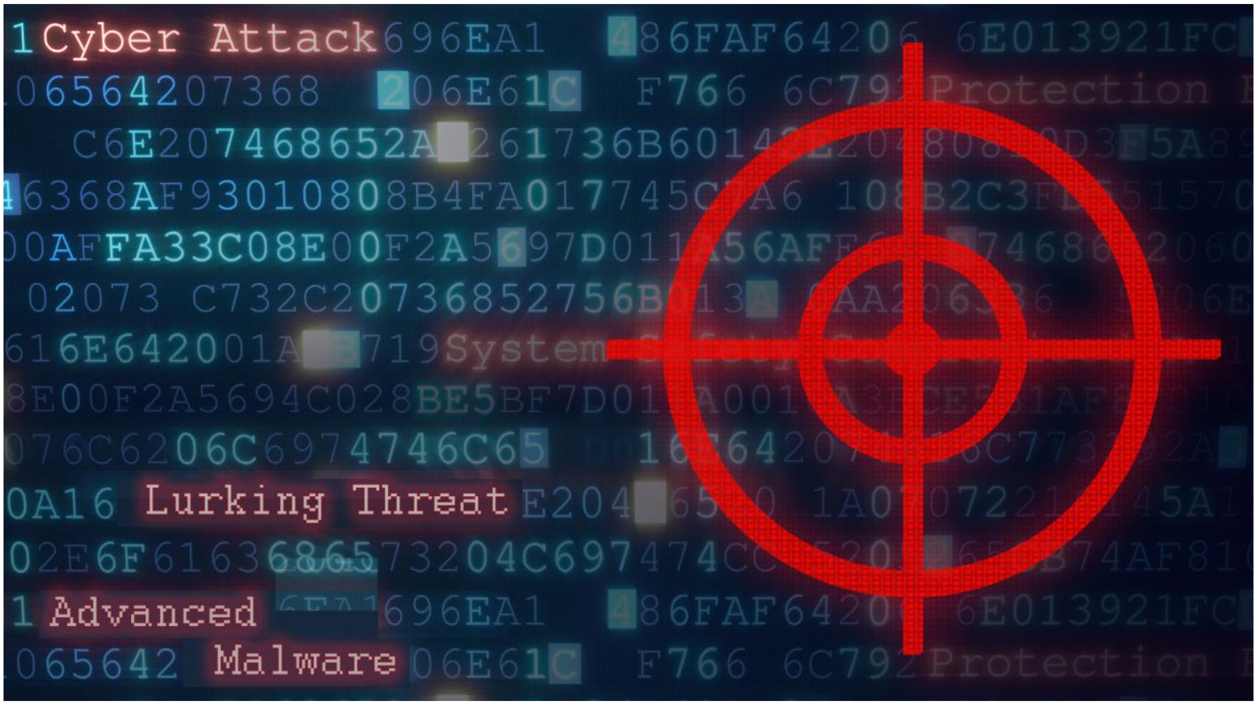


Don’t Wait:
The Evolution of Proactive Threat Hunting

Executive Summary

Sponsored by Raytheon

Independently conducted by Ponemon Institute LLC

Publication Date: June 2016

Connect with us: #DontWaitHunt

Don’t Wait: The Evolution of Proactive Threat Hunting

Ponemon Institute, June 2016

Part 1. Executive Summary

The purpose of “Don’t Wait: The Evolution of Proactive Threat Hunting” survey, sponsored by Raytheon, is to examine how organizations are deploying managed security services to strengthen their security posture. The research also looks at the critical success factors, barriers and challenges to having a successful relationship with managed security services providers.

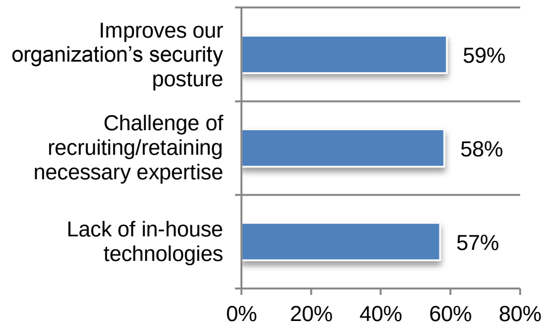
We surveyed 1,784 chief information security officers and other senior IT security leaders in North America, Europe, Middle East and Asia Pacific[1] who are familiar with their organizations’ managed security service practices. Managed security services providers (MSSPs) are engaged by organizations to manage and strengthen its IT environment’s security by providing services including security information and event management (SIEM), network security management (NSM), endpoint detection and response (EDR), incident response, forensics and more.

Security tools such as anti-virus, firewalls, intrusion detection and sandbox technologies, are built upon the assumption that attackers adhere to a known set of tools and tactics. Today, while a majority of MSSPs focus on these traditional, reactive tools, some provide more advanced, proactive services. Proactive threat hunting services can effectively find sophisticated and damaging threats, including previously undetected attacks, and stop them before businesses suffer damage.

In this study, 56 percent of respondents use an MSSP and 22 percent say they plan to engage an MSSP in the future. The Key Findings section of the full version of this report provides analysis of the 56 percent who are engaged with a provider. In many cases, it is a serious security incident such as a data breach that motivates companies to engage an MSSP to strengthen their security posture.

A key takeaway is that organizations using MSSPs understand the primary benefits of leveraging external expertise. Eighty percent view MSS as essential, very important or important to their overall IT security strategy. Figure 1 shows the primary reasons to have an MSSP is to improve security posture (59 percent). This is followed closely by the need to reduce the challenge of recruiting and retaining necessary talent (58 percent) and the lack of in-house security technologies (57 percent).

Figure 1. Main reasons organizations use MSSPs



The following are the seven most salient research findings.

1. MSSPs help companies achieve a stronger security posture. With evolving cyber threats, organizations face the critical challenge of lack of expertise, personnel and resources. MSSPs are seen as filling these gaps to improve their security.

[1] The countries represented in these regions are: United States, Canada, United Kingdom, Denmark, France, Germany, Netherlands, Brunei, Kuwait, Saudi Arabia, Oman, Qatar, UAE, India, Australia, Japan, Singapore and South Korea.

Many organizations worldwide still typically wait until after a breach before the money is allocated to engage an MSSP. Two-thirds of organizations not currently using an MSSP say that the top trigger would be a significant data loss resulting from an IT security incident.
A breach would confirm that the organization's risk of compromise is high, so it becomes a priority.

2. A shift from reactive services to proactive services offered by providers and demanded by organizations is occurring but still in early stages. The lack of proactive threat hunting services could be contributing to the daily barrage of media headlines about data breaches in organizations worldwide. It highlights a need for organizations to be doing more to protect their networks from the most insidious threats. Currently, MSSPs offer cybersecurity assessment (39 percent), integration services (31 percent) and digital forensics and incident response (DFIR) engineering and/or assessment (28 percent). Only 16 percent say their MSS offers proactive threat hunting to find advanced threats based on behaviors and anomalies.

3. Interoperability with security intelligence tools such as SIEM is essential or very important. When asked what characteristics of MSSPs are essential or very important, the number one feature is high interoperability with the company's security intelligence tools such as SIEM (73 percent). Also critical are speedy deployment (65 percent), round-the-clock threat monitoring and management (63 percent), a tried and tested service offering (62 percent) and scalability of services (61 percent). Not as critical are compliance with data protection requirements (52 percent) or indemnification for service failures (36 percent).

Whether organizations use MSSPs or not, interoperability/integration between MSSP and customer is top priority. Those currently not using one say it is difficult to find MSSPs that would support or integrate with our systems and requirements. Fifty-three percent list difficulty finding vendors strong in interoperability as the reason they choose not to outsource.

4. MSSPs provide insights about security events and a better understanding of the external threat environment. Sixty-five percent of respondents believe their MSSP leverages insight gained from monitoring a large number of security events from a global customer base and 53 percent say the MSSP helps to better understand the external threat environment through the collection and analysis of information on attackers, methods and motives. More than half (51 percent) say it effectively mitigates the risks after they are identified.

5. MSSPs have identified existing software vulnerabilities that are more than three months old. Fifty-four percent of respondents say their MSSPs identified exploits of existing software vulnerabilities greater than three months old, and 45 percent say exploits of existing software vulnerabilities less than three months old have been discovered. They also revealed Web-borne malware attacks (51 percent). New threats are often going undetected because typical providers are not actively identifying new threats but importing threats identified by industry into their toolsets.

6. Responsibility for relationships with MSSPs is shifting. Fifty-nine percent say responsibility for the MSSP is shifting from IT to the lines of business. Today, however, the IT (43 percent) or IT security professional (15 percent) owns their organizations' relationships with MSSPs. This represents a trend that MSS services are not considered a commodity but a **strategic element and competitive advantage** companies can foster. One reason for this shift is in many organizations the CEO and board of directors now have a responsibility to the shareholders to ensure that companies are protected.

7. A lack of visibility into the outsourcer's IT security infrastructure is a barrier to successful outsourcing of security services. Fifty-one percent say a lack of visibility into the outsourcer's IT security infrastructure is the main hindrance to a successful approach to outsourcing. Other barriers are inconsistency with the organization's culture (49 percent) and turf or silo issues between the organization's IT security operations team and the outsourcer (46 percent).

Even though the lion's share of information security leaders agree that MSS is an important part of their overall cybersecurity strategy, most of those are still focusing on basic commodities and ignoring proactive approaches such as threat hunting. Outsourcing to providers with highly trained experts will become a necessity as organizations mature their IT infrastructure and the MSSP partners improve technologies and approaches. The old adage of building higher walls has proven insufficient in the face of cyber threats that are more complex and sophisticated. The current, most-effective security concept is detect, isolate and eradicate through an in-house team, a managed security service provider, or a hybrid solution that includes both.

Part 2. Conclusion

The old cybersecurity concept of defend, detect and respond is insufficient in the face of today's sophisticated threats. The current, most-effective security concept is detect, isolate and eradicate through an in-house team or with a managed security service provider. Proactive threat hunting becomes a "must" for organizations as cyberthreats from cyber criminals, nation states and other malicious actors become more difficult to detect and deflect.

The shift from reactive services to proactive service is occurring today. Even though the lion's share of information security leaders agree that MSS is an important part of their overall cybersecurity strategy, most of those are still focusing on commodity prevention-based services and ignoring proactive security. Organizations need to reverse their strategies if they are to remain competitive in today's global economy.

The concern for many companies is whether an MSSP will work seamlessly with their current systems and whether their data will be safe. The strongest MSSP is solution agnostic, allowing the data to stay with the client, providing actionable reports, building historical perspectives, and proactively hunting for problems.

Insufficient personnel and lack of in-house experts are the top challenges to a robust security posture. Organizations lacking adequate numbers of elite cyber professionals or staffs with the skills the company needs can turn to managed security service providers. As the cost of these employees increases, it will become more challenging to retain talent. A model is needed that supports this and grows staff as needed. Savvy organizations choose vendors able to offer proactive threat hunting that scales with this growth.

To meet organizational challenges of keeping up with the latest technologies, accessing elite talent and staying ahead of emerging cyberthreats, a strong managed security service provider can serve as a trusted partner focused on meeting each customer's unique needs. Savvy information security leaders don't wait until their organization has become a victim.

Part 3. Recommendations

Information security leaders worldwide in all organization sizes and industries can take steps to understand how proactive threat hunting and traditional managed security services can help them achieve organizational objectives and reduce risk.

- Identify the organization's specific needs and requirements and what can and should be done in-house or by outsourcing
- Evaluate information security staff skill sets and team size
- Consider the value added by commodity services against proactive threat hunting to find and mitigate the sophisticated and damaging threats in today's rapidly evolving landscape
- Evaluate the current vendor, if any, based on the following criteria:
    - Ability to do proactive hunting of malware and other advanced threats

- Willingness to work with any new or existing technologies (product agnostic)
  - Ability to scale services with the growth of the organization
- Ensure a new or current vendor can advise on the best solutions that fulfill their needs and requirements

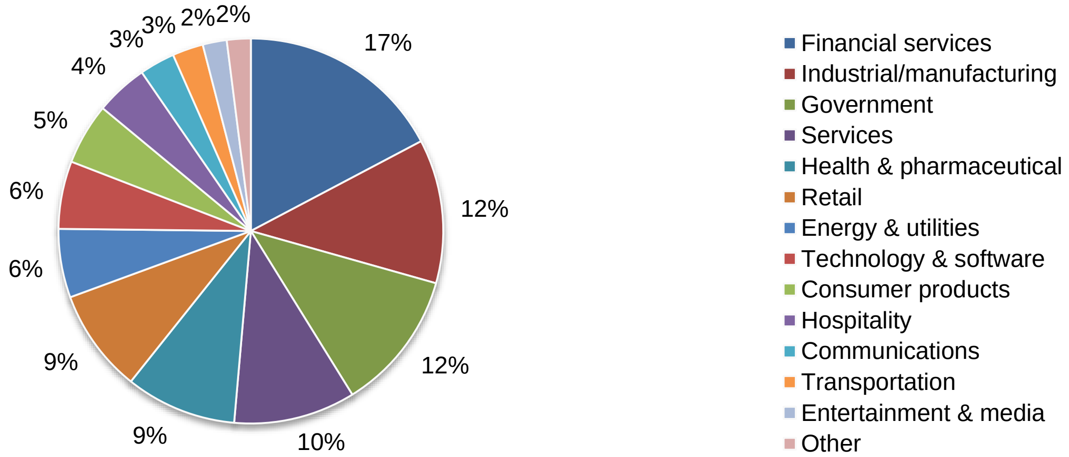
Part 4. Methods

A sampling frame of 51,712 IT security practitioners in North America, Europe, Middle East and Asia Pacific were selected to participate in this survey. To ensure reliability, the selected participants are familiar with their organizations' managed security services. Table 2 shows 1,967 total returns. Screening and reliability checks required the removal of 183 surveys. Our final sample consisted of 1,784 surveys or a 3.4 percent response.

Table 2. Sample response	Freq	Pct%
Sampling frame	51,712	100.0%
Total returns	1,967	3.8%
Rejected or screened surveys	183	0.4%
Final sample	1,784	3.4%

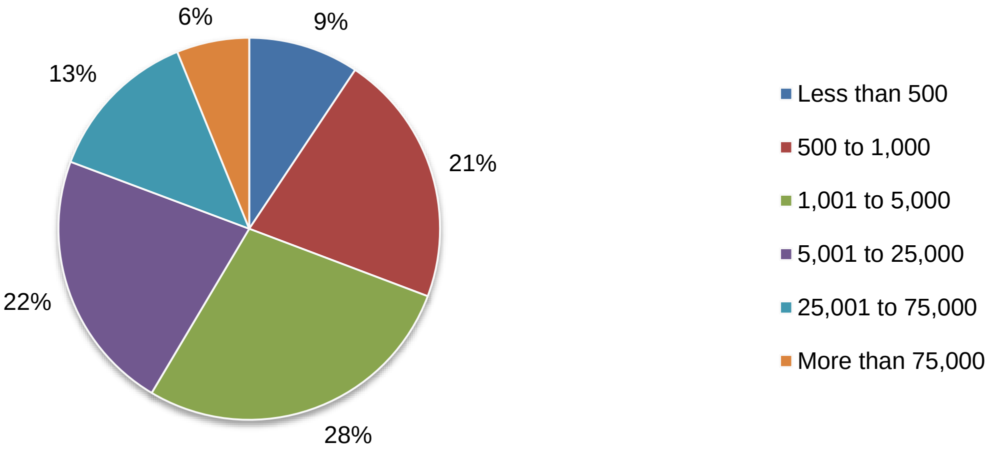
Pie Chart 1 reports the industry classification of respondents' organizations. This chart identifies financial services (17 percent) as the largest segment, followed by industrial/manufacturing (12 percent) and government sector (12 percent).

Pie Chart 1. Primary industry focus



Pie Chart 2 shows 70 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 2. Global employee headcount



Part 6. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of IT security practitioners who are familiar with their organizations' managed security services. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

This document does not contain technology or technical data controlled under either the U.S. International Traffic in Arms Regulations or the U.S. Export Administration Regulations.
Cleared for public release. Ref# E16-6SP5