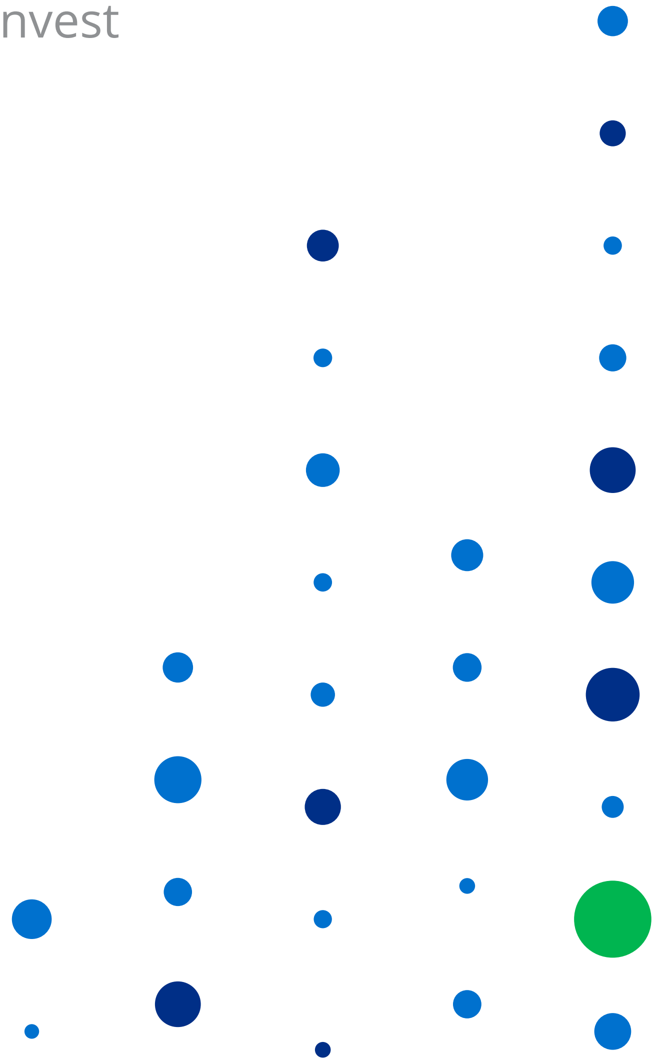
Recorded Future

WHITE PAPER

The Buyer's Guide to Cyber Threat Intelligence

11 Questions to Answer Before You Invest



Introduction

The modern threat landscape is vast, complex, and constantly evolving. The idea that businesses can be fully secured against any and all potential threats has become untenable.

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.

Gartner defines threat intelligence as, "evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." [1]

This definition highlights the three factors that distinguish threat intelligence from mere data and information. At its heart, threat intelligence:

1. Must be evidence-based.
2. Must relate to an existing or emerging threat.
3. Must inform decision making.

If any of these requirements are missing, more processing is required before information can be considered threat intelligence.

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 vendor 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.

---

[1] "Market Guide for Security Threat Intelligence Products and Services," Gartner, (July 20, 2017).

> “Threat intelligence done right is a window into the world of your adversary.”

Recorded Future

1. Which categories of threat intelligence are most valuable to you?

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 your area of need, we subdivide threat intelligence into four categories and their targeted use cases:

Operational Threat Intelligence — This is related to specific, impending attacks, and is often consumed by senior security staff. This is what comes to mind most commonly when people think of threat intelligence; the ability to identify when and where attacks will come in advance.

Strategic Threat Intelligence — This type of intelligence gives a wide view, designed to inform the decisions of executive boards and senior officers. This type of intelligence is rarely technical, and is most likely to cover topics such as the financial impact of cybersecurity or major regulatory changes, such as the General Data Protection Regulation (GDPR).

Tactical Threat Intelligence — Often referred to as tactics, techniques, and procedures (TTPs), tactical threat intelligence relates to the specific attack vectors favored by threat actors in your industry or geographic location. 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 suitably prepared. For example, if spear phishing is identified as a prominent attack vector in your industry, you might invest in additional security training for highly privileged users.

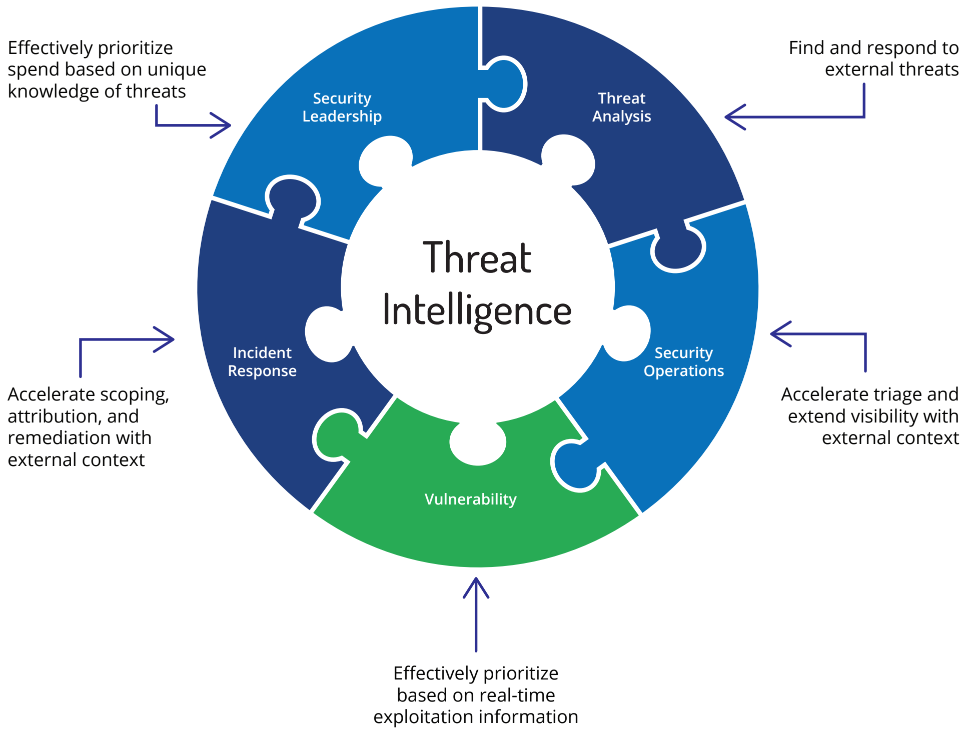
Technical Threat Intelligence — Usually consumed automatically, technical threat intelligence comprises a stream of indicators which can be used to automatically identify and block suspected malicious communications. A good example might be a feed of IP addresses suspected to be malicious, from which any communications would be automatically 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 analysts.

None of these categories are intrinsically “better” than others. Instead, they can be used side-by-side to form a cohesive threat intelligence capability. Businesses may decide to initially only consume technical 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.

2. Who will be using threat intelligence?

Security decision makers have traditionally quantified the risk from the threats they face based purely on internal factors or what they read in the news. Now, there is the opportunity to apply intelligence uniquely relevant to your business.

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, there are significant security advantages to that. The diagram below shows examples of how different teams inside organizations use threat intelligence:



Threat Intelligence
Security Leadership
Threat Analysis
Security Operations
Vulnerability
Incident Response
Effectively prioritize spend based on unique knowledge of threats
Find and respond to external threats
Accelerate triage and extend visibility with external context
Effectively prioritize based on real-time exploitation information
Accelerate scoping, attribution, and remediation with external context

“Now there is the opportunity to apply intelligence uniquely relevant to your business.”

3. Will intelligence be integrated with your existing security processes and infastructure?

Closely related to who in your organization will be using threat intelligence, is where they will be using this intelligence. Is it better to integrate into existing systems, or will users be comfortable learning a new solution and interface to access the intelligence they need? Integrating into existing systems is an effective way to make the intelligence accessible and usable without overwhelming teams with new technologies or too much data.

By combining internal and external data points, genuine intelligence can be produced — intelligence that is both relevant to your business and placed in the context of the wider threat landscape. Key operational objectives like empowering vulnerability management or incident response benefit far more from having specific, relevant, contextualized intelligence in the right place at the right time. This is the primary reason why so many threat intelligence solutions are designed to integrate with SIEMs and other security tools, either through turnkey integrations with established partners or APIs.

In the end, the combination of internal and external sources can help cut through the noise and identify the most urgent issues. When evaluating threat intelligence solutions, it's important to understand if the solution is capable of integrating with your existing solutions and supporting your security teams' use cases.

4. How are finished intelligence reports part of your threat intelligence strategy?

Finished reports are produced and used to inform high-level strategy decisions. Threat reports, whether produced internally or by a security vendor, can give you strong insight into broad industry trends, commonly used attack vectors, and emerging threats. This type of intelligence is highly valuable when making investment decisions, or hammering out policy documents.

When evaluating threat intelligence solutions, in addition to the requirements of your different security teams, consider the needs of the executive team. These days, it's inevitable that leaders in your organization will ask questions about the latest security headline, so you want to make sure you're partnered with a threat intelligence provider that can address these business needs, particularly during spikes in capacity requirements from a resource-constrained team.

5. How much expertise will you need to get started?

The level of value you get from the threat intelligence you ingest is directly related to your ability to make it relevant to your organization and effectively apply it to existing or new security processes. There are numerous products and services designed to help you implement threat intelligence, all that's required from your team are clear objectives on the advantages you expect it to bring.

The vendor who can help you toward these goals almost certainly provides a combination of technical capabilities and expertise in empowering other businesses to get the most from threat intelligence.

Technical support and professional services from a vendor must be there to help you use any software, address potential issues, and work to integrate intelligence with the existing security systems you need. And of course, this support should be available when you need it, through communication channels that best suit your business.

The supplier you choose should also be a company full of threat intelligence experts. These specialists are equipped to understand your needs and can help you get the most from your investment by enabling you to produce your own threat intelligence. You'll want to be able to call on these services whenever it suits you, and they should be ongoing, working with you to identify potential new advantages to be gained from threat intelligence in your organization.

6. Which sources of threat data do you need?

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:

Technical

This type of data is available in huge quantities, often for free. Due to its binary nature, integrating it with existing security technologies is easy, although a great deal of further analysis will be needed to derive real context.

Media

These sources often provide useful indicators of new and emerging threats, but they will prove difficult to connect with relevant technical indicators to measure genuine risk.

Forums

Because these channels are specifically designed to host relevant discussions, they are a potentially valuable source of threat information. With that said, you'll still need to spend time on collection and analysis to identify what is truly valuable.

Dark Web

Often, this is the source of very specific, tactical, and technical threat information, but it's incredibly hard to access, particularly for the higher-tier criminal communities. Additionally, as many of these communities are non English speaking, language is often a challenge.

Social Media

Undoubtedly, there are masses of potentially useful data on offer from social media channels, but it's hard to determine false positives and misinformation. Typically, you'll find many references to the same threats and tactics which can place a heavy burden on human analysts.

You may also find that some providers specialize in producing intelligence from particular sources, like social media or dark web.

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.

If you're only ingesting open source threat feeds, for example, you will lack the context necessary to make informed decisions. How could you possibly know which of the thousands of vulnerabilities discovered each year should be patched first? Or whether you should act immediately, rather than wait for the next scheduled maintenance period? Look for solutions that can 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 aid you to reach your objectives, it's vital to consider the balance of data sources versus 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 you also need one that can contextualize and prioritize relevant alerts while simultaneously cutting out the noise.

7. How will your threat intelligence capability scale?

Perhaps your initial financial and human investment in threat intelligence will be comparatively small, but as time goes on, and you look to apply intelligence in more places, the more manual your processes are, the more exponentially resource intensive they become. In reality, the sheer volume of available threat data makes collection and processing functionally impossible for humans to perform alone. Even with alerts aggregated and normalized into one location (as is done by simple threat intelligence platforms), your team will be quickly overwhelmed.

Threat intelligence providers using human analysts alone face the same challenge. Humans are time consuming and expensive to scale. An effective solution is one in which the simple tasks — data aggregation, comparison, labeling, and contextualization — are completed by machines, leaving humans to do only what they can: make effective, informed decisions. Using automation in this way will give you the confidence that as your needs change, your threat intelligence solution can effectively scale to meet them.

Examine the level to which vendors employ automation, not just to cross-reference or aggregate data, but also to add context that really equips your teams to make risk-based decisions with confidence. Keep in mind that with threat intelligence, more data can be better — as long as it's properly analyzed, structured, and delivered in an easy-to-consume format.

8. Do you need your threat intelligence delivered in real time?

We've already established that there are massive volumes of threat data. This data is easily available in real time, but a great deal of it will have no real value in identifying threats relevant to your organization, your industry, or your infrastructure. This is why balancing speed and context is perhaps the most important factor in the production of actionable threat intelligence.

Without context, determining a suitable response to alerts is very difficult. However, at the same time, context can't always be found instantaneously, and many security events are time-sensitive. Taken to extremes, this can result in you making the right decision very slowly, or the wrong decision very quickly.

This is why striking a balance is so important. To provide maximum benefit, you need a solution which can balance the speed of new data with the context you'll need to make a quick decision based on actual risk.

9. Do you need an all-in-one solution or separate software tools?

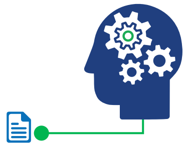
There has been a common misconception for some time that in order to “do” threat intelligence, an organization simply needs to purchase a platform, and subscribe to a few feeds.

In reality, this approach can create an even bigger headache. Subscribing to even a small number of feeds risks an overwhelming influx of alerts, each of which must be triaged promptly by a human analyst to ensure nothing is missed. Since many alerts are either false positives or simply irrelevant, analysts end up spending an inordinate amount of time achieving very little.

To shed some light on these issues, here are the four primary types of threat intelligence services and technologies available to organizations:

1. Human Analyst Reports

Outsource your production of threat intelligence by subscribing to a human analyst service. 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, an online portal.



Pros:
- Minimizes pressure on in-house resources.
- Provides access to a wide variety of sources.
- No capital expenditure required.

Cons:
- Distances in-house analysts from intelligence-gathering process.
- Inherently slower than in-house solutions.
- Relies on analysts less familiar with your business.

2. Threat Data Feeds

Real-time streams of threat indicators or artifacts provided by a third party, intended to help you learn from the access and visibility of other organizations. Feeds are invariably delivered online and typically focus on a specific type of data, like IP addresses suspected of being related to malicious activity. A huge number of free and paid feeds are available, covering every imaginable area of cybersecurity.

Pros:
- Many feeds contain highly valuable alerts.
- Real-time data can inform near instant automated response.
- Readily available and easy to get started with.

Cons:
- Lack of context makes alerts hard to process (data, not intelligence).
- Volume of false positives is huge.
- Overwhelming for human analysts.

3. Threat Intelligence Platforms

Threat feeds are rarely used in isolation. Threat intelligence platforms are employed to combine feeds into a single stream using a standardized technology, usually STIX/TAXII. While most basic platforms stop here, more complete products offer additional functionality such as normalized feeds, SIEM integration, as well as automation and orchestration.

Pros:
- Combines inputs into a single stream.
- Integration with SIEMs enables a degree of automation.

Cons:
- Vital alerts could be missed as analysts cannot cope with incoming volume.
- Lack of context can make processing alerts slow and cumbersome.
- Analysts eventually stop triaging alerts and become disillusioned.

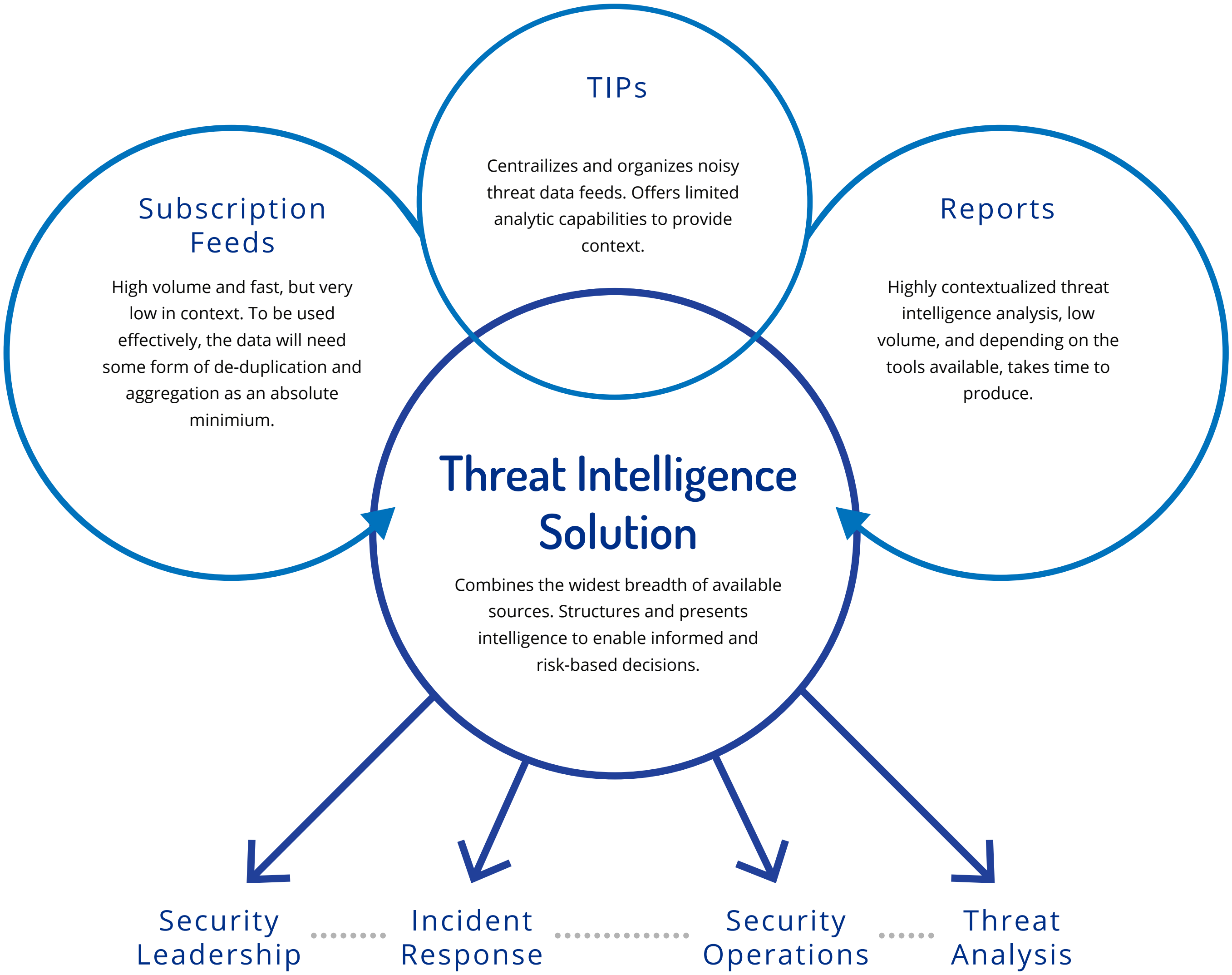
4. Universal Threat Intelligence Solution

Combines the capabilities of offerings defined above. Presents threat data (including all types of feeds) and information from throughout the public and hidden web, using a combination of machine-learning techniques including natural language processing (NLP) to produce contextualized, relevant intelligence at scale. Leading solutions will also offer human intelligence services powered by their technology.

Pros:
- Easily actionable by machines and humans.
- Alerts are fully contextualized.
- Enables more defenders to work with more intelligence.
- Extracts data from entire public and hidden web, irrespective of source language.

Cons:
- May require a greater initial investment.

As you evaluate what is available from threat intelligence vendors, make sure you've considered which of these types of offerings are most likely to meet your needs. Try ranking their capabilities by importance and quickly rule out vendors that don't have them. Most organizations will require a combination of some or all of the above — either at the start or as your program grows. Therefore, it's important to think about long-term needs when evaluating these options. Additionally, if you've already made investments in other security systems, look for solutions that will integrate with them through partnerships or a flexible API.



TIPs

Centralizes and organizes noisy threat data feeds. Offers limited analytic capabilities to provide context.

Subscription Feeds

High volume and fast, but very low in context. To be used effectively, the data will need some form of de-duplication and aggregation as an absolute minimium.

Reports

Highly contextualized threat intelligence analysis, low volume, and depending on the tools available, takes time to produce.

Threat Intelligence Solution

Combines the widest breadth of available sources. Structures and presents intelligence to enable informed and risk-based decisions.

A true threat intelligence solution combines key features from threat data feeds, threat intelligence platforms, and reports created by analysts.

“Without context, determining a suitable response to alerts is very difficult.”

10. Where is the best place to deploy the solution?

Most threat intelligence solutions are bringing externally available data into your organization for analysis or for integration with security software already installed on-premises. This flow of data from the outside in is suited perfectly for cloud-based deployment, saving on implementation efforts and removing the need for patching or upgrades.

As the solution is unlikely to hold any confidential or valuable corporate data, there are fewer security concerns. That said, you should ensure that any SaaS product carefully considers security by anonymizing any data that goes into it and provides two-factor authentication, as well as integrations with any directory services your business uses.

The biggest advantage to a cloud-based implementation is immediacy. Newly collected and analyzed intelligence should be available immediately with the cloud — not making use of information available in real time isn't how to get the best out of threat intelligence. New features or analysis techniques should also be available immediately in the cloud, avoiding potentially time-consuming, on-premise hardware upgrades.

11. How will you future-proof your threat intelligence investment?

The simplest way to maximize your threat intelligence investment is to ensure you've selected a vendor able to grow with your requirements. If you're in the early stages and decide to only implement a solution that can provide sources of threat data or analyst-curated reports, when the time comes to integrate intelligence with other security products, or employ your own threat intelligence experts, you run the risk of needing to start over from scratch. Research all of a potential supplier's capabilities so that you can be sure they don't just enable you to meet your short-term goals, but can meet your criteria as your needs evolve.

We've also already mentioned that your chosen vendor should be full of threat intelligence experts — this also means its most likely able to provide ongoing training or even certification to enable your teams and validate their effectiveness.

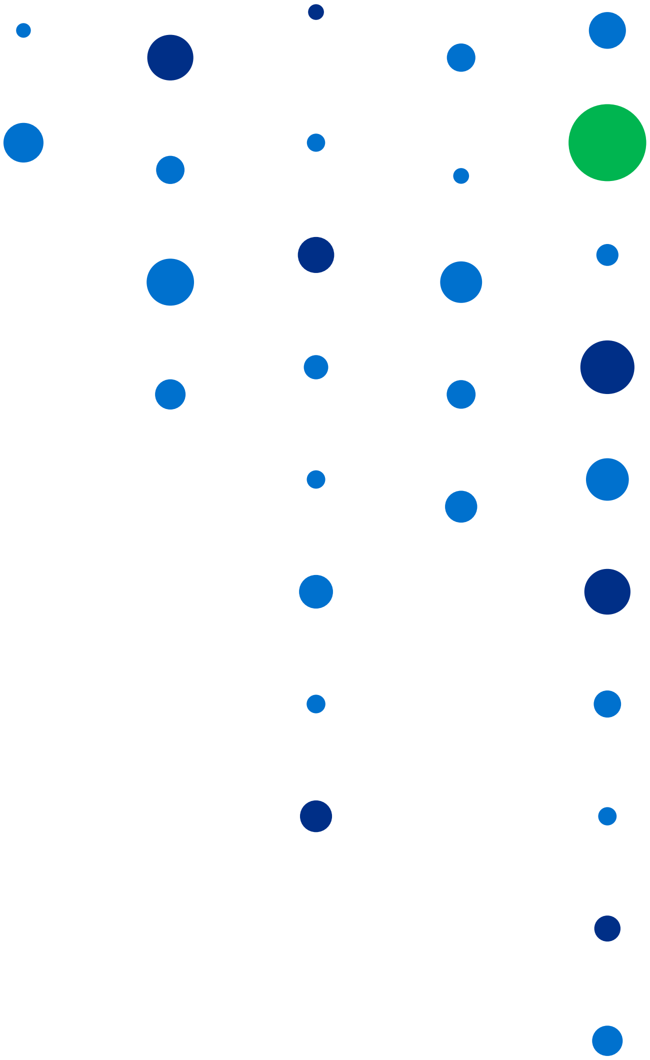
Threat Intelligence RFP Template

To start the process of selecting a threat intelligence solution, we have provided a template you can use to build an RFP, helping you to assess the capabilities of vendors you are evaluating. You can download it here.

Get Informed and Be Proactive

Once you're satisfied with how you have answered these questions, you should be equipped to make an informed decision about how to best to invest in threat intelligence. As you go through your selection process, keep your use cases (current and future) front of mind and follow this mantra:

Decide what you need threat intelligence for, and choose the solution that not only best provides what you need to achieve it today, but also adds the potential to become a partner that both equips and enables your security teams as you move forward.



Recorded Future

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

© Recorded Future, Inc. All rights reserved. All trademarks remain property of their respective owners.