Bryan, Garnier & Co

Cybersecurity

THREAT INTELLIGENCE AND ORCHESTRATION AT THE FOREFRONT OF THE NEW SECURITY REVOLUTION

TECHNOLOGY WHITE PAPER FEBRUARY 2020

Contents

2 DEMAND FOR CYBERSECURITY SOLUTIONS IS ON THE RISE

8 FROM PREVENTION TO DETECTION: THE CAT-AND-MOUSE GAME BETWEEN THREAT ACTORS AND CYBERSECURITY VENDORS

16 PREVENTION AND DETECTION TOOLS ARE REACTIVE. TAKING THE NEXT STEP MEANS BEING PROACTIVE: THE RISE OF CYBER THREAT INTELLIGENCE

23 CONCLUSION

Organizations today are embracing technologies such as cloud services and mobile computing to enhance employee productivity, generate new revenue sources and improve operating efficiency.

More broadly, the number of communications is exploding, as is the internet of things (IoT) – and data is everywhere. This emergence of an increasingly distributed IT infrastructure, along with the explosion in its diversity, scale and importance has greatly increased vulnerability to attacks. As a result, cybersecurity has become more critical for governments and corporations alike.

In this paper, we explore the reasons behind the growth of the cybersecurity market. We also look back to the launch of cybersecurity solutions to understand why prevention-based solutions such as antivirus software have failed in the past, examining how the market reacted to that failure with the emergence of detection-based tools such as Endpoint Detection and Response. Finally, we explore how the market is once again changing its paradigm, taking a more proactive stance to fend off cyber threats using Cyber Threat Intelligence and orchestration.

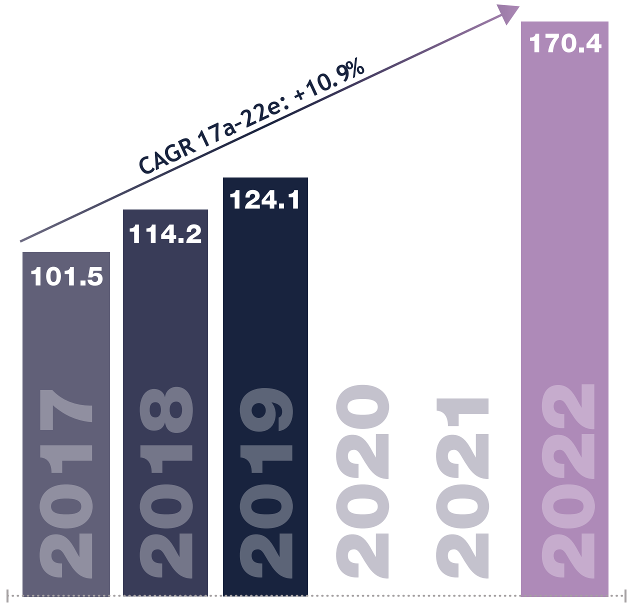
Greg Revenu
Managing Partner
Technology

David Vignon
Research Analyst
Software

Charlie Pujo
Director
Technology

Demand for cybersecurity solutions is on the rise

FIG. 1: CYBERSECURITY SPENDING (IN $BN) CONTINUES TO INCREASE



Source: Gartner, Forecast Analysis: Information Security, Worldwide, 2Q18 Update

THE MARKET IS GROWING FAST

Investment in cybersecurity remains a top priority for most organizations. Worldwide spending on information security products and services reached more than USD124 billion in 2019, an increase of 8.7% from 2018, according to Gartner. Overall, between 2017 and 2022, the market is expected to grow at a 10.9% CAGR. In terms of geographical distribution, the main market remains the United States, accounting for approximately 40% of spending, followed by China (less than 10%), Japan and the United Kingdom. There is no reason for this pace to slow, as all businesses need to increase their level of protection against various digital threats.

THE MAIN GROWTH DRIVER IS THE INCREASING COMPLEXITY OF THE GLOBAL LANDSCAPE

Contrary to popular belief, the number of breaches has been relatively stable in the last five years and is not the reason behind the strong growth the cybersecurity market is experiencing.

Instead, there have been three main drivers of growth: 1) the complexity of the global landscape, with the digitalization of businesses resulting in new IT architectures and many more potentially vulnerable devices; 2) increasing regulatory pressure to protect users better; and 3) the fact that threats are continuously evolving.

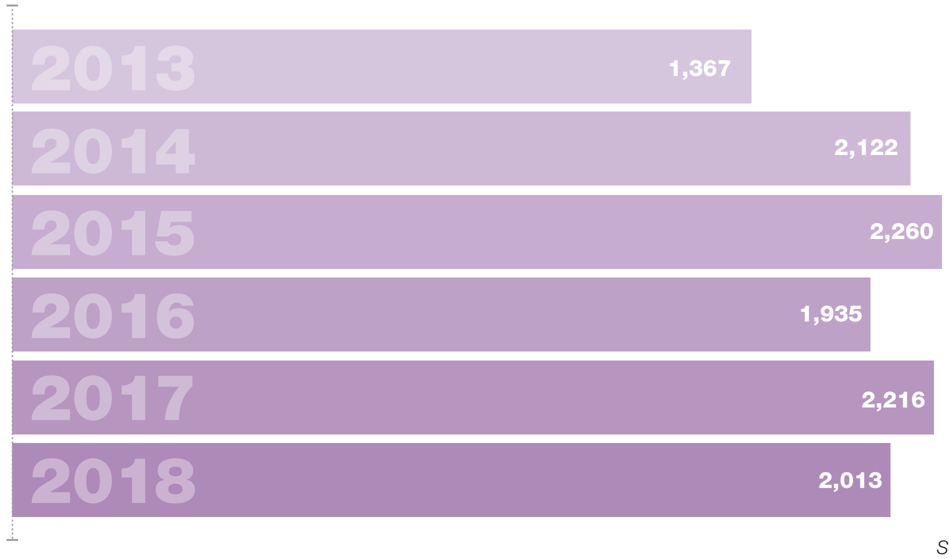
THE IT LANDSCAPE HAS SEEN PROFOUND CHANGE

While the IT landscape was defined by PCs in the early 2000s, it has since seen deep change. The advent of cloud computing has driven massive growth in data volumes: IDC predicts that by 2025, the amount of data created globally is expected to grow fivefold and reach 175 zettabytes, compared to 33ZB in 2018. At the same time there has been exponential growth in the number and diversity of endpoints, driven by mobility, the emergence of IoT and the development of 4G and now 5G networks. These changes have had strong implications for the cybersecurity market. They expand the attack surface (the number of entry points or "attack vectors" through which an unauthorized user can penetrate), and make the perimeter that needs to be protected much more challenging to define and more volatile.

CYBER THREATS ARE INCREASINGLY COMPLEX

Alongside changes in IT, the threat landscape has also changed profoundly since the early 2000s, when viruses (malware that propagates by inserting a copy of itself into and becoming part of another program), worms (similar to a virus but is a standalone piece of software) and Trojans (malware which looks legitimate in the first place) were the main weapons.

FIG. 2: STABLE NUMBER OF BREACHES SINCE 2013



Source: Verizon Data Breach Investigations Reports, 2014-2018

Nowadays, hackers are more organized, sometimes state-backed, and they have benefitted from technological innovation, just like the organizations they are trying to penetrate. The last decade has given rise to a host of new cyber threats:

- **Advanced Persistent Threat –** a set of stealthy and continuous computer hacking processes that is often state-backed.
- **Ransomware –** malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
- **IoT DDoS –** IoT Distributed Denial of Service, an attack whose aim is to make a server, service or infrastructure unavailable through IoT devices.
- **Fileless threats –** use a type of malware that does not leverage an executable file, therefore leaving no signature.
- **Ransomware-as-a-Service (RaaS) and Malware-as-a-Service (MaaS) –** Even hackers have caught the "as-a-service" fever! These are platforms on which hackers can offer their ransomware, malware and technical support to anyone who is willing to pay a fee for the solution or share the ransom, democratizing cyber criminality.

CASE STUDY:

BRITISH AIRWAYS

British Airways, the first company to be fined under GDPR for data breach

In July 2019, the UK Information Commissioner's Office (ICO) announced its intention to fine British Airways GBP183m (or 1.5% of its revenue) following its disclosure of a data breach that had happened almost a year earlier. That breach had resulted in data about 500,000 customers being compromised. This was the first fine under the new GDPR policy and was closely followed by another fine, this time for hotel operator Marriott, for GBP99m.

REGULATORY PRESSURE IS INTENSIFYING

While the IT landscape is evolving, regulatory bodies are also adapting their compliance requirements. In the European Union, the GDPR (General Data Protection Regulation), which came into force in early 2018, has set a global standard for data protection, inspiring others such as the State of California and Japan to implement look-alike regulations. In the United States, the most notable regulations to impact cybersecurity include the HIPAA (Health Insurance Portability and Accountability Act) or the Gramm-Bleach-Liley Act, which state that entities in the health and financial sectors, respectively, must employ technical, administrative and physical safeguards to protect customer information from unauthorized access or use. These are just some examples of regulations that require better cybersecurity processes, but regulations in this field have been enacted at different levels: country, state and industry. Overall, regulatory pressure has been a strong driver of the cybersecurity market and this is expected to continue.

CYBERATTACKS HAVE AN INCREASING FINANCIAL IMPACT AND LONG-TERM REPUTATIONAL CONSEQUENCES

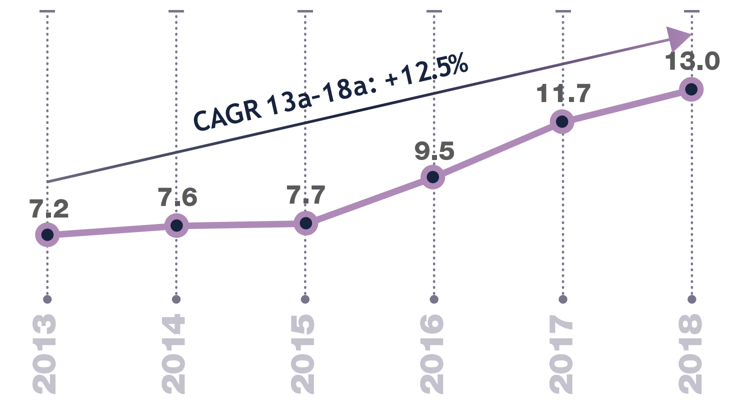
The implementation of better cybersecurity tools and processes has also been driven by the direct consequences that a breach can have on an institution, be it a government, a public agency, or an enterprise. Although the most famous cyberattacks have targeted large corporations, SMEs are also vulnerable and are increasingly being targeted.

OPERATIONAL ISSUES

Cybercrime has become more and more expensive for organizations. It can block part or all of an organization's operation, preventing it from earning money, steal money or even hijack a company by requesting a payment to restart disrupted operations. And there can also be fines if user data records are exposed.

Another way a cybersecurity breach can cost an organization money is through cyber espionage.

FIG. 3: RISING COST OF CYBERCRIME PER ORGANIZATION (IN $M)



Source: Accenture. The sample (n=355) includes organizations with a minimum of approximately 5,000 seats

According to Symantec, the most likely reason for an organization to experience a targeted attack was intelligence gathering, which is the motive for 96 percent of groups.

This activity aims to steal classified or sensitive data, which could result in the loss of competitive advantage. As cyber espionage is often state backed, the repercussions for threat actors are minimal.

REPUTATIONAL ISSUES

However, the consequences of cyberattacks are not just financial. In recent years, high-profile cases have damaged the reputation of several companies. One example is Yahoo, which in 2016 disclosed data breaches that had taken place in 2013 and 2014. Verizon reduced its takeover price by USD350m as a result.

Cybersecurity breaches and reputational damage can have consequences on many levels. Customers may find an alternative to the company; investors may divest; regulators may launch an investigation; politicians may reinforce current regulations; and finally, media could depict the organization in a negative way.

STRATEGIC ISSUES

For governments, cybersecurity has far-reaching implications, from the protection of state secrets to ensuring that critical services such as energy, banking, healthcare and transport are working properly. Every country runs a huge range of IT-powered essential infrastructure and services to keep things running smoothly. The effects of a cyberattack here could significantly disrupt the economy and the society, even beyond the shores of the targeted country.

FIG. 4: SHORT AND LONG-TERM POTENTIAL IMPACT OF A CYBERATTACK

SHORT-TERM IMPACT	LONG-TERM IMPACT
▪ Operations disrupted ▪ Data manipulated or deleted ▪ Theft of money, IP, customer data or other sensitive information ▪ Ransom payments	▪ Fines ▪ Loss of competitive advantage caused by the leak of sensitive data or intellectual property ▪ Reputational damage

Source: Bryan, Garnier & Co

CASE STUDY:

EQUIFAX®

Equifax data breach

In September 2017 US-based credit reporting agency Equifax announced that it had identified a data breach. This led to the leak of names, addresses, dates of birth, social security numbers and drivers' license numbers for 143 million Americans, as well as 200,000 credit card numbers. Although Equifax learned about the breach at the end of July 2017, it only publicized it in early September. In the aftermath of the breach, then-Equifax CEO Richard Smith retired, and the market capitalization of the company decreased by around USD5bn. Since then, Equifax has spent USD1.4bn upgrading its security.

CASE STUDY:

WannaCry, “the worst ransomware outbreak in history”

WannaCry is the name of a May 2017 ransomware attack that infected Windows computers, encrypting files located on the hard drive and demanding a ransom in bitcoin (from USD300 to USD600) to decrypt them. WannaCry is estimated to have infected more than 230,000 computers in over 150 countries. In the UK, the National Health Service – a major client for Sophos – had to cancel 19,000 appointments and operations because of the ransomware, costing it an estimated GBP92m in lost business and IT costs.

From prevention to detection: the cat-and-mouse game between threat actors and cybersecurity vendors

> *“Antivirus is dead”*
>
> **BRIAN DYE,**
> SENIOR VICE PRESIDENT, IT, SYMANTEC.
> WALL STREET JOURNAL, MAY 2014

FIRST, ANTIVIRUS SOFTWARE, THEN ENDPOINT PROTECTION PLATFORMS: TOOLS WHICH USED TO BE THE “BE ALL AND END ALL”…

To understand today’s cybersecurity market it is essential to understand its origins. In the early 1990s, the first cybersecurity solutions on the market were antivirus (AV) software packages. These products worked by scanning all the binaries on a given system and testing them against a database of “signatures”. Introduced in 2007, Endpoint Protection Platforms (EPP) were the next step. Instead of relying on static signatures to identify viruses, they introduced the use of signatures that scanned for “malware families”.

In addition, EPPs offered an integrated security solution which included not only an antivirus, but also a personal firewall to detect and minimize the threat of malicious access to system resources through inbound and outbound network connections and other tools such as data encryption, intrusion prevention system (IPS) and data loss prevention (DLP).

An EPP is preventative, and is mostly signature-based, which proved to have several weaknesses. Malware solutions were evolving, and some authors started to add extra bytes to files to change the signature or to encrypt strings that could be easily read by binary scanning. However, the main issue with EPPs is that they are file-based tools, and hackers developed “fileless” malware, exploiting built-in applications and processes (a tactic called “living off the land”) and compromising networks by “phishing” users for credentials. This new wave of tactics, techniques and procedures was not leaving signatures behind, sidestepping EPPs (see WannaCry case study above on a ransomware which used fileless techniques).

…BUT THEIR LIMITATIONS LED TO THE EMERGENCE OF DETECTION-BASED TOOLS

While EPPs were the main security tool, another type of security solution, Security Information and Event Management (SIEM), came to the market. These solutions were part of a push to gain visibility of network traffic and logs to identify security threats but were unable to act on the endpoints.

ADVENT OF EDR

In 2013, Gartner analyst Anton Chuvakin coined the term “Endpoint Detection and Response (EDR)” to describe a new family of security tools that focused on bringing more visibility into what was happening specifically on an endpoint. Whereas EPPs were based on prevention, EDR platforms work with a new detection-led approach based on detecting anomalies and responding accordingly. While an EPP would identify a threat based on its signature and quarantine any file suspected of being a malware, an EDR works by detecting suspicious activities and providing alerts to security teams that could trigger further investigation. In order to work, an EDR records every file execution and modification, registry change, network connection and binary execution across an organization’s endpoints.

Aside from detection, EDR tools also integrate forensic analysis and remediation capabilities. These enable the alerted security team to delve deeper into the infected endpoint and to intervene remotely to stop the threat.

In the age of cloud and mobility, EDRs have had to adapt quickly and some providers are now offering an extension of their desktop EDR for smartphones, IoT objects and more recently for containers (virtualized Operating Systems) in data centres. In the next decade, we expect serverless architectures (or Function-as-a-Service, “FaaS”) to gain ground, removing the endpoint as we know it today. EDR tools will need to continue to evolve to be able to instrument, i.e. to collect data from those new architectures, either through APIs or by being embedded directly into the source code of the function.

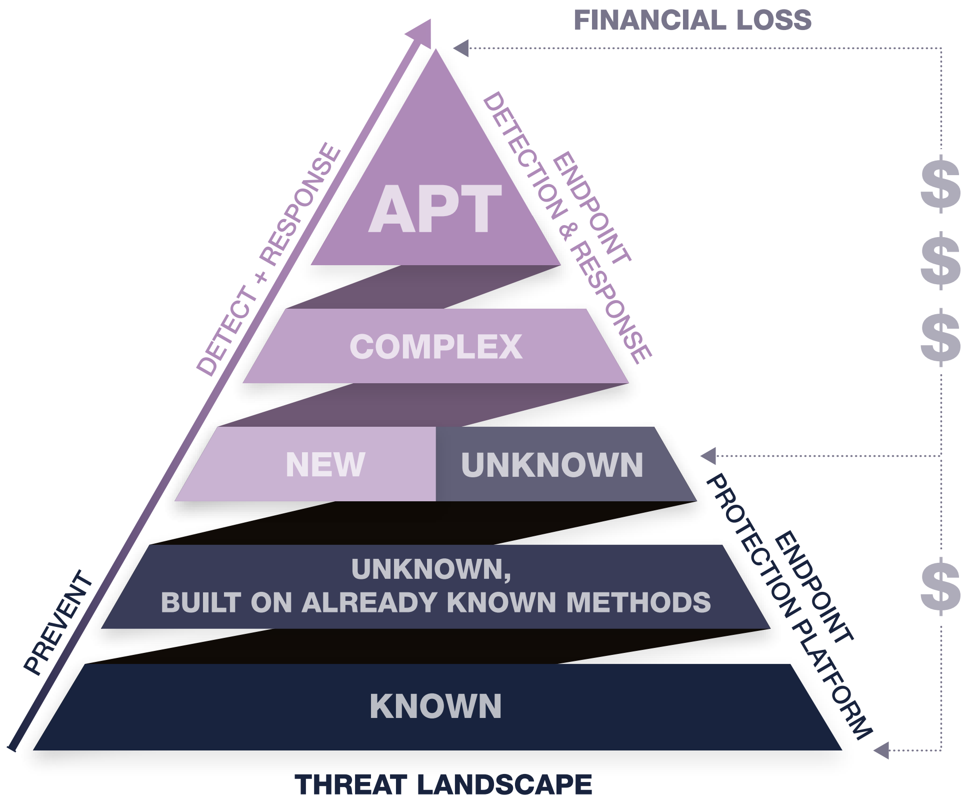
CONVERGENCE OF EDR AND EPP

The lines between EPP and EDR are becoming blurred today. Most EPP providers are introducing EDR capabilities inside their solution, while EDR providers are adding prevention capabilities. Although the solutions are converging, the fundamental approach has changed. Prevention is still needed but can mostly only take care of known commoditized threats, while detection-led tools are useful for dealing with the more advanced, complex and unknown threats that cause the most harm for organizations today.

Current solutions are slow to detect and contain breaches

279 days: *average time to identify and contain a breach in 2019, up 4.9% since 2018. (Identification took 206 days and containment 73 days)*

FIG. 5: EDR AND EPP HELP PROTECT THE COMPANY FROM DIFFERENT THREATS



Source: Kaspersky daily blog, May 2018

ENDPOINT DETECTION AND RESPONSE IS PART OF A WIDER ARRAY OF NEW COMPLEMENTARY SECURITY TOOLS

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) / TELEMETRY

SIEM tools provide the backbone of IT infrastructure monitoring. They aggregate data from multiple systems, and analyze it to detect abnormal behavior or potential cyberattacks and alert security teams. SIEM provides the types of data needed to meet many compliance and regulatory requirements, as well as for deeper forensic analysis.

Although they first appeared during the 2000s with companies such as ArcSight (acquired by HP in 2010) or Q1 Labs (acquired by IBM in 2011), SIEM tools saw their first revolution in 2010 with the emergence of log management players making their first steps in security such as Splunk and its ability to index in near real-time at low cost or Elastic, allowing SIEMs to operate at a much larger scale and with significantly better performance.

SIEM saw a further revolution in 2014-2015 with improved analytics that used machine learning, and convergence with User and Entity Behavior Analytics (UEBA) tools, which make SIEMs better at detecting abnormal behaviour. SIEMs complement EDR tools, as they aggregate data from multiple sources, not just endpoints, and generally provide better correlation capabilities. However, |they do not replace EDR tools, which act as a sensor on the endpoints and are used to collect or “instrument” data and provide remediation capabilities.

CASE STUDY:

How Elastic is changing the security game...

elastic

Elastic is famous for its ElasticSearch search engine, and more generally the Elastic Stack. The open-source Elastic Stack has been used by security analysts to detect and mitigate malicious behavior. However, 2019 marked the year when Elastic fully entered the security market, first by releasing Elastic SIEM in June and then by closing the acquisition of Endgame, an endpoint security solutions provider, in October. Elastic’s software is open source, offering subscriptions to its stack for users who want to add functionality. Elastic has made its SIEM free, with its endpoint protection, detection and response stack however only included in the paid version of its software. This is a game-changer in the security industry, as other EPP and EDR providers have been pricing their offer per endpoint. Elastic’s pricing is based on resource capacity, eliminating the traditional per-endpoint pricing.

CASE STUDY:

Leading other major security players to follow the same path

CROWDSTRIKE

After Elastic’s decision to end the per-endpoint pricing for its EDR, Crowdstrike followed the same approach and in November 2019 announced the availability of its Falcon platform on AWS, with billing based on consumption. We expect this trend to continue in the near future, with other players announcing new pricing methods.

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR)

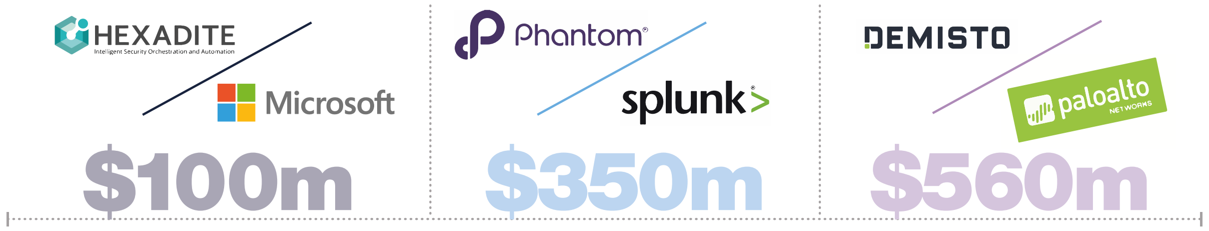
The emerging SOAR solutions integrate with other security tools inside an organization, providing an additional layer that aims to improve the speed at which an organization can respond to a security event.

SOAR solutions can enhance the capabilities of EDR and SIEM solutions by providing the "missing link" between them. They can orchestrate information from the two solutions and automate the response.

SOAR tools are especially effective against low-level security events as they can automatically apply incident response (IR) procedures already tested in earlier incidents, allowing security teams to focus on more advanced threats.

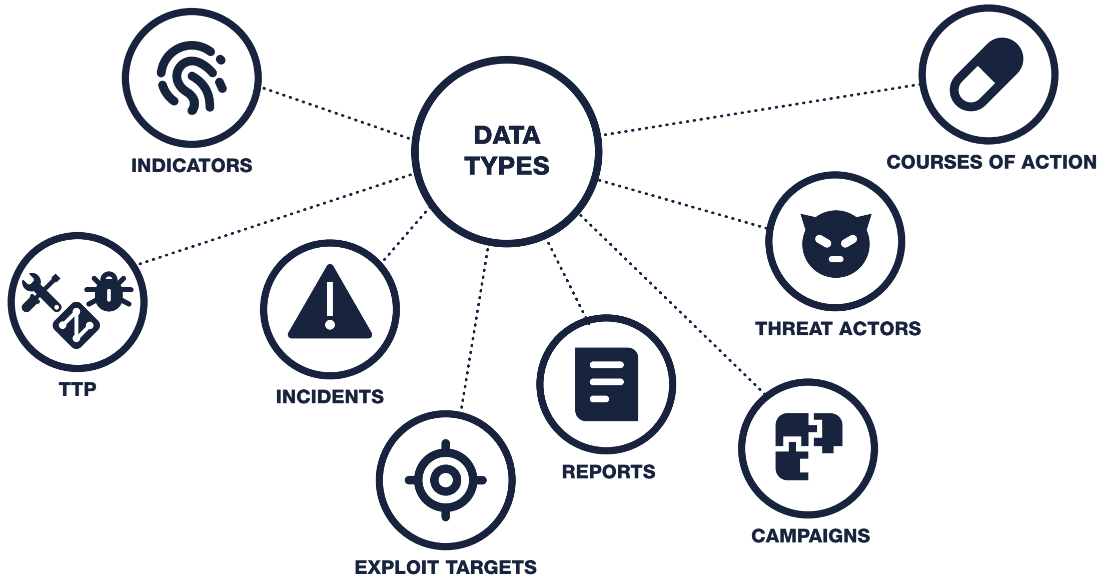
SOAR solutions are a hot commodity right now, as evidenced by the two large recent transactions: Palo Alto Networks' acquisition of Demisto for USD560m to pair it with its EDR; and Splunk, a SIEM solution provider, acquiring Phantom Cyber for USD350m.

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR)



Source: Palo Alto Networks; Splunk; Reuters

FIG. 6: OVERVIEW OF CYBER THREAT INTELLIGENCE DATA TYPES



Source: Bryan, Garnier & Co

CYBER THREAT INTELLIGENCE (CTI) SOFTWARE

More than a tool, CTI is a discipline. It enables the aggregation, analysis and sorting of all the data related to a cyberattack, attacker identities, their motivations, modus operandi and tactics, techniques and procedures. In more concrete terms, CTI can, for example, help identify the different malware families used over time with a specific attack or who is involved in an attack. For over 20 years, CTI has been used together with other tools to empower other security solutions. It took off with Snort (open source) and SourceFire (commercial), which are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), both created by SourceFire founder Martin Roesch. These tools are used to monitor networks for malicious activity or policy violations and need CTI feeds to operate.

Since then, the use of CTI has been steadily rising over the past two decades, notably expanding in recent years inside corporations, with emergent software tools called Threat Intelligence Platforms (TIP) and the reorganization of processes inside security teams. Unlike EDR and SIEM tools, which are focused on internal information, CTI is dedicated to external threat information and its goal is to describe what a "needle" looks like. Without CTI, security tools are looking for a needle in a haystack without knowing what the needle looks like. CTI can be vital to providing a comprehensive view of the threat landscape, understanding and predicting attacks and threat developments. TIPs are thus very useful to visualize and make sense of the threat landscape, investigate threats and specific attacks to provide context and insights into specific attacks that organizations experience, as well as to facilitate analyst collaboration. They help identify key information such as attacker type, group, motivations and techniques (see Fig. 6).

The CTI market is split between content providers, technology providers and service providers.

- Content providers analyze information derived from technical sources such as network traffic, files and human sources, including the infiltration of hacker and fraud groups or cooperation with industry groups to infer complex information on cyber threats.
- A technology provider sells a Threat Intelligence Platform (TIP), which facilitates the aggregation of CTI from multiple sources, as well as the normalization, enrichment, correlation, and analysis of the data before threat information is disseminated and shared.
- An organization can outsource these tasks to service providers.

CASE STUDY: FOCUS ON CYBER THREAT INTELLIGENCE TECHNOLOGY PROVIDERS

The acquisition of iSIGHT Partners by FireEye marked the start of CTI technology deals

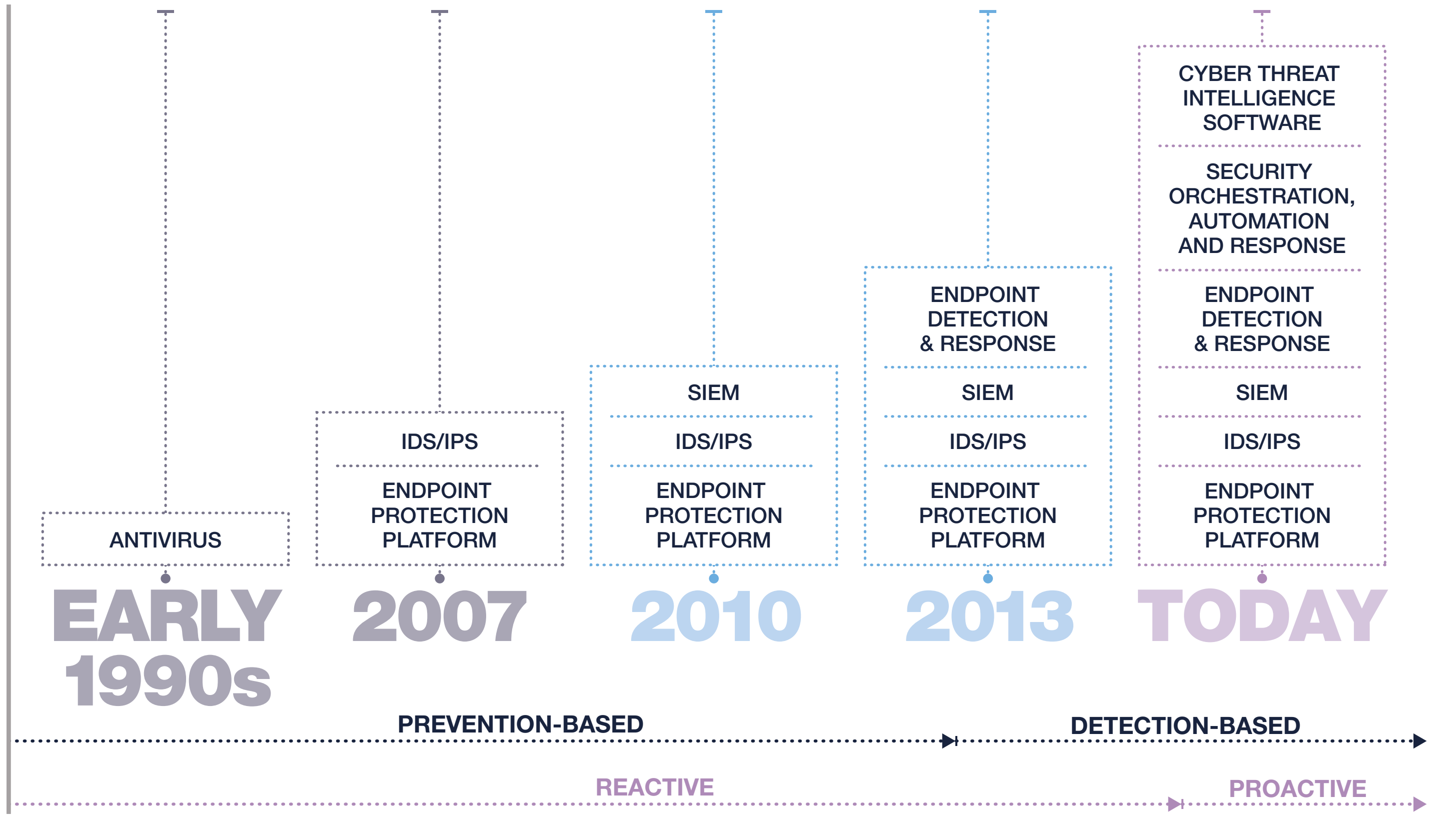
In 2016, FireEye, a major EDR player, acquired iSIGHT Partners, the biggest Threat Intelligence provider at the time, in a deal valued at USD275m. This acquisition was followed by three threat intelligence platform providers raising funds in the space: Anomali, which raised USD30m in a Series C and USD40m in a Series D; EclecticIQ, which raised USD19.5m in two rounds; and Threat Quotient, which raised USD42m in two rounds.

ANOMALI	: $96m raised
EclecticIQ	: $20.5m raised
THREATQUOTIENT	: $64.5m raised

OUR TAKE ON THE MARKET

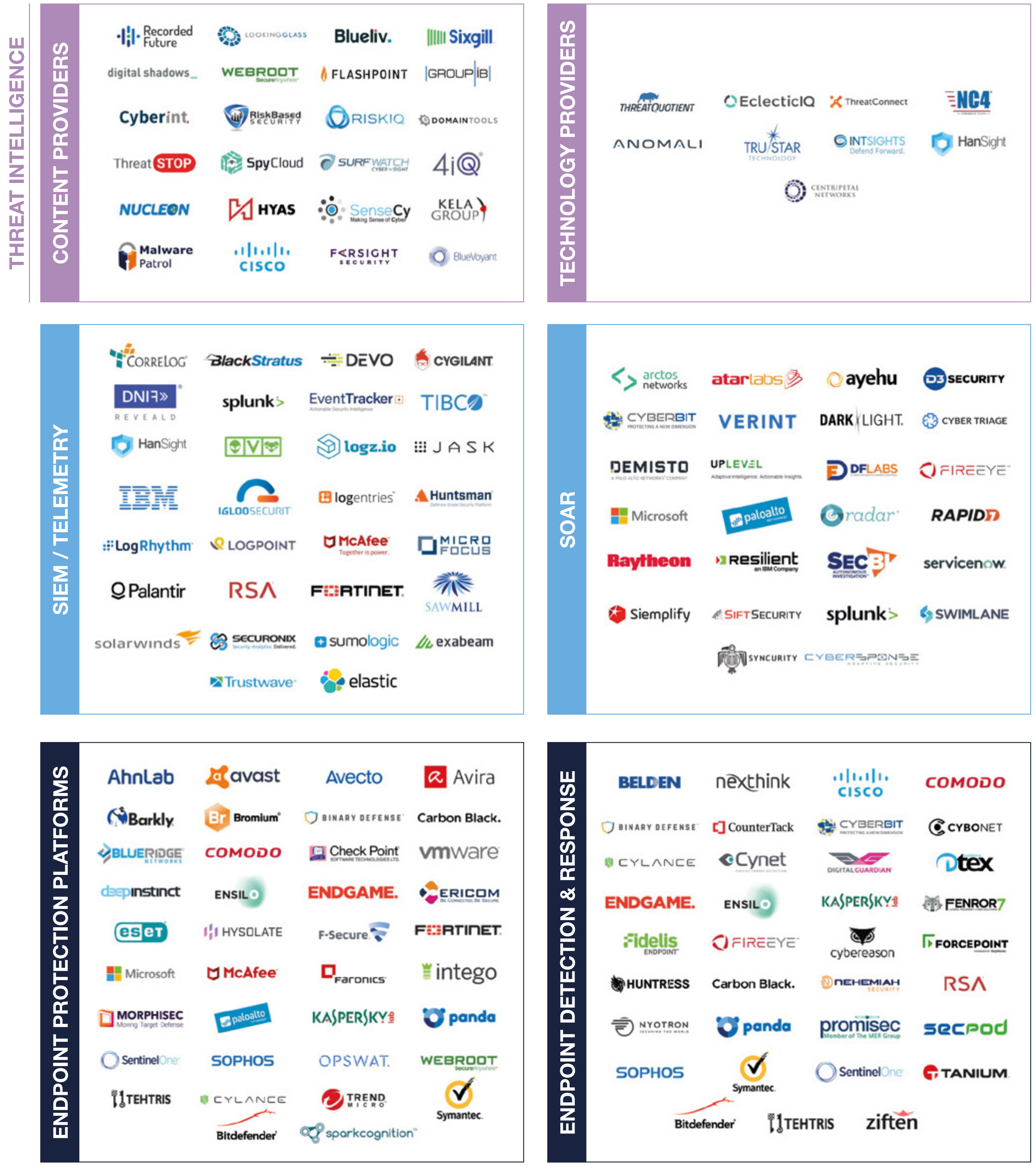
The cybersecurity market has known profound change. Tools with new approaches have been released as time has gone by, adding new security layers on top of the exisiting solutions. More than tools, the mindset of cyber defenders has also evolved. In 2013, prevention-based solutions such as Endpoint Protection Platforms were complemented by new detection-led tools such as Endpoint Detection & Response. However, this is not sufficient to efficiently fend off threats, and cyberdefenders have to take a proactive, rather than a reactive, approach. The use of Cyber Threat Intelligence software solutions and Orchestration tools enables this proactive stance.

FIG. 7: EVOLUTION OF THE CYBERSECURITY MARKET


ANTIVIRUS
EARLY 1990s
IDS/IPS
ENDPOINT PROTECTION PLATFORM
2007
SIEM
IDS/IPS
ENDPOINT PROTECTION PLATFORM
2010
ENDPOINT DETECTION & RESPONSE
SIEM
IDS/IPS
ENDPOINT PROTECTION PLATFORM
2013
CYBER THREAT INTELLIGENCE SOFTWARE
SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE
ENDPOINT DETECTION & RESPONSE
SIEM
IDS/IPS
ENDPOINT PROTECTION PLATFORM
TODAY
PREVENTION-BASED
DETECTION-BASED
REACTIVE
PROACTIVE

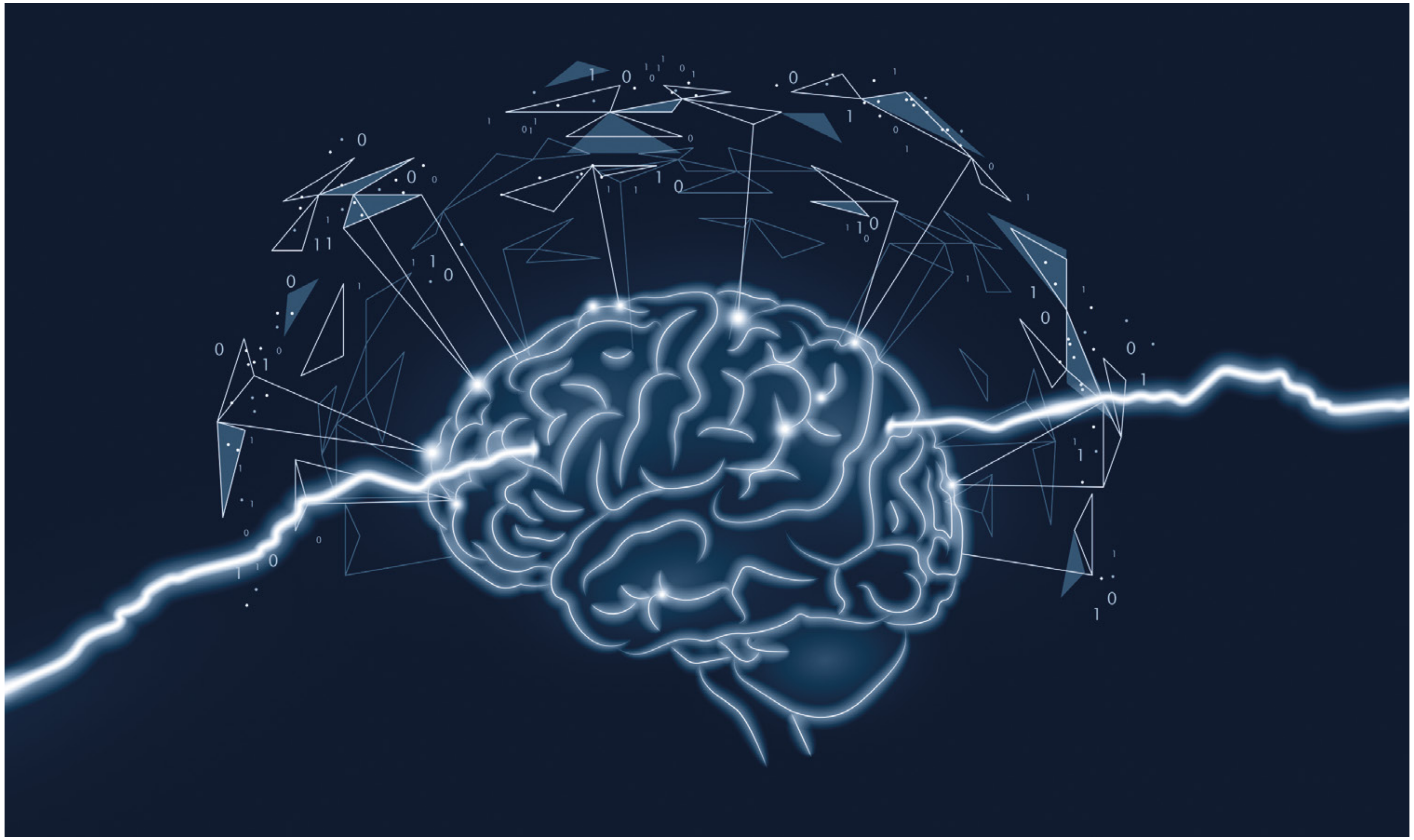
Source: Bryan, Garnier & Co

FIG. 8: LANDSCAPE OF THE THREAT INTELLIGENCE, SIEM, SOAR, EPP AND EDR MARKETS



Source: Bryan, Garnier & Co

Prevention and detection tools are reactive. Taking the next step means being proactive: the rise of Cyber Threat Intelligence



ORGANIZATIONS ARE ADAPTING THEIR CYBERSECURITY PROCESSES TO ENABLE A MORE PROACTIVE STANCE

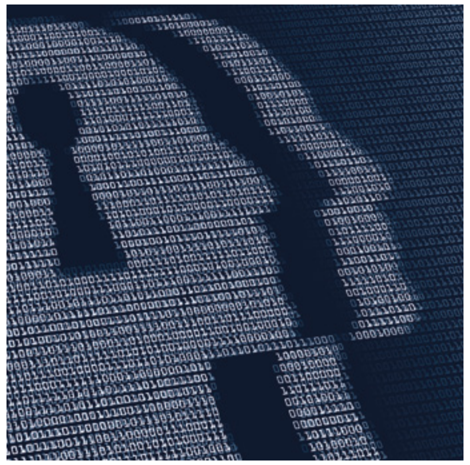
Tools alone are not enough for an organization to have a mature and efficient cybersecurity practice. Organizations also need to put in place processes and teams, and give them the means to collaborate.

Security Operations Center (SOC): Alone, a SOC will handle all the security operations of an organization, although its capabilities can be extended by a third-party security provider. The two main roles of the SOC are maintaining security-monitoring tools and investigating potentially suspicious activities. SOCs focus on internal information. Their role is mainly prevention, although they tend to have more and more detection and response responsibilities. The main issue faced by a SOC are the numbers of false positives and assessing the anomalies to investigate in priority.

Incident Response team: When an organization has an Incident Response (IR) team, also known as a Computer Emergency Response Team (CERT), it takes over the investigation and response process. However, its responsibilities are not limited to investigating an anomaly and responding to a threat, but also include developing an incident response plan, and testing for and resolving system vulnerabilities.

IR teams are mainstream in large organizations nowadays. Unlike SOC, they focus on detection and response.

CTI team: Compared to incident response and security operations practices, threat intelligence is still in the "early adoption" phase. Although it is increasingly common for governments to have a CTI practice, corporations have only just begun to develop CTI teams. The first companies to introduce CTI in their processes have been global financial institutions and operators of critical infrastructure, helped by governments.



Having a CTI practice is the first step an organization can take towards taking a more proactive approach to cybersecurity. Although the practice is still underdeveloped in the enterprise market, it is now being adopted by large corporations in many industries. When an organization lacks a dedicated CTI team, its responsibilities are fragmented between the SOC and IR teams and CTI is mostly used as a reactive tool.

> *According to a study by (ISC)2, the shortage of cybersecurity workers is close to four million globally.*

Companies can also choose to extend their security capabilities by engaging third-party security providers such as Managed Security Service Providers (MSSP) or Managed Detection and Response (MDR) providers, who are specialized MSSPs with strong Incident Response skills.

However, and as is the case with corporations, third-party security providers struggle to find and retain talent in an industry where labour shortage is a common issue. According to a study by (ISC)2, the world's largest nonprofit association of certified cybersecurity professionals, the shortage of cybersecurity workers is close to four million globally.

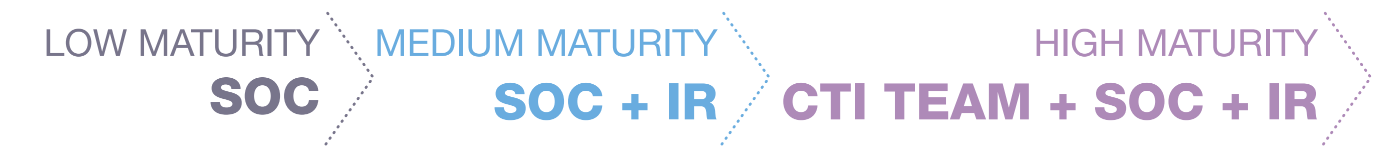
INTEGRATING THREAT INTELLIGENCE IS BECOMING A MUST-HAVE FOR MODERN THREAT-FACING SOLUTIONS

On its own, Cyber Threat Intelligence will only have limited use. Intelligence needs to be pervasive in an organization: it should be fed to key decision makers and to other security teams and tools. Decision makers such as CISOs (Chief Information Security Officers) can make use of Cyber Threat Intelligence to more effectively communicate their organization's cybersecurity needs and goals to other members of the executive team, better assess the risks faced by the industry and to identify the right strategy to mitigate those risks.

More operational teams such as the SOC and the IR teams also benefit from CTI in their day-to-day operations, as it improves their efficiency. By integrating CTI into a SIEM, the SOC will benefit from better information, which will lead to a better process for prioritizing which threats are the most critical. SIEM tools will also benefit from more information, which will improve their threat detection capabilities by reducing the number of false positives and increasing the probability of detecting stealthy threats. The latter is also true for EDR solutions, for which CTI will also prove helpful to determine the best course of action once a threat has been detected. Finally, combining CTI and a SOAR will enable a better assessment of the risks posed by a detected anomaly, a better damage assessment if the anomaly proved to be a malware, and a quicker response.

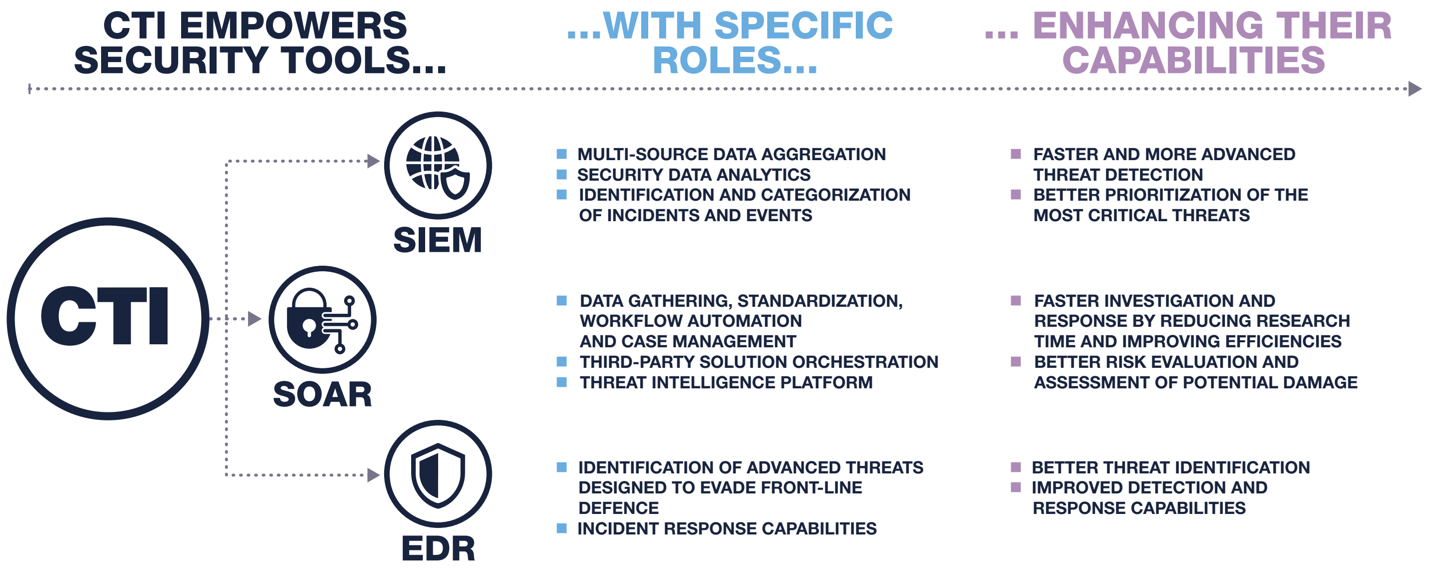
To make the most of CTI, a Threat Intelligence Platform is helpful. It provides a single source of truth that feeds all other solutions, reduces the chance that details on an attack are missed and increases the chance of catching an attack.

FIG. 9: ORGANIZATION OF CYBERSECURITY PROCESSES IN ORGANIZATIONS



Source: Bryan, Garnier & Co

FIG. 10: CTI IS PERVASIVE AND EMPOWERS EXISTING SECURITY SOLUTIONS


CTI EMPOWERS SECURITY TOOLS...
...WITH SPECIFIC ROLES...
... ENHANCING THEIR CAPABILITIES
CTI
SIEM
SOAR
EDR

SIEM
- MULTI-SOURCE DATA AGGREGATION
- SECURITY DATA ANALYTICS
- IDENTIFICATION AND CATEGORIZATION OF INCIDENTS AND EVENTS

- FASTER AND MORE ADVANCED THREAT DETECTION
- BETTER PRIORITIZATION OF THE MOST CRITICAL THREATS

SOAR
- DATA GATHERING, STANDARDIZATION, WORKFLOW AUTOMATION AND CASE MANAGEMENT
- THIRD-PARTY SOLUTION ORCHESTRATION
- THREAT INTELLIGENCE PLATFORM

- FASTER INVESTIGATION AND RESPONSE BY REDUCING RESEARCH TIME AND IMPROVING EFFICIENCIES
- BETTER RISK EVALUATION AND ASSESSMENT OF POTENTIAL DAMAGE

EDR
- IDENTIFICATION OF ADVANCED THREATS DESIGNED TO EVADE FRONT-LINE DEFENCE
- INCIDENT RESPONSE CAPABILITIES

- BETTER THREAT IDENTIFICATION
- IMPROVED DETECTION AND RESPONSE CAPABILITIES

Source: Bryan, Garnier & Co

ENABLING THREAT HUNTING

Threat Intelligence not only enhances the capabilities of existing security solutions inside an organization – it also adds the missing piece needed to develop a “Threat Hunting” practice.

Threat hunting means searching for malware or attackers that have penetrated your network. It is a proactive, analyst-driven process that seeks to uncover the presence of attacker tactics, techniques, and procedures within an environment that have been under the radar or perhaps mis-identified as a false positive by a SOC operator or MSSP provider. The goal of Threat Hunting is to ensure that an organization’s reactive becomes everyone else’s proactive. It is an aggressive tactic that works under the assumption that an organization’s systems have been breached even though few or no anomalies have been detected.

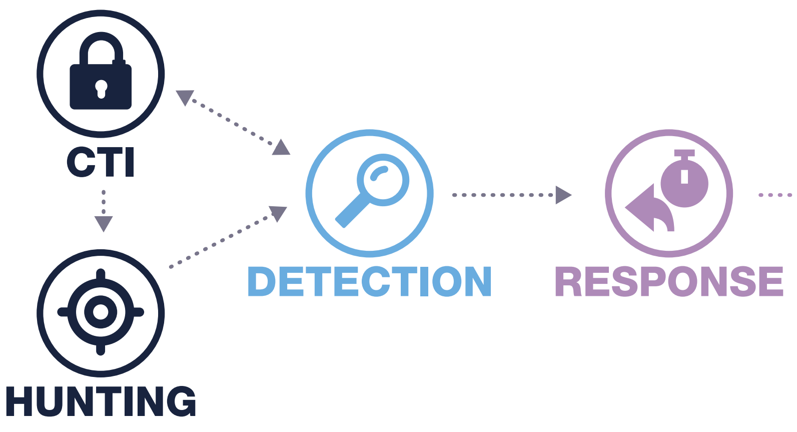
It requires highly skilled analysts and in-depth threat intelligence to know what to look for, and to find malicious activities that are often hard to detect. Threat Hunting requires an analyst to make a hypothesis about the type of threats that may have penetrated the environment. Combining Threat Intelligence (external data) with internal data helps the hunting analyst know the cyber threats that are common in his industry, and what threats are often associated with a previously detected anomaly that could have been considered a false positive.

WHAT’S NEXT FOR THE CYBERSECURITY MARKET? CONSOLIDATION IS LIKELY

In the future, we expect organizations to use fewer cybersecurity vendors to limit the silos between their security teams and solutions. We are already seeing SIEM and EDR vendors (excluding Microsoft and other major tech vendors from the discussion) as most likely to make acquisitions, either in the SOAR or the Cyber Threat Intelligence market, to add in the missing pieces to their offering and acquire key tools needed to become proactive. Ultimately, we could see players boasting a portfolio with the four product types (EDR, SIEM, SOAR, Threat Intelligence) and offering an integrated approach.

This integrated approach could be XDR, a new term that is currently used by only a few vendors but which is gaining popularity. Theoretically, an XDR can collect and aggregate data from virtually everything on a network: an endpoint, container, function or even an email. It works as a central data lake that is independent from other security solutions. All information from an organization’s system are fed into this data lake, which is the central component of its security infrastructure. This results in fewer silos and better overall security. Although players in the market are already advertising their XDR, the market is nascent and current offerings do not include the four solutions.

FIG. 11: HOW THREAT HUNTING, THREAT INTELLIGENCE, AND DETECTION TOOLS INTERACT



A VIRTUOUS CYCLE WITH EACH OF THE PRACTICE FEEDING FROM ONE ANOTHER:

- CTI FEEDS INTO THREAT HUNTING. THREAT HUNTING HELPS TO PROACTIVELY DETECT UNKNOWN THREATS AND THEN CREATE NEW DETECTION PATTERNS
- PROACTIVELY DETECT UNKNOWN THREATS AND THEN CREATE NEW DETECTION PATTERNS

Source: Bryan, Garnier & Co

CYBERSECURITY TRANSACTIONS

	DATE	TARGET	ACQUIRER / INVESTORS	DEAL VALUE (€M)	EV / SALES	TRANSACTION
THREAT INTELLIGENCE – CONTENT PROVIDER	May-19	Recorded Future	INSIGHT PARTNERS	700	n.a.	M&A Deal
	May-19	BlueVoyant	fiserv. TEMASEK	74	n.a.	Fundraising
	Oct-18	CybelAngel	serena bpifrance	10	n.a.	Fundraising
	Feb-18	RISKIQ	Battery	28	n.a.	Fundraising
	Sept-17	digital shadows_	octopus ventures	22	n.a.	Fundraising
	Jan-16	iSIGHTPARTNERS	FIREEYE	252	5.0x	Fundraising
	Dec-15	LOOKINGGLASS	NEWSPRING	47	n.a.	Fundraising

	DATE	TARGET	ACQUIRER / INVESTORS	DEAL VALUE (€M)	EV / SALES	TRANSACTION
THREAT INTELLIGENCE – TECHNOLOGY PROVIDER	Aug-19	NC4	everbridge	75	n.a.	M&A Deal
	Jun-19	ThreatConnect	PROVIDENCE EQUITY	72	n.a.	M&A Deal
	Jan-18	ANOMALI	VENTURES LUMIACAPITAL	33	n.a.	Fundraising
	Nov-17	EclecticIQ	KEEN	14	n.a.	Fundraising
	Oct-17	THREATQUOTIENT	Adams Street	26	n.a.	Fundraising

SIEM / IDS

DATE	TARGET	ACQUIRER / INVESTORS	DEAL VALUE (€M)	EV / SALES	TRANSACTION
Sept-19	DARKTRACE	VITRUVIAN PARTNERS	43	n.a.	Fundraising
May-19	sumo logic	Battery WiNG	98	n.a.	Fundraising
May-19	exabeam	Lightspeed	67	n.a.	Fundraising
Oct-18	solarwinds	–	431 (EV: €5,683m)	7.7x	IPO
Oct-18	elastic	–	216 (EV: €4,352m)	11.6x	IPO
Jul-18	AV ALIEN VAULT	AT&T	510	4.8x	M&A Deal
May-18	LogRhythm The Security Intelligence Company	THOMABRAVO	n.a.	n.a.	M&A Deal
Nov-17	logz.io	OPENVIEW	20	n.a.	Fundraising
Apr-17	LOGPOINT	evolution EQUITY PARTNERS	9	n.a.	Fundraising
Jan-16	Palantir	ventures.	810	n.a.	Fundraising
Jul-13	SOURCEfire	CISCO	1,715	10.2x	M&A Deal
Oct-11	Q1 Labs	IBM	n.a.	n.a.	M&A Deal
Sept-10	ArcSight An HP Company	hp	1,067	7.6x	M&A Deal

SOAR

DATE	TARGET	ACQUIRER / INVESTORS	DEAL VALUE (€M)	EV / SALES	TRANSACTION
Oct-19	SWIMLANE	ENERGY IMPACT PARTNERS	21	n.a.	Fundraising
Mar-19	DEMISTO	paloalto NETWORKS	411	10.0x	M&A Deal
Feb-18	Phantom	splunk>	247	n.a.	M&A Deal
Jul-17	KOMAND	RAPID7	13	n.a.	M&A Deal
May-17	HEXADITE Intelligent Security Orchestration and Automation	Microsoft	89	n.a.	M&A Deal
Jun-16	BrightPoint SECURITY	servicenow	18	n.a.	M&A Deal

EDR

DATE	TARGET	ACQUIRER / INVESTORS	DEAL VALUE (€M)	EV / SALES	TRANSACTION
Oct-19	SOPHOS	THOMABRAVO	3,583	5.7x	M&A Deal
Aug-19	Carbon Black.	vmware	1,895	10.0x	M&A Deal
Jun-19	CROWDSTRIKE	–	546 (EV: €10,433m)	15.8x	IPO
Jun-19	ENDGAME.	elastic	208	11.8x	M&A Deal
Apr-19	SentinelOne	INSIGHT PARTNERS	106	n.a.	Fundraising
Feb-19	CYLANCE	BlackBerry	1,231	n.a.	M&A Deal
Dec-18	nexthink	Index Ventures	75	n.a.	Fundraising
Oct-18	TANIUM	WELLINGTON MANAGEMENT	172	n.a.	Fundraising
Jul-17	GUIDANCE SOFTWARE	opentext	171	2.0x	M&A Deal

Conclusion

The cybersecurity market will undoubtedly continue to grow. The first endpoint security revolution, driven by a process that went from being prevention-led to detection-led at the beginning of the 2010s, led to the emergence of new large players displacing incumbents such as Symantec and McAfee. The market is now gradually changing its paradigm, abandoning its reactive stance in favor of a more proactive approach. In this process, Threat Intelligence is expected to play a key role, enhancing the performance of existing tools and enabling the development of Threat Hunting practices, while TIPs and orchestration tools will allow security teams to focus on more advanced and complex threats.

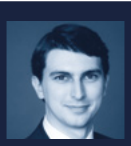
The market is also likely to consolidate, with SIEM and EDR vendors looking to acquire Threat Intelligence and SOAR players, which are the missing pieces towards a more proactive stance. This could lead to more actors developing XDR solutions, enabling a more consolidated approach to cybersecurity inside an organization.

BRYAN, GARNIER & CO

White paper authors

Greg Revenu
Managing Partner
Technology
grevenu@bryangarnier.com

Charlie Pujo
Director
Technology
cpuho@bryangarnier.com



David Vignon
Research Analyst
Software
dvignon@bryangarnier.com

Technology team

INVESTMENT BANKING

PARIS

Greg Revenu
Managing Partner
Technology
grevenu@bryangarnier.com

Olivier Beaudouin
Partner
Technology & Smart Industries
obeaudouin@bryangarnier.com

Guillaume Nathan
Partner, Digital Media
& Business Services
gnathan@bryangarnier.com

Thibaut De Smedt
Partner, Application
Software & IT Services
tdesmedt@bryangarnier.com

Philippe Patricot
Managing Director
Technology
ppatricot@bryangarnier.com

MUNICH

Falk Müller-Veerse
Partner
Technology
fmuellerveerse@bryangarnier.com

EQUITY RESEARCH ANALYST TEAM

Olivier Pauchaut
Managing Director
Financials & Fintech
opauchaut@bryangarnier.com

Thomas Coudry
Managing Director
Telecoms & Media
tcoudry@bryangarnier.com

Bruno de La Rochebrochard
Business Services
bdelarochebrochard@bryangarnier.com

Eric Lemarié
Smart Industries
elemarie@bryangarnier.com

Gregory Ramirez
Software & IT Services
gramirez@bryangarnier.com

Xavier Regnard
Smart Industries
xregnard@bryangarnier.com

David Vignon
Software
dvignon@bryangarnier.com

Fréderic Yoboué
Semiconductors
fyoboue@bryangarnier.com

EQUITY CAPITAL MARKETS

Pierre Kiecolt-Wahl
Partner
Head of ECM
pkiecoltwahl@bryangarnier.com

EQUITY DISTRIBUTION

Nicolas d'Halluin
Partner
Head of US Distribution
ndhalluin@bryangarnier.com

Corporate transactions

Bryan, Garnier & Co leverage in-depth sector expertise to create fruitful and long lasting relationships between investors and European growth companies.

BITFURY
Private Placement
$80 000 000
Sole Placement Agent

LEXSI
Acquired by
orange
Undisclosed
Advisor to the Sellers

InfoVista
Acquired by
THOMABRAVO
Public to Private
€ 85 000 000
Sole Advisor to the Buyers

codenomicon
Acquired by
synopsys
Undisclosed
Advisor to the Sellers

FircoSoft
Acquired by
rbi reed business information
Undisclosed
Co-Advisor to the Seller

About Bryan, Garnier & Co

Bryan, Garnier & Co is a European, full-service growth-focused independent investment banking partnership founded in 1996. The firm provides equity research, sales and trading, private and public capital raising as well as M&A services to growth companies and their investors. It focuses on key growth sectors of the economy including Technology, Healthcare, Consumer and Smart Industries & Services. Bryan, Garnier & Co is a fully registered broker dealer authorized and regulated by the FCA in Europe and the FINRA in the U.S. Bryan, Garnier & Co is headquartered in London, with additional offices in Paris, Munich, Stockholm, Oslo, Reykjavik as well as New York and Palo Alto. The firm is a member of the London Stock Exchange.

Bryan, Garnier & Co Technology, Smart Industries & Services Equity Research Coverage

adyen
altice
altran
ALTEN
ASM international
ASML
Atos
Besi
bouygues
Capgemini
CAST
DASSAULT SYSTEMES
dialog
easyVISTA
ekinops
indra
iliad
Infineon
ingenico GROUP
legrand
materialise
NEMETSCHEK GROUP
orange
RIBGroup
sage
SAP
Schneider Electric
software
somfy
soitec
sopra steria
ST life.augmented
SWORD
TEMENOS
TIM
wirecard
worldline
vivendi

8 ANALYSTS | 70+ STOCKS COVERED

With more than 150 professionals based in London, Paris, Munich, Stockholm, Oslo and Reykjavik as well as New York and Palo Alto, Bryan, Garnier & Co combines the services and expertise of a top-tier investment bank with a long-term client focus.

Bryan, Garnier & Co

LONDON
Beaufort House
15 St. Botolph Street
London
EC3A 7BB
UK
T: +44 (0) 20 7332 2500

PARIS
26 Avenue des Champs-Elysées
75008 Paris
France
T: +33 (0) 1 56 68 75 00

MUNICH
Widenmayerstrasse 29
80538 Munich
Germany
T: +49 89 242 262 11

STOCKHOLM
Malmskillnadsgatan 32
6th Floor
111 51 Stockholm
Sweden
T: +46 722 401 080

OSLO
Beddingent 8, Aker Brygge
Postbox: 0117 Oslo
0250 Oslo
Norway
T: +47 21 01 64 00

REYKJAVIK
Höfðatorg, Katrínartún 2
105 Reykjavik
Iceland
T: +354 554 78 00

NEW YORK
750 Lexington Avenue,
16th Floor
New York NY 10022
USA
T: +1 (0) 212 337 7000

PALO ALTO
394 University Avenue
Palo Alto
California CA 94301
USA
T: +1 650 283 18 34

BRYANGARNIER.COM

DISCLAIMER

This document is based on information available to the public and other sources deemed reliable. No representation or warranty, express or implied, is or will be made in relation to, and no responsibility or reliability is or will be accepted by Bryan Garnier & Company or any of its officers, employees or advisers as to the accuracy or completeness of this document or any other written or verbal information available to the recipient or its advisers. While all reasonable care has been taken to ensure that the facts stated are accurate and the opinions given are fair and reasonable, neither we nor any of our affiliated companies nor any of our, or their directors, representatives or employees, accepts responsibility or liability for any loss or expense arising directly or indirectly from the use of this document or its or its contents. This document is not and should not be construed as an offer, or a solicitation of any offer, to buy or sell securities. Bryan, Garnier & Co is authorised and regulated by the Financial Conduct Authority (FCA) in the United Kingdom.