

# SANS 2020 Threat Hunting Survey Results

A SANS Survey

# SANS 2020 Threat Hunting Survey Results

Written by **Mathias Fuchs**
and **Joshua Lemon**

December 2020

*Sponsored by:*

**Analyst1**
**Anomali**
**BlackBerry**
**Cisco Systems**
**Corelight**
**DomainTools**
**Secureworks**
**Sophos Inc.**
**Swimlane**
**ThreatQuotient**

Analyst Program

# Executive Summary

This is SANS' fifth year of conducting the Threat Hunting Survey to examine how the cybersecurity industry is currently supporting threat hunting and how security professionals are conducting threat hunting in their organizations. Our goal is to better understand where we currently are in the development of the threat hunting field and to provide guidance on where the industry should focus its efforts as it continues to move the needle to favor defenders. Based on the results from the 2020 survey, this paper will provide an informed view on what the data tells us and where we need to focus our future threat hunting efforts.

This year, the number of organizations using threat hunting as a form of compliance or a checkbox activity continued to increase. We examine why this is concerning and what risks it can pose to an organization. Results show that threat hunting teams are starting to formalize their processes and procedures, a trend that is moving in the right direction for the industry overall.

For this year's survey, we changed some of our previous survey questions to better understand the makeup of threat hunting teams and how they are performing their work—be it with tooling, staffing, or capabilities. We wanted to take a dive deeper into how threat hunters are fulfilling their missions, which tools they are selecting, and why they are using certain tools or procedures. Our hope is to continue this trend to see how threat hunters' views, along with the technology and education of threat hunters, change over time.

As a result of our updated survey questions, we found that performing threat hunting is not the primary task for a significant majority of threat hunting team members and looked at what other roles these team members fulfill when not hunting. We also examined how respondents apply threat intelligence to their hunting and discovered a significant gap in the use of automated tools to aid in the curation of useful and applicable threat intelligence.

Outside of intelligence, we found that the gap between threat hunting tools and tools used in the SOC is narrowing to the point of almost merging. This includes the correlating data and gathering external sources and references. Targeting tactics, tools, and procedures (TTPs) for hunting malicious actors within a network, however, is one process that puts threat hunting teams well outside of the function of the SOC. We saw a positive rise in hunting teams using TTPs to chase down threat actors.

The survey also improved our understanding of the usefulness of hunting for vulnerabilities or unknown misconfigurations in an environment. With the increased media attention given to threat actors leveraging vulnerabilities, we wanted to understand if this was a focus area for threat hunting teams already.

In this paper we've included not only our findings, complete with raw results and trends, but also recommendations of how organizations can further push the boundaries of threat hunting and better defend their networks from threat actors. Figure 1 (on the next page) provides a snapshot of key demographics for the respondents to this survey.

### Key Findings

- **52%** of organizations find value in looking for unknown threats
- **48%** of hunt teams are storing threat intelligence in unstructured files (e.g., PDFs, text files, spreadsheets)
- **75%** of threat hunting staff perform other key functions in their organization
- **43%** of hunting teams are using automated solutions for threat hunting
- **53%** of organizations are using ad hoc methods to measure the effectiveness of threat hunting

### Top 4 Industries Represented

- Cybersecurity
- Banking and finance
- Government
- Technology

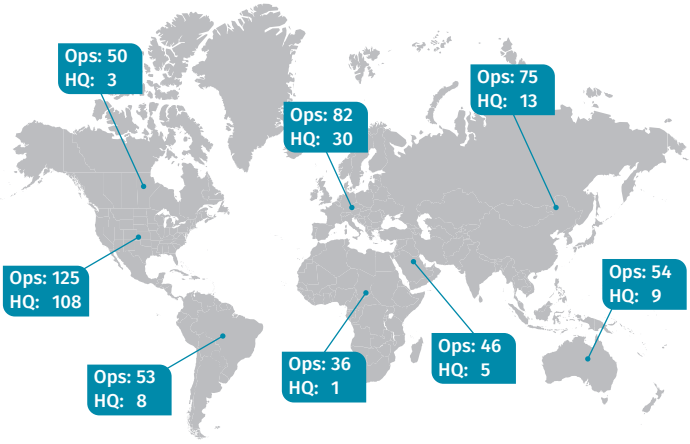
*Each gear represents 10 respondents.*

### Organizational Size

- **Small** (Up to 1,000)
- **Small/Medium** (1,001–5,000)
- **Medium** (5,001–15,000)
- **Medium/Large** (15,001–50,000)
- **Large** (More than 50,000)

*Each building represents 10 respondents.*

### Operations and Headquarters




### Top 4 Roles Represented

- **Security administrator/ Security analyst**
- **Threat hunter**
- **Incident responder**
- **Security manager or director**

*Each person represents 10 respondents.*

*Figure 1. Survey Demographics*

## What Does Threat Hunting Mean to Organizations Today?

The definition of *threat hunting* is still a very controversial topic in 2020. Whenever introducing new strategies to find evil, there are various methods. Some organizations define how their threat hunting operations need to work and build up teams to meet those goals. Unfortunately, others continue to use the still-quite-common approach of running threat hunting operations with the tools and data the organization already has. Instead of defining goals that threat hunting needs to meet to succeed in providing maximum value to the organization, those organizations define threat hunting to ensure that they can claim that they have some form of threat hunting. While that approach might still render results, they will not be as tangible to the organization or its security posture. We frequently see this at compliance-driven IT organizations. Some standards require them to have threat hunting in place, which urges them to set up a form of threat hunting to tick that box.

A successful threat hunting strategy comes with having a clear goal and well-managed resources to meet that goal, not simply some warm bodies to meet a checkbox requirement.

To better understand the forms of threat hunting our respondents implemented, we asked if and how they implemented threat hunting.

Only 15% claimed they don't execute any form of threat hunting today, while another 12% said they at least plan to implement it in the foreseeable future, as shown in Figure 2. In the 2018 Threat Hunting Survey Report,[1] only 75% of respondents claimed they had threat hunting in place, meaning that this year's respondents reported an increase of 10 percentage points in organizations implementing threat hunting, which we perceive as an excellent trend.

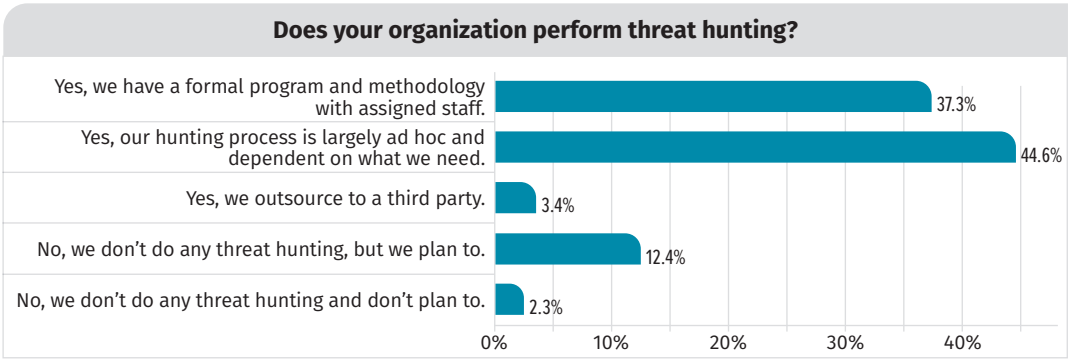



*Figure 2. Threat Hunting Operations*

Almost half (45%) of respondents run an ad hoc hunting process that is dependent on their needs. That makes it more difficult to have dedicated resources for threat hunting and leads to less consistent results. Also, the majority of respondents measure the success of threat hunting on an ad hoc basis, making it even more difficult to get numbers that justify employing a sufficient number of dedicated threat hunters.

In this year's survey, the silver lining is that 37% of respondents claimed to have a formal program and methodology with assigned staff for threat hunting. We consider this a massive leap forward for threat hunting as an established part of many organizations' security postures. An increase in professional threat hunting teams can significantly impact many aspects of organizational security and the security product market through:

- Improving detection with feedback to the SOC from skilled threat hunting teams
- Influencing buying decisions, thus challenging tools and intelligence vendors to sell less vaporware
- Supporting SOCs in identifying dangerous visibility gaps and avoidable detection gaps
- Discovering vulnerabilities, even though that is not the hunting team's primary goal

## Dedicated Threat Hunting Teams vs. Multifunction Roles

For most organizations, threat hunting is not a full-time role. Some organizations either fully outsource the function, because they may not have staff with the appropriate skills or capacity, or staff members have other functions and perform threat hunting during quieter periods. This year, we wanted to better understand the model respondents are using to support threat hunting activities. Just 19% of respondents are working as full-time threat hunters at their organizations, and 75% are using staff that also fulfill other roles within the organization.

[1] "SANS 2018 Threat Hunting Survey Results," September 2018, www.sans.org/reading-room/whitepapers/analyst/2018-threat-hunting-survey-results-38600 [Registration required.] Percentage is from the survey data not included in the report.

It is not surprising that many respondents are also relying on other roles within their organizations to perform a threat hunting function. This can be a reasonable approach depending on the size of the network you need to cover and the available resourcing. In some circumstances, pulling staff out of some of the higher-stress roles—such as incident response or reparative functions, including detection tuning or triage—creates a healthier balance of work tasks. This year's research showed that, when they aren't focusing on threat hunting, 75% of respondents are focusing on incident response or forensics. Just over half (51%) performed a security architecture/engineering role, and a little over a third (37%) performed system administration functions. See Figure 3.

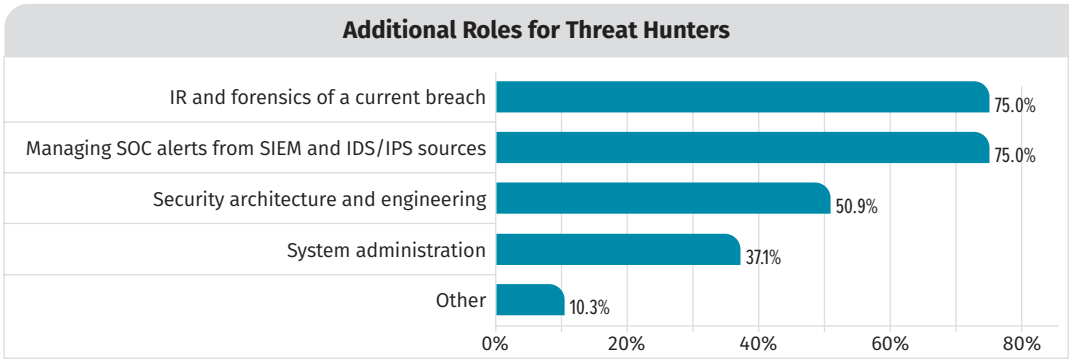



*Figure 3. Additional Roles to Threat Hunting*

The approach of tasking technically knowledgeable staff to perform threat hunting can have a significant benefit and, in some cases, be even more beneficial than using third parties. Leveraging staff who have deep knowledge of your environment means they can see when something does not seem right. This type of skill can greatly increase the speed at which hunters find anomalies. Our only caution: Ensure that you give staff members dedicated time to conduct the hunt—so they can complete the mission and not have to abandon it partway through to complete something else. This also applies to the 75% of organizations that are using incident response staff for hunting. While it is a perfect match in skills, ensure that your hunters continue to hunt. Even if they uncover an incident, the incident should be handled by a different team—so the hunters can complete their mission. This type of focus can also speed up the scoping phase for the incident response team if you do uncover an incident.

> Staff wearing multiple hats for security operations works only if they wear one at a time. If you're juggling multiple hats, you've just become a clown.

## Views on Threat Hunting and Incident Response

Last year's[2] and this year's Threat Hunting Surveys showed that incident responders frequently double as threat hunters. Figure 4 shows that dedicated threat hunters are still the exception rather than the norm. Why is that, and is it a good idea?

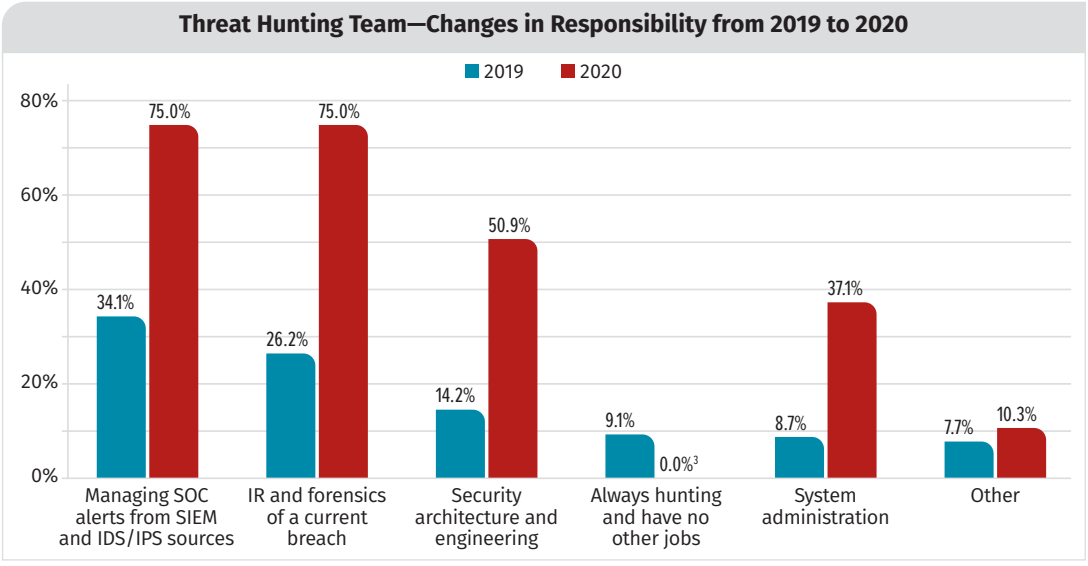



*Figure 4. Year-Over-Year Changes in Threat Hunters' Other Roles*

[2] "SANS 2019 Threat Hunting Survey: The Differing Needs of New and Experienced Hunters," www.sans.org/reading-room/whitepapers/analyst/2019-threat-hunting-survey-differing-experienced-hunters-39220 [Registration required.]

[3] No 2020 respondents indicated that their threat hunting teams had no other jobs.

To answer that question, we need to focus on the commonalities and differences between threat hunting and incident response. While threat hunting comes in various shapes and forms, the most sophisticated way of threat hunting is hypothesis-based hunting. In this case, the hunter envisions an attack scenario that might have happened in the organization. That scenario leads to a hypothesis that subsequently must be tested. Testing that hypothesis usually requires intimate knowledge about the suspected attack path as well as the right tool set and visibility to either accept or reject the hypothesis.

Incident responders usually know that an attack occurred and start their investigation with limited knowledge about the attack path. This results in incident responders extending their knowledge about the attack and establishing visibility to investigate further. The tools and techniques needed for this analysis overlap broadly between incident response and threat hunting. For that reason, it tends to be beneficial to use incident responders when building up threat hunting operations. Over time, the threat hunting organization will be able to transform into a dedicated threat hunting team. Even then, they'll still need input from various other entities such as the SOC, IR, and threat intelligence teams.

Because we observed the results on how common it was for organizations to have threat hunting teams made up by members of other teams, we wanted to understand how common it is for organizations to have dedicated threat hunters and what techniques they most often apply.

The majority (73%) of respondents have staff that are allocated to a threat hunting team, while only 18% have no allocated threat hunters at all. The remaining 9% don't know whether they have a dedicated team at all, which is somewhat concerning. So, the numbers indicate a certain professionalization of threat hunting within respondents' organizations. Now that we know that there are many staff within an organization allocated to threat hunting, how do they usually perform a hunt mission? A majority (61%) use threat intelligence, such as adversary TTPs, to hypothesize where attackers might be found.

So, almost two-thirds of respondents have arrived at the top of the pyramid regarding threat hunting techniques. Still, over 50% claim that reacting to an alert initiates their threat hunting efforts, which technically doesn't qualify as threat hunting.

## Conducting Searches for Threats or Indicators of Compromise (IoCs)

Ideally, as security software and SOCs evolve, the gap between successful attack techniques and detection capabilities should decrease, making threat hunting obsolete—something the detection industry regularly promises. That's a suggestion we don't see coming true anytime soon.

What are some of the shortcomings of automated alerting tools that threat hunting can iron out? If we boil it down to the bare minimum, two factors give SOCs and their tooling a hard time in their efforts to detect threats: thresholds and context.

Automated alerting technologies detect many suspicious data points every day. To limit alerts to a manageable amount, certain thresholds need to be in place. If they are set too low, the number of alerts will overload analysts with false positives, inevitably leading to alert fatigue. In that state, analysts start missing true positives. If the threshold is set

too high, true positives will be filtered out. The ugly truth is, no matter how thresholds and filters are set, there will always be false positives in the alerts, and there will always be true positives that were filtered out. These filtered-out true positives are why threat hunting is so essential.

The second shortcoming of automated alerting tools, context, can now be addressed by many Security Orchestration, Automation and Response (SOAR) tools. The typical organization has a multitude of potential alerting and enrichment sources in place. A SOAR ties them together and helps define an individual alert's criticality, giving more context by linking data from various sources. Threat hunters can significantly contribute to design and extend semi-automatic runbooks that define how SOAR solutions handle enrichment actions and the classification of alerts.

Threat hunting also significantly augments a SOC because testing a hypothesis can have three results:

- The hypothesis can be accepted and become an incident response case.
- The hypothesis can be rejected, so no action is needed.
- The hypothesis could neither be accepted nor rejected because the threat hunters couldn't get the data required to make an informed decision.

If the available tools and data sources are not sufficient for the threat hunters, they will be insufficient for the SOC. This potentially leads to considerable gaps in the SOC's detection capability and an incident response team's visibility.

In threat hunting, it is possible to set thresholds very low for a very narrow set of artifacts needed to test the hypothesis.

## Using Automation and Enrichment

One of the critical factors for successful threat hunting is losing as little time as possible in compiling data. As mentioned previously, if data is not available for the threat hunting team, it'll also be missing for the SOC, hence opening visibility gaps. For this reason, it's important to store and curate data from internal and external sources carefully. Once data has been compiled and visibility established, good documentation is another crucial point to reduce efforts in subsequent hunts.

When asked how organizations prepare for threat hunting, 60% of respondents (the most common response) indicated they prepare by providing external enrichment sources to SOC and alerting systems, as shown in Figure 5. Assuming the same sources are available to threat hunters, this is an easy and beneficial first step for automation. There's little use in having threat hunters check every single hash they come across on the reputation source's website.

**How has your organization prepared for threat hunting?** ***Indicate whether you are performing this currently, planning to do so in the next 12 months, or have no plans.***

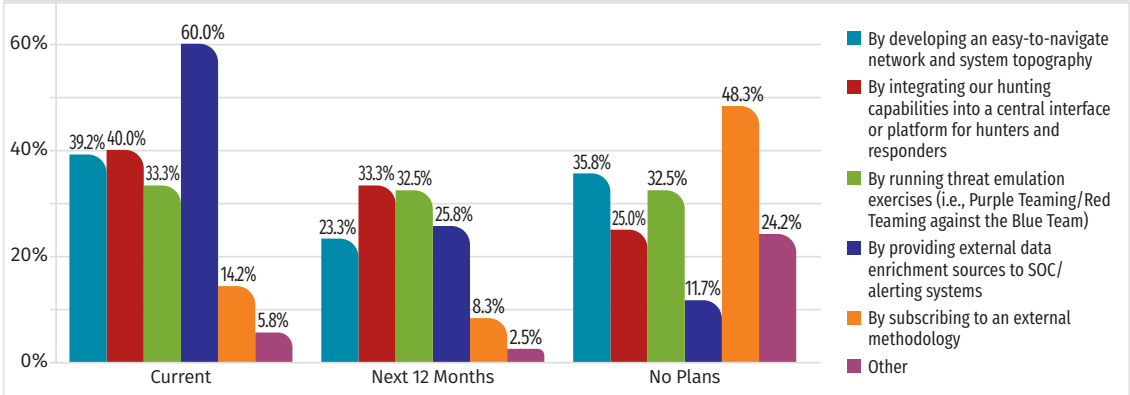



*Figure 5. Preparing for the Hunt*

With 40% of respondents integrating their hunting capabilities into a central platform for hunters and responders, results indicate how closely interconnected SOC and threat hunters are, despite being two different units.

The third current means of preparing, used by 39% of respondents, is to start by developing an easy-to-navigate network and system topography that supports SOC, threat hunting teams and, ultimately, incident responders, thus giving them contextual awareness. One of the significant challenges when investigating breaches is to establish an overview of the networks and assets. If that information already exists in a quickly usable form, it's a good start.

A third of respondents (33%) prepare by running threat emulation exercises. While that does not immediately give the respondents any solution to their tooling and visibility problems, it can highlight important points for improvement.

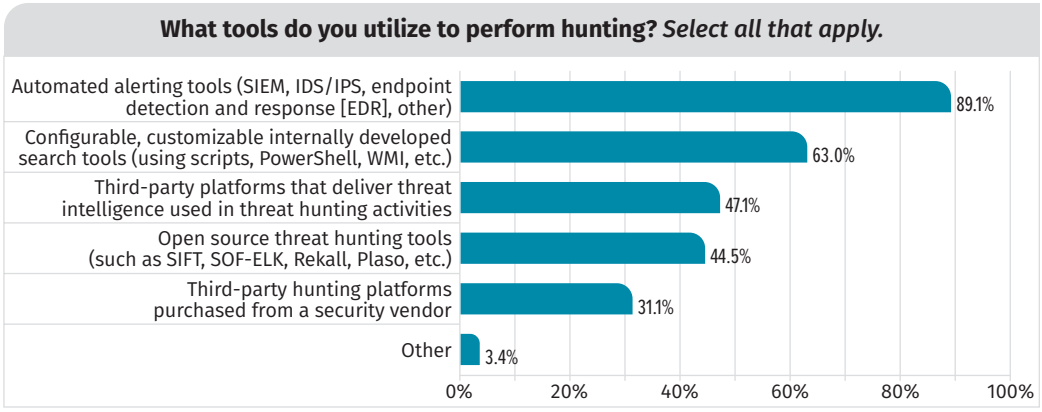



*Figure 6. Threat Hunting Tools*

The survey also explored the tools organizations are using for threat hunting. The majority of respondents (89%) put their trust in SIEMs and endpoint detection and response systems (EDRs), which are usually useful tools to establish visibility if configured correctly. Custom search tools were second, at 63%. See Figure 6.

Third-party platforms come next, with 47% of respondents using them to deliver the threat intelligence used in threat hunting activities. These tools usually support efforts to generate a decent hunting hypothesis. No. 4, open source threat hunting tools such as SIFT, SOF-ELK, Plaso, and others, are used by 45% of respondents.

Only 31% use dedicated third-party threat hunting tools purchased from a security vendor. These numbers imply that organizations are either satisfied with what they already use or that vendors don't currently deliver tools that add enough value for organizations to use them. There are opportunities to improve.

In addition to the tools organizations are using, the survey investigated what data threat hunters look for and how easily they can acquire it. Figure 7 (on the next page) shows that threat hunters mostly work with endpoint data, such as endpoint security data and endpoint process activity. They also seem to be able to obtain these datasets quickly. The biggest hurdle appears to be the collection of and access to full packet captures (PCAPs), with 26% indicating they need these datasets but are unable to get them. While full PCAPs are useful in investigations and threat hunting, they are big chunks of data that are complex to handle and search. The ratio between data and potential findings is worse than it is in carefully collected endpoint data.

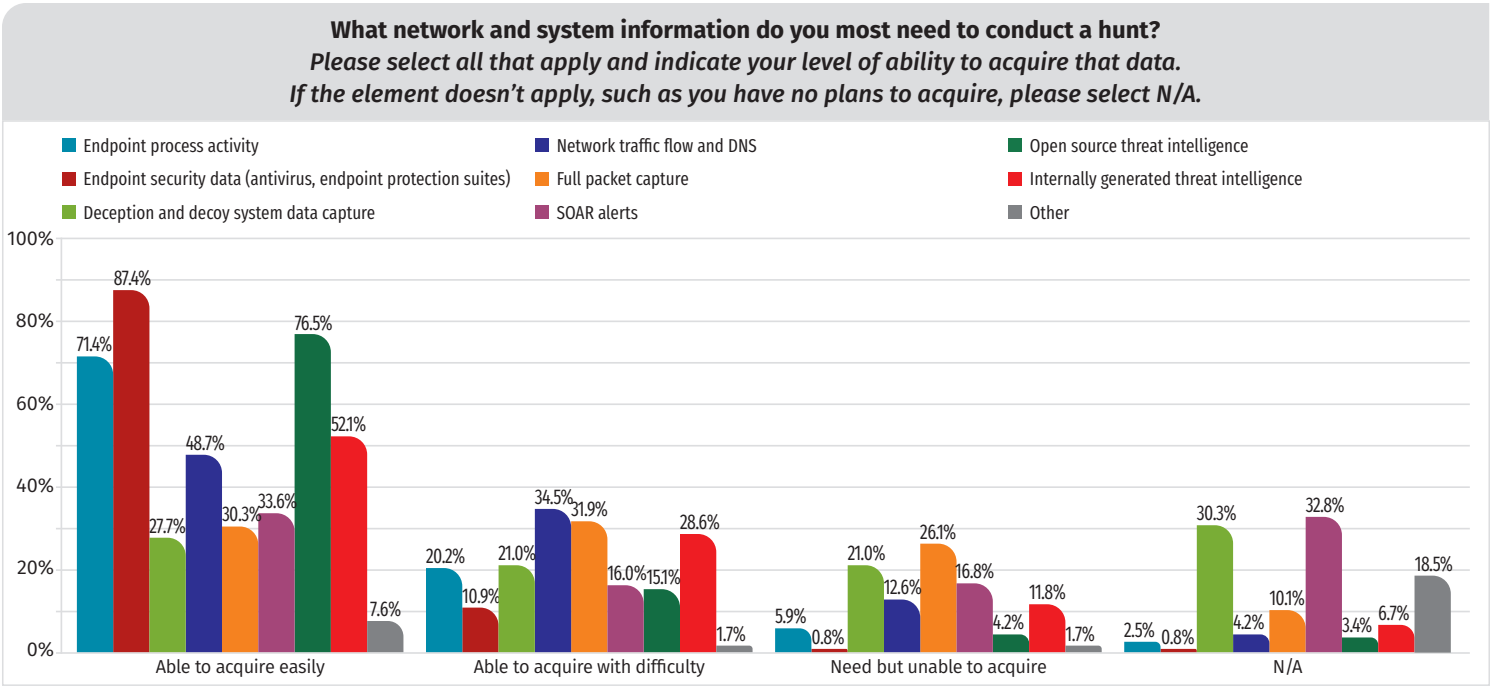



*Figure 7. Information Needed for a Hunt*

Threat hunting and SOC teams can meet many challenges by using and customizing SOAR systems. These systems are meant to reduce context switching, jumping from security system to security system to get a cohesive view on a finding. Context switches come with task-switching costs, as the American Psychological Association points out.[4] That means hunters and analysts will be not only less productive, but also more prone to failure. Of teams using a SOAR or an automation solution built in-house, only 6% said their hunters and analysts can work 100% solely within the SOAR. However, 57% say their teams spend at least 50% of their time within the SOAR.

That is also reflected in what respondents who use a SOAR said is the most-used feature in their SOAR solutions. For 73%, the most-used features are both enrichment of alerts with data sources other than the one that generated the alert and enrichment of alerts with data from intelligence sources. Close behind in use, with 71%, is alert tracking and chaining. Being able to track and link alerts enables teams to use their resources more wisely when working with data and might enable them to correlate SOC alerts and threat hunting hypotheses.

Among respondents who use automation, 49% feel that the tools do what human operators need to assist in their hunts, 25% did not give an opinion on the topic, and only 27% felt that the tools don't deliver what human operators need. In our experience, dissatisfaction often goes back to poor customization or integration of a tool rather than a tool's capability.

[4] "Multitasking: Switching costs," March 2006, www.apa.org/research/action/multitask

# Approaches to Hunting

Collecting threat intelligence from an organization's internal incidents and putting that intelligence into action can enable threat hunting missions to uncover threat actors. As part of this year's survey, we wanted to better understand how organizations are collecting and applying threat intelligence to aid their hunting missions. The ability for an incident response team or threat intelligence team to quickly produce, curate, and store threat intelligence can determine how quickly that intelligence can be operationalized for threat hunting.

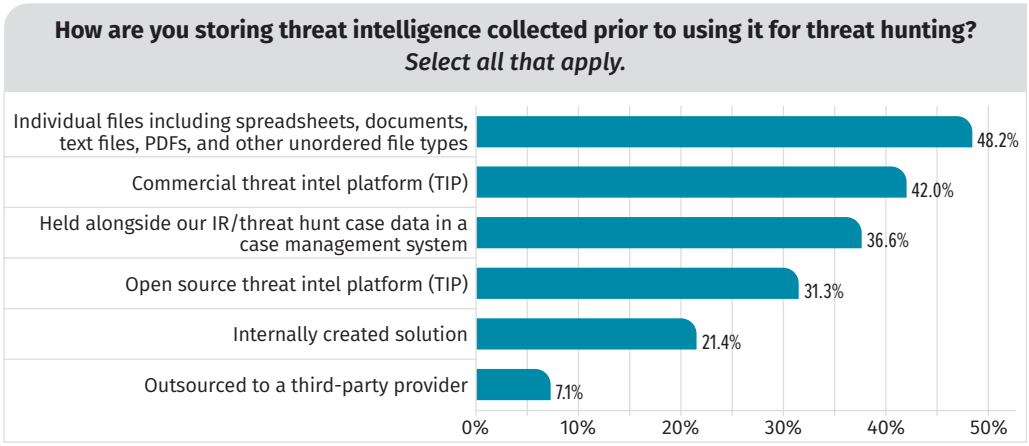



*Figure 8. Storing Threat Intelligence for Hunt Missions*

We asked respondents to tell us about all the ways they store threat intelligence once it's collected. Just under half (48%) indicated that they are using traditional file storage, such as spreadsheets, PDFs, text files, and other unordered file types. That is not surprising, given that this is how threat intelligence has been stored and shared for many years. See Figure 8.

It's reassuring to see there are also a good portion of organizations using either a commercial, open source, or internally developed threat intelligence platform. Of those using a dedicated platform to store threat intelligence:

- 42% use a commercial platform
- 31% use an open source platform
- 21% use an internally developed solution

We also discovered that a higher-than-expected number of organizations (37%) are storing their case data for incidents or threat hunting on the same platform on which they hold their threat intelligence information. In a lot of ways, this makes sense—it is often where you're already collecting and preserving evidence from your incident response cases, so it reduces the number of different platforms or systems that incident response, threat intel, or hunting staff need to move between. It also provides the opportunity for organizations to streamline the correlation between intelligence gathered from previous incidents, threat hunting, and active cases.

A small number of respondents (7%) indicated they outsource their threat intelligence collection to a third-party provider. Following the trend we have seen in the past three years of threat hunting surveys, organizations are insourcing a lot of their cybersecurity operational information and tasks.

## Applying Threat Intel to the Hunt

How organizations are sorting through and operationalizing the intelligence they have for threat hunting is vital to understanding how it is applied. Threat intelligence is as useful as ornaments on a shelf—unless an organization can apply it successfully. We found that most respondents (36%) are manually applying the threat intelligence they have collected, as shown in Figure 9. This result was expected, given that the majority of respondents also said they store threat intelligence in unstructured files, such as spreadsheets, text files, and PDF documents. If 48% of respondents are not storing their data in a structured manner, it would suggest that any hunting would be a very manual process.

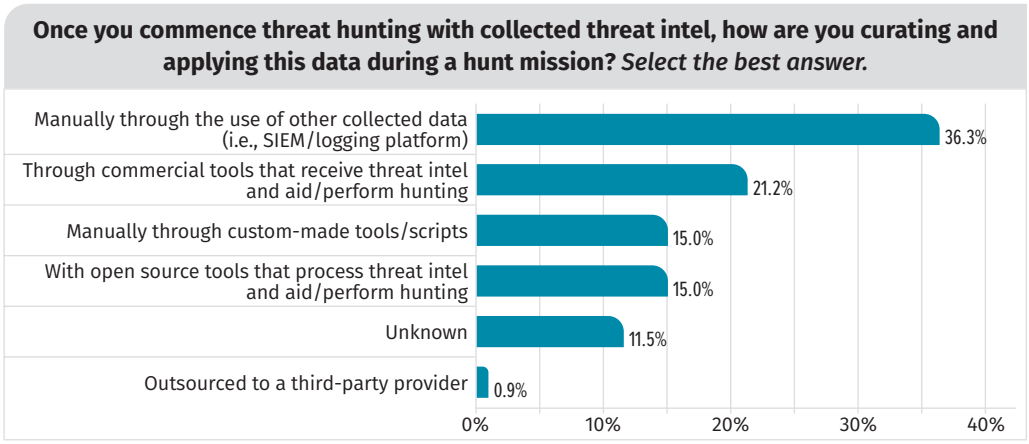



*Figure 9. Applying Threat Intelligence to Hunt Missions*

While threat hunting is intended to find malicious activity that your SOC or alerting platforms cannot, maturing organizations realize that they must leverage automation to reduce threat hunting dwell time. We are seeing a fairly even spread of tooling types, with the organizations that have introduced some automation to aid threat hunting—although only 6% prefer commercial tooling over internally developed or open source tools.

Respondents are using a unique variety of tool types and platforms as part of their threat hunting activities, but a few patterns are worth noting. Organizations that have gone down the path of using a large number of commercial tools often stick to a common brand or supplier, with very little mixing of commercial tools. While this makes sense from a business perspective—in terms of getting discounts, reducing complexity with support, and reducing integration complexity—it can mean getting the right EDR tool but settling for an average log analysis tool or vice versa. On the other hand, organizations that have embraced open source tooling mix many open source tools and various commercial vendors instead of sticking with one common commercial vendor. One final interesting observation is that more organizations than expected are using tool tools such as Jupyter Notebooks for open source visualizations with threat hunting. While there are other open source visualization tools and log collections mentioned, this one in particular was a pleasant surprise given that Jupyter was intended as an interactive execution environment, not a security visualization tool.

## Hunting for the "Hard to Find" Threats

Part of threat hunting is looking for those unknown threat actors that you just haven't caught yet—or your alerting platforms haven't been able to find. Last year's survey found that many organizations were relying more on telemetry they had in a log platform and less on searching for threat actors that are not showing up in their logging systems.

This year, just over half (52%) of respondents indicated that their organizations find it useful to look for unknown attacks in their environment (see Figure 10). Capability and tooling aside, that's a strong response from threat hunting teams indicating that looking for unknown threats provides value to their overall mission of securing their environment. However, we also see that over one quarter (30%) have no idea if there is any value in them hunting for unknown threat actors. This is fairly concerning, because it shows that a large portion of both hunters and organizations either being unable to measure the value of threat hunting or not knowing where or how to start looking for unknown threats.

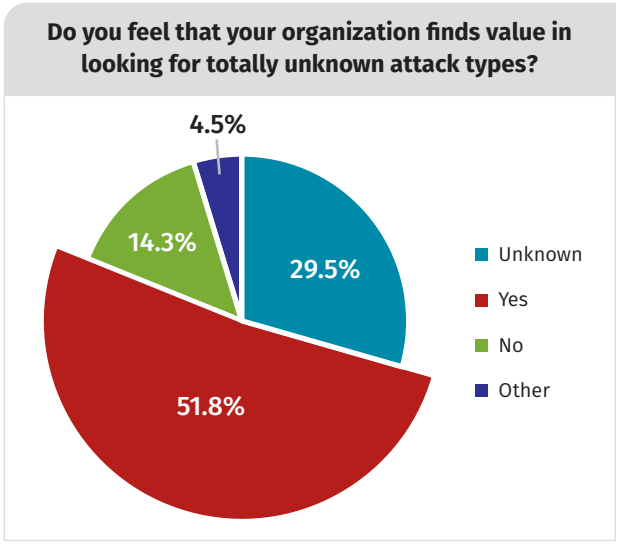



*Figure 10. Value of Hunting Unknown Attack Types*

Approaching the concept of looking for threat actors is not always easy. There is no standardized approach or framework that allows everyone to start at a common place. However, we see that organizations are looking for both understanding their attack surface and common threat actors. As shown in Figure 11, 80% of respondents are applying knowledge they can gather about threat actors targeting their organization to hunting for the threat actor in their environments. It's interesting to find this is the most common way of looking for threat actors, given that it's also one of the most challenging when it comes to gathering timely and accurate threat intelligence about those threat actors and their intent.

The second most common technique for finding unknown threat actors is data stacking, used by 44% of respondents. *Data stacking* is the process of using telemetry you have from endpoints and the network to enable your search for outliers in the data. This is the most reliable method for hunting threat actors because it requires little input from third parties and less speculation about external data sources. However, it does present a challenge when it comes to gathering the data for analysis, although in reality it is the same type of data needed for the other techniques used by respondents.

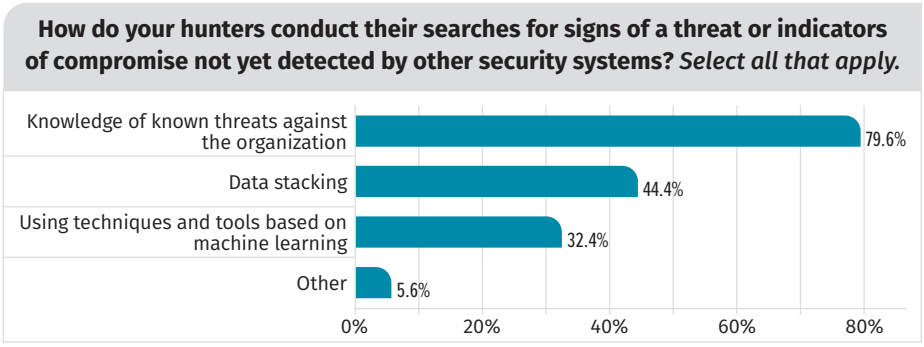



*Figure 11. Searching for Signs of a Threat or IoCs*

Use of machine learning to find unknown threats is being leveraged by 32% of respondents. The concept of using machine learning for cybersecurity has been a controversial one, let alone using it for threat hunting or incident response. Being able to catch unknown threats with machine learning would take a significant amount of data and assumes consistent actions by both users and threat actors. The users would need

to act in the same way every time they use a computer, and threat actors would need to act the exact same way every time they attempt to compromise a computer. While it is true that threat actors use the same techniques if they continue to work, the threat actors are also humans and make human mistakes. The challenge in using machine learning to find unknown threat actors was highlighted by Darren Bilby from Google back in 2017 in his presentation at the FIRST 2017 conference[5] and was raised again last year by Adi Ashkenazy and Shahar Zini in their presentation from BSides Sydney 2019.[6] Threat actors could successfully make a cybersecurity product using machine learning to identify malicious tools as known safe tools to bypass the machine learning algorithm. It is admirable that organizations are attempting to use this technique; however, as an industry we still have a lot to perfect with the use of machine learning for cybersecurity.

The past 12 months have seen a significant re-education of organizations that threat actors actively target vulnerability to leverage access into an environment. In October 2020 we even saw the NSA take the overt step of providing advice publicly about the top 25 vulnerabilities targeted by Chinese threat actors.[7] The tactic of threat actors targeting vulnerabilities is not new; however, recently it's slowly been on the rise. The survey showed that 80% of threat hunting teams are actively engaged in looking at vulnerabilities and misconfigurations that their threat actors may be trying to leverage. This also means 20% either did not look at these vulnerabilities and misconfigurations or did not know whether their hunting teams assessed this attack surface. Of those paying attention to vulnerabilities and misconfigurations, it was almost an even split—with 32% of organizations spending less than a quarter of their hunt missions doing this and 34% of organizations spending anywhere from a quarter to half their time hunting for threat actors leveraging this attack surface.

## Measuring Threat Hunting Effectiveness

Because threat hunting requires the allocation of budget and resources, measuring the affect it has is important. In last year's survey, we established that most organizations still struggle to measure threat hunting in a consistent way. Apparently, this trend didn't change very much, with the largest portion of respondents (28%) still unable to specify how much threat hunting improved the overall security of their organizations.

The organizations that do have methods in place to measure the effectiveness of threat hunting claim they mostly use ad hoc methods or measure their success based on industry-based frameworks, such as the MITRE ATT&CK® framework, as depicted in Figure 12.

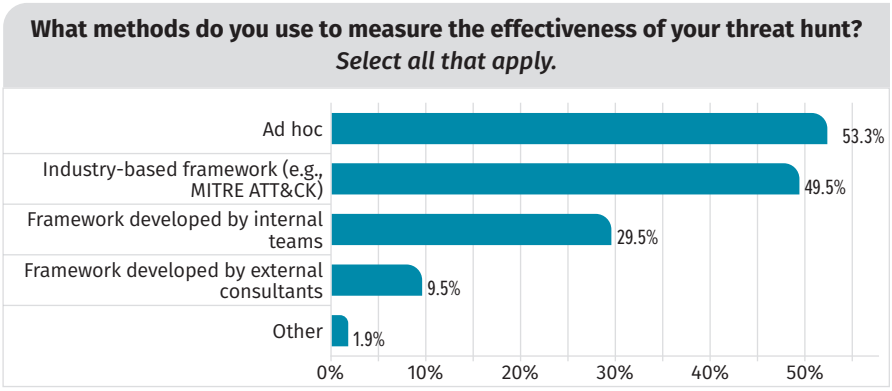



*Figure 12. Methods to Measure Threat Hunting*

[5] "Darren Bilby: A Decade of Lessons in Incident Response," FIRST 2017, June 2017, https://youtu.be/6qssVEHrpWo

[6] "Attacking Machine Learning: The Cylance Case Study," BSides Sydney, 2019, https://skylightcyber.com/2019/07/18/cylance-i-kill-you/Cylance%20-%20Adversarial%20Machine%20Learning%20Case%20Study.pdf

[7] "Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities," October 2020, https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF

While approximately half of respondents do not plan to increase their investment in threat hunting staff, only 34% don't plan any change in their investments for tooling. That might relate to the currently unsatisfying number of context switches and the lack of tool support for threat hunting operations. Furthermore, it may also explain why over a quarter of respondents (30%) said they didn't know whether their organization finds value in looking for unknown attacks or compromises. By implementing good tools and reducing context switches, the effectiveness and efficiency of every single threat hunter will increase.

## Conclusion

This year's threat hunting survey showed that there is still no clear consensus on what threat hunting entails. While 37% of respondents have a formal threat hunting program, 85% claim that they implemented threat hunting in some form. In reality, many organizations claim to run threat hunting programs to tick a box in a compliance report rather than to find new threats in their environment.

Still, most threat hunters are not full-time threat hunters, instead splitting their time with other responsibilities. The trend to staff threat hunting operations with incident responders and SOC analysts remains unbroken. While incident responders are very familiar with the task of finding new, unknown threats, SOC analysts might have difficulties deviating from their routine of analyzing alerts to actively search for signs of a breach.

What threat hunters struggle with the most are frequent context switches, given that only a few respondents said that they never need to switch tools while doing their job. So, jumping between applications is one area that has a huge potential for improvement and increased efficiency. Manual analysis also factors into efficiency. Most respondents (36%) are manually applying the threat intelligence they have collected. One of the reasons appears to be that almost half of respondents don't store threat intelligence in a platform but rather use traditional file-based methods such as spreadsheets or PDFs.

What surprised us is that just under half of respondents do not see a positive value in hunting for new, unknown threats. We believe that uncovering unknown threats is one of the main arguments for threat hunting, while daily threats can be thwarted by a SOC.

For the path forward, the most crucial topics that must be addressed are establishing a common understanding of threat hunting, improving tools to reduce context switches, and making threat hunting more measurable. The low-hanging fruit for many respondents would be to switch their intelligence management system from document-based to an open-source or commercial platform to make threat intelligence easier to consume, evolve, and apply.

In conclusion, threat hunting became more pervasive in the industry, but the general value is still not widely understood, nor is there a gold standard for threat hunting today.

## About the Authors

**Mathias Fuchs**, a certified instructor for SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics, is head of investigation & intelligence at InfoGuard AG, where he is actively engaged in running the incident response (IR) practice. In that role he uses his knowledge to shape his team; develop the necessary forensic, IR and threat hunting capabilities; and proactively mediate security vulnerabilities that would be more difficult to manage later. Prior to joining InfoGuard, Mathias was a principal consultant at Mandiant, where he led large-scale cybersecurity investigations. He also was the lead security architect at T-Systems and a security consultant for international clients in a variety of industries.

**Joshua Lemon** is a certified instructor for SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and SANS FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. He is a managing director at Ankura, leading their APAC Digital Forensics and Incident Response practice in Australia, where he assists government and commercial clients with combatting sophisticated compromises, maturing their cyber defense and response programs, and threat hunting for malicious adversaries. Previously, he worked as a director at Salesforce.com in their international Salesforce Security Response Centre (SSRC), where he headed up the team responsible for looking at new cutting-edge ways to approach incident response at scale.

## Sponsors

**SANS would like to thank this survey's sponsors:**

ANALYST1 · cisco · SOPHOS · ANOMALI · corelight · SWIMLANE · BlackBerry · DOMAINTOOLS · THREATQUOTIENT · Secureworks