Market Guide for Security Threat Intelligence Products and Services

12 August 2024 - ID G00794923 - 29 min read

By Analyst(s): Jonathan Nunez, Ruggero Contu, Mitchell Schneider

Initiatives:Security Operations; Build and Optimize Cybersecurity Programs; Meet Daily Cybersecurity Needs

Security and risk management leaders struggle to know what threats constitute real concerns for their organizations. They should use this research to select the right security threat intelligence products and services, and to understand and respond more efficiently to the threat landscape.

Overview

Key Findings

- The demand for threat intelligence (TI) products and services continues to increase across enterprises of various sizes and industry verticals, but many organizations still lack adequate focus and structure to make the best use of the TI they've chosen to consume, limiting its utility.
- As TI awareness becomes ubiquitous across the enterprise, a new cadre of stakeholders look to benefit from the foresight of what more targeted and nuanced intelligence can provide. New use cases are needed to address the disparate needs of the wider business that offer more value than a majority of current security products.
- Security operations leaders and business leaders alike demand a shift from reactive intelligence to also include proactive intelligence-led threat intervention. This new requirement stems from the need to avert business disruption by factoring the threat landscape in the "shift-left" movement.
- As the demand for TI increases, prospective buyers are focusing on innovations and advancements in an effort to differentiate from the large number of vendors in the marketplace.

Recommendations

Security and risk management (SRM) leaders responsible for security operations should:

- Establish priority intelligence requirements and use those as the foundation to develop a comprehensive target operating model for their TI operations. Through this new structure, employ the TI life cycle and measure its output for effectiveness.
- Focus on digital risk protection services, external attack surface management, threat hunting and threat exposure management as additional use cases that provide wider organizational benefit.
- Evaluate TI vendors who provide more than just indicators of compromise in an effort to deliver actionable, proactive insights. Some offerings to consider are indicators of attack, MITRE ATT&CK mapping, digital risk protection services (DRPS) or external attack surface management (EASM) enrichments and vetted information-sharing communities.
- Promote providers who invest in innovative TI capabilities, such as advanced analytics, generative AI (GenAI), crowdsourced intelligence and improved investigation portals to accelerate time to value.

Market Definition

The security threat intelligence products and services market refers to the combination of products and services that deliver knowledge (context, mechanisms, indicators, implications and action-oriented advice), information and data about cybersecurity threats, threat actors and other cybersecurity-related issues. The output of these products and services aims to provide or assist in the curation of information about the identities, motivations, characteristics and methods of threats, commonly referred to as tactics, techniques and procedures (TTPs). The intent is to enable better decision making and improve security technology capabilities to reduce the likelihood and impact of a potential compromise.

Threat intelligence (TI) products and services support the different stages of a TI process life cycle. In particular, this involves defining the aims and objectives, collecting and processing intelligence originating from various sources, analyzing and disseminating it to different stakeholders within the organization, and regularly providing feedback on the entire process. These products and services support ongoing security investigations and assist in preventing future breaches by prioritizing infrastructure hardening. TI tools and services are most commonly cloud-based products and services, but can also be delivered "as a service."

Mandatory Features

The mandatory features for services in this market include:

- Indicators of compromise (IoCs), including malicious or suspicious ratings, such as IP addresses, URLs, domains and file hashes.
- Direct technical intelligence collection or research, enabling the consumer to tailor collection or search functionality for relevant IoCs.
- Configuration of alerting thresholds based on predefined criteria.
- Machine-to-machine integrations to either push or pull intelligence artifacts through to multiple solutions.
- Out-of-the-box enrichments to IoCs, such as tentative attribution, geolocation data and registration information.
- An interactive user portal with built-in analysis functionalities such as contextualized dashboards, configurable alerting and search features.
- IOC scoring or risk rating as a way to illustrate confidence in maliciousness or suspiciousness.
- Investigative support options, which may include ad hoc requests-for-information, longer-term analysis or recurring analyst augmentation.

Common Features

The common features for this market include:

- TTP enrichment of IOCs, provided typically in two formats: threat actor profiles and MITRE ATT&CK enrichments.

- Malware sandboxing, providing the ability to dynamically extract IoCs from malware samples by detonating the malware in a provider (cloud or on-premises) sandbox.
- Vulnerability intelligence tailored for vulnerability prioritization, often highlighting actively exploited vulnerabilities and the associated IoCs.
- Finished intelligence reporting, including technical/tactical analysis reports as well as operational and strategic intelligence products.
- Visual representation of weighted connections between IOCs and threat actors
- Network telemetry enrichments such as passive DNS, sinkhole traffic and global sensor network telemetry.
- Industry-specific curation such as advanced search filters, industry-specific query parameters and dashboards.
- Built-in priority intelligence requirement curation.
- Metrics reporting tailored for operational governance.
- Forensic analysis support.
- Support for multi-format sharing methods across industry communities

Market Description

The security threat intelligence products and services market, otherwise known as the TI market, offers multiple solutions and services to help organizations understand and prepare for their own unique threat landscape and bolster their prevention and analytics capabilities. Such capabilities can also help them improve their other operational efforts such as threat detection, incident response, threat hunting and threat exposure management.

Core Capabilities

For end users to effectively utilize, security threat intelligence vendors must be able to technically deliver:

- Indicators of compromise (IOCs), including malicious or suspicious ratings, such as IP addresses, URLs, domains and file hashes.
- Direct technical intelligence collection or research, and enable the consumer to tailor collection or search functionality for relevant IOCs.

- Configure alerting thresholds based on predefined criteria.
- Support machine-to-machine integrations to either push or pull intelligence artifacts through to multiple solutions.
- Integrate or provide out-of-the-box enrichments to IOCs, such as tentative attribution, geolocation data and registration information.
- Provide an interactive user portal with built-in analysis functionalities such as contextualized dashboards, configurable alerting and search features.
- Provide IOC scoring or risk rating as a way to illustrate confidence in maliciousness or suspiciousness.
- Offer investigative support options which may include ad hoc requests for information, longer-term analysis or recurring analyst augmentation.

Optional Capabilities

The TI market offers feature-rich solutions that often have additional capabilities. Table 1 below includes a nonexhaustive list of optional TI capabilities seen in the marketplace.

Table 1: Optional TI Capabilities

(Enlarged table in Appendix)

Market segment	Optional features
Threat intelligence	■ Tactics, techniques and procedures (TTPs) enrichment of IOCs, provided typically in two formats: threat actor profiles and MITRE ATT&CK enrichments. ■ Malware sandboxing, providing the ability to dynamically extract IOCs from malware samples by detonating the malware in a provider (cloud or on-premises) sandbox. ■ Vulnerability intelligence tailored for vulnerability prioritization, often highlighting actively exploited vulnerabilities and the associated IOCs. ■ Finished intelligence reporting including technical/tactical analysis reports as well as operational and strategic intelligence products. ■ Node graph visualizations such as link-end analysis graphs and built-in Maltego Transforms. ■ Network telemetry enrichments such as passive DNS, sinkhole traffic and global sensor network telemetry. ■ Industry-specific curation such as advanced search filters, industry-specific query parameters, and dashboards. ■ Built-in priority intelligence requirement curation. ■ Metrics reporting tailored for operational governance. ■ Support with forensic analysis. ■ Vulnerability intelligence. ■ Supporting sharing across industry communities.
Threat intelligence, featuring DRPS	■ Third-party risk assessments, geared toward evaluating the risks associated with an entity's supply chain based on threat intelligence activity. ■ Domain abuse monitoring, typically for threats associated with customer domains, such as typosquatting and phishing. ■ Dark web services that monitor the deep and dark web for mentions related to the customer organization. Typical use cases are data leakage, fraud and threat actor attribution. ■ Social media monitoring for violation of social media policies, account takeover, VIP/executive protection and sentiment analysis. ■ Takedown services for the remediation of DRPS findings such as illicit domain/website removals and hijacked account revocations.
Threat intelligence, featuring EASM	■ Discovery of external, digital assets (on-premises and cloud) typically identifying Internet Protocol version 4 (IPv4) assets, web applications, domains and Secure Sockets Layer (SSL) certificates. ■ Enumeration of software vulnerabilities and security weaknesses for remediation prioritization, typically using discoverability and exploitability as factors for risk scoring. ■ TI attack surface enrichments, adding the relevant attributes associated with actively exploited vulnerabilities. ■ Support/advisory on remediation to exposures identified.

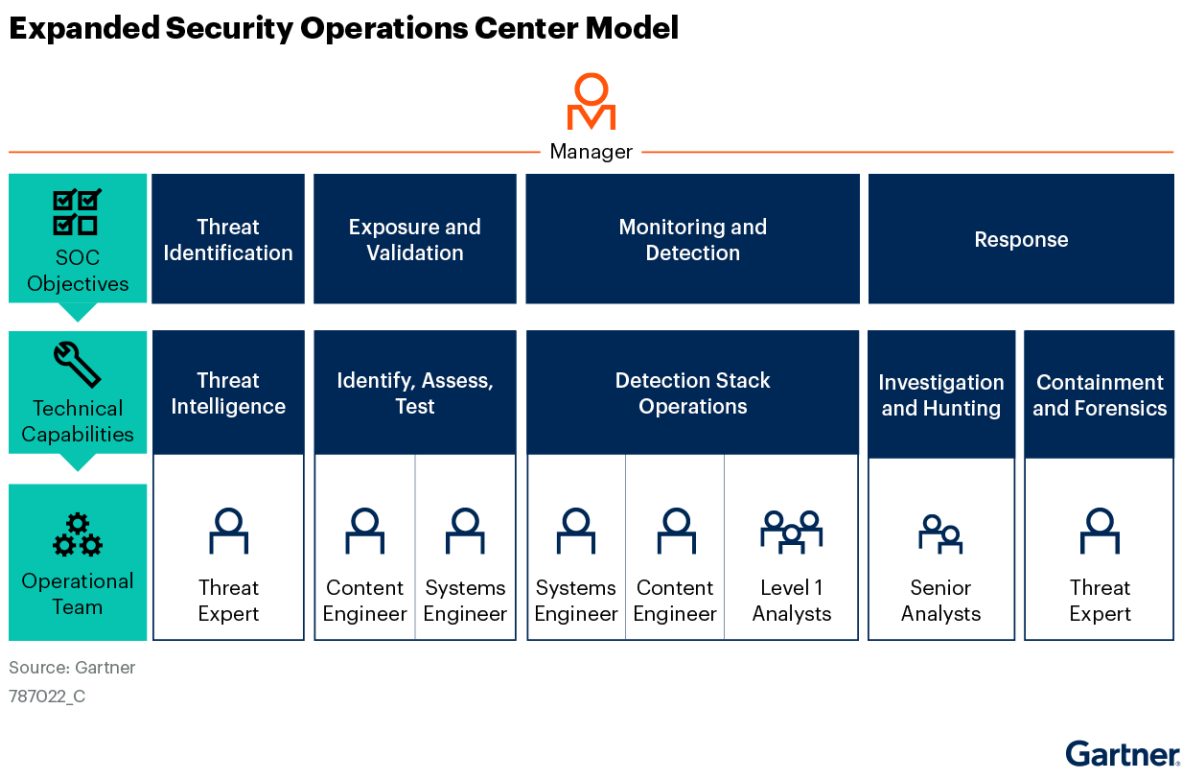
Source: Gartner (August 2024)

The security threat intelligence products and services market has a large number of vendors. Gartner monitors more than 100 of them from the commercial space alone, an approximate 20% increase from 2023. Clients will often have an overwhelming number of options to choose from (see Tool: Vendor Identification for Security Threat Intelligence Products and Services).

Market Direction

TI is a core function of a modern, expanded, security operations center (SOC) (see Figure 1). Security programs that underestimate the TI value or fail to properly operationalize TI will find it difficult to defend against imminent threats and anticipate potential future security impacts. Based on Gartner's 2Q24 forecast, global TI spending is expected to grow at an annual growth rate of 21.7% in 2024 with $4.6 billion expected spend by 2028 (see Forecast: Information Security, Worldwide, 2022-2028, 2Q24 Update).

Figure 1: Expanded SOC Model



Organizations continue to not only show interest in TI-led initiatives but also prioritize them, as evidenced by the SANS 2023 Cyberthreat Intelligence Survey, where 51% of the surveyed organizations staffed a dedicated in-house TI capability, a 14% increase from 2022 and the largest increase since 2020. [1]

Key Factors Driving Interest in the Security Threat Intelligence Products and Services Market

- Expanding end-user use cases
- Consolidation trend of vendors offering broadening ranges of use cases
- Innovation drives differentiation

Expanding Use Cases

As awareness of TI's value spreads across the organization, business leaders look to onboard new requirements and use cases where they may better utilize the actionable insights made possible by TI. See Table 2 for the top three use cases Gartner identified in end-user inquiries.

Table 2: Example Expanding Use Cases

(Enlarged table in Appendix)

Use case	Description	TI support	Benefit
Threat hunting	Proactively searching for evidence of compromise across organizational technology domains	Provides relevant TTPs/IOCs/IOAs including probable exploitation vectors based on threat landscape activities	▪ Can identify attacks that have evaded detection before significant business impact occurs ▪ Surfaces vulnerabilities and weaknesses that can pose material risk to the business before impact occurs
Threat detection, use case development	Building threat detection use cases, for the real-time detection of threats	Provides curated indicators of compromise, increasing the efficacy of alerting use cases	▪ Reduces false positives in detection use cases ▪ Increases speed of investigation, in turn reducing mean-time-to-detect metrics ▪ Assists in establishing attack severity at the point of alerting, allowing for better workload prioritization
Threat exposure management	Discovering, prioritizing and mobilizing resources to close or reduce risky exposures	Exposure assessment — Can identify which vulnerabilities across your digital estate are being, have been or will be exploited in the wild, and to what degree	▪ Can help prioritize actively exploitable vulnerabilities, driving down the number of findings requiring immediate fixes ▪ Can help proactively identify vulnerabilities at imminent risk
Threat exposure management	Validating exposures, testing security controls and mobilizing resources to close or reduce risky exposures	Adversarial exposure validation — Based on information collected about active attack campaigns and techniques, TI can identify what TTPs are likely to be used against your technology stack to compromise or immobilize your organization	Can help identify the threat actor attributes and artifacts most likely to impact your organization, resulting in more accurate and timely cybersecurity validation exercises and therefore higher priority and effective fix recommendations

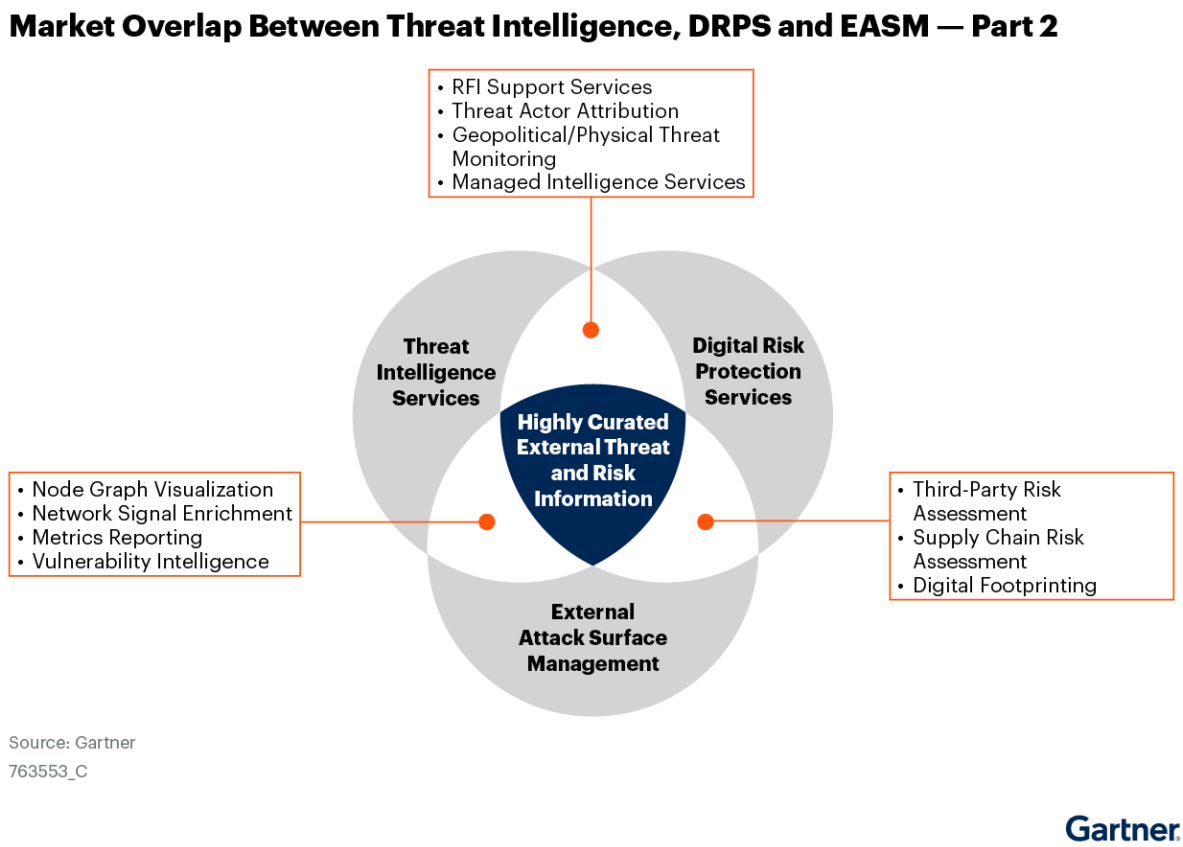
IOAs = Indicators of attack
IOCs = Indicators of compromise

Source: Gartner

Consolidation Upward Trend

According to Gartner's end-user inquiries, SRM leaders have shown a greater interest in consolidating TI services with DRPS and EASM, up from approximately 5% in 2022 to 35% in 2024. The TI vendor community has responded in kind with approximately 40% of all providers offering cross-domain products and services (see Figure 2). There are two notable reasons that contribute to this trend: ease of procurement and curation.

Figure 2: Market Overlap Between Threat Intelligence, DRPS and EASM — Part 2



Most organizations only have one procurement team that's charged with managing contract life cycle for all purchasing across all departments; as a result, SRM leaders find they are disproportionately engaged with procurement. This in turn creates a backlog, making buying tools and services complicated and drawn-out, especially if the buyer is required to make the bid competitive. Therefore, many TI buyers want to curtail as much of this burden as possible while sacrificing as little value as possible by aligning with a trusted provider for the multitude of use cases and requirements they might have.

Secondly, there is an ever-increasing demand for curated TI. End users have realigned their expectation of intelligence, they no longer want to be flooded with generic indicators, but instead want a curated set of indications they can focus on. Some of this is a result of recent budgetary constraints where organizations no longer have the internal resourcing to process vast amounts of intelligence, or a result of organizations not yet mature enough to have onboarded the requisite numbers of staff. Either way, the triangulation or correlation of TI, DRPS and EASM can produce substantially more accurate intelligence for the consuming organization, often tailored to their unique threat landscape.

Innovation Drives Differentiation

Much like in years passed, key differentiation among vendors is increasingly blurred, making it even more difficult for end users to appropriately assess as they venture down a cumbersome procurement journey. Many of these buyers are leading with questions regarding innovation, as therein lies the seeming key differentiation. The market has responded with a number of noteworthy advancements:

- GenAI
- Crowdsourced intelligence
- Advanced analytics
- Improved investigation portals
- Expansion in geophysical intelligence

While GenAI has been much of the hype in 2023 and into 2024, TI presents a low barrier to entry where use cases can easily be adopted for use by consumers and implemented quickly by providers. Some of these use cases or GenAI-enabled functions include automated enrichments, collection evaluation/gap analysis, priority intelligence requirement (PIR) generation and reporting. These GenAI uses enable faster scalability and better use of TI programs, products and services.

Other vendors have leveraged the power of crowdsourcing to collect prevetted indicators of compromise across a large spectrum of industries, geographies and organizational demographics. These providers not only benefit from receiving indicators from cyber defenders and incident responders in real time and globally, but they also benefit from a global ranking system where all users can rank or rate whether they benefited from particular indicators. Collectively, this can serve as a great way for the community of defenders to collaborate on establishing a reputable set of known bad IOCs. Historically, the ISACs have been a good representation of these communities. However today, many vendors have expanded on this notion by offering their own intelligence-sharing communities, leveraging the power of their collective technologies (sensors) and services (incident response, threat hunting and SOC analysts). For defenders, this additional source of TI can help reduce false positives while accelerating investigations.

“Shift left” has arrived in the TI marketplace. There is now a tranche of vendors branding improved diagnostics as “predictive intelligence.” This is intelligence that analyzes early signals of an adversary building infrastructure to support attacks or indicators of the organization being targeted (e.g., “dark web whispers”). Analyzing these signals’ findings can help refine priorities in exposure remediation workloads by enriching those exposure findings with exploitation probability which can be found in open sources (i.e., The Cybersecurity Infrastructure and Security Agency [CISA] known exploited vulnerabilities [KEV], Exploit Prediction Scoring System [EPSS]) or commercial sources. Some commercial providers have even coined new terms to describe these new types of early warning signals which are meant to indicate attacker intent.

Many of the veteran providers have invested in investigation portals, unlocking significant value in their services which in some cases were previously difficult to obtain. In a marketplace that has evolved to challenge threat intelligence platforms (TIPs) and security orchestration, automation and response (SOAR) solutions, these vendors aim to deliver highly actionable insights and speed up the investigative process by presenting their own, proprietary information in more consumable ways. These changes reflect a shift from working individual events to performing in-depth investigations supported by an investigative workflow. Vendors providing these updates have taken advantage of consolidating cross-domain offerings (TI, DRPS and EASM) into a singular platform for better correlation and enrichment, increasing the overall value of the three services for the customer. There have been five notable advancements in this area, see Table 3.

Finally, the need to assess threats arising from logical and physical convergence has driven a number of vendors to expand their capabilities to deliver geophysical/political intelligence. These capabilities will help enterprises monitor physical incidents and political or activist-related threats that can result in threats to executives, overall business or nation-states.

Table 3: 5 Advancements in High-Performing Investigation Platforms

(Enlarged table in Appendix)

Advancement	Features
Optimized graphical user interface	■ Faster searches ■ More native enrichments ■ Natural language processing ■ Enhanced tagging capabilities
Nodal network graphs	■ Native link-end analysis ■ In-depth relationship modeling
Case management	■ Investigator support ■ Historical archive ■ Annotation and artifact logs
Native integrations	■ API push, pull functionality ■ Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) compatibility
Reporting	■ On-demand report generation ■ Metrics dashboards ■ Watchlisting ■ News feeds

Source: Gartner

There have been several acquisitions in the TI marketplace by a mix of larger TI providers, managed security service providers, investment firms, telecommunication providers and others. This is a clear indication that TI continues to be a critical capability for all security and risk programs.

2023 saw several acquisitions in the TI market.

In the first and second quarters of 2023:

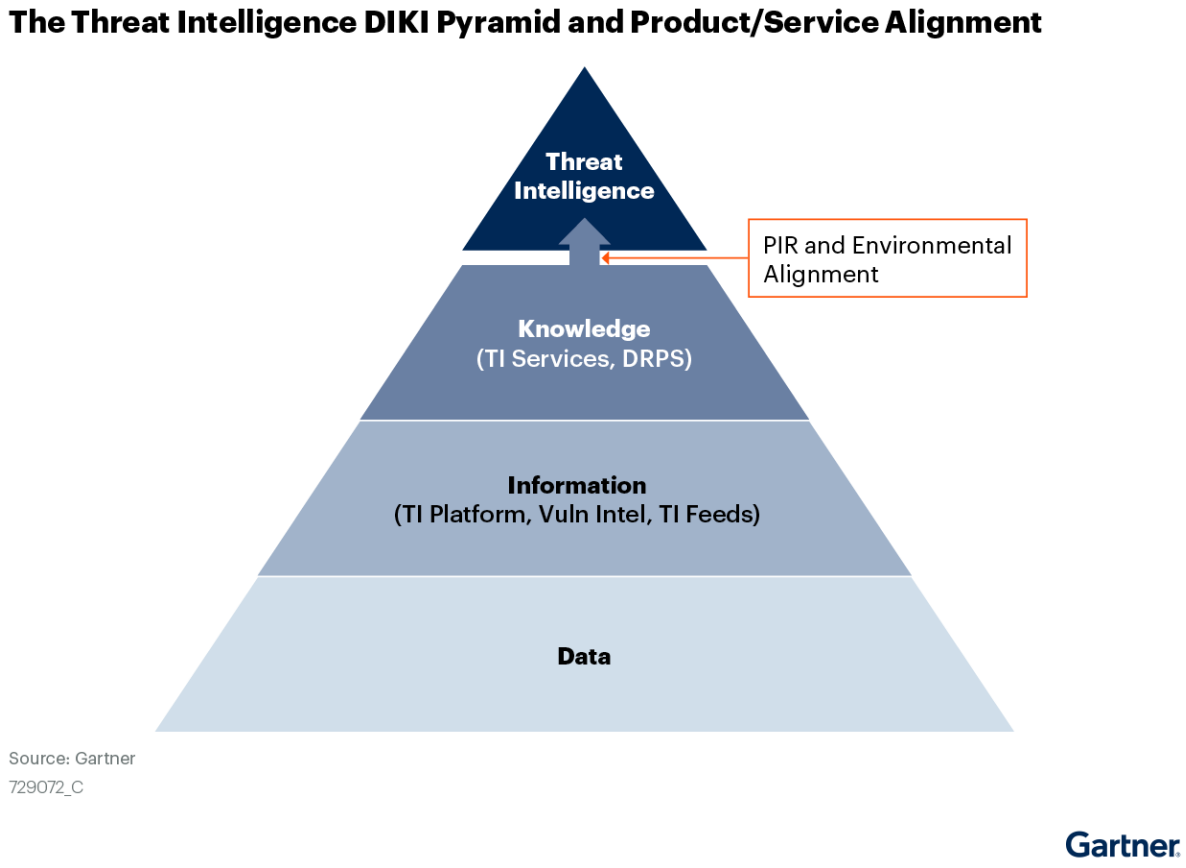
- ZeroFox acquires LookingGlass
- ReliaQuest acquires agent software assets and engineering team from EclecticIQ
- Group-IB finalized exit from Russia
- Accenture acquires Morphus
- Okta acquires Bad Packets
- Charlesbanks Capital Partners acquires Maltego
- Telsy acquires TS-Way
- Blattner Technologies acquires Jigsaw Security Enterprise

In the third and fourth quarters of 2022:

- Recorded Future acquires Hatching to extend Intelligence Cloud coverage with malware analysis
- Bastion Security Group acquires threat intelligence provider Cassini
- Netcraft acquires FraudWatch
- Zurich Holding Company acquires SpearTip
- Spire Capital acquires Cobwebs

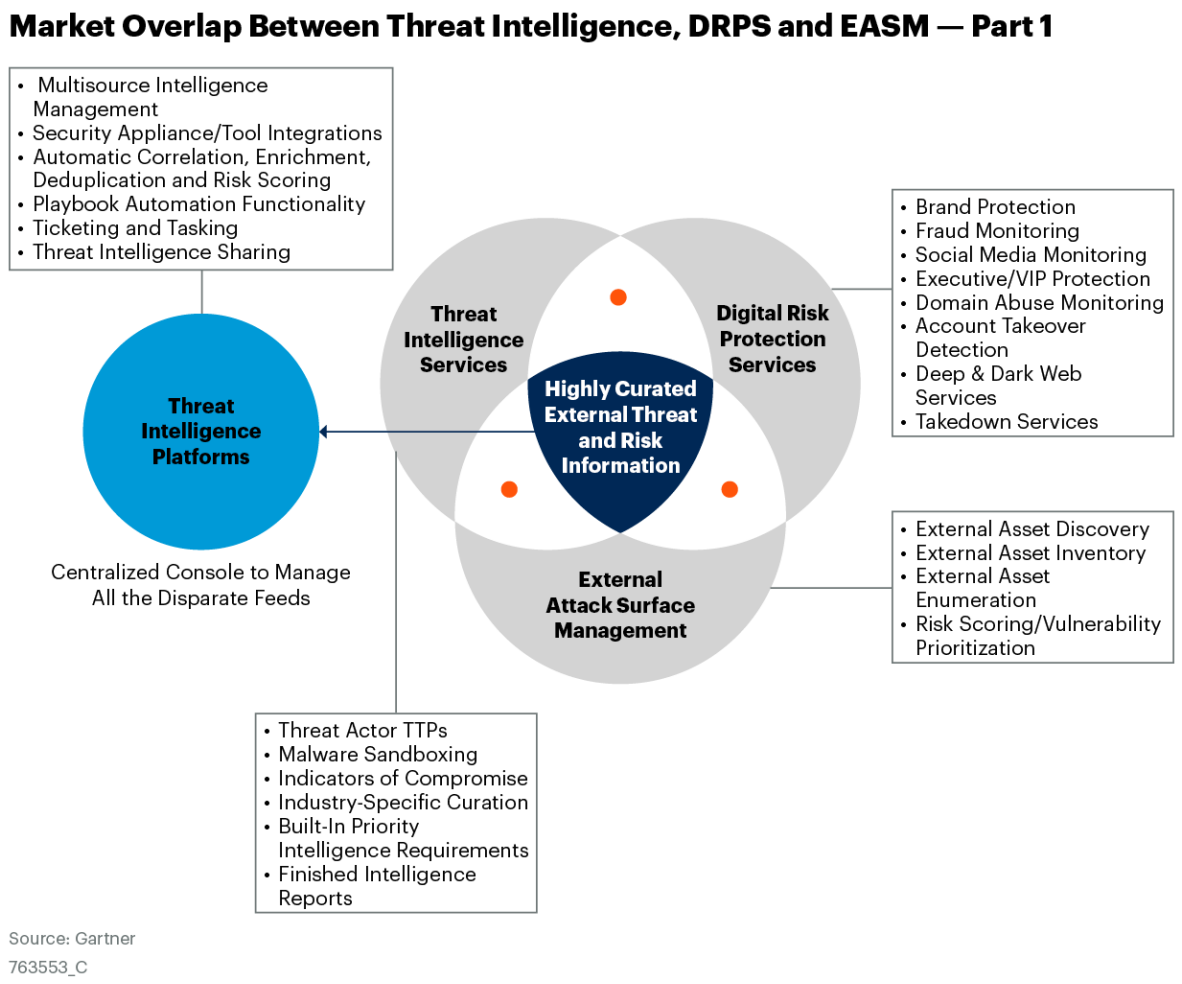
It is commonplace to see TI outputs from service and product vendors tagged and categorized with alignment to industry-recognized attack life cycle frameworks (like MITRE ATT&CK or the Lockheed Martin [Cyber Kill Chain]). Gartner recommends — and buyers have rightly demanded — a common taxonomy for contextual threat information across disparate platforms (including threat detection platforms). It was only natural for TI vendors to implement these industry-recognized frameworks as the basis of their tagged content, particularly by TIP vendors that automate the delivery of intelligence to those disparate security solutions in an environment. This tagging capability assists in moving incident and event artifacts higher up the TI data, information, knowledge, intelligence (DIKI) pyramid by adding context and insight (see Figure 3). This ultimately allows the client to match vendor knowledge with their own priority intelligence requirements (PIRs) and environmental context to make the knowledge actionable, accurate and timely TI.

Figure 3: The Threat Intelligence DIKI Pyramid and Product/Service Alignment



A significant number of vendors continue to exist in the TI marketplace, with larger suppliers offering a wide range of use cases and services, including DRPS and sometimes EASM. The TI market has a wide range of offerings dependent on the dataset/type and requirement for TI analyst support (see Figure 4).

Figure 4: Market Overlap Between Threat Intelligence, DRPS and EASM — Part 1



Market Analysis

TI point solutions enable organizations to collect, curate, process and disseminate TI within them as well as deliver available TI in the form of feeds, reports and access to analysts via investigative portals. However, operationalizing and automating intelligence is where organizations begin to see value. Mature security organizations with dedicated TI teams often demand more features and functionalities to collect, curate and disseminate their own intelligence while ingesting external TI sources to extend and validate their findings. It is not unusual to see mature organizations consume a dozen or more TI sources across multiple styles like free/open sources, computer emergency response teams (CERTs), information sharing and analysis centers (ISACs) and commercial providers. There is an overlap between these sources. In many areas, one vendor/provider has more visibility than others and there is no “one TI provider to rule them all” in this dispersed market landscape.

There is not a single security threat intelligence source — whether open-source, commercial off-the-shelf or government-created, in the market today — which has visibility into all types of threats.

Less-mature security programs with a limited number or lack of dedicated TI experts on staff are more likely to choose TI point solutions that focus on aggregated machine-readable threat intelligence (MRTI) feeds (see Table 1) with high-level contextual information or rely on DRPS. Many providers have integrations that are ready for use and can ease the burden of operationalizing TI inside the client organization. These less mature programs are not interested in (or not ready for) advanced features such as graph analytics, link analysis or tagging and threat actor modeling. Organizations that run such programs may turn to service providers for highly curated end-to-end intelligence services that directly interface with existing processes and investments in order to significantly reduce their time to value.

Threat Intelligence Subscription Services

TI subscription services deliver the essential information and data that organizations need to consume and apply as TI, based on their unique threat landscape and environment. Buyers will find numerous categories of data delivery methods and content types, some with all-inclusive pricing models and some modular. Table 4 provides a list of the common services offered by these subscriptions.

Table 4: Examples of Threat Intelligence Subscription Services

(Enlarged table in Appendix)

Subscription services	Description	Primary delivery method
Indicator feed	Curated lists of indicators, predominantly atomic, focused on adversary infrastructure and malware technical details. IP addresses, URLs, domains and file hashes are some examples of atomic indicators that TI vendors will deliver as part of a subscription.	Machine-readable threat intelligence
Threat actor profiles	A list of threat actor profiles categorized by national government affiliation and/or grouped by objective (e.g., espionage, financially motivated or hacktivist). These profiles are often utilized for attribution and communicating TTPs used by the threat actor to accomplish their goals.	Human- and machine-readable intelligence
Portal	Paid-for access to curated threat information and data, often in the form of news stories, vulnerability information, top trends visuals and library of reports. TI portals are the primary delivery method and client interface for TI services.	Human- and machine-readable intelligence
Threat news	Collection of open-source, private-group- and provider-created cyberthreat news. Some providers offer news feeds tailored to specific verticals, while others may offer filtering based on user-defined profiles.	Human-readable intelligence
Technical threat analysis reports	The results of reverse engineering malware or the inner workings of a botnet are delivered in technical reports for clients to consume. These reports typically provide a list of atomic indicators at the end of the report and may include a list of known detection signatures.	Human- and machine-readable readable intelligence
Takedown services	Incident response services geared toward the technical remediation of DRPS findings intended to defraud or damage the brand. These services typically target domain/website misuse (phishing, typosquatting, fake sites), fake/rogue mobile applications, logo/trademark infringement, and fraudulent social media accounts and posts.	Managed or automated services
Managed intelligence services	Services geared to provide end-to-end TI operations. Typically consists of intelligence collection, analysis and reporting or a combination thereof.	Managed services
Request for information support	Provides organizations with an existing TI function the ability to submit an RFI for additional/enhanced support. Common uses are analysts requiring additional information/context related to an indicator, or needing additional information about a particular TTP or related attribute.	Professional or managed services
Examples: **Machine-readable intelligence:** JSON, comma-separated values (CSV), Structured Threat Information eXpression (STIX), Trusted Automated eXchange of Intelligence Information (TAXII), API, Cyber Observable eXpression (CybOX), yarCAPEC, YARA, Sigma. **Human** - **readable intelligence:** PDF-formatted reports, HTML posts within a service portal. **Takedown services:** Serviced manually by the DRPS provider (typically provided via credits) or supplied to the customer via user interface automation. **Managed services:** Directly from the TI provider, or supplied through a managed security services provider. **Professional services:** TI advisory services.		

Source: Gartner (August 2024)

Threat Intelligence Platforms

Aggregation, management and operationalization of TI are the core use cases addressed by TIPs. A parallel exists between TIPs and SOAR solutions due to an overlap in automating enrichment of tickets and indicators with TI and pushing intelligence to security technologies. It is often advisable to use technology, such as TIP, to aid with TI sharing, either publicly or privately with other organizations. A TIP allows for TI to be exported and ingested at high speed in machine-readable formats that systems at each end can generate and parse efficiently. It also allows organizations to consume large volumes of TI in various formats for storage, deduplication, ranking and automated workflow use cases.

Digital Risk Protection Services

DRPS stretch detection and monitoring activities outside of the enterprise perimeter by searching for threats to enterprise digital resources, such as IP addresses, domains and brand-related assets. DRPS solutions provide visibility into the open (surface) web, dark web and deep web environments by providing contextual information on threat actors and the tactics and processes that they exploit to conduct malicious activities.

DRPS providers support a variety of roles (such as chief information security officers [CISOs], risk, compliance and legal teams, HR and marketing professionals) to map and monitor digital assets. They also support mitigating activities such as site/account takedowns and the generation of customized reporting. Takedown services can include forensics (postinvestigation and data recovery) and after-action monitoring.

External Attack Surface Management

EASM is an adjacent technology market that overlaps with DRPS and TI. It is a combination of technology, processes and managed services that provides visibility of known and unknown digital assets to give organizations an outside-in view of their environment (see Competitive Landscape: External Attack Surface Management). This, in turn, can help organizations prioritize threat and exposure treatment activity. However, Gartner predicts that EASM capabilities will be assimilated into other security solutions (i.e., DRPS, TI, vulnerability management, exposure assessment and adversarial exposure validation) in the near future, and may no longer be a stand-alone market in the next three to five years.

Vulnerability Intelligence

Vulnerability intelligence provides an understanding of the state of vulnerabilities that are being exploited by named attacks and threat actors; as well as analytics of the likelihood that vulnerabilities in an organization's environment will be exploited in the wild.

This quantifiable knowledge provides key insights for an organization to understand what its threat landscape actually looks like, and essentially produces two benefits:

- Reducing the overwhelming quantity of vulnerabilities that the organization has to weed out.
- Showing the organization which threats represent the highest risks.

Outside of TI services, many traditional vulnerability assessment tools have vulnerability intelligence capabilities. However, some pure-play vulnerability prioritization technology (VPT) vendors have been playing a key role in the vulnerability assessment market (see Market Guide for Vulnerability Assessment).

Threat Intelligence Sharing

It is well-understood, but not particularly visible publicly, that TI-sharing networks have real value for security programs. Gartner recommends that all organizations that are looking to use TI in their security programs, regardless of size and industry vertical, investigate the options they have for participating in this kind of collaborative capability.

Information Sharing and Analysis Centers

Many information sharing and analysis centers (ISACs) have been very successful in building sharing networks that considerably enhance the visibility of prevailing threats, helping their clients or organizations from various verticals to detect and prevent threats. This is a list of member ISACs under the U.S. National Council of ISACs.

Malware Information Sharing Platform and Threat Sharing

Malware Information Sharing Platform (MISP) is an open-source TI platform. It can be used to collect, store, distribute and share machine-readable TI. It gained momentum as an open-source project after the North Atlantic Treaty Organization (NATO) decided to use it and provided development resources to improve it. It is released under the Affero General Public License (AGPL) and is in use by some managed security services providers.

MISP is widely adopted by organizations looking for simple, low-cost TIP functionality. Organizations can leverage open-source intelligence (OSINT) provided by many MISP communities. They can integrate OSINT into their threat detection and response processes without the need to acquire any commercial TI sources.

CERTs

Most regions today have a local computer emergency response team (CERT), and a number of them have services that include TI feeds and/or related services.

Some examples of CERTs include:

- AUSCERT
- Carnegie Mellon CERT

- CERT-EU
- CERT-In
- CISA

Representative Vendors

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.

Vendor Selection

Gartner has included a range of providers in this research to ensure coverage from geographical, vertical and capabilities perspectives. Gartner estimates that more than 100 providers in this market claim to offer stand-alone TI services. Those included in this Market Guide:

- Are visible to Gartner clients (based on inquiries).
- Represent a broad geographic range based on locations of headquarters and areas of focus.
- Provide stand-alone TI products and services, which means the client does not have to purchase an additional non-TI product or service to get access to TI offerings.
- Have a notable community following across social media platforms.
- Have significant market tenure.

Table 5: Representative Vendors in the Threat Intelligence Market

(Enlarged table in Appendix)

Vendor	Headquarters	Product names
Anomali	California, U.S.	▪ Anomali ThreatStream ▪ Anomali Security Analytics ▪ Anomali Copilot
CloudSEK	Singapore	▪ CloudSEK XVigil ▪ CloudSEK SVigil ▪ CloudSEK BeVigil Enterprise ▪ CloudSEK BeVigil Community ▪ CloudSEK Exposure
Constella Intelligence	California, U.S	▪ Identity Monitoring ▪ Deep OSINT Investigations ▪ Synthetic Identity Fraud Detection
CrowdStrike	Texas, U.S.	▪ Falcon Adversary OverWatch ▪ Falcon Adversary Intelligence ▪ Falcon Adversary Intelligence Premium ▪ Falcon Exposure Management
CybelAngel	Paris, France	▪ Dark Web Monitoring ▪ Domain Protection ▪ Data Breach Prevention ▪ Account Takeover Prevention ▪ Asset Discovery and Monitoring

Cyberint	Petah Tikva, Israel	▪ Argos Platform
		  ▪ Attack Surface Management
		  ▪ Phishing Detection
		  ▪ Social Media Monitoring
		  ▪ Forensic Canvas
		  ▪ Vulnerability Intelligence
		  ▪ Risk Intelligence Feeds (IOC)
		  ▪ Cyber Threat Intelligence
		  ▪ Dashboard and Reports

Cybersixgill	Tel Aviv, Israel	▪ Cyber Threat Intelligence ▪ Vulnerability Exploit Intelligence ▪ Attack Surface Management ▪ MSSP Solutions
ReliaQuest	Florida, U.S.	▪ GreyMatter Threat Intelligence ▪ GreyMatter Digital Risk Protection
Google (Mandiant)	Virginia, U.S.	▪ Attack Surface Management ▪ Digital Threat Monitoring ▪ Threat Intelligence

Flashpoint	New York, U.S.	▪ Flashpoint Ignite Platform
		  ▪ Flashpoint Cyber Threat Intelligence
		  ▪ Flashpoint Vulnerability Management (VulnDB)
		  ▪ Flashpoint Physical Security Intelligence
		  ▪ Flashpoint National Security Intelligence
		  ▪ Flashpoint Managed Attribution

Group-IB	Singapore	▪ Threat Intelligence ▪ Fraud Protection ▪ Digital Risk Protection ▪ Attack Surface Management
IBM Security	New York, U.S.	▪ IBM X-Force Exchange ▪ X-Force Threat Intelligence Essentials ▪ X-Force Threat Intelligence Standard ▪ X-Force Premium Threat Intelligence

Intel 471	Delaware, U.S.	▪ TITAN Cybercrime Intelligence Platform
		  ▪ Adversary Intelligence
		  ▪ Credential Intelligence
		  ▪ Malware Intelligence
		  ▪ Marketplace Intelligence
		  ▪ Vulnerability Intelligence

Rapid7 (IntSights)	New York, U.S.	▪ Threat Command
		  ▪ Digital Risk Protection
		  ▪ Clear, Deep, & Dark Web Protection
		  ▪ IOC Management & Enrichment
		  ▪ Rapid Remediation & Takedown
		  ▪ Seamless Automation
		  ▪ Expansive Threat Library
		  ▪ Advanced Investigation & Threat Mapping

NSFOCUS	Beijing, China	▪ NSFOCUS Threat Intelligence ▪ Exposed Internet Surface Analysis (EISA) ▪ Attack Threat Monitoring
Microsoft	Washington, U.S.	▪ Defender Threat Intelligence — standard version ▪ Defender Threat Intelligence — premium version
Orange Business	Paris, France	▪ Managed Threat Intelligence ▪ Threat Intelligence Feeds ▪ Managed Cybercrime Monitoring ▪ Managed Vulnerability Intelligence
Palo Alto Networks (Cortex)	California, U.S.	▪ Cortex XSOAR Threat Intelligence Management ▪ Cortex Xpanse
Thoma Bravo (Proofpoint)	California, U.S.	▪ Emerging Threats Intelligence

QAX	Beijing, China	▪ QAX TIP
		  ▪ Vulnerability Intelligence
		  ▪ APT Archive
		  ▪ Email Attack Detection
		  ▪ Cloud-Based Intelligence

QuoIntelligence	Frankfurt am Main, Germany	▪ Mercury 2.0
		  ▪ Threat Intelligence
		  ▪ Risk Intelligence
		  ▪ Digital Risk Protection

Recorded Future	Massachusetts, U.S.	▪ Intelligence Cloud Modules
		  ▪ Brand Intelligence
		  ▪ SecOps Intelligence
		  ▪ Threat Intelligence
		  ▪ Vulnerability Intelligence
		  ▪ Third-Party Intelligence
		  ▪ Geopolitical Intelligence
		  ▪ Payment Fraud Intelligence
		  ▪ Identity Intelligence
		  ▪ Attack Surface Intelligence

Sekoia.io	Rennes, France	▪ Sekoia Intelligence (CTI) ▪ Sekoia.io TIP
Telos	Virginia, U.S.	▪ Telos Advanced Cyber Analytics
Verizon	New York, U.S.	▪ Threat Intelligence Services ▪ Dark Web Hunting
ZeroFox	Maryland, U.S.	▪ ZeroFOX Protection ▪ ZeroFOX Intelligence ▪ ZeroFOX Disruption ▪ ZeroFOX Response ▪ ZeroFOX External Attack Surface Management

Source: Gartner (August 2024)

Market Recommendations

According to the SANS 2023 Cyberthreat Intelligence Survey, 59% of organizations have documented PIRs, a 25% increase from 2022. [1] However, according to our client inquiries, while a growing number of organizations are formalizing their programs, they're still struggling to close the larger maturity gap. These organizations should focus on measuring the effectiveness of their programs and using that data to tune program or intelligence shortcomings (see How to Evaluate Your Threat Intelligence Program's Effectiveness).

Gartner has, for a number of years, recommended a simple and pragmatic way to get the most from a TI program. At a high level, end-user organizations should concurrently:

- **Acquire — There are a plethora of services available today.** End users need to be selective and ensure that they are "acquiring" the right blend of TI. For example, there's not much use in getting an IOC malware feed if you are looking to improve your vulnerability management program. The key here is to identify the right TI solutions for your business objectives while ensuring they align with the maturity of your security program (see Define Threat Intelligence Requirements to Improve SecOps Efficiency).

- **Aggregate — Clients regularly use a dozen or more intelligence feeds/services.** Therefore, it is critical to determine how, once you've obtained all the potentially useful threat information and data, you can aggregate it and align it to PIRs, which will turn it into true TI. TIP/SOAR tooling is an example of this capability from a technology point of view, but people/processes cannot be eliminated from the equation.

- **Action — Even today, a key issue is actionability.** Security and risk management leaders must understand that just knowing is not enough; they must be able to take action. TI done well improves your SecOps staff's effectiveness, your process efficiency and your technologies' efficacy. Keeping PIRs in mind will help enormously with focusing on the end goal and making sure business needs are being addressed, no matter what you do.

Recommendations:

- Optimize TI investments by building a TI program that tailors threat landscape and real-time threat information to business risks to aid in the executive decision-making process.

- Promote cohesion among intelligence services by correlating across your external threat data for better prioritization.

- Focus on intelligence providers that use advanced curation techniques to provide highly actionable insights in order to reduce the burden of prolonged analysis across large, mixed datasets.

Acronym Key and Glossary Terms

AGPL	Affero General Public License
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
CERT	computer emergency response team
DIKI	data, information, knowledge, intelligence
DRPS	digital risk protection services
EASM	external attack surface management
IOC	indicator of compromise
IPv4	Internet Protocol version 4
ISAC	intelligence sharing and analysis center
MISP	Malware Information Sharing Platform
MRTI	machine-readable threat intelligence
OSINT	open-source intelligence
PIR	priority intelligence requirement
SIEM	security information and event management
SOAR	security orchestration, automation and response
SOC	security operations center
SSL	Secure Sockets Layer
TI	threat intelligence
TIP	threat intelligence platform
TTPs	tactics, techniques and procedures
VPT	vulnerability prioritization technology

Evidence

[1] SANS 2023 CTI Survey: Keeping Up with a Changing Threat Landscape, SANS Institute (registration is required to download this report).

Note 1: Gartner's Initial Market Coverage

This Market Guide provides Gartner's initial coverage of the market and focuses on the market definition, rationale for the market and market dynamics.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

3 Ways to Apply a Risk-Based Approach to Threat Detection, Investigation and Response

Forecast: Information Security, Worldwide, 2022-2028, 2Q24 Update

SOC Model Guide

Define Threat Intelligence Requirements to Improve SecOps Efficiency

Innovation Insight: Attack Surface Management

Market Guide for Vulnerability Assessment

Tool: Vendor Identification for Security Threat Intelligence Products and Services

---

Table 1: Optional TI Capabilities

Market segment	Optional features
Threat intelligence	■ Tactics, techniques and procedures (TTPs) enrichment of IOCs, provided typically in two formats: threat actor profiles and MITRE ATT&CK enrichments. ■ Malware sandboxing, providing the ability to dynamically extract IOCs from malware samples by detonating the malware in a provider (cloud or on-premises) sandbox. ■ Vulnerability intelligence tailored for vulnerability prioritization, often highlighting actively exploited vulnerabilities and the associated IOCs. ■ Finished intelligence reporting including technical/tactical analysis reports as well as operational and strategic intelligence products. ■ Node graph visualizations such as link-end analysis graphs and built-in Maltego Transforms. ■ Network telemetry enrichments such as passive DNS, sinkhole traffic and global sensor network telemetry. ■ Industry-specific curation such as advanced search filters, industry-specific query parameters, and dashboards. ■ Built-in priority intelligence requirement curation. ■ Metrics reporting tailored for operational governance. ■ Support with forensic analysis.

Market segment	Optional features
	■ Vulnerability intelligence. ■ Supporting sharing across industry communities.
Threat intelligence, featuring DRPS	■ Third-party risk assessments, geared toward evaluating the risks associated with an entity's supply chain based on threat intelligence activity. ■ Domain abuse monitoring, typically for threats associated with customer domains, such as typosquatting and phishing. ■ Dark web services that monitor the deep and dark web for mentions related to the customer organization. Typical use cases are data leakage, fraud and threat actor attribution. ■ Social media monitoring for violation of social media policies, account takeover, VIP/executive protection and sentiment analysis. ■ Takedown services for the remediation of DRPS findings such as illicit domain/website removals and hijacked account revocations.

Market segment	Optional features
Threat intelligence, featuring EASM	■ Discovery of external, digital assets (on-premises and cloud) typically identifying Internet Protocol version 4 (IPv4) assets, web applications, domains and Secure Sockets Layer (SSL) certificates. ■ Enumeration of software vulnerabilities and security weaknesses for remediation prioritization, typically using discoverability and exploitability as factors for risk scoring. ■ TI attack surface enrichments, adding the relevant attributes associated with actively exploited vulnerabilities. ■ Support/advisory on remediation to exposures identified.

Source: Gartner (August 2024)

Table 2: Example Expanding Use Cases

Use case	*Description*	*TI support*	*Benefit*
Threat hunting	Proactively searching for evidence of compromise across organizational technology domains	Provides relevant TTPs/IOCs/IOAs including probable exploitation vectors based on threat landscape activities	■ Can identify attacks that have evaded detection before significant business impact occurs ■ Surfaces vulnerabilities and weaknesses that can pose material risk to the business before impact occurs

Use case ↓	*Description* ↓	*TI support* ↓	*Benefit* ↓
Threat detection, use case development	Building threat detection use cases, for the real-time detection of threats	Provides curated indicators of compromise, increasing the efficacy of alerting use cases	■ Reduces false positives in detection use cases ■ Increases speed of investigation, in turn reducing mean-time-to-detect metrics ■ Assists in establishing attack severity at the point of alerting, allowing for better workload prioritization
Threat exposure management	Discovering, prioritizing and mobilizing resources to close or reduce risky exposures	Exposure assessment — Can identify which vulnerabilities across your digital estate are being, have been or will be exploited in the wild, and to what degree	■ Can help prioritize actively exploitable vulnerabilities, driving down the number of findings requiring immediate fixes ■ Can help proactively identify vulnerabilities at imminent risk

Use case	*Description*	*TI support*	*Benefit*
Threat exposure management	Validating exposures, testing security controls and mobilizing resources to close or reduce risky exposures	Adversarial exposure validation — Based on information collected about active attack campaigns and techniques, TI can identify what TTPs are likely to be used against your technology stack to compromise or immobilize your organization	Can help identify the threat actor attributes and artifacts most likely to impact your organization, resulting in more accurate and timely cybersecurity validation exercises and therefore higher priority and effective fix recommendations

IOAs = Indicators of attack
IOCs = Indicators of compromise

Source: Gartner

Table 3: 5 Advancements in High-Performing Investigation Platforms

Advancement ↓	*Features* ↓
Optimized graphical user interface	■ Faster searches ■ More native enrichments ■ Natural language processing ■ Enhanced tagging capabilities
Nodal network graphs	■ Native link-end analysis ■ In-depth relationship modeling
Case management	■ Investigator support ■ Historical archive ■ Annotation and artifact logs
Native integrations	■ API push, pull functionality ■ Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) compatibility

Advancement ↓	*Features* ↓
Reporting	■ On-demand report generation ■ Metrics dashboards ■ Watchlisting ■ News feeds

Source: Gartner

Table 4: Examples of Threat Intelligence Subscription Services

Subscription services	*Description*	*Primary delivery method*
Indicator feed	Curated lists of indicators, predominantly atomic, focused on adversary infrastructure and malware technical details. IP addresses, URLs, domains and file hashes are some examples of atomic indicators that TI vendors will deliver as part of a subscription.	Machine-readable threat intelligence
Threat actor profiles	A list of threat actor profiles categorized by national government affiliation and/or grouped by objective (e.g., espionage, financially motivated or hacktivist). These profiles are often utilized for attribution and communicating TTPs used by the threat actor to accomplish their goals.	Human- and machine-readable intelligence
Portal	Paid-for access to curated threat information and data, often in the form of news stories, vulnerability information, top trends visuals and library of reports. TI portals are the primary delivery method and client interface for TI services.	Human- and machine-readable intelligence

Subscription services	Description	Primary delivery method
Threat news	Collection of open-source, private-group- and provider-created cyberthreat news. Some providers offer news feeds tailored to specific verticals, while others may offer filtering based on user-defined profiles.	Human-readable intelligence
Technical threat analysis reports	The results of reverse engineering malware or the inner workings of a botnet are delivered in technical reports for clients to consume. These reports typically provide a list of atomic indicators at the end of the report and may include a list of known detection signatures.	Human- and machine-readable readable intelligence
Takedown services	Incident response services geared toward the technical remediation of DRPS findings intended to defraud or damage the brand. These services typically target domain/website misuse (phishing, typosquatting, fake sites), fake/rogue mobile applications, logo/trademark infringement, and fraudulent social media accounts and posts.	Managed or automated services
Managed intelligence services	Services geared to provide end-to-end TI operations. Typically consists of intelligence collection, analysis and reporting or a combination thereof.	Managed services

Subscription services	Description	Primary delivery method
Request for information support	Provides organizations with an existing TI function the ability to submit an RFI for additional/enhanced support. Common uses are analysts requiring additional information/context related to an indicator, or needing additional information about a particular TTP or related attribute.	Professional or managed services
Examples: **Machine-readable intelligence:** JSON, comma-separated values (CSV), Structured Threat Information eXpression (STIX), Trusted Automated eXchange of Intelligence Information (TAXII), API, Cyber Observable eXpression (CybOX), yarCAPEC, YARA, Sigma. **Human** - **readable intelligence:** PDF-formatted reports, HTML posts within a service portal. **Takedown services:** Serviced manually by the DRPS provider (typically provided via credits) or supplied to the customer via user interface automation. **Managed services:** Directly from the TI provider, or supplied through a managed security services provider. **Professional services:** TI advisory services.		

Source: Gartner (August 2024)

Table 5: Representative Vendors in the Threat Intelligence Market

Vendor	Headquarters	Product names
Anomali	California, U.S.	■ Anomali ThreatStream ■ Anomali Security Analytics ■ Anomali Copilot
CloudSEK	Singapore	■ CloudSEK XVigil ■ CloudSEK SVigil ■ CloudSEK BeVigil Enterprise ■ CloudSEK BeVigil Community ■ CloudSEK Exposure
Constella Intelligence	California, U.S	■ Identity Monitoring ■ Deep OSINT Investigations ■ Synthetic Identity Fraud Detection

Vendor	Headquarters	Product names
CrowdStrike	Texas, U.S.	■ Falcon Adversary OverWatch ■ Falcon Adversary Intelligence ■ Falcon Adversary Intelligence Premium ■ Falcon Exposure Management
CybelAngel	Paris, France	■ Dark Web Monitoring ■ Domain Protection ■ Data Breach Prevention ■ Account Takeover Prevention ■ Asset Discovery and Monitoring

Vendor	Headquarters	Product names
Cyberint	Petah Tikva, Israel	■ Argos Platform ■ Attack Surface Management ■ Phishing Detection ■ Social Media Monitoring ■ Forensic Canvas ■ Vulnerability Intelligence ■ Risk Intelligence Feeds (IOC) ■ Cyber Threat Intelligence ■ Dashboard and Reports
Cybersixgill	Tel Aviv, Israel	■ Cyber Threat Intelligence ■ Vulnerability Exploit Intelligence ■ Attack Surface Management ■ MSSP Solutions
ReliaQuest	Florida, U.S.	■ GreyMatter Threat Intelligence ■ GreyMatter Digital Risk Protection

Vendor	Headquarters	Product names
Google (Mandiant)	Virginia, U.S.	■ Attack Surface Management ■ Digital Threat Monitoring ■ Threat Intelligence

Flashpoint	New York, U.S.	■ Flashpoint Ignite Platform
		  ■ Flashpoint Cyber Threat Intelligence
		  ■ Flashpoint Vulnerability Management (VulnDB)
		  ■ Flashpoint Physical Security Intelligence
		  ■ Flashpoint National Security Intelligence
		  ■ Flashpoint Managed Attribution

Group-IB	Singapore	■ Threat Intelligence ■ Fraud Protection ■ Digital Risk Protection ■ Attack Surface Management

Vendor	Headquarters	Product names
IBM Security	New York, U.S.	■ IBM X-Force Exchange ■ X-Force Threat Intelligence Essentials ■ X-Force Threat Intelligence Standard ■ X-Force Premium Threat Intelligence

Intel 471	Delaware, U.S.	■ TITAN Cybercrime Intelligence Platform
		  ■ Adversary Intelligence
		  ■ Credential Intelligence
		  ■ Malware Intelligence
		  ■ Marketplace Intelligence
		  ■ Vulnerability Intelligence

Vendor	Headquarters	Product names
Rapid7 (IntSights)	New York, U.S.	■ Threat Command ■ Digital Risk Protection ■ Clear, Deep, & Dark Web Protection ■ IOC Management & Enrichment ■ Rapid Remediation & Takedown ■ Seamless Automation ■ Expansive Threat Library ■ Advanced Investigation & Threat Mapping
NSFOCUS	Beijing, China	■ NSFOCUS Threat Intelligence ■ Exposed Internet Surface Analysis (EISA) ■ Attack Threat Monitoring
Microsoft	Washington, U.S.	■ Defender Threat Intelligence — standard version ■ Defender Threat Intelligence — premium version

Vendor	Headquarters	Product names
Orange Business	Paris, France	■ Managed Threat Intelligence ■ Threat Intelligence Feeds ■ Managed Cybercrime Monitoring ■ Managed Vulnerability Intelligence
Palo Alto Networks (Cortex)	California, U.S.	■ Cortex XSOAR Threat Intelligence Management ■ Cortex Xpanse
Thoma Bravo (Proofpoint)	California, U.S.	■ Emerging Threats Intelligence
QAX	Beijing, China	■ QAX TIP ■ Vulnerability Intelligence ■ APT Archive ■ Email Attack Detection ■ Cloud-Based Intelligence

Vendor	Headquarters	Product names
QuoIntelligence	Frankfurt am Main, Germany	■ Mercury 2.0 ■ Threat Intelligence ■ Risk Intelligence ■ Digital Risk Protection
Recorded Future	Massachusetts, U.S.	■ Intelligence Cloud Modules ■ Brand Intelligence ■ SecOps Intelligence ■ Threat Intelligence ■ Vulnerability Intelligence ■ Third-Party Intelligence ■ Geopolitical Intelligence ■ Payment Fraud Intelligence ■ Identity Intelligence ■ Attack Surface Intelligence

Vendor	Headquarters	Product names
Sekoia.io	Rennes, France	■ Sekoia Intelligence (CTI) ■ Sekoia.io TIP
Telos	Virginia, U.S.	■ Telos Advanced Cyber Analytics
Verizon	New York, U.S.	■ Threat Intelligence Services ■ Dark Web Hunting
ZeroFox	Maryland, U.S.	■ ZeroFOX Protection ■ ZeroFOX Intelligence ■ ZeroFOX Disruption ■ ZeroFOX Response ■ ZeroFOX External Attack Surface Management

Source: Gartner (August 2024)