2020

Cybersecurity INSIDERS

The Importance of Threat Hunting Automation for XDR

Hunters.

INTRODUCTION

Extended Detection & Response (XDR) is a promising, emerging solution category that the industry is turning toward in order to improve threat detection and response by crossing all attack surfaces and reducing alert noise.

While the pace and breadth of threats outstrip human-based detection and single-point solutions, it also overwhelms SOC teams triage with a deluge of alerts and false-positives. Organizations worldwide are beginning to add XDR correlations to their existing security stack, both for detection efficacy and overall SOC operational efficiency.

However, correlation is only one piece of the puzzle. Threat hunting has long been an effective framework for cohesive threat analysis and data connection across sparse, siloed areas of the enterprise. Unfortunately, due to the scarcity in domain expertise, it has also been extremely difficult to scale. Automating proactive threat hunting processes for XDR can transform this equation.

In 2020, Cybersecurity Insiders conducted in-depth research on threat hunting in SOC detection and response to gain deeper insights into the maturity and evolution of the XDR security practice. The research confirms that threat hunting automation can transform extended detection and response.

Organizations realize that threat hunting is viable to improve defenses against current and future attacks, and moreover, that automating them can play a critical role in XDR solutions. Security leaders can provide their security analysts with powerful technologies to enable earlier detection at scale, reduce dwell time, and improve breach detection.

Key findings include:

- 82% of respondents agree that attackers typically dwell in a network between 1-15 days, on average, before they're discovered by the SOC. Only 13% report they can detect attacks within the same day, and almost half of organizations (47%) within 5 days.
- Respondents think 38% of advanced, emerging threats are missed by traditional security tools.
- Organizations confirm that it takes 4x more time to detect threats without a threat hunting solution, and more than twice the time to investigate threats without a threat hunting solution.
- The most important capability that cybersecurity professionals consider critical to the effectiveness of their threat hunting solutions is automatic detection (69%), followed by threat intelligence (62%), and integration and normalization of multiple data sources (48%).
- The top benefits organizations derive from threat hunting automation include improved detection of advanced threats (63%), followed by reduced investigation time (55%), and saving time manually correlating events (47%).

We would like to thank Hunters for supporting this important research. We hope you find this report informative and helpful as you continue your efforts in protecting sensitive data, systems and workloads.

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity INSIDERS

SECURITY OPERATIONS CHALLENGES

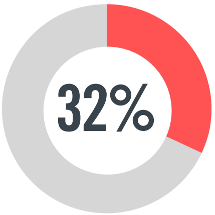
The top three security operations challenges experienced by IT organizations include the perennial shortage of cybersecurity skills in-house (51%), followed by the cost and complexity of building in-house security operations (38%), tied with the lack of continuous 24x7 security coverage (38%). These are the exact same issues managed security services are designed to address.

What are the top three security operations challenges for your IT organization?

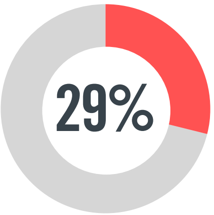
51%
Cybersecurity skills shortage in-house

38%
Cost and complexity of building in-house

38%
Lack of 24x7 security coverage



Speed of incident response issues



No visibility into overall security posture

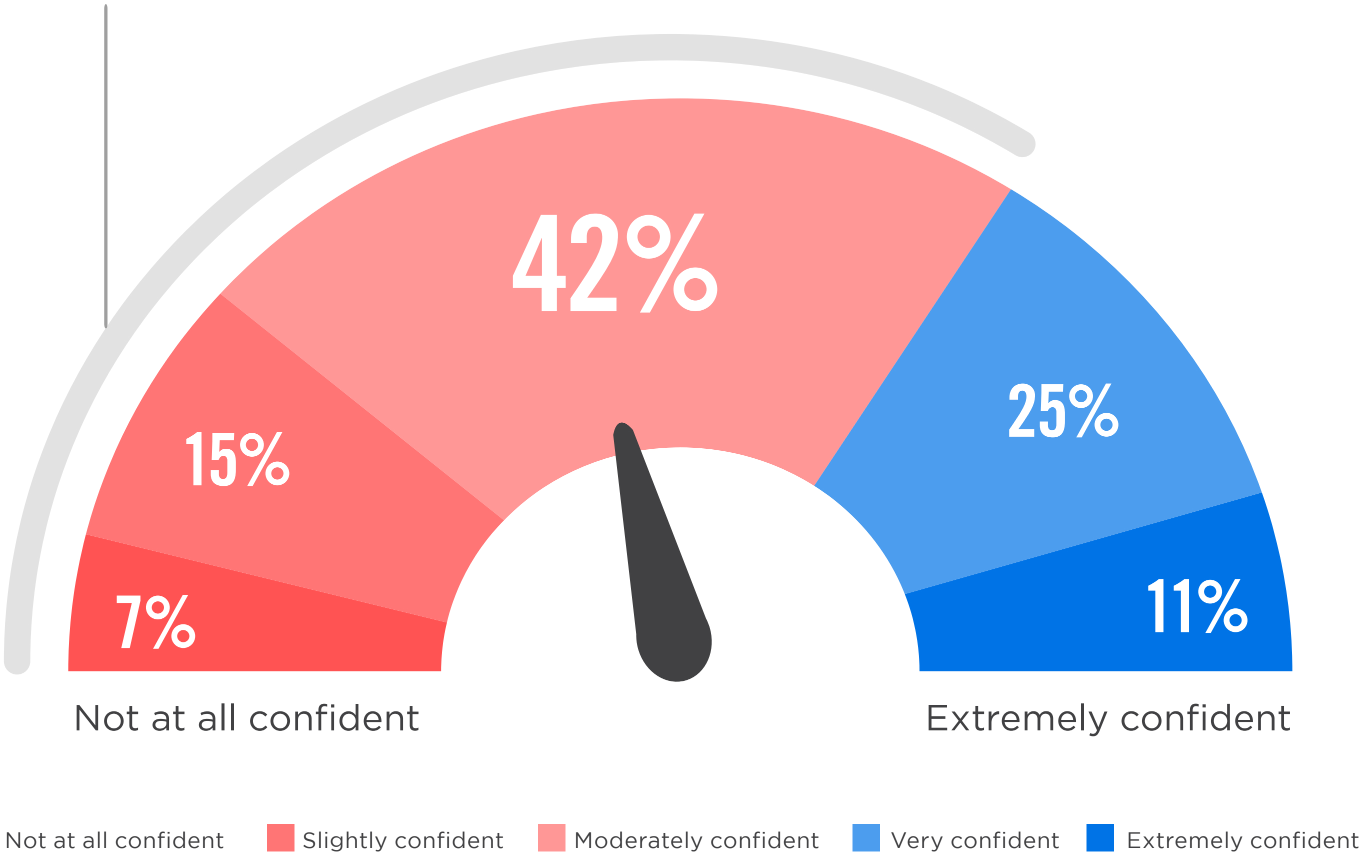
Lack of detection and response capabilities 27% | Speed of deployment and provisioning issues 26% | Lack of customization of correlation rules and reports 19% | Not able to meet compliance requirements 17% | Getting adequate budget approved 14% | Can't effectively deal with cloud security 6% | Other 8%

ATTACK RESPONSE CONFIDENCE

The majority of respondents (64%) are moderately confident (or less) in their ability to respond to a cyberattack. This finding coincides with other recent industry research to show that there is an overall need for dedicated, 24x7 security threat detection and response.

▶ How confident are you in your organization's ability to respond to a cyberattack?

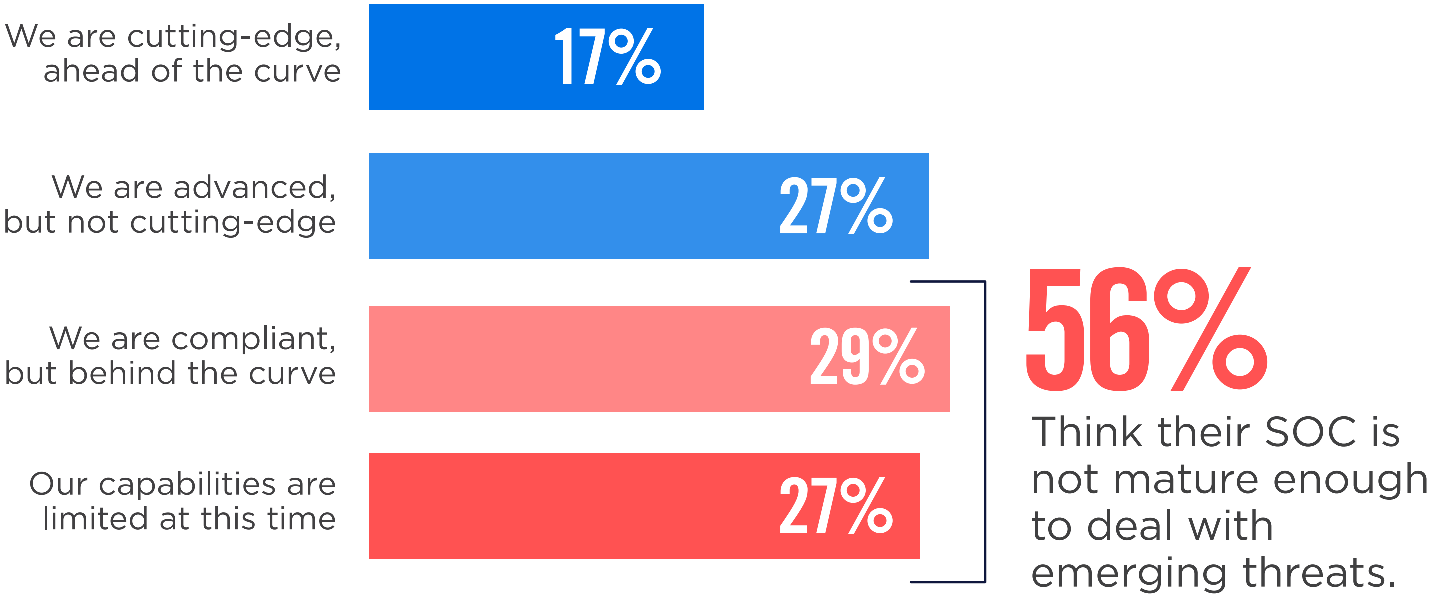
64% Feel moderately confident to not confident at all in their ability to respond to a cyberattack.



SOC 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 (44%) believe they are at least advanced (27%) or cutting-edge (17%) in their ability to address emerging threats.

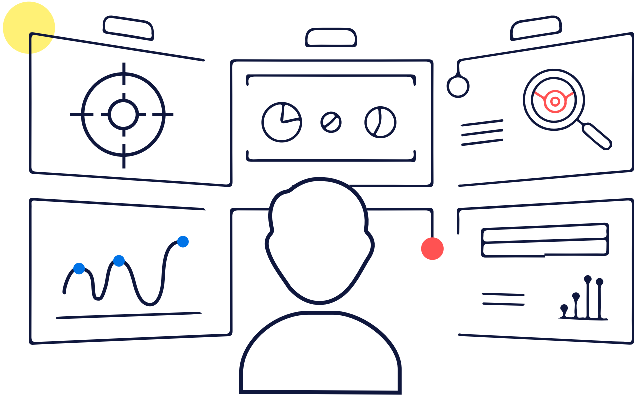
Which of the following best reflects the maturity of your SOC in addressing emerging threats?

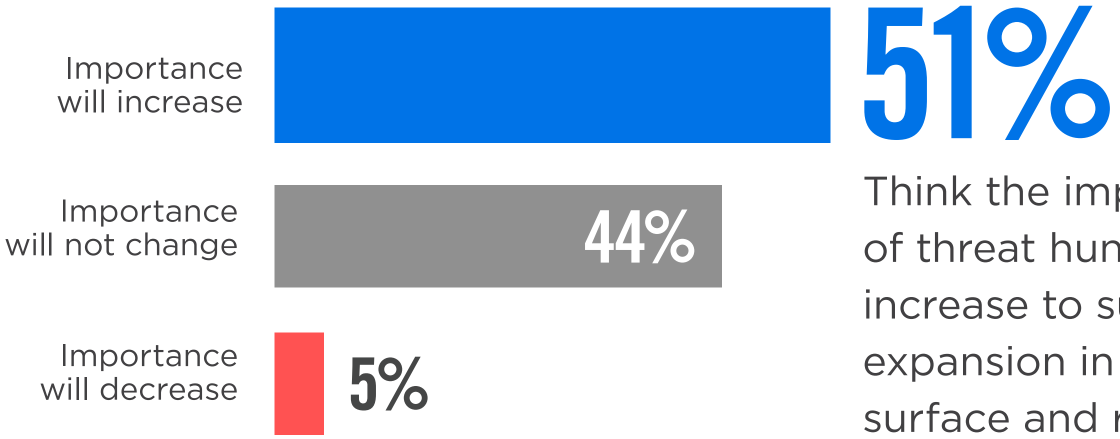

We are cutting-edge, ahead of the curve
17%
We are advanced, but not cutting-edge
27%
We are compliant, but behind the curve
29%
Our capabilities are limited at this time
27%
56%
Think their SOC is not mature enough to deal with emerging threats.

THREAT HUNTING AUTOMATION

When asked about the future importance of threat hunting automation, a majority of organizations (51%) believe the importance of threat hunting will increase to support expansion in attack surface and remote workforce.

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?



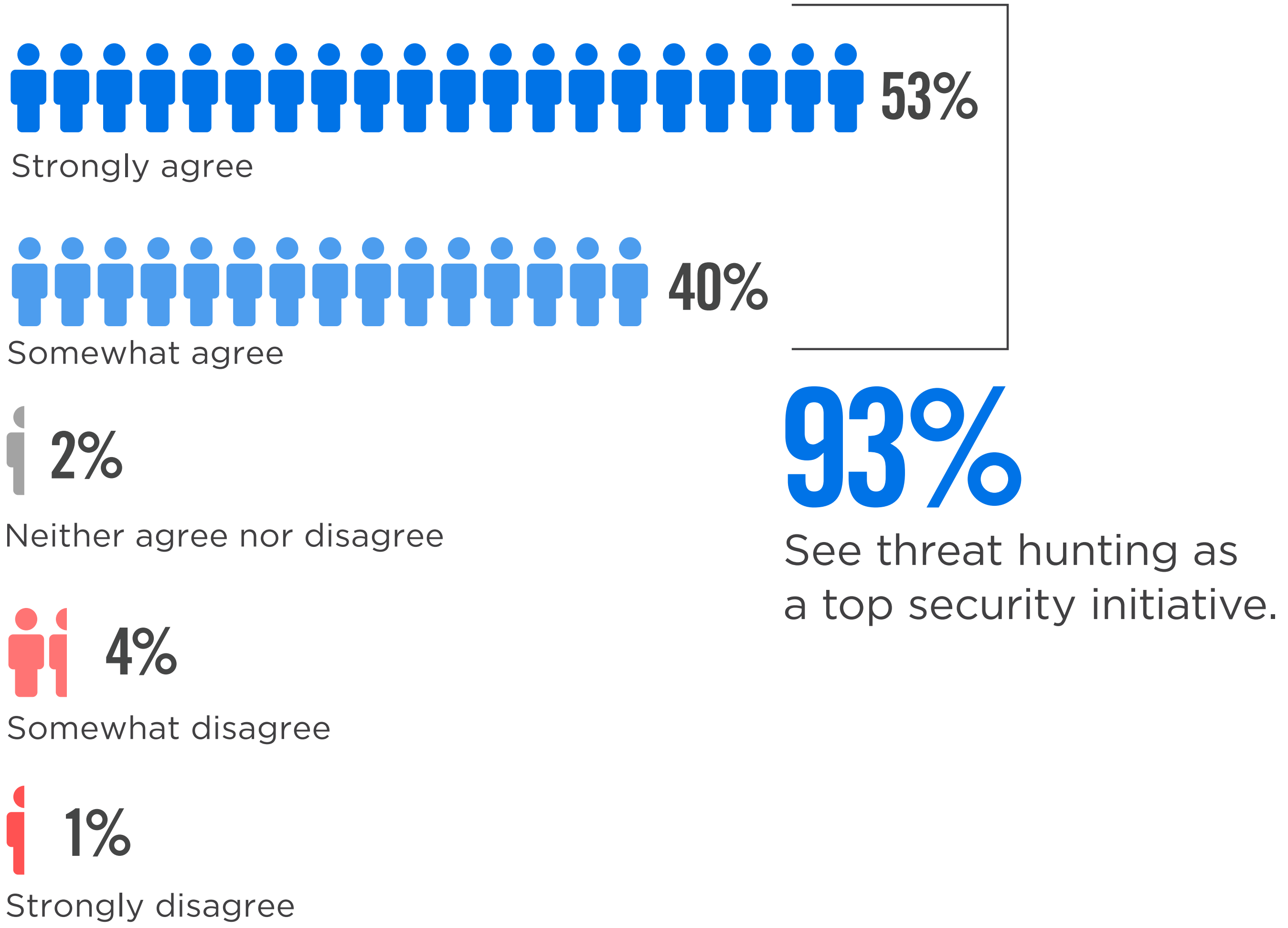


Think the importance of threat hunting will increase to support expansion in attack surface and remote workforce.

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.”



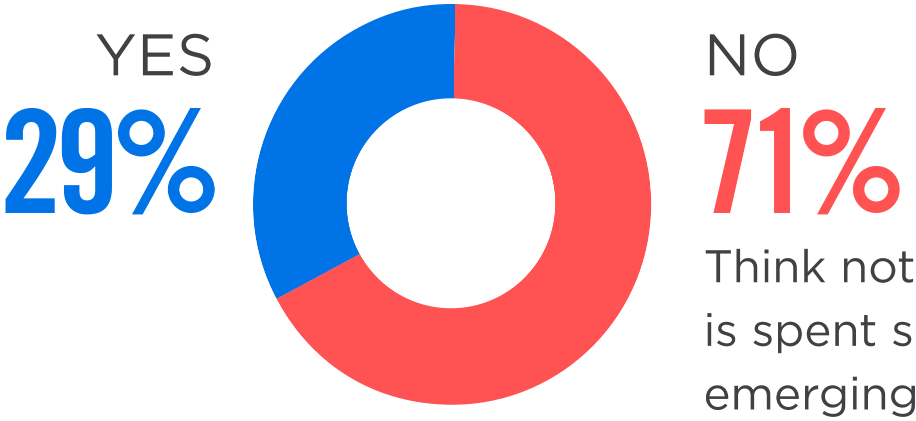
93%

See threat hunting as a top security initiative.

ADVANCED THREATS 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 responses 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?



Think not enough time is spent searching for emerging and advanced threats.

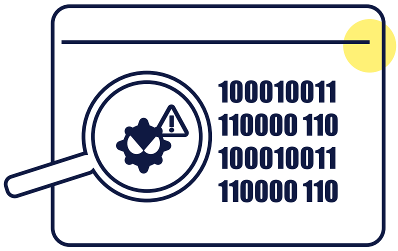
BREACH DISCOVERY

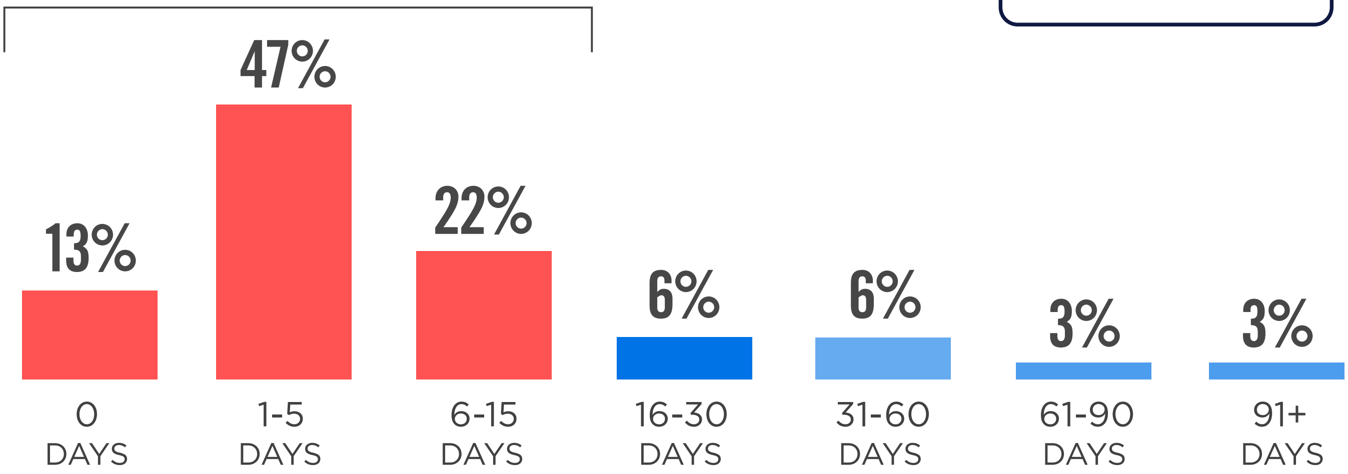
Nearly three-quarters of respondents agree that attackers typically dwell on a network between one and 15 days, an average (82%) before they're discovered by the SOC. Only 13% report they can detect attacks within one day, almost half (47%) within five days.

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

82%

Attest that attackers dwell between 1-15 days, an average before found in their network.

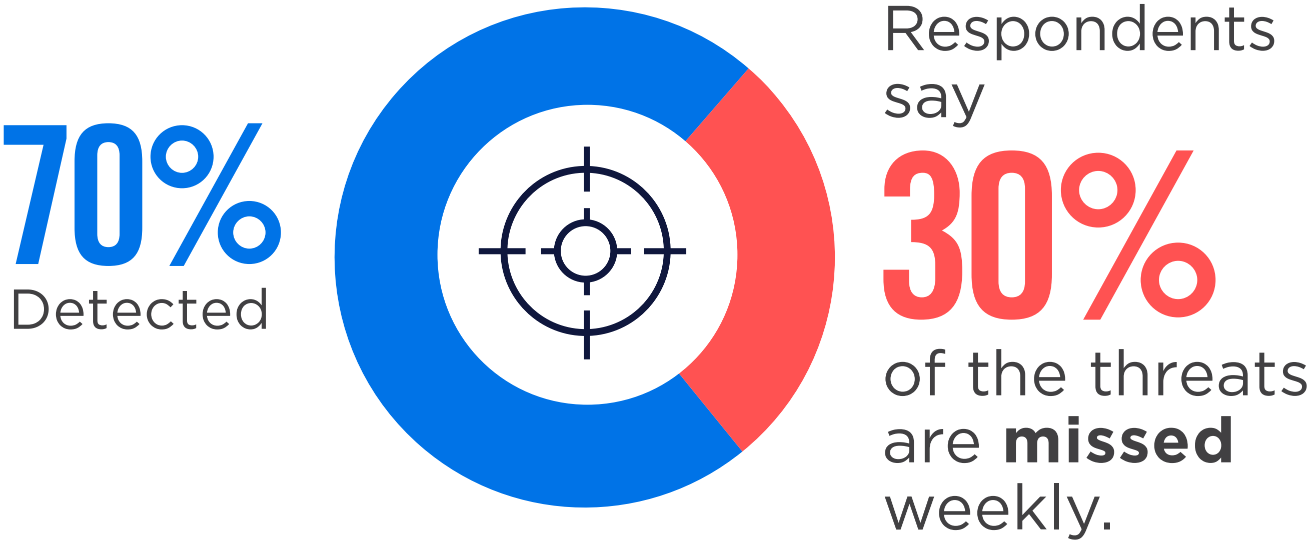




MISSED SECURITY THREATS

When asked about a typical week at your SOC, respondents said they think 30% of the threats are missed weekly.

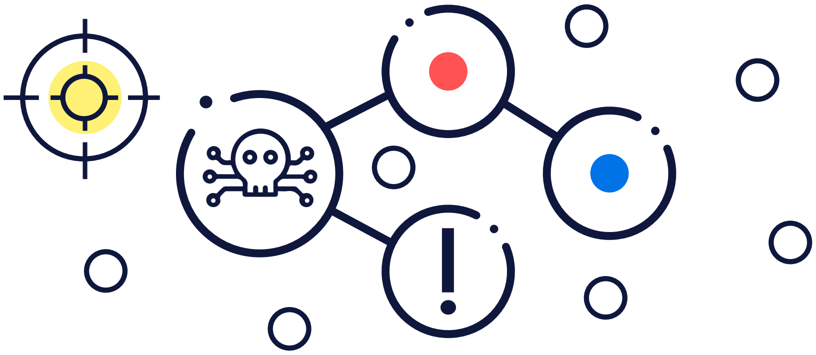
In a typical week at your SOC, what percentage of security threats do you think are missed?



THREATS MISSED BY TRADITIONAL SECURITY TOOLS

Respondents think that 38% of advanced and emerging threats are missed by traditional security tools.

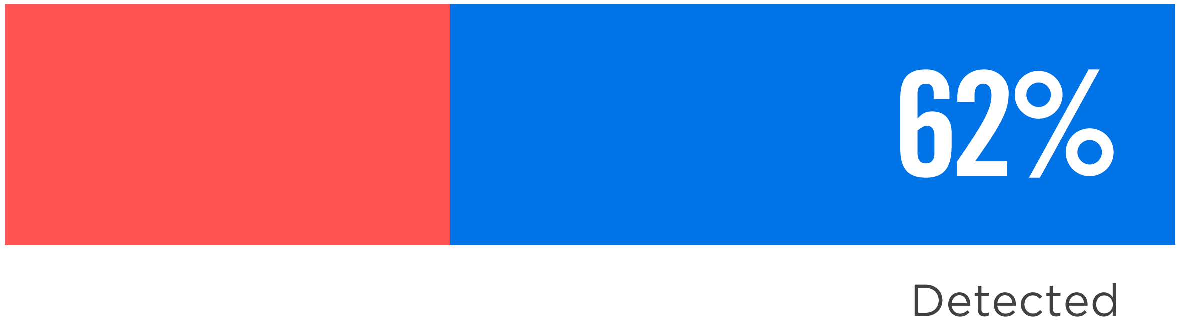
What percentage of emerging and advanced threats are missed by traditional security tools?



Respondents say

38%

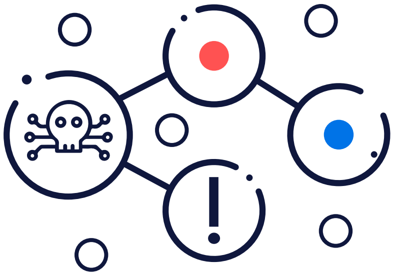
Of advanced and emerging threats are **missed** by traditional security tools.



TIME TO DETECT AND INVESTIGATE

Threat hunting solutions can speed the detection and investigation of threats. Respondents claim it takes four times longer to detect threats WITHOUT a threat hunting solution, and 2.3 times longer to investigate WITHOUT a threat hunting solution.

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



	Time to detect	Time to investigate
WITH a threat hunting solution	10hrs	16hrs
WITHOUT a threat hunting solution	41hrs	38hrs

It takes **4X more time** to detect threats without a threat hunting solution.

It takes **2.3X more time** to investigate threats without a threat hunting solution.

DATA COLLECTION SOURCES

Most organizations prioritize data from denied (77%) and allowed (73%) firewall/IPS traffic, together with web and email filter traffic (70%), and endpoint activity (70%) as the most important data sources to collect. There are numerous security relevant datasets 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

70%
Web and email filter traffic

70%
Endpoint activity

68%
System logs

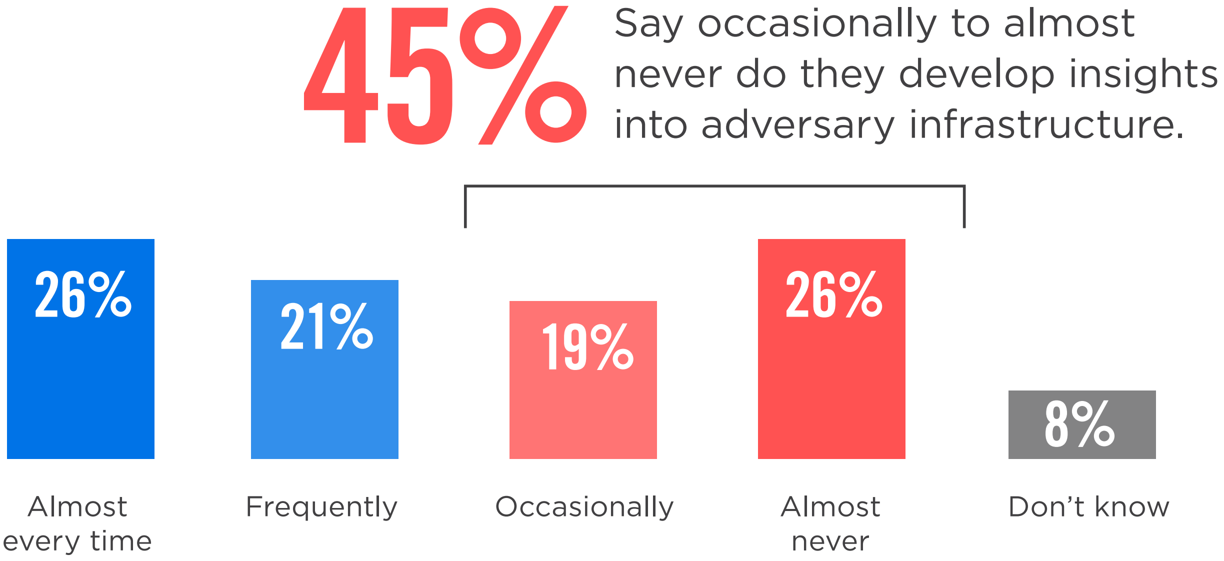
58%
DNS traffic

Threat intelligence sources 57% | 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%

INSIGHTS INTO ADVERSARIES

About a quater of security teams say they almost never evaluate adversary domains and IP addresses to develop insights into adversary infrastructure (26%) and 19% say it happens occasionally as part of their threat hunting process.

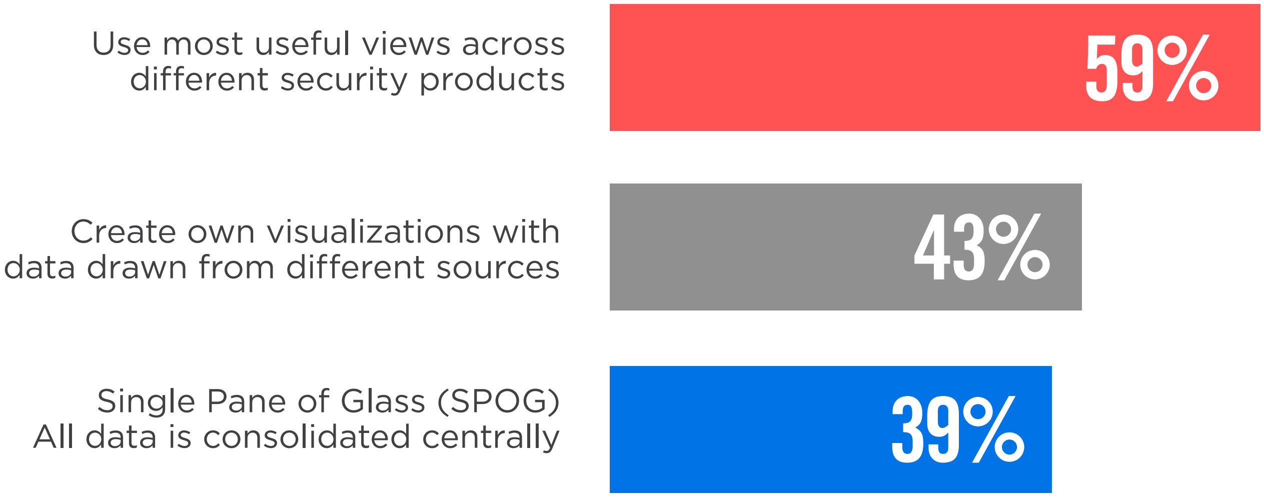
How often do you develop insights into adversary infrastructure (domains and IP addresses) as part of your hunt activities?



SOC ANALYSIS TOOLS

Fifty-nine percent of SOCs use the most useful views across different products and 43% create their own visualizations with data drawn from different sources.

▶ How does your SOC currently operate in terms of views and analysis?



Other 7%

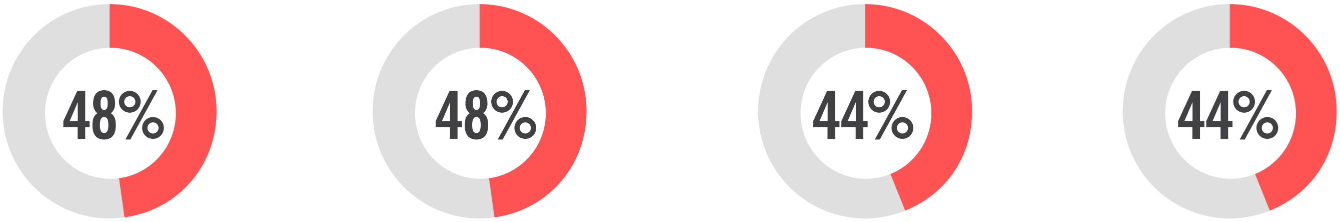
KEY HUNTING TECHNOLOGY CAPABILITIES

The most important capability that cybersecurity professionals consider critical to the effectiveness of their threat hunting solution 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 technology?

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

Machine learning and automated analytics 38% | Automated workflows 37% | Vulnerability scanning 37% | Intuitive data visualization 29% | Combined visibility across hybrid cloud and on-premises environments 27% | Other 2%

BENEFITS OF THREAT HUNTING AUTOMATION

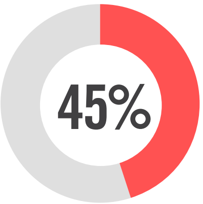
Threat hunting solutions provide security analysts with powerful tools to enable earlier detection, reduce dwell time, and improve defenses against future attacks. The top benefits organizations derive from threat hunting platforms include improved detection of advanced threats (63%), followed by reduced investigation time (55%), and saving time manually correlating events (47%).

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

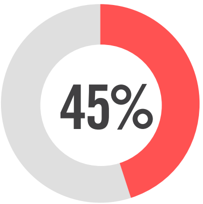
63%
Improving detection of advanced threats

55%
Reducing investigation time

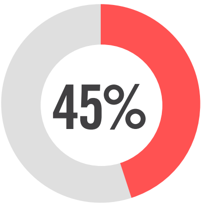
47%
Saving time manually correlating events



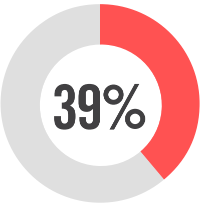
Reducing time wasted on chasing false leads



Reducing attack surface



Discovering threats that could not be discovered otherwise



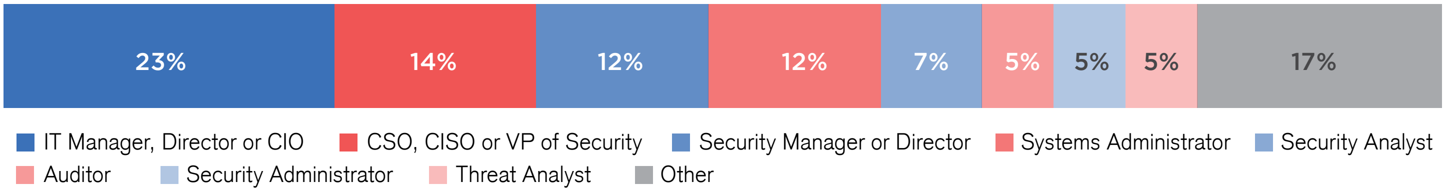
Connecting disparate sources of information

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%

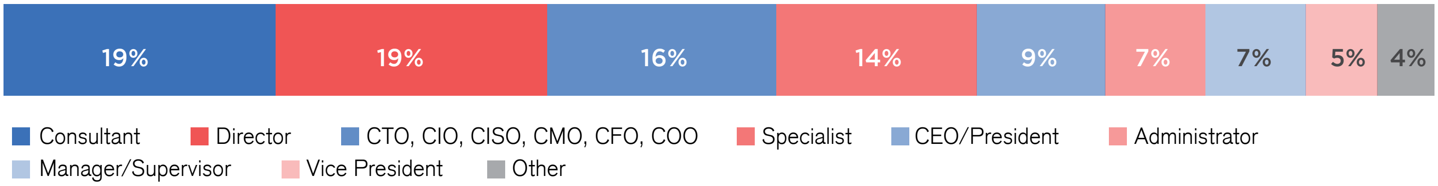
METHODOLOGY & DEMOGRAPHICS

The Importance of Threat Hunting Automation for XDR Report is based on the results of a comprehensive online survey of cybersecurity professionals, conducted in August 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.

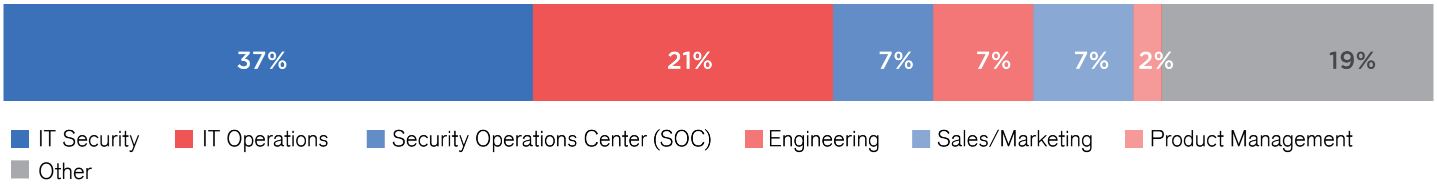
PRIMARY ROLE



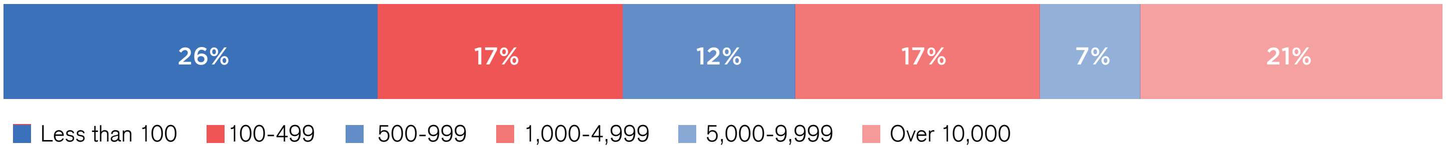
CAREER LEVEL



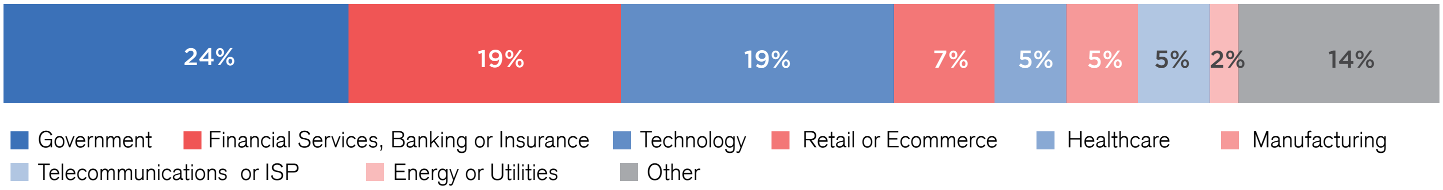
DEPARTMENT



COMPANY SIZE



INDUSTRY



Hunters.

Hunters delivers the industry's first open XDR to automate expert threat hunting techniques for context-rich data connections. Hunters.AI, the company's platform autonomously searches for attack techniques and detects cyber threats that bypass existing controls, across surfaces. It ingests raw data and rich security telemetry from a wide array of data sources and IT environments like cloud, endpoint, and network, and enriches threat signals with unique tactics, techniques and procedure-based (TTP) attack intelligence. It then applies ML and cloud-based analytics to correlate threat patterns, and provide high fidelity attack stories for cybersecurity team response.

hunters.ai