Cybersecurity
INSIDERS

# The State of Threat Hunting

Intrusion

# INTRODUCTION

As many SOCs struggle 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.

Cybersecurity Insiders conducted the fifth annual threat hunting research project to gain deeper insights into the state and evolution of this security practice.

### Key findings include:

- The top challenge facing SOC teams is detecting advanced threats, yet only 10% of practitioners feel "very confident" in their organization's ability to uncover them.
- Thirty-five percent of SOC teams report the frequency of threats is increasing at a rate of 2×, and an estimated 38% of threats are missed.
- A third of security practitioners (34%) are unsure about the financial impact a breach would have on their organization.
- Nearly half of respondents (46%) don't have a way to determine where to focus their threat hunting efforts, and nearly a quarter (24%) don't have a way of determining which assets are the most critical.
- The top 3 most important threat hunting tool capabilities are threat intelligence (62%), automatic detection (57%), and integration and normalization of multiple data sources (47%).

We would like to thank Intrusion for supporting this important research. We hope you find this report informative and helpful as you continue your efforts to protect your organizations against evolving cyber threats.

Thank you,

Holger Schulze

**Holger Schulze**
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

# SOC CHALLENGES

Cybersecurity professionals are facing increasing challenges due to a worsening threat environment and limited resources to effectively protect their IT environment. Fifty-two percent of cybersecurity professionals consider detection of advanced threats to be the top challenge facing their SOC. Lack of expert security staff to assist with threat mitigation is a close second (47%), followed by too much time wasted on false positive alerts (40%).

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

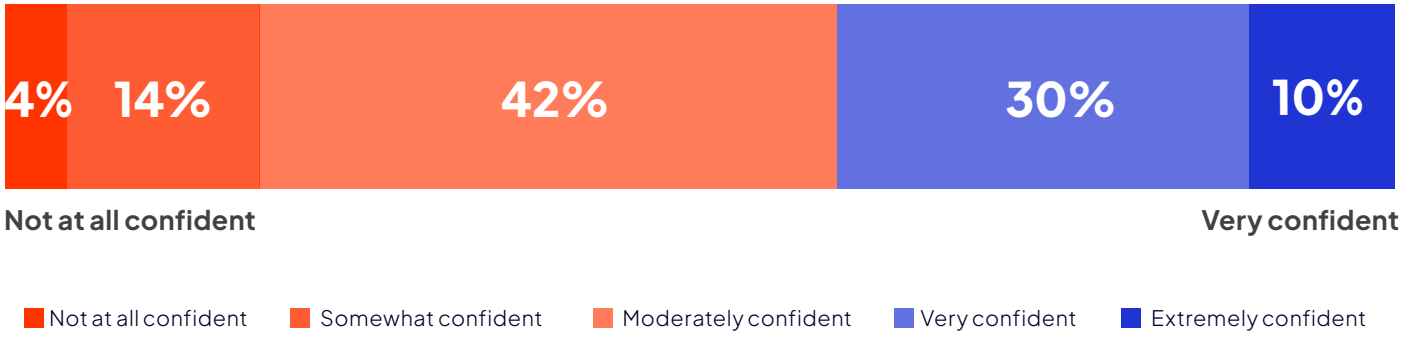

Lack of visibility into critical data due to encryption 28% | Lack of proper reporting tools 26% | Working with outdated SIEM tools and SOC infrastructure 22% | Other 7%

# CONFIDENCE IN ABILITY

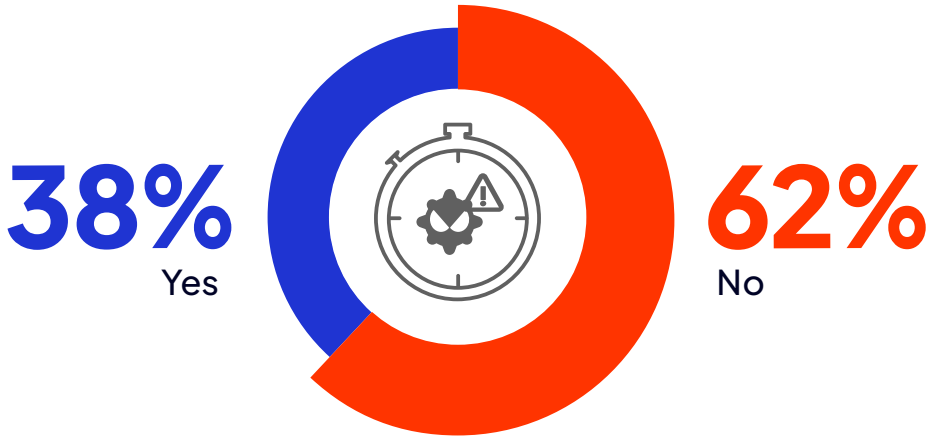
It is essential that cybersecurity teams have the skills and tools to detect a variety of different threats. Sixty percent of respondents are at most only moderately confident in their team's ability to uncover advanced threats. Additionally, 62% of cybersecurity professionals feel their SOC does not spend enough time searching for advanced threats.

### How confident are you in your security team's ability to uncover advanced threats?

**60%** of respondents are at most moderately confident in their security team's ability to uncover advanced threats




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

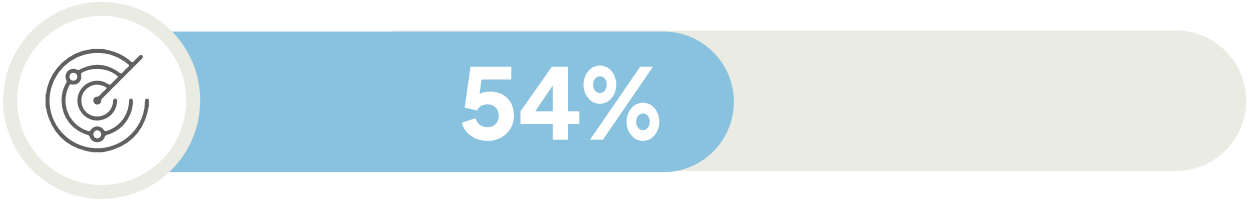


# VULNERABLE ASSETS

It is critical for cyber teams to focus scarce resources on vulnerable assets and identify where to target threat hunting efforts. A majority of organizations (76%) say they can determine which of their assets are most likely to be attacked; however, only 54% of organizations can effectively determine where to focus their threat hunting efforts.

**Do you have a mechanism for identifying vulnerable assets?**


We can determine which assets are most critical (likely to be attacked)

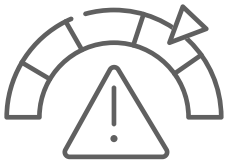



We can determine where to focus our threat hunting efforts

# RISING THREAT LEVELS

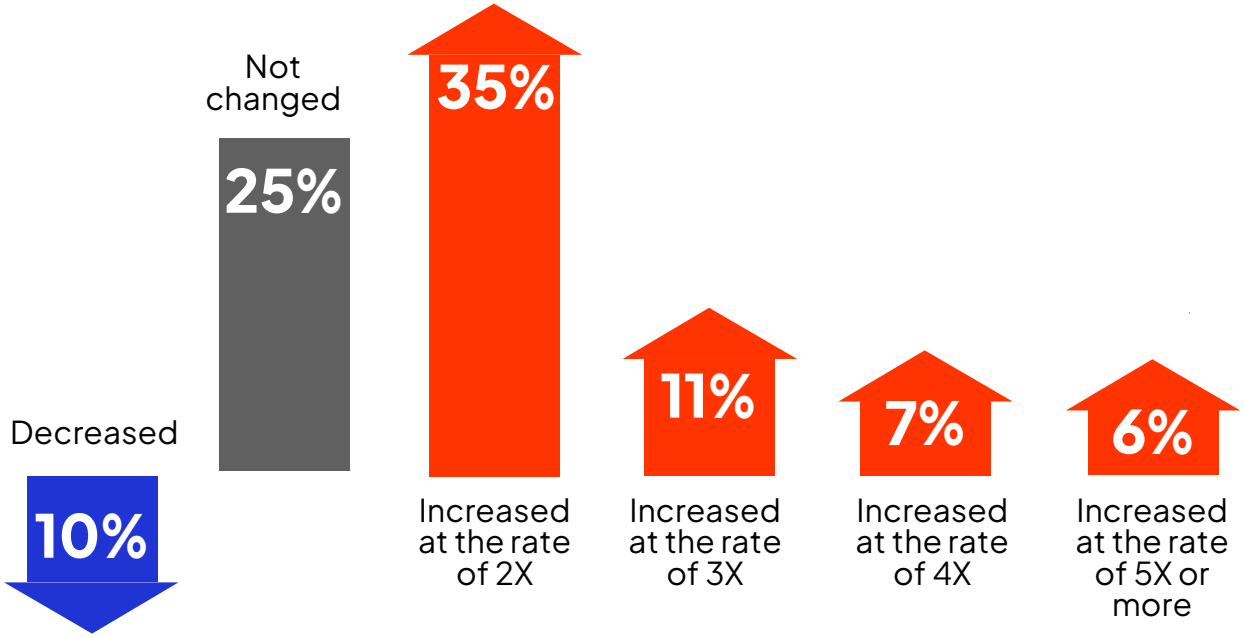
In addition to a rise in the complexity and sophistication of cyber attacks, the number of threats facing cybersecurity teams is increasing as well. Over half of organizations (59%) observed an increase in threats by a factor of two or higher compared to the previous year.

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



**59%**

**of organizations report an increase in the frequency of security threats during the past year**




Other 6%

# SECURITY THREATS MISSED

Many organizations in our survey are responding to attacks only after they have become active. This reactive posture partly contributes to more than a third (38%) of security threats being missed and remaining undetected.

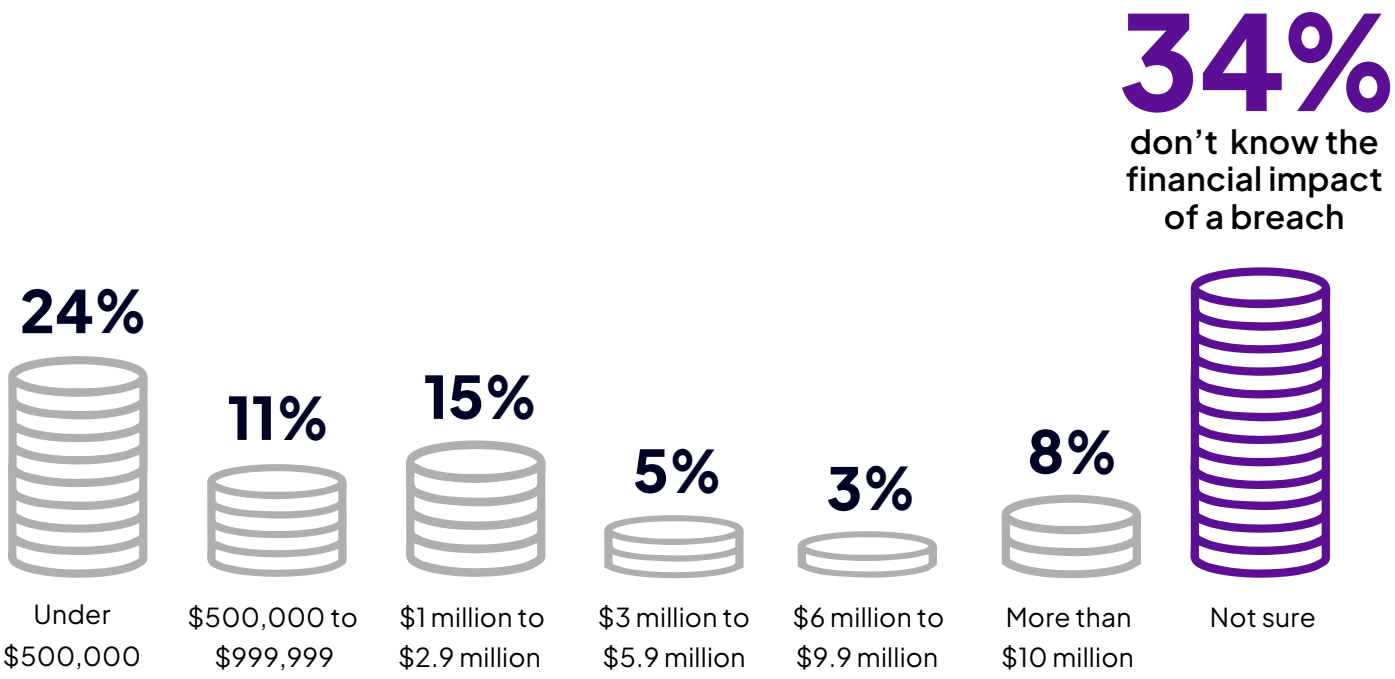
**In a typical week at your SOC, what percentage of security threats do you think are missed?**

**38%** of security threats are missed (on average)

# FINANCIAL IMPACT

The financial impact of a security breach can be detrimental to an organization; however, interestingly, 34% do not know the impact of a breach. Almost a third of cybersecurity professionals (31%) estimate that the impact of an undetected breach is $1M or more. Eight percent of organizations estimate the financial impact is over $10M.

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



# THREAT HUNTING GOALS

Organizations highlight a broad range of goals for their threat hunting program. Reducing exposure to internal threats was named by more than half of the organizations (53%). This is followed by improving the speed and accuracy of threat response (50%) and reducing the attack surface (46%).

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

**53%**
Reduce exposure to internal threats

**50%**
Improve speed and accuracy of threat response

**46%**
Reduce attack surface

**45%**
Reduce number of breaches and infections

**44%**
Reduce time to containment (prevent spread)

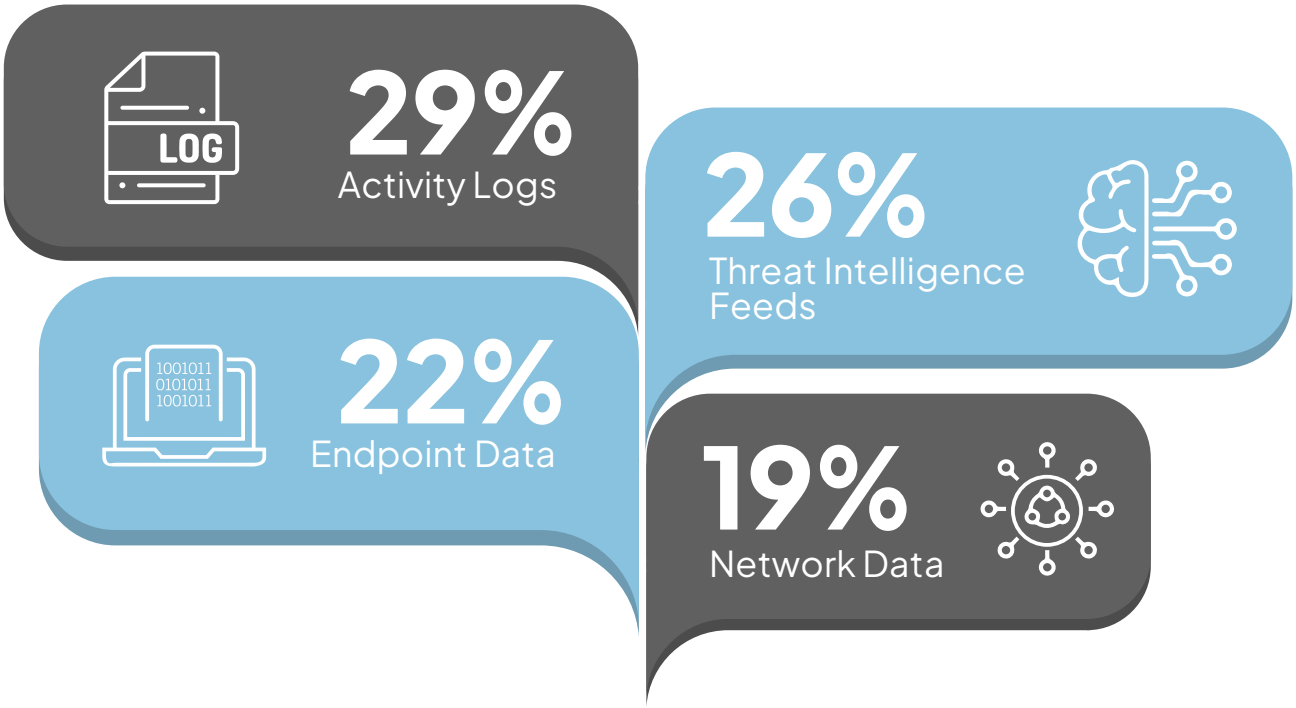

**42%**
Reduce exposure to internal threats

Reduce dwell time from infection to detection 41% | Optimize resources spent on threat response 35% | Other 5%

# VALUABLE DATA SOURCES

Activity logs (29%) and threat intelligence feeds (26%) lead the list of most valuable data sources for investigating known threats. Given the shift to remote work, endpoint data is also high on the list of valuable data sources (22%).

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

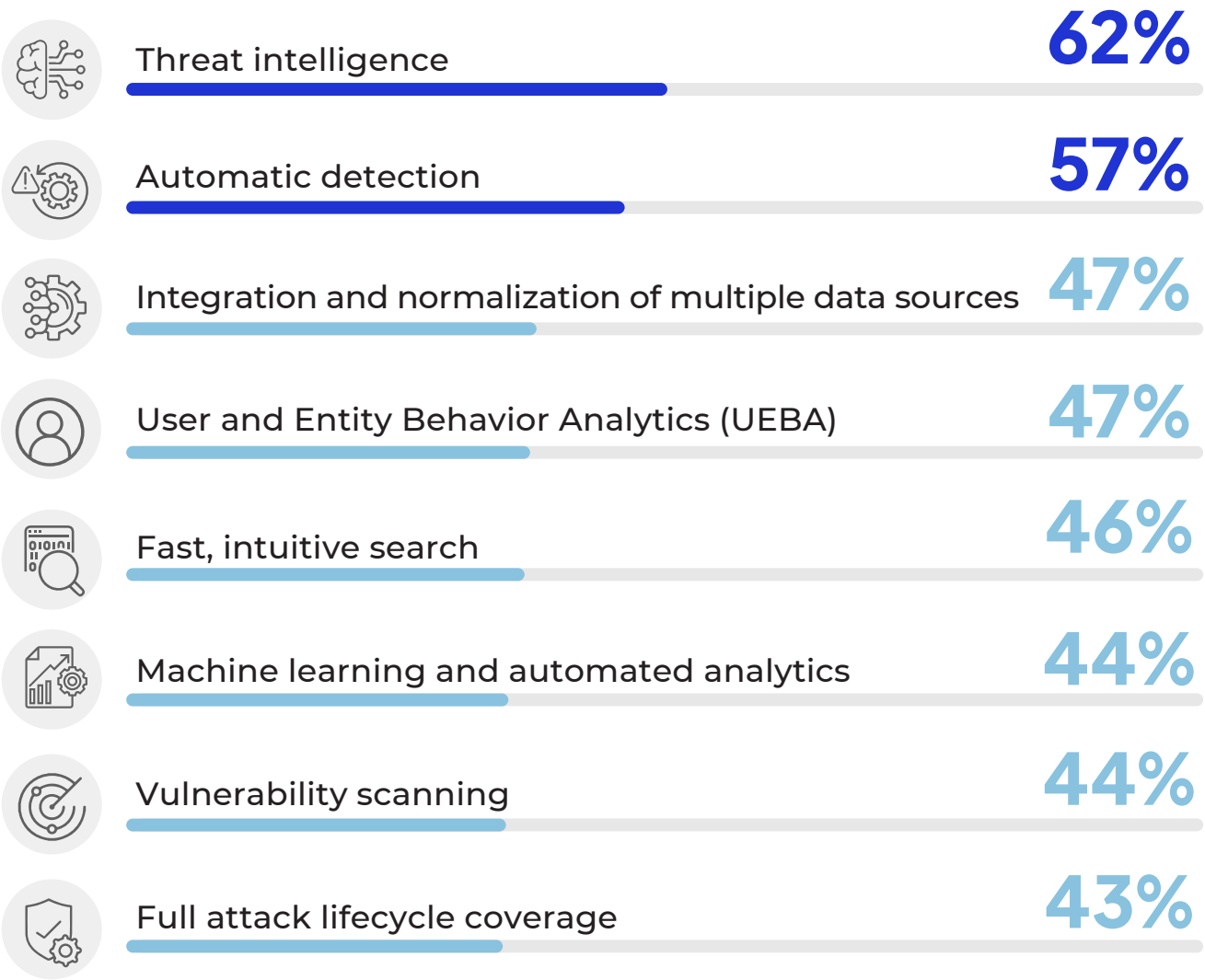



Other 4%

# THREAT HUNTING TOOLS

There is a diverse portfolio of technology tools for threat hunting. Threat intelligence is the most critical capability to have (62%), along with automatic threat detection (57%).

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

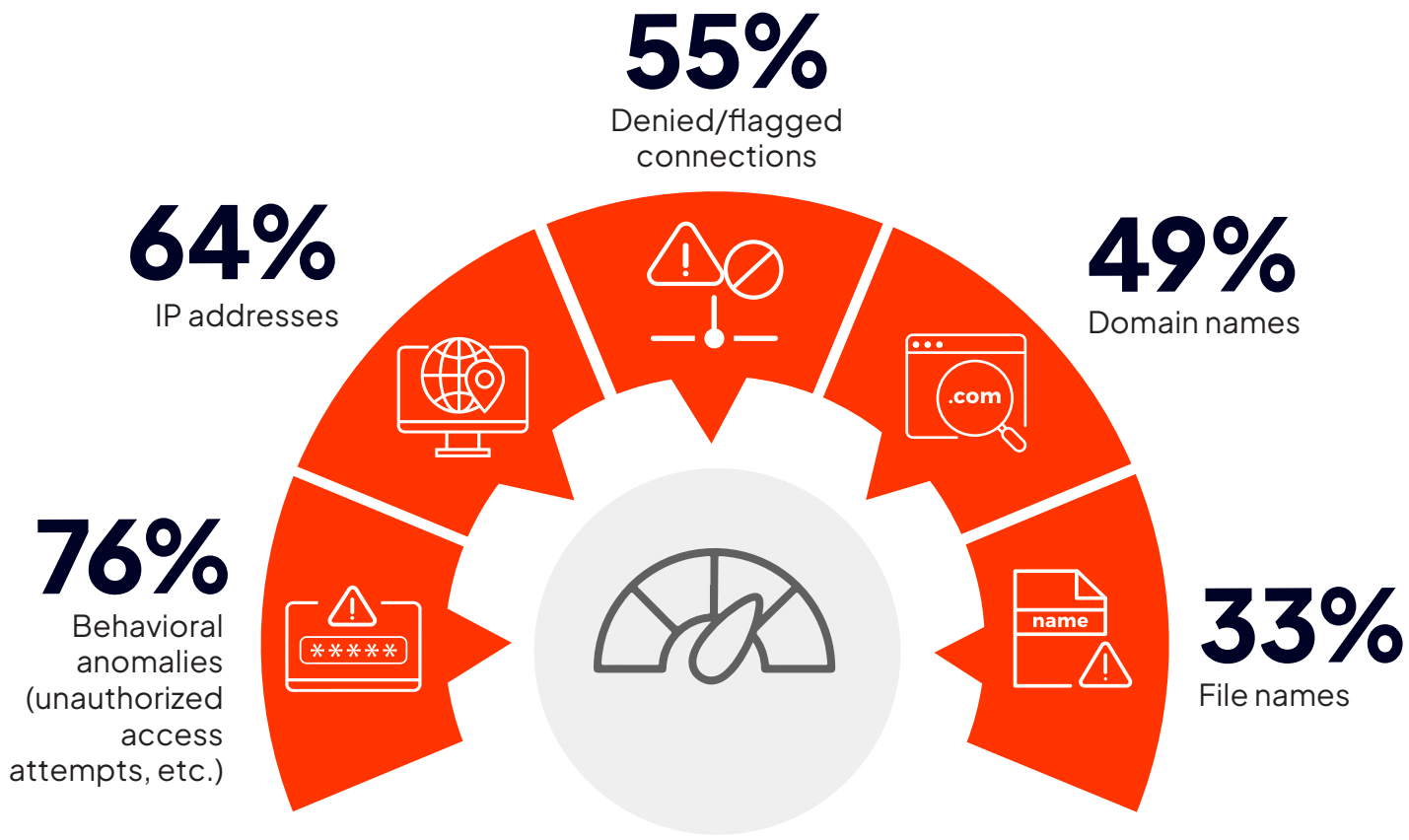



Intuitive data visualization 39% | Automated workflows 38% | Combined visibility across hybrid cloud and on-premises environments 30% | Other 2%

# THREAT INDICATORS

We asked threat hunters what threat indicators they most frequently investigate as part of their daily missions. The most common threat is behavioral anomalies (76%), followed by suspicious IP addresses (64%) and denied/flagged connections (55%).

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

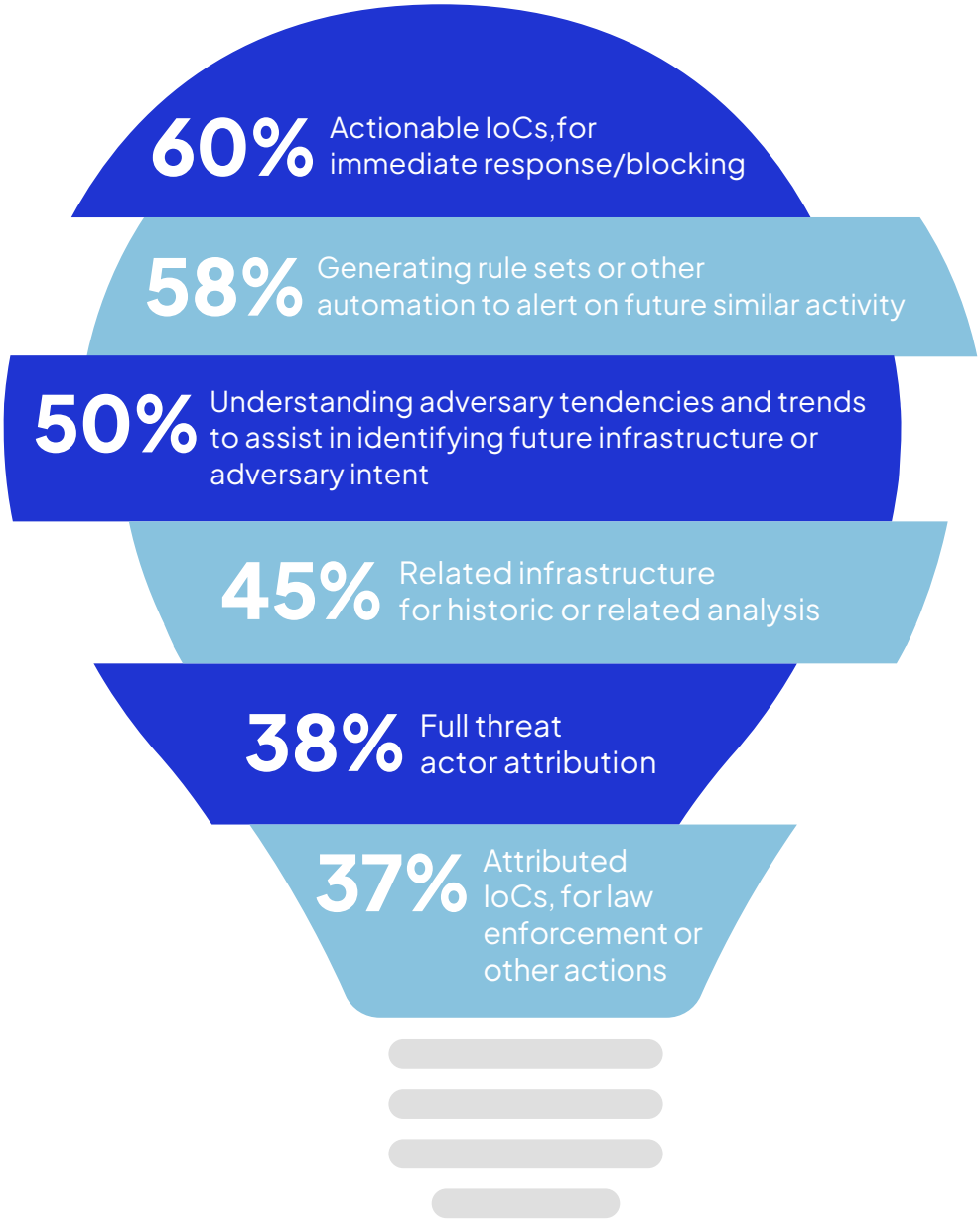



Not sure/other 9%

# INSIGHTS INTO ADVERSARIES

Threat hunting can provide valuable insights into adversary infrastructure and allow organizations to become more proactive. Through threat hunting, 60% of organizations in our survey identify actionable indicators of compromise while 58% generate rule sets or alert automations on future similar activity. Fifty 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?**

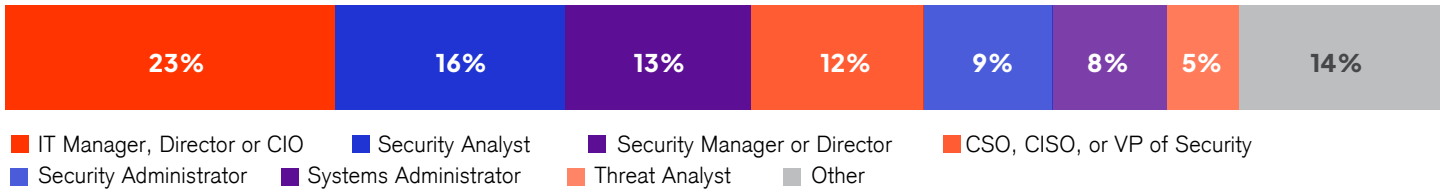



Other 2%

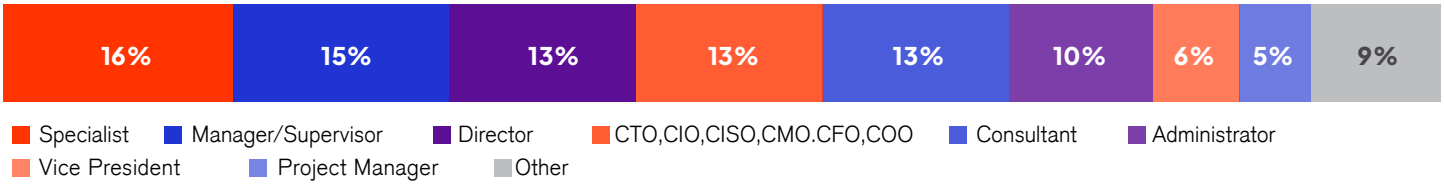
# METHODOLOGY & DEMOGRAPHICS

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

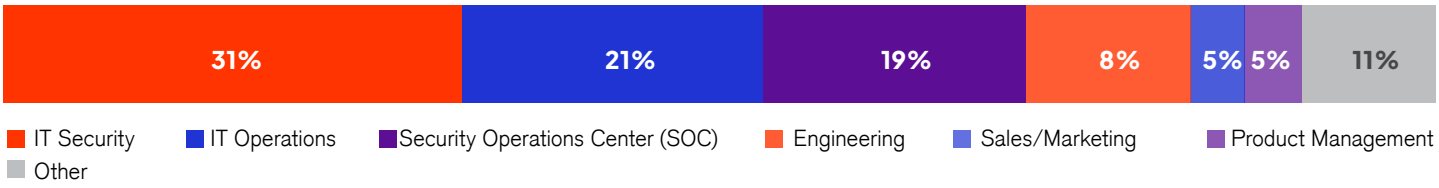
## PRIMARY ROLE



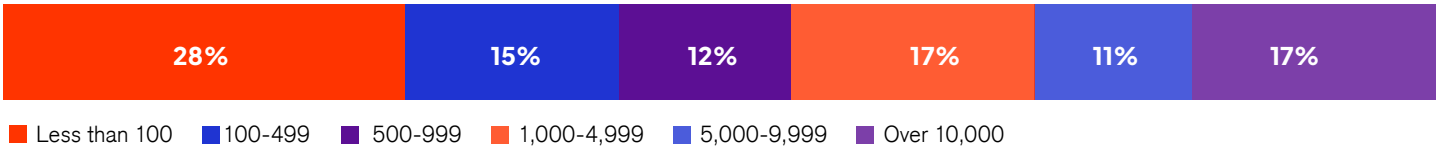

## CAREER LEVEL



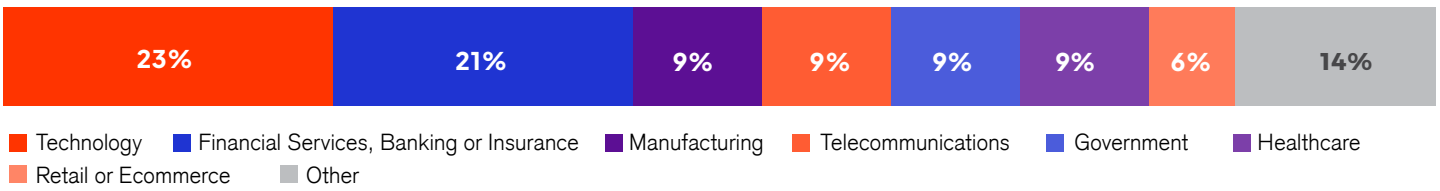

## DEPARTMENT




## COMPANY SIZE




## INDUSTRY




Intrusion combines network visibility, advanced threat intelligence, and automated detection and response to help security teams know what threats are active in their environment while staying protected. The Intrusion Global Threat Engine powers everything we do and contains historical data, known associations and reputation intelligence of over 3 trillion IPs, domains, and hostnames. Our threat hunting device, Intrusion Shield, observes traffic flow and instantly blocks known malicious or unknown connections from both entering or exiting your network, making it an extremely effective solutions for preventing Zero-Day and ransomware attacks.

**See the unseen and know the unknown with Intrusion.**

# 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**


**GET THE MEDIA KIT**
**or contact us for more details at:**
**info@cybersecurity-insiders.com**