Market Guide for Security Threat Intelligence Products and Services

Published 20 May 2020 - ID G00720431 - 38 min read

By Analysts Craig Lawson, Brad LaPorte, Mitchell Schneider, John Collins, Ruggero Contu

Threat intelligence capabilities can make your digital business more resilient. Security and risk management leaders will need to evaluate the capabilities and features of TI offerings and match them to the needs of their security programs based on the use cases described in this research.

Overview

Key Findings

- The utilization of threat intelligence has expanded beyond traditional security operations use cases and is even being leveraged by other functions within the organization, such as fraud, risk management, human resources and marketing.
- Client interest in industry-led (ISAC's), government (CERTs) and commercial TI has continued to increase and expand. There are still large numbers of providers in this market, with startups still entering it.
- Investment and client interest in threat intelligence platforms (TIPs) has increased in the past year. TIPs are also aggressively moving to deliver full SOAR functionality, which also includes SOA and SIRP.
- Clients globally are now taking a more proactive community information-sharing approach to security.
- The number and diversity of TI services, as well as expertise, has created an environment in which purchasers often struggle to compare services, and there's still no single provider to address all of them. Many vendors can provide access to information. Fewer provide truly anticipatory content or curation based on customized intelligence.
- The value of these services is sometimes constrained by the customer's ability to afford, absorb, contextualize and, especially, use the information provided by the services.

Recommendations

Security and risk management leaders responsible for strategizing and planning security operations should:

- Assess the level of security skills, resources and maturity of their security organization and ensure they know their use cases before considering investing in a TI. It may be more beneficial to rely on a TI provider by an MSSP or from TI in existing products.
- Define their organizations' TI use cases, such as security telemetry augmentation, deep/dark web monitoring, phishing investigations, incident response and analyst augmentation.
- Identify and align vendor specialties to the most relevant TI use cases for their organization, and use this to drive vendor selection.
- Use the three Gartner-defined requirements that need to be concurrently leveraged to get value from TI successfully — acquire, aggregate and take action.
- Investigate the use of open-source intelligence (OSINT), CERTs, information sharing and analysis center services to develop informed tactics for current threats and plan for future threats (commercial offerings are not for every organization).

Market Definition

This document was revised on 27 May 2020. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

TI products and services provide knowledge and information about security threats and other security-related issues (see "How Gartner Defines Threat Intelligence"). Intelligence-led initiatives provide information about the identities, motivations, characteristics and methods of threat actors and then, importantly, give you options to operationalize this in your cybersecurity programs. This information is derived from technical sources (for example, network traffic and files retrieved from malware archives) and human sources, including the infiltration of hacker and fraud groups, liaison work with law enforcement, incident response engagements, and cooperation with industry groups to share in an industry.

Market Description

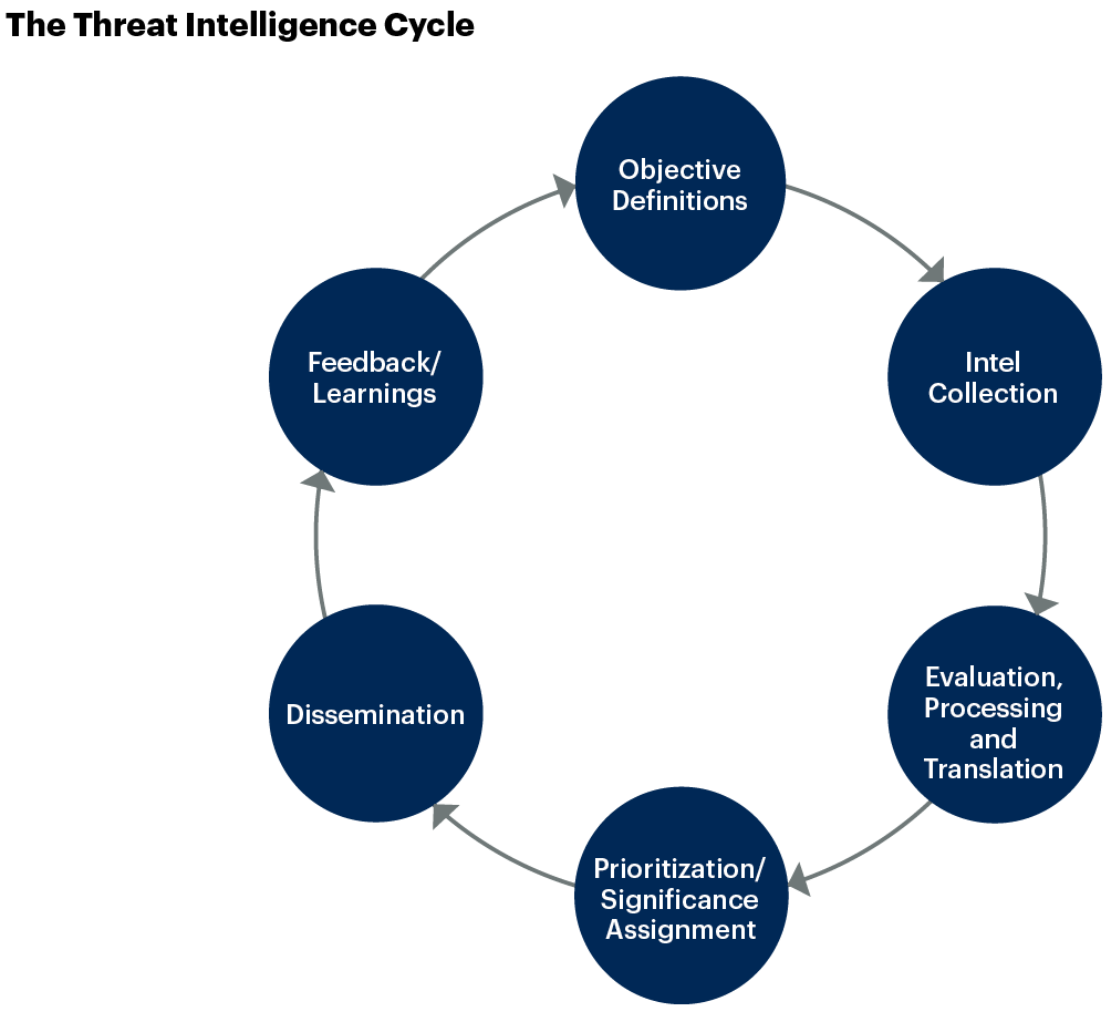
The threat intelligence market is composed of vendors that provide technologies and services that allow for the management and curation of threat intelligence. TI technologies are referred to as threat intelligence platforms, which may be sold as stand-alone solutions or as part of a SOAR solution. TI services may include monitoring the clear (surface) web, dark web and deep web, delivered in the form of feeds as MRTI and/or via reports for HUMINT. These may be provided

directly by TI vendors or as native (sometimes premium) content through various security technology vendors for SIEM, EDR, IDPS, NGFW, SWG, SEG and CASB, to name a few.

These all enable organizations to leverage the threat intelligence life cycle to their programs to help pursue a CARTA.

Figure 1 shows the typical intelligence life cycle, and it is worth noting while this is a start, this process is iterative and should constantly be reevaluating itself. As requirements change/evolve, so should your data acquisition, aggregation and action plans.

Figure 1. The Threat Intelligence Cycle



Source: Gartner

720431_C

Market Direction

The threat intelligence market remains large, with a sprawling number of vendors delivering a range of capabilities. Gartner still believes that the vendors that can deliver on the key use cases described in the Market Analysis section will be the ones that are able to deliver more value to organizations. While not perfect, this value can be roughly described as being able to assist three or more personas

(**people**), help improve/speed for up to three or more **processes,** and help improve three or more existing **technologies.**

End users are continuing to actively investigate opportunities to improve their ability to predict, prevent, detect and respond to issues presented by the prevailing threat landscape (see "Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats"). Threat intelligence products and services are proving to be a credible option for all four of these high-level requirements.

Market Analysis

Vendors Are Still Looking to Tailor Offerings to a Broader List of Vertical Industries and Organizational Sizes

TI service clients typically have assets of significant value (for example, financial assets, intellectual property or assets that support critical infrastructure), protected or otherwise sensitive information (such as user identities or classified security information), leverageable services (for example, network bandwidth), or large customer bases.

The information obtained from the product or service often feeds into a multiyear planning and deployment cycle in their security programs. TI services appeal primarily to large enterprises that have significant brand presence or higher-risk profiles, and generally have security organizations with more mature security programs.

However, some service providers are expanding their focus to include midsize organizations and have been pursuing this objective for several years by providing prepackaged, easier-to-consume offerings at lower price points into a range of technologies and maturity levels. They often do this by limiting the amount of customization and access to dedicated analysts, while making the TI easier to consume for IT teams of all sizes, including small ones. An example of this is threat intelligence gateways (TIGs) (see "Emerging Technology Analysis: Threat Intelligence Gateways") and DNS firewalls, where the end solution is relatively easy to deploy and maintain, and TI is aggregated and actionable as an immediate outcome on deployment.

Larger organizations have, for the most part, already invested in various flavors of TI. They are focusing on integration and are using multiple services (aka additive versus net new spending). Gartner expects this piece of the market (the midmarket) to be the biggest raw growth opportunity defined by smaller deal sizes, but a significantly higher volume of deals. Gartner has seen large enterprises compose 40%, small organizations compose 30% and government/public/education compose 30% of our overall search analytics over the past year.

A limiting factor for organizations in deriving value from these services is often their capacity to act on the volume of intelligence they receive from commercial providers if they go down this route. They

may find that monitoring credible, publicly available sources of threat information (such as open-source intelligence [OSINT]) will address their needs adequately.

Vendors Often Consume Similar Information

Clients that decide to purchase services from multiple providers for the purpose of correlating information from disparate sources should ensure that the sources are truly disparate.

Vendors share some intelligence content or use OEM-type commercial relationships. VirusTotal, Proofpoint's EmergingThreats, Hail a TAXII, Webhose.io and Webroot are good examples of credible sources of TI that are commonly used in many other products and services. This does not mean one vendor's offering is the same as another's; it simply means some content will be common to both because it comes from the same source. Vendors do this to provide a greater volume of content or richer content for a specific offering, particularly when a sharing partner operates in a different market or offers a differentiated service covering a different part of the threat landscape.

Vendor Capabilities Vary

Generally speaking, the utility of the intelligence offering is closely linked to the strength of the intelligence process described in Figure 1, as well as to the capabilities of the analysts executing that process.

The collection, processing and analysis of raw information is a differentiator for services. Depending on your organization's requirements, the vendor's capability in the following areas will be important decision points:

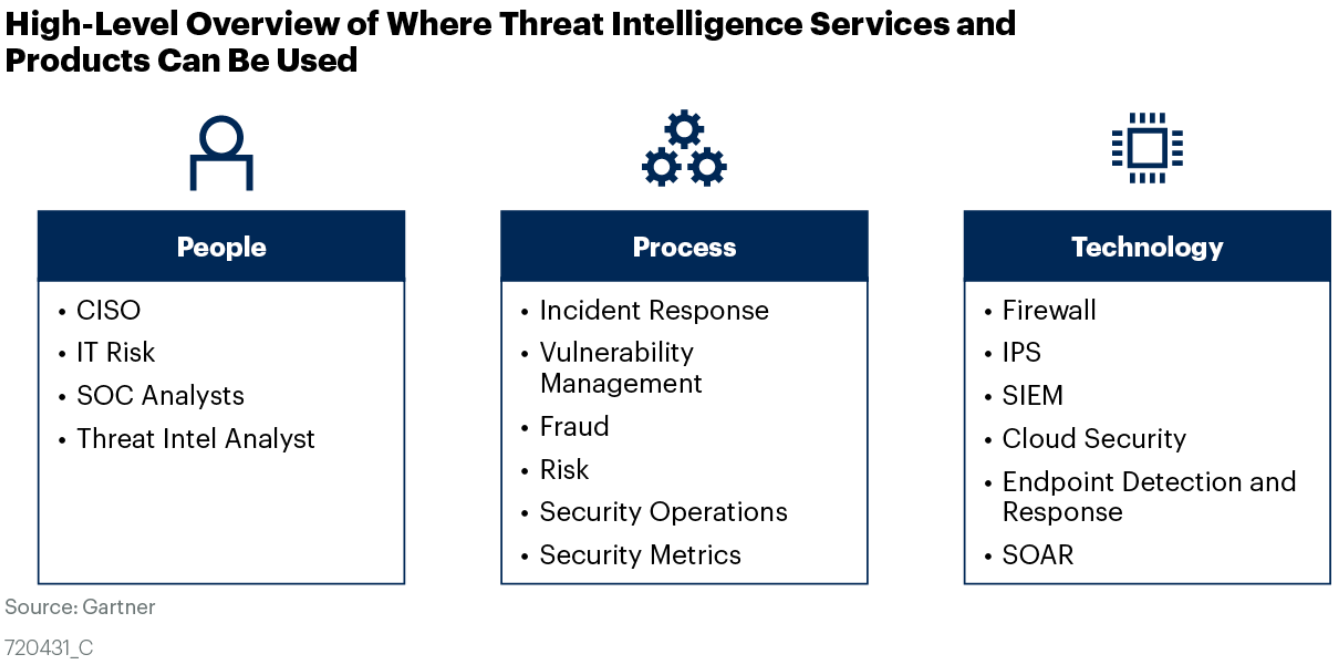
- Whether the content is based only on telemetry from current network/host activity, or whether the vendor infiltrates the dark web and has visibility to threat actor activity.
- Whether the content is gathered only from open sources or includes closed (nonpublic) sources as well.
- Whether the raw information is harvested from English-speaking sources only or the vendor collects and interprets non-English sources as well. There is an undeniable geopolitical and vertical industry nature to advanced TI services, and it's important security leaders look to capture this requirement if it's needed for their intelligence program.
- Whether the vendor provides a series of individual data points or, alternatively, correlates and analyzes disparate data points and draws informed conclusions.
- Whether the vendor has the ability and capacity to tailor the content specifically to the risks and threats (for example, infrastructure attacks or threat actors) your organization must manage.
- Whether the vendor disseminates the content in a form your organization can consume.

The ability of multilingual analysts to synthesize content from different communities is a strong differentiator. Approximately 25% of vendors report that they have multilingual capabilities, and a small number also have staff members in particular locales to facilitate this capability. Depth of analysis is improved by having analysts who speak multiple languages, have formal linguistics skills and come from diverse cultural backgrounds, so that nuances and intentions can be more effectively comprehended. This is not something that artificial intelligence (AI) or automation is likely to deliver in the foreseeable future.

Popular TI Use Cases

Taking a use-case-centric view is still the ideal and pragmatic way to start a journey and improve your security program with intelligence-led initiatives (see Figure 2). In some client inquiries, Gartner has seen clients start by getting a service first, then trying to get that investment to fit the use cases later. Instead, we recommend deciding what you want from TI in the first place — that is, what end do you have in mind? Then determine what you'd be prepared to slice out of or find additional funding for from your security budget.

Figure 2. High-Level Overview of Where Threat Intelligence Services and Products Can Be Used

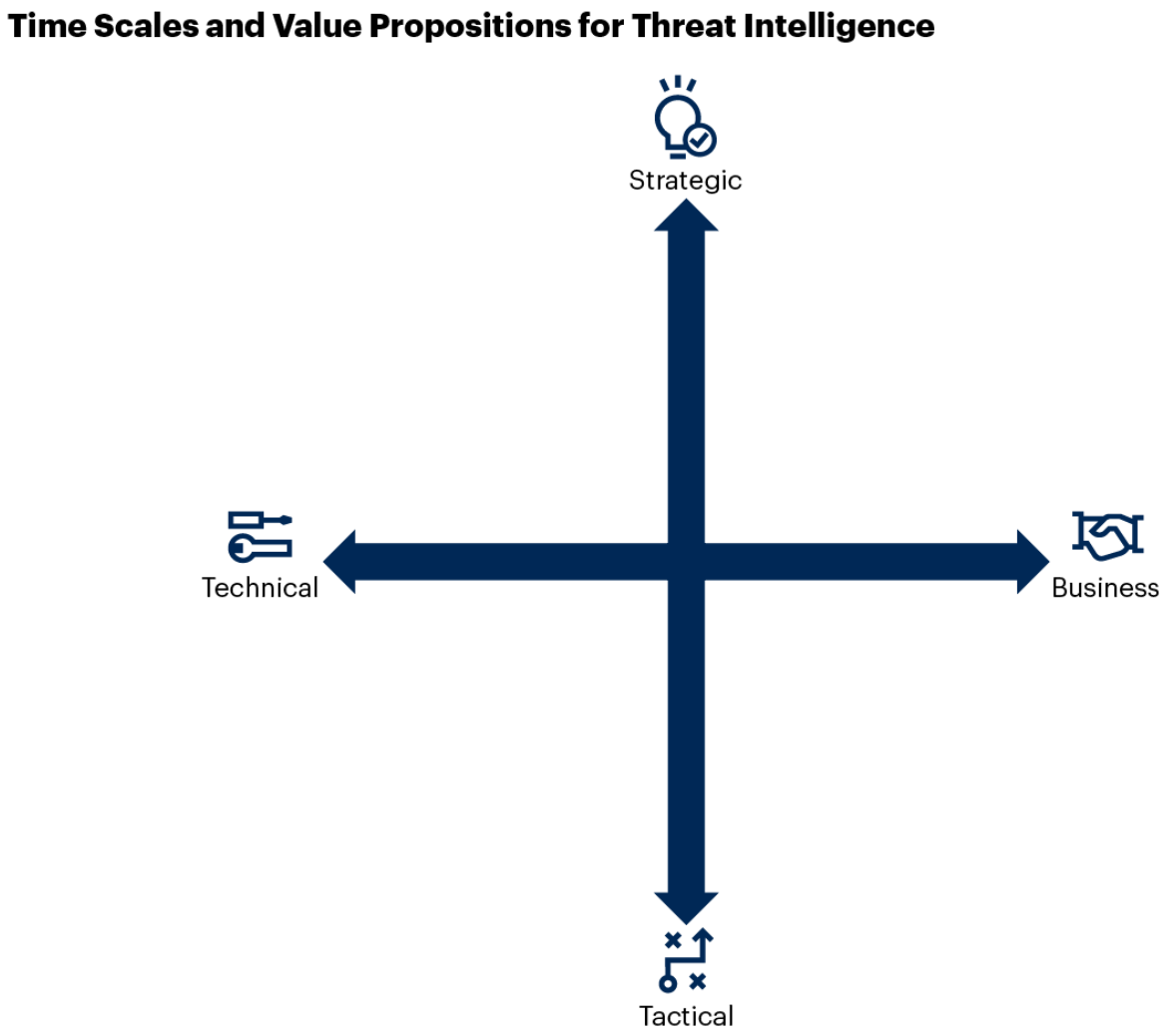


Source: Gartner
720431_C

Figure 3 depicts a simple way to consider how TI services can add value to your security program. As it shows, TI can be a combination of:

- **Tactical or strategic** — In terms of its area of your security program you are looking to address, which roughly aligns with "time." How long in the future or the near past is this form of TI?
- **Technical or business** — In general terms, applies to whether the TI is more focused on security operations or risk management.

Figure 3. Time Scales and Value Propositions for Threat Intelligence



Source: Gartner
720431_C

There is no one “right” choice here. Depending on your use-case needs and maturity, you could decide to use only tactical/technical TI at this point. However, in general, strategic/business TI is more expensive than technical/tactical services. We are seeing TI being used strategically by CISOs now and not just service SOC types of use cases.

Nor is there one right method. You may have security operations that can benefit from tactical/technical TI, such as high-delta updates for malicious domain names. Risk-management-focused people might want technical TI, but more of a business focus (supply chain ratings). Other people may want more business-focused, strategic TI, which could relate to markets and geographies. This can all be consumed by the same organization, but often by different personas.

Below, in no particular order, is a list of popular use cases for TI that Gartner sees from its inquiries with end-user organizations.

Capture and Leverage What You Create

A long underrated capability is for organizations to make use of the TI they see and are creating themselves. This is often a good place to begin investing your time. Organizations are often capturing novel threat intelligence themselves. You don't have to have a TI service to start. Things like malware sandboxes and other technologies like deception technology are all generating useful threat intelligence.

Example No. 1: The telemetry from your ATD (or sandbox) solution, say Lastline or FireEye, discovers an advanced piece of malware. This solution delivers very detailed telemetry on this threat with a full breakdown on files, registry keys, IP addresses, domain names, file hashes and threat persistence details. You can then use this intelligence for a full and rapid investigation of if/when/where this threat has made it into your environment.

Example No. 2: A deception technology (see "Improve Your Threat Detection Function With Deception Technologies" and "Solution Comparison for Six Threat Deception Platforms") is deployed to lay traps throughout your organization, looking for threats to trip over them. Things like honey tokens and fake servers and services are typical deployment options. When an alert is triggered, you then have information on an active threat in your environment, in a similar form to example No. 1 above. This rapidly improves your ability to perform accurate and timely incident response.

Security Technology Telemetry Enrichment

A good starting point in any program is to improve the things you already have. Earlier MRTI research (see "Innovation Insight for Machine-Readable Threat Intelligence") showed that MRTI is now available, sometimes as an add-on subscription, to a large number of security technologies. Credible examples include SIEM, firewalls, IDPS systems, SWGs, endpoint detection and response (EDR) and newer extended detection and response (XDR) technologies (see "Innovation Insight for Extended Detection and Response"). Vendors have been using TI extensively for some time now in their research teams and back ends to deliver better security content.

Others offer extensions to existing content via intelligence or reputation feed add-on subscriptions. These are recommended because they are often an affordable extension to products/services, so there's no need to deploy more technology, and because they are used to improve blocking and detection capabilities for the solutions you've already deployed.

Example No. 1: The Digital Shadows app for Splunk's SIEM integration for maintaining threat and alert watchlists (most vendors include them) have existing logs flowing in from existing SIEMs and EDR products. TI data is overlaid on top of existing logs to detect threats by matching indicators of compromise (IOCs), such as IP addresses, file hash and domain names.

Example No. 2: Trend Micro's Reputation Digital Vaccine (DV) for its TippingPoint IPS system. TI has been a boon for IPS, and many clients report improved detection and blocking capabilities for a range of threats simply by enabling the intelligence subscription for their IDP systems.

Example No. 3: Perch Security's managed threat intelligence service that takes multiple sources of TI, aggregates and delivers that into on-premises appliances and can offer a managed service around how the solution is run and managed.

Example No. 4: EclecticIQ's Fusion Center. Its TIP is configured with help from bundled TI integrations that include numerous feeds tailored and preintegrated for your specific organization and industry vertical. It can, at any time, change the mix of TI going into the TIP platform, without having to sign a plethora of agreements with other TI providers. This means that the downstream integrations and the use of TI in technology (such as SIEM and EDR) and in processes (such as incident response) are more effective.

Example No 5: Threat intelligence gateways (TIGs) take large amounts of MRTI from multiple sources, then prepackage and integrate it into a turnkey-like appliance that can be used to augment existing network security solutions.

Example No. 6: Recorded Future's Fusion feature allows you to nominate other TI sources you want and have Recorded Future aggregate this together and deliver it to you via its existing integration options, reducing the need for a fully featured SOAR/TIP solution.

Example No. 7: Anomali Lens is a plug-in that allows for very useful TI enrichment to happen when viewing any content (structured or otherwise) in a browser. It connects back to your TIP in real time to present threat context from your own current and historical data. It also supports the MITRE ATT&CK framework in how IOCs are visualized back to its users.

Sample Threat Intelligence Gateway Vendors: Bandura Cyber, Centripetal Networks, Gigamon, Ixia, LookingGlass Cyber Solutions, PacketViper, Perch Security, RiskAnalytics

Phishing Detection

Phishing is a pernicious and prevalent threat that remains an effective way to gain access to organizations' resources. TI can help identify elements of phishing campaigns to speed up detection/response actions and help with proactive measures, such as prevention/prediction.

Example No. 1: User-initiated. In this example, a user suspects an email and sends it to a monitored/shared email address for the company (such as security@example.com). Technologies such as TIP or security automation and orchestration (SAO) can take that email and perform enrichment and levels of automated investigation on its content without analyst intervention, drastically improving the context around this potential threat. Items such as domain name, email header, URLs and attachments can be investigated automatically, with TI enhancing the ability to respond. The analyst is then presented with the outcome of this investigation, including:

- This domain is known to deliver phishing content, via lookups on services such as DomainTools and VirusTotal.

- The provider for this domain is known to be a bulletproof hosting ISP, regularly hosting malicious domains and content.
- The text and structure of the message is similar to other phishing attempts by certain threat actors or against certain types of organizations that you may have seen before.
- Attachments were sent to a malware sandbox for inspection, and here is the outcome of the inspection of the binary or PDF file. If it proves to be malicious, then the indicators can be added to a threat library for use in other tools and processes.
- The URL was investigated and shown to have only been created one hour ago. It is linked to other previous phishing activity from the ISP, domain name registrant.

From here, an organization can take action, sometimes automatically on this process. It can remove the email from the user's inbox, searching for it in others and also removing it. It can scan the SIEM, looking for activity of the URLs used in the phishing attempt to check for prior activity during the past 90 days. It can then block the URL from being accessed on the SWG and DNS services.

Sample Vendors: EclecticIQ, Palo Alto XSOAR (formerly Demisto), ServiceNow, Siemplify, Splunk (Phantom), Swimlane, ThreatConnect and ThreatQuotient are vendors that pull together TI and leverage it for this use case.

Example No. 2: Community-initiated. In this example, an organization is participating in consuming commercial, open-source or industry-led sharing TI. A new phishing threat is identified by the service/community and forwarded into the sharing network. This then follows roughly the same flow listed in Example No. 1 above.

Sample Vendors: Area 1 Security, DomainTools, PhishLabs, Cofense and RiskIQ.

Threat Hunting

While it takes advantage of threat intelligence to identify nefarious activity, threat hunting is a tremendous source of intelligence as a stand-alone method (see "How to Hunt for Security Threats"). Tactics, techniques and procedures (TTPs) are often harvested via threat-hunting engagements, whether executed by internal resources or outsourced to a vendor that specializes in threat hunting. TTPs go beyond signature detection by using a combination of endpoint (EDR/EPP), network traffic analysis (NTA) and retained log analysis. Tactical indicators are leveraged for signature-based detections, but these are easily modified by threat actors to avoid detection in their future engagements. TTPs are more painful for threat actors to change because this involves creating an overall playbook for them to execute. For example, threat hunting can determine that a threat actor leveraged a spear phishing campaign directed at a target's HR staff, directing them to change their Active Directory password on the company's Outlook Web Access (OWA) website. The OWA site is a fake recreation designed to harvest username and password from victims, which are used for access

by the threat actor. Once the threat actor has access using an authorized user account, they create more accounts, dump credential hashes until they find a domain admin account and then install numerous persistence mechanisms throughout the environment. None of what was just described involved any malware and relied heavily on native operating system functionality, which is extremely hard or even impossible to detect with signature-based methods. This is where threat hunting excels at collecting and detecting TTPs of threat actors in future engagements. It is critical for organizations to share their findings to help other organizations disrupt ongoing or future attacks.

It is imperative for internal threat hunting programs to plan how TTPs and tactical indicators will be harvested, operationalized and maintained through the intelligence life cycle. Deciding to outsource threat hunting operations also requires careful collection planning to ensure the hunting service delivers findings so it can be operationalized.

It is also worth noting that the majority of managed detection and response vendors support threat hunting use cases for their clients.

Sample Endpoint Vendors: CrowdStrike, Kaspersky, SentinelOne, VMware (Carbon Black).

Sample Network Vendors: Corelight, ExtraHop, Vectra, Verizon (ProtectWise).

Sample Threat Hunting Platforms: Devo, Elastic, Exabeam, Splunk.

Sample Threat Hunting Service Providers: CrowdStrike, Secureworks.

Vulnerability Prioritization

In our updated vulnerability management methodology, "Implement a Risk-Based Approach to Vulnerability Management," we established that only roughly one-eighth of all vulnerabilities in the past decade were actually exploited in the wild. These vulnerabilities are heavily reused and leveraged in a wide range of threats, such as remote access trojans (RATs) and ransomware. The Common Vulnerabilities and Exposures (CVE) naming and Common Vulnerability Scoring Systems (CVSSs) are excellent to have and are critical for initial classification, and they also allow for analytics over long time scales. However, threat actors are under no obligation to obey the scoring methodologies that organizations use. TI integrations are enabling insight on which vulnerabilities are being leveraged by threat actors and is arguably one of the best use cases in modern enterprises for threat intelligence. This quantifiable knowledge provides key insight in the understanding of what an organization's threat landscape actually looks like.

Some traditional vulnerability assessment tools have this capability now. However, it has been led by smaller pure-play vulnerability prioritization technology (VPT) vendors. These vendors take vulnerability assessment telemetry and then leverage OEM TI (Risk Based Security and Recorded Future being popular choices), to allow for the application of novel advanced analytics to provide a

threat-landscape-centric view of this information presented in the context of your organization. Analysts are then presented with:

- A better prioritization of how to address vulnerabilities in their environments via remediation (for example, patching) and/or mitigation (for example, compensating controls like virtual patching)
- An understanding of what adversaries' TTPs would actually look like

Sample Vendors: HelpSystems (Core Security), Exodus Intelligence, Flexera, IBM QRadar, Kenna Security, NopSec, RiskSense, Qualys, Rapid7, RedSeal, Resolver (RiskVision), Risk Based Security, Skybox Security, Tenable, vFeed.

Surface, "Deep" and "Dark" Web Monitoring

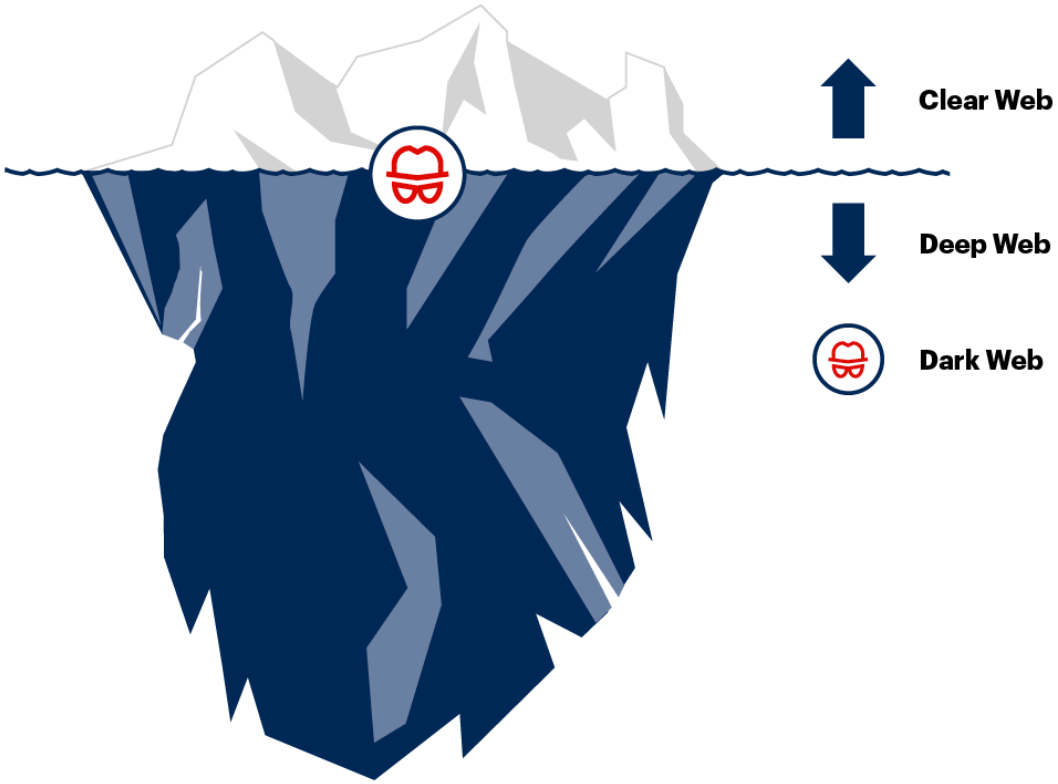
The definition of the deep/dark web can be confusing and, from interactions with Gartner clients, organizations are interested in at least understanding what it is.

The deep web is often the part of the internet that average users won't understand accessing (such as the onion router [ToR] or Invisible Internet Project [I2P] sites). However, they could do so if they were more technically savvy. This often provides a level of anonymity that can make attribution difficult. There is a lot of content available on the deep web, some of which relates to activities from threat actors.

The dark web can be on the surface (regular) internet or on the deep web (see Figure 4). However, it has the distinction of being run by threat actors that are actively policing the access and use of these forums and portals to prevent detection/infiltration by agencies, such as law enforcement and intelligence agencies.

Figure 4. The Different Types of Internet Sources Used for Intelligence Gathering

The Different Types of Internet Sources Used for Intelligence Gathering



Source: Gartner
720431_C

Like the general (surface) internet, deep and dark websites can have their own risks of compromise to users who navigate them. Extra precautions are strongly advised for end users looking to investigate these kinds of sites. A value proposition of TI services is that they do this on an organization's behalf. Getting at this information involves more than building repositories or data lakes to store copies of it all. It takes many years of experience in tradecraft to be able to actively infiltrate these kinds of underground information exchanges. These analysts will not be commoditized for the next decade. Their skills are rare and highly valued, and it often takes years of work to get to a practitioner level of skills.

Clients can use these services to get prior warning of threats, understand threats (how they work and where they're being seen), whether their organizations are being spoken about, and, in general, to understand threat actors in terms of their TTPs. TTPs can be used in proactive ways, so that things such as alerts can be set if:

- "A phishing template is being sold for my bank."
- "An exploit kit is now using the latest Adobe vulnerability to spread."
- "POS terminal malware that targets my manufacturer is now for sale in the underground."

- “Credentials for my organization have been stolen and are now for sale in the underground.”
- “There is intellectual property for my organization/agency that is now for sale or has been leaked to the internet that should not be there.”

Sample Vendors: Blueliv, CYFIRMA, DarkOwl, Digital Shadows, Flashpoint, IntSights, Kaspersky (see Note 2), KELA, LookingGlass Cyber Solutions, Recorded Future, Sixgill, SOCRadar, Terbium Labs, Webhose.io.

TI Analyst Augmentation

Some services provide dedicated or part-time access to TI analysts for your security program. This is a relatively new role for most security organizations. Only the highest 1% of organizations have either a role or responsibilities listed for other employees in their teams. There is also an acute shortage of these people in the employment market. Some intelligence providers, via tailored services, effectively let you “rent a slice” of their threat analysts. They can be tasked with specific TI-related tasks that directly focus on your organization.

Sample vendors: Digital Shadows, FireEye, Flashpoint, IBM, Intel 471, Secureworks.

TI Sharing

It is now well-understood, but not particularly visible publicly that TI sharing networks have real value for security programs. Some ISACs (such as FS-ISAC) have been very successful at building sharing networks that considerably enhance the visibility of prevailing threats that then provides opportunities for the prevention and detection of threats. In addition, several governments are advocating the sharing of threat data to both government and commercial organizations. Gartner recommends that all organizations, regardless of industry vertical, that are looking at using TI in their security programs, investigate the options they have for participating in this kind of capability. It is often advisable to use technology, such as TIP, to aid this capability.

The Traffic Light Protocol (TLP) is a standards-based approach that is further facilitating the sharing of information. The TLP defines ways to mark and classify information, so that it is appropriate for various audiences.

Sample Vendors: Analyst Platform, Anomali, Cyware Labs, EclecticIQ, IntSights, MISP, Sixgill, ServiceNow, ThreatConnect, ThreatQuotient, TruSTAR.

Threat Actor Tracking

This approach is the entry into threat modeling to understand the who, what, why and how. Formally, this defines the Diamond Model, which organizations leverage to determine attribution based on historical “battles” via incident response or threat hunting eviction engagements with a threat actor

group. Additionally, it is important to corroborate intelligence and findings with peers in the intelligence community to validate the identification of a threat actor. The MITRE ATT&CK framework provides an industry-recognized repository of threat actor TTPs based on intelligence collection by various organizations that track threat actors. This has presented a problem for the industry because there is no standard naming convention for threat actor groups, and there is no single “Rosetta Stone” to align the various naming standards for various threat actor groups.

Although recognizing the physical identification of perpetrators remains a significant challenge, they do regularly leave behind digital artifacts of themselves that can be tracked and followed via their various personas. Their digital exhaust, called TTPs in cybersecurity parlance, leave behind traceable elements.

This is arguably one of the most-advanced TI use cases because it often requires an expensive list of staffing and technologies invested over a long time. However, it can produce large benefits because, once you establish and have the TTPs correlated, actors’ behaviors appear and are often repeated. This is where TI can be proactive. TI can be used to get notifications on things such as an exploit for a vulnerability being for sale, malware purpose-built to target POS terminals or domain names being registered that are almost certainly for phishing attacks. One rhetorical question to ask here is, “Who are the top 20 threat actor/actor groups that aim to disrupt my digital business?”

Sample Vendors: Blueliv, CrowdStrike, Digital Shadows, FireEye, Flashpoint, Intel 471, Kaspersky (see Note 2), Secureworks.

Intelligence Analyst Investigations Tools

One nontrival thing that often goes unnoticed in the area of TI is the use of specialized tools that analysts rely on day to day. These tools are used extensively by intelligence analysts, security operations, threat hunters, incident response and forensic professionals.

These types of tools continue to prove their worth in delivering intelligence in useful ways to organizations’ security programs. They enable tasks such as:

- Allowing secure and anonymous access to the internet for research.
- Providing the hosting of virtual desktops with prebuilt tooling and other persona attributes, such as languages.
- Support the use of ephemeral assets that can be used for investigations and leave no meaningful artifacts for investigators, should they themselves be compromised. There is a high risk of this happening in cases where infiltration to deep/dark web locations is being attempted.
- Visualization of the large datasets for better human pattern matching and analysis.
- Support for team-based investigations.

- Support for doing extensive OSINT types of investigations and the stitching together of various types of data (breadcrumbs) to paint a better picture of a threat or threat actors.

Sample Vendors: Amazon Detective, Analyst Platform, Anomali, CounterCraft, Dispel, King & Union, IBM i2, Paterva's Maltego, Authentic8's Silo Research Toolbox, Sixgill, ThreatConnect, ThreatQuotient.

Adversarial Misinformation Campaigns

An emerging use case is the ability of threat actors of various levels of sophistication to conduct misinformation campaigns for profit/damage to end-user organizations. Analysis of several misinformation campaigns have demonstrated a pattern or method that threat actors use to profit from or damage organizations. This attack method can be mapped to the Adversarial Misinformation and Influence Tactics and Techniques (AMITT) framework, loosely based on the MITRE ATT&CK framework. AMITT is a development that is addressing the intersection of cybersecurity and online misinformation campaigns and their components by using familiar methods of describing threats, like the MITRE ATT&CK framework, and extensions to standards like STIX to allow organizations to operationalize a response to these threats (see "How Disinformation-as-a-Service Affects You" and "3 Key Trends for Information Security in 2020").

Sample Vendors: Unisys, FireEye.

Representative Vendors

Market Introduction

A list of credible vendors is provided below (see Table 1). It is not, nor is it intended to be, a complete list of all vendors or offerings on the market or a competitive analysis of the vendors' features and functions. In addition, providers below can often provide multiple TI-related services/products. This is also not a definitive list of each provider's services.

Because of the sheer number of vendors in this market, we have broken up the offerings into three primary buckets around where we see commonalities of how end users "acquire," "aggregate" and "action" threat intelligence (see Figures 5 and 6).

Figure 5. The Three Things to Do Well Concurrently to Get Value From Threat Intelligence

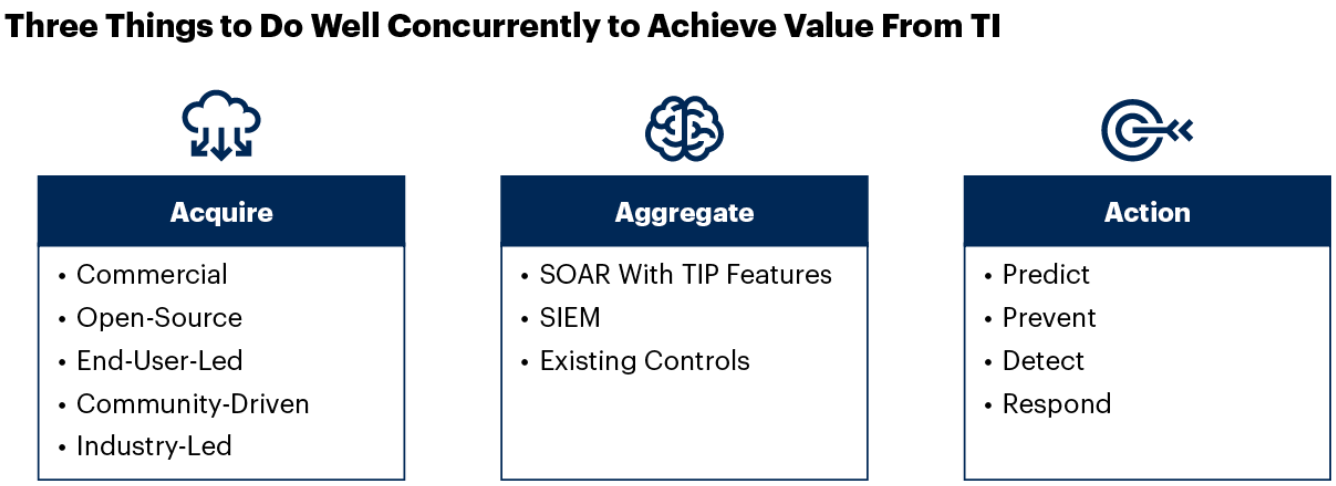


Figure 6. High-Level Items to Take Into Account When Considering Threat Intelligence

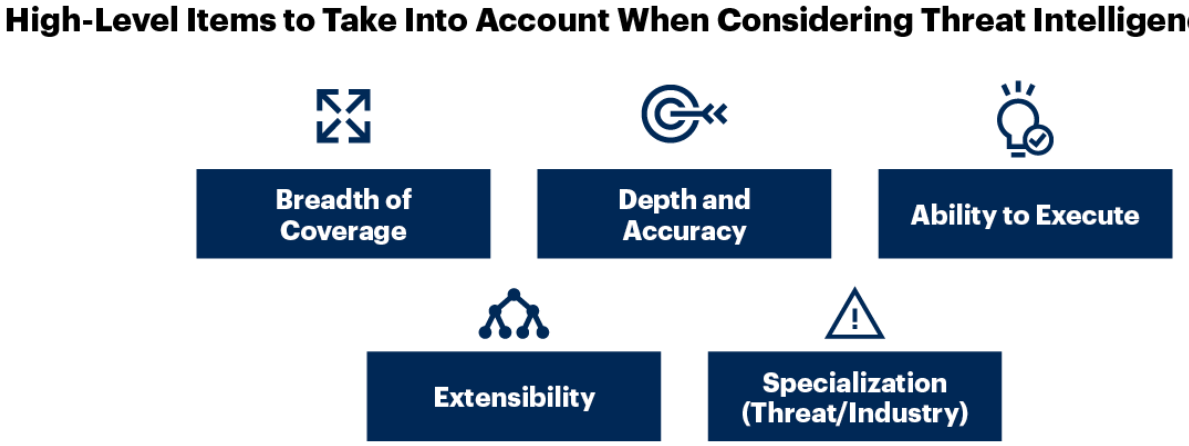


Table 1: Threat Intelligence Services Primarily for Acquisition and/or Aggregation

Example Use Cases	*Provider Name*	*Service*
TIP	Analyst Platform	illuminate
TI and TIP	Anomali	Anomali ThreatStream, Match, Lens+

Example Use Cases	*Provider Name*	*Service*
TIG	Bandura Cyber	Bandura Cyber Threat Intelligence Protection platform
TI and TIP	Blueliv	Threat Compass
TIG	Centripetal Networks	CleanINTERNET
TI	Cofense	Cofense Intelligence
TI	CrowdStrike	Falcon X
TI	Cyberint	Cyberint Cyber Intelligence Suite
TI and TIP	Cyware Labs	Cyber Fusion Suite, Cyware Threat Intelligence eXchange (CTIX)
TI	DarkOwl	DarkOwl
TI	Digital Shadows	SearchLight
TI	DomainTools	Iris Investigation Platform, Domain Risk Score
TI and TIP	EclecticIQ	EclecticIQ Platform, EclecticIQ Fusion Center
TI	FireEye	Threat Intelligence Subscriptions, Intelligence Capability Development, Digital Threat Monitoring
TI	Flashpoint	Flashpoint Intelligence Platform, Flashpoint Alerting
TI	VirusTotal (Google)	VirusTotal

Example Use Cases	*Provider Name*	*Service*
TI	Group-IB	Group-IB Threat Intelligence
TI	IBM Security	IBM QRadar Vulnerability Manager, IBM X-Force Incident Response and Intelligence Services (IRIS), IBM X-Force Exchange
TI	Intel 471	Adversary Intelligence, Malware Intelligence
TI and TIP	IntSights	Threat Command, Threat Intelligence Platform, Vulnerability Risk Analyzer, Threat Third Party
TI	Kaspersky (see Note 2)	Kaspersky Threat Intelligence
TI	KELA	RADARK, DARKBEAST, Intelligence SOC
TI and TIP	LookingGlass Cyber Solutions	scoutPRIME, scoutSHIELD, scoutTHREAT, Managed Threat Intelligence
TI	National Council of ISACs	Information Sharing and Analysis Centers (ISACs)
TI and TIP	NSFOCUS	NSFOCUS Global Threat Intelligence, NSFOCUS Security Labs, NTIP
TI	Palo Alto Networks	Cortex XSOAR (formerly Demisto), AutoFocus, Unit 42
TI	PhishLabs	Phishing Threat Indicator Feed, Digital Risk Protection
TI	Proofpoint	Emerging Threats Intelligence
TI	Recorded Future	Recorded Future for Threat Intelligence, Threat Intelligence Platform

Example Use Cases	*Provider Name*	*Service*
TI	ReversingLabs	Explainable Threat Intelligence
TI	RiskIQ	Illuminate, RiskIQ Security Intelligence Services
TI	Secureworks	Attacker Database, Countermeasures, Enterprise Brand Surveillance, Global Threat Intelligence,Threat Intelligence Support
TI	Sixgill	Deep and Dark Web Threat Intelligence Platform, Darkfeed
TI	Team Cymru	Threat Intelligence Feeds, Augury, Enterprise Intelligence Service
TI and TIP	ThreatBook	ThreatBook Threat Intelligence Management Platform
TIP	ThreatConnect	ThreatConnect's Threat Intelligence Platform
TIP	ThreatQuotient	ThreatQ
TIP	TruSTAR	TruStar Intelligence Platform
TI	ZeroFOX	ZeroFOX Intelligence Services, ZeroFOX Alpha Team

This table covers the Acquire and Aggregate functions of representative product/services

Source: Gartner (May 2020)

Action

The ability to take action on received threat intelligence is critical and can be embedded in the product or service itself. TI can also be augmented by the above two categories of TI services and products if they support open-source standards, such as STIX/TAXII, or support the use of APIs within their own ecosystem. A significant point of the threat intelligence market is that MRTI is now in most security products on the market, including firewalls (see "Magic Quadrant for Network

Firewalls"), IDPS (see "Market Guide for Intrusion Detection and Prevention Systems"), NTA (see "Market Guide for Network Traffic Analysis"), EPP (see "Market Guide for Endpoint Detection and Response Solutions"), EDR (see "Market Guide for Endpoint Detection and Response Solutions"), SIEM (see "Magic Quadrant for Security Information and Event Management"), SWGs (see "Magic Quadrant for Secure Web Gateways"), vulnerability assessment (see "Market Guide for Vulnerability Assessment"), XDR (see "Innovation Insight for Extended Detection and Response"), deception technologies, DNS security, and cloud access security brokers (CASBs) (see "Magic Quadrant for Cloud Access Security Brokers"), to name a few. Security services are also delivering flavors of TI embedded into them. Markets such as MSSP (see "Magic Quadrant for Managed Security Services, Worldwide") and managed detection and response (MDR) (see "Market Guide for Managed Detection and Response Services") are prime examples.

All of the above listings are representative and do not represent the entire TI market. Gartner is tracking more than 100 vendors in this market with vendors that have various threat intelligence capabilities. Providers often deliver capabilities from more than one of the three basic categories (acquire, aggregate, action) groups, but are only listed in one above.

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Recommendations

Before purchasing a service, have a detailed plan for how you will use it and start with an end in mind. Understand who and what tools/processes consume it and how they will use it. Also understand what decisions you expect to make on the basis of the content provided, as well as "who" and "how" those decisions will be made.

Pricing models are becoming more consistent across the market. In general, though, an end-user organization can expect to pay in the lower tens of thousands of dollars for a basic service that includes tactical content, such as IP reputation feeds, risky URLs and indicators of compromise. More advanced strategic content — which includes information about actors' motives, intentions, and capabilities developed or tailored for the individual client — can cost several hundreds of thousands of dollars or more.

There are still a large number of providers in the market, and the number appears to be growing. Not all services that are marketed as TI actually provide that type of content, so it is important to understand what problem you are trying to solve. For example, are you interested in vulnerability information? This is not TI. However, if you are trying to find out what your adversaries are doing or even planning (for example, what vulnerabilities are being exploited) and want to find out without drawing attention to yourself, then a TI service may be valuable.

Included earlier in this research are numerous other intelligence methodologies (such as the Diamond Model) that describe processes around the generation, gathering and processing of TI.

From many hundreds of Gartner inquiries, we have boiled this down to three things that end users must do, concurrently well, to derive benefits from TI. These can be broadly grouped into acquiring, aggregating and actioning TI.

Acquire

Historically, and for some time to come too, we believe there will be no single TI service that will deliver everything. There is still a significant number of vendors in this market, with more entering or offering various services that are specialized, normally in different domains in terms of what part of the threat landscape they cover. For example, some are proficient at malware IOCs, internet domain information, social media monitoring or dark/deep-web monitoring, but it is rare to find one that is excellent across all these domains.

Once they start looking at TI, most organizations quickly find no shortage of TI available in various forms. The ideal is to arrive at the right "blend" for your organization. You could have budget constraints and/or only need to address certain threats or problems. Figure 6 describes, at a high level, how to tackle the thought process and selection of a TI provider for your organization. Although there are likely to be other criteria, five attributes can help you understand market offerings, as well as how to make better selections for your organization.

Breadth of Coverage

What areas of the threat landscape, what use cases can the provider deliver and in what form factors (MRTI, reports or threat analyst access)? For example:

- What threats do they cover?
- Are they focused on phishing, malware, deep/dark web, social media?

All of these are, to a large degree, disciplines in their own right.

Depth and Accuracy

Just as important as how much information is available is how that information can be specifically targeted for you. Concurrently, having a high level of action-oriented fidelity is important. Some flavors of TI can age out in time frames measured in hours.

Ability to Execute

How long has the provider been in the market? How viable is it? If its client base doubles, could it service you with the same level of satisfaction? Is it financially viable?

Extensibility

Are you able to use the TI in multiple ways, for different processes and within a range of tools? Some TI comes in a "black box," which can be described as single-purpose or single-use. If you want/need

to use TI in multiple tools and processes, having it available in ways and formats that support this is a must.

Specialization

Many TI providers are deep specialists in the specific areas and techniques they use to understand the threat landscape. Understanding this specialization is key. It will help you align provider capabilities with the perspective you need to address the risks for which you need assistance.

Aggregate

Once you receive multiple formats and types of TI in various volumes, you need to be able to gather it all together in one place and aggregate it. This involves such things as the deduplication of overlapping intelligence, enrichment, storage, sharing and downstream orchestration/automation use cases. The SOAR market is converging where TIPs are adding features of SIRP and SOA and vice versa. Where previously we have seen many clients deploy multiple tools (often TIP and SOA) to achieve SOAR, this need is being reduced by the ongoing convergence. Meaning only one tool is being required. They are still the most sophisticated examples of products that aggregate large volumes of TI for enrichment, normalization, deduplication, search, and usage in other tools and processes.

Action

Because there is so much TI, just knowing about something can be considered academic per se, if you aren't then taking this and "doing something" with the knowledge you have (see "How to Use Threat Intelligence for Security Monitoring and Incident Response"). This is still the biggest issue with adding intelligence-led initiatives to your cybersecurity program, as well as the biggest opportunity for security leaders if they can convert information into action. IT security leaders are advised to start with this end in mind. Define the problems you have or the information you lack, and use that to inform your decisions on the types of action you need to be able to take. Use that to decide what types of TI to "acquire" and how you will need to "aggregate" it to achieve your intelligence-led security initiatives.

Note 1
Representative Vendor Selection

The sample vendors listed in this publication are representative only, and each list is not intended to be exclusive or exhaustive. The vendors and solutions provided are those that most closely illustrate the marketplace trends described and provide the individual capabilities described in each section. Vendors are listed in alphabetical order only, and the overall list of representative vendors has been validated using Gartner's responses to client inquiries, gartner.com search statistics, as well as data from Gartner's Peer Insights website to ensure that the most frequently mentioned vendors/solutions are represented.

Additionally, due to the sheer size of sources and products/services in this market there remain interesting noncommercially focused services per se that are also relevant to this market.

Free TI Sources

abuse.ch

Critical Stack

Dshield

Malc0de

Malwaredomains.com

Proofpoint (Emerging Threats Intelligence)

SANS Institute

Shadowserver Foundation

HAILATAXII

CERTs

Most countries today have a national CERT of the same flavor, and a number of them have services that include TI feeds and/or related services (see "Computer Security Incident Response Teams," Software Engineering Institute (SEI)" for a list of CERTs).

ISACs and Others

FIRST

Financial Services Information Sharing and Analysis Center (FS-ISAC) and other ISACs (see "Market Guide for Security Threat Intelligence Products and Services").

Note 2
Kaspersky

In September 2017, the U.S. government ordered all federal agencies to remove Kaspersky's software from their systems. Several media reports, citing unnamed intelligence sources, made additional claims. Gartner is unaware of any evidence brought forward in this matter. At the same time, Kaspersky's initial complaints have been dismissed by a U.S. District of Columbia court.

Kaspersky has launched a transparency center in Zurich where trusted stakeholders can inspect and evaluate product internals. Kaspersky has also committed to store and process customer data in Zurich, Switzerland. Gartner clients, especially those who work closely with U.S. federal agencies,

should consider this information in their risk analysis and continue to monitor this situation for updates.

Note 3
Gartner's Initial Market Coverage

This Market Guide provides Gartner's coverage of the threat intelligence market and focuses on the market definition, rationale for the market, productive end-user use cases and market dynamics.