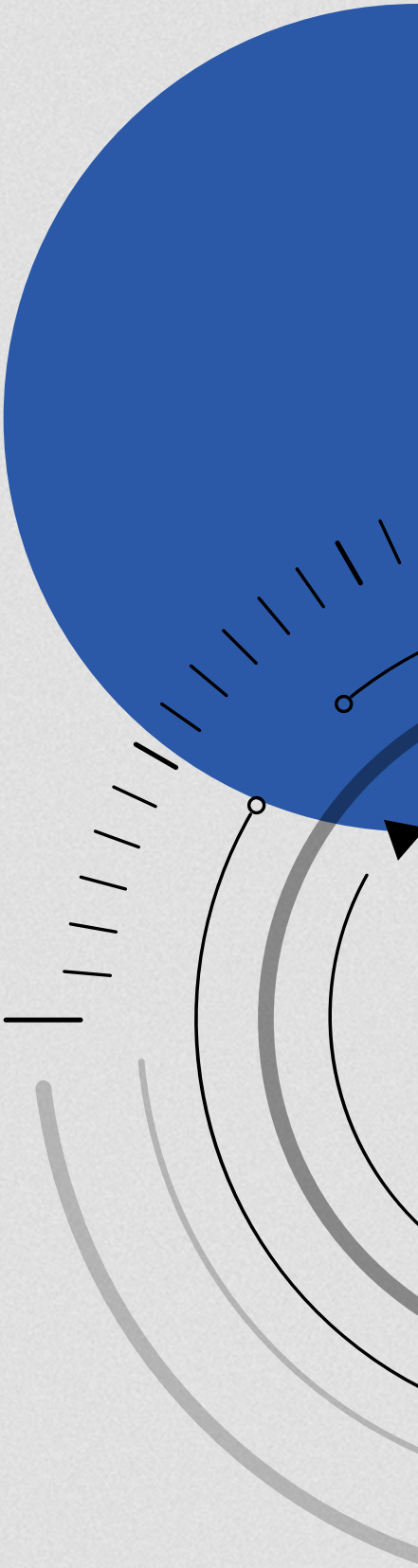
What is threat intelligence?

Before we jump in, let's define the term "threat intelligence." It comes from the more general term "intelligence" which is the product of a process that includes collecting data, analyzing it, and viewing it in context. It generally includes predictions of future behavior and recommended courses of action. Thus, even today, where there are automated systems that can collect and parse data far faster than any team of people, the human element remains essential to make sense of that data by providing context and direction.

The term threat intelligence has evolved and taken different meanings over the years. It can be associated with the practice of conducting intelligence analysis, the many software solutions that either collect and create intelligence or aggregate it, and even spans outside of just the cyber-realm where the term threat intelligence can be aligned to geopolitical issues or physical threats as well.

The Carnegie Mellon Software Engineering Institute defines threat intelligence as "acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities... to offer courses of action that enhance decision making."[1]

To level set, threat intelligence is more than just finding free feeds and looking at them; it is a combination of finding and acquiring the most relevant data that gives you unique insight into your threat landscape. Threat intelligence organizes relevant information in a way that makes it useful for analysis, and then disseminates it across the organization(s) so it can be actionable and inform decision making.



QUESTIONS TO ASK A VENDOR:

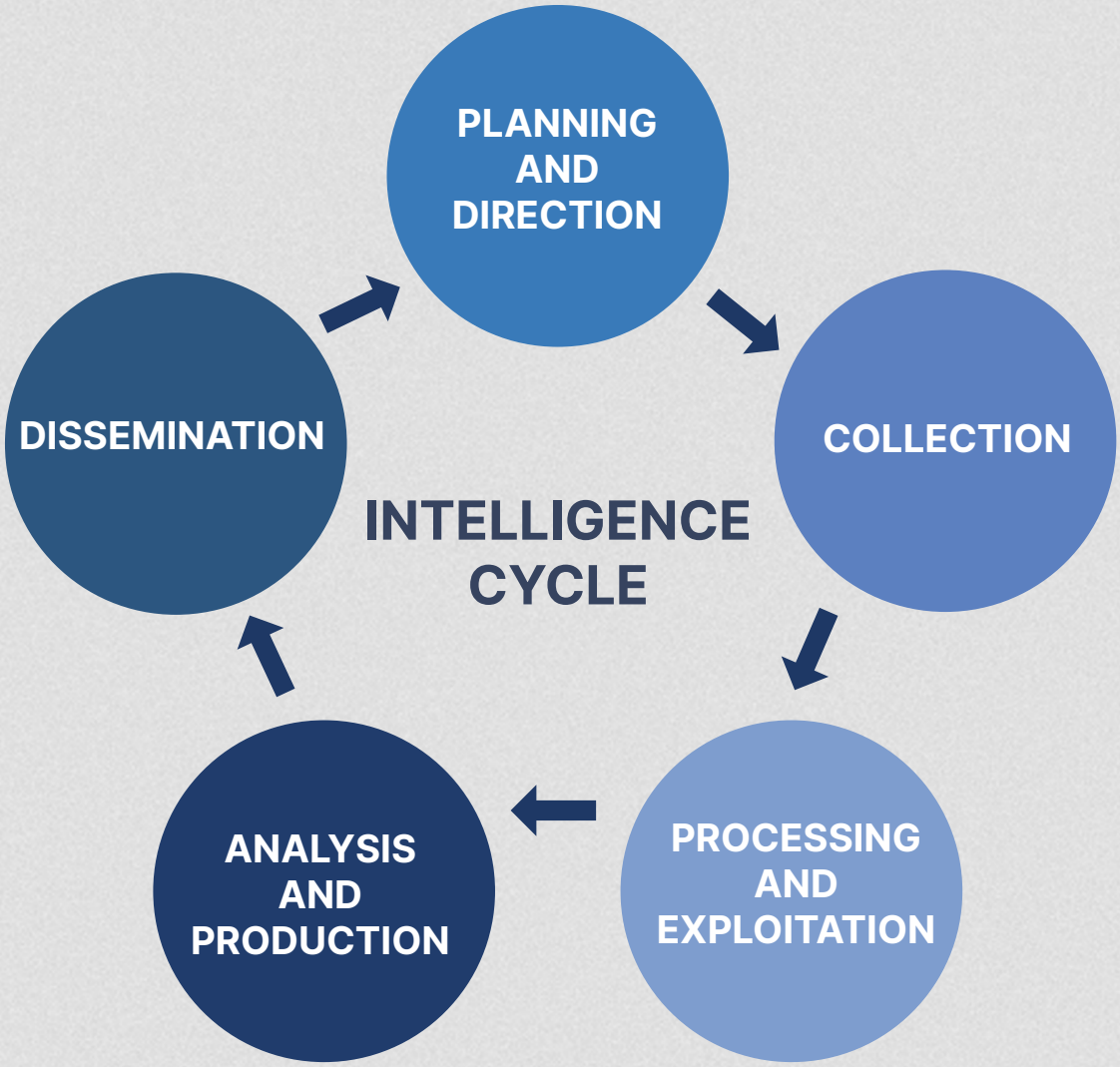
What's your definition of threat intelligence, how does your company think about it?

Are you an intelligence creator or aggregator?

1 https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=546578

What is the intelligence cycle and why does it matter?

To understand this concept a little deeper it helps to understand the intelligence cycle, which is the process of how intelligence is created and used. The intelligence cycle is a process first developed by the CIA, following five steps: direction, collection, processing, analysis and production, and dissemination. The completion of a cycle is followed by feedback and assessment of the last cycle's success or failure, which is then iterated upon.



But how does this apply to threat intelligence being used within your organization?

DIRECTION

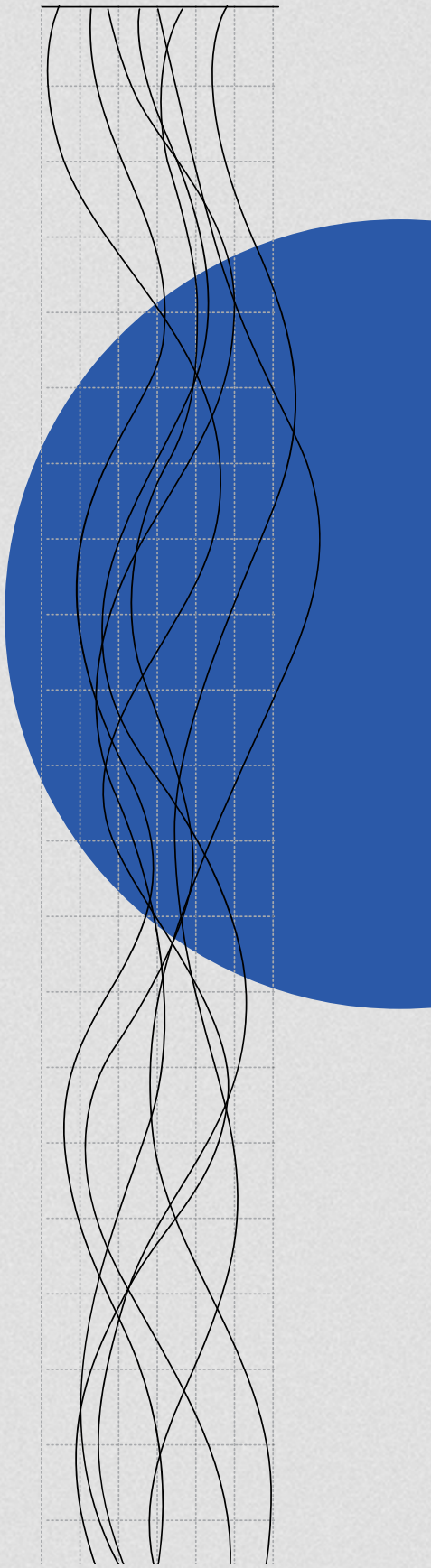
Just as in the wider intelligence community, direction comes from above — an organization's CISO, for example, or the leader of an organization's security operations center (SOC). The essential elements of threat intelligence provide information needed to give proper direction to analysts from both the physical and the digital realms: Where a government agency might focus on a certain geographical area, a SOC might choose to focus on the direct threats to their network and identifying indicators of compromise.

COLLECTION

Data is gathered from both technical and human sources. These days, when it might take millions or even billions of individual data points to build a sufficiently large sample size to identify reliable patterns, the automation offered by threat intelligence helps significantly reduce the time it takes during the collection stage. Data collected from only public sources is often not enough — cooperating with other organizations to share private data from closed sources and even having an active presence on the dark web leads to more complete data sets.

PROCESSING

Just as the large sets of data make automation necessary in the collection phase, automation is also necessary to process that data into something comprehensible — and many threat intelligence products offer effective automated tools to produce reports and other resources. But strong teaming between humans and machines is essential — an expert eye can provide the additional context and intuition needed to eliminate ambiguity. In an industry where seconds, let alone days, can make all the difference in responding to a threat, the right direction provided by a human expert can help even the fastest automated process do a smart and efficient search rather than rely on brute force alone.



ANALYSIS AND PRODUCTION

As mentioned prior, the processed data must be made coherent and sorted effectively, and again, no automation can really make up for human analysis. As defined above, intelligence includes an analysis of motivations and predictions about future behavior, and that kind of analysis can only be done well by personnel armed with the right technology.

DISSEMINATION

The finished product goes back to the top, starting the cycle again. This could be by way of finished intelligence reports, briefings from the team, alerts, or any other way that stakeholders choose to consume intelligence.

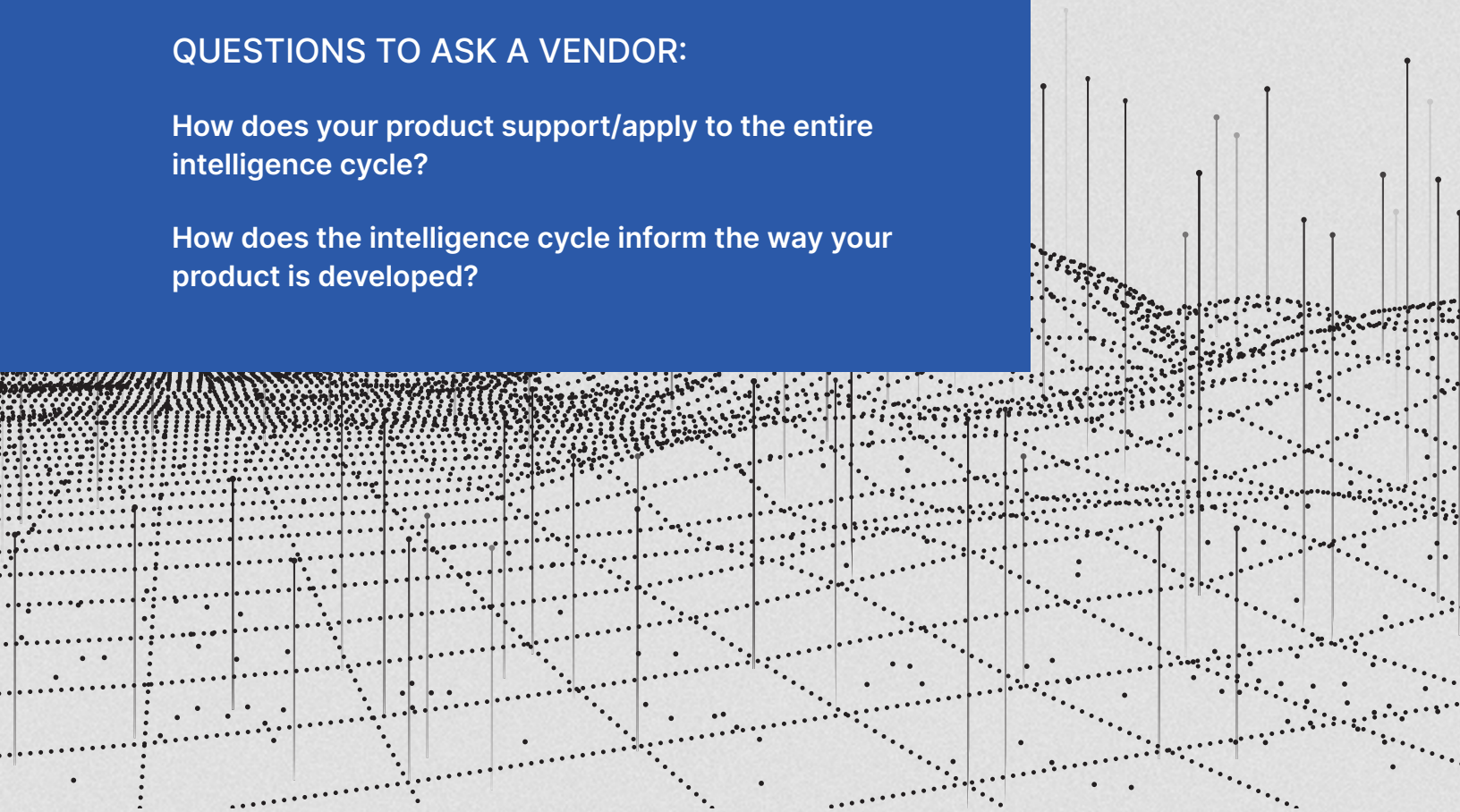
FEEDBACK

The effectiveness of one cycle of threat intelligence will determine the essential elements of information needed for the next cycle, including what areas to focus on when collecting data and how fast action needs to be taken going forward.

QUESTIONS TO ASK A VENDOR:

How does your product support/apply to the entire intelligence cycle?

How does the intelligence cycle inform the way your product is developed?



What are the different types of threat intelligence and who consumes it?

Threat intelligence comes in many different "flavors" and categories, and deciding which is best for your organization largely depends on your intended use cases. To help you identify what types of intelligence can best support your organization, examine the following three categories of intelligence and their targeted use cases:

Strategic Threat Intelligence

This type of intelligence gives a wide view, designed to inform the decisions of executives and senior leaders of risks posed to their organization from cyber or physical threats. It is rarely technical, and is most likely to cover topics like industry threat trends, geopolitical trends, emerging technology and threats, compliance and regulatory standards, and financial impact of security events. Leaders with this level of intelligence can use it to create an intelligence-led security strategy, maximize security investments, or inform other stakeholders.

STAKEHOLDERS/CONSUMERS:

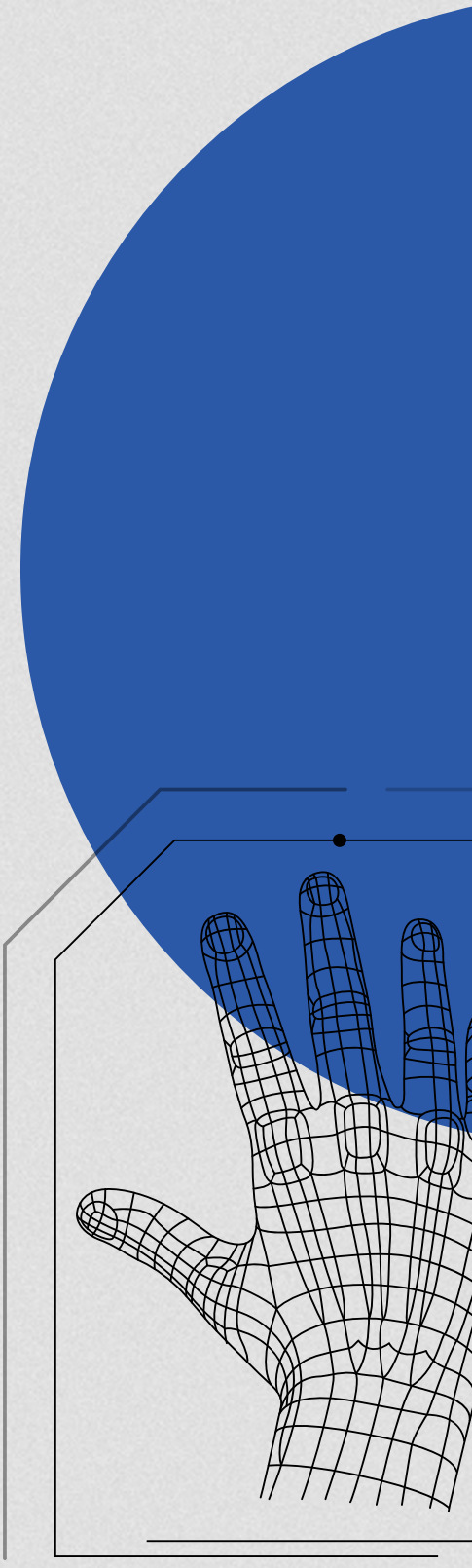
- C-Suite (CISO, CIO, CSO, CTO)
- Board Members
- Senior VPs
- Intelligence Leaders (Cyber and Physical)

Operational Threat Intelligence

Far more in-depth than strategic threat intelligence, operational threat intelligence is used to understand the "who, what, why, when, and how" about threats targeting the organization. Analysts can conduct deep analysis on threat actors and their tactics by creating reports that inform other security teams to enable them to take action. This is typically related to specific, impending attacks, and is often consumed by senior security staff or cyber threat intelligence teams.

STAKEHOLDERS/CONSUMERS:

- Security Leaders
- SOC Manager
- Threat Hunter
- Cyber Threat Intelligence Team
- Incident Responders



Tactical Threat Intelligence

Usually consumed automatically, tactical threat intelligence comprises a stream of indicators which can be used to automatically identify and block suspected malicious communications. A good example might be a feed of IP addresses suspected to be malicious, from which any communications would be automatically vetted or blocked. This type of intelligence is typically transient and available in extremely high volumes, hence the need to process it automatically rather than involving human analysis. Typically, this form of intelligence is highly actionable and is used by operational staff, such as incident responders, to ensure technical controls and processes are prepped and put in place.

STAKEHOLDERS/CONSUMERS:

- SOC Analyst
- IT Analyst
- Vulnerability Management
- Security Architects (for integrations)

None of these categories are intrinsically "better" than others. Instead, they can be used side-by-side to form a cohesive threat intelligence capability. Depending on an organization's needs and capabilities, it may decide to initially only consume technical or tactical threat intelligence, as it's the most readily available. But as needs change over time, most organizations will expand the types of threat intelligence they ingest, making it critical to select a vendor that delivers multiple categories and a solution that can expand over time.

QUESTIONS TO ASK A VENDOR:

Do you provide intelligence across these three categories? Can you show me examples?

What type of intelligence do you invest the most heavily in?

Who should use threat intelligence?

At the most senior levels, security decision makers have traditionally assessed and quantified the risk from the threats they face based purely on internal factors, industry trends, or what they read in the news. With threat intelligence there is the opportunity to understand current and emerging threats uniquely relevant to your organization/industry and how they affect your overall security strategy and decision making.

In addition, teams across your security organization can benefit from more informed decision making and unique perspectives. Intelligence that can be easily consumed and comprehended has the potential to revolutionize how different roles in your organization operate day to day.

The diagram below shows examples of how different teams inside an organization use threat intelligence. This diagram is designed to give you an idea of some of the most common teams and uses of intelligence, but these aren't the only teams who would benefit from intelligence:

QUESTIONS TO ASK A VENDOR:

How can your intelligence and product support the different teams in my organization, both the decision makers as well as the security group?

Who are the typical consumers of intelligence from your product?

What types of sources should a threat intelligence vendor collect from?

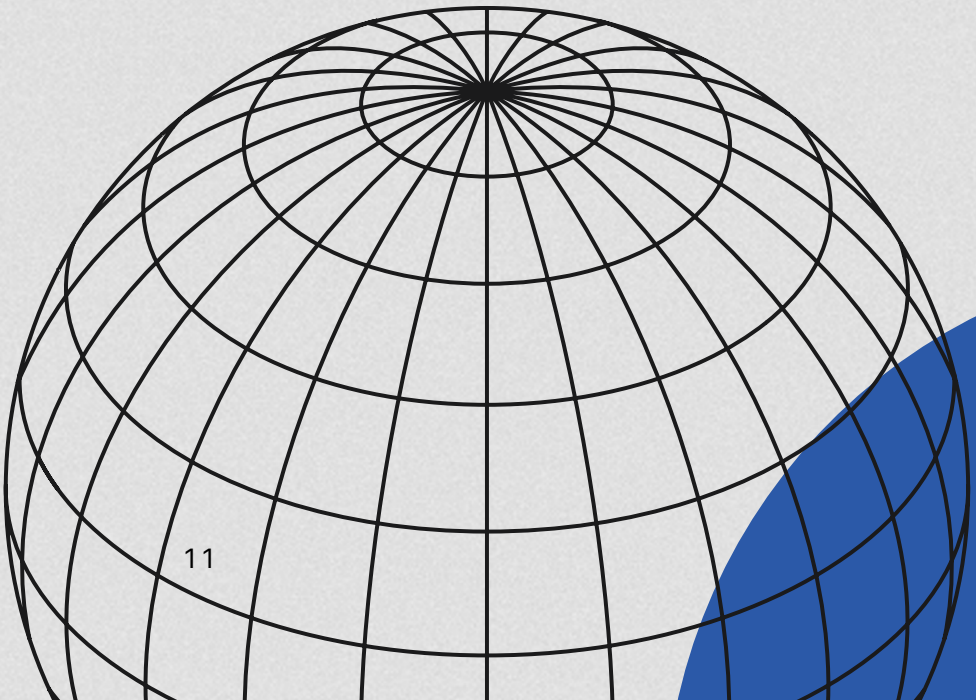
To be truly valuable, your threat intelligence program must consider the broadest possible range of threat data sources within the scope of the objectives you set. You must also bear in mind that without processing, these sources are only data, and not intelligence.

Any threat intelligence vendor you choose should have access to many or all of the following sources:

- Forums
- Threat Feeds
- Paste Sites
- Dark Web
- News
- Mainstream and alternative social media and blogs
- Code repositories
- Technical data including network telemetry, passive DNS, netflow, endpoint data, and more
- Foreign language sources
- Vendor-created finished intelligence

You may also find that some providers specialize in producing intelligence from particular sources, like social media or dark web which is good, but may not necessarily provide the context or complete view to effectively investigate or address a threat.

For most organizations, it's the combination of all or most of the above sources that is most powerful. Integrating and analyzing data from multiple sources can give you unique insights, deep context, and a balanced view that cannot be achieved any other way. Depending too heavily on one or two sources of data will lead to missed opportunities, and ultimately, skewed perspectives.



For example, if you're only ingesting open source threat feeds, you will lack the context necessary to make informed decisions. Questions that come to light as a result of using or limited sources which lack context are: How could you possibly know which of the thousands of vulnerabilities discovered each year should be patched first? Should you act immediately, rather than wait for the next scheduled maintenance period? Look for solutions that add this kind of context to give you clear indications of risk that can be applied to your wider security strategy.

When evaluating which solution will best enable you to reach your objectives, it's vital to consider the balance of data sources versus the insights each will deliver. You need a solution which consumes data from a wide range of sources (including any you already have access to), but also one that contextualizes and prioritizes relevant alerts while simultaneously cutting out the noise.

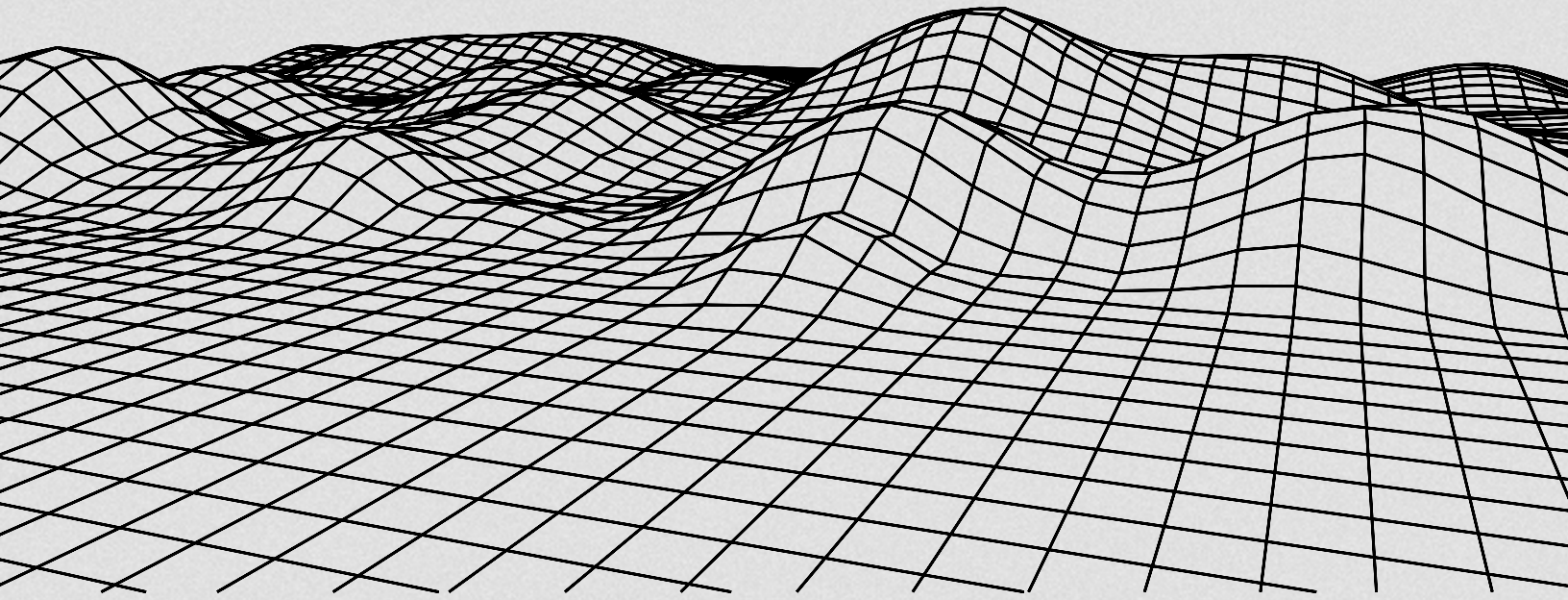
QUESTIONS TO ASK A VENDOR:

How diverse are the sources you collect from?

Do you support collection in foreign languages?

How quickly can you add new sources?

Do you have a finished intelligence team? What topics do they cover? Can I task them?



How should I measure a threat intelligence solution's value?

In a study conducted by Johns Hopkins University for CISA, they set out to answer the question "how can an organization assess a product, service, or feed and associated cost to ascertain what solution best aligns with the organization's requirements?" They found that the best indicator of value of a threat intelligence provider is whether the intelligence is both relevant and usable.

"There are two areas of consideration to assess the potential value of a CTI feed: relevance and usability. However, most organizations only focus on relevance. While determining if an offering is relevant is important, it is not enough. The organization / customer / consumer also needs to make sure the information is usable and applicable in their environment; that it is actionable and can be used to drive the operational processes and decisions in a timely manner with minimal impact to local resources."[2]

2 https://www.cisa.gov/sites/default/files/publications/Assessing%20Cyber%20Threat%20Intelligence%20Threat%20Feeds_508c.pdf

Is the intelligence relevant?

- **Applicable** - The intelligence from the vendor has information directly related to threats and risks relevant to the organization and industry.
- **Accurate** - An organization needs to make sure that the intelligence they get is accurate enough for how they intend to use it.
- **Timely** - The information is providing insight into threats in time for the organization to make relevant risk decisions.

Is the intelligence usable?

- **Machine-readable** - The data is provided in a structured format that can be processed in an automated manner.
- **Consumable** - The data can be accessed and converted into information that is used by operational processes in a timely manner.
- **Actionable** - The data can be converted into information that is used directly by decision-making processes within the timeframe that making the decision has value.

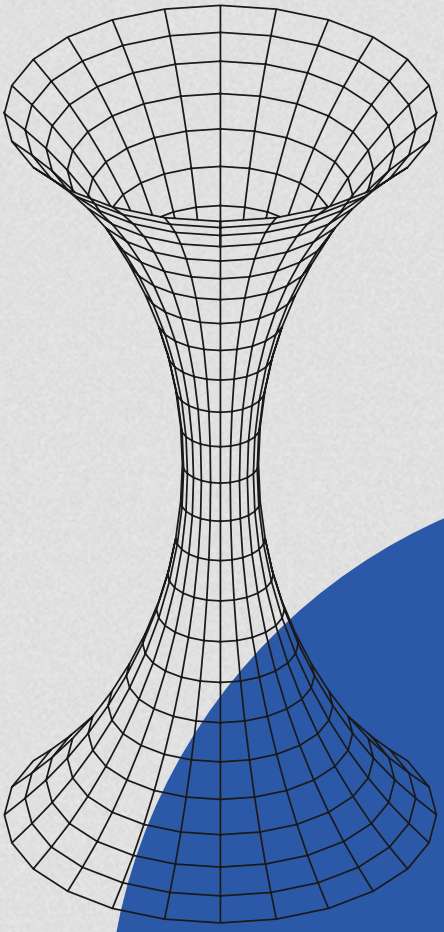
IS IT RELEVANT?

APPLICABLE	ACCURATE	TIMELY
Threats of interest? What/who are the sources of threat for the provider?	How noisy is the information? How confident are they? Do you know how they derive certain content?	How long does it take to generate the information? How quickly is it shared?

IS IT USABLE?

MACHINE-READABLE	CONSUMABLE	ACTIONABLE
What is the sharing infrastructure? Can you access in an automated manner?	Can you access and inject into operational processes in an automated manner? Is the information consistent in usage and existence?	Can you use the information to make operational decisions in a timely fashion?

How do I consume threat intelligence?



- **Comprehensive Intelligence Platform** - Unlike feed aggregators, intelligence providers provide threat data (including all types of feeds) and information collected from open, technical, and dark web sources, using a combination of machine-learning techniques including natural language processing (NLP). The collected information is used to produce relevant and actionable intelligence at scale which is typically disseminated to users through a SaaS-based portal that allows for querying and deep analysis or through tailored alerts. Leading solutions will also offer human intelligence services powered by their technology.
- **Direct Integrations with Security Tools & API** - Security teams should be able to get intelligence delivered directly to the tools they use through out of the box integrations with SIEMs, SOAR platforms, vulnerability management, endpoint, ticketing, link analysis, and more. Advanced security teams could also leverage an API to expand on the existing integrations, or to create specialized threat intelligence integrations with their custom or proprietary security products and workflows.
- **Finished Intelligence** - Report writing is one of the most time-consuming functions of a security team. With threat intelligence you can outsource the production of intelligence reports by consuming finished intelligence reports written by an intelligence vendor.
- **Managed Services** - Instead of receiving alerts directly, a security vendor will consume massive quantities of information on your behalf. If they deem something relevant to your organization, you'll be informed via a reporting service — typically, via an online portal, and they will assist with potential actions you can take. In addition, if the vendor identifies fraudulent websites, social media handles, or typosquatted domains, they will get them taken down on your behalf.

Where do I start?

Get buy-in from leadership

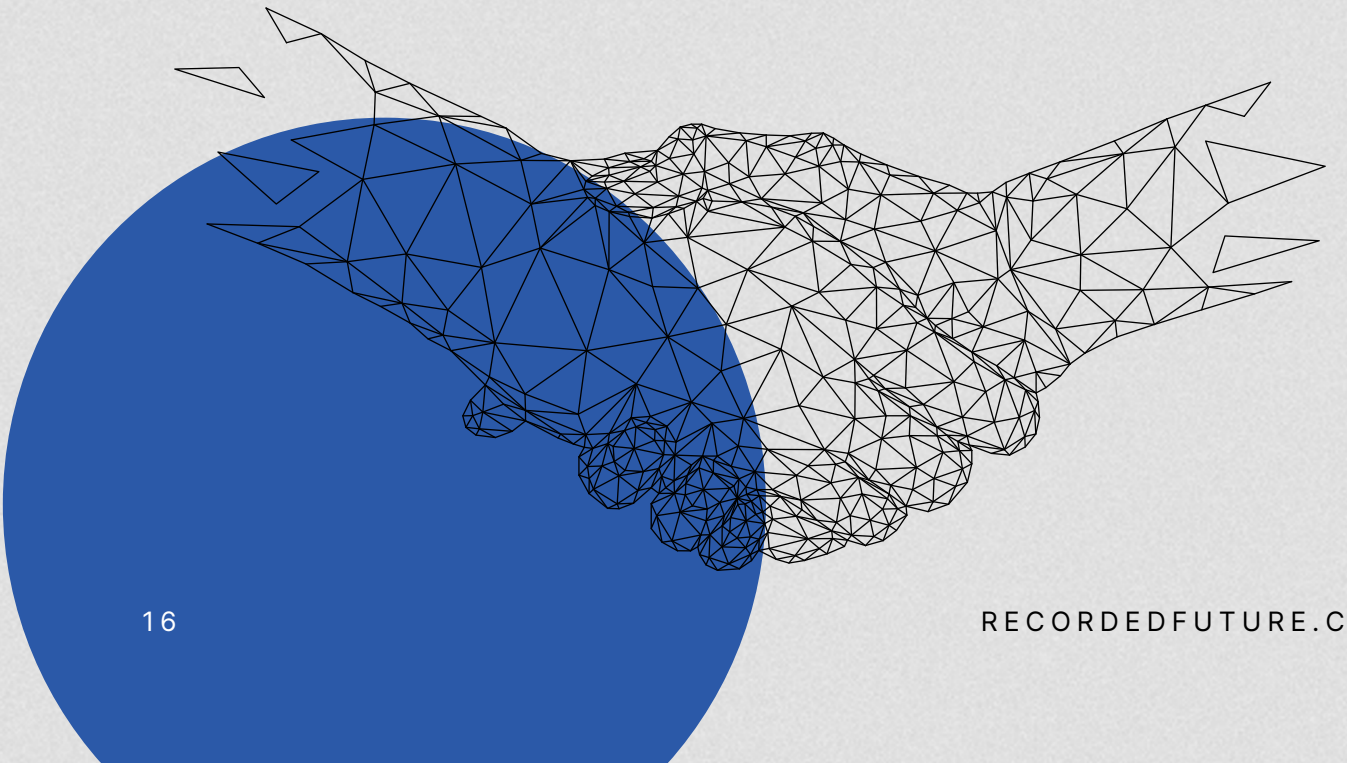
The C-suite and other leaders must assess and manage risk by balancing limited available resources against the need to secure their organizations from ever-evolving threats. In order to get buy-in from leadership, they need to understand that threat intelligence helps map the threat landscape, calculate risk, and give security personnel the context to make better, faster decisions.

Today, security leaders are tasked with:

- Assessing business and technical risks, including emerging threats and "known unknowns" that might impact the business
- Identifying the right strategies and technologies to mitigate the risks
- Communicating the nature of the risks to top management, and justify investments in defensive measures

Threat intelligence helps leaders across all of these activities and is a critical resource, providing information on general trends, such as:

- Which types of attacks are becoming more (or less) frequent?
- Which types of attacks are most costly to the victims?
- What new kinds of threat actors are coming forward and which assets and enterprises they are targeting?
- Which security practices and technologies have proven to be the most (or least) successful in stopping or mitigating these attacks?



Threat intelligence also enables security teams to assess whether an emerging threat is likely to affect their specific enterprise based on factors such as:

- **Industry** — Is the threat affecting other organizations in our vertical?
- **Technology** — Does the threat involve compromising software, hardware, or other technologies used in our enterprise?
- **Geography** — Does the threat target facilities in regions where we or our suppliers have operations?
- **Attack Method** — Have methods used in the attack, including social engineering and technical methods, been used successfully against our company or similar ones?

With this level of intelligence, gathered from a broad set of external data sources, security decision makers are able to gain a holistic view of the overall risk landscape and prioritize the greatest risks to their enterprise.

Here are five key areas that you can bring forward to security leaders to help them understand the value intelligence brings by making them more informed and educated on the risks impacting their organization:

- **Assess Risk** — With so many threats stemming from cyber, physical, influence, and even supply chain, it's hard to understand which you should care about and what you should do about them. Threat intelligence helps leaders assess threats in the context of risk to their business so they can prioritize the threat vectors and actors that can actually cause harm to their people and assets and stop wasting time and resources on threats that don't matter.
- **Mitigation** — Threat intelligence helps security leaders prioritize the vulnerabilities and weaknesses that threat actors are most likely to target, giving context on the TTPs those threat actors use, and therefore the weaknesses they tend to exploit.
- **Communication** — CISOs are often challenged by the need to describe threats and justify countermeasures in terms that will motivate non-technical business leaders, such as cost, impact on customers, and new technologies to implement. Threat intelligence provides powerful ammunition for these discussions, such as the impact of similar attacks on companies of the same size in other industries or trends and intelligence from the dark web indicating that the enterprise is likely to be targeted.

- **Supporting Leaders** — Threat intelligence can provide security leaders with a real-time picture of the latest threats, trends, and events, helping them respond to a threat or communicate the potential impact of a new threat type to business leaders and board members in a timely and efficient manner.
- **Security Skills Gap** — CISOs must make sure the IT organization has the necessary human capital to carry out its mission. But because of the skills shortage in cybersecurity, existing security staff are frequently burdened with unmanageable workloads. Threat intelligence automates some of the most labor-intensive tasks, rapidly collecting data and correlating context from multiple intelligence sources, prioritizing risks, and reducing unnecessary alerts. Powerful threat intelligence also helps junior personnel quickly "upskill" and perform above their experience level.
- Establish intelligence requirements, identify gaps, and invest.
- Establish or review intelligence requirements.
- Identify intelligence gaps and invest in those areas.
- Measure intelligence source effectiveness.
- Produce strategic reports and assessments for executives and attribute it to intelligence.
- Tie it to metrics, such as decreased dwell time, efficiency, etc.

Start by continuing this conversation and getting a demo from the most trusted intelligence provider here.

About Recorded Future

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,300 businesses and government organizations across 60 countries.

Learn more at recordedfuture.com.