MARKET PERSPECTIVE

How Global Threat Intelligence Vendors Address the Nuances of Regional Markets

Cathy Huang Christopher Kissel Frank Dickson

THIS IDC MARKET PERSPECTIVE EXCERPT FEATURES ESET

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: How Global Threat Intelligence Vendors Address the Nuances of Regional Markets

This IDC Market Perspective is primarily focused on threat intelligence (TI) from non-U.S. vendors and the dynamics of international markets. The largest global regional consumer of threat intelligence is the United States, and the largest TI platform and service providers are headquartered in the United States. However, the adversary resides in all jurisdictions and attacks businesses and governments everywhere where there is an internet presence (which is to say everywhere).

Key Takeaways

- Global systems integrators and managed security service providers have a greater influence of threat intelligence purchase in international markets than in the United States.
- Threat intelligence should be actionable, and that dashboards and customer support should be offered in the native language of the threat intelligence purchaser.
- Threat intelligence collection is hampered by data sovereignty laws.

Recommended Actions

- Threat intelligence data should be expressed in terms of threats, tactics, and procedures preferably in the MITRE ATT&CK for enterprise framework.
- TI vendors should develop country-specific risk maps.
- TI vendors should be widely integrated with firewall providers, endpoint detection and response, SIEM platforms, and other cybersecurity defenses to quickly turn insights into response.
- The threat intelligence community has a fiduciary responsibility to assist law enforcement agencies.

Source: IDC, 2023

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC Market Perspective: How Global Threat Intelligence Vendors Address the Nuances of Regional Markets (Doc # US49127923). All or parts of the following sections are included in this excerpt: Introduction, Global Threat Intelligence and Global Clientele, Industry Dynamics, Different Types of TI Vendors, Detailed Vendor Examples, and Advice for the threat intelligence provider. Also included is Figure 1.

NEW MARKET DEVELOPMENTS AND DYNAMICS

Introduction

Threat intelligence (TI) is unique in that it enhances both prevention and detection in cybersecurity. If a threat intelligence vendor can find adversarial tactics in the wild or profile what has been exploited, hopefully the information can help populate firewalls or other malware-based detection systems; this being preventative. If a business is experiencing a series of indicators of compromise (IoC), the hope is that the IoCs can be correlated with the threats, tactics, and procedures (TTPs) of the adversary; this being crucial to detection.

Unfortunately, threat intelligence is becoming increasingly necessary. Threat actors were often opportunistic criminals. However, as witnessed in the ongoing geopolitical conflict between Russia and Ukraine, nation-state adversaries are getting actively involved to cause disruption to critical infrastructure organizations, including telecommunication, energy, government, healthcare, and transportation sectors.

The new ISO 27001 standard (formally launched on October 25, 2022) added threat intelligence as an important control, highlighting the growing importance of TI in an organization's security management. It sets a precedent for other certifications as well as regulation to increasingly mandate TI functions.

Moreover, threat intelligence is an important part of endpoint detection and response (EDR), extended detection and response (XDR), and really any flavor of incident detection and response (IDR) platform or approach. Very often, TI is an embedded feature of XDR that cybersecurity software vendors are purchasing or licensing threat intelligence to round out their XDR platforms.

Similarly, MDR vendors and managed security services providers (MSSPs) will leverage threat intelligence to augment and improve their services delivery because TI provides value in enhancing the efficacy and proactiveness of organizations' cyberdefense capabilities, whether it's threat investigation process or adversary identification and overall cybersecurity posture and prevention. The quality of TI is and will increasingly become a differentiator in terms of buying products.

Global Threat Intelligence and Global Clientele

The largest global regional consumer of threat intelligence is the United States. IDC estimates roughly 65% of TI revenue comes from United States–based business. Self-evidently, the wealthy and largest businesses buy the most TI, with financial industries, critical infrastructure, and governmental industries leading the way.

The largest TI vendors have headquarters and the majority of their analysts in the United States. Mandiant, CrowdStrike, Recorded Future, and Anomali are centered in the United States. Major consultancies such as Booz Allen and PwC have significant TI professional services. We note that these companies that we just mentioned also have global footprints.

The focus of this document though is on TI vendors that reside outside of the United States and non-U.S. global buyers. Every TI vendor has specific needs, but there are a few important differences between U.S. and non-U.S. TI buyers:

- Systems integrators and managed security service providers have greater influence with their clients than their U.S. counterparts have with theirs. In many markets, the systems integrators are a strategic advisor of cybersecurity tool purchases. In several markets, the large telecom companies such as Orange, BT, and LG Uplus provide threat intelligence and other cybersecurity tools to their clients.
- Regulatory environments in different regions effect what services TI vendors can offer. This is both good and bad for TI vendors. Data collection can be problematic for TI vendors due to data sovereignty laws (bad). Often, regulators such as the Monetary Authority of Singapore require that individuals affected by a breach are notified within 72 hours of the breach, this being a driver for TI vendors.
- Threat intelligence purchases may be more opportunistic in non-U.S. markets rather than persistent as it is in the United States. IDC has been tracking ransomware activities since 1H21. We learned that the sheer number of ransomware attacks in Asia/Pacific was significantly higher in 2H21 than in either 1H21 or 1H22.
- IDC believes that artificial intelligence and automation will have a positive effect on TI. Part of the expense of threat intelligence is the human curation of data sets. Artificial intelligence will find relevant patterns more quickly and automation will make the dissemination of TI easier and less expensive. TI as a SaaS becomes a practical product making TOI purchases more feasible for midsized companies globally.

Industry Dynamics

Even though the threat landscape has been constantly evolving, there is an enhanced level of optimism among cyberdefenders due to threat intelligence being shared more widely and technology improving. Structured threat information expression (STIX) and trusted automated exchange of indicator information (TAXII) are widely used as common languages for threat intelligence exchange or sharing. Moreover, the MITRE ATT&CK framework normalizes the language of threats, tactics, and procedures, enabling vendors to show where there are gaps, what the severities are, and how TI remediates the threat.

The creation of the Cybersecurity and Infrastructure Security Agency (CISA) in the United States facilitates the sharing of threat intelligence between private and public entities. Its Joint Cyber Defense Collaborative (JCDC) brings together the whole federal cyberinformation system on one platform focused on cyberdefense and operations. The JCDC alliance is made up of the largest technology companies that see bits of pieces of threat environments and then CISA can enrich it with various government views to have real-time continuous persistent collaboration to have a more complete picture of the risk for critical infrastructure organizations and others that can use the intelligence in their security efforts.

In the private sector, in August 2022, AWS, along with 17 other security vendors like Broadcom, CrowdStrike, IBM Security, Palo Alto Networks, and Splunk introduced the Open Cybersecurity Schema Framework (OCSF), with the attempt to address the inconsistency, incompleteness, and issues of data normalizing. Although the framework is not restricted to cybersecurity nor to security events, the initial focus of the framework has been a schema for cybersecurity events. In a world where every vendor has a different data structure, the framework has the great potential to curate heterogeneous data sets to create homogeneity to enable analysis.

Globally, different regulatory standards shape how threat intelligence vendors can go-to market. For example, established in May 2018, the German Privacy Act Bundesdatenschutzgesetz (BDSG) sets strict guidelines on how data collection and data processing is enabled in Germany. The net effect is that data containing personally identifiable information (PII) does not travel outside of German borders.

Different Types of TI Vendors

Worldwide Threat Intelligence Coverage Preview (TIP/TISS): Surfacing the Adversary Before They Disrupt You! (IDC #US49931022, December 2022) detailed out common threat intelligence use cases, capabilities, and some high-level trends. The focus of this document is on how different types of threat intelligence vendors address customer needs. It also has included three detailed vendor examples to illustrate how the vendors position their TI offerings and go-to-market plans for their threat intelligence.

Professional Services Firms

IDC decides to make only a subtle differentiation between threat intelligence platforms (TIPs) and threat intelligence security services (TISSs) because almost all threat intelligence is a combination of TIP and TISS. Nonetheless, we acknowledge there is a difference between a professional service firm like Booz Allen and TIP vendors. In fact, Booz Allen has a strong track record of winning big cybersecurity services, including threat intelligence contracts from the U.S. federal government.

Professional services firms tend to start their engagement with a detailed assessment, analyzing existing processes, intelligence needs, data sources, and stakeholder requirements. From there, the vendors will deliver specific threat intelligence services to client organization specifically. The service onboarding is developed in close partnership with the executive team, security leaders, and relevant stakeholders.

Global Systems Integrators

Many global systems integrators (GSIs) have comprehensive cybersecurity portfolios and balanced footprints across the EMEA, Americas, and APAC regions. Take an example of Wipro, an Indian-headquartered GSI that offers an integrated portfolio of risk and cybersecurity services across advisory, design, implementation, and managed services. The vendor does a great job in positioning its cybersecurity expertise and offerings including threat intelligence as a service, Secureye (i.e., brand name for its contextualized threat intelligence services) from a vertical-oriented approach, such as telecommunication, manufacturing, BFSI, and distribution.

Over the past few years, Wipro has made several notable acquisitions, such as Edgile and Ampion, which not only boost its cybercapabilities but also strengthen its region-specific advisory and delivery capabilities. For example, in August 2022, Wipro launched Wipro Shelde Australia, a sovereign cybersecurity offering for the Australian government and critical infrastructures based on its Ampion acquisition (i.e., Ampion is an Australia-based provider of cybersecurity, DevOps, and engineering services that was acquired by Wipro in April 2021).

Telecommunication Service Providers/Managed Security Services Providers

Telecommunication providers are uniquely positioned in the threat intelligence market. Take the example of NTT communications as one of the world's largest telecommunications providers. Its

Global Threat Intelligence platform can access up to 40% of the world's internet traffic and over 1200 honeypots across 23 countries. Since 2017, NTT has specifically included and enhanced user entity behavior Analytics (UEBA) and dark web crawls into its real-time analysis.

NTT has taken a highly integrated approach that customers can use a single point of contact to get a consolidated threat intelligence information that is based on a wide range of security domains. In addition, NTT combines its proprietary SIEM, machine learning, advanced analytics, and a team of experienced security analysts to deliver the security outcome per client's expectation.

Cloud Services Providers

While Google completed one of the biggest acquisitions ($5.4 billion with Mandiant) in the tech industry, Microsoft's threat intelligence capabilities and offerings are also attributed to relevant acquisitions the company made. In 2021, Microsoft acquired a late-stage start-up vendor RiskIQ in the threat intelligence and attack surface management domain for more than $500 million in cash. The combination of RiskIQ's attack surface management and threat intelligence empowers security teams to assemble, graph, and identify connections between their digital attack surface and attacker infrastructure and activities to help provide increased protection and faster response.

In the mid of 2022, Microsoft entered into an agreement to acquire Miburo, a cyberthreat analysis and research company specializing in the detection of and response to foreign information operations. Miburo's research teams detect, and attribute malign and extremist influence campaigns across 16 languages.

Threat Intelligence Start-Ups

Cybersecurity never lacks innovation. In the space of threat intelligence, there are many niche start-ups. Take an example of Cyjax, a United Kingdom–based threat intelligence start-up. It is established in 2012 with the mission to be the preeminent supplier of digital threat intelligence for enterprises, SMBs, and governments around the world. Its core cyberthreat intelligence platform, Cymon, works continuously to discover any known and unknown cyberthreats. The vendor uses its technology to investigate the deep and dark areas of the web and to bring to the surface risk information relevant to client organization.

Moreover, the vendor enables customers to meet the newly adapted cyberthreat intelligence requirements of the ISO 27001 framework.

Another example will be CYFIRMA, a threat discovery and cyberintelligence company founded in 2017. CYFIRMA is headquartered in Singapore, with offices located in the United States, Japan, Singapore, and India. Its core offering, DeCYFIR, is positioned as unique external threat landscape management (ETLM) platform to provide personalized, predictive, and multilayered intelligence (for more details, refer to the section titled as "Detailed Vendor Examples").

Digital Risk Protection Providers

IDC sees digital risk protection as adjacent to threat intelligence, but not the exact same thing. Take an example of ZeroFox, founded in 2013 with headquarter in Baltimore, United States. The patented ZeroFox SaaS technology processes and protects millions of posts, messages, and accounts daily across the social and digital landscape.

The primary use cases of its platform are externally focused: brand protection, domain protection, executive/VIP protection, dark web monitoring and threat actor engagement, adversary disruption/takedowns, breach response, and external threat intelligence. In the past 12 months, ZeroFox has delivered 2 million deep and dark web alerts and performed 630,000 takedowns. It can also help identify shadow IT in the form of new or potentially vulnerable or compromised IP addresses, and hostnames.

Detailed Vendor Examples

This excerpt was prepared for ESET but also included the following vendors: Cyberint, Cybersixgill, CYFIRMA, and Kaspersky.

ESET Threat Intelligence Services

Founded in 1987, ESET is still privately owned. ESET has its global headquarter and largest research and development center in Bratislava, Slovakia, with several others in Canada (Montreal), Czech Republic, Poland, and Romania. On top of these R&D facilities, ESET operates global offices in all key regions, including United States (San Diego). Globally, ESET employees over 2,000 people, and its largest product is endpoint protection and detection suite, which is used by more than 400,000 business customers. ESET has also thriving threat intelligence services that can improve ability to predict and prevent potential security incidents, thanks to geographically unique mix of curated TI data coming from European Union, CEE, Japan Asia, Africa, and Middle East, and actionable, targeted industry vertical cybersecurity research.

ESET threat intelligence consists of two main components: ESET Premium APT reports and ESET proprietary and curated intelligence data feeds. Data feeds are provided directly to its customers, depending on their organization's specific needs. The ESET approach to threat intelligence is strategic (threat actors and motivations; tactical [threats, tactics, and procedures]; operational [information about specific attacks and how they affect networks]; and technical [what are the indicators of compromise]). Specific feeds include a botnet, domain, URL, malicious files, IP, and APT feeds. Second, ESET supplements its data through its APT Reports PREMIUM. Twice a month, clients receive an Activity Summary Report and three times a month clients receive a technical analysis threat intelligence report and a month overview report for C-level executives about the threat research it has conducted. It should be noted that ESET practices are ISO 27001 and ISO 9001 certified and that ESET is a significant contributor to MITRE ATT&CK. Most recently, ESET has become a member of Joint Cyber Defense Collaborative.

ESET has thought about the chasm between threat intelligence feeds and how threat intelligence should be optimized for use by its customers:

- ESET provides feeds in JSON and STIX v2.0 formats.
- Through a TAXII server that is updated several times an hour.
- Out-of-the-box integrations with SIEM, SOAR, and other threat intelligence providers.
- Indicators of compromise with details (hashes, filenames, timestamp, first seen, etc.).
- YARA and Snort rules that can be imported to perimeter defenses to block threats.

ESET monitors nefarious threat actors everywhere on the globe. The company monitors activities from APT groups originating from China, Iran, the Middle East, Eastern Europe, North Korea, and Russia.

Worth noting for ESET is behind the scenes it uses advanced filtering to efficiently classify threat types and then ESET researchers add insights. The combination of supervised and unsupervised learning produces low false positive feeds. The data feeds have a confidence score allowing SOC teams to address the most serious threats first.

ADVICE FOR THE THREAT INTELLIGENCE PROVIDER

When studying various types of threat intelligence providers, especially the nuanced differences among United States–headquartered TI vendors versus non-United States–headquartered vendors, IDC offers the following advice to all TI providers:

Country-Specific Risk Map

Tracking global political events and malicious cyberactivity is a challenge for any organization. The key to effective "geocyber" protection is the level of research and knowledge to be country/region specific.

As such, a risk map that details recent attacks and threats taking place in a country or region and may also include information about legal developments, this can be particularly beneficial for companies engaged globally. In China, for example, it has been enacting laws that have an impact on foreign businesses operating there. By keeping track of these developments, TI can ensure the right parties are informed of any potential disruption to customers, team members, or operations in the country or region.

Articulate Results Along the Lines of the MITRE ATT&CK Framework

It may not be necessary to use the exact verbiage and formal language of MITRE ATT&CK for enterprise, but when a threat intelligence vendor uncovers an insight about how an adversarial TTP acts within an environment (that is how goes through initial execution, privilege escalation, lateral movement, collection phases, etc.), expressing this in this specific way is helpful. Most cybersecurity tools and SOC procedures are aligned to act in concert with MITRE findings.

Collaborate with Law Enforcement Agencies

It is highly beneficial when threat intelligence vendors work with national and regional law enforcement agencies such as INTERPOL, EUROPOL, police agencies, and Computer Emergency Response Teams (CERTs) worldwide. Very often, these TI vendors have the expertise to offer takedown services requested by these legal authorities.

Persona-Based Dashboard

A custom-built dashboard enables varying personas to tailor the threat intelligence and make it actionable. For instance, the marketing or PR team can monitor the organization's brand, while a purchasing team can track third-party suppliers, and physical security teams can stay informed about street protects that might be taking place close to the company's location.

Work with Other Cyberdefenders

Besides the previously mentioned Open Cybersecurity Framework, which helps define a common schema for data flowing in from security tools, the Cyber Threat Alliance (CTA) was founded in 2014 by a group of security practitioners from a few leading cybersecurity firms. Members of the CTA share information about cyberthreats in real time, allowing them to better understand and defend against emerging threats, with the goal of better protecting their customers and the broader internet community from cyberthreats. As of September 2022, CTA has 36 members headquartered in 11 countries. The members have shared over 280 million observables along with associated context, averaging around 350,000-400,000 per day.

Expand the Use Case of Threat Intelligence

The traditional approach to penetration testing has proven effective in helping organizations identify common vulnerabilities in systems and business applications. Financial regulators like the European Central Bank are now demanding a more holistic approach to testing an entity's ability to anticipate, prevent, detect, and respond to sophisticated attacks. A threat intelligence-led red team test involves the use of techniques to simulate an attack on an entity's critical functions and underlying systems (i.e., its people, processes, and technologies).

LEARN MORE

Related Research

- *Worldwide Threat Intelligence Coverage Preview (TIP/TISS): Surfacing the Adversary Before They Disrupt You!* (IDC #US49931022, December 2022)
- *What Threat Intelligence Platforms and Threat Intelligence Security Services (TIP/TISS) Are Asked in a Request for Proposal (RFP)* (IDC #US49933622, December 2022)
- *Can Google and Mandiant Stick the Landing, or Will We Be Left None the (m)Wiser?* (IDC #US49935022, December 2022)
- *Worldwide Tier 2 SOC Analytics and Cloud-Native XDR Forecast, 2022-2026: Will XDR Become the Shining Light in a Dimming Global Outlook?* (IDC #US47705521, November 2022)

Synopsis

This IDC Market Perspective provides an overview of how different types of threat intelligence (TI) vendors offer their TI offerings and meet customer needs. Threat intelligence becomes a requisite today to empower faster threat investigations and efficacy of security operation centers, thus enhance the proactiveness of organization's cyberdefense capabilities. It also has included three detailed vendor examples to illustrate how the vendors position their TI offerings and go-to-market plans for their threat intelligence.

"When studying various types of threat intelligence vendors, it is interesting to see big influence of security services vendors like global systems integrators, telecommunication providers, MSSPs in the TI market. It implies the importance of process and people, in addition to the technology and platform in order to make TI function powerful and actionable," says Cathy Huang, research director, Worldwide Security Services at IDC.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright Notice