White Paper

Towards Threat Wisdom: Combining Data, Context and Expertise to Optimise Threat Intelligence

Sponsored by: SecureData

Duncan Brown
November 2015

IDC OPINION

Threat intelligence is one of the primary trends within the broad cyber security market. Yet it is one of the least well understood, and many companies have experienced poor results with their deployments as a result of insufficiently scoped and defined programmes.

IDC conducted a study of large UK companies to determine their understanding of threat intelligence and to identify the key factors to success.

Key Findings From the Study

Threat intelligence is a service. Much has been made of the concept of threat intelligence, where data from multiple sources is collated and correlated to provide actionable advice for security operations. Many providers offer data feeds and other resources that they brand as a threat intelligence. But our survey shows that enterprises regard threat intelligence as a combination of both products and services, and in some cases exclusively delivered as a service. This is partly because of the increase in adoption of security services more generally, and also due to the lack of in-house skills and resources with which to absorb and utilise threat intelligence.

Threat intelligence means faster response. Companies utilise threat intelligence for a variety of reasons, but the most prevalent by far is that it allows them to prepare better for attacks and respond to them faster. This is important as the number and severity of attacks increases, and also because of the importance of discovering attacks early, rather than having a sustained penetration for weeks or months.

Are CISOs myopic when it comes to threat intelligence? Chief information security officers (CIOSs) integrate their threat intelligence capabilities with feeds from their own security infrastructure, but they ignore other external data sources, such as threat feeds, and even disregard other data from within their own organisation, such as physical security information. We think this misses an opportunity to provide a holistic and integrated view of security across the entire organisation. Are CISOs being short-sighted?

In fact, our study shows that enterprises intend to invest in such insight and context as a priority in the coming year. So it's less a case of myopia and more one of maturity, as CISOs understand the importance of increased context.

Firms outsource for better performance. Our study shows that around two-thirds of organisations outsource some or all of their security operations to a third party. One might think that they do this because of cost drivers, or because they cannot find sufficient staff to resource those operations.

In fact, our survey suggests that the primary driver for outsourcing is to achieve better performance, most notably in improvements in visibility, monitoring and overall control of security.

Methodology

For this white paper, IDC conducted a survey of UK-based organisations with at least 500 employees. We conducted 300 interviews across a broad range of industries including technology, media and telecoms; financial services; professional services; manufacturing and construction; transport, travel and leisure; and retail. We spoke to heads of IT and security. Interviews were conducted via telephone using computer assisted telephone interviewing (CATI) technology. The survey was conducted between September and October 2015.

TABLE OF CONTENTS

IN THIS WHITE PAPER

This IDC White Paper examines the understanding and use of threat intelligence by large companies in the UK, and highlights the limited boundary and scope of information that is typically considered as input into threat intelligence capability.

SITUATION OVERVIEW

Modern security operations face an unprecedented level of challenges, both from external sources and within their own organisations.

Most companies in the UK have embarked on programs of digital transformation, in which they seek to incorporate new core capabilities such as mobile, clouds, analytics and social, in order to deliver a new and better experience for their customers, suppliers and employees. This means opening their organisations in order to integrate with other technologies and make it easier for external parties to engage. But this, of course, also exposes organisations to an increased attack surface against which malicious threats may be targeted.

Meanwhile, the number and type of attacks is expanding exponentially. Cyber-attacks are no longer the preserve of amateurish hackers; they are the result of professional organisations that are resourceful and persistent. Today's cyber-attacks are well-planned, methodical and determined to penetrate your organisation. Companies need not only to detect and prevent threats from attacking their institution, but also to assess the threat of vulnerabilities applicable to their organisation, to respond to threats that have evaded detection, and to remediate these threats as quickly as possible.

Dealing with digital transformation requirements and an ever-increasing attack threat landscape would be hard enough, if organisations could find enough human resources to meet the challenges faced by security operations. But a global cyber security skills shortage means that companies struggle to find enough people to deliver the required services and capability.

Firms have traditionally dealt with security threats by employing large-scale event monitoring systems that scoop up vast quantities of information about what is happening on their network. Firms also use external threat information feeds to alert them to possible attacks. Combining numerous events with this external information creates a vast quantity of data, through which an organisation must hunt for the crucial evidence of an imminent (or already successful) attack.

But such approaches require constant tuning to detect and minimise false positives, to review and revise the relevance of data feeds, and to optimise the timeliness of priority alerts.

Adding context to this plethora of information would help organisations understand more about the likelihood of an attack. Security managers could ask: Are threats being seen by similar organisations? Are threats relevant to my firm's infrastructure consideration? Would threats be mildly inconvenient or catastrophic to my organisation?

The fact is, though, that many organisations do not have the capabilities, either skilled resources or technologies, to be able to interpret event, threat and contextual information, or to tune results on a continuous basis. They have a multitude of threat information: what they lack is threat intelligence.

IDC conducted a survey of 300 larger organisations (with 500 employees or more) to examine their attitudes and approaches to threat intelligence. This report outlines our findings and provides recommendations for companies to maximise the benefit of true threat intelligence.

What do Enterprises Understand by the Term "Threat Intelligence"?

What's in, What's Out?

All of our respondents have heard the term threat intelligence, and 90% of them stated that they are familiar with the term. Firms differ, though, on what they understand by threat intelligence (see Figure 1). More than three-quarters of our respondents (77%) regard threat intelligence as security incident and event management (SIEM), and slightly less as risk-based analysis of threats and recommended remediation (73%). Over 60% of respondents include remediation of attacks (61%) and data feeds of vulnerabilities and other threats (64%) as a core element of threat intelligence.

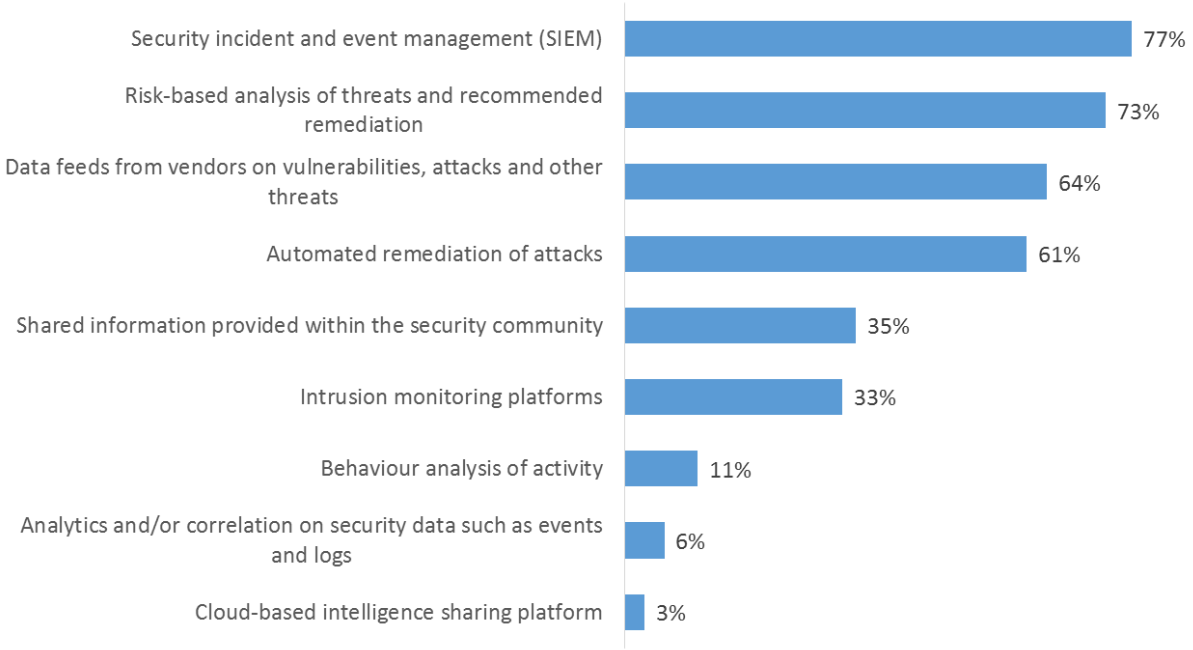
A minority of surveyed organisations think that threat intelligence includes intrusion monitoring (33%), or the sharing of information within the security community (35%). An even smaller group includes analytics, either based on behaviour (11%) or correlation of security data (6%). Almost no respondents (3%) think that cloud-based intelligence sharing is part of threat intelligence. These numbers betray a somewhat traditional view of intelligence and discount the more innovative developments in threat intelligence.

There are few differences across industry sectors, with financial services firms more focused on risk-based analysis of threats than respondents generally (85% versus 73%).

FIGURE 1

Understanding Threat Intelligence

Q. What is your understanding of the term threat intelligence?



Source: IDC, 2015

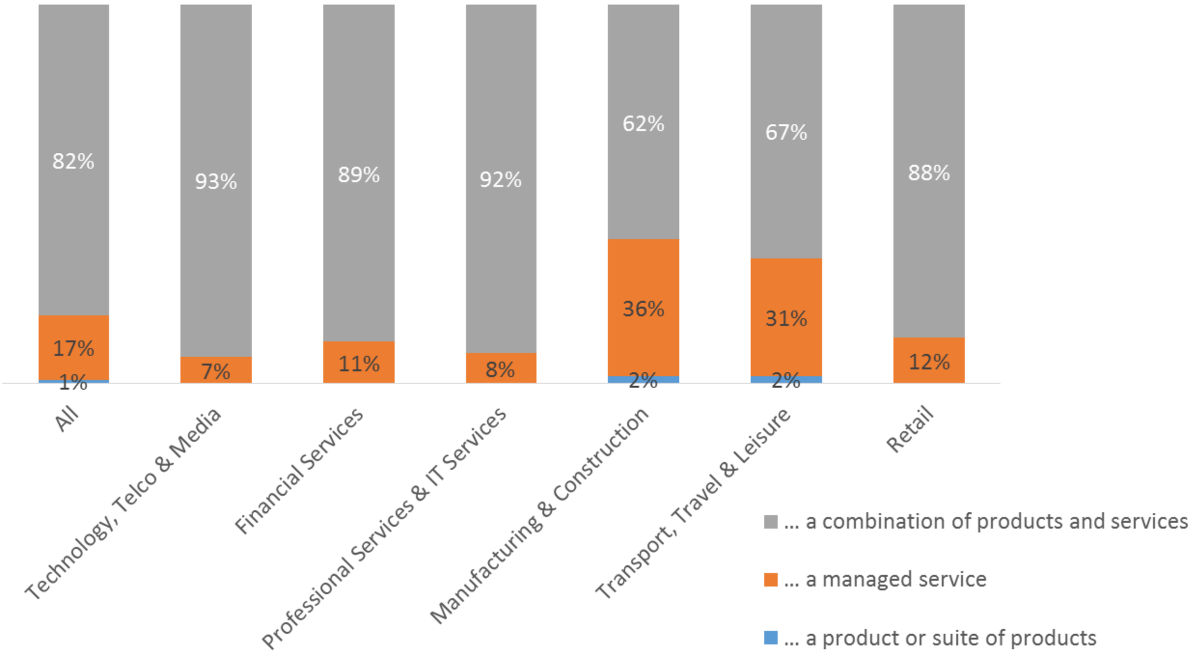
Threat Intelligence as a Service

99% of our sample believe that threat intelligence is a combination of products and services, or a pure managed service.

A very high 96% of firms say that they currently use threat intelligence products and services in their organisations, and all respondents say that they will be using threat intelligence within the next 24 months. This shows that, notwithstanding the differences in definitions, all large firms have a high awareness and adoption (or intent to adopt) of threat intelligence. Manufacturing and construction firms have the lowest adoption rate (85%), and all technology, financial services and retail firms had adopted threat intelligence.

FIGURE 2

In Your View, is "Threat Intelligence"...



Source: IDC, 2015

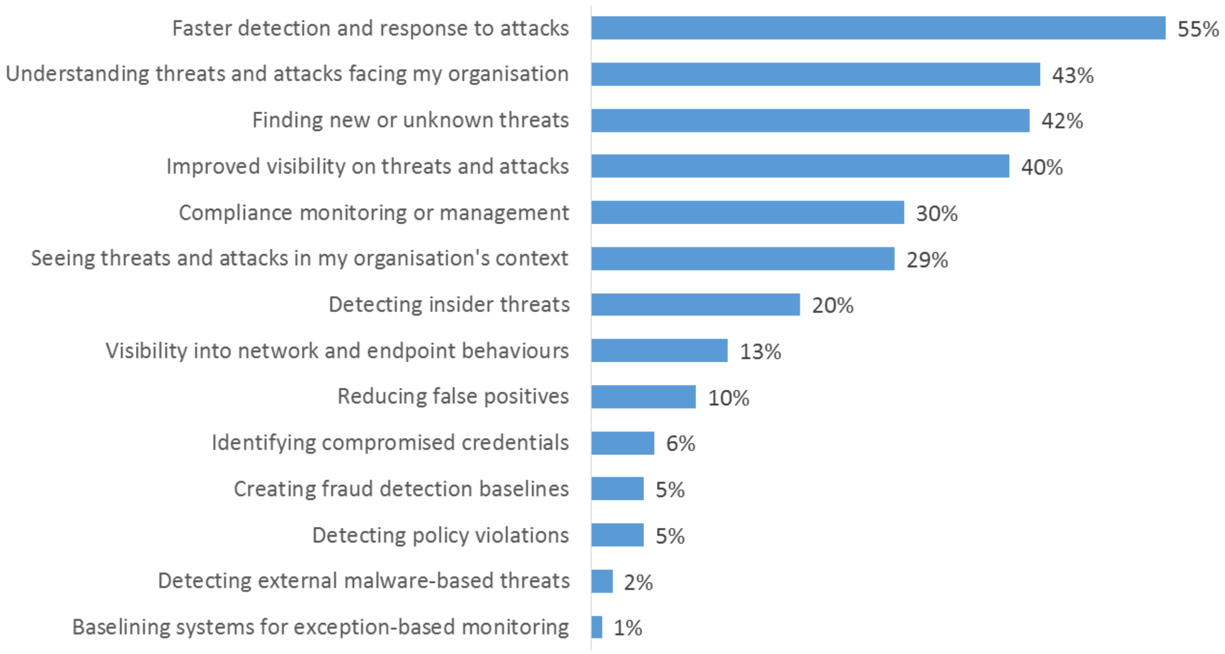
Threat Intelligence Means Faster Response

Over half (55%) of our respondents believe that faster detection and response to attacks is the primary benefit of threat intelligence. This is, by far, the most popular response and it illustrates the imperative of finding attacks before or as they happen, and responding to them quickly.

FIGURE 3

Threat Intelligence: Perceived Benefits

Q. What benefits do you see threat intelligence providing



Source: IDC, 2015

Also important is the understanding of threats facing the respondents' own organisations. We think this is an extremely important attribute for threat intelligence and are encouraged at 43% of companies with this view. Curiously, though, seeing attacks and threats within an organisation's context was much less important (29%): this apparent contradiction may be explained by respondents being more focused on direct threats to them, rather than a wider and more contextual basis for threat assessment. We explore this issue in more detail later in this study.

More obvious threat intelligence attributes are improved visibility and finding new or unknown threats; compliance monitoring is also important.

Financial services show the most divergence from the broad picture, with improved visibility on threats and attacks much less important (19% versus 40%), but reducing false positive much more important than the total average (48% versus 10%). This is most likely a function of the maturity of threat intelligence within financial services, with these business having mature SIEM deployments.

The Perceived Need for Threat Intelligence

Are CISOs Myopic?

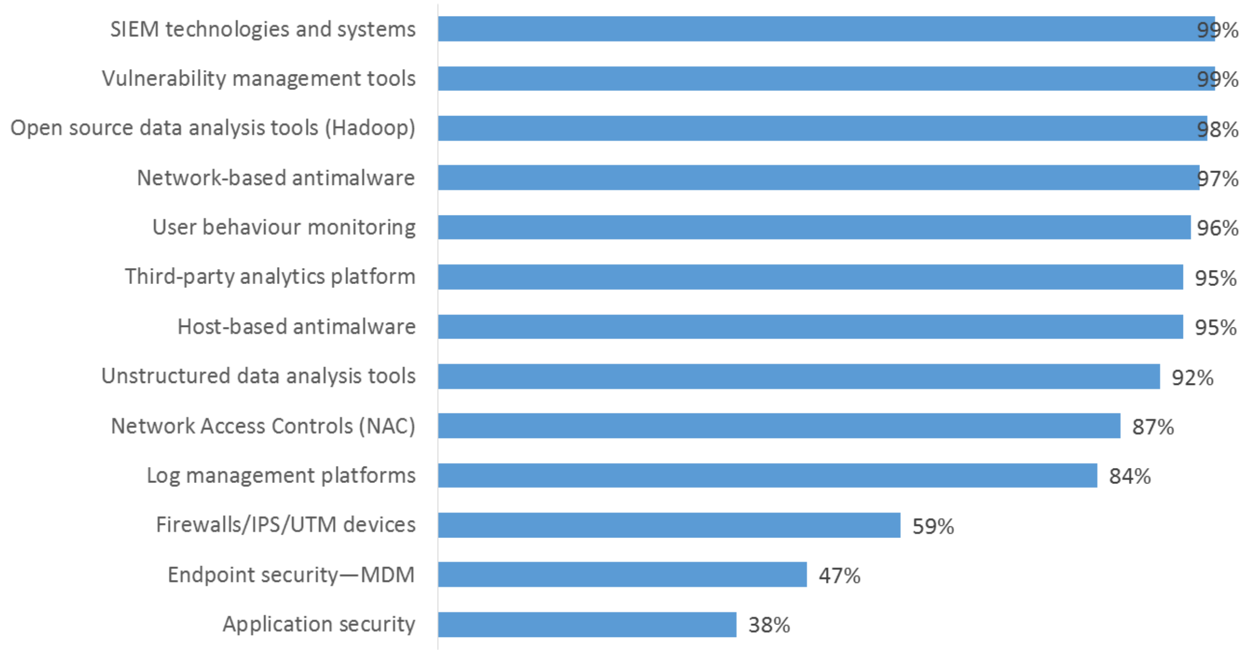
Respondents in our survey show a high propensity to integrate security feeds from within their existing infrastructure. Many organisations already collect a substantial amount of information across their IT security infrastructure. Firewalls are the near-ubiquitous data provider in our sample. But fewer than 60% of respondents integrate data from their firewall or UTM devices into their threat intelligence platform. And although 86% of organisations use an MDM to manage mobile devices, less than half (47%) integrate data from their system with their threat intelligence platform.

Of interest, application security is making an appearance as a key correlation input. AppSec is relatively immature within many organisations, but application vulnerabilities remain a key vector for exploits. IDC expects an increased emphasis on AppSec in the next 12 months, and we would expect the low number of 38% to increase.

FIGURE 4

Using Detection Technologies Within Threat Intelligence

Q. Do you correlate any detection technologies information within a threat intelligence platform?



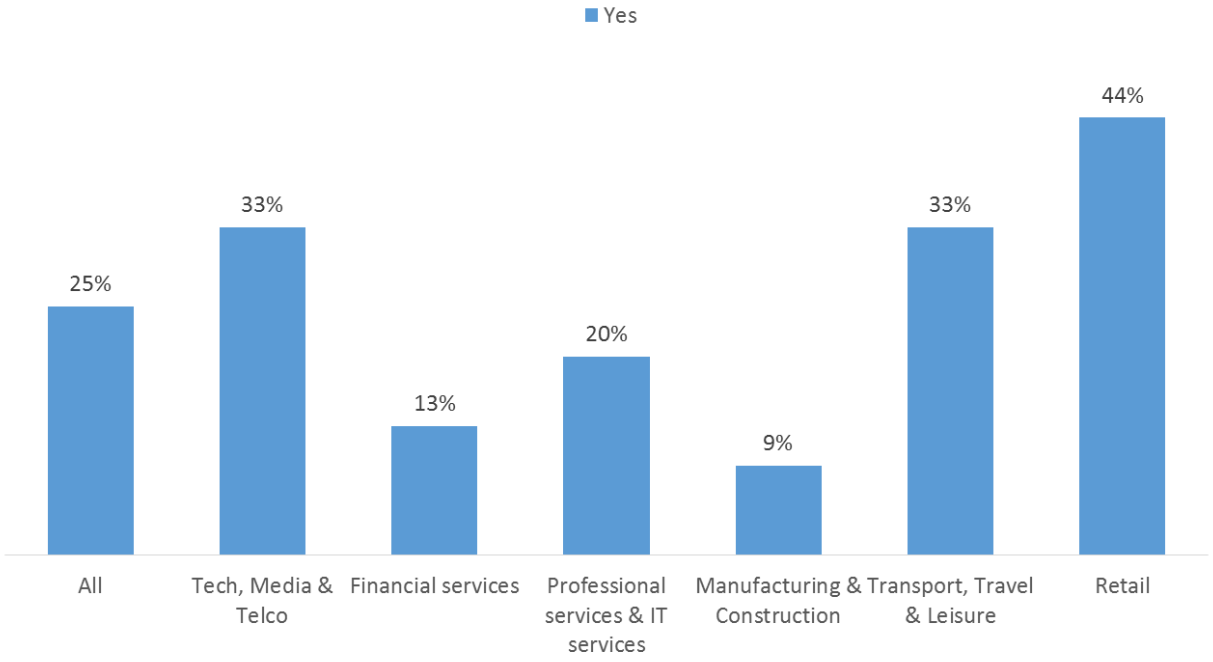
Source: IDC, 2015

But our survey shows that they are much less likely to integrate and correlate data from other systems, such as physical security. Only one-quarter of firms correlates such data, the most prevalent source being door entry controls and surveillance systems. Similarly, only 34% of firms correlate external data such as threats or attacks on peer companies into the threat intelligence platform. Of those that do use external sources, the most common type is open source (52%), followed by industry peers (41%) and government sources (28%).

FIGURE 5

Combining Physical Security Data With Threat Intelligence

Q. Do you correlate any non-IT data, such as physical security data, into your threat intelligence platform?



Source: IDC, 2015

Importantly, although a minority of firms correlate all security-related data, 97% would do so if they were able. This points to a perception among the majority of the respondents that they are unaware that holistic correlation is possible or affordably realistic.

Where Threat Intelligence is Heading

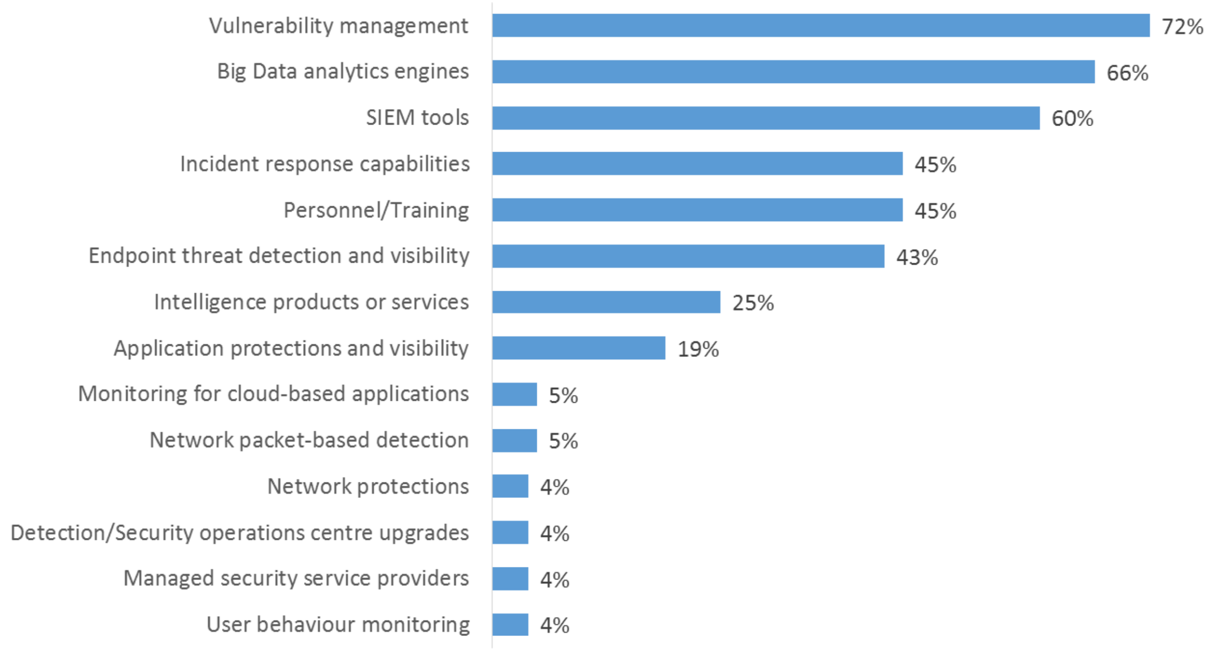
So the current situation seems to suggest that CISOs are only focusing on security information that is immediately related to their security estate: they are not considering the wider context in which their business operates, either from a physical security and application security perspective or from a broader industry viewpoint. Does this mean that CISOs are myopic when it comes to threat intelligence?

In fact, our research uncovers a good deal of intent to expand their understanding and assessment of internal vulnerability and risk dimensions for their organisations. The top three answers when questioned on threat intelligence investment priorities are vulnerability management (72%), Big Data analytics engines (66%) and security information management (SIEM) tools (60%). We think that companies are recognising the difficulty in understand outputs from security systems, and having to continuously adapt the environment. This is tough, and so companies plan to invest in this technology soon. It's more an issue of maturity than myopia.

FIGURE 6

Threat Intelligence Investment Plans

Q. Where do you plan to invest in relation to threat intelligence?



Source: IDC, 2015

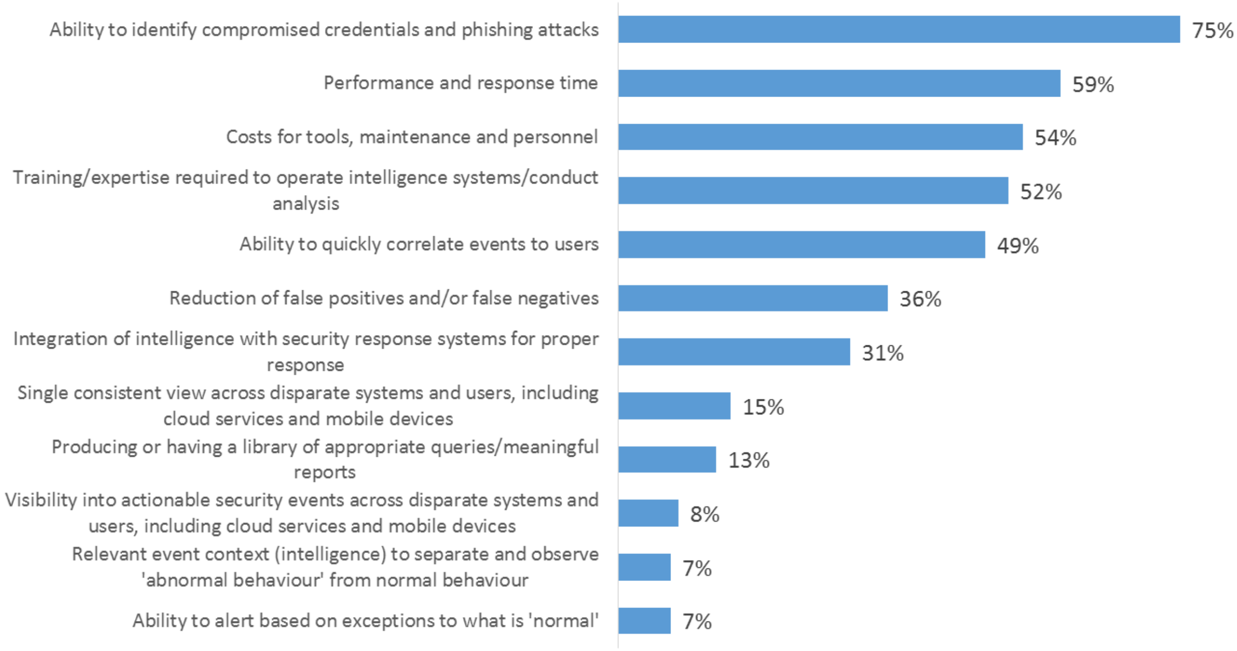
Security's Biggest Challenges in Using Threat Intelligence

Performance, skills & education, and costs are the biggest challenges faced by security executives today. The ability to identify compromised credentials and phishing attacks tops the list of challenges (75%), relating directly to a demand for better user education in password management (or alternatives to passwords) and in detecting phishing. Credential theft is still the number one threat attack area experienced by organisations today. This issue is followed by performance and response time (59%), training and expertise (52%) and costs for tools, maintenance and personal (54%).

FIGURE 7

Challenges

Q. What are your biggest challenges today in utilising threat intelligence?



Source: IDC, 2015

Behind these well-established challenges come more analytics-based issues. The ability to correlate events (49%) and to reduce false positives and/or negatives (36%) are surprisingly high in our survey, showing the importance of speed of analysis of events occurring within security operations, while improving the accuracy of that analysis.

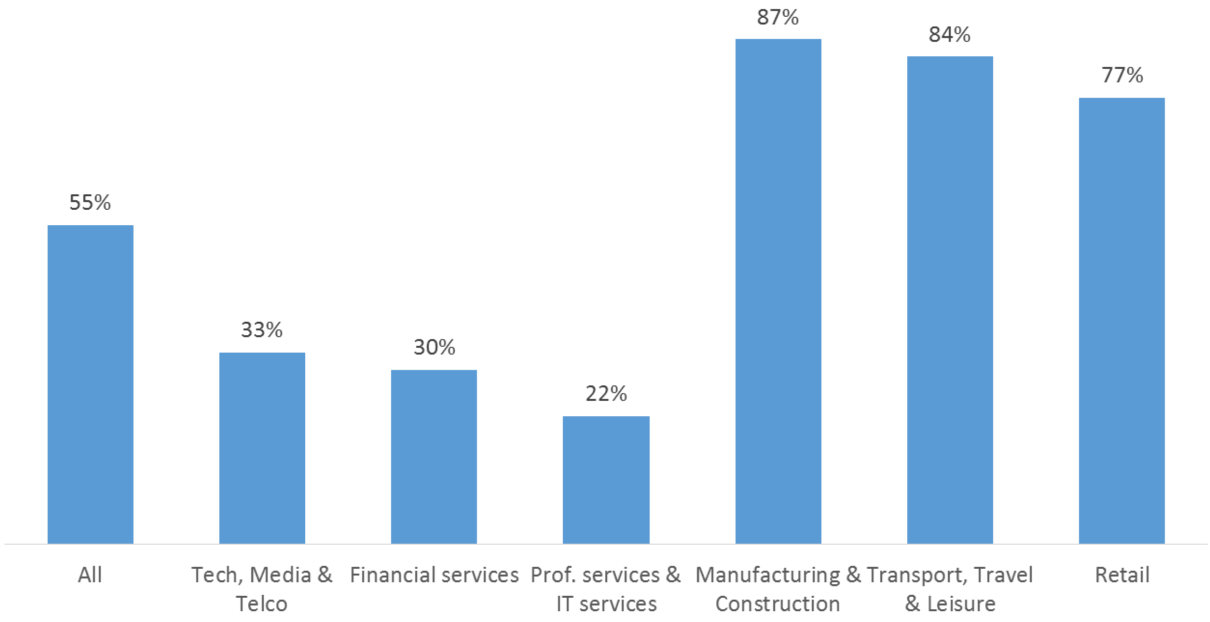
Firms Outsource for Better Performance

Over half of our sample (55%) outsource some or all of their security operations to a third party. The most common reason for doing this is to achieve better visibility, monitoring, and control of security (35%). Firms also seek better or earlier threat detection (21%), and vulnerability management (15%). Importantly, lower cost is a driver for just 4% of all respondents.

FIGURE 8

Managed Security Services

Q. *Do you use managed security services, or outsource some part of your security operations to a third party?*



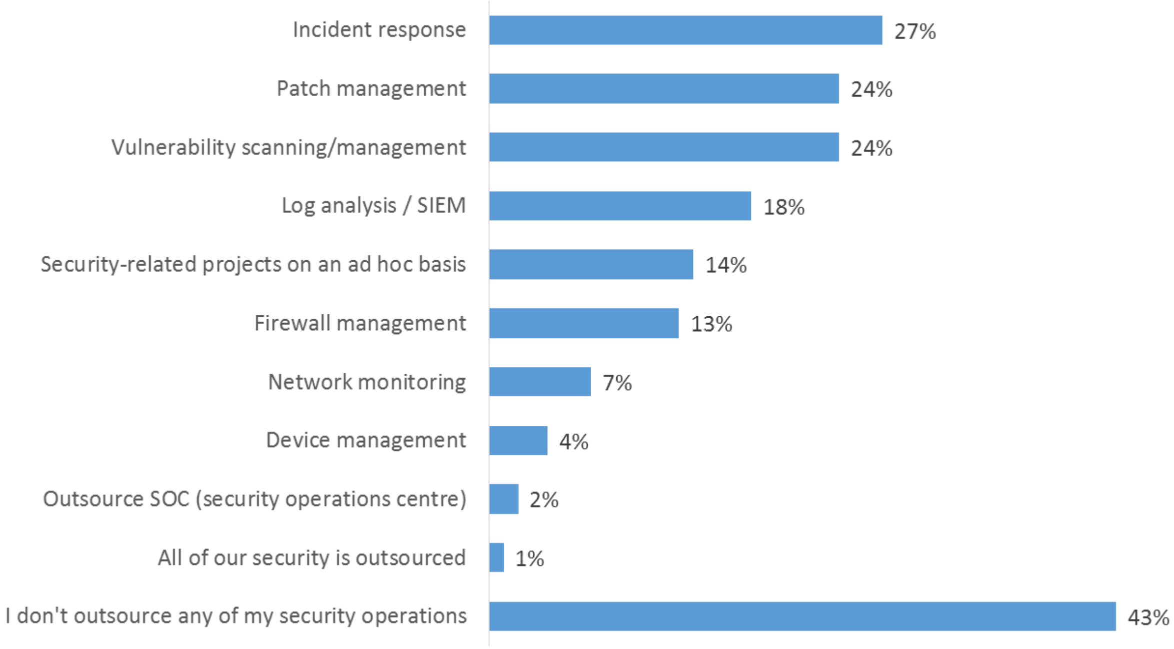
Source: IDC, 2015

Firms use outsourcing for a variety of functions, most commonly incident response (27%), vulnerability scanning/management (24%), patch management (24%), log analysis (18%), and firewall management (13%). Ad-hoc security-related projects are also commissioned (14%).

FIGURE 9

Outsourced Security Operations

Q. Which parts of your security operations do you outsource to a third party?



Source: IDC, 2015

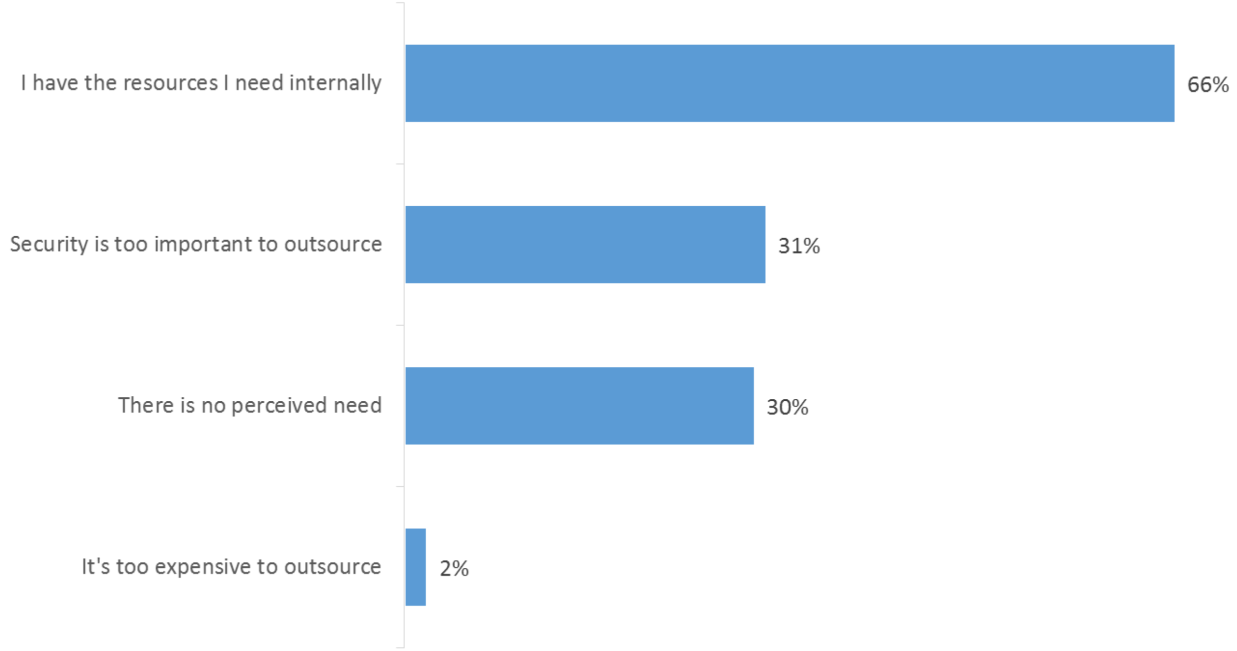
The biggest impediment to using external third parties to deliver security is that companies have the resources required and there is no perceived need. Around one-third (31%) believe that security is too important to outsource. Again, cost is not a factor: only 2% of respondents think that outsourcing is too expensive.

From an industry perspective, financial services is the outlier that believes that security is too important to outsource (82% versus 31% for the whole survey). 100% of the manufacturers that do not outsource do not perceive a need (n=7).

FIGURE 10

Not Using Managed Services

Q. Why do you not use managed security services?



Source: IDC, 2015

FUTURE OUTLOOK

Threat intelligence is one of the most commonly-discussed topics in the domain of security, but like all trends it is prone to overuse. Our study shows that enterprises have very specific requirements for threat intelligence that exceed the rhetoric commonly seen in the market.

Threat intelligence is not simply information. It is a service delivering a collated and correlated range of data feeds and sources to provide actionable advice to security operations. Importantly, it draws information from across the enterprise, both within security operations infrastructure and more broadly across the organisation. Getting this holistic view of security beyond IT is critical to understanding the full context of threat information.

CISOs are faced with major security challenges these days. The number and type of threats is expanding rapidly, and they are under pressure to secure their organisations while enabling other business initiatives such as digital transformation. Responding quickly to attacks, and identifying breaches quickly, is core to optimising security operations. Some organisations remain reluctant to adopt a services-led approach to threat intelligence, and those firms are missing out on the provision of deep insight into their security operations, as well as improved security performance.

CHALLENGES/OPPORTUNITIES

Implementing threat intelligence services is not easy. The range of data feeds, both within an organisation and externally, can be vast, and security operations often risk being overwhelmed with data from events and alerts; digesting threat information can be a slow and painful process. Most organisations also lack contextual awareness (though they rate it as important). Continuously monitoring context, as it changes over time, requires a level of automation that is rare in enterprises.

Among the numerous pressures for time and the inevitable reactivity to incidents, security operations managers must fit in the consumption of threat intelligence. Often, it does not seem an immediate priority.

Yet properly implemented and holistic threat intelligence that which spans an organisation's entire context can save time and money, while improving overall security operations performance. Taking time to focus on threat intelligence will pay long-term dividends.

CONCLUSION

Enterprises should adopt an organisation-wide, holistic approach to threat intelligence. Context is key, and must range beyond traditional security operations to include an organisation's physical infrastructure, as well as threat information from peers, governments and other sources.

Threat intelligence is best delivered, and consumed, as a service. Most organisations do not have the in-house skills to implement and operate threat intelligence to its maximum effectiveness.

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-insights-community.com
www.idc.com

Copyright Notice