Market Guide for Security Threat Intelligence Products and Services

4 May 2023 - ID G00763553 - 27 min read

By Jonathan Nunez, Ruggero Contu, **and 1 more**

Security and risk management leaders struggle to know what threats should 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

- Although a larger variety of organizations are choosing threat intelligence (TI) services and products to enrich their security programs, many haven't formalized these programs, resulting in a lack of defined requirements, diminished actionability and an overall lack of long-term program defensibility.
- Increased end-user demand for vendor consolidation in all security markets has led to the inclusion of TI features from adjacent markets in security threat intelligence, namely digital risk protection services (DRPS) and external attack surface management (EASM).
- Analytics, data science and automation have taken root in the TI domain with the goal of fostering better curation in real time and at scale.
- Few organizations today have an accurate picture of their own threat landscape. Successful TI services and programs have risk assessment capabilities associated with threat actor groups, tactics, techniques and procedures (TTPs), indicators of compromise (IOCs), exploits and others, and can align their requirements with business expectations.

Recommendations

Security and risk management leaders responsible for security operations should:

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

- Promote cohesion among existing intelligence services by correlating relevant attributes across all available external threat data sources for better risk quantification and prioritization.
- Focus on intelligence providers that use advanced curation techniques (e.g., priority intelligence requirements [PIRs], visualizations, analytics and hyperenrichments) to deliver insights that focus on actionability in order to reduce the burden of prolonged analysis across large, mixed datasets.

Market Definition

This document was revised on 19 May 2023. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

TI products and services deliver knowledge, information and data about cybersecurity threats and other organization-specific threat exposures (see **How Gartner Defines Threat Intelligence**), including but not limited to indicators of compromise (IOCs), threat actor attribution and campaigns. The output of these products and services aim 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 risk and the chance of being compromised.

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 prediction capabilities (see Note 1). Such capabilities can also help them improve their other operation efforts such as threat detection, incident response, threat hunting and threat exposure management.

Core Capabilities

To be shortlisted for selection, security threat intelligence vendors must be able to:

- Provide IOCs including malicious or suspicious ones, 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.
- Establish machine-to-machine integrations to either push or pull intelligence artifacts.
- Integrate or provide out-of-the-box enrichments to IOCs such as geolocation information and registration information.
- Provide an interactive user portal with built-in analysis functionalities such as intelligence dashboards and search features.

- Provide IOC scoring or risk rating as a way to illustrate confidence in maliciousness or suspiciousness.

Optional Capabilities

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

Table 1: Optional TI Capabilities

Market Segment	Optional Features
Threat intelligence	• 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. • 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.

Market Segment	Optional Features
Threat intelligence, featuring DRPS	• Third-party risk assessments, geared toward quantifying 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 which 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.

Source: Gartner (May 2023)

Common Use Cases

Depending on their desired outcomes and needs, organizations use TI products and services in various ways, such as:

- Supporting incident response activities via intelligence research, artifact correlation and TTP identification.
- Correlating findings with active threats for remediation-workload management to assist in vulnerability prioritization.
- Leveraging real threat actor behaviors for attack emulation to support security control validation.

- Threat detection enrichments and correlations (use-case development).
- Proactive threat hunting (for example, creating a System Monitor query for malicious macro execution that has been uncovered by a technical malware report, but not found by endpoint detection tools).

The security threat intelligence products and services market has a large number of vendors. Gartner monitors more than 80 of them from the commercial space alone (see Table 3). Clients will often have an overwhelming number of options to choose from (see **Tool: Vendor Identification for Security Threat Intelligence Products and Services**).

TI point solutions enable organizations to collect, curate, process and disseminate TI within them as well as delivering 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 overlap between these sources. In certain areas, one vendor/provider has more visibility than others.

> **There is not a single TI source, whether open-source, commercial off-the-shelf or government-created, in the market today, which has visibility into everything.**

Less mature security programs with a limited number of or no 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.

Market Direction

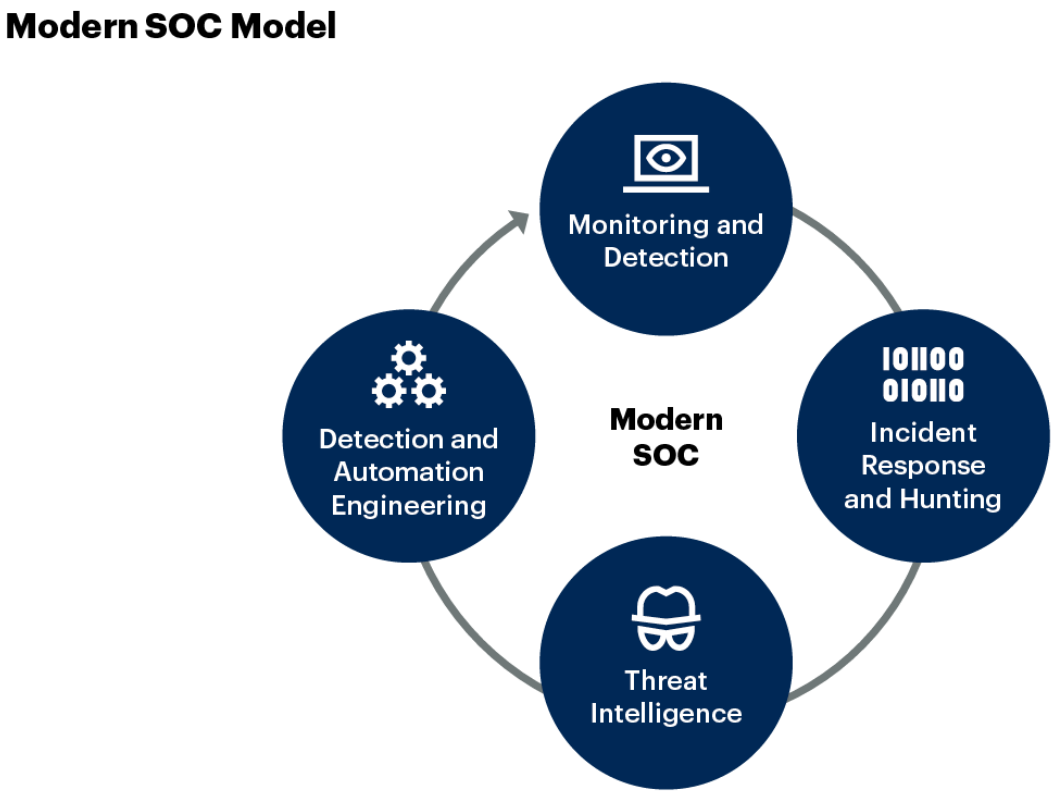
TI is a core function of a modern security operations center (SOC) (see Figure 1). Security programs that underestimate the TI value or fail to properly operationalize TI will find it difficult to defend against imminent threats and predict future security impacts. Based on Gartner's latest

forecast, global TI spending is expected to grow at a compound annual growth rate of 15.5% to reach $2.8 billion by 2026 (see **Forecast: Information Security and Risk Management, Worldwide, 2021-2027, 1Q23 Update**).

Other factors driving interest in the TI market are:

- Threat intelligence platform (TIP) and TI vendors are expanding into new markets such as security orchestration, automation and response (SOAR), supplementing security information and event management (SIEM) platforms and extended detection and response (XDR), external attack surface management (EASM) and third-party risk management. These innovations and the evolution of the market have helped to increase opportunities for the vendors aligned to this space and, as a result, have attracted significant investment.
- With the growing need for curated TI, many large TI vendors have now started to offer EASM as an add-on feature, aiming to deliver highly actionable IOCs to customers that may be susceptible to active exploits. A quantifiable attack surface, which is assessed for security vulnerabilities and weaknesses, can be a great facilitator in tailoring TI collection and analysis to an imminently exploitable attack surface. In other words, knowing what attackers will likely exploit can greatly increase the actionability of derived intelligence.

Figure 1: Modern SOC Model



Source: Gartner
763553_C

Gartner

Organizations are becoming more interested in TI capabilities. According to the SANS 2022 Cyberthreat Intelligence Survey, 36.1% of the surveyed organizations staffed an in-house TI capability while 51% leveraged a hybrid model combining in-house resources with managed threat intelligence services in 2022. [1] This illustrates the continued demand for TI products and services to support intelligence operations.

There have been several acquisitions in the TI marketplace by a mix of larger TI providers, managed security service providers, cloud service providers, insurance providers and others. This is a clear indication that TI is being elevated from a feature capability to a critical capability for all security and risk programs.

The year 2022 saw several notable acquisitions in the TI market.

In the first and second quarters of 2022:

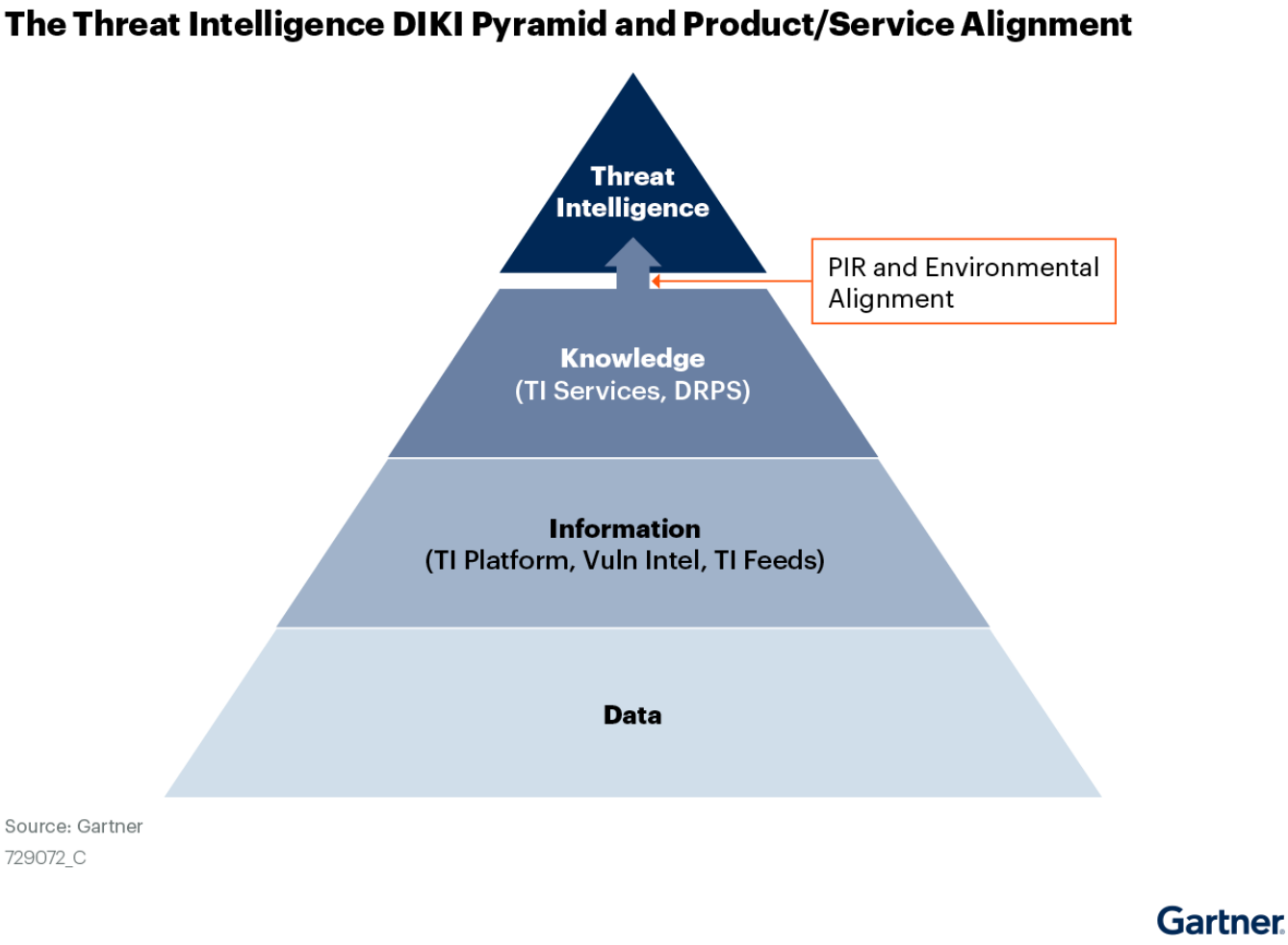
- Crossword Acquires Threat Intelligence Company, Threat Status Limited
- CSW Acquires Early Warning Vulnerability and Threat Intelligence Organization for Predictive, Pre-Breach Insights Into Exploitable Vulnerabilities
- Kroll Acquires Crisp, Trusted Provider of Real-Time Risk Intelligence
- Microsoft to Acquire Miburo to Boost Threat Intelligence Research Into New Foreign Cyberthreats
- ReliaQuest Bets on Growth With Digital Shadows Acquisition

In the third and fourth quarters of 2022:

- Recorded Future Acquires Hatching to Extend Intelligence Cloud Coverage With Malware Analysis
- Flashpoint Acquires Open-Source Intelligence Leader Echosec Systems
- Google + Mandiant: Transforming Security Operations and Incident Response
- vxIntel Joins Arctic Wolf to Boost Detection and Threat Intelligence
- Celerium Acquires Dark Cubed
- Allurity Acquires CSIS Security Group
- Intel 471 Acquires SpiderFoot
- Orange Cyberdefense Acquires Swiss Companies SCRT and Telsys
- Cyber Insurtech BOXX Insurance Acquires Palo Alto-Based Cyberthreat Intelligence Company Templarbit

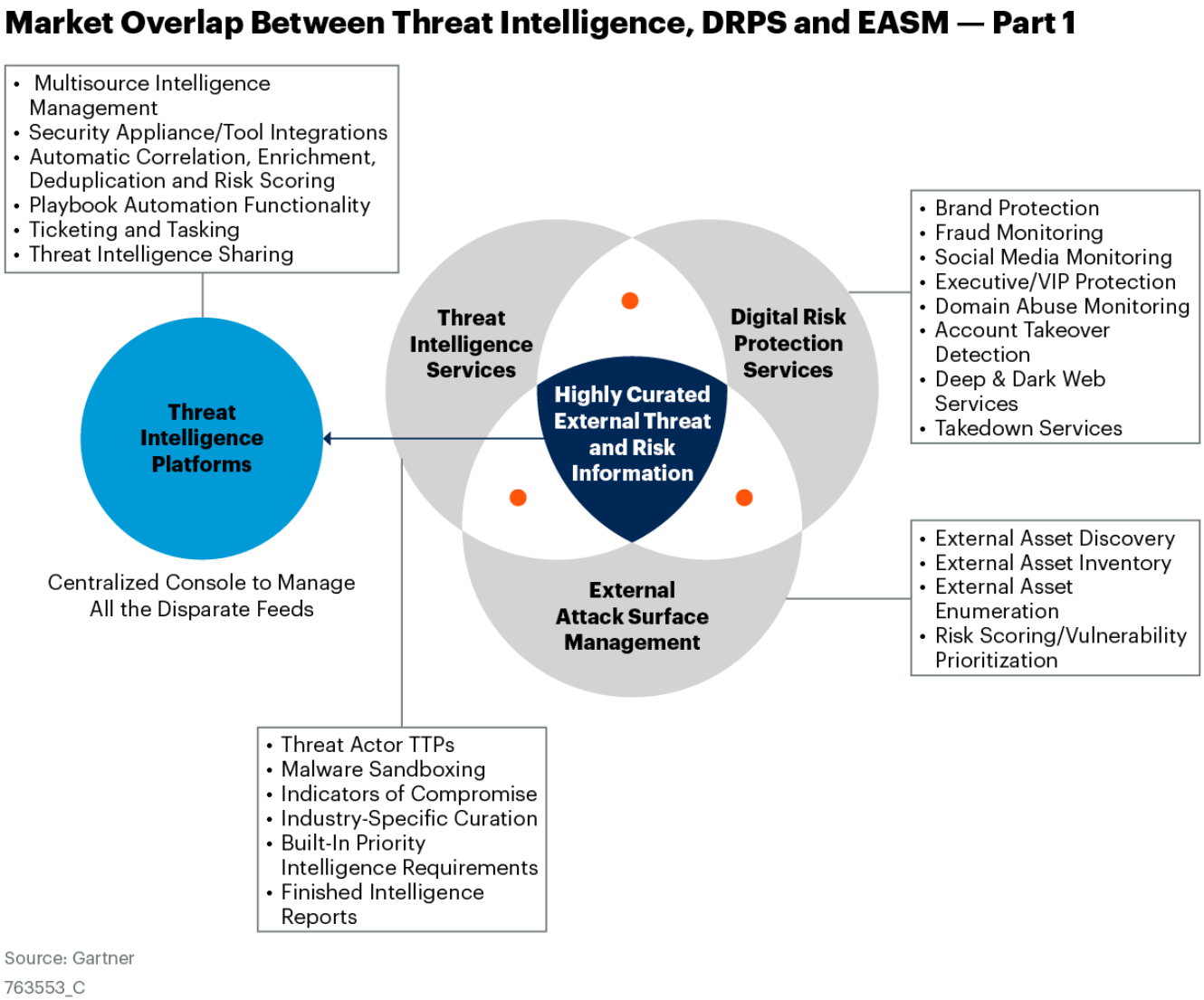
It is commonplace to see TI content from service and product vendors tagged and categorized with alignment to industry-recognized attack life cycle frameworks (like MITRE ATT&CK or the Lockheed Martin [Cyber Kill Chain]). Gartner recommends — and buyers have rightly demanded — a common taxonomy for contextual 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 (see Figure 2) by adding context and insight. 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 2: 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 based on different data as well as access to TI analysts (see Figure 3).

Figure 3: Market Overlap Between Threat Intelligence, DRPS and EASM — Part 1

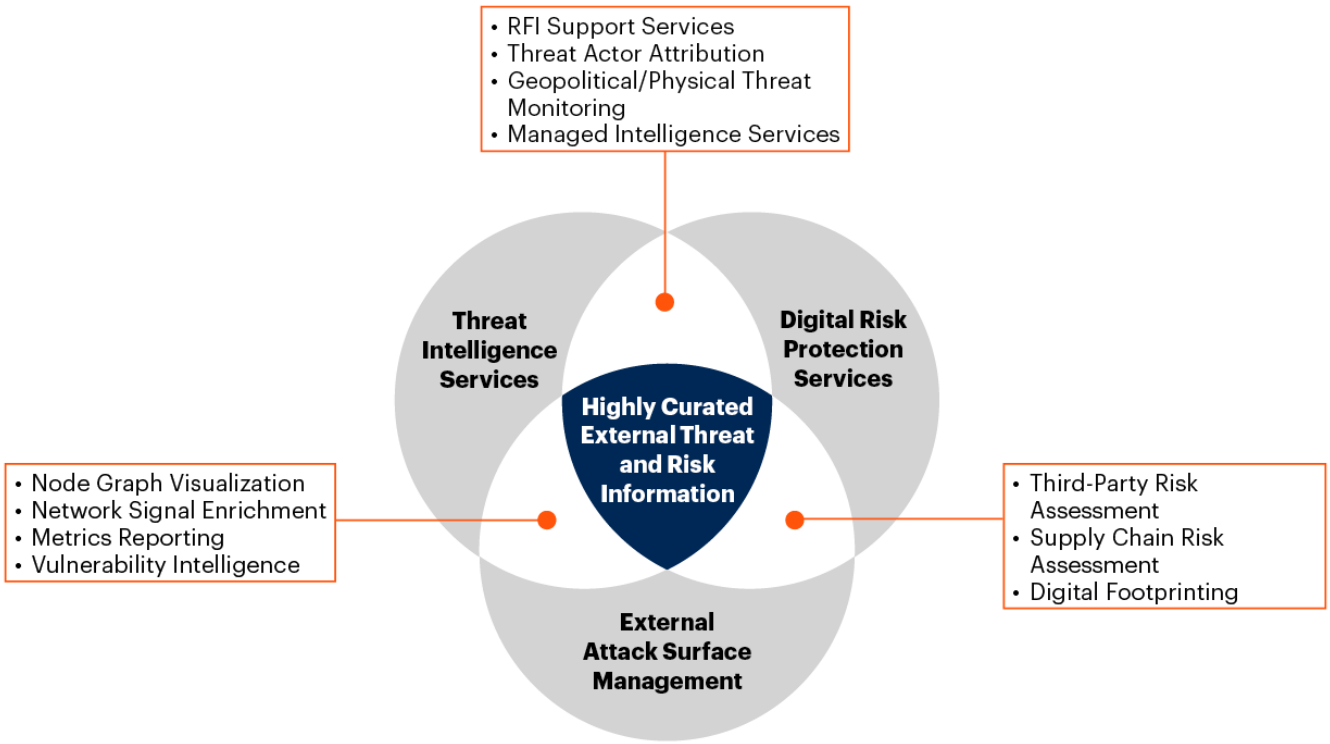


Source: Gartner
763553_C

Gartner

Figure 4: Market Overlap Between Threat Intelligence, DRPS and EASM — Part 2

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



Source: Gartner
763553_C

Gartner.

Market Analysis

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 2 provides a list of the common services offered by these subscriptions.

Table 2: 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, URL, domain, file hashes are some examples of atomic indicators that TI vendors will deliver as part of a subscription.	Machine-readable intelligence

Subscription Services	Description	Primary Delivery Method
Threat actor profiles	A list of threat actor profiles categorized by national government affiliation and/or grouped by objective (espionage, financially motivated or hacktivist, for example). These profiles are often utilized for attribution and communicating TTPs used by the threat actor to accomplish their goals.	Human-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-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-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

Subscription Services	Description	Primary Delivery Method
Managed intelligence services	Services geared to provide end-to-end threat intelligence 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 (May 2023)

Threat Intelligence Platforms

Aggregation, management and operationalization of threat intelligence are the core use cases addressed by TIPs. A parallel has existed between TIPs and security orchestration automation and response (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.

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, 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 (post-investigation and data recovery) and after-action monitoring (see **Emerging Tech: Adoption Growth Insights in Digital Risk Protection Services**).

External Attack Surface Management

EASM is an emerging and adjacent technology market that overlaps with DRPS. 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 **Innovation Insight for 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, and breach and attack simulations) 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 leveraged by named threats 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, some traditional vulnerability assessment tools have vulnerability intelligence capabilities. However, small pure-play vulnerability prioritization technology (VPT) vendors have been playing a leading 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 at using TI in

their security programs, regardless of size and industry vertical, investigate the options they have for participating in this kind of 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 certain industry 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 and Threat Sharing (MISP) is an open-source TI platform. It can be used to collect, store, distribute and share machine-readable threat intelligence. 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).

MISP is widely adopted by organizations looking for a 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 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**

Curation Is the Key

The demand for TI products and services continues to increase, and so do the supplies, as evidenced by the market expansion. The amount of data available for intelligence collection is becoming endless. This situation, coupled with the fact that most organizations still do not have a formalized TI program, has resulted in a need for the curation of information being collected. Some vendors have already met this need.

Curation, or organizing and customizing intelligence specifically for your organization, can be accomplished in a variety of ways. In the traditional sense, security and risk management leaders can build their priority intelligence requirements and use them as a foundation for data collection, analysis and dissemination. This approach looks to build a foundation with curation as core tenant, which in turn narrows the scope for all subsequent data collection, information processing and analysis, increasing actionability. In the absence of PIRs, some vendors have built-in post-processing capabilities to hyperenrich/correlate the intelligence information with other artifacts that are uniquely relevant to the customer organization.

In some instances, intelligence providers are sourcing the customer's internal telemetry (network logs or syslogs) and correlating those attributes with TI to produce alerts. These alerts consist of threat indicators which can be ingested directly into the customer's security appliances for near real-time intervention, or into a SIEM or case management platform.

In other cases, vendors are leveraging data science techniques and other external TI sources for correlations at scale. For example, they conduct external attack surface mapping, prioritize the findings with TI (active threats), and layer the output with public network telemetry to determine compromise (i.e., command and control communications). Some vendors have even gone one step further by finding the associated exfiltrated data via dark web data-leakage services. In essence, whichever combination is on offer, by enlarge, most of the innovation in this space is pointed in the direction of layering a combination of correlations across TI, DRPS and EASM. It is aimed at holistically gathering as much external threat information about the affected entity as possible and then tailoring the TI results for maximum actionability.

Threat intelligence continues to play a centrifugal role as organizations evolve their security programs to identify and prioritize their external threat exposures.

Threat Actor Attribution, Call to Action

Government entities, law enforcement agencies and large financial sector organizations with dedicated TI teams, and TI vendors have historically been the most interested in who is behind an attack. Security and business leaders have been increasingly focused on shortening the overall investigation and remediation time and ensuring the continuity of business operations. But they have not typically been concerned with the attribution of a threat actor, primarily because there is little to no legal action they can take. To be clear, there is value in knowing the behaviors and history of threat actor TTPs to know where they pivot if unsuccessful, for example. However, as they don't have dedicated resources to perform threat actor analysis, many commercial organizations are focusing more on operationalizing TI first and foremost to prevent and detect. Knowing who attacked is just a bonus.

The recently updated sanctions lists of the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) include cyberthreat actors and highlight a need for organizations at large to start paying attention, especially those based in the U.S. In 2021, the U.S. Department of the Treasury issued an updated advisory detailing the risks now associated with facilitating ransomware payments to OFAC-designated malicious cyberthreat actors. The advisory also includes a range of enforcement actions such as civil monetary penalties. [2]

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.

Market Introduction

The vendors listed below are representative of the broad TI market which includes a variety of TI Products (platforms) and services (feeds, reports, managed services). They provide core TI capabilities and in some cases, optional capabilities from the adjacent DRPS and EASM markets.

Table 3: Representative Vendors in the Threat Intelligence Market

Vendor	Headquarters	Product Names
Analyst1	Virginia, United States	• Analyst1 Threat Intelligence Platform
Anomali	California, United States	• ThreatStream • Match • Lens • Attack Surface Management • Digital Risk Protection
bfore.ai	Montpellier, France	• PreEmpt Active Defense • PreCrime Brand • PreCrime Network

Vendor	Headquarters	Product Names
CloudSEK	Singapore	• XVigil • SVigil • BeVigil
Constella Intelligence	California, United States	• Dome • Analyzer • Tracker • Hunter • Intelligence API
CrowdStrike	California, United States	• Falcon Intelligence: Automated Threat Intelligence • Falcon Intelligence Premium: Cyber Threat Intelligence • Falcon Intelligence Elite: Cyber Threat Intelligence Analyst • Falcon Intelligence Recon • Falcon Intelligence Recon+
CybelAngel	Paris, France	• Dark Web Monitoring • Domain Protection • Data Breach Prevention • Account Takeover Prevention • Asset Discovery & Monitoring (ADM) • External Attack Surface Management

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	• Dynamic Vulnerability Exploit (DVE) Intelligence • API Integrations • Threat Intelligence • Cybersixgill SaaS Investigative Portal
Cyware	New Jersey, United States	• Cyware Situational Awareness Platform (CSAP) • Cyware Fusion and Threat Response (CFTR) • Cyware Threat Intel Crawler • Orchestrate • Cyware Threat Intelligence eXchange (CTIX) • CTIX Lite • CTIX Spoke

Vendor	Headquarters	Product Names

DomainTools	Washington, United States	• Iris Internet Intelligence Platform
		• Threat Intelligence Feeds
		  • Threat Intelligence APIs
		  • Predictive Risk Scoring Feeds
		  • Domain Visibility Feeds

EclecticIQ	Amsterdam, The Netherlands	• EclecticIQ Platform

Mandiant, part of Google Cloud	Virginia, United States	• Mandiant Advantage Platform
		  • Automated Defense
		  • Breach Analytics for Chronicle
		  • Threat Intelligence
		  • Digital Threat Monitoring
		  • Attack Surface Management
		  • Security Validation
		  • Managed Defense

Flashpoint	New York, United States	• Compromised Credentials Monitoring • Brand Exposure Protection • Payment and Credit Card Fraud Mitigation • Echosec • VulnDB • Managed Attribution • Flashpoint Automate

Vendor	Headquarters	Product Names
Group-IB	Singapore	• Threat Intelligence • Fraud Protection • Digital Risk Protection • Attack Surface Management • Managed Extended Detection and Response (XDR) • Business Email Protection
IBM Security	New York, United States	• IBM X-Force Exchange • IBM X-Force Exchange API • X-Force Exchange API's Early Warning Feed • Advanced Threat Protection Feed • IBM i2 Security Connect • IBM i2 Analyst's Notebook

Intel 471	Delaware, United States	• TITAN Cybercrime Intelligence Platform
		  • Adversary Intelligence
		  • Credential Intelligence
		  • Malware Intelligence
		  • Marketplace Intelligence
		  • Vulnerability Intelligence

IntSights, a Rapid7 company	New York, United States	• Threat Command • Threat Intelligence Platform (TIP) • Threat Third Party • Vulnerability Risk Analyzer

Vendor	Headquarters	Product Names
LookingGlass	Virginia, United States	• scoutPRIME • scoutTHREAT • scoutINSPECT
NSFOCUS	Beijing, China	• NSFOCUS Threat Intelligence (NTI) Portal • Threat Analysis Reports • Actionable Data Feeds
Microsoft	Washington, United States	• Microsoft Defender Threat Intelligence

Orange Cyberdefense	Paris, France	• Managed Threat Intelligence Services
		  • Threat Intelligence Feeds
		  • Managed Cybercrime Monitoring
		  • Managed Vulnerability Intelligence

Palo Alto Networks	California, United States	• AutoFocus
PhishLabs, a part of Fortra	South Carolina, United States	• PhishLabs Digital Risk Protection Platform

Vendor	Headquarters	Product Names
Proofpoint, a part of Thoma Bravo	California, United States	• Aegis Threat Protection Platform • Sigma Information Protection Platform • Intelligent Compliance Platform
QAX	Beijing, China	• Vulnerability Intelligence • APT Archive • Email Attack Detection • Cloud-Based Intelligence

QuoIntelligence	Frankfurt am Main, Germany	• Mercury 2.0 Services
		  • Threat Intelligence Platform
		  • Risk Intelligence
		  • Digital Risk Protection
		  • TIBER-EU Exercises

Recorded Future	Massachusetts, United States	• 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
ReliaQuest	Florida, United States	• SearchLight • Advisory Services • Custom Intelligence Services
SecAlliance	London, United Kingdom	• ThreatMatch Intelligence Portal • Fused Intelligence Services • Threat Intelligence Platform • TIBER-EU Exercises
Sekoia.io	Paris, France	• Sekoia.io CTI • Sekoia.io TIP
Silobreaker	London, United Kingdom	• Silobreaker Cyber Threat Intelligence • Silobreaker Physical Risk Intelligence • Silobreaker Strategic and Political Intelligence • Silobreaker Brand Threat Protection

SOCRadar	Delaware, United States	• Extended Threat Intelligence
		  • ThreatFusion
		  • RiskPrime
		  • 3rd Party Threat Intelligence
		  • AttackMapper
		  • Takedown Services

Vendor	Headquarters	Product Names
Team Cymru	Florida, United States	• Pure Signal Recon • Pure Signal Orbit • IP Reputation Feed • Controller Feed (C2) • Botnet Analysis and Reporting (BARS)
Telos	Virginia, United States	• Telos Advanced Cyber Analytics
ThreatConnect	Virginia, United States	• ThreatConnect Threat Intelligence Platform • Intelligence-Powered Security Operations • ThreatConnect Risk Quantifier (RQ)
ThreatQuotient	Virginia, United States	• ThreatQ Platform • ThreatQ Investigations • ThreatQ TDR Orchestrator • ThreatQ Data Exchange
Verizon	New York, United States	• Threat Intelligence Services • Dark Web Hunting
ZeroFox	Maryland, United States	• ZeroFOX Protection • ZeroFOX Intelligence • ZeroFOX Disruption • ZeroFOX Response

Vendor	Headquarters	Product Names

Source: Gartner (May 2023)

Market Recommendations

The core of any TI program is priority intelligence requirements (PIRs), used to identify where the organization will focus intelligence efforts and what tools are required to achieve it. According to the SANS 2022 Cyberthreat Intelligence Survey, the percentage of organizations with documented PIRs fell almost 4% between 2021 and 2022 from 39% to 35.4%, and it stood at 30.3% in 2019. [1]

According to our client inquiries, a significant number of organizations are still at the bottom of the DIKI pyramid even after buying TI solutions. They are overwhelmed with data because they have not defined what they really need to focus on and care about. Security and risk management leaders must demand that PIRs be defined for their organizations before any TI product purchases are made (see **Define Threat Intelligence Requirements to Improve SecOps Efficiency**).

To help address these ongoing and systemic problems, Gartner has for a number of years recommended a simple and pragmatic way to get the most from TI services. At a high level, an end-user organization 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 in line with business objectives as well as ensuring it aligns with the maturity of your security program.

- Aggregate. Clients regularly use a dozen or more intelligence feeds/services. Therefore, it is critical to determine how, once you have got all the potential 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.

- Act. Even today, a key issue is actionability. Security and risk management leaders must understand knowing is not enough and they must be able to take action. Keeping PIRs in mind will be enormously helpful because you will not lose the end goal and can make sure that you are addressing the PIRs, no matter what you do.

Recommendations:

- Optimize TI investments by building a TI program which tailors predictions 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 risk quantification and 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 and Threat Sharing
MRTI	machine-readable threat intelligence
OFAC	Office of Foreign Assets Control
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
XDR	extended detection and response

Evidence

[1] **SANS 2022 Cyber Threat Intelligence Survey**, SANS Institute.

[2] **Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments** (PDF), Office of Foreign Assets Control, U.S. Department of the Treasury.

Note 1: Representative 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 85 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.