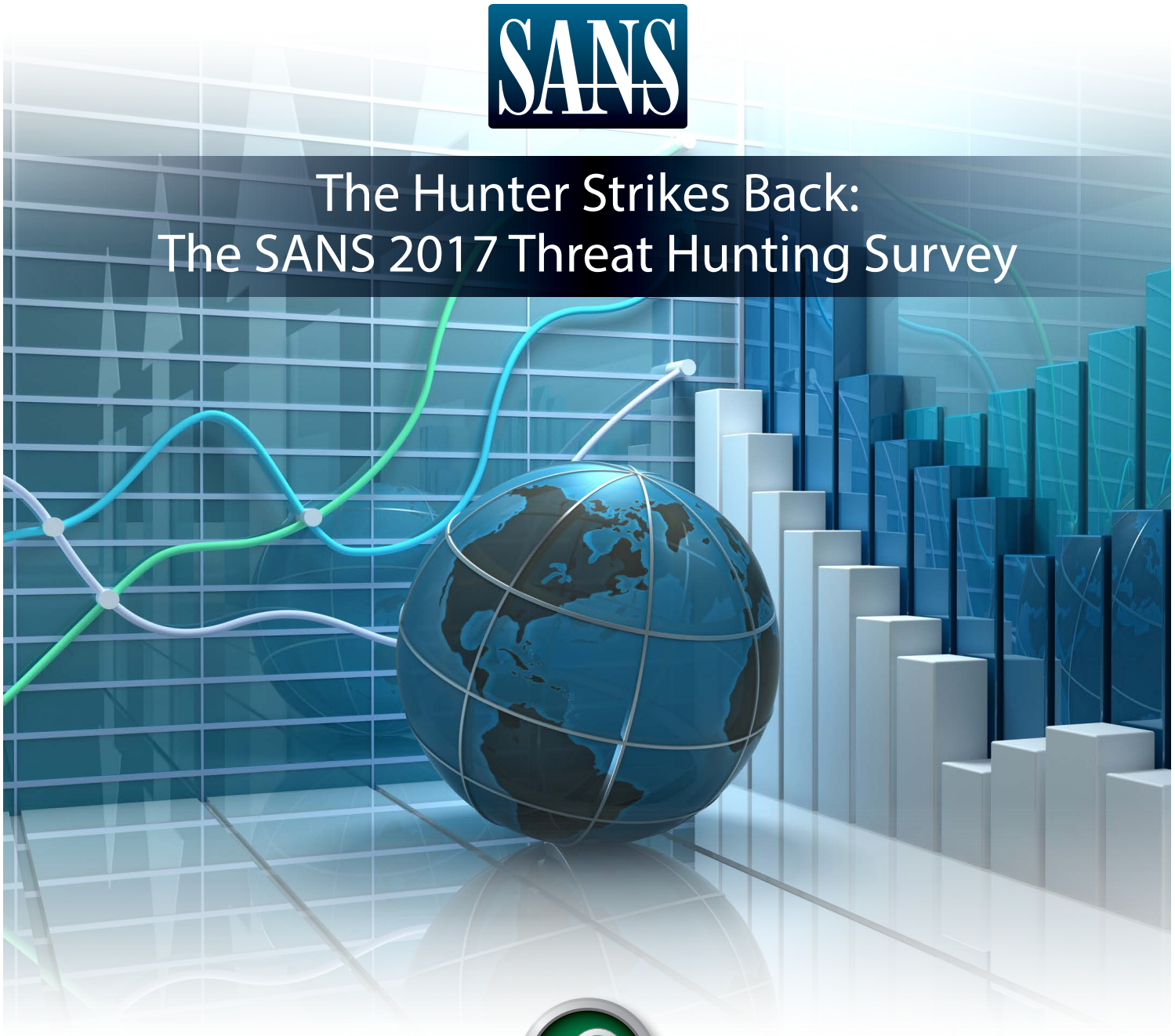

The Hunter Strikes Back: The SANS 2017 Threat Hunting Survey

A SANS Survey

Written by Rob Lee and Robert M. Lee

April 2017

Sponsored by
Malwarebytes

Executive Summary

Threat hunting is a focused and iterative approach to searching out, identifying and understanding adversaries that have entered the defender's networks.[1] Results just in from our new SANS 2017 Threat Hunting Survey show that, for many organizations, hunting is still new and poorly defined from a process and organizational viewpoint.

Key Results

claim they do threat hunting on an ad hoc basis

consider endpoint security data necessary in their threat hunting data feeds, with **73%** needing access and authentication logs

say their threat hunting capability generates automated alerts and performs automated pattern matching

of those threat hunting achieved measurable improvements in security based on their threat hunting efforts

report improvements in speed and accuracy of response due to threat hunting, and the same percentage have been able to reduce exposures through threat hunting

Unfortunately, most organizations are still reacting to alerts and incidents instead of proactively seeking out the threats. Threat hunting itself cannot be fully automated. The act of threat hunting begins where automation ends, although it heavily leverages automation. With that said, many organizations are finding success with a focus on core continuous monitoring technologies and relying on more security automation in their environments to make hunting more effective.

The survey, taken by 306 respondents, reveals that most organizations that are hunting tend to be larger enterprises or those that have been heavily targeted in the past. The survey reveals a number of other interesting data points, including the fact that of the organizations that achieve measurable improvements in their security, 91% measured improvements in speed and accuracy, while the same percentage said the use of hunting reduced their exposures.

The survey also shows that threat intelligence and hunting must go hand in hand to work effectively. Responses indicate intelligence is key to being effective in threat hunting, and that focusing on people and training are paramount for that effectiveness.

This paper looks at the state of threat hunting and suggests approaches organizations can take to enhance their threat hunting programs.

[1] "The Who, What, Where, When, Why and How of Effective Threat Hunting," February 2016, www.sans.org/reading-room/whitepapers/analyst/who-what-where-when-effective-threat-hunting-36785

Understanding the Respondents

Over the past few years, organizations that are adopting threat hunting tactics and strategies are increasing. But most of the growth is limited to the financial, high tech, military/government and telecommunications sectors. These are the sectors directly afflicted with targeted attacks by numerous threat groups supported by organized crime and nation-states. Healthcare is inching higher in representation, as this sector has been plagued by ongoing ransomware attacks over the past few years.[2] Survey respondents came from predominantly these same sectors, as noted in Table 1.

Table 1. Top Five Industries Represented

Industry	Percentage
Financial services, banking and insurance	19.0%
Government	14.4%
High tech	13.1%
Telecommunications or ISP	7.5%
Healthcare	5.9%

The general category of "Other" represented 14% of our sample, the same as government, and was composed largely of consulting and security service providers, as well as respondents in the insurance, legal, and oil and gas industries.

Security analysts, their direct managers and incident responders/threat analysts accounted for 65% of the respondents for this report. These same groups of active information security personnel are the groups responsible for conducting threat hunting activities. See Figure 1.

What is your primary role in your organization?

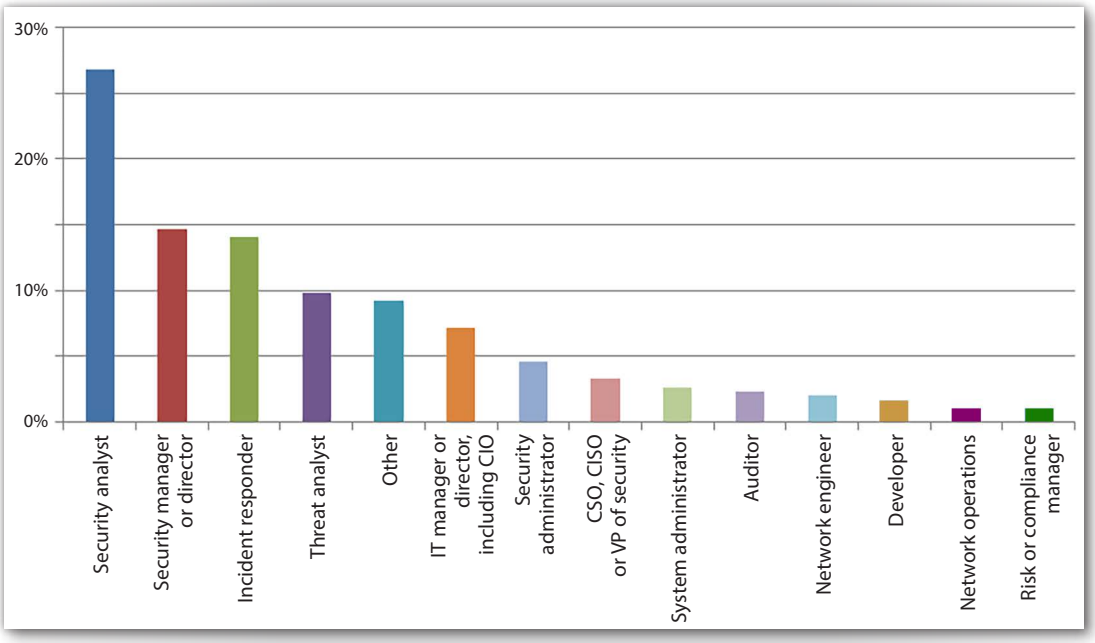

Figure 1. Respondents' Roles

[2] "12 healthcare ransomware attacks of 2016," December 29, 2016, www.beckershospitalreview.com/healthcare-information-technology/12-healthcare-ransomware-attacks-of-2016.html

Threat Hunting: The Newborn Child in IT Security

Threat hunting is new for most security teams, and it is primarily accomplished through unstructured and fairly untested "hunting" capabilities. Even though 27% of the teams have defined their own methodologies for hunting, only 5% are using external guidance from published sources to create their methodologies, and 7% outsource to a third party. The majority, 45%, engage in hunting on an ad hoc basis. See Figure 2.

Does your organization perform threat hunting?

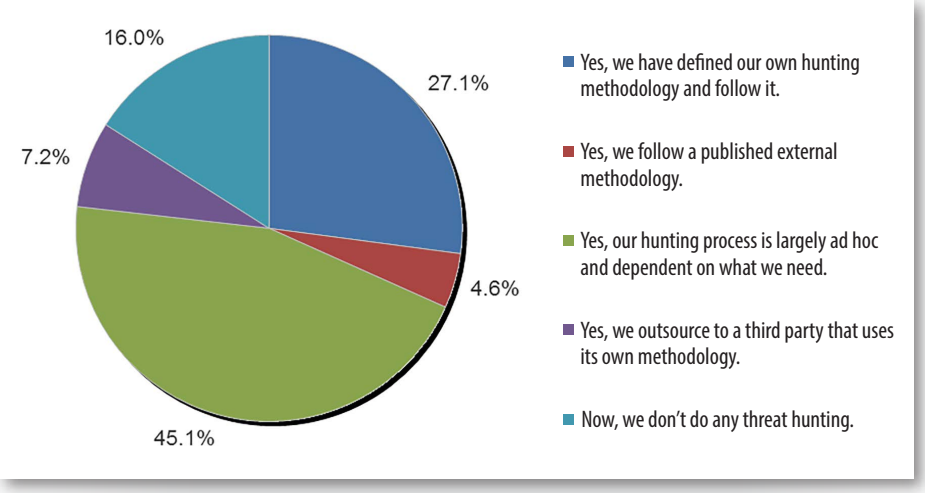

Figure 2. Threat Hunting in Practice

Part of the reason so few teams use externally provided methodologies is that there are not a lot of public reference resources for teams seeking to adopt hunting practices. There are very few published guidelines for proper threat hunting tactics and strategies across the security industry.

Respondents Describe the Challenge

"Our security department is new, and just starting the program formally. Any threat hunting would have been sporadic and based on some event that was triggered."

"The focus on security is fairly new to our company, so we are still developing our threat hunting methodology."

"Security has not been a high priority in our org previously. We are, however, developing a security team to threat hunt as well as [handle] incident response."

Moreover, many organizations are not mature enough to fully adopt threat hunting capabilities. The survey demonstrates that most organizations are still struggling to adopt more formal threat intelligence capabilities into their security operations centers (SOCs), which is a requirement for proper threat hunting to occur. The survey results also detail a significant number of groups outside the largest of enterprises and government that are still struggling with putting together security operations and mature incident response capabilities, which are prerequisites for dedicated hunting capabilities.

Threat hunting is new, and its emergence is reminiscent of the initial information security operations of the late 1990s and early 2000s. Most of it is internally learned and not well documented. Helping to correct the lack of overall threat hunting experience, an increasing number of larger organizations have dedicated their teams to threat hunting in their daily security operations. These hunting teams are slowly sharing their results, techniques and findings with the community through conferences, whitepapers, blogs and small online collaborative groups.

Resources Online

- **The ThreatHunting Project:** www.threathunting.net
- **Enterprise Detection & Response:** http://detect-respond.blogspot.com
- **"The Who, What, Where, When, Why and How of Effective Threat Hunting":** www.sans.org/reading-room/whitepapers/analyst/who-what-where-when-effective-threat-hunting-36785
- **"Generating Hypotheses for Successful Threat Hunting":** www.sans.org/reading-room/whitepapers/threats/generating-hypotheses-successful-threat-hunting-37172

Given the lack of frameworks, selecting from the many new products or services specializing in threat hunting is a "buyer beware" environment. Some service and product companies have simply relabeled their products as "threat hunting," because they help "detect threats." Although threat hunting is used to detect threats, it is much more than that.

Hunting is about taking a proactive—as opposed to a reactive—approach to identifying incidents. A reactive organization begins incident response (IR) when an alert or notification comes in. The alert could come from a third party, such as the FBI, or it could come from the organization's own security sensors. The best analogy to a reactive approach is that the IR team is largely waiting to be called into action and relying on the accuracy of the notifications it is receiving. Most organizations start building their IR teams as a reactive organization, and there is nothing wrong with that. In many cases, the IR team is largely composed of augmentation staff that normally fulfill other duties during their regular jobs. As the organization grows larger, or if it has an increasing number of incidents, the team is likely to become permanent. Even larger organizations likely still augment their IR teams with additional internal personnel or might contract to third-party contractors that provide such services.

ADVICE

Any organization looking to acquire services or products from "threat hunting" companies should exercise additional due diligence to discern whether the product will meet its needs, especially because the concept is relatively new. Be sure to ask for recommendations from peers in the community to determine what works so the organization can seek similar capabilities.

Organizations move from being reactive organizations to becoming hunting organizations when they realize they are not detecting their incidents early enough. The idea of a hunting-based response doesn't mean it is an either/or approach. A key element of becoming a hunting organization is adopting a mindset that assumes an adversary is already present. That opens the organization's eyes to detect key indicators of an attack.

Most hunting organizations are also reactive. The distinction is that they begin to task their IR teams to actively engage and hunt for adversaries inside their environment. To accomplish this task, the team will typically be armed with known malware, patterns of activity or accurate threat group intelligence to aid them in their search.

Organizations that decide to create a hunting organization sometimes fail to see the importance of proper threat intelligence for driving the search in the right areas. Simply tasking a team to "find evil" isn't enough. The team needs to know the difference between normal and abnormal as a prerequisite. It needs to know typical hacker tools and techniques. It needs to be skilled in both network- and host-based forensics and response to look for the footprints of these adversaries. Finally, it helps if the organization has invested heavily in a cyber threat intelligence capability that will help guide the team to the right locations on the network to look for specific indicators and techniques associated with threat groups interested in the specific data or capability that the organization owns.

Having such capabilities is an achievable goal. But be prepared. Hunting involves both a manual and a semi-automated scanning of systems looking for evil.

Continuous Hunting: Not There Yet

Asking organizations whether they accomplish threat hunting is a hard question to assess correctly. For example, if you present this scenario to an individual: *"You are downtown in a large city walking alone to your car. Do you look for potential threats?"*, he or she is likely to answer *"Yes."* Threat hunting in an organization is very similar.

In our survey, most organizations feel they conduct threat hunting regularly. See Figure 3.

How often does your organization perform threat hunting?
Select the most appropriate.

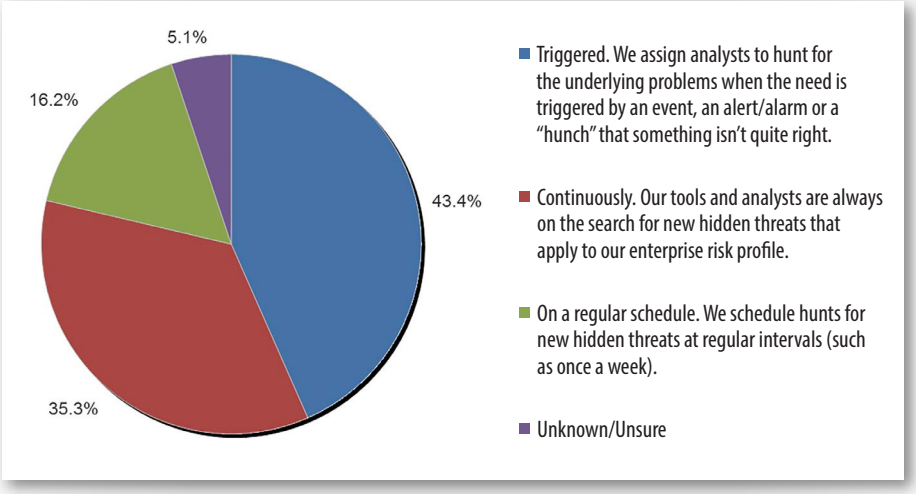

Figure 3. Threat Hunting Regularity

Yet, because threat hunting is new, respondents could also be categorizing activities related to antivirus, IDS or security information and event management (SIEM) alerts as "threat hunting" activities. These data sources are likely used in hunting, but all three are reactive and response technologies, whereas hunting is more proactive than reactive. Our survey brings this issue to the forefront, with 43% initiating searches responding to alerts, and only 35% continuously searching for new hidden threats.

The *"reactive trend"* is a very important takeaway because it shows that most organizations are not accomplishing hunting prior to detecting the event. They are simply responding to alerts provided by intrusion detection systems. This is "business as usual" in the information security industry. Hunting still plays a large role in the "incident scoping" phase of the incident response, given that the incident intelligence is now guiding the hunters on where to find additional compromised hosts. This phase helps determine the total number of compromised systems and measures the level of severity of the breach.

From our perspective, this is very positive and likely indicates that the organization is approaching formal proactive threat hunting operations and is developing skills along the way. If you ask senior or expert threat hunters where they learned to "hunt," most will say it was through their involvement in IR and scoping the extent of the breach. The IR team transitioning from reacting to incidents to hunting for threats themselves is a great sign that many organizations are likely on the cusp of formalizing their threat hunting capabilities over the next few years. The only challenge, which we will discuss later, is retaining the staff that is learning these newfound threat hunting skills.

Threat Hunting Methodology Required

From our perspective, to accomplish continuous hunting you must have a set methodology, and only 32% state they have a methodology that they follow in-house. Without a set methodology, organizations are simply guessing where to look, using random techniques that may or may not work.

Recommendations

Our recommendation is that organizations that are properly engaging in incident response begin to dedicate full-time teams to incident response and assign them the task of threat hunting. We also advise organizations to begin scoping out threat intelligence and how it can be used to initiate targeted hunts across their enterprise. If an organization has poor visibility into its networks, it would first need to start the buildout of capabilities that provide continuous monitoring capabilities across their networks and endpoints.

In summary, try this approach:

1. The security operations center's (SOC's) continuous monitoring helps detect threats better and reduces dwell time.
2. The full-time IR team evolves into the threat hunting team.
3. Teams integrate internal and external threat intelligence feeds into continuous monitoring and assign the IR hunting team to target likely locations where adversaries might exist.

Mainly SOC-Based Hunting

One of the key questions of the survey asks: "What activities would initiate an active threat hunt in your environment?" Examining the results, it seems that hunting appears to be more centered on "reactive" indicators instead of proactive intelligence. This means that more organizations are following a traditional SOC "security monitoring" approach as opposed to utilizing predictive cyber threat intelligence (CTI) to do targeted inspections of likely locations of adversarial activity. For example, 87% use alerts/alarms from other tools, which indicates use of more traditional detection approaches that are not as scalable or accurate. See Figure 4.

What activities would initiate an active threat hunt in your environment?
Select all that apply.

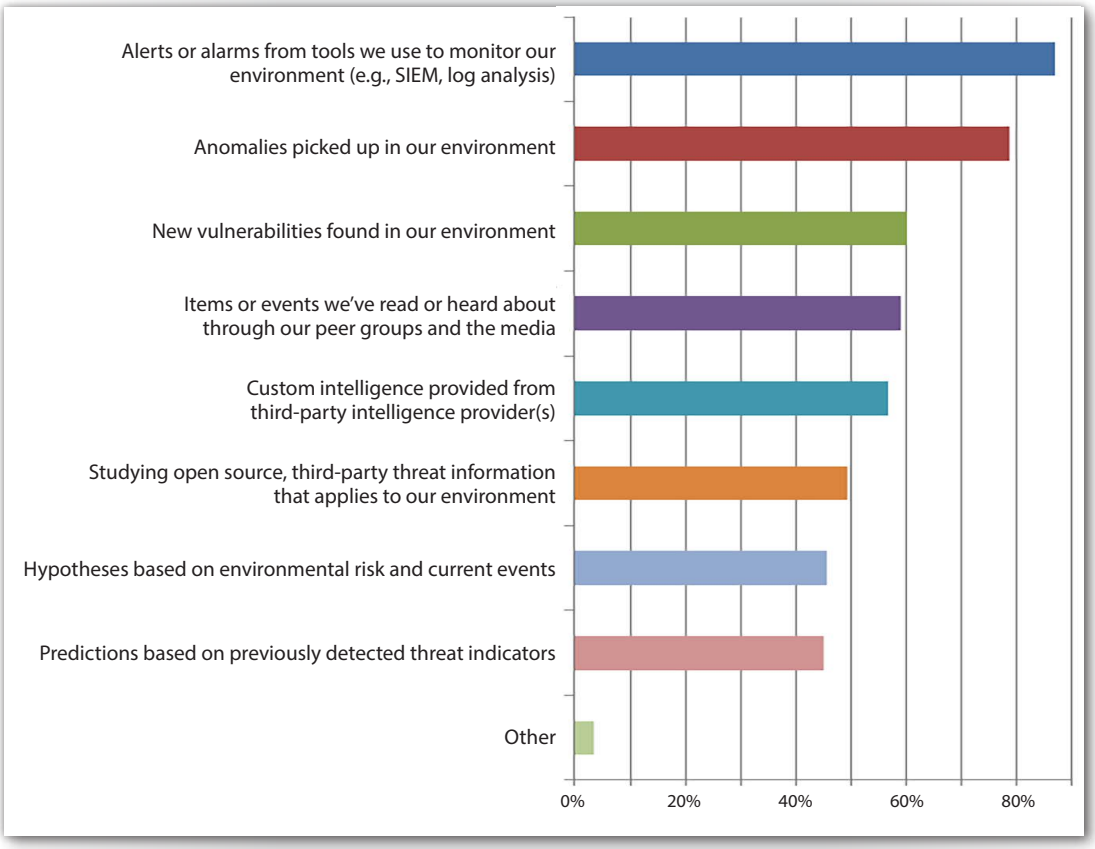

Figure 4. Active Hunt Initiators

Such approaches can increase false positives. The reactive capabilities being used in "hunting" are not customized to the specific threats facing an organization.

Another contributor to the false positives problem is that 79% use anomalies in their environments to guide their hunting. Many anomalies are false positives, and differentiating false positives from anomalies is increasingly difficult. Although anomaly detection can provide some success, organizations can leverage more effective hunting capabilities to reduce the time and effort that cyber security teams might encounter while chasing the source of the anomalistic blip on the radar.

TAKEAWAY:

Not every adversary is targeting your organization, but the more you understand who is targeting you and what the adversary might be after, the more you move threat hunting away from reactive incident response scoping toward proactive intelligence-driven hunting.

What is encouraging is that 49% use open source third-party intelligence in their threat hunting operations, while 57% also use custom intelligence from intelligence providers. Without CTI, organizations attempting proactive hunting are shooting in the dark, as they will have limited knowledge on where to find and uncover likely adversaries targeting their organization. According to the SANS 2017 Cyber Threat Intelligence Survey,[3] many organizations do not yet have a formal internal team working on threat intelligence. To begin this process, we recommend that teams that are just starting out seek companies providing threat intelligence feeds and look to industry resources, if available.

Bottom line: Organizations that create or ingest modern threat intelligence feeds for tuning sensors to initiate hunting operations are more successful at threat hunting. Organizations need to consider that hunting is more than advanced security monitoring and move their hunting mindset strategically through targeted approaches using threat intelligence to provide hunting accuracy.

[3] "Cyber Threat Intelligence Uses, Successes and Failures: The SANS 2017 CTI Survey," March 2017, www.sans.org/reading-room/whitepapers/analyst/cyber-threat-intelligence-uses-successes-failures-2017-cti-survey-37677

Threat Hunting Still a Nascent Activity

Most organizations often borrow staff from other resources and even outsource threat hunting to accomplish their goals. Only 31% of respondents report having a full staff dedicated to hunting. Organizations tend to pull their hunting staff teams from other staff (16%), in an ad-hoc manner (13%), or outsource services (6%). Because hunting is continuous, this could lead to ongoing challenges in most security environments, with staff being pulled in different directions and unable to provide the level of service needed. See Figure 5.

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

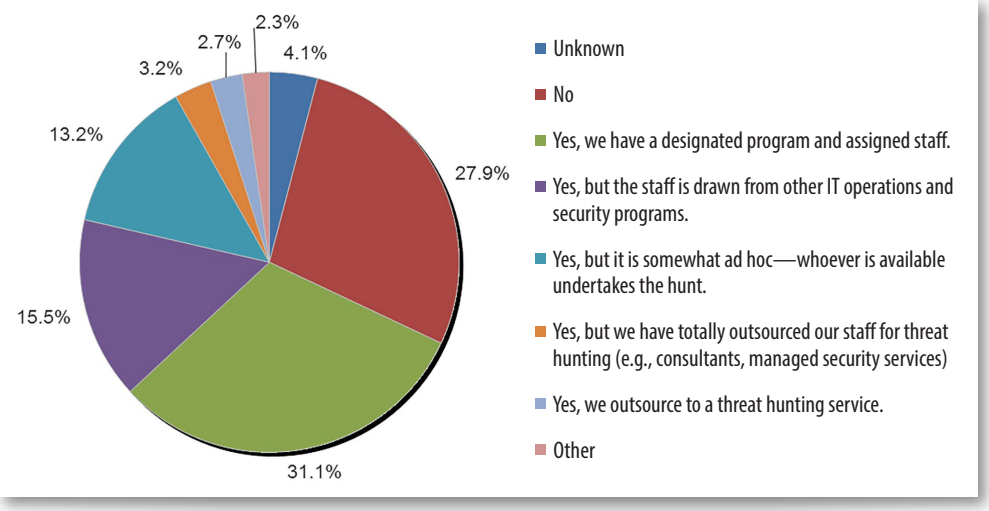

Figure 5. State of Threat Hunting Staffing

It is also apparent that many threat hunting organizations are prioritizing "technology" over personnel, as shown in Figure 6.

In what areas do you spend your threat hunting resources?
Rank in order with "First" being the highest spending priority and "Fourth" being the lowest.

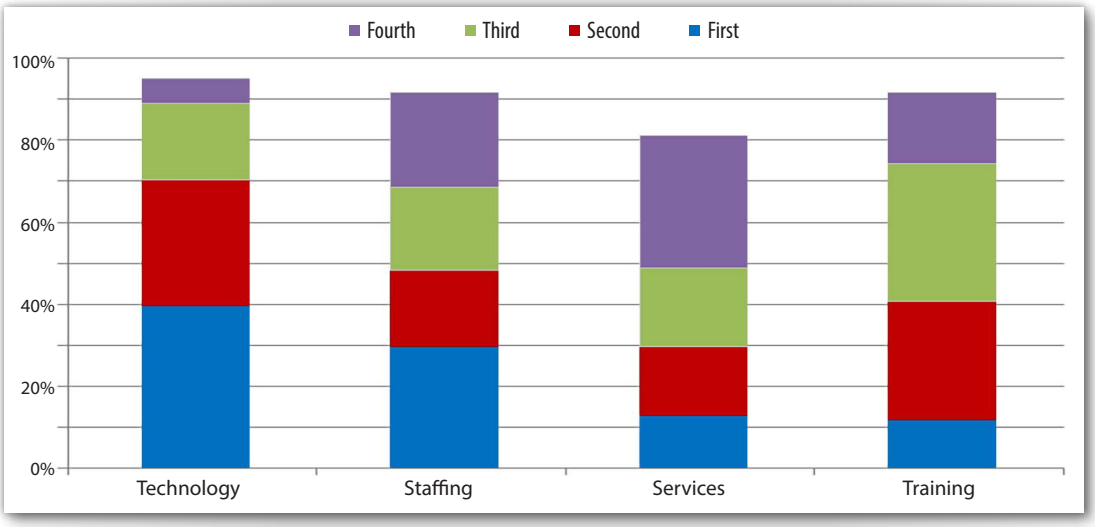

Figure 6. Threat Hunting Spending Priorities

TAKEAWAY:

Staffing and staff training need to be considered a bit more important because automation in threat hunting does not formally exist. While automation is valuable to threat hunting, threat hunting cannot be fully automated because there is always a need for human intuition to stay ahead of sophisticated human threats.

Intrusion detection capabilities and proper logging are key to proper data collection, and hunting requires more than just technology to succeed. Threat intelligence, scalability and analysts are needed to drive those capabilities to succeed. Threat hunting automation is similar to spell-check in a word processor. While it can help to identify mistakes, it is, by its nature, largely human driven and is more of a tool, rather than true automation.

Threat Hunting Skills and Tools

Threat hunting tools driven by trained analysts can help increase the scalability and accuracy of threat hunting operations. Core technical skill sets and knowledge areas are also key to a successful threat hunting team. The two key areas defined by the participants include core security operations capabilities and digital forensics and incident response (DFIR) skills. Baseline knowledge of networks and endpoints make up the first tier of knowledge. These knowledge areas are essentially understanding typical network traffic and endpoint services across multiple locations inside an enterprise network. These skills are rated appropriately, as they are core capabilities and are, therefore, mandatory for threat hunting to be effective.

In the same grouping, we also observe both threat intelligence and analytics. Security analytics provide short- and long-term historical views of data in motion and at rest across the network and hosts, enabling threat hunting teams to begin to spot anomalies. Moreover, threat intelligence provides the key difference for hunt teams to focus on areas targeted by adversaries, in addition to being on the lookout for key adversary tactics, techniques and procedures (TTPs) in use across the enterprise. Without threat intelligence fine-tuning a team's area of focus, most teams find themselves overwhelmed by the massive amount of data they must analyze.

Security Operations Skills: Tier 1 Rankings

- Log analysis and use of analytics tools 80%
- Knowledge of baseline network activity 78%
- Threat analysis (including the use of threat intelligence) 70%
- Understanding of baseline endpoint apps, users and access 66%

DFIR skills make up the second tier of required skills, given that incident response and forensic skills are the baseline capabilities needed to perform hunting on single hosts and at scale across an organization's enterprise network. DFIR skills are usually ranked to follow core capabilities because trained analysts use them to help identify and extract new threat intelligence used to identify compromised hosts using Tier 1 skills.

Digital Forensics and Incident Response Skills: Tier 2 Rankings

- Incident response 66%
- Network forensics 58%
- Endpoint forensics 50%
- Malware analysis 49%
- Memory forensics 38%

The two tiers are grouped together perfectly. We recommend that organizations initially focus on building out the core capabilities when trying to build a threat hunting team. Arm your team with the ability to examine baseline network and endpoints. Then, be able to use security analytics and threat intelligence to identify compromised hosts more efficiently and at a scale that pairs up with the size of your network.

Existing Infrastructures Used

Across the board, most respondents used their existing infrastructures (91%) for threat hunting. Existing infrastructure, such as log files, SIEM analytics and intrusion detection systems, are valuable to threat hunters. But it still takes humans to conduct threat hunting and to be on the lookout for anything these tools aren't consolidating and catching themselves. Most of these capabilities are rule-based and provide reactive detection. See Figure 7.

Most of the data stacking today is done manually by hunting teams, but in the future, this capability could become more automated to help make hunting teams more efficient and accurate in identifying the endpoints for closer inspection.

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

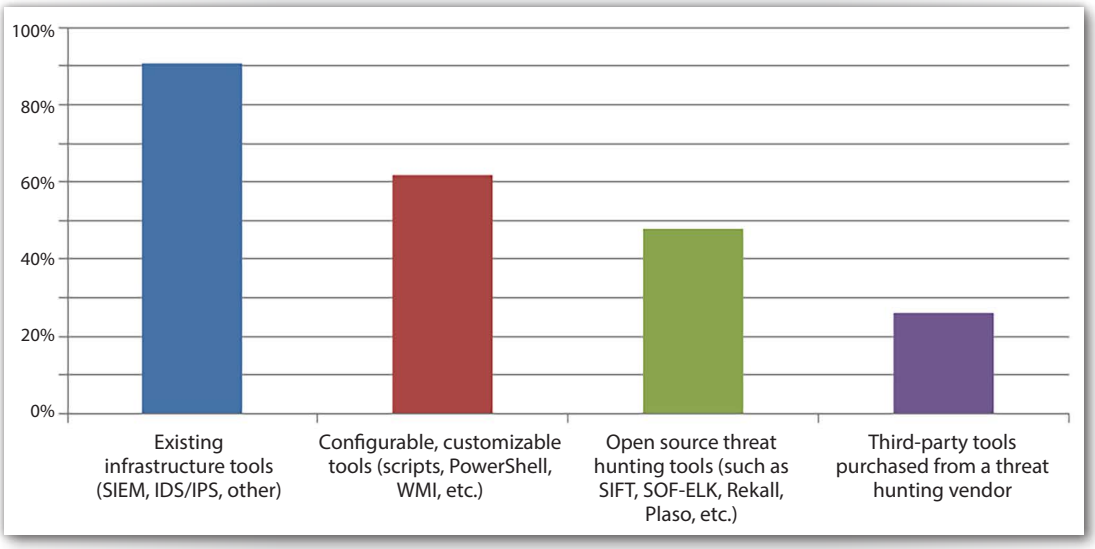

Figure 7. Threat Hunting Tools

Most organizations initially lack the capability to detect advanced adversaries, even when leveraging the capabilities listed in Figure 7. Initially, most operations teams are treating hunting as an aggressive SOC exercise using detection signatures. Because most adversaries emulate normal users, signatures typically do not detect them. To succeed, any organization would need a properly tuned and baselined security environment and the ability to reduce the number of false positives likely encountered.

New tools and capabilities are being developed that will enable threat hunters to utilize existing infrastructure data they're already collecting and identify systems for more proactive inspection. For example, a common technique used in threat hunting is called data stacking. Data stacking pulls similar data across hundreds of endpoints in a network to identify whether there are anomalies present on just a few systems.

For example, a hunter might use data stacking to examine which processes are started up at boot on similar workstations across a specific business unit in organizations. Anomalies found by this technique are usually less prone to false positives. For example, most of the startup programs should be similar on each workstation endpoint. If one of the systems has a few services not found on the rest, it might warrant a closer inspection.

Hunting Automation: Fully Automated or Semi-Automated?

Automation is such a misunderstood word, especially in the context of threat hunting. Hunting needs capabilities to help enhance speed, accuracy and effectiveness. The best hunting teams heavily leverage automation to aid in increasing the scale and efficiency of hunts across the enterprise. However, by its definition, hunting is best suited for finding the threats that surpass what automation alone can uncover. Threats are, after all, moving targets. Still, it is important to recognize the intertwined nature of automation and the human process of threat hunting.

Tools and capabilities that aid threat hunting are SOC driven. Traditional information security architecture such as SIEM analytics, log file analysis, intrusion detection and antivirus are largely automated capabilities based on signature-based rules fed and maintained by analysts. When you begin to introduce hunting concepts using these capabilities, they often record, identify and possibly ignore small anomalies that often are the barely visible tracks of advanced adversaries. Ignoring these trivial anomalies is easy because there are too many to properly vet in even a modest-sized network. After discovery, most security teams realize that their sensors did, in fact, record the adversaries' activities. At the time those alerts occurred, however, the teams were too overwhelmed to pay any attention to them.

These capabilities can be enhanced greatly by utilizing threat intelligence effectively. With proper intelligence, additional threat indicators of compromise and the right analysts using properly tuned tools, some seemingly benign alerts would be identified as major events. Threat hunting, threat intelligence and security operations can move together in harmony.

Of the survey respondents, 16% say they are using threat hunting via fully automated alerts. The number of fully automated hunting capabilities actually in use is a small percentage and is likely tied directly to the fact that hunting is difficult to automate across the many processes and human functions still involved. The majority of respondents stated that their threat hunting capabilities are semi-automated or not automated at all, as shown in Figure 8.

Does your threat hunting system currently generate automated alerts and perform pattern matching?

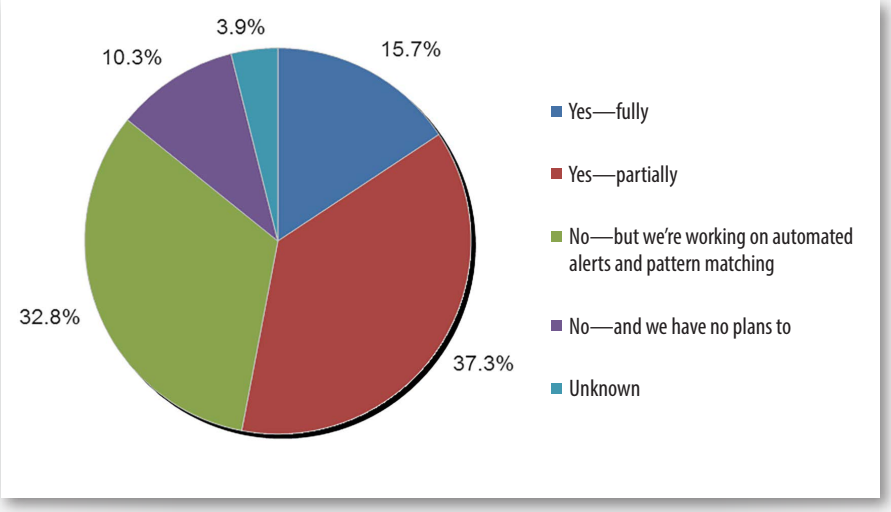

Figure 8. Automation of Alerts and Pattern Matching

The lack of true automation highlights the idea that it is a challenge to fully automate threat hunting. Such a realization brings to the forefront that over-reliance on standard SOC reporting tools such as SIEM/IDS tends to skew reports of hunting effectiveness because they aren't hunting—they are performing intrusion detection. Having said that, SIEM/IDS data can be used to help identify anomalies in hunts.

Tool and Capabilities Focus Recommendations

- **Core technologies**—SIEM and analytics, continuous monitoring of endpoints and network
- **DFIR technologies**—Scalable analysis capabilities that can examine multiple endpoints simultaneously
- **Cyber threat intelligence feeds**—Both internal and external needed
- **Personnel and training**—Trained talent required for hunting

While we applaud automation in increasing the speed, scalability and accuracy of threat hunters, understand how much you should automate. Consider seeking tools to enhance and scale hunting activities, but not drive them. It is more appropriate to invest heavily in threat intelligence feeds and in training and hiring skilled personnel than it would be to seek capabilities that claim they can fully automate hunting activities.

A Choke Point?

In the survey, 77% of respondents said endpoint data was critical for conducting hunts, and 73% selected access and/or authentication logs. Threat intelligence feeds, including vendor and information sharing and analysis center (ISAC) feeds, are rated in the middle of the types of data feeds needed for hunting, being selected by only 64% of respondents, which also shows that targeted and specific hunts are not being done by respondents because targeted hunts cannot be accomplished without threat intelligence. Targeted hunting with threat intelligence has proven, especially recently, to reduce the dwell time of adversaries in networks, leading to more efficient identification of threats. See Figure 9.

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

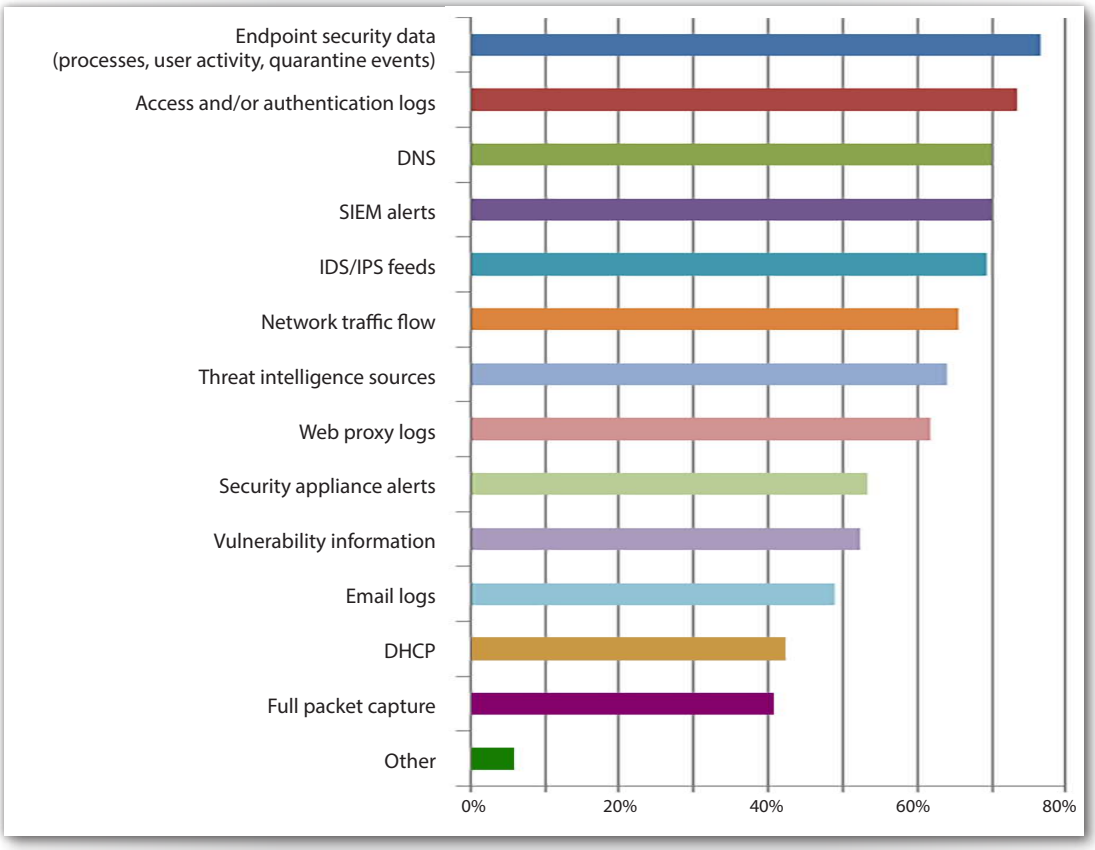

Figure 9. Critical Data Feeds

While endpoint security data rated high on what is needed, endpoint-related data rated lower on the overall scale of what is actually being collected. Just 71% collect endpoint artifacts and patterns. Another 58% gathered file monitoring data, and 42% monitored user activity. Because many advanced persistent threats (APTs) replicate standard users and credentials, effective threat hunting is limited by the difficulty in detecting activity based on network data alone. The lower numbers in endpoint analytics collected when compared to what respondents believe is needed show that many respondents feel that endpoint data is more obscure and harder to obtain. See Figure 10.

TAKEAWAY:

Most organizations do not have a clear capability to examine endpoints at scale effectively. It takes too long to analyze system after system independently. Newer technologies that can help scale analysis of endpoints across an enterprise have only existed for a few short years and have not yet made a large impact on the community.

What specific collections of data do you collect and analyze during hunt missions?
Select all that apply.

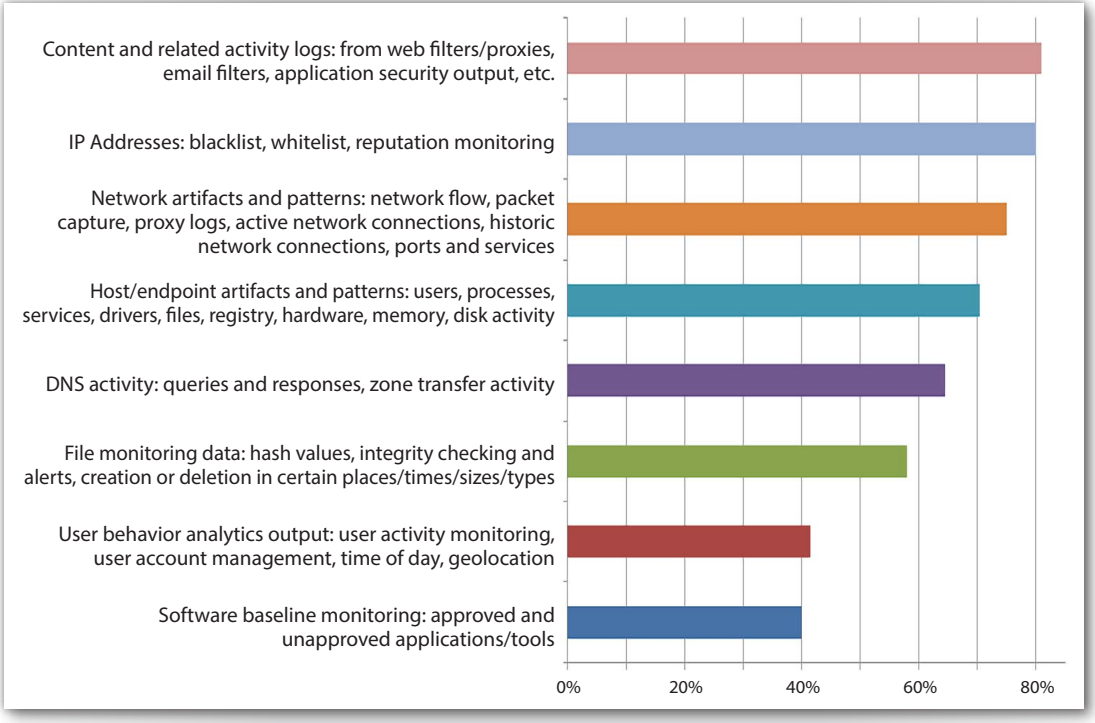

Figure 10. Data Collected and Analyzed During Hunts

TAKEAWAY:

Each hunt has its specific objectives, and the information sources differ with each specific objective. Security monitoring is the overall process, whereas hunting is specific and targeted, based on the perceived risk.

Although network data-based data collections were rated high on the survey, endpoint analysis data is still a gaping hole in most hunting operations.

Logfile data across multiple hosts can already be easily ingested into SIEM and other analytical systems. Because it is easier to obtain, the more critical systems you can pull logfiles from, the better the horizon view across an organization. It is often a good idea to log allowed traffic as well as denied or anomalous traffic, since malicious activity, such as data exfiltration, often masquerades as legitimate traffic. Logfile analysis gives perspective into unauthorized credential access, lateral movement by adversaries and malware execution on systems. When collected from multiple systems, logfile analysis can be used to identify anomalies through systems that are not acting in the same manner as the others in your baseline comparisons.

Threat Hunting Can Improve Security

Respondents indicate that, despite the immaturity of their threat hunting efforts, the efforts are paying off. In the survey, 60% felt their use of threat hunting provided measurable improvement in the security of their organizations. Yet, interestingly, 36% stated they were unsure and only 3% said no.[4]

There are many legitimate reasons a respondent might not be sure about how threat hunting adds to increased security. Some respondents may be early on in adopting a new threat hunting program and unable to provide an answer yet. Others may simply not feel they have the quantitative data to conclusively support an answer. However, it is important to develop metrics to assess the value of security endeavors. Many organizations will take this a step further and develop key performance indicators (KPIs) to determine long-term value, changes and opportunities for improvement.

The survey attempted to extract insight about what some of those improvements might be, based on some common KPIs used by others across the security industry. Specifically, the survey sought to determine whether there was:

- No improvement
- Some improvement
- Significant improvement
- Total improvement (Some + Significant)

This was done across the following areas:

- Speed and accuracy of response
- Attack surface exposure/Hardened network and endpoints
- Reducing dwell time (infection to detection)
- Time to containment (detect/prevent spread or lateral movement)
- Amount of actual breaches based on the number of incidents detected
- Exposure to external threats
- Resources (e.g., staff hours, expenses) spent on response
- Reducing frequency/Number of malware infections
- Other

[4] Percentages don't add up to 100% due to rounding error.

The results indicated that for those respondents who found an improvement in threat hunting, there was improvement across each of the indicated areas for at least 74% of the participants. The highest total improvement areas were the speed and accuracy of response and an improvement in attack surface exposure, with 91% of respondents experiencing improvement in both of these areas, as shown in Table 2.

Table 2. Improvements Attributed to Threat Hunting

Answer Options	No Improvement	Some Improvement	Significant Improvement	Total Improvement
Speed and accuracy of response	4.2%	51.7%	39.2%	90.8%
Attack surface exposure/ Hardened network and endpoints	5.8%	47.5%	43.3%	90.8%
Reducing dwell time (infection to detection)	6.7%	54.2%	34.2%	88.3%
Time to containment (detect/prevent spread or lateral movement)	8.3%	46.7%	40.0%	86.7%
Amount of actual breaches based on the number of incidents detected	12.5%	56.7%	27.5%	84.2%
Exposure to external threats	13.3%	52.5%	30.8%	83.3%
Resources (e.g., staff hours, expenses) spent on response	17.5%	49.2%	29.2%	78.3%
Reducing frequency/ Number of malware infections	22.5%	44.2%	30.0%	74.2%
Other	14.2%	7.5%	3.3%	10.8%

TAKEAWAY:

The intent of hunting is not directly aimed at making attack exposure improvements, but the byproduct of threat hunting may lead to this improvement and, thus, help position organizations to better deal with future intrusions.

The first area, speed and accuracy of response, is an ideal metric to help determine whether hunters perform their jobs in an efficient and timely manner, thus reducing the likelihood of persistence by the adversary. The second area, an improvement in reducing attack surface exposure, is an interesting metric, because hunting is focused on adversaries and is not focused on identifying and remediating vulnerabilities, hardening architecture and systems, or tuning passive defenses. However, the fact that over 90% of respondents saw an improvement in this area due to their hunting shows that threat hunting can be successful even without the presence of threats.

The option that saw the least improvement was the reduction in number of malware infections, with 23% of respondents answering that there was no improvement. This naturally makes sense. Defenders often have little control over how many times the adversary will attempt an intrusion or how many times users click on a phishing email. Metrics that demonstrate the adversary has more control than the defender should be given less priority when measuring success. Instead, it's better to focus on metrics where the defenders' improvements can be rated over time, such as the time to containment, which saw a significant improvement response of 40%.

Understand New, Evolved and Known Threats

The survey asked respondents about their understanding of the threats they face and whether over the past 12 months their previously undetected threats were known to existing security systems, unknown (new) or evolved from threat patterns discovered. If the threats were known to existing security systems, there was likely some problem with the system that required tuning. It's good that threat hunting caught those threats, but they should, ideally, represent only a small portion of the activity. However, respondents indicated that the known threats were not significantly different than the new threats. This might indicate that traditional passive defenses in the environment, such as anti-malware systems, need more tuning to facilitate the hunters' focus on new threats.

ADVICE:
Best practice would dictate having a small percentage representing the inability to determine whether discovered threats are new, known or evolved from known threats. Aim for less than 15% of cases where teams cannot determine whether the threat is new or not.

In a different way of wording the problem, respondents indicated that, for a significant portion of what was uncovered, they simply did not know whether it was new, known or evolved, as indicated by the 30%, 27% and 41% selection of "unknown" in each category. See Figure 11.

Over the past 12 months, how many previously undetected threats did you find by actively searching for threats? How many were known to existing security systems, and how many were previously unknown (new) or evolved from other threat patterns?

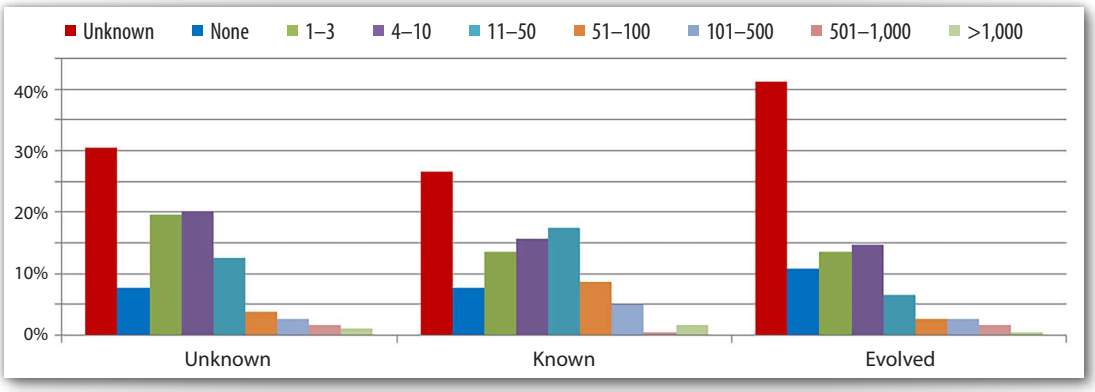

Figure 11. Detection of Previously Unknown Threats

Organizations should ensure that the teams performing threat hunting are doing so on top of an environment that best suits this type of work. That means making proper investments in architecture and passive defenses to make the environment more defendable. Additionally, the environment should facilitate visibility, and use of threat intelligence should be tailored to help teams answer questions about whether or not the threat is new, known or evolved from known threats.

Proactive Approaches Best

Each year various industry reports indicate that the time to detect or uncover threats in their environments ranges from days, to weeks, to a year or more.[5] The average usually hovers around a couple of weeks or months. In this survey, more than 50% of the respondents detected serious threats in under 24 hours, with 20% detecting within 8 to 24 hours, and 28% needing 1 to 8 hours to detect a threat. Another 12% said they detected threats in under 1 hour. That is phenomenal. Likewise, responding to the threats once uncovered similarly followed the detection pattern with more than 50% of response actions taking place in less than 24 hours after detection. See Figure 12.

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?

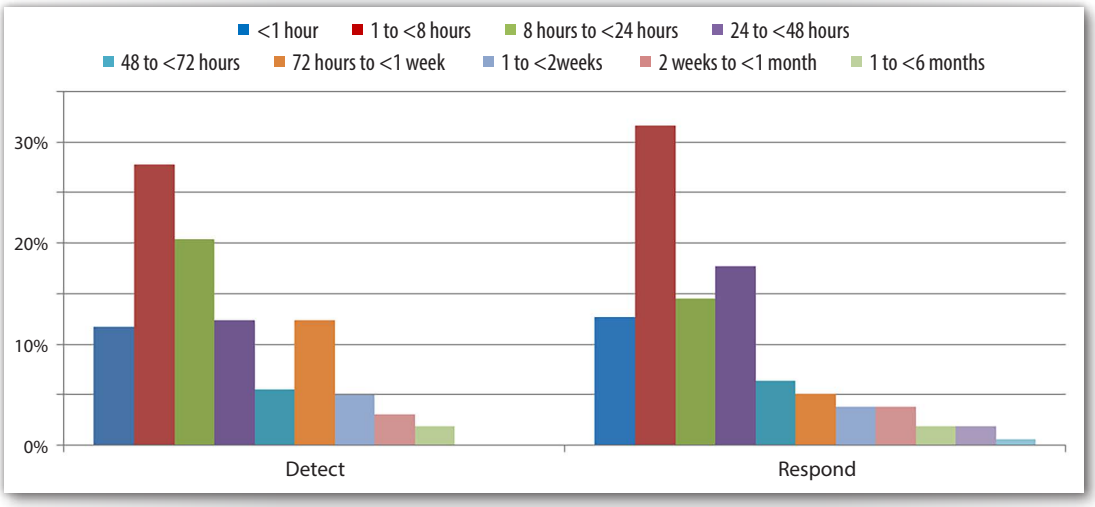

Figure 12. Threat Hunting Detection and Response Times

It is important to understand the phrasing of the question to fully appreciate the value. The question specifically asked participants how long it took them to uncover serious threats from the time they started to look. This means that many of those threats could have still been in the environment for much longer. Just because an organization has a threat hunting team does not mean it automatically gets to benefit from such industry-leading detection times. The threat hunters must be empowered to search out these threats and be allowed to focus on hunting, not on menial security- or organization-related tasks.

[5] "2016 Data Breach Investigations Report," www.verizonenterprise.com/verizon-insights-lab/dbir/2016

People, Process and Technology Needed

There can never be perfect security, so organizations must balance the right investment in people, process and technology to achieve their right level of security. How much of that investment should be leveraged toward threat hunting? The vast majority of respondents indicated they would be making more investment in threat hunting personnel, tools and capabilities over the next 24 months. Overall, 65% of participants indicated their organizations would make additional investments in threat hunting, with increases of 10%, 25% and 50% capturing 21%, 23% and 15% of the responses, respectively. Only 6% indicated organizational reductions in investment in threat hunting. Another 30% believe they have found a proper fit where they are now and do not anticipate a change in their investment.

The No. 1 choice for where respondents would invest more resources, with 49% of respondents putting it in their top three, was the improved ability to search through data and information. Given the large amounts of data organizations have to sift through to identify malicious activity, this is a very reasonable request. The second most popular choice, with 48% of respondents including it in their top three, was the ability to connect the dots between disparate sources of information and indicators of compromise. The third most popular choice, with 47% of the community including it in their top three, was more staff with investigative skills to conduct searches. The fourth highest rated wish was better detection, chosen by 46%. It is unsurprising that the least popular choice was better storage. Most teams have found themselves with a plethora of data but not enough time in the day to search through it. See Figure 13.

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

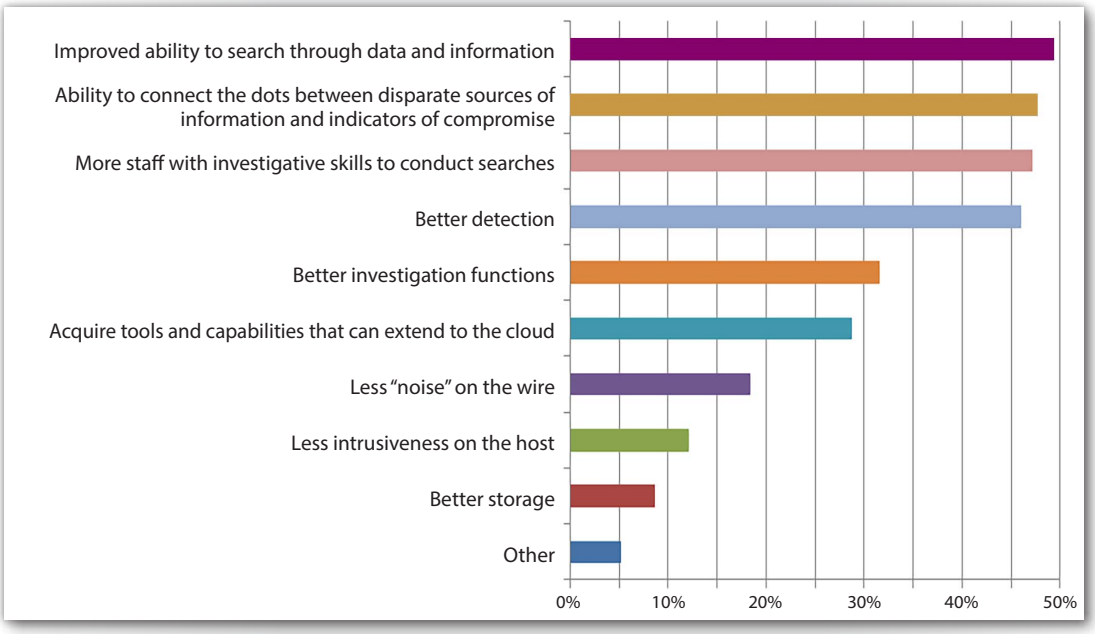

Figure 13. Desired Improvements in Threat Hunting Tools and Capabilities

These improvements all rely on the triad of people, processes and technology. Improved search capabilities can be a technology problem, where better leveraging of analytics and machine learning could help. But better trained individuals following predefined processes are going to be more efficient with the searches conducted. In the same way, the ability to connect the dots better speaks more to analytical processes and approaches to the problem, with the right people leveraging the right technology. The desire for more people with investigative skills is found throughout the industry. There simply never seem to be enough people. Technology, processes and training will continue to help you make the best use of your personnel.

Conclusion: Leverage It Wisely

The 2017 Threat Hunting Survey polled members from around the community on various topics, including the effectiveness, approach and investment in hunting. Results make it clear that threat hunting is a newer discussion in the larger information security community, but an effective one. That discussion is, however, somewhat muddied by the lack of a clear understanding of where incident response ends and threat hunting begins.

Organizations are beginning to take a proactive approach to threat hunting, taking security into their hands instead of waiting for the breach notice to come across the wire. More organizations need to take that leap. And, they are starting to understand that any threat hunting approach can only be partially automated. In fact, the act of threat hunting leverages the results of automation, but it truly begins where automation ends. Organizations need to ensure that they have appropriately trained staff to provide the needed services. IR team members are the logical ones to tap and expand their knowledge base to engage in threat hunting.

Increased investments will be made in this space. That means there will be organizations, teams and individuals coming forward with tools, people and processes that work for them but that may not be well suited for all environments. It is of paramount importance that teams looking to build a threat hunting capability educate themselves appropriately so they can make wise investments.

About the Authoring Team

Rob Lee is the curriculum lead and author for digital forensic and incident response training at the SANS Institute. With more than 15 years of experience in computer forensics, vulnerability and exploit discovery, intrusion detection/prevention and incident response, he provides consulting services in the Washington, D.C. area. Before starting his own business, Rob worked with government agencies in the law enforcement, defense and intelligence communities as a lead for vulnerability discovery and exploit development teams, a cyber forensics branch, and a computer forensic and security software development team. Rob was also a director for MANDIANT, a company focused on investigating advanced adversaries, such as the APT, for five years prior to starting his own business and co-authored *Know Your Enemy: Learning About Security Threats*, 2nd Edition.

Robert M. Lee, a SANS certified instructor and author of the "ICS Active Defense and Incident Response" and "Cyber Threat Intelligence" courses, is the founder and CEO of Dragos, a critical infrastructure cyber security company, where he focuses on control system traffic analysis, incident response and threat intelligence research. He has performed defense, intelligence and attack missions in various government organizations, including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Author of *SCADA and Me* as well as *Threat Intelligence and Me* and a nonresident National Cyber Security Fellow at New America, focusing on critical infrastructure cyber security policy issues, Robert was named EnergySec's 2015 Energy Sector Security Professional of the Year and one of Forbes' 30 under 30 (2016).

Sponsor

SANS would like to thank this survey's sponsor:

Malwarebytes