2021

Cybersecurity
INSIDERS

THREAT HUNTING REPORT

DOMAINTOOLS

INTRODUCTION

Threat hunting continues to evolve for organizations that focus on proactively detecting and isolating Advanced Persistent Threats (APTs) that might otherwise go undetected by traditional, reactive security technologies.

While many SOCs are struggling to cope with the current security threat workload, more organizations are adopting 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 2021, Cybersecurity Insiders conducted the fourth annual threat hunting research project to gain deeper insights into the maturity and evolution of the security practice.

Key finding include:

- The survey reveals that cybersecurity professionals see timely detection of advanced threats (55%) and lack expert security staff to mitigate such threats (52%) as the top challenges facing their SOC. This is followed by a lack of confidence in automation tools catching all threats (37%) and too much time being wasted on false-positive alerts as the top challenge for their SOC.
- Organizations highlight a broad range of goals of their threat hunting program. However, reducing exposure to external threats was named by more than half of the organizations surveyed (51%). This is followed by reducing the number of breaches and infections (45%) and reducing attack surface (43%).
- Although threat hunting is still an emerging discipline, it is not surprising that most organizations agree that threat hunting should be a top security initiative (88%).
- Threat hunting platforms provide security analysts with powerful tools to enable earlier detection, reduce dwell time, and improve defenses against future attacks. This year, more organizations (68% in 2021 versus 63% in 2020) highlight improving detection of advanced threats as the main benefit of using a threat hunting platform for security analysts.

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

We hope you enjoy the report.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

THREAT HUNTING GOALS

Organizations highlight a broad range of goals for their threat hunting program. However, reducing exposure to internal threats was named by more than half of the organizations (51%). This is followed by reducing the number of breaches and infections (45%) and reducing the attack surface (43%).

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

51%

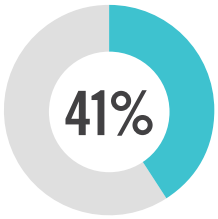
Reduce exposure to internal threats

45%

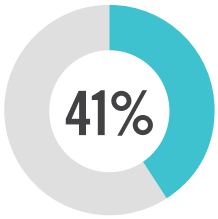
Reduce number of breaches and infections

43%

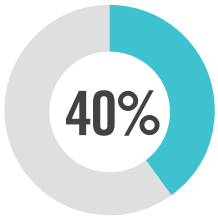
Reduce attack surface



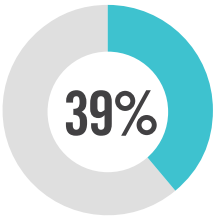
Reduce time to containment (prevent spread)



Reduce exposure to external threats



Improve speed and accuracy of threat response



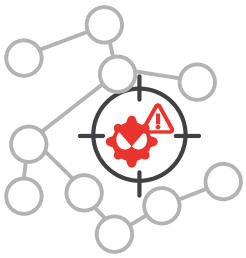
Reduce dwell time from infection to detection

Optimize resources spent on threat response 31% | Other 7%

KEY SECURITY CHALLENGES

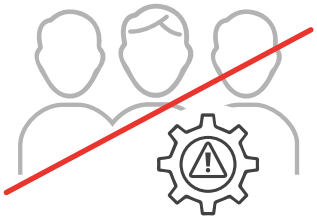
The survey reveals that cybersecurity professionals prioritize timely detection of advanced threats (55%) and lack of expert security staff to mitigate such threats (52%) as the top challenges facing their SOC. This is followed by lack of confidence in automation tools catching all threats (37%) and too much time wasted on false positive alerts (36%).

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



55%

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

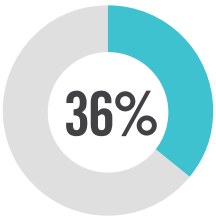


52%

The lack of expert security staff to assist with threat mitigation

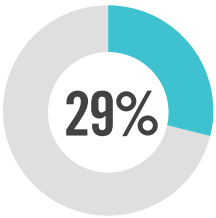
37%

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



Slow response time to advanced threats

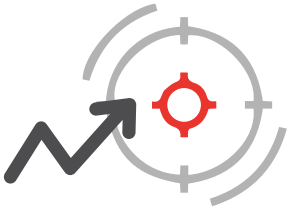
Lack of proper reporting tools

Working with outdated SIEM tools and SOC infrastructure 19% | Other 9%

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. This year, five percent more organizations (68% in 2021 versus 63% in 2020) highlight improving detection of advanced threats as the main benefit for using a threat hunting platform for their security analysts.

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

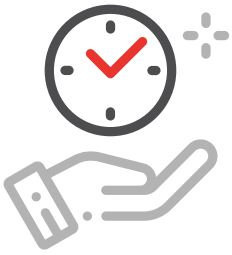


68%

Improving detection of advanced threats

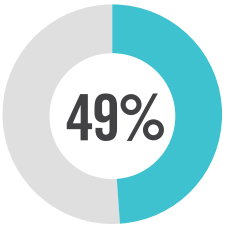
55%

Reducing investigation time

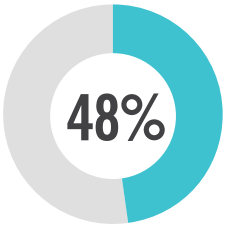


55%

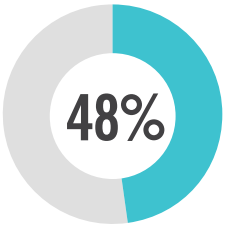
Saving time manually correlating events



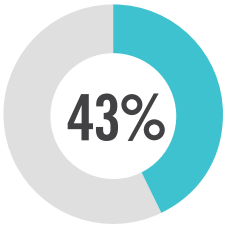
Discovering threats that could not be discovered otherwise



Reducing time wasted on chasing false leads



Reducing attack surface



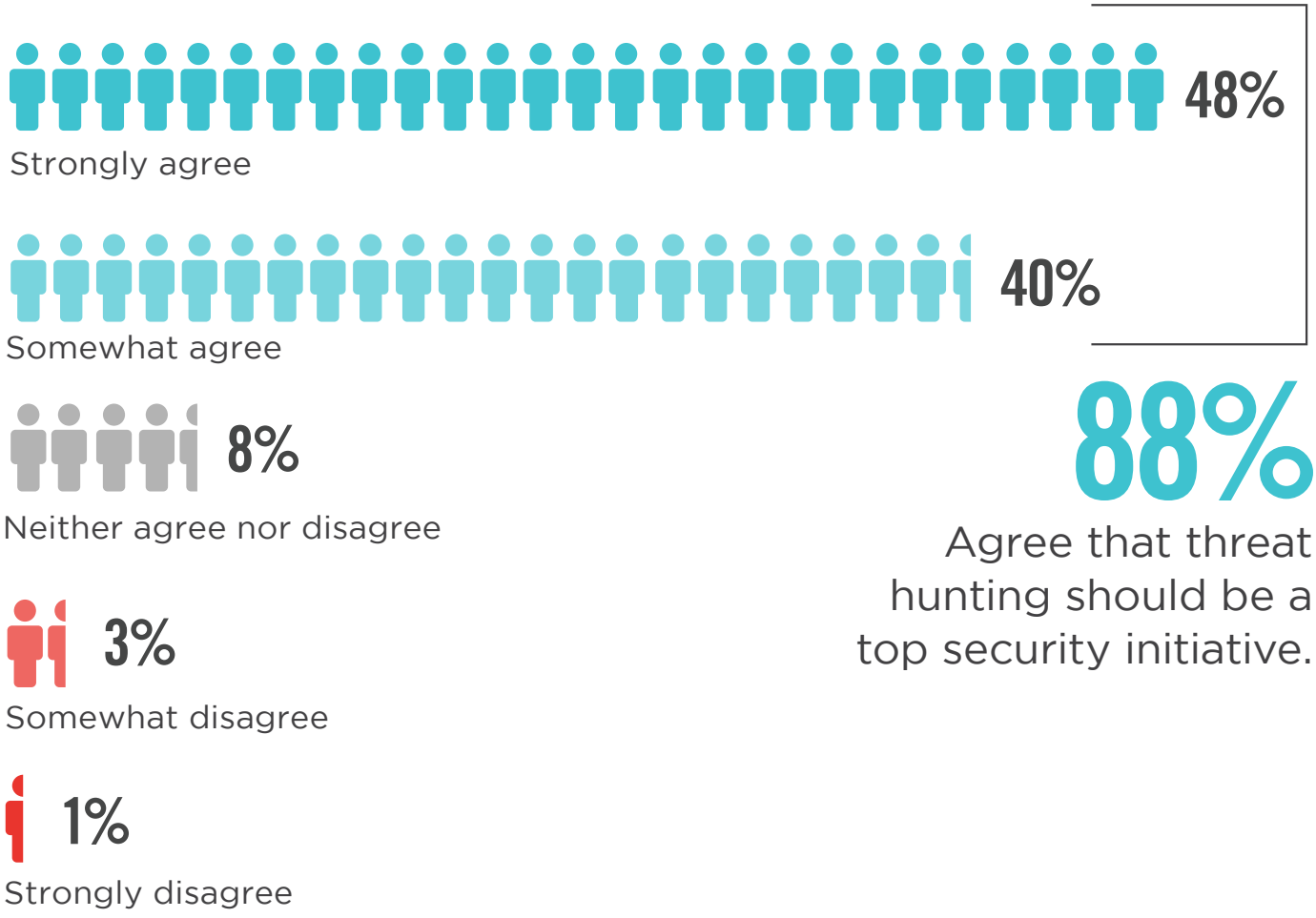
Creating new ways of finding threats

Connecting disparate sources of information 39% | Reducing extra and unnecessary noise in the system 38% | Saving time scripting and running queries 35% | Other 3%

THREAT HUNTING PRIORITY

Although threat hunting is still an emerging discipline, it is not surprising that most organizations agree either strongly (48%) or somewhat (40%) that threat hunting should be a top security initiative.

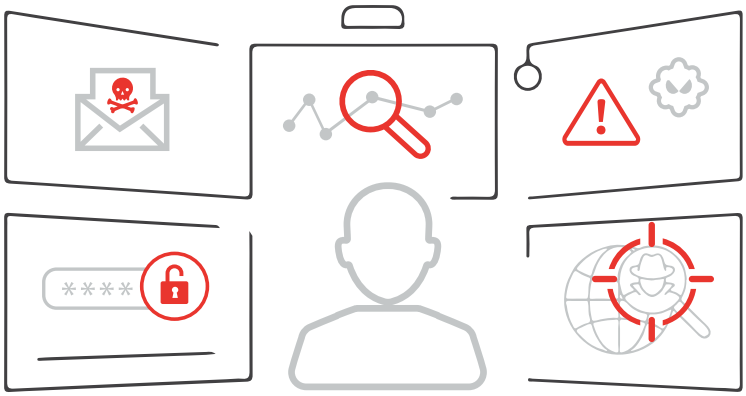
What is your level of agreement with the following statement? "Threat hunting should be a top security initiative."

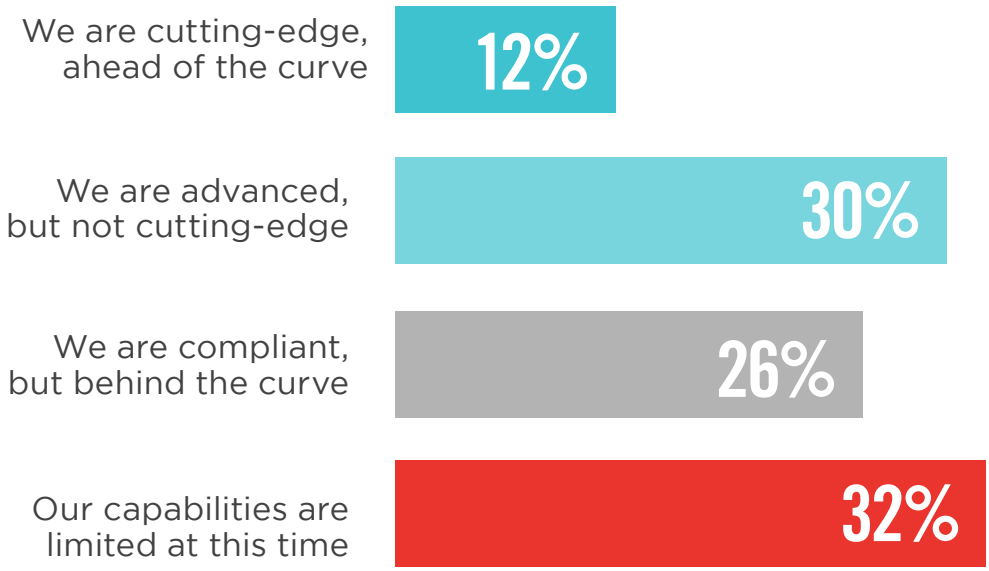


THREAT MANAGEMENT MATURITY

Security Operations Centers (SOCs) continually face rapidly evolving threats to secure and defend their environments against. From a maturity perspective, only 12% of organizations claim to have a mature cutting edge SOC for addressing emerging threats.

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

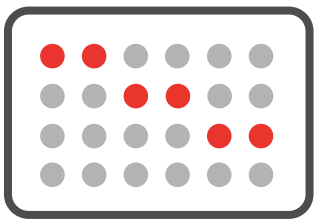




THREAT HUNTERS SKILLS

Based on feedback from organizations data analysis and reasoning skills are in high demand for protection against security threats. For example, pattern recognition (76%), data analytics (70%), and deductive reasoning (67%) are the most important attributes that organizations look for when hiring threat hunters.

What are the most important skills for threat hunters?



76%

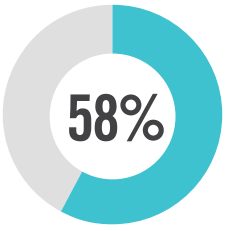
Pattern recognition

70%

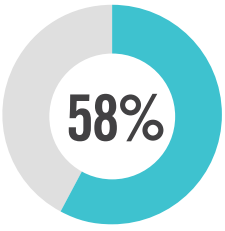
Data analytics

67%

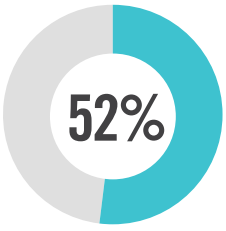
Deductive reasoning



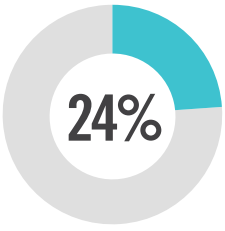
Malware analysis



Data forensics



Communication



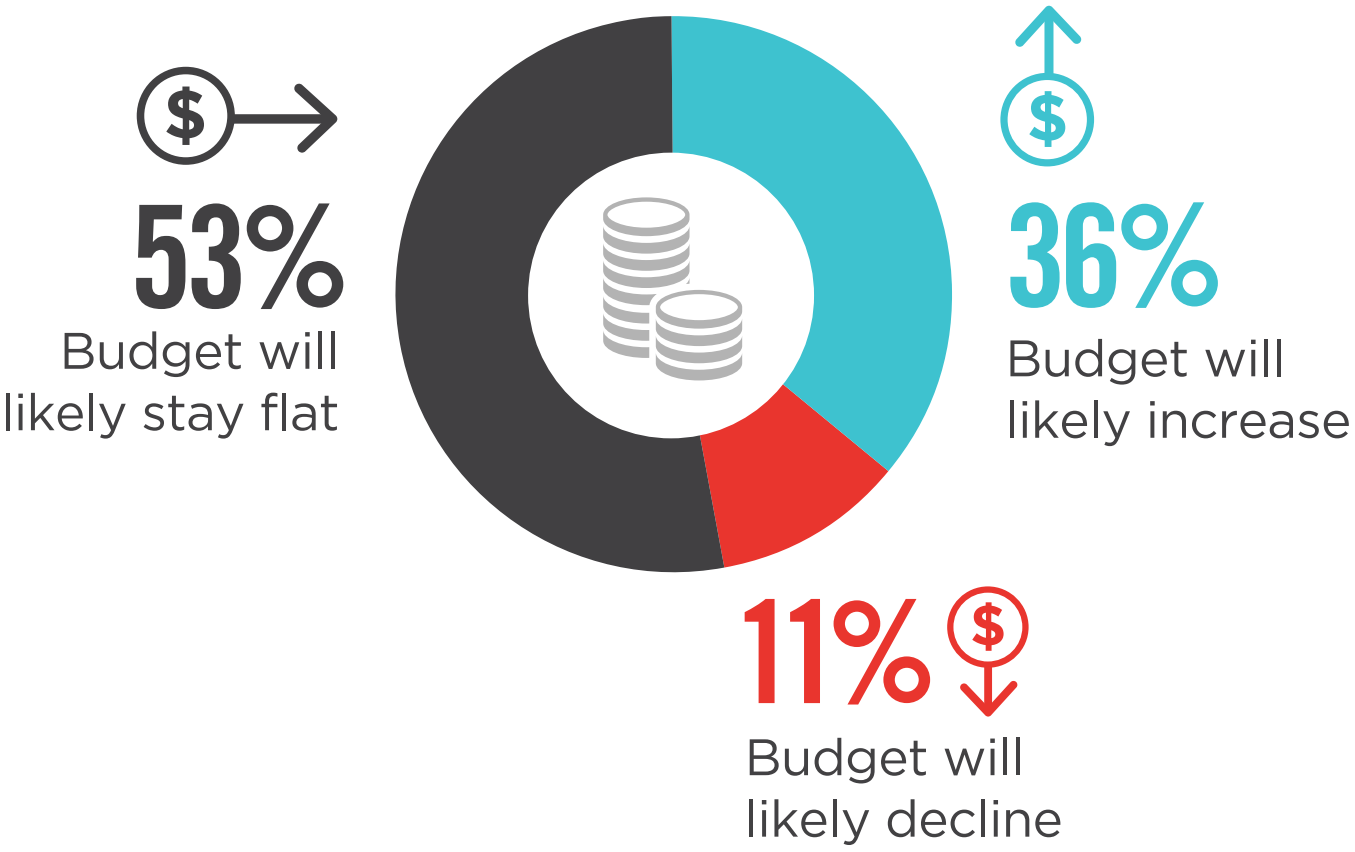
Writing scripts and code

Other 3%

THREAT HUNTING BUDGET

Year after year, there is not much change in how organizations are allocating their threat hunting budget. Last year, 37% of organizations were likely to increase their budgets; this year 36% will grow their threat hunting spend. Similarly, last year 50% kept budgets flat; this year 53% percent will hold threat hunting budgets steady.

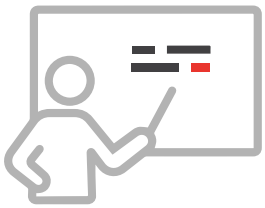
How is your organization's threat hunting budget going to change in the next 12 months?



INVESTMENTS FOR BETTER THREAT HUNTING

Organizations claim investing in more training (45%), better endpoint detection and response (43%), better network detection and response (43%), and better SIEM (40%) would have had the biggest impacts on their threat hunting abilities.

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



45%

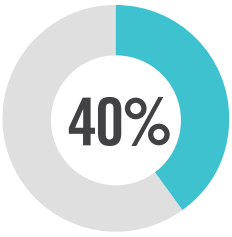
More training for existing staff

43%

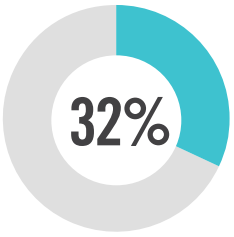
Better Endpoint Detection & Response (EDR)

43%

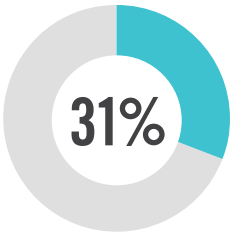
Better Network Detection & Response (NDR)



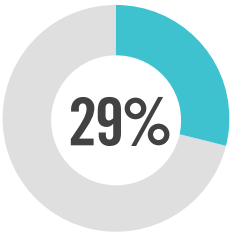
Better SIEM



More staff



Better threat feeds



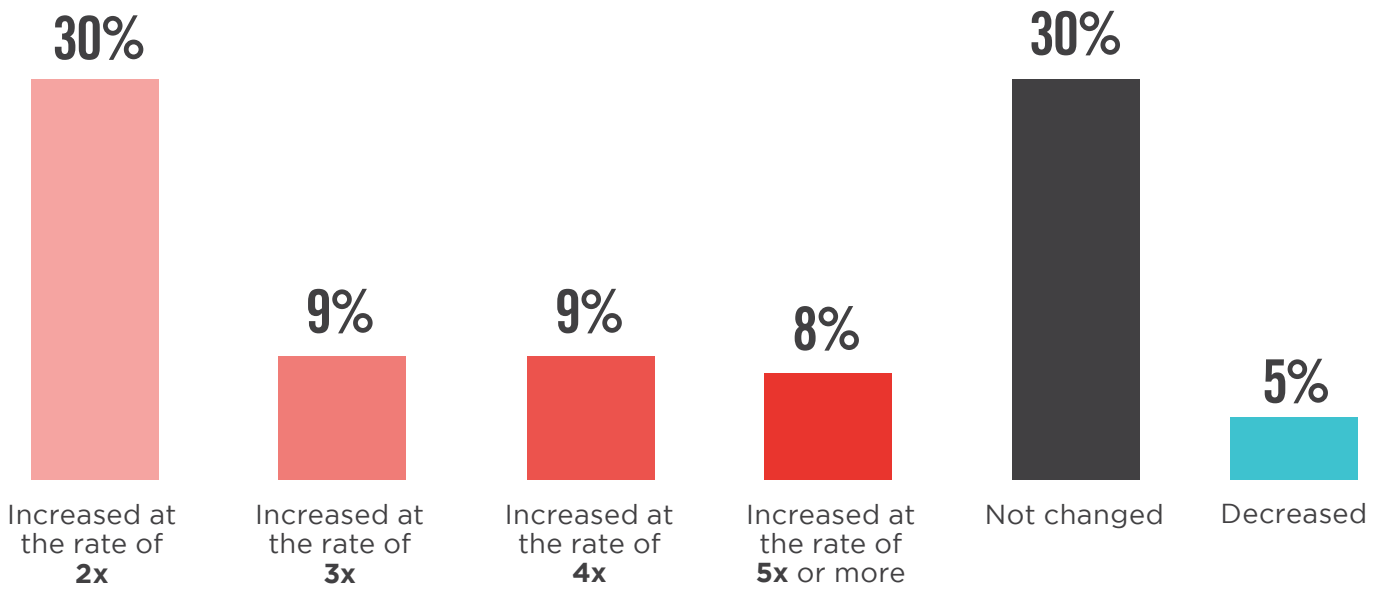
Better technology

More technology 14% | Other 3 %

FREQUENCY OF CYBER THREATS

While there has not been much change year after year in the number of organizations that are seeing a decrease in the frequency of security threats, five percent more organizations this year have found a way to stabilize the frequency of threats facing their organization.

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



Don't know 9%

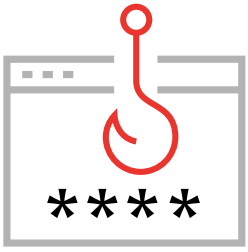
MOST COMMON ATTACKS

The three most common attacks that organizations proactively discover include malware (76%), phishing (71%), and network intrusions (46%).

What are the most common attacks proactively discovered through threat hunting?

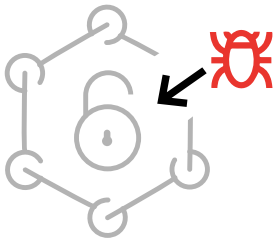
76%

Malware



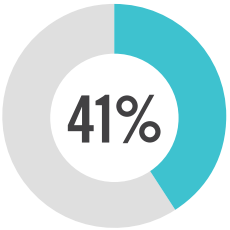
71%

Phishing

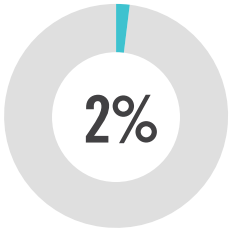


46%

Network intrusion



Ransomware



Supply chain compromise

Other 2%

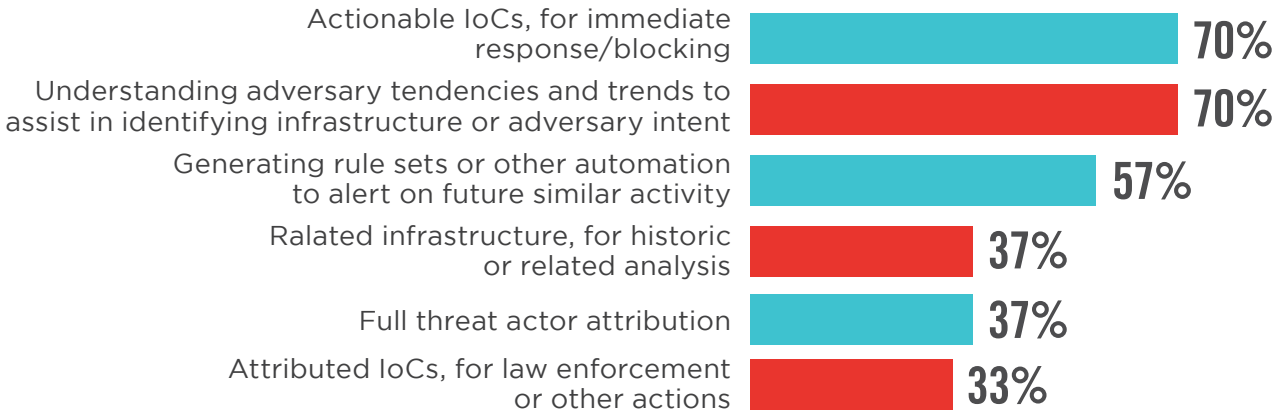
INSIGHTS INTO ADVERSARIES

Sixty-eight percent of all organizations, at least occasionally develop insights into adversary infrastructures as part of their threat hunting activities. When they glean insights from threat hunting, organizations discover actionable IoCs, for immediate response/blocking and better understanding adversary tendencies and trends to assist in identifying infrastructure or adversary intent.

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

68% **Of all organization at least occasionally develop insights into adversary infrastructures as part of their threat hunting activities.**

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

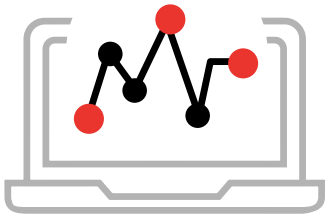


Other 3%

DATA COLLECTION SOURCES

Organizations collect a host of data to analyze security risks. This year, endpoint activities (72%) and system logs (71%) take the top two spots for what organizations assess. Firewall traffic is third (69%), falling two notches over last year.

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

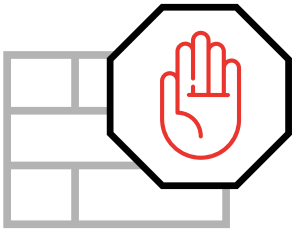


72%

Endpoint activity

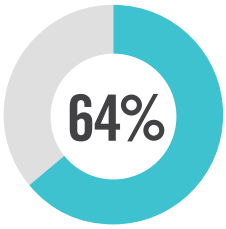
71%

System logs

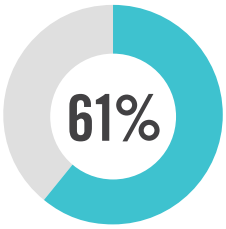


69%

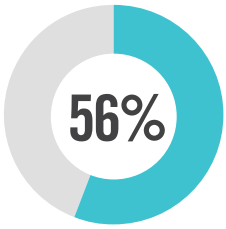
Firewall/IPS denied traffic



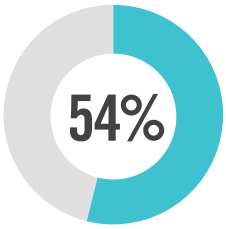
Firewall/IPS allowed traffic



Web and email filter traffic



Network traffic



Threat intelligence sources

Active directory 53% | DNS traffic 52% | Server traffic 47% | Web proxy logs 45% | User behavior 39% | File monitoring data 36% | Packet sniff/tcpdump 33% | Don't know/other 12%

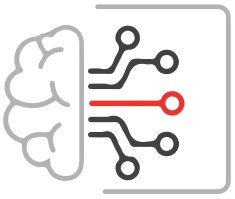
MOST VALUABLE DATA SOURCES

The top three valuable data sources for investigating known threats include activity logs (31%), threat intelligence feeds (24%), and network data (21%), followed by endpoint data (18%).

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

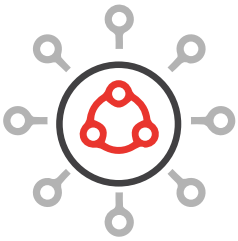
31%

Activity logs



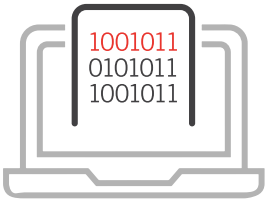
24%

Threat intelligence feeds



21%

Network data



18%

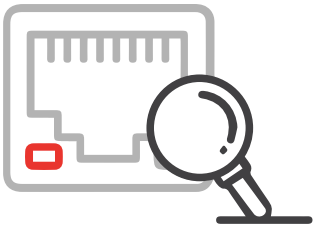
Endpoint data

Other 6%

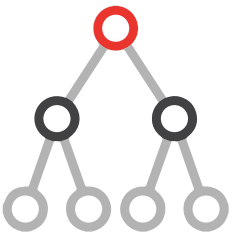
POPULAR RECONNAISSANCE ACTIVITIES

Port scanning is the most used activity for reconnaissance, with 73% of organizations including this technique in their threat hunting efforts.

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

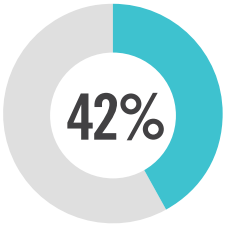


73%
Port scanning

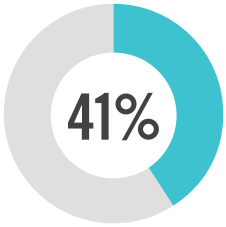


54%
Active directory enumeration

44%
Host enumeration

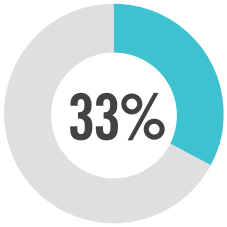


Remote system discovery



LDAP queries

Password policy discovery



Service enumeration

Open share enumeration 31% | None 10% | Other 4%

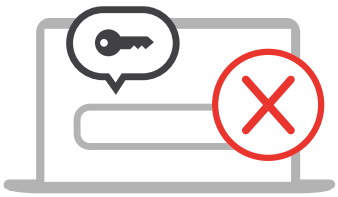
ACTIVE DIRECTORY BEHAVIORS

There are three active directory events organizations look for as part of their threat hunting activities: attempts to reset admin and sensitive account passwords (67%), login failures (61%), and domain policy changes (48%).

Which of the following active directory events do you look for as part of your threat hunting activities?

67%

Attempt to reset admin and sensitive account passwords

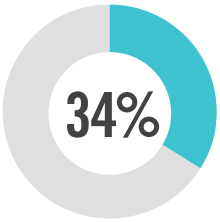


61%

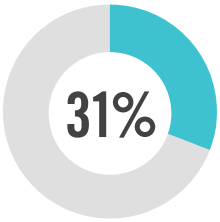
Logon failure

48%

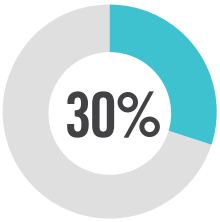
Domain policy was changed



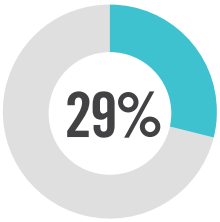
DSRM account password change attempt



SID history added to an account/ attempt failed



Kerberos authorization ticket (TGT) was requested



Kerberos policy was changed

User requests a Kerberos service ticket 24% | Custom special group logon tracking 24% | None 10% | Other 4%

THREAT HUNTING TECHNOLOGIES

There is a diverse portfolio of technologies for threat hunting. While last year endpoint detection and response and SIEM were equally sited (55%) as the top technologies, this year endpoint detection and response is the clear leader with 63% of organizations integrating these tools into their threat hunting efforts.

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

63%

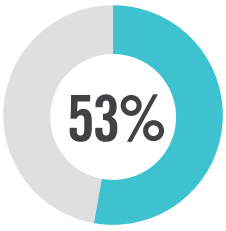
Endpoint Detection & Response (EDR)

56%

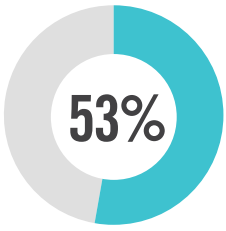
SIEM

54%

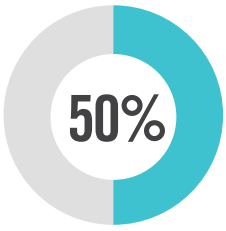
Anti-phishing or other messaging security software



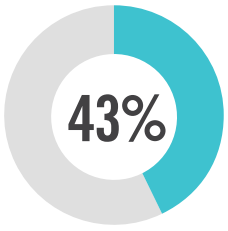
NGFW, IPS, AV, web application firewall, etc.



Network IDS/ Network Detection and Response (NDR)



Vulnerability management



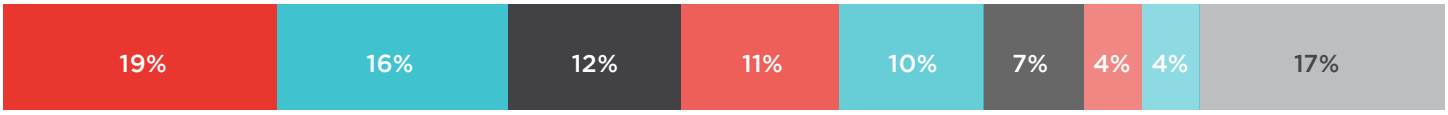
Threat intelligence platform

Enrichment and investigation tools 29% | Security Orchestration, Automation and Response (SOAR) 19% | Not sure/ other 12%

METHODOLOGY & DEMOGRAPHICS

This Threat Hunting Report is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in February 2021, 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



IT Manager, Director or CIO | CSO, CISO or VP of Security | Security Analyst | Security Manager or Director | Systems Administrator | Security Administrator | Threat Analyst | Auditor | Other

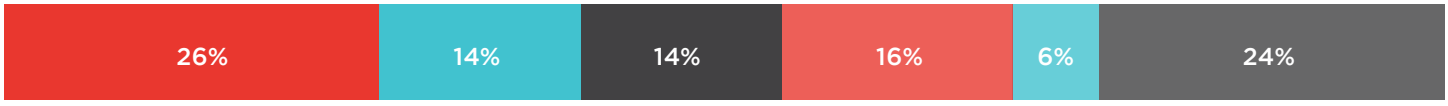
CAREER LEVEL

Director | Specialist | CTO,CIO,CISO,CMO.CFO,COO | Manager/Supervisor | Consultant | Administrator | Owner | CEO/President | Other

DEPARTMENT

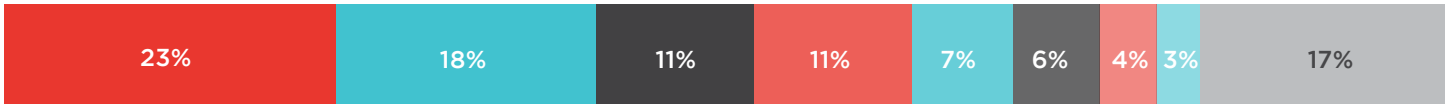
IT Security | IT Operations | Security Operations Center (SOC) | Engineering | Sales/Marketing | Product Management | Other

COMPANY SIZE



Less than 100 | 100-499 | 500-999 | 1,000-4,999 | 5,000-9,999 | Over 10,000

INDUSTRY



Technology | Financial Services, Banking or Insurance | Government | Healthcare | Manufacturing | Telecommunications or ISP | Retail or Ecommerce | Energy or Utilities | Other

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