2019

Cybersecurity
INSIDERS

THREAT HUNTING REPORT

DOMAINTOOLS

INTRODUCTION

Threat hunting is a new discipline for most organizations, established in response to new security challenges to focus on proactively detecting and isolating advanced persistent threats (APTs) that might otherwise go undetected.

While many SOCs are struggling to cope with the current security threat workload, 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.

In 2019, Cybersecurity Insiders conducted the third annual research project on threat hunting to gain deeper insights into the maturity and evolution of the security practice. The research confirms that organizations are increasing their operational maturity and investments in threat hunting. Organizations realize that proactively uncovering security threats pays off with earlier detection, faster response, and effective denial of future exploits that can damage business operations.

We would like to thank DomainTools for supporting this unique research.

We hope you will enjoy the report.

Thank you,

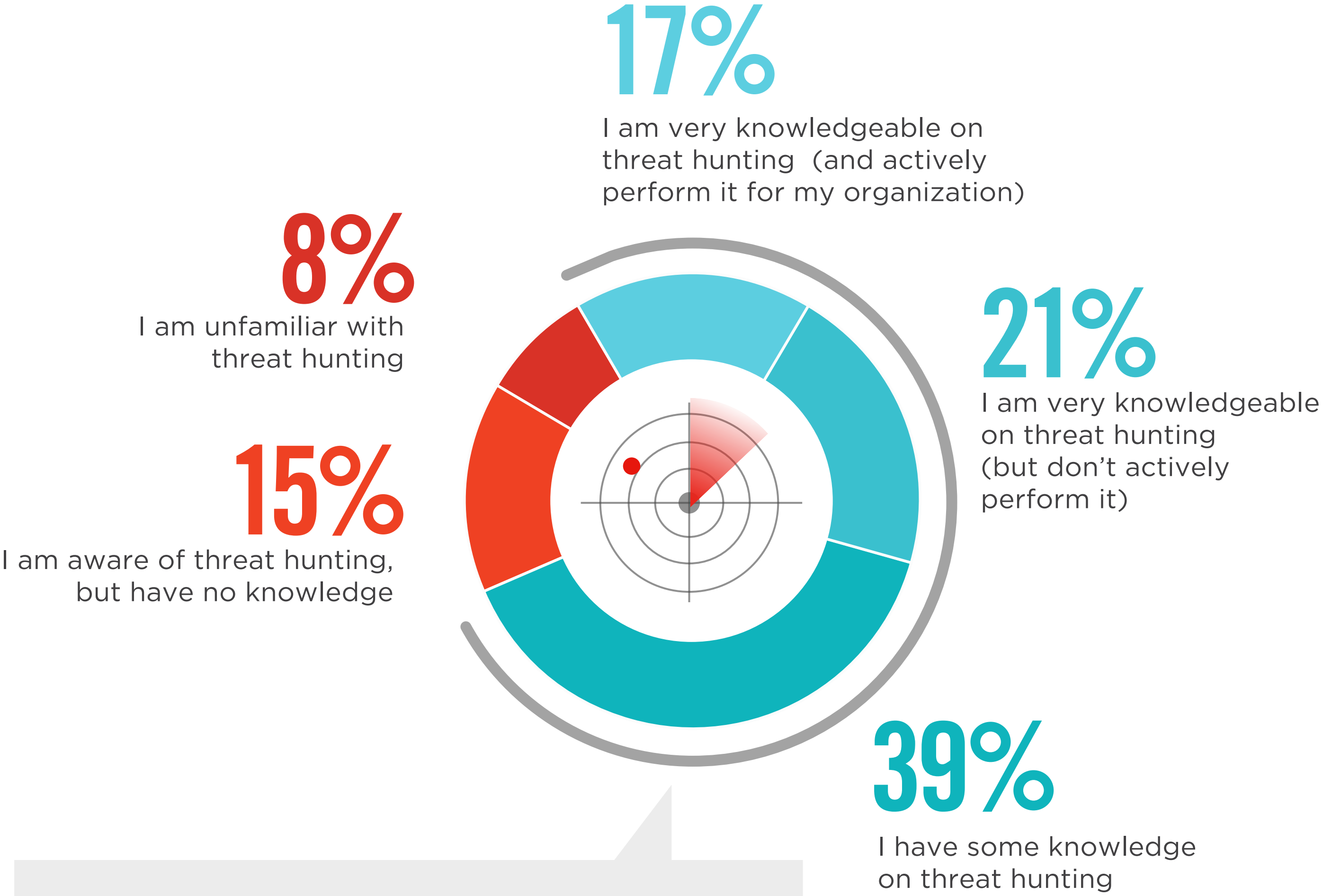
Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

FAMILIARITY WITH THREAT HUNTING

The survey reveals that cybersecurity professionals are recognizing the growing significance of proactively hunting threats. Over the past year, industry awareness for threat hunting has increased. Almost 8 in 10 respondents have at least some knowledge or are very knowledgeable about the topic. This represents an increase of 4 percentage points compared to last year's survey.

How familiar are you with threat hunting?

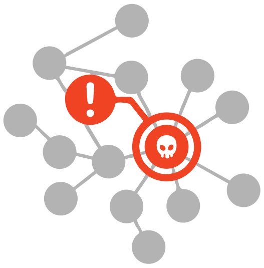


77% **Have a moderate or high degree of knowledge about threat hunting**

KEY SECURITY CHALLENGES

The survey results reveal that cybersecurity professionals prioritize detection of advanced threats (55%) as the top challenge for their SOC. Too much time wasted on false positive alerts (45%) and lack of expert security staff to mitigate such threats (43%) follow.

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



55%

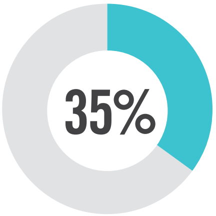
Detection of advanced threats (hidden, unknown, and emerging)

45%

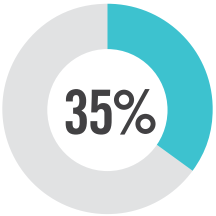
Too much time wasted on false positive alerts

43%

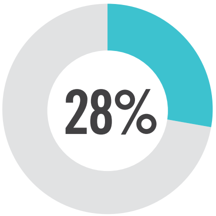
The lack of expert security staff to assist with threat mitigation



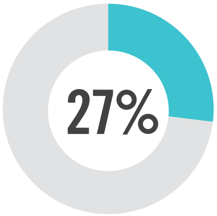
Slow response time to advanced threats



Lack of confidence in automation tools catching all threats



Working with outdated SIEM tools and SOC infrastructure



Lack of proper reporting tools

Other 5%

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 (58%), improving speed and accuracy of threat response (53%) and reducing the number of breaches (52%).

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

58%

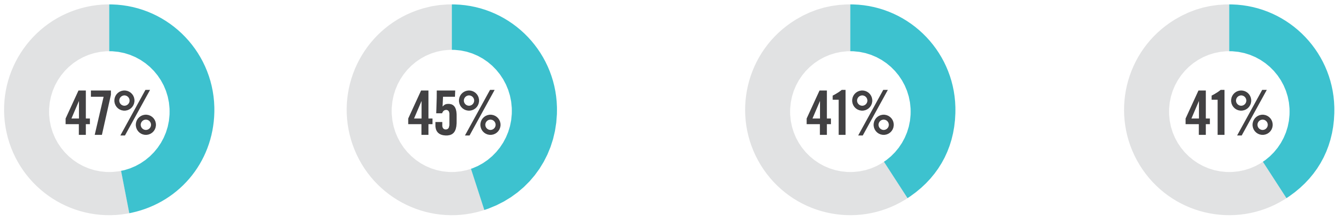
Reduce exposure to external threats

53%

Improve speed and accuracy of threat response

52%

Reduce number of breaches and infections



47% Reduce time to containment (prevent spread)

45% Reduce attack surface

41% Reduce exposure to internal threats

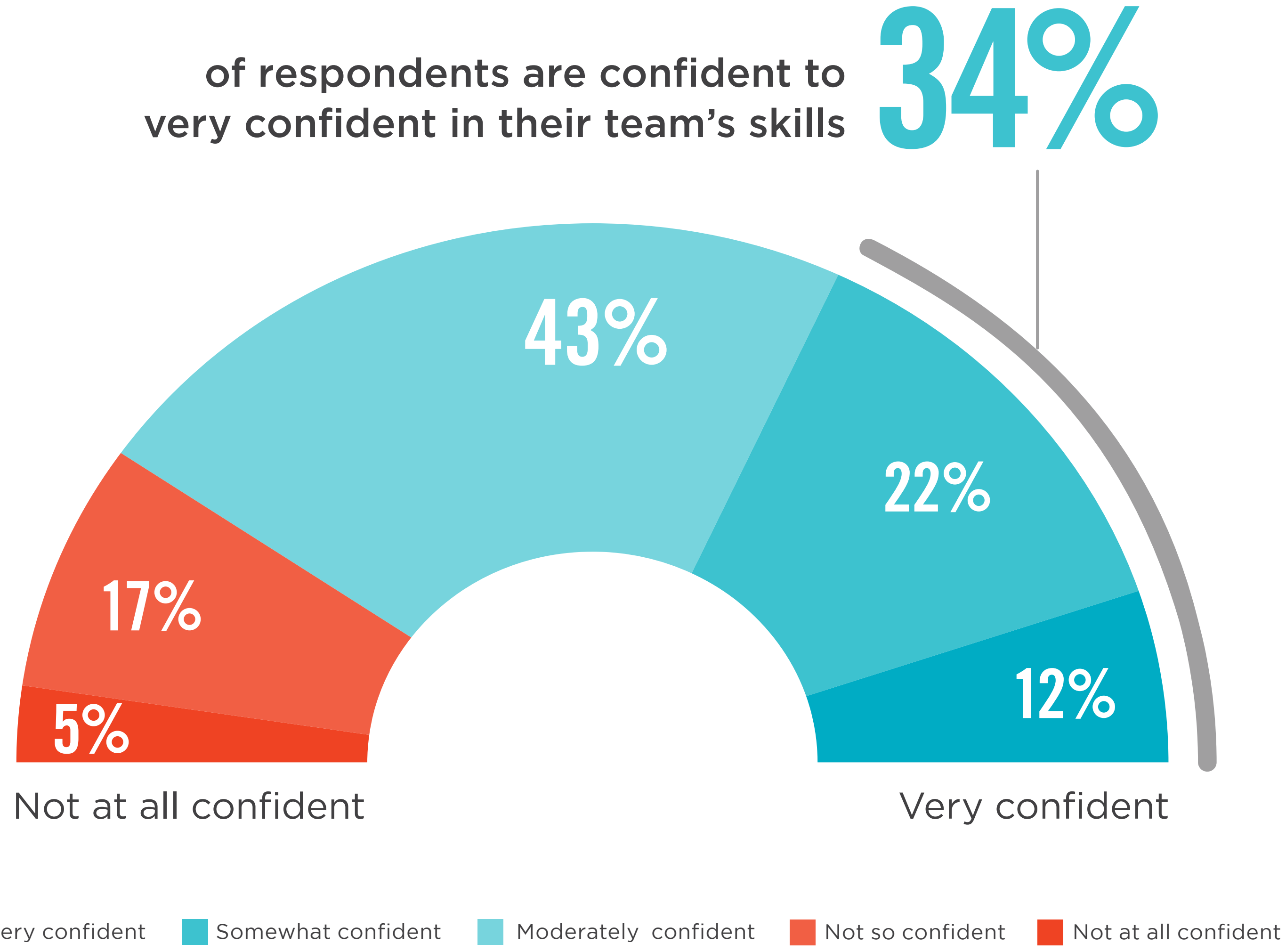
41% Optimize resources spent on threat response

Reduce dwell time from infection to detection 35% | Other 5%

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 1 percentage point increase over last year.

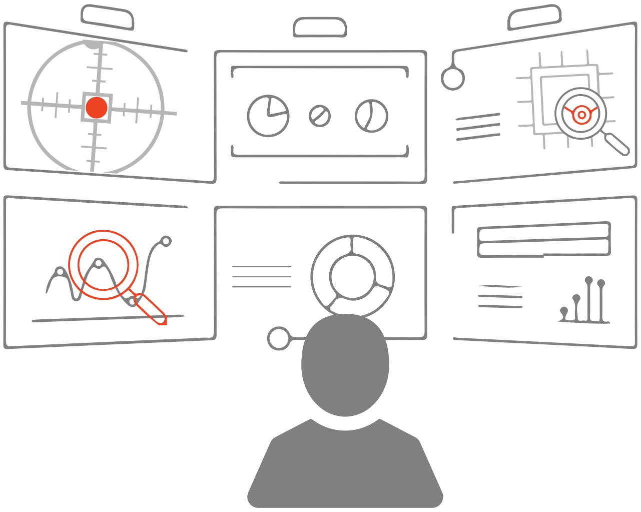
How confident are you in your security team's ability to uncover advanced threats?

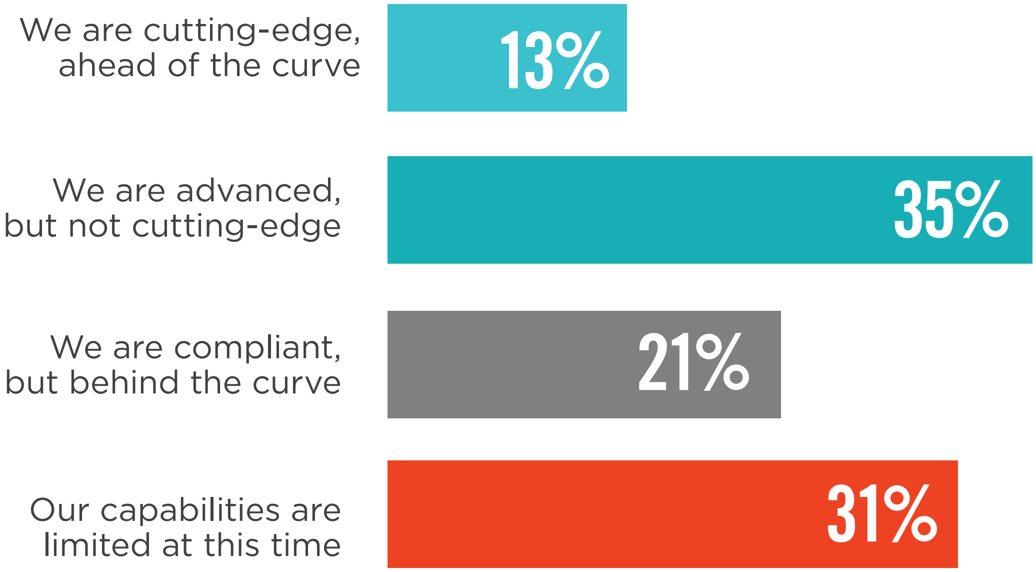


THREAT MANAGEMENT MATURITY

Security Operations Centers (SOCs) continually face rapidly evolving threats to secure and defend their environments against. From a maturity perspective, nearly half of SOCs (48%) believe they are cutting-edge or advanced in their ability to address emerging threats - up from 43% last year.

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

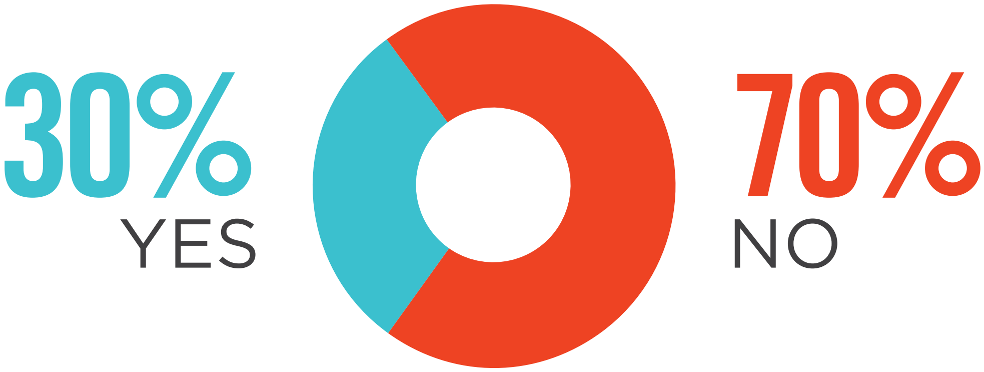


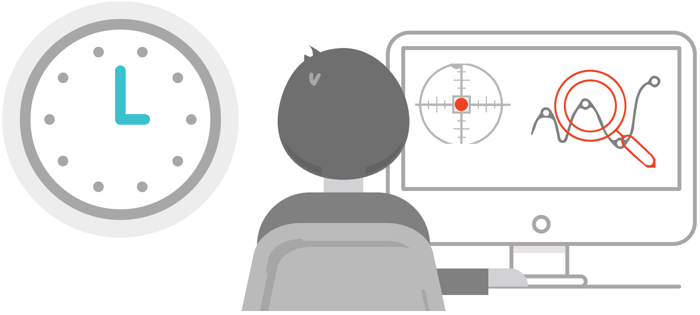

We are cutting-edge, ahead of the curve
13%
We are advanced, but not cutting-edge
35%
We are compliant, but behind the curve
21%
Our capabilities are limited at this time
31%

THREAT HUNTERS IN SOCS

Traditionally, SOC's approach to threats and the tools they use - such as antivirus, IDS, or SIEM - are reactive in nature, responding to detected threats. While we are seeing a continued shift toward early, proactive detection of new, unknown threats and quicker response, seventy percent of respondents still believe their SOC does not spend enough time proactively searching for new threats, slightly improving by 6 percentage points compared to last year.

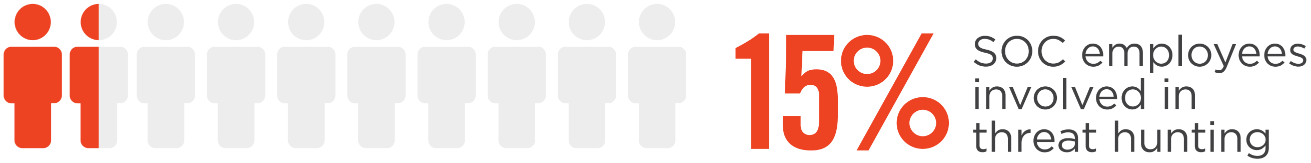
Do you feel enough time is spent searching for emerging and advanced threats at your SOC?





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

A majority of organizations have less than 5 security professionals dedicated to threat hunting. The average percentage of threat hunters in SOC teams is 15 percent, virtually unchanged from last year.



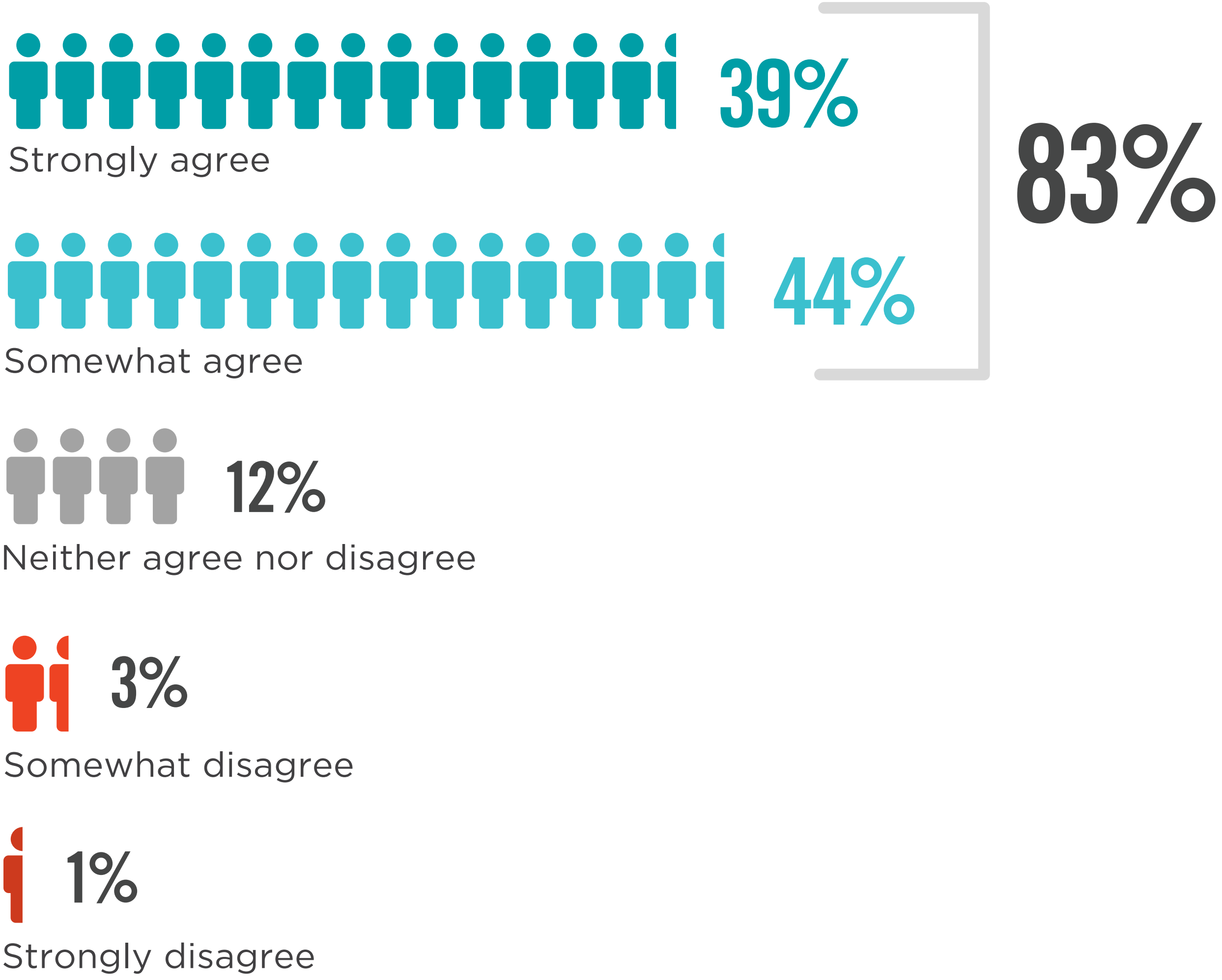
THREAT HUNTING PRIORITY

Although threat hunting is still an emerging discipline, 83 percent of organizations agree that threat hunting should be a top security initiative to provide early detection and reduce risk.

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

more than 80% of respondents

believe threat hunting is of major importance

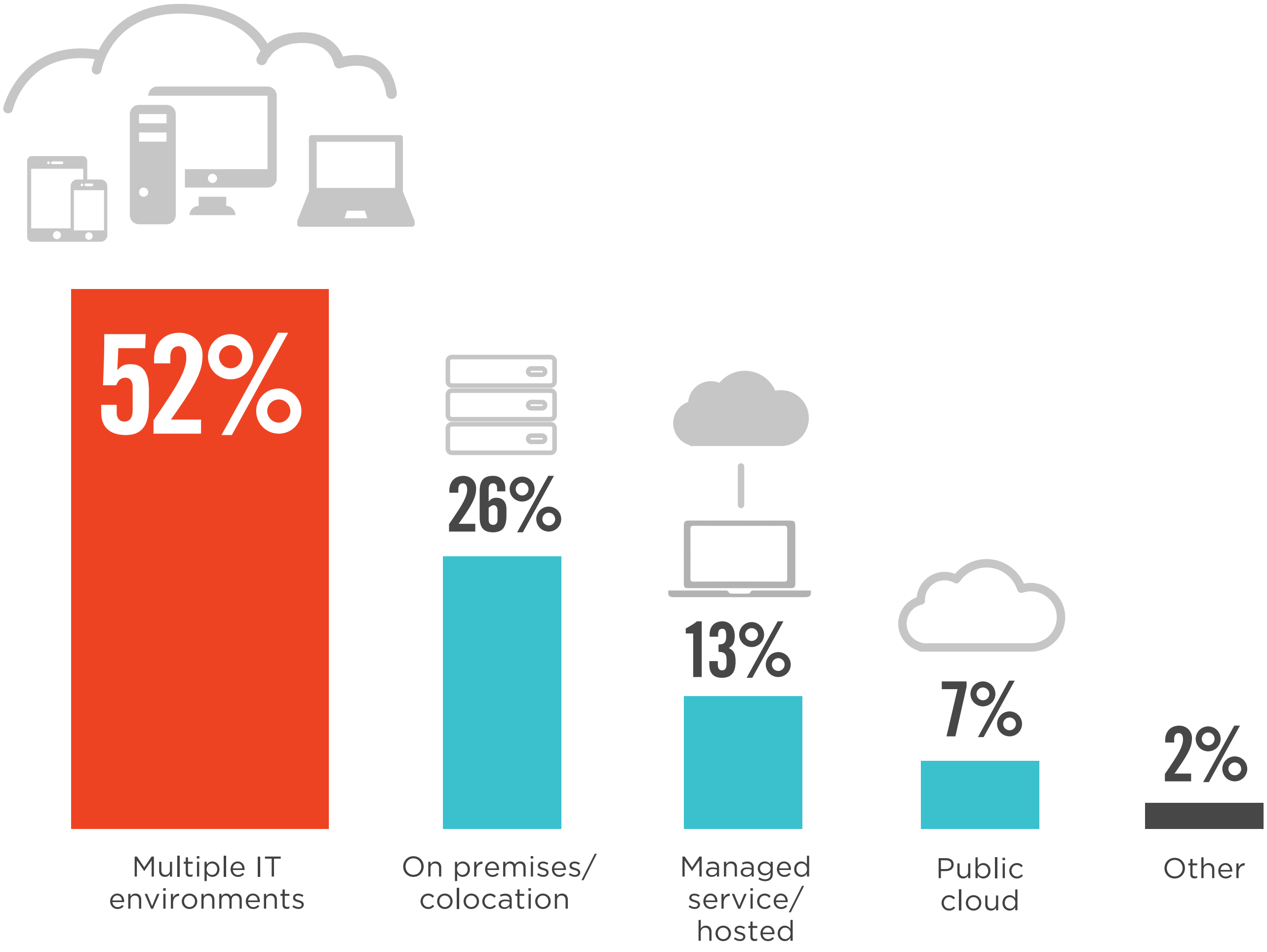


THREAT HUNTING ACROSS IT ENVIRONMENTS

More than half (52%) of respondents manage multiple IT environments (up from 49% last year), significantly increasing the complexity of orchestrating security across multiple IT environments.

By employing tools and automation alongside SOC personnel, organizations can make more 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?

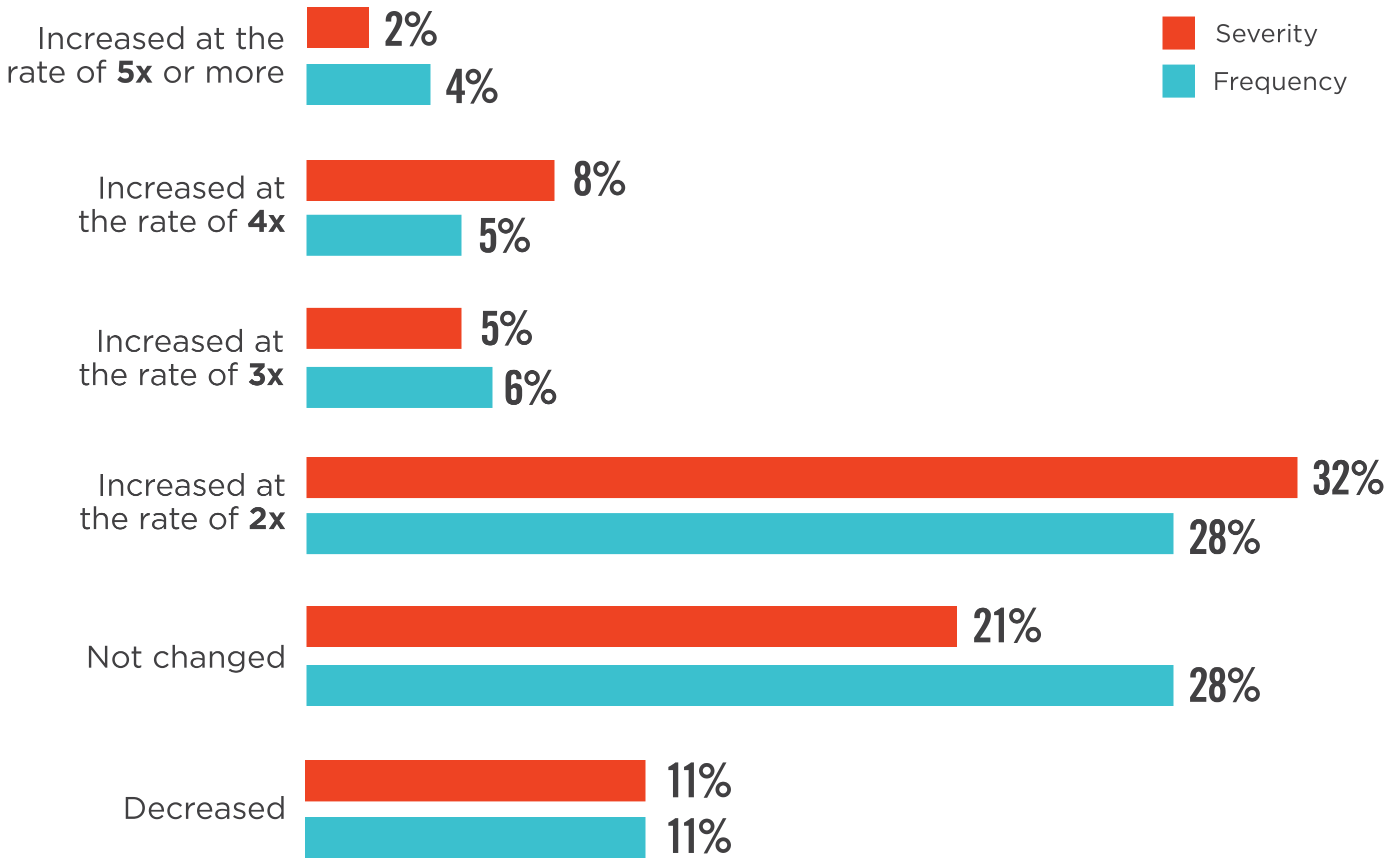


SEVERITY & FREQUENCY OF CYBER THREATS

Cybersecurity professionals are facing an ongoing challenge of constantly defending against security threats, not only in terms of volume of attacks but also their severity.

46 percent of organizations have experienced an increase of severity of attacks at a rate of 2x or more over the last 12 months (down from 51% last year). Less than half of the SOCs in our survey (43%) have experienced an increase in the frequency of cyber attacks over the last 12 months (down from 56% last year). Only 11 percent of respondents signaled a decrease in attack severity and frequency.

Which of the following best describes the change in severity and frequency of security threats faced by your organization in the past year?



Don't know severity 21% | Don't know frequency 19%

ATTACK DISCOVERY

Organizations report dwell times over 13 days. Nearly all respondents agree that attackers dwell on a network for some period of time before they're discovered by the SOC.

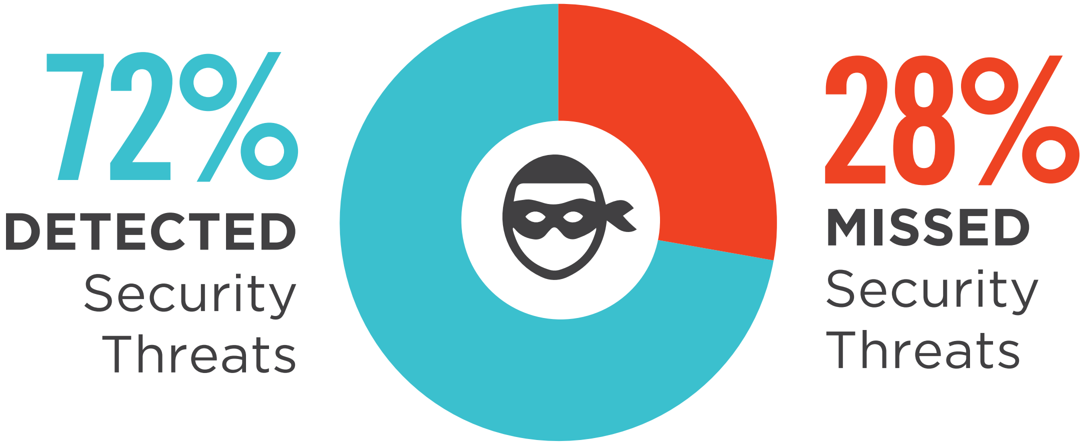
On average, how many days do attackers who breached your security defenses dwell in your network before they are discovered by your SOC?

13 DAYS

Average time attackers dwell on networks until discovered

SOCs report they are missing an average of 28 percent of security threats.

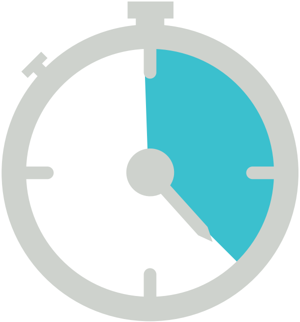
In a typical week at your SOC, what percentage of security threats do you feel are missed?



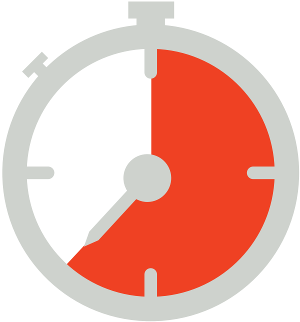
TIME SPENT ON THREAT HUNTING

Respondents spend an average of 62% of their time with alert triage and reacting to security threats compared to 38% of time spent proactively seeking threats. This represents a deterioration compared to last year's survey where 40% said they proactively detect threats in their SOC.

▶ **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?**



VS.

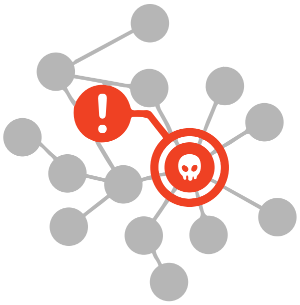


38%
Proactively
detecting threats

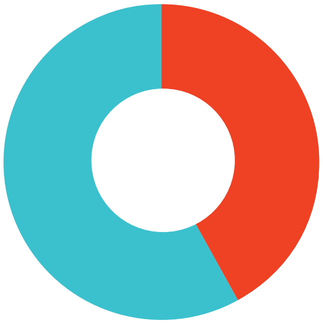
62%
Reacting to
security threats

SOCs report their traditional security tools are missing an average of 42% of advanced security threats.

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



58%
DETECTED
by traditional
security tools



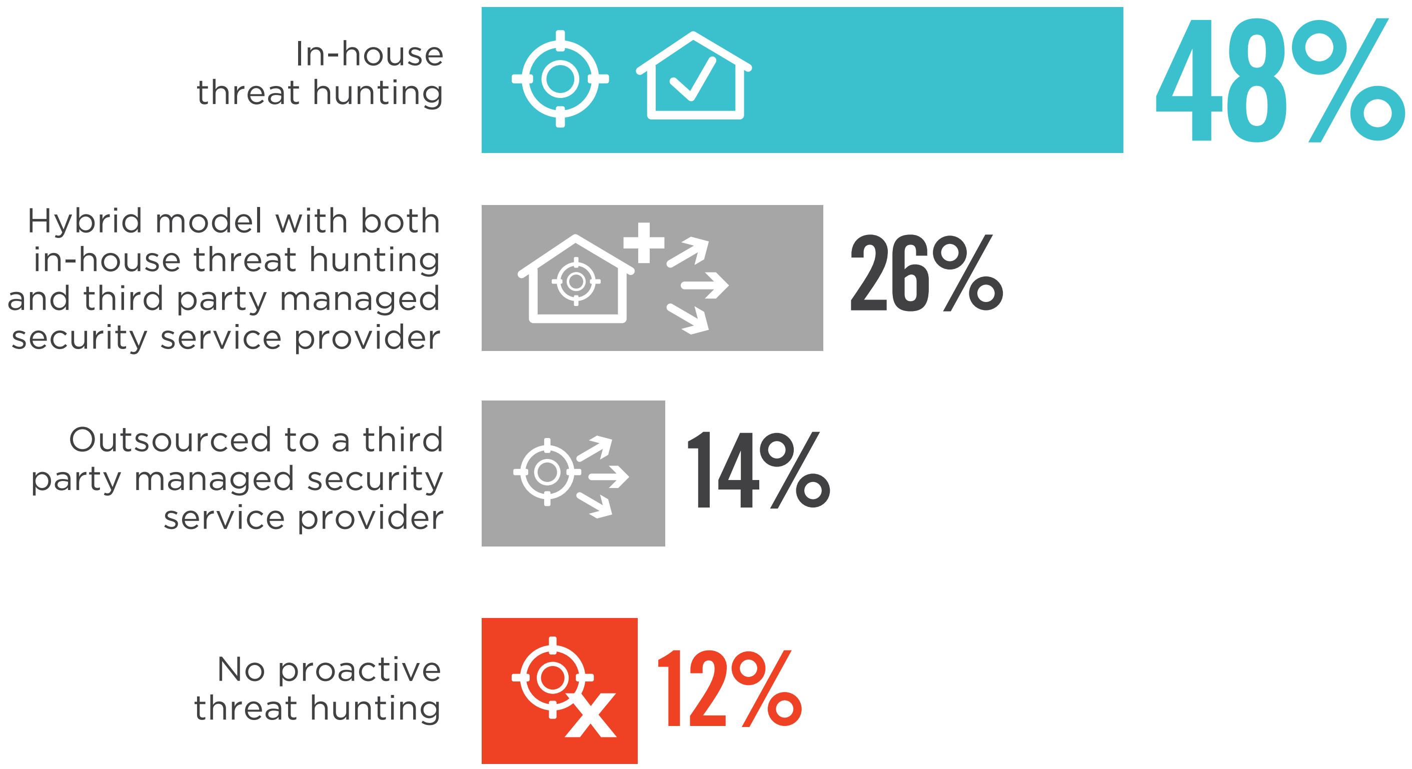
42%
MISSED
by traditional
security tools

SOURCING OF THREAT HUNTING

Today, almost half of organizations solely use in-house staff (48%) to proactively hunt threats. This is a marked decline from 56% of organizations who managed threat hunting in-house last year.

In the survey, 40% of organizations partner with Managed Security Service Providers (MSSPs) to help, either in a hybrid model or fully outsourced. This is up from 33% in last year's survey, reflecting a continuing trend towards outsourcing security operations.

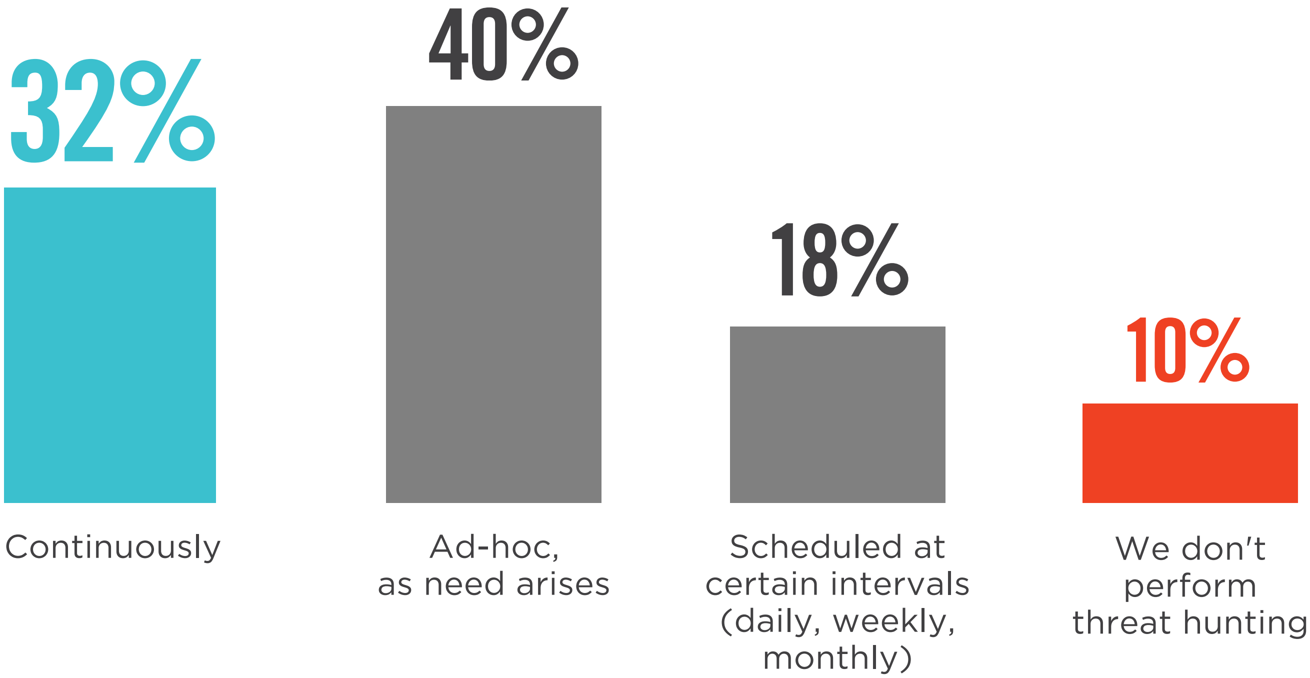
How is your threat hunting performed?



THREAT HUNTING FREQUENCY

Early, proactive detection of cyber breaches and rapid response can mitigate the impact of damages. While the number of organizations performing proactive threat hunting is increasing, only a third (32%) continuously hunt threats, and 40% perform threat hunting only reactively, as the need arises.

How frequently does your organization perform threat hunting?



DATA COLLECTION PRIORITIES

Effective threat hunting needs to include a wide array of data sources to detect anomalies and suspicious activity early on.

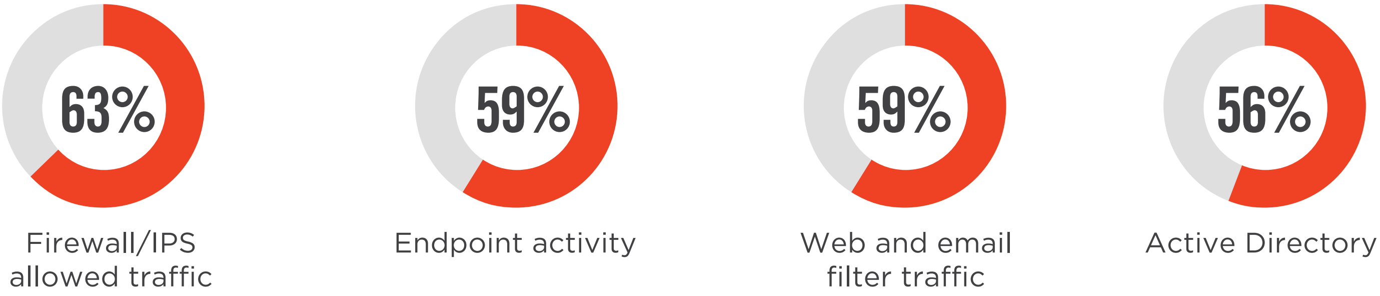
Most organizations prioritize system logs as the most important data sources to collect (66%), followed by firewall/IPS traffic (65%), and network traffic (63%). Bottom Line: there are numerous security relevant datasets to investigate. The best practice is not to depend solely on one source, but to 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?

66% System logs

65% Firewall/IPS denied traffic

63% Network traffic



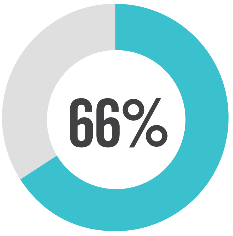
DNS traffic 50% | Server traffic 50% | User behavior 45% | File monitoring data 42% | Packet sniff/tcpdump 40%
Threat intelligence sources 32% | Web proxy logs 25% | Don't know/other 11%

THREAT INDICATORS

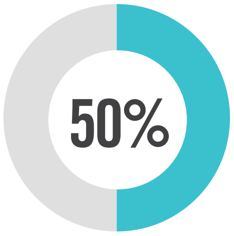
Understanding Indicators of Compromise (IOCs) allows organizations to develop effective defense methodologies that help with rapid detection, containment, and denial of future exploits. Knowing what IOCs to look for aids cybersecurity professionals in threat triage and remediation. Our research reveals that hunt teams most frequently investigate behavioral anomalies (69%), followed by suspicious IP addresses (66%), denied/flagged connections (50%), and suspicious domain names (48%).

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

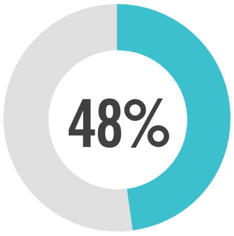
69% Behavioral anomalies (unauthorized access attempts, etc.)



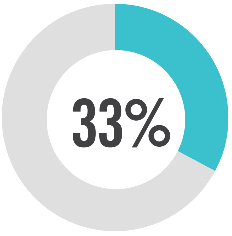
IP addresses



Denied/flagged connections



Domain names



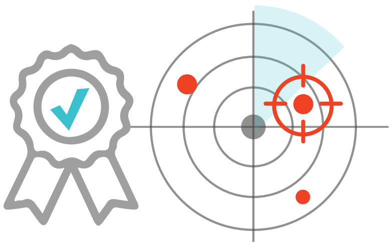
File names

Not sure/other 20%

BENEFITS OF THREAT HUNTING

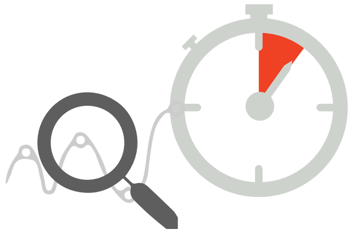
Threat hunting platforms provide security analysts with powerful tools to enable earlier detection, reduce dwell time, and improve defenses against future attacks. The top benefits organizations derive from threat hunting platforms include improved detection of advanced threats (62%), followed by reduced investigation time (59%), and saved time not having to manually correlate events (51%) - tied with creating new ways of finding threats (51%).

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



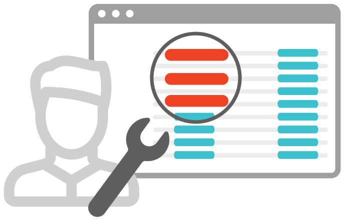
62%

Improving detection of advanced threats



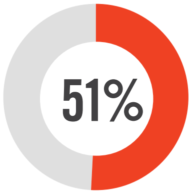
59%

Reducing investigation time

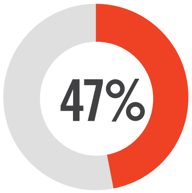


51%

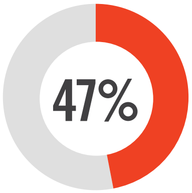
Saving time from manually correlating events



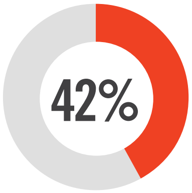
Creating new ways of finding threats



Reducing time wasted on chasing false leads



Discovering threats that could not be discovered otherwise



Saving time scripting and running queries

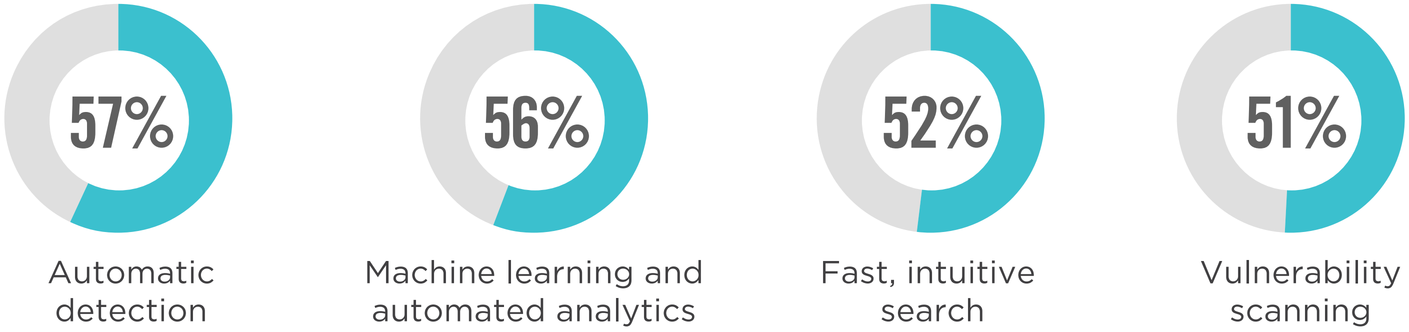
Reducing attack surface 37% | Reducing extra and unnecessary noise in the system 36% | Connecting disparate sources of information 31% | Other 6%

KEY THREAT HUNTING CAPABILITIES

The single most important capability that cybersecurity professionals consider critical to the effectiveness of their threat hunting tools is threat intelligence (64%). Automatic detection (57%), machine learning and automated analytics (56%), fast, intuitive search (52%), and vulnerability scanning (51%) round out the top five required capabilities.

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

64% Threat intelligence



User and Entity Behavior Analytics (UEBA) 49% | Integration and normalization of multiple data sources 46% | Full attack lifecycle coverage 44% | Intuitive data visualization 43% | Automated workflows 38% | Other 6%

THREAT HUNTING TECHNOLOGIES

The market for threat hunting tools is still maturing. Today's organizations cast a wide net and typically use multiple technologies in concert 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 evolving threat hunting posture.

The top technologies that organizations utilize for threat hunting are SIEM (55%) and NGFW/IPS/AV (53%), followed by vulnerability management (48%), and Network IDS (47%), ranked fourth in this year's survey.

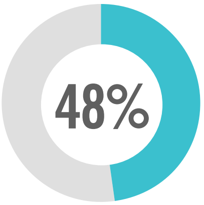
Which technologies do you use as part of your organization's threat hunting approach?

55%

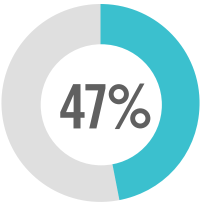
SIEM

53%

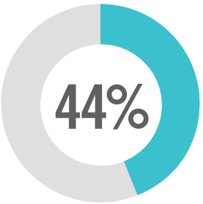
NGFW, IPS, AV,
web application firewall, etc.



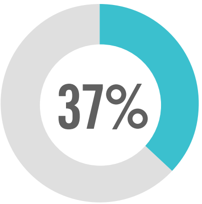
Vulnerability management



Network IDS



Anti-phishing or other messaging security software



Threat intelligence platform

Enrichment and investigation tools 30% | Orchestration (e.g., Phantom, Hexadite, Resilient, etc.) 15% | Not sure/other 16%

THREAT HUNTING INTEGRATION

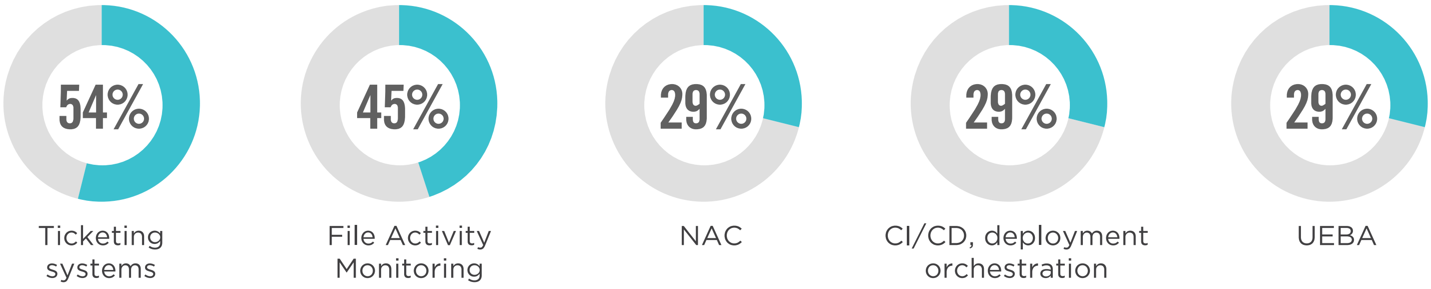
Organizations are integrating a multitude of technologies into their threat hunting platform. Incident response (69%) takes the top spot, followed by SIEM (61%) and active directory (57%) - all three unchanged in priority compared to last year's survey.

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

69% Incident response

61% SIEM

57% Active directory

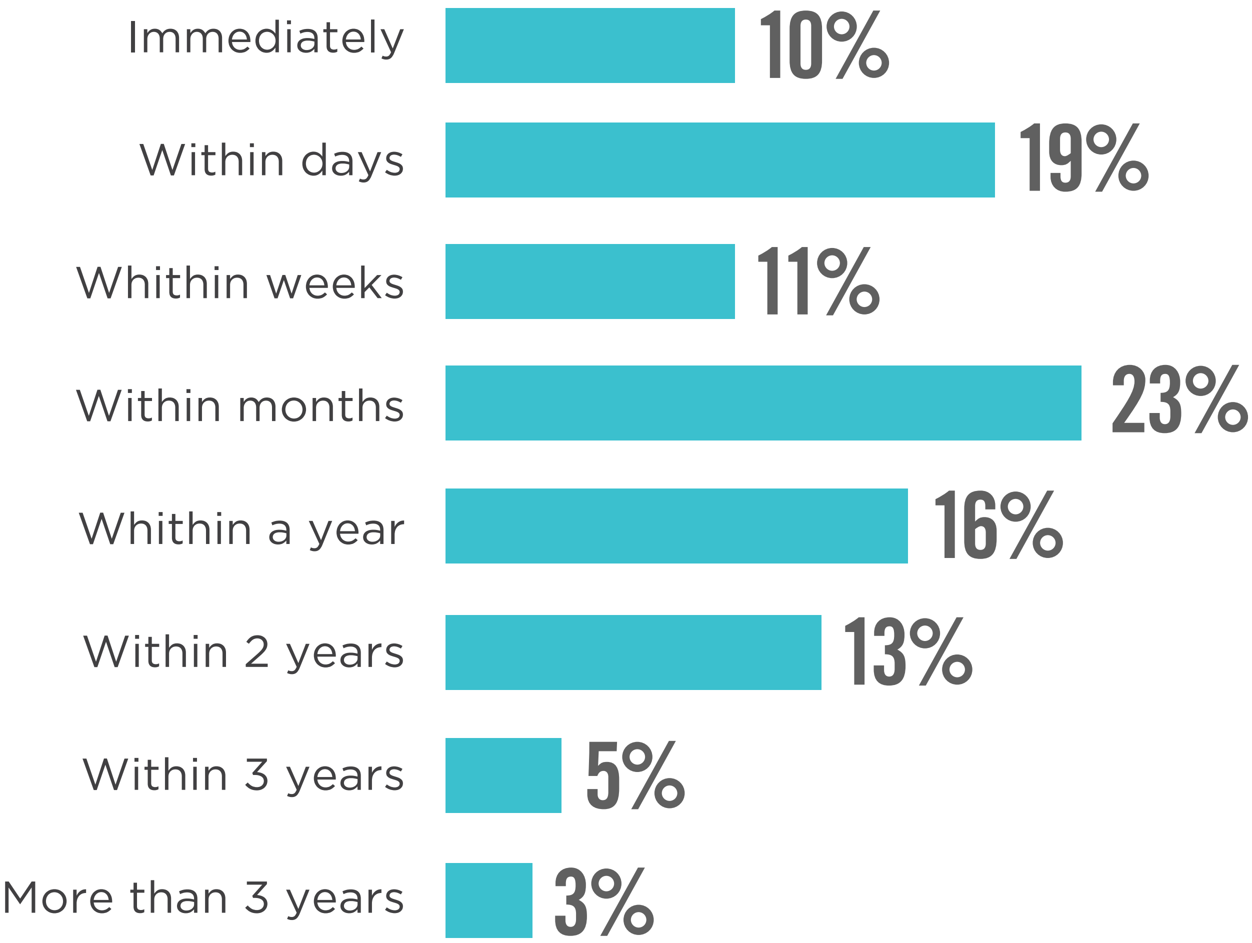


Other 6%

THREAT HUNTING INVESTMENT

When asked how long it takes SOCs to break even on the investment in threat hunting platforms, 79% confirm they reach the breakeven point within a year of deployment.

How long does it take for a SOC to break-even on the investment of a threat hunting platform?



THREAT HUNTING DATA

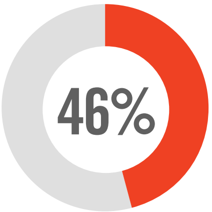
SOCs collect and analyze multiple data sources to add context to their threat hunting activities. The most utilized data includes external threat intelligence feeds (57%), file activity data (51%), and system patch status (47%).

Which contextual information do you use as part of your Threat Hunting data?

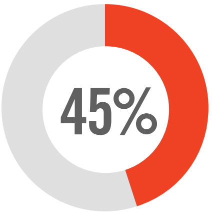
57%
External Threat Intel feeds

51%
File Activity Data

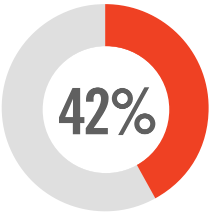
47%
System patch status



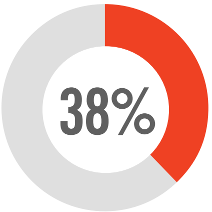
Data Classification



Source blacklist



User permission data



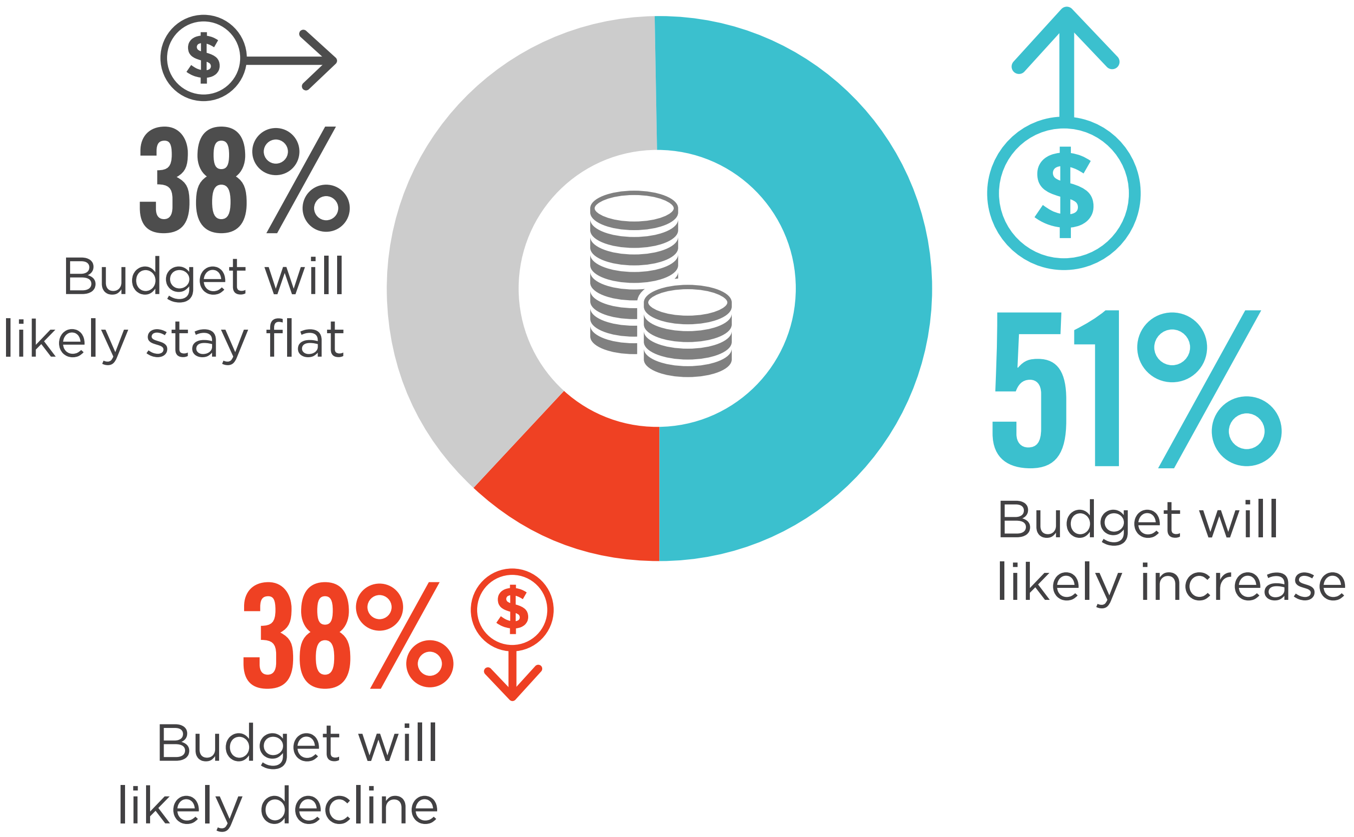
File permission data

Other 9%

THREAT HUNTING BUDGET

A majority of SOCs (51%) will see threat hunting budgets increase over the next 12 months to invest in security staff, new threat hunting technologies, and managed security services.

How is your organization's threat hunting budget going to change in the next 12 months?

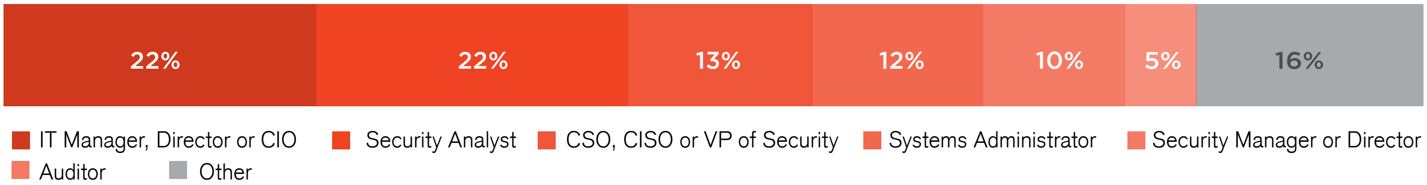


21% of IT security budget will be allocated to threat hunting

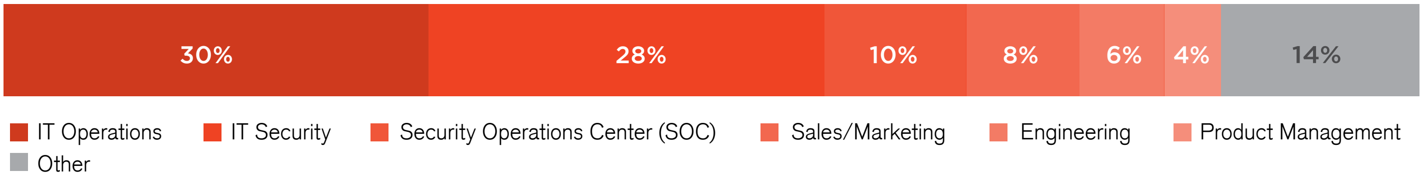
METHODOLOGY & DEMOGRAPHICS

This Insider Threat Report is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in February of 2019 to gain deep insight into the latest trends, key challenges and solutions for insider threat management. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

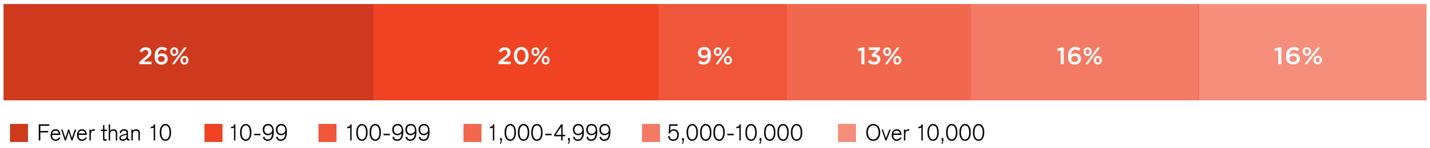
CAREER LEVEL



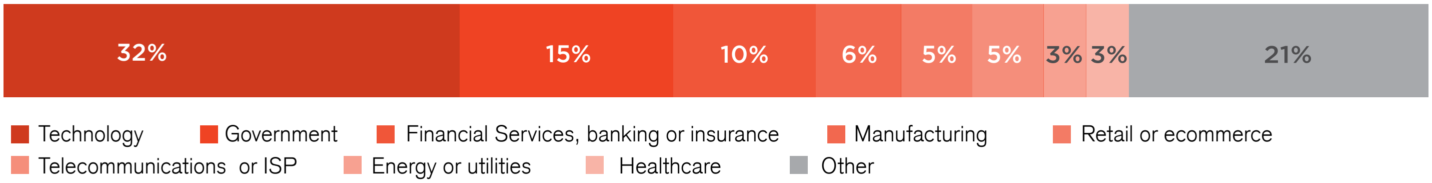
DEPARTMENT



COMPANY SIZE



INDUSTRY



DOMAINTOOLS

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work.

Learn more about how to connect the dots on malicious activity at www.domaintools.com
or follow us on Twitter:@domaintools