WHITE PAPER

Intelligence-Led Security

Sponsored by: IBM

Robert Ayoub
Michael Versace
Christina Richmond

March 2016

INTRODUCTION

While there has been improvement in the amount of time an attacker spends in a network before detection — decreasing from years to days in many cases — the ongoing delay illustrates just how elusive attackers still are compared to an organization's ability to detect a problem. IDC believes that actionable threat intelligence is going to be a significant factor in improving this metric. Threat intelligence has historically been seen as a complex set of activities reserved for security operations centers (SOCs) and advanced security analysts. The tools to collect and apply threat intelligence have generally not existed commercially and the ability to integrate threat intelligence into the traditional security workflow has not been available. Over the last few years, threat intelligence has been growing in importance within the security workflow.

As both threat intelligence security services (TISS) and advanced analytics tools improve, smaller organizations will gain the ability to perform their own threat intelligence and thereby answer very critical questions around security. Having the ability to perform custom analytics will only improve the awareness of attackers against verticals and organizations. More information can help organizations improve their security posture against direct attacks and attacks against their peers, and can also make remediation and incident response much more effective and cost-efficient.

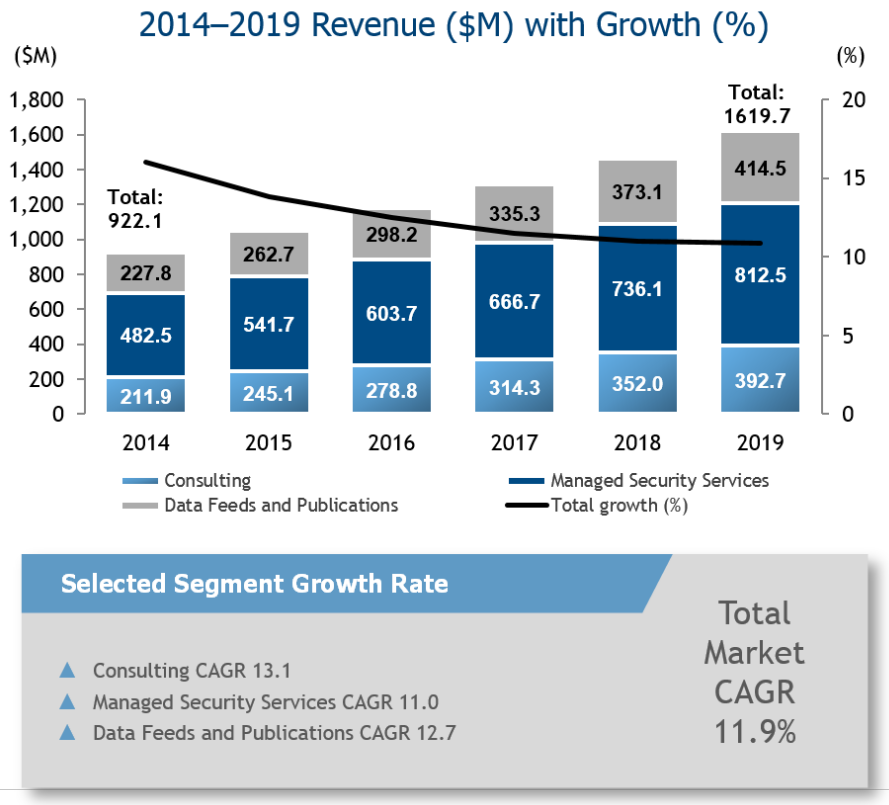
A significant challenge for many organizations has been enabling their analysts to find the "unknown unknown." Whether that unknown is malware lurking within the enterprise or within slight variations in fraudulent transactions, the result has been the same: enterprises continue to fall victim to cybercrime. IBM is addressing this challenge with IBM i2 Enterprise Insight Analysis. By pairing multi-dimensional visual analysis capabilities with powerful analytics tools, IBM is giving the analyst team an effective early-detection, cyberintelligence weapon for its arsenal.

THREAT INTELLIGENCE SECURITY SERVICES MARKET OVERVIEW

TISS grew out of security services providers developing threat detection capabilities to address the challenge of detecting advanced persistent threats (APTs), advanced malware, previously unidentified attacks, and other threats. These attacks are unknown, targeted, low and slow, and adaptive. In the first foray into the study of the TISS market in 2014, IDC forecast the size of the market to be over $800 million. Figure 1 illustrates IDC's forecast for this market through 2019.

FIGURE 1

Threat Intelligence Security Services Forecast 2014-2019



Source: IDC

The threat intelligence market is made up of several distinct facets:

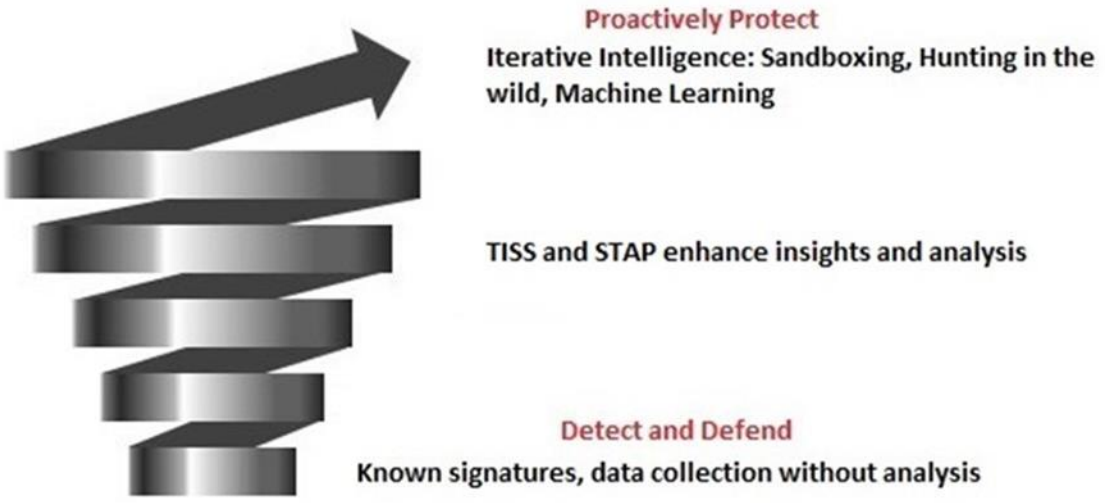
- Data feeds and publications, which provide threat information for action by users or for correlation into customer SIEM and other security automation systems (e.g., GRC, application firewalls)
- Professional security services (PSS) – specifically consultative services – for advanced security event monitoring and management technologies that incorporate a variety of threat related information sources to develop predictive security as well as help set up a threat intelligence program, among other things
- Consulting security services specific to breach and incident response, and forensic analysis
- Managed security services (MSS) that advance global correlation and aggregation of events to preemptively detect security threats for clients through a managed customer premises-based platform (CPE) or cloud service delivery platform

THE "FUNNEL" — ITERATIVE INTELLIGENCE LIFECYCLE

Many organizations find threat intelligence alone to be of limited value. However, when the proper context is added to threat information, an iterative intelligence lifecycle begins to emerge. Figure 2, depicts a spiral as an illustration of what IDC believes modern threat intelligence now looks like – what we now call iterative intelligence. Security processes historically have been two dimensional, looking at snapshots of current attacks at a current point in time. However, to be successful against modern threat landscape security processes requires a 3D approach that learns from past mistakes and incorporates new knowledge at a rapid pace. This iterative process means that past experiences and mistakes are incorporated into future planning. This is especially important as current analysis of threat intelligence incorporates multiple processes occurring at the same time, with some moving forward in time (investigation of false negatives), some relatively static (false positives), and some backward in time (forensics) with the goal of feeding back into forward-motion specialized threat and analysis products.

FIGURE 2

The Threat Intelligence Spiral



Source: IDC

Use Cases

Another change with the advent of iterative threat intelligence is the applicable use cases for that intelligence. These use cases can be much broader than finding malware and cyberattacks. Organizations can extend activities into investigating fraud, employee misconduct, and other incidents that cause data and financial loss, brand value loss, and negative productivity. The ability to extend the number of use cases for threat intelligence has many advantages for the market and for organizations.

THE ADVENT OF APPLIED THREAT INTELLIGENCE

Threat intelligence relies on a compilation of data from a wide variety of sources. There are many different sources of attack information. TISS organizes this rather chaotic process of information-sharing into alerts and data feeds that can be used in existing security tools for comparison to ongoing attacks. Traditional threat intelligence does not provide any action on its own; it is simply data that can be added to existing security tools. This has prevented many organizations from placing much importance on threat intelligence.

Organizations and analysts need the ability to shift threat intelligence from a data feed into actionable results. This is the core of what IDC has termed applied threat intelligence (ATI). ATI comes as a result of the iterative nature of searching, analyzing, hunting for code and IP addresses, adding forensic data, incorporating the data, and looking at alerts, patches and any other relevant data that makes threat information intelligent.

For small and medium-sized businesses, developing ATI is a challenge because senior management wants an expedient solution. In many cases, the CEO or board of an organization only wants to know the answers to three questions when a data breach occurs:

- What was the problem?
- When was it fixed?
- How do we keep this from happening again?

This mentality assumes that a data breach is a one-time event and that once the problem is resolved, the organization is safe. Unfortunately, this does not reflect the rapidly changing threat landscape in which attackers are indiscriminately probing applications and organizations for whatever valuable data they can find. Organizations need to shift their thinking away from viewing data breaches as a one-time event and instead recognize that with every incident they are building a repository of knowledge that addresses:

- How to avoid the old problem(s)
- What works (and what fails) during an incident response to an attack
- How to reduce the time to detect and remediate future attacks
- How to improve the time to detection, remediation, and assessment of compromised information
- How to conduct a forensic investigation and breach notification procedures

In larger enterprises, we can multiply the spiral (refer back to Figure 2). This would include other departments and business units in the same organization that selectively share threat information and mitigation techniques while protecting their intellectual property and external partner's privacy and confidentiality. These iterative intelligence spirals can be further replicated into a collection of associated companies that also share information and techniques.

APPLIED THREAT INTELLIGENCE: A FOUNDATION FOR ANY DIGITAL ENTERPRISE STRATEGY

Today, IDC considers ATI as a foundational component of a digital enterprise strategy and essential for successful business transformation in the digital era. With the growth in adoption of 3rd Platform technologies and the industry innovation and disruption that results, nearly all corporate strategies today contain an increasingly significant digital component. In many industries, digital initiatives now account for a majority of business and revenue growth. Some argue that all corporate strategies are digital; strategies must address a broad set of business, social, and technology trends – including safety and security – that surface with the acceleration of technological change. These trends include the disruption caused by external digital transformation factors, the role of technology and information as strategic business resources, the business and technical threat landscape, the evolution of the talent marketplace, and others factors. IDC believes that by the end of 2017, two-thirds of the CEOs at Global 2000 companies will have digital initiatives aligned with opening new revenue streams, creating information-based organizations, and changing the way work is performed. These initiatives will be at the center of corporate strategies.

As organizations move along the digital journey, cybercriminals continually exploit weaknesses in business processes, training, technologies, and infrastructure. Weaknesses are introduced from multiple angles, including M&A and corporate restructuring, new customer sales and services models, new sourcing and supply chain models, new application and mobility development tools, new ways of consuming IT, and new vendor relationships. By 2017, IDC predicts that the weaknesses in digital initiatives exploited by cybercriminals will produce a significant jump in cybersecurity investments designed to proactively protect enterprise assets.

Even though ATI makes sense as a concept, the reality of embedding it into the existing workflow, or designing it into new business models and processes, is a key challenge for organizations. To reduce the complexity of today's threat landscape, an ATI solution should possess the following three attributes:

Attribute 1 – Connect Anomalies over Time

There was a time when attackers made little attempt to mask their activities. Attacks were more focused on disruption. As a result, attackers were more concerned with the bragging rights associated with defacing Web sites or preventing access to services entirely. Today, attackers have learned to leverage techniques in order to be "low and slow," making it difficult for professionals to see pending attacks over time. A well-respected industry survey of organizations revealed that the median number of days for an organization to be infected with malware before discovery is 205 days.

In order to utilize ATI, analysts must have access to data analysis tools that are constantly tracking a wide variety of metrics around data as it moves through the enterprise. Just as important is collecting information in a matter that allows multiple analysts to look at information holistically, instead of as individual anomalies. In other words, analysts need a product that will track individual anomalous events and work to determine whether a relationship exists between those anomalies.

Attribute 2 – Track Threat Actors and Campaigns

Another key feature for an ATI product is to use externally available threat intelligence to track threat actors and campaigns. An ATI product should have the ability to take all the external security data and compare it to an organization's internal security operations. This perspective is a critical function for an internal cyberintelligence team to make all the data in the security ecosystem relevant and actionable to an organization

Unstructured and structured source data is imported automatically from public, deep Web, vendor, and social media sources. In forums, actors will discuss tactics and post claims on targets they attack. Hackers will often reuse screen names between legitimate and dark Web sites. This correlation can be used to understand relationships between individuals that are otherwise hidden. STIX/TAXI type data may also be ingested concerning historical attacks, which reveal patterns.

Automated social network analysis tools allow analysts to see interpersonal relationships, movements, techniques and procedures among threat actors. An analyst may discover Geo IP address information connected to threat actors which can be used by the security team to identify threats. Understanding the industries targeted by a particular group and how that group penetrated associated defenses can be compared against the organization's current security state.

These capabilities require significant investment by the vendor. Reverse engineering of malware, maintaining honey pots and deception networks, and hunting for threat actors all require a high level of sophisticated analysts that are not easily found within the industry. Providing top-notch threat intelligence enables the entire ATI product to be more effective.

Attribute 3 – Leverage a Security Ecosystem

Finally, integration with other enterprise tools is critical. Visualization and reporting are key capabilities for these systems. The ability to export search results into other security systems such as SIEM, IPS, and NGFWs is a feature that is difficult if an ATI solution is cobbled together from homegrown or open source products, or is made up of solutions from many different vendors. Ensuring that data results can easily flow among different systems will empower business units to utilize ATI to improve their own security posture instead of relying on the SOC or security analyst team to perform the implementation.

THE IBM i2 ENTERPRISE INSIGHT ANALYSIS SOLUTION

IBM i2 Enterprise Insight Analysis (i2 EIA) is an open, interoperable, extendable and scalable solution that helps organizations accelerate the data to decision process by enabling them to perform analysis and advanced analytics at scale and with critical speed. Whether an organization is challenged by large amounts of communications data or looking to turn disparate data into a clear operational picture, i2 EIA is designed to help analysts digest overwhelming and disparate data sets and develop actionable insight for near-real-time decision-making.

IBM i2 EIA enables strategic analysis by incorporating multiple data sources and providing an advanced analytic tool. IBM i2 EIA can automate the process of data collection and ingestion, while enabling analysts to conduct human-led analysis, such as using search queries among analysts to augment and predict searches that will zero in on the actual required result.

IBM i2 EIA is sustainable in that it is designed to enable organizations to be self-learning, thereby helping to reduce training, maintenance and deployment costs. In addition, IBM i2 EIA:

- **Discovers** patterns and relationships in data by performing advanced analytics at scale and at speed.
- **Integrates** with existing infrastructure and data sources, and facilitates information sharing between and among organizations.
- **Scales up,** allowing for customization and supports ATI analytic requirements at the tactical, operational and strategic levels.

IDC spoke to two organizations about their use of IBM i2 EIA.

Case Study 1 - A non-profit, public/private information sharing entity

This entity uses i2 EIA in a more traditional threat intelligence function, taking vast amounts of information from law enforcement and open source feeds and then distilling that information down into actionable data that is distributed to organizations across a wide variety of verticals.

As this organization looked competitively for a solution to help organize the many data feeds and to look for the proverbial "needle in a haystack," i2 EIA stood out for a variety of reasons. First was its ability to allow for a continuous workflow across analysts. The product has the ability to track searches made across analysts and look for emerging patterns. This allows for collaboration among analysts and helps to break one analyst's search out of its potential silo, organizing related searches and even providing direction to analysts on related findings. Second, the visualization abilities of i2 EIA are described by the client as "second to none." Finally, the ability to implement i2 EIA without having a programmer on staff is considered critical to this non-profit organization that has to utilize its existing staff to the fullest.

Case Study 2 – A Multi-State Insurance Company's Fraud Investigation Unit

This fraud investigation unit uses i2 EIA to process vast amounts of claim data in order to identity fraudulent claims, and to identify and build cases against criminal groups that commit insurance fraud. While this use case is significantly different from the non-profit's use case, many of the underlying requirements are the same.

This client needed a solution that can help evaluate large amounts of disparate data and look for patterns such as names on claims that are similar but not exact. The client also needed a solution that can monitor searches across many analysts, looking for groups that may be operating in consort across multiple cities or even states. Visualization is critically important for this client, whose analysts rely on visualization to identify trends and improve search terms.

This client states that search speed is a critical requirement and that i2 EIA handles large amounts of data extremely quickly. The ability to learn from historical searches and cases is another key advantage that provides very noticeable results, reducing investigation times down from days and weeks to hours and minutes.

CHALLENGES AND OPPORTUNITIES

While the promise of ATI is appealing for many enterprises, there have been many market challenges that have prevented most from adopting ATI into their workflows. Below are a few challenges specific to the threat intelligence market.

Lack of Visibility and Education

- Assumption: Security is a complicated undertaking to say the least. IT staffs have their hands full with day-to-day responsibilities and typically don't have the bandwidth to keep up with a specialized area like threat intelligence. In spite of having implemented standard countermeasures like firewalls, antivirus, and identity management, many organizations still do not have a view into what's happening across their environments at any given point in time. In the absence of problem alerts, it's all too easy to assume that there are no problems and therefore no actions need be taken. While "information is power" in this situation, chief

information security officers (CISOs) and executives are between the proverbial rock and a hard place. They realize they need to know more to make informed decisions, but the amount and complexity of the information is overwhelming, especially when all employees should be educated about cybersecurity.

- Impact: When decision-makers and decision-influencers are unclear or unsure about what to do, they may delay security decisions or make inappropriate decisions, thereby increasing risk because security vulnerabilities aren't addressed. Sales cycles may lengthen and/or stall out if security vendors aren't organizing and delivering essential, role-based information.

Shortage of Security Talent

- Assumption: Security talent is in short supply globally, so all parties in the market are feeling the pinch. Only a few global organizations and government agencies can afford to fund their own threat intelligence operations, and they may find it difficult to compete with TISS providers that can offer a variety of roles, rapid advancement, and attractive career paths.
- Impact: Lack of talent may constrain the growth of the TISS market.

CONCLUSION

Threat intelligence started with raw data, moved to information tied to customers' specific infrastructure, and provided selective guidance on remediation. Initially, threat intelligence was a closed community mostly populated by large government agencies, very large enterprises (mostly financial), and security researchers. The data was highly technical and the resulting market was relatively small because of the sophistication needed.

In the next few years, threat intelligence and its sister, iterative intelligence, will be deciding factors in customer selection of security products and services vendors. Tools and services based on iterative intelligence will help customers educate themselves using past experience. Given the scarcity of experienced IT security analysts, the internal training processes afforded by iterative intelligence could help train and retain IT people. Likewise, the promotion of communities would also stimulate collaboration and further education. Iterative intelligence could help inject some logic into the increasingly irrational clamor over the necessity of public/private collaboration on threat information. Finally, iterative intelligence must be available to small and medium-sized businesses as they see increased attacks like wire fraud and intellectual property theft.

IDC believes that more enterprises will be evaluating dedicated solutions to improve their analysis of threat intelligence and provide actionable results that IT can then implement across the enterprise. This iterative process will improve as historical data is analyzed and multiple data sources can be evaluated. IBM's i2 EIA solution is a strong competitor in this space, as IBM has a long history in the security field and is applying that legacy through i2 EIA in order to increase the overall security of any enterprise in any industry.

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

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com