2018

THREAT HUNTING REPORT

Cybersecurity INSIDERS

Crowd Research Partners

IBM Security

THREAT HUNTING
2018 REPORT

TABLE OF CONTENTS

INTRODUCTION

Organizations are experiencing new and evolving cyberthreats that are increasing in both sophistication and frequency, often overwhelming Security Operation Center (SOC) staff.

In response to the new challenges, threat hunting is a developing security practice that focuses on proactively detecting and isolating advanced persistent threats (APTs).

Many SOCs are going through a posture shift as they are pivoting from traditional reactive security postures to a hybrid approach that includes proactive hunting of threats.

In 2018, the Information Security Community on LinkedIn conducted its second annual online research project on threat hunting to gain further insights into the maturity and evolution of the security practice.

The research confirms that organizations realize that proactively uncovering security incidents pays off with earlier detection, faster response, and denial of future exploits.

We would like to thank our sponsor IBM Security for supporting this unique research.

We hope you will enjoy the report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity INSIDERS

Holger.Schulze@Cybersecurity-Insiders.com

KEY SURVEY FINDINGS

1. **Threat hunting is gaining momentum** - Organizations are increasingly utilizing threat hunting platforms (40 percent), up 5 percentage points from last year's survey. Threat hunting is gaining momentum and organizations are making the investment in resources and budgets to shift from reacting to attacks to the creation of proactive threat hunting programs and dedicated teams. Six out of 10 organizations in our survey are planning to build out threat hunting programs over the next three years.

2. **Threat hunting delivers strong benefits** - Organizations are growing more confident in their security teams' ability to quickly uncover advanced attacks. A third of respondents are confident to very confident in their threat hunting skills, a 7 percentage point increase over last year. Threat Hunting tools improve the speed of threat detection and response by a factor of 2.5x compared to teams without dedicated threat hunting platforms. The top benefits organizations derive from threat hunting include improved detection of advanced threats (64 percent), followed by reduced investigation time (63 percent), and saved time not having to manually correlate events (59 percent).

3. **Threat management challenges** - Detection of advanced threats remains the #1 challenge for SOCs (55 percent), followed by lack of security expertise (43 percent). 76 percent of respondents feel that not enough time is spent searching for emerging and advanced threats in their SOC. Lack of budget (45 percent) remains the top barrier to SOCs who have not yet adopted a threat hunting platform.

4. **Most important threat hunting capabilities** - The most important threat hunting capabilities for cybersecurity professionals is threat intelligence (69 percent), followed by User and Entity Behavior Analytics (UEBA) (57 percent), automatic detection (56 percent), and machine learning and automated analytics (55 percent).

5. **Threat frequency and severity increases** - A majority of 52 percent say threats have at least doubled in the past year. Based on this trend, the number of advanced and emerging threats will continue to outpace the capabilities and staffing of organizations to handle those threats..

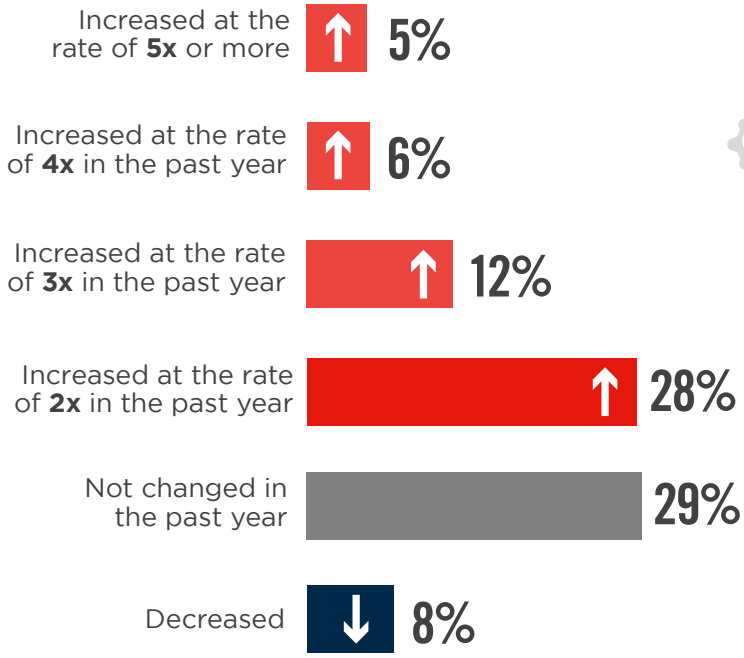
THREAT HUNTING

SEVERITY & FREQUENCY OF CYBER THREATS

Cybersecurity professionals have an ongoing challenge of constantly defending against increasing number of security threats, not only in terms of volume of attacks but also their severity (damage and impact). In the past 12 months, the severity of security attacks directed at organizations has increased. Nearly 52 percent of organizations have experienced at least a doubling of security attacks. Only 8 percent of respondents signaled a decrease in attacks.

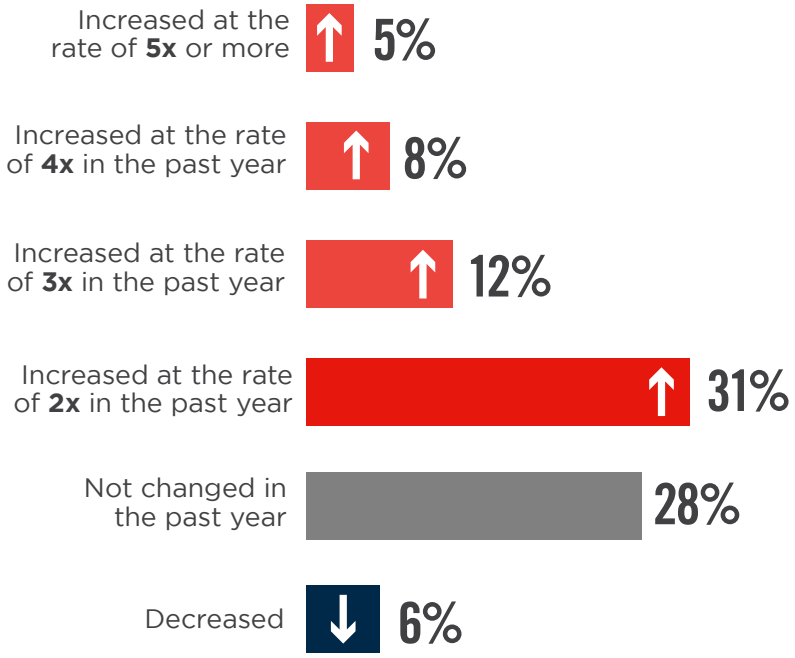
Over half of the SOCs (56 percent) polled have experienced an increase in the frequency of cyber attacks over the last 12 months. Only 6 percent say the frequency has decreased. The results further illustrate the need for organizations to pivot from a purely reactive security stance to becoming more proactive by hunting threats and adversaries.

Which of the following best describes the change in severity (potential damage and impact) of security threats faced by your organization in the past year?



Don't know 12%

Which of the following best describes the frequency of security threats faced by your organization compared to the previous year?

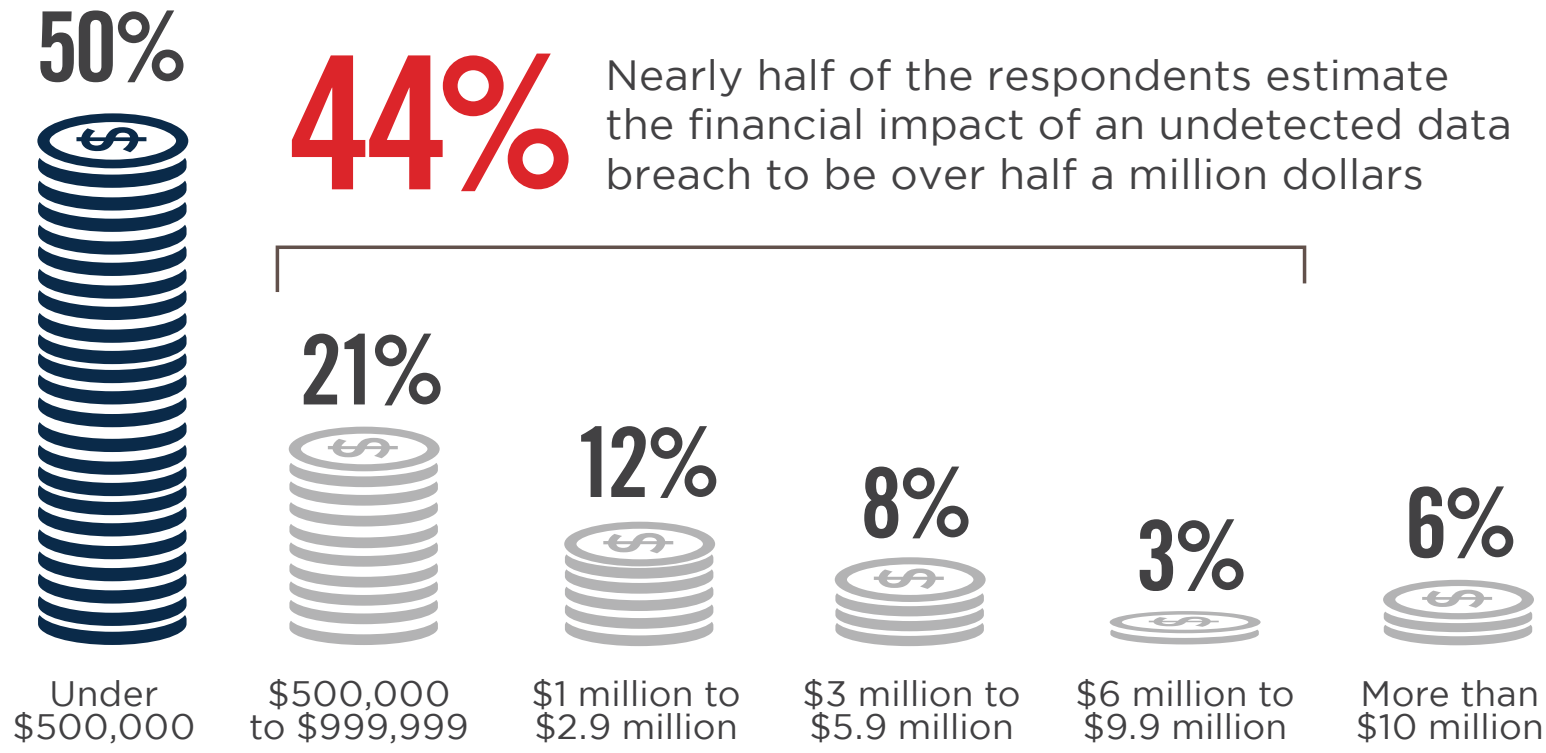


Don't know 10%

FINANCIAL IMPACT OF CYBER THREATS

Data breaches are becoming far more costly to manage. Nearly half (44 percent) of the respondents estimate the financial impact of an undetected data breach to be over half a million dollars. Alarmingly, 6 percent believe the cost to exceed 10 million dollars.

What is the estimated financial impact of a security threat that goes undetected and results in a breach at your organization?



THREAT HUNTING GOALS

The primary goal of any comprehensive cybersecurity program is to protect the organization's resources and information against external and internal threats. Cybersecurity professionals recognize that proactively hunting threats will reduce the overall risk to the organization.

The top three objectives that threat hunting programs focus on: reducing exposure to external threats (56 percent), improving speed and accuracy of threat response (52 percent) and reducing the number of breaches (49 percent).

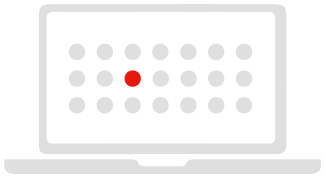
What are the primary goals of your organization's threat hunting program?

56%

Reduce exposure to external threats

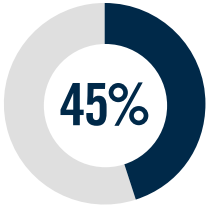
52%

Improve speed and accuracy of threat response

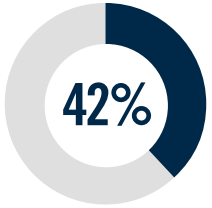


49%

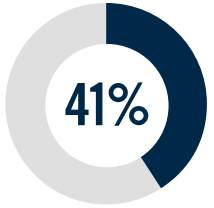
Reduce number of breaches and infections



Reduce time to containment (prevent spread)



Reduce attack surface



Reduce exposure to internal threats

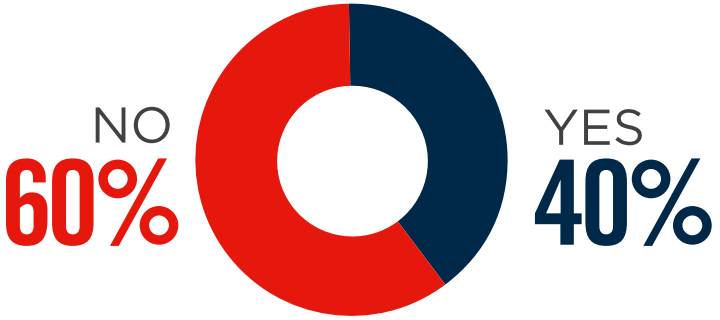
Reduce dwell time from infection to detection 39% | Optimize resources spent on threat response 34% | Other 8%

ADOPTION OF THREAT HUNTING

Threat hunting platforms enable security analysts to discover advanced threats faster and at scale. The positive news is organizations are increasingly utilizing threat hunting platforms (40 percent), up 5 percentage points from last year's survey.

Threat hunting is gaining momentum and organizations are making the investment in resources and budget to shift from reacting to attacks to the creation of proactive threat hunting programs and dedicated teams. Six out of 10 organizations in our survey are planning to build out threat hunting programs over the next three years.

Does your security team currently use a threat hunting platform for security analysts?



If you don't have a threat hunting program in place already, are you planning on building a threat hunting program in the next three years?

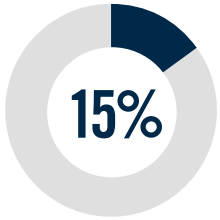
BARRIERS TO THREAT HUNTING

For the second year, lack of budget (45 percent) remains the top barrier to SOCs who have not yet adopted a threat hunting platform - this is up 10 percentage points from last year.

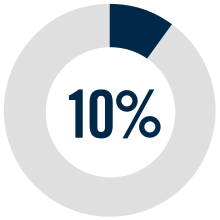
Fortunately, organizations are recognizing the importance of proactively hunting threats and made it both a higher priority (barrier lowered to 10 percent compared to 19 percent in the previous year) and addressed the lack of training (7 percent).

What is the main reason your SOC does not have a dedicated threat hunting platform for its security analysts?

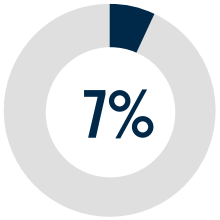
45%
Lack of budget



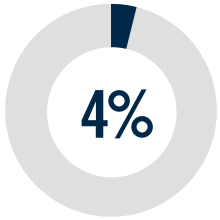
Platform fatigue, we have many platforms



Not a priority for our SOC



Lack of training on threat hunting



Lack of collaboration across departments

Other 19%

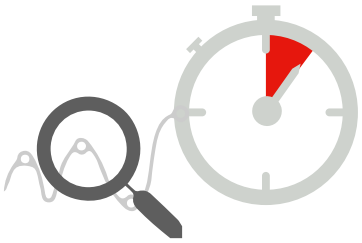
BENEFITS OF THREAT HUNTING

Threat hunting platforms provide security analysts with a suite of powerful tools to provide earlier detection, reduce dwell time, and improve defenses for future attacks. The top benefits organizations derive from threat hunting include improved detection of advanced threats (64 percent), followed closely by reduced investigation time (63 percent), and saved time not having to manually correlate events (59 percent).

What are the main benefits of using a threat hunting platform for security analysts?

64%

Improving detection of advanced threats

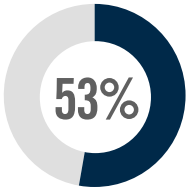


63%

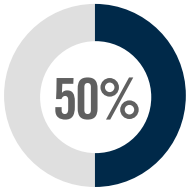
Reducing investigation time

59%

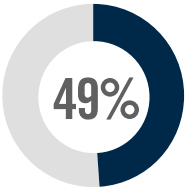
Saving time from manually correlating events



Reducing time wasted on chasing false leads



Discovering threats that could not be discovered otherwise



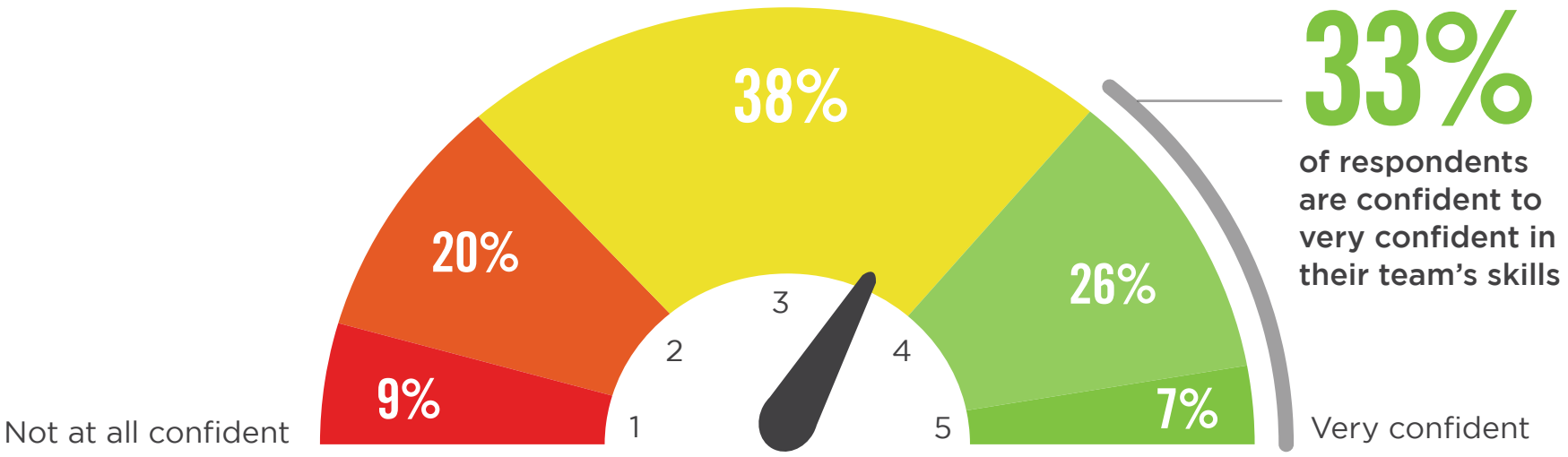
Creating new ways of finding threats

Connecting disparate sources of information 49% | Saving time scripting and running queries 42% | Reducing extra and unnecessary noise in the system 39% | Reducing attack surface 35% | Other 7%

IMPROVING CONFIDENCE

Organizations are becoming more confident in their security team's ability to quickly uncover advanced attacks, compared to last year. A third of respondents are confident to very confident in their team's skills, a 7 percentage point increase over last year.

How confident are you in your SOC's ability to uncover advanced threats?



33%

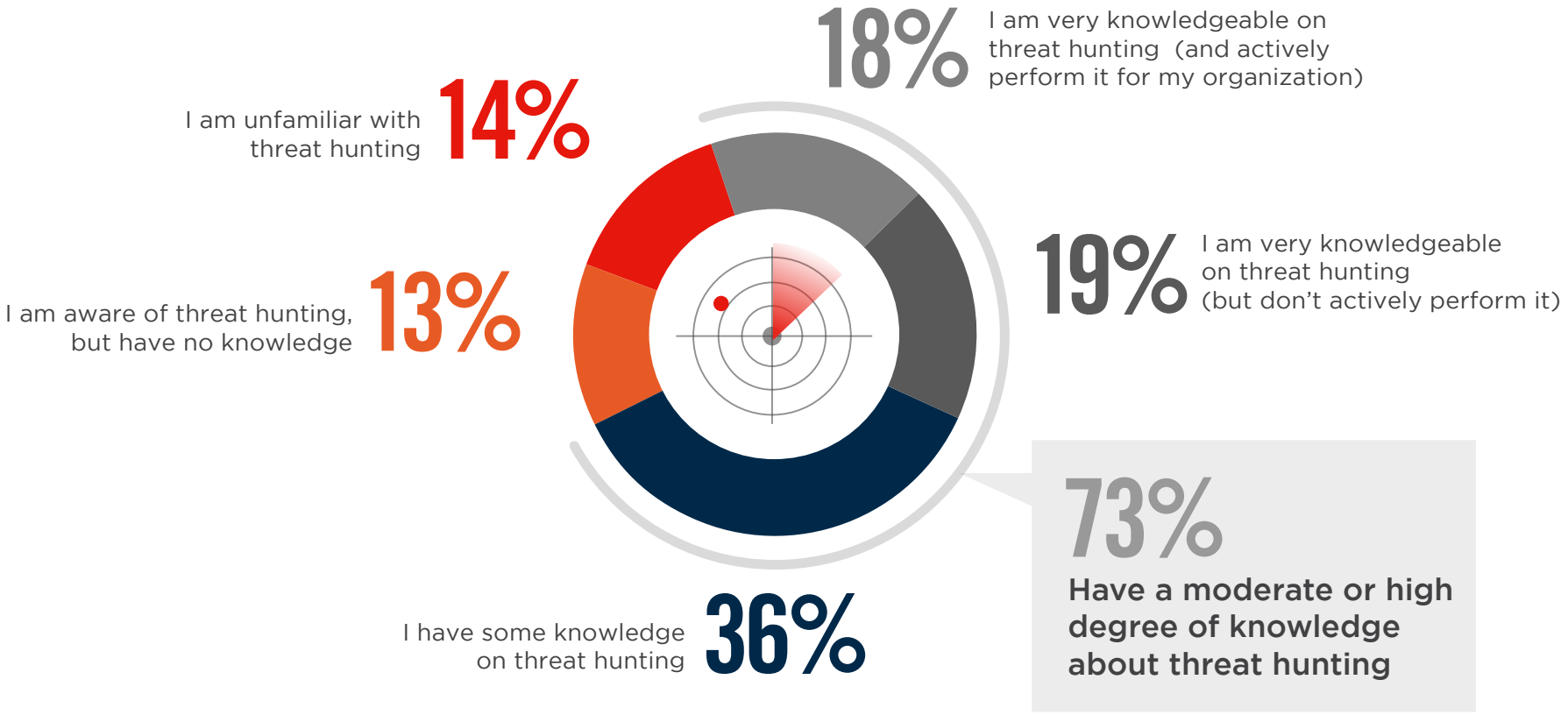
of respondents are confident to very confident in their team's skills

FAMILIARITY WITH THREAT HUNTING

The survey reveals that cybersecurity professionals have recognized the growing significance of proactively hunting threats.

Over the past year, industry awareness in the security category of threat hunting has increased. Seven in 10 respondents have some knowledge or are very knowledgeable about the topic. This is an increase of 13 percentage point compared to last year's survey.

How familiar are you with threat hunting?

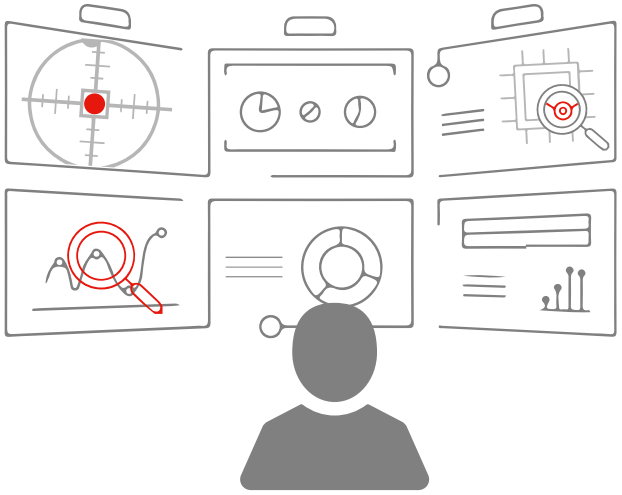


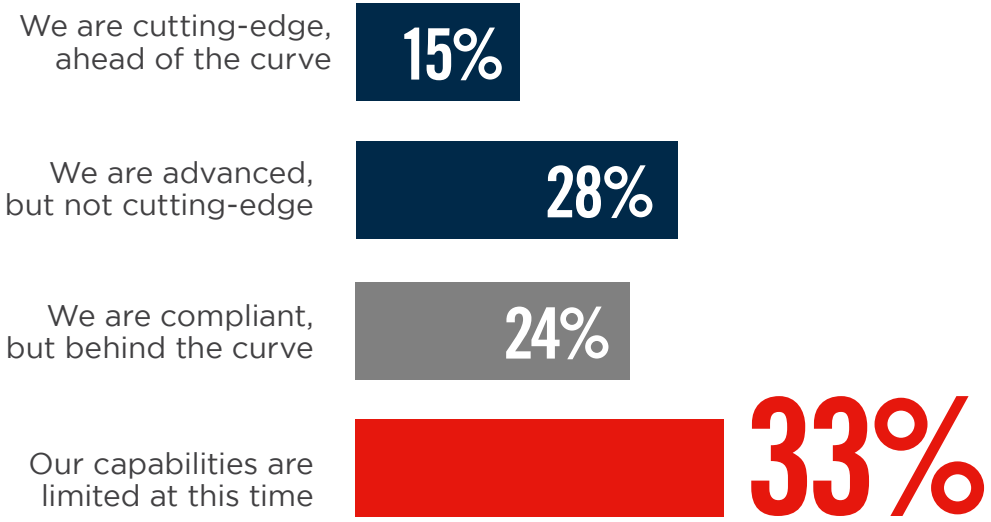
THREAT MANAGEMENT MATURITY

Security Operations Centers continually face rapidly evolving threats and an increasing volume of advanced persistent threats (APT). These challenges make it harder for cybersecurity teams to secure and defend their environments.

From a maturity perspective, nearly 15 percent believe they are cutting-edge, up 8 percent from last year. However, 33 percent of respondents state that their capabilities are limited, a jump of nearly 6 percentage points higher from the previous year.

Which of the following best reflects the maturity of your SOC in addressing emerging threats?

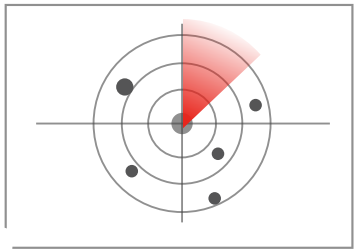


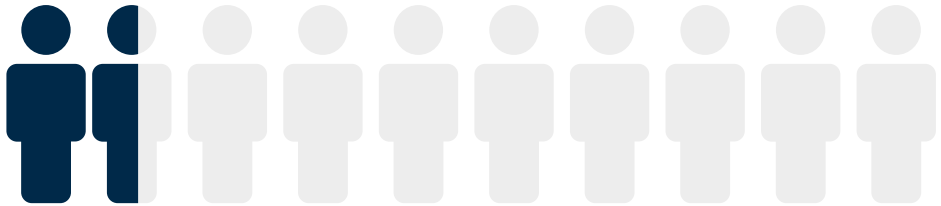


THREAT HUNTERS IN SOCs

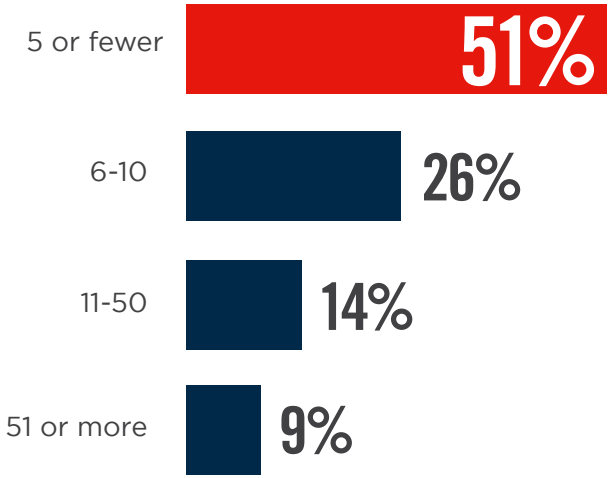
A majority of organizations has less than 5 security professionals dedicated to threat hunting. The average number of threat hunters in SOCs is rising to 17 percent, up from 14 percent in 2017.

Approximately, what percentage of employees at your SOC are threat hunting today?





17% SOC employees involved in threat hunting

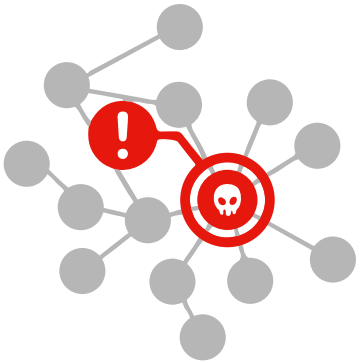


KEY SECURITY CHALLENGES

The survey results reveal that cybersecurity professionals prioritize detection of advanced threats (55 percent) as the top challenge for their SOC. Lack of expert security staff to mitigate such threats (43 percent) rose to second place.

Notably, lack of confidence in automation tools catching all threats (36 percent), jumped from fifth place in last year's survey to third today.

Which of the following do you consider to be top challenges facing your SOC?

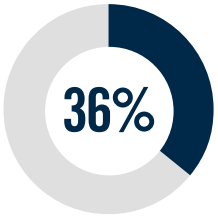


55%

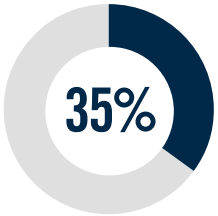
Detection of advanced threats (hidden, unknown, and emerging)

43%

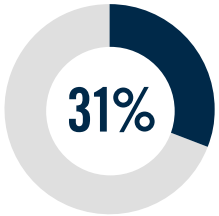
The lack of expert security staff to assist with threat mitigation



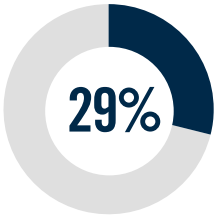
Lack of confidence in automation tools catching all threats



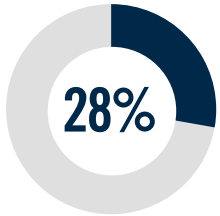
Too much time wasted on false positive alerts



Slow response time to find or detect advanced threats



Working with outdated SIEM tools and SOC infrastructure



Lack of proper reporting tools

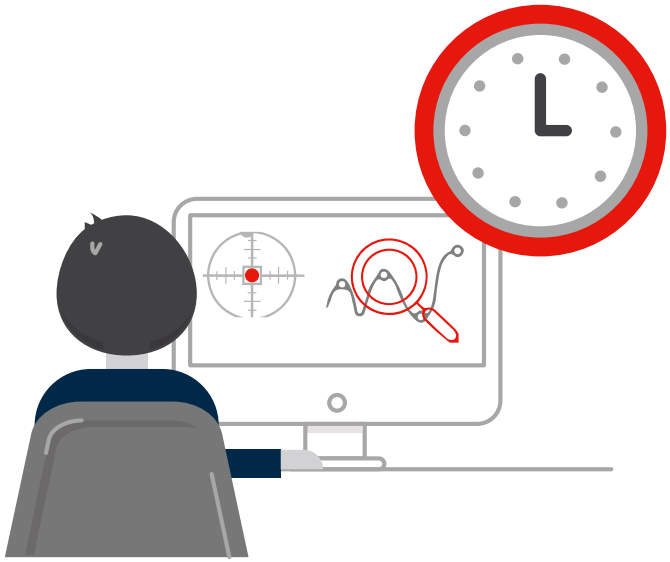
Other 7%

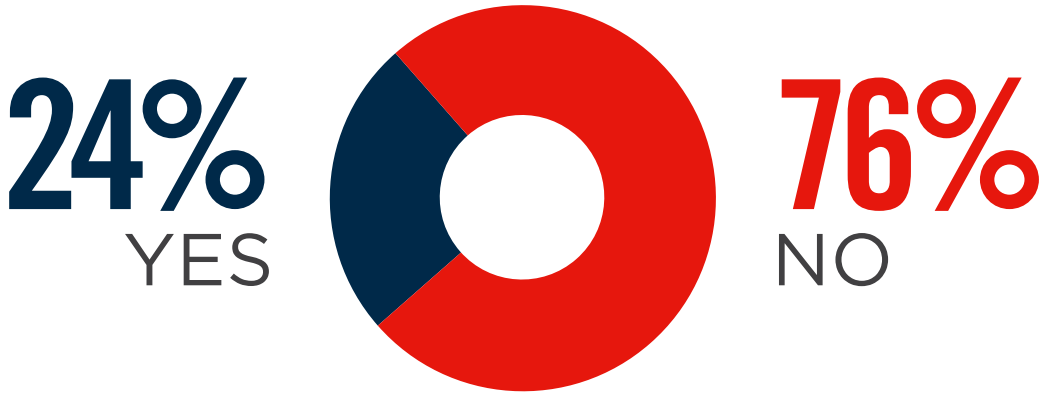
TIME SPENT ON THREAT HUNTING

Traditionally, SOCs approach to threats and the tools they use - such as antivirus, IDS, or security information and event management (SIEM) - are typically reactive response technologies.

This is a reactive posture, whereas they spend a majority of their time reacting to threats, instead of proactively seeking new unknown threats that enable early detection and quicker response. Nearly 3 in 4 (76 percent) respondents believe their SOC does not spend enough time proactively searching for new threats, slightly improving by 5 percentage points compared to last year.

Do you feel enough time is spent searching for emerging and advanced threats at your SOC?





THREAT HUNTING PRIORITY

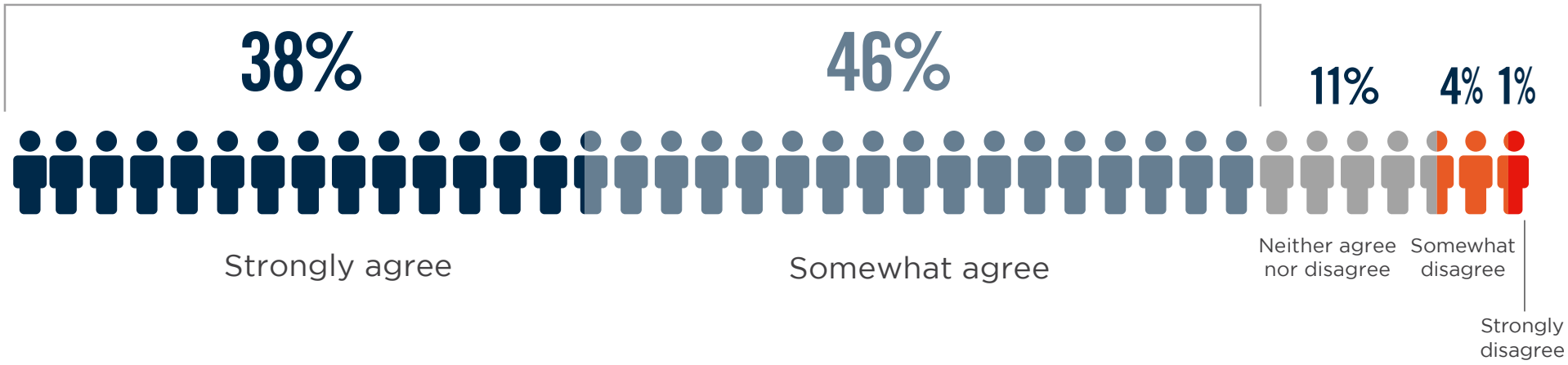
Although threat hunting is still nascent, more and more organizations recognize the value of building a threat hunting program to provide early detection and reduce risk.

Over 84 percent surveyed, agree that threat hunting should be a top security initiative, an increase of 5 percentage points from the year before.

What is your level of agreement with the following statement? "Threat hunting should be a top security initiative."

more than 3/4 of respondents

believe threat hunting is of major importance

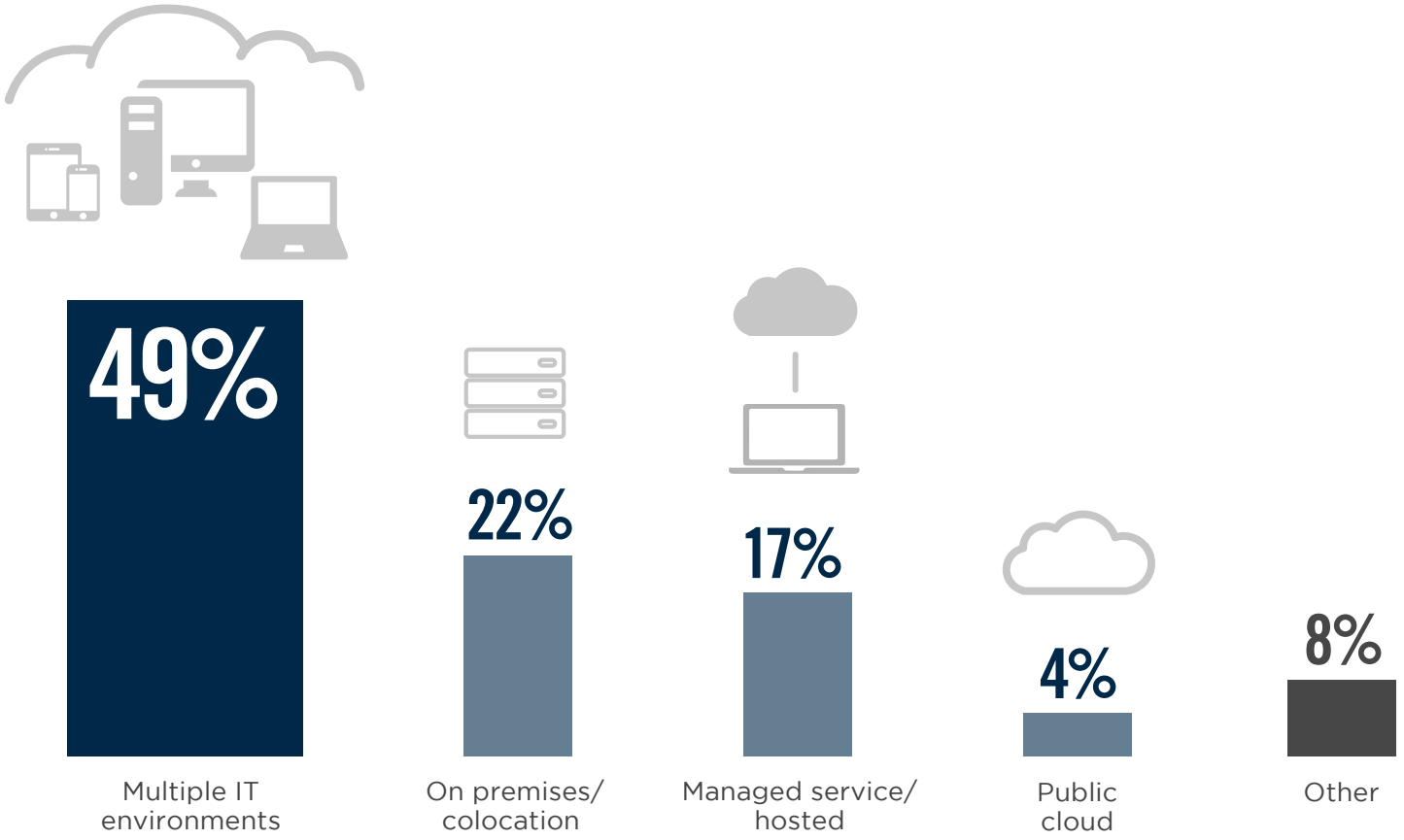


THREAT HUNTING ACROSS IT ENVIRONMENTS

Securing a single IT environment can be quite complex and challenging - orchestrating across multiple IT environments significantly increases the complexity. Nearly half (49 percent) of respondents manage multiple IT environments. Cybersecurity teams will need to evolve to manage and monitor these disparate environments.

By employing tools and automation alongside SOC personnel, organizations can make better informed decisions, resulting in earlier detection, faster responses, and reducing an adversary's dwell time.

What type of IT environment does your threat hunting program primarily focus on?

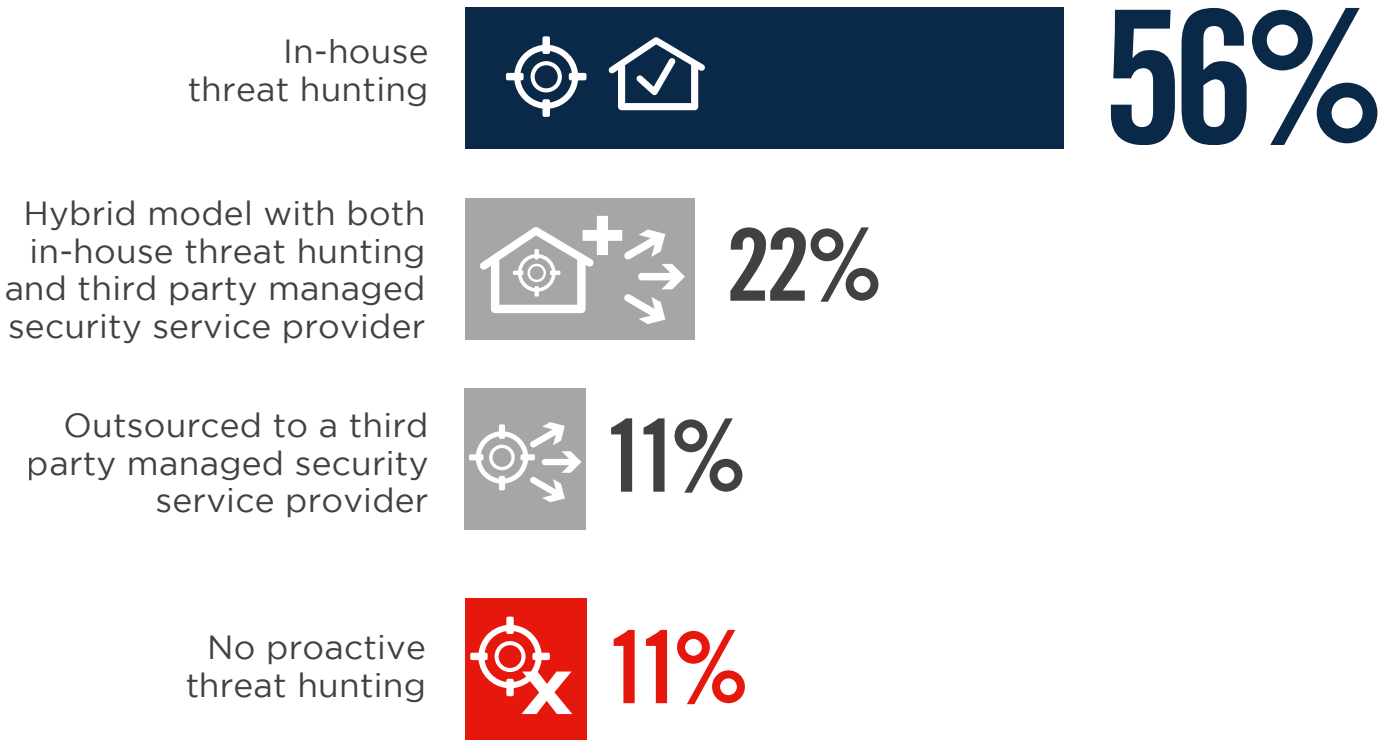


SOURCING OF THREAT HUNTING

Today, a majority of organizations solely use in-house staff (56 percent) to proactively hunt threats. In the survey, over a third (33 percent) partner with Managed Security Services Providers (MSSP) to help. Threat hunting is a new security discipline for most organizations and many are struggling to cope with their existing security threat workload.

The good news, organizations are making the switch to include threat hunting as part of their security framework. They are discovering that proactive threat hunting can reduce the risk and impact of threats while improving defenses against new attacks.

How is your threat hunting performed?

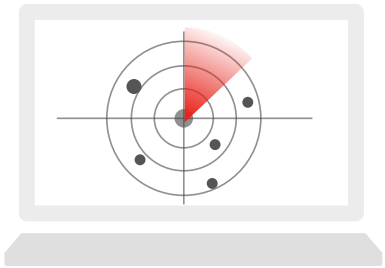


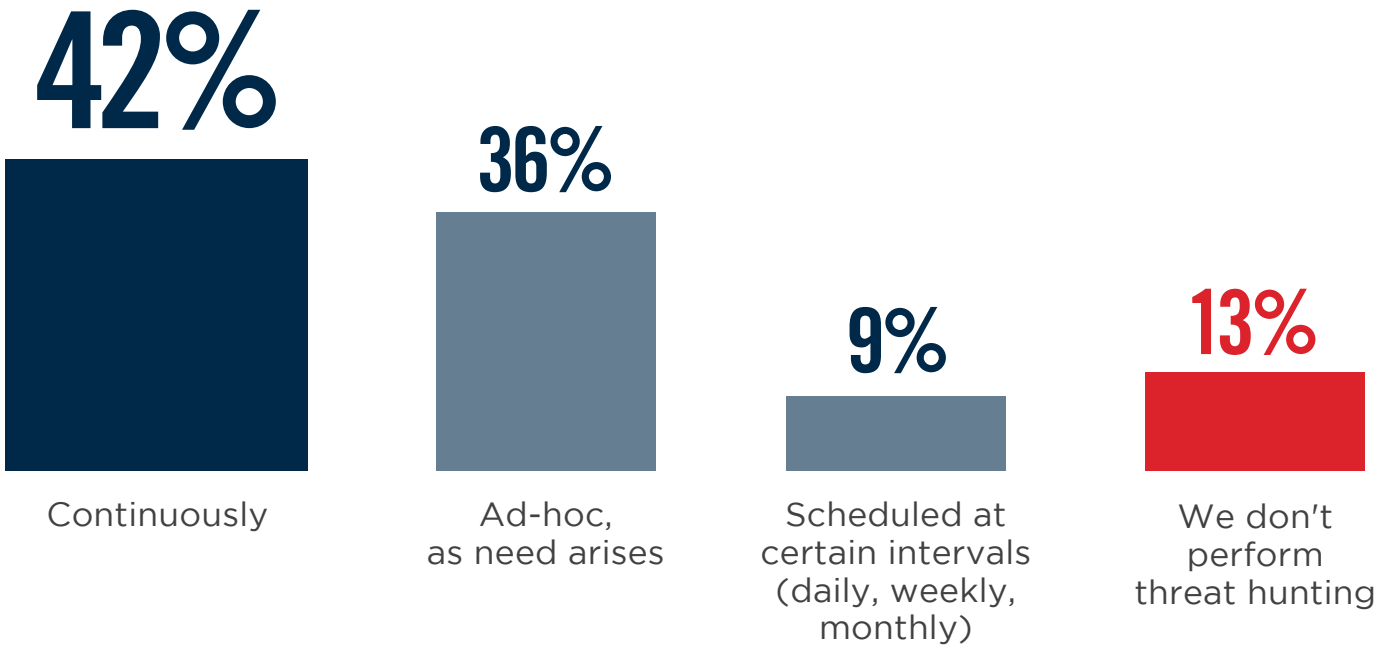
THREAT HUNTING FREQUENCY

Early detection of cyber breaches and rapid response can mitigate the severity and impact of damages.

Forty-two percent of organizations continuously and actively hunt threats, followed by 36 percent who perform threat hunting only reactively, as the need arises. Thirteen percent do not perform any threat hunting.

How frequently does your organization perform threat hunting?



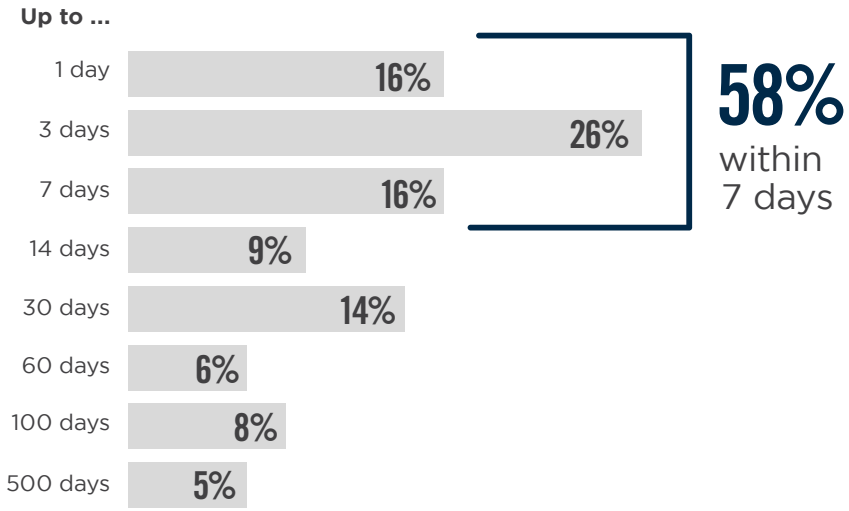


ATTACK DISCOVERY

A majority of organizations (58 percent) discovers most attacks within 7 days. A third of organizations report dwell times over 30 days. Nearly all respondents agree that attackers dwell on a network for some period of time before they're discovered by the SOC.

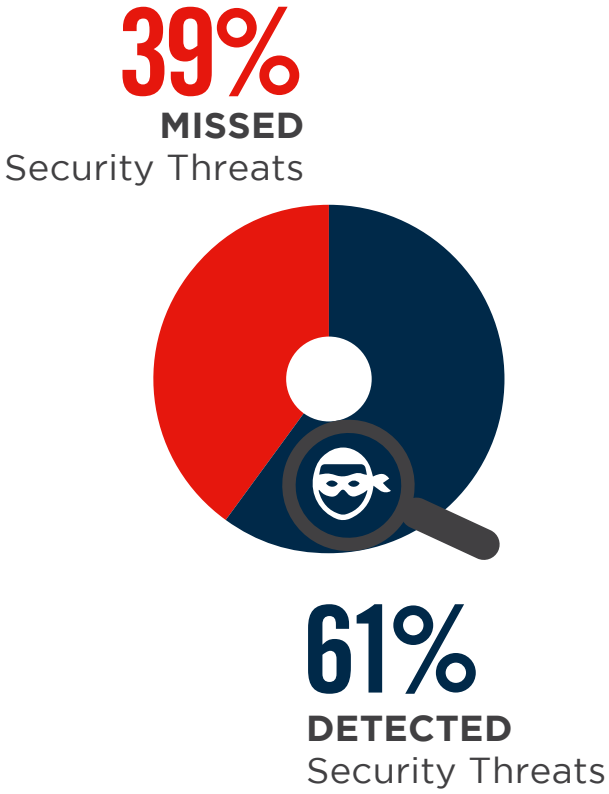
On average, how many days do attackers who breached your security defenses dwell in your network before they are discovered by your SOC?

Average time attackers dwell on networks until discovered



SOCs report they are missing an average of 39 percent of security threats. This represents only a small improvement over the 40 percent of missed threats SOCs reported in 2017.

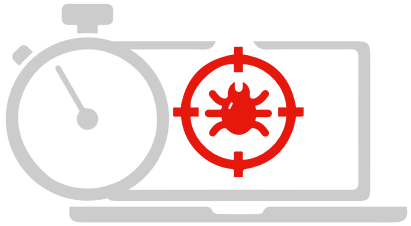
What percentage of emerging and advanced threats are missed by traditional security tools?



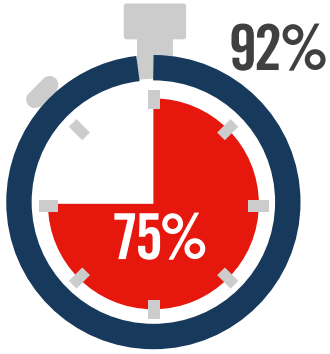
THREAT HUNTING PERFORMANCE

When asked to estimate the amount of time it takes to detect and address threats with vs. without a threat hunting platform, SOCs utilizing threat hunting platforms reported an average performance improvement of 2.5 faster detection and response time.

On average, how many hours does it take to detect and respond to threats WITH / WITHOUT a threat hunting platform?



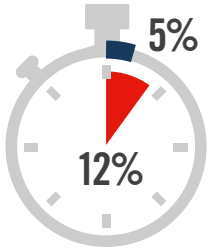
Time to detect & respond



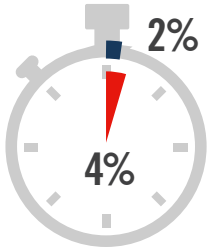
24 hours

2.5x

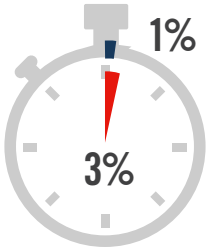
speed improvement of threat detection and response **WITH a threat hunting platform**



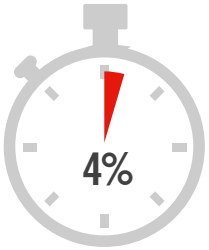
48 hours



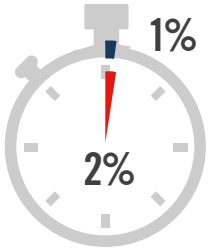
72 hours



96 hours



120 hours



more than 120 hours

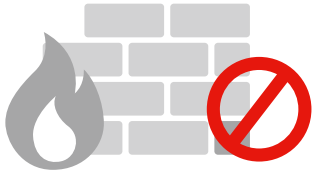
WITH **WITHOUT** **A THREAT HUNTING PLATFORM**

DATA COLLECTION PRIORITIES

Threat hunting includes a wide array of data sources to detect anomalies and suspicious activity. Most organizations prioritize Firewall and IPS logs as the most important data sources to collect and review, as the top choice at 69 percent, followed by web and email filter traffic at 63 percent, and network traffic at 61 percent.

Bottom Line: there are numerous security datasets to investigate. The best practice is not to depend solely on one, but to gather, normalize and analyze a variety of sources for a more complete, timely, and accurate picture.

What kind(s) of data does your security organization collect and analyze?

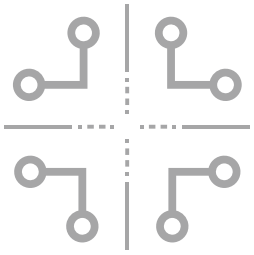


69%

Firewall & IPS logs

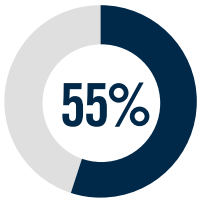
63%

Web and email filter traffic

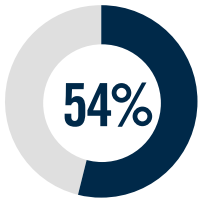


61%

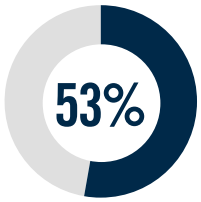
Network traffic



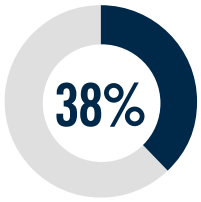
Endpoint activity



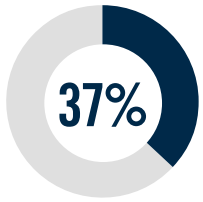
Active directory



DNS traffic



Server traffic



User behavior

Packet sni/tcpdump 37% | System logs 36% | File monitoring data 32% | Don't know 12% | Other 6%

TIME SPENT ON THREAT HUNTING

Respondents spend an average 60 percent of their time with alert triage and reacting to security threats compared to 40 percent of time spent proactively seeking threats.

In a typical week, what percentage of your threat management time is spent with alert triage or reactive response to security threats versus engaging in proactive and innovative detection methods?

40%
Proactively detecting threats

60%
Reacting to security threats

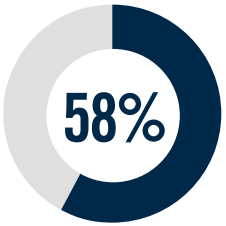
THREAT INDICATORS

Understanding Indicators of Compromise (IOCs) allows organizations to develop effective defense methodologies that help with rapid detection, containment, and denial of future exploits. Knowing what IOCs to look for aids cybersecurity professionals in threat triage and remediation.

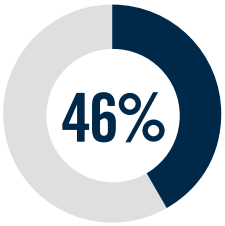
Our research reveals that hunt teams most frequently investigate behavioral anomalies (67 percent), followed by IP addresses (58 percent), and tied for third are both domain names and denied/flagged connections at 46 percent.

What kinds of indicators are most frequently investigated by your hunt team?

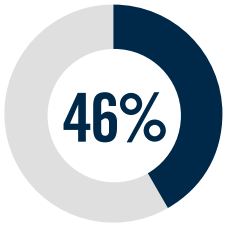
67% Behavioral anomalies (unauthorized access attempts, etc.)



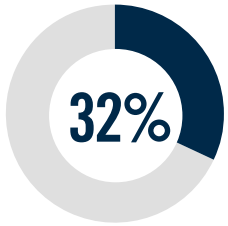
IP addresses



Domain names



Denied/flagged connections



File names

Not sure/Other 24%

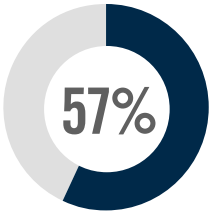
KEY THREAT HUNTING CAPABILITIES

The most important capability that cybersecurity professionals consider critical to their threat hunting tool suite is threat intelligence (69 percent).

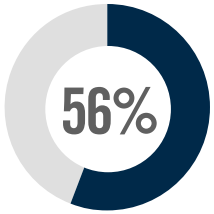
User and Entity Behavior Analytics (UEBA) (57 percent), automatic detection (56 percent), machine learning and automated analytics (55 percent) and full attack lifecycle coverage (55 percent) round out the top five capabilities.

What capabilities do you consider most important regarding the effectiveness of a threat hunting tool?

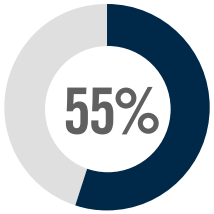
69% Threat intelligence



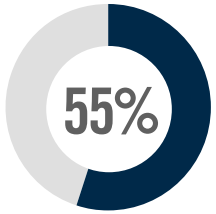
User and Entity Behavior Analytics (UEBA)



Automatic detection



Machine learning and automated analytics



Full attack lifecycle coverage

Vulnerability scanning 47% | Integration and normalization of multiple data sources 45% | Intuitive data visualization 44% | Automated workflows 43% | Fast, intuitive search 43% | Other 5%

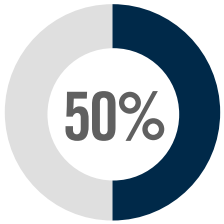
THREAT HUNTING TECHNOLOGIES

The market for threat hunting tools is still maturing, with new entrants emerging. Organizations cast a wide net and use multiple technologies together to achieve deeper visibility across their infrastructure to help identify new threat patterns. Many continue to rely on traditional tools and methods of prevention/detection (e.g., firewalls, IDS, SIEM, etc.) as part of their threat hunting posture.

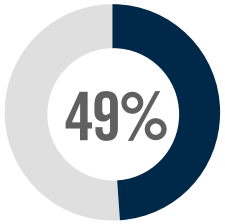
The top three technologies that organizations utilize for threat hunting are NGFW, IPS, AV (55 percent), SIEM (50 percent) and anti-phishing or other messaging security software (49 percent). Interestingly, threat intelligence (39 percent) ranked fourth in this year's survey.

Which technologies do you use as part of your organization's threat hunting approach?

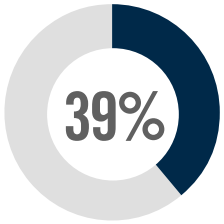
55% NGFW, IPS, AV, web application firewall, etc.



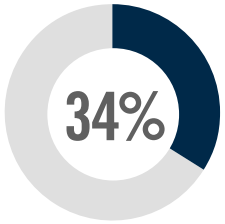
SIEM



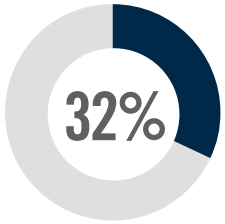
Anti-phishing or other messaging security software



Threat intelligence platform



Enrichment and investigation tools



Vulnerability management

Network IDS 31% | Orchestration (e.g., Phantom, Hexadite, Resilient, etc.) 11% | Not sure/Other 19%

THREAT HUNTING INTEGRATION

Organizations are integrating a multitude of technologies into their threat hunting platform.

Incident response (71 percent) takes the top spot, followed by SIEM (63 percent), and tied for third place (56 percent) are ticket system and active directory.

With what systems would you like your threat hunting platform to integrate?

71%

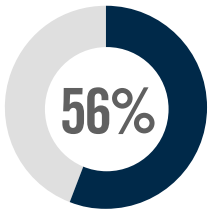
Incident response

63%

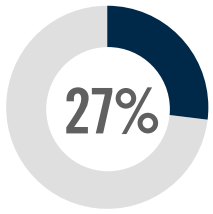
SIEM

56%

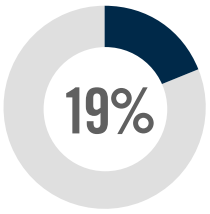
Active directory



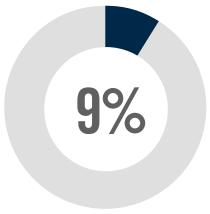
Ticket system



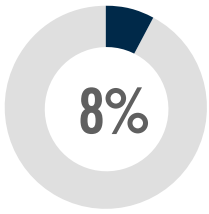
NAC



File activity monitoring



CI/CD, deployment orchestration



UEBA

Other 9%

METHODOLOGY & DEMOGRAPHICS

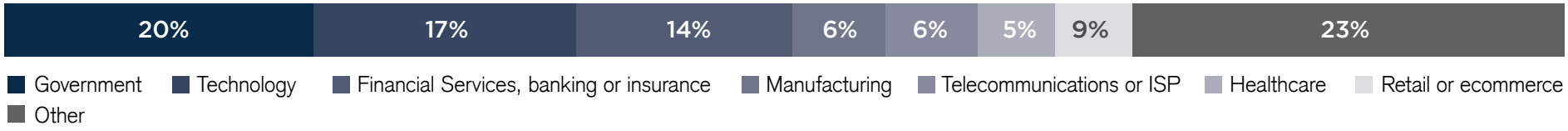
The 2018 Threat Hunting Report is based on the results of an online survey of over 461 cybersecurity and IT professionals to gain more insight into the state of threat management in SOCs. The respondents range from security analysts and IT managers to CISOs. The respondents reflect a representative cross section of organizations of varying sizes across many industries, ranging from financial services to telecommunications and healthcare.

DEPARTMENT

JOB LEVEL

COMPANY SIZE

INDUSTRY



SPONSOR OVERVIEW

IBM Security | www.IBM.com

IBM Security provides the modern SOC with powerful threat hunting capabilities to find threats faster, improve time to detection and reduce the costs and impacts of attacks. IBM i2 arms analysts with advanced analytics and human-led intelligence analysis and investigation tools to detect, disrupt and defeat advanced threats.