Issue 1

Executive Perspectives on Cyber Threat Intelligence

Understanding the Options, the Value, and the Market

Welcome

Today, most IT executives recognize that intelligence is a critical weapon against advanced cyber attacks. Many have seen the strategic planning assumption from Gartner analysts Rob McMillan and Khusbu Pratap:

"By 2018, 60% of large enterprises globally will utilize commercial threat intelligence services to help inform their security strategies."

Yet the market for cyber threat intelligence (CTI) services is still relatively young, and it is not always clear what options are available. This document offers research and analysis describing the what, why and who of cyber threat intelligence and security intelligence services.

The first section, from iSIGHT Partners, outlines a spectrum of options, from basic signature and reputation feeds to genuine cyber threat intelligence. It then describes the advantages of investing in cyber threat intelligence, including greater visibility into threats, faster response to targeted attacks, better executive communication, and improved strategic planning and investment.

The second section is a research note from Gartner, the world's leading IT advisory firm. In a report titled Market Guide for Security Threat Intelligence Services, analysts Rob McMillan and Khusbu

Pratap discuss the need for threat intelligence, the market for threat intelligence services, and leading vendors in the field. I call your attention particularly to the sections:

- Key Findings and Recommendations (page 6)
- Market Definition (page 6)
- Use Cases (page 8)
- Vendor Capabilities Vary (page 11)

The third section offers some basic information about iSIGHT Partners.

Featuring research from Gartner

iSIGHT Partners was founded eight years ago with the mission to fundamentally change the business of cyber security. To that end we:

- Built one of the largest and most capable cyber intelligence organizations on the globe: our team includes more than 250 experts from cyber security, law enforcement and the military and intelligence communities.
- Created a comprehensive intelligence platform to accelerate and enhance the collection, analysis and rapid dissemination of actionable cyber intelligence.
- Invested eight years exploring the online threat underground and compiling a comprehensive knowledgebase of the identities, motivations and techniques of opponents, including cybercriminals, cyber espionage actors and hacktivists.

And we are always guided by the principle that intelligence must be actionable, easy to apply, and directly connected to business objectives.

If you have questions or comments about the information in this document, or would like to explore cyber threat intelligence in more depth, please don't hesitate to contact us at info@isightpartners.com.

Sincerely,

John P. Watters
Chairman and CEO, iSIGHT Partners

Cyber Threat Intelligence: What is it, and What are the Real Advantages?

Surviving in the age of targeted attacks

We have reached the age of advanced targeted attacks. Although enterprises must still protect against mass campaigns, the most serious data breaches and disruptions are the result of well-planned, complex attacks that target specific companies or industries.

Recent highly publicized cases include cybercriminals targeting retailers, banks and others for financial gain, and "hacktivists" and state-supported hackers threatening media companies, financial institutions and government agencies for political purposes. Other examples include private and government-supported companies stealing engineering and business process information from defense firms and manufacturers, and financially savvy hackers targeting healthcare and pharmaceutical companies for inside information driving stock prices.

These innovative adversaries are continuously morphing existing attack methods and developing new ones. They cannot be stopped with firewalls, intrusion prevention systems and antimalware software alone. Their actions cannot be detected with more malware signatures or additional reports on last year's campaign techniques. In fact, most enterprises are swamped by too much raw threat data: too many alerts, too many vulnerability warnings and patches, too many reports about every kind of malware, phishing attack and DDoS variation.

Clearly, enterprises need threat intelligence. But as Rob McMillan and Khushbu Pratap of Gartner warn, "not all 'threat intelligence' is the same."

What separates basic threat data feeds from genuine cyber threat intelligence? What kind of intelligence can inform you about next week's attacks instead of last year's, and help you focus on the ten alerts a day that really matter out of the thousands you see?

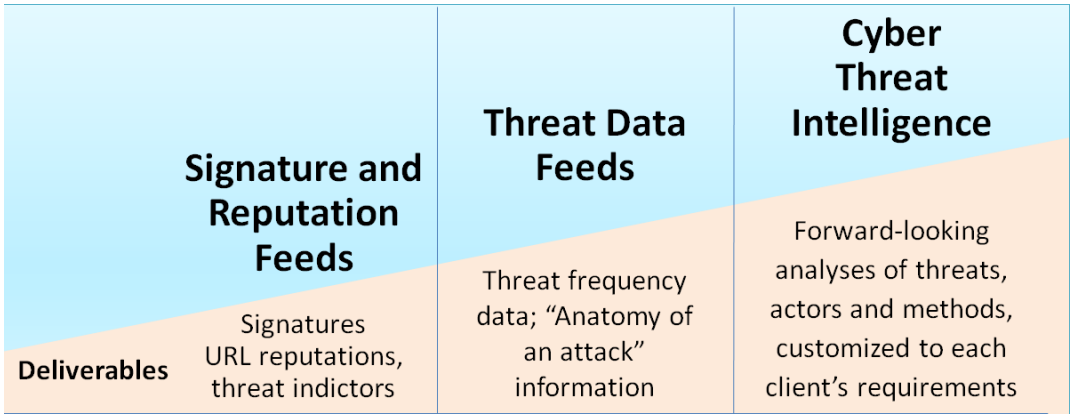
Threat information services can be placed on a spectrum that runs from *signature and reputation feeds, to threat data feeds, to cyber threat intelligence,* as shown in Figure 1.

Signature and reputation feeds typically take the form of malware "signatures" (file hashes), URL reputation data, and intrusion indicators, sometimes supplemented by basic statistics (e.g., "Today's top 10 malware threats"). The primary value of threat data feeds is to improve the effectiveness of next-generation firewalls (NGFWs), intrusion prevention systems (IPSs), secure web gateways (SWGs), anti-malware and anti-spam packages and other "blocking" technologies.

"Be aware that not all 'threat intelligence' is the same. Some vendors do not offer much more than information about IP addresses and the implication of URLs in current activity. This provides you with an ability to respond rapidly to the contemporary threat environment, but does not inform you about what may happen in the next month or the next year."

Rob McMillan and Khushbu Pratap, Garter Research Note: Market Guide for Security Intelligence Services

FIGURE 1 A spectrum of threat information services



Source: iSIGHT Partners

Signature and reputation feeds are one facet of a defense-in-depth strategy, but their limitations are quite clear. While they help block mass attacks, they miss targeted attacks for which no signatures exist. While they provide data on individual threat indicators, they don't supply context to help organizations discern whether they, or their employees or customers, are being targeted. And the vast quantities of signatures and reputation scores usually cause SIEM systems and firewalls to generate more alerts than security teams can possibly evaluate.

Threat data feeds include statistical breakdowns on the prevalence, source and targets of common malware and attack activities. Sometimes the staff of the vendors research team publishes "anatomy of an attack" discussions that enumerate the actions taken by a specific piece of malware, or the sequence of actions observed in an advanced, multi-stage attack. Threat reporting is valuable for SOC and IR teams, because it helps them identify patterns associated with attacks.

But most analysis from "threat labs" suffers from key handicaps. Data gathering is passive ("what did we see on our firewalls and network sensors?") and often skewed to the geography and industry profile of the vendor's customer base. Analysis is backward-looking ("here is what we observed attacking networks over the past six months"). There is no intelligence that can be used to recognize what new tactics and techniques malicious actors are planning to employ, or evidence of successful breaches that have not yet been detected.

Cyber threat intelligences (CTI) includes the base level data from signature and reputation feeds and threat data feeds, but goes beyond them in several critical areas. It includes active human and technical information gathering and analysis on a global scale. That means continuously monitoring hacking groups and underground sites where cybercriminals and "hacktivists" share ideas, techniques, tools and infrastructure. It also requires building a staff with diverse language skills and cultural backgrounds who can understand the motives and relationships of adversaries in China, Russia, Eastern Europe and other havens.

Also, CTI is adversary-focused and forward looking, providing rich contextual data on attackers and their tactics, techniques and procedures (TTPs). It might include, for example, determining the motivation and targets of a new variety of cybercriminal, the vulnerabilities they target, the domains, malware and social engineering methods they use, the structure and evolution of their campaigns, and the techniques they are likely to employ to evade current security technologies and practices.

Finally, CTI is customized for each client. A genuine cyber threat intelligence service gathers situational data and intelligence requirements from each client, and provides analysis tailored to the industry, technologies and specific situation of that organization. Top-quality CTI companies provide direct access to analysts, so clients can receive in-depth clarification on intelligence, and submit malware samples for detailed analysis. Customized information gives enterprises the extra context to set priorities and make optimal decisions based on their specific needs and risk profiles, rather than broad industry averages.

Why CTI? It's not just detecting more targeted attacks

Greater visibility into threats

Clearly one of the advantages of CTI is greater visibility into threats. Researchers who are native language speakers, knowledgeable about different cultures, and familiar with slang and colloquial terms can uncover new threat groups, in new locations, who use new malware variants and new social engineering techniques. CTI gives the security staff insight into new indicators of compromise (IOCs) and other clues so they can prevent and detect more attacks. It also gives IT managers and security analysts insight into what applications, systems, and user populations are most likely to be attacked, so efforts can be focused on protecting those high-risk targets.

Faster response to targeted attacks

CTI also supports faster response to targeted attacks. CTI services give security teams detailed information on which threats are most likely to affect the industry and situation of their firm. This "shrinks the problem" by allowing the teams to focus on the small number of alerts and notifications tied to attacks that represent real threats to that specific company. The contextual threat analysis provided by CTI services enables SIEM tools to automatically raise the priority of truly meaningful alerts. They also provide the

context required for security team members to recognize patterns of events that point to specific adversarial campaigns.

Vulnerability patching is another area where CTI can help organizations respond faster to immediate threats. Rather than prioritizing patching efforts based on generic "critical/important/moderate/low" ratings, an organization can prioritize patches based on rich information about each vulnerability, such as how it works, how hard it is to exploit, and whether exploit tools are currently available in the wild. Better prioritization means closing the window faster on immediate threats, rather than wasting time on vulnerabilities labelled as "critical" that in fact pose little risk.

Better executive communication

CISOs often face serious challenges communicating information about security issues to business managers, top executives and Boards of Directors. This makes it extremely difficult to obtain the cooperation – and the funding – justified by actual security threats. CTI provides information that can put a face on adversaries, clarify their motivations, and enable CISOs to better translate cyber threats into business risks.

CTI also provides CISOs with an enhanced business risk vocabulary with terms that are meaningful to non-technical executives. Instead of using technical terms ("last week we evaluated 1,000 alerts and blocked 200 pieces of malware") security managers can talk with the CFO or a division general manager using statements like: "last week we thwarted attacks by a hacktivist group in Eastern Europe bent on degrading our web site and damaging the corporate brand."

Improved strategic planning and investment

CTI services can provide concrete evidence and informed analysis about emerging adversaries and new types of threats. This information can direct enterprises toward planning and investment decisions that improve their security posture while reducing unnecessary risk and spending. Conversely, intelligence can show that some threats are not relevant to specific industries or company types, saving enterprises from investing scarce resources in the wrong places. By improving strategic planning and investment, and by making security teams more effective, CTI services help IT security groups deliver more "bang for the buck."

Source: iSIGHT Partners

In the Market Guide for Security Threat Intelligence Services, reprinted below, Gartner analysts Rob McMillian and Khushbu Pratap highlight a number of key capabilities for top cyber intelligence vendors. These include: content based on infiltrating threat actor groups, content from closed (non-public) as well as open sources, raw material collected and interpreted from non-English-speaking sources, correlating and analyzing disparate data points to draw informed conclusions, content tailored to the risks your organization must manage, and content disseminated in a form your organization can consume.

Contact iSIGHT Partners to learn how we provide these capabilities and more: info@isightparnters.com.

From the Gartner Files

Market Guide for Security Threat Intelligence Services

Threat intelligence helps CISOs use their security spend more efficiently and combat their adversaries more effectively. Threat intelligence services are not easily compared, and CISOs must understand the market to determine which service provider is right for their needs.

Key Findings

- Client interest in commercial threat intelligence services has grown in recent years, and these services are now being utilized across vertical industries other than the traditional government and financial services sectors.
- The term "threat intelligence" is often misunderstood and sometimes misrepresented. Consequently, prospective purchasers do not always understand what service they actually need, or what they are buying.
- The number of vendors purporting to provide threat intelligence services has grown remarkably in the past couple of years. The diversity of expertise and content has created an environment in which purchasers struggle to compare services.
- The value of these services will be constrained by the customer's ability to absorb and, especially, react to the information provided by the services.

Recommendations

Chief information security officers (CISOs):

- Use a commercial threat intelligence service to develop informed tactics for current threats, and to plan for threats that may exist in the midterm future.
- Clearly understand the type of intelligence that you need and how it is to be utilized. Many vendors can provide raw information, but only a comparative few provide truly anticipatory content based on customized intelligence.
- Use this research to determine the right vendor for your threat intelligence requirements. Important elements to consider include the vendor's intelligence capabilities and processes, quality of information sources, format and quality of the deliverables, and pricing.

Strategic Planning Assumptions

By 2018, 60% of large enterprises globally will utilize commercial threat intelligence services to help inform their security strategies.

By 2020, 30% of global enterprises will have been directly compromised by an independent group of cyberactivists or cybercriminals.

Market Definition

"Threat intelligence" is evidence-based knowledge — including context, mechanisms, indicators, implications and actionable advice — about an existing or emerging menace or hazard to IT or information assets. It can be used to inform decisions regarding the subject's response to that menace or hazard.

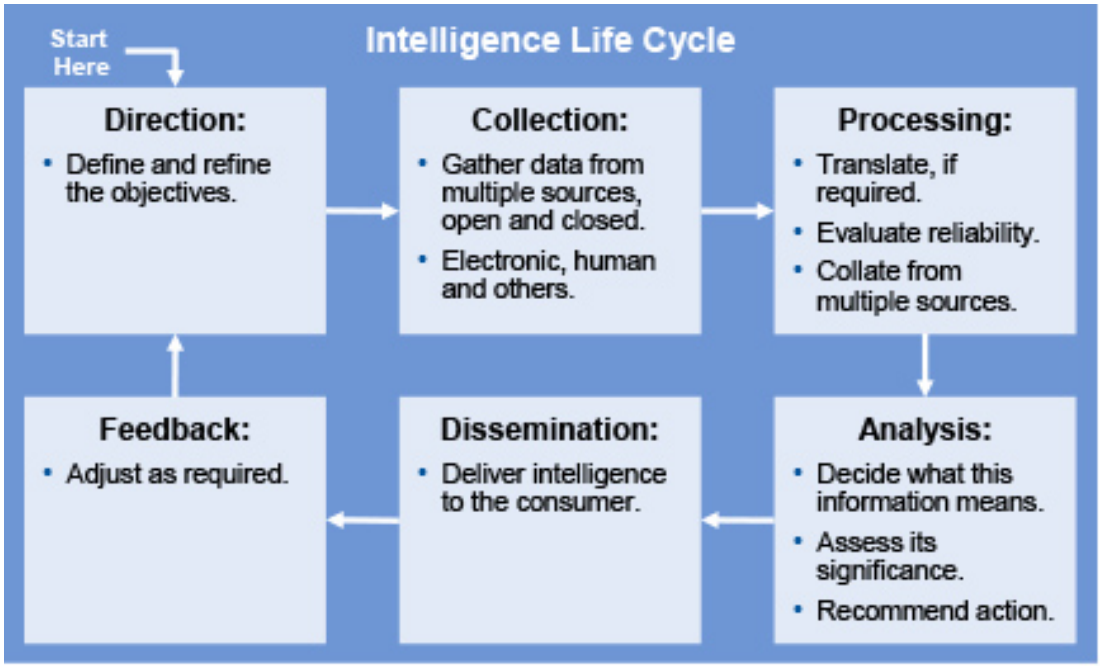
A full definition is available in "Definition: Threat Intelligence." In its traditional sense, "intelligence" is the product of a process, rather than a series of individual data points (see Figure 1).

Threat intelligence services are commercial service offerings that provide knowledge about information security threats and other security-related issues. They also are able to provide various degrees of information about the identities, motivations, characteristics and methods of attackers. This information is derived from technical sources (for example, network traffic and files retrieved from malware archives) and human sources (from example, the infiltration of hacker groups and fraud groups, as well as liaison work with law enforcement).

Service Segmentation

A segmentation model for threat intelligence services is described in "How to Select a Security Threat Intelligence Service." Table 1 provides an extract of that model, which is used to segment the vendors listed in Table 2.

FIGURE 1 Typical Intelligence Life Cycle



Source: Gartner (October 2014)

Table 1. Threat Intelligence Sample of Services Segmented

Degree of Value-Added Interpretation	Core Threat Intelligence	Value-Added Adjacent Services
Higher	**Group 1: Acquisition and Analysis** • Hacker and/or fraudster community infiltration • Social media and open-source monitoring • Targeted vulnerability research • In-depth, custom-made artifact analysis	**Group 2: Incident Recovery Support** • Brand monitoring and protection • Credential recovery • Incident investigation • Phishing site takedown
Lower	**Group 3: Real-Time Monitoring and Notification** • Network activity portal • Real-time event notification	**Group 4: Incident Diagnostics** • Fraudulent transaction correlation and notification • Bogus domain name detection
Source: Gartner (October 2014)		

The key offerings for the purposes of this Market Guide are Group 1, "Acquisition and Analysis," and Group 3, "Real-Time Monitoring and Notification." This research focuses only on core threat intelligence (Groups 1 and 3), and does not include any consideration of value-added adjacent services (Groups 2 and 4).

To be included in this market, the service must be available for purchase as a discrete offering.

Generally, vendors in this market generate their own original content, or alternatively provide what we consider to be an original and substantial interpretation of existing content harvested from other sources. Some vendors in this research are more focused on intelligence sharing or analytics platforms, which aggregate information from other sources and possibly add some metadata that they generate. We consider their inclusion in the market to be marginal. Since the end product is still an intelligence feed and there is some added content (that is, metadata), those vendors are included in this Market Guide, but may be excluded in future versions as the market continues to evolve and segment. Examples of vendors that fall within this category include Codenomicon, Lookingglass and ThreatStream.

Group 1, Acquisition and Analysis, most closely resembles "pure" intelligence in that it usually draws from several types of sources (for example, electronic and human); incorporates factors such as the intent of the threat actors; develops content that has been subjected to a reasonable level of analysis by a human; and delivers intelligence, typically including narrative analysis, that is tailored for the customer and preferably contains some type of anticipatory content.

Group 3, Real-Time Monitoring and Notification, reflects the broader, lay interpretation of the term "intelligence," which has gained a foothold in the market. It refers to information about operational activity that has already occurred and is usually viewed through a technical lens. It does not incorporate any substantial analysis that gives information about the activity beyond indicators harvested from technical sources, nor does it give any depth of insight about the intent behind the activity or its meaning in terms of future developments. Feeds of botnet command-and-control IP addresses are an example of this.

Client Profile

Threat intelligence service clients typically have assets of significant value (for example, substantial financial assets or intellectual property, or assets that support critical national infrastructure), protected or otherwise sensitive information (for example, user identities or classified security information), leverageable services (for example, network bandwidth) or large customer bases. The information obtained from the service often feeds into a multiyear planning and deployment cycle.

Threat intelligence services are likely to appeal to large enterprises that have significant brand presence or higher-risk profiles, and generally have security organizations with more mature security programs. Some service providers are, however, expanding their focus to include midsize organizations.

The limiting factor for small businesses in deriving value from these services is their capacity to act on the intelligence they receive. They may find that monitoring publicly available sources of threat information — such as the United States Computer Emergency Readiness Team (US-CERT) and the SANS Internet Storm Center — addresses their needs adequately.

Use Cases

Clients use information from threat intelligence providers to achieve a wide variety of objectives. For example:

- Develop insights into the identity, motives, and potential methods and actions of hackers, fraudsters, and other adversaries that are targeting the client or the client's vertical industry so that:
- Hazardous situations may be avoided or mitigated.
- Current defensive controls may be adjusted prior to an attack, if possible.
- Future planning is relevant to the emerging threat.
- Diagnose an incident more efficiently and effectively.

- Obtain advance warning of impending attacks against shared IT infrastructure (for example, the global Domain Name System [DNS]), infrastructure controlled by the clients' IT organizations, or online services provided to customers and partners.
- Develop case studies for use during internal incident response training exercises and business continuity management efforts.
- Gather information about emerging malware and other malicious code threats.
- Prioritize vulnerability management activities based on risk criteria that include the likelihood of a given threat materializing.
- Monitor changes to the external environment to define triggering events that will require an infrastructure refresh.
- Assess the preparedness of IT managed service providers.
- Provide security-related input into architectural and procurement decisions.
- Identify issues that may have implications beyond the IT security field (for example, potential brand, legal or business development impacts).

Purchase Justification

Collating, correlating, assessing and analyzing the information that delivers the intelligence product that is ultimately disseminated can be labor-intensive, and requires specialized expertise that is difficult and expensive to obtain. External threat intelligence services provide a cost-effective method to achieve this.

Furthermore, engagement with potential or actual adversaries may bring unwanted attention to the client from those communities. Use of an external service provides a mechanism to gather information at arm's length, thus avoiding scrutiny.

Market Direction

The Market Is Growing in Size and Diversity

We estimate that the market had a total value of $159 million for 2012 and $255 million for 2013, with an annual growth rate of 61%. Average deal sizes range from the low tens of thousands of dollars to the high hundreds of thousands of dollars. The majority of vendors in this market currently generate less than $10 million in revenue from threat intelligence services.

Clients of these services include end-user organizations (government and commercial), managed security service providers (MSSPs) and technology providers.

Gartner's interaction with threat intelligence service providers indicates that traditional consumers of commercial threat intelligence services are government and financial services, and these continue to be the largest consumers. Some organizations (particularly in financial services) use multiple providers, with each provider engaged to either correlate information from disparate sources or, alternatively, fulfill a particular purpose.

However, other vertical industries are now using these services as well, such as airlines, healthcare and health insurance, oil and gas, pharmaceuticals, energy and utilities, and retail and manufacturing.

Pricing Models Are Evolving

Intelligence services are generally based on a subscription model, in which a fee is paid for access to the services for a period of time, such as a year. Different price points may be available for different tiers of service, and this has been driven largely by the need to develop new business in the midmarket. Some vendors have indicated a willingness to negotiate pricing in order to win business. Pricing for annual subscriptions can range from the low tens of thousands of dollars for basic services up to $500,000 or more for sophisticated offerings, with the backing of more comprehensive research lab and human analysis capabilities.

The pricing structure for adjacent services depends on the specific service. For example:

- Brand monitoring may be based on a subscription model.
- Incident investigations may be based on time and materials.
- Site takedowns may be based on a cost-per-event model (for example, with a set number of takedowns in a year included as part of the service, and then an extra cost per takedown thereafter).

Threat Intelligence Exchange Marketplaces Have Emerged

A number of vendors are expanding their service offerings to include platforms that provide value beyond a given vendor's own threat intelligence service.

The first style of platform is effectively a collaboration platform that allows clients to organically form their own online communities to discuss issues of mutual interest. These are effectively social media platforms for security professionals to discuss the threat environment. The IID ActiveTrust platform is an example.

The second style of platform is somewhat akin to an "app store" for threat intelligence content. These platforms allow clients to select different types of content from different sources, including third-party sources.

For example, Check Point announced ThreatCloud IntelliStore in May 2014, and it currently features content feeds from seven other vendors, including CrowdStrike, IID, iSIGHT Partners, SenseCy and more. The arrangement between Check Point and iSIGHT Partners is interesting in that, once an indicator of compromise (IOC) is detected by a Check Point device, the Check Point customer can then get further information about that IOC from the iSIGHT Partners feed.

Cyveillance is another example of a vendor that offers such a platform. This platform allows customers to select feeds from different suppliers, depending on need and budget.

Threat Intelligence Is Integrating With Adjacent Capabilities

One of the benefits of threat intelligence is that it improves decision making in core security processes, such as incident response and policy enforcement. Technical information, such as IP reputation or log extracts, is not as useful in isolation as when other information about the adversary (for example, motive and means) or context (for example, targeting of specific vertical industries or business processes) can be applied.

CISOs and other officers are often required to answer executive questions, such as:

1 Why is a particular policy change being implemented?

2 What is the external incident that occurred? What is its relevance to us?

3 Was the unusual activity we saw a case of an insider acting with malevolence, or an external adversary gaining control of an innocent user's account? How bad is it?

4 What may happen next or at some point in the longer-term future?

The contextual information that threat intelligence can provide, particularly from an Acquisition and Analysis service, allows the technical information to be interpreted in context. This is important for separating actual or potential incident activity from false positives.

Consequently, there is growing integration of threat intelligence content with adjacent activities, such as security monitoring, incident response and forensic assessment. For example:

- iSIGHT Partners provides an intelligence feed to the Co3 Systems incident response platform.
- Mandiant, which is now owned by FireEye, initially established its position in the market on the basis of its forensic capabilities, and subsequently developed a threat intelligence service.

It is likely that, in the short term, more MSSPs will offer threat intelligence capabilities as well, either as a native capability or as a channel partner for an existing threat intelligence service provider. Dell SecureWorks is an example of a vendor that currently provides services in both markets. This may prove to be attractive to organizations in the midsize market.

Vendors Are Waiting on Customers to Mature

Several vendors have noted that the demand side of the market still has to mature before the value of Real-Time Monitoring and Notification services is fully realized.

A key element of this maturation will be clients' ability to absorb intelligence content more effectively, particularly via automation. Some vertical industries are enthusiastic to adopt Structured Threat Information eXpression- (STIX-) formatted intelligence information; however, many clients currently are not in a position to consume standard formats like this.

This will change as clients seek to leverage threat intelligence to prevent hostile action, instead of merely detecting it.

This requirement means that clients must have access to and implement products that are able to consume intelligence content drawn from multiple data sources.

Market Analysis

Vendors Share Information

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

Vendors do share some intelligence content collaboratively. This does not mean that a particular vendor's offering is exactly the same as another vendor's offering; it simply means that some content will be common to both because it comes from the same source. Vendors do this to provide a greater volume of content or richer content, particularly where a sharing partner operates in a different market or offers a differentiated service.

Examples of groups of vendors that share information include the following (see Note 1):

- CSIS Security Group, Fox-IT and Group-IB
- Check Point and iSIGHT Partners, and other ThreatCloud IntelliStore vendors
- IID and Malcovery

These collectives are an example of the way in which the market will continue to evolve within the context of the Coalition Rule scenario.

Vendor Capabilities Vary

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

Collection, processing and analysis of raw information can be a differentiator. Depending on client requirements, the vendor's capability in the following areas may be important:

- Whether the content is based only on logs from current network activity, or whether the vendor infiltrates and communicates with threat actor groups
- Whether the content is gathered only from open sources, or includes closed (nonpublic) sources as well
- Whether the raw information is harvested from English-speaking sources only, or whether the vendor collects and interprets non-English sources as well
- Whether the vendor provides a series of individual data points, or, alternatively, correlates and analyzes disparate data points and draws informed conclusions
- Whether the vendor has the capability and capacity to tailor the content specifically to the risks (for example, infrastructure attacks, fraud) that your organization must manage
- Whether the vendor disseminates the content in a form that your organization can consume

On this last point, vendors that provide only Real-Time Monitoring and Notification services tend to focus only on technical sources. Vendors that provide Acquisition and Analysis services may also include other relevant information, such as geopolitical or economic factors.

The ability of multilingual analysts to synthesize content from different communities is a differentiator. Approximately 25% of vendors (mostly Acquisition and Analysis vendors) report that they have multilingual capabilities, and a very small number (for example, iSIGHT Partners, SenseCy and Verisign iDefense) also have staff members located in particular locales. One vendor has noted that the depth of analysis is improved by having analysts who not only speak multiple languages, but also understand the linguistics so that nuances and intentions can be more effectively comprehended.

Demonstrating the Value Proposition

One of the challenges for vendors providing Acquisition and Analysis content is convincing senior management within client organizations of the value of the service, which can be expensive

(see Note 2). Gartner's expectation is that this will change in the midterm as board-level interest in security and security planning continues to grow.

On the other hand, Real-Time Monitoring and Notification services have gained in popularity because end-user organizations have had to respond quickly to change in the external threat environment. The generally less expensive price points make these services more easily affordable. A number of vendors now provide APIs that allow machine-readable threat intelligence (MRTI) to be accessed more easily, and it is becoming a key channel for the consumption of content in some cases.

The advent of MRTI has overcome a problem that some vendors have observed within client organizations, as explained below. In some end-user organizations, operational teams often would not receive intelligence content that could be used to defend the organization. This would occur because the team primarily consuming the service — usually the security team — would use that content for its own purposes, but neglect to relay any relevant content to the operational teams.

MRTI provides operational teams with up-to-date information about the current environment, thus allowing dynamic changes to security controls (for example, intrusion prevention systems) as conditions change. This is particularly valuable with respect to defense against Day 0 attacks.

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.

A summary of service offerings, which was described in the Market Definition section above, is provided below. Since vendors tend to have subtle differences between their offerings, mapping each vendor to this segmentation matrix is not always an exact science. Table 2 provides what Gartner considers to be a reasonable mapping of vendor offerings to the market segmentation approach discussed earlier.

Even where multiple service providers cover a single service group, there may be differences in the extent and quality of their offerings. For example, some vendors that have been placed in Group 1 (Acquisition and Analysis) deliver a reasonable level of customized analysis for clients, thus providing a case for their membership in that group, since customized analysis goes beyond what is typically provided in Group 3 (Real-Time Monitoring and Notification). However, only some of those vendors provide anticipatory content — that is, they make predictions about how the client may be attacked or how the threat environment may evolve, and they outline response options for the client before these events occur. This type of content is a clear differentiator between two vendors that may both appear in the Acquisition and Analysis group (see Table 2).

A summary of each vendor is provided below (also see Note 3). Each summary includes guidance on relative pricing expectations. To develop this guidance, we asked each vendor to explain how its pricing model works and what its average deal size is. As discussed above, pricing models are not consistent across the market. Furthermore, each client has its own requirements; thus, the price for a service offering consumed by each client is highly variable. Consequently, the guidance that we provide below is of a general nature, and a particular client may find that its own requirements result in a pricing arrangement that varies from the relative guidance provided.

In that context, we have framed guidance regarding pricing expectations within the following structure:

- Deals below $100,000 per annum are considered to be at the low end of the spectrum.
- Deals above $500,000 per annum are considered to be at the high end of the spectrum.
- Deals between $100,000 per annum and $500,000 per annum are considered to be midrange.

BAE Systems Applied Intelligence

This is one of five firms certified by CESG within the U.K. to assist in the response to security incidents on networks of national significance. This work and the vendor's MSSP business partially inform its intelligence content. BAE Systems Applied Intelligence appears to have a strong process underpinning its capabilities. The company has a major focus in the U.K., the U.S. and Australia, and has a presence in 28 countries across EMEA and the Asia/Pacific region. BAE Systems Applied Intelligence has relatively strong links to government. Pricing tends to be in the midrange of the spectrum.

Table 2. A Representative List of Threat Intelligence Service Providers

Vendor	Headquarters	Group 1:Acquisition and Analysis	Group 3: Real-Time Monitoring and Notification
BAE Systems Applied Intelligence	Guildford, U.K.	X	X
Booz Allen	McLean, Virginia	X	
BrandProtect	Mississauga, Ontario	X	X
Check Point Software Technologies	Tel Aviv, Israel		X
Codenomicon	Oulu, Finland		X
CrowdStrike	Irvine, California	X	X
CSIS Security Group	Copenhagen, Denmark	X	X
Cyveillance	Reston, Virginia	X	X
Dell SecureWorks	Atlanta	X	X
Digital Shadows	London	X	
FireEye (Mandiant)	Milpitas, California	X	X
Fox-IT	Delft, Netherlands	X	X
Group-IB	Moscow	X	X
IBM (Internet Security Systems)	Armonk, New York	X	X
IID	Tacoma, Washington		X
iSIGHT Partners	Dallas	X	X
Lookingglass	Arlington, Virginia		X
Malcovery	Birmingham, Alabama	X	X
Norse	San Mateo, California	X	X
One World Labs	Denver	X	X
RSA, The Security Division of EMC	Bedford, Massachusetts	X	X
SenseCy	Netanya, Israel	X	X
Symantec	Mountain View, California	X	X
Team Cymru	Lake Mary, Florida	X	X
ThreatStream	Redwood City, California		X
Verisign	Reston, Virginia	X	X
Webroot	Broomfield, Colorado		X

Source: Gartner (October 2014)

Booz Allen

Booz Allen has a strong focus on customized, predictive intelligence. Consistent with this, analysts constitute a comparatively high proportion of its staff. Booz Allen appears to have a strong process underpinning its capabilities. It derives the vast majority of its business from North America, with a minor presence in EMEA. Its primary vertical industry is financial services, with a smaller presence in manufacturing and natural resources, and others. Booz Allen is on the more expensive end of the pricing spectrum, which is not surprising, given the focus of its product.

BrandProtect

BrandProtect's major focus is on brand monitoring and, to a lesser extent, anti-phishing, rather than on intelligence about direct attacks against client infrastructure. Therefore, it is a marginal entrant in this market. Within the context of brand

monitoring, this vendor is seen by others as a legitimate competitor. Its intelligence approach is quite simple: It relies on the monitoring of keywords in various channels, most notably social media. Its pricing is structured so it can service smaller and larger clients. The majority of its business is in North America, with financial services being its major vertical industry.

Check Point Software Technologies

Check Point's services are confined to intelligence about current activity rather than predictive intelligence. It provides feeds that include malware signatures, file indicators, and address indicators that can be used by Check Point devices (only) to make real-time policy decisions. Pricing is very much at the low end of the spectrum — one of the least expensive offerings in this market — which is to be expected because the service is relatively basic in the context of this market. Check Point is well-established globally via its other product lines.

Codenomicon

Codenomicon's offering is different from most vendors in that the deliverable is a software platform (AbuseSA) rather than a traditional style of information delivery service. This vendor does not generate its own intelligence, thereby making it a marginal inclusion in this market; however, its platform, which aggregates information harvested from other sources, is sufficiently noteworthy to include it at this time. Codenomicon's key market is the government sector in EMEA, particularly national computer security incident response teams (CSIRTs).

CrowdStrike

CrowdStrike is a relatively new company, but it has established a solid reputation for expertise. Intelligence content covers the full spectrum of decision-making horizons, from short-term (for example, minutes) operational decisions, either by humans or by automation, to long-term (for example, five years) strategic decisions. Pricing is toward the medium to high end of the spectrum, which is to be expected given the service offerings, and potential clients notice this. The majority of business is derived from North America, with interests across multiple vertical industries, including media, government and others.

CSIS Security Group

Although it shares the CSIS acronym with the Canadian Security Intelligence Service, this Danish company is a separate entity. Its major focus is on financial e-crime prevention and response, particularly in the European theater, and operational practitioners tend to be major consumers of its content. The vast majority of its business is in EMEA, mostly in the financial services sector. CSIS did not provide pricing data.

Cyveillance

Cyveillance began as a specialist in threat intelligence services in 1997 and was acquired by QinetiQ in 2009. Its reputation is arguably founded on its ability to monitor brand issues and financial crime; however, both Cyveillance and a reference customer cite interesting use cases in which intelligence content was used for the protection of physical assets and events. The vendor has a relatively high proportion of analysts. Pricing is in the low to midrange. The majority of its business is derived from North America, but spread relatively evenly across a broad range of vertical industries, including financial services, media, manufacturing and natural resources, retail, transportation, and utilities.

Dell SecureWorks

Dell SecureWorks offers a broad spectrum of threat intelligence services, including global (generic) feeds and more customized feeds to suit high-end client requirements. Clients tend to have a range of factors that elevate their risk (for example, multinational operations, controversial public perceptions or high degrees of investment in intellectual property). The vendor has established a strong reputation for expertise, rating the second-highest number of mentions among competitors and a relatively high number of mentions among reference sites. Pricing options range across the spectrum from low to high, depending on requirements, with high pricing potentially being a point of concern for some prospects.

Digital Shadows

Digital Shadows is one of the few vendors in the market that does not explicitly provide commoditized Real-Time Monitoring and Notification content, although the customized content that it generates is available in real time

and can be exported in a STIX-compatible format. This vendor sees its strength as being in the breadth of the threat actors that it tracks. Pricing is in the low to midrange, which is somewhat less than might be expected for such an analysis-heavy offering. Most clients are in the North American and European markets. The major vertical industry is financial services, with a relatively even smattering of clients across other vertical industries, such as media, manufacturing and natural resources, and utilities.

FireEye

FireEye's offering is based on its acquisition of Mandiant in early 2014. Its pedigree is in forensic support and incident response services. This company established a global consciousness in early 2013 with a widely publicized and well-received report covering advanced persistent threat research. Threat intelligence as a stand-alone service is a comparatively recent FireEye offering, and is arguably not as well-established as some of its rivals' offerings in terms of content developed for the executive level. Pricing is in the midrange, and major vertical industries include financial services as well as manufacturing and natural resources.

Fox-IT

Fox-IT delivers a broad array of content to support tactical and strategic decision making; it also provides coverage of infrastructure threats and, to some extent, financial crime and brand protection. This is notable, given the relatively small size of the company; however, it does have a healthy proportion of analysts on staff. Fox-IT considers that being headquartered in the Netherlands provides it with an advantage in terms of gaining high-quality intelligence from countries elsewhere in Europe, such as Russia. The traditional market for this vendor has been Europe, particularly Scandinavia and the U.K. Key vertical industries include financial services, retail and media. Pricing is in the midrange.

Group-IB

Eastern Europe is generally recognized as a key point of origin of threat and fraud activities. As a Moscow-headquartered company, Group-IB arguably has a market advantage with regard to developing insight into these communities. It focuses mostly, albeit not solely, on electronic fraud and brand issues. It has established a solid base of clients, mostly in Europe, with a focus on financial services. Pricing tends to be in the midrange.

IBM

IBM's offerings are based on the integration of acquired and organic capabilities, including the Internet Security Systems and X-Force researchers acquisition in 2006, Watchfire in 2007, Trusteer in 2013, as well as IBM Security Services and IBM Research & Development. Most of the offerings are available only as bundled services, with the exception of the X-Force Threat Analysis Service and the Advanced Cyber Threat Intelligence Service. There is an accompanying Content Analysis SDK that provides access to the threat intelligence feed. The X-Force Threat Analysis Service is available for a nominal charge. Pricing for the Content Analysis SDK and the Advanced Cyber Threat Intelligence Service varies.

IID

The pedigree of this company is in phishing takedowns and the provision of reliable DNS services; ultimately, it morphed into a threat intelligence service. Its strength is in the Real-Time Monitoring and Notification space; its service offerings fall only marginally in the Acquisition and Analysis category. Its key vertical industries include financial services, particularly in North America. Pricing is squarely in the midrange.

iSIGHT Partners

This vendor historically specialized in threat intelligence services, and has more recently added some support for incident response. Its core capabilities are well-respected, and it has a high number of analysts on staff. It is one of the few vendors with intelligence-gathering personnel in all major regions, including Western and Eastern Europe, Asia, the Middle East, and South America. This vendor has been extremely successful at generating brand awareness, having the highest number of mentions from competitors as well as reference sites. Key vertical industries include financial services and government. iSIGHT has adopted an innovative pricing model that incorporates the market cap of the client, among other factors. Accordingly, pricing ranges from the low end to the high end of the spectrum, generally around the mid- to high range.

Lookingglass

This company's major offering is a platform for fusing and analyzing information from multiple feeds, although it also provides original content. Reference sites have noted high degrees of responsiveness to client needs; however, a shortage of staff is sometimes noticeable. The majority of its business is derived from North America, with a focus on financial services and government. Pricing ranges from the low end to the high end of the spectrum, generally around the midrange.

Malcovery

Malcovery is one of a group of relatively new vendors in this market. Its innovation for detecting email-based threats, particularly phishing activity, has won praise, particularly in the context of its affordability. All business is derived from North America. Its major vertical industry is financial services, with a smattering of coverage across other vertical industries, including media and retail. Pricing is in the low to midrange, with deals generally toward the low end.

Norse

Norse provides relatively standard MRTI-type content — such as IP addresses and malware URLs, along with geolocation data — generated from its own network of honeynets (not client networks). The honeynets are configured to look like an array of different devices, from standard servers to specialized medical delivery systems. An interesting innovation is a quasi-predictive capability based on devices in close proximity to the source of an attack. Reference clients have reported that the quality of Norse's content, particularly around Tor-based networks, has been a differentiator. As with other newer and smaller vendors in this market, Norse's customer responsiveness is counterbalanced at times with problems arising from lack of resources. Most of its business is derived from North America. Its customer base is spread fairly evenly across banking and securities, government, technology, and communications and media. Pricing tends to be in the low to midrange, with average deals in the midrange.

One World Labs

One World Labs has what it considers to be a unique and differentiating level of automation to harvest and analyze content — particularly content drawn from Tor and other "dark Web" traffic. Pricing starts at the low end, but is mostly in the medium band of the spectrum. The majority of business is based in North America. Interest is spread relatively evenly across a number of vertical industries, with the highest interest in financial services and healthcare.

RSA, The Security Division of EMC

RSA's offerings are somewhat different from others in this market. It has threat intelligence capabilities relating to infrastructure (via RSA Live) and fraud (via FraudAction), although only FraudAction is available as a stand-alone product. FraudAction's capabilities are well-established, and it is now being used in an array of vertical industries other than (the traditional) financial services. One reference site noted specifically that the existing satisfaction with the service was partly due to an understanding of specific client needs. Pricing information is not available.

SenseCy

SenseCy is a relatively new player in this market. Its major focus is on content that falls within the Acquisition and Analysis category, although it does provide Real-Time Monitoring and Notification content. Major focus areas include Islamic-based hacktivism as well as the Chinese and Russian underground. Not surprisingly, given the location of its headquarters in Netanya, Israel, the majority of SenseCy's business is in the Middle East, mostly in the financial services sector. Pricing depends on the services selected and can run across the spectrum from the low to high range, with deals generally at the low end of the spectrum.

Symantec

Within this market, Symantec is best-known for its long-standing DeepSight service, which stands squarely in the Real-Time Monitoring and Notification segment. Symantec's higher-end services provide greater depth of analysis, and, on this basis, it is a marginal vendor in the Acquisition and Analysis segment. Symantec provides tiered service levels to support low-end and high-end budgets; the greatest volume of customers are at the lower price points, but high-end deals constitute a significant portion of revenue. Not surprisingly, for a company of Symantec's size, its business is distributed across multiple geographies and vertical industries, with a slight skewing toward North America and financial services, respectively.

Team Cymru

Team Cymru provides a mix of commercial services via Team Cymru and not-for-profit services via Team Cymru Research NFP. Team Cymru is quite secretive about its capabilities and descriptions of its services, beyond the minimal information provided via its website and some marketing brochures. Thus, making an assessment of the quality and pricing of its commercial services is difficult (although one reference site indicates satisfaction with the services).

ThreatStream

ThreatStream is yet another new and still-small organization in this market. Its key senior staff members have a strong security information and event management (SIEM) — that is, ArcSight — background, and this shows in its product offerings. The vendor's automation capabilities have proved to be effective, with SIEM integration being the key factor in at least one critical win. The majority of its business is in North America, primarily in government and financial services. Pricing is in the low to midrange.

Verisign

Verisign, via its iDefense service, is a well-established service provider in terms of longevity, and it maintains a high level of brand awareness. It continues to have attractive features for the buyer, such as a comprehensive service offering, a strong intelligence process and a high proportion of analysts (with multilingual expertise) spread across multiple geographies; however, other providers now have these features as well. As a result, iDefense is now operating in a more challenging marketplace. The majority of Verisign's business is derived from North America. The major vertical industries that it services are financial services and media. Pricing tends to be in the midrange.

Webroot

Webroot's pedigree is in malware solutions, but it branched out in 2010 to offer threat intelligence with its BrightCloud services. A significant portion of its threat intelligence business is delivered via OEM channels, and reference customers are primarily other vendors. Consequently, information about its distribution across vertical industries is not available. The company recently introduced service offerings for enterprises. Most business is derived from North America, with a significant portion from Europe. Pricing information is not available, although deal sizes range across the spectrum from small to large (OEM deals tend to be at the large end).

Market Recommendations

Before purchasing a service, have a plan for how you will use it. Understand who will consume it and how they will use it. Also understand what decisions you expect to make on the basis of the content provided, and how those decisions will be made.

There is a plethora of service providers in the market, and the number appears to be growing. Not all services that are marketed as threat intelligence actually provide that type of content, so it is important to understand what problem you are trying to solve.

For example, are you interested in vulnerability information? This is not threat intelligence. However, if you are trying to find out what your adversaries are doing or even planning, and you want to find out without drawing attention to yourself, then a threat intelligence service may be valuable.

Be aware that not all "threat intelligence" is the same. Some vendors do not offer much more than information about IP addresses and the implication of URLs in current activity. This provides you with an ability to respond rapidly to the contemporary threat environment, but does not inform you about what may happen in the next month or the next year. Other vendors can provide advice on adversarial capabilities and plans, but this information is expensive and almost always involves a degree of informed inference.

Use Acquisition and Analysis services to inform your long-term security strategy. It can take up to two years or more to be ready for an emerging threat. These services can provide insight into the identity, capabilities and plans of potential adversaries.

Use Real-Time Monitoring and Notification services to develop an agile response to rapid changes in the external threat environment. Consider MRTI to automate your response.

Understand that this is not yet a mature market, and that we can expect ongoing volatility in the array of vendors and their capabilities in the short to midterm.

Evidence

This research is based on two major sources of primary research: vendor surveys and client inquiries.

We looked at a total of 32 vendors for this research. This is only a portion of the vendor population claiming to offer threat intelligence.

Each surveyed vendor was asked to provide information about its service offering, its market, examples of its product and reference site information. Three vendors reported that they do not provide threat intelligence services as stand-alone offerings, so they were excluded from this research. A fourth vendor was excluded on the basis that, although it claims to provide threat intelligence, it really provides information only about vulnerabilities and exploit code, which is insufficient to meet the inclusion criteria. Finally, HP would have been included, but, ultimately, we omitted it because its Threat Central offering was not yet generally available. This left the 27 vendors that we have included in the Representative Vendors section.

Most vendors were quite open and cooperative with this research. Team Cymru, however, declined to respond to the survey. Therefore, our summary of it is based on publicly available information only.

We followed up with a sample of reference sites for most vendors. Instances in which we did not follow up included vendors that were unwilling or unable to provide reference sites — or, in a few cases, in which the survey results became available well after the survey period had closed. In cases where we did have samples of reference sites, we surveyed a minimum of two, where available, for each vendor. Some reference sites declined to respond, citing confidentiality issues; this, in itself, could be interpreted as an indication of a misalignment between vendor and client expectations. We received a response rate of about 50% to the reference site surveys, with a total of 25 responses received.

The second major source of primary research was client inquiries. Gartner analysts field inquiries on threat intelligence services roughly on a weekly basis. Although these inquiries rarely indicate the state of the market, they do provide insight into client needs — some that are met and some that aren't — as well as information about actual or intended use cases.

Note 1. Sharing of Threat Intelligence Among Vendors

There are indications that other vendors are also sharing information with each other; however, because the information we received appeared to be somewhat inconsistent in some cases, we did not list these other arrangements.

Additionally, a new consortium has been established in 2014: the Cyber Threat Alliance. It was announced just prior to the publication of this research.

Note 2. Demonstrating the Value Proposition

This was also a recurring theme among end-user clients during an analyst-user roundtable discussion at Gartner's Security & Risk Management Summit in June 2014.

Note 3. The Region From Which the Majority of a Vendor's Business Is Derived

For each vendor, we indicate the region from which most of its business is derived. If a customer is classified as, for example, "North American" for the purpose of a deal with a particular vendor, this does not mean that such a vendor may service only the North American part of the customer's organization. In other words, if a particular vendor draws the majority of its business from North America, then it may still (and, in many cases, does) have customers in other regions, develop intelligence drawn from raw information that is sourced from other regions, and service North American customers that are distributed internationally.

Source: Gartner Research Note G00259127, Rob McMillan, Khushbu Pratap, 14 October 2014

About iSIGHT Partners

Since 2007, iSIGHT Partners has focused exclusively on analyzing and understanding the global threat ecosystem. The firm has been recognized as the leader and the main founder of the commercial cyber threat intelligence field.

Comprehensive Coverage of Threats

iSIGHT Partners threat intelligence provides deep analyses of adversaries and the tactics they employ to target enterprises and critical infrastructure. It delivers enhanced vulnerability and exploitation research, with expertise spanning all of the major threat categories: cybercrime, cyber espionage and hacktivism.

True Global Research

A research team distributed across 16 countries includes over 250 experts with the local backgrounds and native language skills to understand the colloquial terms used in underground communities, along with the social, business, political and cultural contexts of threat actors. Eight years of exploration in the threat underground and adversary marketplaces provide a unique depth of knowledge about the motivations, goals and methods of threat actors and their supporting ecosystems. Human research is supported by over 20 technical data collections systems, including a global network of sensors, "honeypots" and other data collection devices.

Analysis and Context Fused with Technical Data

iSIGHT Partners provides analysis and rich threat context narratives that allow security teams to understand advanced attacks and focus on real, high-impact threats. Technical information and tags for automated consumption by SIEM systems and other security technologies help protect networks in real time and allow operations teams to separate meaningful alerts from "noise." Data and context are packaged to support multiple roles in the IT organization, including security operations, infrastructure operations, patch management, incident response, security analysis, and executive communications.

World-Class Intelligence Collection, Analysis and Dissemination Processes, Built on Industry-Leading CTI Platforms

iSIGHT has invested heavily in the processes, tools and technologies necessary to collect threat information from around the globe and distill it into insights and actionable intelligence.

ThreatScape Intelligence Platform (TIP) is the most sophisticated commercial cyber threat intelligence platform ever developed. TIP supports every aspect of the intelligence collection, analysis and production lifecycle, from managing intelligence requirements, to gathering human and technical threat data, to conducting malware analysis, to fusing technical information with threat context, to producing finished intelligence products.

The ThreatScape Cloud is the most advanced cyber threat intelligence distribution system available in the market. It offers a variety of tools and technologies to disseminate the strategic and tactical intelligence that matters most to individuals and security tools within client organizations. Components of ThreatScape Cloud include:

- ***MySIGHT Portal***, a web portal that enables clients to search eight years of finished intelligence and to customize the delivery of alerts and reports.
- ***ThreatScape API & SDK***, features that provide direct, programmatic integration between iSIGHT Partner's comprehensive, context rich threat intelligence and a wide range of security tools. iSIGHT offers out of the box integration with SIEM, firewall, secure gateway, IPS, GRC, analytics and threat intelligence platform products from over a dozen vendors.

- ***ThreatScape Browser Plugin***, a tool that enables simplified, web-based integration between browsers and iSIGHT Partners' rich intelligence holdings. ThreatScape Browser Plugin scans web pages for indicators of comprise (e.g., IP, Domains, Hashes), and leverages ThreatScape API to search and deliver contextually rich information about potential threats to a new tab in the browser.

Customer Partnerships

iSIGHT Partners customer base is a who's who of the largest U.S. and global brands, including eight of the top 10 U.S. banks, three of the top four card issuers, over 250 government entities, and numerous leading healthcare, technology, petroleum, retail, consumer goods and beverage companies. Client Engagement Representatives work with clients to obtain specific intelligence requirements and tailor customized intelligence programs. Customers can direct queries to the iSIGHT intelligence team, and submit malware samples and suspicious URLs for detailed analysis. Workflow tools and metrics ensure effective interaction over time.

Bottom line

iSIGHT Partners mission is to fundamentally change the business of cyber security. Effective cyber threat intelligence can have a major impact on enterprises at the operational, technological and strategic levels, enabling them to stay ahead of ever more sophisticated threat actors. We provide customers with detailed, customized, forward-looking analysis and technical data so they can better understand threats, separate meaningful alerts from noise, respond faster to attacks, better communicate security issues with management, and improve strategic planning and investment. We encourage readers to learn as much as possible about this exciting field, then contact us to find out how cyber threat intelligence can be applied with maximum effect in your organization.