2022

Cybersecurity
INSIDERS

THREAT HUNTING REPORT

DomainTools

INTRODUCTION

As many SOCs are struggling to cope with the rising security threat workload, more organizations continue to adopt threat hunting as an integral part of their security operations. They are discovering that proactive threat hunting can reduce the risk and impact of threats that might otherwise go undetected by traditional security technologies, all while improving defenses against new attacks.

In 2022, Cybersecurity Insiders conducted the fifth annual threat hunting research project in partnership with DomainTools to gain deeper insights into the state and evolution of this security practice.

Key findings include:

- While most organizations take a proactive threat hunting stance (64%), more than a third are responding to threats only after they have been detected (36%). This reactive posture partly contributes to about a third of security threats remaining undetected (37%).
- Over half of organizations (56%) observed an increase in threat levels by at least a factor of two compared to the previous year.
- Through threat hunting, 61% of organizations identify actionable indicators of compromise while 59% can generate rule sets or alert automation on future similar threat activity.
- Fifty-one percent of organizations find threat hunting produces a deeper understanding of adversary behavior and trends.

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

We hope you are able to take away actionable insights from this important report.

Thank you,

Holger Schulze

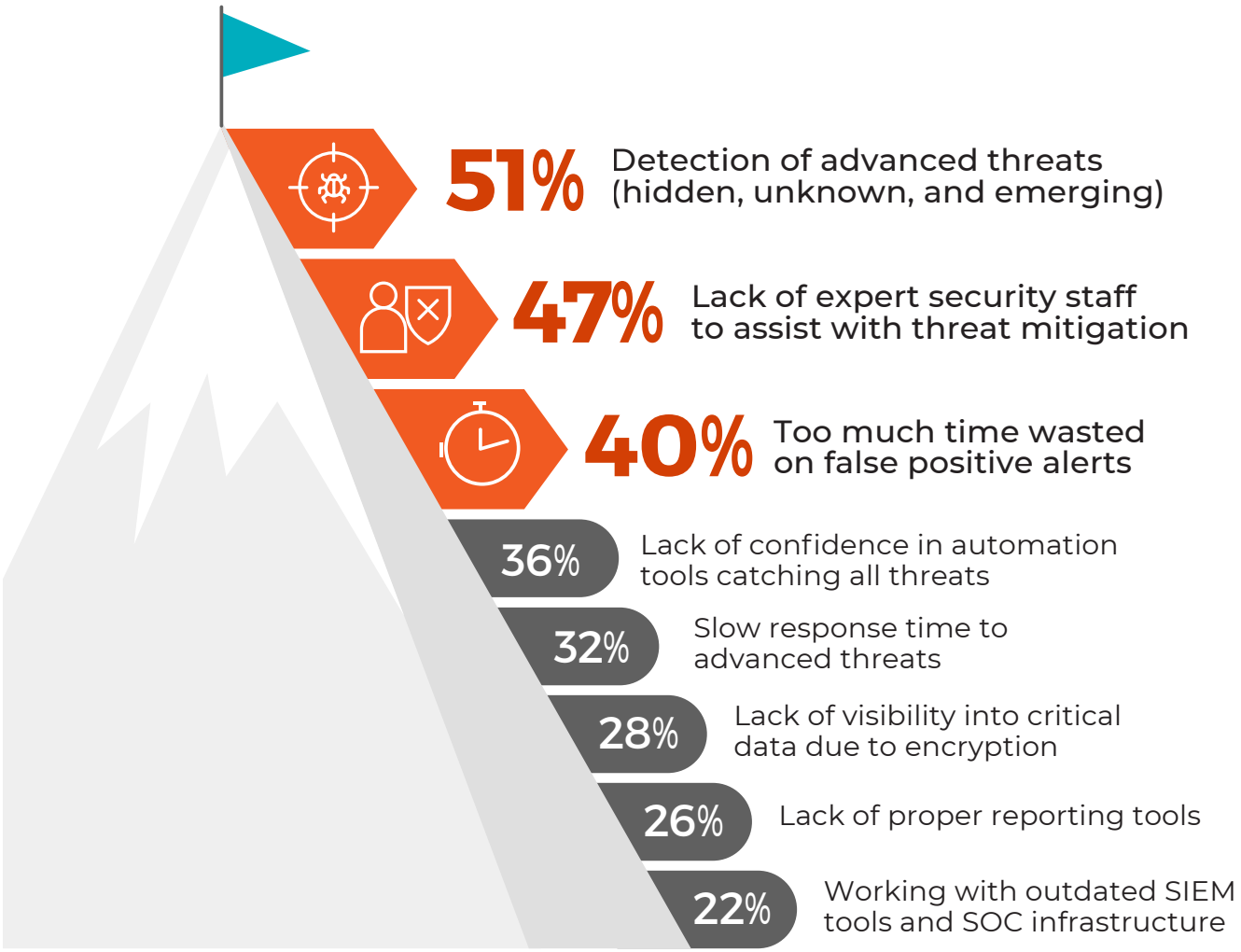
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

SOC CHALLENGES

Fifty-one percent of cybersecurity professionals consider detection of advanced threats to be the top challenge facing their SOC (down four percentage points from last year). Lack of expert security staff to assist with threat mitigation is a close second (47% - down four percentage points from last year). This year, lack of confidence in automation tools catching all threats (36%) and too much time wasted on false positive alerts (40%) switch places as the third and fourth top challenges.

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

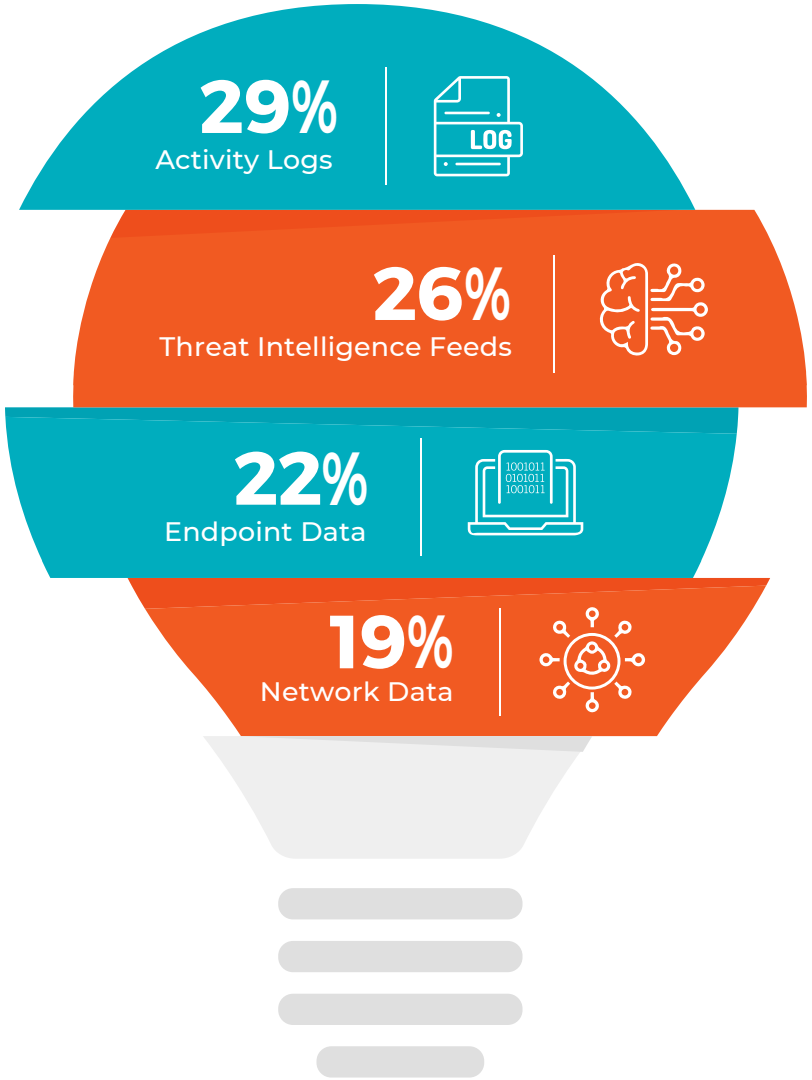


Other 7%

MOST VALUABLE DATA SOURCES FOR THREAT HUNTING

In this year's study, activity logs (29%) and threat intelligence feeds (26%) lead the list of most valuable data sources for investigating known threats. However, endpoint data jumps four percentage points compared to last year's survey (18% to 22%) to become the third most valuable data source. The data suggest this is influenced by the pandemic shifting people to remote work.

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

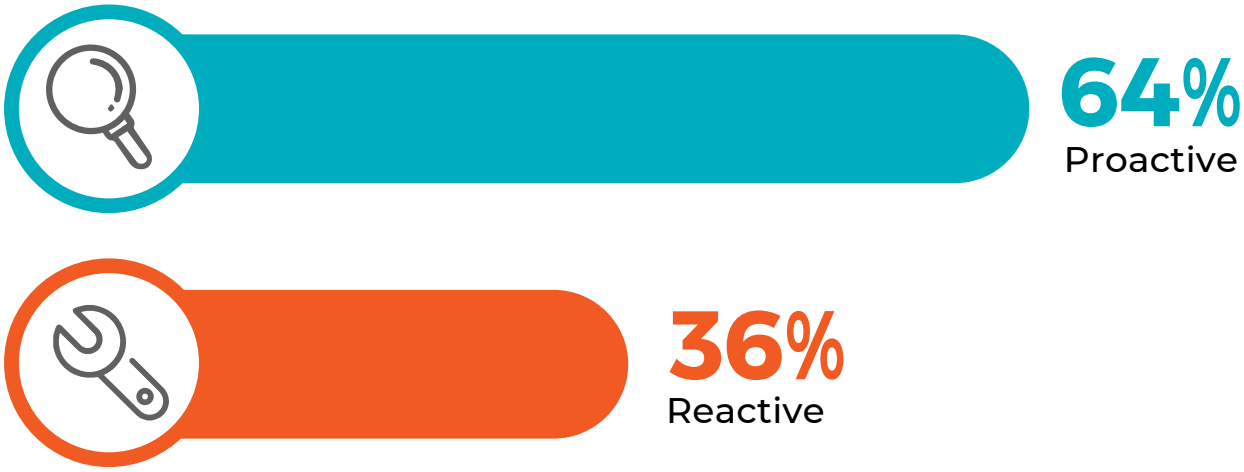


Other 4%

PROACTIVE VERSUS REACTIVE THREAT HUNTING

While most organizations in our survey take a proactive threat hunting stance (64%), over a third of organizations are responding to threats only after they have been detected (36%). This reactive posture partly contributes to about a third of security threats remaining undetected (37%).

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

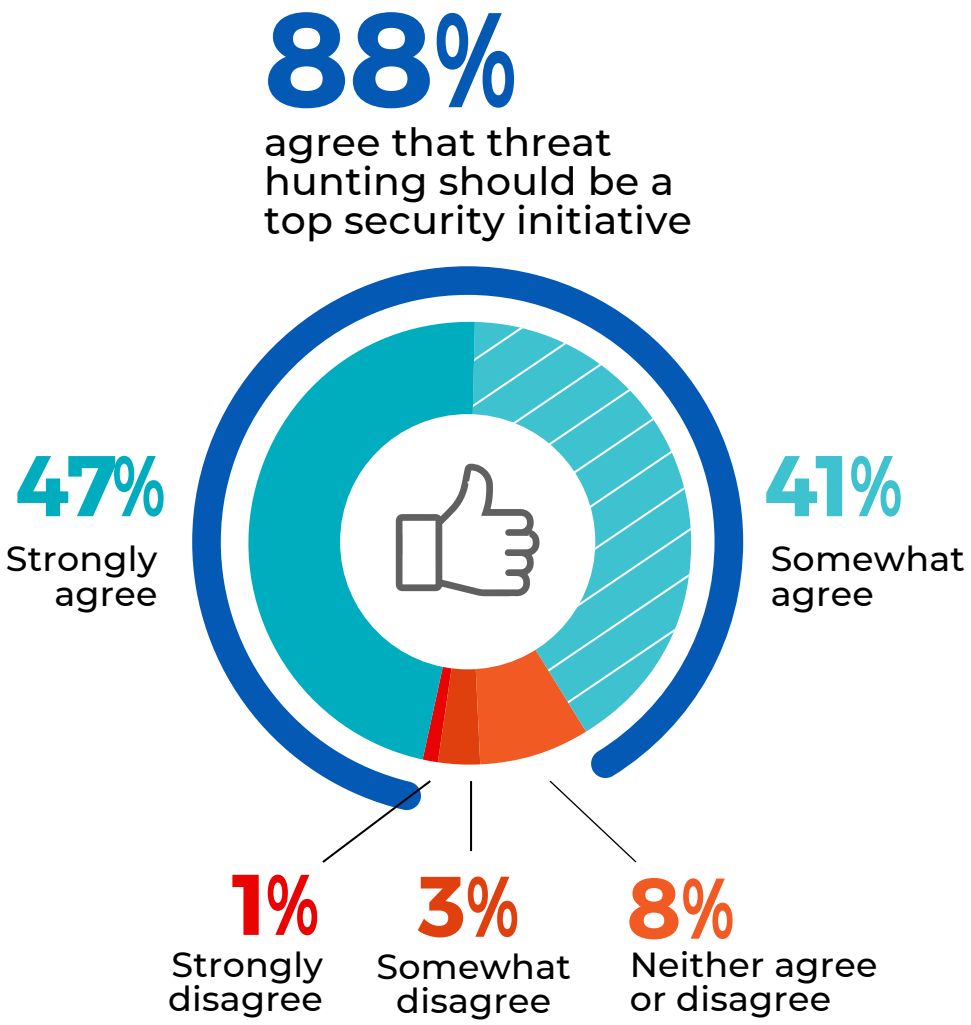


In a typical week at your SOC, what percentage of security threats do you think are missed?

THREAT HUNTING PRIORITY

With threat hunting now an established cybersecurity practice, most organizations agree that threat hunting should be a top security initiative (88%).

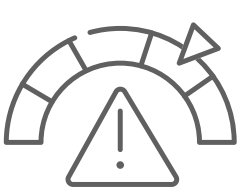
What is your level of agreement with the following statement? "Threat hunting should be a top security initiative."



RISING THREAT LEVELS

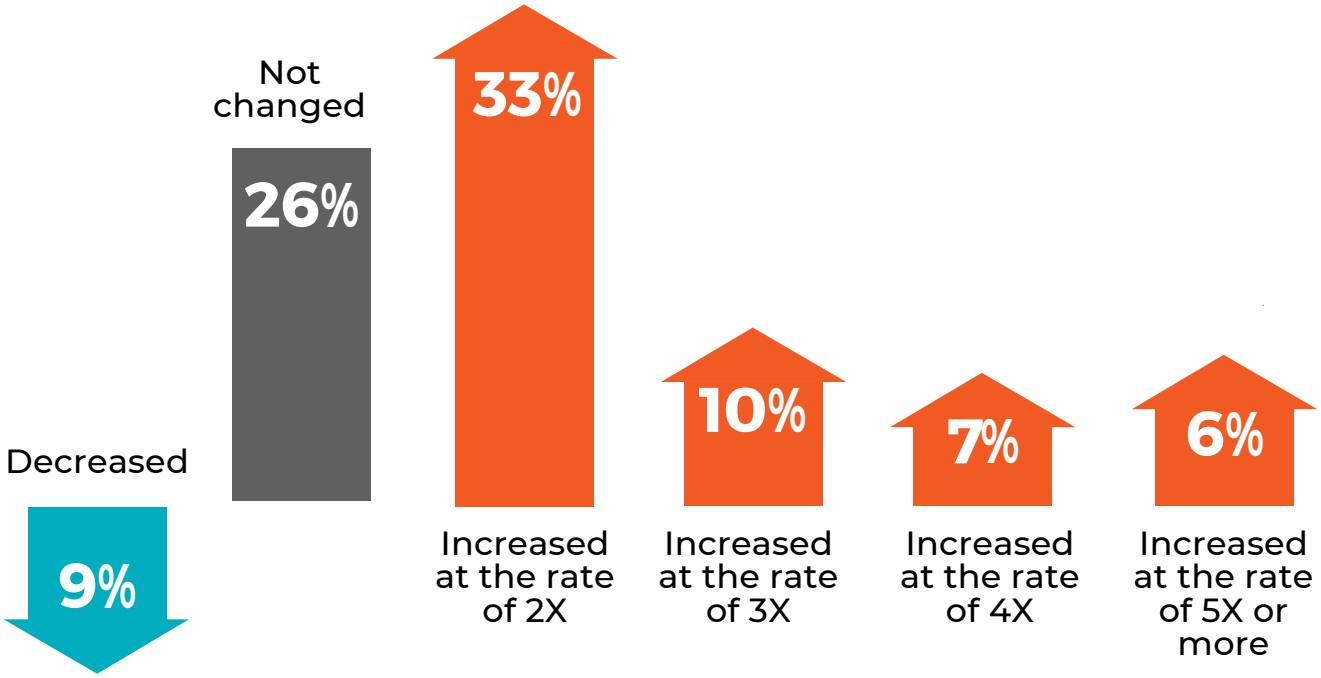
In addition to a rise in the number of cyber attacks, the severity of threats is increasing as well. Over half of organizations (56%) observed an increase in threat levels by a factor of at least two compared to the previous year.

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?



56%

of organizations report an increase in threat levels during the past year

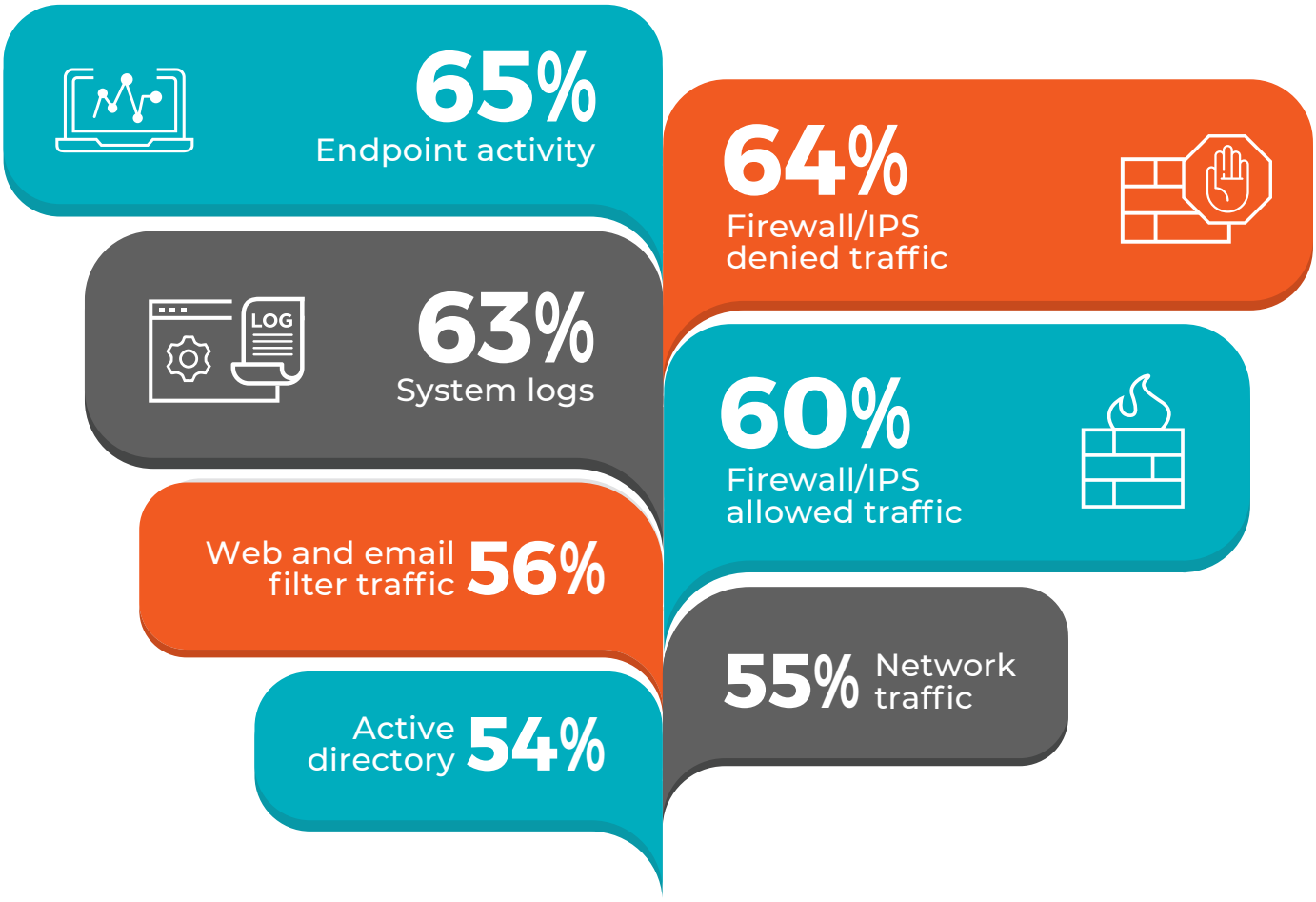


Don't know 9%

DATA COLLECTION SOURCES

Threat hunting is only as effective as the data sources that are collected and analyzed. The top three data sources for threat hunting include endpoint activity (65%), Firewall/IPS denied traffic (64%) and system logs (63%).

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



DNS traffic 47% | Web proxy logs 44% | Server traffic 43% | User behavior 40% | File monitoring data 37% | Packet sniff/tcpdump 32% | Don't know/other 9%

THREAT INDICATORS

We asked threat hunters what threat indicators they most frequently investigate as part of their daily missions. The most common threats are behavioral anomalies (76%), followed by suspicious IP addresses (65%) and denied/flagged connections (55%).

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

76%

Behavioral anomalies
(unauthorized access attempts, etc)

65%

IP addresses

55%

Denied/flagged connections

49%

Domain names

34%

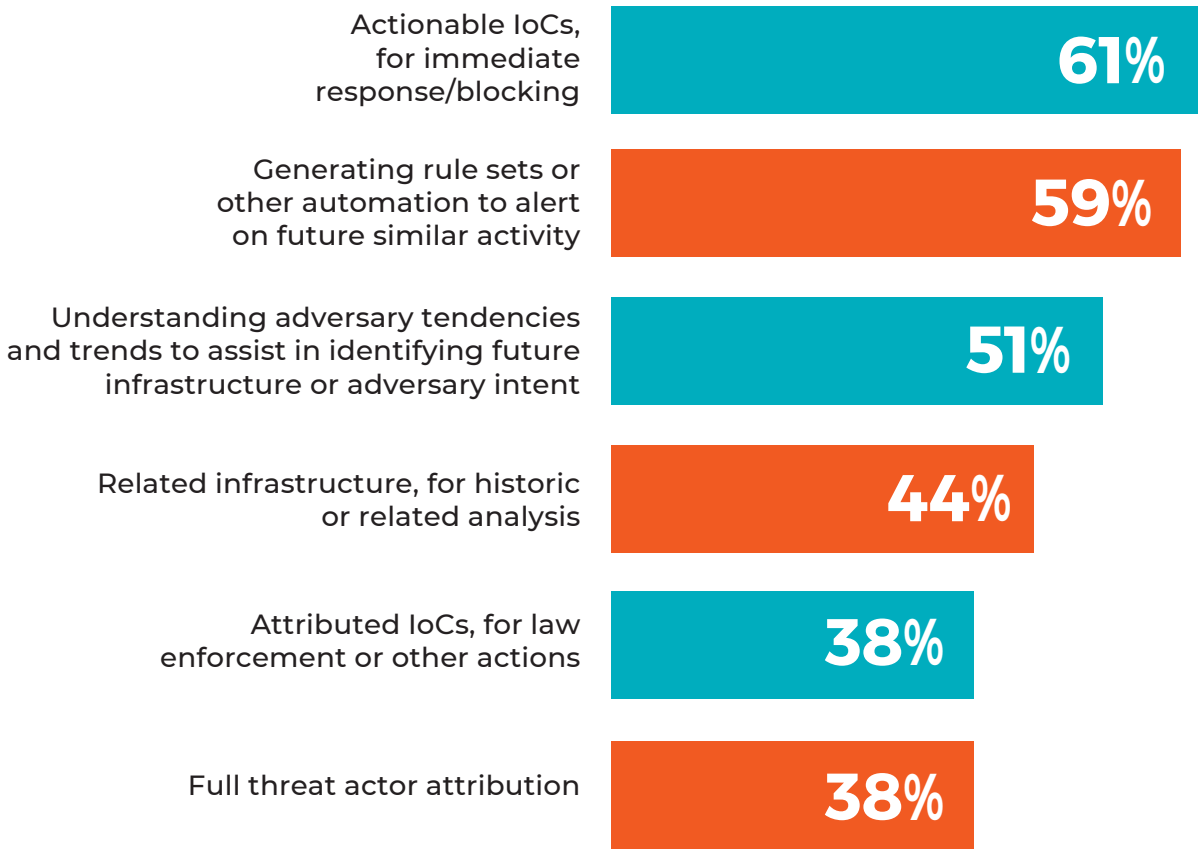
File names

Not sure/other 9%

INSIGHTS INTO ADVERSARIES

Threat hunting can provide valuable insights into adversary infrastructure and allow organizations to become more proactive. Through threat hunting, 61% of organizations in our survey identify actionable indicators of compromise while 59% can generate rule sets or alert automations on future similar activity. Fifty-one percent of organizations find threat hunting produces a deeper understanding of adversary behavior and trends.

What are the most useful insights into adversary infrastructure that threat hunting produces?

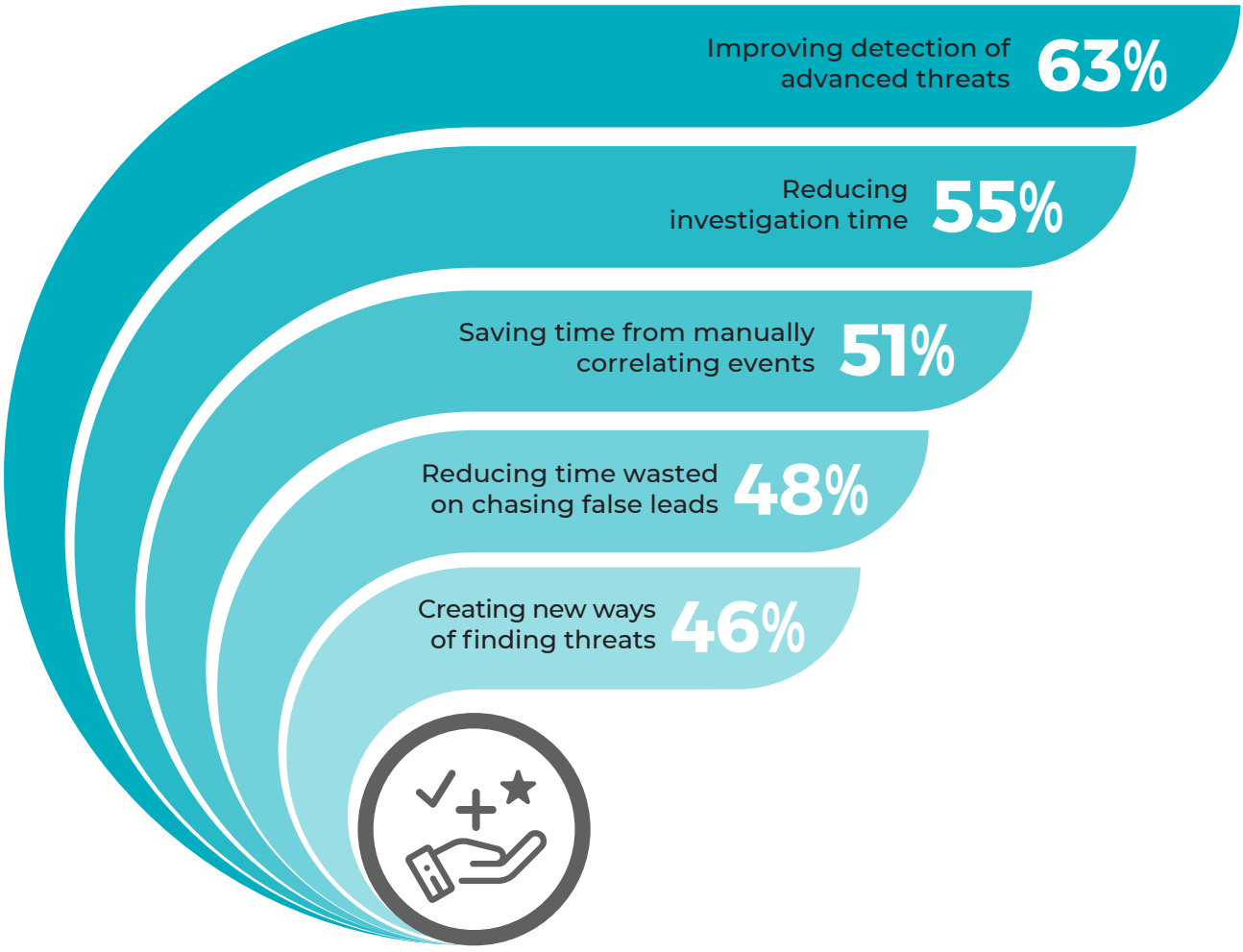


Not sure/other 9%

BENEFITS OF THREAT HUNTING PLATFORMS

Threat hunting platforms provide security analysts with powerful tools to enable earlier detection, reduce dwell time, and improve defenses against future attacks. Threat hunters highlight improving detection of advanced threats (63%), reducing investigation time (55%) and saving time from manually correlating events (51%) as the main benefits of using a threat hunting platform for security analysis.

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

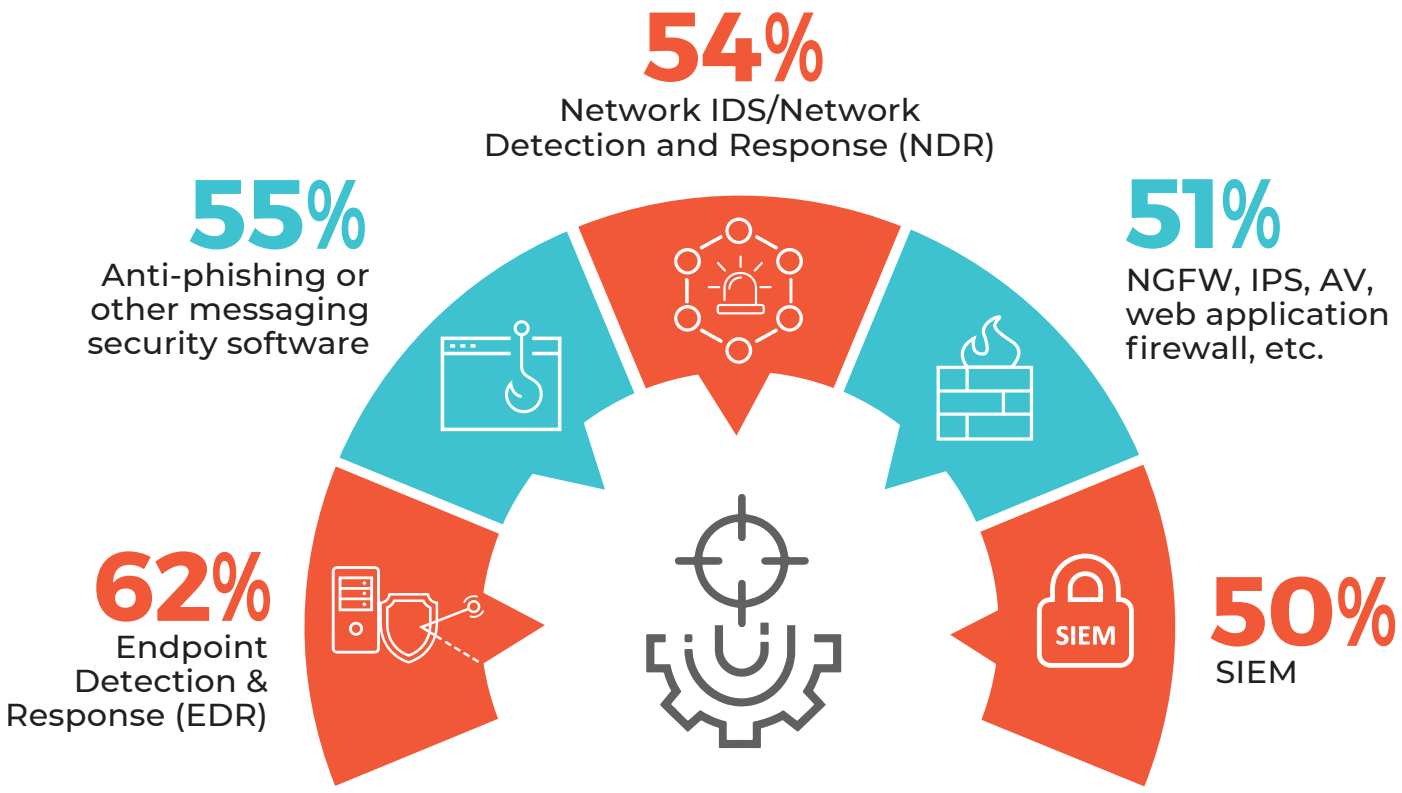


Discovering threats that could not be discovered otherwise 43% | Reducing attack surface 42% | Connecting disparate sources of information 39% | Reducing extra and unnecessary noise in the system 39% | Saving time scripting and running queries 34% | Other 3%

MOST POPULAR THREAT HUNTING TECHNOLOGIES

We asked threat hunters what technologies they use in their daily hunts. Endpoint detection and response tools top the list (62%), followed by anti-phishing (55%) and network detection and response (54%).

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



Vulnerability management 47% | Threat intelligence platform 43% | Security orchestration, automation and response (SOAR) 29% | Enrichment and investigation tools 29% | Not sure/other 10%

THREAT HUNTING INVESTMENTS

What investments would make the biggest difference in organizations' threat hunting abilities? Threat hunters prioritize investing in training (45%), network detection and response (44%), and endpoint detection and response (43%).

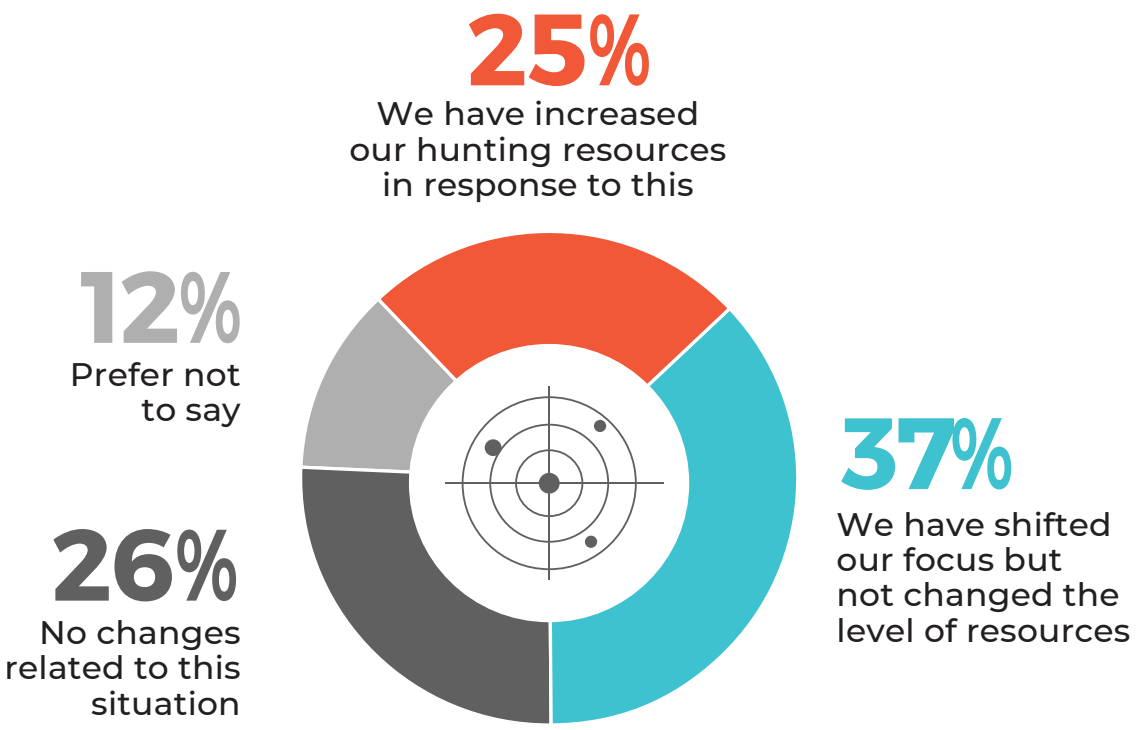
What investments would make the biggest difference in your threat hunting abilities?

Other 2%

IMPACT OF RUSSIA UKRAINE WAR

We asked threat hunters whether the Russian war against Ukraine has changed threat hunting activities. Forty-eight percent of cybersecurity professionals confirm a recent rise in threat activity. This rise is causing a shift in threat hunting focus (37%) and an increase in resources allocated to threat hunting (25%).

How has the war in Ukraine changed your threat hunting activities, if at all?

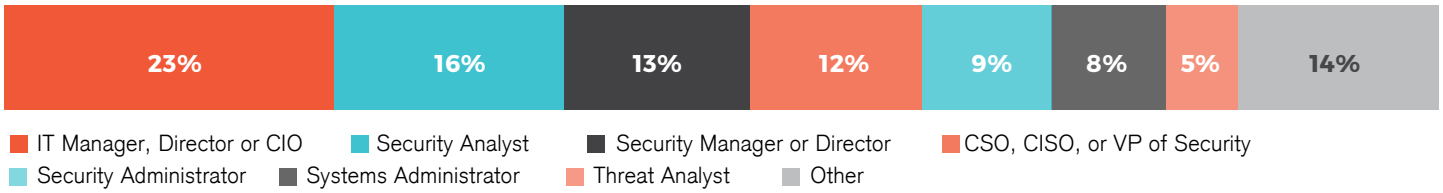


If you are a defender of critical infrastructure (ICS/OT specifically), has your hunting uncovered increased activity since the invasion of Ukraine?

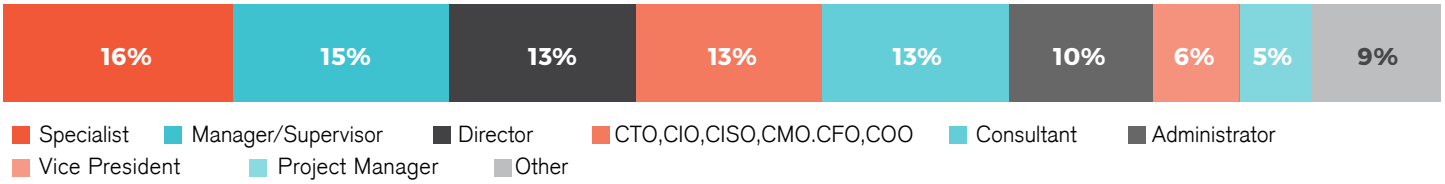
METHODOLOGY & DEMOGRAPHICS

This Threat Hunting Report is based on the results of a comprehensive online survey of 335 cybersecurity professionals, conducted in May 2022, 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.

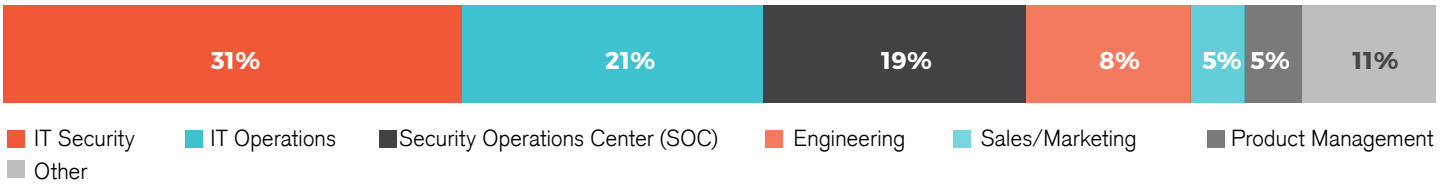
PRIMARY ROLE



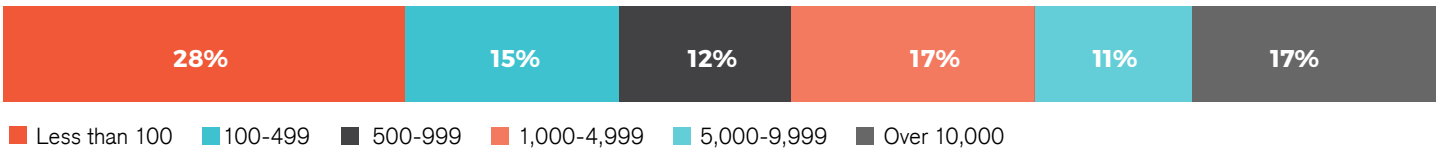
CAREER LEVEL



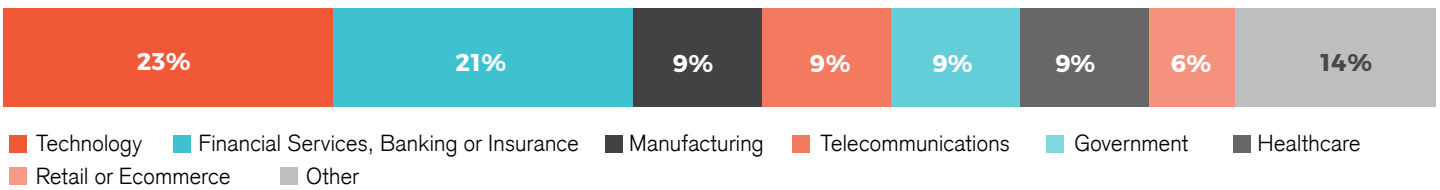
DEPARTMENT



COMPANY SIZE



INDUSTRY



DomainTools 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

or follow us on Twitter:@domaintools

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 500,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit www.cybersecurity-insiders.com