2020

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 operations. They are discovering that proactive threat hunting can reduce the risk and impact of threats while improving defenses against new attacks.

In 2020, 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.

Key finding include:

- Although threat hunting is still an emerging discipline, 93% of organizations agree that threat hunting should be a top security initiative to provide early detection and reduce risk. Fifty-three percent strongly agree, an increase of nine percentage points since last year's survey.
- More than half of organizations (61%) have experienced an increase in the severity of attacks at a rate of 2x or more over the last 12 months. A similar share of SOCs (64%) have experienced an increase in the frequency of cyber attacks over the last 12 months.
- Understanding Indicators of Compromise (IOCs) allows organizations to develop effective defense methodologies that help with rapid detection, containment, and denial of future exploits. Our research reveals that hunt teams most frequently investigate behavioral anomalies (74%), followed by suspicious IP addresses (59%) and denied/flagged connections (59%, tied).
- When asked whether organizations are seeing challenges when hiring of threat hunting professionals as a remote workforce in the wake of the COVID epidemic, four of six say that hiring of threat hunters will become more difficult. Half say that hiring difficulty will be about the same, only 10% see hiring to be less difficult.

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

We hope you will enjoy it.

Thank you,

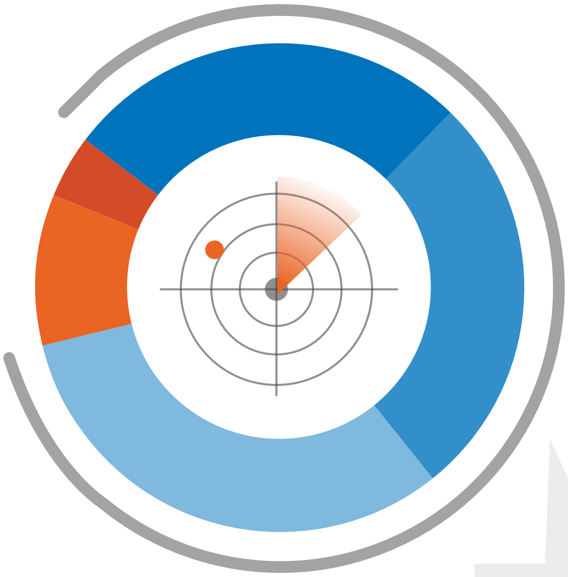
Holger Schulze

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 9 in 10 respondents have at least some knowledge or are very knowledgeable about the topic.

How familiar are you with threat hunting?



86%

Have a moderate or high degree of knowledge about threat hunting

THREAT HUNTING GOALS

The primary goal of any comprehensive cybersecurity program is to protect an organization's cyber resources against external and internal threats. The top three objectives that threat hunting programs focus on include reducing exposure to external threats (57%), improving the speed and accuracy of threat response (54%), and reducing the number of breaches (53%).

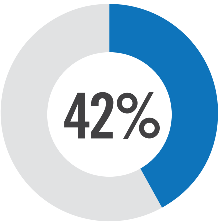
What are the primary goals of your organization's threat hunting program?

53%

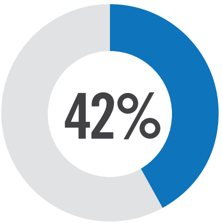
Reduce exposure
to internal threats

50%

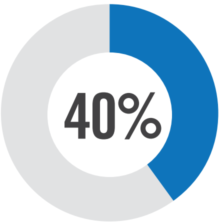
Reduce attack
surface



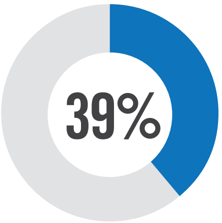
Reduce dwell time from infection to detection



Reduce exposure to external threats



Reduce time to containment (prevent spread)



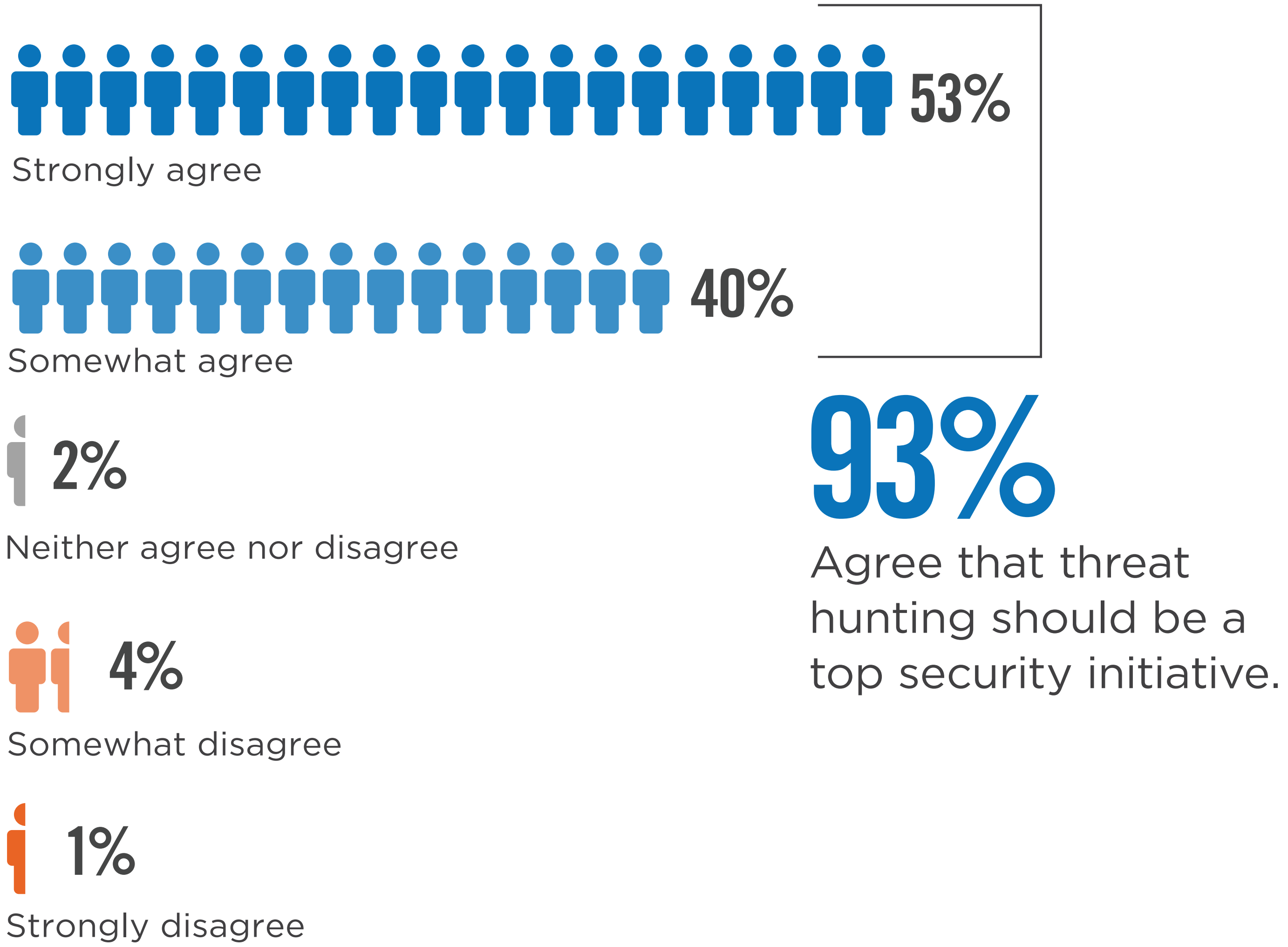
Reduce number of breaches and infections

Improve speed and accuracy of threat response 36% | Optimize resources spent on threat response 31% | Other 7%

THREAT HUNTING PRIORITY

Although threat hunting is still an emerging discipline, 93% of organizations agree that threat hunting should be a top security initiative to provide early detection and reduce risk. Fifty-three percent strongly agree, an increase of nine percentage points since last year's survey.

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



INVESTMENTS FOR BETTER THREAT HUNTING

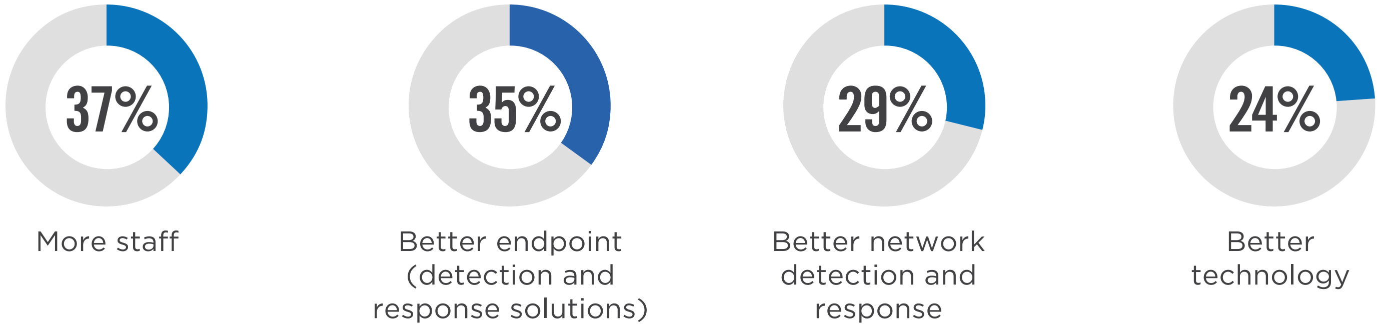
When asked about the investments that would help organizations improve their threat hunting abilities, training for existing staff made the top choice (39%). This is followed by investments in a cluster of technologies, including SIEM (39%) and better threat feed (39%).

What investments would make the biggest difference in your threat hunting abilities?

39%
More training for existing staff

39%
Better SIEM

39%
Better threat feeds

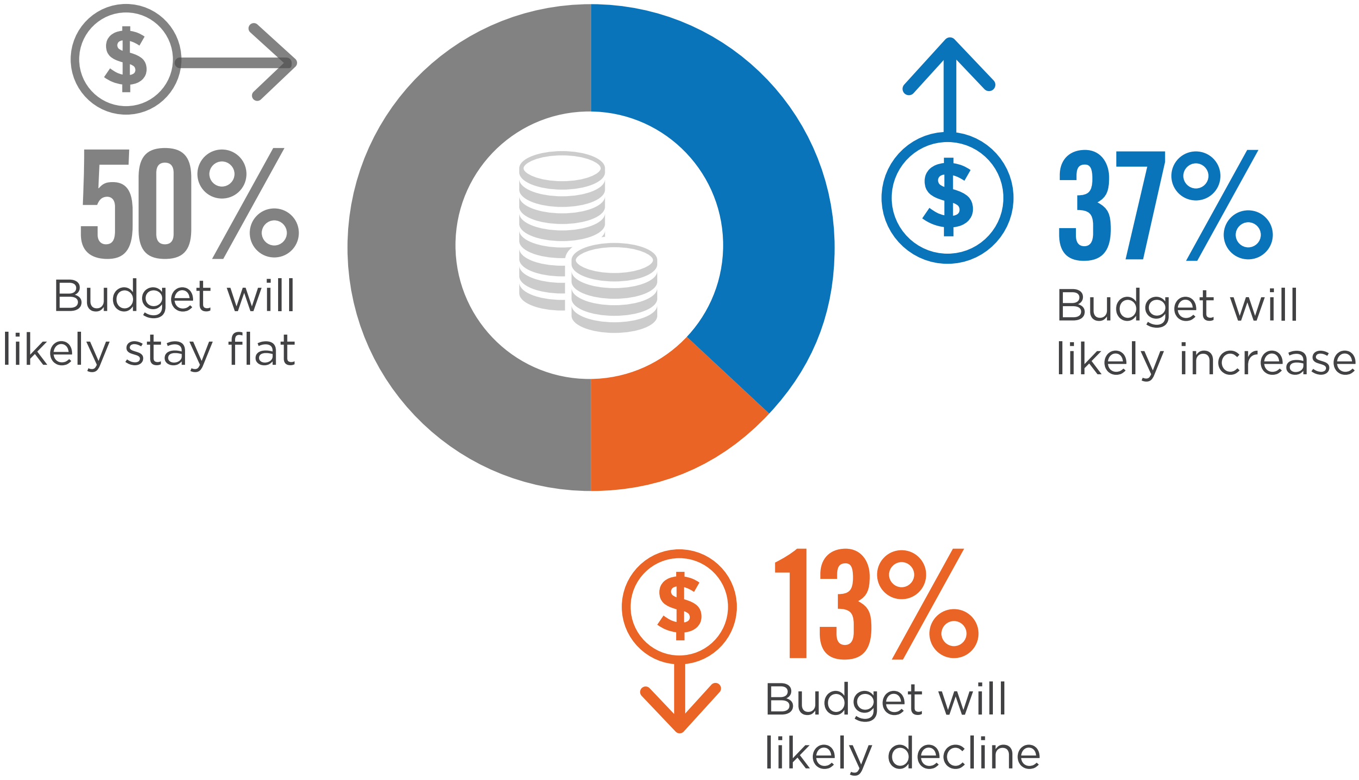


More technology 16% | Other 4%

THREAT HUNTING BUDGET

Half of SOCs (50%) will likely see threat hunting budgets stay flat over the next 12 months.Thirty-seven percent willlikely increase budget to invest in security staff, training, new threat hunting technologies, and managed security services.

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

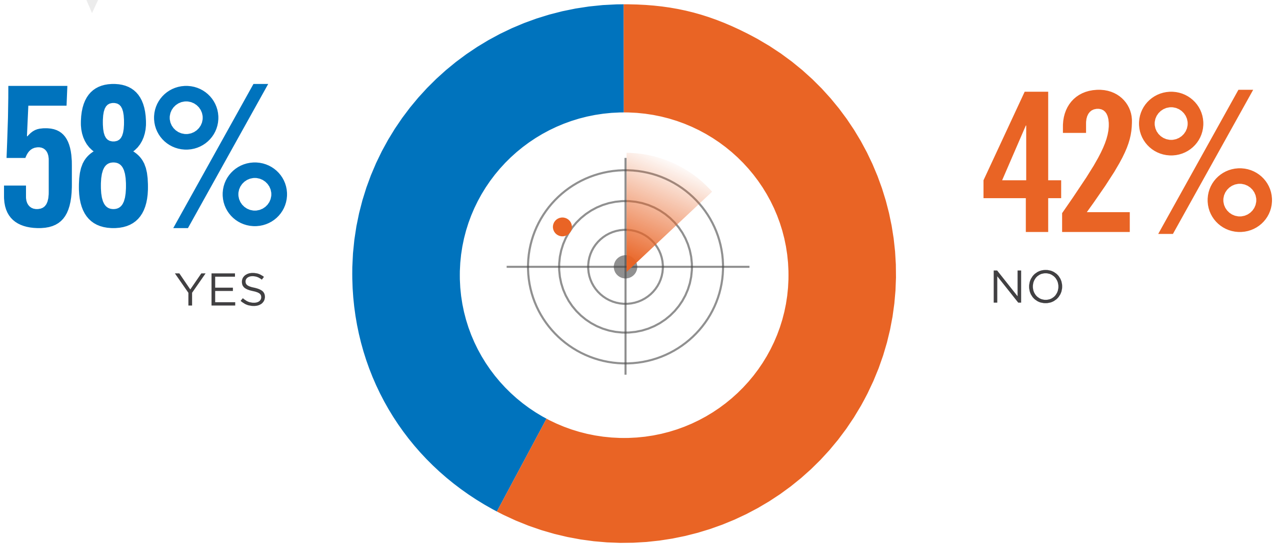


INTENTIONS TO DEVELOP A THREAT HUNTING PROGRAM

More than half (58%) of organizations that do not have an established threat hunting program plan to build one over the next three years. This is consistent with the viewpoint that threat hunting should be a top security initiative.

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?

More than half of organizations plan to build one over the next three years.

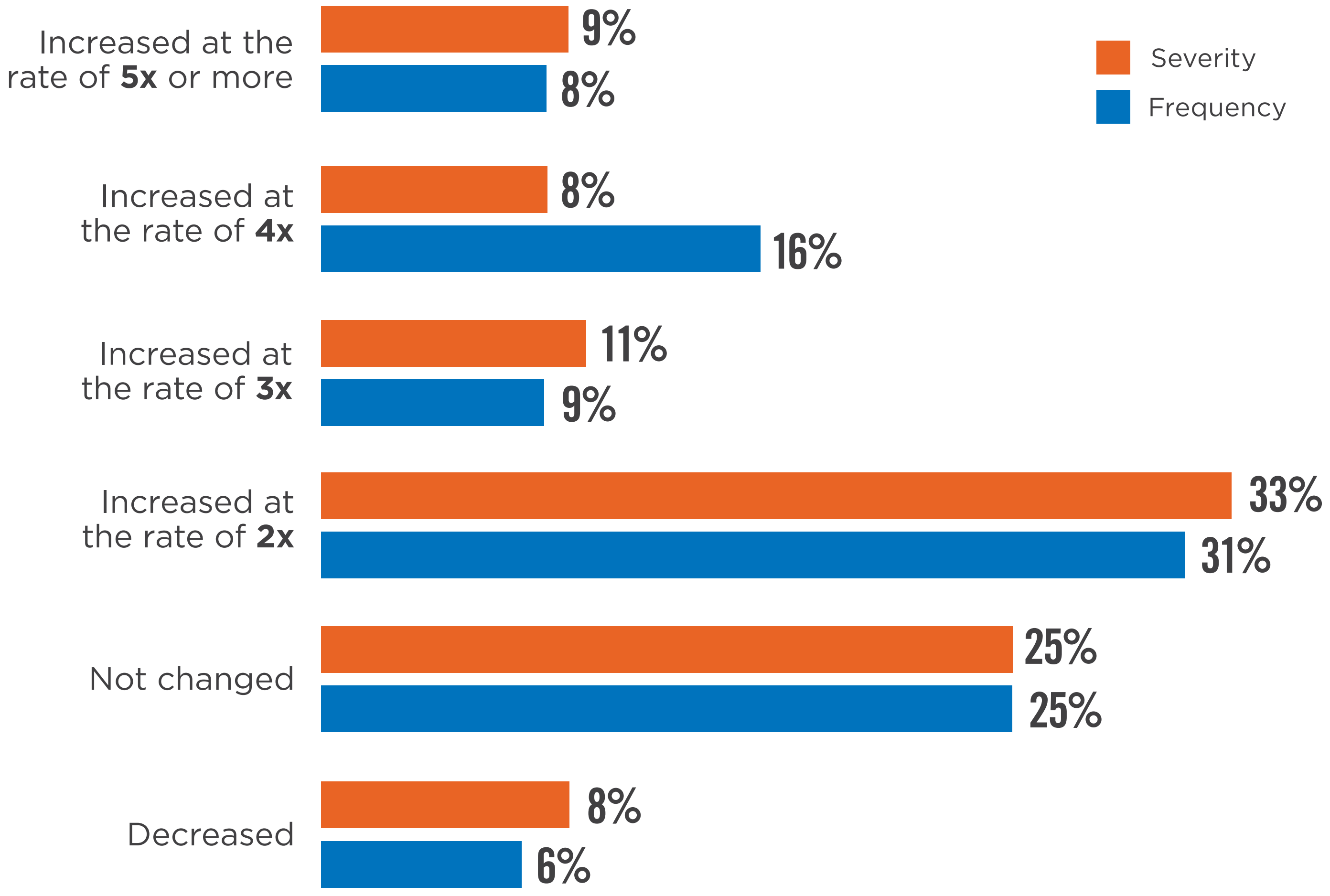


SEVERITY & FREQUENCY OF CYBER THREATS

Cybersecurity professionals are facing an ongoing challenge of constantly defending against security threats, not only in terms of frequency of attacks but also their severity. More than half of organizations in our survey (61%) have experienced an increase in the severity of attacks at a rate of 2x or more over the last 12 months.

A similar share of SOCs in our survey (64%) have experienced an increase in the frequency of cyber attacks over the last 12 months. Only few respondents signaled a decrease in attack severity (8%) and frequency (6%).

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

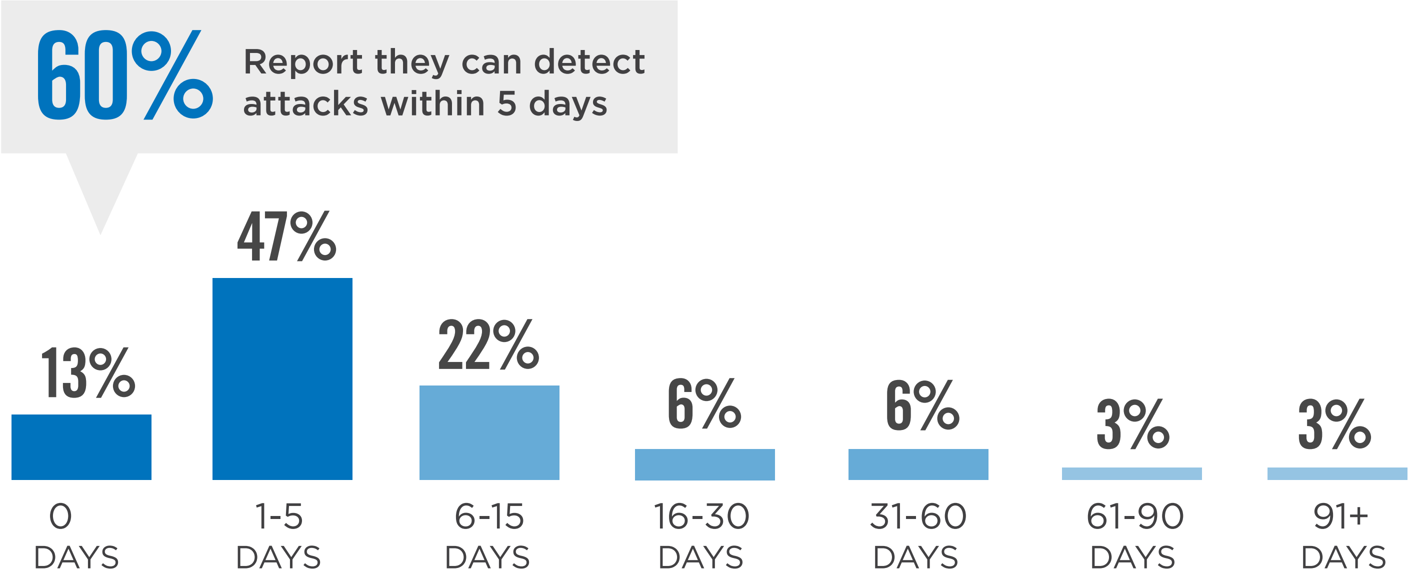


Don't know severity 6% | Don't know frequency 5%

ATTACK DISCOVERY

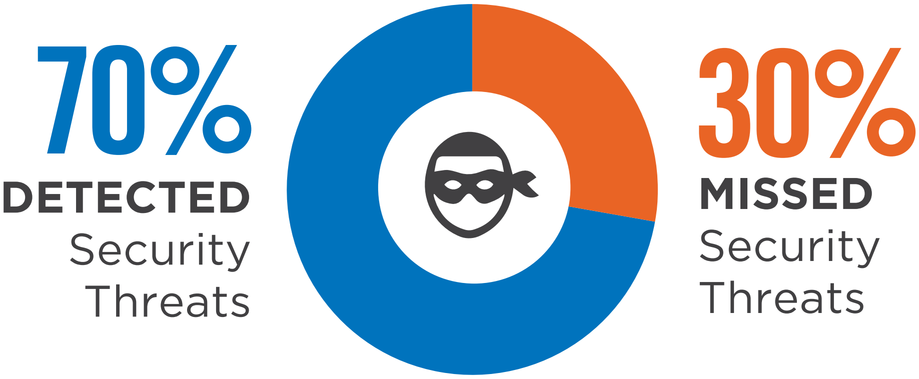
Only 13% report they can detect attacks within 1 day, almost half (47%) within 5 days. Nearly all respondents agree that attackers typically dwell on a network for some period of time before they're discovered by the SOC.

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



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

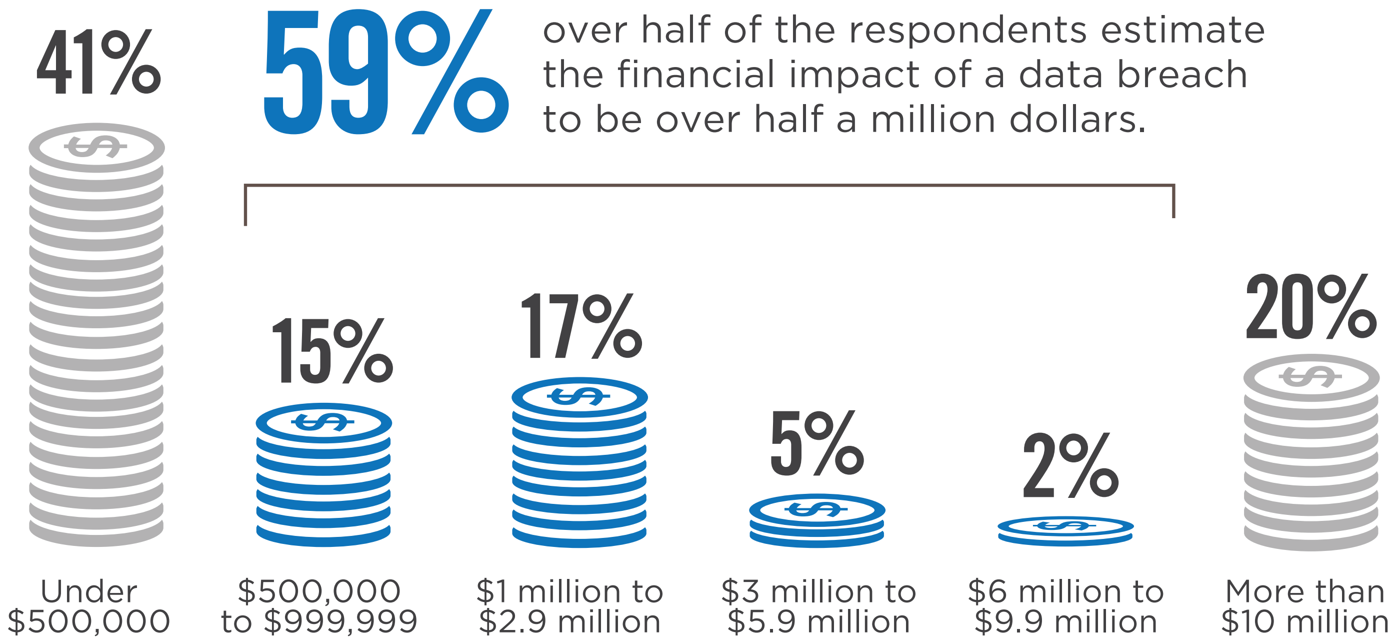
SOCs report they are missing an average of 30 percent of security threats.



FINANCIAL IMPACT

The financial impact of a data breach can vary based on the data and processes impact by the security incident. Over half of the survey respondents (59%) estimate the financial impact of a data breach to be over half a million dollars.

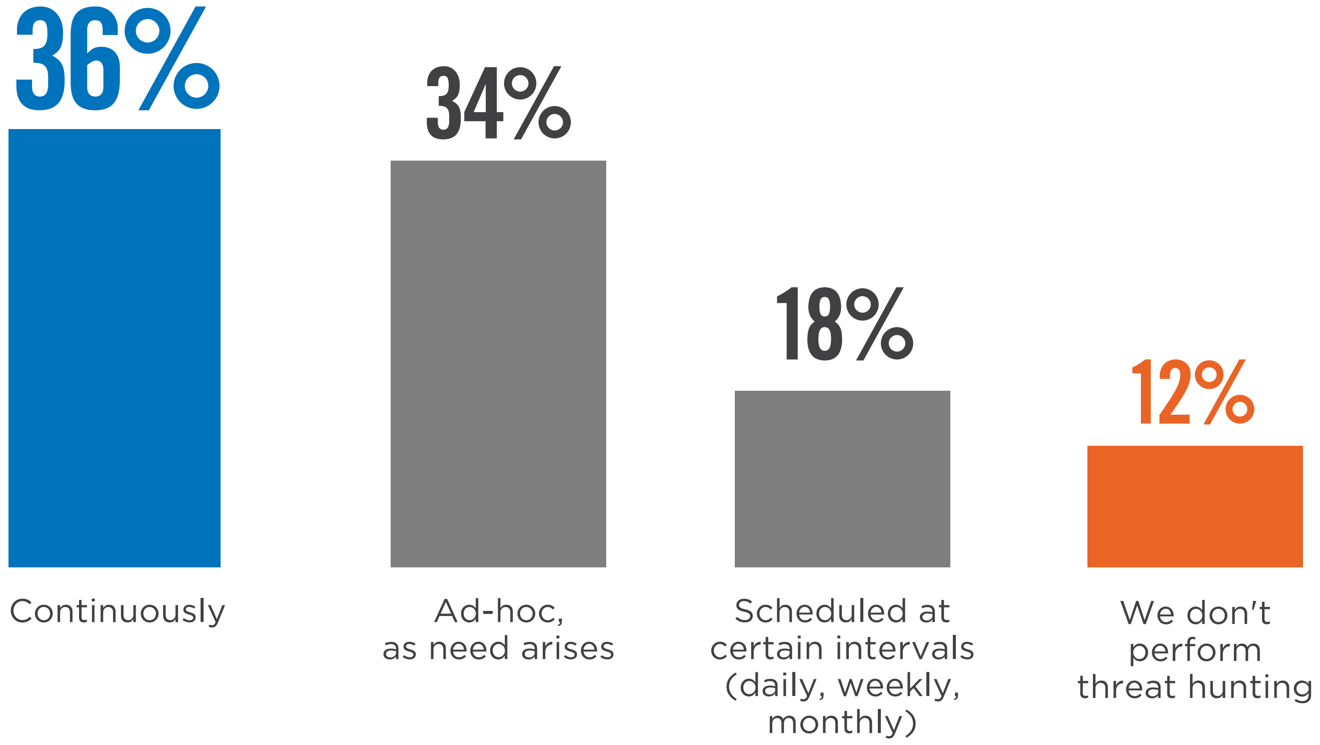
▶ **What is the estimated financial impact of a security threat that goes undetected and results in a breach at your organization?**



THREAT HUNTING 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 about a third (36%) continuously hunt threats, and 34% perform threat hunting only reactively, as the need arises.

How frequently does your organization perform threat hunting?



KEY SECURITY CHALLENGES

The survey reveals that cybersecurity professionals prioritize timely detection of advanced threats (56%) as the top challenge for their SOC. This is followed by a lack of expert security staff to mitigate such threats (48%) and lack of confidence in automation tools catching all threats (40%).

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

56%

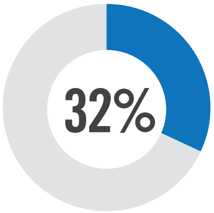
Detection of advanced threats (hidden, unknown, and emerging)

48%

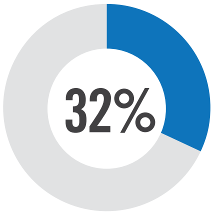
The lack of expert security staff to assist with threat mitigation

40%

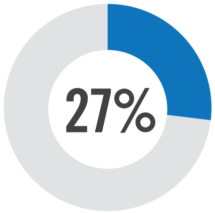
Lack of confidence in automation tools catching all threats



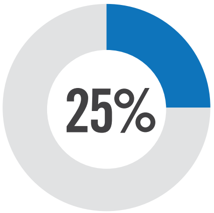
Too much time wasted on false positive alerts



Lack of visibility into critical data due to encryption



Working with outdated SIEM tools and SOC infrastructure



Lack of proper reporting tools

Slow response time to advanced threats 24% | Other 14%

DATA COLLECTION SOURCES

Most organizations prioritize data from traffic denied by firewall/IPS (77%) together with firewall/IPS traffic (73%). This is followed by web and email filter traffic and endpoint activity tied with 70%. 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.

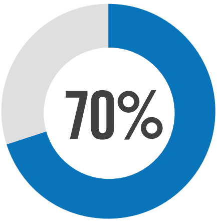
What kind(s) of data does your security organization collect and analyze?

77%

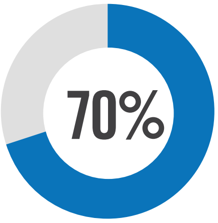
Firewall/IPS denied traffic

73%

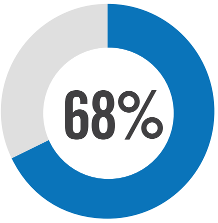
Firewall/IPS allowed traffic



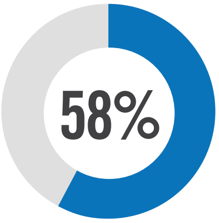
Web and email filter traffic



Endpoint activity



System logs



DNS traffic

Threat intelligence sources 58% | Network traffic 57% | Active Directory 55% | Web proxy logs 47% | Server traffic 47% | Packet sniff/tcpdump 40% | User behavior 40% | File monitoring data 37% | Don't know/other 12%

THREAT HUNTING DATA

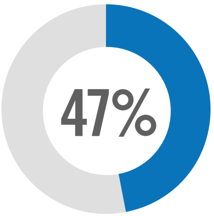
SOCs collect and analyze multiple data sources to add context to their threat hunting activities. The most utilized data includes external threat intelligence feeds (60%), file activity data (51%), and user behavior data (51%).

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

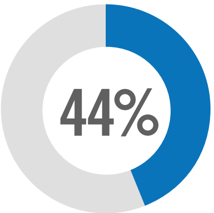
60%
External threat intel feeds

51%
File activity data

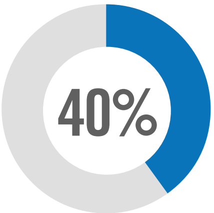
51%
User behavior data



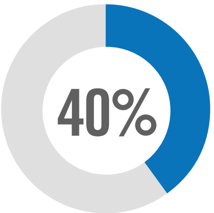
System patch status



Asset Inventory Data



Source blacklist



Network Protocol Data

Data Classification 38% | File permission data 38% | User permission data 38% | Other 2%

MOST VALUABLE DATA SOURCES

Among the many data sources organizations analyze in order to find hidden threats, activity logs are considered most valuable by a third (32%). This is followed by threat intelligence data (23%), endpoint data (20%) and network data (18%).

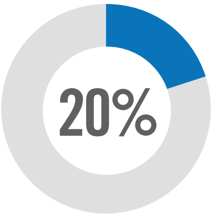
What is the most valuable data source for your organization when threat hunting or investigating known threats?

32%

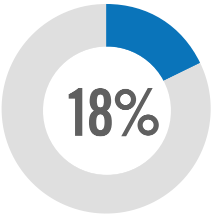
Activity logs

23%

Threat intelligence feeds



Endpoint Data



Network Data

Other 7%

THREAT INDICATORS

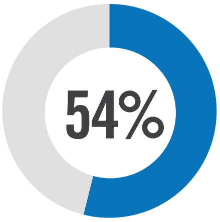
Understanding Indicators of Compromise (IOCs) allows organizations to develop effective defense methodologies that help with rapid detection, containment, and denial of future exploits. Our research reveals that hunt teams most frequently investigate behavioral anomalies (74%), followed by suspicious IP addresses (59%) and denied/flagged connections (59%).

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

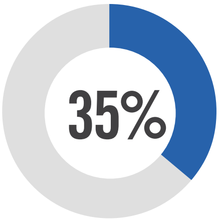
74%
Behavioral anomalies
(unauthorized access attempts, etc)

59%
Domain names

59%
Denied/flagged connections



IP addresses



File names

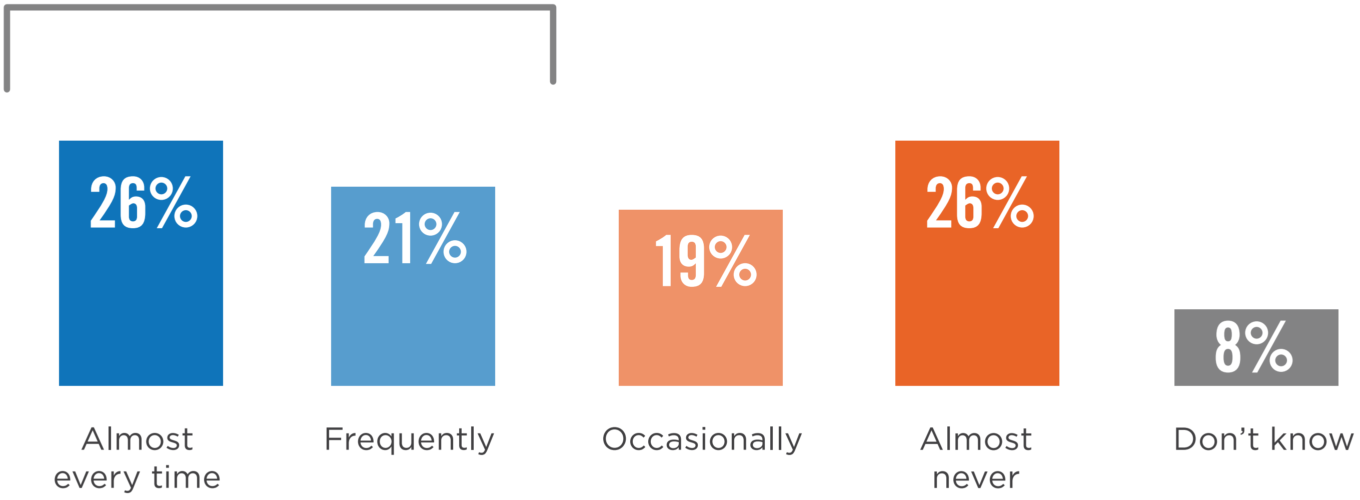
Not sure/other 13%

INSIGHTS INTO ADVERSARIES

About half (47%) of security teams evaluate adversary domains and IP addresses to a significant degree as part of their threat hunting process.

How often do you develop insights into adversary infrastructure (domains and IP addresses) as part of your hunt activities?

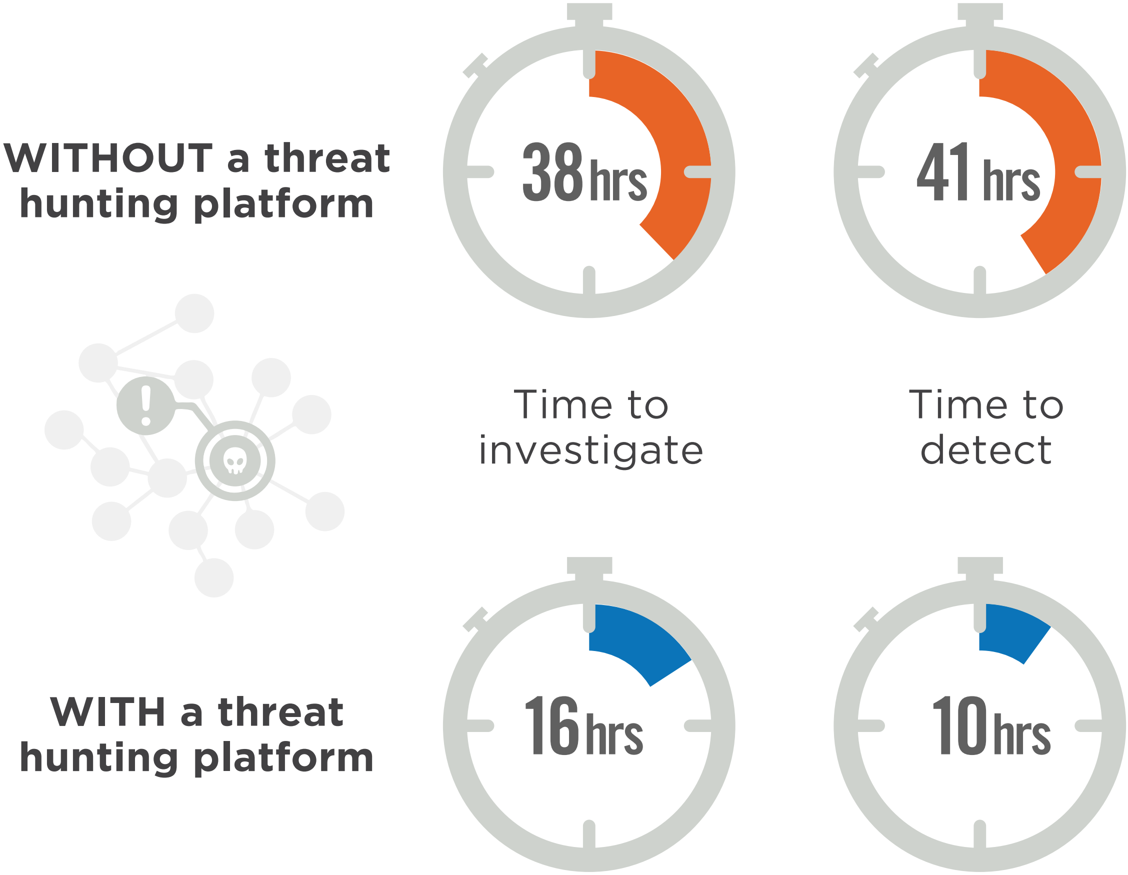
47% Of security teams evaluate adversary domains and IP addresses as part of their threat hunting process.



THREAT HUNTING PLATFORM IMPACT

Deploying a threat hunting platform can pay off significantly. While it takes organizations without a threat hunting platform an average of 41 hours to detect a threat, organizations that utilize a threat hunting platform reduce detection time to only 10 hours. Similarly, time to investigate is dramatically reduced by threat hunting platforms, from 38 hours down to 16, on average.

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



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 (63%), followed by reduced investigation time (55%), and saving time manually correlating events (47%).

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

63%

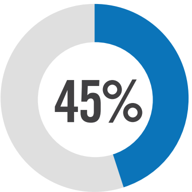
Improving detection of advanced threats

55%

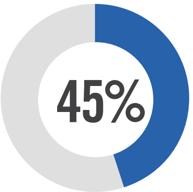
Reducing investigation time

47%

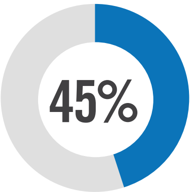
Saving time manually correlating events



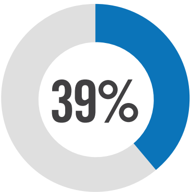
Reducing time wasted on chasing false leads



Reducing attack surface



Discovering threats that could not be discovered otherwise



Connecting disparate sources of information

Saving time scripting and running queries 37% | Reducing extra and unnecessary noise in the system 37% | Creating new ways of finding threats 29% | Other 4%

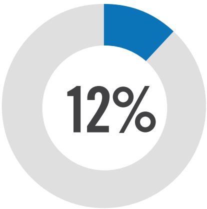
REASONS FOR LACK OF THREAT HUNTING TOOLS

Lack of budget is the main reason for organization that don’t deploy a dedicated threat hunting tool (32%), followed by platform fatigue caused by too many security tools (18%).

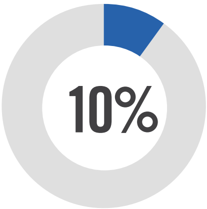
What is the main reason your SOC does not have a dedicated threat hunting platform for its security analysts?

32%
Lack of budget

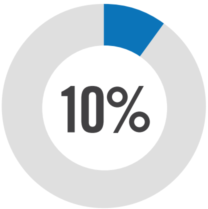
18%
Platform fatigue,
we have many platforms



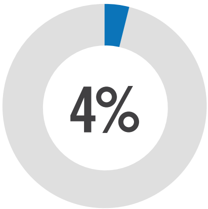
Lack of tools with adequate hunting/investigation workflows



Lack of training on threat hunting



Not a priority for our SOC



Lack of collaboration across departments

Other 14%

KEY THREAT HUNTING CAPABILITIES

The most important capability that cybersecurity professionals consider critical to the effectiveness of their threat hunting tools is automatic detection (69%), followed by threat intelligence (62%), integration and normalization of multiple data sources (48%), and user and Entity Behavior Analytics (UEBA) (48%).

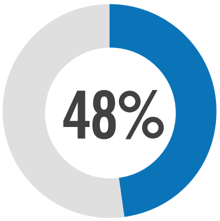
What capabilities do you consider most important regarding the effectiveness of a threat hunting tool?

69%

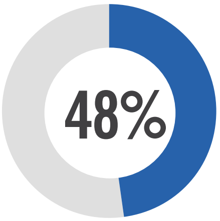
Automatic detection

62%

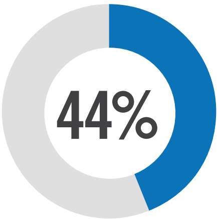
Threat intelligence



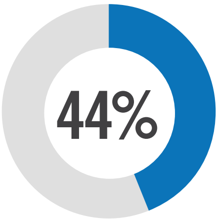
Integration and normalization of multiple data sources



User and Entity Behavior Analytics (UEBA)



Fast, intuitive search



Full attack lifecycle coverage

Intuitive data visualization 46% | Full attack lifecycle coverage 46% | Automated workflows 41% | Combined visibility across hybrid cloud and on-premises environments 13% | Other 6%

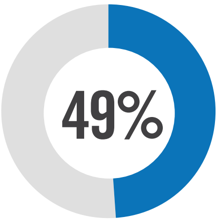
THREAT HUNTING TECHNOLOGIES

Today's organizations typically deploy multiple technologies in concert to achieve deeper visibility across their infrastructure. Most frequently used are endpoint detection and response solutions (65%) followed by SIEM (55%) and NGFW/IPS/AV (55%).

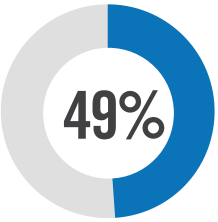
Which technologies do you use as part of your organization's threat hunting approach?

55%
Endpoint Detection & Response (EDR)

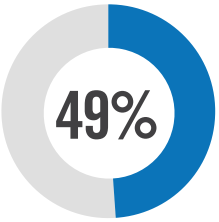
55%
SIEM



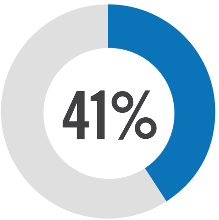
NGFW, IPS, AV, web application firewall, etc.



Network IDS/ Network Detection and Response (NDR)



Anti-phishing or other messaging security software



Vulnerability management

Threat intelligence platform 39% | Enrichment and investigation tools 33% | Security orchestration, automation and response (SOAR) 22% | Not sure/other 8%

SYSTEMS INTEGRATION

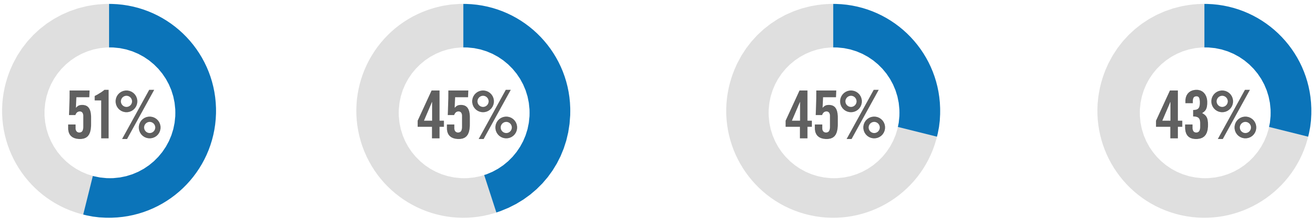
Vendae corepre core am volorit aquidem odigentota nos estem. Nam repre num faccate mporem et, con non commo eum nullatur? Solorep erchitasi dis modis quundis assimpos alicime reicaturest, sit eos et ommolori odis denis dolores andi vero eic tem. Sandam am repudaectem fuga. Et ut repernatem elitiis et ipsunt, od que sincium, nat.

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

69% Incident response

59% SIEM

53% Network Detection & Response (NDR)



51% Active Directory

45% Ticketing systems

45% Endpoint Detection & Response (EDR)

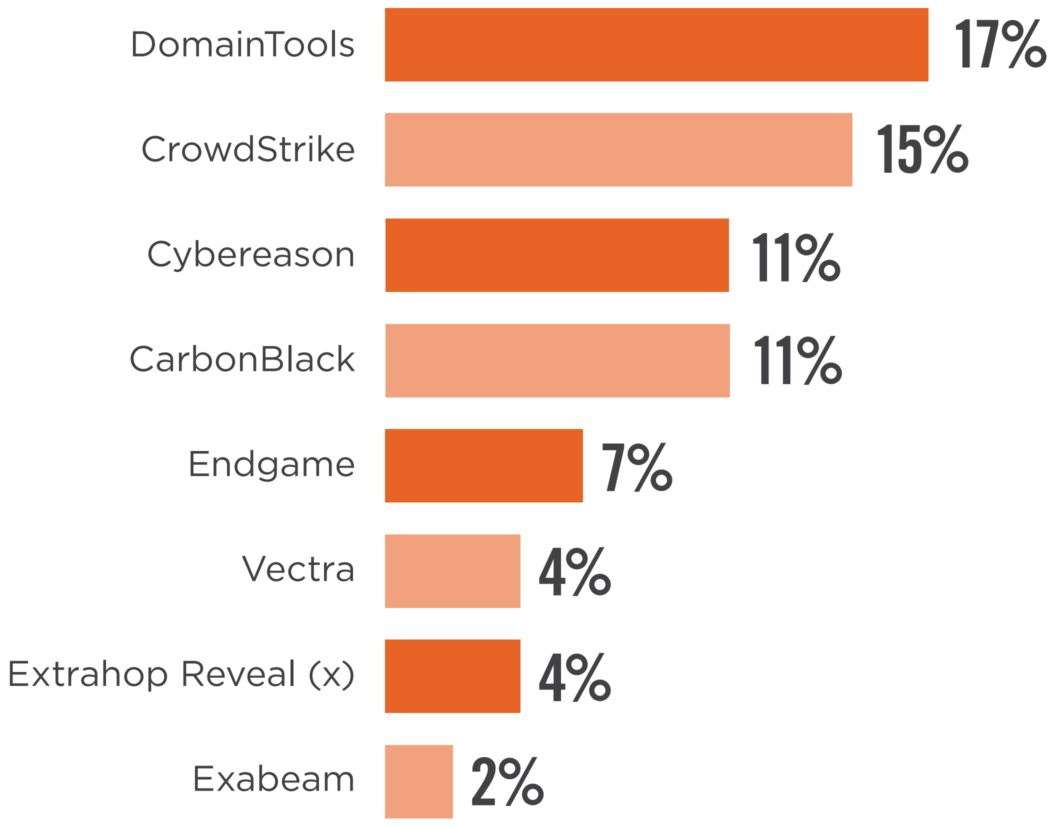
43% File Activity Monitoring

UEBA 31% | CI/CD, deployment orchestration 20% | Other 2%

THREAT HUNTING TOOLS USED

Over the last few years, a number of dedicated threat hunting solutions have emerged. The most popular threat hunting platform in our survey is DomainTools (17%), followed by CrowdStrike (15%) and Cybereason (11%).

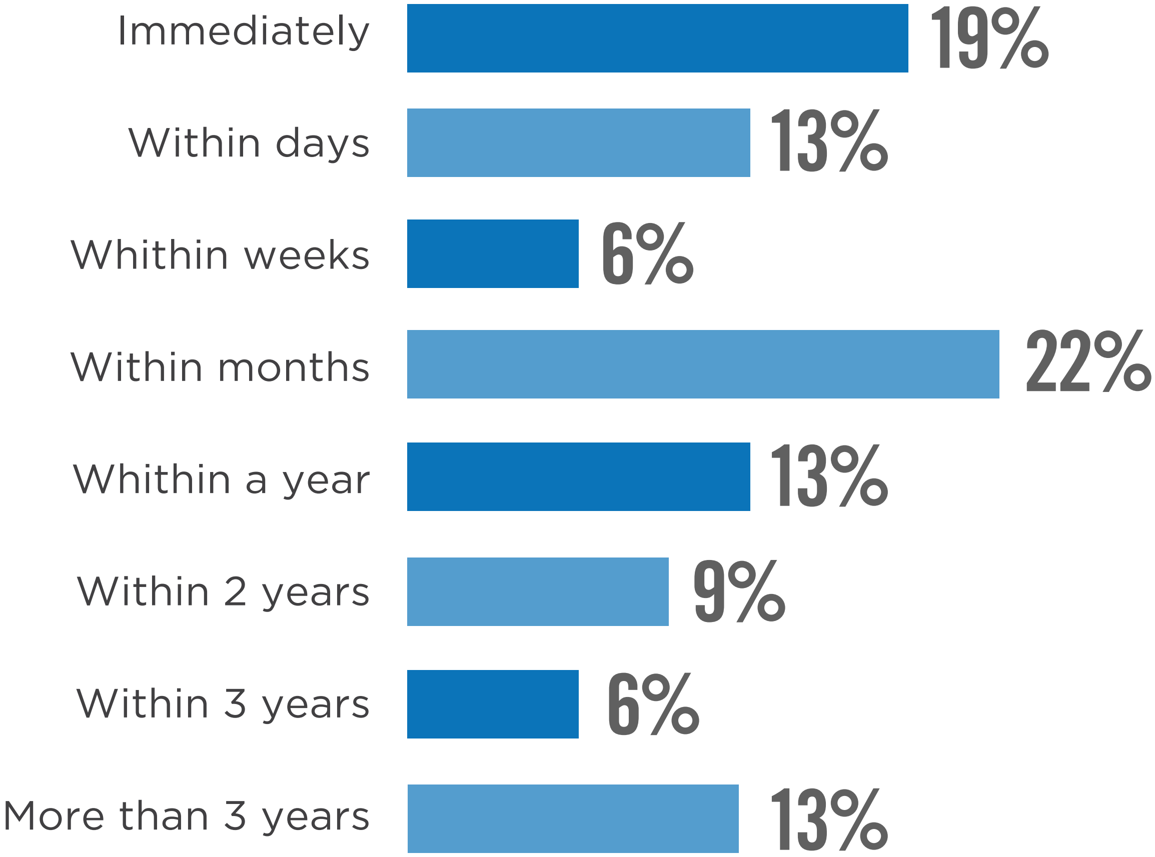
What threat hunting tool does your organization use most today?



THREAT HUNTING INVESTMENT

We asked how long it takes for a security operations center to break even on the investment in a threat hunting platform. A majority of 60% confirm their threat hunting investment would start to pay for itself within months of deployment.

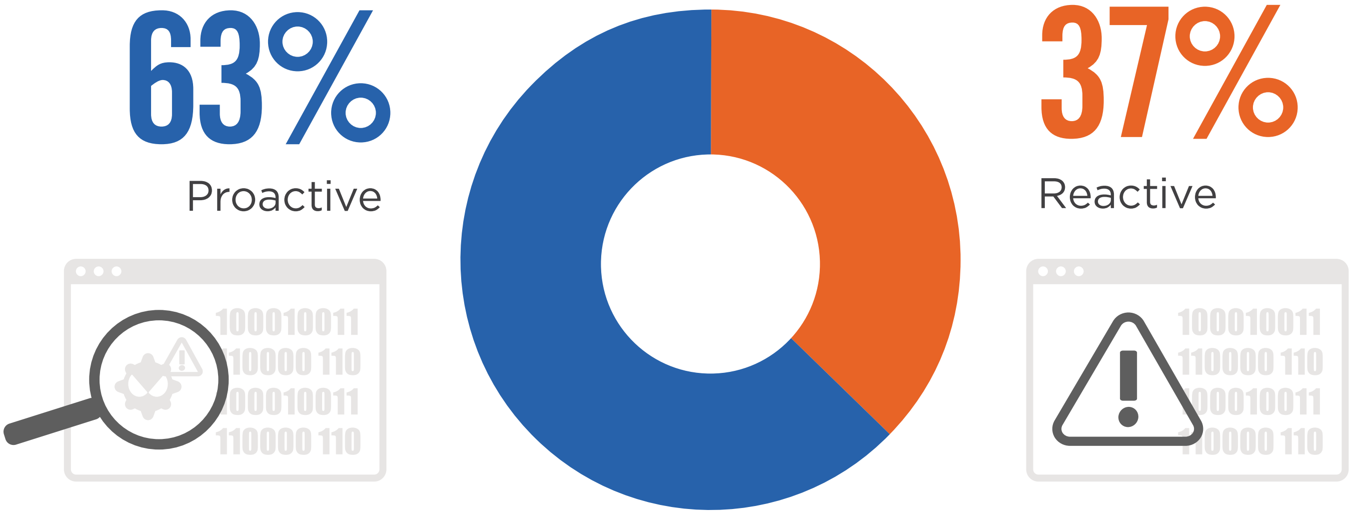
▶ **How long does it take for a SOC to break-even on the investment of a threat hunting platform?**



PROACTIVE VS REACTIVE THREAT HUNTING

Organizations' threat hunting efforts are trending toward proactive postures before threats are detected (63%) vs. reactive postures (37%) to respond to detected threats.

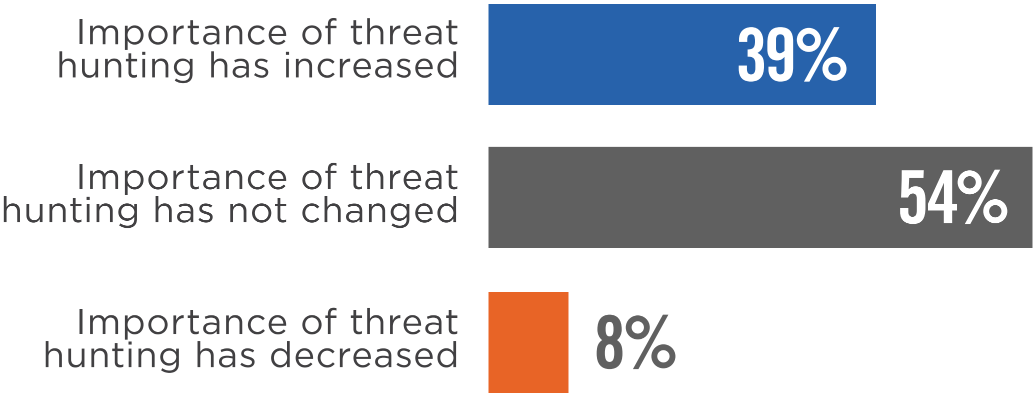
Are your threat hunting efforts proactive (commencing before any threat is detected) or reactive (in response to an existing detection or IOC)?



THREAT HUNTING
REMOTE WORKFORCE

Since the start of the COVID-19 epidemic, well over a third of organizations (39%) have placed more emphasis on threat hunting to accommodate the new threats introduced by work from home scenarios. Only a small minority of 8% report a decrease in in threat hunting importance.

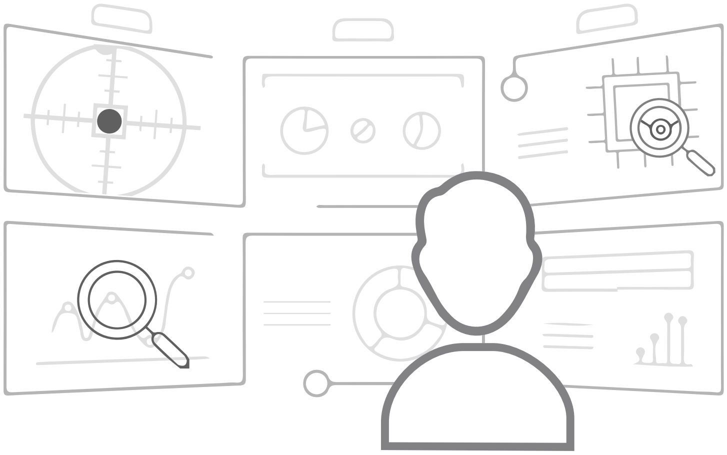
Has threat hunting as a priority changed with a more remote workforce since the COVID epidemic?

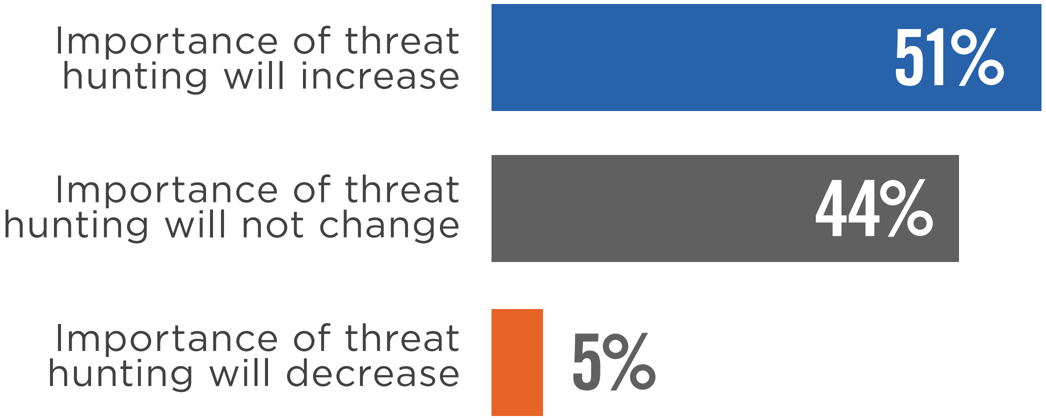

Importance of threat hunting has increased
39%
Importance of threat hunting has not changed
54%
Importance of threat hunting has decreased
8%

THREAT HUNTING AUTOMATION

We asked how the importance of threat hunting will change in the face of increasing automation of the function to support an expanding attack surface and remote workforces. A majority of 51% confirms the importance of threat hunting will increase, only 5% see a decrease of importance.

Threat hunting is reported to be one of the most common security activities to be automated in 2020. Do you see this changing to support the expanding attack surface and a more remote workforce?

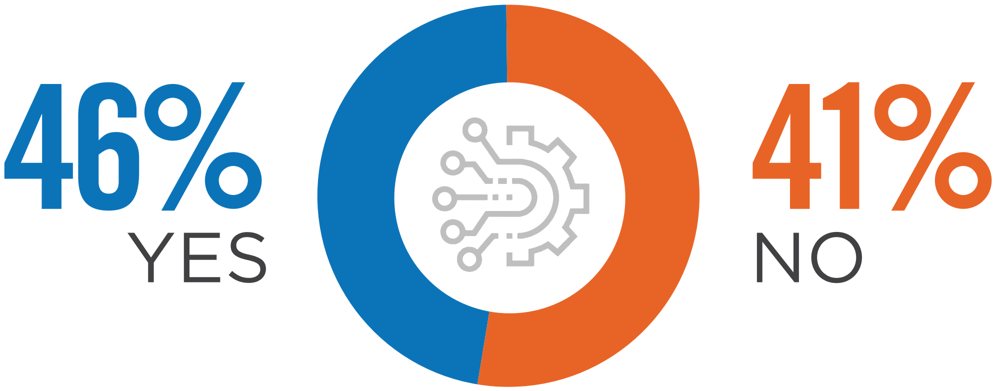



Importance of threat hunting will increase
51%
Importance of threat hunting will not change
44%
Importance of threat hunting will decrease
5%

THREAT HUNTING DURING COVID-19

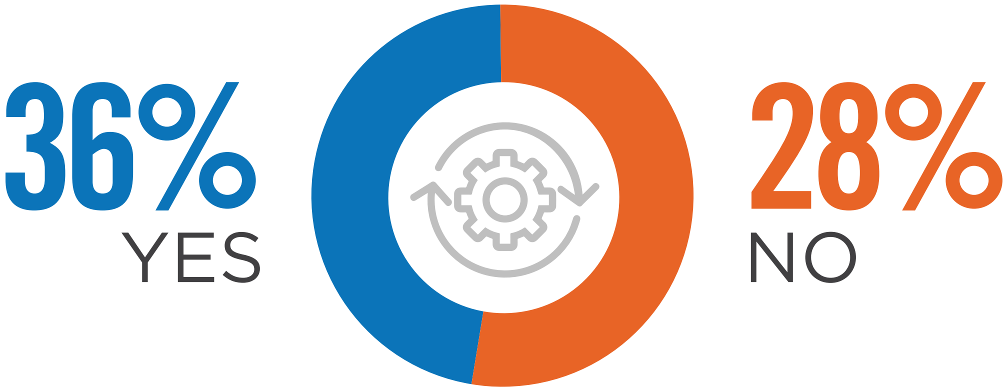
An alarming trend we see is that less than half of security professionals have access to threat hunting tools while working from home. And only about a third (36%) can confirm that machine-learning algorithms can spot unusual patters now that everyones normal patters have changed significantly due to work from home scenarios.

Do you have access to threat hunting automation tools, techniques and processes when working from home?



Not sure 13%

Are machine-learning algorithms able to spot deviations from normal patterns, when everyone's normal patterns have changed due to the COVID-19 Pandemic?

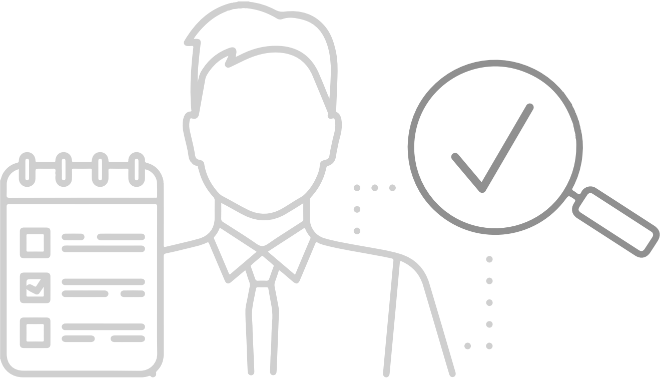


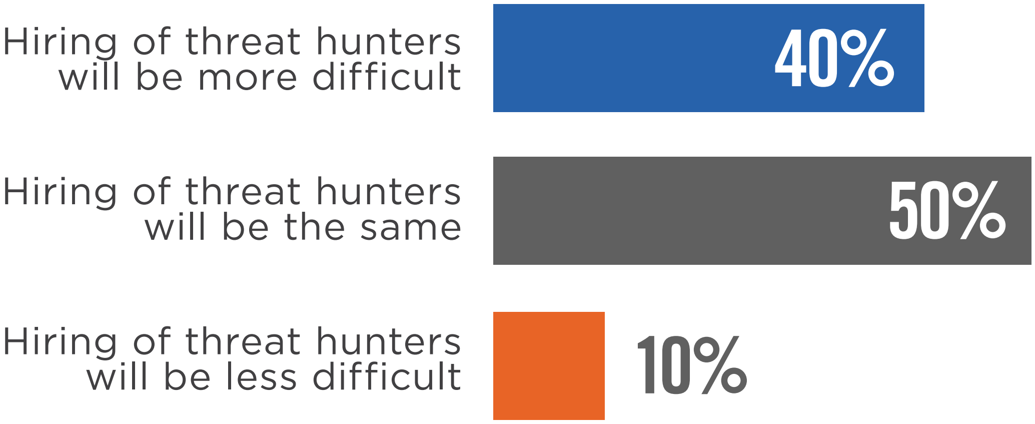
Not sure 36%

HIRING QUALIFIED THREAT HUNTERS

When asked whether organizations are seeing challenges when hiring of threat hunting professionals as a remote workforce, four of six say that hiring of threat hunters will be more difficult. Half say that hiring difficulty will be about the same, only 10% see hiring to be less difficult.

Do you anticipate hiring qualified threat hunters to be more or less problematic with a more remote workforce?

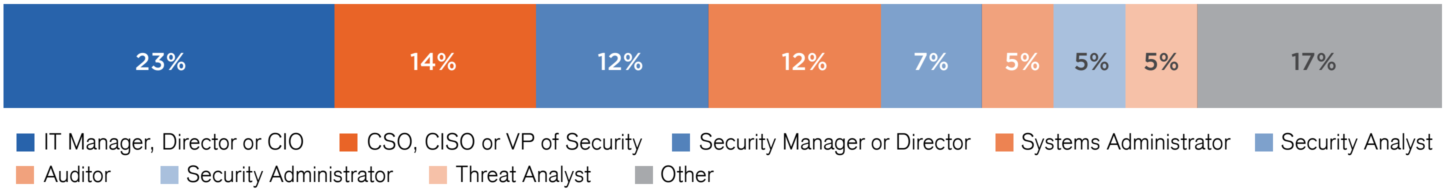



Hiring of threat hunters will be more difficult
40%
Hiring of threat hunters will be the same
50%
Hiring of threat hunters will be less difficult
10%

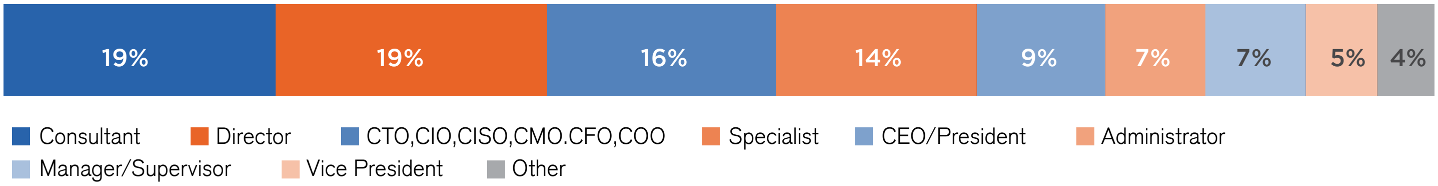
METHODOLOGY & DEMOGRAPHICS

This Threat Hunting Report is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in February of 2020 to gain deep insight into the latest trends, key challenges and solutions for threat hunting 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.

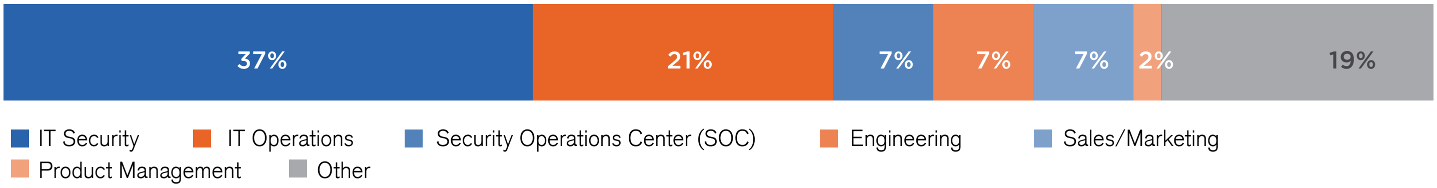
PRIMARY ROLE



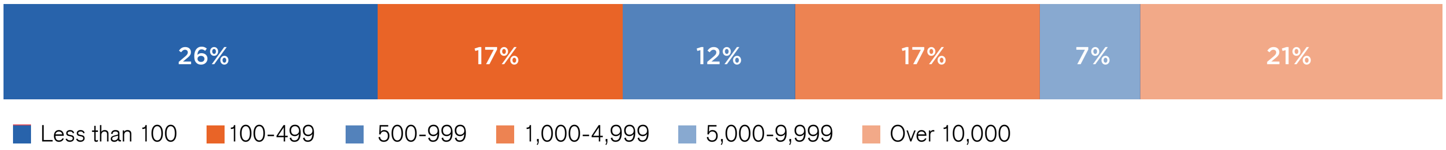
CAREER LEVEL



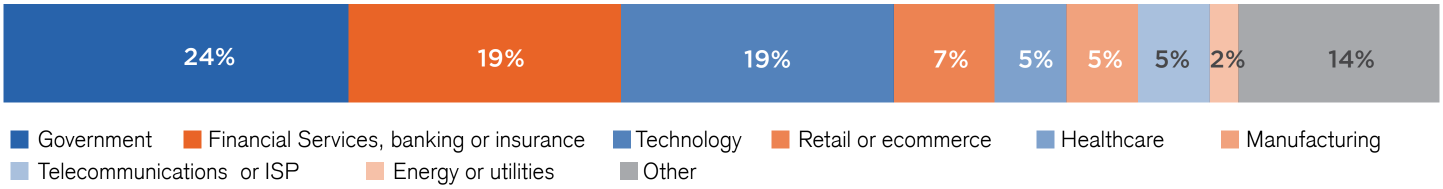
DEPARTMENT



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