2020

Cybersecurity INSIDERS

THREAT HUNTING REPORT

ExtraHop

Rise Above the Noise.

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:

- Given the importance of threat hunting as a top initiative, it’s not surprising that a majority (51%) of organizations currently use a threat hunting platform.
- A majority of security professionals (71%) still believe their SOC does not spend enough time proactively searching for new threats.
- Fifty-four percent of organizations feel they are behind the curve or limited in their threat hunting capabilities.
- Organizations’ threat hunting efforts are surprisingly balanced between proactive (52%) and reactive postures (48%) to detect and respond to threats, with a slight focus on proactive hunting.
- While training for existing staff tops the list (57%) when asked about the investments that would help organizations improve their threat hunting abilities, security professionals highlighted a need for better, not more, tools as well.

We would like to thank ExtraHop, for sponsoring this report.

We hope you will enjoy it.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity INSIDERS

KEY SECURITY CHALLENGES

The survey reveals that cybersecurity professionals prioritize timely detection of advanced threats (55%) as the top challenge for their SOC. This is followed by a lack of expert security staff to mitigate such threats (46%) and too much time being wasted on false positive alerts (44%).

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

55%

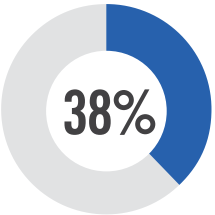
Detection of advanced threats (hidden, unknown, and emerging)

46%

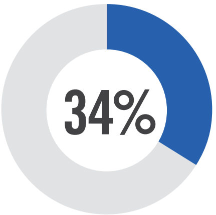
The lack of expert security staff to assist with threat mitigation

44%

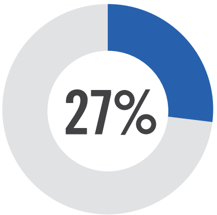
Too much time wasted on false positive alerts



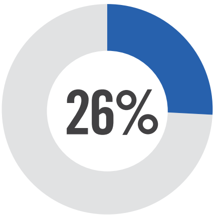
Slow response time to advanced threats



Lack of confidence in automation tools catching all threats



Working with outdated SIEM tools and SOC infrastructure



Lack of proper reporting tools

Lack of visibility into critical data due to encryption 8% | Other 6%

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?**

57%

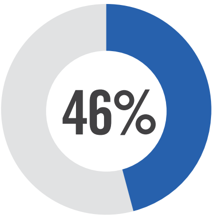
Reduce exposure
to internal threats

54%

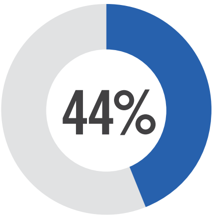
Improve speed
and accuracy
of threat response

53%

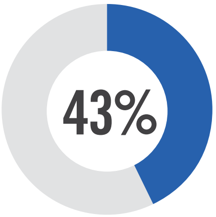
Reduce number of
breaches and infections



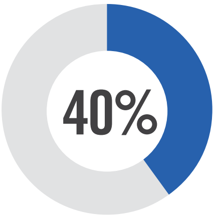
Reduce time
to containment
(prevent spread)



Reduce attack
surface



Reduce exposure
to external threats



Optimize
resources spent on
threat response

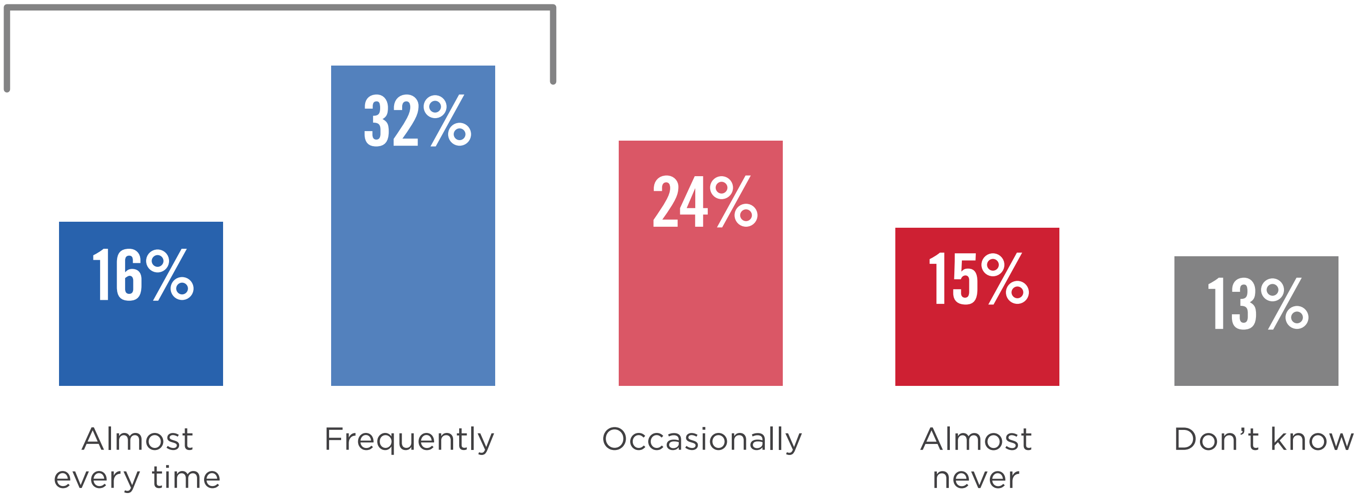
Reduce dwell time from infection to detection 39% | Other 6%

INSIGHTS INTO ADVERSARIES

About half (48%) 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?

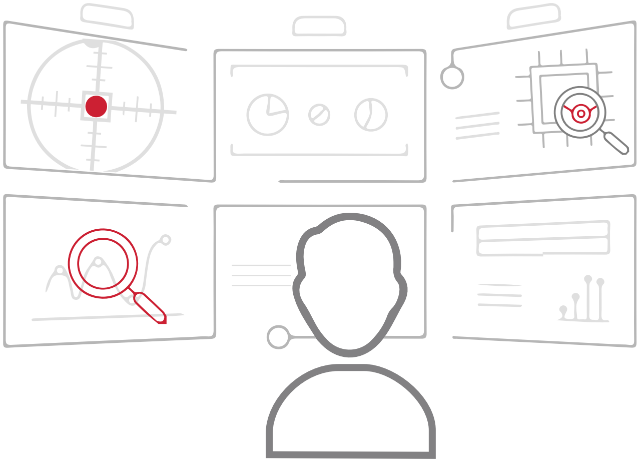
48% Of security teams evaluate adversary domains and IP addresses as part of their threat hunting process.

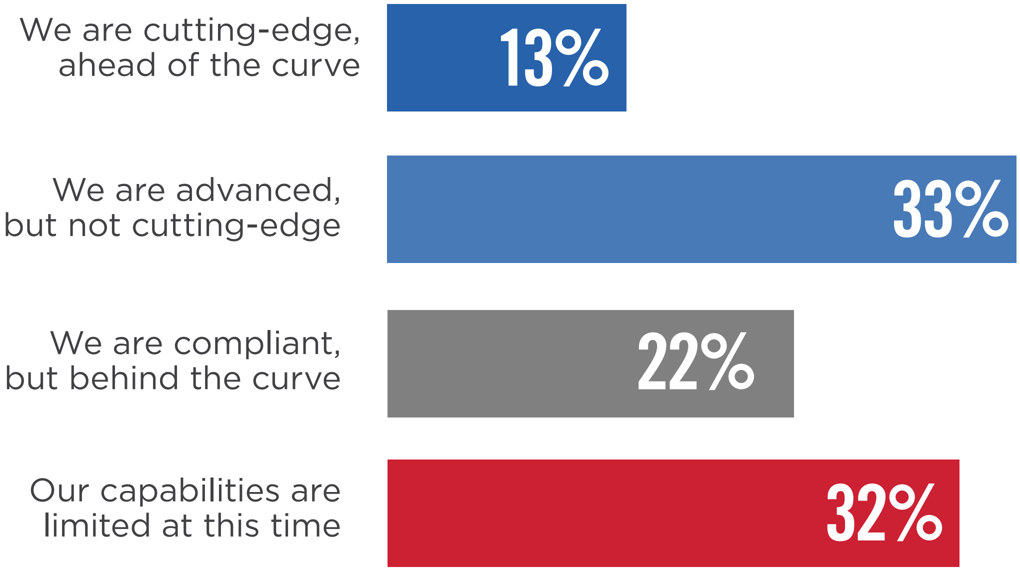


THREAT MANAGEMENT MATURITY

Proactive threat hunting emerged only a few years ago as a new cybersecurity discipline created to tackle threats proactively before they are detected by other systems. Against this backdrop, nearly half of SOCs (46%) believe they are at least advanced (33%) or cutting-edge (13%) in their ability to address emerging threats.

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

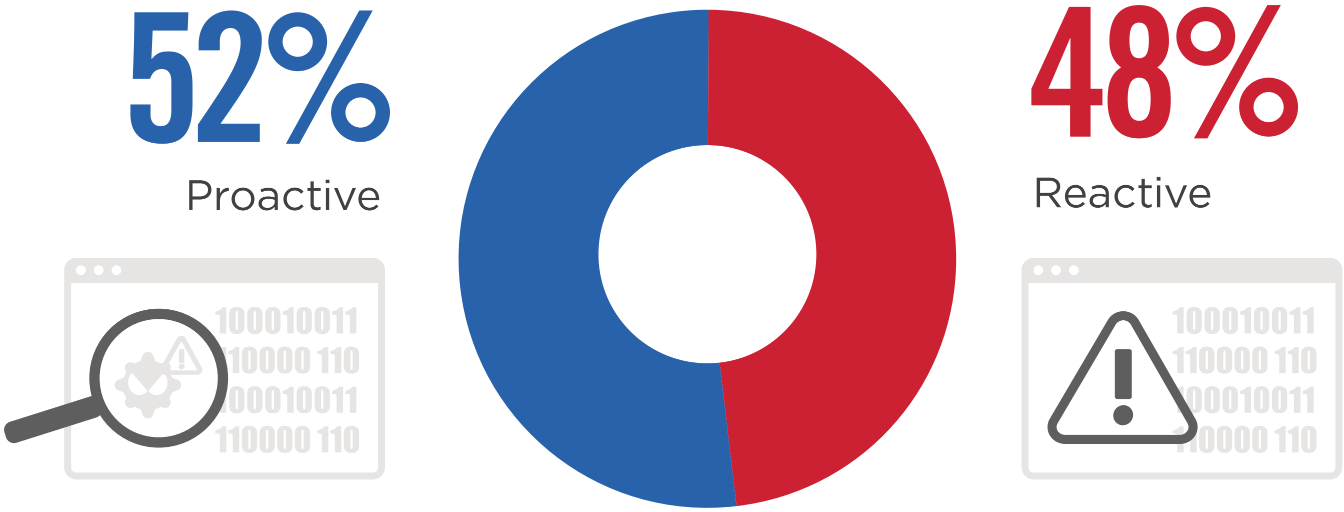



We are cutting-edge, ahead of the curve
13%
We are advanced, but not cutting-edge
33%
We are compliant, but behind the curve
22%
Our capabilities are limited at this time
32%

PROACTIVE VS REACTIVE THREAT HUNTING

Organizations' threat hunting efforts are surprisingly balanced between proactive (52%) and reactive postures (48%) to detect and respond to threats, with a slight focus on proactive hunting.

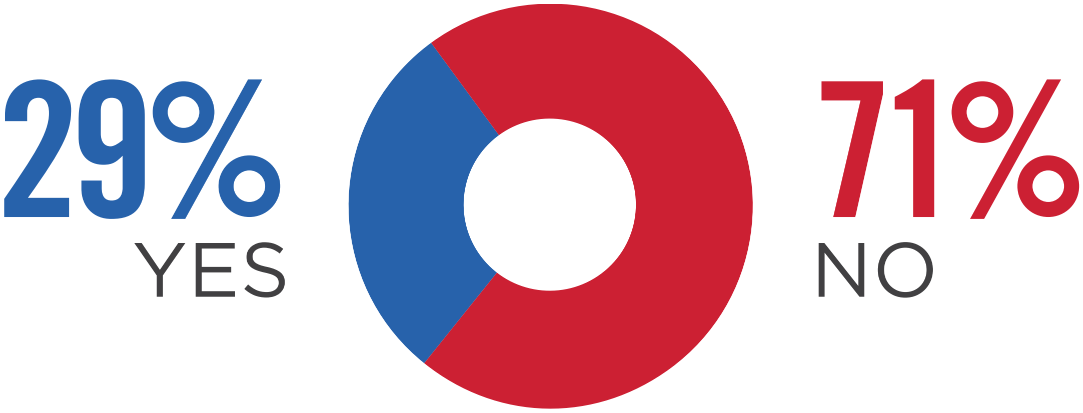
Are your threat hunting efforts proactive (commencing before any threat is detected) or reactive (in response to an existing detection or IOC)?

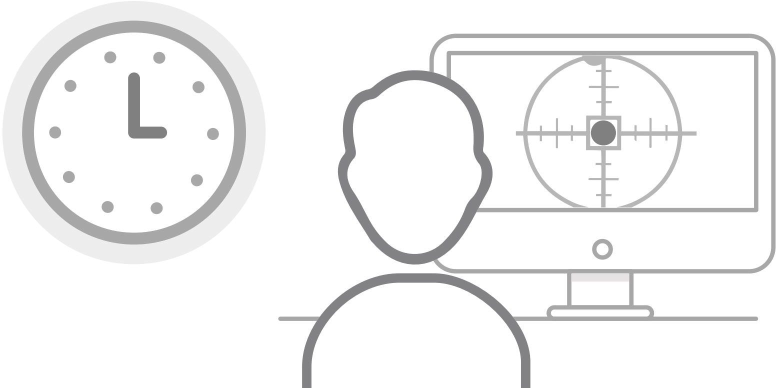


THREAT HUNTERS IN SOCS

The traditional approach to threats and the tools used by SOCs - such as antivirus, IDS, or SIEM – is 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 as part of the threat hunting paradigm, a majority (71%) still believe their SOC does not spend enough time proactively searching for new threats.

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

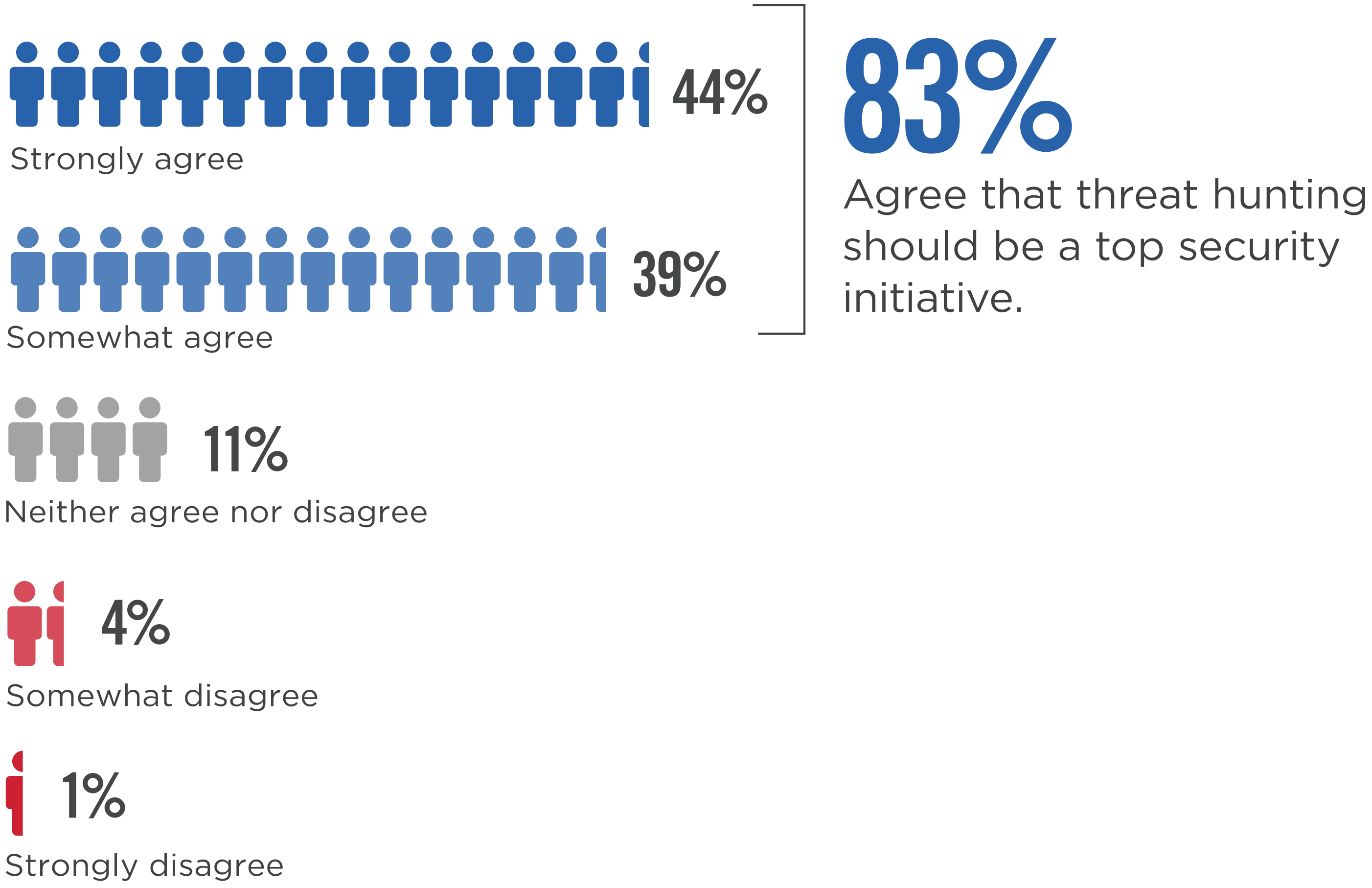




THREAT HUNTING PRIORITY

Although threat hunting is still an emerging discipline, 83% of organizations agree that threat hunting should be a top security initiative to provide early detection and reduce risk. Forty-four percent strongly agree, an increase of five 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".

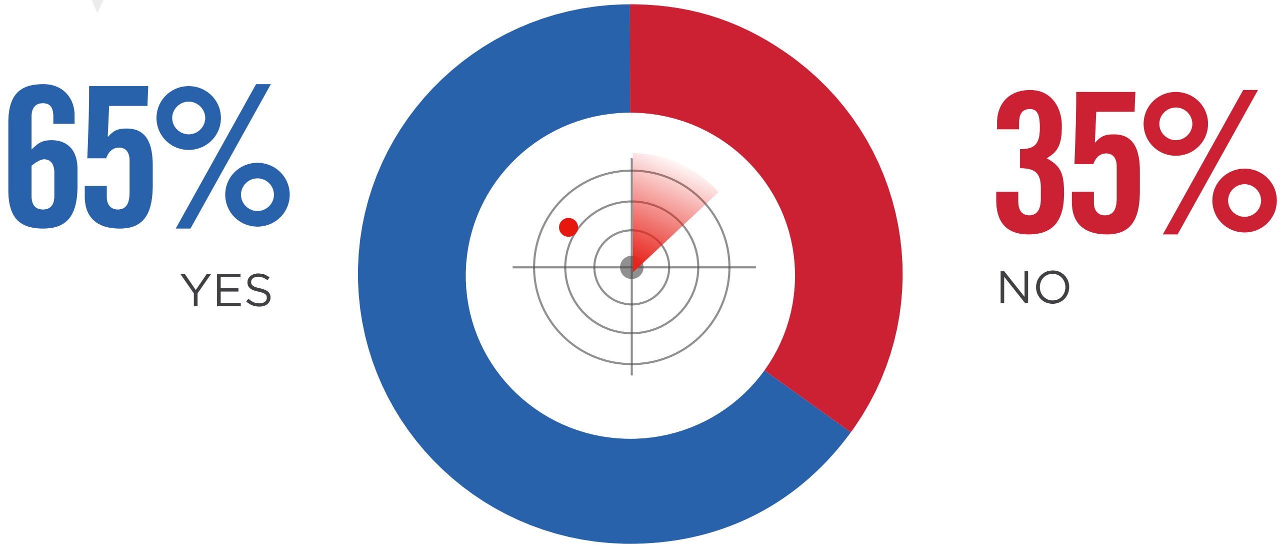


INTENTIONS TO DEVELOP A THREAT HUNTING PROGRAM

Roughly two-thirds (65%) 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?**

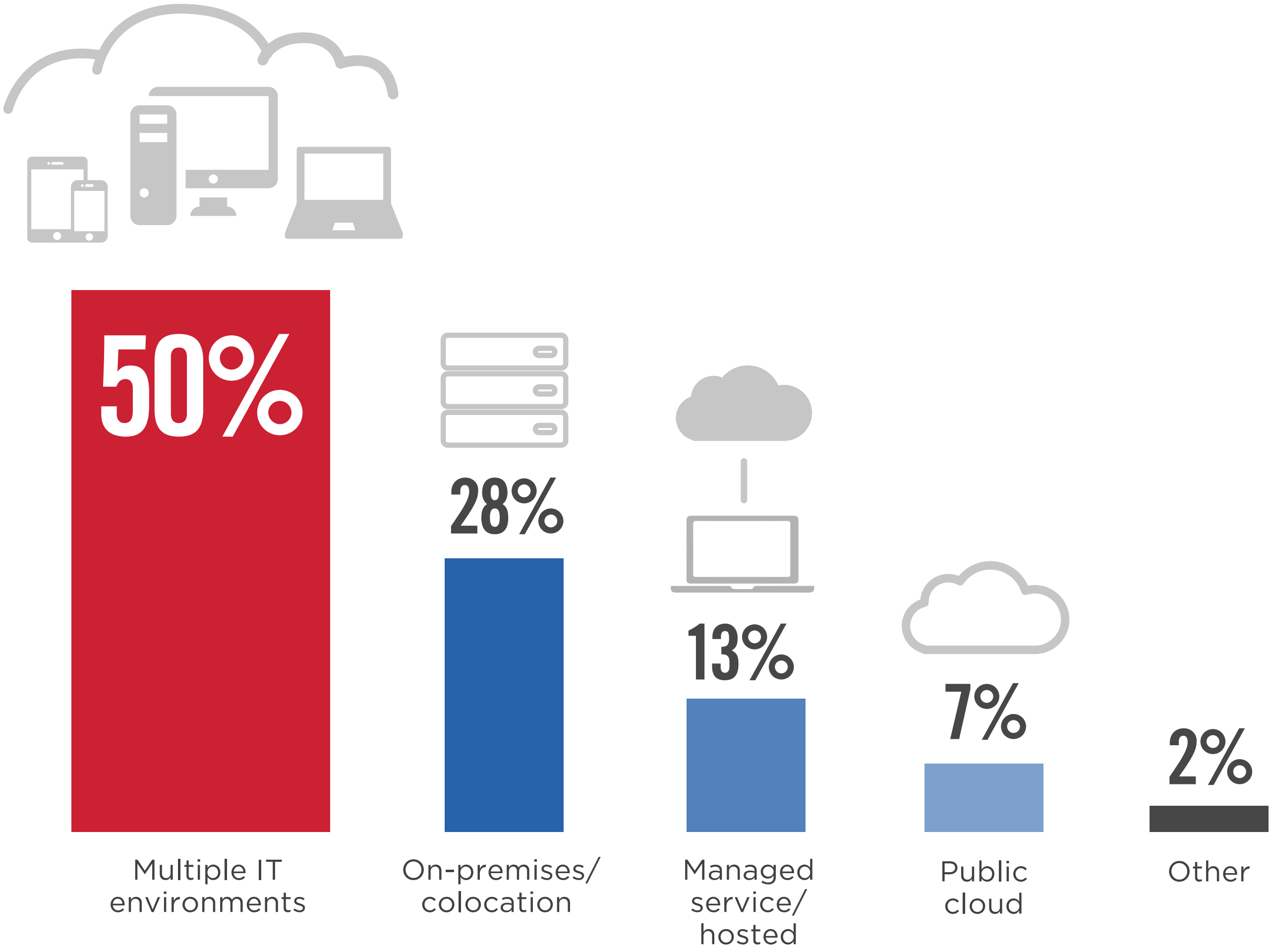
Roughly two-thirds of organizations plan to build one over the next three years.



THREAT HUNTING ACROSS IT ENVIRONMENTS

When asked what types of IT environments threat hunting teams typically focus on, half of respondents manage multiple IT environments (50%), which significantly increases the complexity of orchestrating security. This is followed by on-premises environments (28%) and managed/ hosted environments (13%).

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

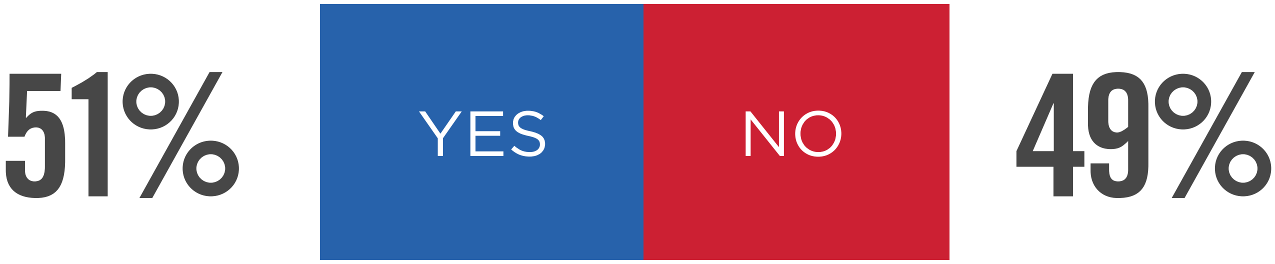


THREAT HUNTING PLATFORM

Given the importance of threat hunting as a top initiative, it's not surprising that a majority (51%) of organizations currently use a threat hunting platform.

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

23%
40%
78%
EXFIL-10 | 2016-11-17 04:52
EXFIL-10 | 2016-11-17 04:52
EXFIL-10 | 2016-11-17 04:52
Entry 1 | 016-11-17 04:52
Entry 2 | 016-11-17 04:52
Entry 3 | 016-11-17 04:52
ABINDS-10 | 2016-11-17 04:52
ABINDS-10 | 2016-11-17 04:52
ABINDS-10 | 2016-11-17 04:52
ABINDS-10 | 2016-11-17 04:52

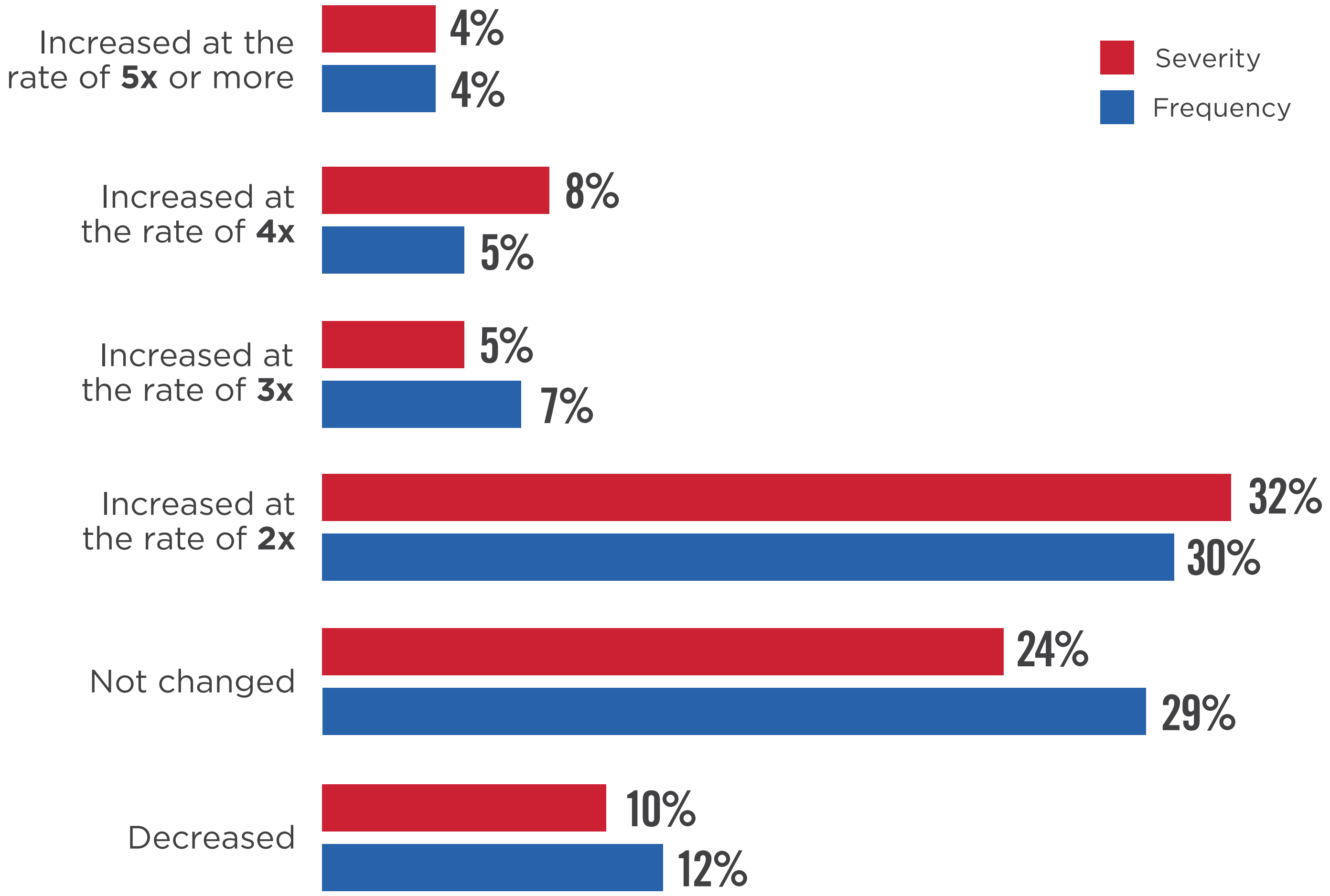


SEVERITY & FREQUENCY OF CYBER THREATS

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. Half of organizations in our survey (49%) 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 (46%) have experienced an increase in the frequency of cyber attacks over the last 12 months. Only few respondents signaled a decrease in attack severity (10%) and frequency (12%).

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

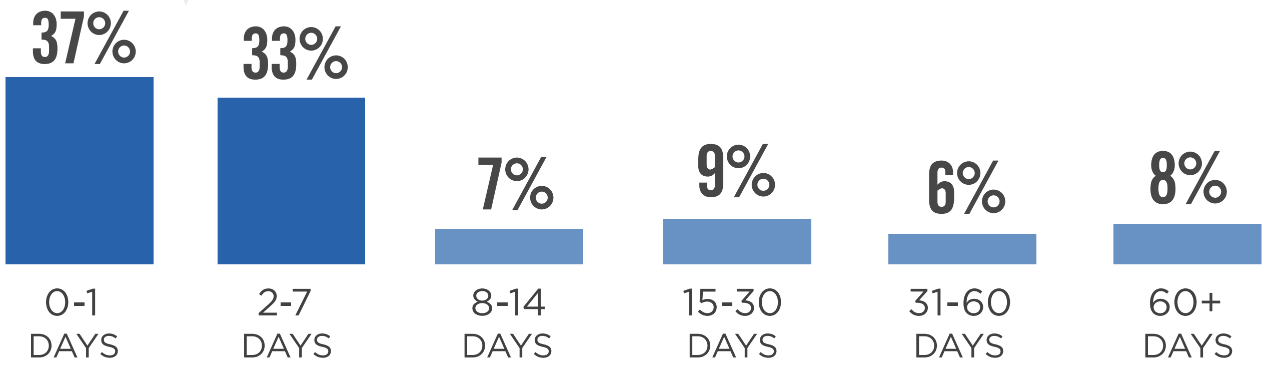


Don’t know severity 17% | Don’t know frequency 13%

ATTACK DISCOVERY

Organizations report average dwell times of 13 days before attacks are discovered. Over a third of respondents (37%) report they can detect attacks within 1 day, another third (33%) within 7 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?



70% Report they can detect attacks within 7 days

13 DAYS Average time attackers dwell on networks until discovered

DATA COLLECTION SOURCES

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

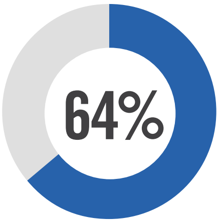
Most organizations prioritize data from traffic denied by firewall/IPS (67%) together with system logs (67%) as the most important data sources to collect. This is followed by data from traffic allowed by firewall/IPS traffic (65%), and network traffic (64%). Bottom line: there are numerous security 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?

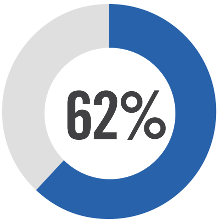
67%
Firewall/IPS denied traffic

67%
System logs

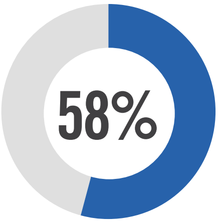
65%
Firewall/IPS allowed traffic



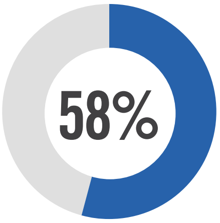
Network traffic



Endpoint activity



Web and email filter traffic



Active directory

DNS traffic 52% | Server traffic 49% | User behavior 46% | Threat intelligence sources 42% | File monitoring data 42% | Packet sniff/tcpdump 40% | Web proxy logs 34% | Don’t know/other 12%

THREAT INDICATORS

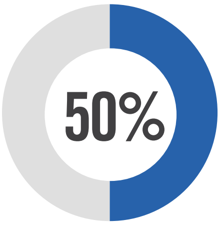
Understanding Indicators of Compromise (IOCs) allows organizations to develop effective defense methodologies that help with rapid detection, containment, and denial of future exploits. Our research reveals that hunt teams most frequently investigate behavioral anomalies (71%), followed by suspicious IP addresses (65%), denied/flagged connections (53%), and suspicious domain names (50%).

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

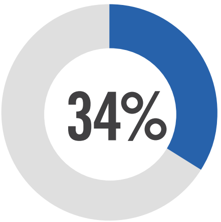
71%
Behavioral anomalies
(unauthorized access attempts, etc)

65%
Suspicious
IP addresses

53%
Denied/flagged
connections



Domain names



File names

Not sure/other 20%

BENEFITS OF THREAT HUNTING

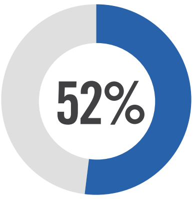
Threat hunting platforms provide security analysts with powerful tools to enable earlier detection, reduce dwell time, and improve defenses against future attacks. The top benefits organizations derive from threat hunting platforms include improved detection of advanced threats (66%), followed by reduced investigation time (59%), and creating new ways of finding threats (55%).

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

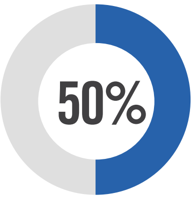
66%
Improving detection of advanced threats

59%
Reducing investigation time

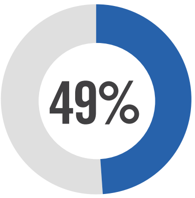
55%
Creating new ways of finding threats



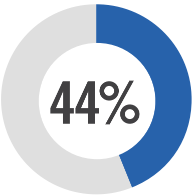
Saving time manually correlating events



Reducing time wasted on chasing false leads



Discovering threats that could not be discovered otherwise



Reducing attack surface

Saving time scripting and running queries 41% | Reducing extra and unnecessary noise in the system 40% | Connecting disparate sources of information 34% | Other 6%

KEY THREAT HUNTING CAPABILITIES

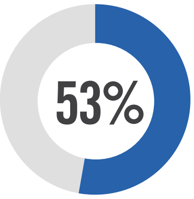
The single most important capability that cybersecurity professionals consider critical to the effectiveness of their threat hunting tools is integration of threat intelligence (66%). Automatic detection (59%), machine learning and automated analytics (54%), fast, intuitive search (53%), and vulnerability scanning (50%) round out the top five threat hunting capabilities.

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

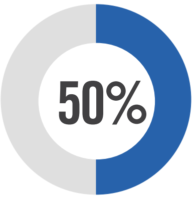
66%
Threat intelligence

59%
Automatic detection

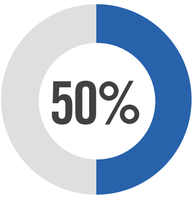
54%
Machine learning and automated analytics



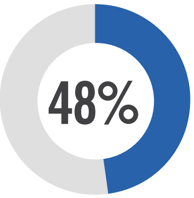
Fast, intuitive search



Vulnerability scanning



User and Entity Behavior Analytics (UEBA)



Integration and normalization of multiple data sources

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 cast a wide net and typically deploy multiple technologies in concert to achieve deeper visibility across their infrastructure. 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 (57%) and NGFW/IPS/AV (55%), followed by vulnerability management (50%), and Network IDS (50%).

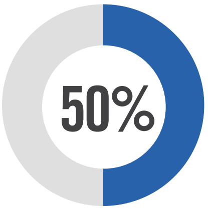
Which technologies do you use as part of your organization's threat hunting approach?

57%

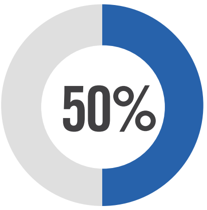
SIEM

55%

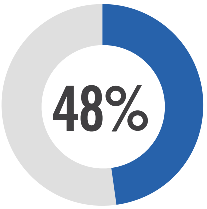
NGFW, IPS, AV,
web application firewall, etc.



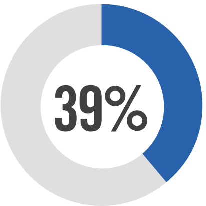
Vulnerability management



Network IDS/Network Detection and Response (NDR)



Anti-phishing or other messaging security software



Threat intelligence platform

Enrichment and investigation tools 33% | Orchestration (e.g., Phantom, Hexadite, Resilient, etc.) 18% | Endpoint Detection & Response (EDR) 18% | Not sure/other 18%

INVESTMENTS FOR BETTER THREAT HUNTING

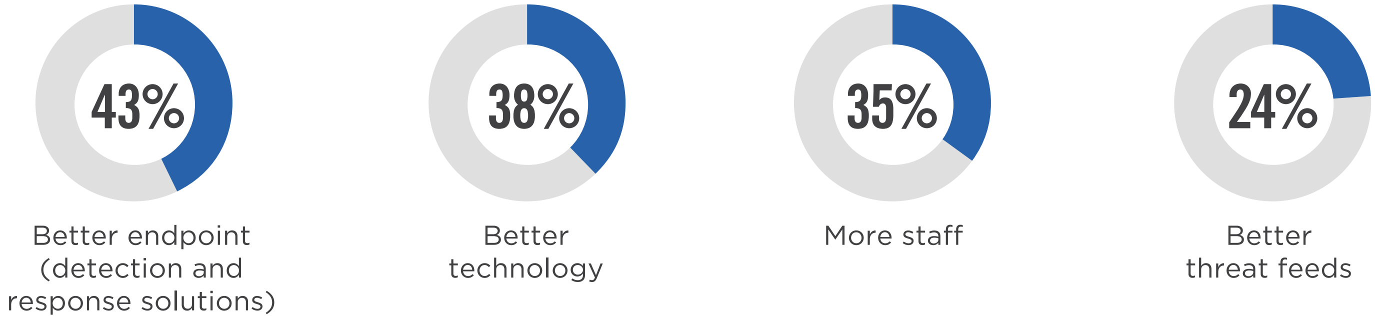
When asked about the investments that would help organizations improve their threat hunting abilities, training for existing staff made the top choice (57%). This is followed by investments in a cluster of technologies, including SIEM (46%), network (46%), and endpoint (43%) detection and response solutions. More staff ranked surprisingly low at 35%.

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

57%
More training for existing staff

46%
Better SIEM

46%
Better network (detection and response solutions)



More technology 11%

ACTIVE DIRECTORY BEHAVIORS

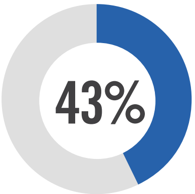
When asked about specific Active Directory behaviors cybersecurity teams look at for threat hunting, account logon ranked highest (58%) followed by querying for privileged accounts (57%) and sensitive security group modifications (51%).

Which of the following Active Directory behaviors do you look for as part of your threat hunting activities?

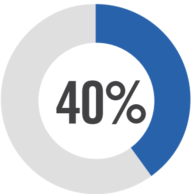
58%
Account logon

57%
Querying for privileged accounts

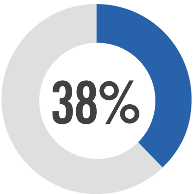
51%
Sensitive security group modifications



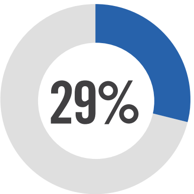
Querying for sensitive servers with service principal names



Querying for sensitive accounts with service principal names



Critical GPO modifications



AdminsSDHolder modification

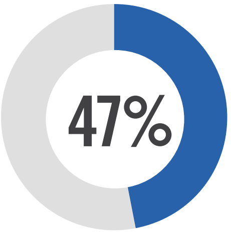
Object Attribute Modifications 28% | SACL/DACL Modifications 24% | None 12% | Other 4%

POPULAR RECONNAISSANCE ACTIVITIES

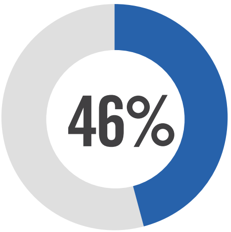
Active Directory enumeration (62%) stood out as the single most relevant reconnaissance activity cyber teams look for as part of their threat hunting. This is followed by LDAP queries (47%), host enumeration (46%), and service enumeration (45%).

▶ **Which of the following reconnaissance activities do you look for as part of your threat hunting activities?**

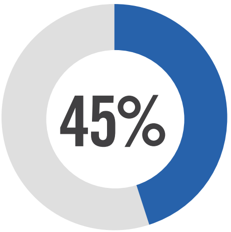
62% Active directory enumeration



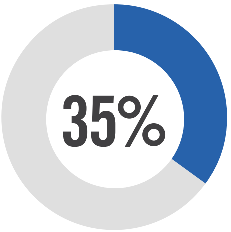
LDAP Queries



Host enumeration



Service enumeration



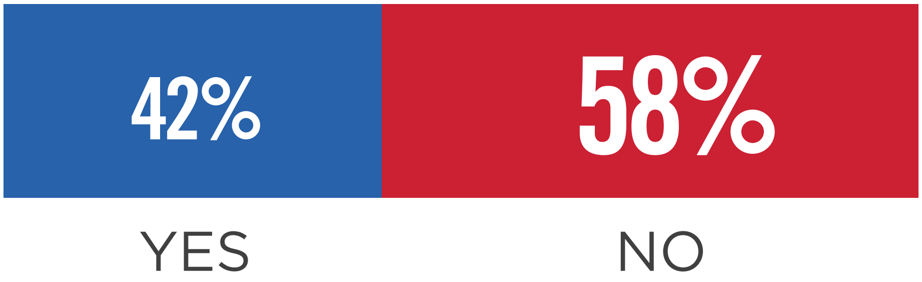
Open share enumeration

Port Scanning 20% | None 16% | Remote System Discovery 16% | Password Policy Discovery 14% | Other 5%

THREAT HUNTING VISIBILITY

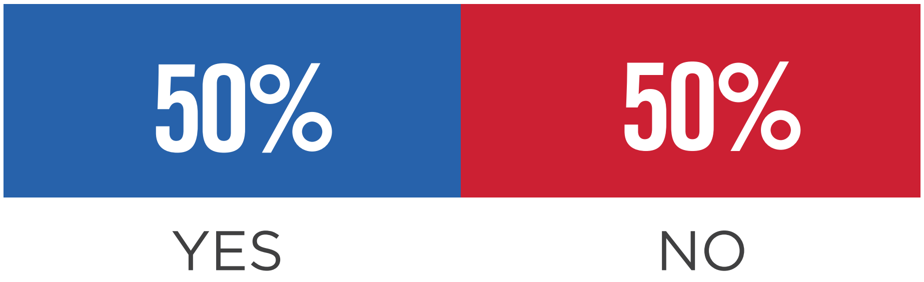
A majority of organizations (58%) do not encrypt traffic with TLS 1.3.

Does your organization encrypt internal traffic with TLS 1.3 / perfect forward secrecy?



Half of organization (50%) report that they lost threat hunting capabilities due to TLS 1.3 encryption being enabled on internal network traffic.

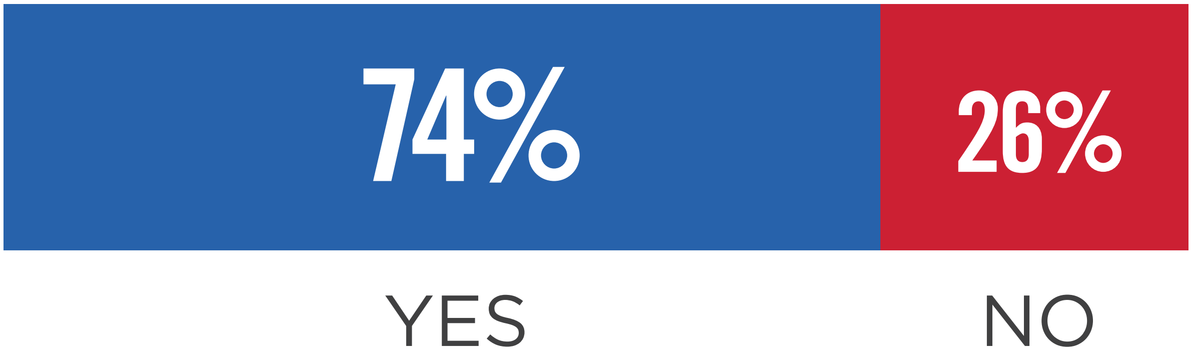
Has your SOC lost threat hunting capabilities or general visibility due to TLS 1.3 / perfect forward secrecy being enabled on internal traffic?



CRITICAL ASSETS

A majority of organizations (74%) confirm they have a way to identify critical IT assets to focus their threat hunting efforts.

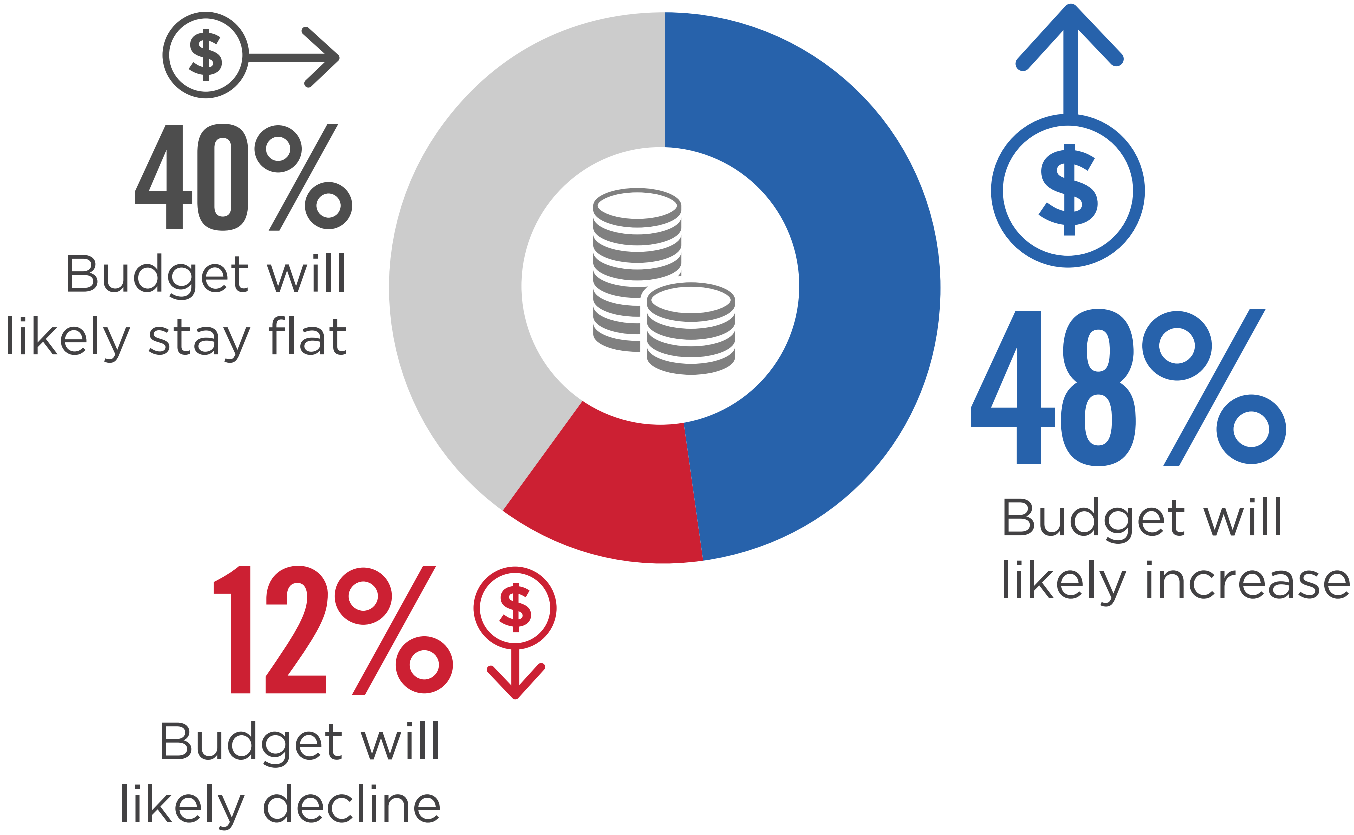
Do you have a way to identify your critical assets (likely to be attacked) in order to focus your threat hunting efforts?



THREAT HUNTING BUDGET

About half of SOCs (48%) will likely see threat hunting budgets increase over the next 12 months to invest in security staff, training, new threat hunting technologies, and managed security services.

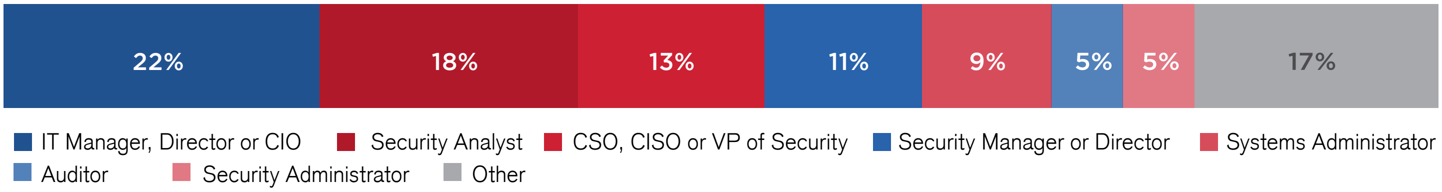
▶ **How is your organization's threat hunting budget going to change in the next 12 months?**



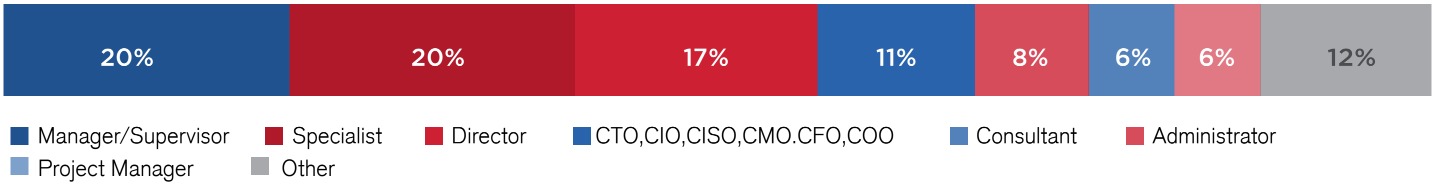
METHODOLOGY & DEMOGRAPHICS

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.

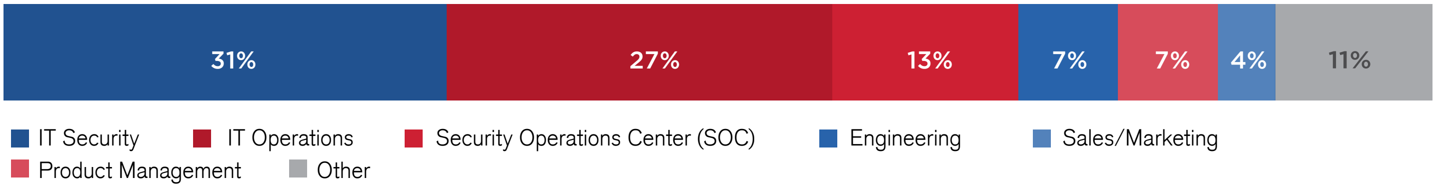
PRIMARY ROLE



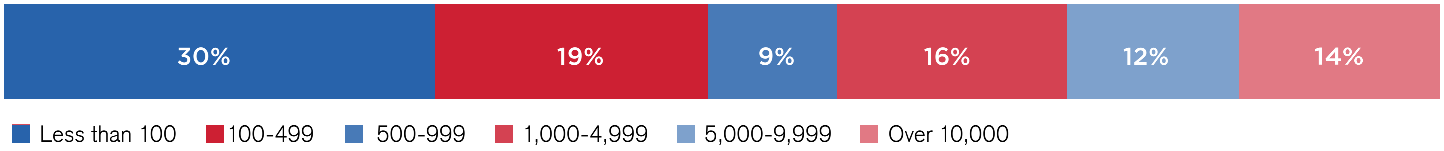
CAREER LEVEL



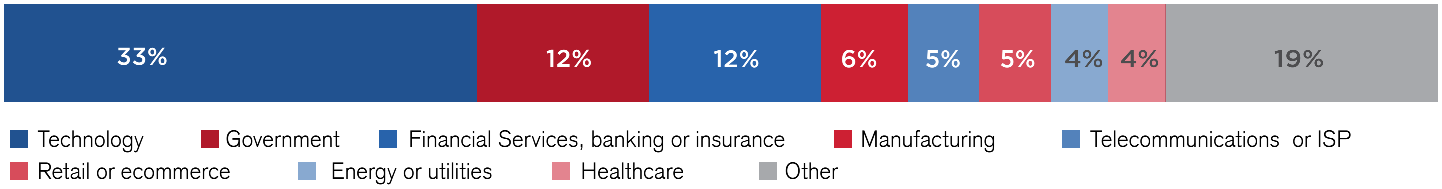
DEPARTMENT



COMPANY SIZE



INDUSTRY



ExtraHop

Rise Above the Noise.

ExtraHop delivers cloud-native network detection and response to secure the hybrid enterprise. Our breakthrough approach applies advanced machine learning to all cloud and network traffic to provide complete visibility, real-time threat detection, and intelligent response. With this approach, we give the world's leading enterprises including The Home Depot, Credit Suisse, Liberty Global and Caesars Entertainment the perspective they need to rise above the noise to detect threats, ensure the availability of critical applications, and secure their investment in cloud. To experience the power of ExtraHop, explore our interactive online demo or connect with us on LinkedIn and Twitter.

www.extrahop.com