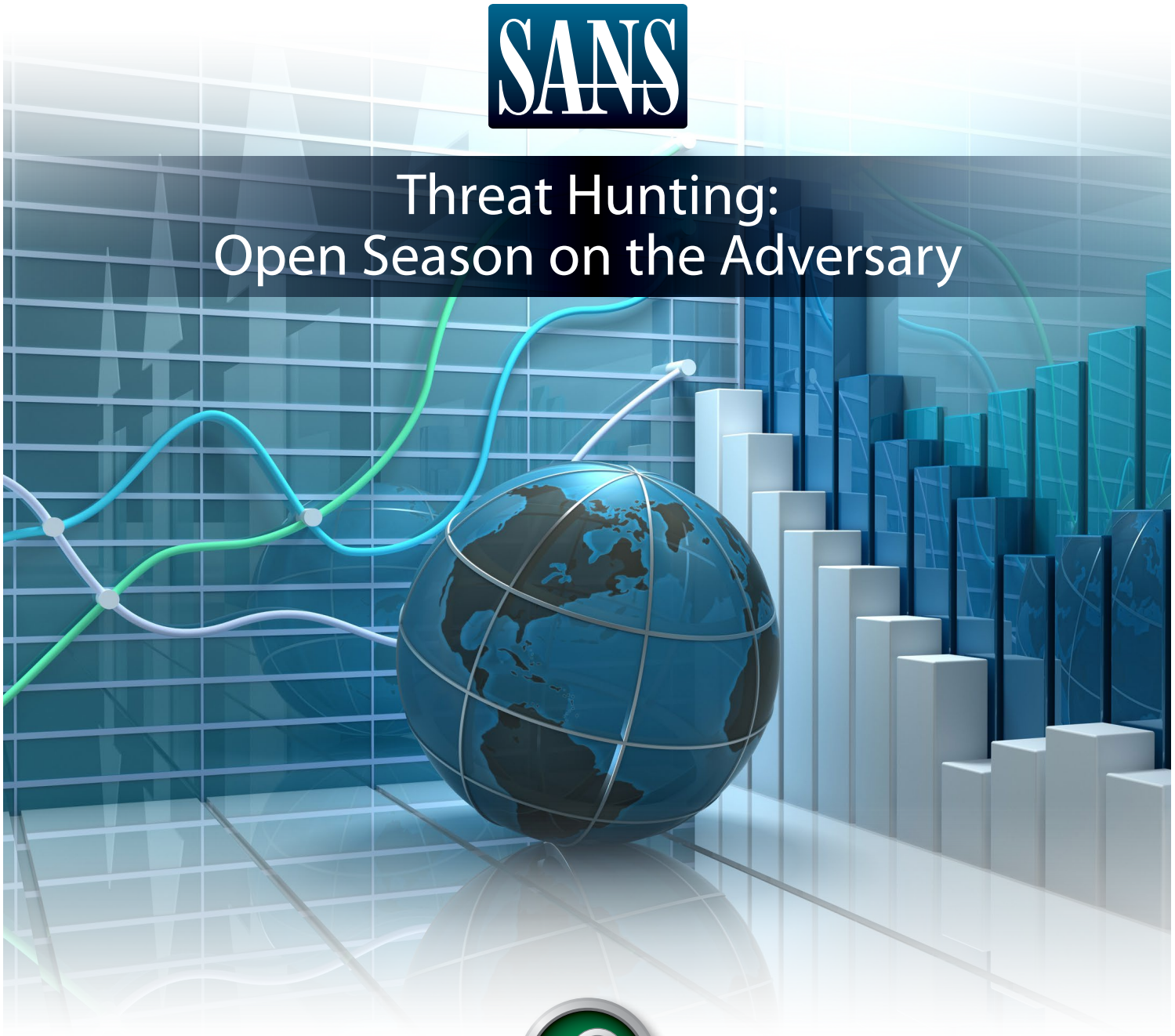

Threat Hunting: Open Season on the Adversary

A SANS Survey

Written by Dr. Eric Cole

April 2016

Sponsored by
Malwarebytes

Executive Summary

Threat Hunting

Threat hunting is the act of aggressively tracking and eliminating cyber adversaries from your network as early as possible.

In 2016, three absolute facts are relevant when it comes to security: 1) an organization cannot prevent all attacks; 2) an organization's network is going to be compromised; and 3) 100% security does not exist. This means that adversaries will breach your organization's protection—if they haven't already. The goal of security, then, is not just about stopping adversaries, but also about controlling and minimizing the overall damage from an incursion. The main method for finding adversaries already in our networks is threat hunting—an area on which security personnel are increasingly focusing their attention.

Benefits of Threat Hunting

say threat hunting found previously undetected threats on their enterprise

of those implementing threat hunting have reduced attack surfaces

enhanced speed and accuracy of response by using threat hunting

Responses from 494 participants to the first SANS survey on threat hunting reveal that nearly 86% of organizations are involved in threat hunting today, albeit informally, as more than 40% do not have a formal threat-hunting program in place. Results indicate 86% of respondents believe anomalies are the biggest trigger driving threat hunting, as opposed to 41% who hunted based on hypotheses, while 51% of respondents say hunts are also triggered by third-party sources, including threat intelligence.

Responses indicate that organizations are still figuring out exactly what a threat-hunting program should look like, how to attract the right skills and how to automate their processes. Currently, respondent organizations rely heavily on known indicators of compromise (IOCs), manual analysis, utilizing existing tools and augmenting them with customizable tools to perform threat hunting. They need to get to the point where they have the skills and capability to launch hunts automatically and on a regular basis, without waiting first to see an IOC.

Shortcomings with Current Programs

say their hunting is not invisible to the adversary

say their threat-hunting programs need to be improved

are dissatisfied with how long it takes them to hunt for threats

To build a mature threat-hunting program, adopt the following goals:

- To provide early and accurate detection
- To control and reduce impact and damage with faster response
- To improve defenses to make successful attacks increasingly difficult
- To gain better visibility into the organization's weaknesses

Overall, many organizations are experiencing enough benefits from threat hunting to make more of an investment in it. For example, 52% of respondents say they measured reduced risk as a result of hunting. Unfortunately, the rest are unsure or don't know, highlighting the need for more formalized programs.

These and other results, along with advice and best practices for threat hunting, are provided in the following report.

For organizations that are performing threat hunting, less than 3% follow any formal, published, external methodology, as illustrated in Figure 1.

Does your organization perform threat hunting?

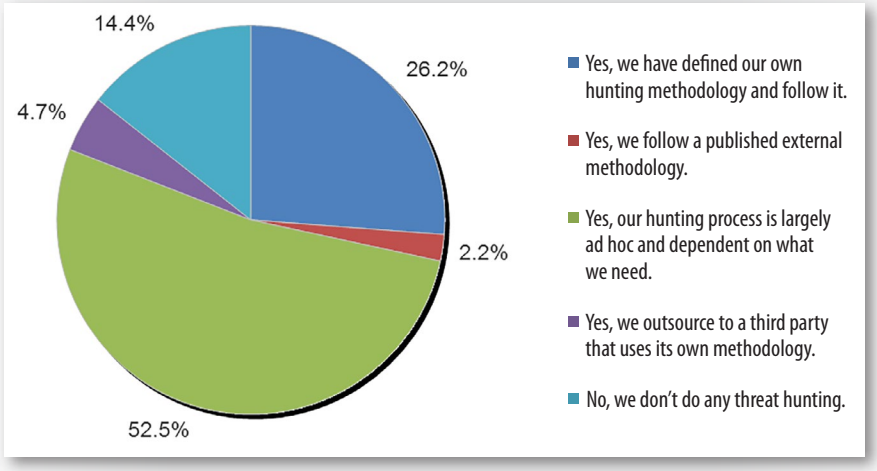

Figure 1. More than half of all hunting is based on ad hoc processes.

A significant portion of threat hunting (53%) being performed is still ad hoc, which means there is not a repeatable process, and organizations are wasting resources trying unverified methods that provide minimal value. The problem with letting need drive threat-hunting capabilities is that it is a very reactive approach. Instead of proactively looking for the adversary using known methods, those using ad hoc processes are responding to what they see in their environment.

While many technical folks recognize the value of threat hunting, their organizations are still reluctant to build out a formal threat-hunting program, as shown in Figure 2.

Does your organization have a formal threat-hunting program with assigned staff?

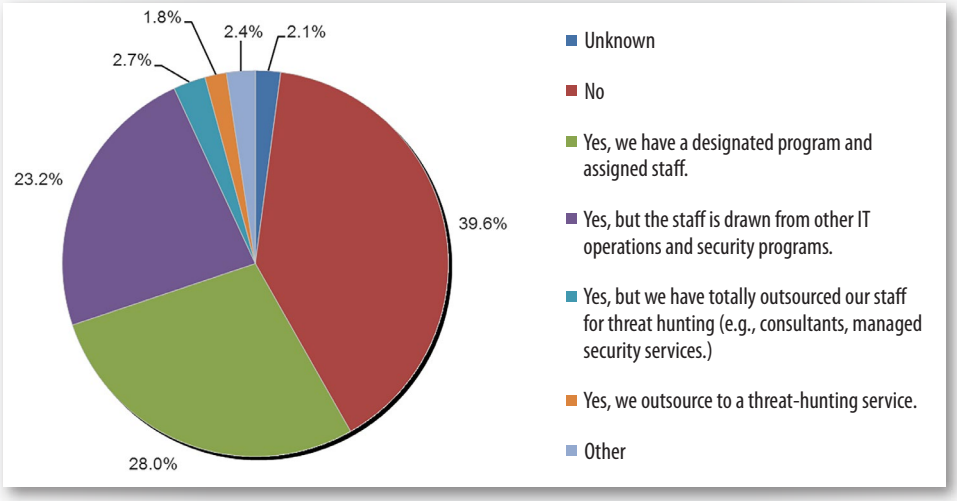

Figure 2. Many organizations do not have a dedicated program for threat hunting.

The first part of a successful hunting program is having a formal process built on a well-defined methodology. The second part is continuously performing threat hunting. The more frequently an organization hunts for threats, the timelier the detection of the adversary is likely to be and the less damage there may be to an organization. See Figure 3.

Ideally, threat hunting must be done on a continuous basis utilizing automated tools, with manual expertise alerted when anomalies are detected. The adversary never sleeps and neither can your threat-hunting capabilities.

How often does your organization perform threat hunting?

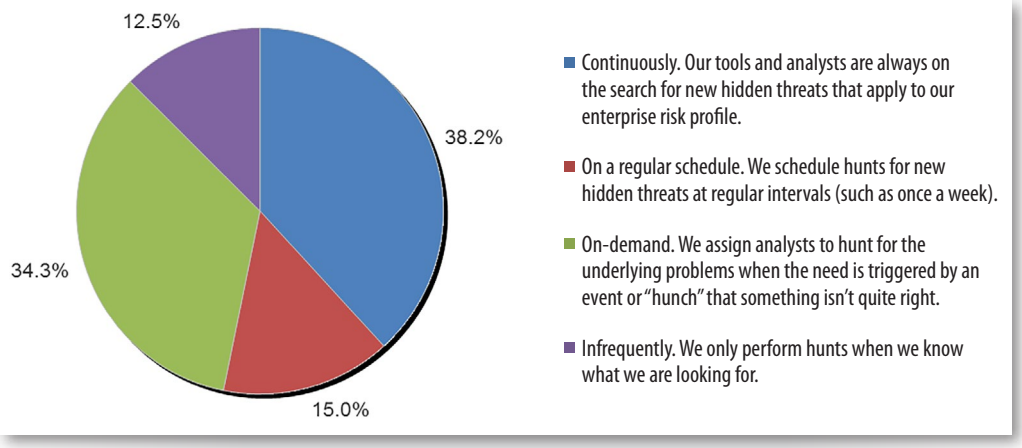

Figure 3. Continuous threat hunting is ideal.

Ideally, threat hunting must be done on a continuous basis utilizing automated tools, with manual expertise alerted when anomalies are detected. The adversary never sleeps and neither can your threat-hunting capabilities.

Moving to the Next Level

To take threat hunting to the next level, organizations should adopt these key strategies:

- Build threat hunting on a solid and realistic understanding of how the adversary works and operates.
- Start with published IOCs with the goal of moving toward detecting advanced attacks via anomalies and correlation of behavior.
- Adapt and adjust to the unique needs of your organization.
- Investigate, understand and re-utilize useful threat data discovered during hunts.
- Create metrics, such as dwell time, to track overall progress and maturity of the hunting efforts.

Who's Hunting

While the participants in this survey came from a wide range of organizations of varying sizes, the largest group (22%) represents companies from 1,001 to 5,000 employees and contractors. Remaining respondents are fairly evenly divided, with 20% from companies with more than 50,000 employees, 18% from companies of 100 to 1,000 employees, 17% from companies between 10,001 to 50,000 employees, and 12% from companies with 5,001 to 10,000 employees and contractors.

The financial services sector represented 22% of the survey base, followed by government, high tech and education. Financial organizations have very high-valued targets and tend to be advanced with the security solutions they deploy. Threat hunting is likely an area they are exploring as a means of improving their overall security posture. See Figure 4.

What is your organization's primary industry?

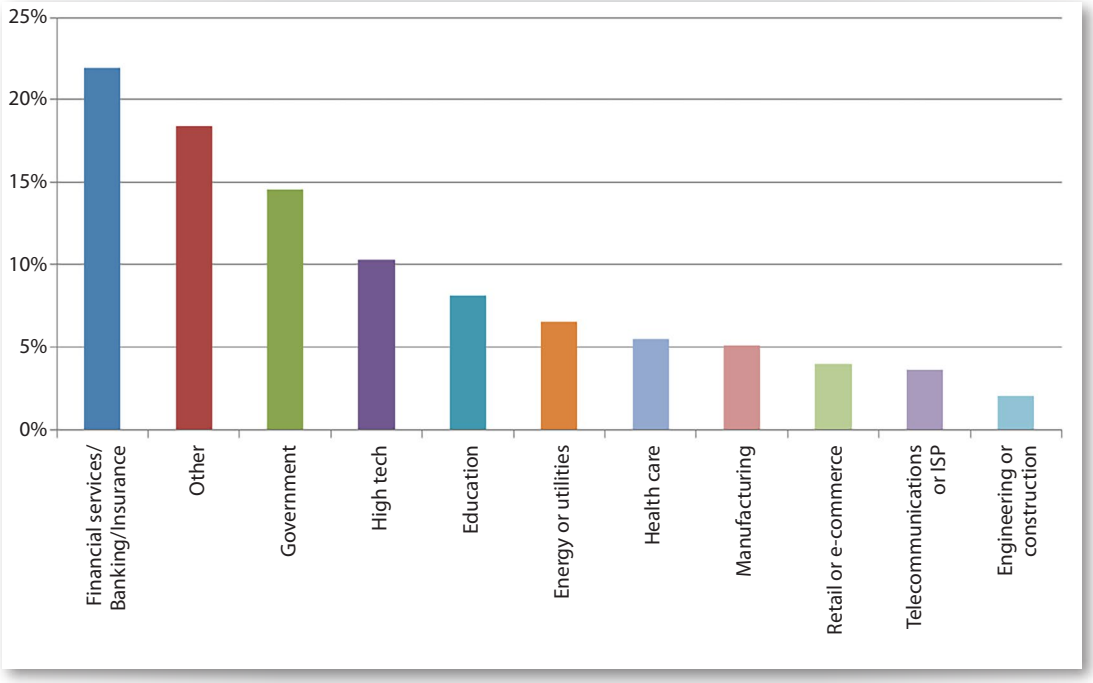

Figure 4. Participants' Primary Industries

The "Other" category is filled with many cross-over titles, particularly consulting services in areas of cyber security, defense contracting, software testing, and storage.

The primary positions of people who replied to the survey were security analysts (29%), security managers or directors (15%), and incident responders (13%)—roles that make up a large portion of the SANS community.

Staffing and Skills

For any security program to be successful, it must be an integration of people, processes and technology. Typically, organizations invest in technology first, and when it fails, they invest in formal processes and appropriate personnel for managing the process. With threat hunting, technology is the primary focus, but what is surprising (and very good news) is that people are also a priority.

To have an effective hunting program, organizations need trained staff who can configure, manage and interpret the results of the technology. It is no surprise that organizations are investing not only in technology, but also in people and training. See Figure 5.

What do you spend your threat hunting resources on?
Rank in order, with "First" being the highest spending priority and "Fourth" being the lowest. Indicate those that aren't applicable (N/A).

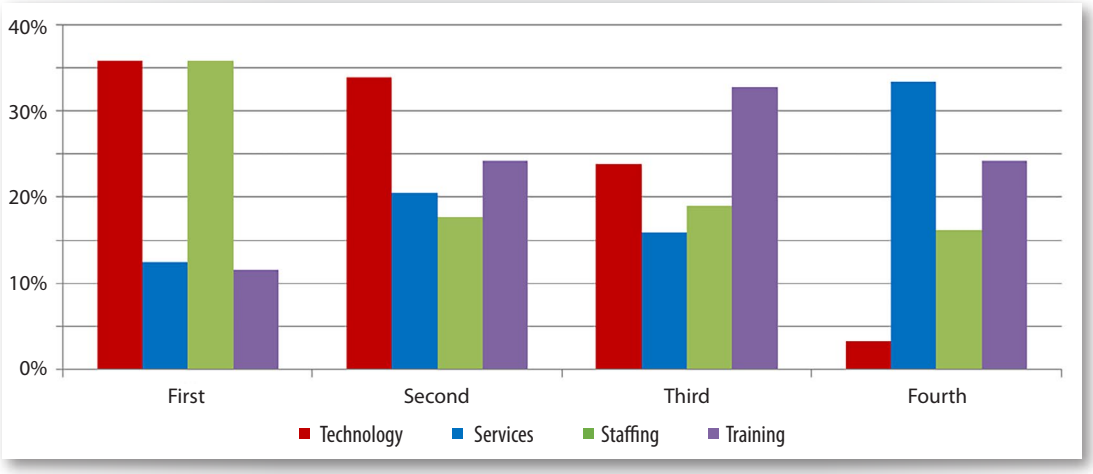

Figure 5. Staffing and Training Investment on Threat Hunting

People who work in hunting do not always have extensive experience, making training a necessity. While it is a natural step for incident responders and those with security operations center (SOC) experience to transition into threat-hunting roles, people with those qualifications are in high demand and often cannot be pulled from their current duties. As a result, traditional security personnel are being retrained in these new skills.

Without appropriate processes and supporting services, people will continue to struggle in implementing a long-term, sustainable solution. It is no surprise that incident handling/response and forensics are the most highly valued skills for hunting, as illustrated in Figure 6, because these jobs often focus on finding pieces of evidence that are hidden on a system or cannot be easily found.

What skills do you value for your threat-hunting operations? *Select all that apply.*

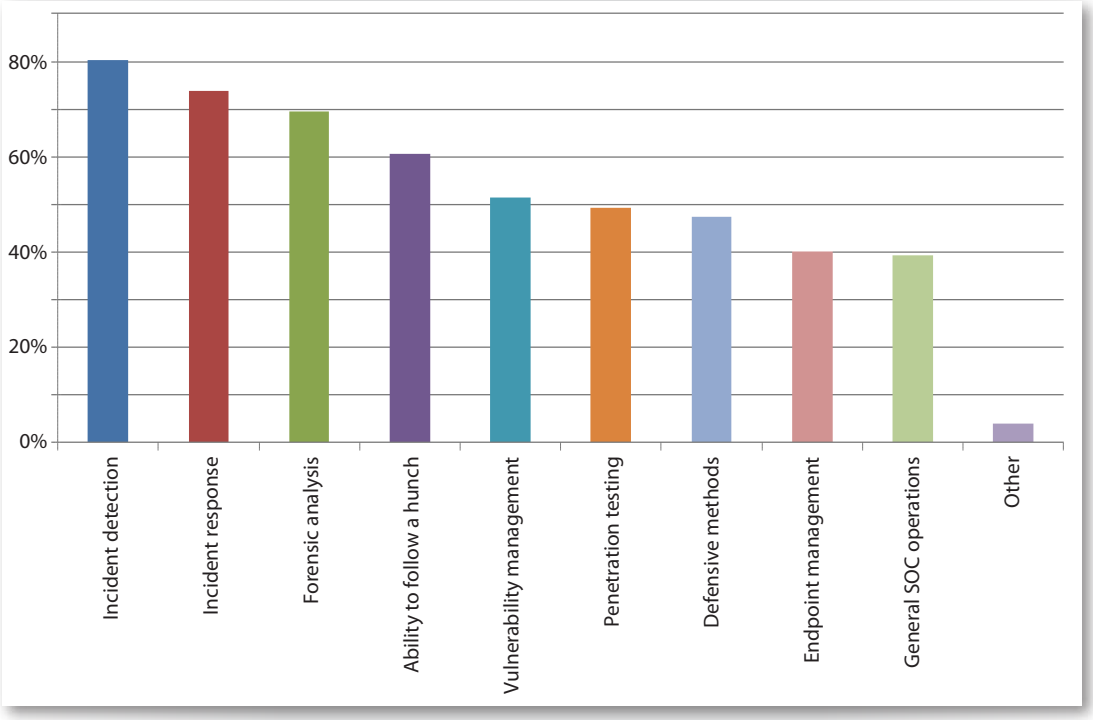

Figure 6. Skills Needed for Hunting

In addition to the technical skills, a threat hunter also needs investigative skills to continue to follow a hunch if something looks suspicious or does not make sense.

Value of Hunting

The trick to a successful hunting program is to have key metrics to show a positive ROI on the hunting efforts. Because your organization is going to be compromised, threat hunting is all about limiting damage and potential exposure of information, so reduced exposure and time to repair should be your key metrics.

Threat hunting plays a critical role in early detection of an adversary, as well as faster removal and repair of vulnerabilities uncovered during the hunt. This fact is not lost on respondents, 52% of whom say their organizations recognize the value in threat hunting, as shown in Figure 7.

Has threat hunting shown value by providing a measurable reduction in risk to your organization?

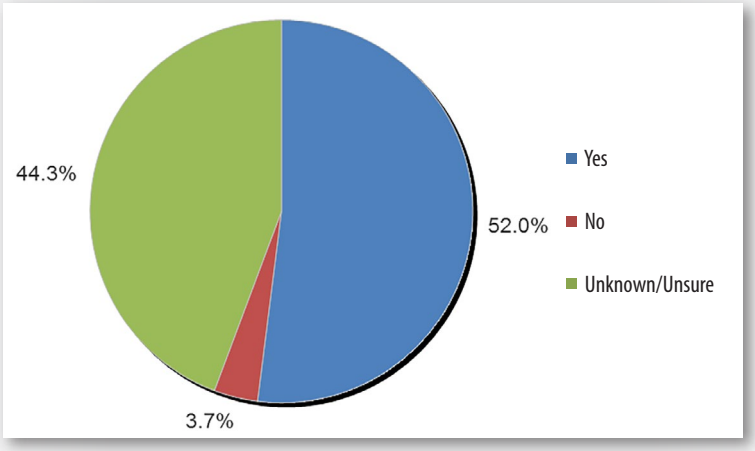

Figure 7. Value of Threat Hunting

Results also show threat hunting is still in its infancy in terms of formal processes and methods. Although more than half of the respondents (52%) have found value in threat hunting in the form of a measurable reduction in risk, 88% of organizations are not satisfied with their current capabilities and feel there is room for improvement; see Figure 8.

Do you still need to improve your threat-hunting tools and capabilities?

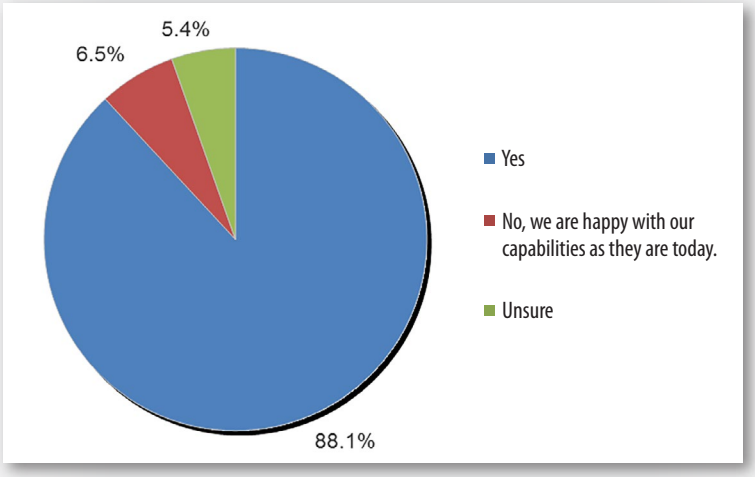

Figure 8. Improvements Needed in Threat-Hunting Capabilities

Overall, threat hunting is recognized as adding value, but organizations need to continue to develop their threat-hunting methodologies.

Reduced Attack Surface

Instead of focusing on traditional methods of prevention (i.e., firewalls) and detection (i.e., IDS), organizations are recognizing the value of using threat hunting to reduce the overall risk to the organization, as illustrated in Figure 9.

Which of the following indicators have shown a measurable reduction in risk that ties to the maturity of your threat-hunt cycle (i.e., preparation, response, follow-up)?
Select all that apply.

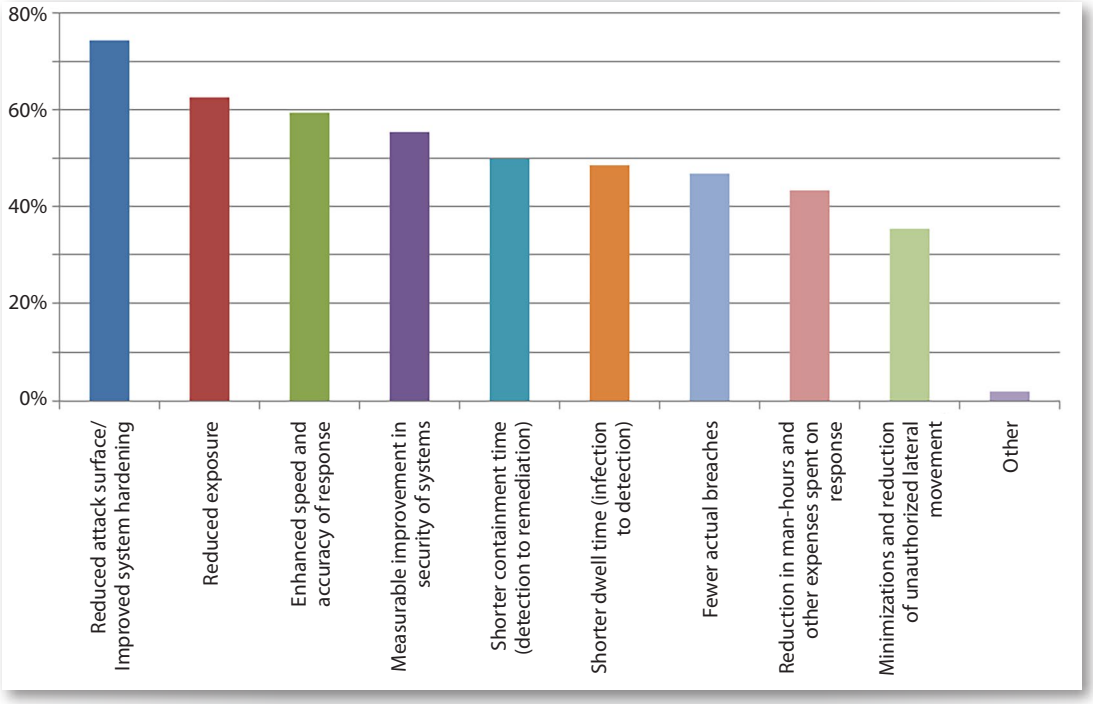

Figure 9. Key Improvement Indicators for Threat Hunting

Many executives do not recognize how big the security problem is within their own organizations. Threat hunting can provide meaningful metrics for them to understand the problem and more clearly see their exposures.

The key indicators that organizations are gaining value from threat hunting focus on reducing the attack surface (74%), reducing exposure (63%) and increasing the speed of containing and controlling damage (59%). These are also very useful metrics you can use to sell threat hunting to your executives and show a positive ROI for their investment in threat hunting.

Response Time

In building a threat-hunting program, three key indicators you should use to track the success of your program are:

- **Dwell time**—how long is the adversary in your organization?
- **Lateral movement**—how much damage is the adversary causing, in terms of how many systems are compromised?
- **Reinfection**—how many times has your organization been compromised by the same adversary or the same threat?

If you are not seeing measurable improvement in these areas, your threat-hunting program needs work.

While threat hunting is becoming a very common term used in security, many organizations (56%) are still trying to figure out how to optimize their hunting process. See Figure 10.

Are you satisfied with how long it takes you to hunt for threats?

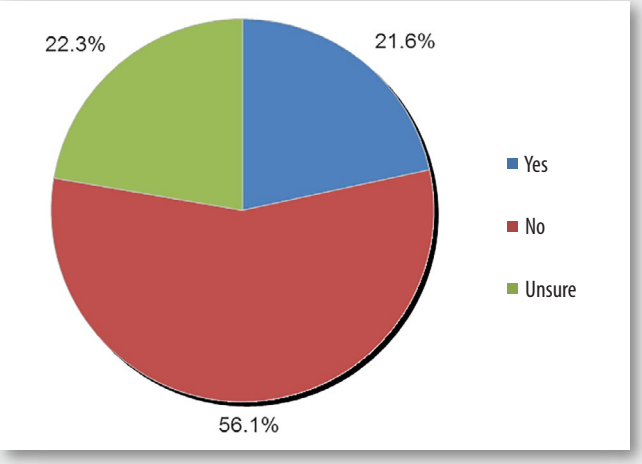

Figure 10. Overall Satisfaction with Hunting Programs

Organizations are starting to catch more adversaries with hunting. However, the amount of damage being caused by those adversaries is still not acceptable and needs to be reduced. A key indicator of overall success and satisfaction with a hunting program is the length in time it takes to detect and stop an adversary. The longer it takes to uncover a serious threat, the less successful the program is. See Figure 11.

On average, how long does it take you to proactively uncover a serious threat from the time you start to pursue it? How long does it take you to respond?

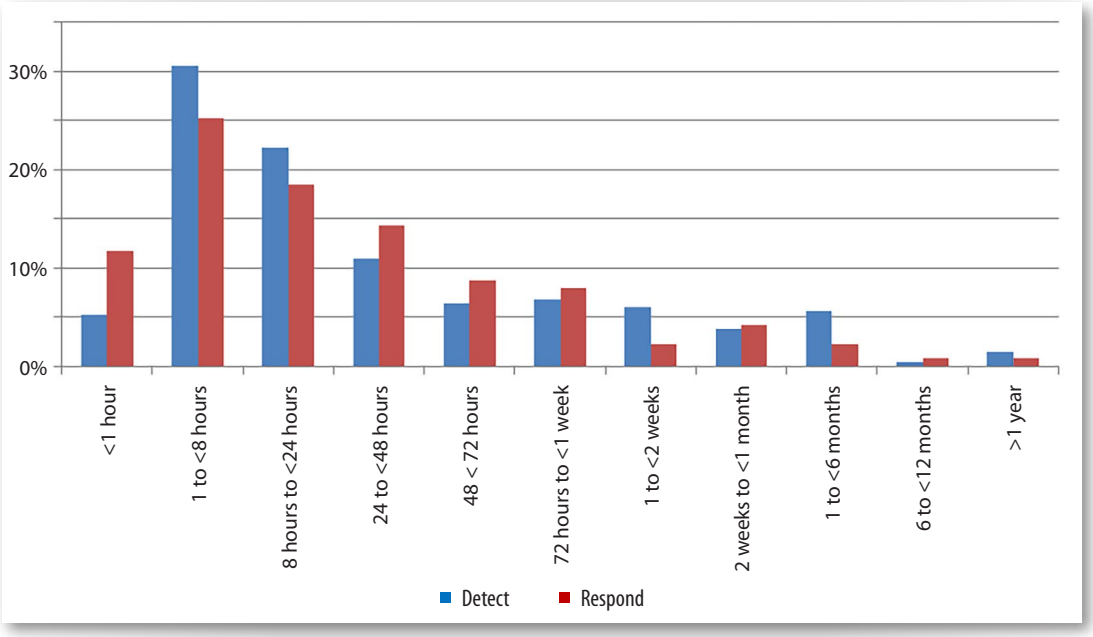

Figure 11. Length of Time to Detect and Respond to an Attack

It is important to point out that the information in this figure is extremely optimistic. Many organizations have no idea how long they have been compromised because their hunting programs are not very mature, meaning they would naturally miss many attacks.

Achieving ROI from Threat Hunting

To increase the overall value of your hunting program, perform the following steps:

- Identify clear metrics to track the overall success.
- Create a documented process for hunting.
- Whenever a new threat is found, update the process.
- Utilize automated methods of hunting as much as possible.
- Augment automated methods with manual intelligence.
- Provide ongoing metrics to executives to justify the program.

One of the many reasons adversaries are so successful is that they utilize automation to launch targeted attacks against a large number of organizations. Automation allows the human brain to scale and accomplish a significant amount in a short period of time. Cyber defenders need to harness the power of automation to properly scale their threat-hunting program and combat the automated threats launched against them.

Levels of Automation

The survey responses show varying levels of automation. Only 1% say they have fully automated their threat-hunting processes, and the majority (24%) say their programs are 26–50% automated. When aggregated, 36% have achieved automation of 51% or more; while 64% have not yet achieved reached that level of automation. See Figure 12.

How much of your threat-hunting capability is automated or machine assisted?

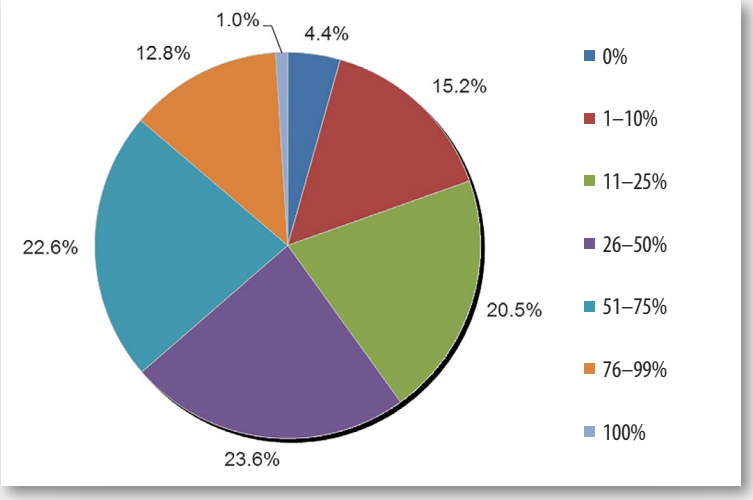

Figure 12. Varying Levels of Automation

It is important to note that threat hunting cannot be 100% automated; human experts must be involved with advanced analytics. The goal, however, is to use automation for repetitive, time-consuming tasks to find the events of interest. Humans can then analyze the high-priority events to determine the threat and the overall impact to the organization. To put it another way, computers would analyze large amounts of information that have a low probability of an attack, while humans analyze small amounts of information that have a high probability of an attack.

Triggers for Hunting

According to respondents, the most common trigger for launching a hunt, selected by 86%, is an anomaly or anything that deviates from normal behavior (see Figure 13). Of course, to use anomalies to trigger threat hunting, you must have a good idea of what "normal" is and have proper baselines in place.

What triggers active threat hunting on your network and endpoints?
Select all that apply.

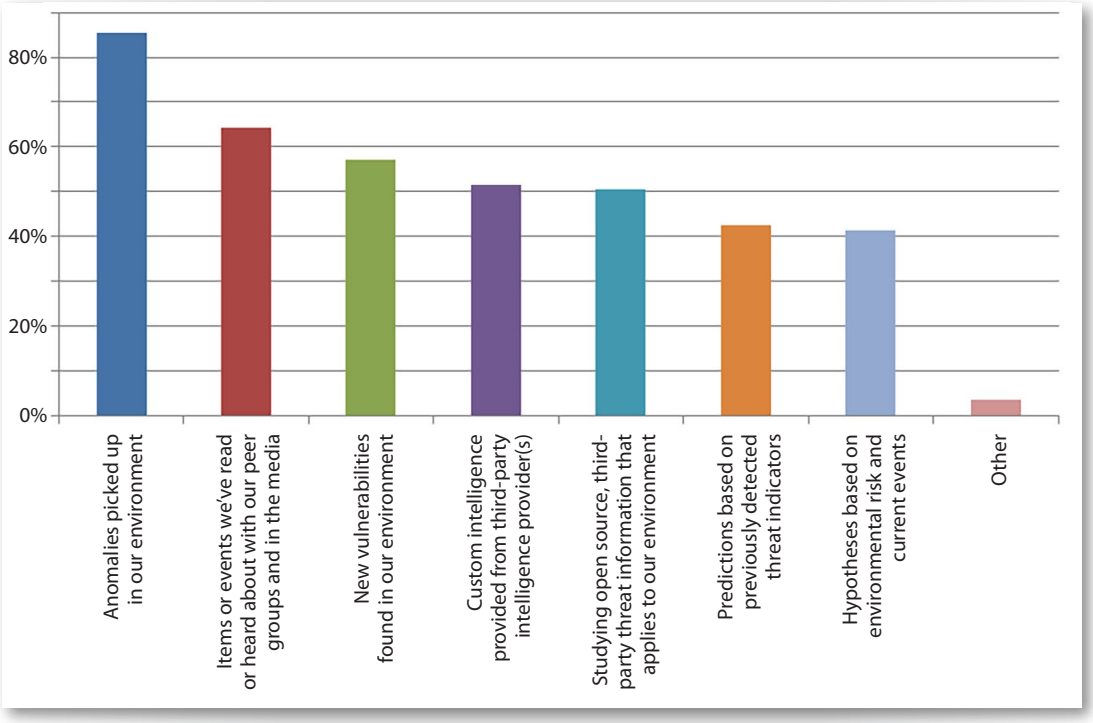

Figure 13. Triggers that Activate Hunting

These results indicate that organizations are also looking outward, to peers and media, as well as intelligence providers, to determine what to hunt for.

In addition to anomaly detection, it is also very valuable to use third-party sources and threat intelligence to guide your hunting program, chosen as a key trigger by 51% of respondents. Even in large organizations, it is not feasible that you would see or understand all attacks. By utilizing threat sources from thousands of organizations, you have much more valuable information for making proper decisions.

Types of Data Needed in the Hunt

The results of a hunting program are directly tied to the threat intelligence that is driving the program. If an organization has no idea what it is looking for, it will most likely not find anything of value. On the other hand, the more useful information driving the threat-hunting program, the more likely the organization is to find information of value.

The top seven data feeds respondents cite as being critical include IDS/IPS feeds, access and/or authentication logs, DNS, network traffic flow, endpoint security feeds, SIEM alerts and threat intelligence sources, all receiving recognition from more than 60% of respondents. See Figure 14.

What are the critical data feeds you need to conduct a hunt?
Select all that apply.

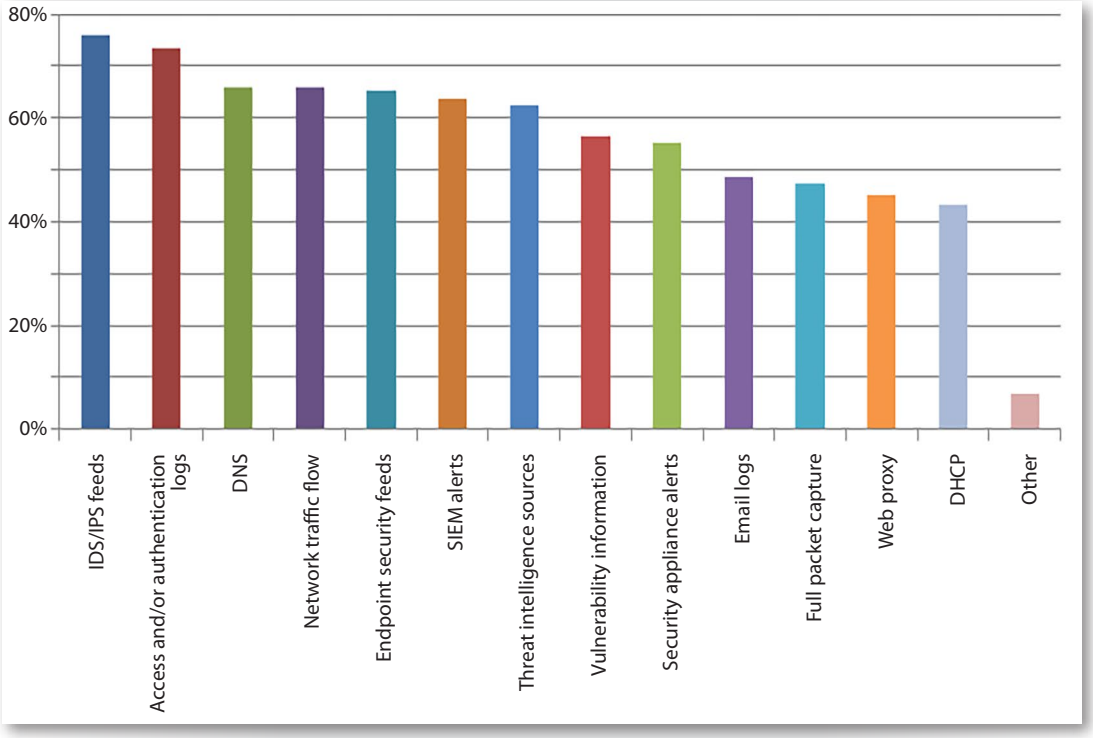

Figure 14. High-Value Data Needed

Hunters need critical data intelligence from all reporting systems in the enterprise to have a successful threat-hunting program. Consider this analogy: If you live outside a major city and need to drive in during rush hour, you could just pick a route and drive. Depending on road conditions, accidents and weather, you might arrive in time for your meeting—or you might not. The odds are not in your favor. However, if you listen to the news, monitor traffic and weather conditions, and pick a route based on up-to-date information (gather data intelligence), the probability of arriving on time increases exponentially.

Methods of Threat Hunting

In performing threat hunting, two general methods are used: network- or host-based hunting. Network-based hunting involves monitoring and analyzing network traffic to look for indicators that an adversary might be on your network. Host-based hunting involves analyzing an individual computer, looking at both what is installed on the computer and what is running on the systems, with the goal of finding signs of compromise.

While network hunting is used slightly more often by organizations, both network- and host-based hunting are required to detect hidden threats in the enterprise.

Data Needed for Hunting

Most participants utilized basic searching techniques to perform threat hunting in their environments. If an organization has not actively hunted, basic searching techniques will yield some initial results, but their value will be reduced over time once the basic points of compromises have been discovered. To continue to mature the hunting capabilities and find more advanced adversaries, you must collect data to drive the analysis. Letting data drive analysis enables organizations to perform more advanced methods of detection, such as statistical analysis and machine learning. In reviewing the survey data, it is not surprising that as the methods of hunting increase in sophistication, fewer organizations use those methods. Figure 15 illustrates this concept and provides a guide to threat-hunting maturity and the next steps organizations should take as they progress toward more mature and advanced hunting capabilities.

Blacklist, whitelist and reputation monitoring are the top sources of data sought in the majority of hunts.

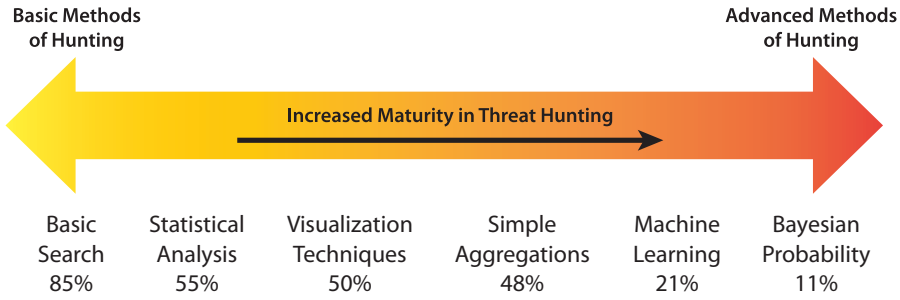

Figure 15. Maturity of Threat-Hunting Techniques

It is not surprising that most organizations initially utilize network-based hunting as their starting point for analysis, with the top three collection methods—IP addresses (84%), network artifacts and patterns (81%), and DNS activity (68%)—all drawn from network traffic. See Figure 16.

What types of collections do you utilize during hunt missions?
Select all that apply.

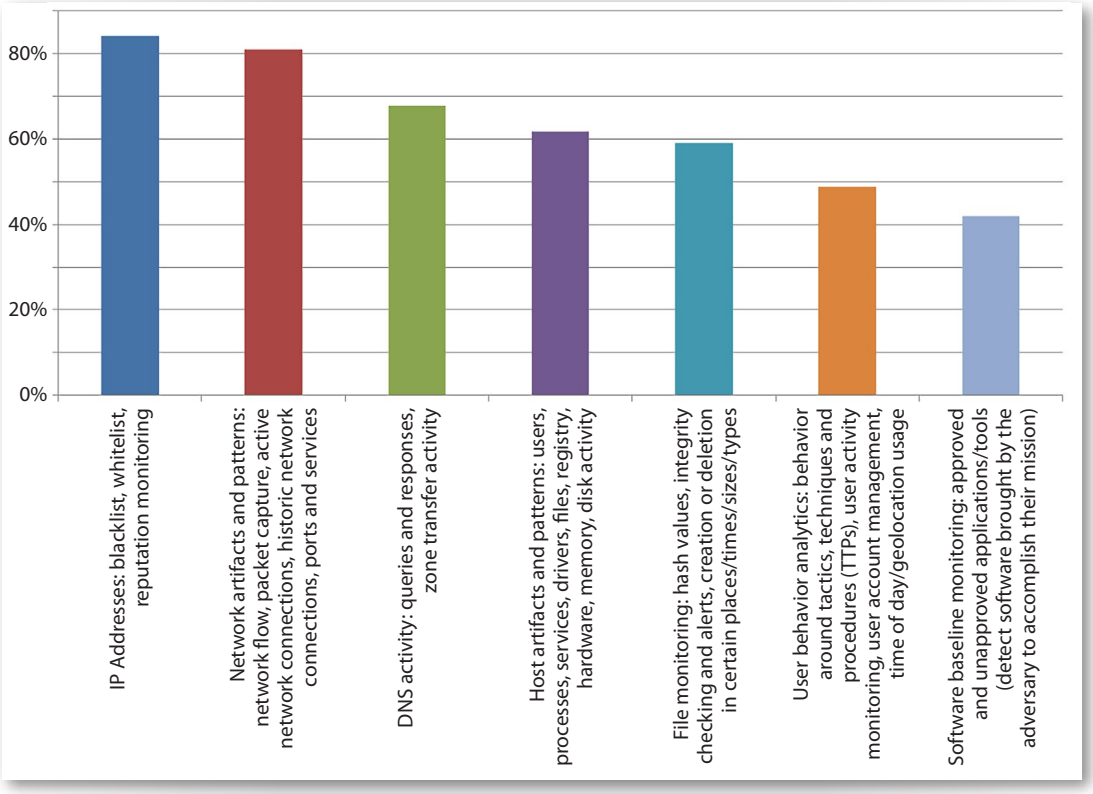

Figure 16. Data Collection that Drives the Hunting Mission

Network-based data collection is most popular because network analysis is more scalable in the collection and analysis of the information. With network traffic, one sensor can gather data from thousands of systems and correlate them in one location.

With host-based analysis, data collection is done on each system, typically through agents, which are harder to deploy and could make the process more time-consuming. In addition, host-based analysis often requires more details about the system that is being investigated, so it takes more time to customize, configure and perform analysis. For example, a database server would be analyzed differently than a web server would be.

Analyzing the Data

One of the statements you often hear in security is, "It's all about the data." For threat hunting, it is no different. If you have solid, accurate data, you will be able to find the adversary—and if you have bad data, your threat-hunting efforts will consume a lot of time and yield minimal results. One of the misleading aspects of data-driven threat hunting is that the *quantity* of the data matters. Not only is this approach wrong, but it can often lead to producing so much information that finding the adversary is borderline impossible. While data is important, the *quality* of the data is more important than the quantity. As your organization continues to perform threat hunting, the need for quality data should drive the data-collection process. When you find data that is valuable and useful, collect more of it. Look at the data you collect periodically and if you haven't used a type of data in a while, remove it from the collection process.

The most utilized method of host-based hunting consists of host artifacts and patterns: users, processes, services, drivers, files, registry, hardware, memory, disk activity.

Threat-hunting tools and methods should ultimately drive the data that is collected. For example, as an organization increases its sophistication from basic searching to statistical and Bayesian analyses, some previously gathered data will no longer be as valuable and new sources of data will be required. It is important to let the tools and techniques of threat hunting drive the sources from which data are collected and then analyzed.

Another great way to verify and validate the data-collection process is via visualization techniques. By graphically plotting the data flows and information being gathered with the results of the hunting process, it is easy to see which methods are yielding results. If certain data feeds have a higher probability of finding compromised systems and other techniques are yielding lower results, adjust the data collection based on positive result metrics.

Tools Used for Hunting

Doing anything in security by hand can be very difficult, if not impossible. Tools allow people to scale and perform tasks more efficiently. However, it is important to remember that a tool by itself has little or no value if it is not installed, configured and managed correctly by a human. It is the integration of tools and people that leads to effective solutions in threat hunting.

While organizations can purchase specialized tools to perform threat hunting, 87% of respondents are using existing tools to aid in finding, tracking and catching the adversary, while 67% are using vendor-provided or open source threat-hunting tools, as shown in Figure 17.

It is the integration of tools and people that leads to effective solutions in threat hunting.

What tools do you utilize to perform hunting?
Select all that apply.

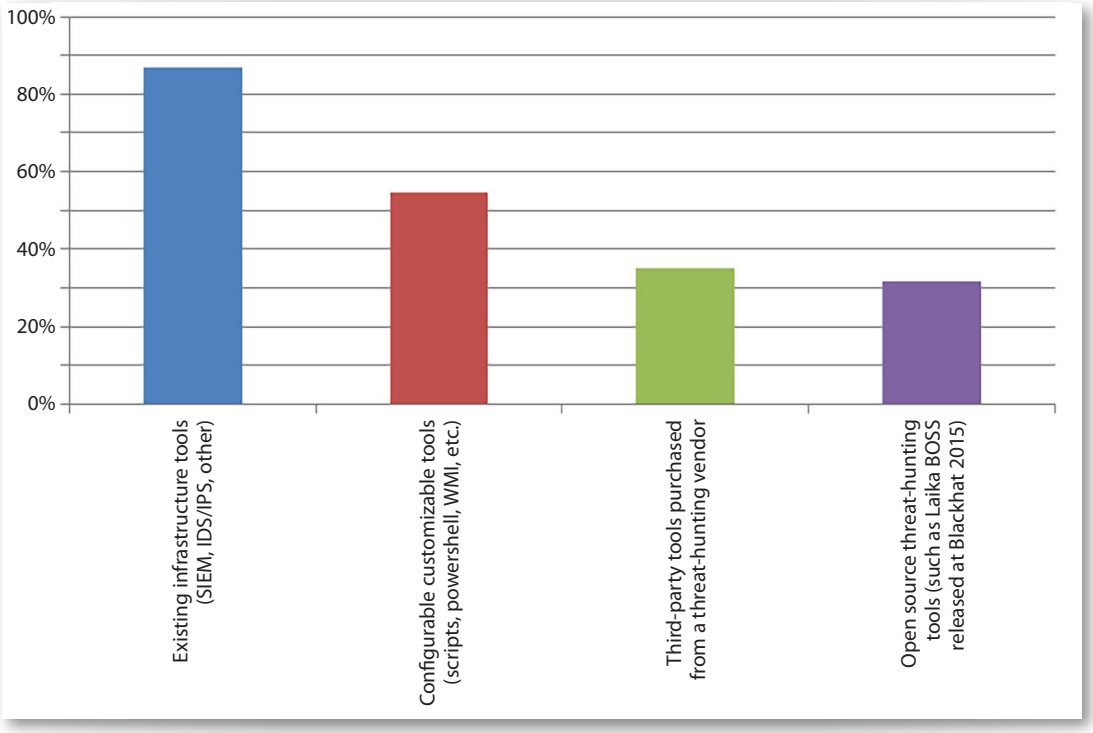

Figure 17. Tools Utilized to Perform Hunting

Use Tools to Find and Close Gaps

From a threat-hunting maturity perspective, it is always good to use existing tools to help understand the environment and, most important, to find gaps in your current capabilities. Once the gaps have been identified, try to write custom scripts to help enhance the capabilities of existing tools. In cases where that cannot be done, utilize specialized third-party hunting tools to start increasing the visibility and capability of your hunting program.

Based on the current immaturity of the threat-hunting market, the data in Figure 17 aligns with exactly what we would expect to see. Most organizations are utilizing existing tools to understand their environment. Slightly more mature organizations are writing scripts to enhance their capabilities, and very mature organizations are utilizing third-party tools. While open source tools are available, security teams typically use them in cases where organizations do not have budgets to buy commercial tools. Because organizations that utilize open source tools are very limited in resources, use of such tools is usually tied to more ad hoc, reactive hunting capabilities.

Next Steps in Threat Hunting

If you want your current threat hunting activity to align with best practices, focus on the following areas:

- Use formal methods of threat hunting
- Integrate people, processes and technology
- Balance automated and manual methods of threat hunting
- Look for known and never-before-seen malicious activity to drive the threat-hunting program

With these processes in place, organizations have more of a chance of catching previously unknown or undetected threats, as well as improving their response.

The value of threat hunting is twofold: The primary benefit is finding new advanced threats that existing technologies are missing. The secondary benefit is discovering gaps in existing technologies and using those discoveries to close vulnerabilities, thereby improving risk posture by reducing attack surfaces.

This is supported in the survey, where 70% of respondents found known threats, which could indicate a gap in current technology or a misconfiguration of existing devices. In addition to finding known threats, 52% found one or more previously undetected threats, and 40% found advanced threats. This shows that the respondents' hunting programs are finding exposures that would not have been detected with other technology currently in place. This indicates it is important to look not just for known threats but also for unknown threats and anomalous behavior.

The primary function of threat hunting is to find advanced, unknown threats, enabling early detection to control the overall damage. However, a second valuable purpose of hunting is to verify and validate how well existing tools are working in your environment. For example, if your threat-hunting capability is finding 25% of known attacks, the main question is: Why didn't your firewall, IDS and antivirus catch those attacks? This could indicate a failure in existing devices or show configuration errors. Essentially, you can use the data to follow up and reduce the attack surface by looking for such gaps. Alternatively, existing technology may have caught the attack but analysts failed to react or take action. Therefore, as you evolve your threat-hunting program, do not think of using it just to find advanced attacks, but also use it as verification for existing tools and processes.

Cover Your Tracks

Because threat hunting is primarily focused on finding advanced threats, it is important to remember that the goal of advanced threats is to be stealthy, targeted and data focused. Advanced adversaries do not want to be caught. In performing hunting, then, it is important to remember that while your primary role is to be the hunter, you will also be hunted by the adversary, who is trying to find your capabilities and render them useless. To prevent attackers from detecting your hunting and observation of their activities, all your communications, deployments and operations need to be covert.

It is important to remember that while you are hunting, you are also being hunted.

Ensuring and verifying that your threat hunting is stealthy and not detectable is indicative of a more advanced or mature hunting program. Since threat hunting is an emerging practice, it is not surprising that 53% of respondents say their organizations do not have capabilities that enable them to hide from the adversary, as illustrated in Figure 18.

Do your hunting tools and processes render themselves undetectable to the advanced adversary? ***Select the best answer.***

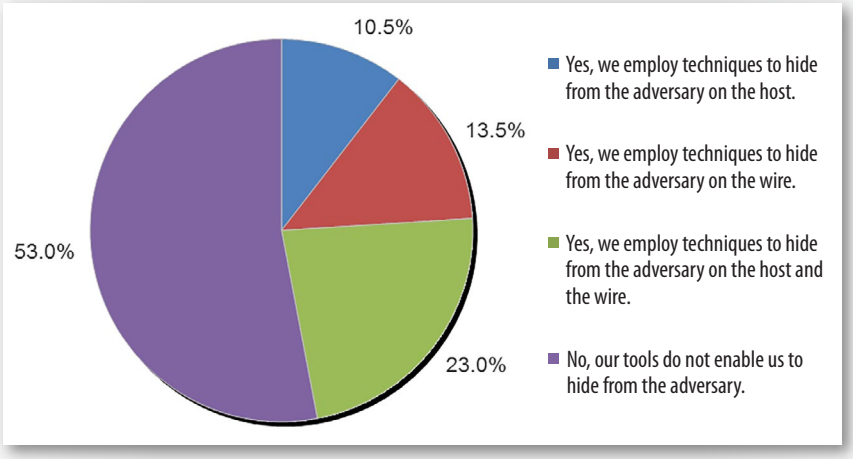

Figure 18. Overall Effectiveness of Threat-Hunting Capabilities

Only 23% have hunting processes on both the host and the network that respondents consider to be invisible to attackers. If an advanced attacker is on the network and knows he or she is being hunted, you may not see that attacker at all, despite your best hunting efforts.

Improvements Needed

As organizations continue to grow their threat-hunting capabilities, they are still looking for improvement. For example, 58% still need better detection, 57% want more automated tools and 54% need more skilled staff. See Figure 19.

What do you still need with respect to threat-hunting tools and capabilities?
Please indicate your top three, in no particular order.

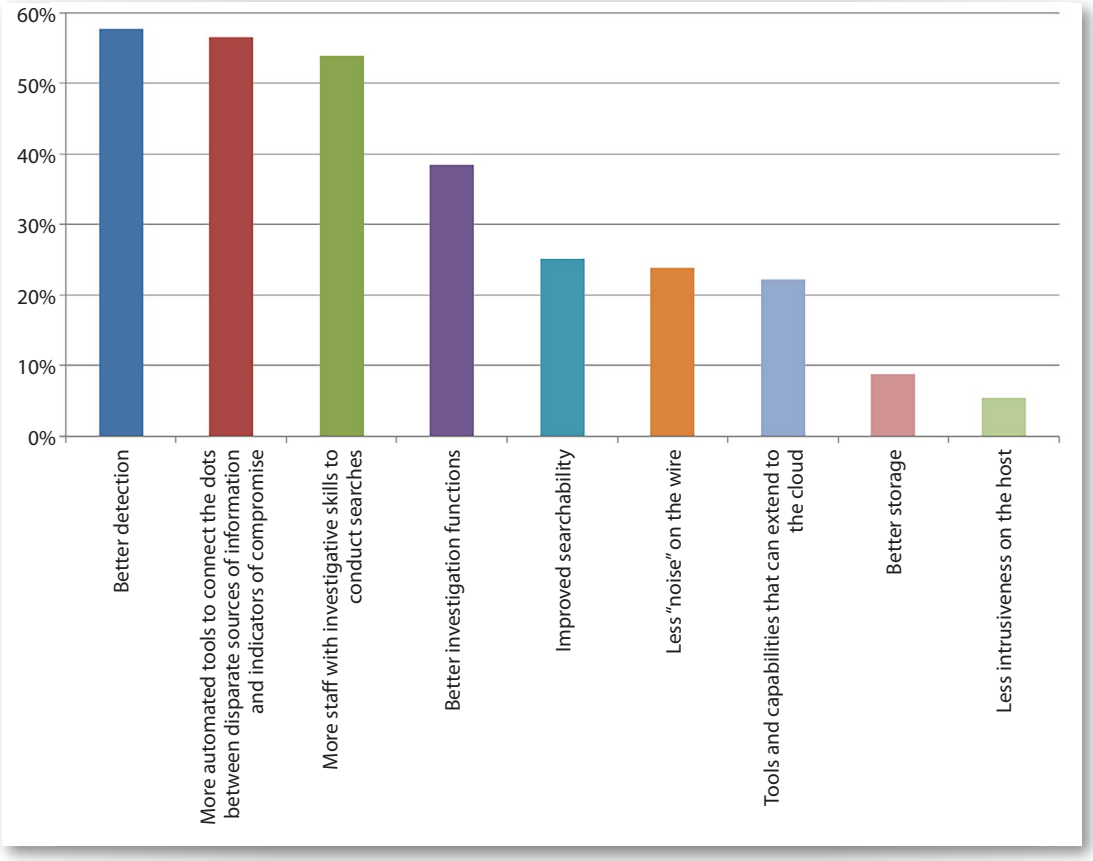

Figure 19. Areas of Improvement in Threat Hunting

Because many organizations initiate their hunts in reaction to anomalies and then turn the anomaly over to smart people who perform an analysis, a natural limitation exists. Therefore, utilizing customized tools and automation will improve detection and allow the limited staff to analyze more events and catch more adversaries.

Spend More on Hunting

Respondents are willing to spend money on future investments in threat hunting, despite the shortcomings they've cited in this survey. Some 62% of the respondents are planning to increase their spending on threat hunting in the coming year, with over 42% increasing it by 25% or more, and less than 5% reducing their expenditures. See Table 1.

Table 1. Changes in Investment in Threat Hunting

Percent Change in Investment in Threat-Hunting Tools	Percentage of Respondents
100% Increase	5.9%
75% Increase	1.8%
50% Increase	11.4%
25% Increase	22.5%
10% Increase	20.7%
No Change	32.8%
Reduction in Investment	4.9%

Actions always speak louder than words. It is one thing for executives to say something is important, but ultimately they will spend money on areas that they feel are really important.

Improve Your Road Map

As you continue to build out your road map for threat hunting and look at next steps, focus on building a robust threat-hunting program that not only catches unknown attacks, but can also verify that existing tools and capabilities are working properly. Think of threat hunting as an enhancement and complementary to existing tools, not as a replacement. Second, all the threat hunting in the world will not be effective if the adversary can find it and render it useless. As you continue to mature your hunting capabilities, it is important to make your techniques invisible to attackers and then continue to verify that the techniques are not detectable.

Conclusion

Threat hunting is an evolving area in which survey respondents are finding real value. Because traditional security measures are failing, organizations are looking for new methods and techniques to detect adversaries already inside their networks and to control the overall damage.

While many organizations are performing threat hunting, it is often an ad hoc process with no formal methods or procedures. Responses also show that threat hunting contains many moving parts, so it is important to constantly evolve your threat-hunting program to demonstrate improvements and maintain the support of organizational leadership.

Recognize that threat hunting requires a balance of people, process and technology. Allow automation/tools to perform the time-consuming tasks and train humans to perform the high-end analyses. Knowing what to manage through technology and what to assign to people will guide your formal method of threat hunting with a built-in process-improvement method. Document both mistakes and failures, and continuously update your hunting methods.

The more you can learn about how the adversary works, the more successful you will be. It is, however, important that you continually work to keep your hunting activities hidden from the adversary so you can observe and then remove the threat before the adversary discovers that he or she is being monitored.

Finally, have clear metrics, such as dwell time and lateral movement, to track overall success and show a positive ROI to executives.

About the Author

Eric Cole, PhD, is a SANS faculty fellow, course author and instructor who has served as CTO of McAfee and chief scientist at Lockheed Martin. He is credited on more than 20 patents, sits on several executive advisory boards and is a member of the Center for Strategic and International Studies' Commission on Cybersecurity for the 44th Presidency. Eric's books include *Advanced Persistent Threat, Hackers Beware, Hiding in Plain Sight, Network Security Bible* and *Insider Threat*. As founder of Secure Anchor Consulting, Eric puts his 20-plus years of hands-on security experience to work helping customers build dynamic defenses against advanced threats.

Sponsor

SANS would like to thank this survey's sponsor:

Malwarebytes